



DoD PKI

Automatic Key Recovery

Philip Noble

(520) 538-7608 or DSN 879-7608,

philip.e.noble.civ@mail.mil

U.S. Army Information Systems Engineering Command

Fort Huachuca, AZ 85613-5300

22 Mar 13



The Problem:

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 Solution:

Steps to Recover Private Encryption Keys

The following slides identify steps to recover private encryption keys, escrowed by DISA, from CACs that do not have the “Auto Key Recovery” functionality.



URL for Key Recovery

<https://ara-1.c3pki.chamb.disa.mil/ara/Key>

Or

<https://ara-2.c3pki.den.disa.mil/ara/Key>

This is the Automatic Key Recovery URL.

Note: The URL address shown above is 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

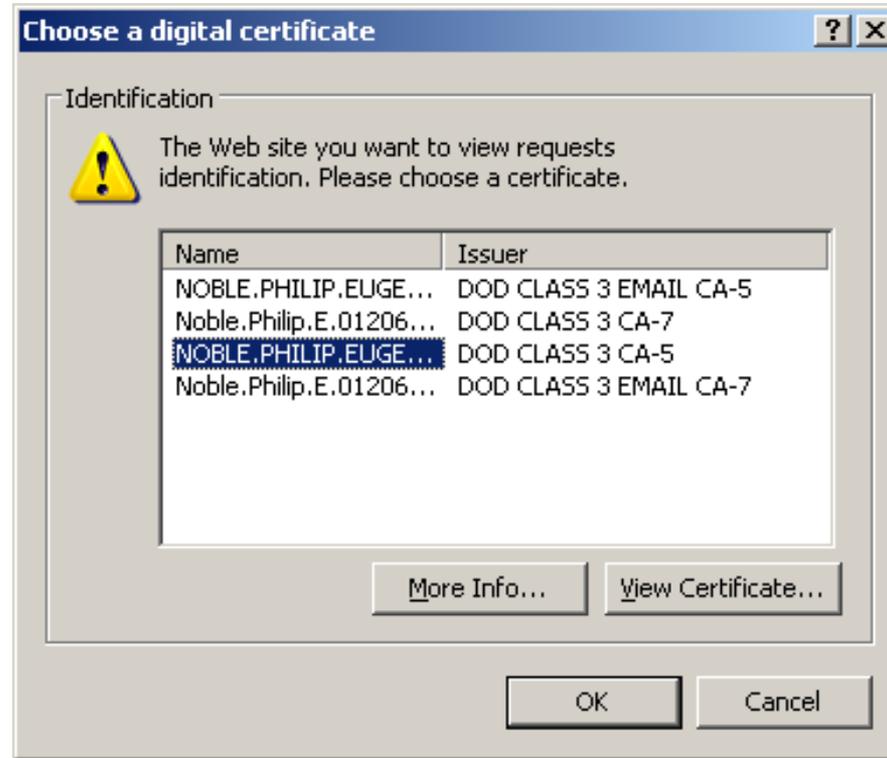
<https://ara-1.c3pki.chamb.disa.mil/ara/Key>

Or

<https://ara-2.c3pki.den.disa.mil/ara/Key>



Choose Your CAC Identity Certificate



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.



Warning Banner

Cannot find server - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <https://ara-1.c3pki.chamb.disa.mil/ara/Key>

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

Automated Key Recovery
For Official Use Only

Please Wait.

The Automated Key Recovery Agent is gathering information.
This process can take several minutes.
Please do not hit the "Back" button during this process.
If the list does not appear within one minute, please contact your system administrator.

Logon

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

100 Items, 1 Unread

Start | Inbox - Microsoft Outlook | The Automated Key Rec... | Cannot find server - ... | 9:47 AM

Dismiss the warning by clicking "OK".

ISEC: Excellence in Engineering



Processing Your Request



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

File Edit View Favorites Tools Help

Address <https://ara-1.c3pki.chamb.disa.mil/ara/Key>

 **DEFENSE INFORMATION SYSTEMS AGENCY**
Global Net-Centric Solutions - The Warrior'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](#)

The Automated Key Recovery Agent will compile a list of Recoverable Keys. Should recovery fail or if the key is unable to be downloaded automatically, contact the Army Key Recovery Agent by sending a signed email to: army.ra@us.army.mil requesting recovery of your private email encryption Key. **Please Wait...**



Key Selection



Auto Key Recovery - Recoverable Key List - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <https://ara-1.c3pki.chamb.disa.mil/ara/Key?value=96287>

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

Automated Key Recovery
For Official Use Only

The following Encryption Keys can be recovered:

Common Name:	NOBLE.PHILIP.EUGENE.1184204718	<input type="button" value="Recover"/>
Organization Affiliation:	USA	
Not Before:	2002-04-29 00:00:00 GMT	
Not After:	2005-04-28 00:00:00 GMT	
Email:	philip.noble@us.army.mil	
Issuer:	DOD CLASS 3 EMAIL CA-4	
Serial #	0x05DCF3	
Revocation Status:	REVOKED	

Common Name:	NOBLE.PHILIP.EUGENE.1184204718	<input type="button" value="Recover"/>
Organization Affiliation:	USA	
Not Before:	2004-01-28 00:00:00 GMT	
Not After:	2007-01-27 00:00:00 GMT	
Email:	philip.noble@us.army.mil	
Issuer:	DOD CLASS 3 EMAIL CA-5	
Serial #	0x0DD98B	

Common Name:	NOBLE.PHILIP.EUGENE.1184204718	<input type="button" value="Recover"/>
Organization Affiliation:	USA	
Not Before:	2003-08-18 00:00:00 GMT	
Not After:	2004-02-02 00:00:00 GMT	
Email:	philip.noble@us.army.mil	
Issuer:	DOD CLASS 3 EMAIL CA-5	

Browse through the list and locate the appropriate key you want to recover. When located, click the adjacent associated “Recover” button.



Acknowledgement of DoD Subscriber



Select “OK”.



Processing Request



Auto Key Recovery - Recovering Key - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Recycle Bin Print Mail Internet Options

Address <https://ara-1.c3pki.chamb.disa.mil/ara/Key?recoverKey=4> Go Links >>

 **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](#)

**The Automated Key Recovery Agent is processing your request.
Please Wait...**

ISEC: Excellence in Engineering



One-time PIN



Auto Key Recovery - Recovered Key - Microsoft Internet Explorer

File Edit View Favorites Tools Help

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

DEFENSE INFORMATION SYSTEMS AGENCY
Global Net-Centric Solutions - The Warrior'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:

[DOWNLOAD](#)
[NOBLE.PHILIP.EUGENE.1184204718_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

[Back to List](#)

[Logout](#)

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

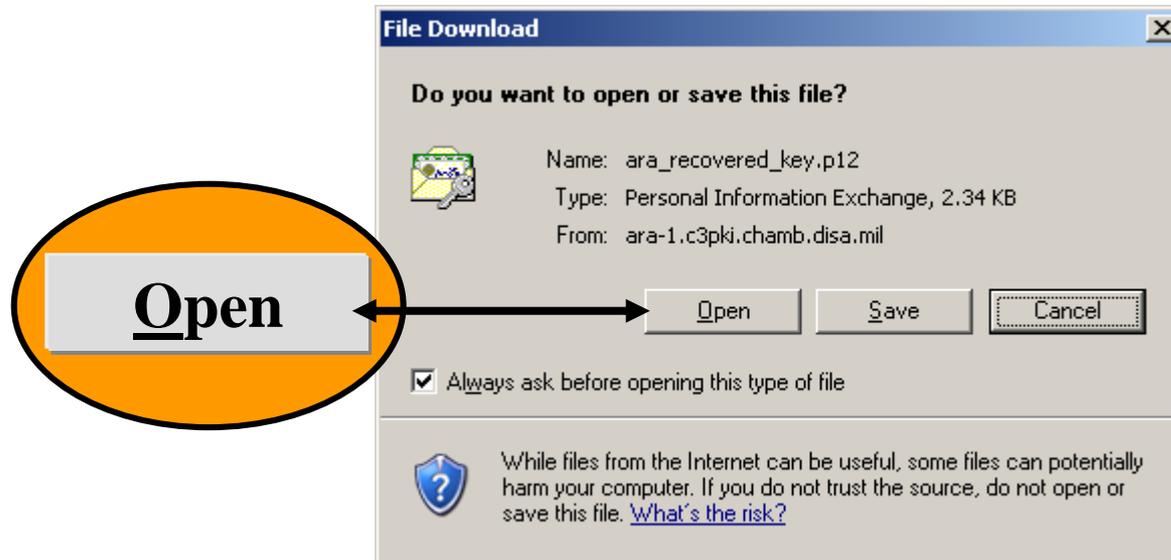
- 1) The Recovered Key will be automatically presented to your browser. You can choose to either save the key to your file system, or open it. If you choose to save it, you can later import the key to your browser using the toolbar 'Tools->Internet Options', select the 'Content' tab and 'Certificates' 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 Trusted sites

Also, you will find instructions for both Netscape and Internet Explorer web browsers.



Installing the Certificate



You will be given the opportunity to install the certificate, click “Open”.



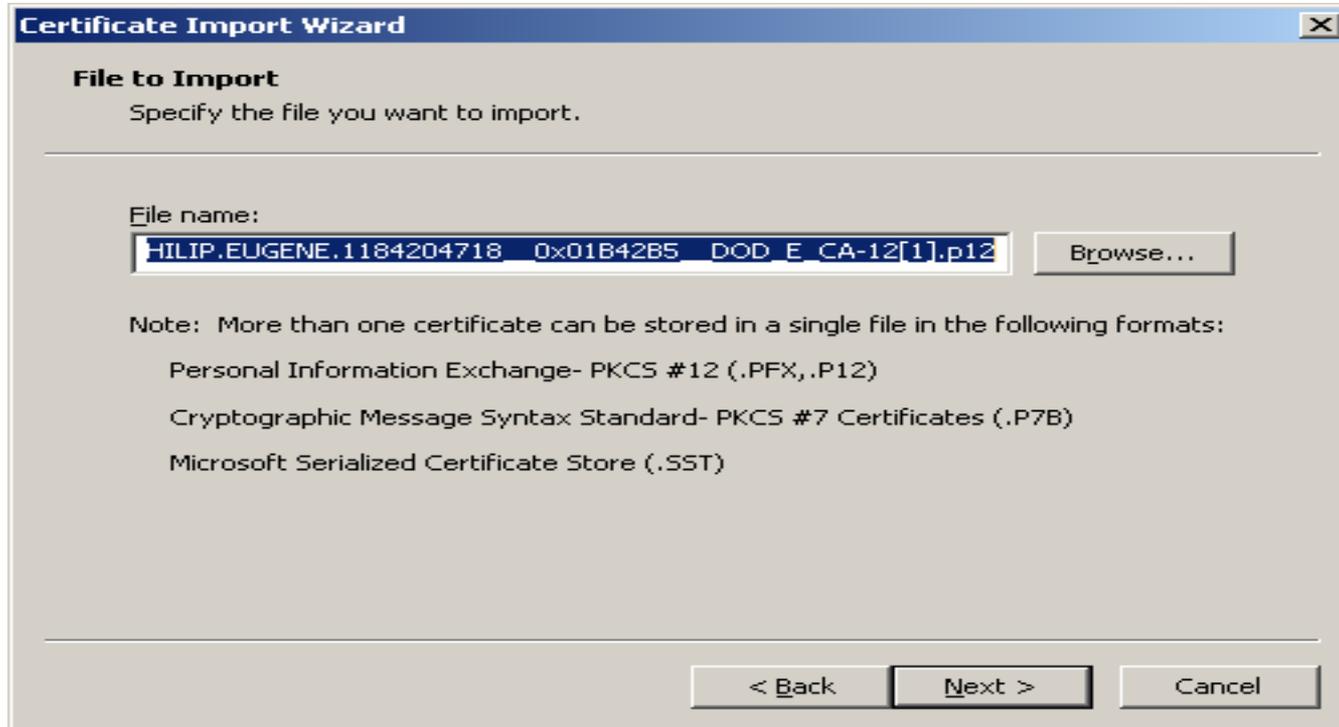
Installing the Certificate (Cont'd)



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.

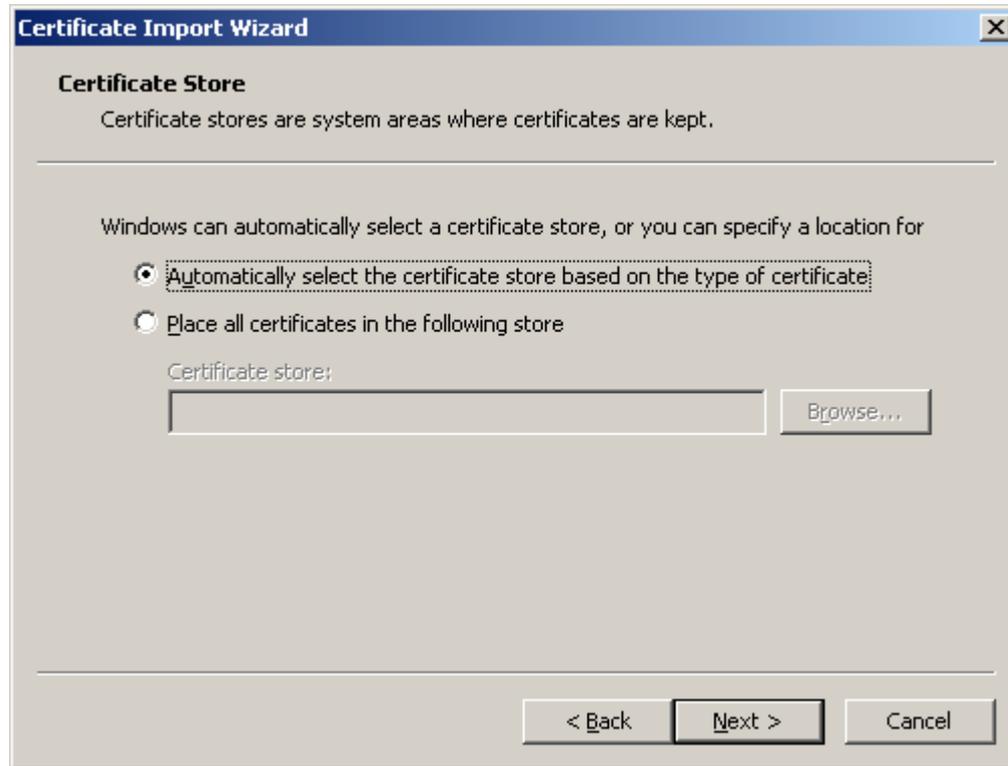
Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

< Back Next > Cancel

Leave the check blocks unchecked, enter your Password, and click “Next”.



Installing the Certificate (Cont'd)



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”**.



Installing the Certificate (Cont'd)



Click “OK”



Installing the Certificate (Cont'd)



Click “OK”.



Medium Security is Not a Choice



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

<http://blogs.technet.com/b/pki/archive/2009/06/17/what-is-a-strong-key-protection-in-windows.aspx>

Use gpedit.msc:

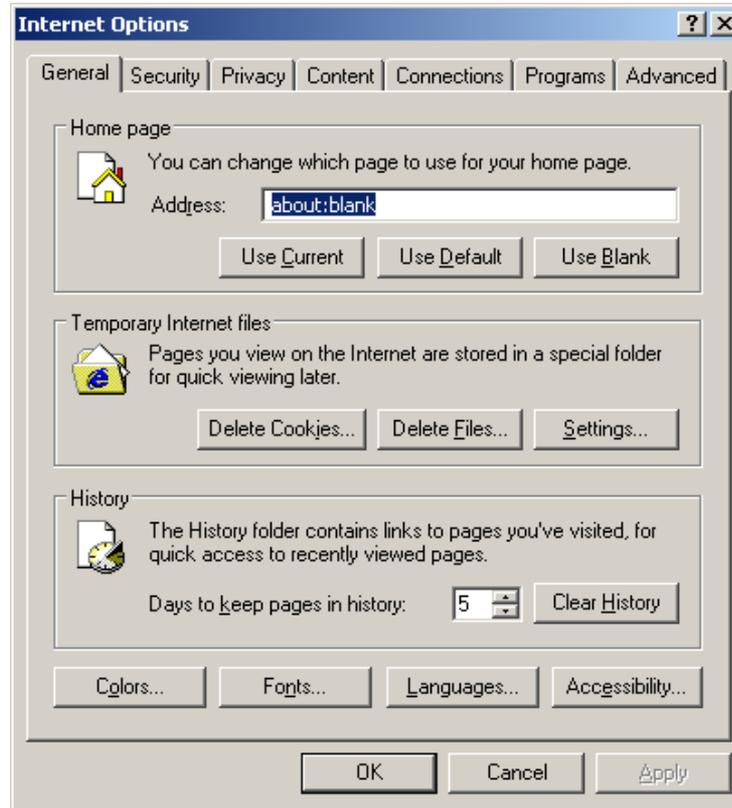
- Local computer policy
 - Windows settings
 - Security settings
 - Local policies
 - Security options

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**



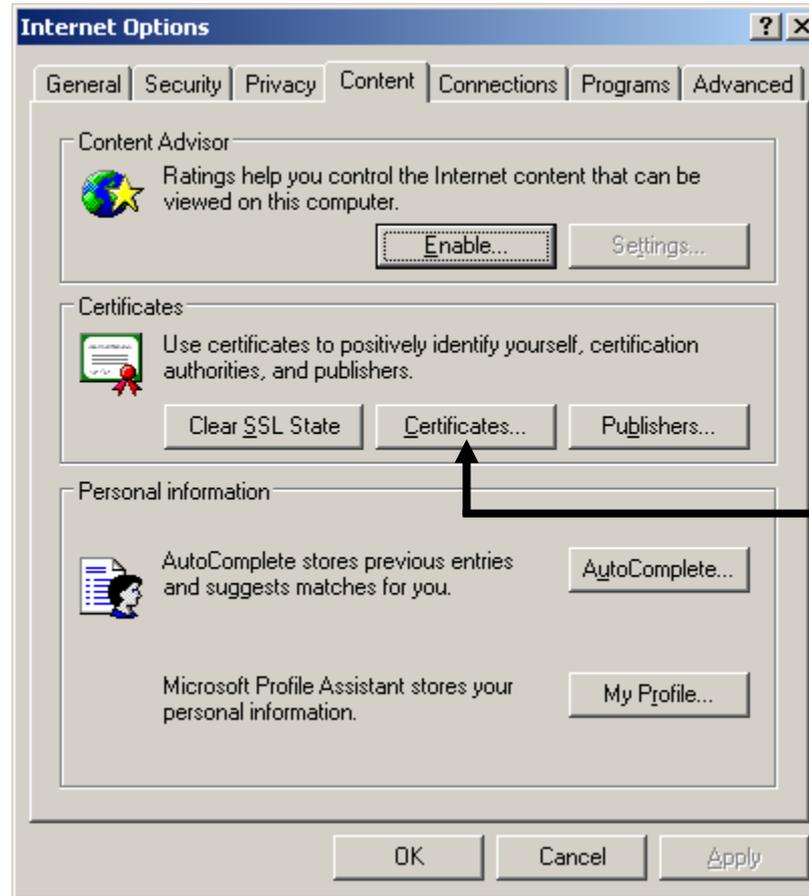
Verifying the Download



You can verify the successful download of your recovered Private Encryption Key by performing the following; Launch Internet Explorer, select “Tools” from the menu, and then “Internet Options”.



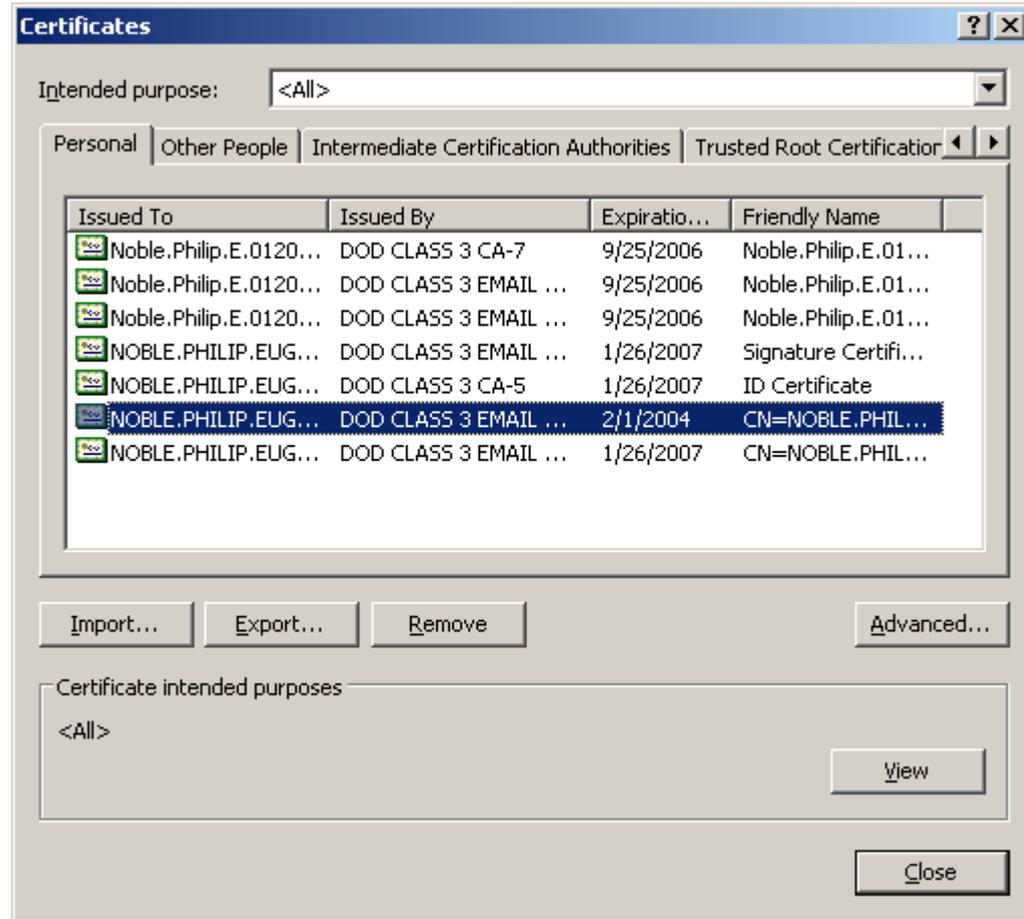
Verifying the Download (Cont'd)



Click the “Content” tab. Now, click “Certificates”.



Verifying the Download (Cont'd)



Select the “Personal” tab and you will see a list of your currently registered certificates, including the recovered new key certificate.



Verifying the Download (Cont'd)



Double-click on the certificate and you can view the specifics of your recovered key (or other current keys) as illustrated above.



Success



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

Last Step: Delete the .P12 file from your computer as this is a security vulnerability and will be detected in a Q-tip Scan

Should recovery fail, contact the Army Key Recovery Agent by sending a signed email to:
Netcom-9sc.registration.authority@mail.mil
requesting recovery of your private email encryption key



Recovery Notification 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.EUGENE.1184204718,OU=USA,OU=PKI,OU=DOD,OU=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,OU=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 (IASSED)

DSN 879-7608

CML 520-538-7608

FAX DSN 879-8709 CML 520-538-8709

philip.e.noble.civ@mail.mil

philip.noble@us.army.smil.mil

philip.noble@conus.army.smil.mil