



DoD PKI Automatic Key Recovery

Philip Noble (520) 538-7608 or DSN 879-7608, philip.noble@us.army.mil U.S. Army Information Systems Engineering Command Fort Huachuca, AZ 85613-5300



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.







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: <u>The URL address shown above is case sensitive</u>.

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

Choose a	digital certificate		? X
Identific	ation		
⚠	The Web site you want to identification. Please choo	o view requests ose a certificate.	
	Name	Issuer	
	NOBLE.PHILIP.EUGE Noble.Philip.E.01206 NOBLE.PHILIP.EUGE Noble.Philip.E.01206	DOD CLASS 3 EMAIL CA-5 DOD CLASS 3 CA-7 DOD CLASS 3 CA-5 DOD CLASS 3 EMAIL CA-7	
	<u>M</u> o	re Info <u>V</u> iew Certificate	
		OK Cano	:el

You will be prompted to identify yourself.

Highlight <u>your</u> 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





Dismiss the warning by clicking "OK".

Processing Your Request



The Automated Key Recovery Agent will compile a list of Recoverable Keys. Please Wait...

Key Selection



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



Microsoft	Internet Explorer	×
2	I acknowledge that I am the DoD subscriber for this escrowed key. I acknowledge the receipt of this recovered key. Per DOD FORM 2842, I agree to use this key for authorized purposes on to protect it from use by others, and to destroy it when no longer needed	ly, i.

Select "OK".



Processing Request



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



One-time PIN



Iso, you will find instructions for both Netscape an Internet Explorer web browsers.







Installing the Certificate





You will be given the opportunity to install the certificate, click "<u>Open</u>".



Certificate Import Wizard

		с.	
		•	
4	_	_	

Tour I	Welcome to the Certificate Import Wizard
	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. To continue, click Next.
	< Back (Next > Cancel

Click "<u>N</u>ext".





e to Import			
Specify the file you wa	nt to import.		
<u>File name:</u>			
HILIP.EUGENE.11842	04718_0×01B42B5_	_DOD_E_CA-12[1].p12	B <u>r</u> owse
Note: More than one o	ertificate can be stor	ed in a single file in the f	ollowing formats
Personal Information	n Exchange- PKCS #1	12 (.PFX,.P12)	
Cryptographic Mess	age Syntax Standard	- PKCS #7 Certificates (.P7B)
Microsoft Serialized	Certificate Store (.SS	it)	
		< Back Next	> Car

Click "<u>N</u>ext".





cincute .		
Passwo	rd	
To m	aintain security, the private key was protected with a password.	
Туре	the password for the private key.	
<u>P</u>	assword:	
4	*****	
R	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 Nevt > Cance	1

Leave the check blocks unchecked, enter your Password, and click "<u>N</u>ext".



erti	ficate Store ertificate chores are system areas where certificates are kent	
_	ercificate stores are system areas where tercificates are rept.	
۷	/indows can automatically select a certificate store, or you can speci	fy a location fo
	Automatically select the certificate store based on the type of a select the certificate store based on the certificate st	certificate
	C Place all certificates in the following store	
	Certificate store:	
		Browse
	,	
	cond. Nuclea	
	< <u>B</u> ack <u>N</u> ext >	> Ca

Ensure that *"Automatically select the certificate store based on the type of certificate"* is selected (as shown above) and click *"Next"*.





×

Certificate Import Wizard

Completing the (Wizard	Certificate Import	
You have successfully completed the Certificate Import wizard.		
You have specified the follow	wing settings:	
Certificate Store Selected	Automatically determined by t	
File Name	D:\Documents and Settings\p	
•		
< <u>B</u> ack	Finish Cancel	

Click "Finish".





×

Importing a new private exchange key

An application is creating a Protected item.
CryptoAPI Private Key
Security level set to Medium <u>Set Security Level</u>
OK Cancel <u>D</u> etails

Click "Set Security Level"





Importing a new private exchange key × Choose a security level appropriate for this item. High œ Request my permission with a password when this item is to be used. Medium Request my permission when this item is to be used. < Back Next > Cancel

Select "High" and "Next"





×

mporting a new	private exchange kev
inporting a nem	prinate energiange ner

Create a password to protect this item.
Create a new password for this item. Password for: CryptoAPI Private Key Password: ••••• Confirm: •••••
 < Back <u>F</u> inish Cancel

Enter Your CAC PIN as a Password and Click "Finish"

Note Vista requires a 14 character password for this step



Importing a ne	w private exchange key	×
	An application is creating a Protected item.	
	CryptoAPI Private Key	
	Security level set to High Set <u>Security Level</u>	
	OK Cancel <u>D</u> etails	

Click "OK"







Click "OK".



Verifying the Download



Internet Options					
General Security Privacy Content Connections Programs Advanced					
Home page					
You can change which page to use for your home page.					
- Address: <u>should stank</u>					
Temporary Internet files					
for quick viewing later.					
Delete Cookjes Delete Files Settings					
History					
The History folder contains links to pages you've visited, for quick access to recently viewed pages.					
Days to keep pages in history: 5 😴 Clear History					
OK Cancel Apply					

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)



(nternet C	options	?×
General	Security Privacy Content Connections Programs Adva	anced
Conte	nt Advisor	[]
	Ratings help you control the Internet content that can be viewed on this computer.	
	Enable Settings	
Certifi	cates	
	Use certificates to positively identify yourself, certification authorities, and publishers.	
	Clear <u>S</u> SL State <u>C</u> ertificates Pu <u>b</u> lishers	
Perso	nal information	Contificator
	AutoComplete stores previous entries AutoComplete	<u>C</u> ertificates
	and suggests matches for you.	
	Microsoft Profile Assistant stores your My Profile	
	OK Cancel App	yiq

Click the "Content" tab. Now, click "Certificates".



Verifying the Download (Cont'd)



Certificates				?>
Intended purpose: <a>	,			•
Proved by a sta				
Personal Other People Ir	htermediate Certification Au	uthorities Tru	sted Root Certification,	<u>•</u>
Issued To	Issued By	Expiratio	Friendly Name	-
Noble.Philip.E.0120	DOD CLASS 3 CA-7	9/25/2006	Noble.Philip.E.01	
Noble.Philip.E.0120	DOD CLASS 3 EMAIL	9/25/2006	Noble.Philip.E.01	
Noble.Philip.E.0120	DOD CLASS 3 EMAIL	9/25/2006	Noble.Philip.E.01	
NOBLE.PHILIP.EUG	DOD CLASS 3 EMAIL	1/26/2007	Signature Certifi	
NOBLE.PHILIP.EUG	DOD CLASS 3 CA-5	1/26/2007	ID Certificate	
NOBLE.PHILIP.EUG	DOD CLASS 3 EMAIL	2/1/2004	CN=NOBLE.PHIL	
NOBLE.PHILIP.EUG	DOD CLASS 3 EMAIL	1/26/2007	CN=NOBLE.PHIL	
1				
	1 1			
Import Export	<u>R</u> emove		<u>A</u> dvance	ed
Certificate intended purpose	es			
<all></all>				
			View	
			⊆los	е

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)



Certificate General Details Certification Path	<u>?×</u>					
Certificate Information						
This certificate has expired or is not yet valid.						
	_					
Issued to: NOBLE.PHILIP.EUGENE.1184204718						
Valid from 8/17/2003 to 2/1/2004						
Issuer <u>S</u> tatem	ent					
	ж					

Double-click on the certificate and 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: Delete the .P12 file from you computer as this is a security vulnerability and will be detected in a Qtip Scan



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=D OD,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=D OD,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 879-7608 CML 520-538-7608 FAX DSN 879-8709 CML 520-538-8709 philip.noble@us.army.mil philip.noble@hqisec.army.mil philip.noble@us.army.smil.mil philip.noble@conus.ds.army.smil.mil