

How to Recover Your Old (Expired) Certificates

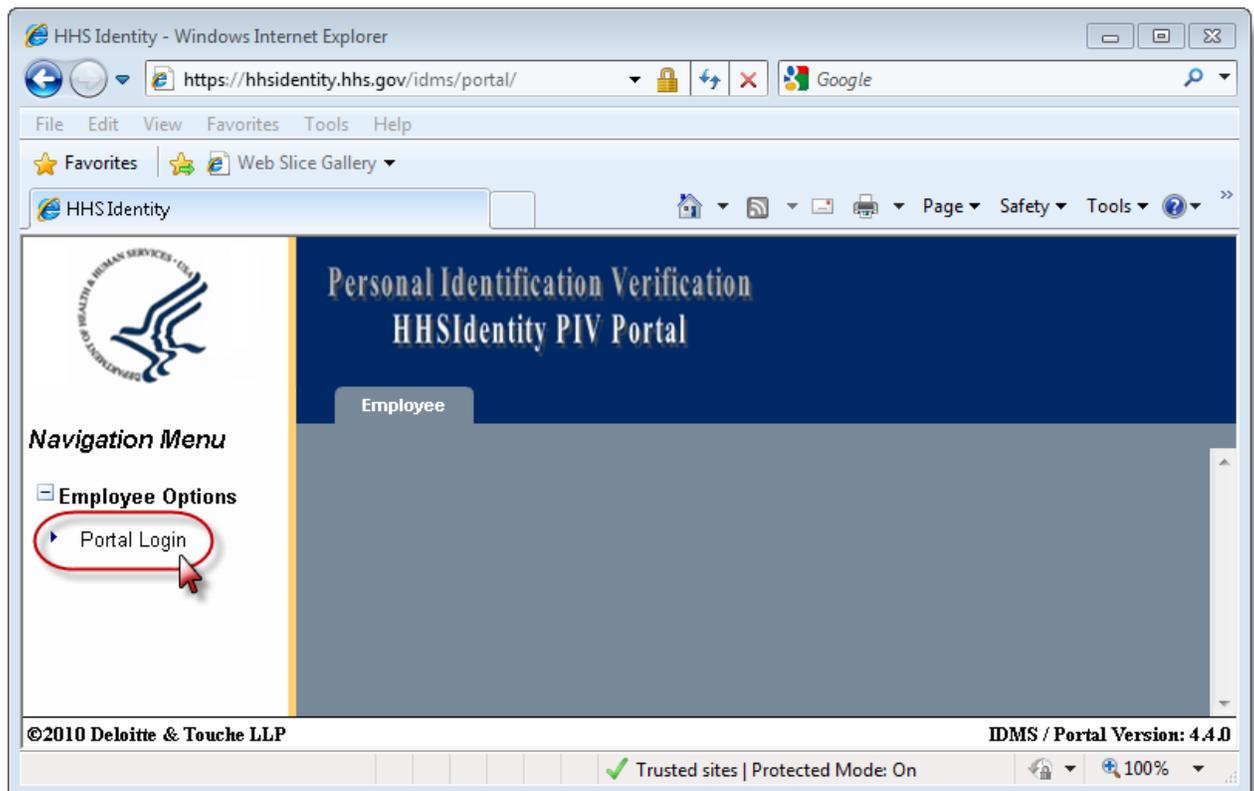
If you want to read signed or encrypted email messages that you sent or received using a now-expired certificate, you first need to recover that certificate from the HHS Identity PIV Portal.

There are three main steps:

- A. Select the expired certificate to recover.
- B. Download and save it to your computer.
- C. Install and secure the certificate with a password.

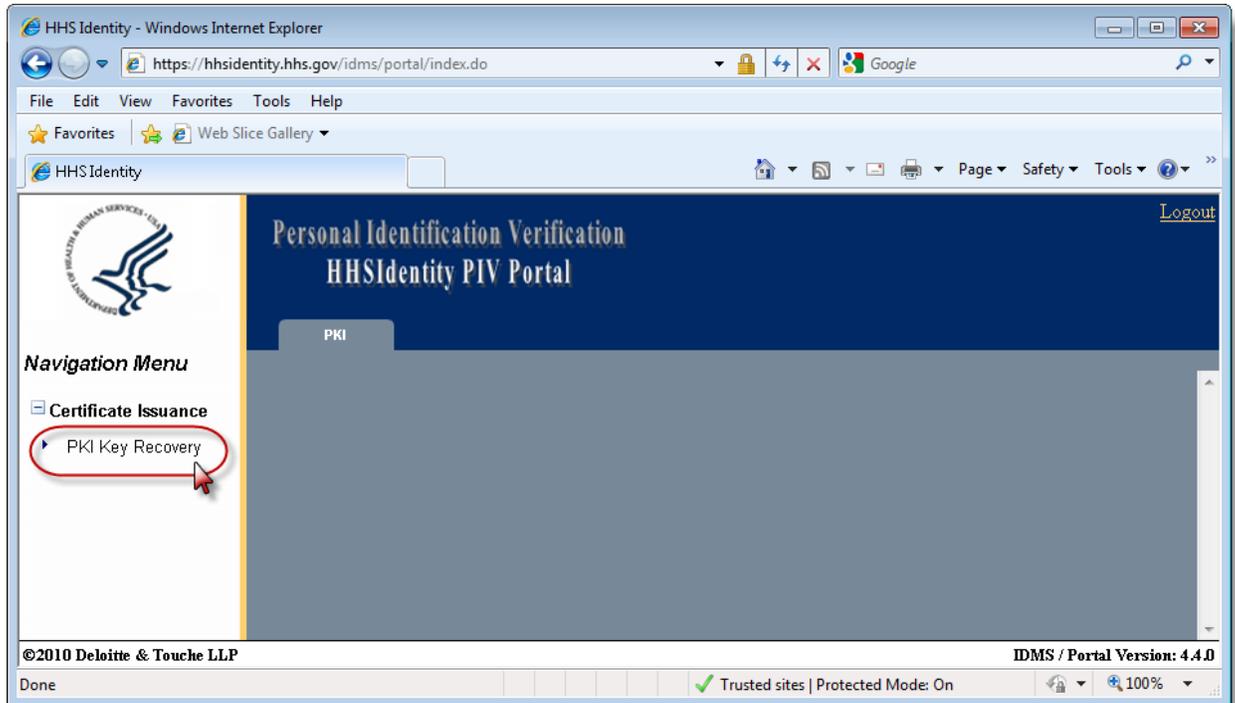
Select a certificate to recover from the HHS Identity PIV Portal

1. Open a session of your Internet browser and go to <https://hhsidentity.hhs.gov/idms/portal/>.
2. From the Navigation Menu, select **Portal Login**.



3. Enter your current PIN when prompted. (Make sure your PIV smart card is inserted in your computer's card reader.)

4. From the Navigation Menu, select **PKI Key Recovery**.



5. Select the radio button next to the certificate with the date range you are looking for. (You want the certificate that was valid at the time the email message was signed or encrypted and sent or received).
6. Select a reason for the certificate recovery from the dropdown menu.
7. Create a passphrase (or password) that will protect the recovered certificate as you download and save it to your computer. When ready, click **Recover Certificates**.



Navigation Menu

- [-] Certificate Issuance
 - ▶ PKI Key Recovery

Personal Identification Verification HHSIdentity PIV Portal

PKI

PKI Certificate Recovery

Listed are the encryption certificates that can be recovered. To begin the certificate recovery process, please select a certificate from the list, and specify a reason for the certificate recovery request and a passphrase to protect the recovered certificate. **Red text marked with an asterisk (*) indicates a required field**

Recoverable Encryption Certificates (Private Keys)

Distinguished Name: UID=0013271090+CN= (Affiliate),OU=People,OU=NIH,OU=HHS,O=U.S. Government,C=US

Certificate Type: PIV Encryption

Select	Status	Issuance Date	Expiration Date	Recovered Date
<input type="radio"/>	Active	Apr 06 2012	Feb 07 2013	
<input type="radio"/>	Inactive	Feb 10 2012	Feb 07 2013	Apr 05 2012
<input type="radio"/>	Inactive	Feb 11 2011	Feb 09 2012	Apr 05 2012
<input checked="" type="radio"/>	Inactive	May 25 2010	May 17 2011	

Certificate Recovery Request Information

Select a reason for Certificate Recovery *

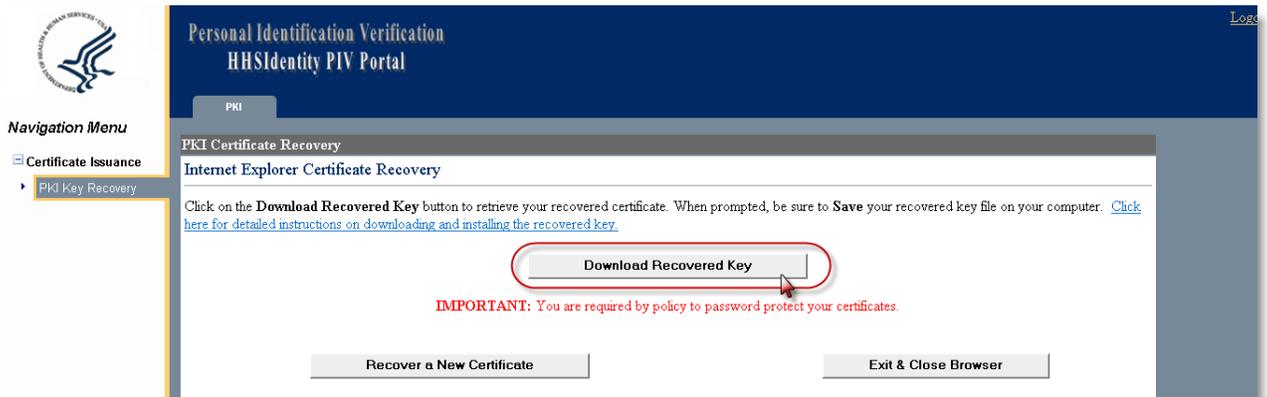
Enter a Passphrase to protect the recovered certificate *

Reenter the Passphrase to protect the recovered certificate *

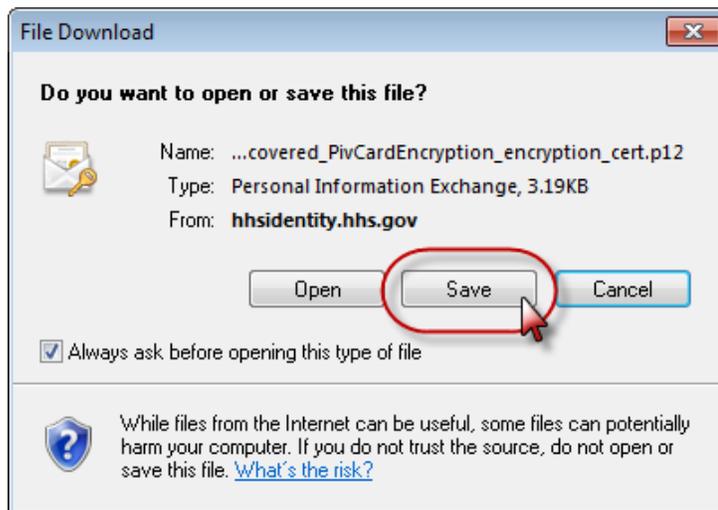
Recover Certificates

Download the recovered certificate

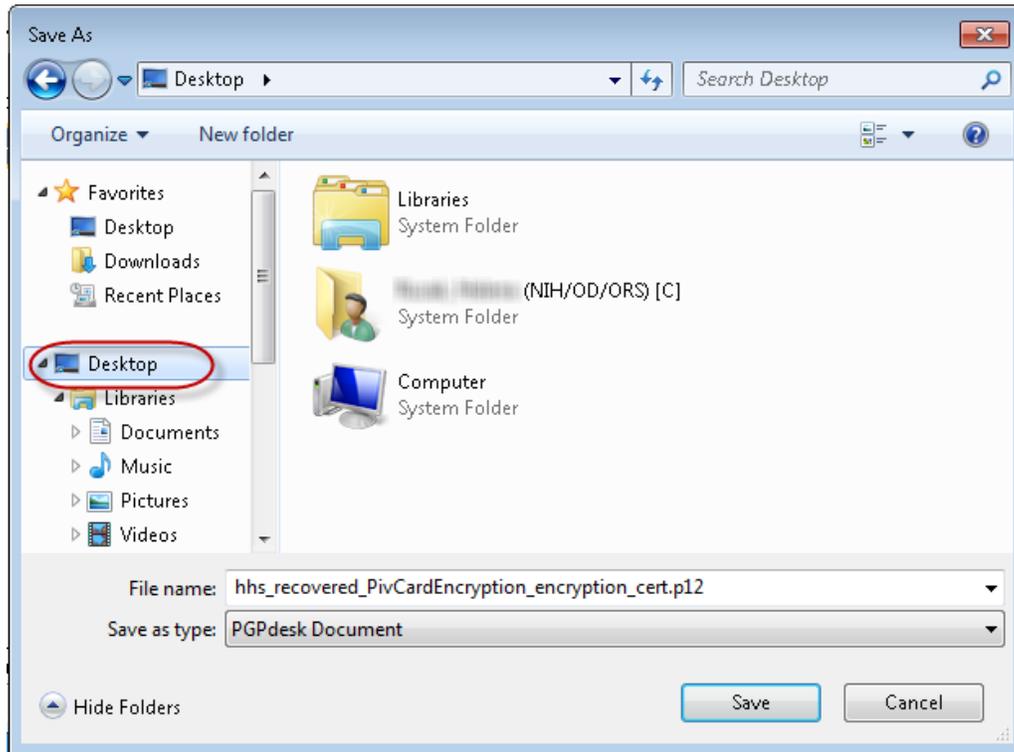
8. Click **Download Recovered Key**.



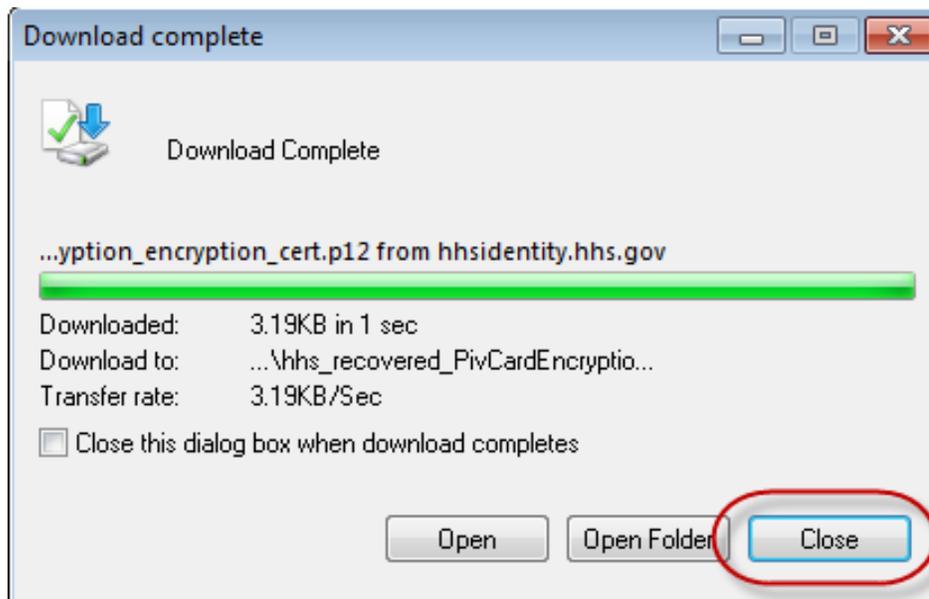
9. Click **Save** from the *File Download* dialog box.



10. Save the file to a location on your computer. You can save it to the Desktop so that it's easy to locate the file for the next step. This file contains a Certificate Import Wizard that will allow you save the certificate to your computer and secure it with a password.

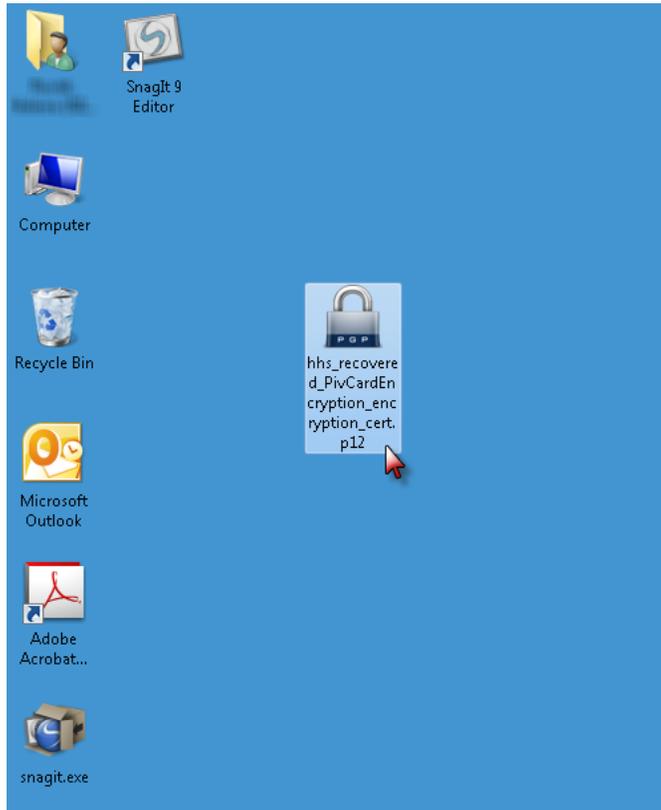


Once saved, click **Close** from the *Download Complete* dialog box.



Install and secure the certificate with a password

11. Locate the downloaded file, and double-click the file to open the Import Wizard.



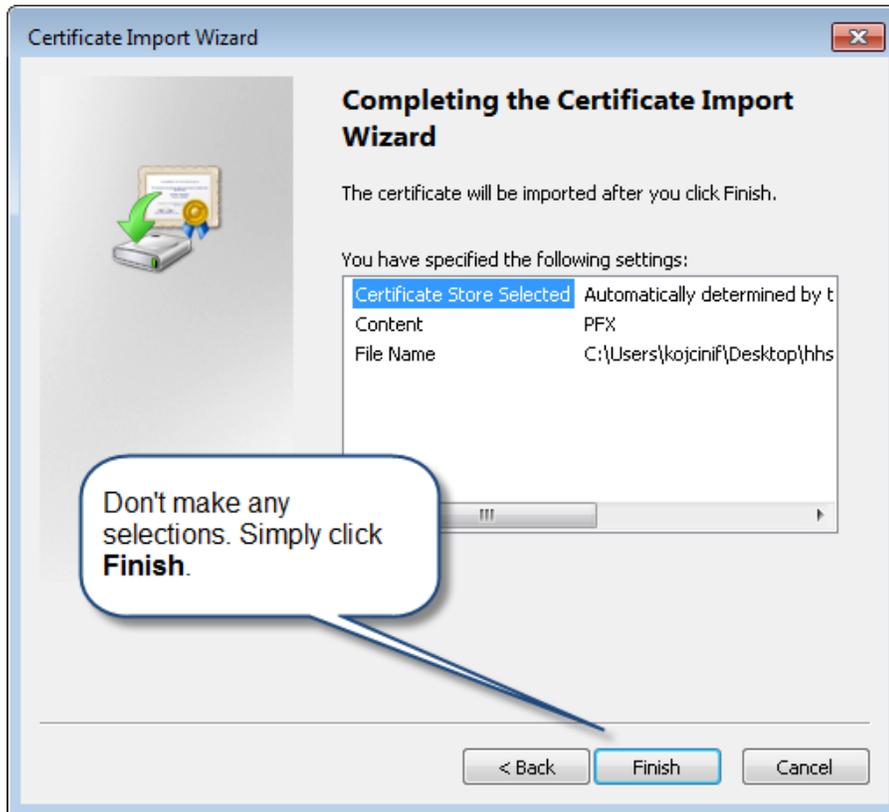
12. Click **Next** to start the Wizard. Click **Next** again to proceed with the import.



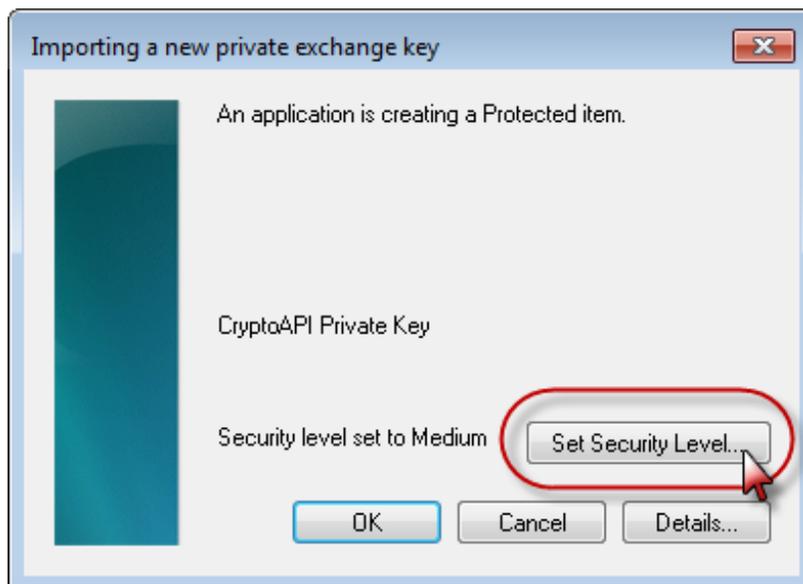
- Enter the passphrase (or password) you created in the HHS Identity PIV Portal (during step 7). Click to select all three options after entering your passphrase, and then click **Next**.

- Make sure the option for *Automatically select the certificate store based on the type of certificate* is selected. Click **Next**.

15. Click **Finish**. (You're not done yet, though!)



16. From the *Importing a New Private Exchange Key* dialog box, click the **Set Security Level** button.



17. Select the security level option “High”. Click **Next**.



Choose a Security Level

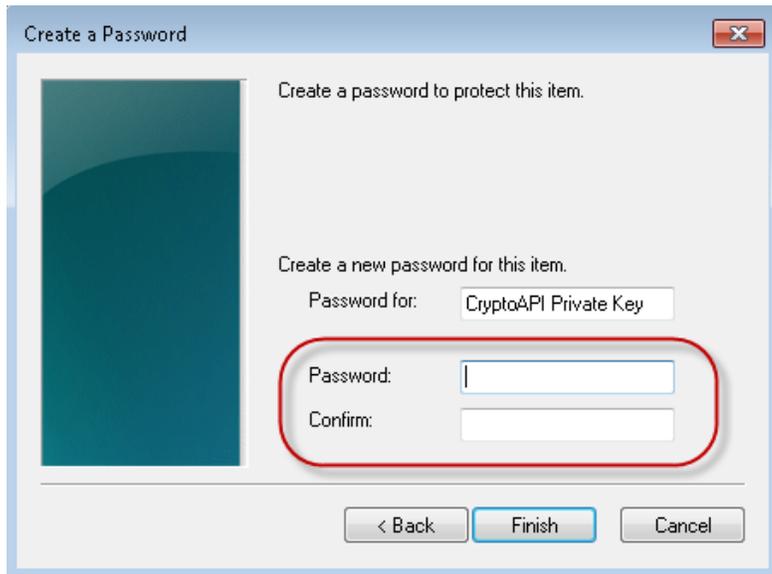
Choose a security level appropriate for this item.

High
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

18. Create and confirm a password to protect the recovered certificate. (A suggestion would be to select your current PIN as a password for the certificate. This will be a password that you need to use each time you want to open email that was signed or encrypted when this certificate was valid.) Click **Finish**.



Create a Password

Create a password to protect this item.

Create a new password for this item.

Password for: CryptoAPI Private Key

Password:

Confirm:

< Back Finish Cancel

The recovered certificate is stored on your computer and protected with the password you entered. When you attempt to open an email message that was originally signed or encrypted with this now-expired certificate, you will be prompted to enter this password.

If you need help, please contact the NIH IT Service Desk at 301-496-4357 or submit a ticket online at <http://itservicesdesk.nih.gov/support>.