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:

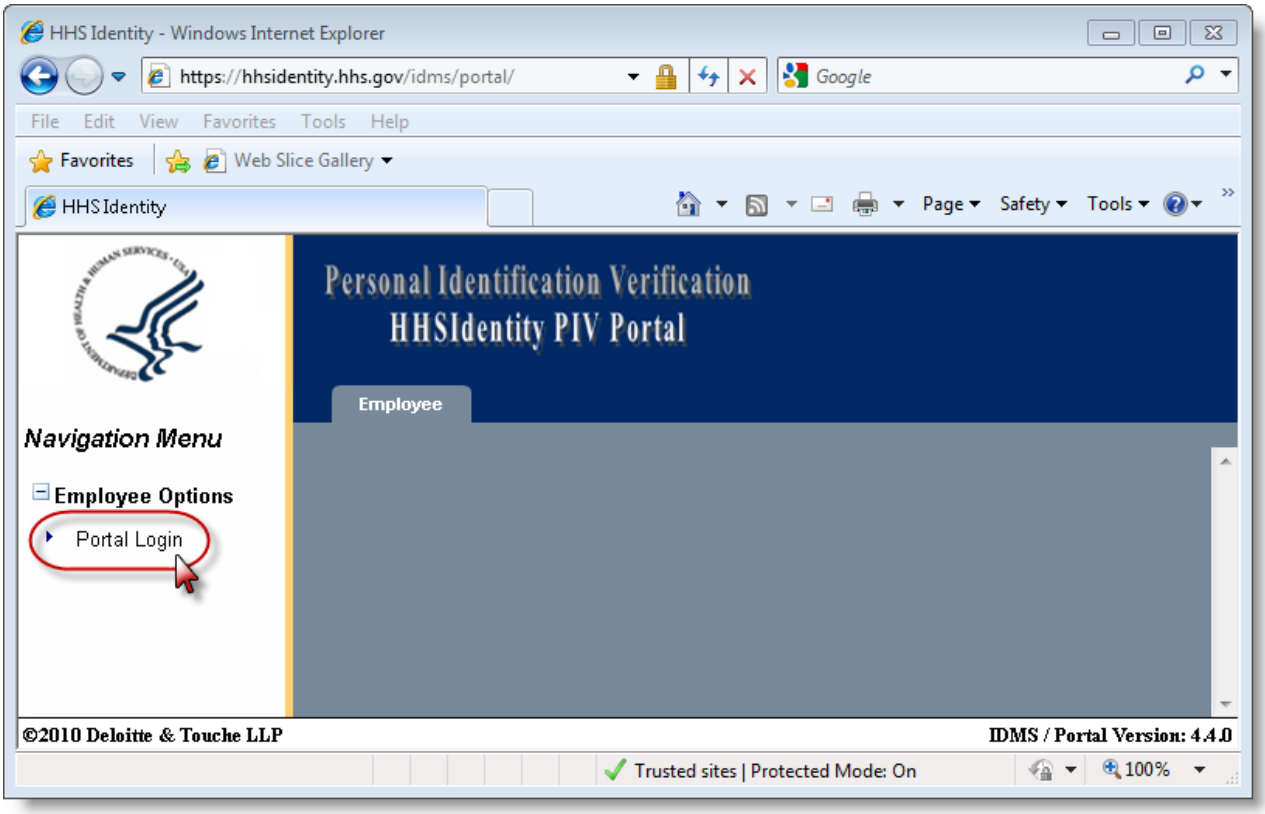
A. Select the expired certificate to recover.

B. Download and save it to your computer.

C. Install and secure the certificate with a password.

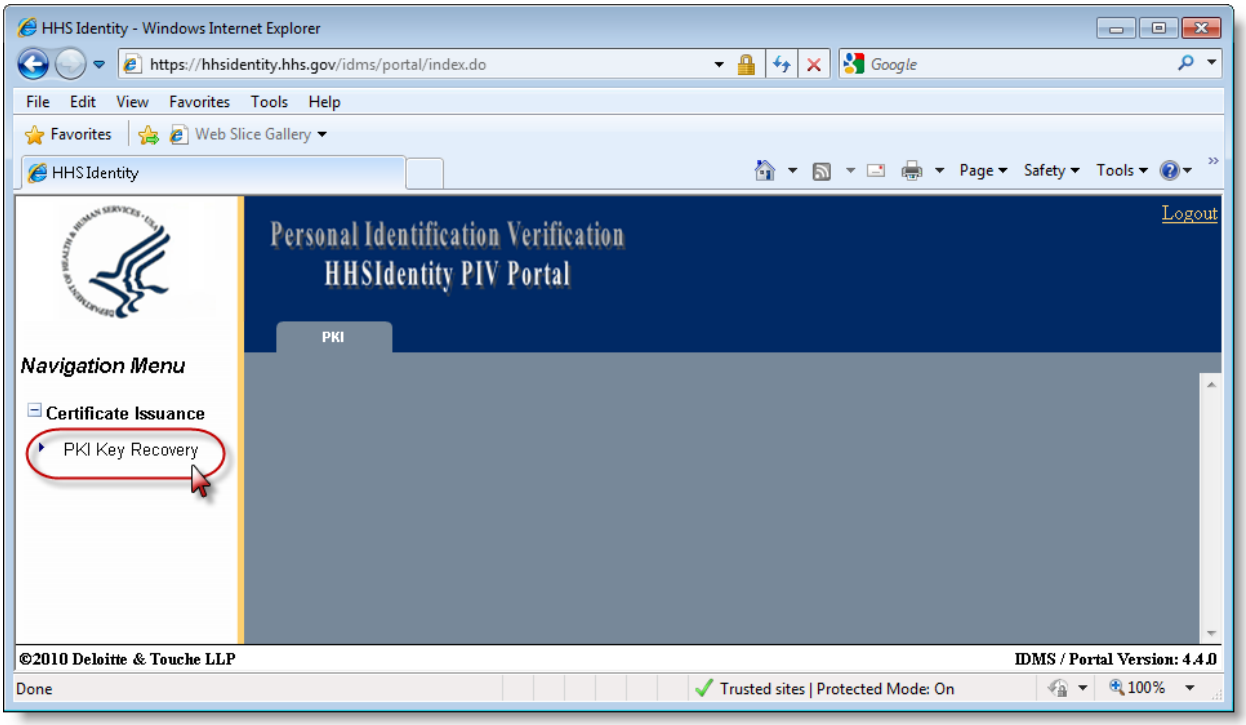
Select a certificate to recover from the HHS Identity PIV Portal

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**.

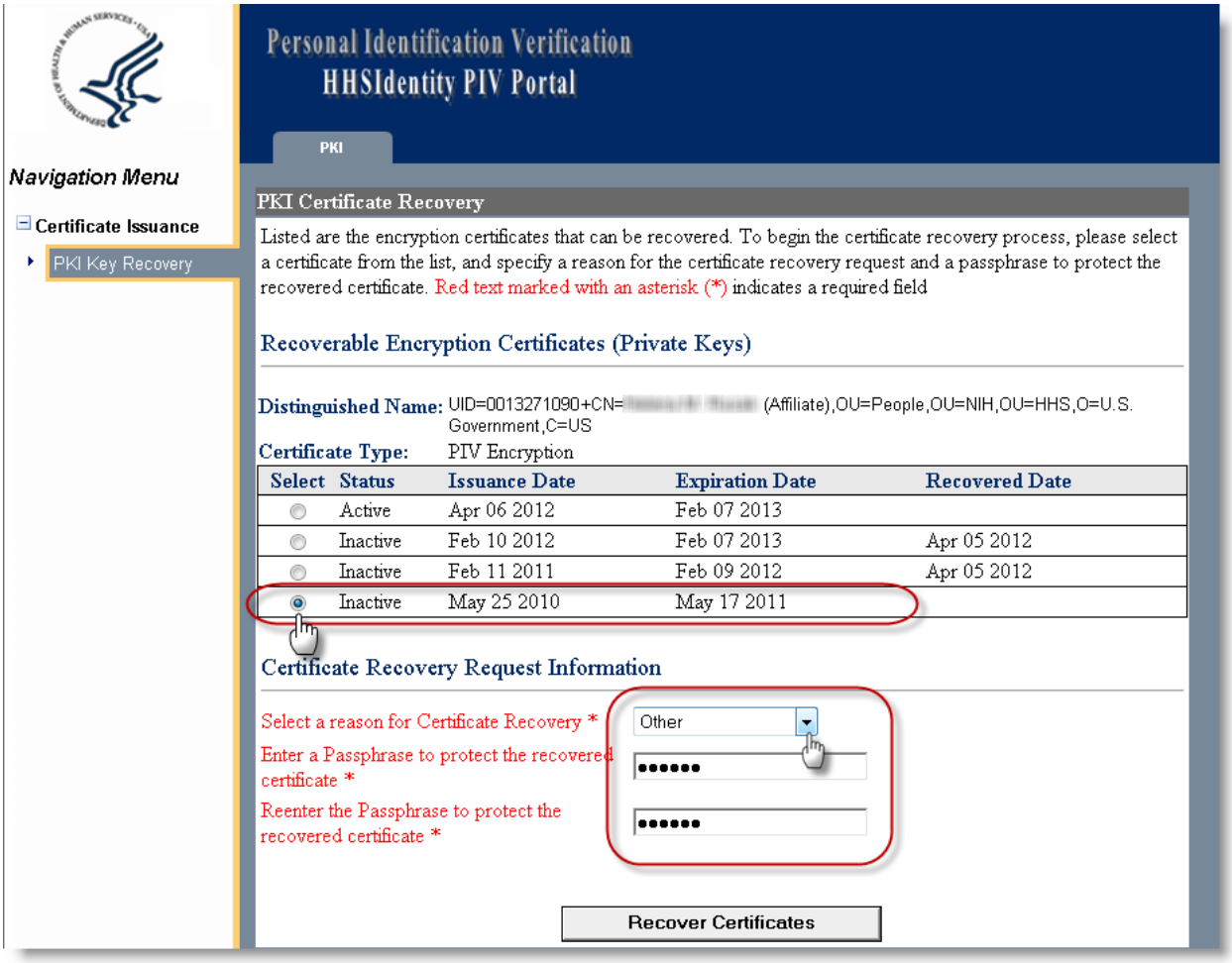


3. Enter your current PIN when prompted. (Make sure your PIV smart card is inserted in your computer's card reader.)

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

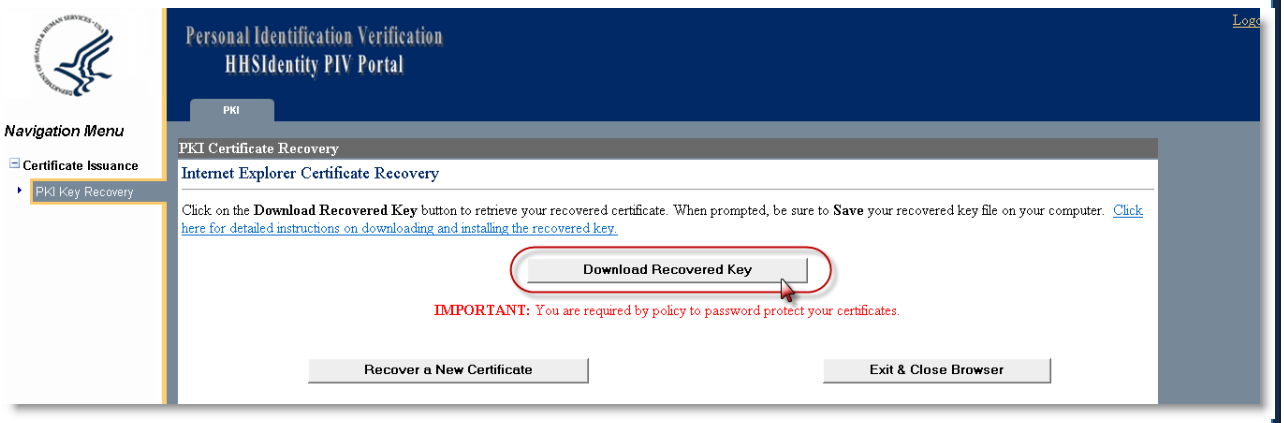


5. Select the radio button next to the certificate with the date range you are looking for. (You want the certificate that was valid at the time the email message was signed or encrypted and sent or received).
6. Select a reason for the certificate recovery from the dropdown menu.
7. Create a passphrase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

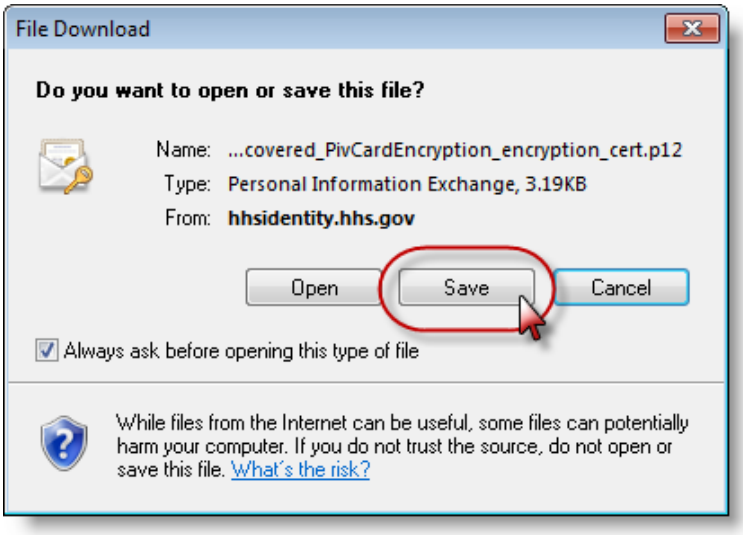


Download the recovered certificate

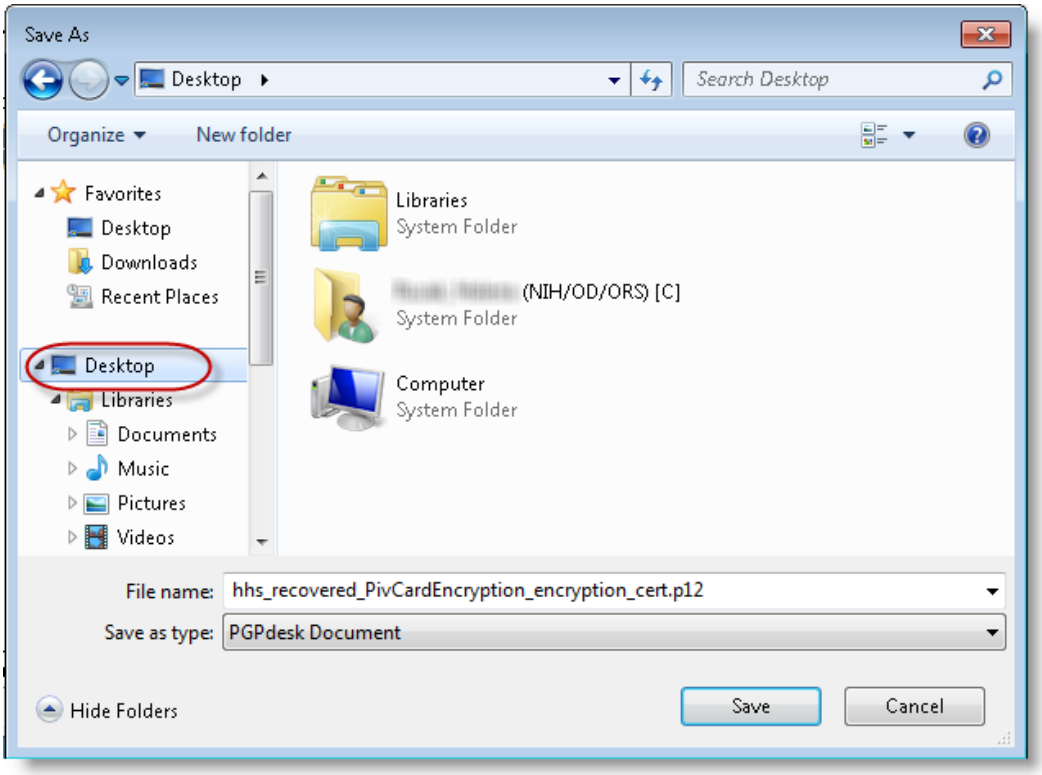
8. Click **Download Recovered Key**.



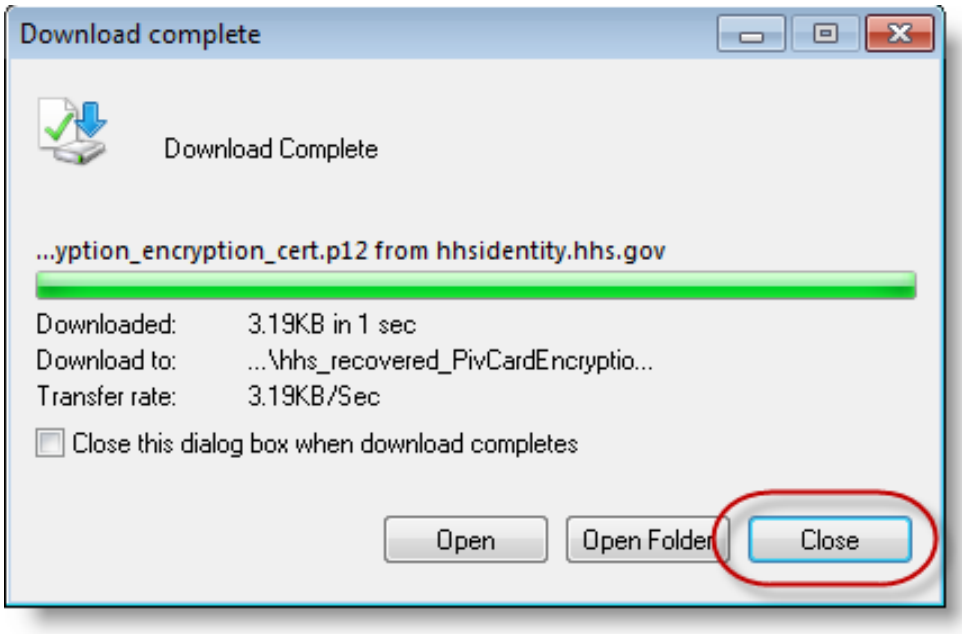
9. Click **Save** from the *File Download* dialog box.



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.

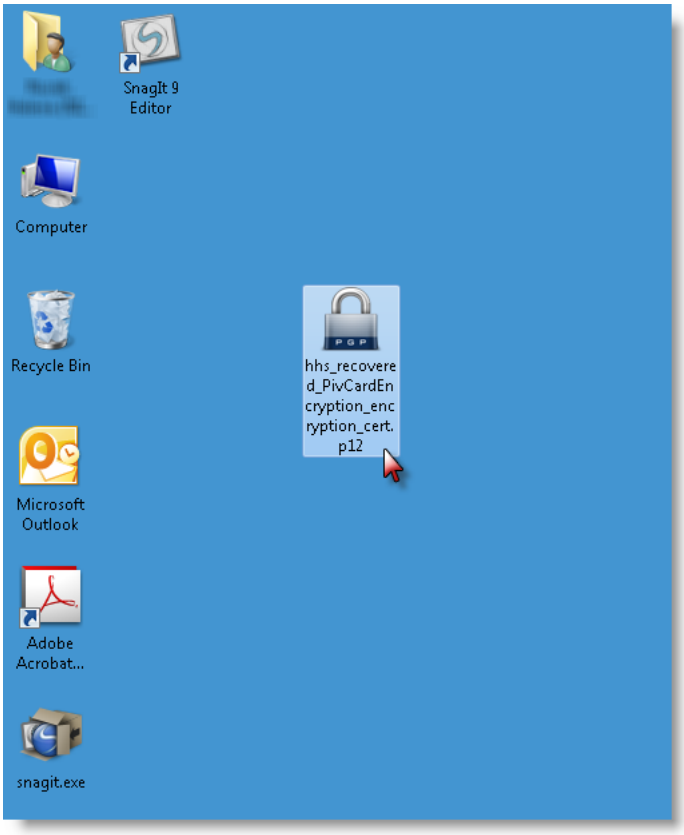


Once saved, click **Close** from the *Download Complete* dialog box.



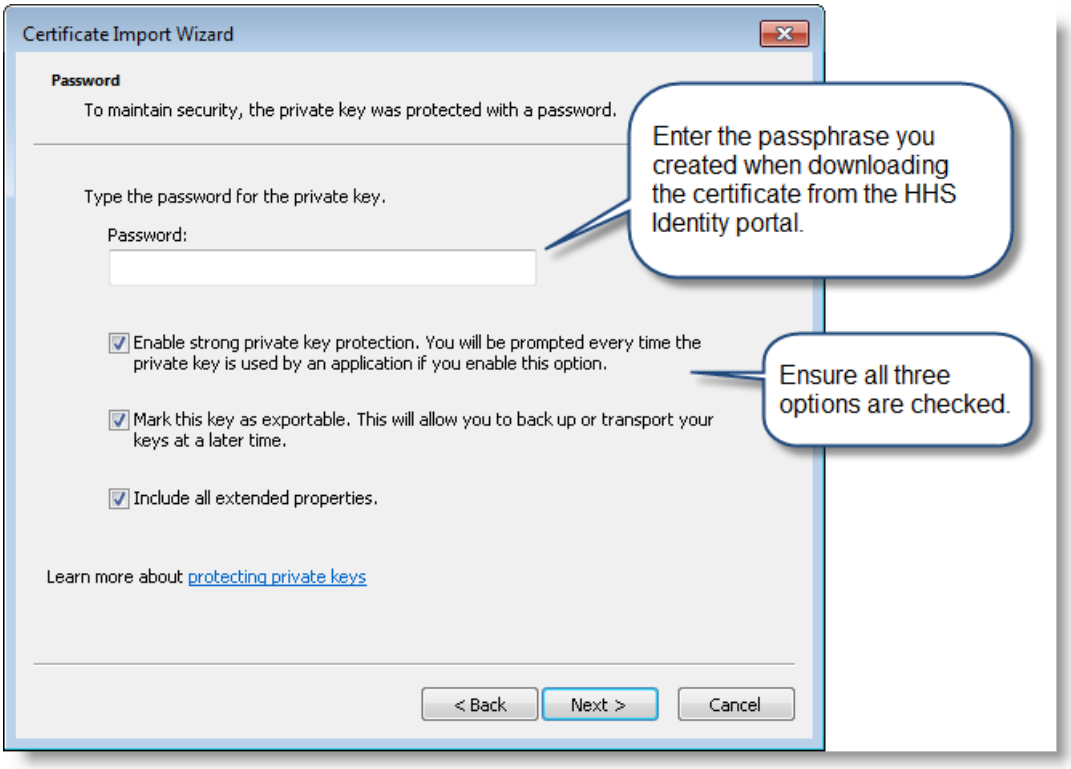
Install and secure the certificate with a password

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

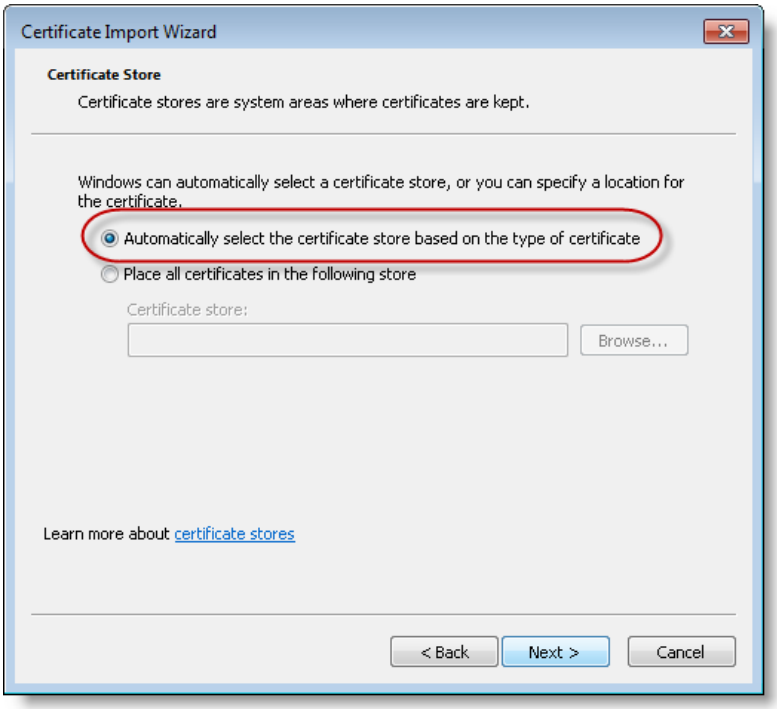


12. Click **Next** to start the Wizard. Click **Next** again to proceed with the import.

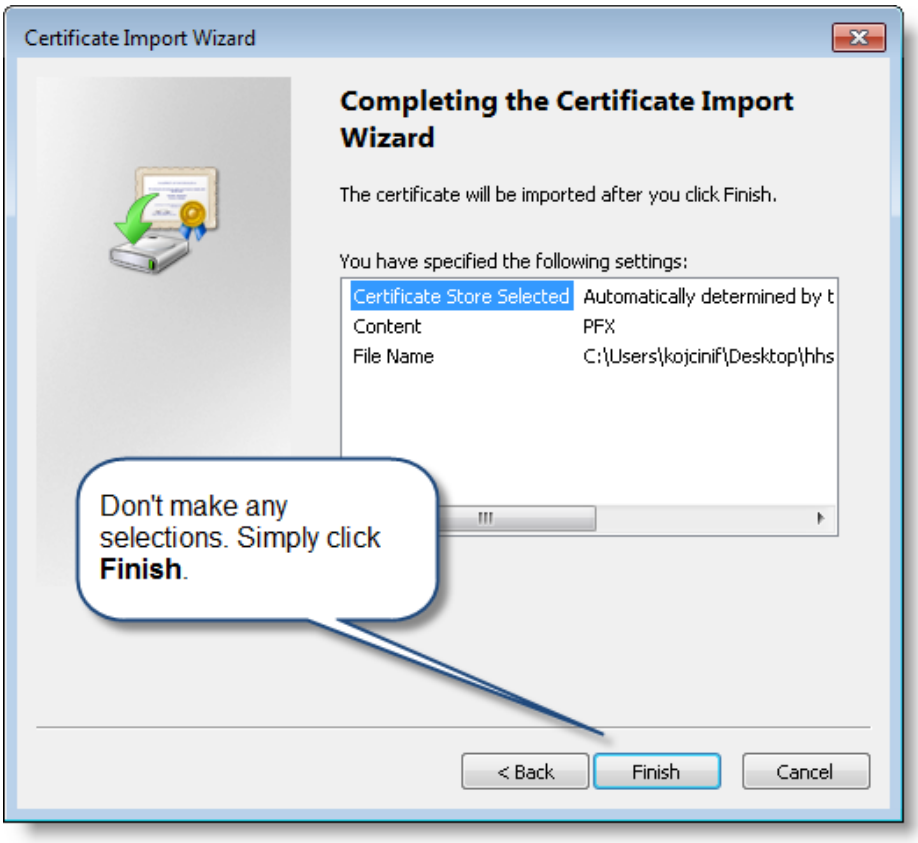
13. Enter the passphrase (or password) you created in the HHS Identity PIV Portal (during step 7). Click to select all three options after entering your passphrase, and then click **Next**.



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

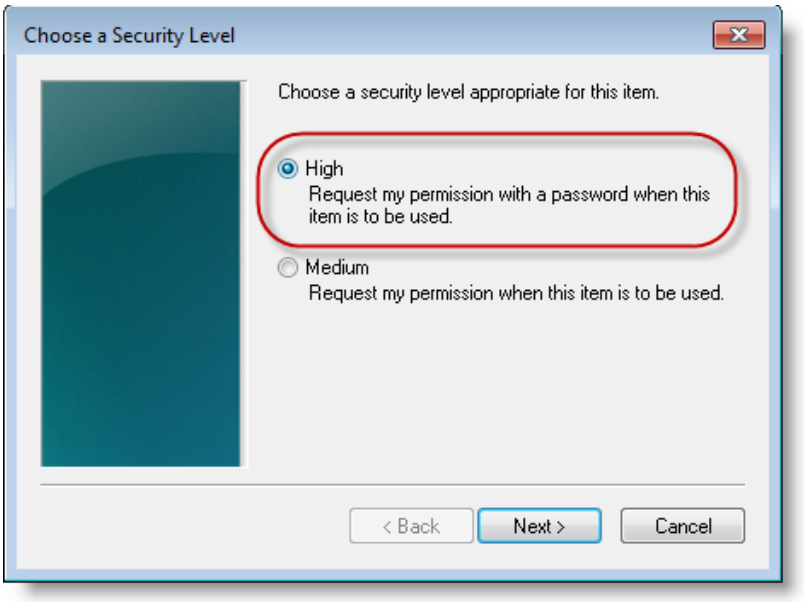


15. Click **Finish**. (You're not done yet, though!)

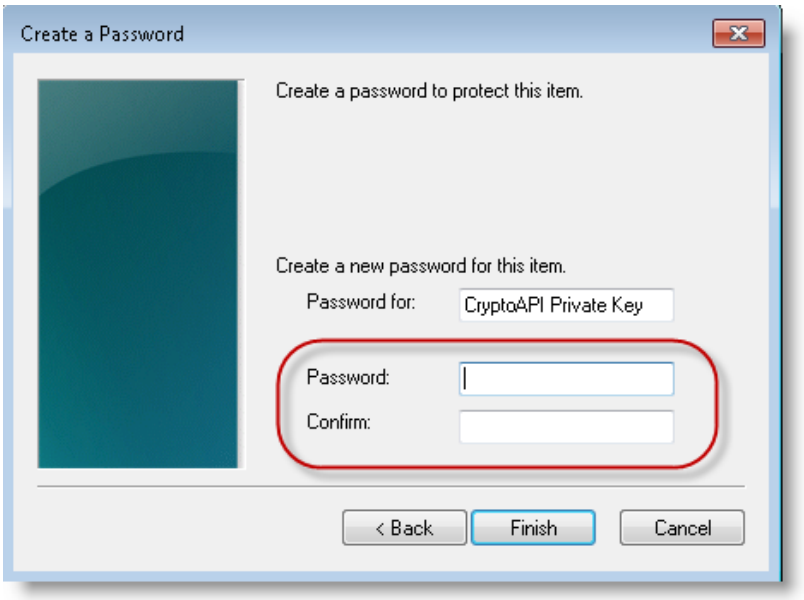


16. From the *Importing a New Private Exchange Key* dialog box, click the **Set Security Level** button.

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



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**.



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://itservicedesk.nih.gov/support.