

How to Replace a Digital Certificate

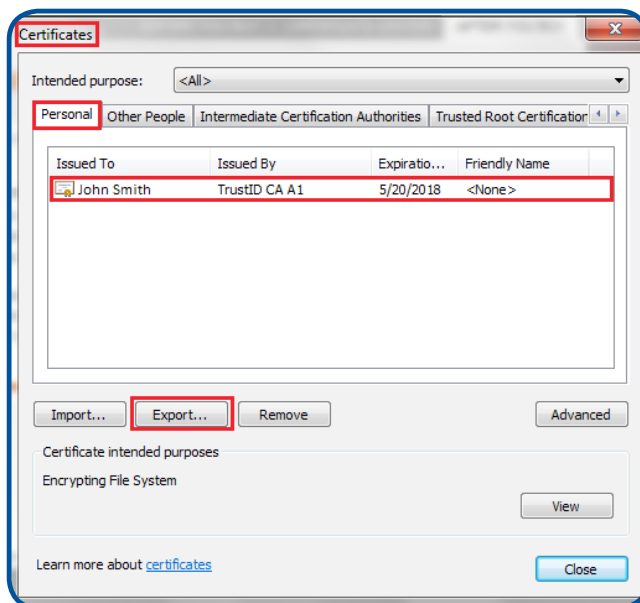
There are some circumstances in which your digital certificate may become unusable. In some cases, access to your certificate can be restored but in other cases it will be necessary to replace the certificate. When a certificate is replaced, the old certificate is revoked.

In this document, IdenTrust will provide answers to frequently asked questions about replacing a digital certificate.

Determine if a Certificate Replacement is Needed

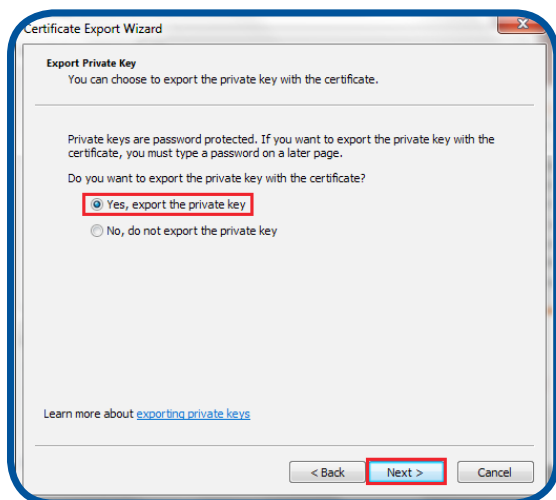
Using Microsoft® Internet Explorer you can determine whether your certificate needs to be replaced by trying to export the certificate. (If you need more detailed instructions for exporting the certificate, please see the IdenTrust document “How to Export a Certificate When Using Microsoft® Windows® OS”.) Try to export the certificate following these instructions:

- Close all open Internet Explorer windows and open a new one.
 - Click on **“Tools”**. Then click on **“Internet Options”**.
 - Click on the **“Content”** tab. Then click on the **“Certificates”** button.
 - Your certificate should be listed under the “Personal” tab. If it is not there, either the certificate was retrieved on a different computer, browser, or device (USB token or Smart card) or it has been deleted. If you cannot find your certificate in one of those places, you will have to replace the certificate.

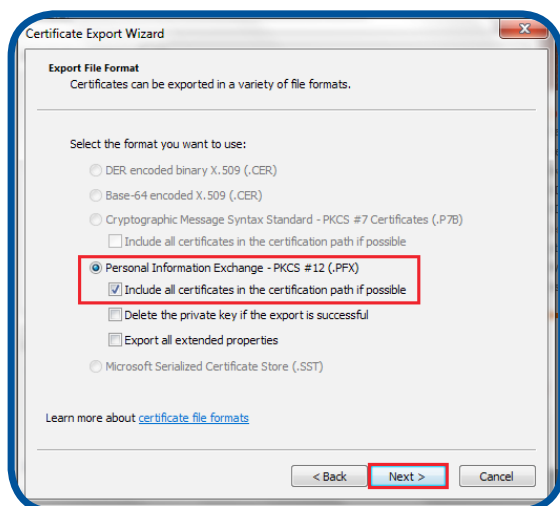


- If your certificate is there, select it by clicking once. Then click **“Export”**. The **“Certificate Export Wizard”** will pop up. Click **“Next”**.

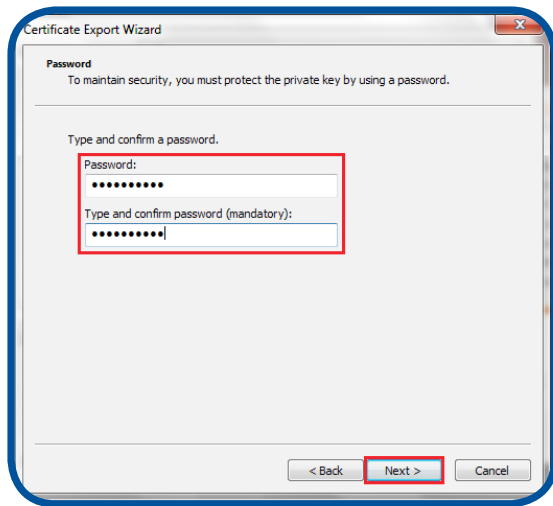
- If the **“Yes, export the private key”** option is grayed out, the private key may reside in a secure device such as a USB token or Smart card which do not allow private key export; or the private key has been deleted from the computer and you will need to replace the certificate.



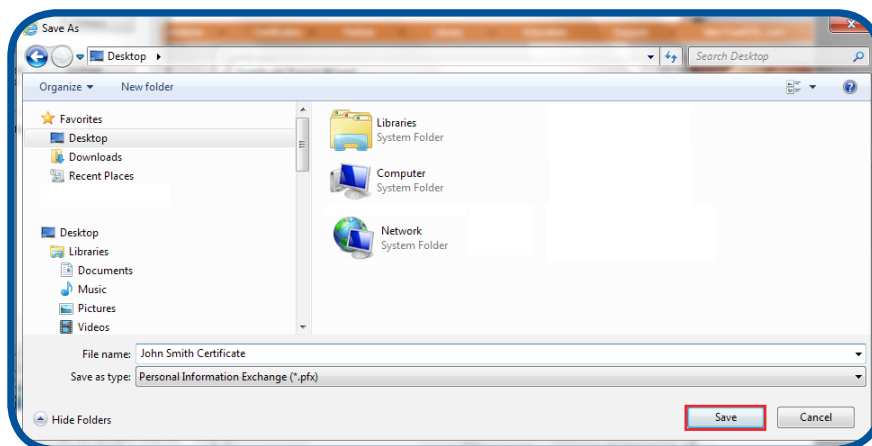
- If the **“Yes, export the private key”** option is available, make sure it is checked. Then click **“Next”**.
 - If available, make sure the **“Enable strong protection”** box is checked. Put a check in the **“Include all certificates in the certification path”** if possible box. Click **“Next”**.



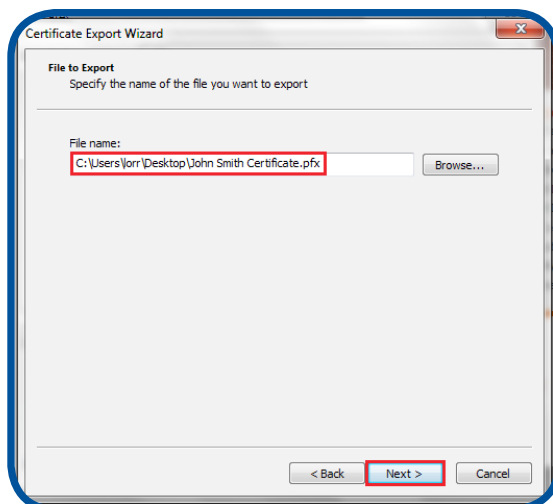
- Type in a password that will be used for exporting and importing this certificate. Re-type it in the second box to confirm it. Click **“Next”**.



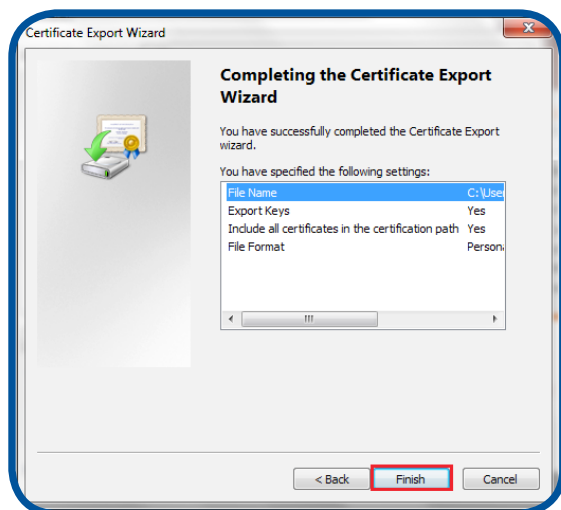
- Click the **“Browse”** button. Choose the drive and folder where you would like to store the exported file. Type in a file name. Click **“Save”**.



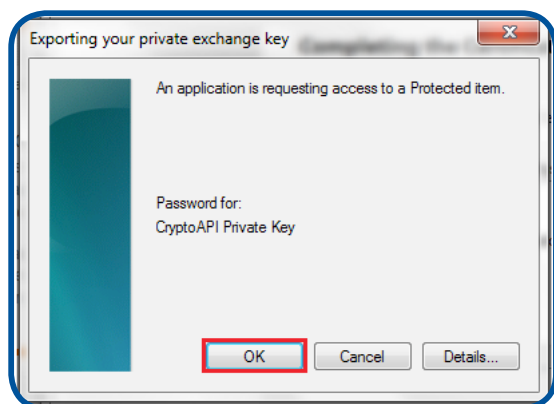
- Click **“Next”**.



- Click **“Finish”**.

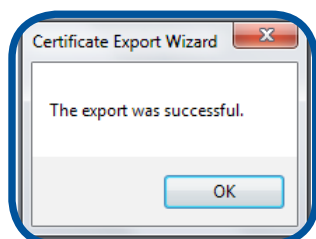


- A window will pop up asking you to confirm that you are accessing a protected item. Click **“OK”**.



If your password is still not accepted, you will need to replace your certificate.

If your password is accepted, a window will pop up saying that **“your export was successful”**. Click **“OK”**. You do not need to replace your certificate.



Replacing Your Digital Certificate

Once you have determined that your certificate needs to be replaced (using the instructions above), replacement is a 3-step process:

- Remove the corrupted certificate from your computer;
- Replace the certificate; and
- Verify replacement.

Step 1: Remove the Corrupted Certificate From Your Computer

- a. Close all open Internet Explorer browser windows.
- b. Open a new Internet Explorer browser window.
- c. Click on **"Tools"**. This will be located on the upper right-hand corner of the screen.
- d. Click **"Internet Options"** at the bottom of the pull-down menu.
- e. Click the **"Content"** tab at the center top of the window.
- f. Click the **"Certificates"** button in the middle of the **"Certificates"** section.
- g. Find the certificate with your name and certificate type on it under the **"Personal"** tab and select it by clicking on it once.
- h. Click the **"Remove"** button.
- i. When you get the message **"You cannot decrypt data encrypted using this certificate. Do you want to delete the certificate?"**. Click **"Yes"**.
- j. Click the **"Close"** button at the bottom of the screen.
- k. Click the **"OK"** button on **"Internet Options"**.
- l. Close Internet Explorer completely.

Step 2: Replace Your Certificate

- a. Log into the **"Certificate Management Center"** by clicking on the orange **"Login"** on the left side of your screen. When you are asked for a certificate to log in with, click **"Cancel"**. Enter your account number (which can be found on the letter you received when you first retrieved your certificate) and your IdenTrust account passphrase.
- b. In the drop-down box under the listing for your **"Valid Certificates"**, select **"I would like to replace my certificate"** and click **"Continue"**.
- c. Follow the on-screen instructions to retrieve the new certificate.
 - You will be given a new activation code to use during this retrieval process. Be sure to write down this activation code.
 - At the end of the retrieval, you will need to verify the installation. This will fail the first time (because you had to click **"Cancel"** in Step 2a) but you will receive instructions to retry and successfully verify the retrieval.

Step 3: Verify Certificate Replacement

- a. You can verify the certificate was installed by testing it. Go to: <https://www.identrust.com/test/> using the computer and browser in which you have your certificate.
- b. Then follow the prompts to complete the test by clicking **"Next"**.
- c. If you do not receive a **"Congratulations"** message at the end; call the IdenTrust support line. You should have access to your computer when you call so that our representative can guide you through alternative certificate replacement steps. Let the representative know that you have followed all of the steps in this "How To" document and whether you experienced any difficulty with any of the steps.