Why should I back up my certificate?

You should *always* keep a backup copy of your ACES Business Certificate on a location external to your computer. Since it's stored locally on your computer, in the Windows certificate store, the certificate is vulnerable to deletion or corruption by viruses, hardware failures, or even updates to your browser or operating system. If this happens, the *only* way to restore your certificate is through a backup copy. We at ORC never have access to your complete certificate, so if it's lost and you don't have a backup copy, your only option is to buy a new one to replace it.

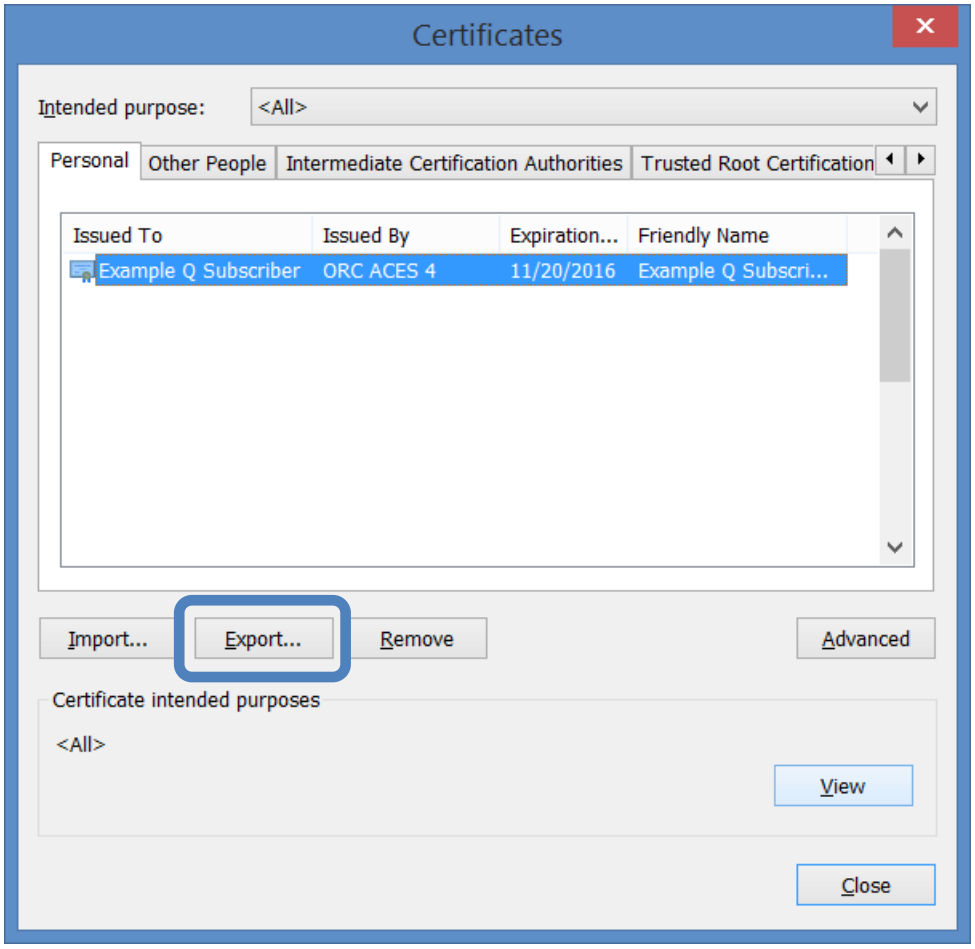
Besides using it to restore your certificate in case of loss, you can also use your backup file to copy the certificate to other computers. As long as you protect it with a secure password on every computer and don't share the certificate with anyone else, you're free to use it on as many computers as you'd like. You can export the certificate from your work PC to your laptop or even your home computer.

How do I create a backup copy of my certificate?

Here's how to back up your certificate in Internet Explorer:

1. Click the Tools button and then click Internet Options.
2. Select the Content tab and then click the "Certificates" button.

3. The Certificates box will open. Your certificate will appear under your full name (first, middle initial, last) in the Issued To column. Select your certificate, and then click the Export button.

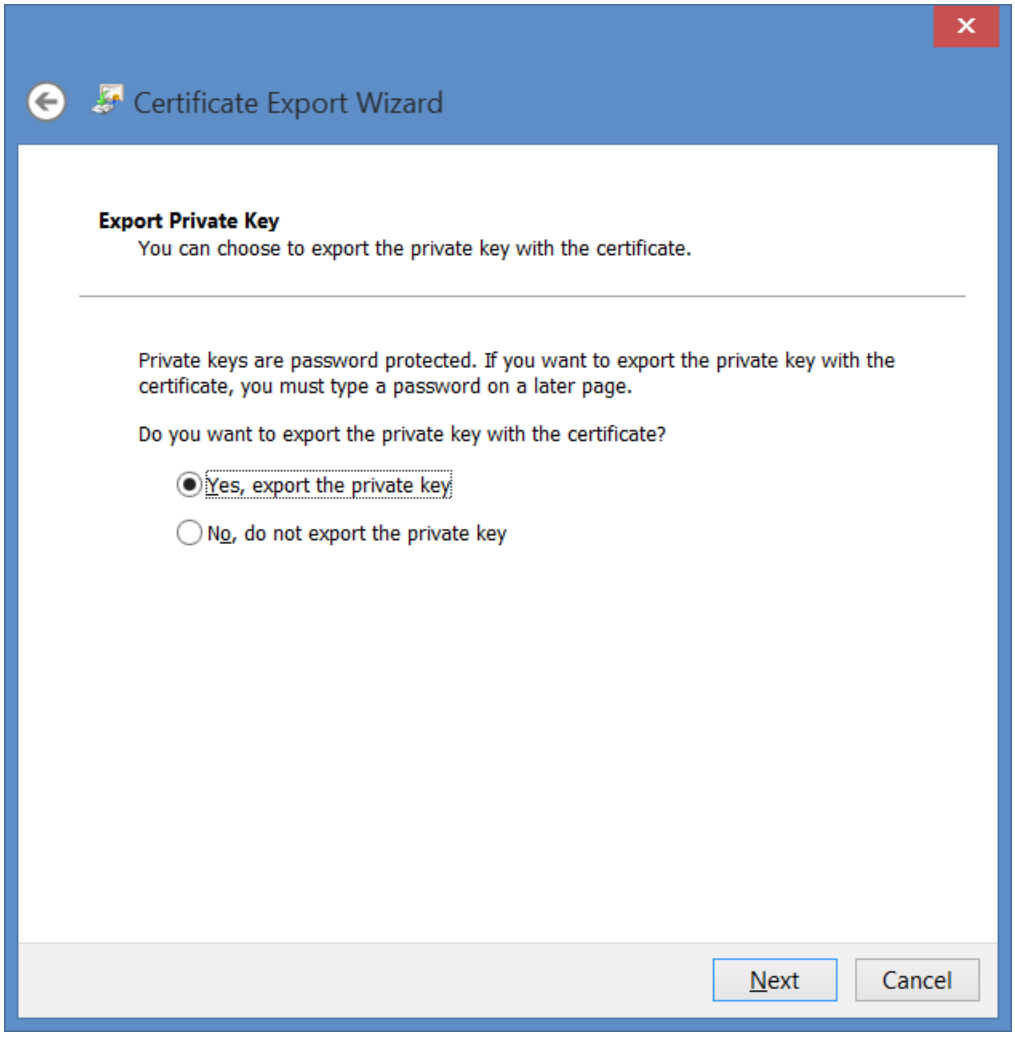


4. The Certificate Export Wizard will open. Click Next.

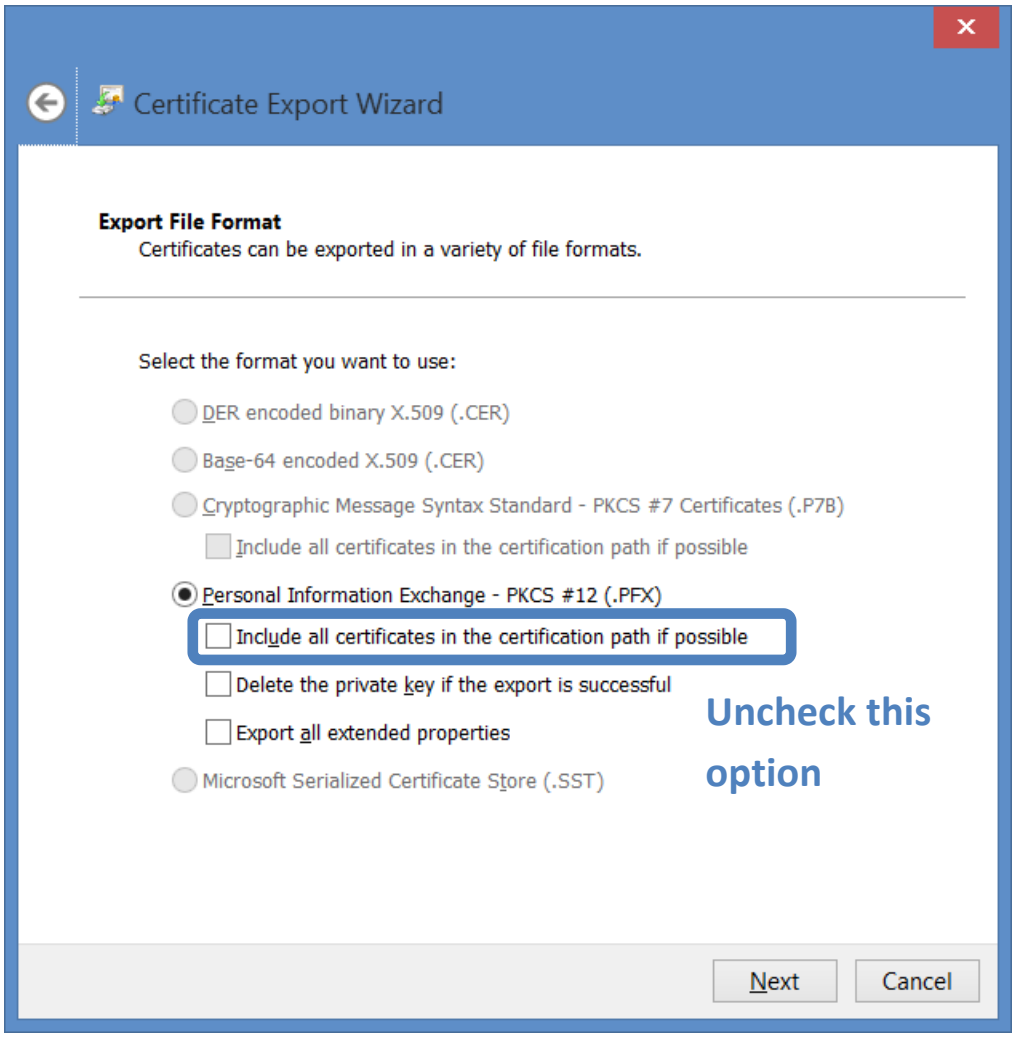
(Instructions continue on next page)

5. Select “Yes, export the private key” and then click Next.

   CAUTION: It’s possible to create a backup file that doesn’t include the private key, but it WON’T be a complete backup copy of your certificate. The certificate won’t work without the private key. If “Yes, export the private key” is greyed out (that is, you can’t select it), stop here and contact our help desk at aceshelp@orc.com.

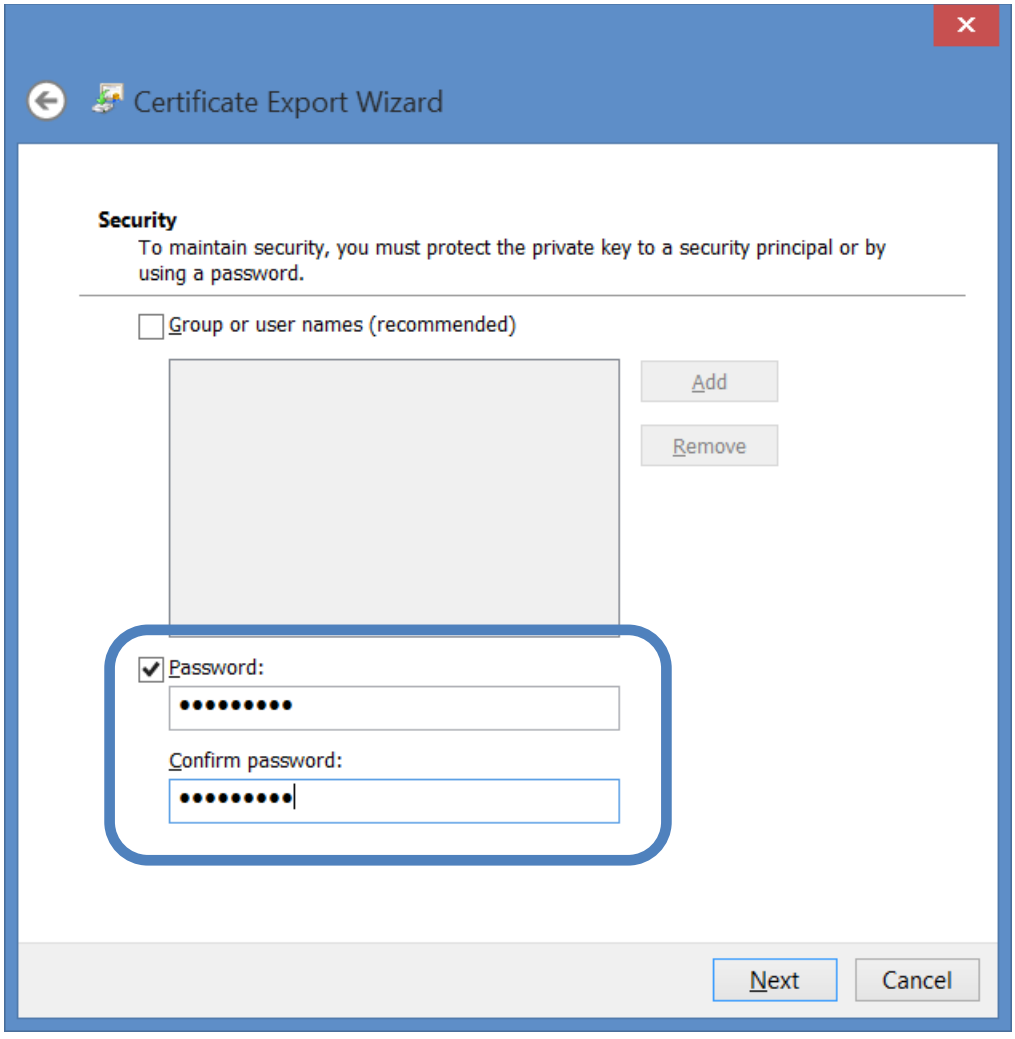


6. Personal Information Exchange is the default file type. You'll see a checkmark next to the option "Include all certificates in the certification path if possible". Uncheck this option before you go further. It's not necessary, and can sometimes cause problems. When you're done, click Next.



7. Now it's time to create a password for this backup file. You'll use this password any time you want to use the backup file to install the certificate somewhere (on another browser or another computer, for example). Click the Password checkbox, enter your password twice, and then click Next.

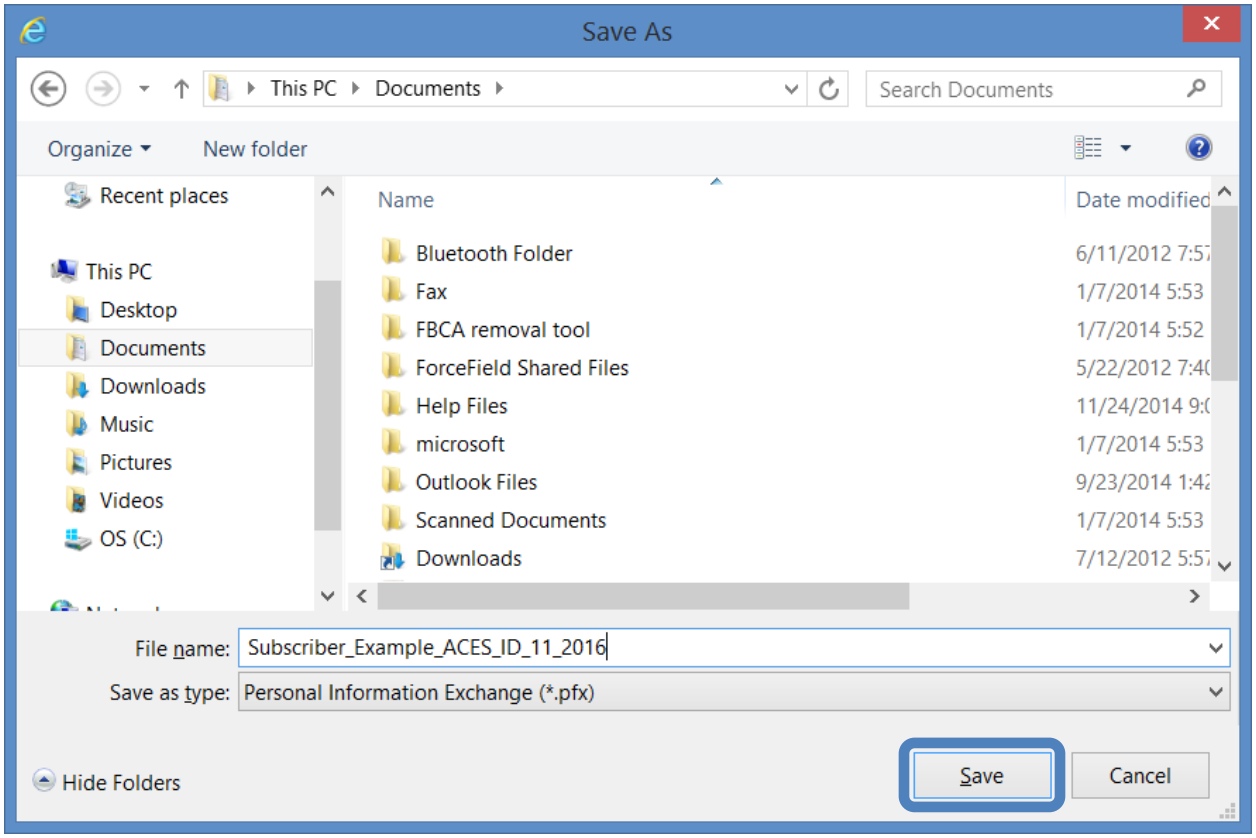
   Note: We suggest the password contain a combination of letters, numbers, and symbols. Make it complex enough that it will be difficult for others to guess, but simple enough that you'll be able to remember it. ORC *cannot* reset this for you if you forget it!



8. Now you'll choose where you want to save the file and what to call it. Take these four steps to set up your save file:
    a. Click the Browse button.
    b. In the left-hand pane, choose a location to save your certificate backup file.

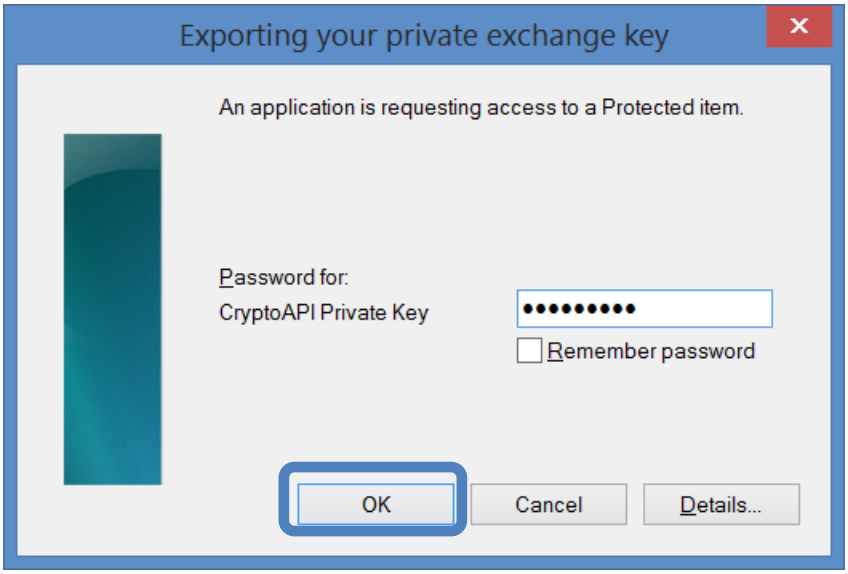
        Reminder: To protect yourself from losing the certificate in the event of a hardware failure, upgrade, or other event, make sure you save your certificate somewhere other than your computer's hard drive. A thumb drive or shared network location works well for this!

    c. In the File Name field toward the bottom of the window, enter a name for your certificate backup file. You're free to name it whatever you like, but we recommend that you use the format: Lastname_Firstname_ACES_ID_MM_YYYY, where "MM" and "YYYY" are the month and year of your certificate's expiration date. This naming scheme will tell you at a glance whose certificate it is, what kind of certificate it is, and when it expires.
    d. Click the Save button.



9. When you click Save, you'll return to the File to Export box. You'll now see the location and file name you chose in the File name box. Click Next.
10. The wizard will summarize the options you chose during the file creation process. Click Finish.
11. A dialog box will appear asking you for the password for your CryptoAPI Private Key. This is the password that you set during the certificate request process on our website, just prior to printing your request forms *or*, if this isn't the browser where you originally made the request, it's the password that you set when you imported the certificate from backup. Enter your password. **DO NOT** click "Remember password". When you're done, click OK.

    Note: As part of the security design of the ACES Certificate Policy, we at ORC have no way to access or reset this password for you. If you don't know it, you won't be able to back up your certificate through Internet Explorer.



An important note about the password:

If you enter the password wrong, you'll get the following error: "Unable to access the Protected item. Please verify that the password you entered is the correct one." The Microsoft certificate store will allow you to create a "false" backup file if you enter the wrong password three or more times. This "false" file will look like a real certificate backup file, but it won't include your certificate's private key. To avoid any possibility of creating such a false file, we strongly recommend that you cancel out of the backup process and start over from the beginning if you receive "Unable to access the Protected item" two times.

12. An alert box will notify you that the backup was successful. Congratulations! You've made a secure backup copy of your ACES Business Certificate!