# ACES Enrollment Key Backup for Internet Explorer

The Enrollment Key Pair is created when you make an online request for a certificate. There will be one Enrollment Key Pair for each certificate request that you have made. Your computer will look for this Enrollment Key Pair when you attempt to import the issued certificate from the certificate server. This Enrollment Key Pair is NOT YET a certificate; it is, rather, the 'foundation' of the certificate (i.e., the Enrollment Key Pair will become the certificate). It has real value prior to your certificate being issued. *(But after you have made a successful backup copy of your issued certificate, that file will be the preferred method of certificate backup and restoration.)*

This procedure is recommended for Subscribers that:

- Have had certificates with a non-exportable Private Key
- Anticipate a major change or upgrade to their computer, operating system, profile, domain, etc. before they will be able to import their issued certificate and make a backup copy of their certificate
- Want to confirm that the Enrollment Key Pair for their certificate request is fully functional.

A successful backup of the Enrollment Key Pair will confirm:

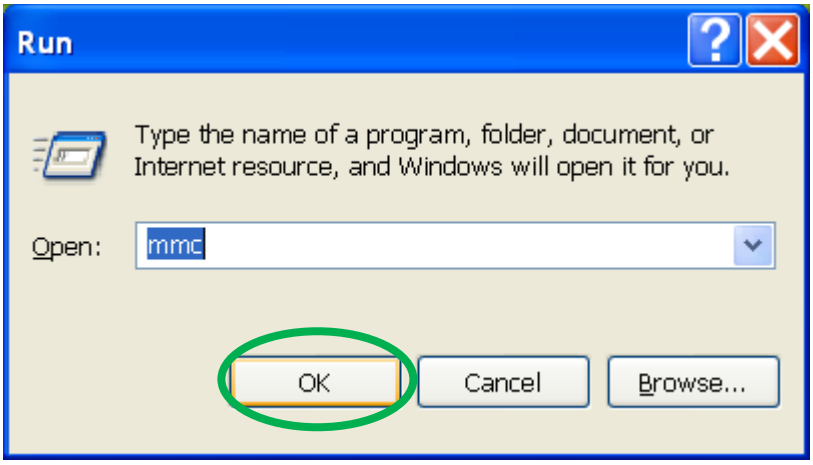
- that the Private Key for your future certificate is fully functional
- that you have set a password on your future certificate's Private Key
- that you and your computer agree on what that password is
- that you have an 'insurance policy' for the success of the entire certificate procedure *(The ACES Help Desk can solve nearly every problem if you have a backup copy of your certificate Enrollment Key Pair.)*

NOTE: These instructions were created on a computer running Windows XP. If you submitted your requests for ORC ACES-Business identity (and encryption) certificate(s) through Internet Explorer on Windows 7 or on Windows 8, some of the dialog prompts may vary.

1. Click on the Windows "**Start**" button for your computer.

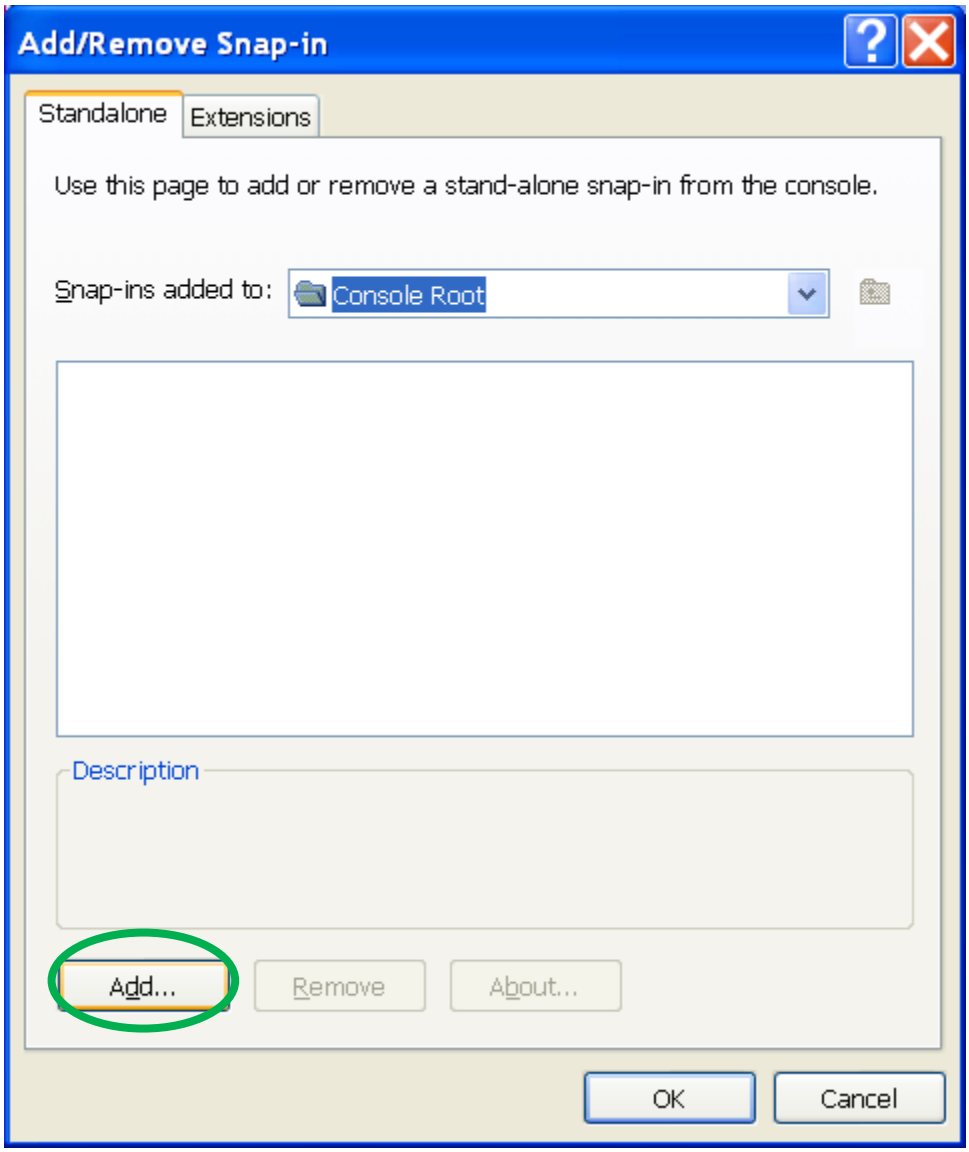
2. Select "**Run**" from the list.

3. Type in "**mmc**" and click the "**OK**" button. If your computer's operating system is Windows 7 or Windows 8, you can search for **MMC**.

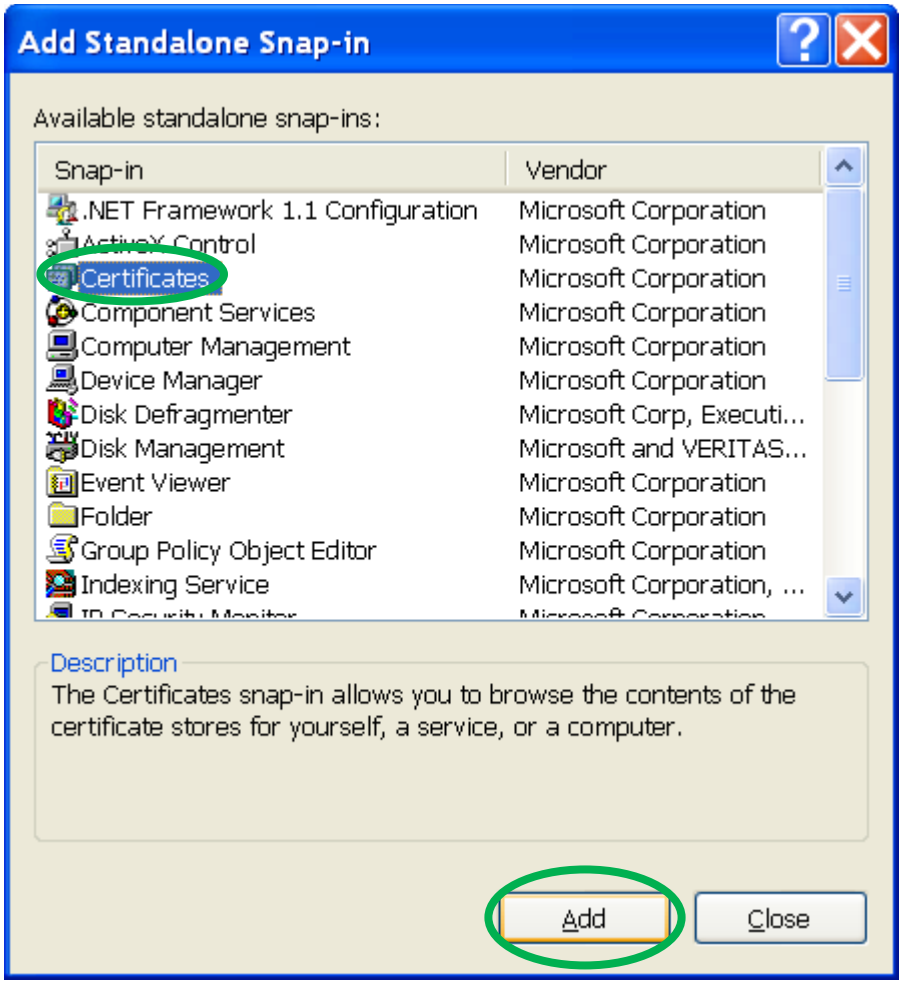



4. Select "**Add/Remove Snap-in**" under the "**File**" menu.

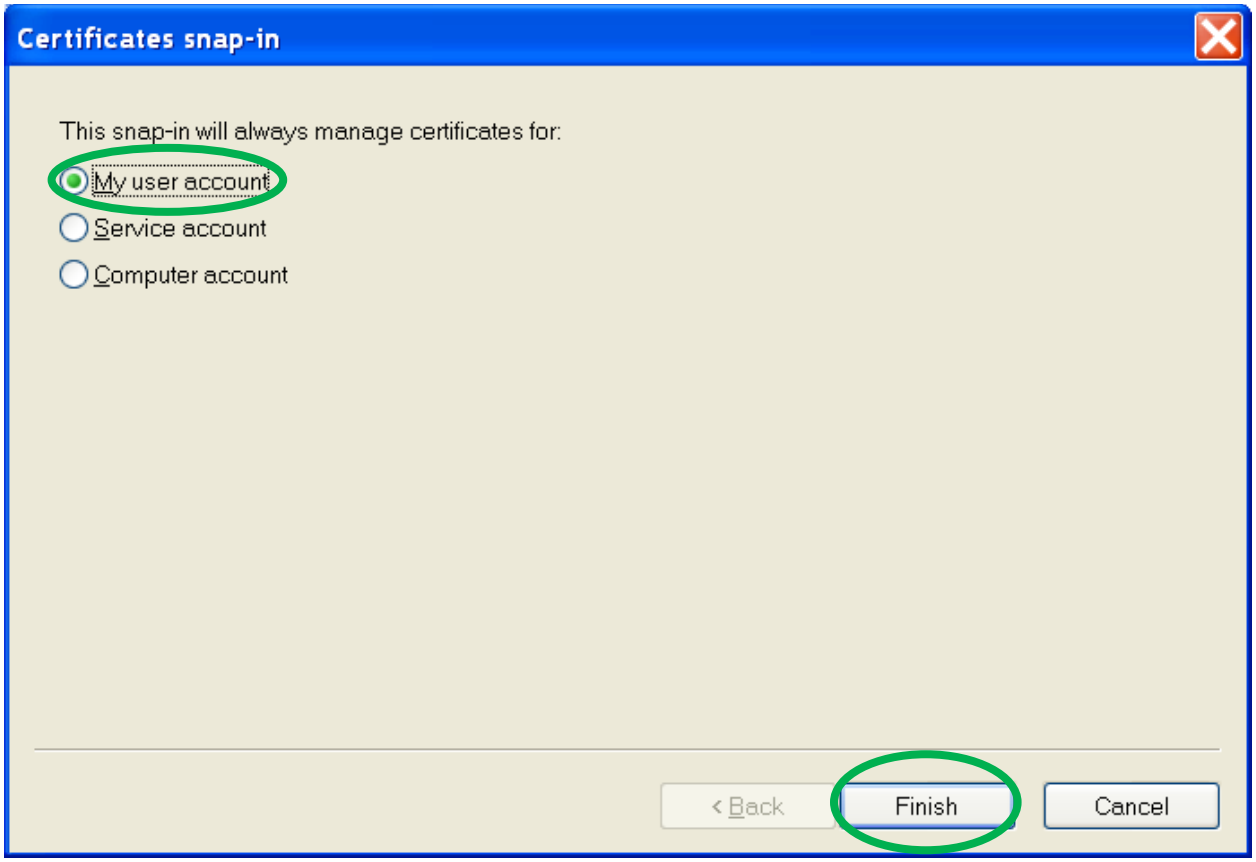
5. At the "**Add/Remove Snap-in**" dialog, click the "**Add**" button.



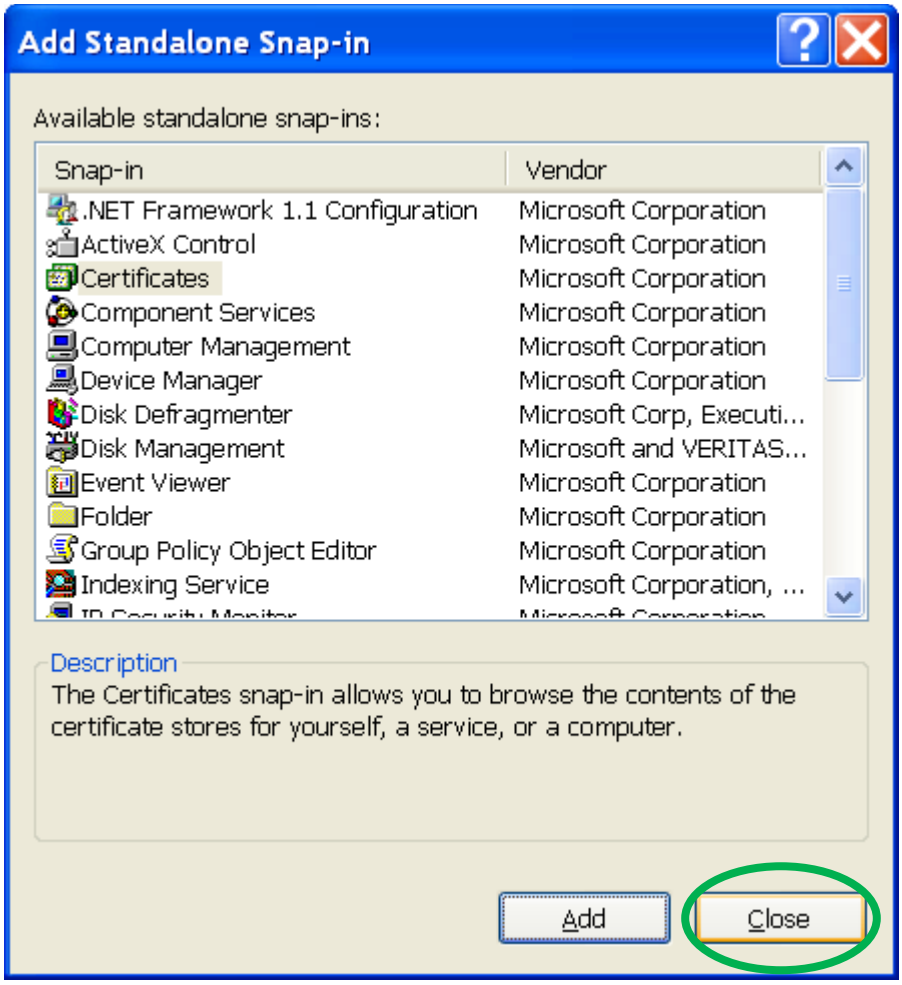
5. Select "**Certificates**" in the "**Add Standalone Snap-in**" dialog and click "**Add**".



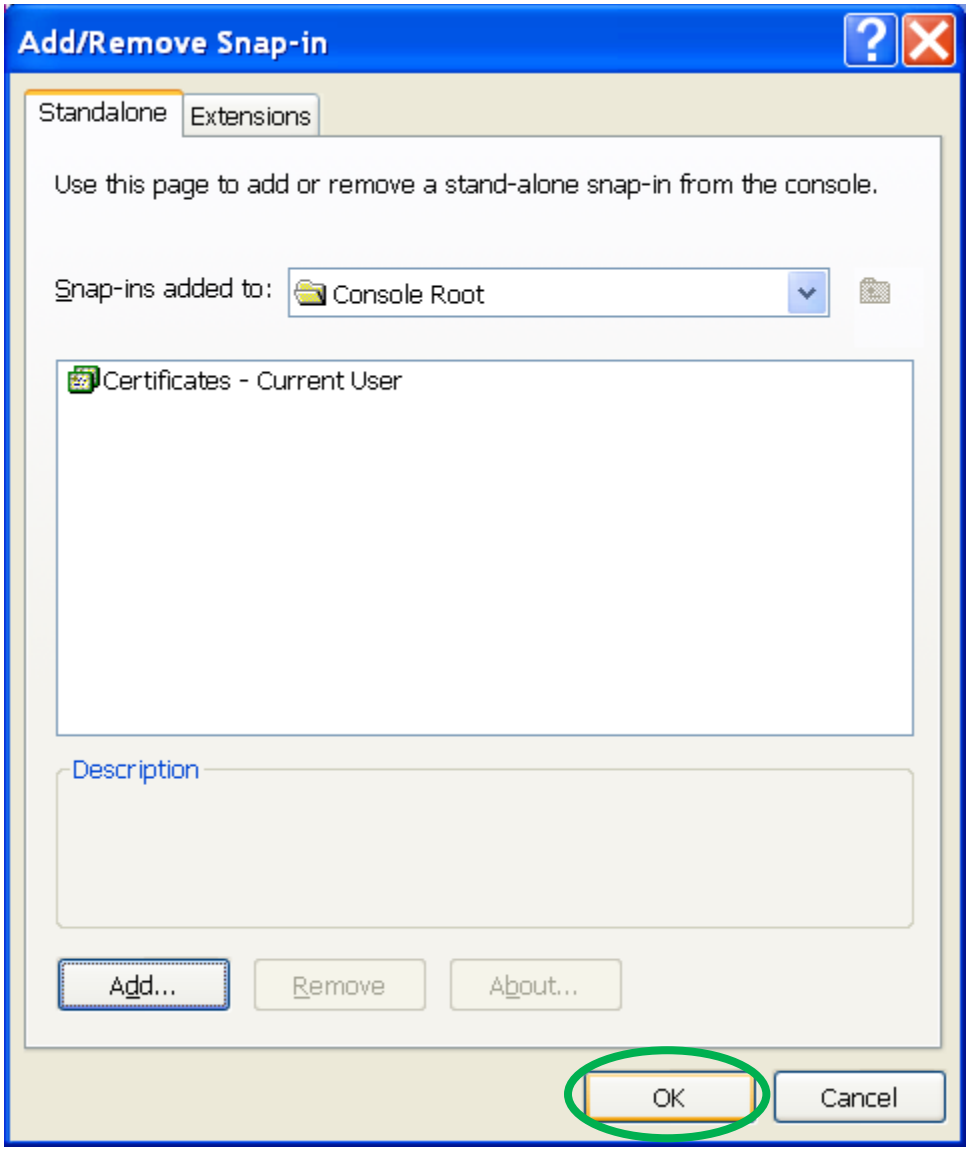
6. At the "**Certificates snap-in**" dialog, select "**My user account**" and click "**Finish**".



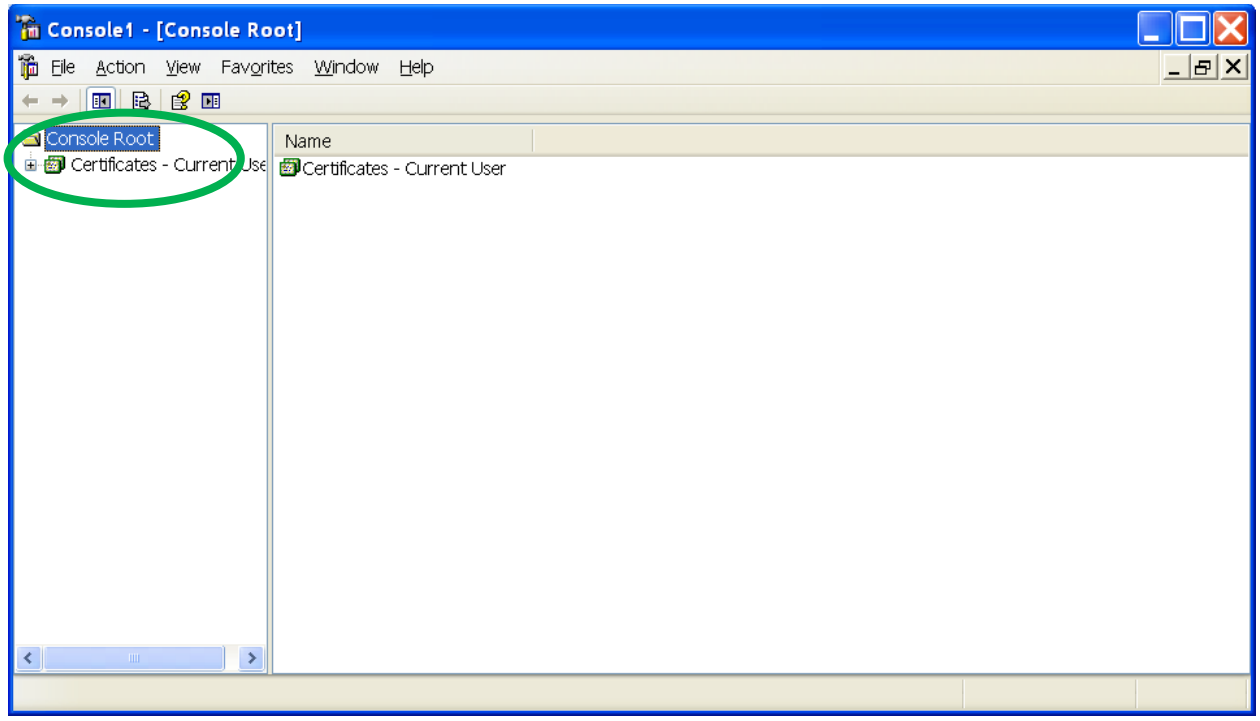
7. Click "**Close**" to close the "**Add Standalone Snap-in**" dialog.



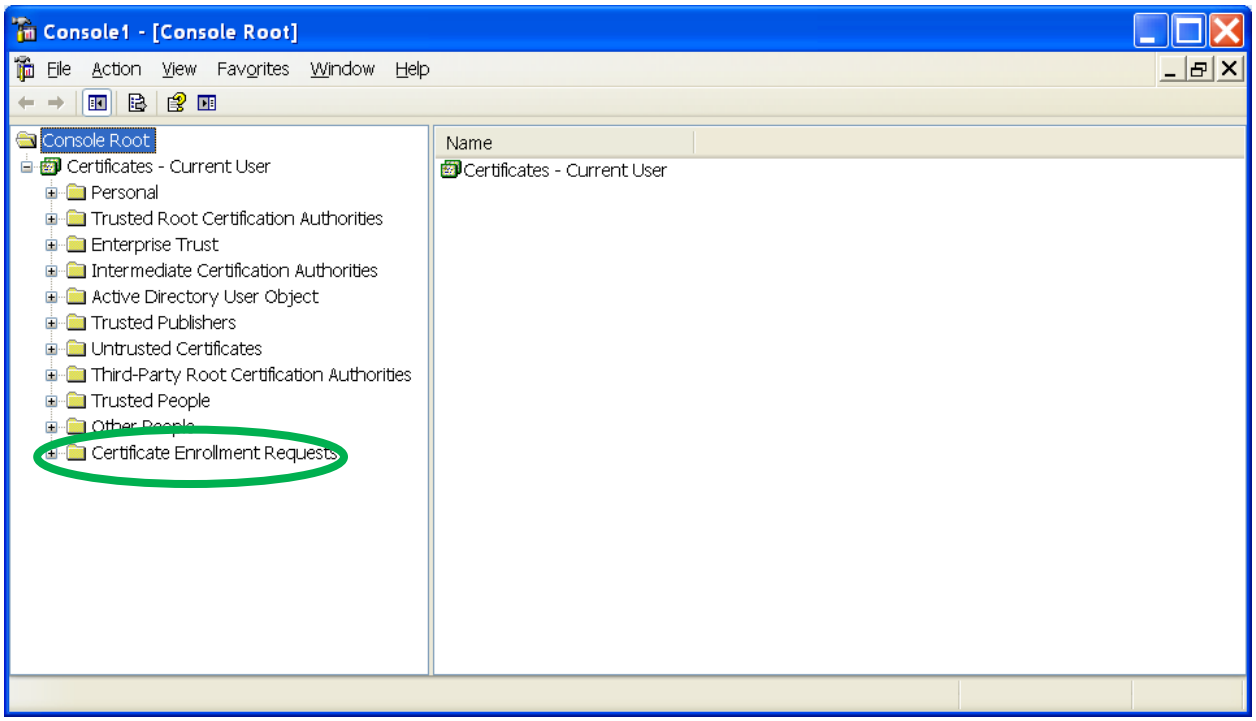
8. Click "**OK**" to close the "**Add/Remove Snap-in**" dialog.



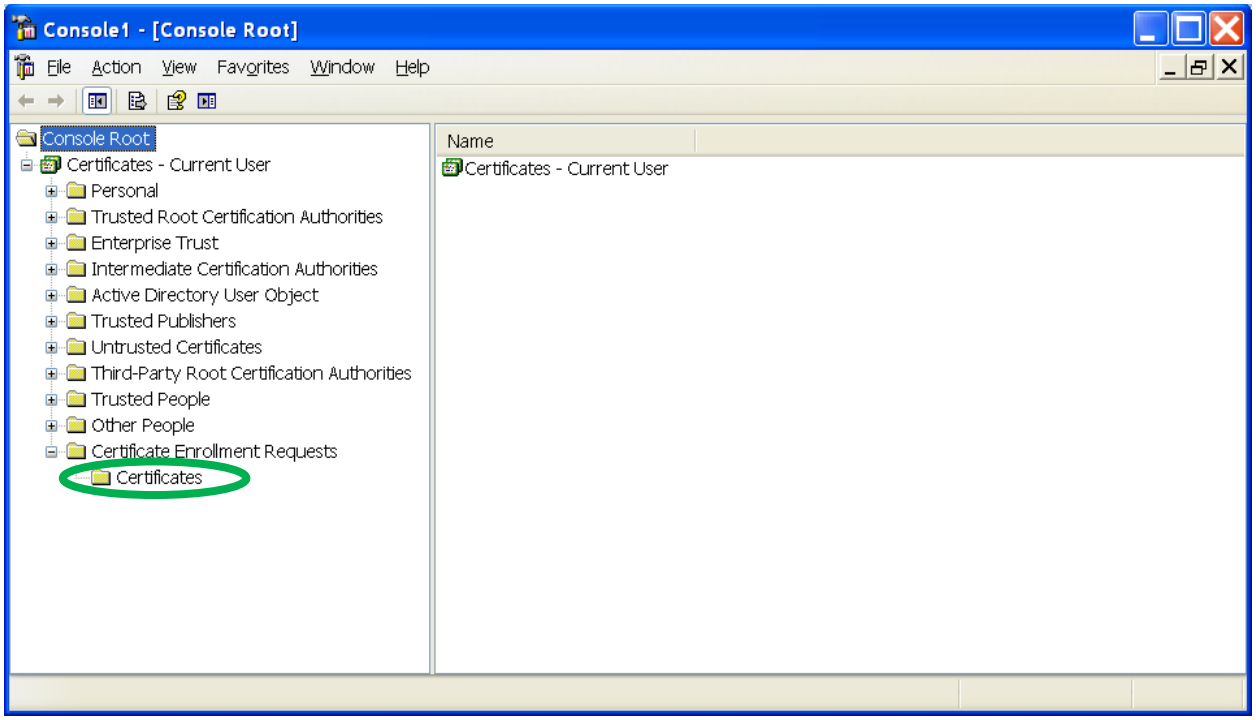
9. Click the plus sign under "**Console Root**" to expand "**Certificates - Current User**".



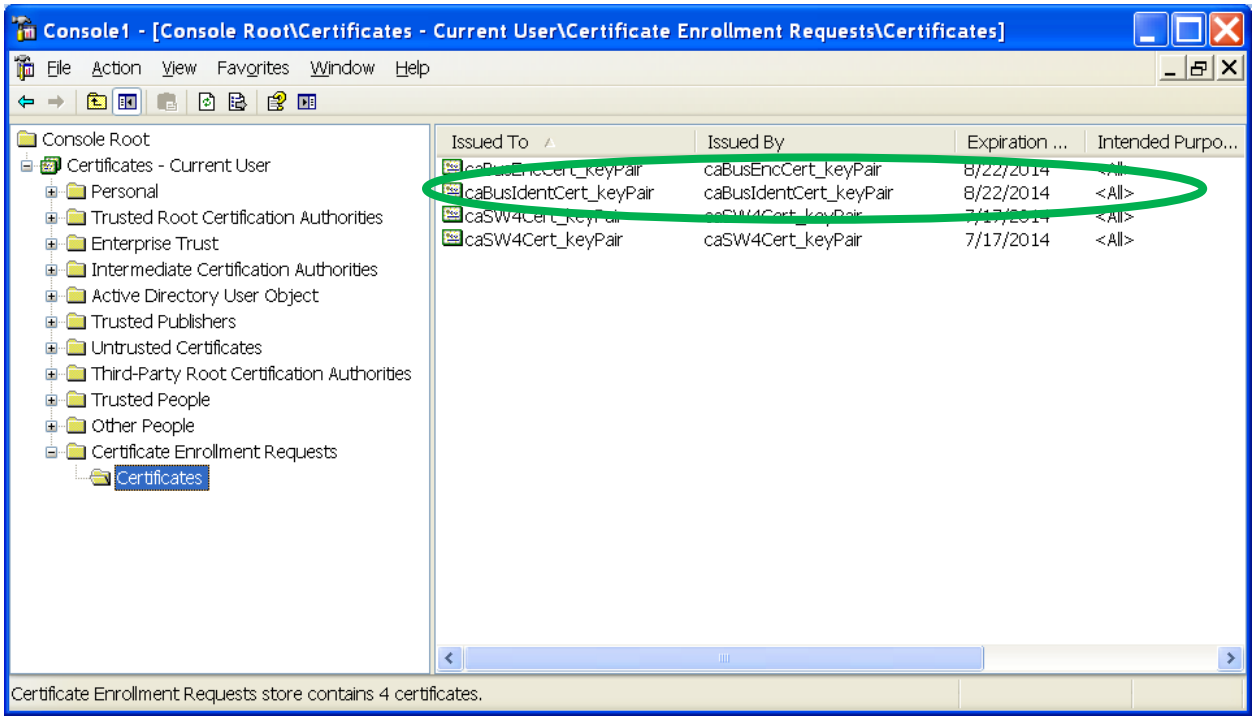

10. Click the plus sign to expand "**Certificate Enrollment Requests**".



11. Select the "**Certificates**" folder under "**Certificate Enrollment Requests**".



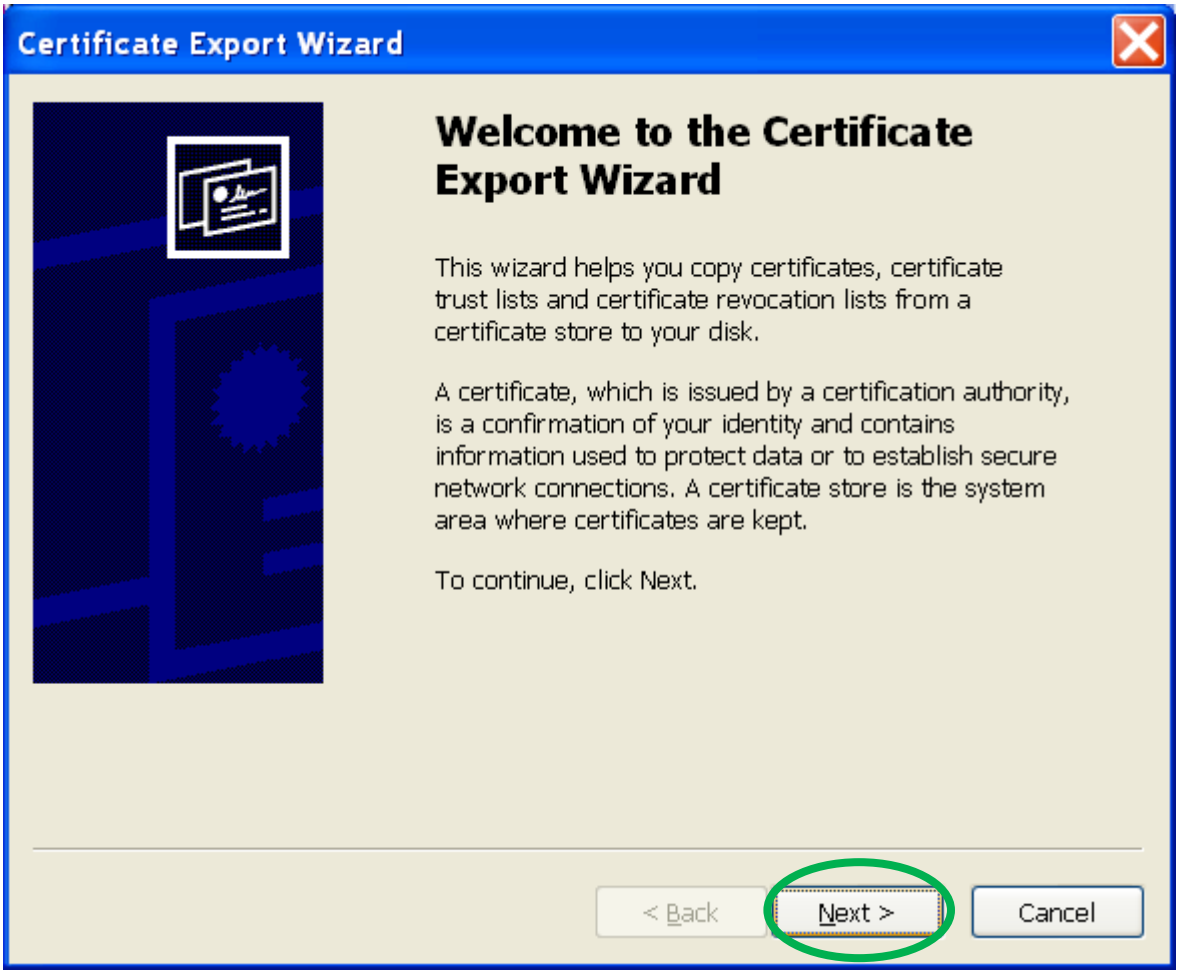
12. In the "**Certificates**" folder under "**Certificate Enrollment Requests**", there should be two entries named "**caBusIdentCert_keyPair**" and "**caBusEncCert_keyPair**" if you have requested one ORC ACES Business identity certificate and one ORC ACES Business encryption certificate. If you only requested an ORC ACES Business identity certificate, you will only see the entry named "**caBusIdentCert_keyPair**".




NOTE: The 2 files named "**caBusIdentCert_keyPair**" and "**caBusEncCert_keyPair**" are the enrollment keys created during the submission of requests for the ORC ACES-Business identity certificate and for the ORC ACES-Business encryption certificate through Internet Explorer. The expiration date for the enrollment keys is one year from the date of ORC ACES certificate request submission. The expiration date of the enrollment keys will not affect the 2 year validity period of the ORC ACES-Business identity (and encryption) certificate(s).

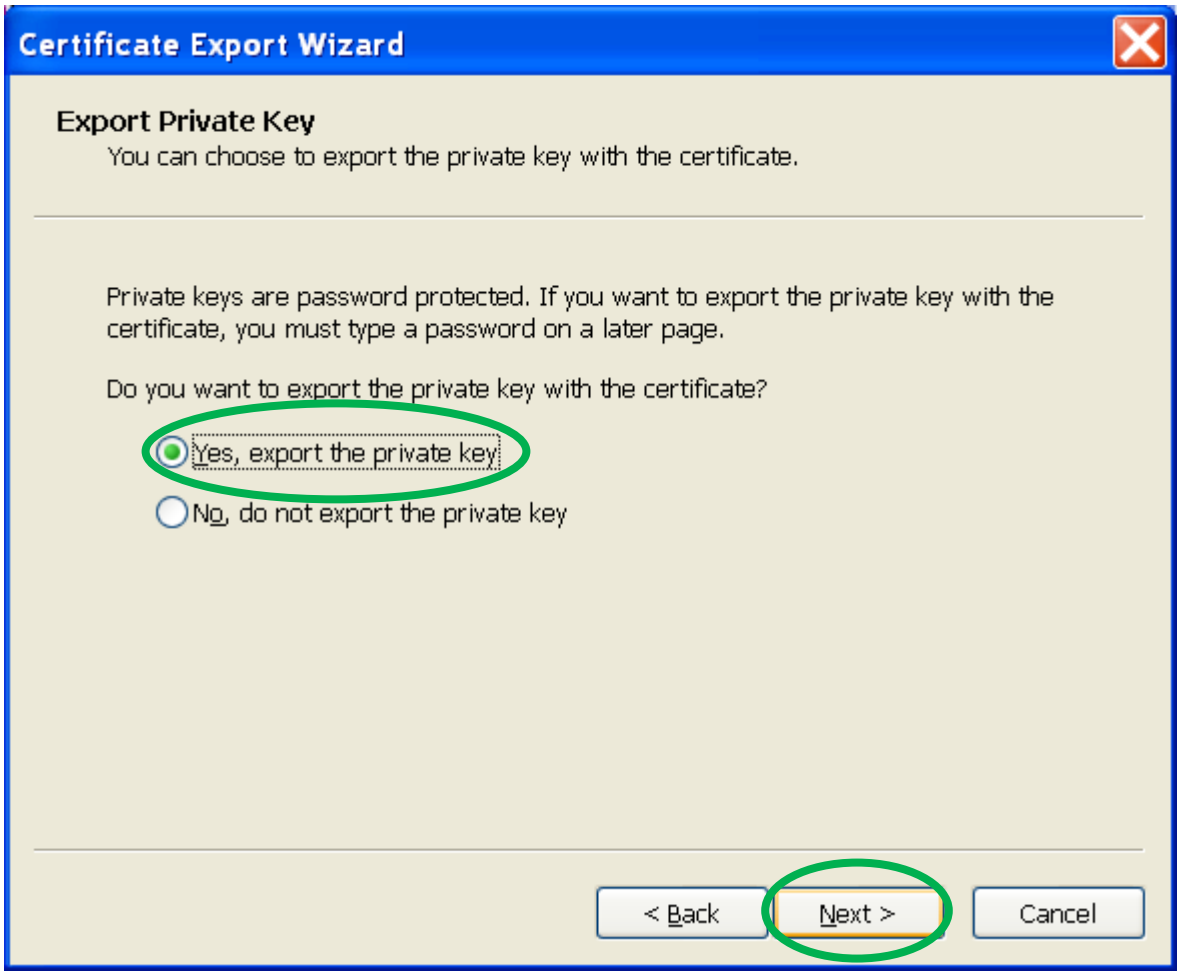
13. **Right Click** on the "**caBusIdentCert_keyPair**" entry and select "**All Tasks**" then "**Export...**".

14. Click "**Next**" in the "**Certificate Export Wizard**" pop-up window.



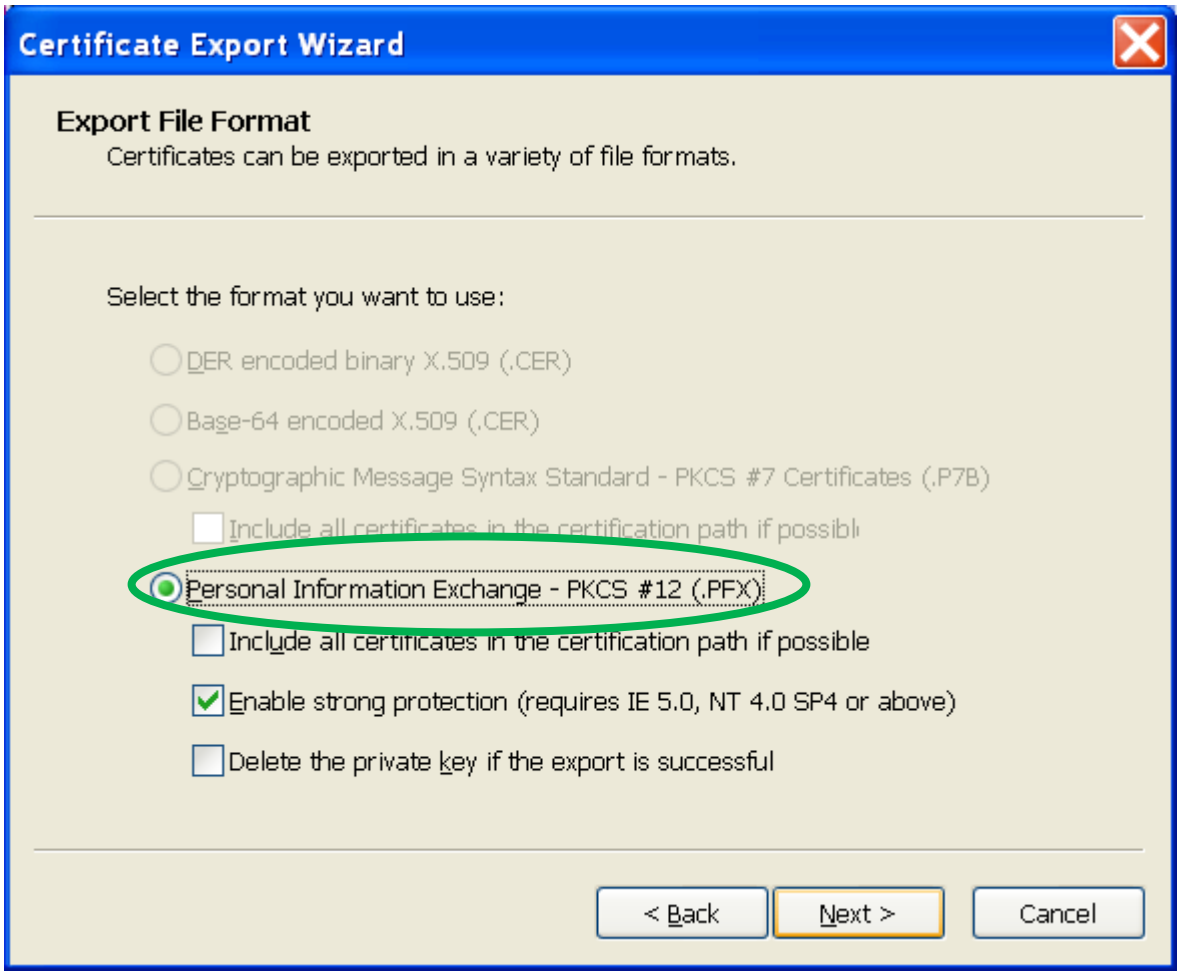
15. Ensure that "**Yes, Export the Private Key**" is selected and click "**Next**".

NOTE: If you cannot select **Yes, Export the Private Key**, STOP! The Private Key for this certificate Enrollment Key Pair has already been marked as non-exportable. That means that you will not be able to make a backup file of a certificate that might be issued against this Enrollment Key Pair. Contact the ORC ACES Help Desk.

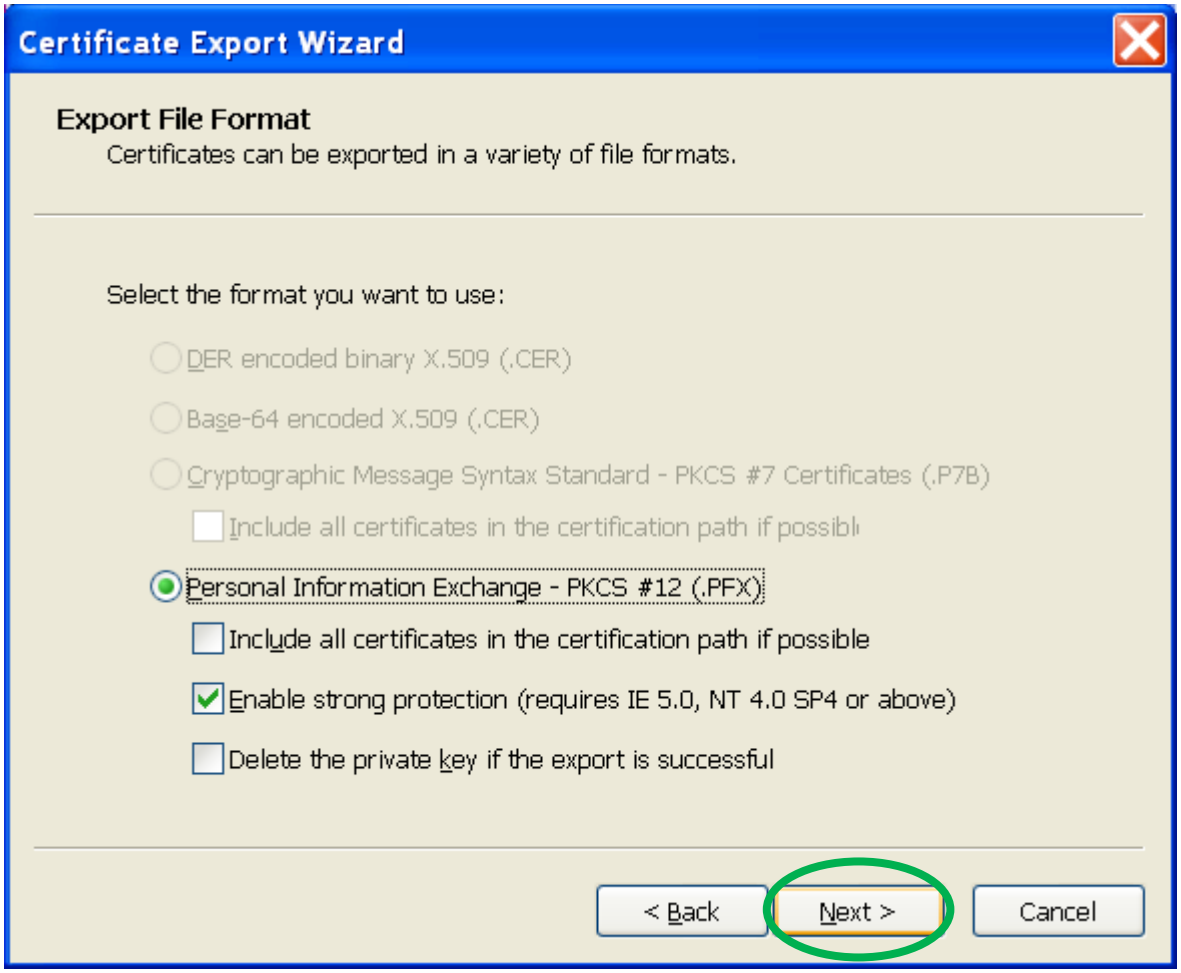


16. Make sure that "**Personal Information Exchange**" and "**Enable Strong Protection**" are selected.

NOTE: More recent versions of Windows (e.g. Windows 7 and Windows 8) might not display "**Enable Strong Protection**" option under "**Personal Information Exchange – PKCS #12 (.PFX)".** If that is the case, please ensure that only "**Personal Information Exchange – PKCS #12 (.PFX)**" is selected.

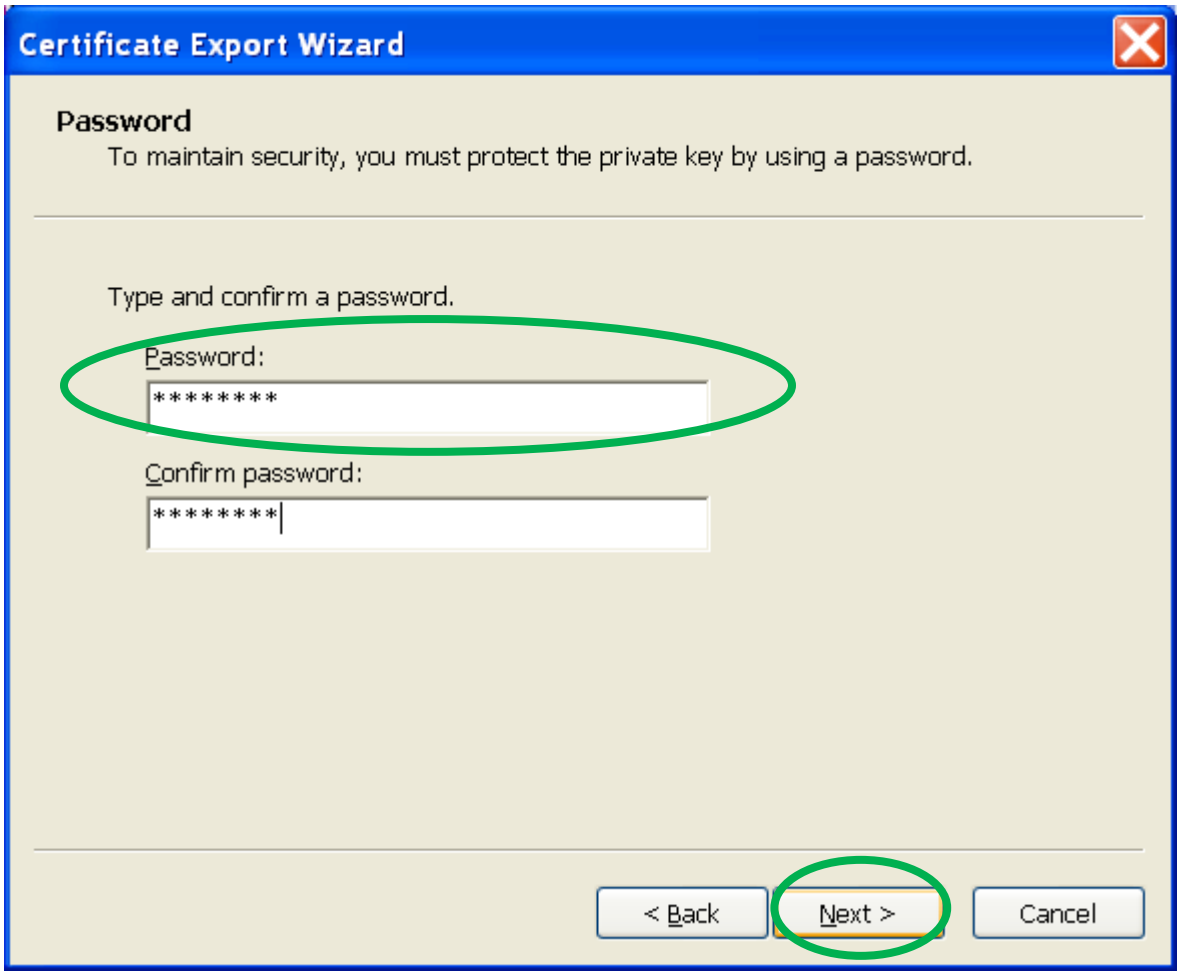


17. Then click "**Next**" on the "**Export File Format**" screen.

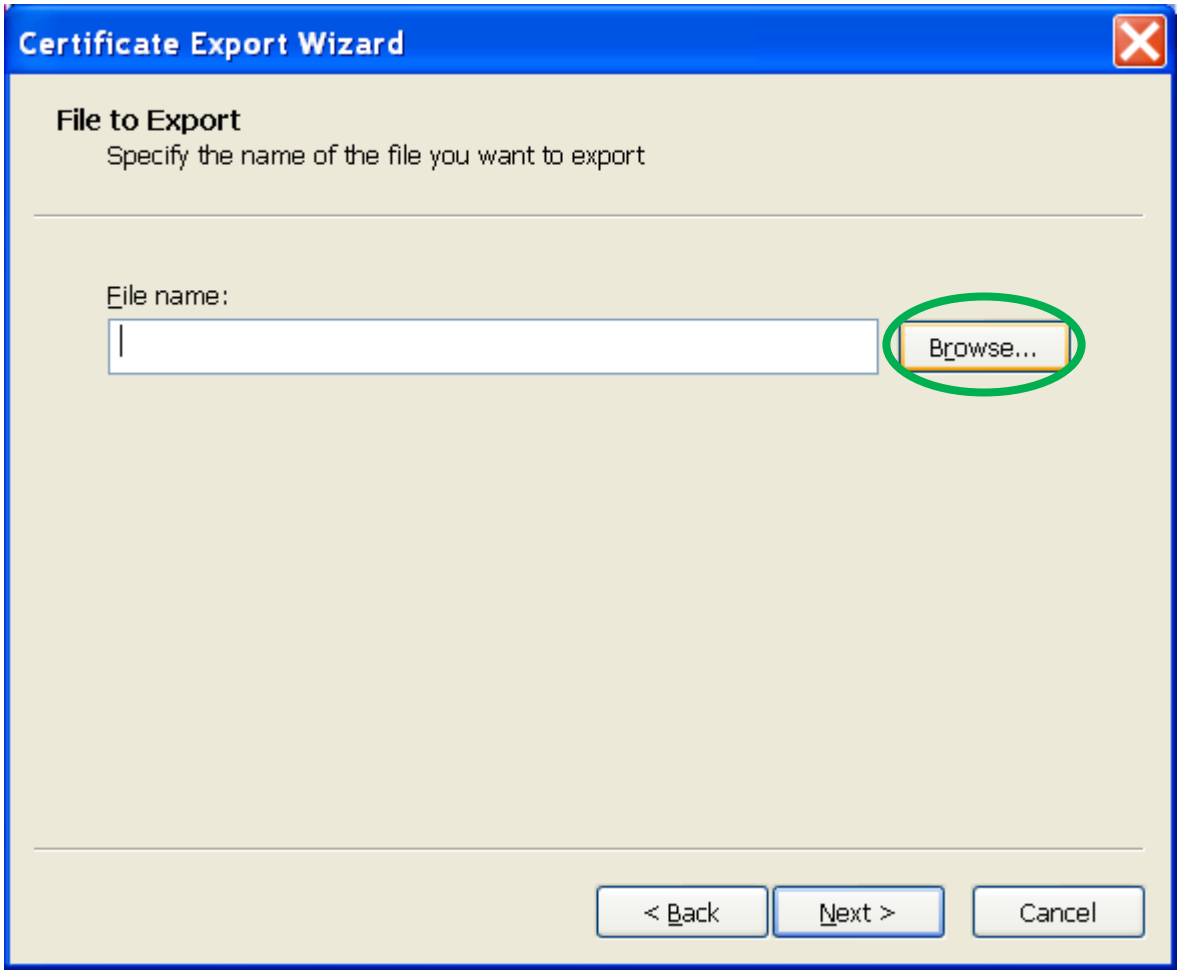


18. Enter the **Private Key Password** to protect the file being created. Then click "**Next**".

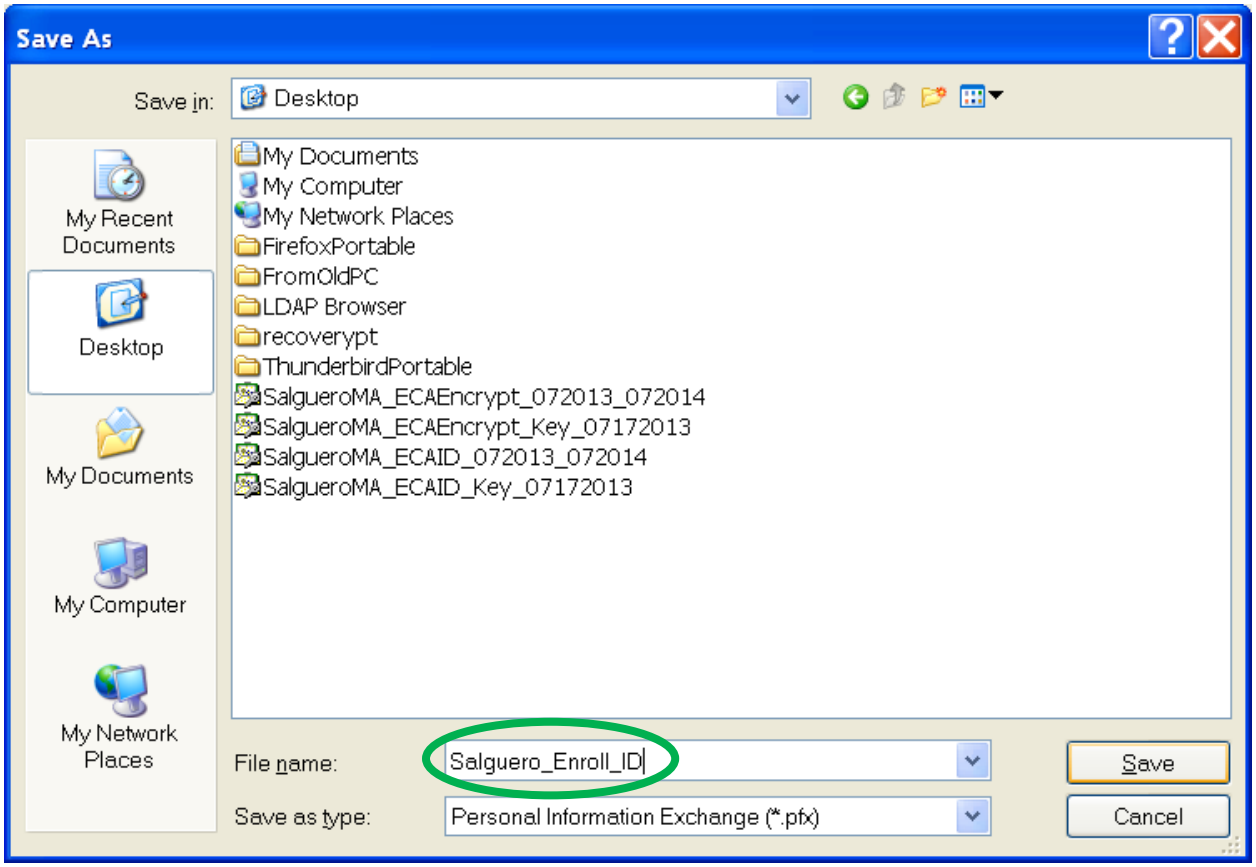
**NOTE: You must type the same private key password here that you created when you requested your ORC ACES-Business identity certificate through Internet Explorer. The private key password is case-sensitive.**



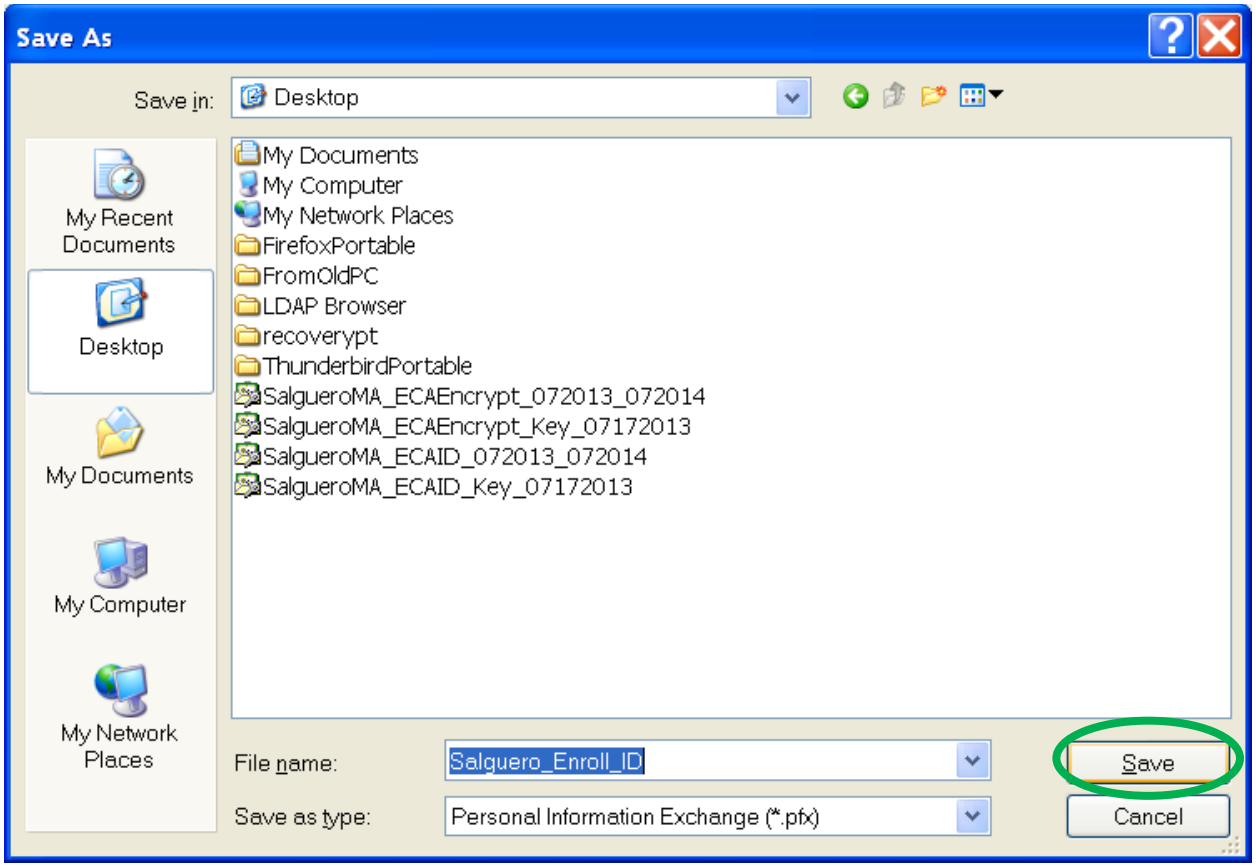
19. Click "**Browse**" on the **File to Export** dialog. Select where you want to save the operational copy of your private key(s). If you save the backup copy of the private key (aka enrollment key) to Desktop, please ensure that you save the .pfx file for the private key to external device (e.g. flash drive, network share folder) as soon as possible. *Make sure that you are the only person with access to your private key copy*.



20. ORC's recommended filename convention is "*yourlastname*_Enroll_ID" (Or "*yourlastname*_Enroll_EN" for an Encryption Certificate Enrollment Key Pair).



21. Click "**Save**".

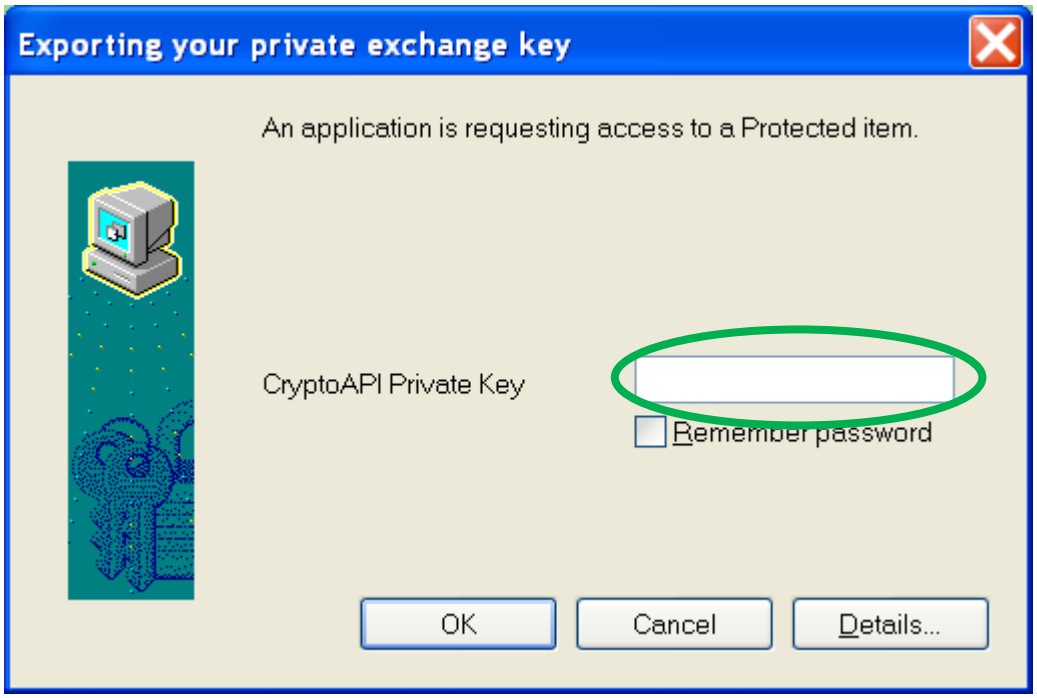



22. Click "**Next**" on the **File to Export** dialog.

23. Click "**Finish**" to complete the saving of your private key.

24. A pop-up window will ask for the private key password that you created when you requested your ORC ACES-Business identity certificate. Enter the **private key password**. Then click "**OK**".

NOTE: Do NOT check the "**Remember password**" box.




25. Another window should appear stating, "**The Export was Successful**". Click "**OK**" to close this window.


NOTE: If you also submitted a request for an ORC ACES Business Encryption Certificate through Internet Explorer, please follow the instructions you used above for saving the ORC ACES Business Identity Certificate private key, but instead **Right Click** on the "**caBusEncCert_keyPair**" entry and select "**All Tasks**" then "**Export...**".