Importing your personal certificate(s) to Microsoft Internet Explorer from a Back-up (or export) file

You may use your Medium Assurance Certificate(s) on any computer that you wish to by importing them onto that computer from a certificate back-up (or export) file. You can identify certificate back-up files from their associated file extensions. Certificate back-up files will have a file extension of ".pfx" or ".p12" (".pfx" is the file extension created when making back-up files from Microsoft Internet Explorer. ".p12" is the file extension created when making back-up files from other applications, like Mozilla Firefox. Most applications that read one of those file types will read both of them.) You will need to know where your certificate back-up files are located, so it is a good idea to search for them before you start the process. The Microsoft icon for a certificate back-up file, looks like this:

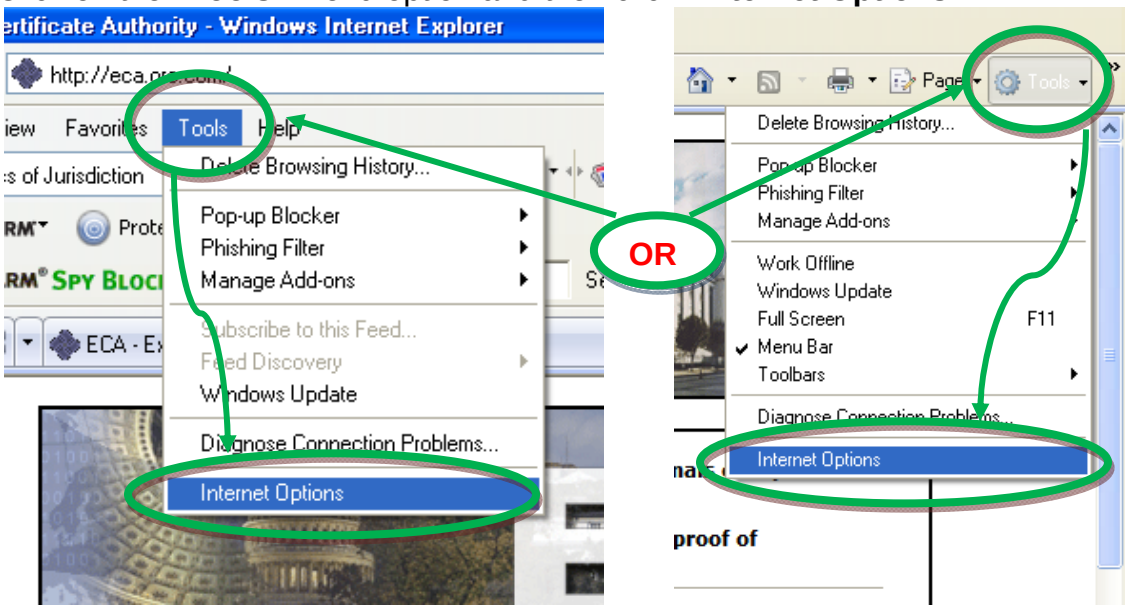
NOTE: These instructions are intended for importing personal Medium Assurance Certificates. Medium Assurance Certificates include Identity and Encryption certificates (personal certificates – used by a person). Medium Assurance Certificates are often referred to as "browser-based certificates" or "software (soft) certificates."
These instructions are not meant for "hardware-based certificates." Hardware based certificates are created on a smart card, or cryptographic token, or other cryptographic device. You cannot import "hardware-based certificates" from an import file, because you cannot create a back-up file of a "hardware-based certificate." (But there should be no need to do so, since the certificate private key resides on the device and not on your computer's hard drive.) Medium-Token Assurance and Medium-Hardware Assurance certificates are "hardware-based certificates."

If you have obtained both an Identity and an Encryption certificate, then you will need to import both of these certificates. (2 certificates means 2 back-up files) The only way to tell the back-up files apart is by the name that you assign to the file.

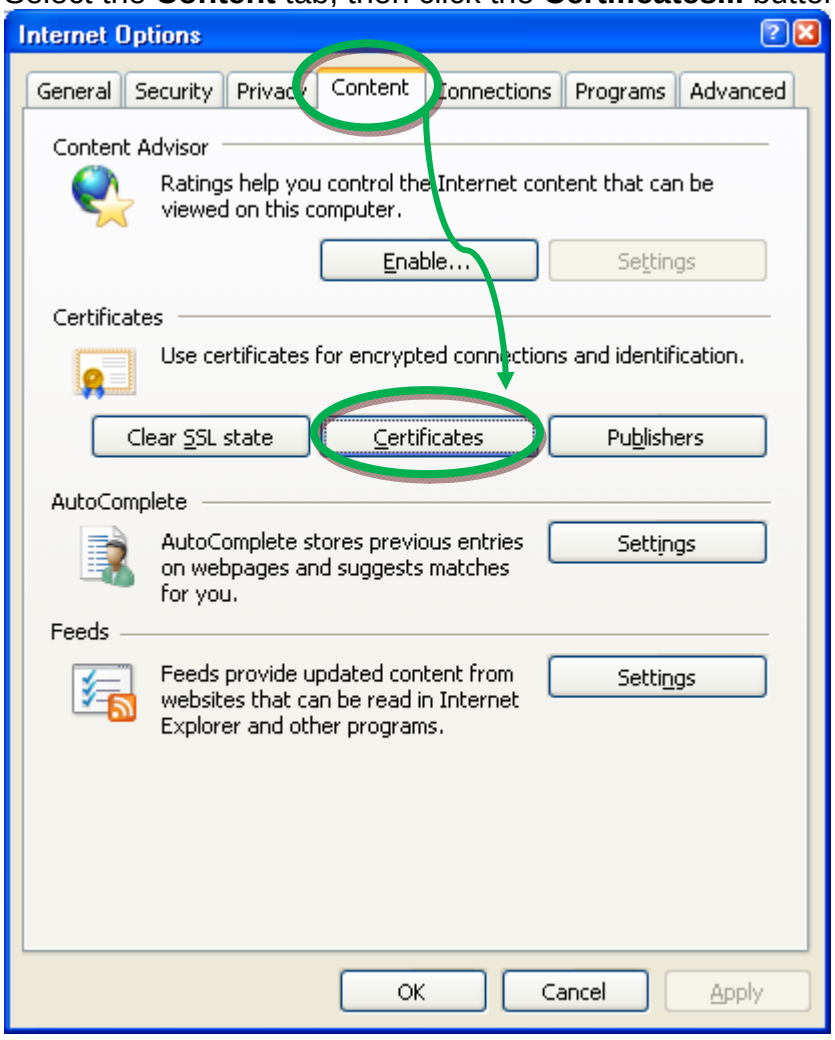
These instructions and associated screen captures were created with Internet Explorer 7 running on a Windows XP operating system. Variations in versions of Internet Explorer and the Windows Operating system will result in some variation of alert boxes and screen images. For the most part, the process and individual steps are the same across Windows platforms. (You might see a dialog box prompting you to 'allow' access on a Windows Vista/ Windows 7 computer; just click the buttons that seem to move the process forward.)

1. Start Internet Explorer

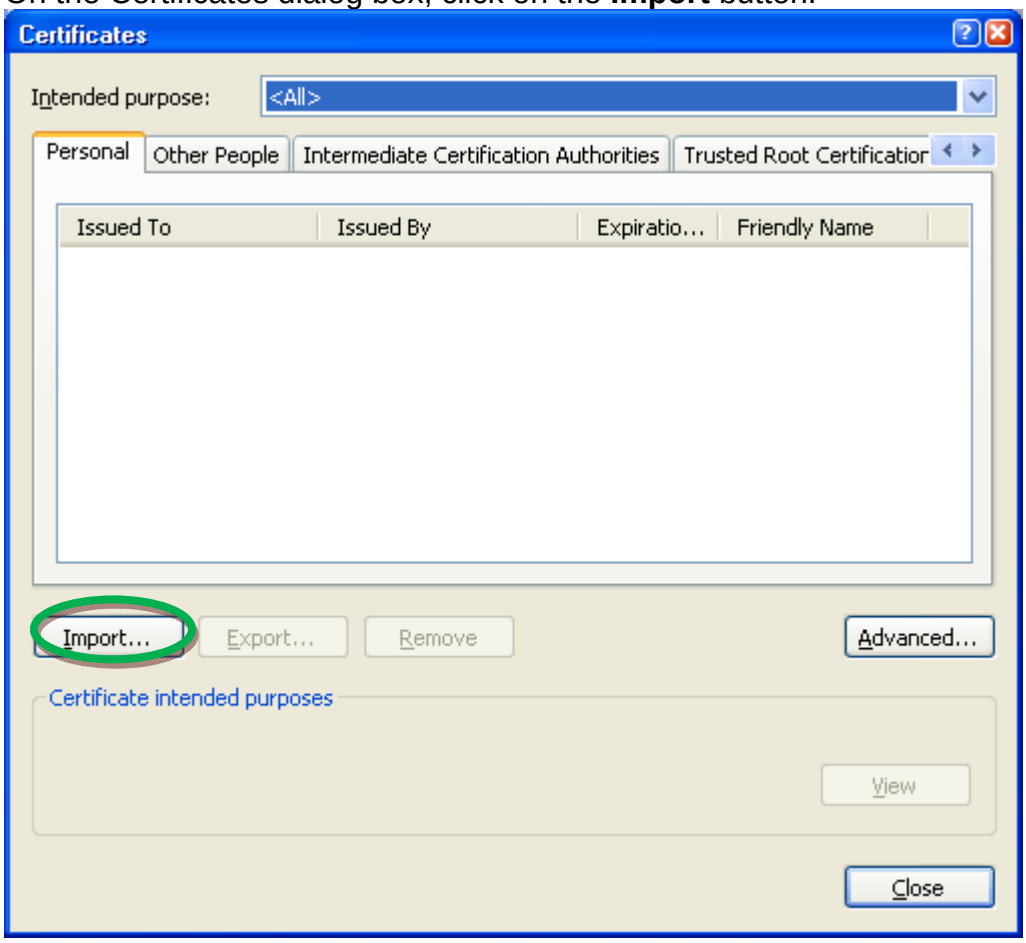
2. Click on the **"Tools"** menu option and then click **"Internet Options..."**.



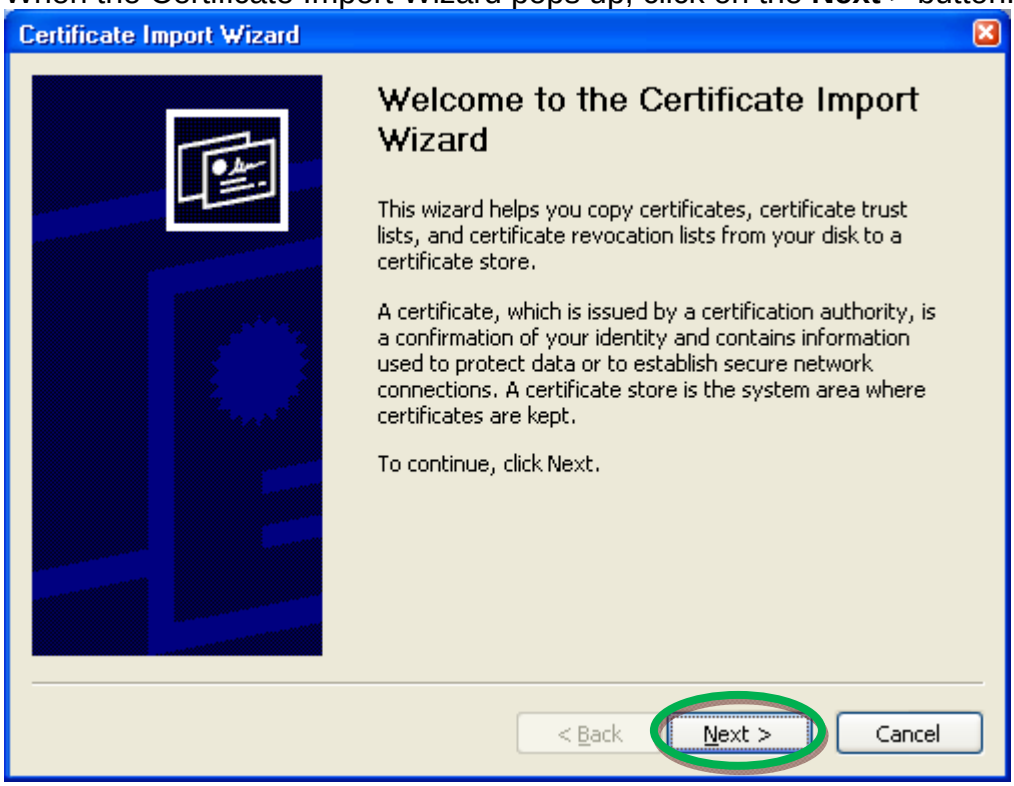
3. Select the **Content** tab, then click the **Certificates...** button.



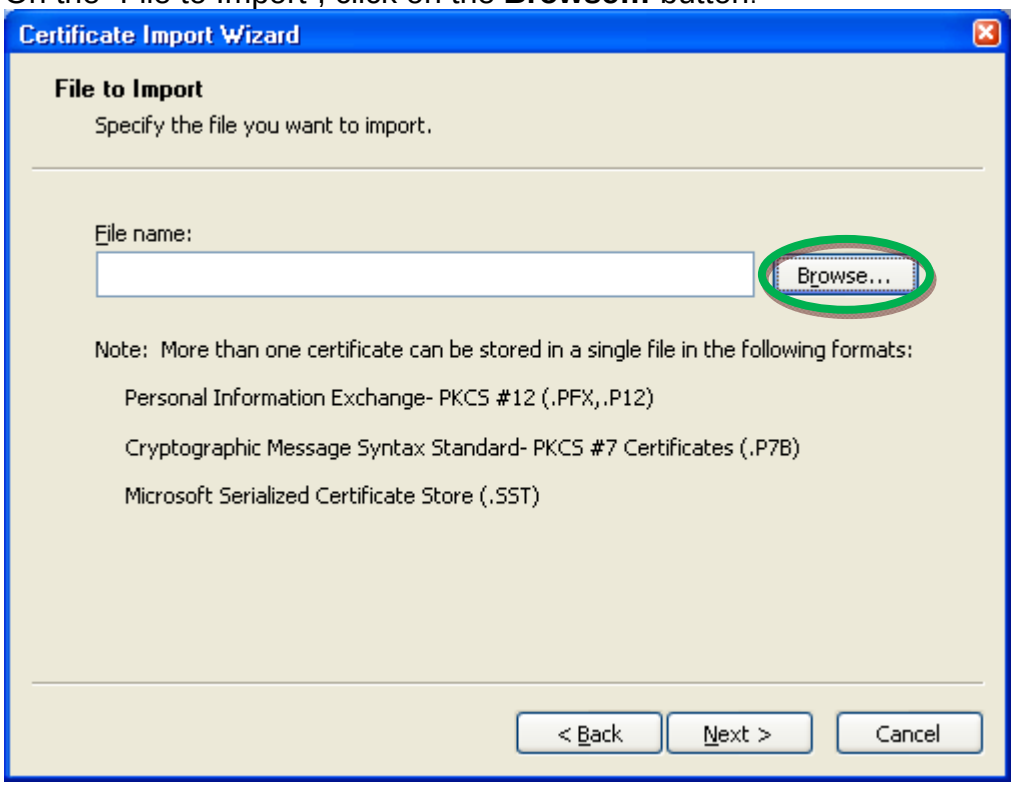
4. On the Certificates dialog box, click on the **Import** button.



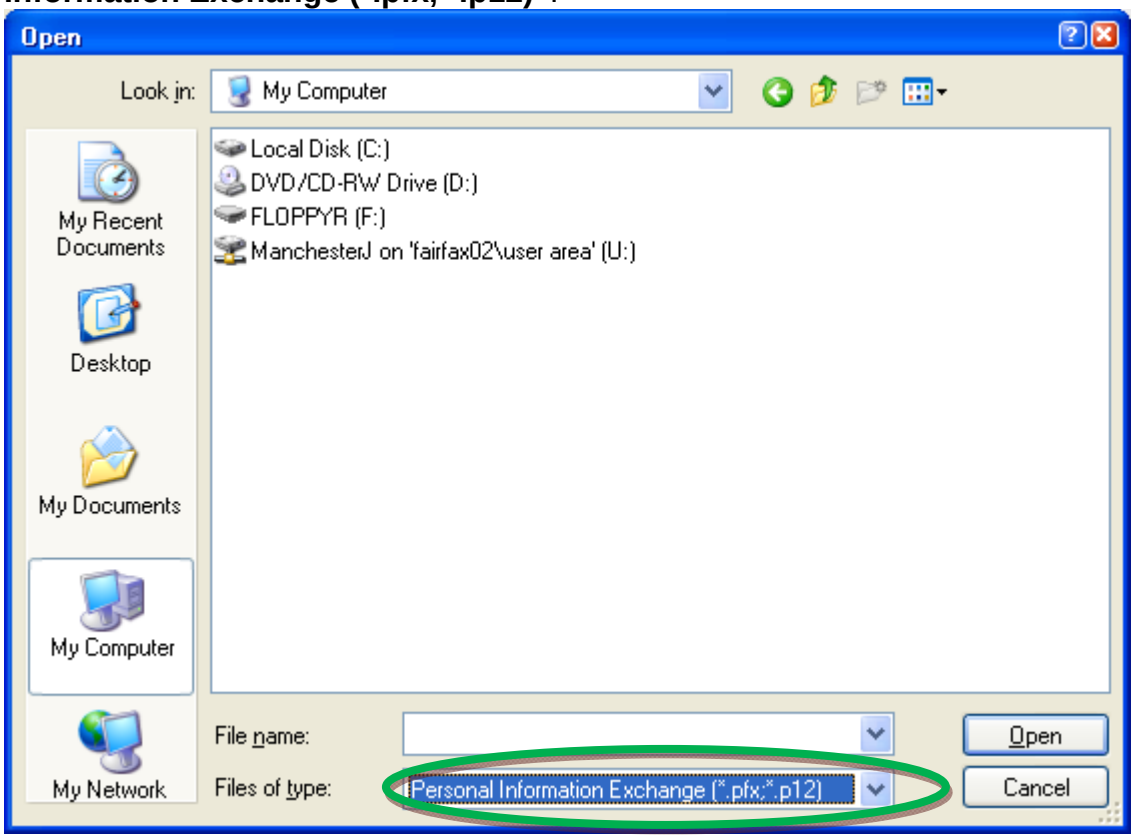
5. When the Certificate Import Wizard pops up, click on the **Next >** button.



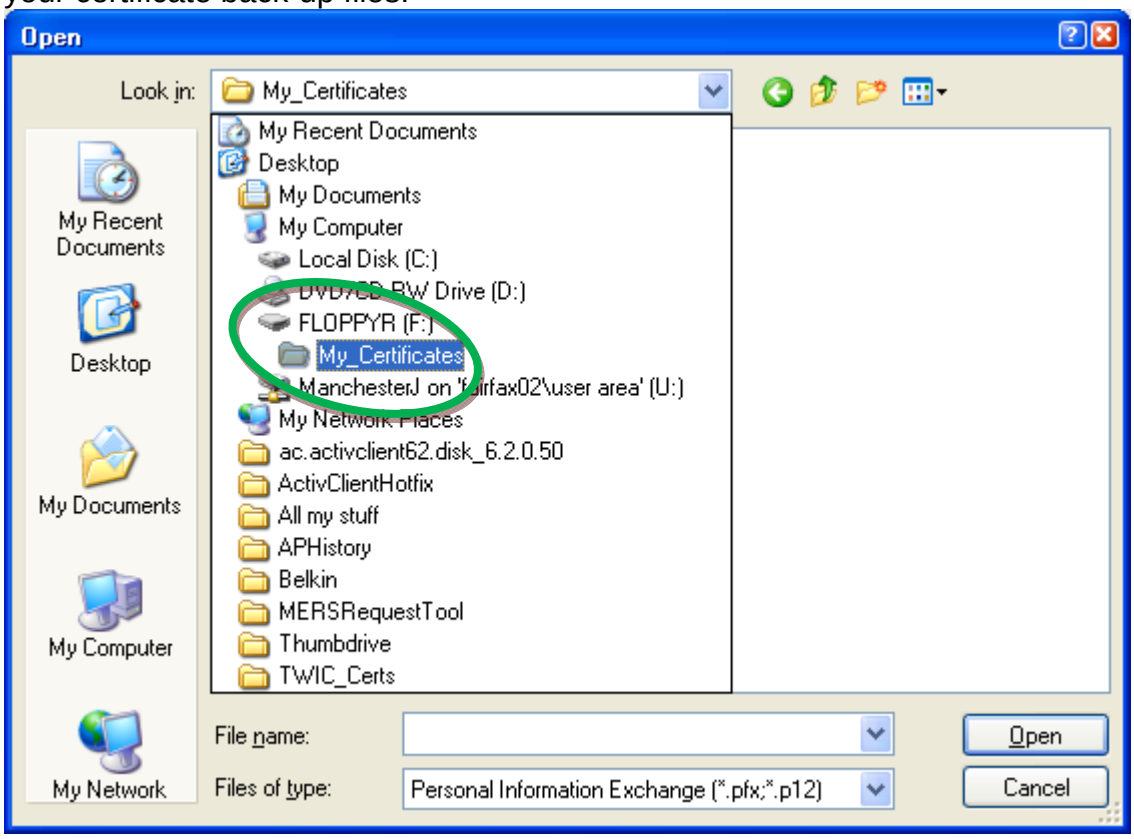
6. On the “File to Import”, click on the **Browse…** button.



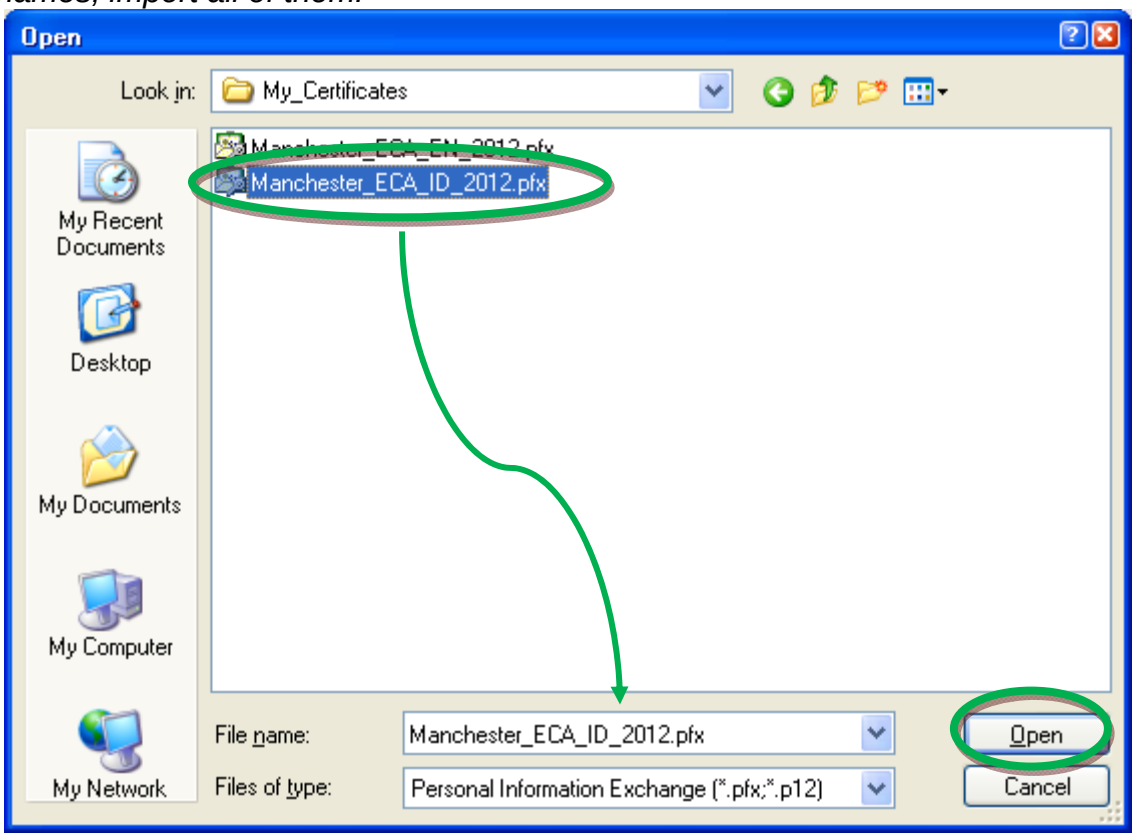
7. On the Open dialog box, change the “Files of type:” pull down to read **“Personal Information Exchange (*.pfx, *.p12)”**.



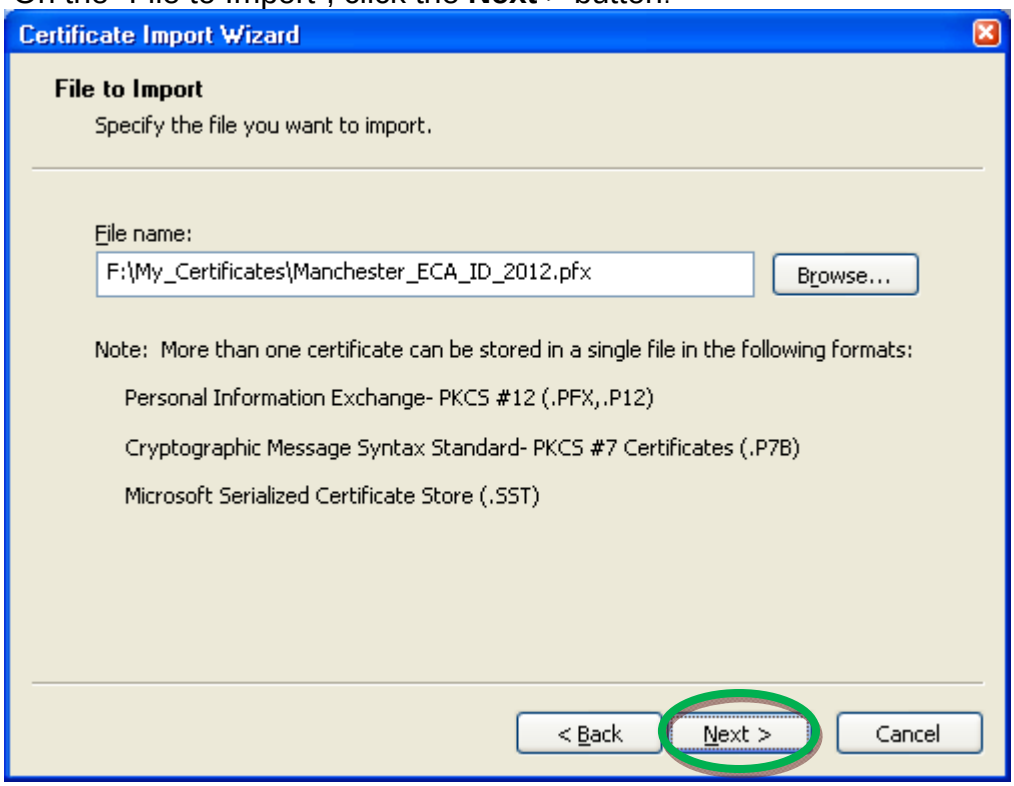
8. On the Open dialog box, use the navigation tools to navigate to the location of your certificate back-up files.



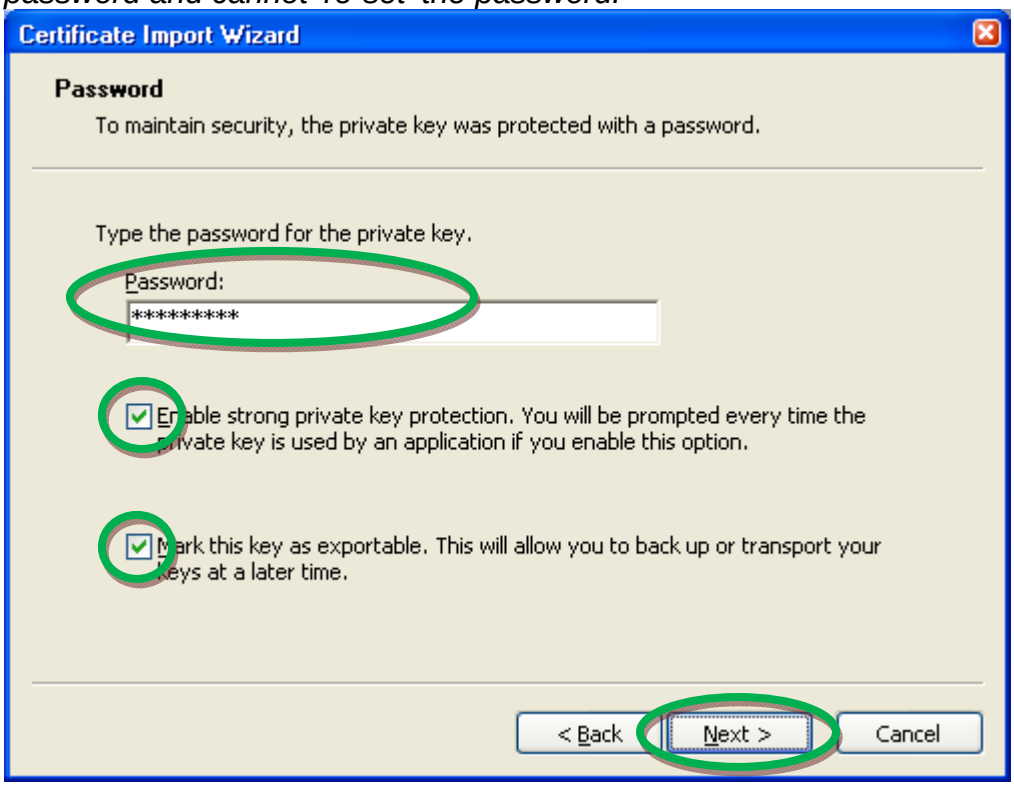
9. On the Open dialog box, select the certificate that you wish to import. (We suggest you start with your Identity Certificate.) Then click the **Open** button. *NOTE: The certificate back-up file names were assigned by you when you created the certificate back-up files. If you cannot tell which is which by the file names, import all of them.*



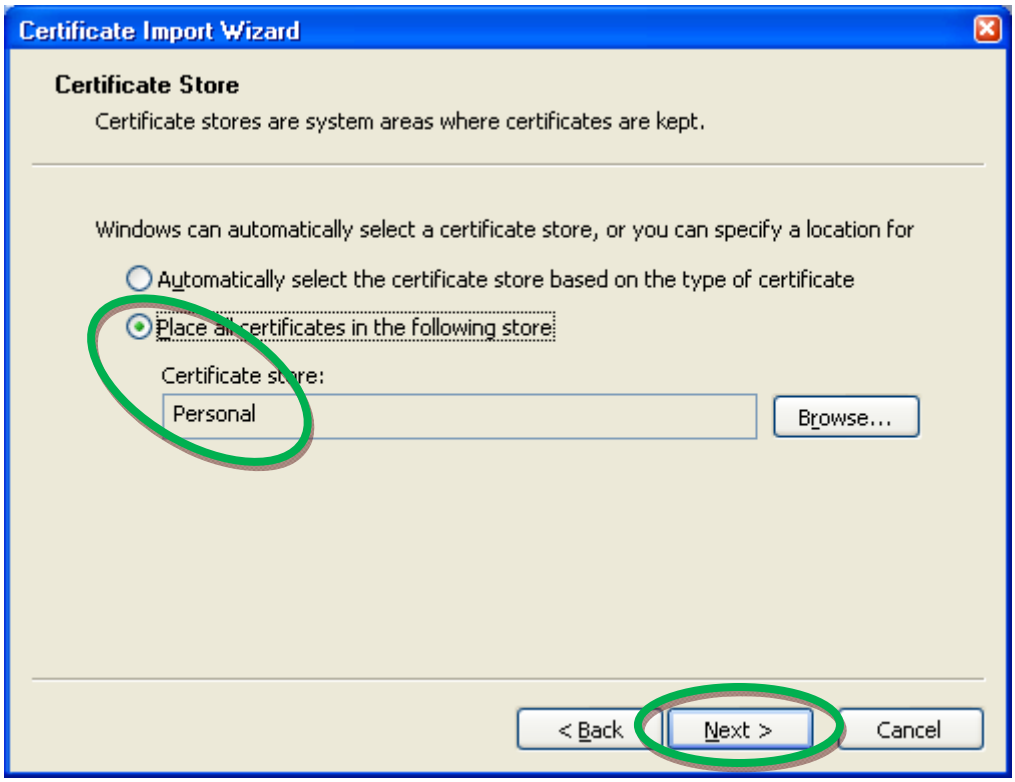
10. On the “File to Import”, click the **Next >** button.



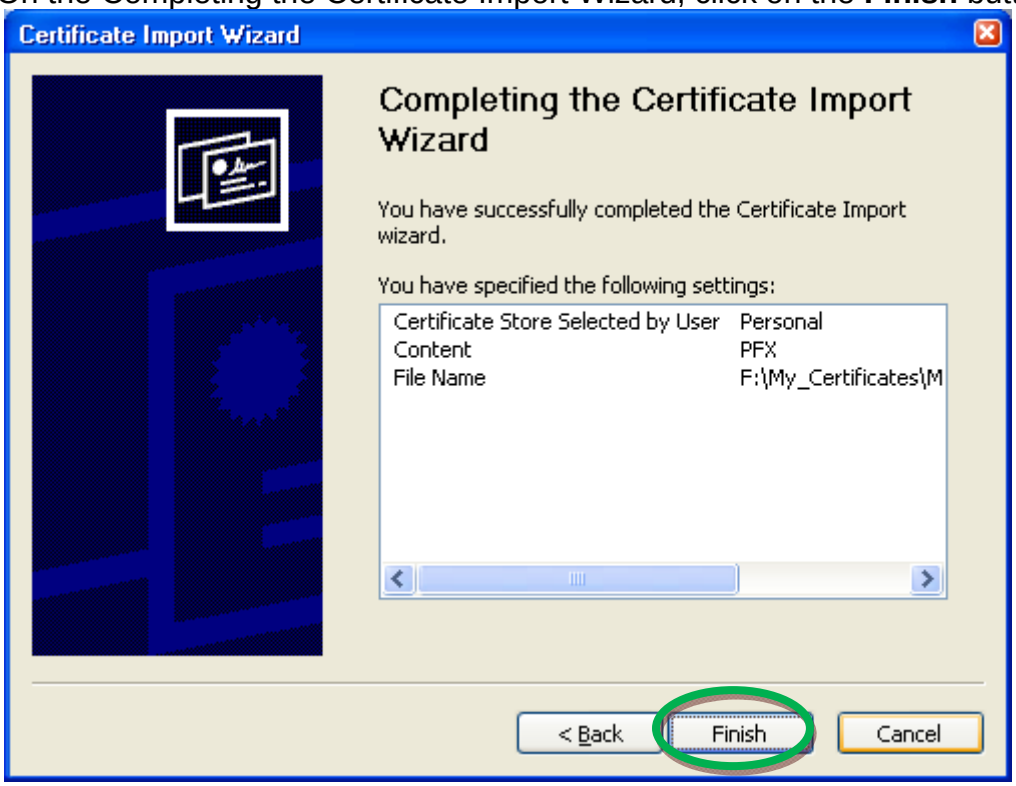
11. In the Password dialog box, enter the password that protects the certificate back-up file. Check all of the check boxes and click the **Next >** button.
NOTE: The certificate back-up file password was assigned by you when you created the certificate back-up files. If you cannot enter the correct password, then you will not be able to import the certificate. ORC does not know the password and cannot 're-set' the password.



12. On the Certificate Store dialog, confirm that “Place all certificates in the following store” is selected and that the selected store is “Personal”. Click the **Next >** button.

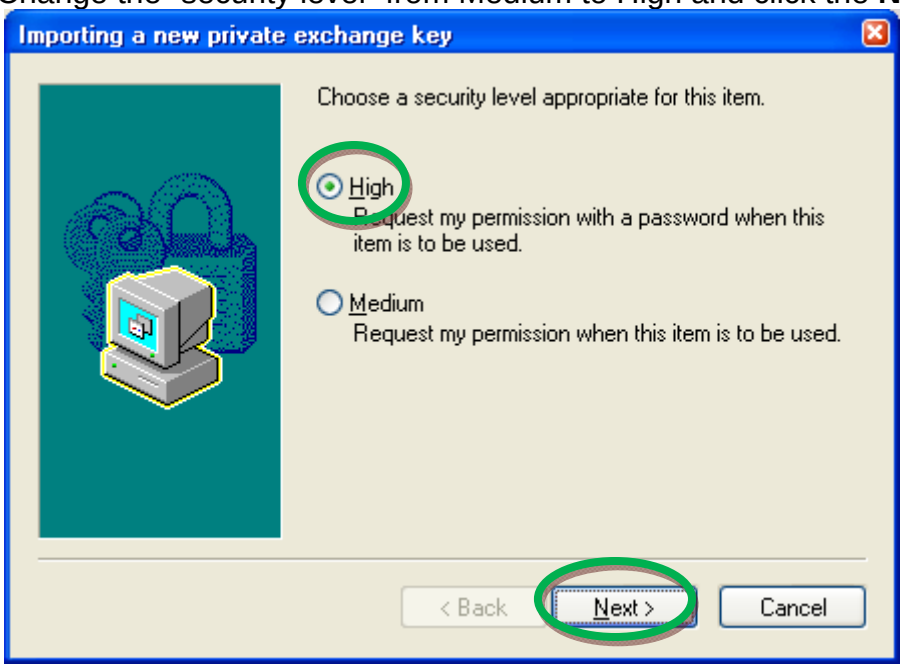


13. On the Completing the Certificate Import Wizard, click on the **Finish** button.

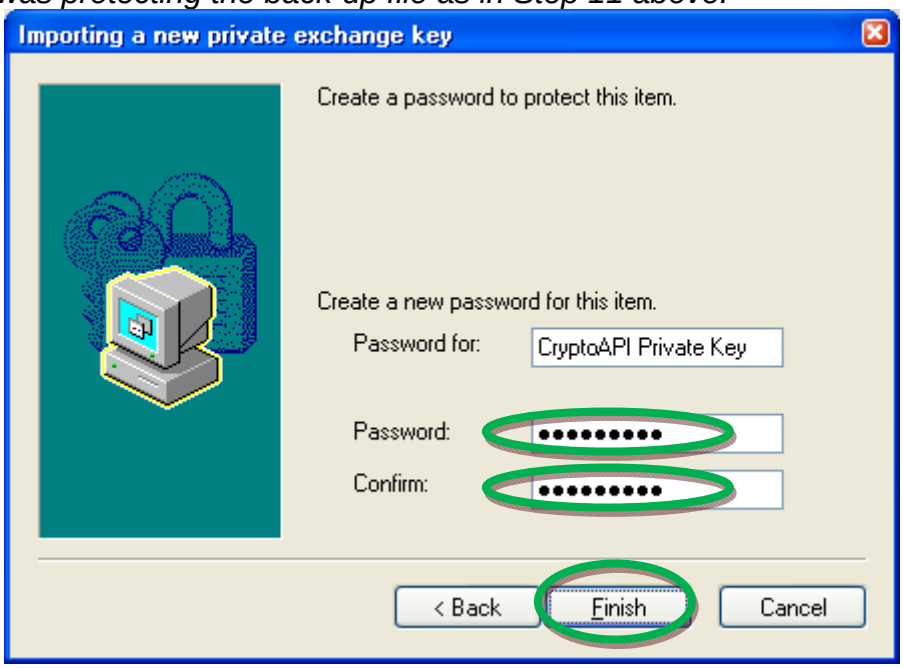


14. On the Importing a new private exchange key dialog box, click on the **Set Security Level…**

15. Change the “security level” from Medium to High and click the **Next >** button

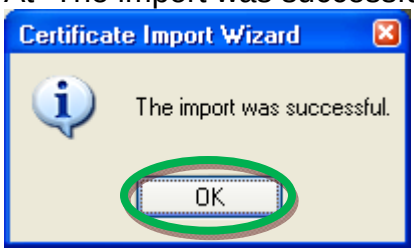


16. Assign and Confirm a password to protect this new installation of your certificate, then click the **Finish** button. *We recommend you use the same password that was protecting the back-up file as in Step 11 above.*

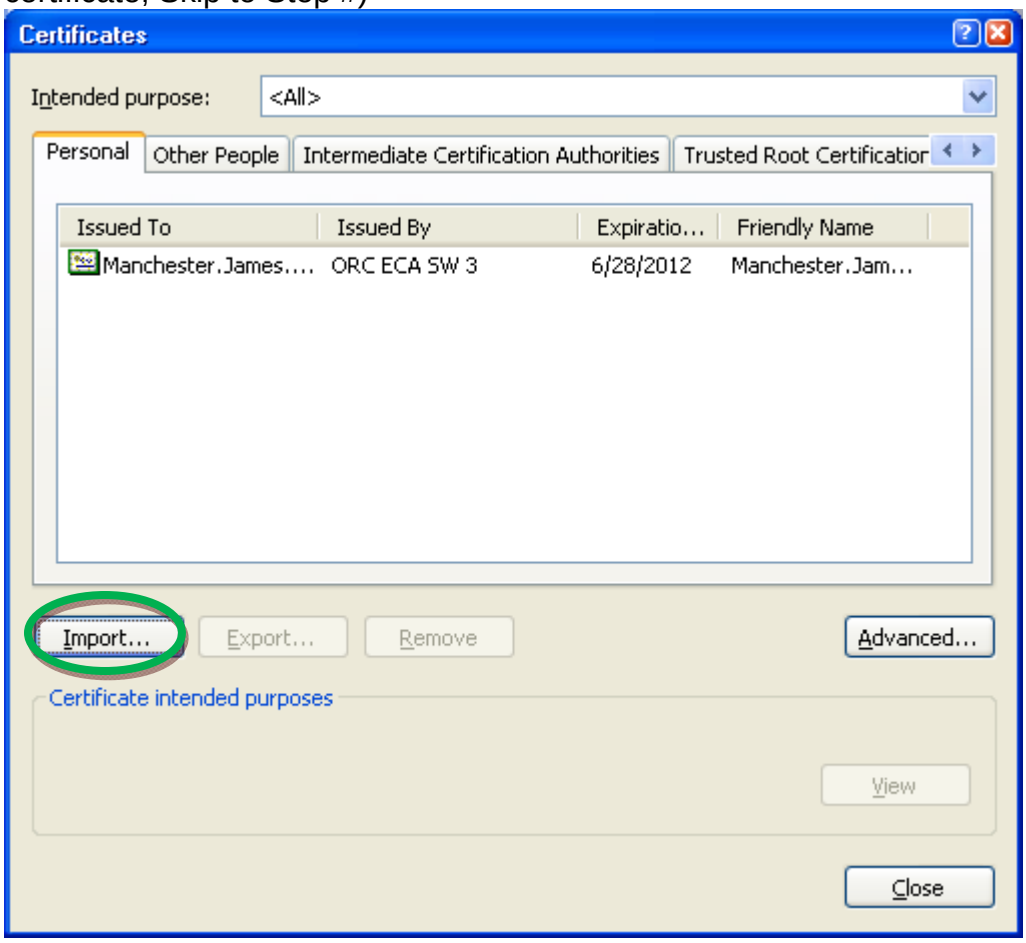


17. Back on the Importing a new private exchange key dialog box, ensure that the Security level is set to High. Click on the click the **OK** button.

18. At “The import was successful, click the **OK** button.

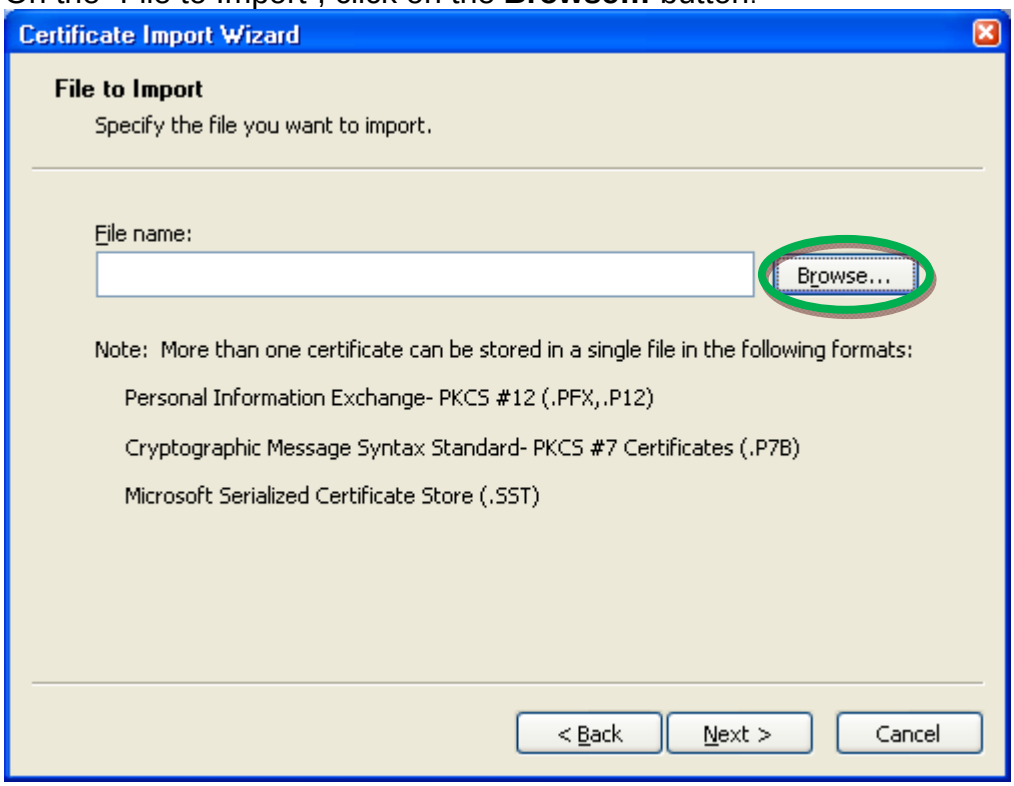


19. Back on the Certificates dialog box; if you need to import another certificate, like your Encryption certificate, click on the **Import** button. (If you only have one certificate, Skip to Step #)

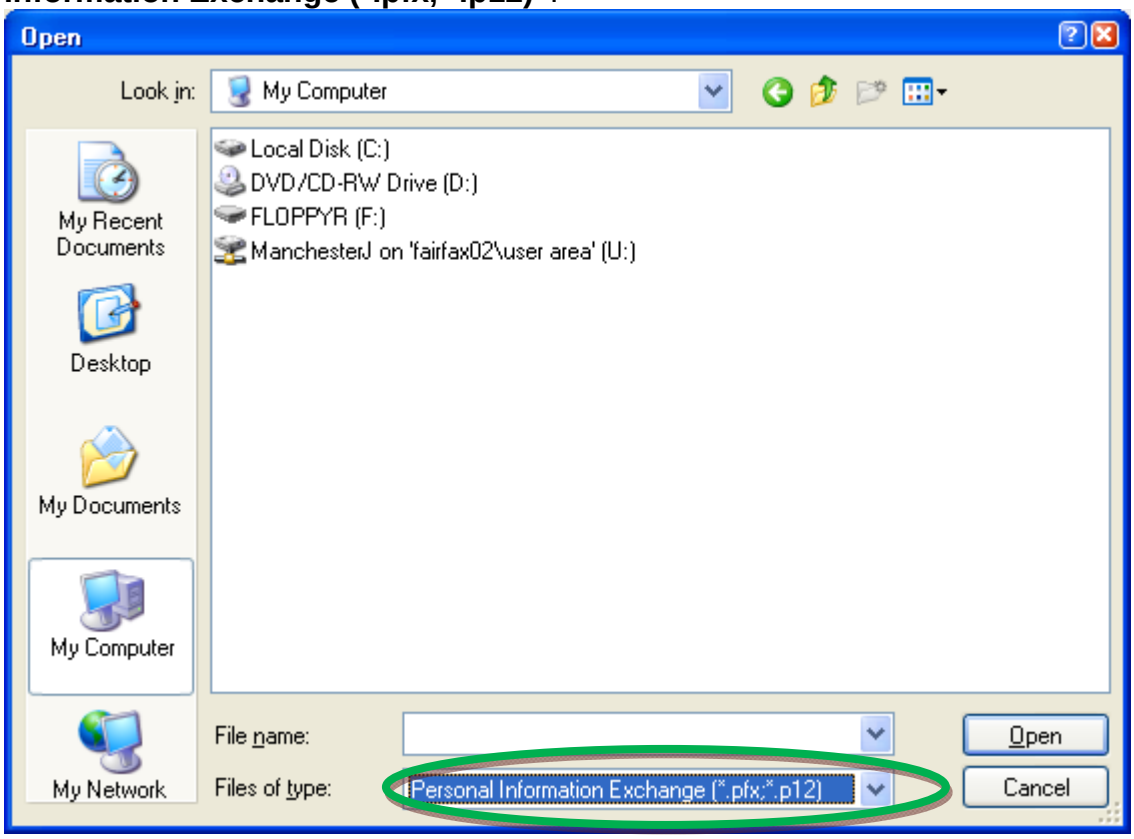


20. When the Certificate Import Wizard pops up, click on the **Next >** button.

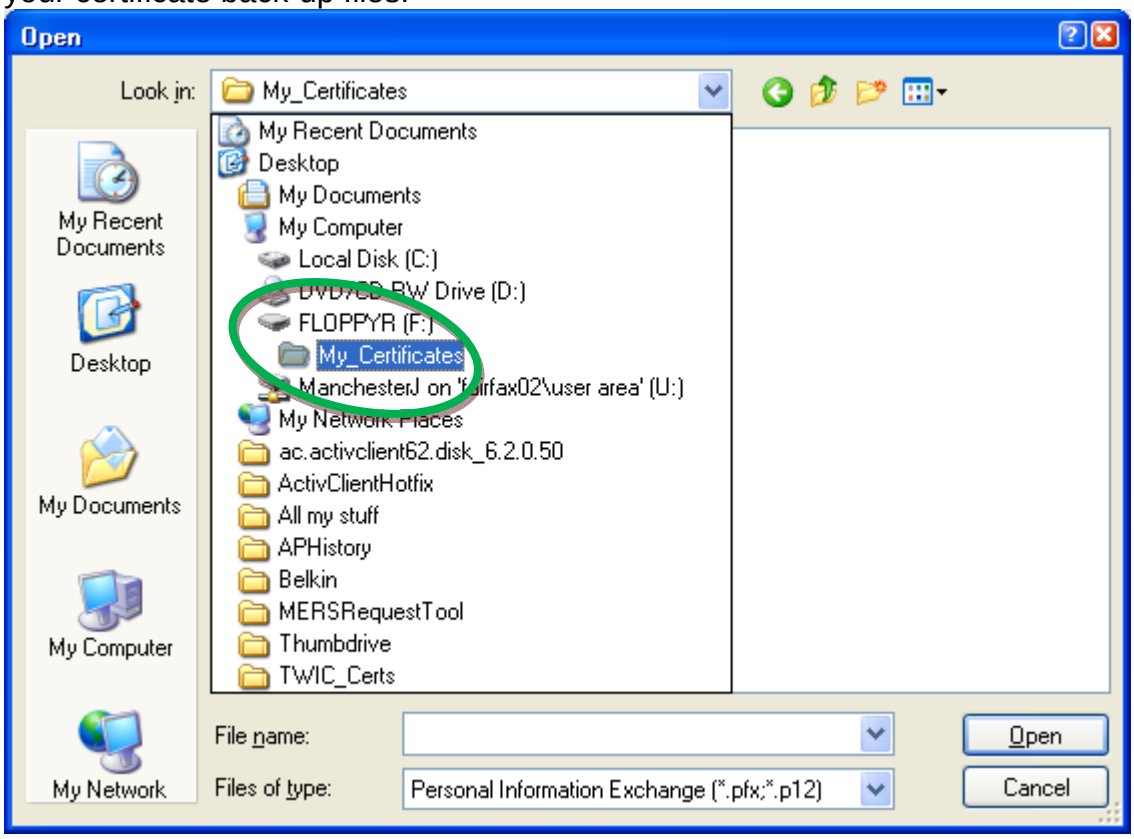
21. On the “File to Import”, click on the **Browse…** button.



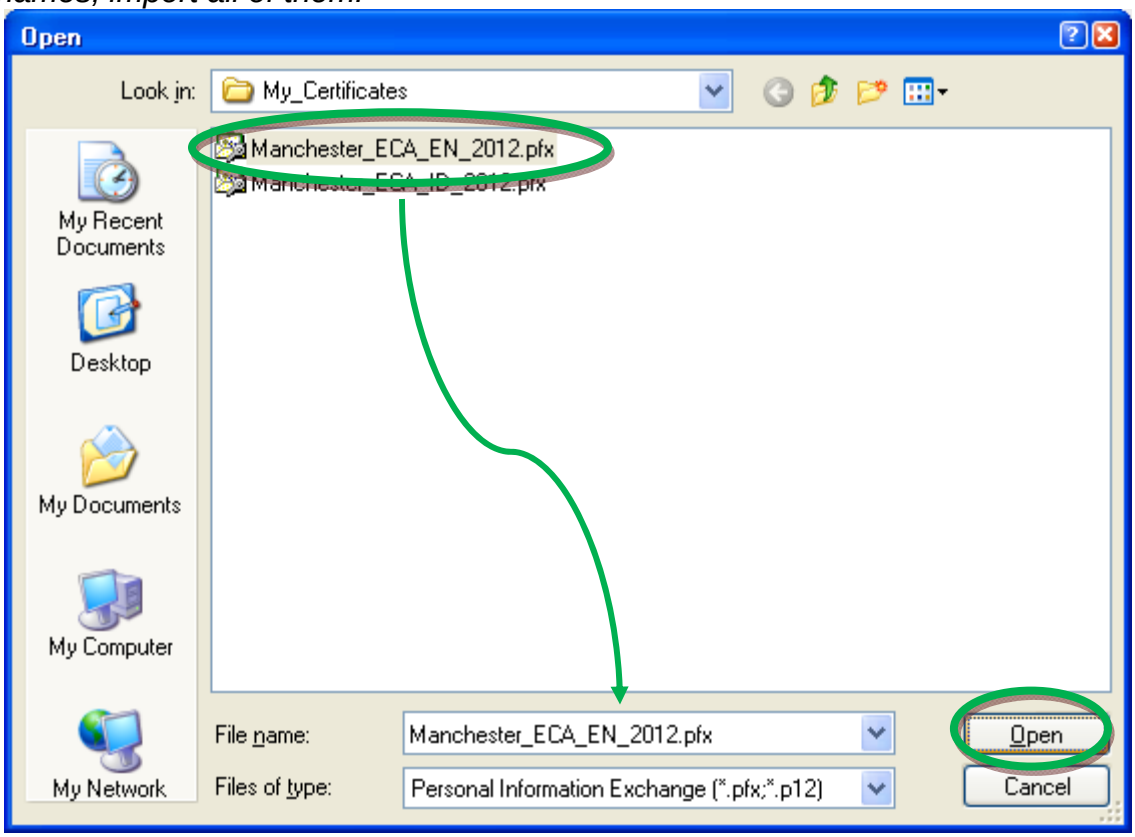
22. On the Open dialog box, change the “Files of type:” pull down to read **“Personal Information Exchange (*.pfx, *.p12)”**.



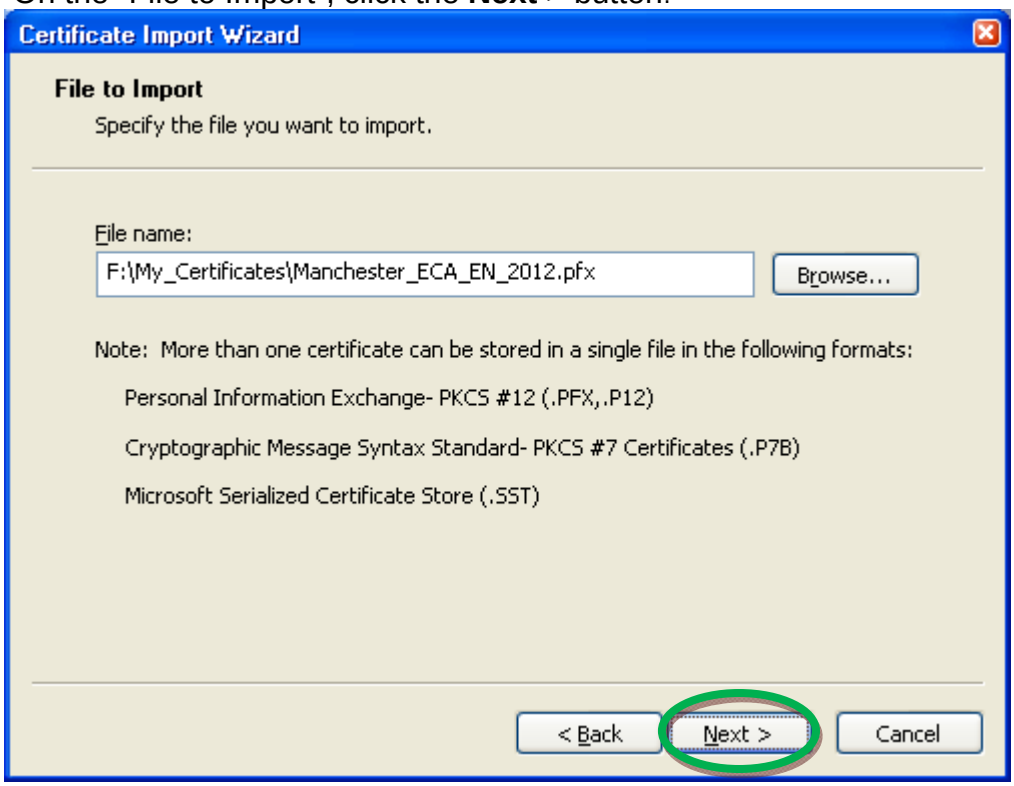
23. On the Open dialog box, use the navigation tools to navigate to the location of your certificate back-up files.



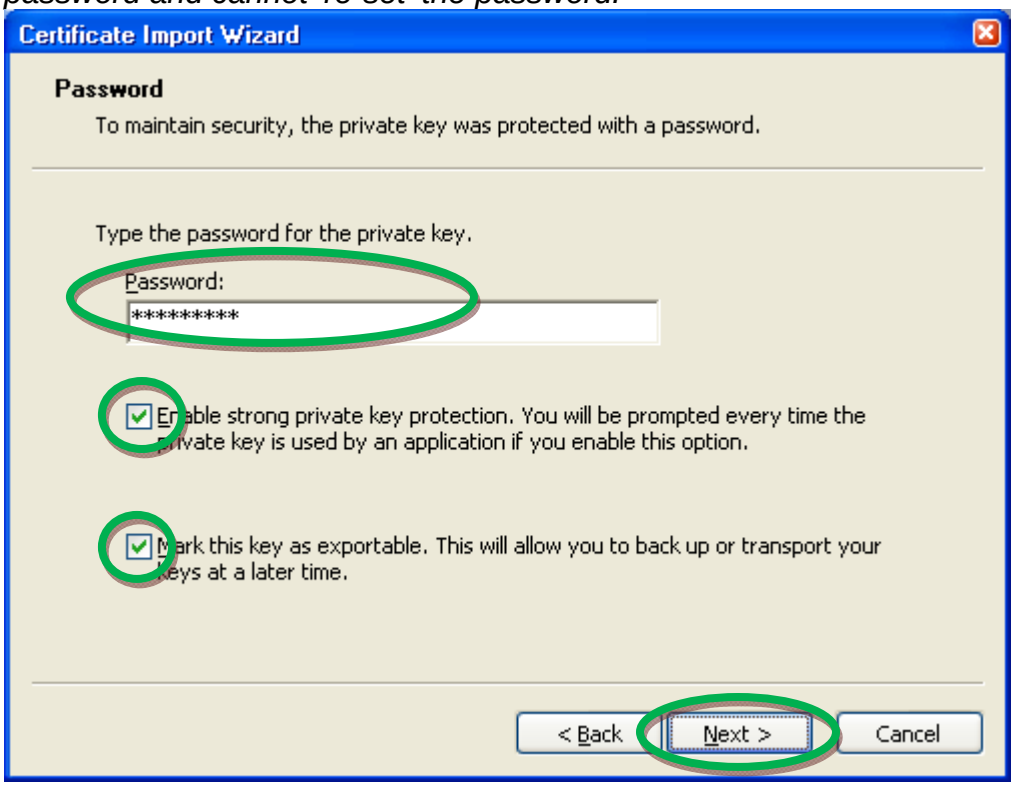
24. On the Open dialog box, select the certificate that you wish to import. (This should be your Encryption certificate.) Then click the **Open** button.
NOTE: The certificate back-up file names were assigned by you when you created the certificate back-up files. If you cannot tell which is which by the file names, import all of them.



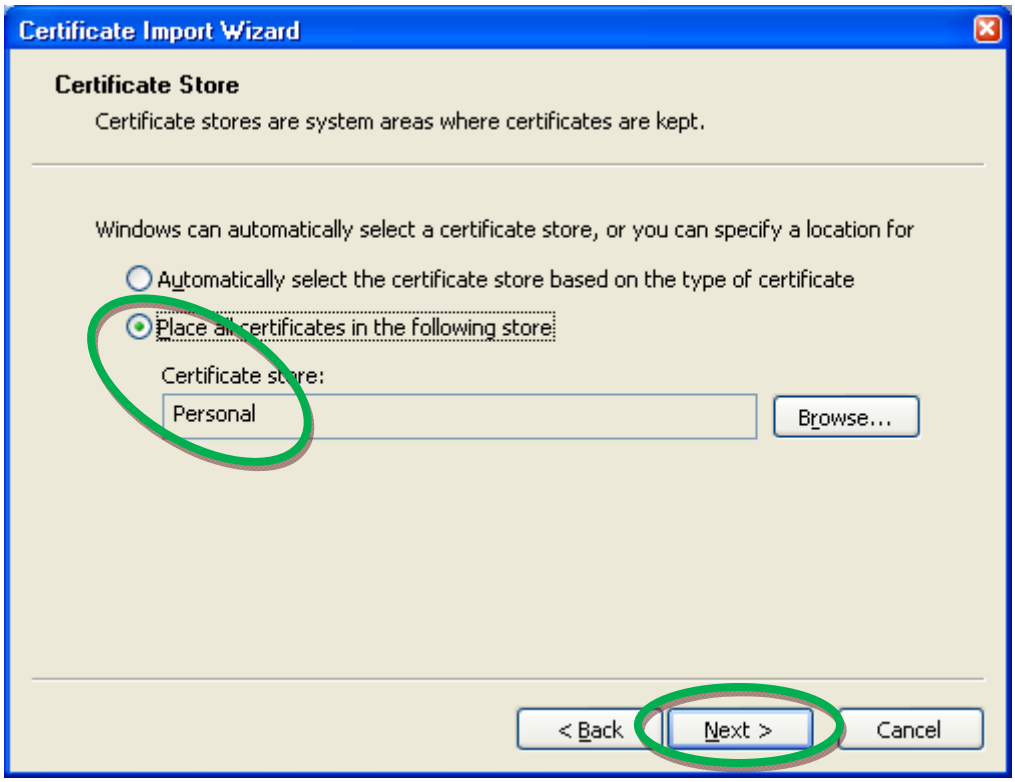
25. On the “File to Import”, click the **Next >** button.



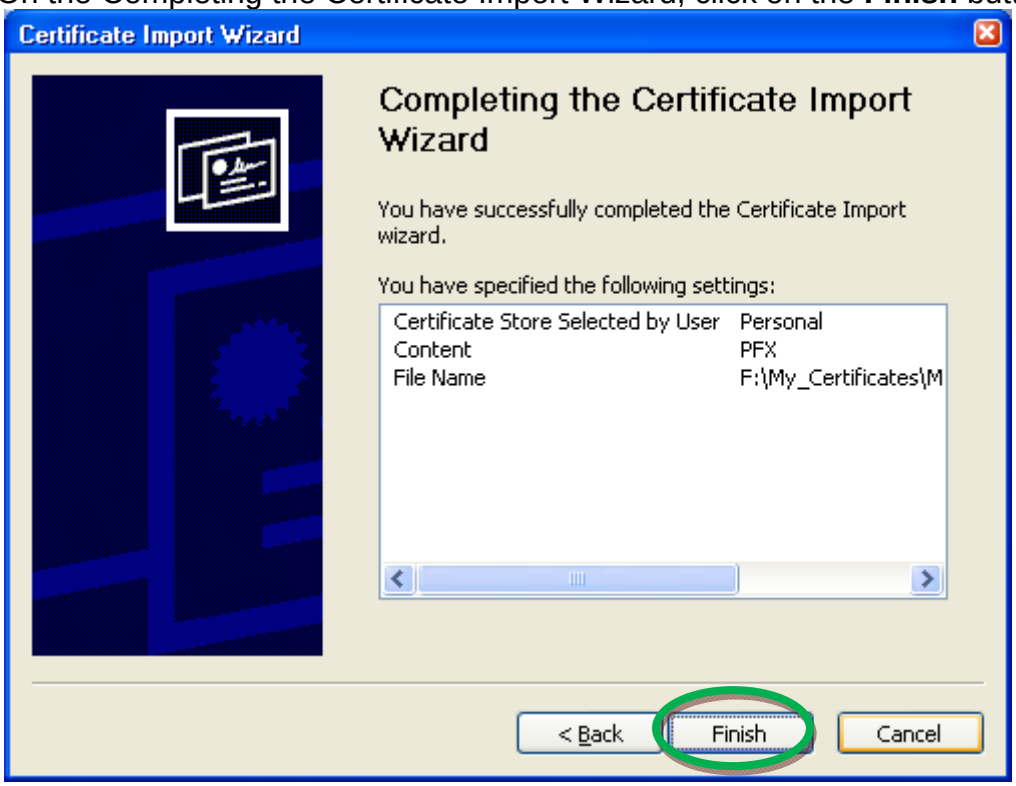
26. In the Password dialog box, enter the password that protects the certificate back-up file. Check all of the check boxes and click the **Next >** button.
NOTE: The certificate back-up file password was assigned by you when you created the certificate back-up files. If you cannot enter the correct password, then you will not be able to import the certificate. ORC does not know the password and cannot 're-set' the password.



27. On the Certificate Store dialog, confirm that “Place all certificates in the following store” is selected and that the selected store is “Personal”. Click the **Next >** button.

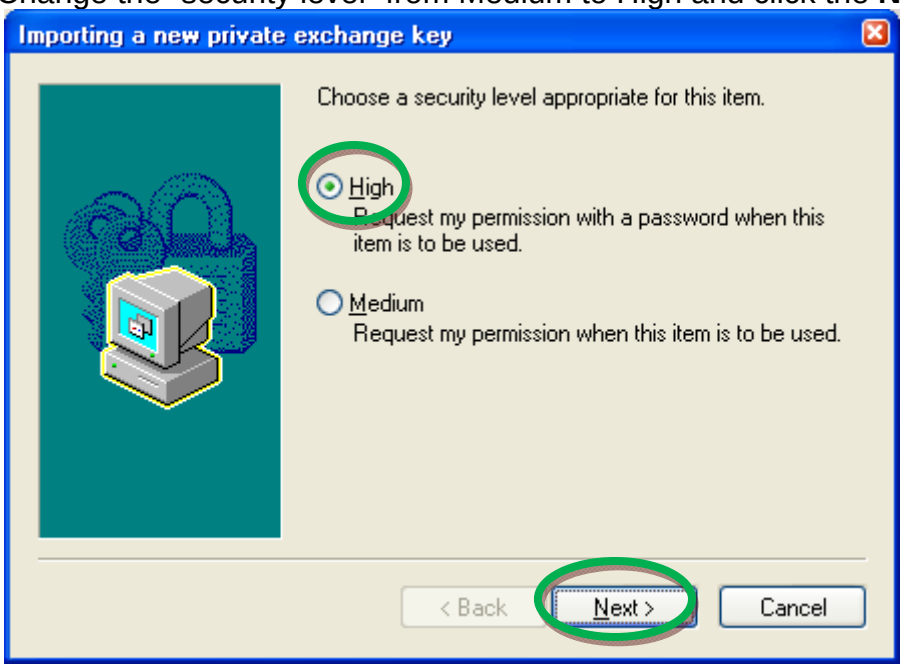


28. On the Completing the Certificate Import Wizard, click on the **Finish** button.

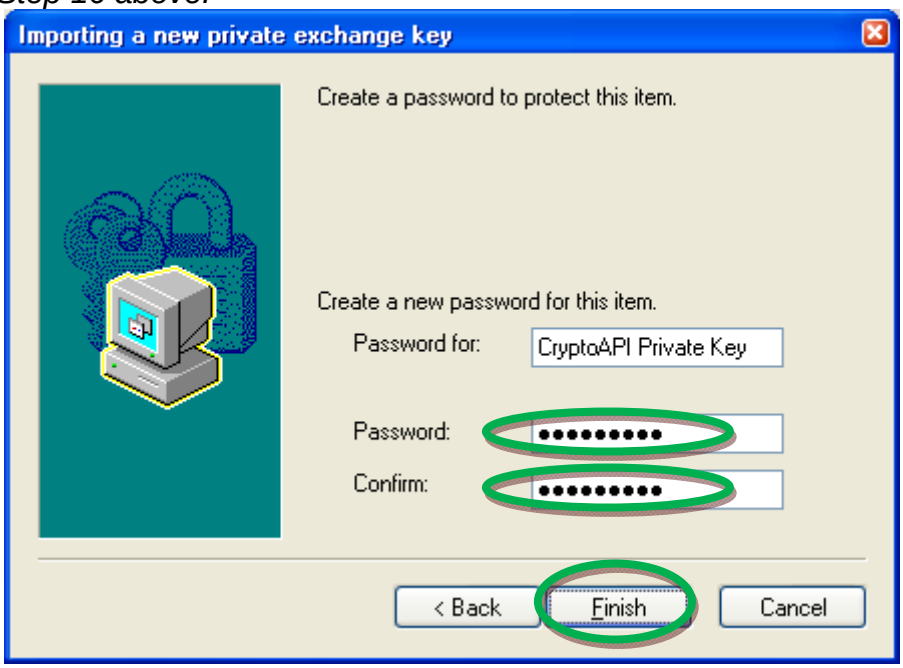


29. On the Importing a new private exchange key dialog box, click on the **Set Security Level…**

30. Change the “security level” from Medium to High and click the **Next >** button

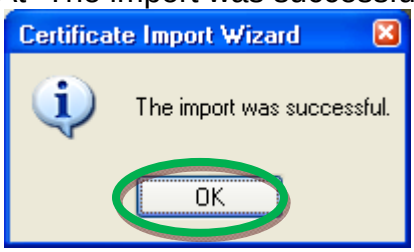


31. Assign and Confirm a password to protect this new installation of your certificate, then click the **Finish** button. *We recommend you use the same password as in Step 16 above.*

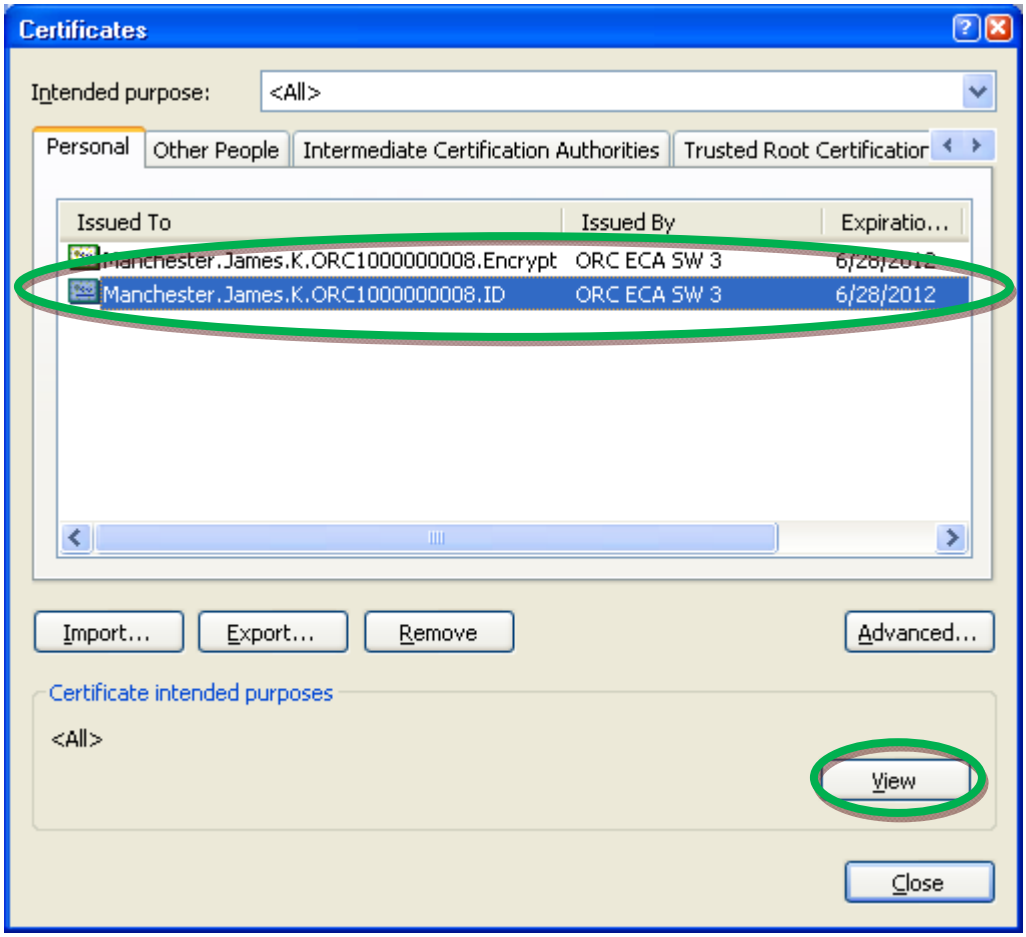


32. Back on the Importing a new private exchange key dialog box, ensure that the Security level is set to High. Click on the click the **OK** button.

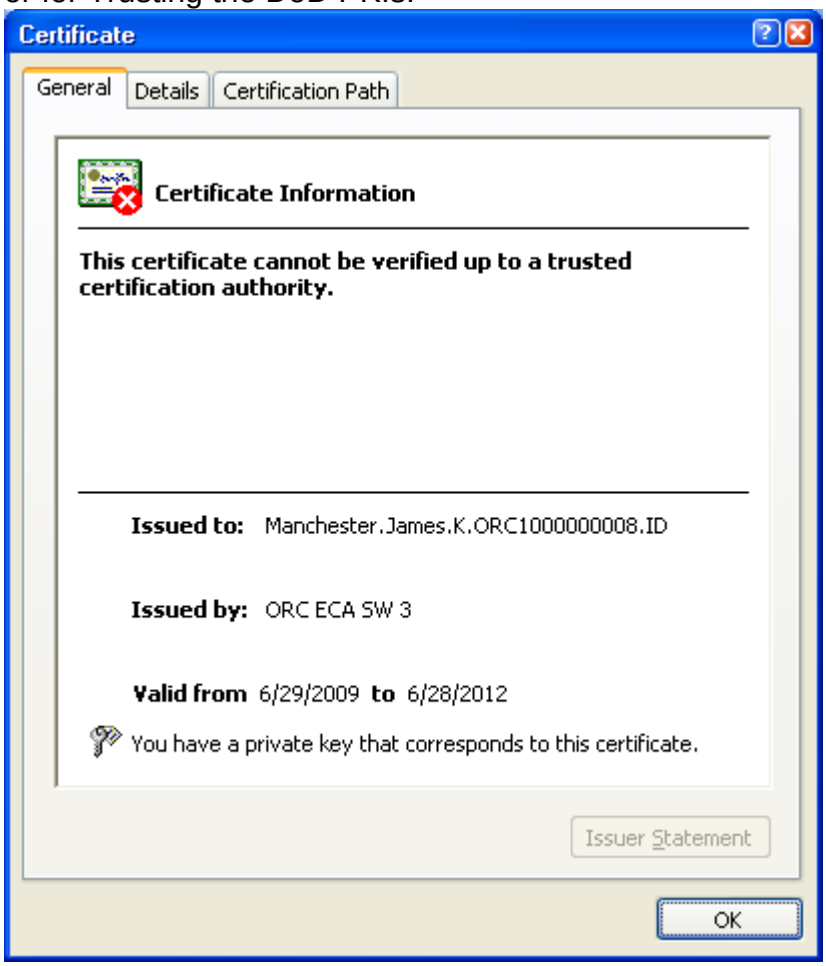
33. At “The import was successful, click the **OK** button.



34. Back on the Certificates dialog box, select one of your certificates and click the **View** button.



35. If your certificate states “This certificate cannot be verified up to a trusted certificate authority, then execute the instructions for Trusting the ORC ECA PKI or for Trusting the DoD PKIs.



36. If your certificate looks like the one shown below, you're your certificates are ready to use.