

Importing your personal certificate(s) to Microsoft 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.) *Please note that Chrome, Edge, Internet Explorer, and Outlook all use the Windows cert store. Once you have installed your certificates into the Windows cert store, they will be available to all of those applications.*

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(s) looks like this:



LastName_ECA7_
EN_BackUpCopy_
_02.05.2019.p12



LastName_ECA7_
ID_BackUpCopy_
_02.05.2019.p12

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.”

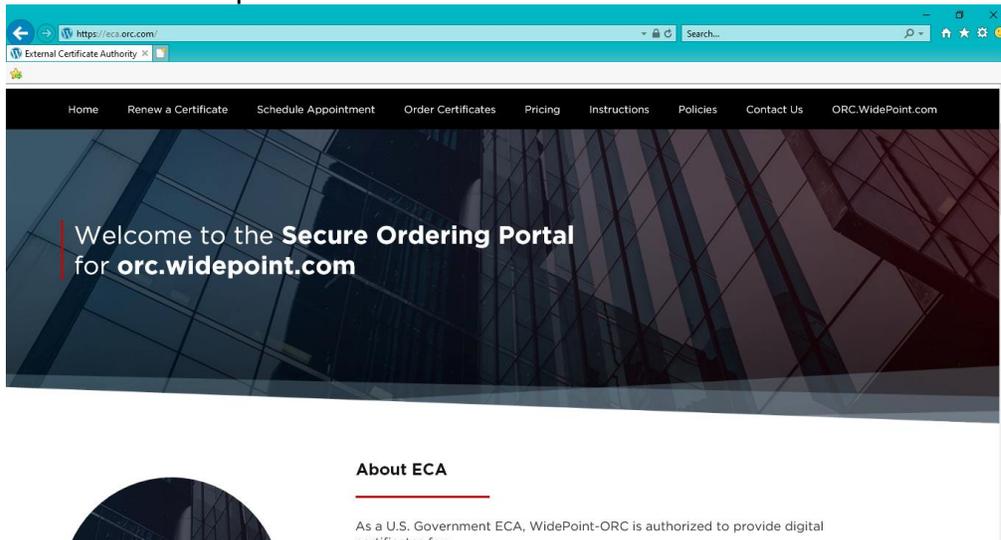
These instructions are not meant for “hardware-based certificates.” Hardware based certificates are created on a smart card, or cryptographic token, or other cryptographic device. You cannot import “hardware-based certificates” from an import file, because you cannot create a back-up file of a “hardware-based certificates.” (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.”

Since you have obtained both an Identity and an Encryption certificate, you will need to import both of these certificates. (2 certificates means 2 back-up files)

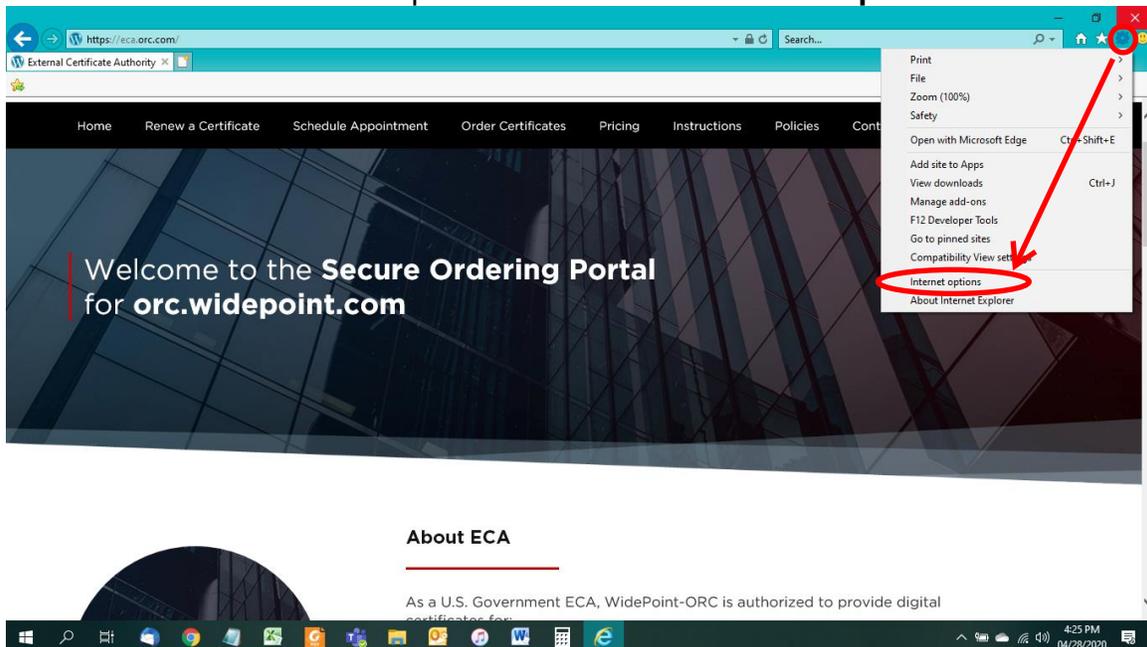
The only way to tell the back-up files apart is by the name that you assign to the file.

These instructions and associated screen captures were created with Internet Explorer 11 running on a Windows 10 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 7 computer; just click the buttons that seem to move the process forward.)

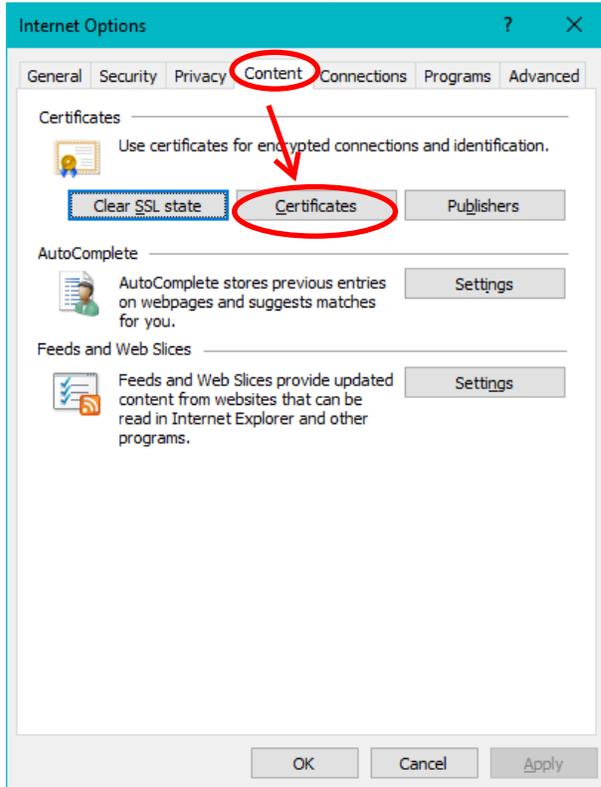
1. Start Internet Explorer



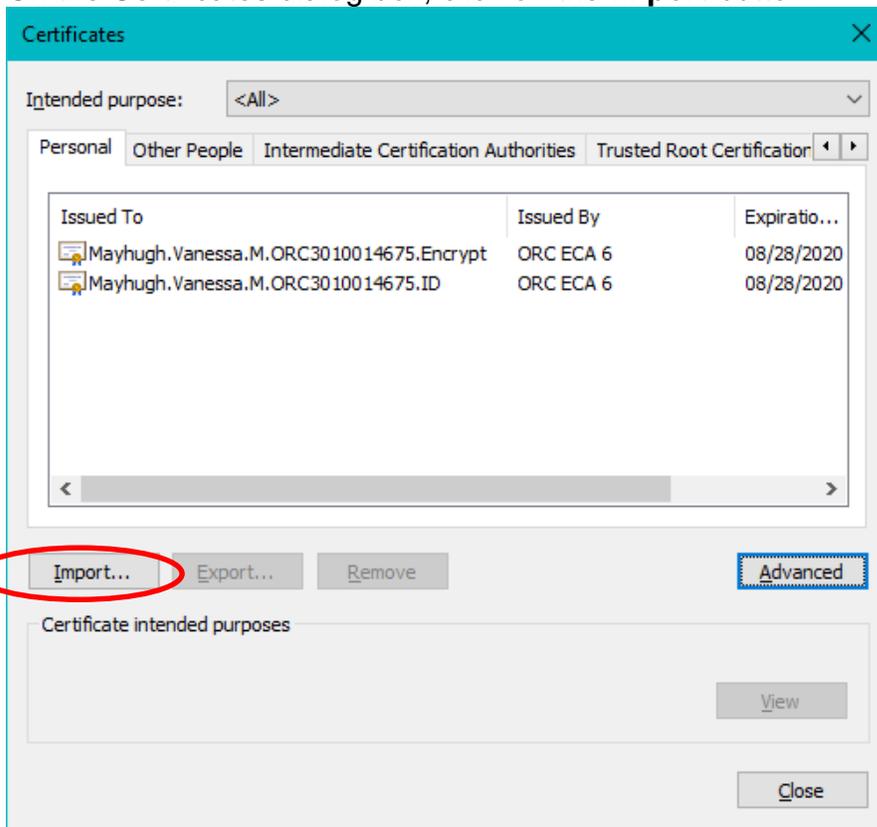
2. Click on the "Tools" menu option and then click "Internet Options...".



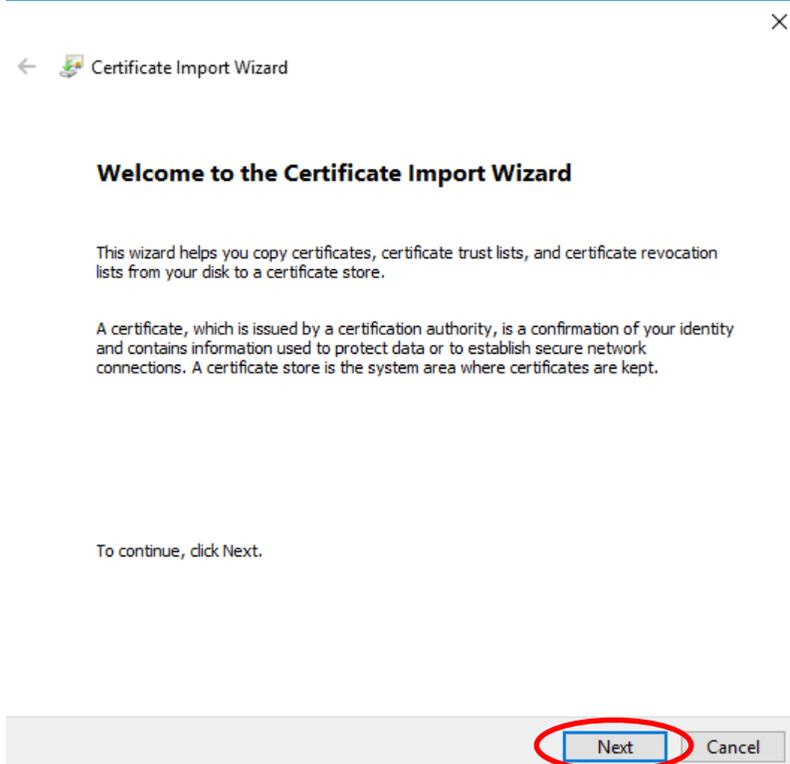
3. Select the **Content** tab, then click the **Certificates...** button.



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.



←  Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

Browse...

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

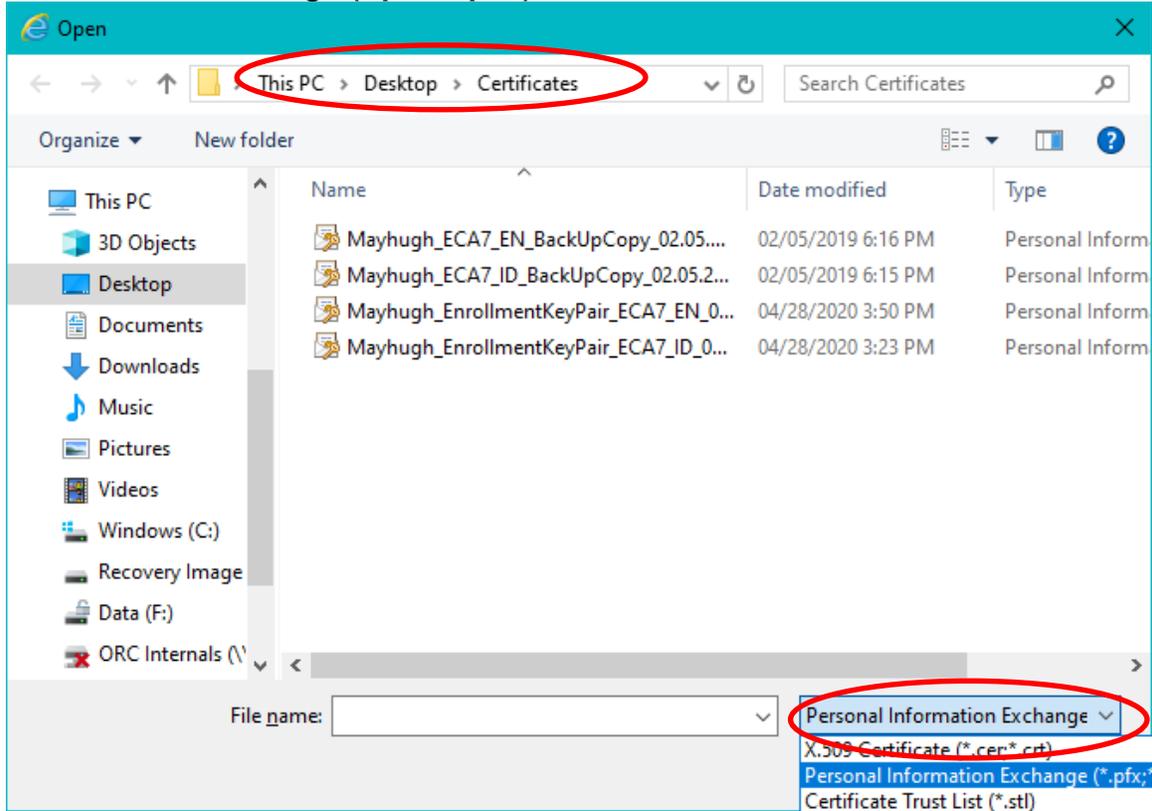
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

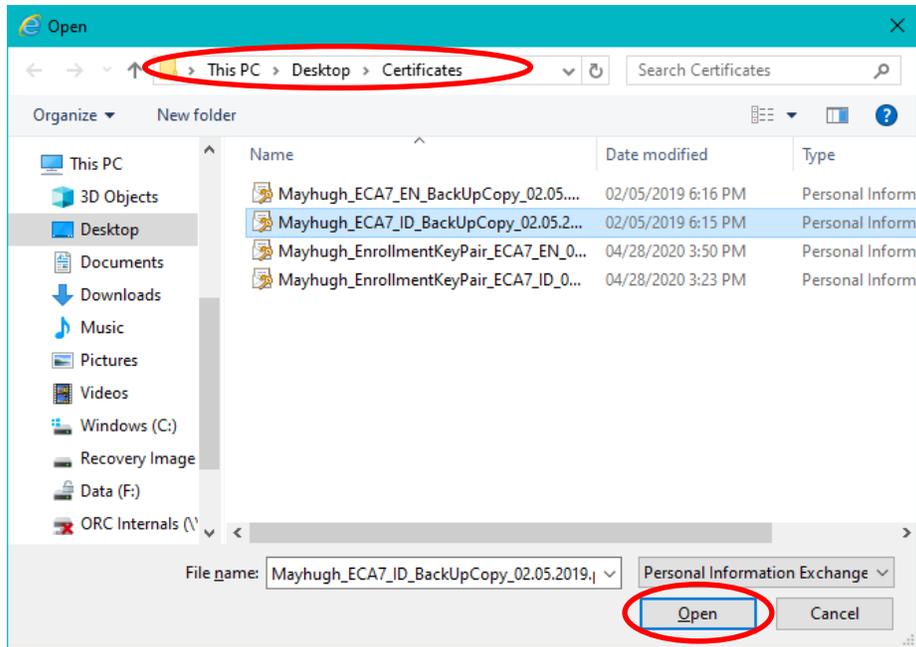
Next

Cancel

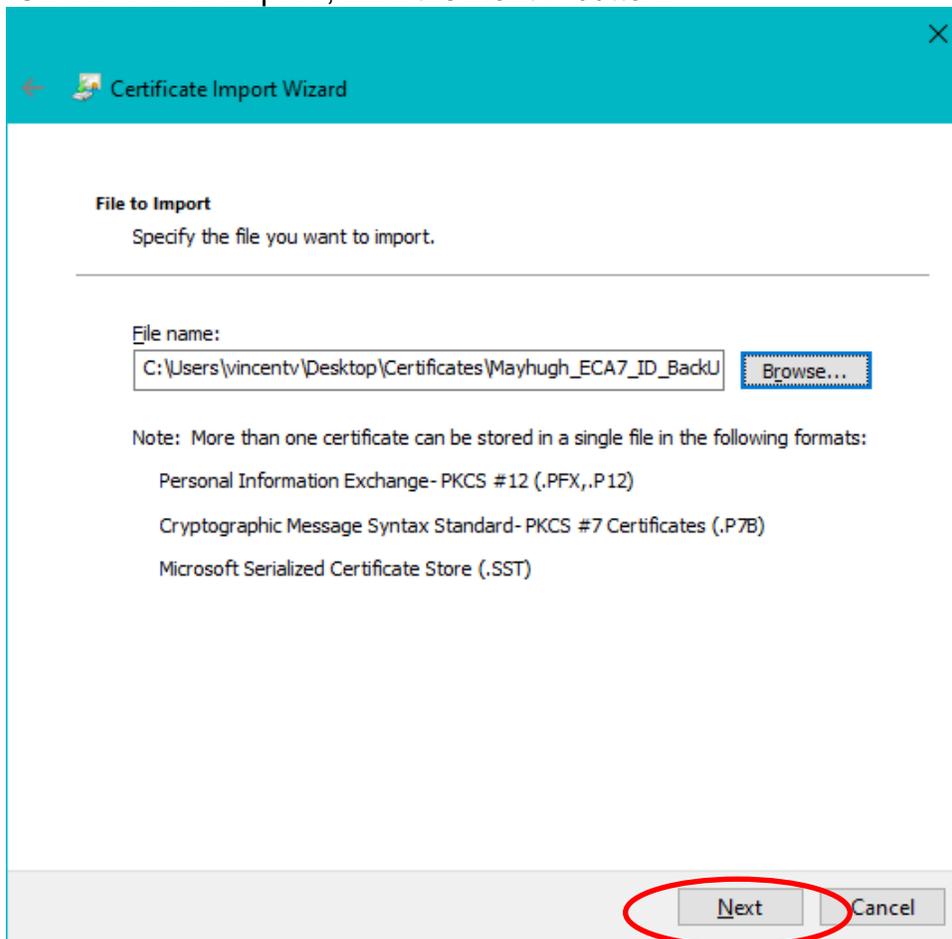
7. On the Open dialog box, change the “Files of type:” pull down to read “**Personal Information Exchange (*.pfx, *.p12)**”.



8. 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.*



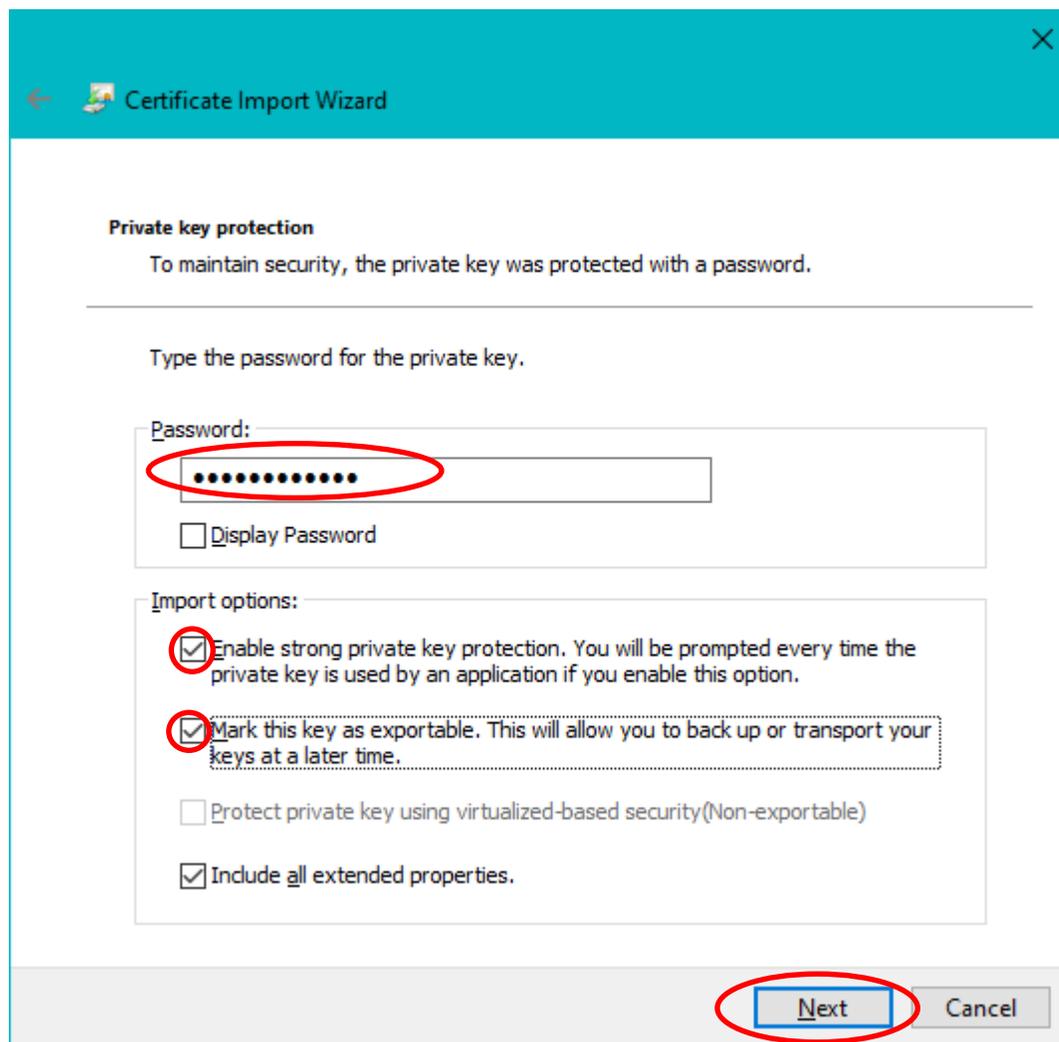
10. On the "File to Import", click the **Next >** button.



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.

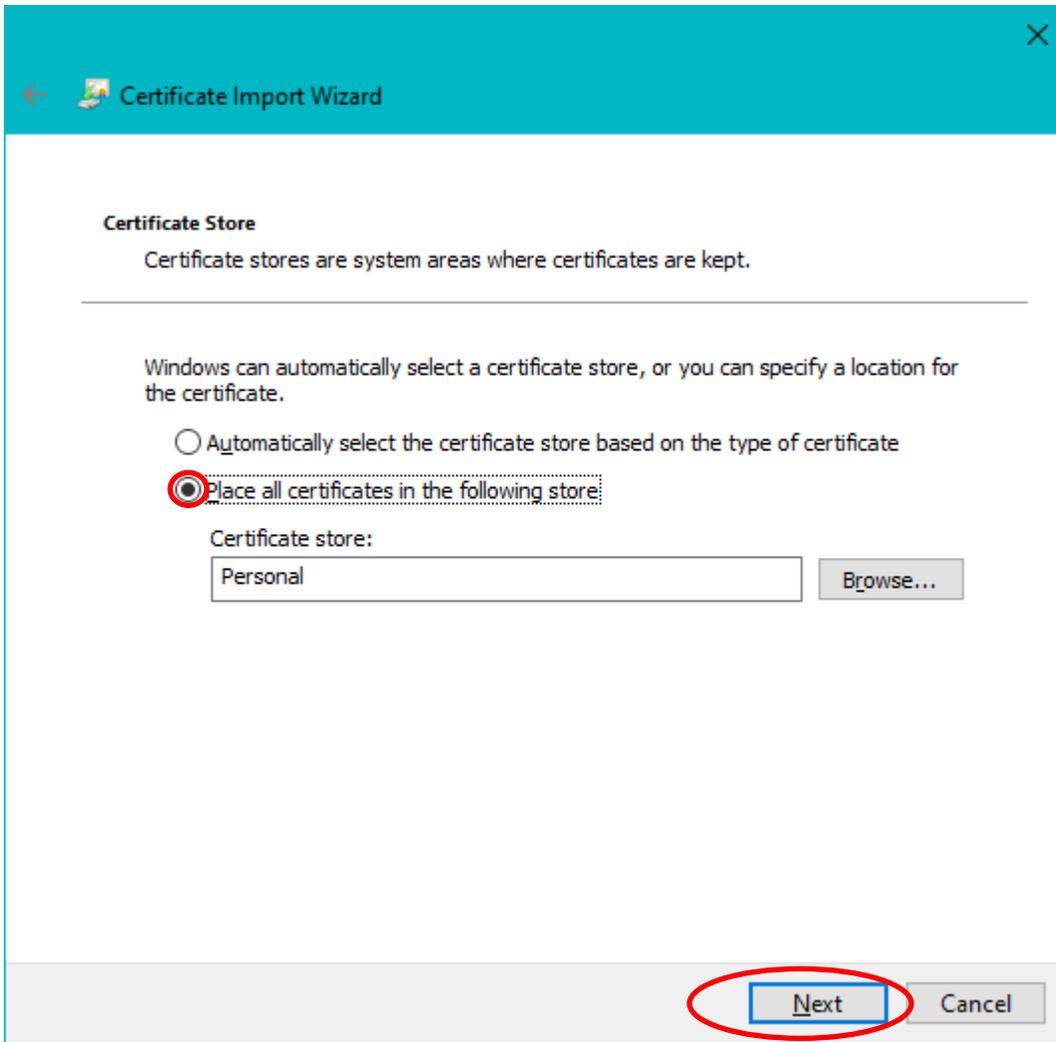
NOTE: The certificate back-up file password was assigned by you when you created the certificate back-up files. If you cannot enter the correct password, then you will not be able to import the certificate.

WidePoint does not know the password and WidePoint cannot re-set the password.

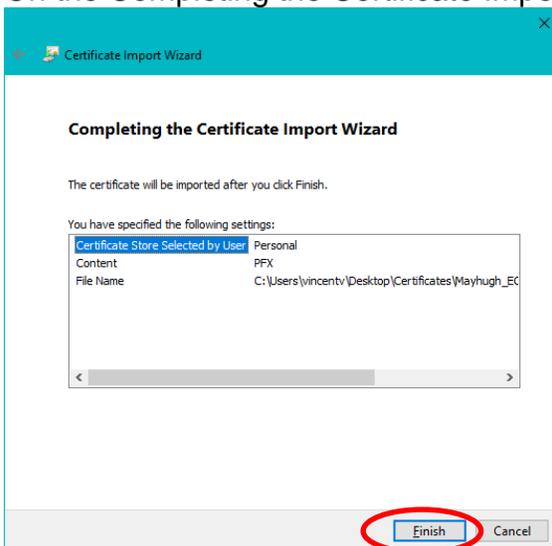


The screenshot shows the 'Certificate Import Wizard' dialog box. The title bar is teal with a back arrow, a certificate icon, and the text 'Certificate Import Wizard'. The main content area is white. Under the heading 'Private key protection', there is a sub-heading 'Private key protection' and a paragraph: 'To maintain security, the private key was protected with a password.' Below this is a horizontal line and the instruction 'Type the password for the private key.' There is a text box labeled 'Password:' containing ten black dots, which is circled in red. Below the text box is a checkbox labeled 'Display Password' which is unchecked. Under the heading 'Import options:', there are four checkboxes: 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.' (checked and circled in red), 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.' (checked and circled in red), 'Protect private key using virtualized-based security(Non-exportable)' (unchecked), and 'Include all extended properties.' (checked). At the bottom right, there are two buttons: 'Next' (circled in red) and 'Cancel'.

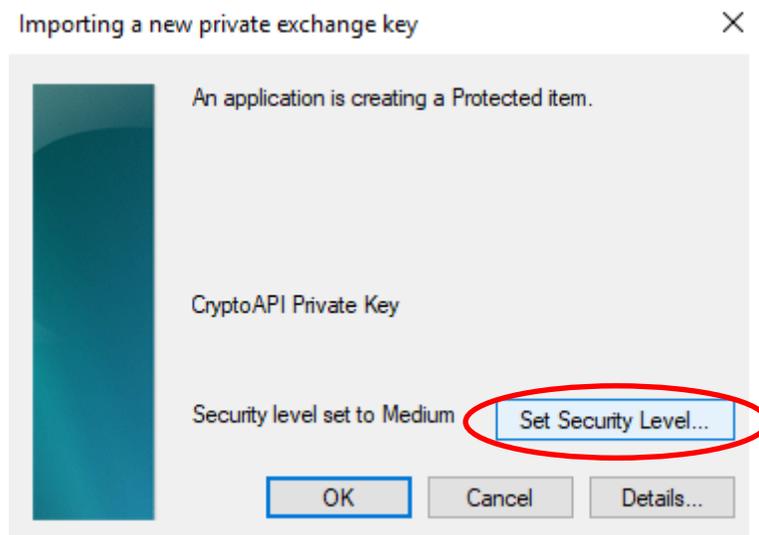
12. On the Certificate Store dialog, confirm that "Place all certificates in the following store" is selected and that the selected store is "Personal". Click the **Next >** button.



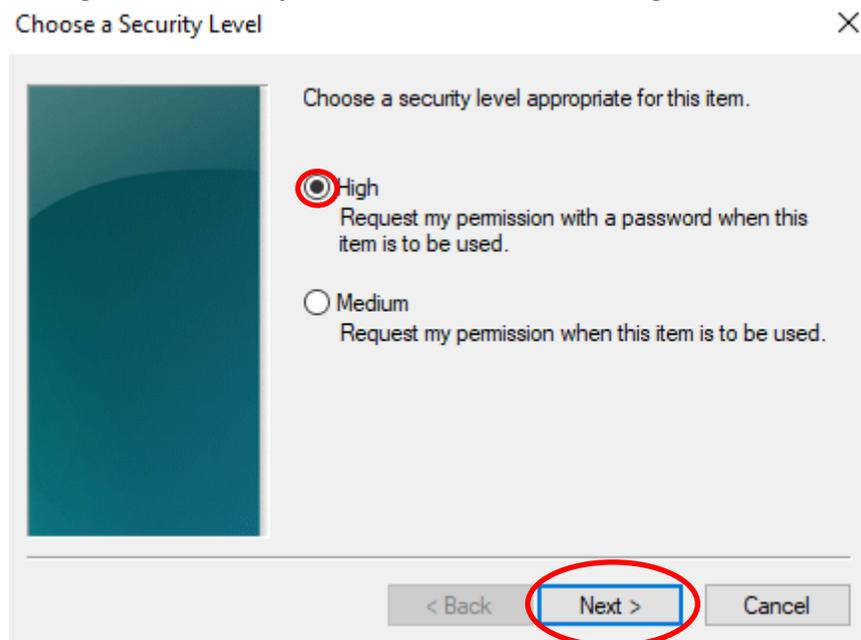
13. On the Completing the Certificate Import Wizard, click on the **Finish** button.



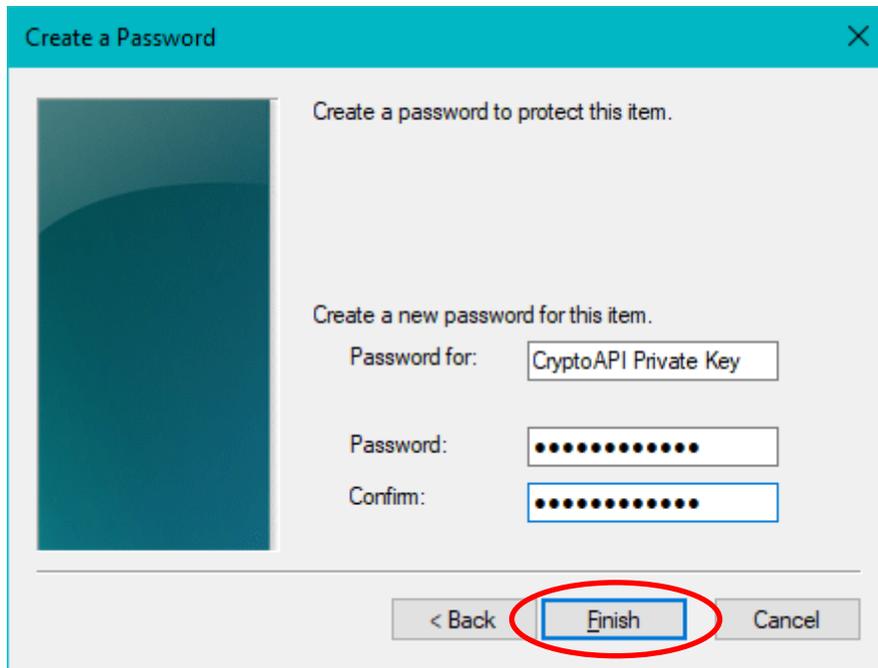
14. On the Importing a new private exchange key dialog box, click on the **Set Security Level...**



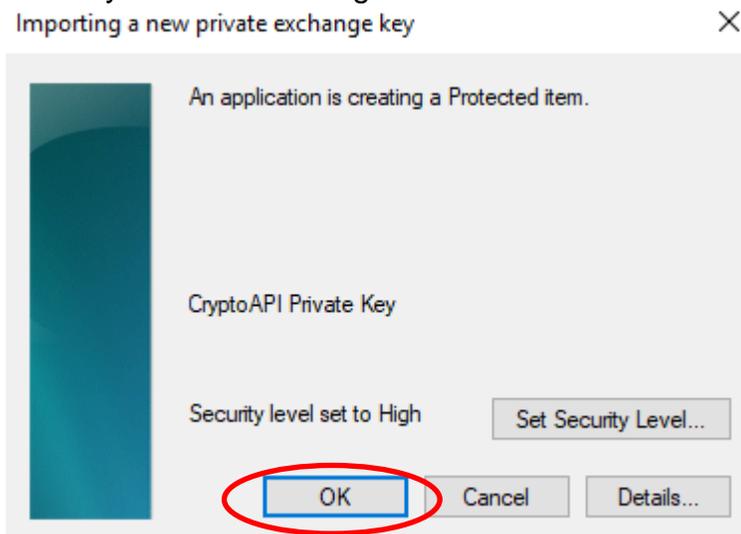
15. Change the “security level” from Medium to High and click the **Next >** button



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.

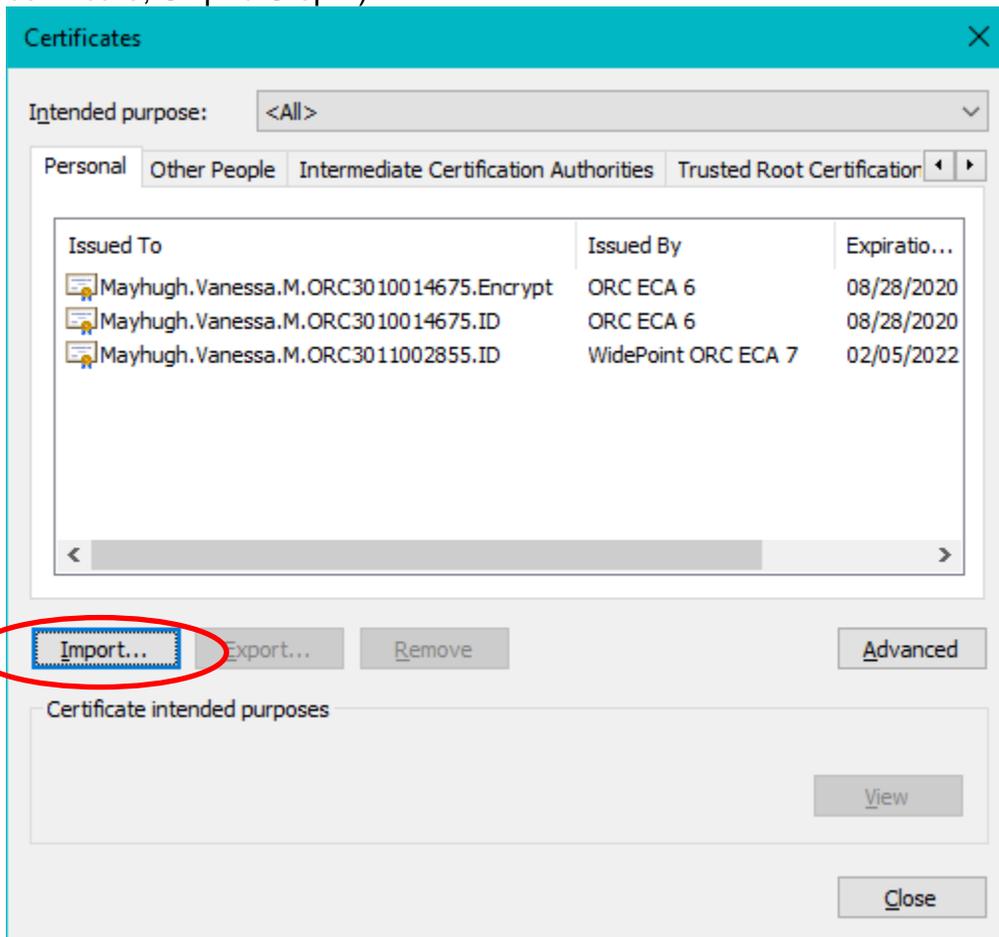
Certificate Import Wizard



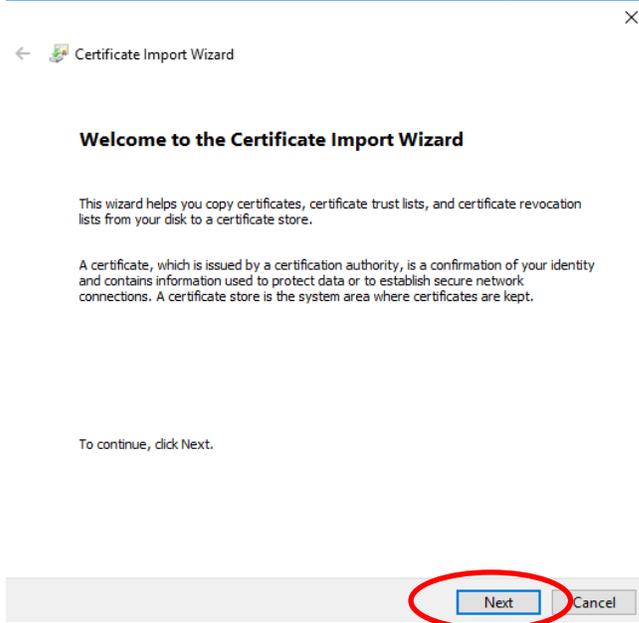
The import was successful.

OK

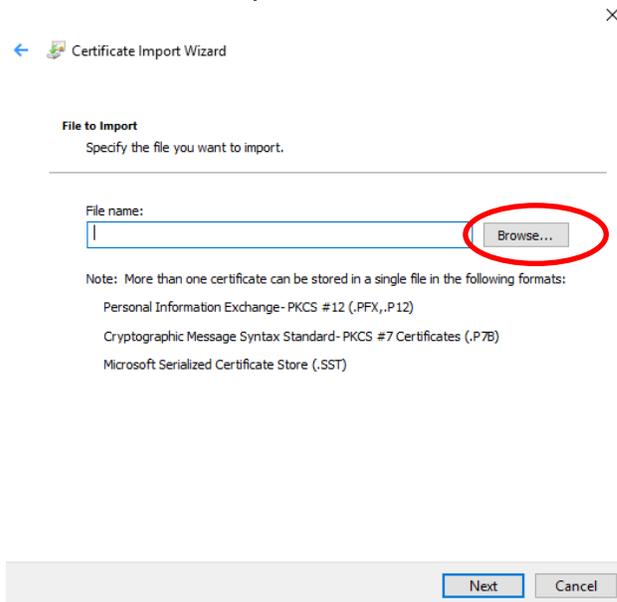
19. Back on the Certificates dialog box; if you need to import another certificate, like your Encryption certificate, click on the **Import** button. (If you only have one certificate, Skip to Step #)



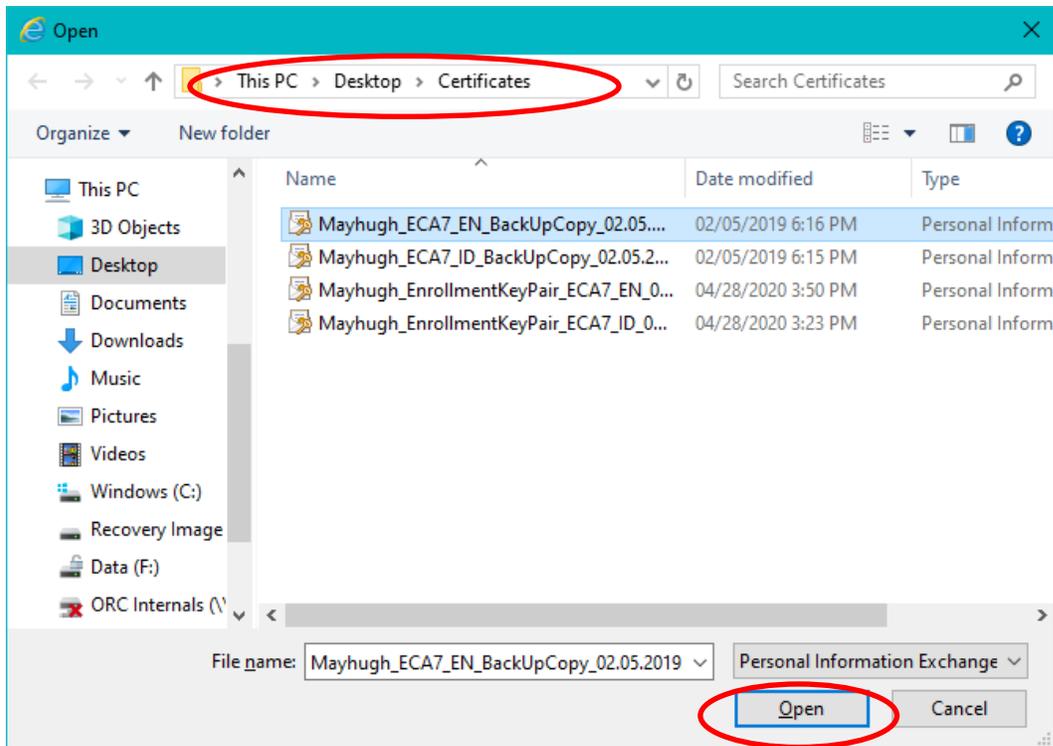
When the Certificate Import Wizard pops up, click on the **Next >** button.



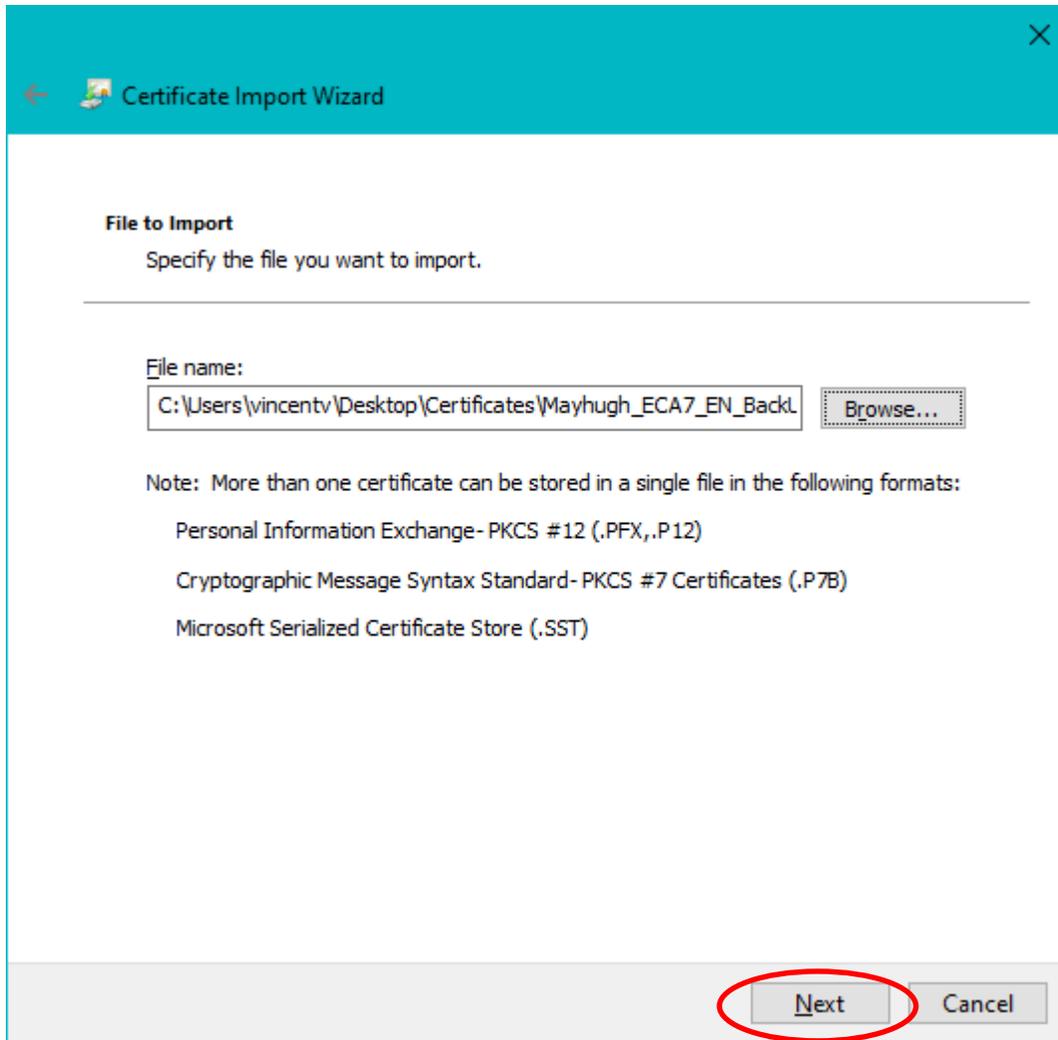
20. On the “File to Import”, click on the **Browse...** button.



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

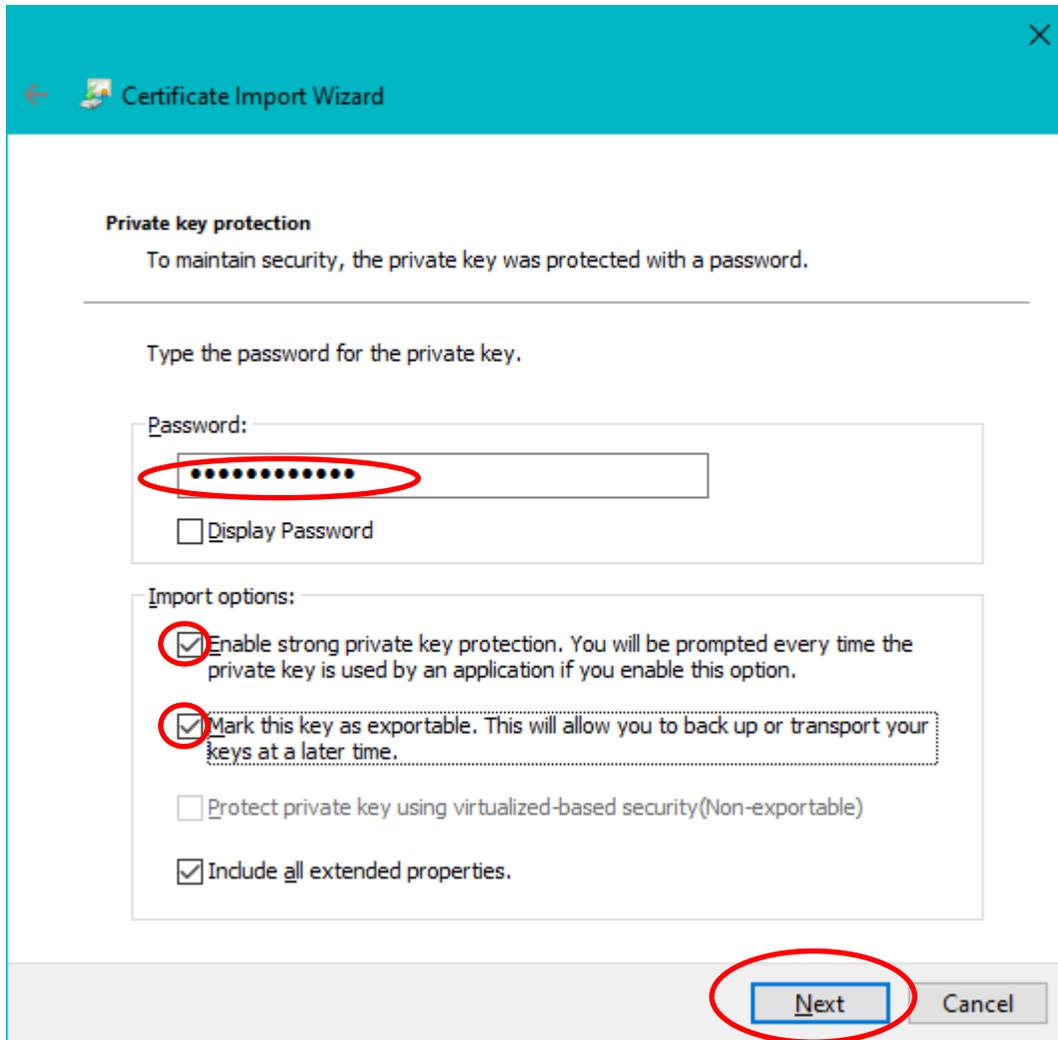


22. On the Open dialog box, use the navigation tools to navigate to the location of your certificate back-up files.
23. On the Open dialog box, select the certificate that you wish to import. (This should be your Encryption certificate.) Then click the **Open** button.
NOTE: The certificate back-up file 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.
24. On the “File to Import”, click the **Next >** button.

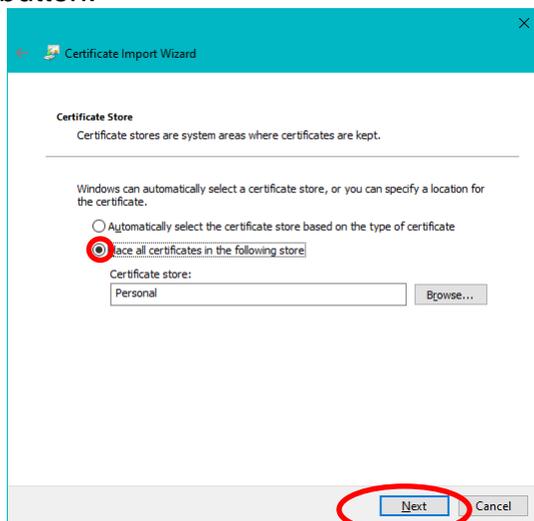


25. In the Password dialog box, enter the password that protects the certificate back-up file. Check all of the check boxes and click the **Next >** button.

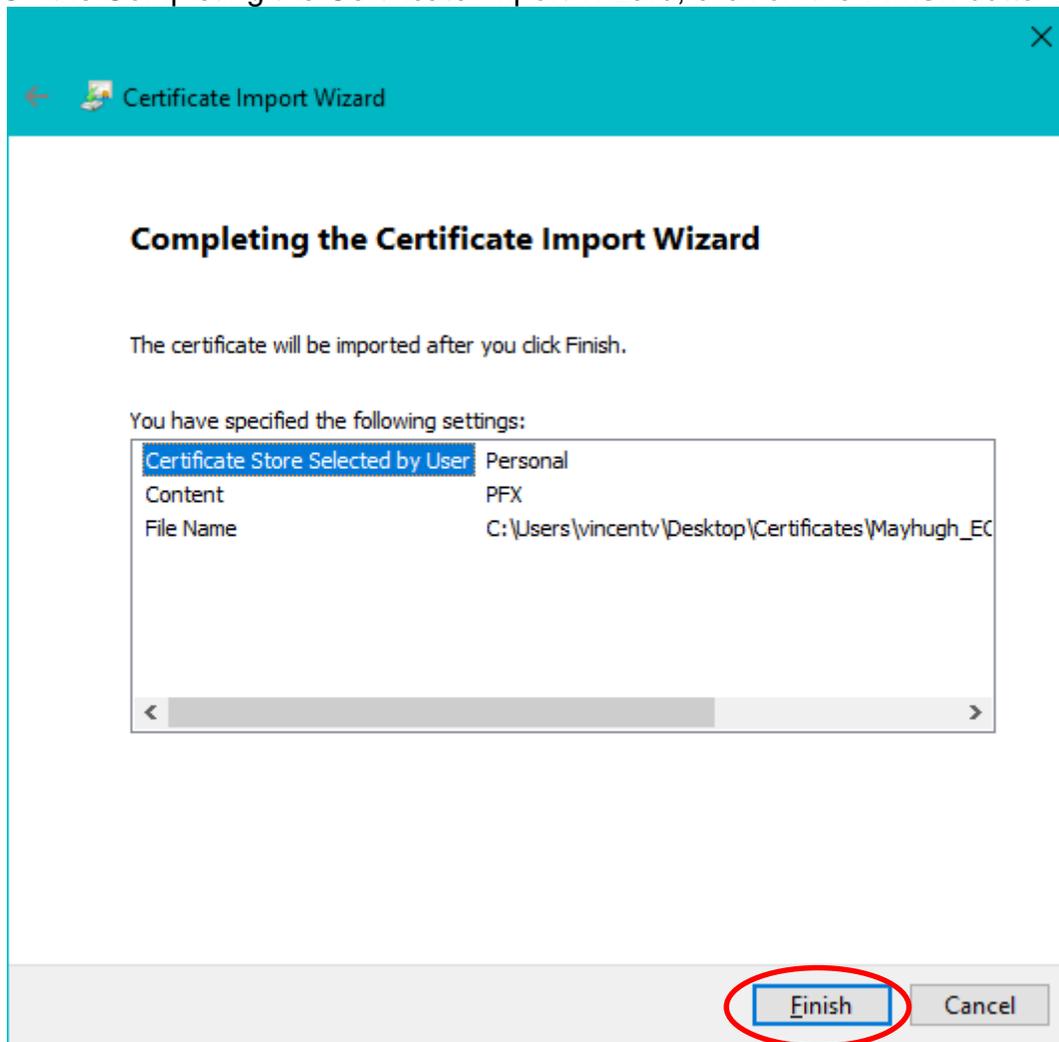
NOTE: The certificate back-up file password was assigned by you when you created the certificate back-up files. If you cannot enter the correct password, then you will not be able to import the certificate. WidePoint does not know the password and WidePoint cannot re-set the password.



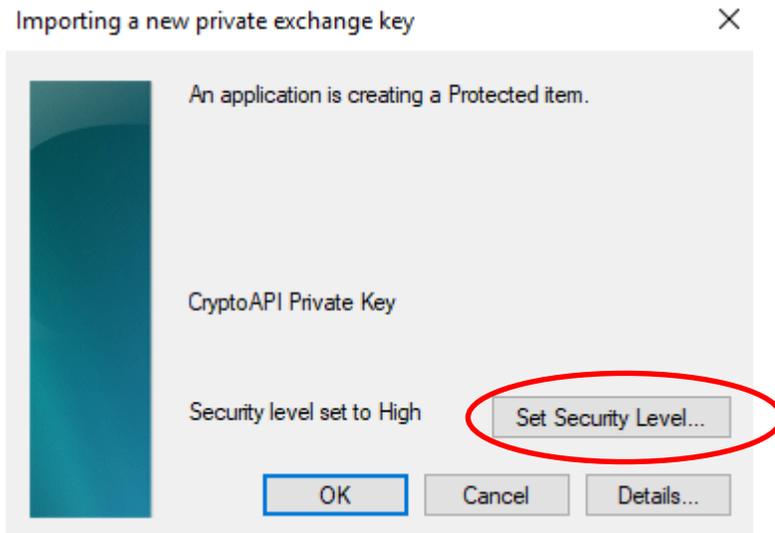
26. On the Certificate Store dialog, confirm that “Place all certificates in the following store” is selected and that the selected store is “Personal”. Click the **Next >** button.



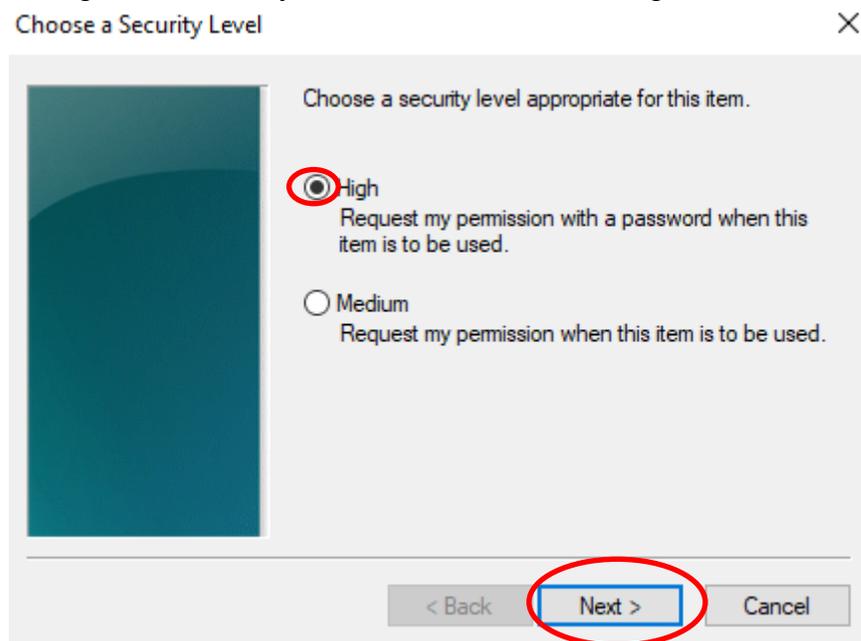
27. On the Completing the Certificate Import Wizard, click on the **Finish** button.



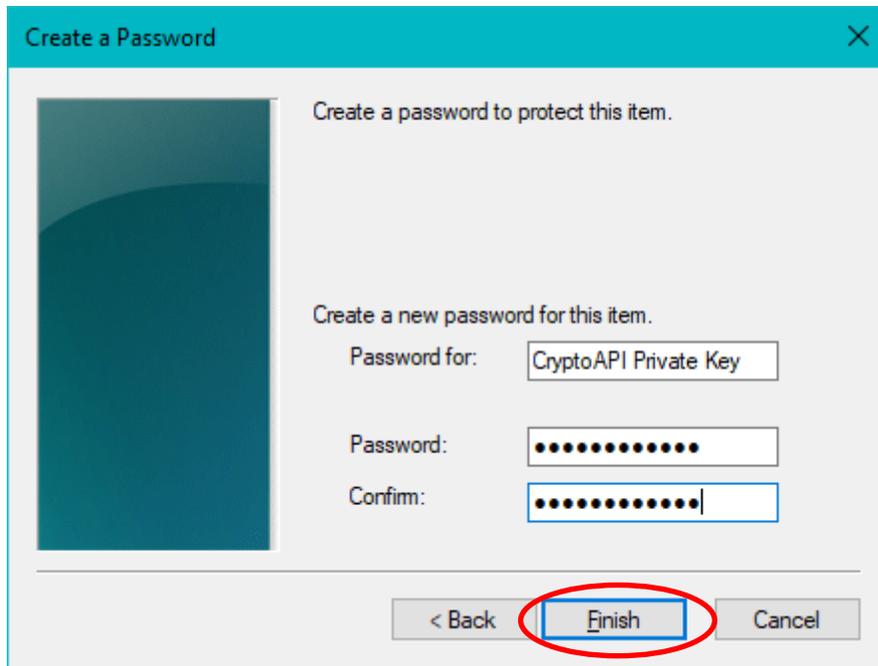
28. On the Importing a new private exchange key dialog box, click on the **Set Security Level...**



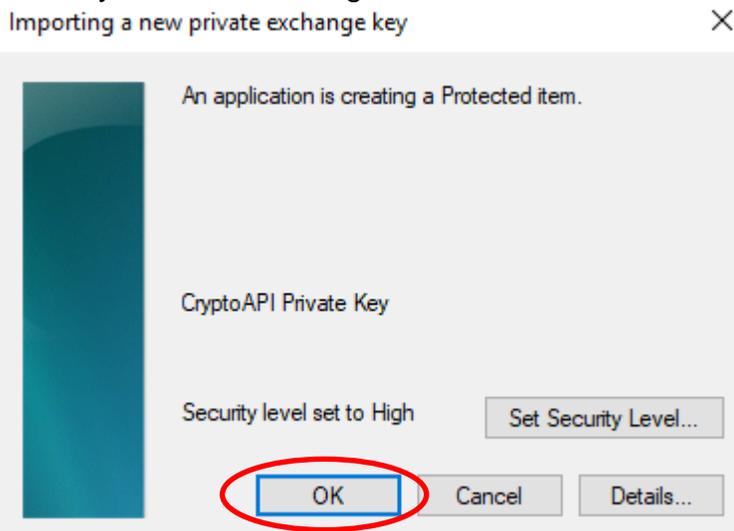
29. Change the “security level” from Medium to High and click the **Next >** button



30. 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.*



31. 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.



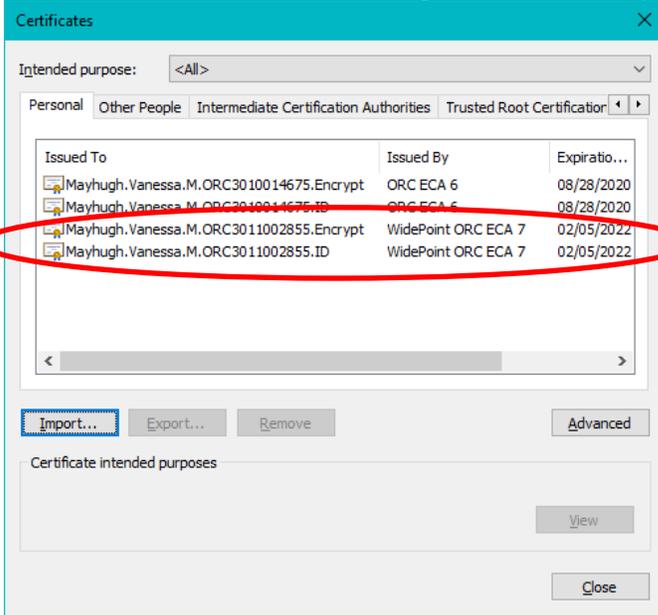
32. At "The import was successful, click the **OK** button.

Certificate Import Wizard

 The import was successful.

OK

33. Back on the Certificates dialog box, if correctly imported you will see the following



Intended purpose: <All>

Personal Other People Intermediate Certification Authorities Trusted Root Certification

Issued To	Issued By	Expiration...
Mayhugh.Vanessa.M. ORC3010014675.Encrypt	ORC ECA 6	08/28/2020
Mayhugh.Vanessa.M. ORC3010014675.ID	ORC ECA 6	08/28/2020
Mayhugh.Vanessa.M. ORC3011002855.Encrypt	WidePoint ORC ECA 7	02/05/2022
Mayhugh.Vanessa.M. ORC3011002855.ID	WidePoint ORC ECA 7	02/05/2022

Import... Export... Remove Advanced

Certificate intended purposes

View

Close