The Enrollment Key Pair is created when you make an on-line 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 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:

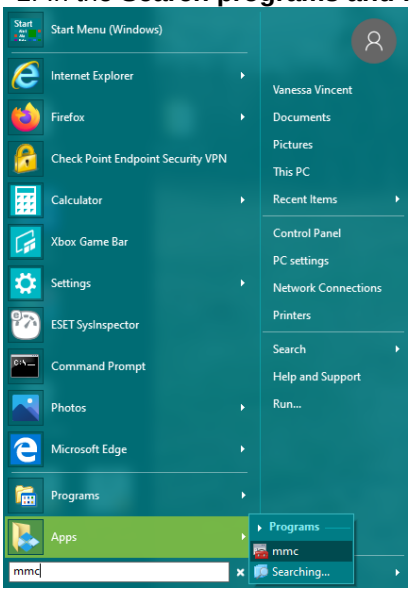
- Have had certificates with a non-exportable Private Key
- Anticipate a major change or upgrade to their computer, operating system, profile, domain, etc. before they will be able to import their issued certificate and make a backup copy of their certificate
- Want to confirm that the Enrollment Key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

A successful backup of the Enrollment Key Pair will confirm:

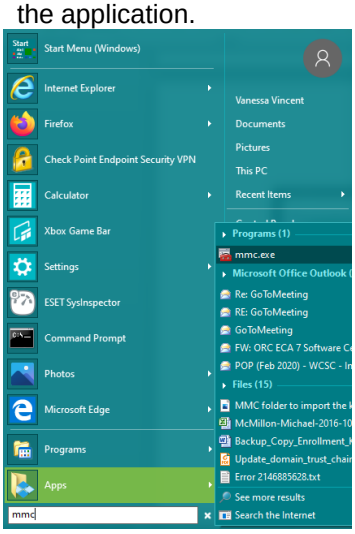
- that the Private Key for your future certificate is fully functional
- that you have set a password on your future certificate's Private Key
- that you and your computer agree on what that password is
- that you have an 'insurance policy' for the success of the entire certificate procedure *(The ECA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

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

2. In the **Search programs and files** field, enter “mmc” and hit the enter key

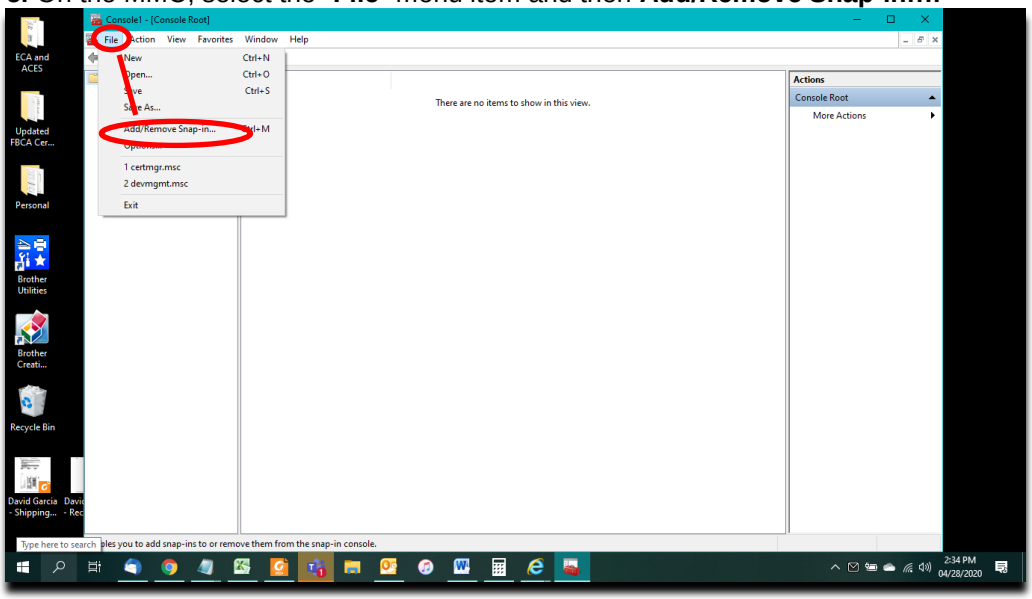


3. In the search results, under Programs (at the top of the screen), double click mmc.exe to run the application.

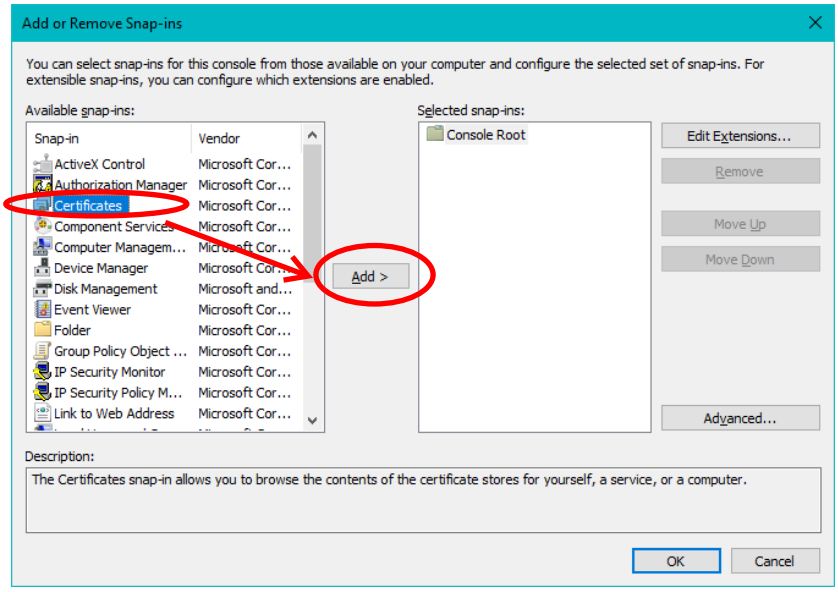


4. If your computer asks if you want to run the Microsoft Management Console (MMC), click the **Yes** button [not pictured]

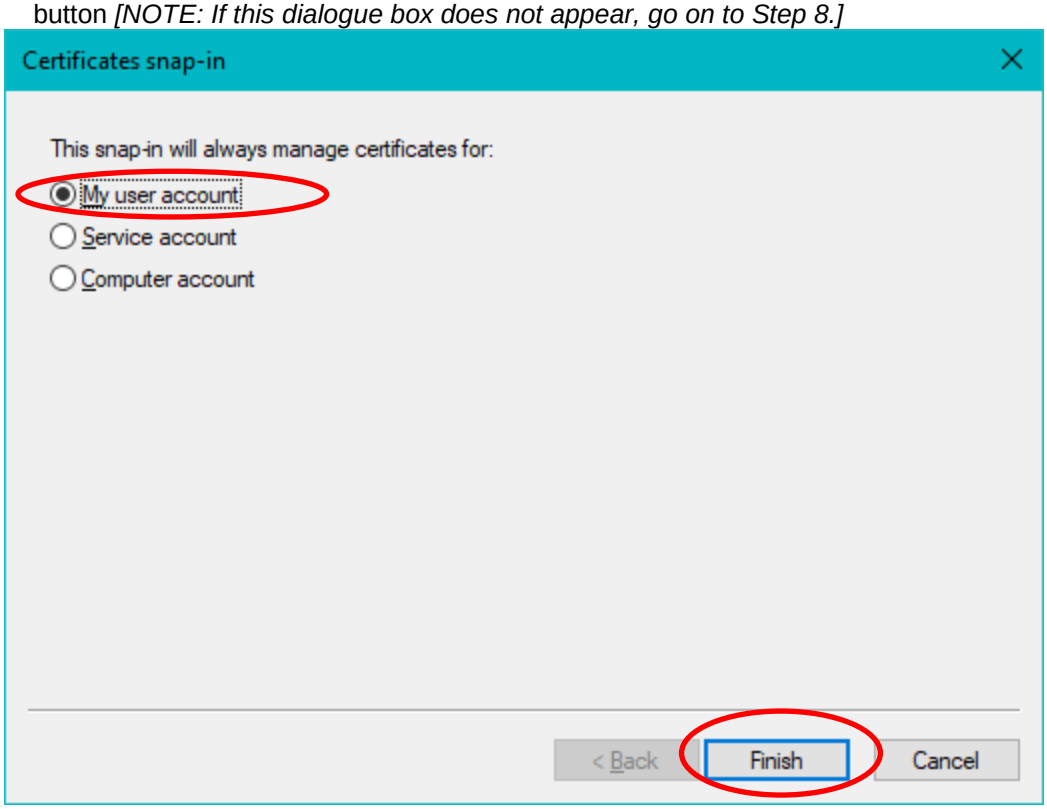
5. On the MMC, select the "**File**" menu item and then **Add/Remove Snap-in….**



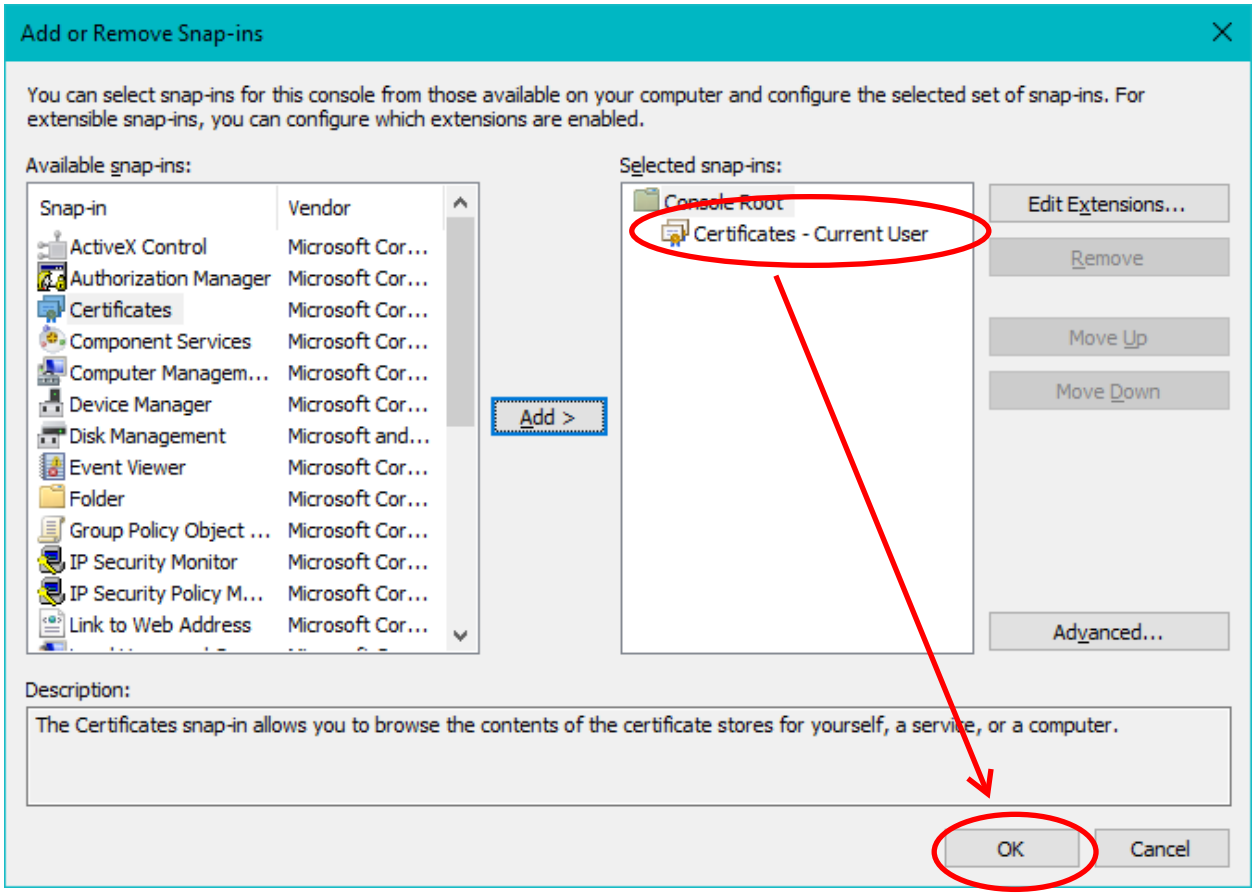
6. On the Add or Remove Snap-ins dialog, select "**Certificates**" and click the "**Add**" button



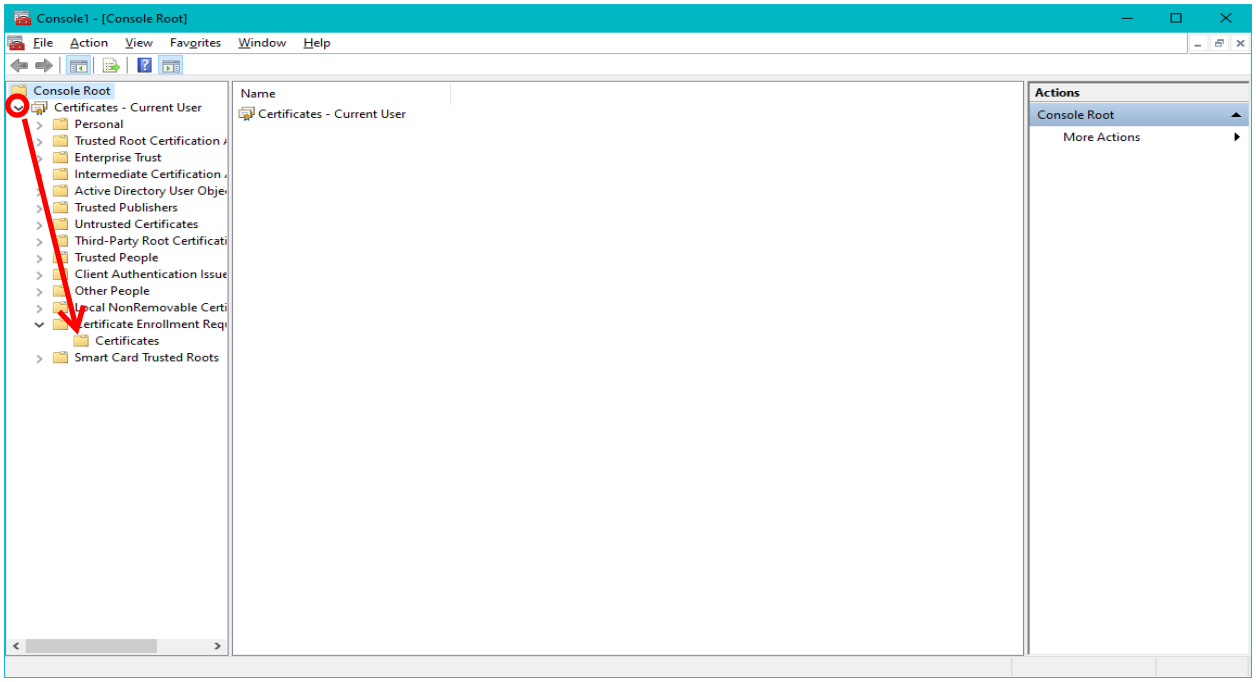
7. If you see a Certificates Snap-in dialog, make sure that My user account is selected and click the Finish button *[NOTE: If this dialogue box does not appear, go on to Step 8.]*



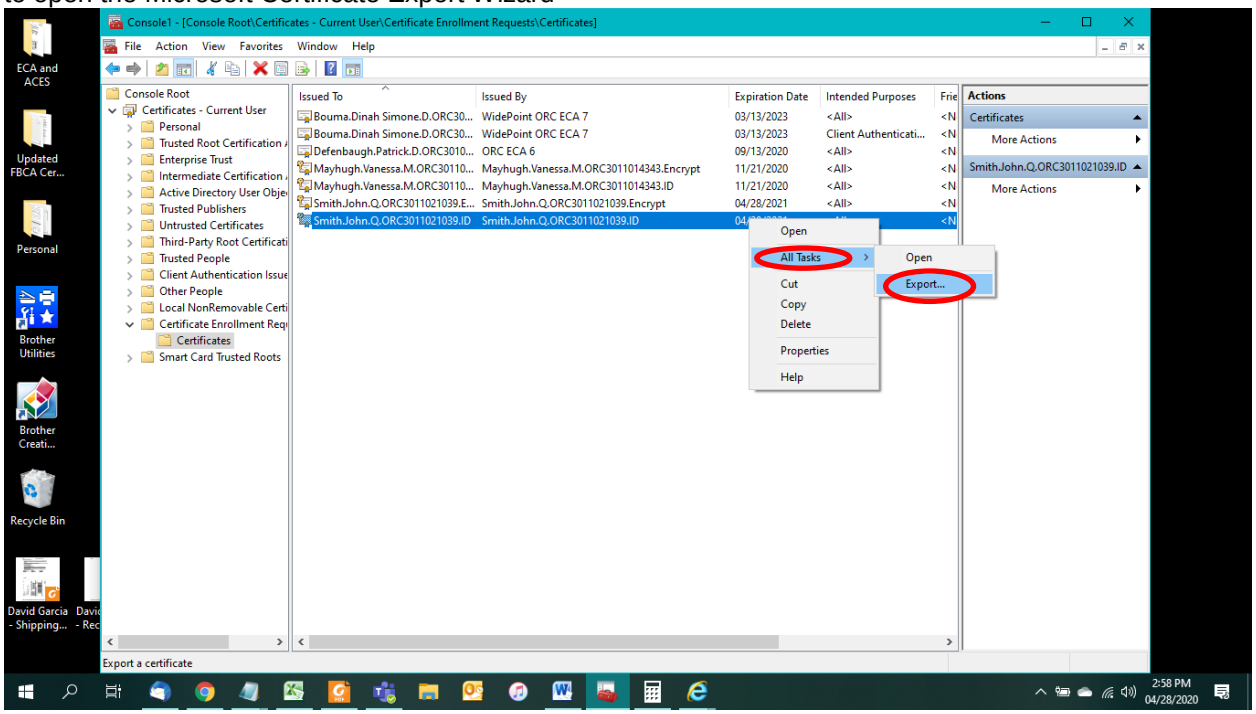
8. Back on the Add or Remove Snap-ins dialog, you should see “Certificates – Current User” under “Console Root”. Click the **OK** button.



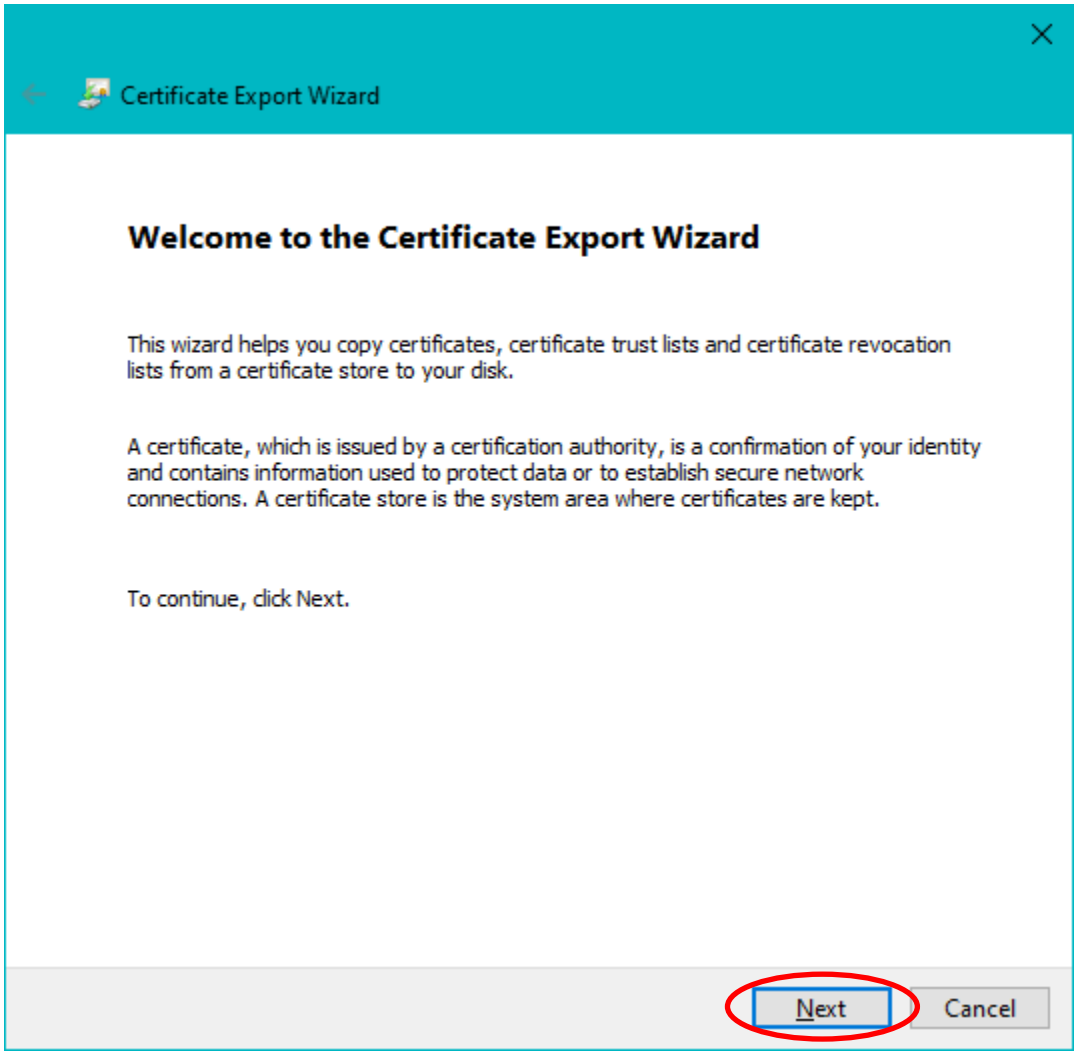
9. Back on the MMC; click the triangle by “Certificates – Current User” to expand the data, then click the triangle by “Certificate Enrollment Requests” to expand that item. Double click on the “Certificates folder”



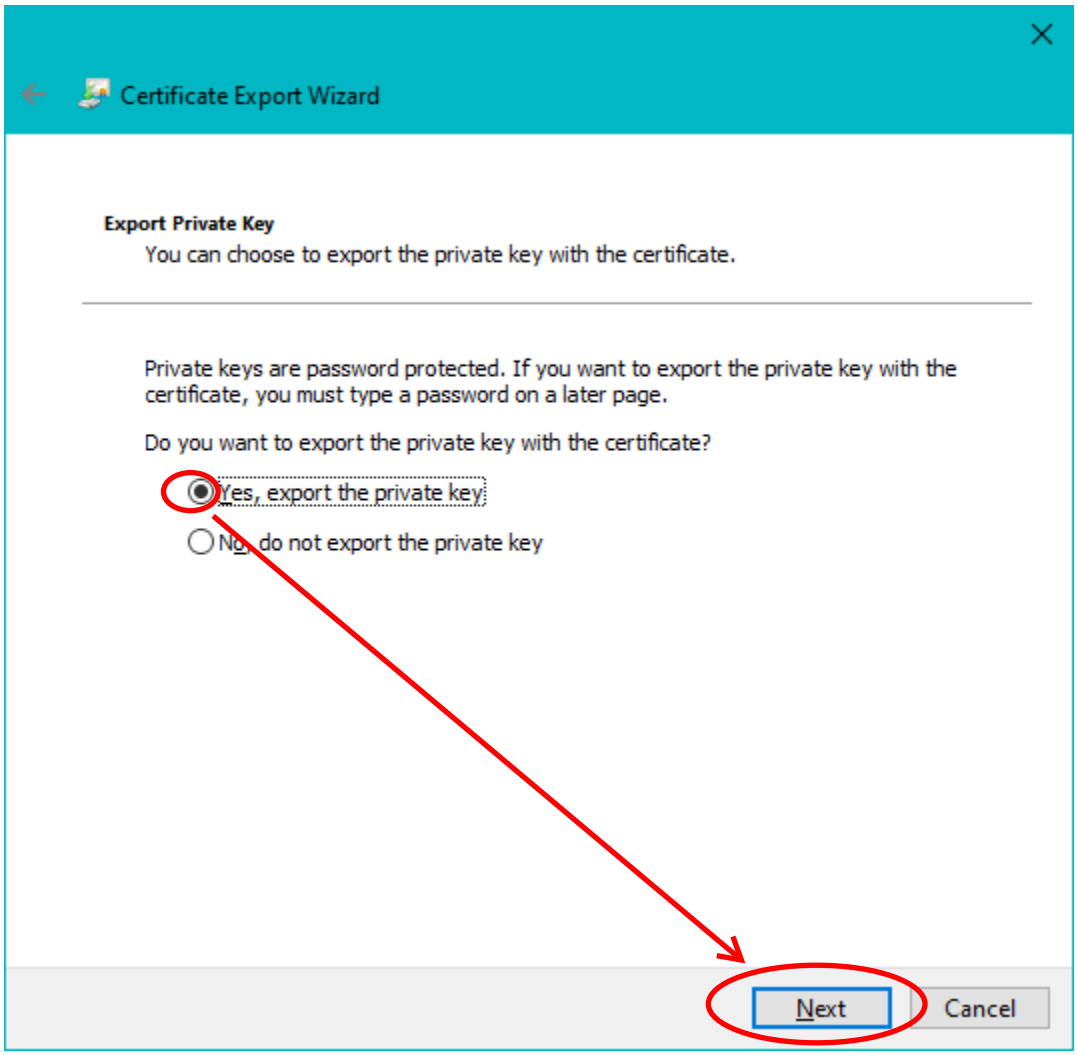
10. Select the entry that reads “LastName.FirstName.MI.ORC#.ID” (this is the key pair for the Identity Certificate) and right-click. From the resulting menu, select **All Task** -> **Export…** to open the Microsoft Certificate Export Wizard



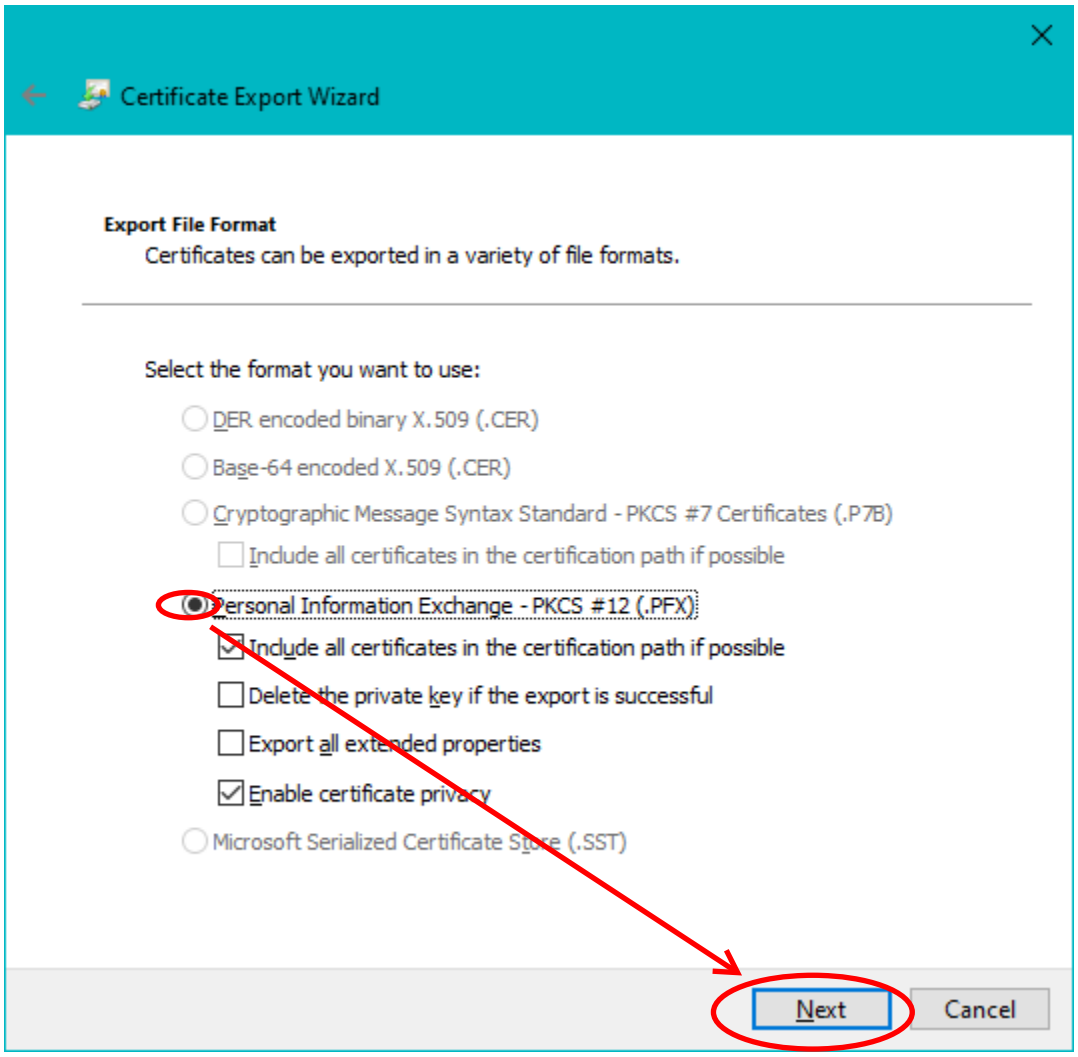
11. Click "**Next**" in the "**Certificate Export Wizard**" dialogue



12. 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 ECA help desk at ecahelp@orc.com*



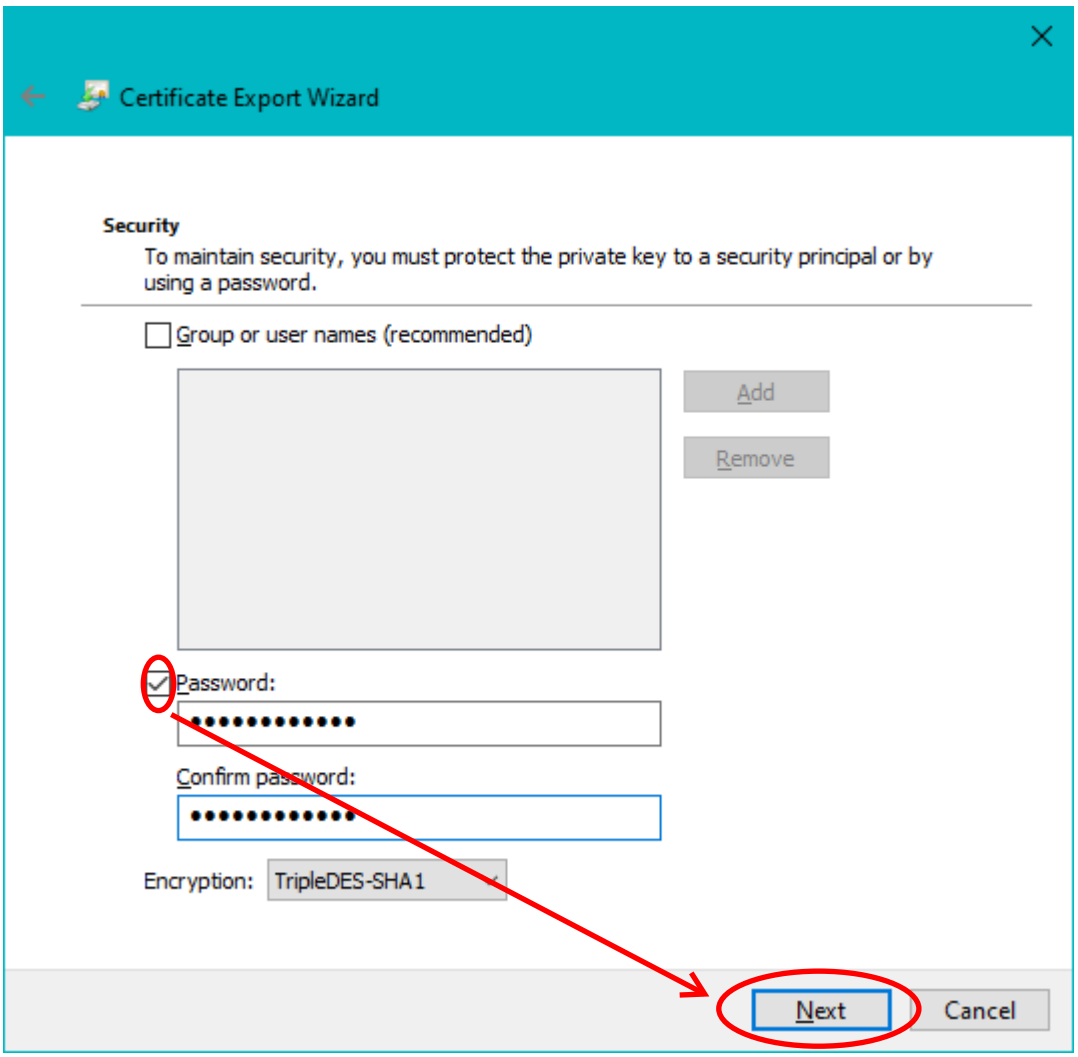
13. On the **"**Export File Format**"** screen, make sure that "**Personal Information Exchange**" is selected. Then click "**Next**"



14. Assign a **Password** to protect the file that you are about to create. (Please note that you are assigning a password at this point.)

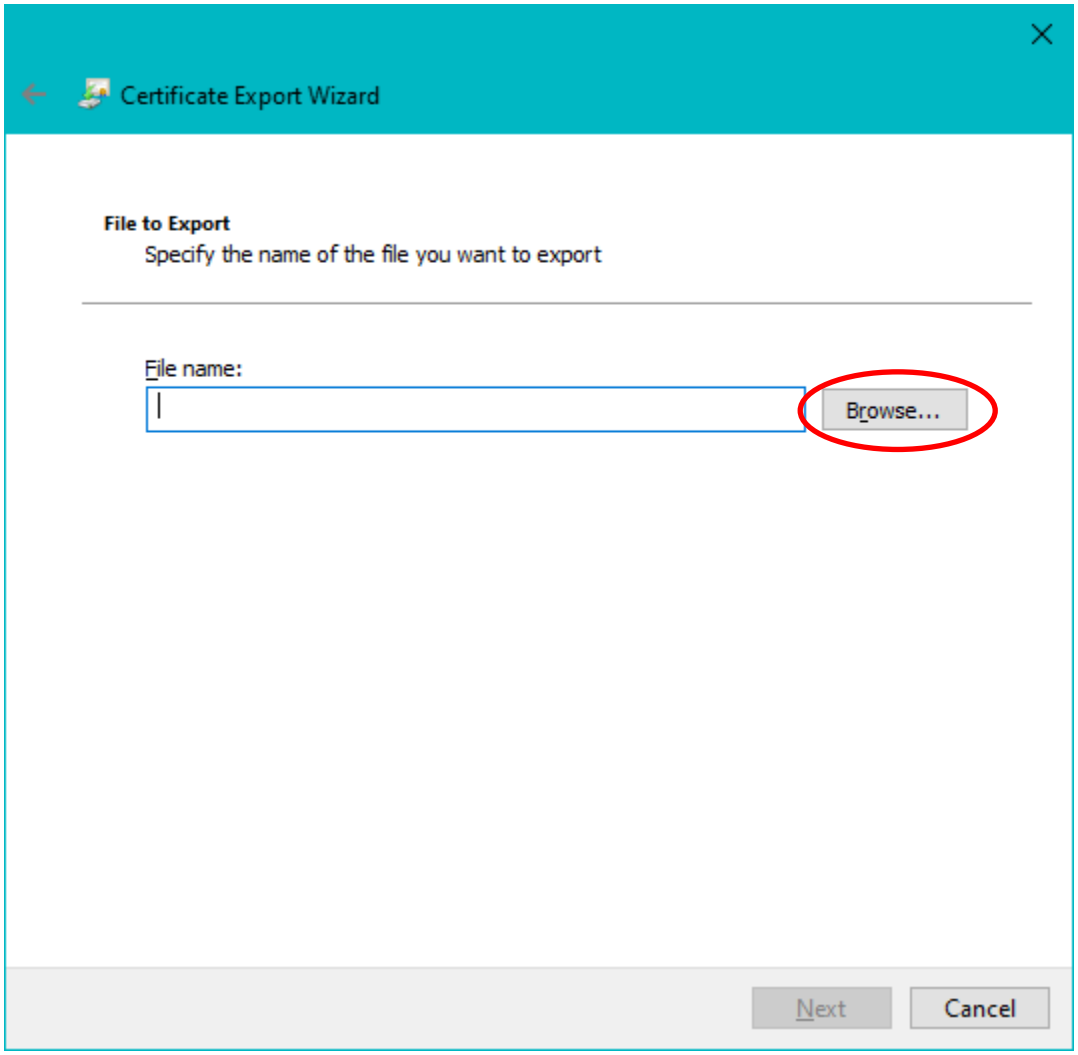
All passwords are case sensitive. It's recommended that your password be compliant with FIPS 112, meaning that it is at least eight characters long, includes upper/lowercase letters, numbers and special characters.

NOTE: ORC recommends that you use the same password here that you created when you requested the certificate.



.

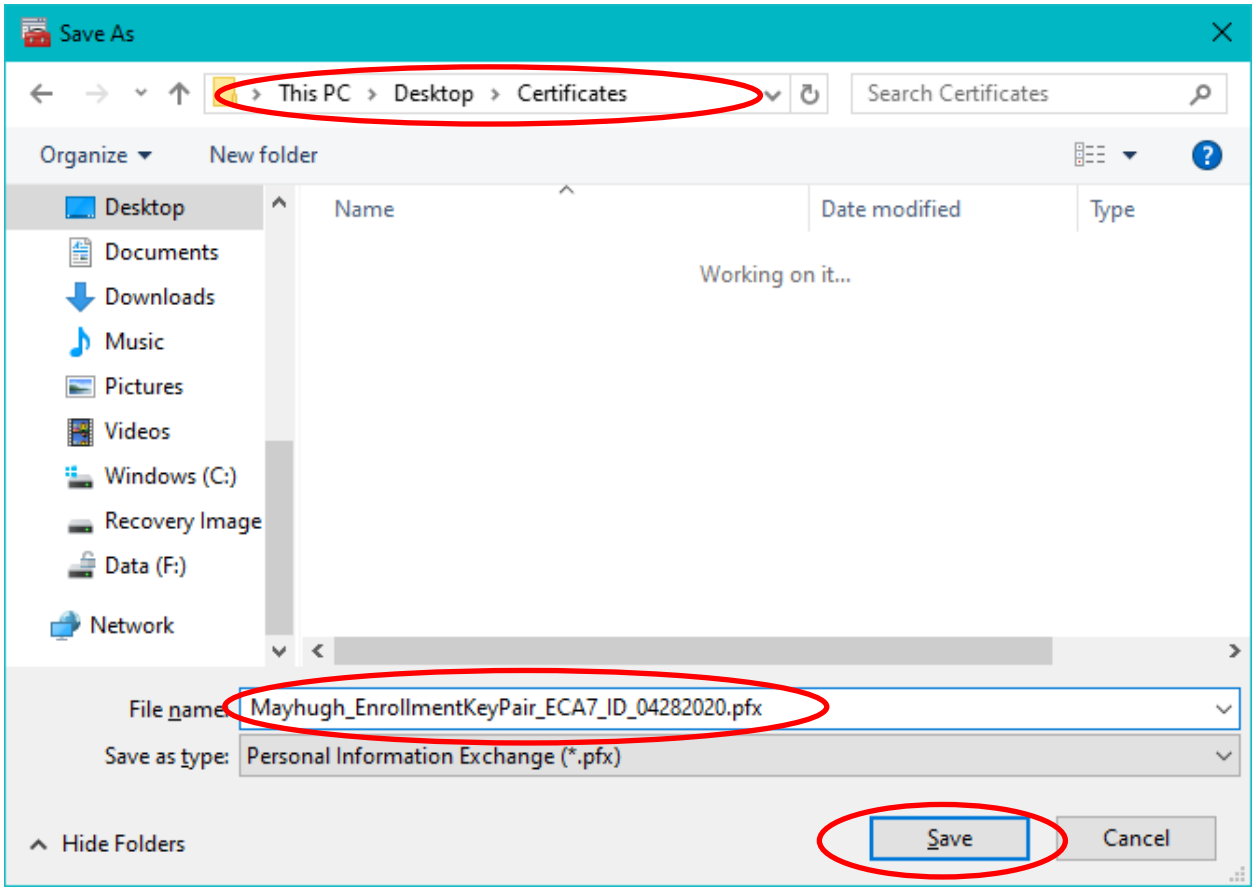
15. Click "**Browse**" and select where you want to save the operational copy of your private key(s); *Make sure that you are the only person with access to your private key copy*.



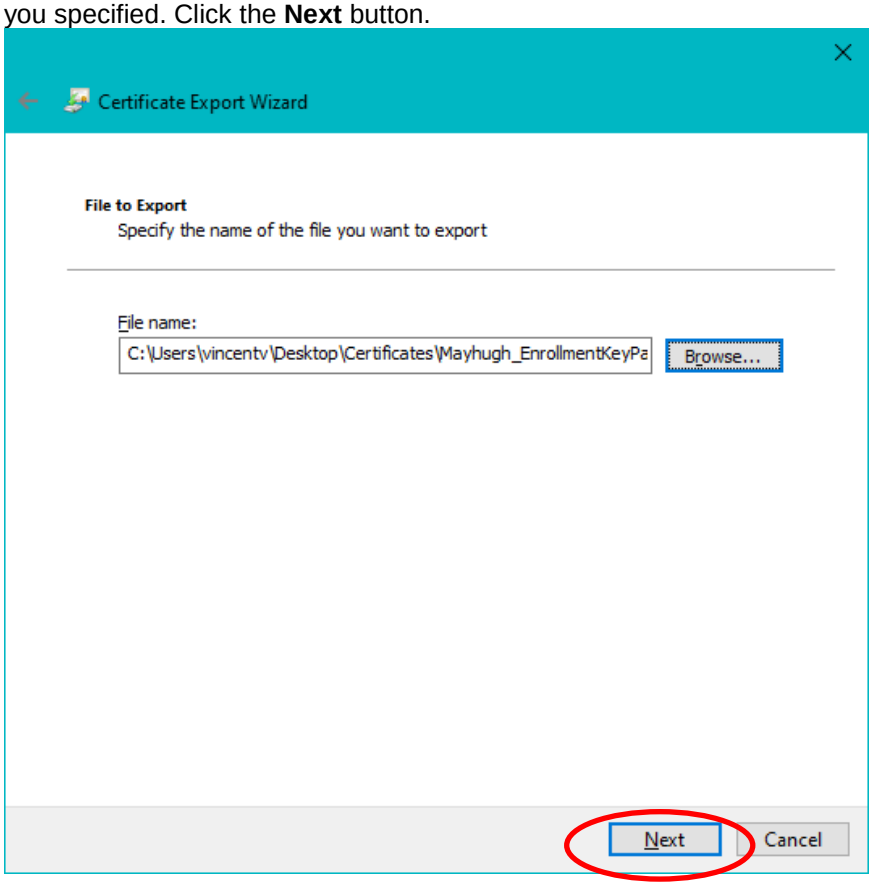
16. Select a location on your computer for the file to be saved. The Desktop is a convenient location to save these Enrollment Key back-up files. Then enter a file name in the **File Name:** field. ORC's recommended filename convention LastName_EnrollmentKeyPair_ECA7_ID_todays date. Then click the **Save** button.

The file name convention shown above is not required. But all certificate back-up files look the same; the only way to tell them apart is by the name that you give to the file when you create it. If you do not follow the naming convention above, ORC may not be able to help you effectively in the future.

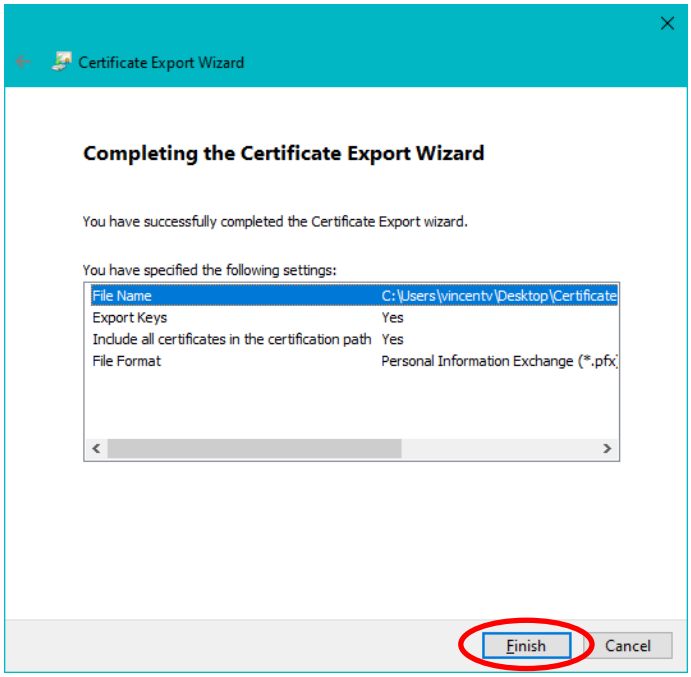
NOTE: You should move the back-up file(s) to an external storage medium when you are finished.

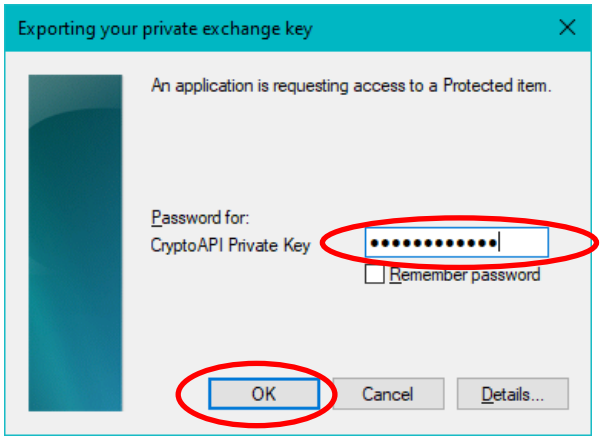


17. Back on the **"**Specify the name of the file…**"** screen, you should see a path and file name that you specified. Click the **Next** button.



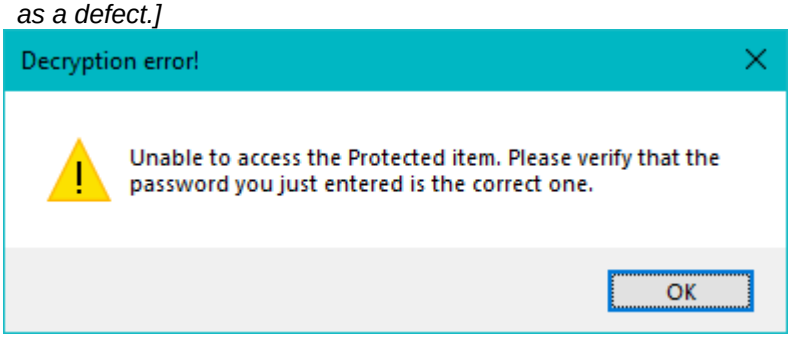
18. Click "**Finish**" to complete the saving of your private key.



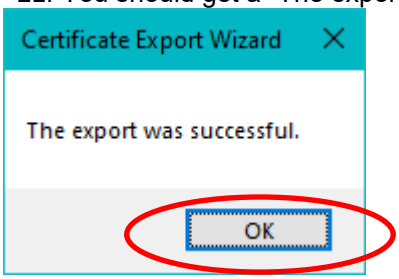


19. A 'pop-up window' will ask for the password that you assigned to the private key when the private key was created by making the certificate request (which you did before you even opened these instructions).. *This is <u>not</u> (necessarily) the password that you assigned in Step 14 above.* Enter the password currently assigned to the private key.

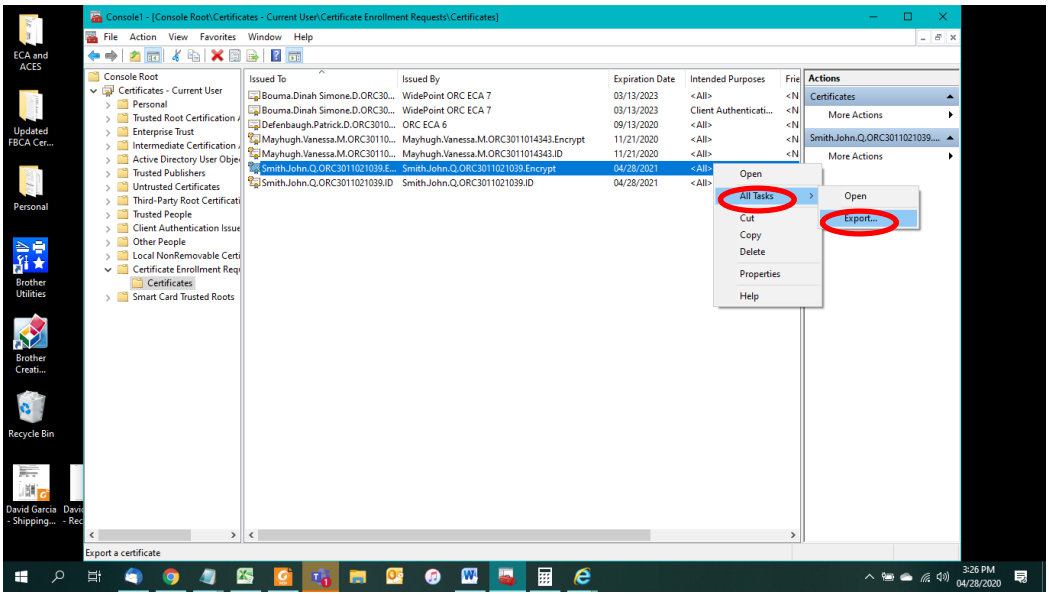
20. **WARNING!** If you get the message below, you have NOT entered the password that was assigned (by you) when the certificate request was made. *[Please be aware that Windows 7 and above have been known to create a file after entering an incorrect password multiple times, but the file is not a true back-up file. This is a Windows problem that ORC has reported to Microsoft as a defect.]*



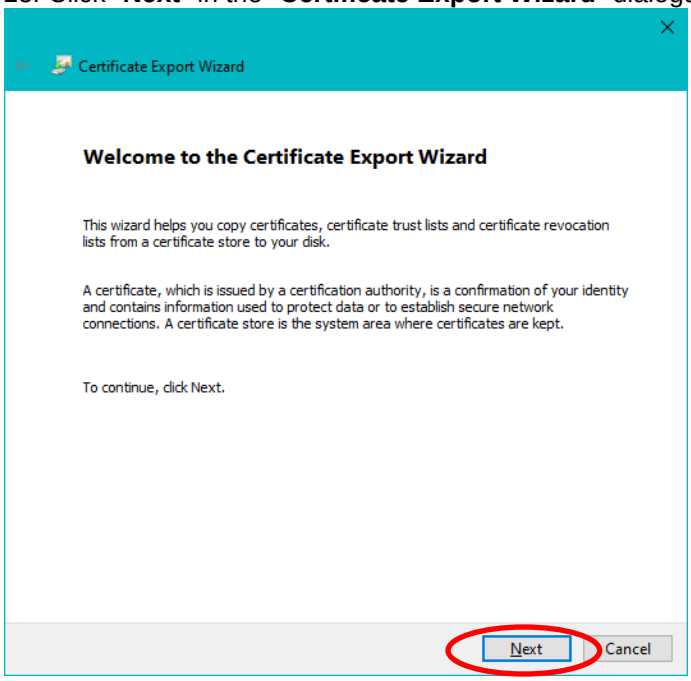
21. You should get a “The export was successful.” message immediately. Click "**OK**".



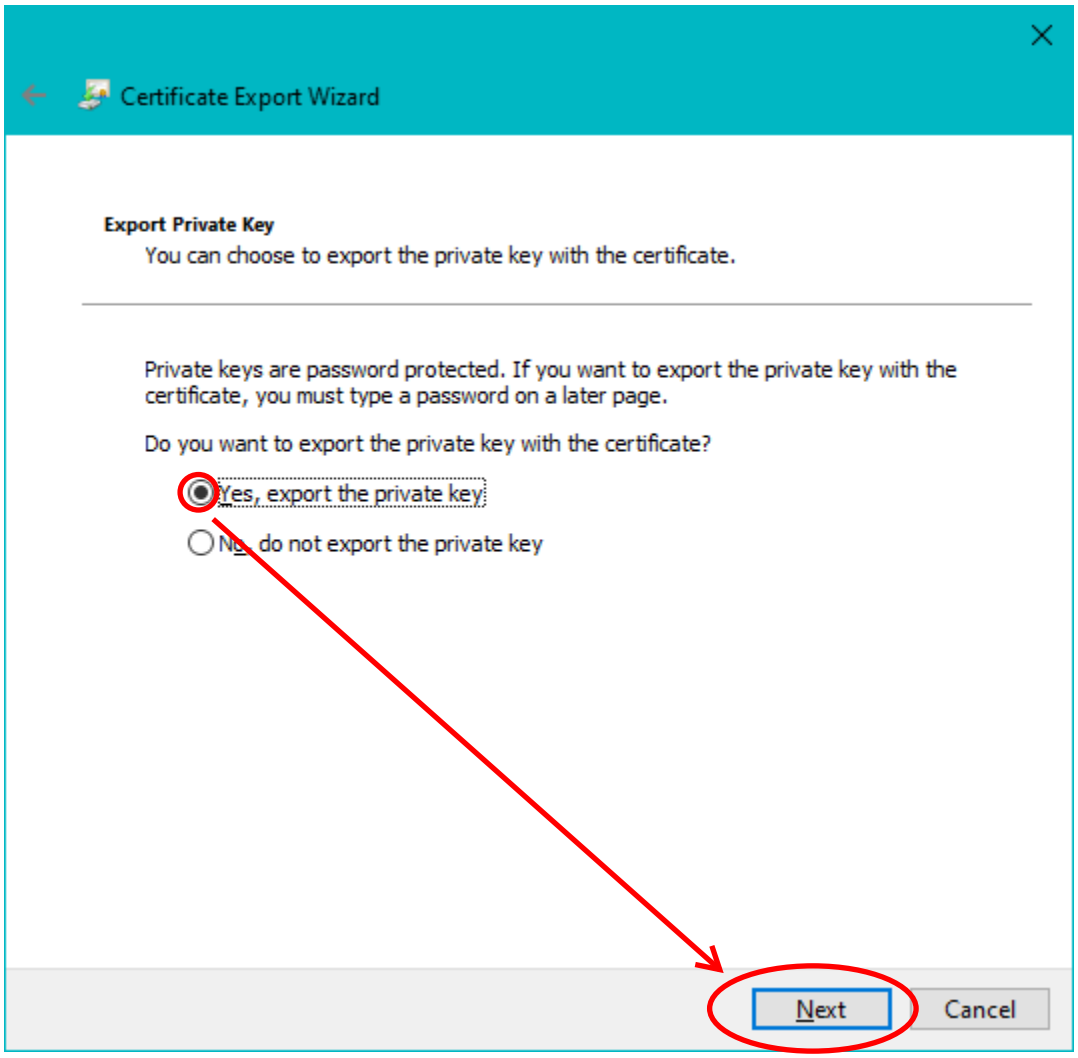
22. Back on the MMC; select the entry that read “*yourlastname*_EnrollKeyPair_ECA7_ID_*todaysdate*” (this is the keypair for the Encryption Certificate) and right-click. From the resulting menu, select **All Task** -> **Export…** to open the Microsoft Certificate Export Wizard



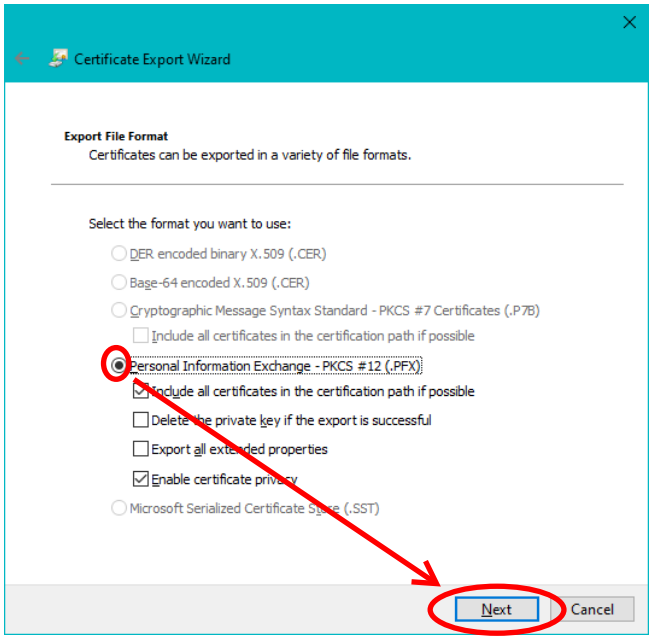
23. Click "**Next**" in the "**Certificate Export Wizard**" dialogue



24. 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 ECA Help Desk.*



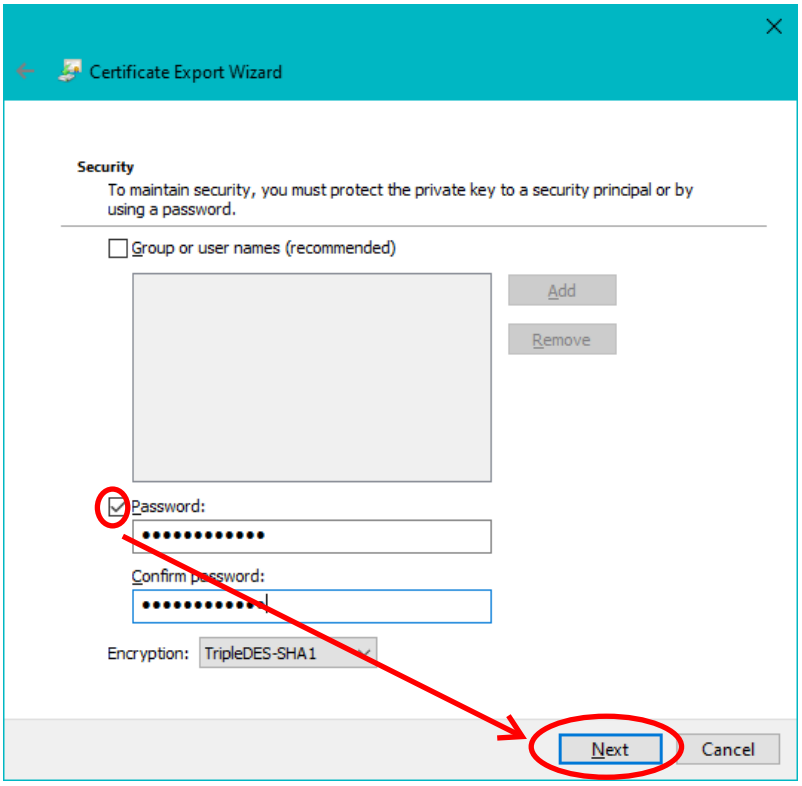
25. On the **"**Export File Format**"** screen, make sure that "**Personal Information Exchange**" is selected. Then click "**Next**"



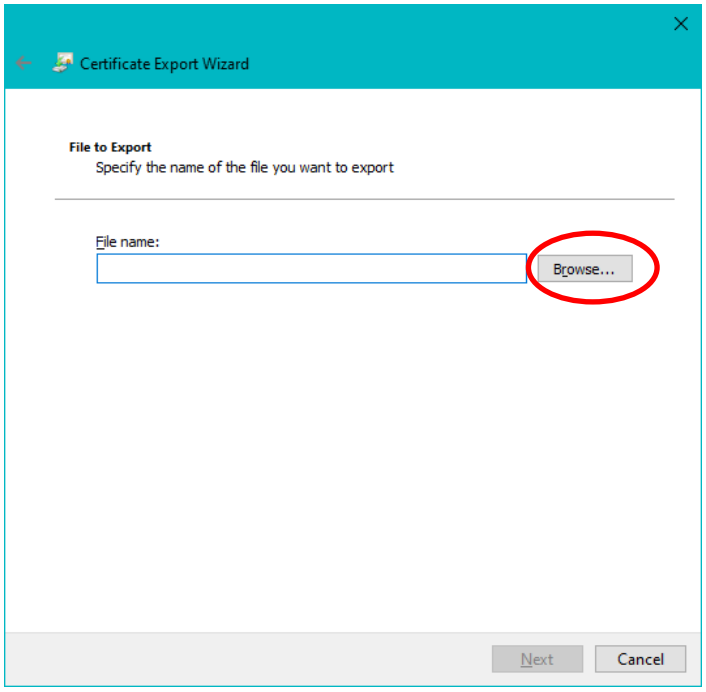
26. Assign a **Password** to protect the file that you are about to create. (Please note that you are assigning a password at this point.)

All passwords are case sensitive. It's recommended that your password be compliant with FIPS 112, meaning that it is at least eight characters long, includes upper/lowercase letters, numbers and special characters.

NOTE: ORC recommends that you use the same password here that you created when you requested the certificate.

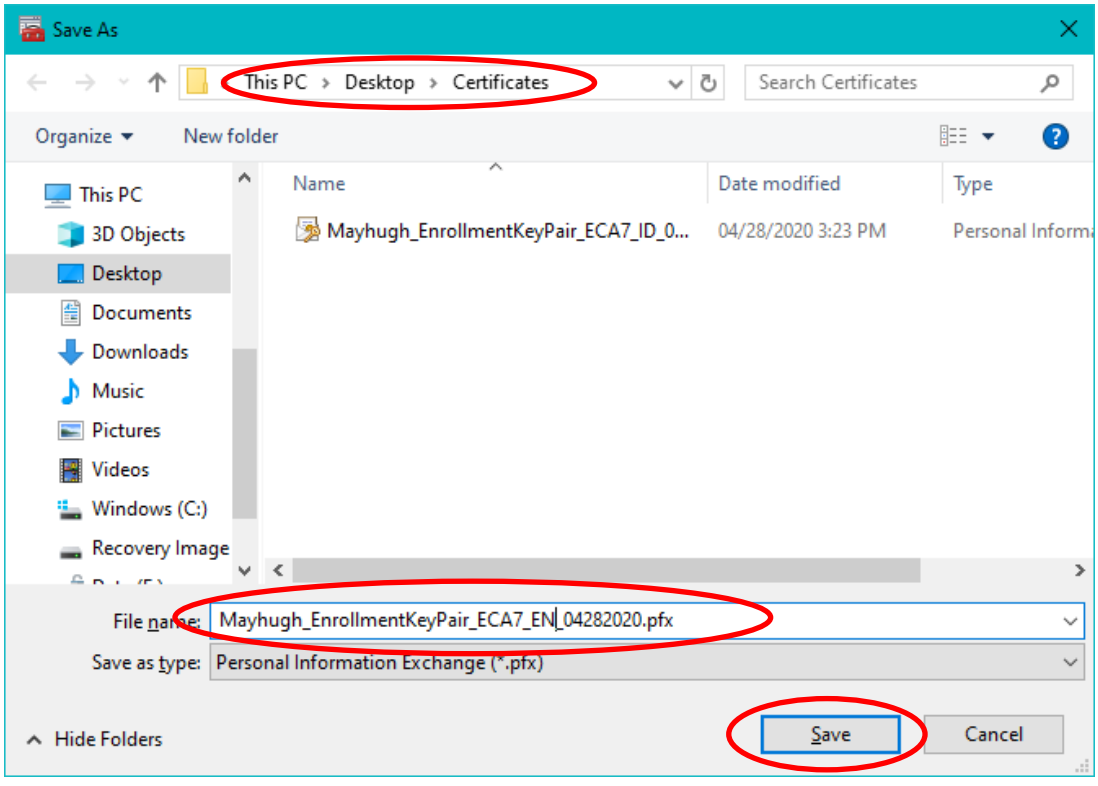


27. Click "**Browse**" and select where you want to save the operational copy of your private key(s); *Make sure that you are the only person with access to your private key copy*.

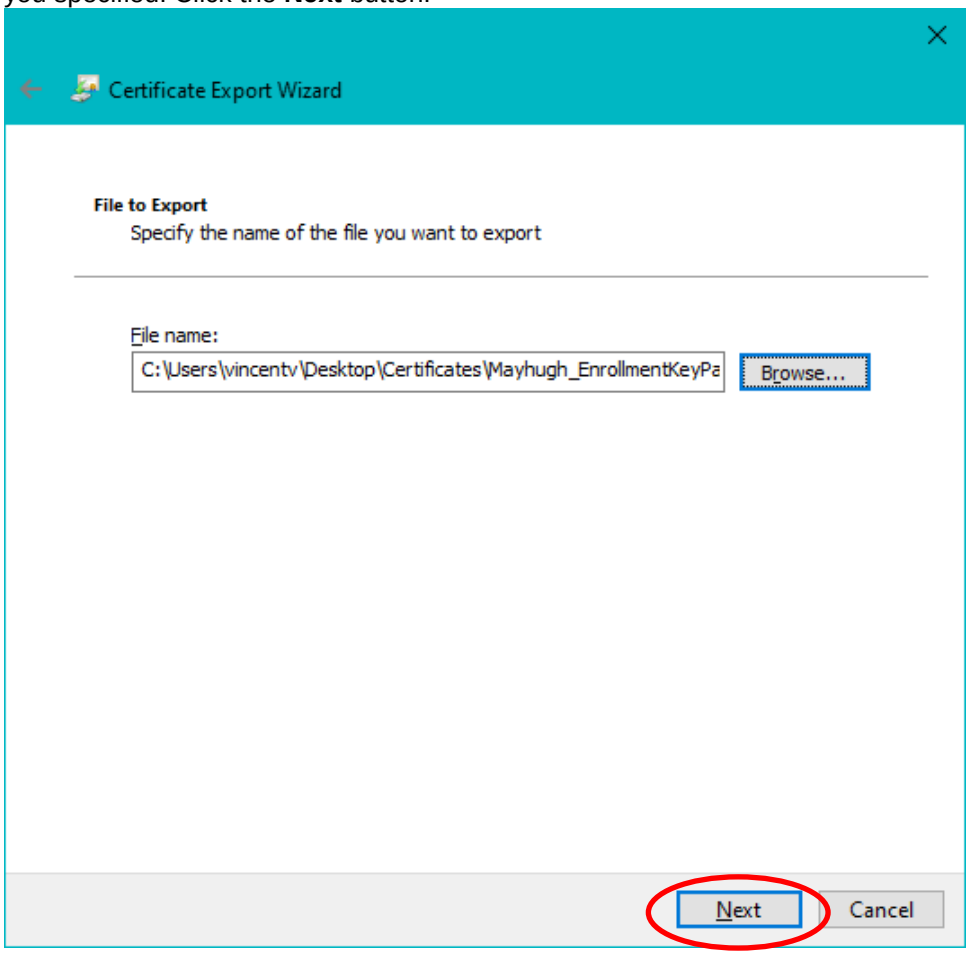


28. Select a location on your computer for the file to be saved. The Desktop is a convenient location to save these Enrollment Key back-up files. Then enter a file name in the **File Name:** field. ORC's recommended filename convention LastName_EnrollmentKeyPair_ECA7_EN_todays date. Then click the **Save** button.

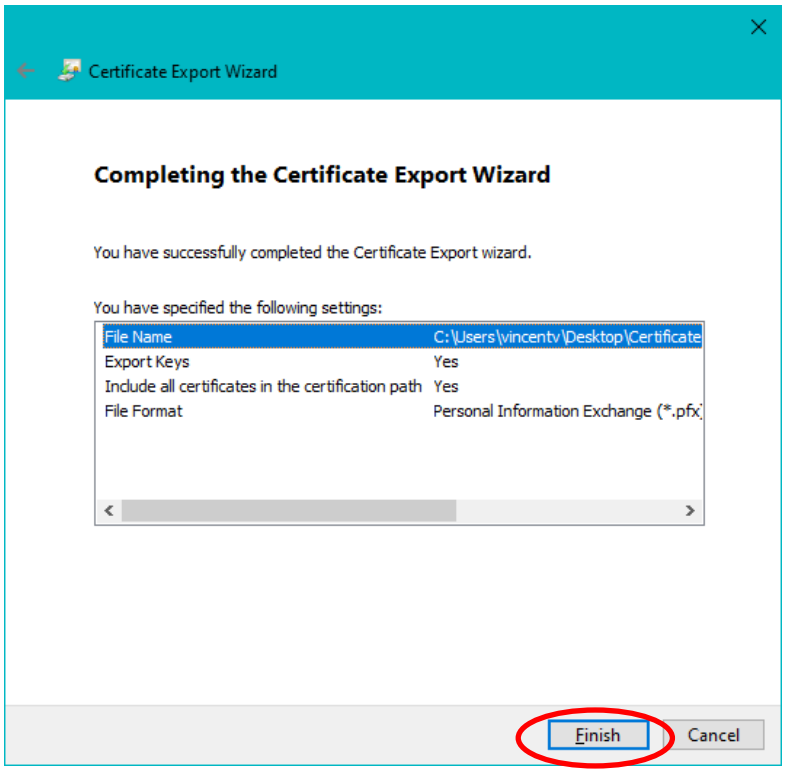
The file name convention shown above is not required. But all certificate back-up files look the same; the only way to tell them apart is by the name that you give to the file when you create it. If you do not follow the naming convention above, ORC may not be able to help you effectively in the future.



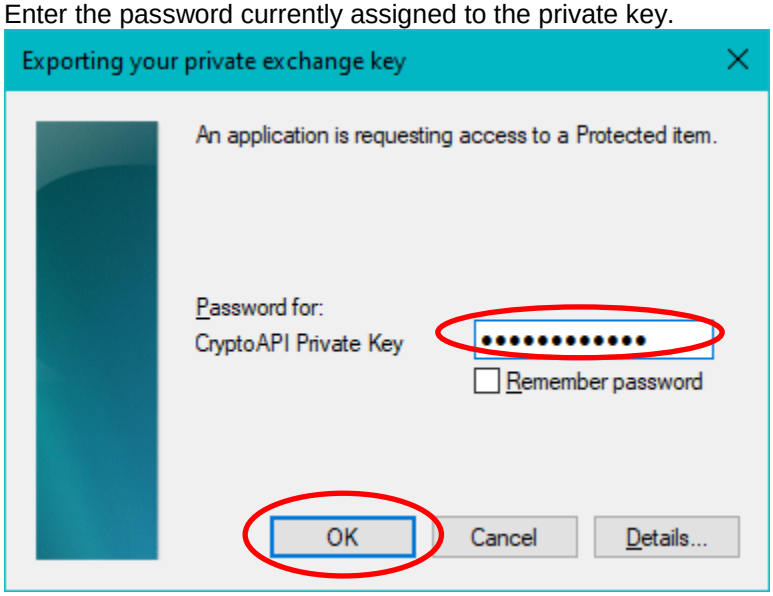
29. Back on the **"**Specify the name of the file…**"** screen, you should see a path and file name that you specified. Click the **Next** button.



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



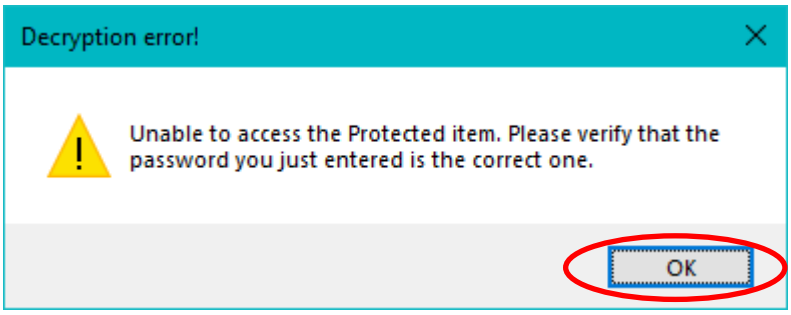
31. A ‘pop-up window’ will ask for the password that you assigned to the private key when the private key was created by making the certificate request (which you did before you even opened these instructions).. *This is <u>not</u> (necessarily) the password that you assigned in Step 14 above.* Enter the password currently assigned to the private key.



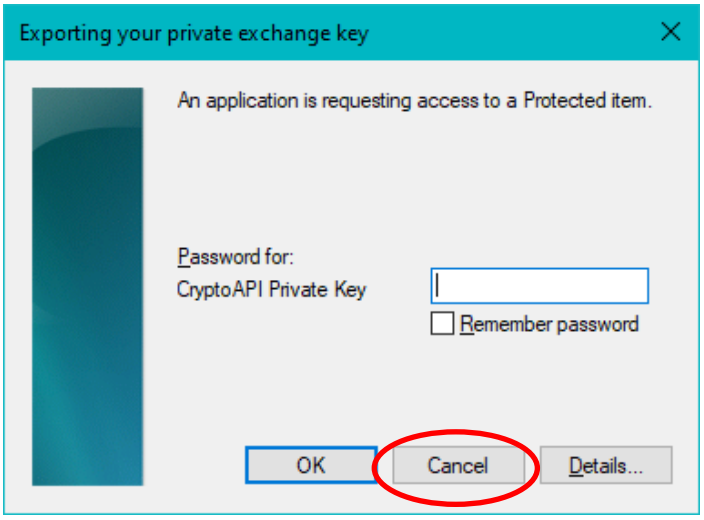
32. **WARNING!** If you get the message below, you have NOT entered the password that was assigned (by you) when the certificate request was made

Windows 7/8/10 has a bug that can create a **<u>FALSE</u> back-up file** if you are not careful. If you should click the Cancel button or enter an incorrect password multiple (4+) times Windows 7,8, and 10 have been known to create a file that is **<u>not</u>** a true back-up file.

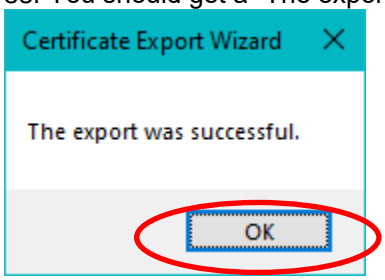
You need to perform his procedure without seeing the ‘error’ message below to ensure that you have a good back-up file. If the file size is less than 2KB, the file is ‘bad’.



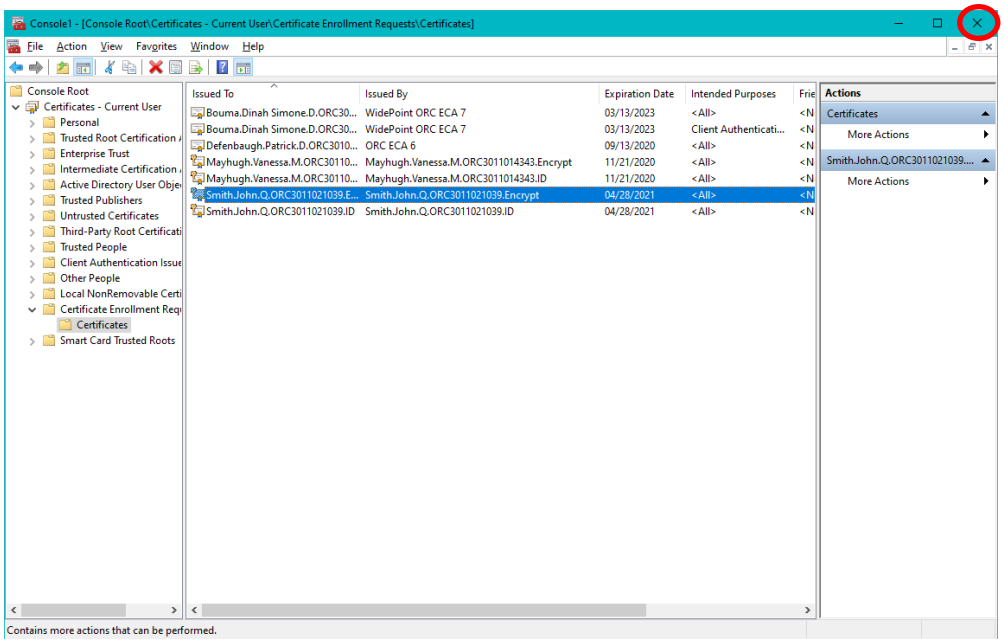
If you get warning above, **cancel** out of the process and **start again** at **Step 10** *(Windows will tell you the back-up was successful, but it was <u>not</u>)*



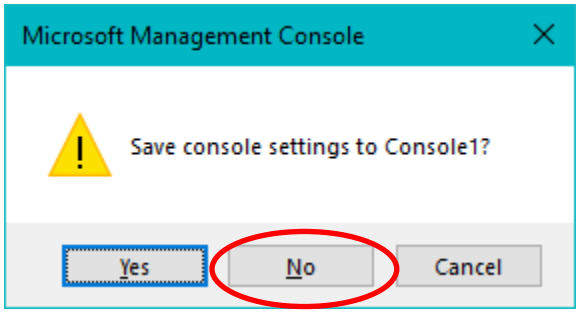
33. You should get a “The export was successful.” message immediately. Click "**OK**".



34. You have successfully backed up your certificate enrollment key pairs. You may close the MMC by clicking the X in the right hand corner of the box



35. When asked if you want to save the console settings, click "**No**".


Microsoft Management Console
Save console settings to Console1?
Yes
No
Cancel