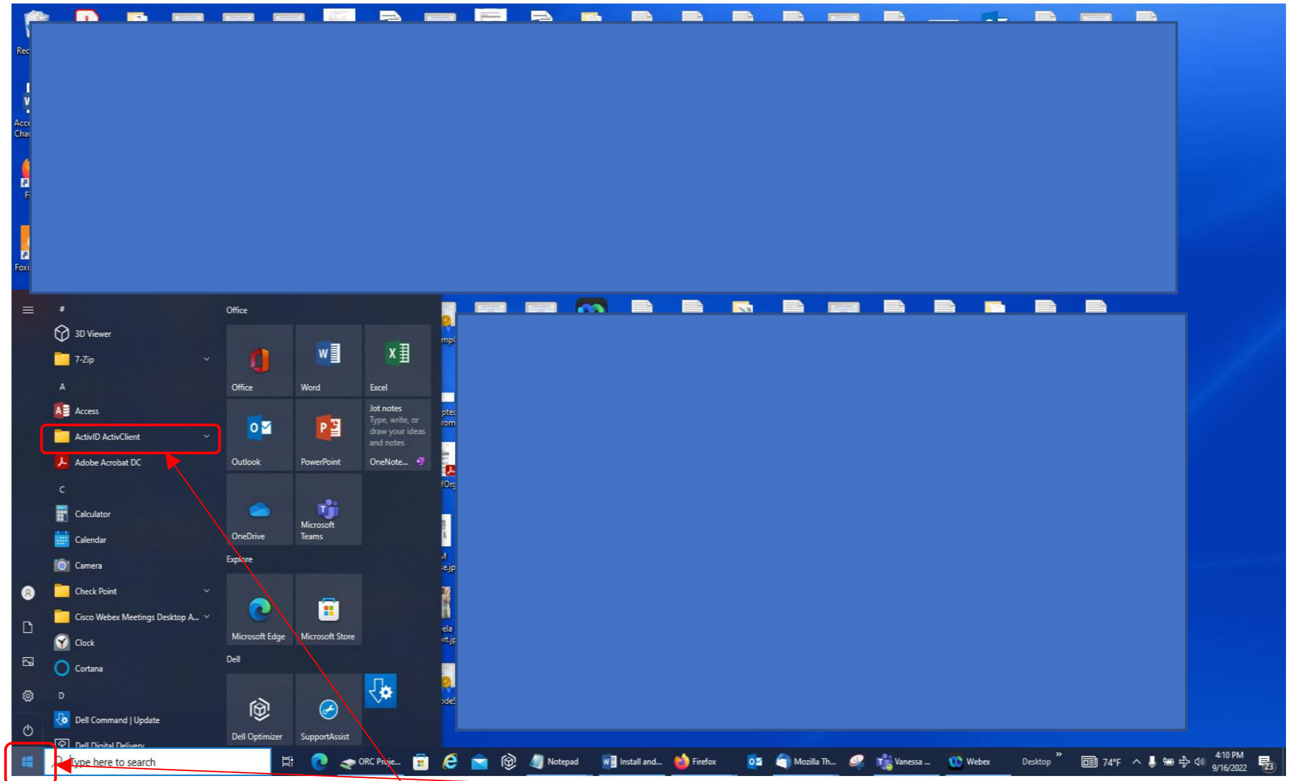
1. The Subscriber will download the WidePointPKISolutionV2.msi file from the WidePoint LRA and put it in a location on the computer C Drive. **<u>IMPORTANT</u>** – The subscriber may need a system administrator to download and/or install this WidePoint Proprietary App; the subscriber needs to check with the system administrator to ensure that the <u>Windows **certReq** Command</u> on that PC is NOT blocked and that the security on the PC does NOT block the download of **<u>.p12</u>** and **<u>.cer</u>** files AND does NOT stop or block the generation/creation of the **<u>.csr</u>** and **<u>.inf</u>** files (these types of files will need to download or be generated into the Public Documents Folder under the Subscriber's User Profile as part of the process).

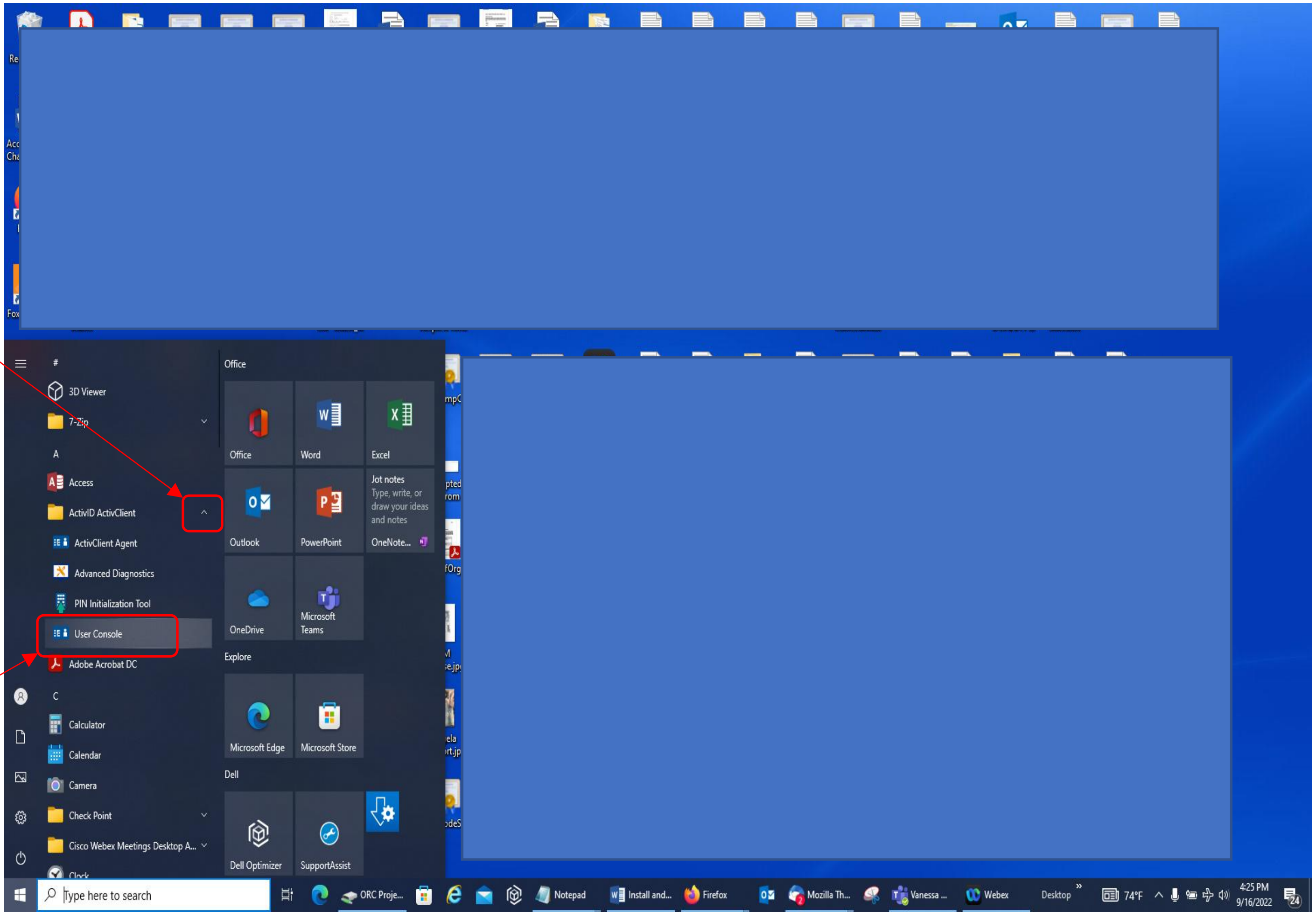
2. The Subscriber will need to check the smartcard or cryptotoken to ensure there is enough space on it to add two more certificates during the download process. Left-click the mouse button on the Windows Start Button and the ActivID ActivClient should appear in the list of programs if ActivClient Software was properly loaded on the PC.



Windows Start Button

ActivID ActivClient Selection

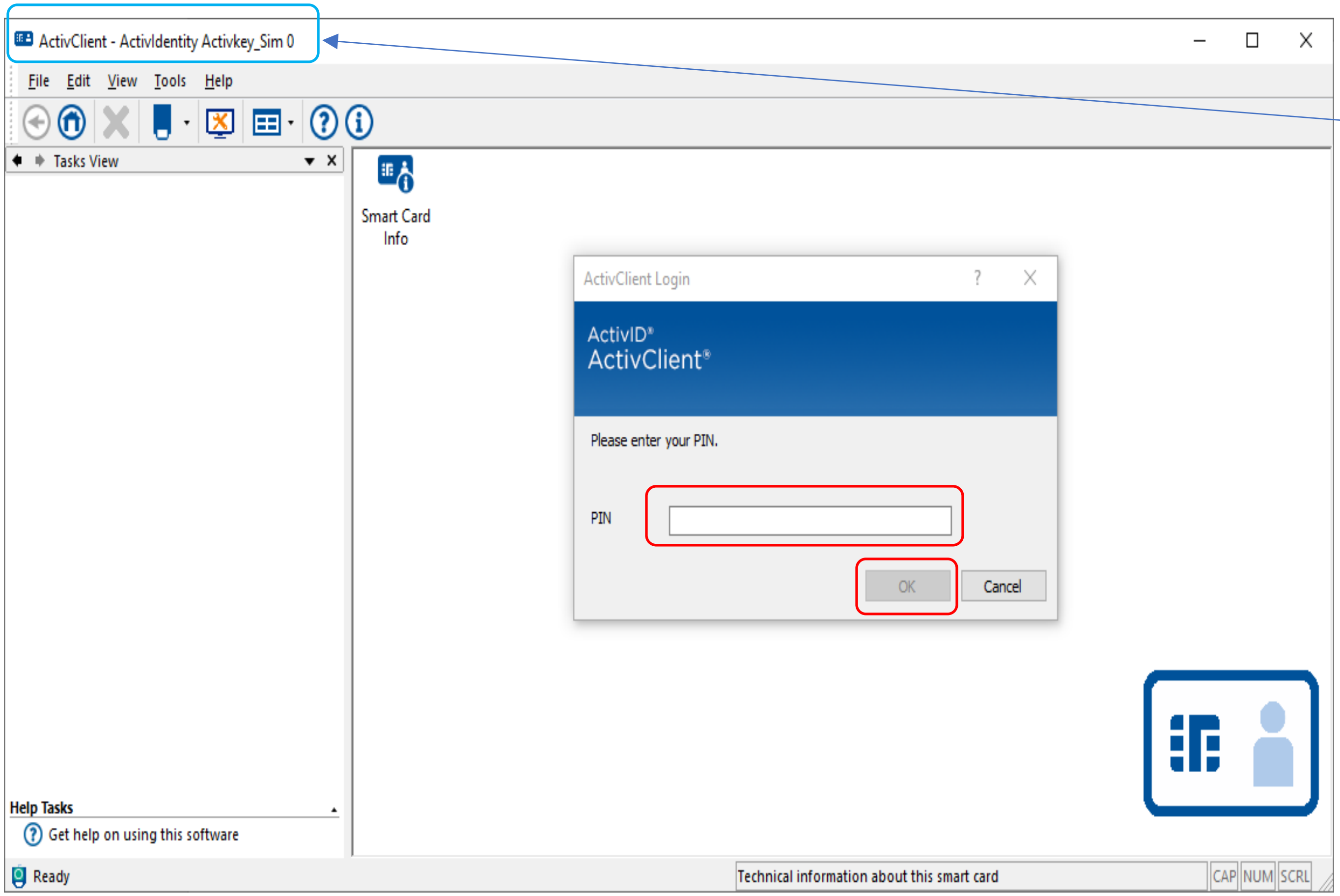
3. Left-click the mouse button on the drop-down arrow for ActivID ActivClient and select User Console from the list.



Drop-down arrow

Select User Console

4. The ActivClient User Console will appear in the screen. Type the PIN Code in for the smartcard/cryptotoken and select the OK Button.



ActivClient - ActivIdentity Activkey_Sim 0

ActivClient Login

Please enter your PIN.

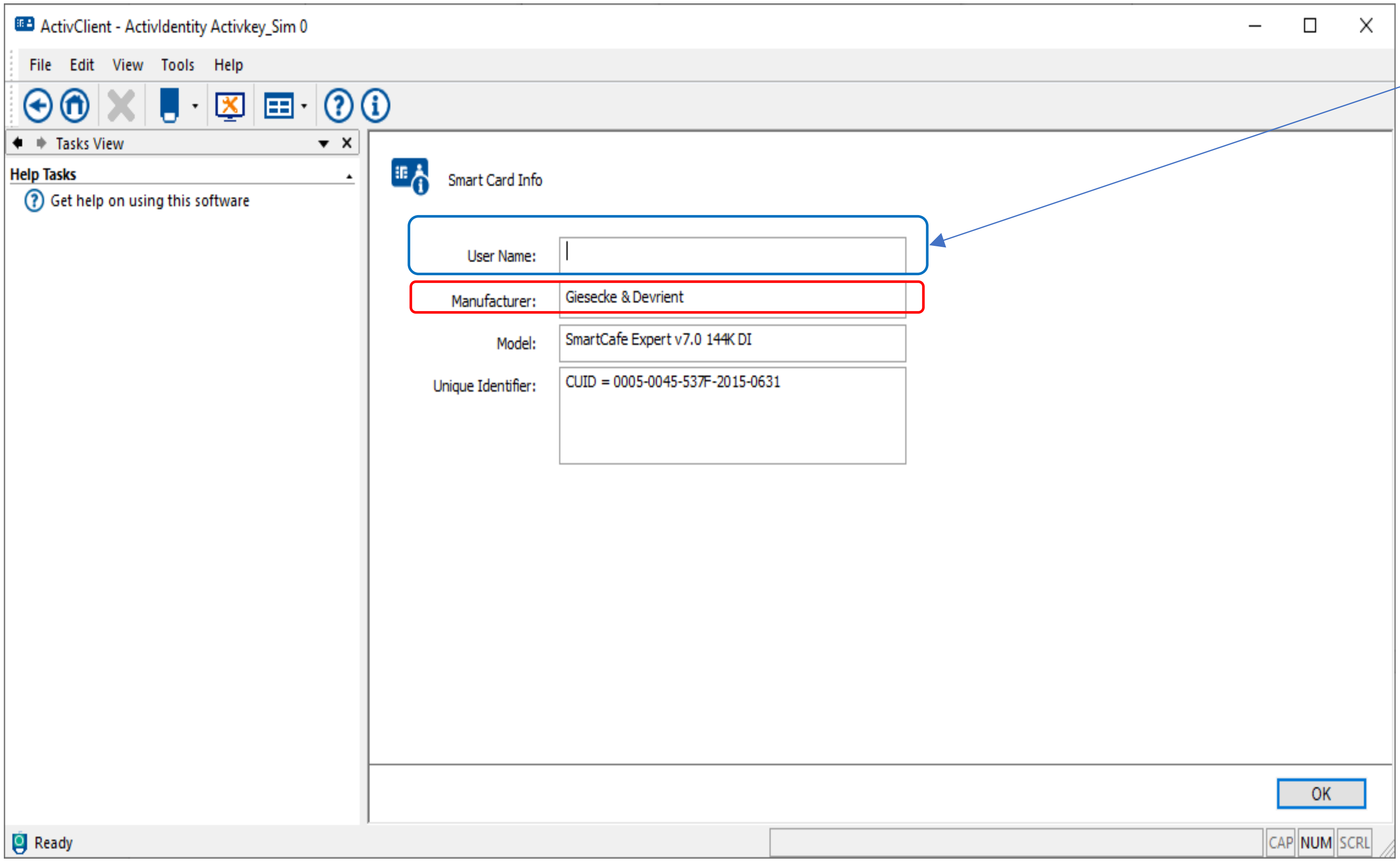
PIN

If you have a cryptotoken (also referred to as USB Token), then the header will say Activkey_Sim 0.

If you have a smartcard, it should say Smartcard.

5. You may or may not get an Unlock Code Screen. If you do get that screen, just click ‘Close.’

6. Open the Smart Card Info Icon by right-clicking the mouse button on it and selecting ‘View smart card info.’ If the Manufacturer says Gemalto, then that device only has spaces for a total of three certificates in My Certificates Folder/Icon (which means that you may have to delete old certificates in order to download the two new certificates if you want to continue using this device; be careful because you may need expired encryption certificates to go back and read the old emails encrypted with them [even after the certificate expiration date]). If the Manufacturer says Giesecke & Devrient or Crescendo, then it should have at least eight spaces for certificates in the My Certificates Folder/Icon. In this case, this USB Token is new and therefore empty, so it does not have a My Certificates Folder/Icon.


ActivClient - ActivIdentity Activkey_Sim 0
File
Edit
View
Tools
Help
Tasks View
Help Tasks
Get help on using this software
Smart Card Info
OK
Ready
CAP
NUM
SCRL

User Name:

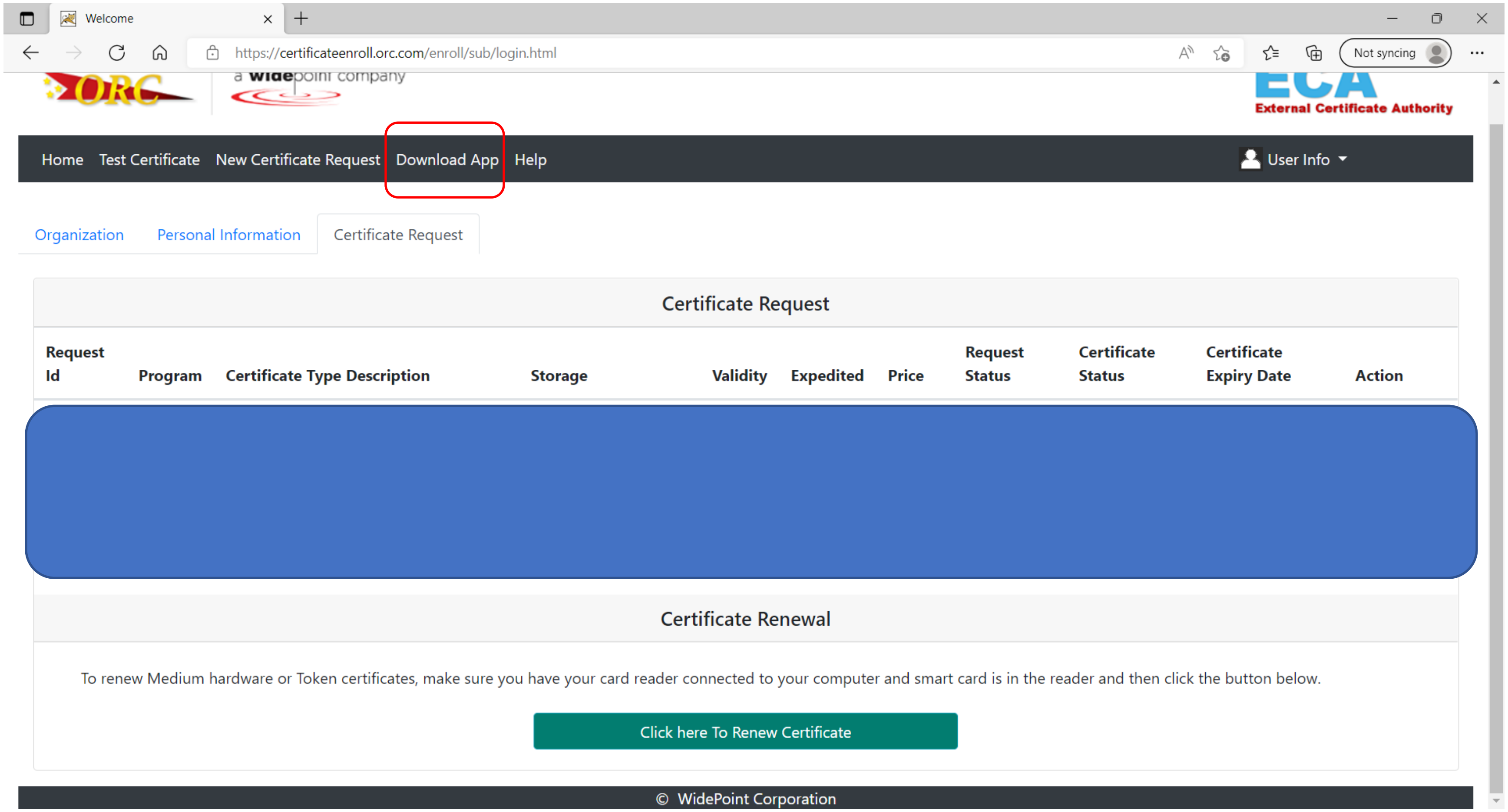
Manufacturer: Giesecke & Devrient

Model: SmartCafe Expert v7.0 144K DI

Unique Identifier: CUID = 0005-0045-537F-2015-0631

If this device previously held certificates, then that person’s name should appear in the User Name Block.

7. The Subscriber will download the WidePoint Proprietary App if he/she has not downloaded it previously. Please note that you cannot have the WidePoint Proprietary App installed over itself or a previous version on the same profile (you can uninstall an existing WidePoint Proprietary App under Control Panel – Programs – Programs and Features). After logging into your ECA Account at our site, you will click on ‘Download App’ in the black menu bar.



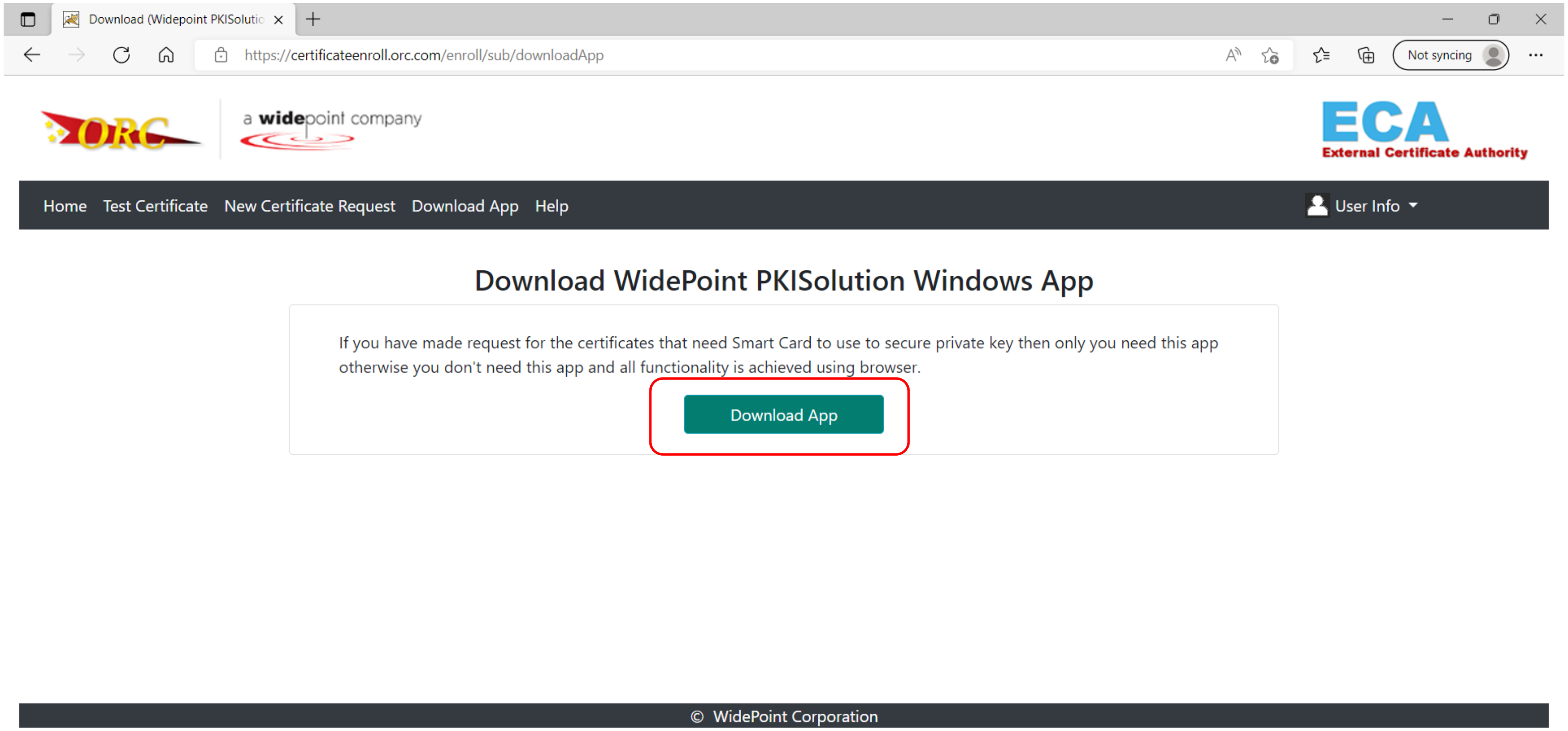
Certificate Request

Request Id	Program	Certificate Type Description	Storage	Validity	Expedited	Price	Request Status	Certificate Status	Certificate Expiry Date	Action
[redacted]										

Certificate Renewal

To renew Medium hardware or Token certificates, make sure you have your card reader connected to your computer and smart card is in the reader and then click the button below.

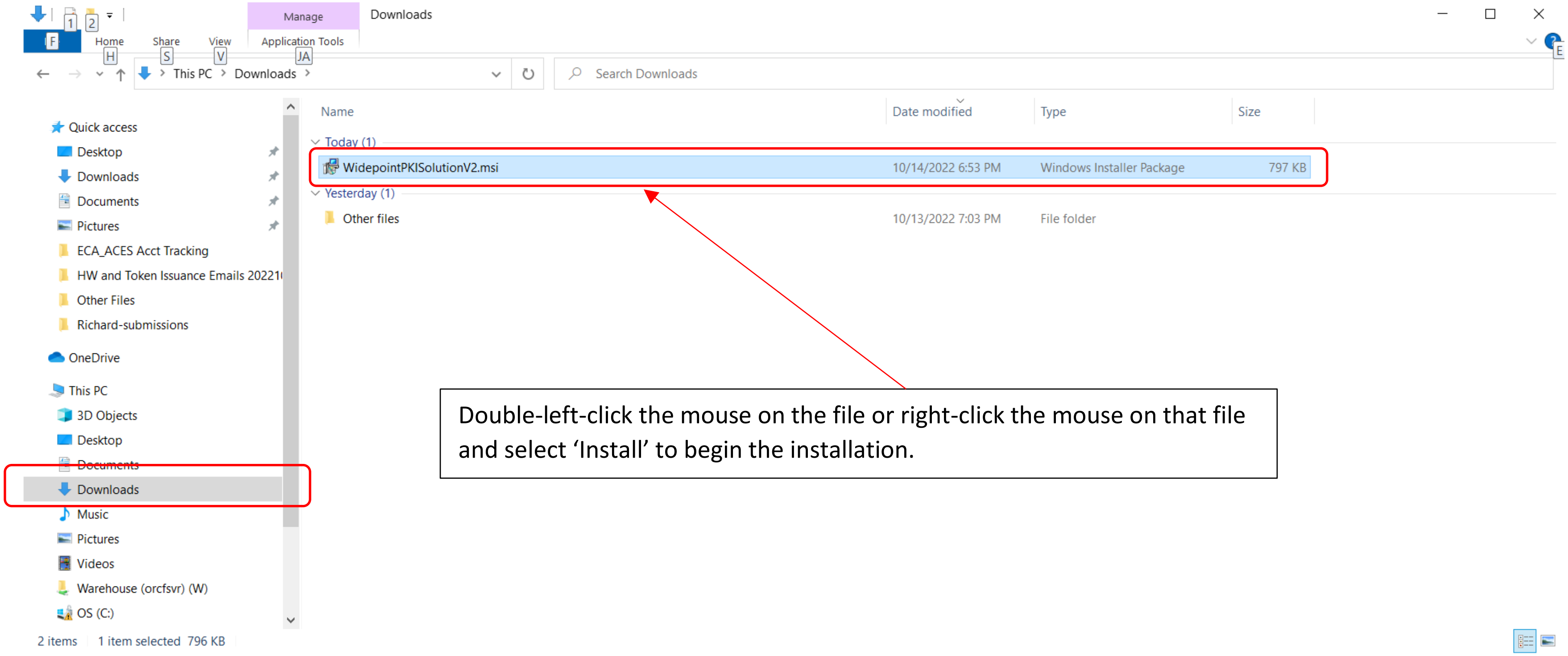
8. You should get the following screen. Select the Download App Button.


Download (Widepoint PKISolutic
https://certificateenroll.orc.com/enroll/sub/downloadApp
Not syncing
ORC
a widepoint company
ECA
External Certificate Authority
Home
Test Certificate
New Certificate Request
Download App
Help
User Info

Download WidePoint PKISolution Windows App

If you have made request for the certificates that need Smart Card to use to secure private key then only you need this app otherwise you don't need this app and all functionality is achieved using browser.

9. You should get an msi file to download. Either open it up on that same screen (if it is located in the upper right-hand corner of your screen) or go to your Downloads Folder to open the file. Please note that if you are using Edge as your browser that you may need to do workaround instructions to get it to download because of Microsoft Defender Software. Your IT Department should be able to assist you with that workaround.

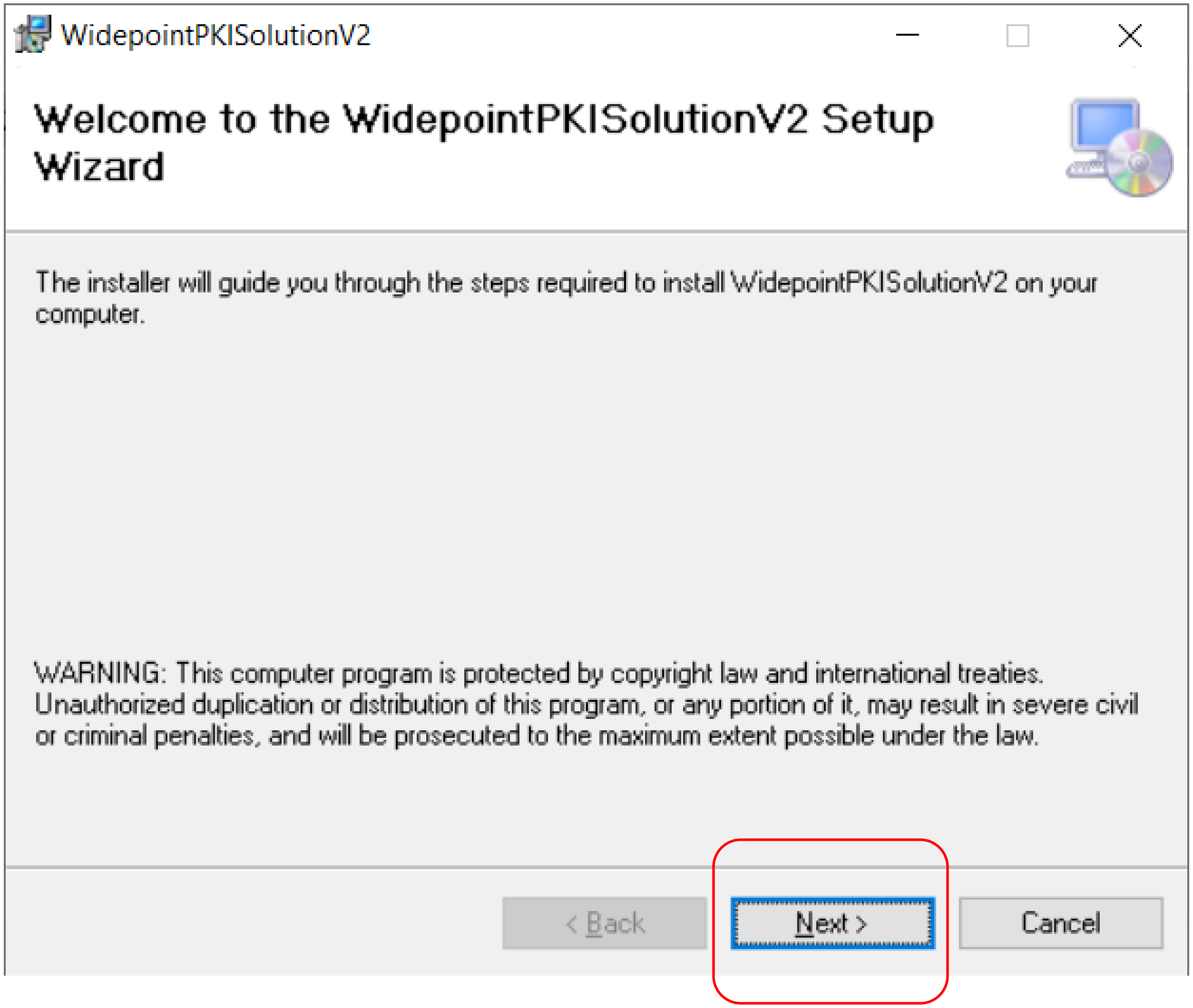


Name	Date modified	Type	Size
Today (1)			
WidepointPKISolutionV2.msi	10/14/2022 6:53 PM	Windows Installer Package	797 KB
Yesterday (1)			
Other files	10/13/2022 7:03 PM	File folder	

2 items 1 item selected 796 KB

Double-left-click the mouse on the file or right-click the mouse on that file and select ‘Install’ to begin the installation.

10. Begin the Installation of the WidePoint Proprietary App.



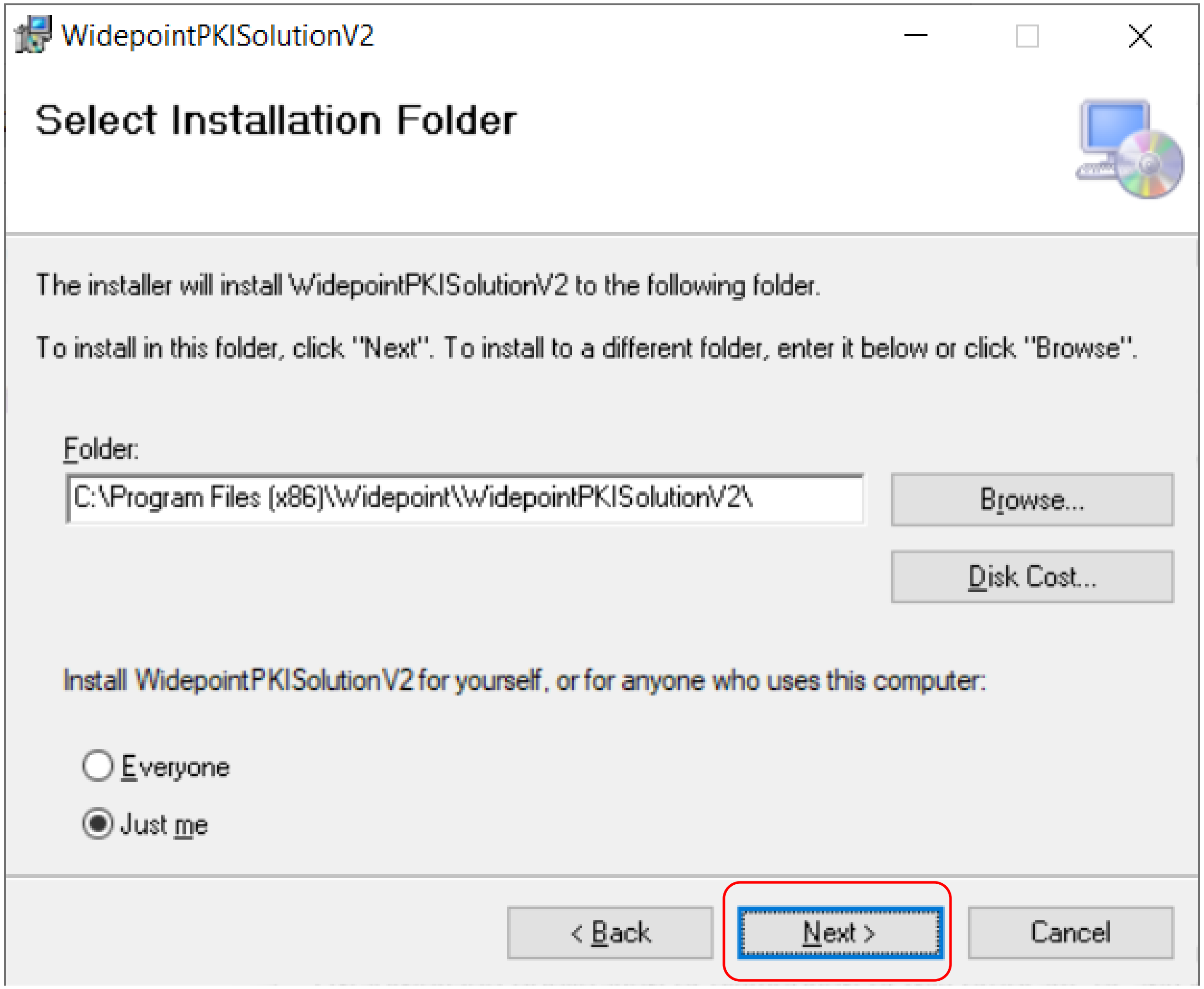
WidepointPKISolutionV2

Welcome to the WidepointPKISolutionV2 Setup Wizard

The installer will guide you through the steps required to install WidepointPKISolutionV2 on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

11. Leave the default settings unless you want to install it in a different location. Remember the folder and location below.



WidepointPKISolutionV2

Select Installation Folder

The installer will install WidepointPKISolutionV2 to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

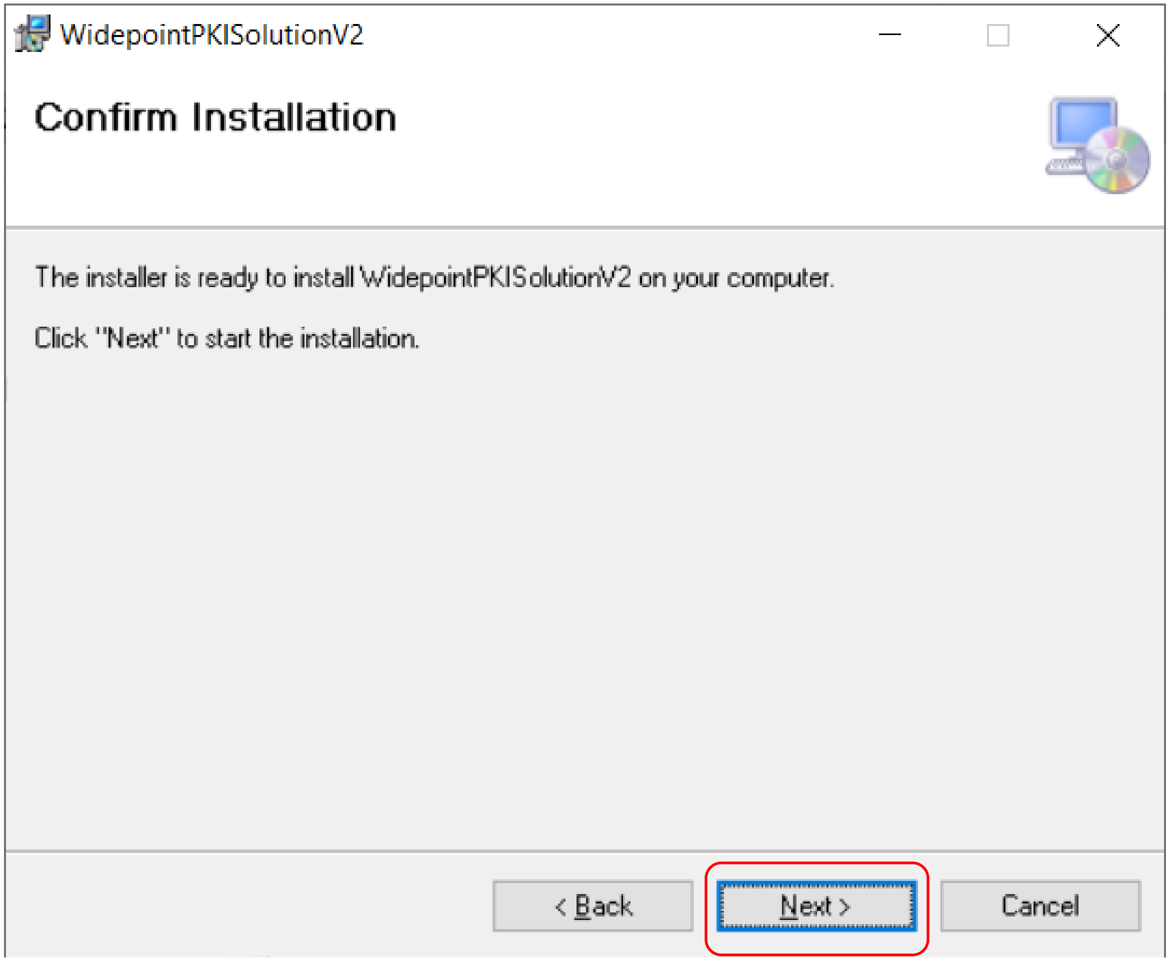
Folder: C:\Program Files (x86)\Widepoint\WidepointPKISolutionV2\

Install WidepointPKISolutionV2 for yourself, or for anyone who uses this computer:

○ Everyone

● Just me

12. Click the Next Button to begin the installation.



WidepointPKISolutionV2

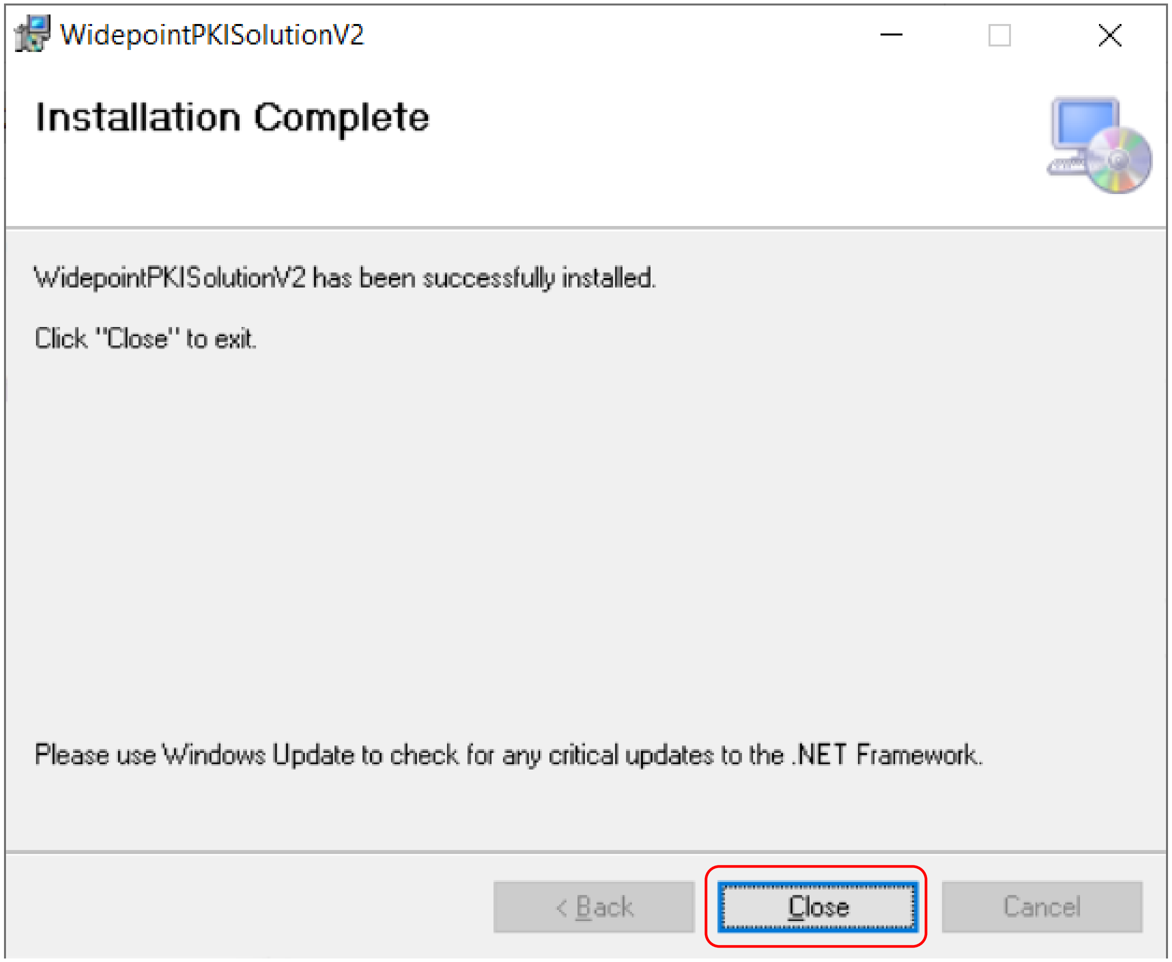
Confirm Installation

The installer is ready to install WidepointPKISolutionV2 on your computer.

Click "Next" to start the installation.

13. If you get prompted for a permissions screen, click YES or CONTINUE after checking with your IT Department.

14. Click the Close Button after your computer has installed the App.



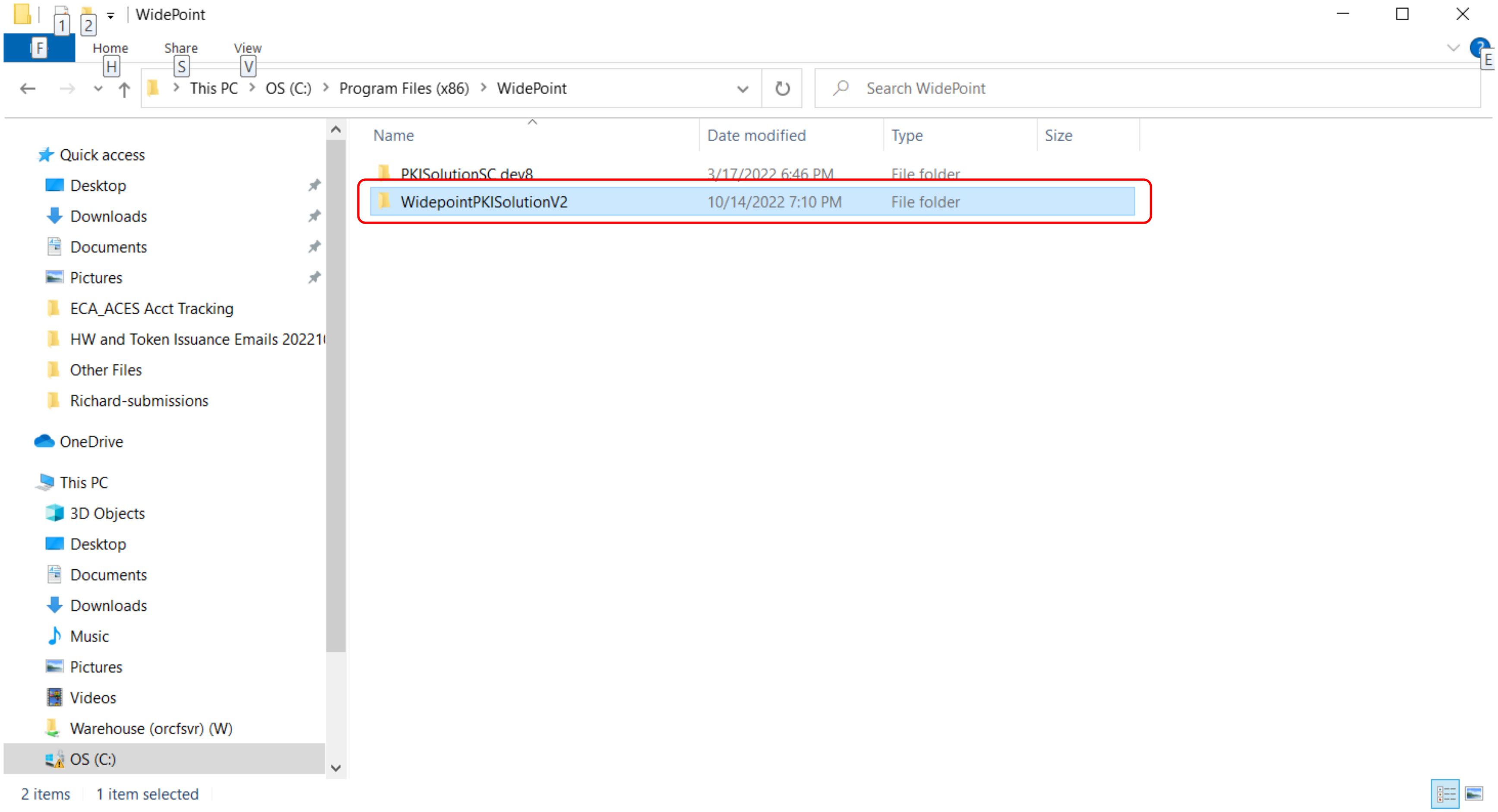
Installation Complete

WidepointPKISolutionV2 has been successfully installed.

Click "Close" to exit.

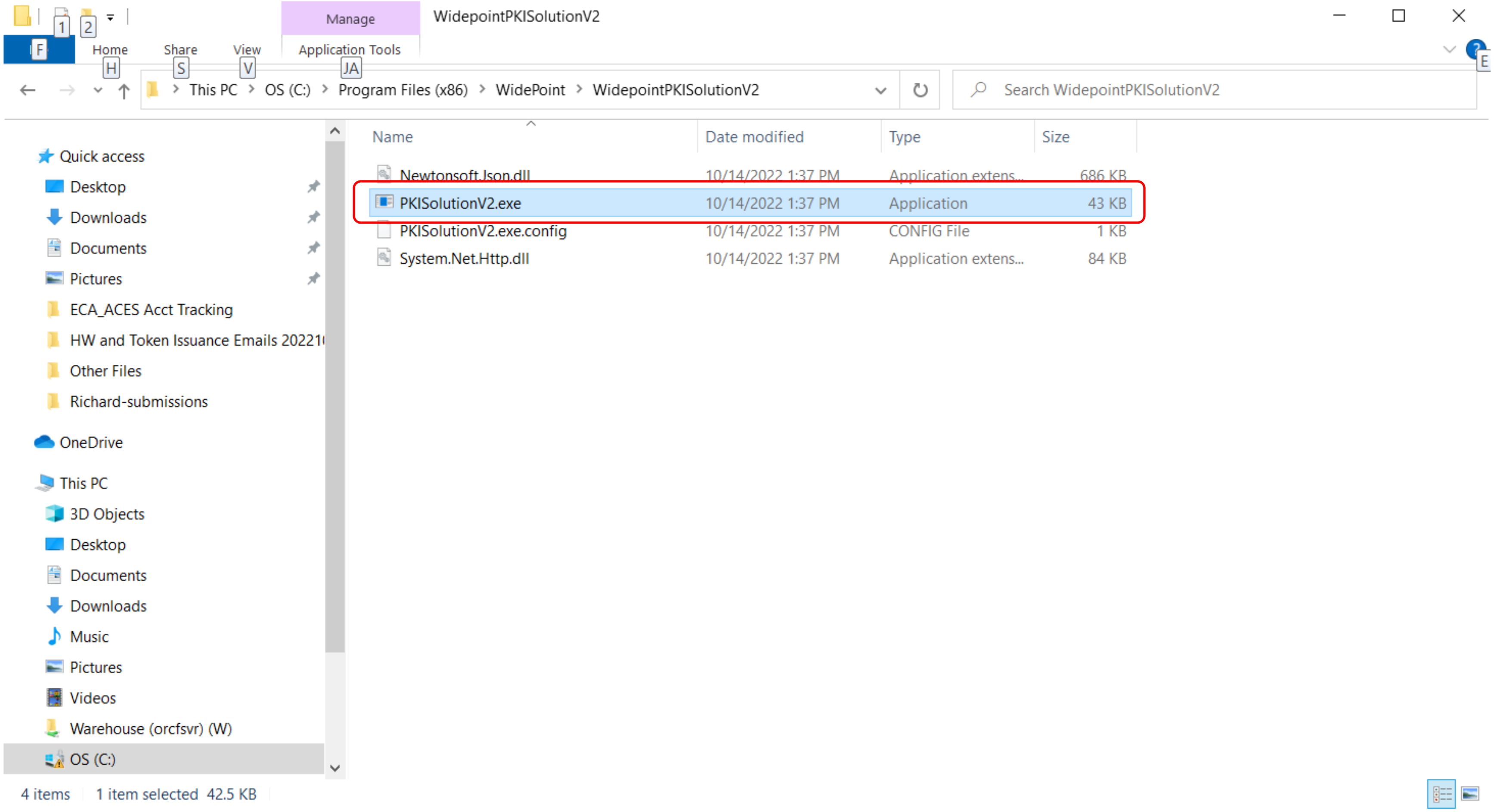
Please use Windows Update to check for any critical updates to the .NET Framework.

15. Go to the location where you sent the App in Step# 11. Open the WidePointPKISolutionV2 Folder.



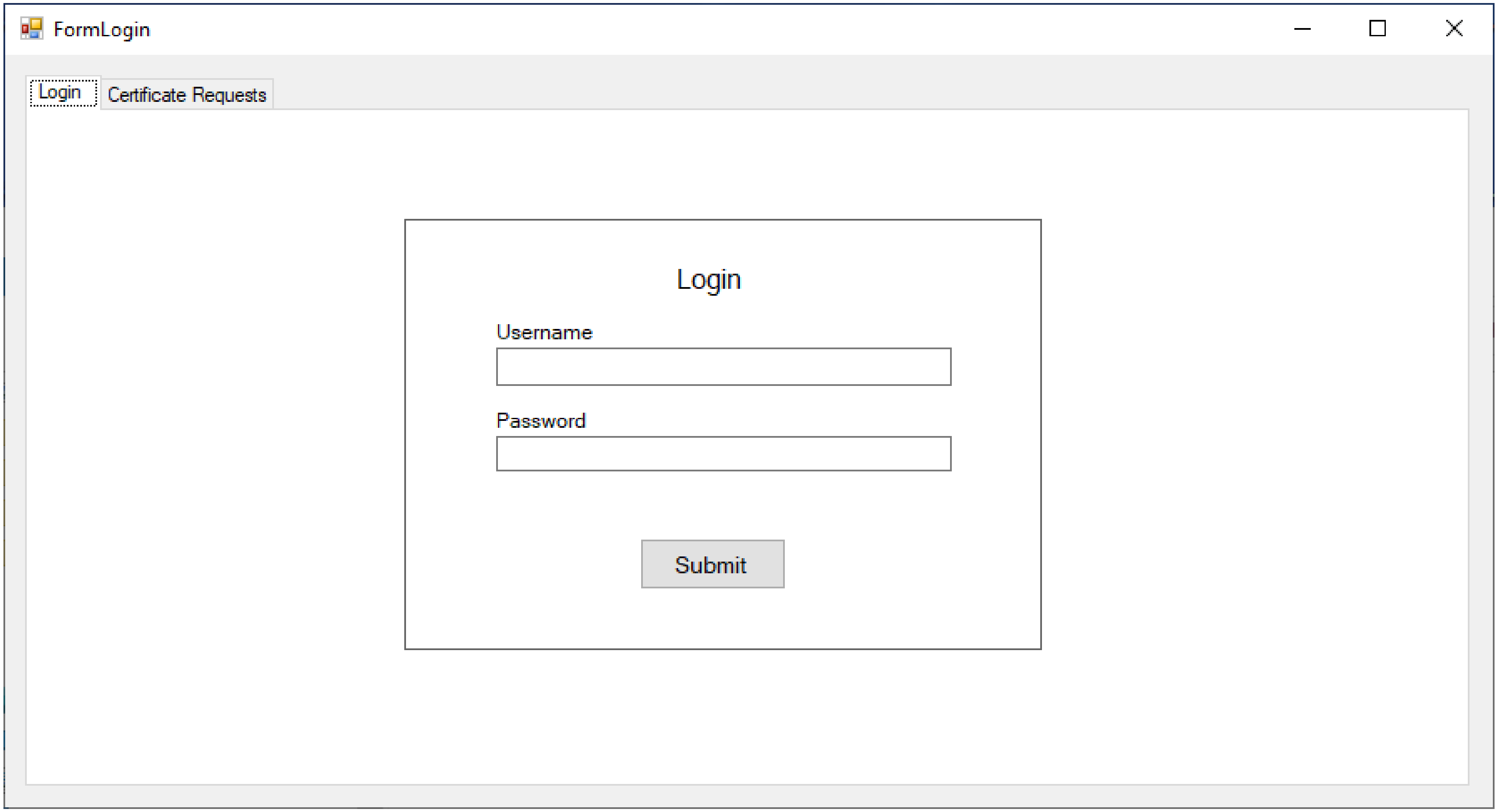
Name	Date modified	Type	Size
PKISolutionSC dev8	3/17/2022 6:46 PM	File folder	
WidepointPKISolutionV2	10/14/2022 7:10 PM	File folder	

16. Open the PKISolutionV2.exe file (it will be of file type ‘Application’).

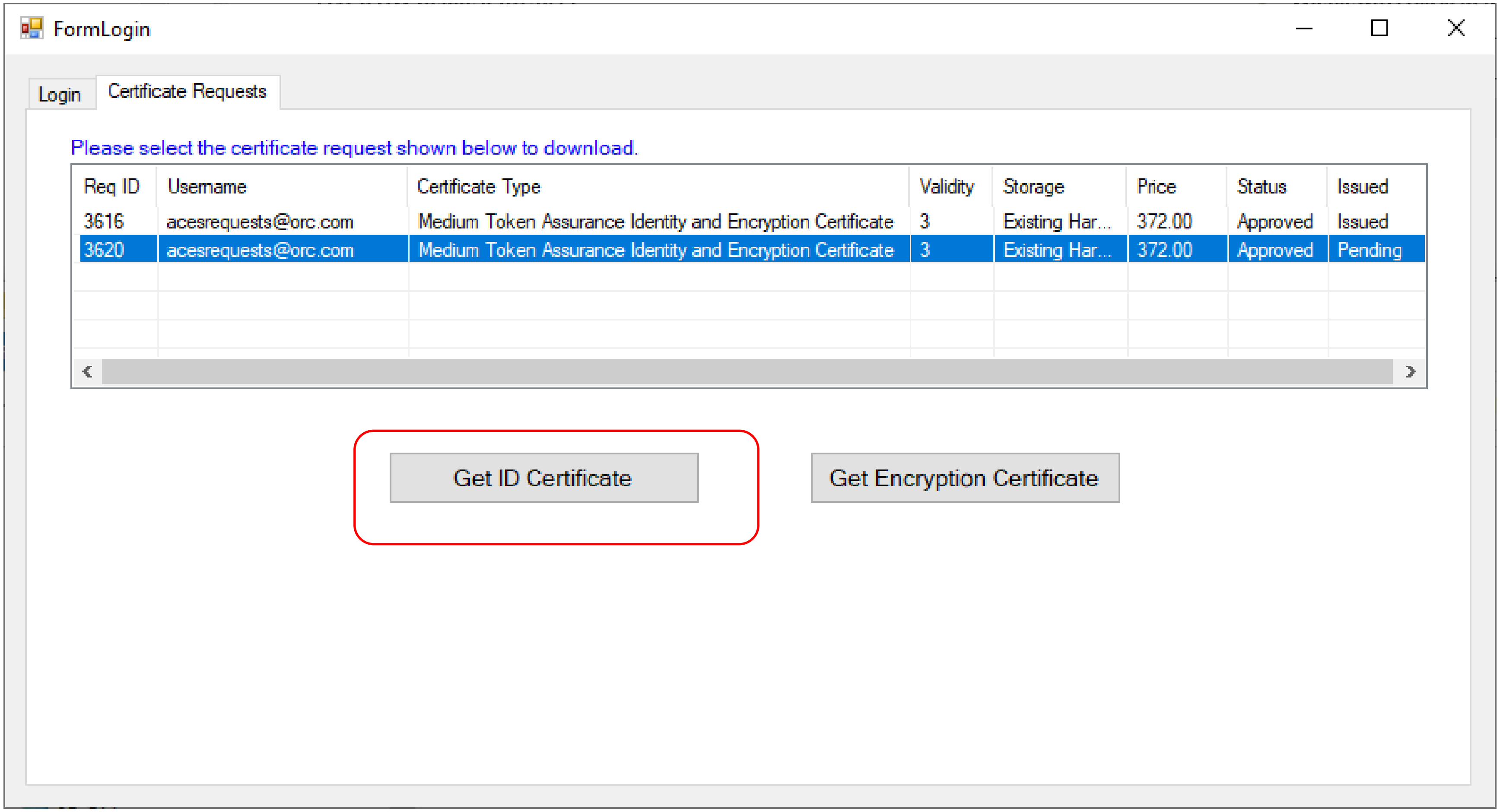


Name	Date modified	Type	Size
Newtonsoft.Json.dll	10/14/2022 1:37 PM	Application extens...	686 KB
PKISolutionV2.exe	10/14/2022 1:37 PM	Application	43 KB
PKISolutionV2.exe.config	10/14/2022 1:37 PM	CONFIG File	1 KB
System.Net.Http.dll	10/14/2022 1:37 PM	Application extens...	84 KB

17. The screen will open to prompt you for your Username and Password for your ECA 8 Account; go ahead and provide that Username and Password. Make sure that you have your smartcard or cryptotoken still inserted (you should probably login to the smartcard ahead of time via the ActivClient User Console).



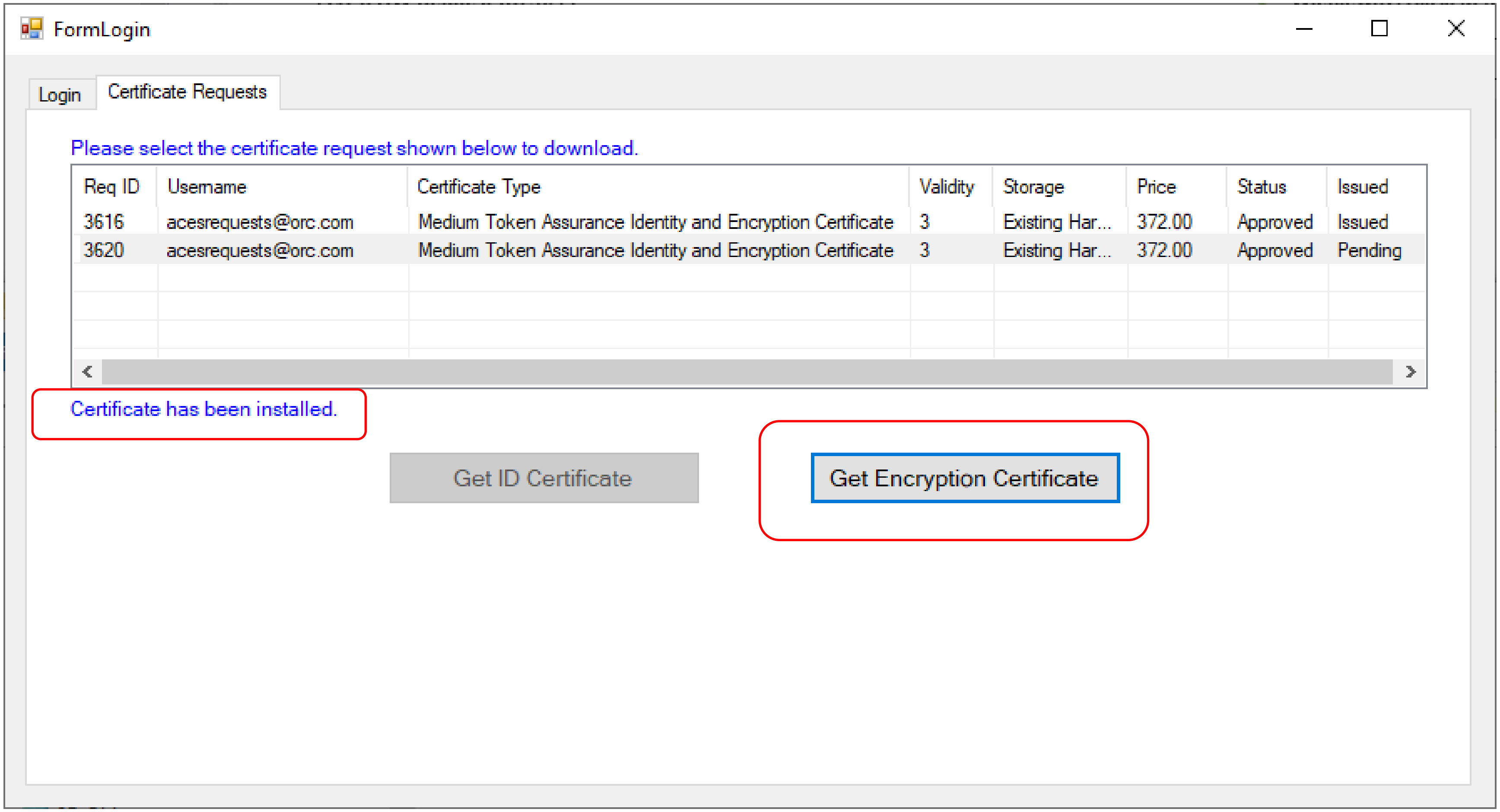
18. Highlight the request to download; it should have Approved under the Status Column and Pending under the Issued Column. Then click on the 'Get ID Certificate' Button. Be patient; it can take 2 to 3 minutes to complete the download of each certificate.



Please select the certificate request shown below to download.

Req ID	Username	Certificate Type	Validity	Storage	Price	Status	Issued
3616	acesrequests@orc.com	Medium Token Assurance Identity and Encryption Certificate	3	Existing Har...	372.00	Approved	Issued
3620	acesrequests@orc.com	Medium Token Assurance Identity and Encryption Certificate	3	Existing Har...	372.00	Approved	Pending

19. You should get the following screen that says your 'Certificate (ID) has been installed.' Highlight your request line again and click the 'Get Encryption Certificate.'

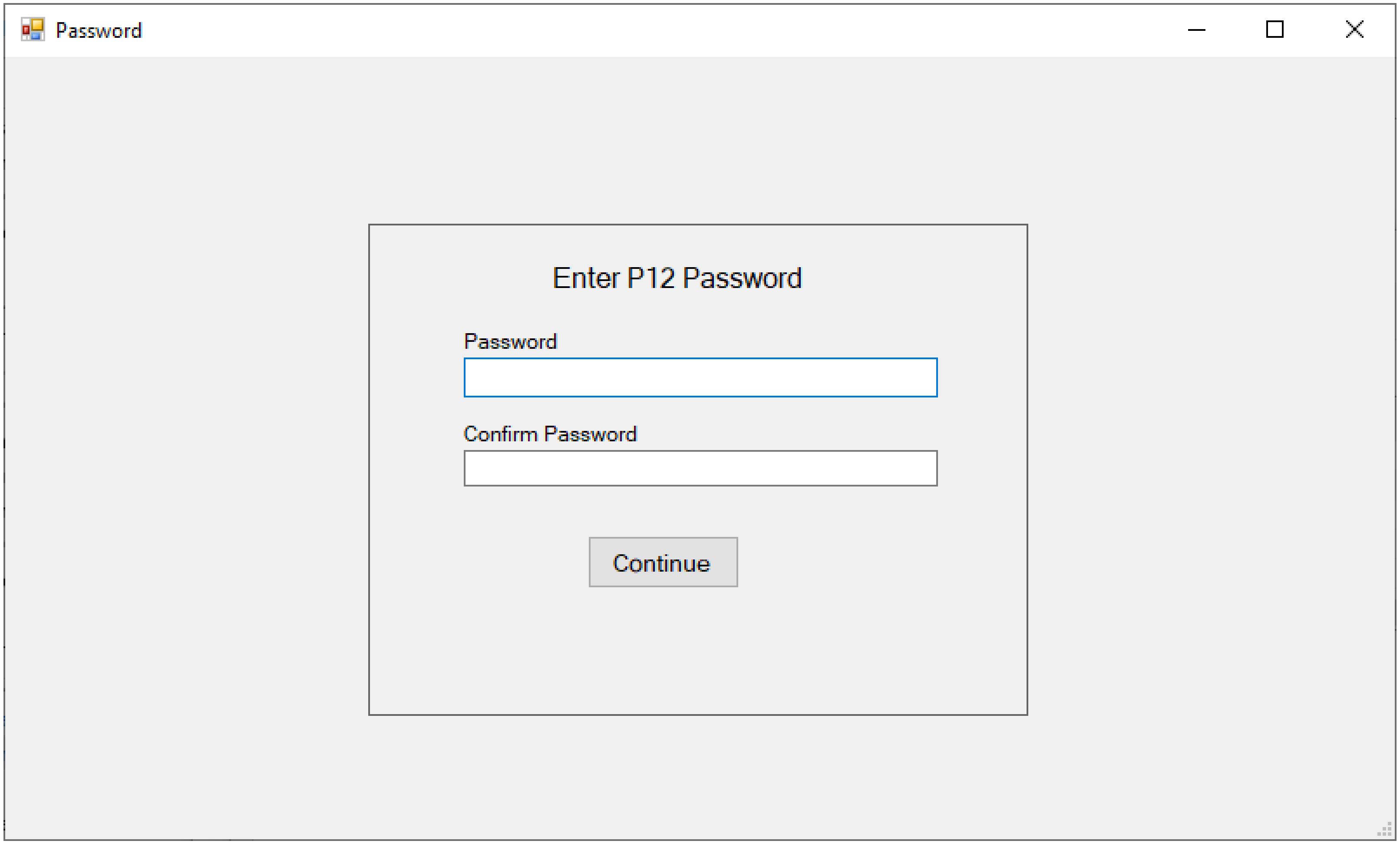


Please select the certificate request shown below to download.

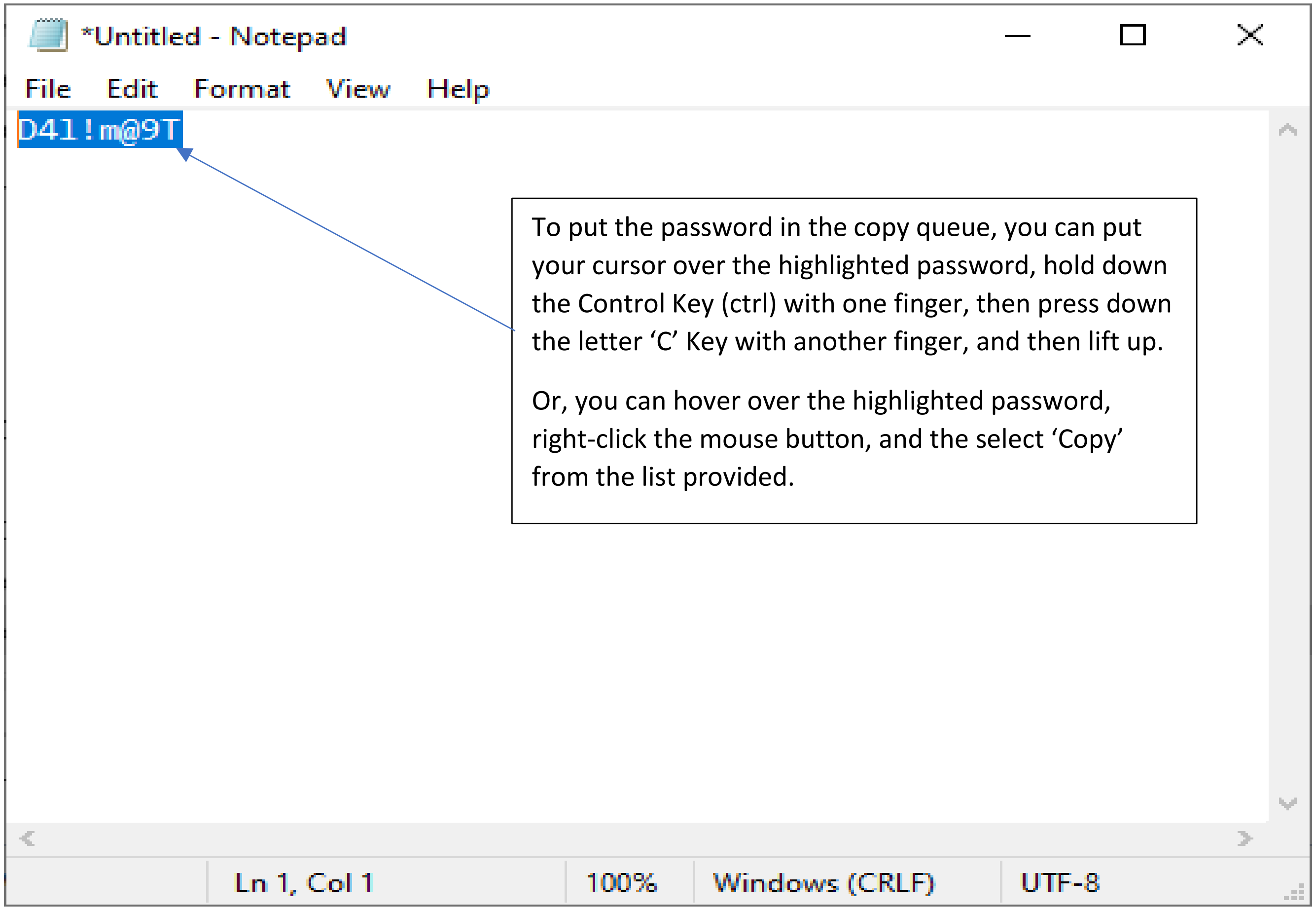
Req ID	Username	Certificate Type	Validity	Storage	Price	Status	Issued
3616	acesrequests@orc.com	Medium Token Assurance Identity and Encryption Certificate	3	Existing Har...	372.00	Approved	Issued
3620	acesrequests@orc.com	Medium Token Assurance Identity and Encryption Certificate	3	Existing Har...	372.00	Approved	Pending

Certificate has been installed.

20. You should get the following Password Screen that will prompt you to create and set a password for a software version (.p12 file) of your encryption certificate that you will have to import onto your smartcard/cryptotoken.



21. Create your password. It is best to open up a blank Notepad File (every PC has Notepad; search for it in the Search Box next to your Windows Start Button); type that password into the Notepad File; highlight it; put it in the copy queue. The reason to use Notepad is that it has no formatting so that it clearly distinguishes between all characters.

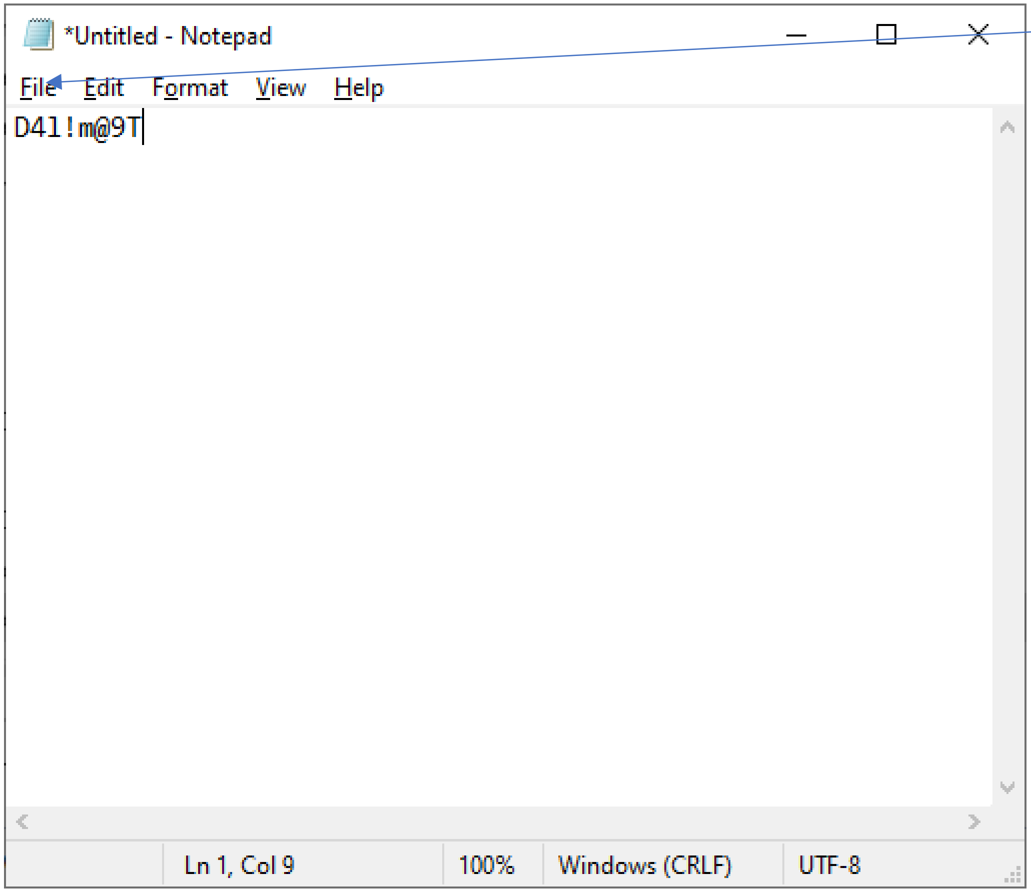


```
D41!m@9T
```

To put the password in the copy queue, you can put your cursor over the highlighted password, hold down the Control Key (ctrl) with one finger, then press down the letter ‘C’ Key with another finger, and then lift up.

Or, you can hover over the highlighted password, right-click the mouse button, and the select ‘Copy’ from the list provided.

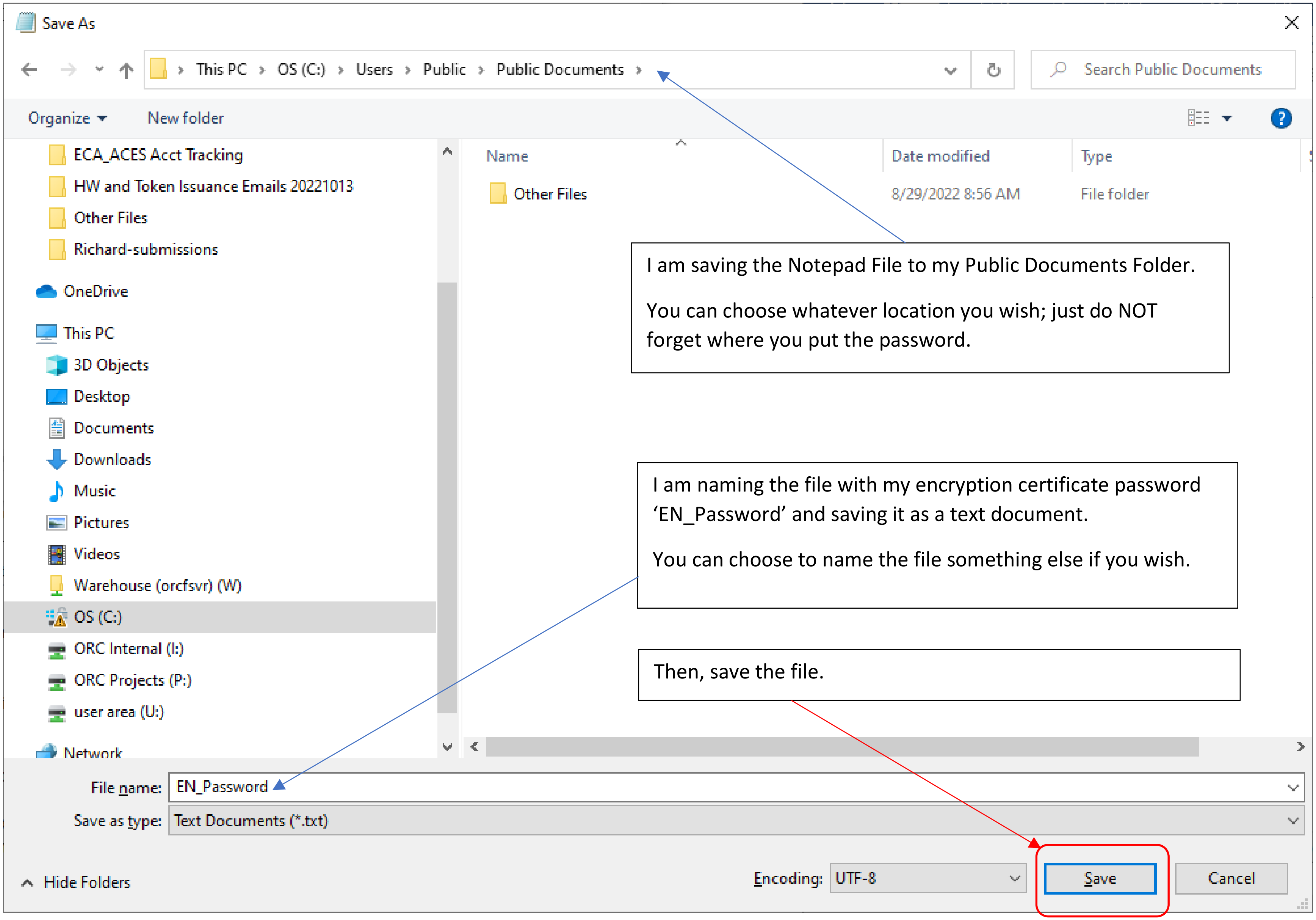
22. Next, you need to make sure that you save a copy of this password somewhere. You can paste it into a Password Manager File; you can carefully write it down on a piece of paper and then lock it up in a secure location; or you can save the Notepad File somewhere. In my example here, I am going to save the Notepad File to my Public Documents Folder for ease of use later and call the file EN_Password.



D41!m@9T

Click on ‘File’ and then select Save As . . .’

Continue the procedure to the next screen . . .



File name: EN_Password

Save as type: Text Documents (*.txt)

Encoding: UTF-8

I am saving the Notepad File to my Public Documents Folder.

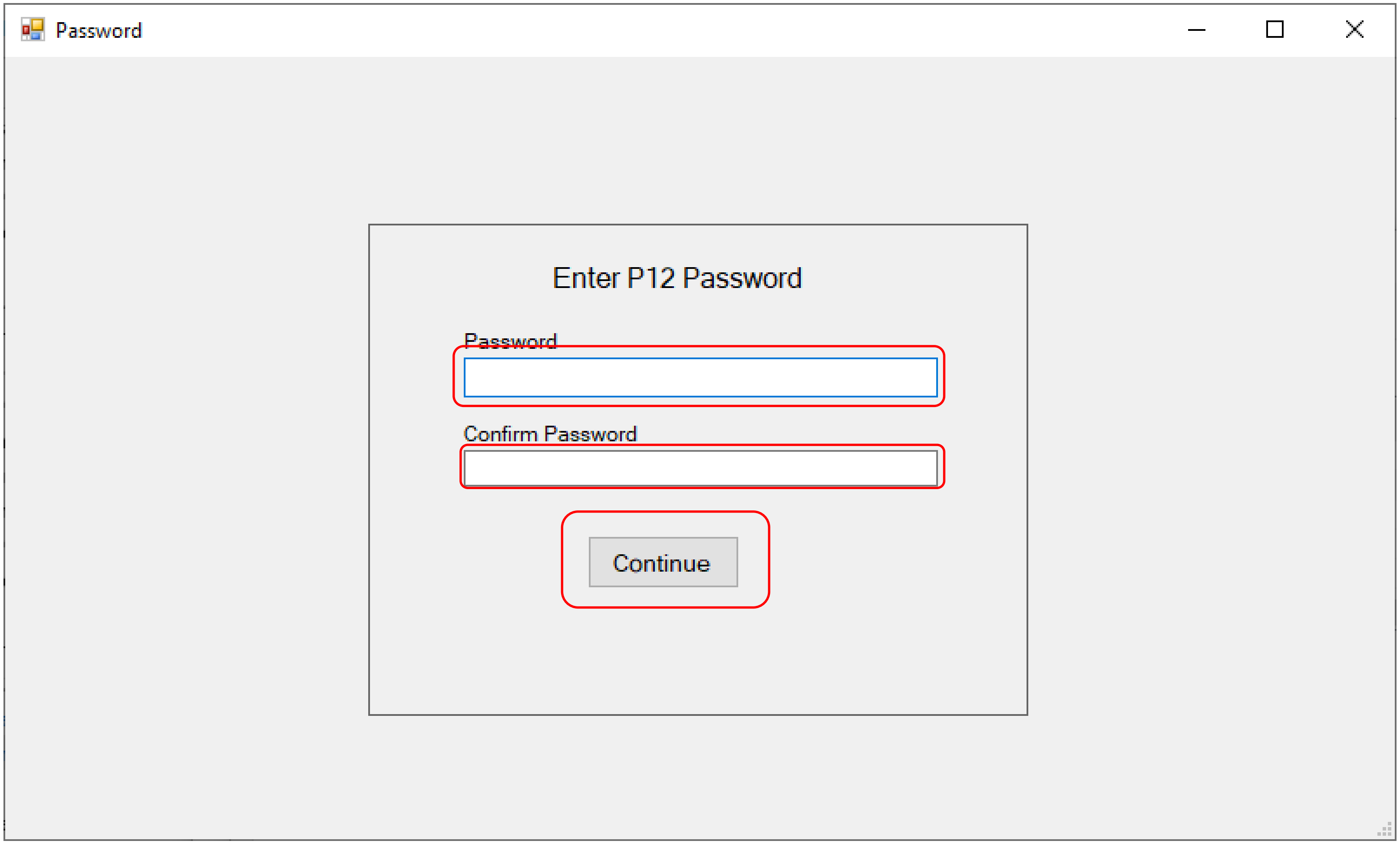
You can choose whatever location you wish; just do NOT forget where you put the password.

I am naming the file with my encryption certificate password ‘EN_Password’ and saving it as a text document.

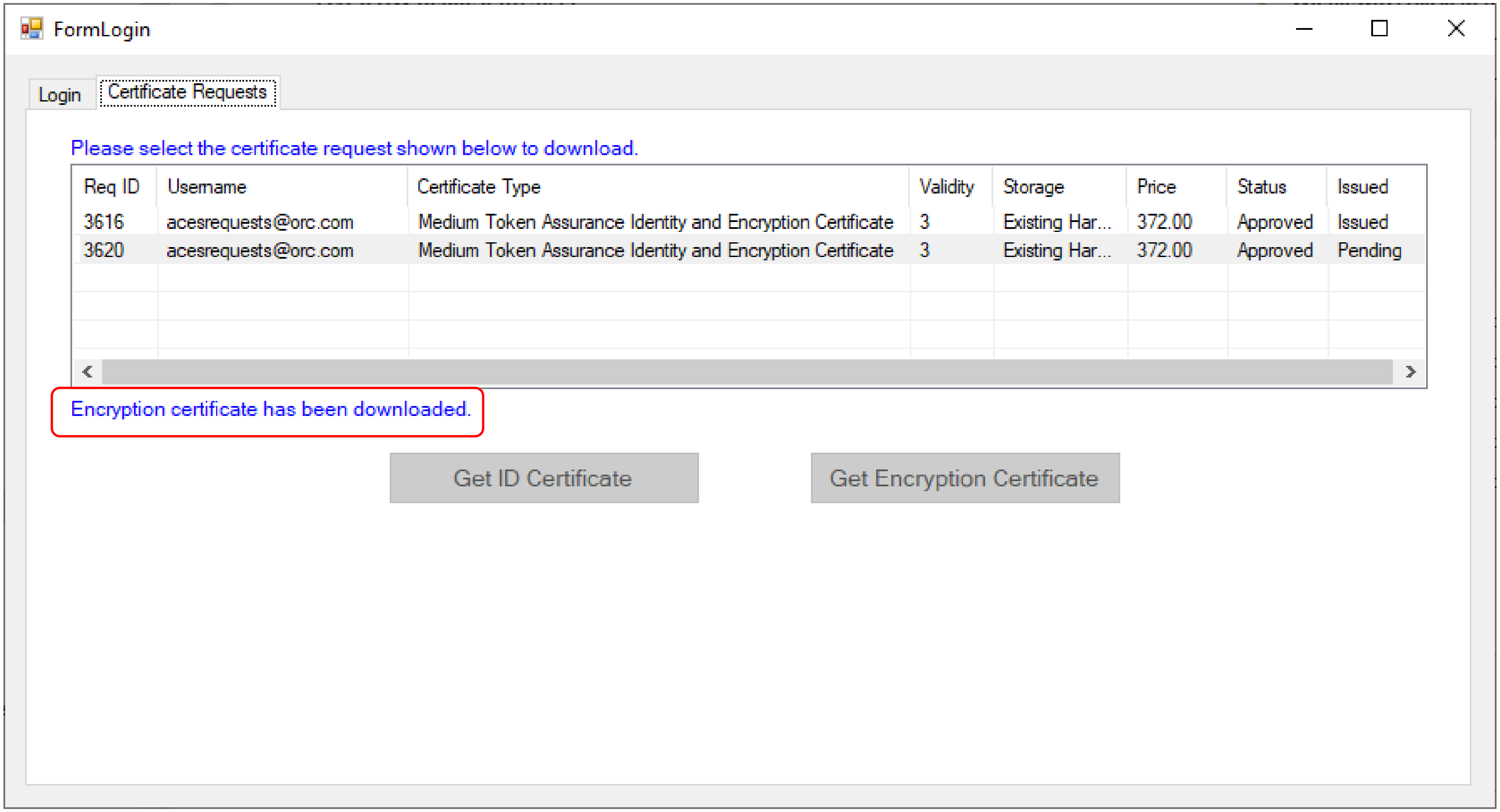
You can choose to name the file something else if you wish.

Then, save the file.

23. Now, go back to the ‘Enter P12 Password’ Prompt Screen from Step# 20 for the downloading of your Encryption Certificate to paste your password into the two boxes and select the Continue Button.



24. You should get the following screen notifying you that your Encryption Certificate has been downloaded (it will be in your Public Documents Folder; the same location where you put the password text file for that certificate, which is C: - Users – Public – Public Documents). Again, it may take a couple of minutes to download, so please be patient waiting for the screen below.

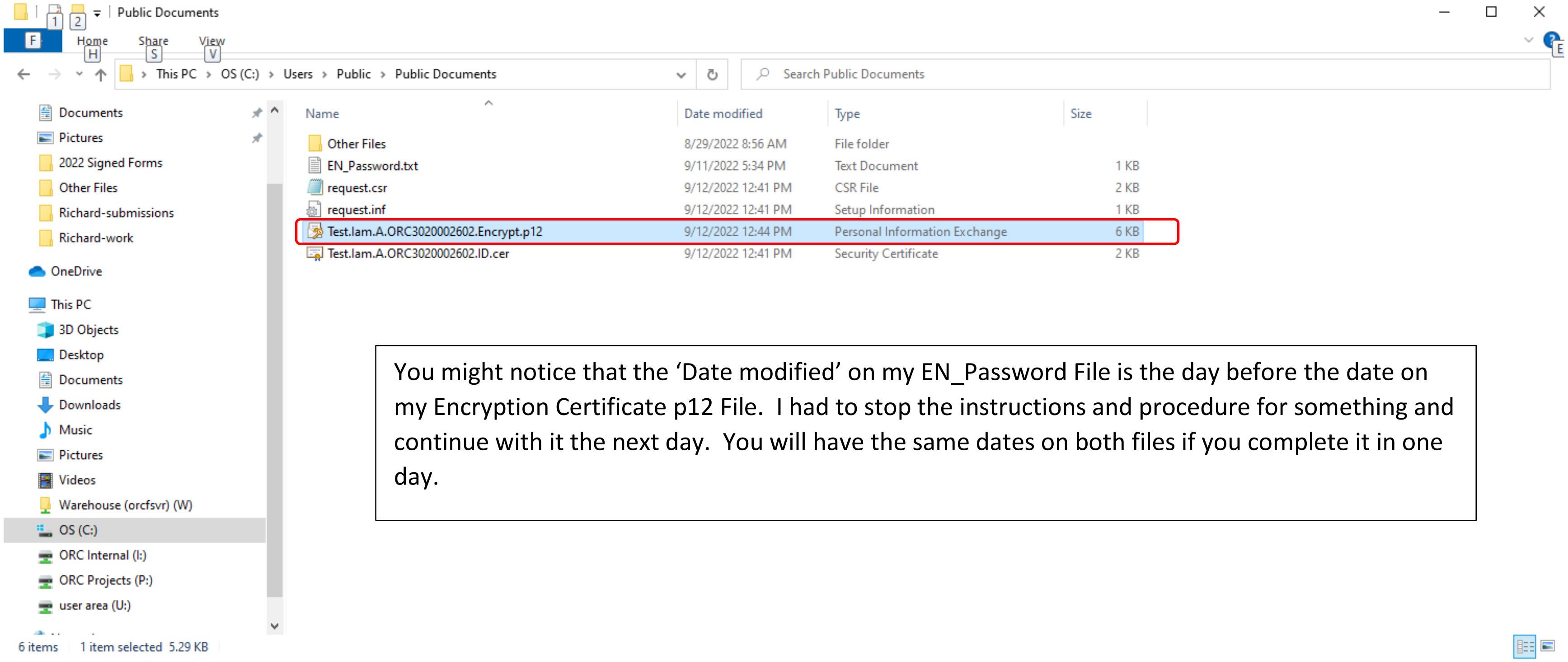


Please select the certificate request shown below to download.

Req ID	Username	Certificate Type	Validity	Storage	Price	Status	Issued
3616	acesrequests@orc.com	Medium Token Assurance Identity and Encryption Certificate	3	Existing Har...	372.00	Approved	Issued
3620	acesrequests@orc.com	Medium Token Assurance Identity and Encryption Certificate	3	Existing Har...	372.00	Approved	Pending

Encryption certificate has been downloaded.

25. Next, check for your encryption certificate (it will be of file type Personal Information Exchange) in that Public Documents Folder (C: - Users – Public – Public Documents).

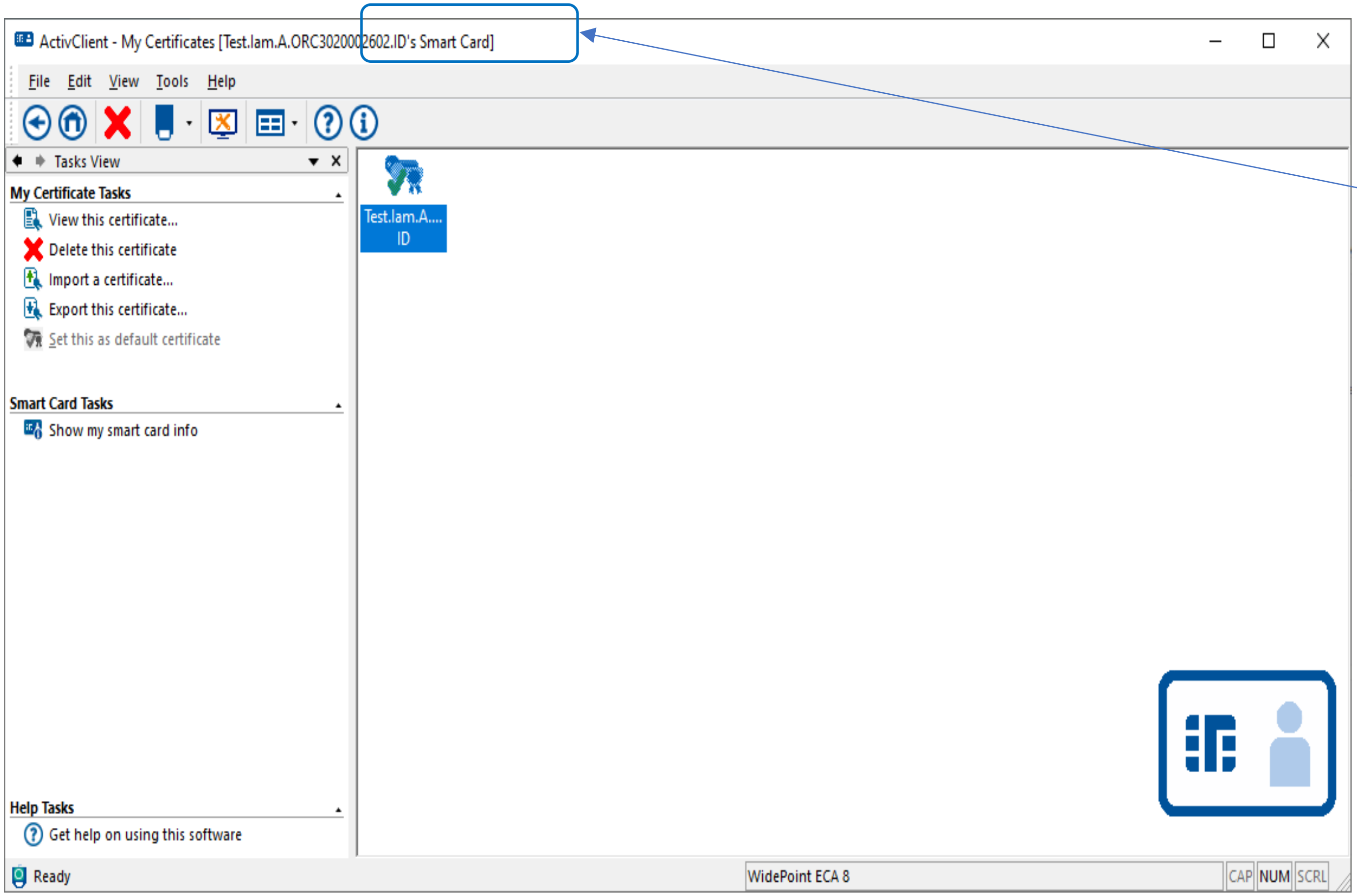


Name	Date modified	Type	Size
Other Files	8/29/2022 8:56 AM	File folder	
EN_Password.txt	9/11/2022 5:34 PM	Text Document	1 KB
request.csr	9/12/2022 12:41 PM	CSR File	2 KB
request.inf	9/12/2022 12:41 PM	Setup Information	1 KB
Test.Iam.A.ORC3020002602.Encrypt.p12	9/12/2022 12:44 PM	Personal Information Exchange	6 KB
Test.Iam.A.ORC3020002602.ID.cer	9/12/2022 12:41 PM	Security Certificate	2 KB

6 items 1 item selected 5.29 KB

You might notice that the 'Date modified' on my EN_Password File is the day before the date on my Encryption Certificate p12 File. I had to stop the instructions and procedure for something and continue with it the next day. You will have the same dates on both files if you complete it in one day.

26. Then, check for your Identity Certificate in the My Certificates Folder in the ActivClient Software User Console by disconnecting your smartcard/cryptotoken from the computer and re-connecting it. Then, log back into your smartcard/cryptotoken.

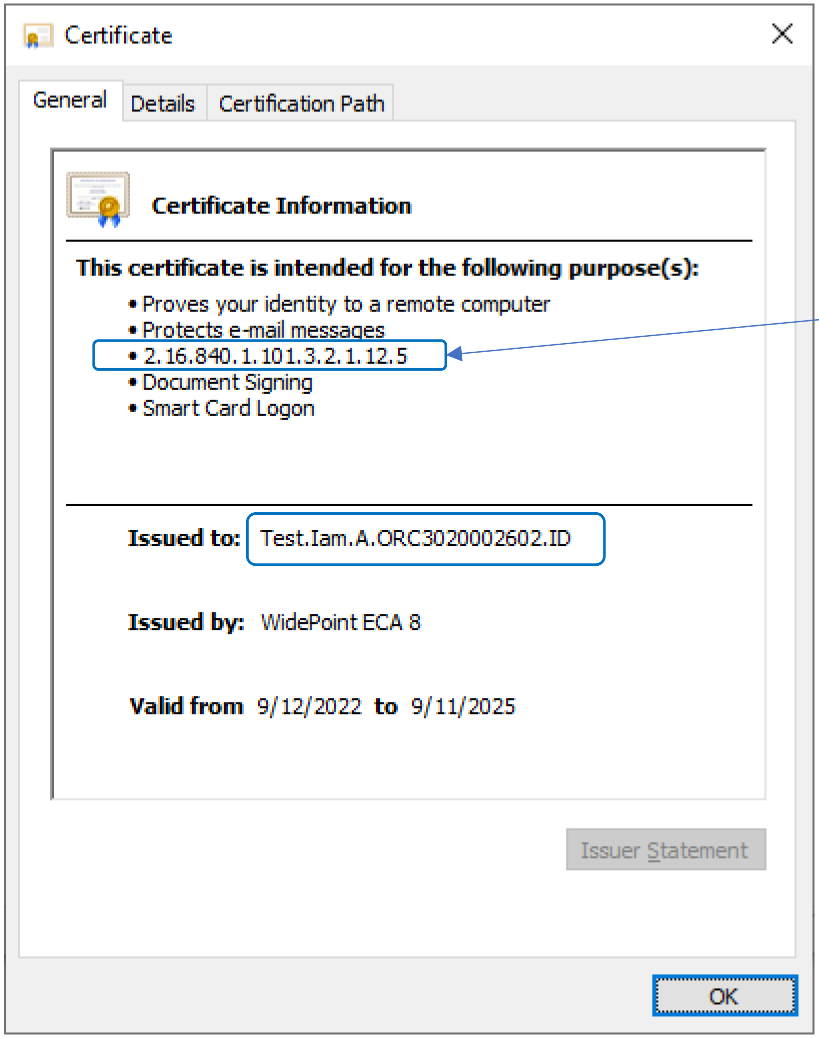


ActivClient - My Certificates [Test.Iam.A.ORC3020002602.ID's Smart Card]

Please note that the header for the ActivClient User Console Screen has changed; it now says Smart Card instead of Activkey_Sim 0 because we changed the device from a USB Token to a smartcard to show the difference in the header section.

<u>YOU WILL NOT CHANGE THE DEVICE DURING THE DOWNLOAD PROCESS!!!!</u>

27. Open up the Identity Certificate to verify the information on it by right-clicking the mouse on it and then left-click ‘View this certificate.’ Click the OK Button when you are finished.



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Protects e-mail messages
- 2.16.840.1.101.3.2.1.12.5
- Document Signing
- Smart Card Logon

Issued to: Test.Iam.A.ORC3020002602.ID

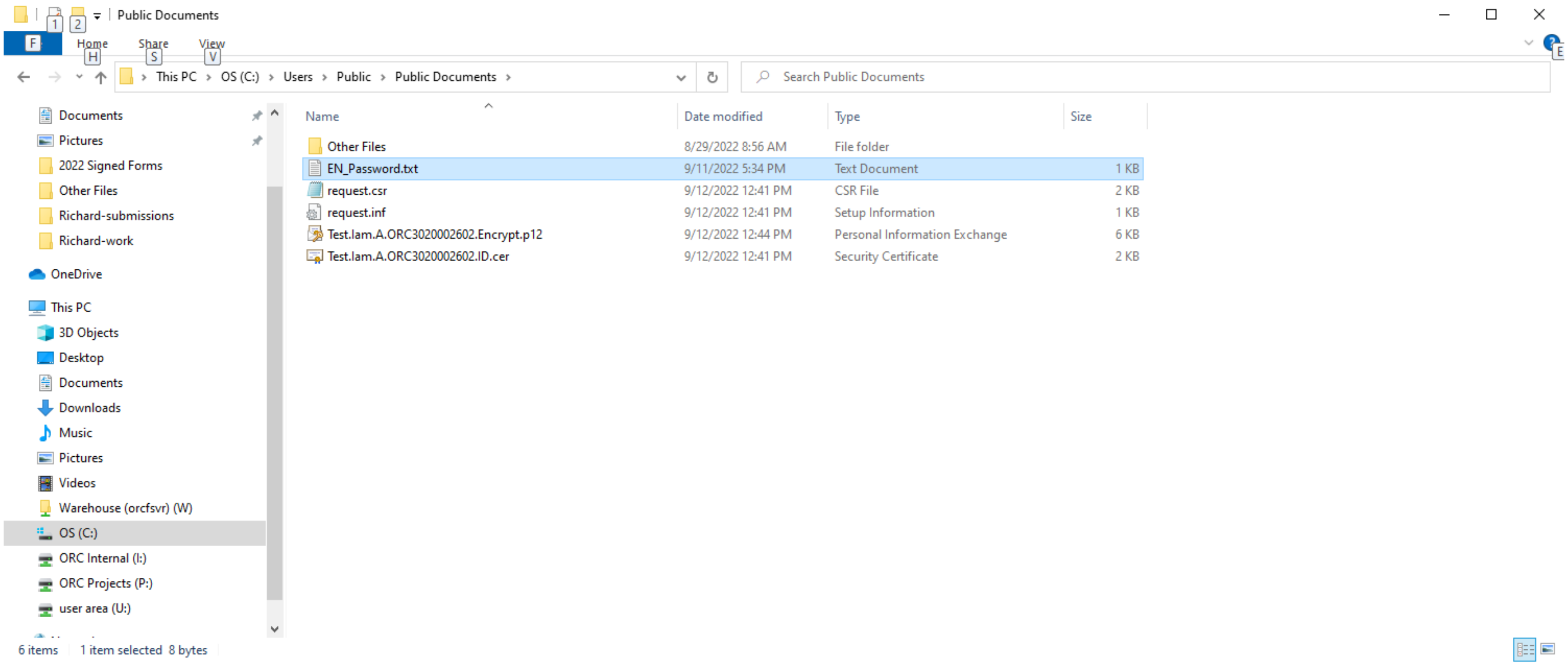
Issued by: WidePoint ECA 8

Valid from 9/12/2022 **to** 9/11/2025

If you got an ECA Medium Token Assurance Identity Certificate, then the certificate policy number will end in a ‘5.’

If you got an ECA Medium Hardware Assurance Identity Certificate, then the certificate policy number will end in a ‘10.’

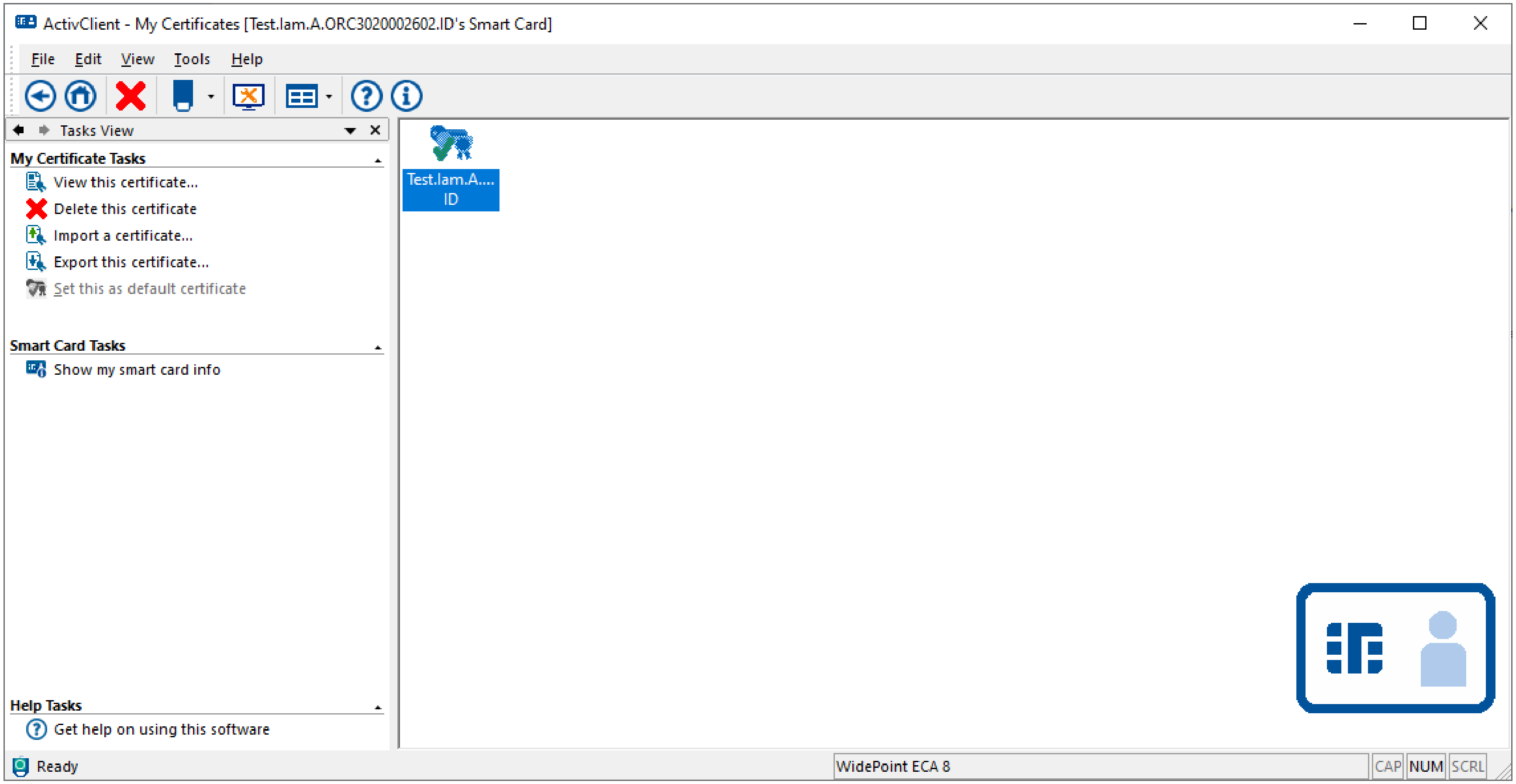
28. Now, import your encryption certificate onto the smartcard/cryptotoken. Go to your Public Documents Folder (C: - Users – Public – Public Documents), open up the EN_Password File, and copy the password into the copy queue (highlight the password, right-click the mouse button on the highlighted password, and select copy). Or, you can wait for the password prompt later in the process/procedure and carefully type it in.



Name	Date modified	Type	Size
Other Files	8/29/2022 8:56 AM	File folder	
EN_Password.txt	9/11/2022 5:34 PM	Text Document	1 KB
request.csr	9/12/2022 12:41 PM	CSR File	2 KB
request.inf	9/12/2022 12:41 PM	Setup Information	1 KB
Test.Iam.A.ORC3020002602.Encrypt.p12	9/12/2022 12:44 PM	Personal Information Exchange	6 KB
Test.Iam.A.ORC3020002602.ID.cer	9/12/2022 12:41 PM	Security Certificate	2 KB

6 items 1 item selected 8 bytes

29. Go back to the ActivClient Software User Console and open up the My Certificates Folder.



ActivClient - My Certificates [Test.Iam.A.ORC3020002602.ID's Smart Card]

My Certificate Tasks

- View this certificate...
- Delete this certificate
- Import a certificate...
- Export this certificate...
- Set this as default certificate

Smart Card Tasks

- Show my smart card info

Help Tasks

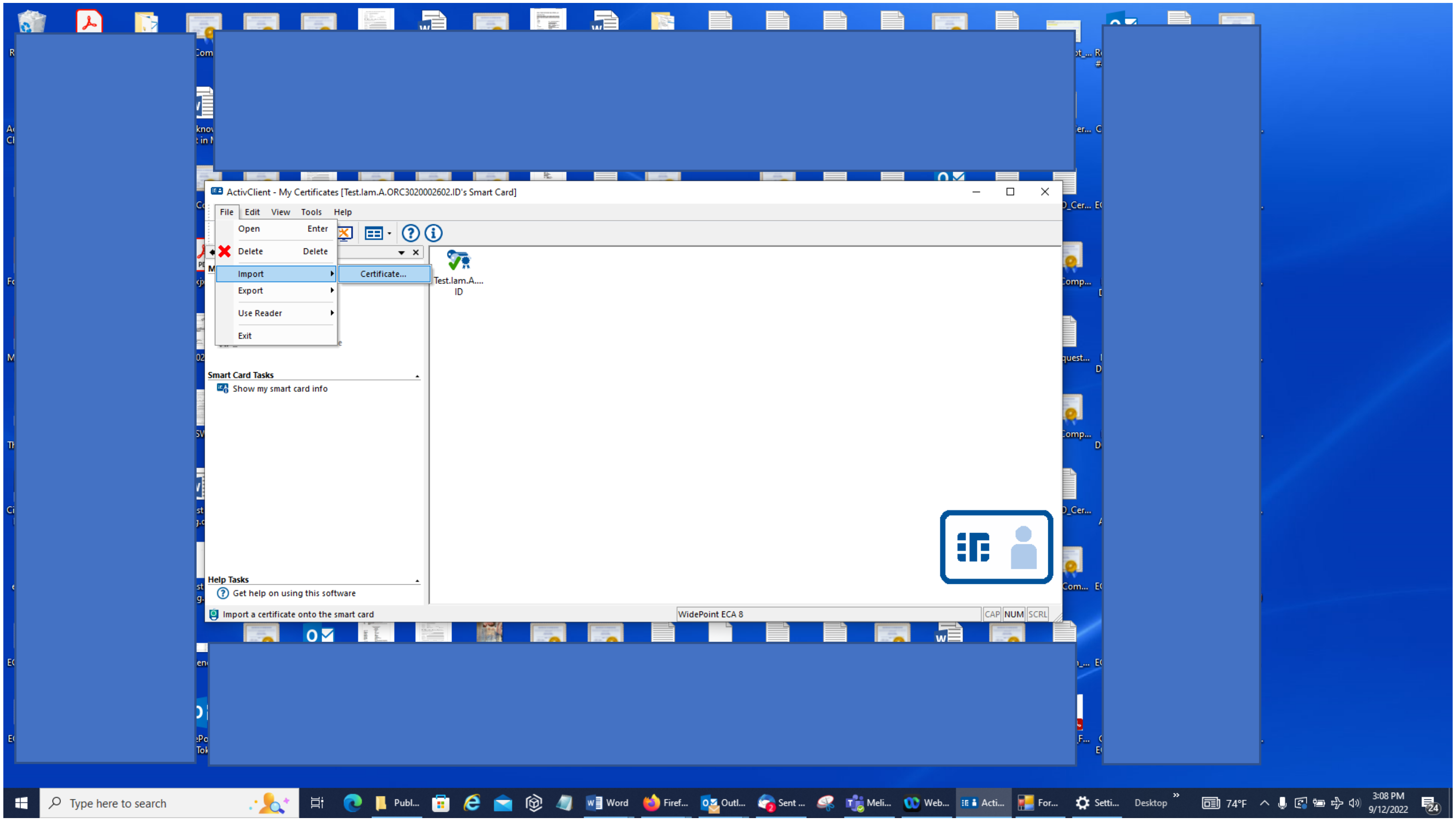
- Get help on using this software

Test.Iam.A.... ID

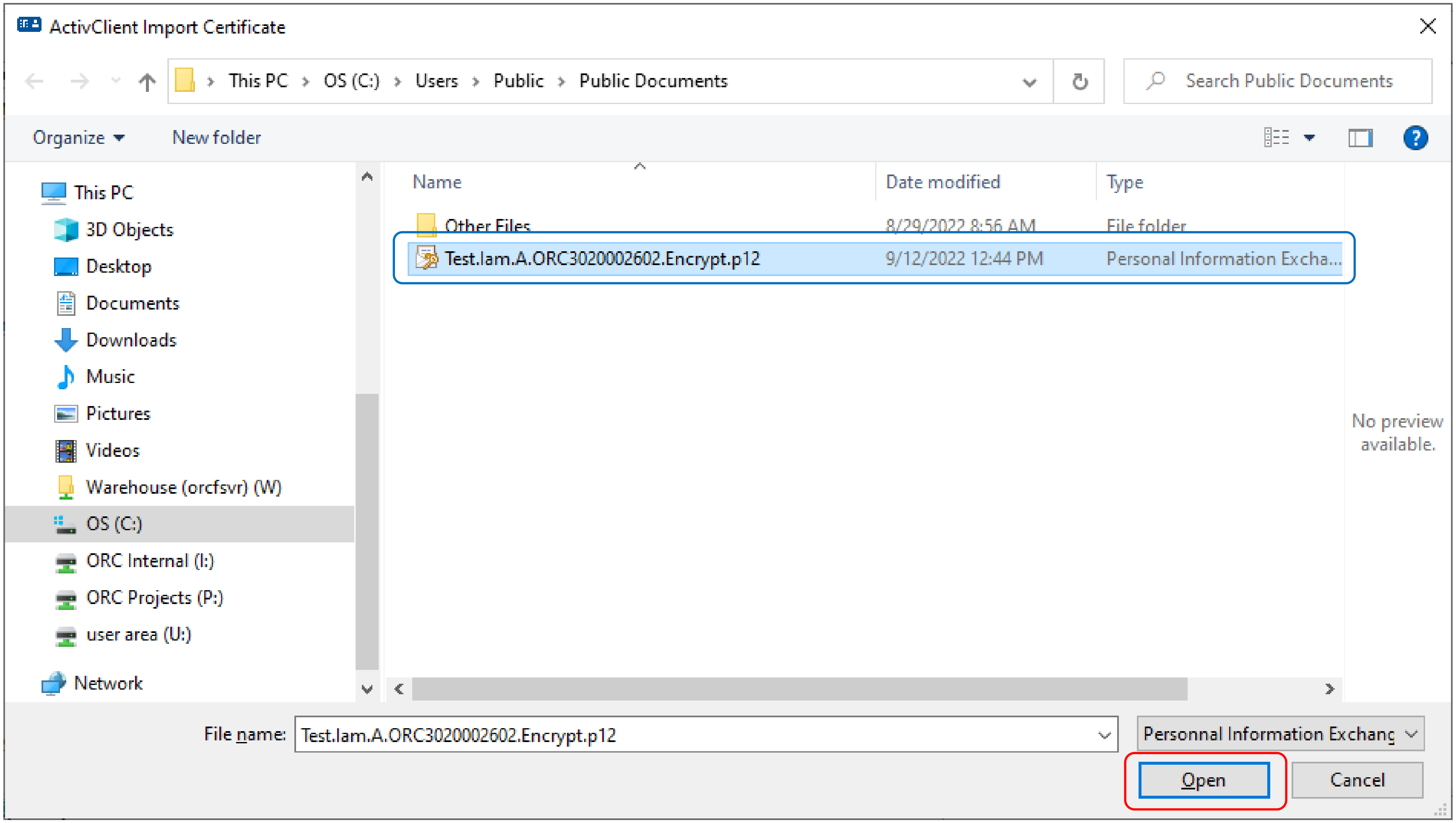
Ready

WidePoint ECA 8

30. Select File in the menu bar, then Import, then Certificate.



31. The computer should go to the Public Documents Folder where your Encryption Certificate is located. Select Open.

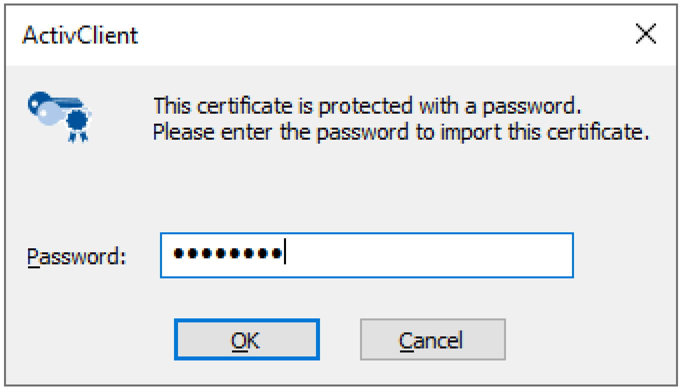


Name	Date modified	Type
Other Files	8/29/2022 8:56 AM	File folder
Test.Iam.A.ORC3020002602.Encrypt.p12	9/12/2022 12:44 PM	Personal Information Excha...

File name: Test.Iam.A.ORC3020002602.Encrypt.p12

Personnal Information Exchang

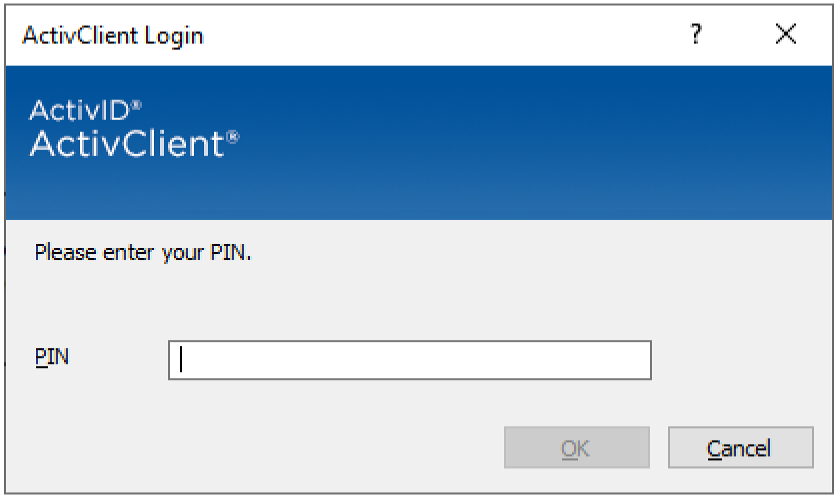
32. You will be prompted for the password that you saved in that EN_Password File (or whatever file name you selected; or you will type the password into the prompt if you wrote it down instead). If your computer does NOT allow you to paste it in, then carefully type that password into the prompt and select the OK Button.



This certificate is protected with a password.
Please enter the password to import this certificate.

Password: ●●●●●●●●

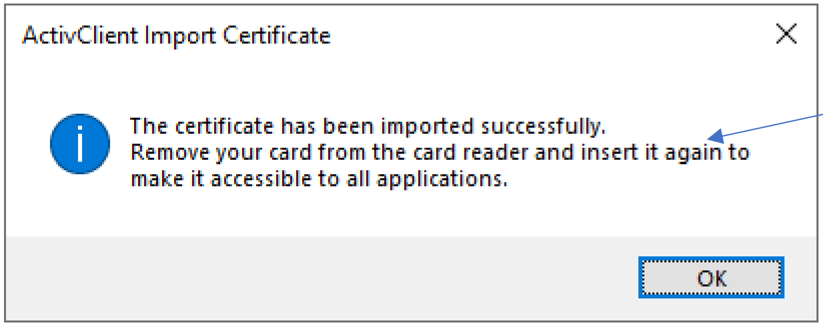
33. You may or may not be prompted for the PIN Code for your smartcard/cryptotoken. If you are, provide it and select the OK Button.



Please enter your PIN.

PIN

34. You should get an ActivClient Import Certificate Screen that will say you imported the certificate successfully. Click the OK Button.

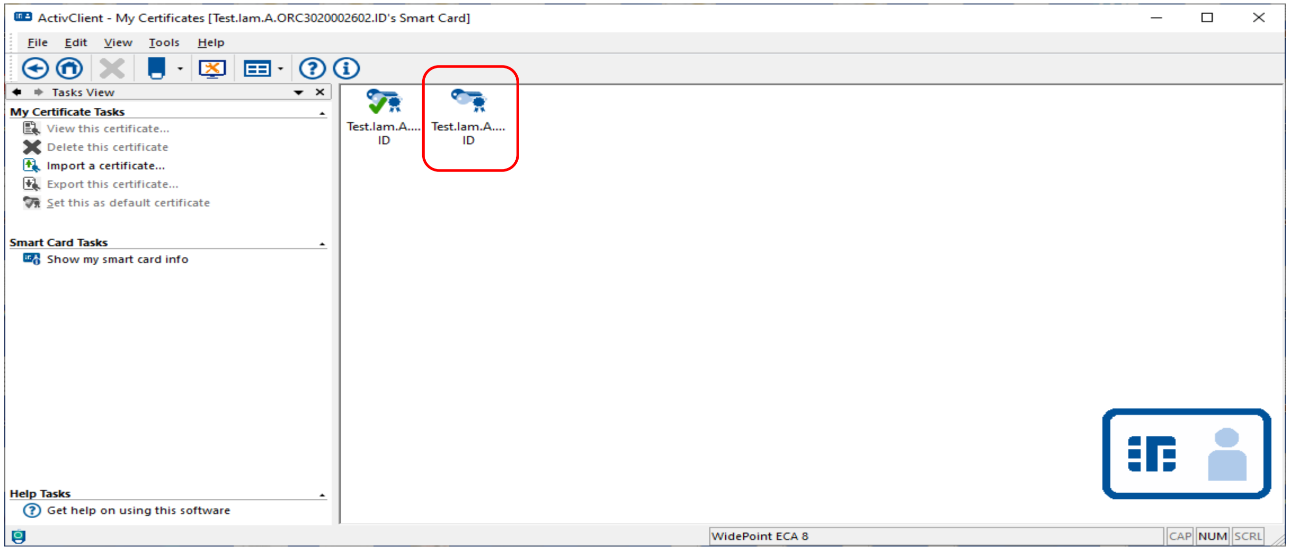


ActivClient Import Certificate

The certificate has been imported successfully.
Remove your card from the card reader and insert it again to make it accessible to all applications.

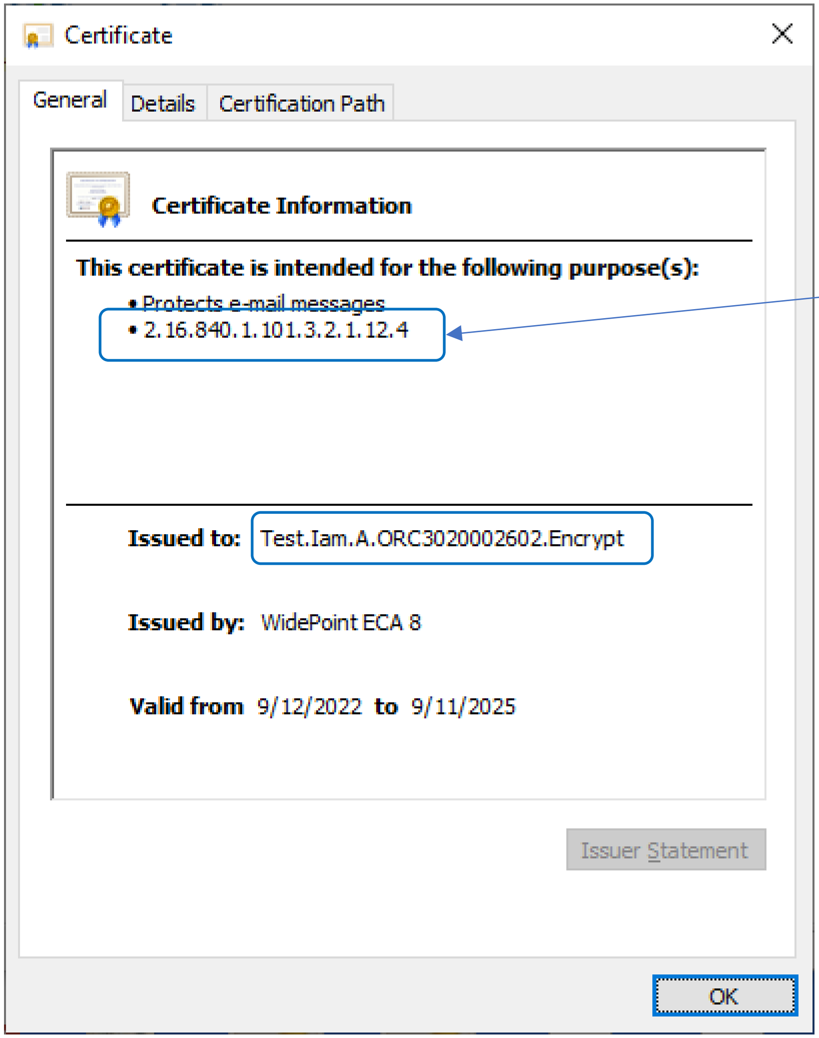
Follow the directions in the screen to the left to disconnect your smartcard/cryptotoken from the PC and then re-connect it.

35. You should now see two certificates (or two additional certificates if you had previous ones on it) on your smartcard/cryptotoken (it will be in the My Certificates Folder). The Encryption Certificate should now be the one without the green checkmark superimposed over it.



ActivClient - My Certificates [Test.Iam.A.ORC3020002602.ID's Smart Card]

36. Open up the Encryption Certificate to verify the info by right-clicking the mouse on it and selecting 'View this certificate.' Click the OK Button when done verifying.



This certificate is intended for the following purpose(s):

- Protects e-mail messages
- 2.16.840.1.101.3.2.1.12.4

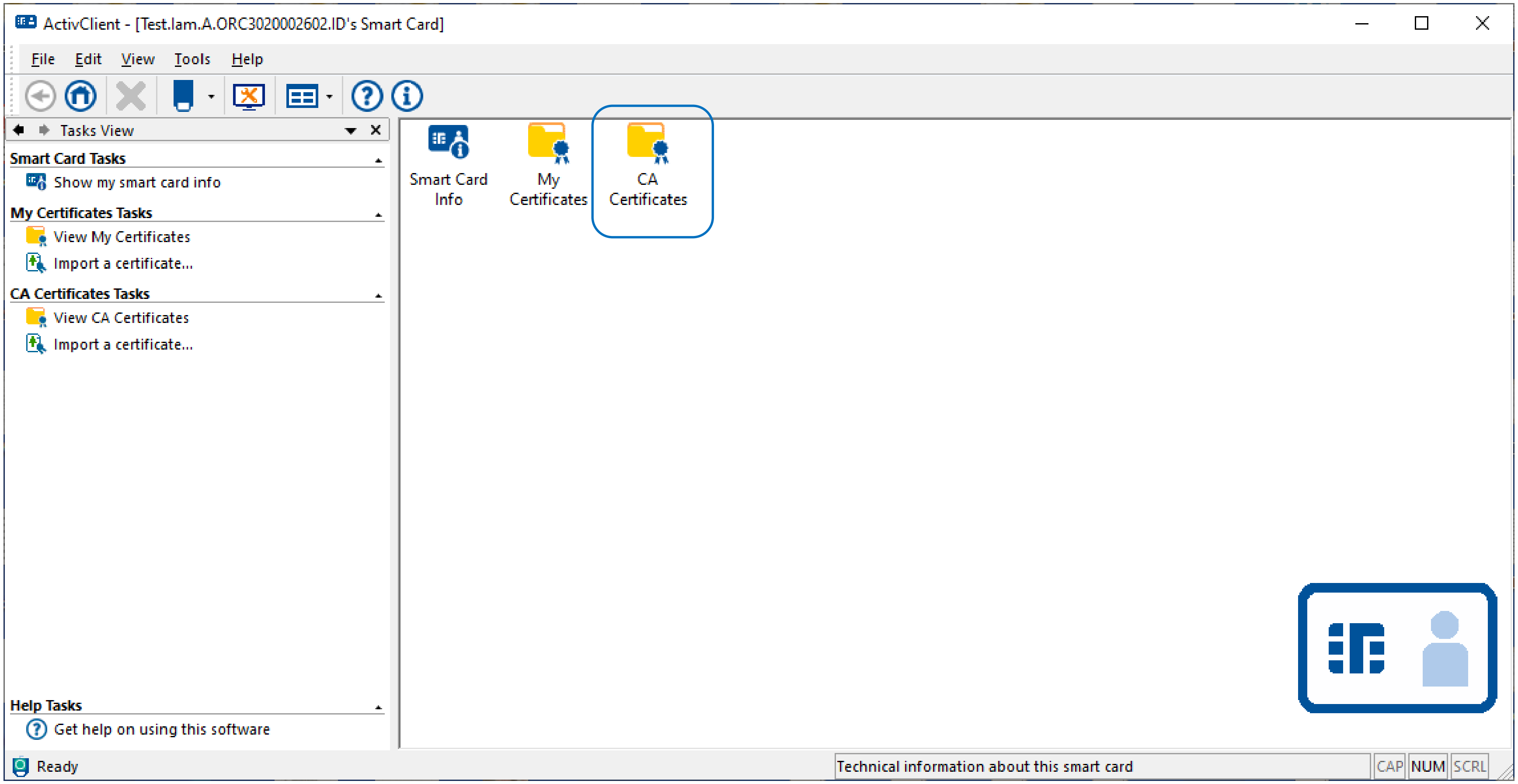
Issued to: Test.Iam.A.ORC3020002602.Encrypt

Issued by: WidePoint ECA 8

Valid from 9/12/2022 to 9/11/2025

Regardless of what level of ECA Certificate you got, the encryption certificate policy will end in a '4.'

37. If you disconnect and then re-connect your smartcard/cryptotoken to the computer and open up the ActivClient User Console as Step# 34 indicates, you probably will see a CA Certificates Folder. It contains the public keys of your ECA Certificate Trust Chain. You can leave it there; it will not harm or interfere with anything.



ActivClient - [Test.Iam.A.ORC3020002602.ID's Smart Card]

38. If you would like to save a backup copy of your .p12 Encryption Certificate File along with the EN_Password File to an external medium, go ahead and do so. Just make sure to lock that external medium in a safe or similar secure facility. It prevents you from having to worry about saving the EN Certificate after this set of certificates expires. However, you should probably delete those two files from your Public Documents Folder when finished to avoid any security issues.

39. You have successfully installed both of your certificates onto your smartcard/cryptotoken. They are ready to be used to access web sites, configure your Email Client application to digitally sign emails or exchange encrypted emails, and/or configure your PDF application to digitally sign documents.

40. Please note that after you import your encryption certificate onto your smartcard/cryptotoken that your PIN Code for your smartcard/cryptotoken will be prompted for you to enter whenever you use your encryption certificate (NOT the password that you used to import it onto the device). However, that password is still needed if you want to keep the backup copy of your encryption .p12 file because that password is still assigned to it.