1. To verify that your ECA Medium Assurance Files properly downloaded, open your Files Explorer Screen (if you do NOT have the below icon on your taskbar, then search for Files Explorer in the Search Box next to your Start Button [this is a search within your computer, not on the Internet]).



2. Within the Files Explorer Screen, you should see two .p12 files listed in your Downloads Folder/Section. If your computer does NOT show file extensions, then look for the File Types to be Personal Information Exchange.



3. You immediately need to save backup copies of **BOTH** of these files to an external network drive (outside of your C: Drive) or flashdrive for operational purposes. These backup files along with the password you assigned to them will allow you to recover the certificates if your computer crashes.



4. Save them to your folder on the network drive in this case. If you use a flashdrive/thumbdrive, make sure that you follow the safe ejection procedure before disconnecting the flashdrive/thumbdrive from the computer.

→ 🕆 🛧 쿺 > This PC → us	ser area (U:) >		~ 7	5.		
	Name	Date modified	Type Siz	ze		
Quick access	eauthra@orc.com_enc_15.p12	2/20/2022 5:40 PM	Personal Information Exchange	6 k	KB	
Desktop	wauthra@orc.com_id_15.p12	2/20/2022 5:40 PM	Personal Information Exchange	4 1	KB	
Downloads	/ Idapbrowser-rr	4/2/2022 4:51 PM	File folder			
Documents	FirefoxPortable	4/2/2022 4:51 PM	File folder			
Pictures	A Other Files	4/2/2022 3:57 PM	File folder			
EJBCA Issuance Emails						
Other Files						
Saml 2.0 Template Emails						
🛫 user area (U:)						
OneDrive						
This PC						
3D Objects						
Desktop						
Documents						
Downloads						
Music						
Pictures						
Videos						
Warehouse (orcfsvr) (W)						
OS (C:)						
ORC Internal (I:)						
OPC Projectr (Pr)						
USES PROJECTS (F.)						
user area (U:)						
Network						

5. Next, you need to import them into the Windows Certificate Store to be able to use them in the browsers and with your applications. Access the Microsoft Management Console (MMC) for your profile on this PC (you may need admin permissions from your IT Department to do this).



Select this mmc run command by clicking the left mouse button on it.

- 6. You should get a User Account Control Screen that will ask you if you want to allow this app to make changes to your device; it will have Microsoft Management Console listed. Click 'Yes' to open up the MMC for your profile on your PC.
- 7. You should then get the Console 1 Console Root Screen below. Click on the word 'File' in the Menu Bar.



8. Select 'Add/Remove Snap-in' from the list.



9. Then, in the Add or Remove Snap-ins Screen, go the Available Snap-ins Side, select the word 'Certificates' to highlight it in blue, and click on the 'Add' Button.



10. You should get a Certificates snap-in screen with 'My user account' selected. Leave it on that selection and click the 'Finish' Button. (Some of you may not get this screen; instead, the computer will jump to the screen on the next page.)



11. You will then get a 'Certificates – Current User' Line on the Selected Snap-ins Side. Click the 'OK' Button.

ole Root	Name		Actions
	Name		Console Root
		inere are no items to snow in this view.	More Actions
		Add or Remove Snap-ins X	
		You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.	
		Available snap-ins: Selected snap-ins:	
		ActiveX Control Microsoft Cor	
		Call Authorization Manager Microsoft Cor	
		Component Services Microsoft Cor Move Up	
		Device Manager Microsoft Cor Device Management Microsoft and Add >	
		Event Viewer Microsoft Cor	
		Group Policy Object Microsoft Cor	
		P Security Policy M Microsoft Corr	
		Advanced	
		Description: The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.	
		ОК Оласе	

12. You should then come back to the main Console 1 – Console Root Screen with the 'Certificates – Current User' Line under the Console Root Folder in the left-side window pane. Click on the arrow or hash mark in front of that line to display the list of folders within that group.



13. Open up the Personal Folder by clicking on the arrow or hash mark (blue outlined box) and then the Certificates Sub-Folder (double-click the left mouse button in the red box) if there is one. If there is NO Certificates Sub-Folder, then highlight the Personal Folder by clicking on it.



14. Next, start the procedure to import the identity certificate from the Downloads Folder/Section of your PC. In the menu bar select 'Action,' then 'All Tasks,' and 'Import.'



15. Select 'Next' on the Welcome to the Certificate Import Wizard Screen that opens up.





16. Click on the 'Browse' Button in the File to Import Screen.

17. Select the Downloads Folder/Section in the Files Explorer Screen and then change the file format in the bottom, right-hand corner of the screen from X.509 Certificate to Personal Information Exchange.



18. Select the certificate file that has 'id' in it so that it appears in the blank File name box at the bottom. Then, select the 'Open' Button.



19. You will see the following screen. Select the 'Next' Button.



20. You will see the following screen, with the exception of the open Notepad File. Open up the Notepad File with the password that you assigned to those certificate download files during the download process while you were logged into your account at our site, highlight it in the Notepad File, and put it in the copy queue (ctrl button + C; or right-click the mouse button on the highlighted password and select 'Copy'). Do NOT use 'yourpassword' as the certificate password!

Recycle Bin	Other Things		
Adobe Acrobat DC	Consolel - [Console Root/Certificates - Current U File Action View Favorites Window He Console Root Console Root Certificates - Current User Certificates - Certification Authorities Certificated Publiches Certificated Publiches Certificate Certification Authorities Certificate Enrollment Reguests Certificate Enrollment Reguests Certificate Enrollment Reguests Certificate Enrollment Reguests Certificate Enrollment Reguests Certificate Roots	Iser/Personal/Certificates] sip	<pre>status Egy Tapination Date Intended Purposes Friendly Name Status Cert Status Egy Certificate Import Wizard Friende synotection To maintain security, the private key, Passmord: Debale programe Key, Passmord Debale key potection, You will be prompted every time the Debale key potection. You will be prompted every time the Debale key potection. You will be prompted every time the Debale key potection. You will be prompted every time the Debale key potection. You will be prompted every time the Debale key potection. You will be prompted every time the Debale key potection. You will be prompted every time the Debale key using virtualized based security(hor export table) Debale key using virtualized based security(hor export table) In Tucket I 100% Windows (CRLF) UTF-8</pre>
Microsoft Teams ecc puttet	Personal store contains 1 certificate. Purchase Orders	<	
ー ア Type her	e to search	💽 what ke 📕 EJBCA	s 🗓 💼 🔞 🤣 🧀 eca post 📑 Issuanc 🍎 ORC We 📴 🛞 😤 Inbox 🧠 🎼 Vanessa 💑 Console Desktop " 🛅 off a ^ 🕄 🛥 🖫 🕬 44/2022 🖏

21. Next, paste your password into the 'Password' Box in the Certificate Import Wizard Screen (you can check to see if it is correct by checking the 'Display Password' Box). Also, check the first, second, and fourth boxes under 'Import options.' Then, click 'Next.'



22. You should see the following screen. 'Place all certificates in the following store' should be selected, and the 'Certificate store' Box should have the word 'Personal' in it. Click 'Next.'



23. Click 'Finish' on the 'Completing the Certificate Import Wizard' Screen.



24. Select the 'Set Security Level' Button.



25. Select the Radio Button for 'High' and click 'Next.'



26. Paste your password into the two blank boxes using the certificate password you typed into Notepad and click 'Finish.'



27. Then, click 'OK.'



28. You should get the following response. Click 'OK.'



29. You will see your identity certificate in the Certificates Sub-Folder of the Personal Folder in the Windows Certificate Store. Notice the gold key symbol on the left edge of the certificate icon at beginning of the line. You may get extra trust chain certificates to appear along with it in that Center Pane; just ignore them.



30. Repeat the process for the encryption certificate. Re-highlight the Certificates Sub-Folder under the Personal Folder in the left margin.

Console1 - [Console Root\Certificates - Current L	Jser\Personal\Certificates]						- 🗆 ×
File Action View Favorites Window He	elp						_ 8 ×
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly N	Actions	
Certificates - Current User	😰 172ac9ba-8ad1-4f07-a0ce-e27b3fa67812	MS-Organization-Access	11/15/2031	Client Authentication		Certificates	
Certificates	Tusso.richard.m.V.OKC302000013.ID	WidePoint ECA 8 Dev	2/19/2025	Client Authenticati	cn=russo.r	More Actions	•
Enterprise Trust							
Active Directory User Object							
> 📔 Trusted Publishers							
> Untrusted Certificates Third Date Reat Certification Authorities							
> Trusted People							
> 🧮 Client Authentication Issuers							
Other People Order DopRemovable Certificates							
 Certificate Enrollment Requests 							
> 🧮 Smart Card Trusted Roots							
	<				>		

31. Then, click on 'Action' in the Menu Bar, then click on 'All Tasks' in the list, and then click on the 'Import' Selection.



32. Then select 'Next' on the 'Certificate Import Wizard' Screen.

← 🛃	Certificate	Import Wizard
-----	-------------	---------------

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location	
Ourrent User	
◯ <u>L</u> ocal Machine	

To continue, dick Next.



 \times

33. Select the 'Browse' Button on the 'File to Import' Screen.

x	
~	
· ·	

🔶 🌛 Certificate Import Wizard

File to Import

Specify the file you want to import.

<u>F</u> ile name:	
1	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)

<u>N</u> ext Cancel

34. Change file type from X.509 Certificate to Personal Information Exchange in the bottom, right-hand corner of the screen and then highlight your new encryption certificate file.



35. When it appears in the 'File name' Box at the bottom of the screen, click on the 'Open' Button.



36. When you go back to the 'File to Import' Screen below, click 'Next.'

\sim
x

🔶 🌛 Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Users\russor\Downloads\eauthra@orc.com_enc_15.p12 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)



37. Paste your password from the Notepad File into the 'Password' Box. Check the first, second, and fourth 'Import options' Boxes. Then, click 'Next.'

			-	
٦	١.	s	۴	
	2	с		
		٦	۰.	

🗧 嵾 Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

assword:			
•••••			
Display Password			
mport options:			
Enable strong priv	vate key protection. Yo	ou will be prompted every time the	
	u by an application if y	ou enable uns option.	
Mark this key as e keys at a later tim	exportable. This will allo ne.	ow you to back up or transport you	Jr.
Protect private ke	y using virtualized-bas	ed security(Non-exportable)	
Include <u>a</u> ll extend	led properties.		
			~

38. Make sure the radio button for 'Place all certificates in the following store' is selected and that 'Personal' is in the 'Certificate store' Box. Then, click 'Next.'

٩.	,	۴	
2	c		
۴	1	۰.	

← 🖉 Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

O Automatically select the certificate store based on the type of certificate

Place all certificates in the following store

Certificate store:

Personal	Browse

Next	Cancel
Next	Cancer

39. Click 'Next' in the screen below.

🗧 嵾 Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Personal
Content	PFX
File Name	C:\Users\russor\Downloads\eauthra@orc.com_enc_:
<	>

<u>F</u> inish	Cancel

40. The 'Importing a new private exchange key' Screen will appear with the 'Security level set to Medium.' Click on the 'Set Security Level' Button.

Importing a r	new private exchange key	×
	An application is creating a Protected item.	
	CryptoAPI Private Key	
	Security level set to Medium Set Security Level	
	OK Cancel <u>D</u> etails	

41. Change the Security Level from Medium to High by selecting the top radio button.



42. Then click 'Next.'



43. Paste your password into both boxes from the Notepad File and click 'Finish.'

Create a Password		\times
	Create a password to protect this item.	
	Create a new password for this item. Password for: CryptoAPI Private Key	
	Password: Confirm:	
	< Back <u>F</u> inish Cancel	

44. Security level will be set to High. Click 'OK' on the next screen.



45. You should get the response that the import was successful. Click the 'OK' Button.



46. Your encryption certificate will appear in the Center Pane. You may get extra trust chain certificates to appear along with it in that Center Pane; just ignore them.

r\Personal\Certificates]				
Issued To	Issued By MS-Organization-Access WidePoint ECA 8 Dev WidePoint ECA 8 Dev ates will be Issued By Wide he example above says!	Expiration Date 11/15/2031 2/19/2025 2/19/2025 ePoint ECA 8 and	Intended Purposes Client Authentication Secure Email Client Authenticati	Friendly N russo.richa cn=russo.r
	\Personal\Certificates]	\Personal\Certificates] Issued To Issued To Issued To Intraceled and the state of the	\Personal\Certificates] Issued To Issued By Expiration Date I172ac9ba-8ad1-4f07-a0ce-e27b3fa67812 MS-Organization-Access 11/15/2031 Irusso.richard.m.V.ORC3020000013.Encrypt WidePoint ECA 8 Dev 2/19/2025 Irusso.richard.m.V.ORC3020000013.ID WidePoint ECA 8 Dev 2/19/2025 Again, your NEWLY issued certificates will be Issued By WidePoint ECA 8 and NOT by WidePoint ECA 8 Dev as the example above says!	\Personal\Certificates] issued To issued To I12ac9ba-8ad1-4f07-a0ce-e27b3fa67812 MS-Organization-Access I1712/2031 Client Authentication Invsso.richard.m.V.ORC302000013.Encrypt WidePoint ECA 8 Dev 2/19/2025 Secure Email Prusso.richard.m.V.ORC302000013.ID WidePoint ECA 8 Dev 2/19/2025 Client Authentication Again, your NEWLY issued certificates will be Issued By WidePoint ECA 8 and NOT by WidePoint ECA 8 Dev as the example above says!

47. Next, select your identity certificate (Issued To ends in .ID).

🚟 Console1 - [Console Root\Certificates - Current U	lser\Personal\Certificates]					
<u> F</u> ile <u>A</u> ction <u>V</u> iew Fav <u>o</u> rites <u>W</u> indow <u>H</u> e	łp					
🗢 🔶 📶 🠇 🖬 🗶 🛅						
 Console Root Certificates - Current User Personal Certificates Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Active Directory User Object Trusted Publishers Untrusted Certificates Trusted People Client Authentication Issuers Cher People Local NonRemovable Certificates Smart Card Trusted Roots 	Issued To Issued To Issued To Interpret Additional State Sta	Issued By MS-Organization-Access WidePoint ECA 8 Dev WidePoint ECA 8 Dev	Expiration Date 11/15/2031 2/19/2025 2/19/2025	Intended Purposes Client Authentication Secure Email Client Authenticati	Friendly Name russo.richard.m.V.O cn=russo.richard.m	S Acti Cer rus:

48. Double-left click the mouse button on that identity certificate to open it up. Your screen should like this, except for Issued To, Issued By, and Validity Dates.

