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....

🚡 Concole1 - [Console Root]	
File ction View Favorites Window	Help _ & ×
New Ctrl+N	
Open Ctrl+O	Actions
Save Ctrl+S	There are no items to show in this view.
Save As	More Actions
Add/Remove Snap-in Ctrl+M	
Options	
1 eventvwr.msc	
2 secpol.msc	
3 gpedit.msc	
4 devmgmt.msc	
Exit	
Enables you to add snap-ins to or remove them fro	om the snap-in console.

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

nap-in	Vendor	*		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor				
Authorization Manager	Microsoft Cor				<u>R</u> emove
Certificates	Microsoft Cor	-			
Component pervices	Microsoft Cor	=			Move Up
Computer Managem	Microsoft Cor				
Device Manager	Microsoft Cor				Move <u>D</u> own
Disk Management	Microsoft and		<u>\</u> dd >		
Event Viewer	Microsoft Cor				
Folder	Microsoft Cor				
Group Policy Object	Microsoft Cor				
IP Security Monitor	Microsoft Cor				
IP Security Policy M	Microsoft Cor				
Link to Web Address	Microsoft Cor	-			Ad <u>v</u> anced
·-			L		
cription:					
Link to Web Address	Microsoft Cor	-			Ad <u>v</u> anced

7. If you see a <u>Certificates Snap-in</u> 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 <u>Add or Remove Snap-ins</u> dialog, you should see "Certificates – Current User" under "Console Root". Click the **OK** button.

Add or Remove Snap-ins					×
You can select snap-ins for t extensible snap-ins, you car	his console from th I configure which e	iose xter	available on you nsions are enable	ur computer and configure the selected s ed.	set of snap-ins. For
Available <u>s</u> nap-ins:		_	1	Selected snap-ins:	
Snap-in	Vendor	4		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor Microsoft Cor			도둑 ^µ Certificates - Current User	Remove
Component Services	Microsoft Cor Microsoft Cor				Move Up
Device Manager Disk Management	Microsoft Cor Microsoft and		<u>A</u> dd >		Move <u>D</u> own
Event Viewer	Microsoft Cor Microsoft Cor Microsoft Cor				
IP Security Monitor	Microsoft Cor Microsoft Cor				
Link to Web Address	Microsoft Cor	Ŧ			Ad <u>v</u> anced
Description: The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.					
				C	OK Cancel

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.

Console1 - [Console Root]			- 0 x
Eile Action View Favorites	<u>W</u> indow <u>H</u> elp		- 8 ×
Console Root	Name	Actions	
Personal	🗟 Certificates - Current User	Console Root	^
Trusted Root Certification.		More Actions	•
Enterprise Trust			
Intermediate Certification i			
Active Directory User Objection			
Irusted Publishers			
Dird-Party Root Certification			
Trusted People			
🔥 🚞 Other People			
Certificate Enrollment Requ			
Certificates			
Smart Card Trusted Roots			
۰ III • •			

10. Select the entry that reads "caUserCert_keyPair" (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

🚡 Console1 - [Console Root\Certificat	tes - Current User\Certificate En	rollment Requests\Certificates]		
File Action View Favorites	Window Help			- 8 ×
Console Root	Issued To	Issued By	Actions	
Certificates - Current User	CaEncorptionCert_keyPair	caEncryptionCert_keyPa	ir Certificates	-
 Figure Formation Trusted Root Certification 	CaUserCert_keyPair	Open	More Actions	•
 Enterprise Trust Intermediate Certification 		All Tasks)	Open eyPair	•
 Active Directory User Object Trusted Publishers Untrusted Certificates Third-Party Root Certificat Trusted People Other People Certificate Enrollment Require Certificates Smart Card Trusted Roots 		Cut Copy Delete Properties Help	ixport	•
✓ Ⅲ ► Export a certificate	< <u> </u>			

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 can not 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 <u>ECA Help Desk</u>.



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

Certificate Export Wizard
Export File Format Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
ersonal Information Exchange - PKCS #12 (.PFX)
Todude all certificates in the certification path if possible
Delete the private key if the export is successful
Export <u>all extended properties</u>
 Microsoft Serialized Certificate Store (.SST)
Learn more about <u>certificate file formats</u>
< <u>B</u> ack <u>Next</u> Cancel

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.

Certificate Export Wizard	x
Password To maintain security, you must protect the private key by using a password.	
Type and confirm a password. Prasword:	
Type and <u>c</u> onfirm password (mandatory):	
< <u>Back</u> Next > Can	cel

.

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.*

Certificate Export Wizard
File to Export Specify the name of the file you want to export
Eile name:
< Back Next > Cancel

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 is "*yourlastname_*Enroll_ECA_ID_todaysdate" (Or " *yourlastname_*Enroll_ECA_EN_todaysdate " for your Encryption Certificate Enrollment Key Pair). 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 abel 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.

ᡖ Save As			x
🕞 🕞 🗢 💻 Desktop	► ► ► ► ► ► ► ► ► ► ► ► ► ► ► ► ► ► ►	top	٩
Organize 🔻 New fo	lder		0
4 🔆 Favorites	Name	Size	Ite 🖍
📃 Desktop	📜 Libraries		
Do ynloads	🔋 James Manchester		=
🔚 Recent Places	📃 📭 Computer		
	🗣 Network		
4 📜 Libraries	🐌 13DEcLogs		Fil
Documents	퉬 Desk Top 04_20_2012		Fil
🖻 🌙 Music	🌗 DeskTop_11_08_2012		Fil
Pictures	🕌 LRAs		Fil 👻
🗅 🛃 Videos	✓ (•
File <u>n</u> ame Vo	urlastname_ECA_ID_Enroll_14Dec2012		-
Save as type: Per	sonal Information Exchange (*.pfx)		-
) Hide Folders	Save	Cance	:

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.

Certificate Export Wizard		×
	Completing the Certificate Exp Wizard You have successfully completed the Certificate	port
	wizard. You have specified the following settings:	
	Eile Name	C:\Lise
	Export Keys	Yes
	Include all certificates in the certification path	No
	File Format	Personi
	< <u> </u>	4
	< <u>B</u> ack Finish	Cancel

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.

Exporting you	r private exchange key	×
	An application is requestir	ng access to a Protected item.
	<u>P</u> assword for: CryptoAPI Private Key	Remember password
	ОК	Cancel <u>D</u> etails

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 has 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.]

Decryption	error!
	Unable to access the Protected item. Please verify that the password you just entered is the correct one.
	OK

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



22. Back on the MMC; select the entry that reads "caEncryptionCert_keyPair" (this is the key pair for the Encryption Certificate) and right-click. From the resulting menu, select **All Task** -> **Export...** to open the Microsoft Certificate Export Wizard

🚡 Console1 - [Console Root\Certificates - Current User\Certificate Enrollment Requests\Certificates]			
Image: File Action View Favorites Window Help _ ☞ × Image: Image: Image: File Action View Favorites Window Help _ ☞ ×			
Console Root Certificates - Current User Personal Circuited Root Certification Circuited Root Certification Circuited Publishers Circuited Publishers Circuited Certificates Circuited People Circuited People Circuited Enrollment Require Circuited Certificates Circuited Signat Card Trusted Roots	Issued To	Issued By Open All Tasks Cut Copy Delete Properties Help	Actions Certificates More Actions Open Export s •
Export a certificate			

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 <u>ECA Help Desk</u>.



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

Certificate Export Wizard		
Export File Format Certificates can be exported in a variety of file formats.		
Select the format you want to use:		
DER encoded binary X.509 (.CER)		
Base-64 encoded X.509 (.CER)		
Oryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)		
Include all certificates in the certification path if possible		
ersonal Information Exchange - PKCS #12 (.PFX)		
Include all certificates in the certification path if possible		
Delete the private key if the export is successful		
Export <u>all extended properties</u>		
 Microsoft Serialized Certificate Store (.SST) 		
Learn more about <u>certificate file formats</u>		
< <u>B</u> ack Cancel		

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.

Certificate Export Wizard	x
Password To maintain security, you must protect the private key by using a password.	
Type and confirm a password. Prasword:	
Type and <u>c</u> onfirm password (mandatory):	
< Back Next > Car	ncel

.

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*.

Certificate Export Wizard	×
File to Export Specify the name of the file you want to ex	xport
Eile name:	Browse
	< Back Next > Cancel

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 is "*yourlastname_*Enroll_ECA_EN_todaysdate" 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 abel 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.

Certificate Export Wizard		×
	Completing the Certificate Exp Wizard You have successfully completed the Certificate wizard.	D ort Export
	You have specified the following settings:	
	File Name Export Keys Include all certificates in the certification path File Format	C:\Use Yes No Person;
	< <u> </u>	Þ
	< <u>B</u> ack Finish	Cancel

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.

Exporting your private exchange key			
	An application is requesting access to a Protected item.		
	Password for: CryptoAPI Private Key		
	OK Cancel <u>D</u> etails		

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 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 and 8 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>)

Exporting your private exchange key			
	An application is requesting access to a Protected item.		
	Password for: CryptoAPI Private Key		
	OK Cancel <u>D</u> etails		

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 red X symbol.

🚡 Console1 - [Console Root\Certificates - Current User\Certificate Enrollment Requests\Certificates]			
File Action View Favorites Window Help			
🗢 🔿 🖄 🗊 📋 🙆 🛃			
Console Root	Issued To	Issued By	Actions
▲ Gertificates - Current User	CaEncryptionCert_keyPair	caEncryptionCert_keyPair	Certificates
Feisonal Trusted Root Certification.	🛱 caUserCert_keyPair	caUserCert_keyPair	More Actions
Enterprise Trust			
Intermediate Certification , Active Directory User Object			
Active Directory oser Objection Trusted Publishers			
Untrusted Certificates			
Third-Party Root Certificat			
Other People			
a 📔 Certificate Enrollment Requ			
Certificates			
۰ III ۲	•	4	
Certificate Enrollment Requests store contains 2 certificates.			

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



This document last modified 01 December 2012