

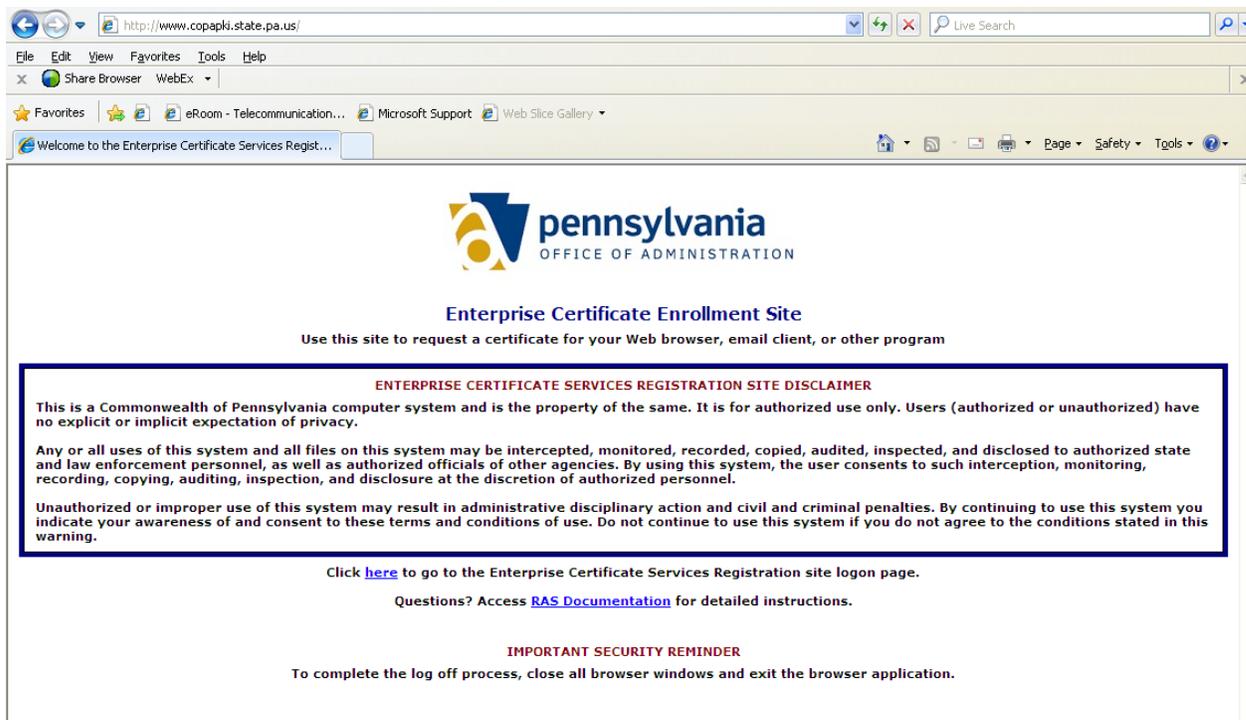
Juniper VPN – ARA users for MAC

I. Download a Digital Certificate

Digital certificate are required to connect to the Commonwealth’s VPN system. The digital certificates **MUST** be downloaded on a Microsoft Windows machine and then copied onto the MAC machine. The instructions in this section describe the method for downloading the digital certificate.

A. Personal Certificate Download and Installation

1. Open Internet Explorer, go to <http://www.copapki.state.pa.us>.
2. The *Enterprise Certificate Services Registration Site* screen is displayed.
3. Select “**Click [here](#)**” below the disclaimer box. This will allow you to request a certificate that will ensure RAS security.



The screenshot shows a web browser window with the address bar displaying <http://www.copapki.state.pa.us/>. The page content includes the Pennsylvania Office of Administration logo, the title "Enterprise Certificate Enrollment Site", and a disclaimer box. The disclaimer text is as follows:

ENTERPRISE CERTIFICATE SERVICES REGISTRATION SITE DISCLAIMER

This is a Commonwealth of Pennsylvania computer system and is the property of the same. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized state and law enforcement personnel, as well as authorized officials of other agencies. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized personnel.

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. Do not continue to use this system if you do not agree to the conditions stated in this warning.

Click [here](#) to go to the Enterprise Certificate Services Registration site logon page.

Questions? Access [RAS Documentation](#) for detailed instructions.

IMPORTANT SECURITY REMINDER

To complete the log off process, close all browser windows and exit the browser application.

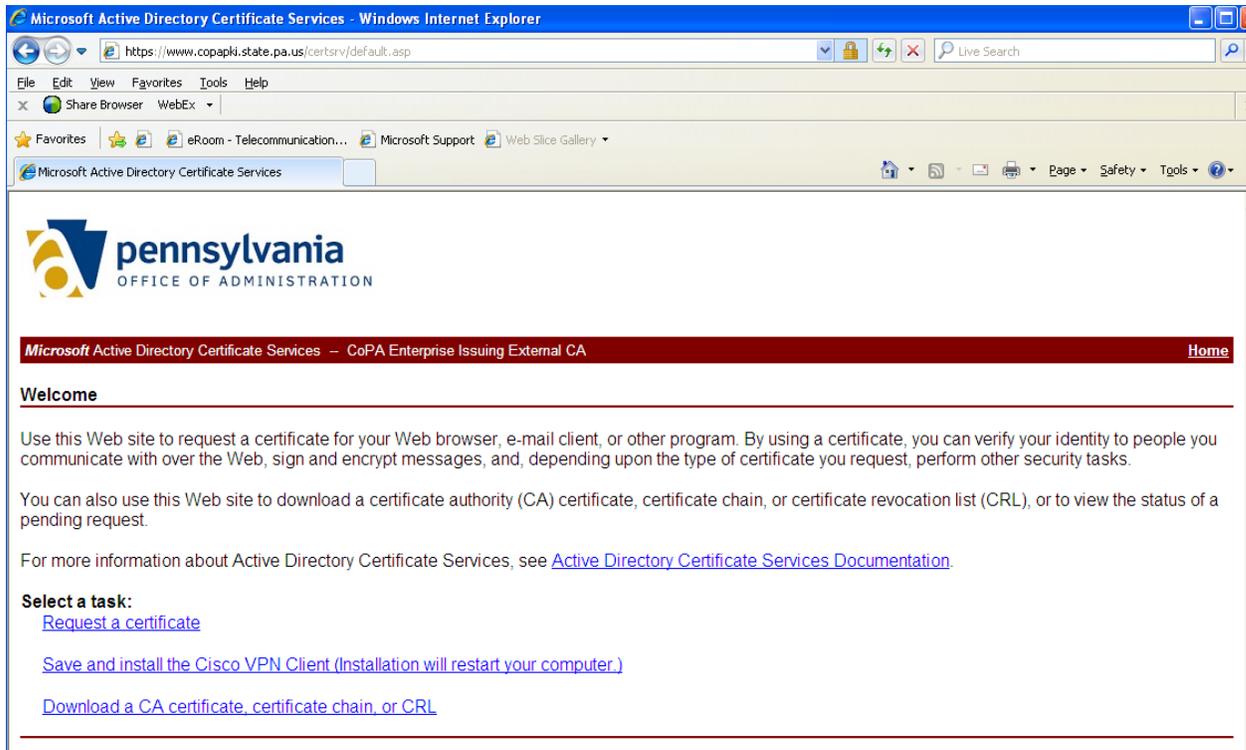
4. Click “**Yes**” if the *Security Alert* screen is displayed.



4. Enter your **ARA Username and Password** (the ones you were assigned when your account was created. Your username will be prefixed by the agency’s three-letter identifier. Example: dlic-jsmith.)
- The Username must be prefixed by **user**
 - Windows 2000 users **ONLY** will have the domain line displayed. Enter **USER** in the domain box.



5. Select the “[Request a certificate](#)” link.



The screenshot shows a Windows Internet Explorer browser window displaying the Microsoft Active Directory Certificate Services website. The address bar shows the URL <https://www.copapki.state.pa.us/certsrv/default.asp>. The page features the Pennsylvania Office of Administration logo and a navigation bar with the text "Microsoft Active Directory Certificate Services - CoPA Enterprise Issuing External CA" and a "Home" link. The main content area is titled "Welcome" and contains the following text:

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

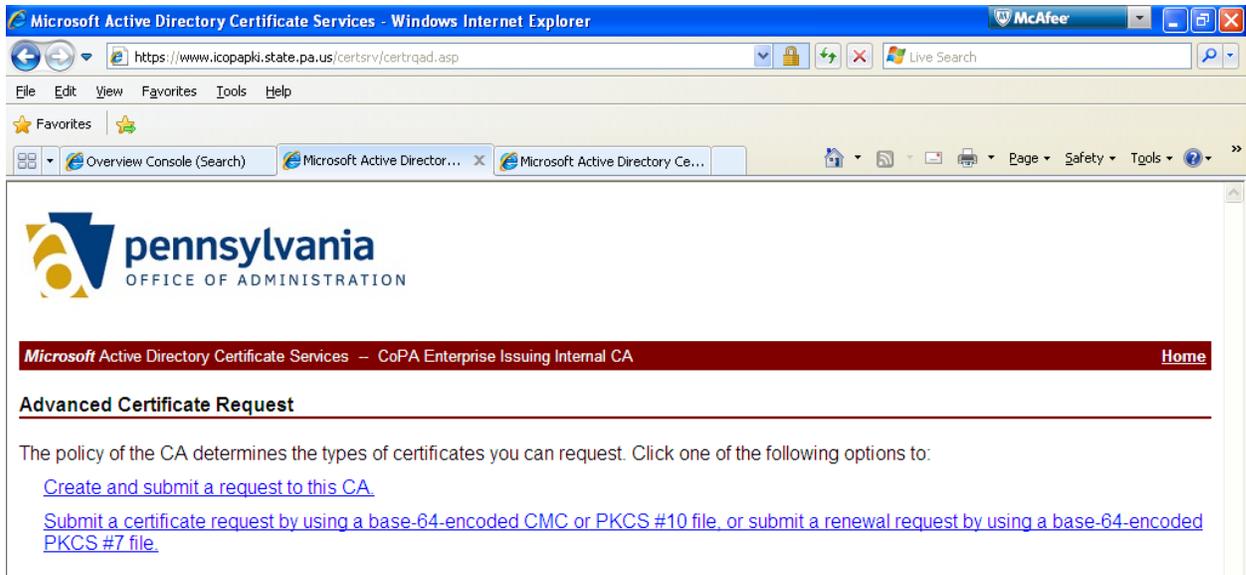
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [Save and install the Cisco VPN Client \(Installation will restart your computer.\)](#)
- [Download a CA certificate, certificate chain, or CRL](#)

6. Select the “[Create and submit a request to this CA.](#)” link.

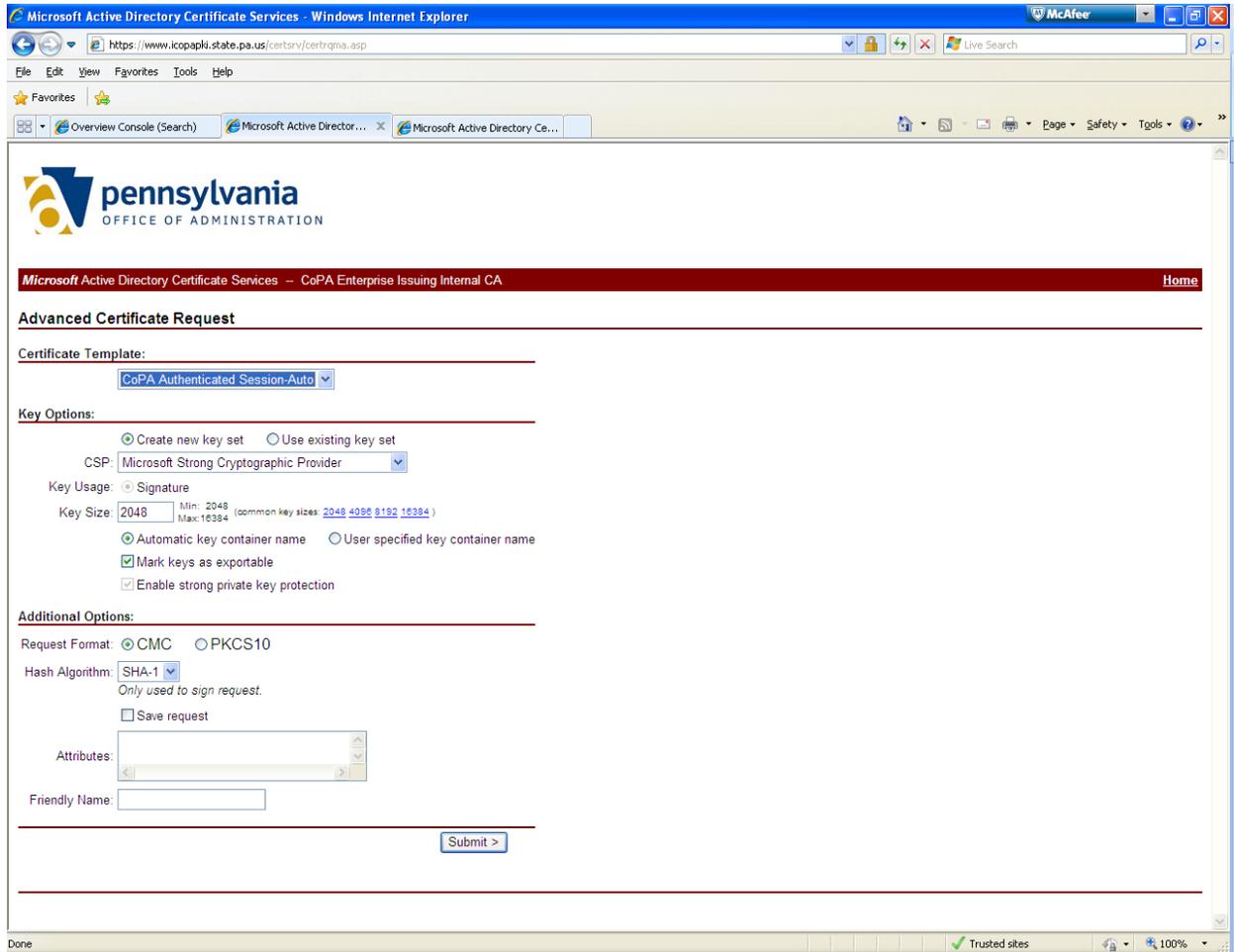


The screenshot shows a Windows Internet Explorer browser window displaying the Microsoft Active Directory Certificate Services website. The address bar shows the URL <https://www.icopapki.state.pa.us/certsrv/cetrqad.asp>. The page features the Pennsylvania Office of Administration logo and a navigation bar with the text "Microsoft Active Directory Certificate Services - CoPA Enterprise Issuing Internal CA" and a "Home" link. The main content area is titled "Advanced Certificate Request" and contains the following text:

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

- [Create and submit a request to this CA.](#)
- [Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)

7. Select the following options on the *Advanced Certificate Request* screen:
 - a. In the “Certificate Template” drop-down select the template type
 - i. **“CoPA Authentication Session-Auto”**
 - ii. Select a different option if required.
 - b. In the “Key Options” drop-down make sure the following is displayed:
 - i. CSP: **“Microsoft Strong Cryptographic Provider”**
 - c. Select the **“Submit”** button to start generating the request.



8. Select **“Yes”** on the *Potential Scripting Violation* screen.



9. Select the “**Set Security Level**” button.



10. Select “**High**” to make this certificate password protected and then click “**Next>**”.



11. Enter the following information on the *Creating a new RSA signature key* screen and select **“Finish”** when completed.
- Enter a **unique password** in the “Password” field that will also be used through the Export and Import process. Anything alpha and/or numeric will work.
 - Re-enter** the unique password in the “Confirm” field.
 - This Password remains the same for this yearly certificate. It is important that you remember this password. If you forget the password it cannot be recovered or reset.



NOTES: Please be aware of the following:

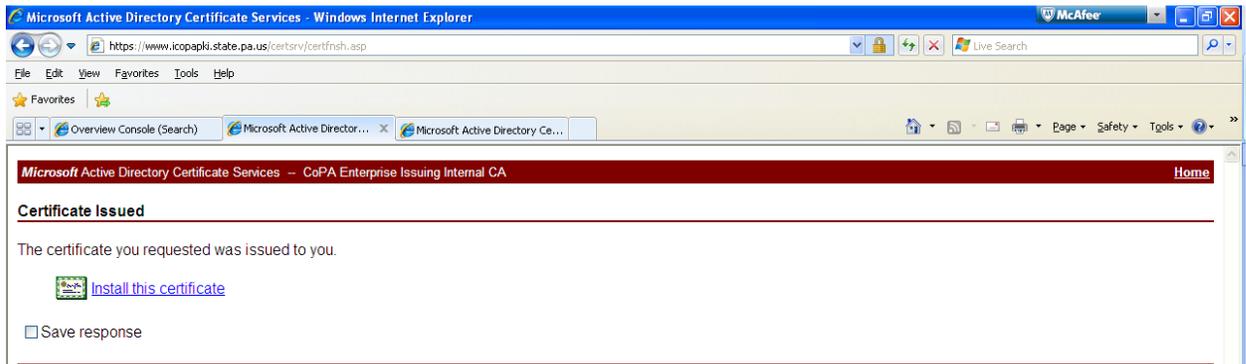
Windows XP - “Password for:” field = **CryptoAPI Private Key** will be displayed.

Windows 2000 - “Password for:” field will be **empty**.

12. Select **“OK”** to confirm the setting.



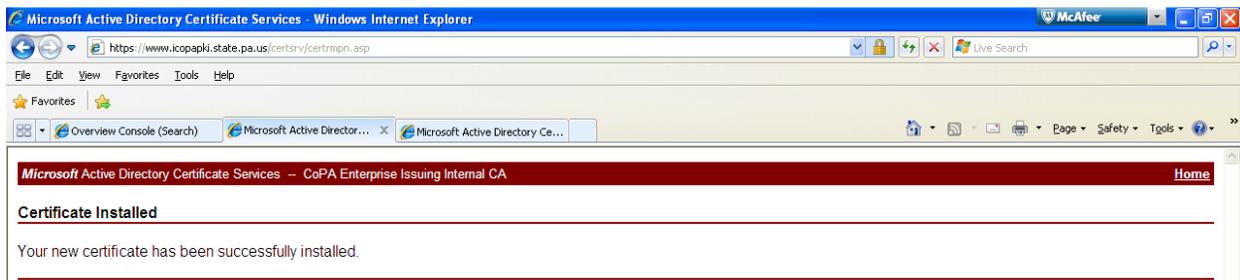
13. Select “[Install this certificate](#)”. It may take a few moments for the certificate icon to appear so please be patient and wait for the icon to appear before clicking the link.



14. Select “**Yes**”. The next screen may take a few minutes to appear.

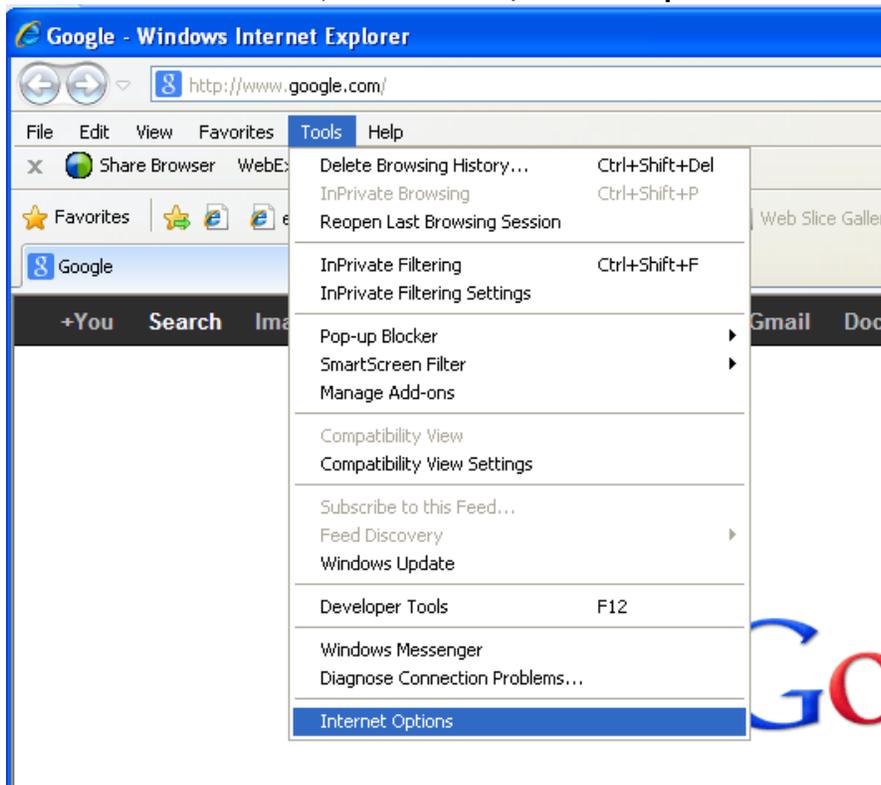


15. A “**Certificate Installed**” confirmation message is displayed when the certificate has been successfully downloaded and installed. Close (X) the screen.

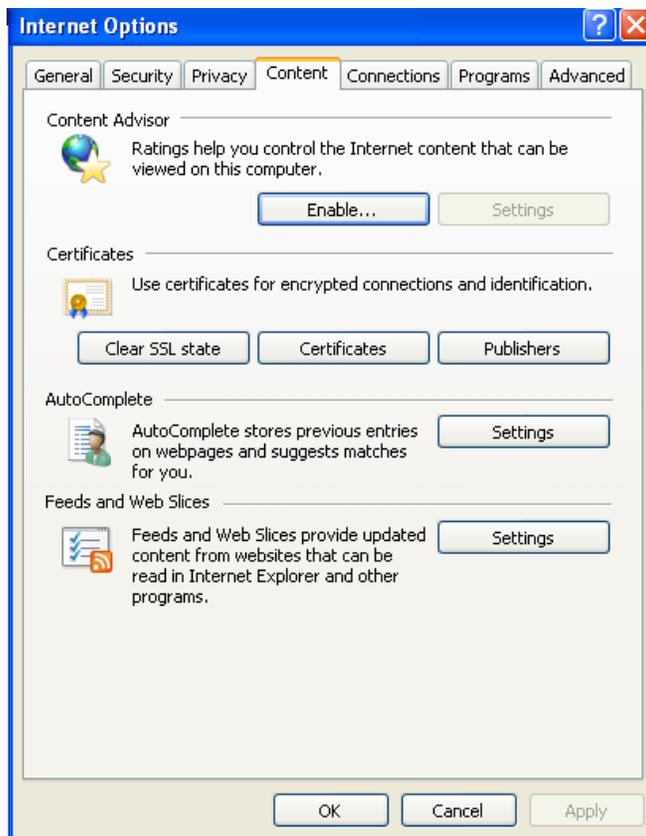


B. Export certificate to thumb drive or other external media.

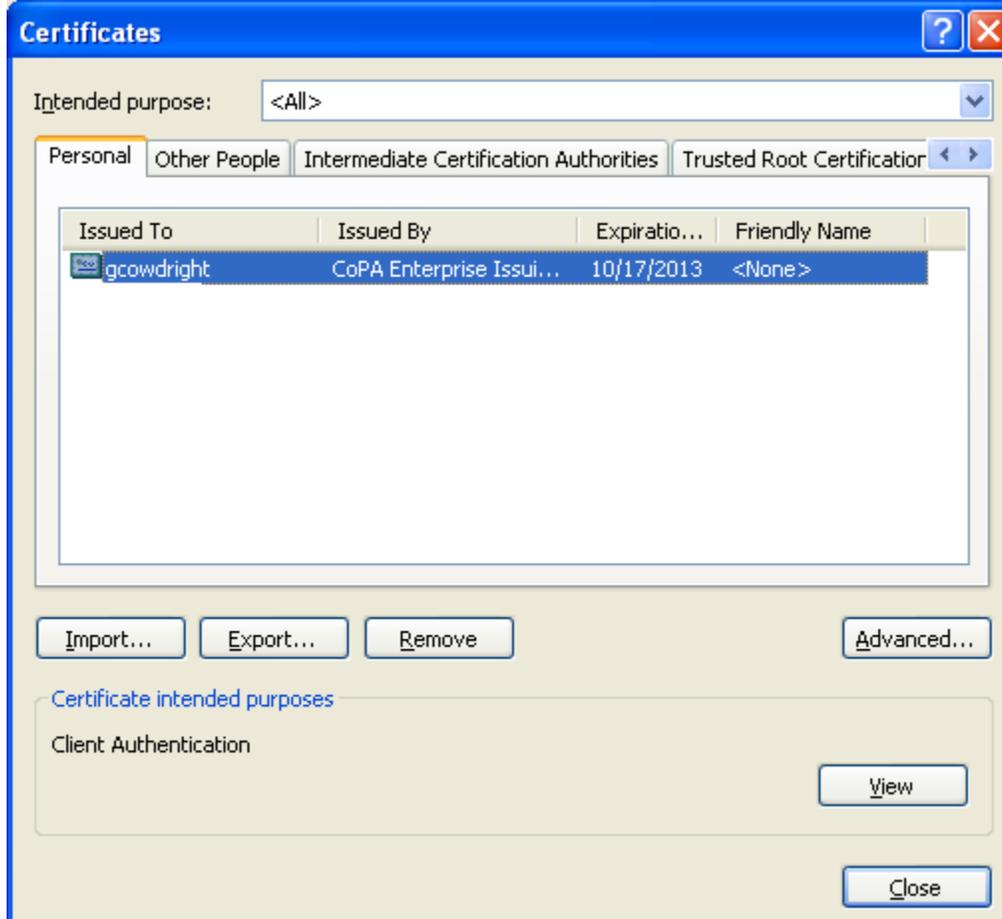
1. On your Windows machine, open Internet Explorer.
2. On the menu bar, click on **Tools, Internet Options**



3. Click on the **Content** tab; click on the **Certificates** button.



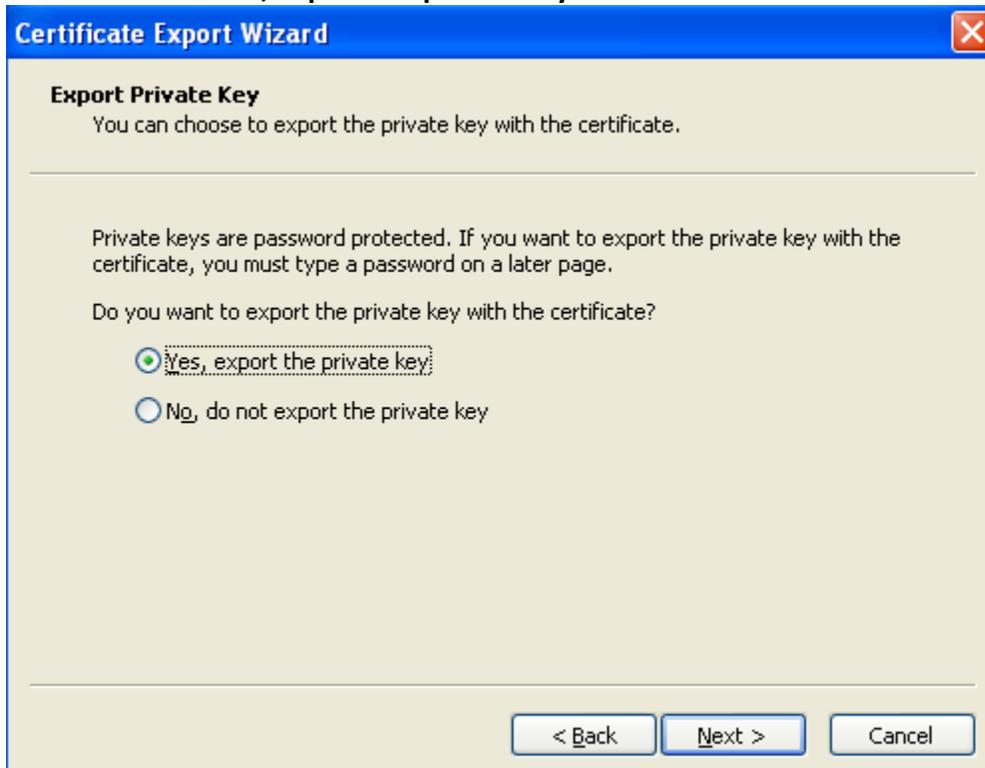
4. Highlight the certificate that you just installed, and click on the **Export** button.



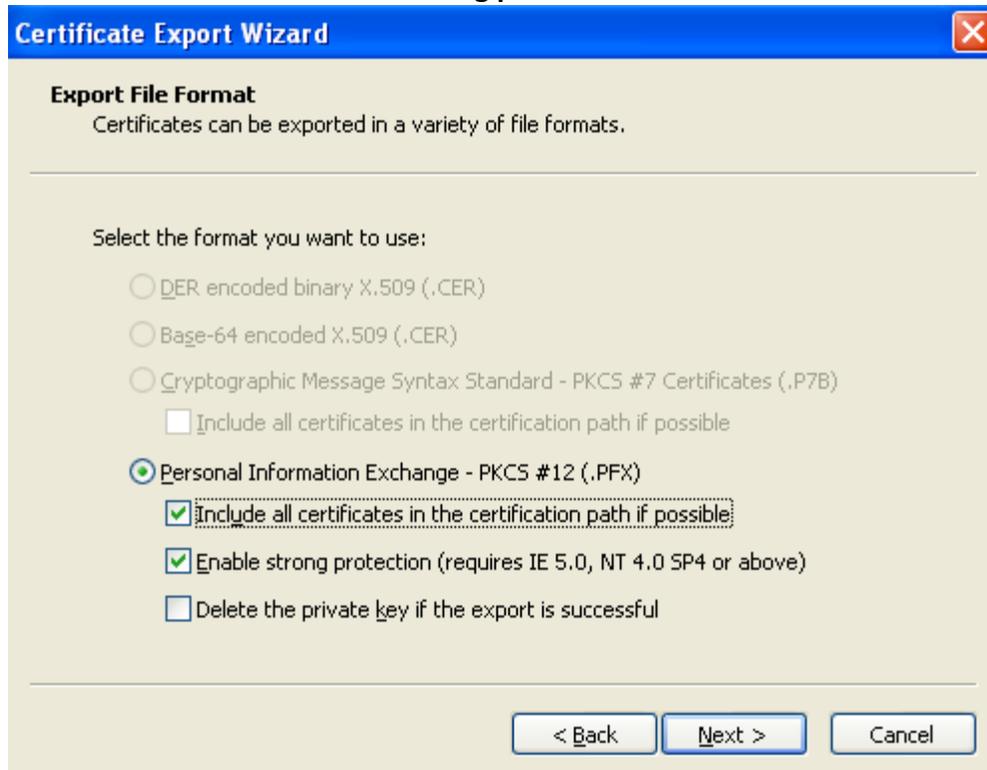
5. Click on **Next**



6. Click on **Yes, export the private key**. Click on **Next**.



- Put check marks in front of **Include all certificates in the certification path if possible** and in front of **Enable strong protection**. Click on **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
- Personal Information Exchange - PKCS #12 (.PFX)
 - Include all certificates in the certification path if possible
 - Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
 - Delete the private key if the export is successful

< Back Next > Cancel

- Enter your certificate password and confirm it. Click on **Next**.



Certificate Export Wizard

Password
To maintain security, you must protect the private key by using a password.

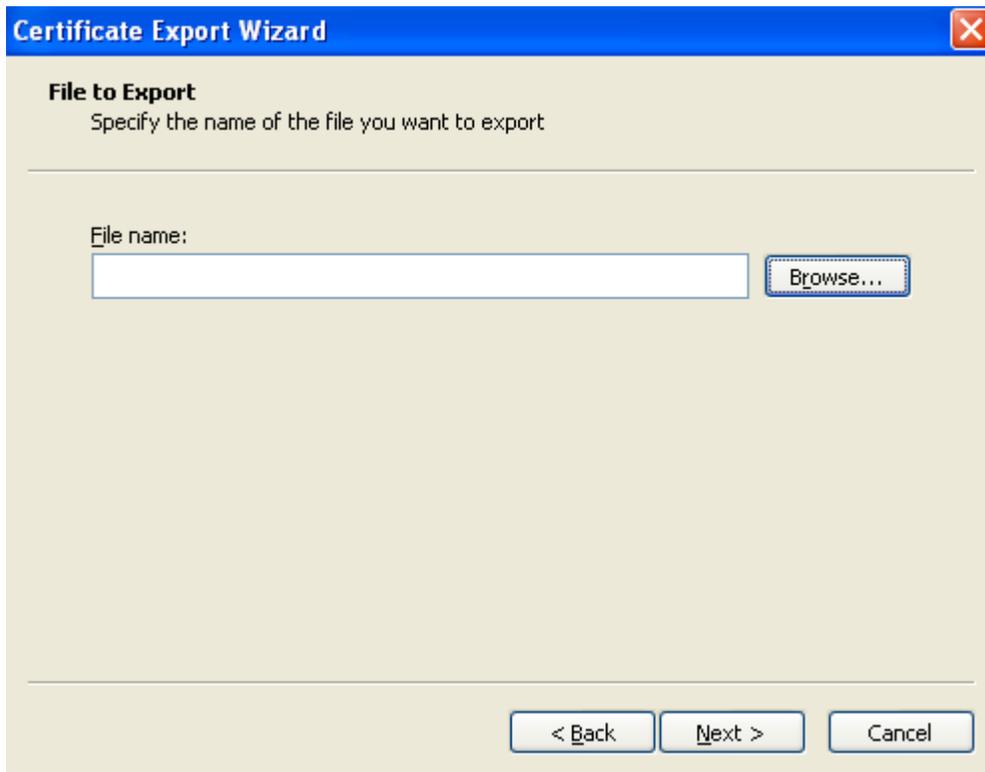
Type and confirm a password.

Password:

Confirm password:

< Back Next > Cancel

9. Click on the **Browse** button



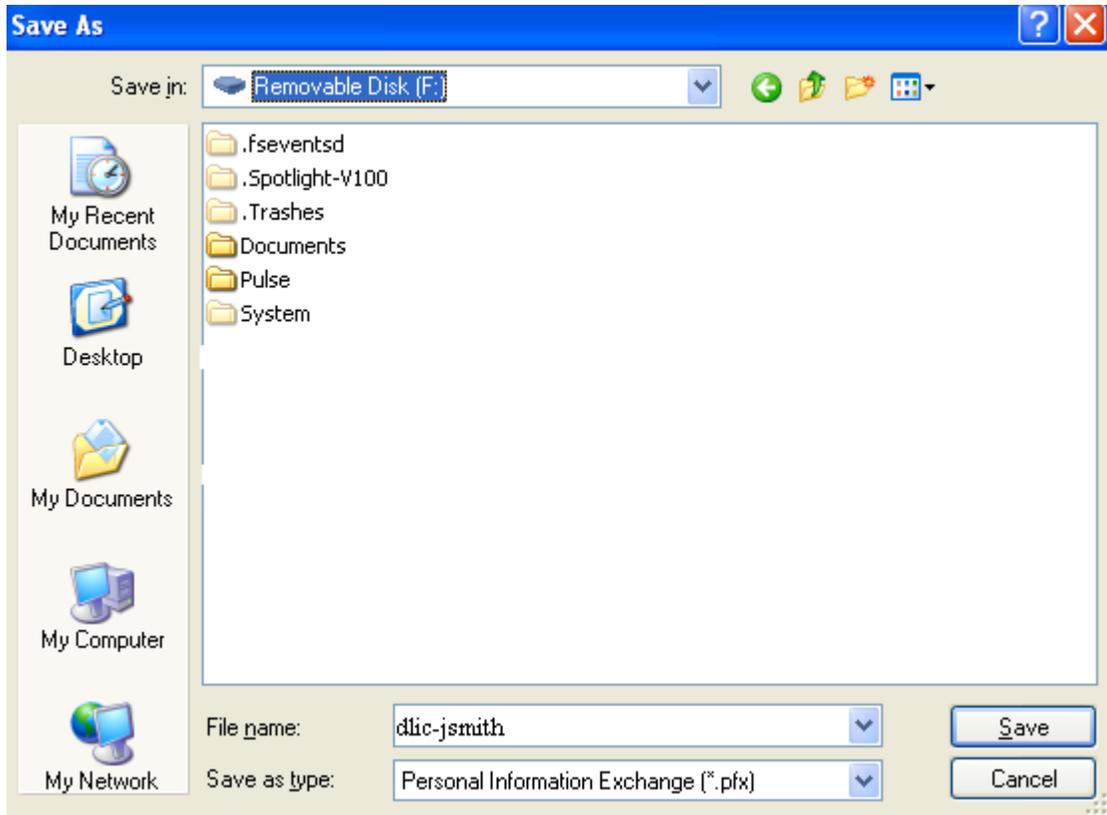
Certificate Export Wizard [X]

File to Export
Specify the name of the file you want to export

File name:

The image shows a Windows-style dialog box titled "Certificate Export Wizard" with a close button (X) in the top right corner. The main area is titled "File to Export" and contains the instruction "Specify the name of the file you want to export". Below this is a horizontal line, followed by the label "File name:" and an empty text input field. To the right of the input field is a "Browse..." button. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

10. In the **Save in:** box, navigate to the location of your external media.
11. In the **File name:** box type in your username.
12. Click on **Save**



13. The path you chose should appear in the **File name:** box. Click on **Next**.



14. Click on **Finish**



15. Enter your certificate password in the **CryptoAPI Private Key** box. Do NOT check **Remember Password**.



16. You have successfully exported your digital certificate.



II. Install Juniper Connect for MAC

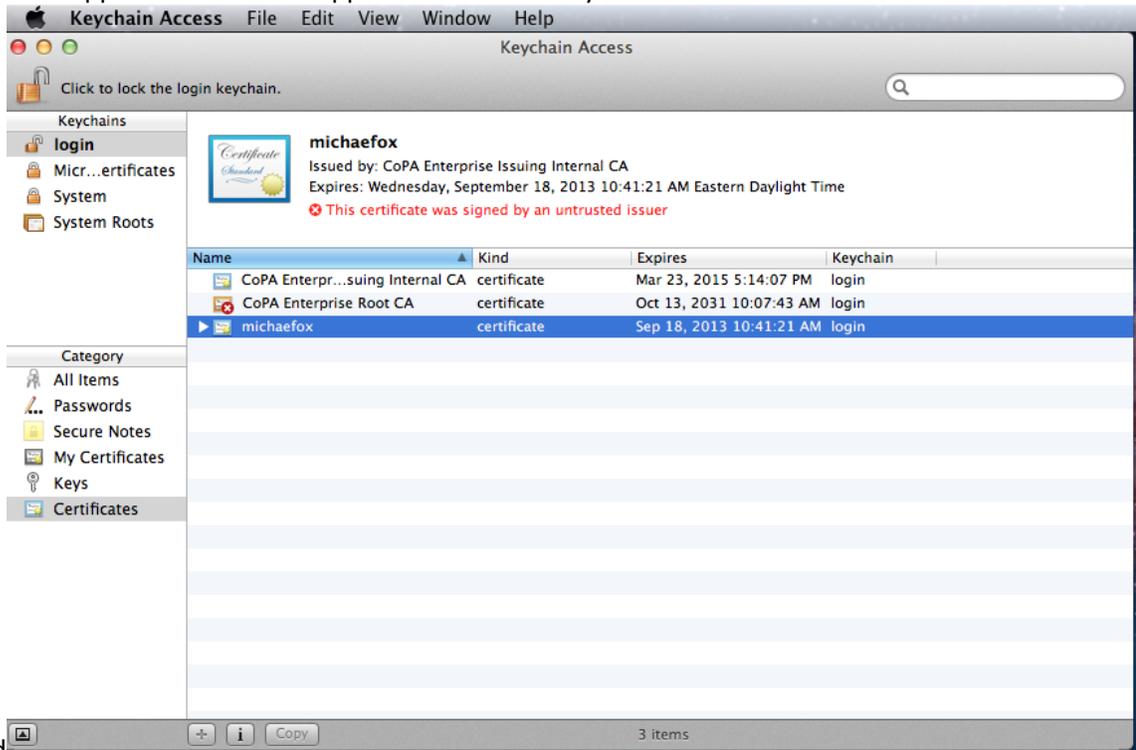
Copy your Certificate to your desktop with either a USB key or another method:



Double Click your Certificate which will usually be your username.PFX and then enter your certificate password when prompted



The Keychain application will then appear and show that your certificates have been



installed

Open Safari or whatever Internet browser you have installed on your Mac and connect to <https://moose.pa.gov>. Sign in with your CWOPA credentials



**Welcome to the
COPA Secure Access SSL VPN**

Username Please sign in to begin your secure session.
Password
Realm

The site will then redirect to installing the network connect service and once connected you will see the following screen.

