Making your Medium-Token Assurance Certificate Request with Mozilla Firefox

IMPORTANT: These instructions are written step-by-step; do not perform an action before the instructions tell you to do so.

Before you make your certificate request via Firefox you must already have performed the following procedures:

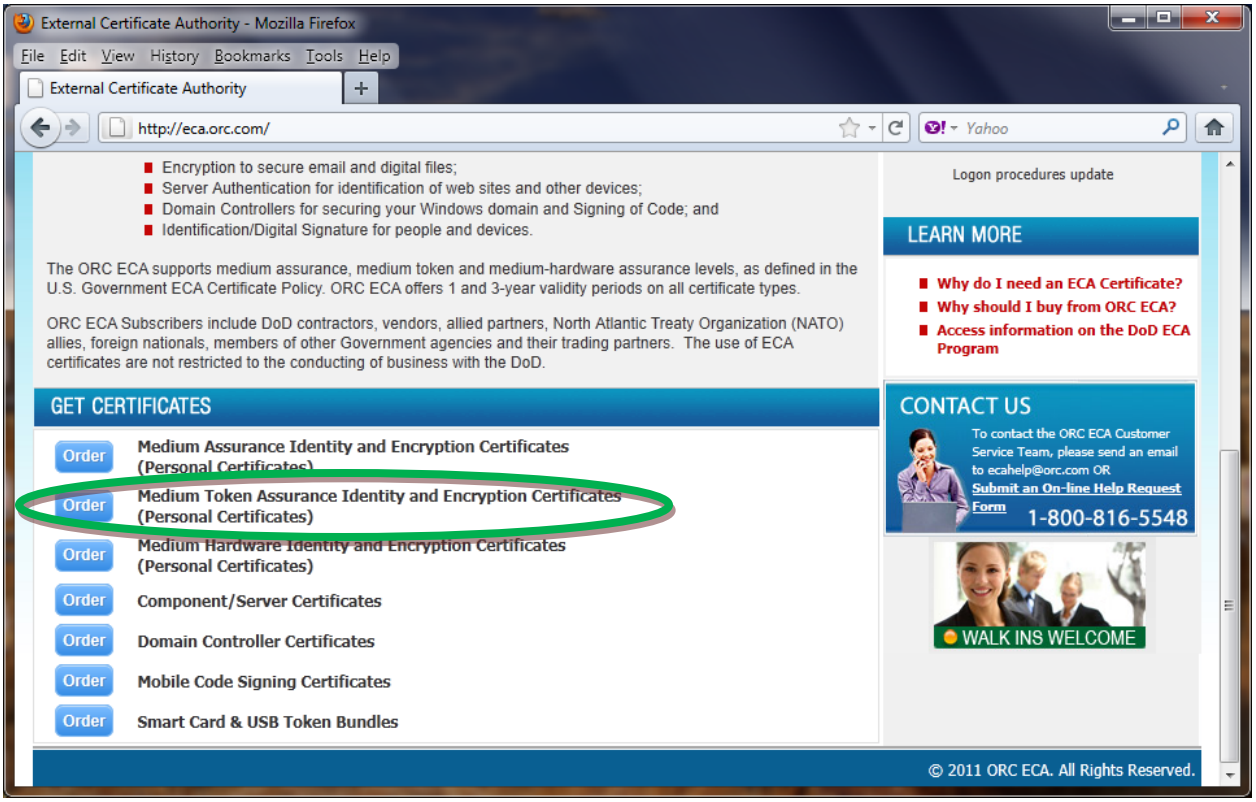
- Successfully installed the ActivCleint software and re-started your computer
- Initialized (set a PIN) on your smart card or ActivKey SIM Token
- You must be logged onto your computer under your normal user profile (or Username) [Your IT support person may have had to log-on as the Administrator to install Firefox or ActivClient; but the we want the user logged on now, not the Administrator.]

Please Note: Making the certificate request via Mozilla Firefox will not prevent nor impede your use of the certificates in Microsoft Internet Explorer (or other Microsoft application). On the contrary, Firefox generally performs certificate request functions in a 'cleaner' manner than the Microsoft operating system. When the entire certificate issuance process is complete, your certificates will be available in both Firefox and Microsoft.

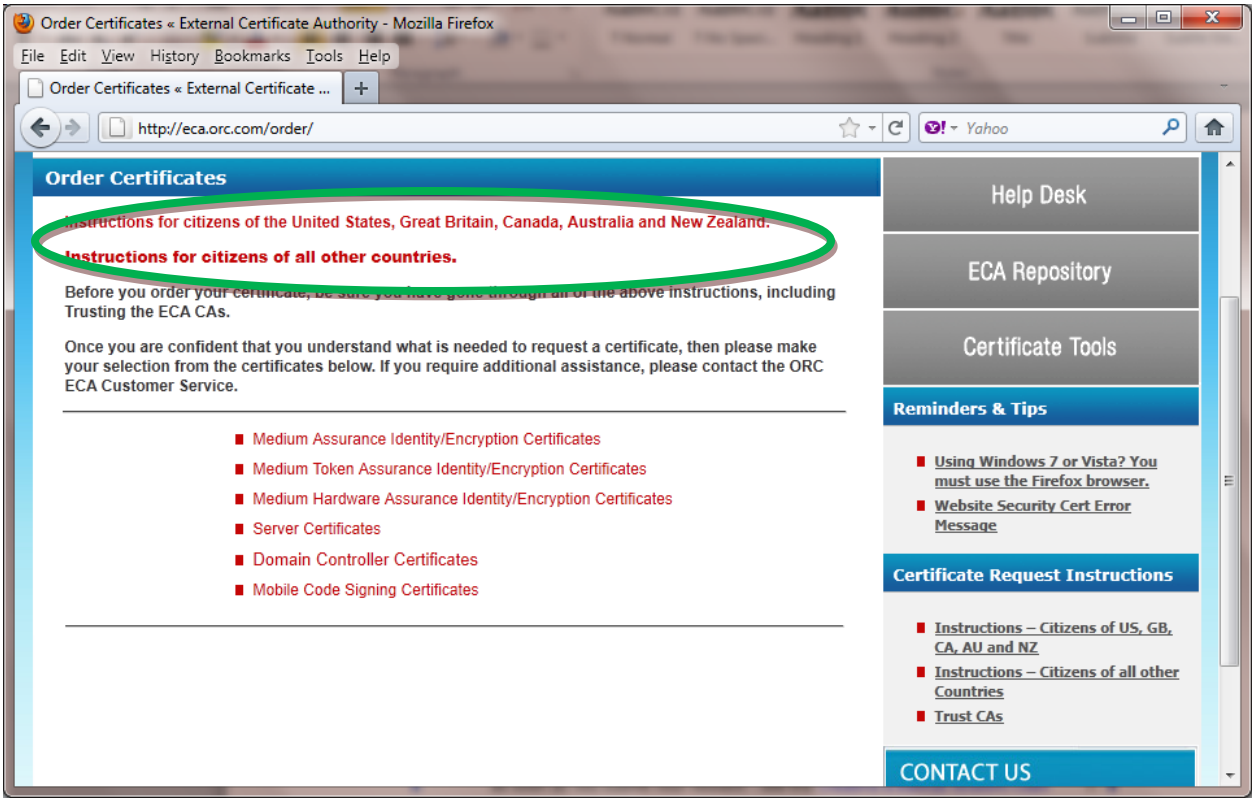
Connect your smart card reader and slide you card into the reader (chip up and in) or plug your ActivKey SIM token into a USB port.

1. Start Firefox and go to: http://eca.orc.com

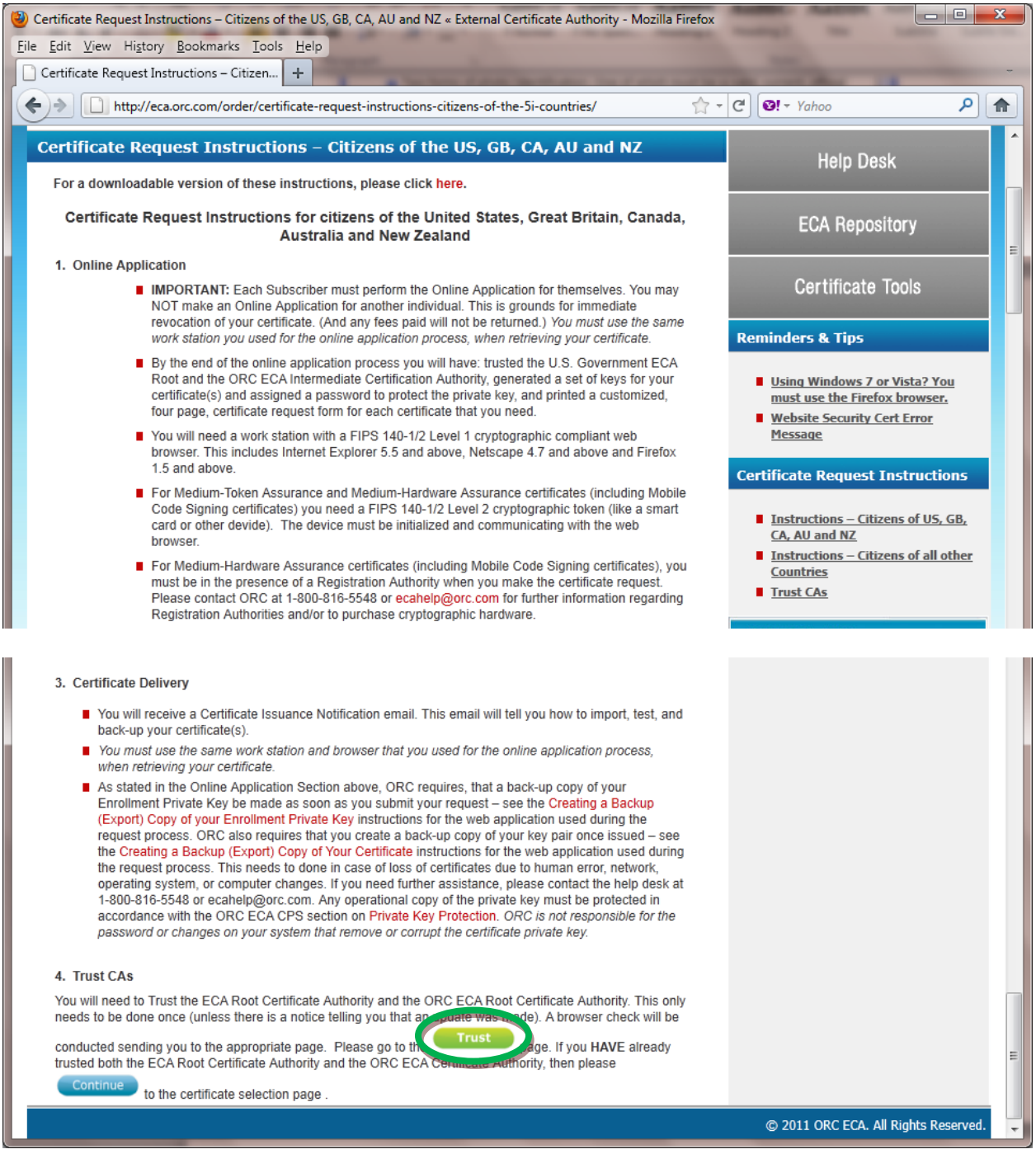
2. Scroll down and click the "**Order**" button for Medium-Token Assurance Certificates



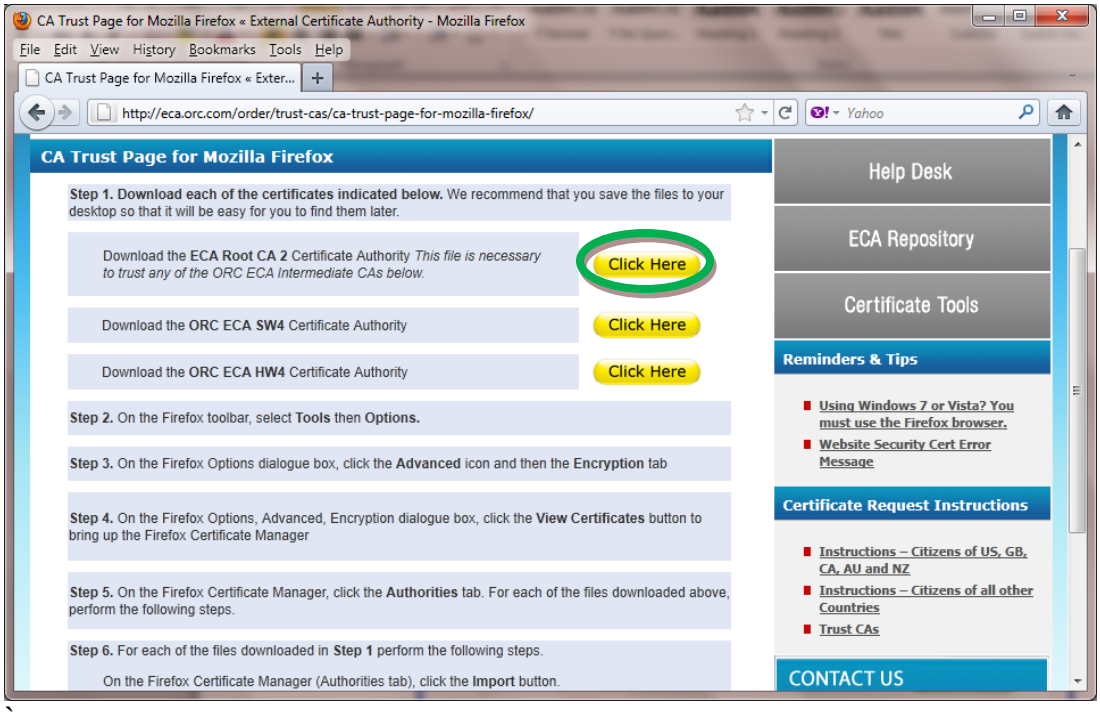
3. Read the appropriate instructions depending on your citizenship



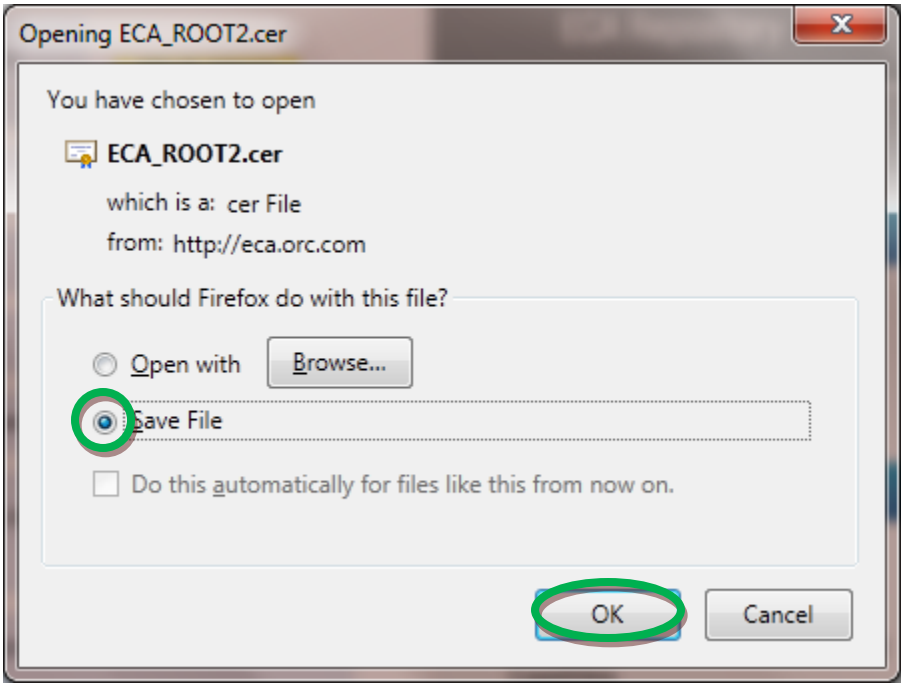
4. Read the Certificate Request Instructions page and click the **Trust** button



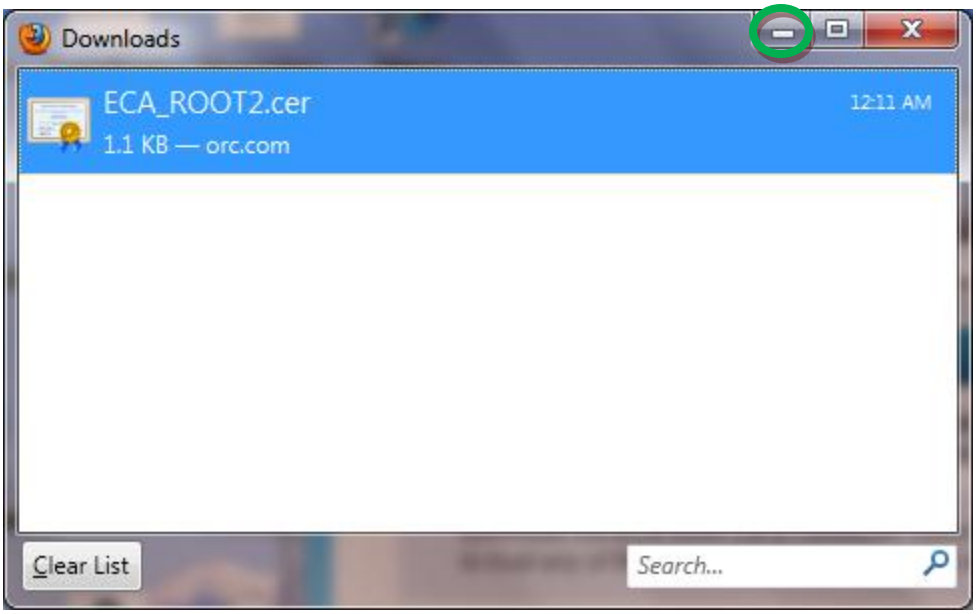
5. On the CA Trust page for Mozilla Firefox page… (This section executes the instructions as indicated on the web page.)
    a. Download all 3 files indicated in **Step 1** on the page by clicking on the **Click Here** button



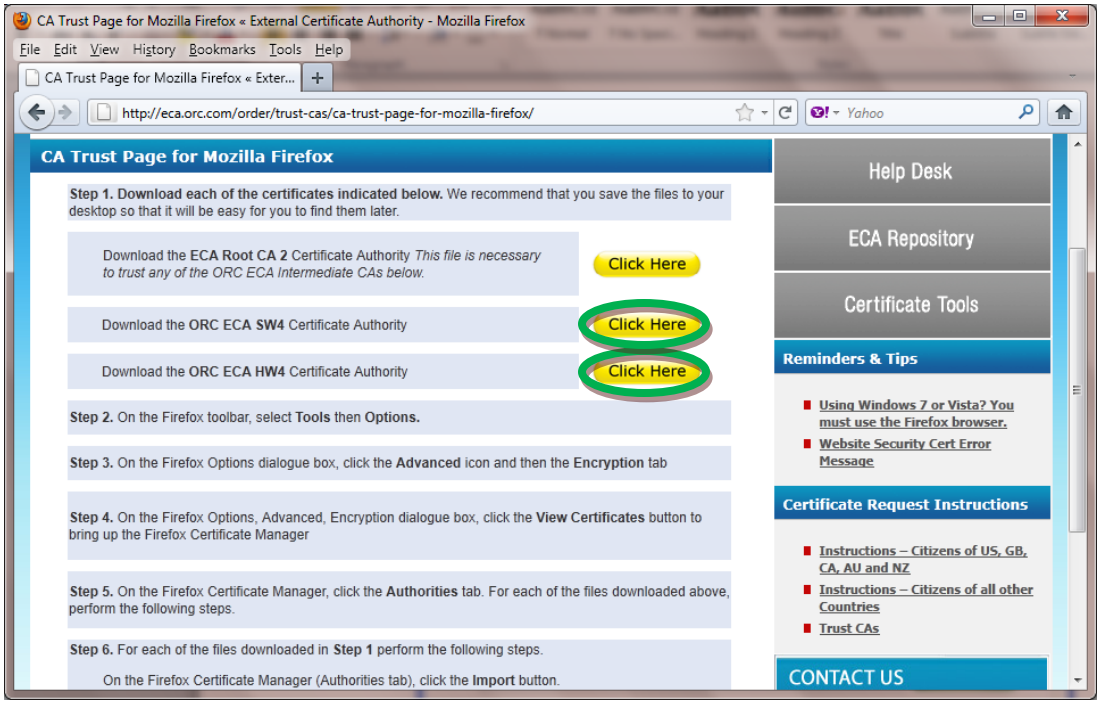
    b. This should bring up the following dialog box, select **Save File** and click the **OK** button



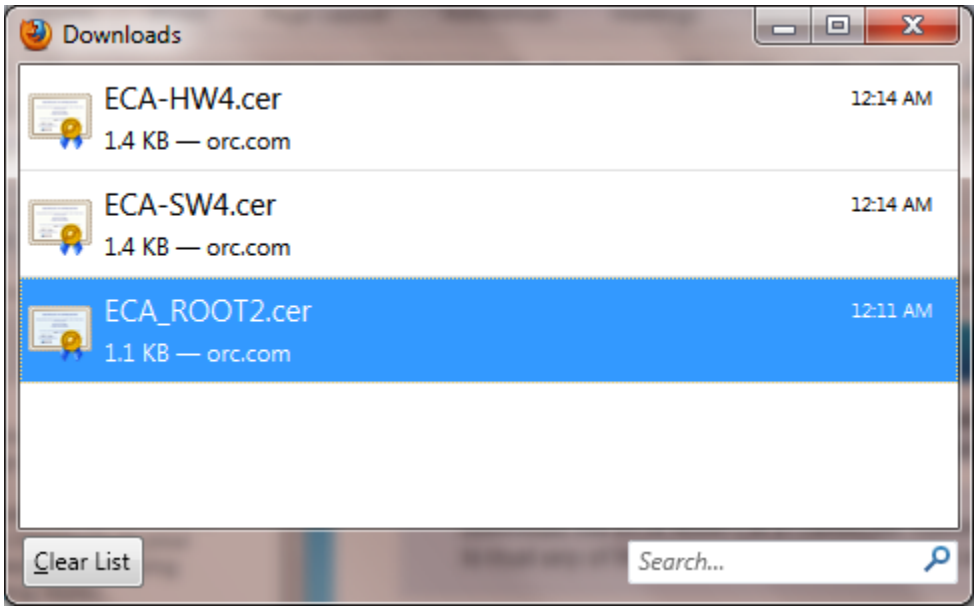
c. This should bring up the Firefox Downloads dialog box. (Note: You do not need to do anything in this box, it is just informing you that Firefox is downloading files.) Minimize the Downloads dialog box.



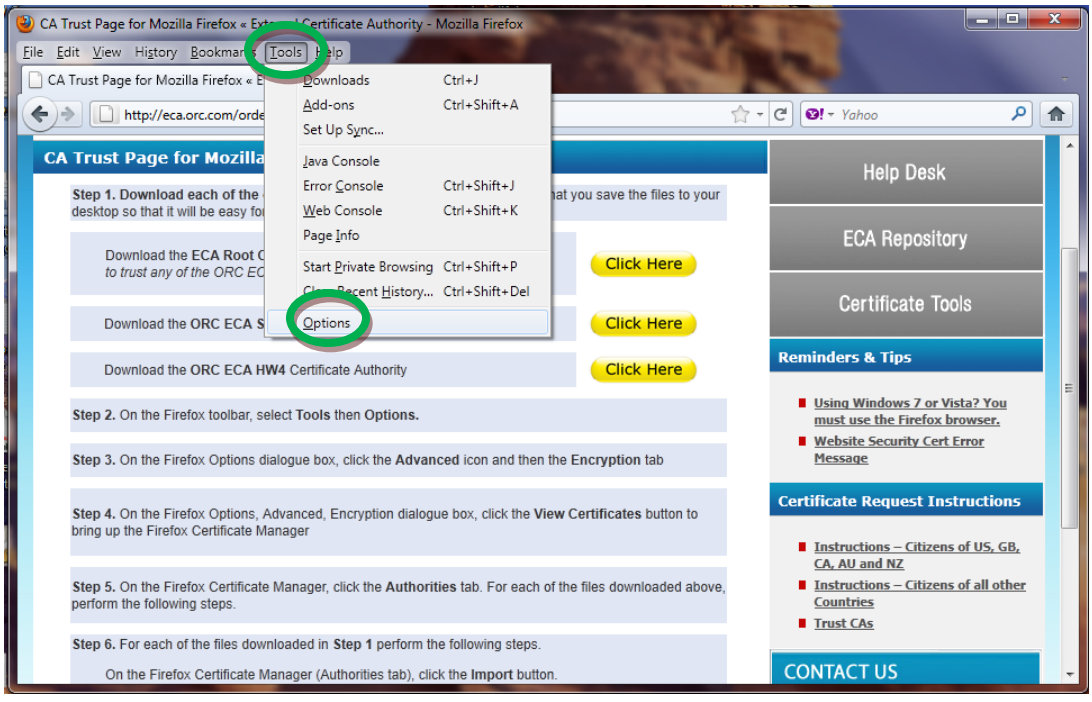
d. Go back to the web page and download the other two files indicated in Step 1.



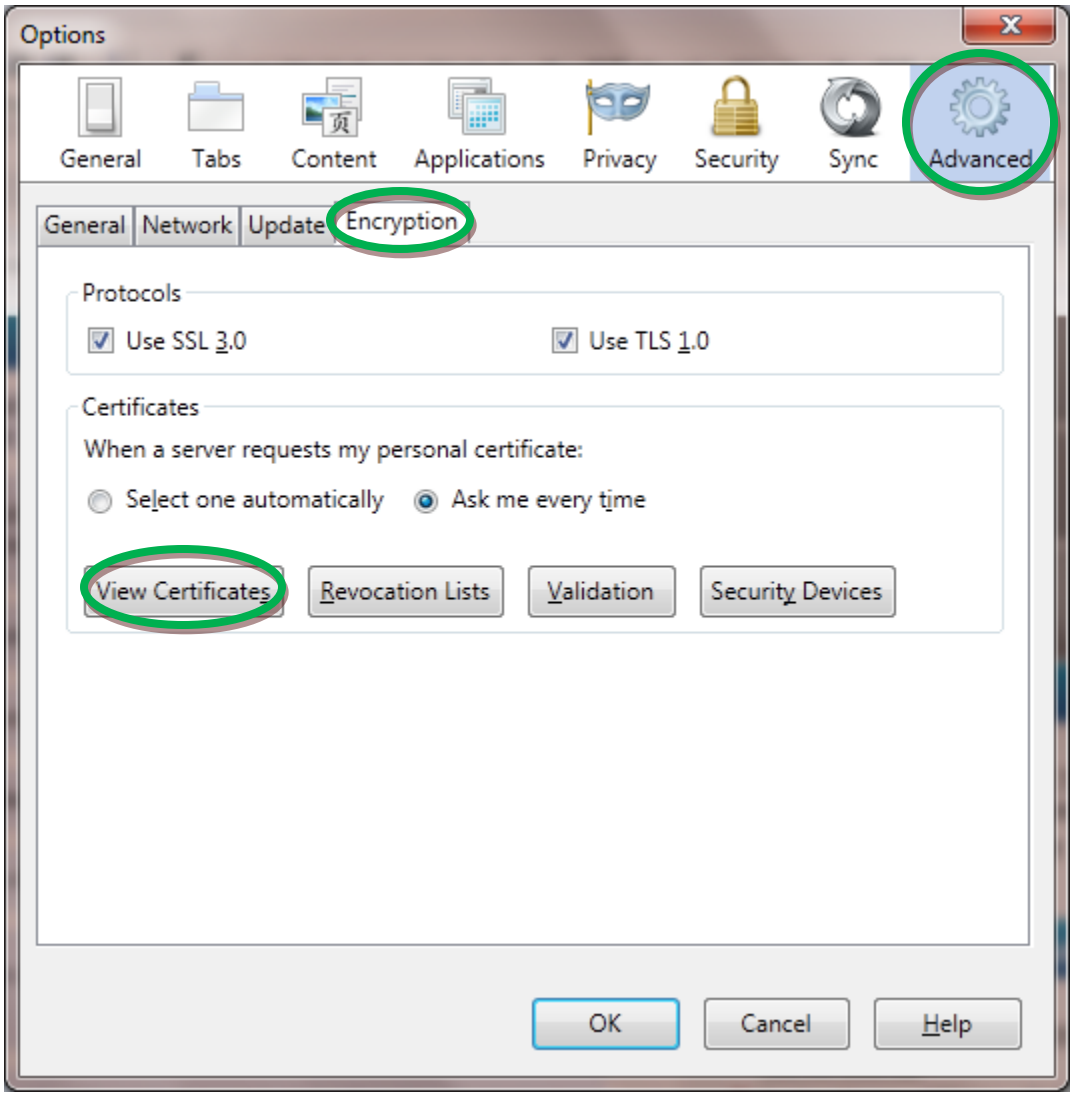
e. Look at the Firefox Downloads dialog box. (It should look something like this.)



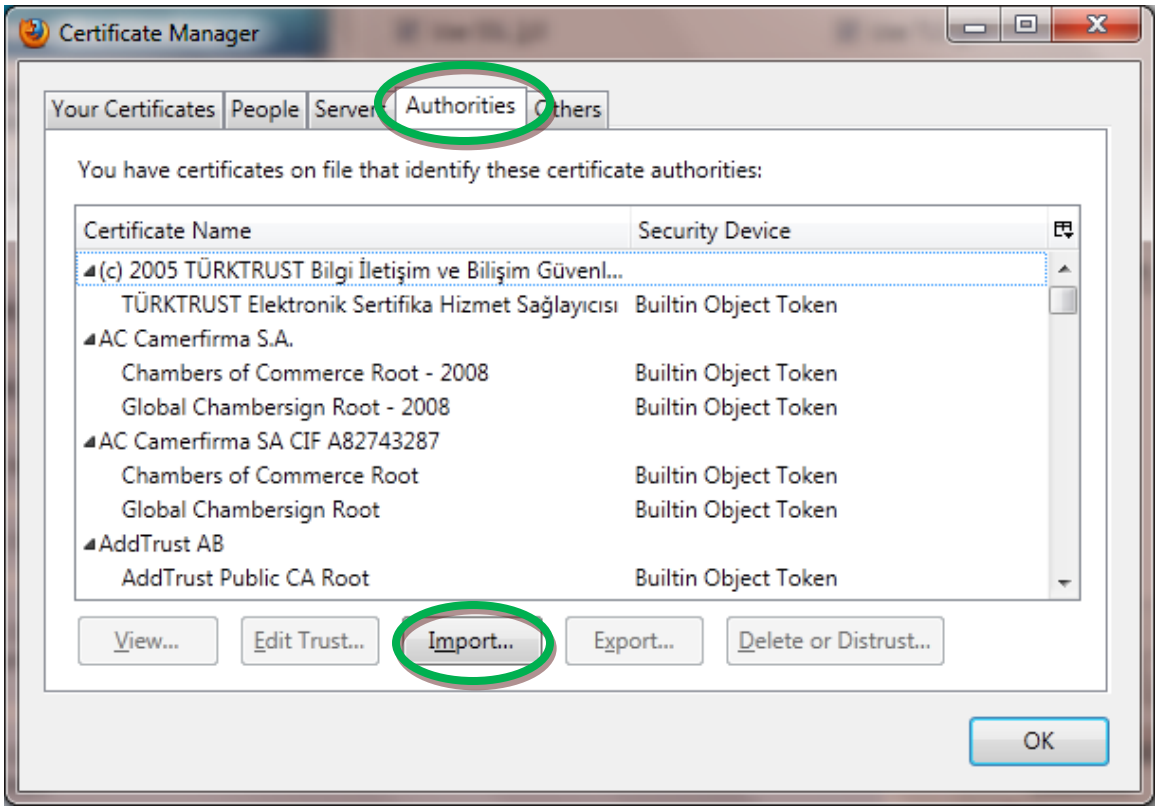
f. On the Firefox toolbar, select **Tools** then **Options...**



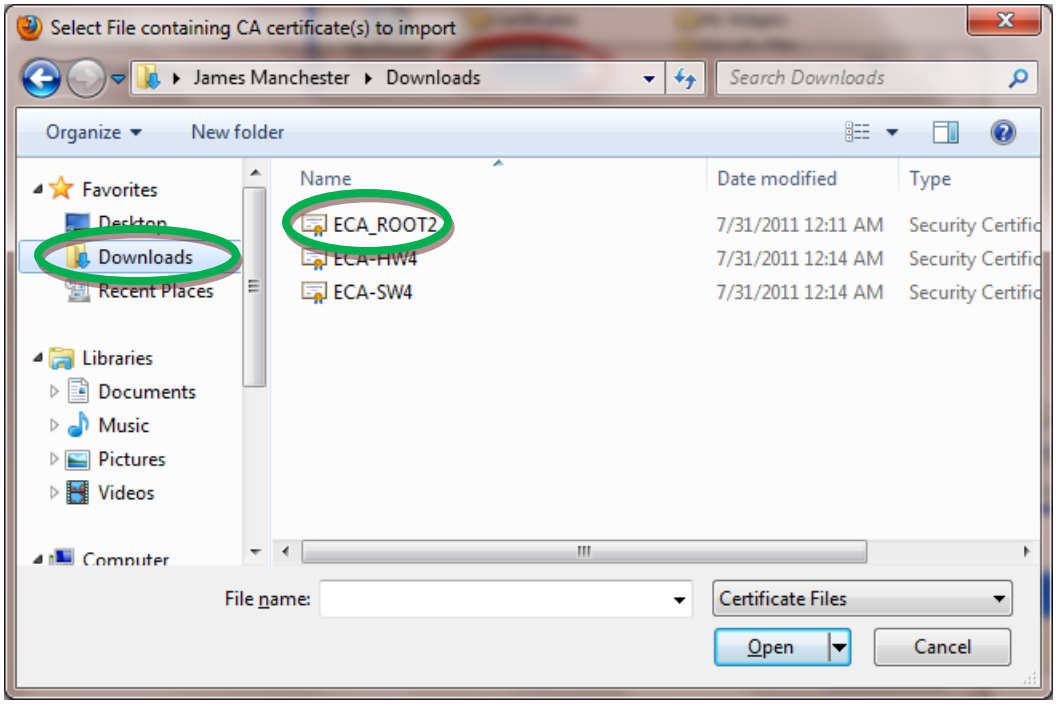
g. On the Firefox Options dialogue box, click the **Advanced** icon and then the **Encryption** tab, then click the **View Certificates** button



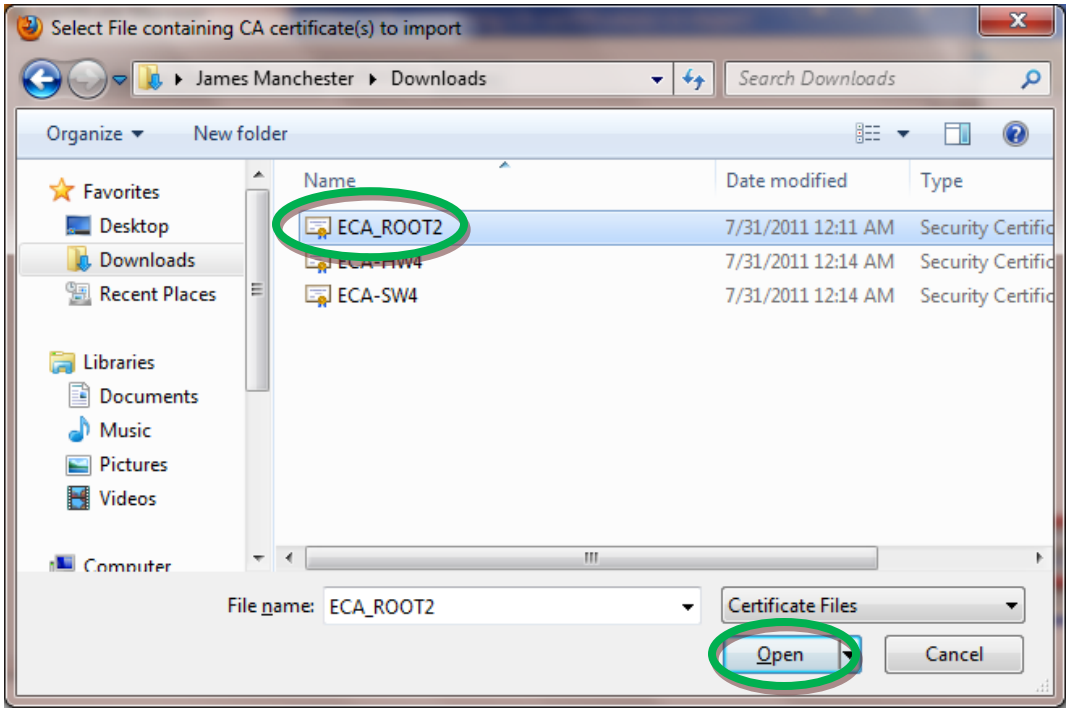
h. In the Firefox Certificate Manager, click the **Authorities** tab, then click the **Import** button



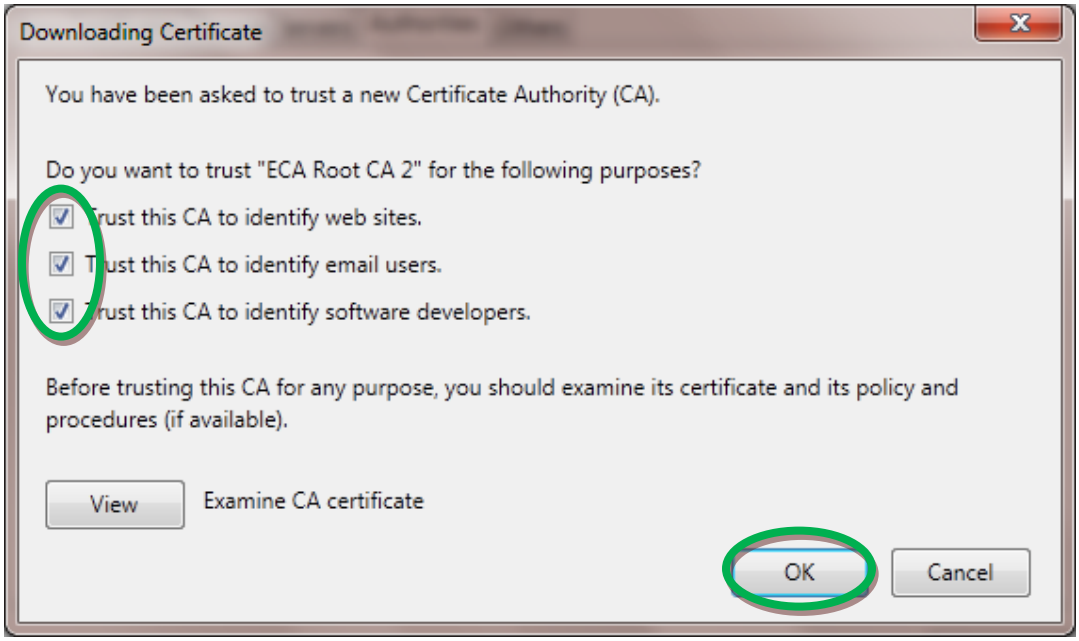
i. In the Select File containing CA certificate(s) to import dialogue box, navigate to the location where you saved the imported ".cer" files from above. (If the files are not in the location shown in the screenshot perform a search on your computer for files named "*.cer" to find out where the files were saved.)



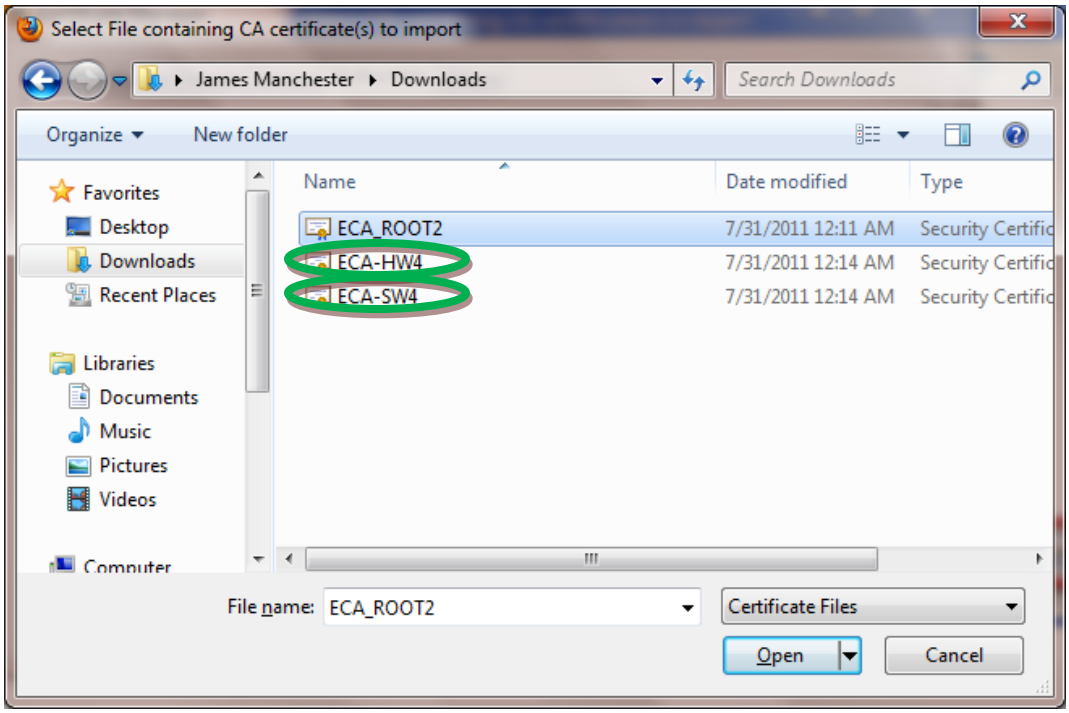
j. Select the file named "**ECA-ROOT2.cer**" and click the **Open** button



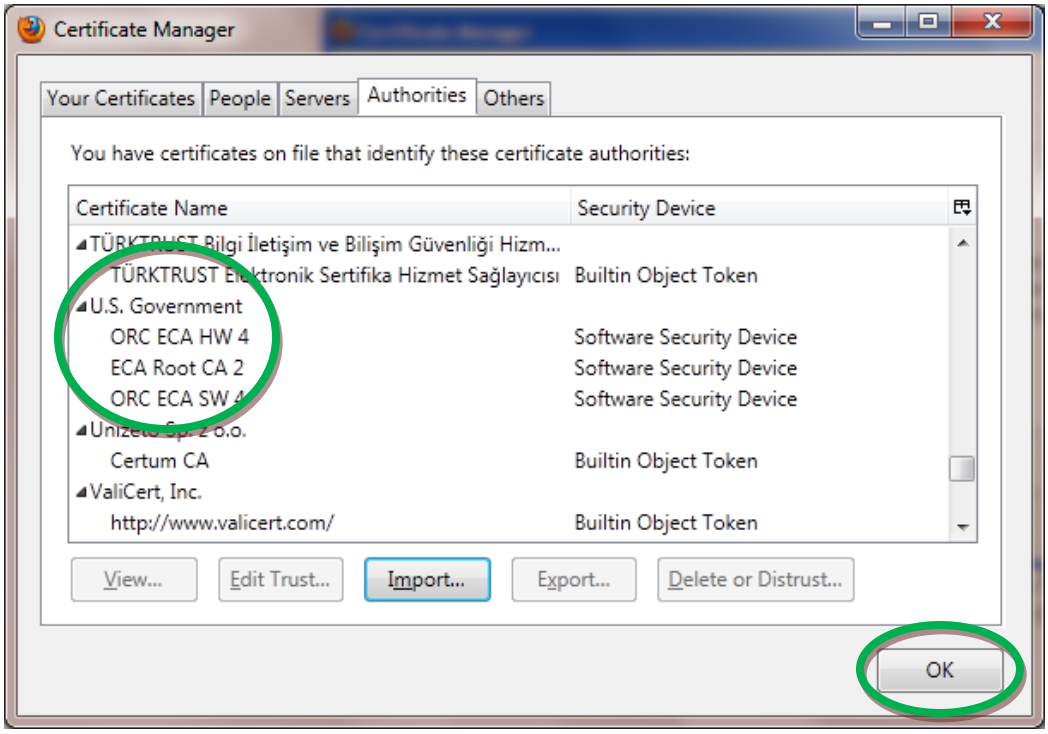
k. Check all three (3) check boxes and click the OK button



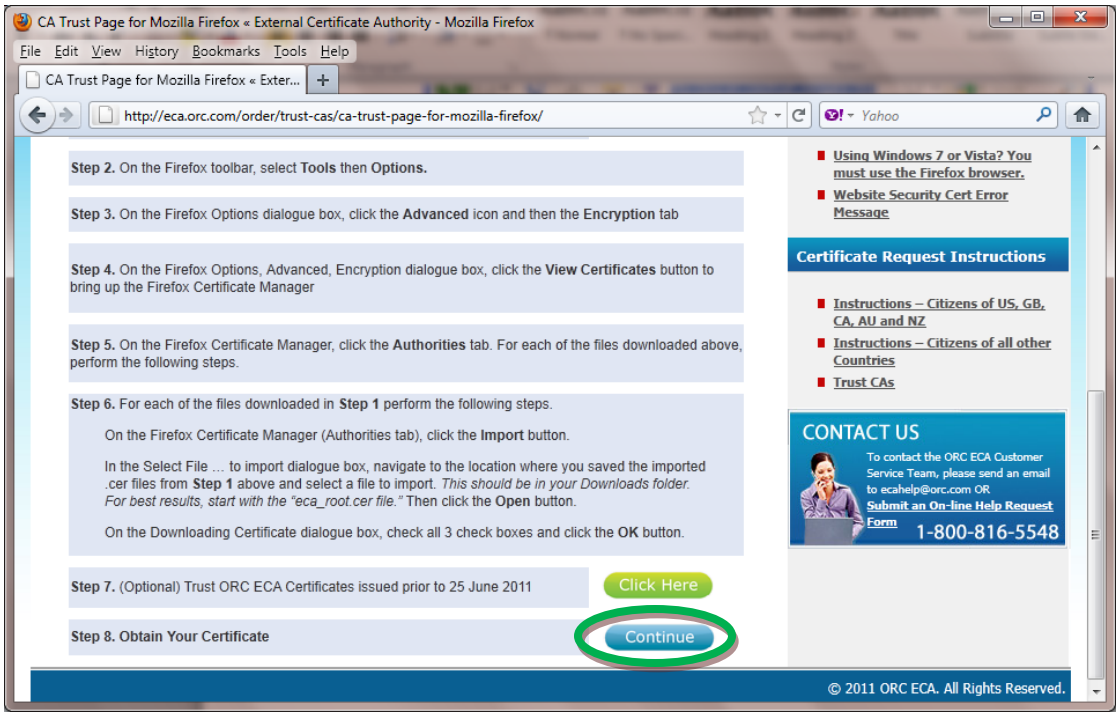
l. Then in the Firefox Certificate Manager, perform the exact same function for the other two files.



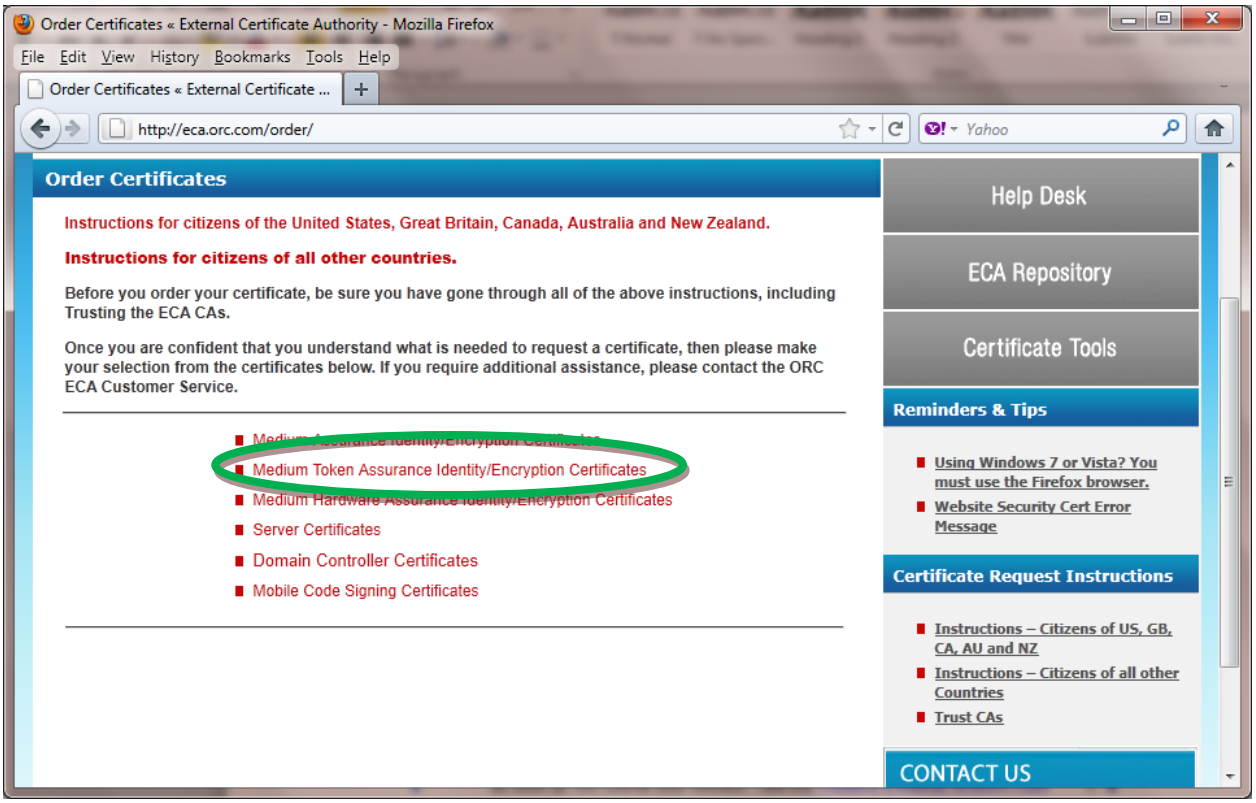
m. When you are done, you should see something like this in the U.S. Government section in the Firefox Certificate Manager – Authorities. Click the **OK** button.



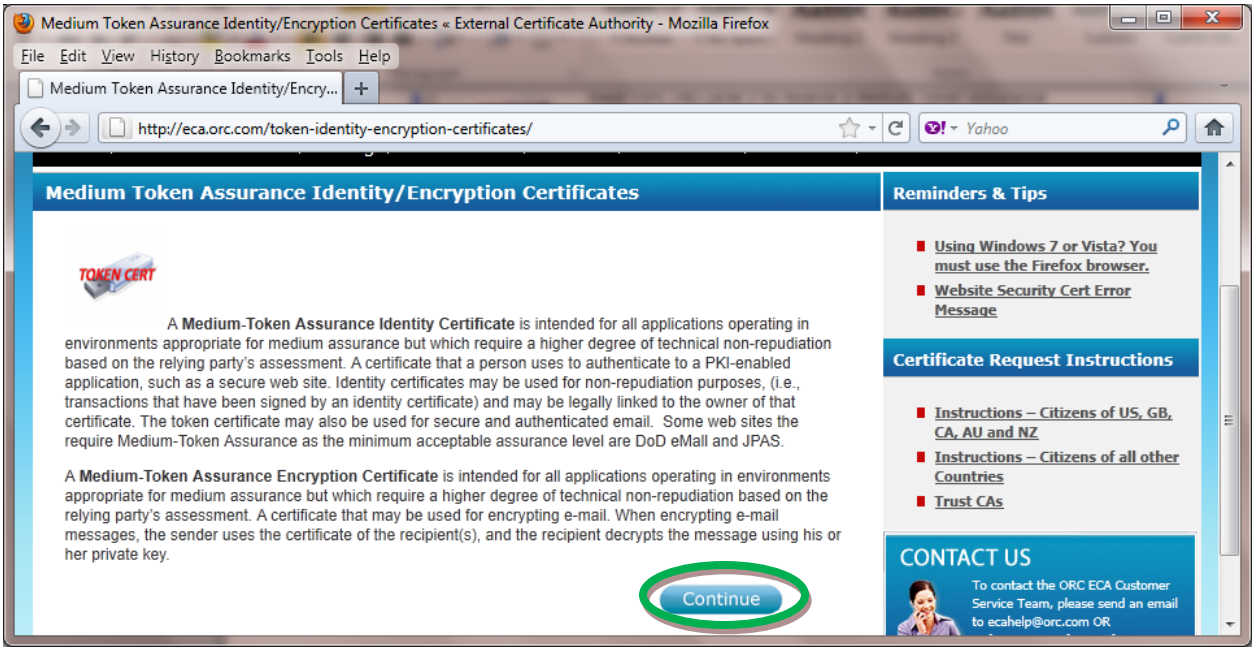
n. Back on the Trust the Root Certificate Authority web page, scroll down to Step 8 and click the "**Click Here**" button



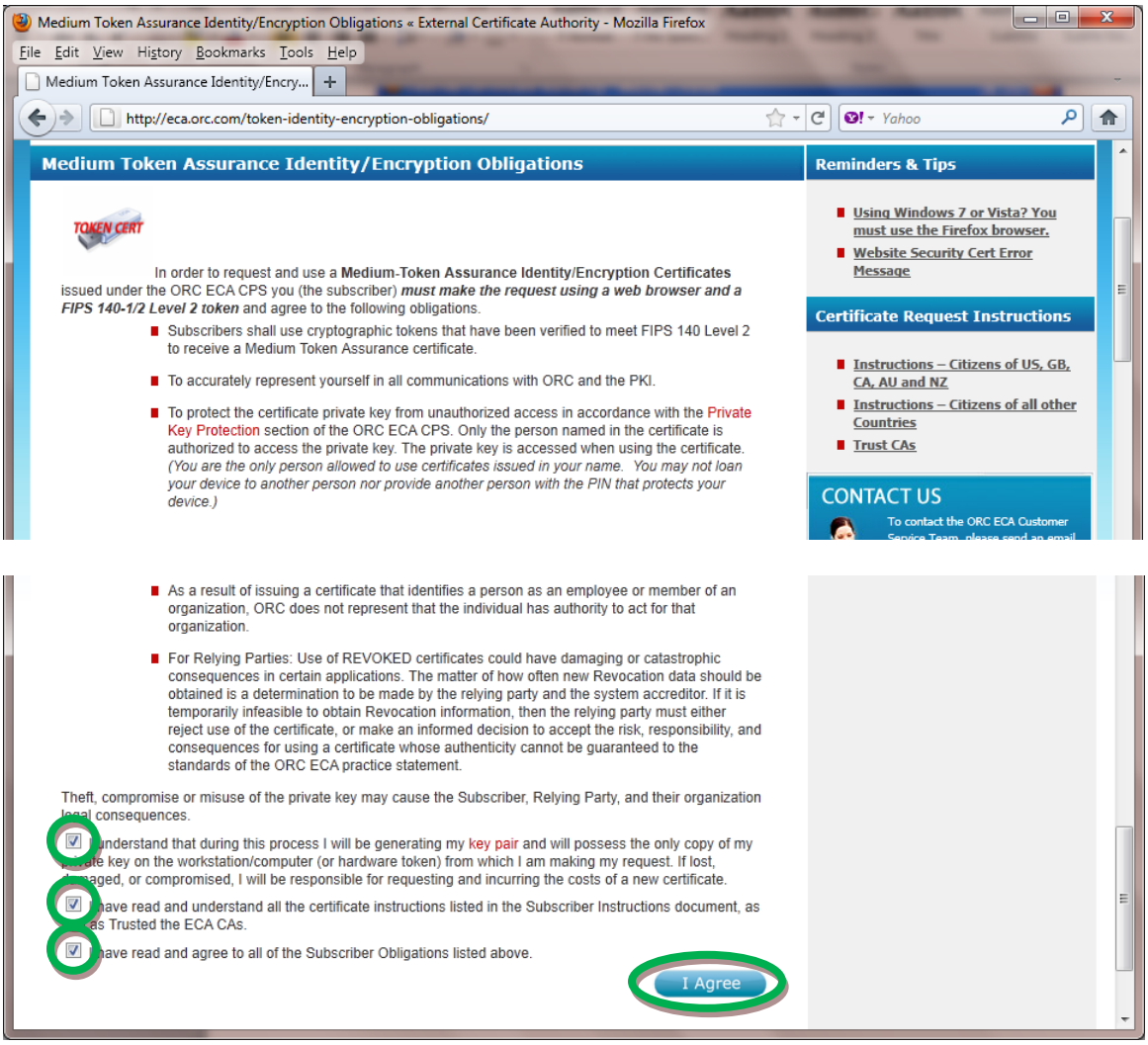
6. Back on the Order Certificates page, select a click the Medium-Token Assurance Identity/Encryption Certificate



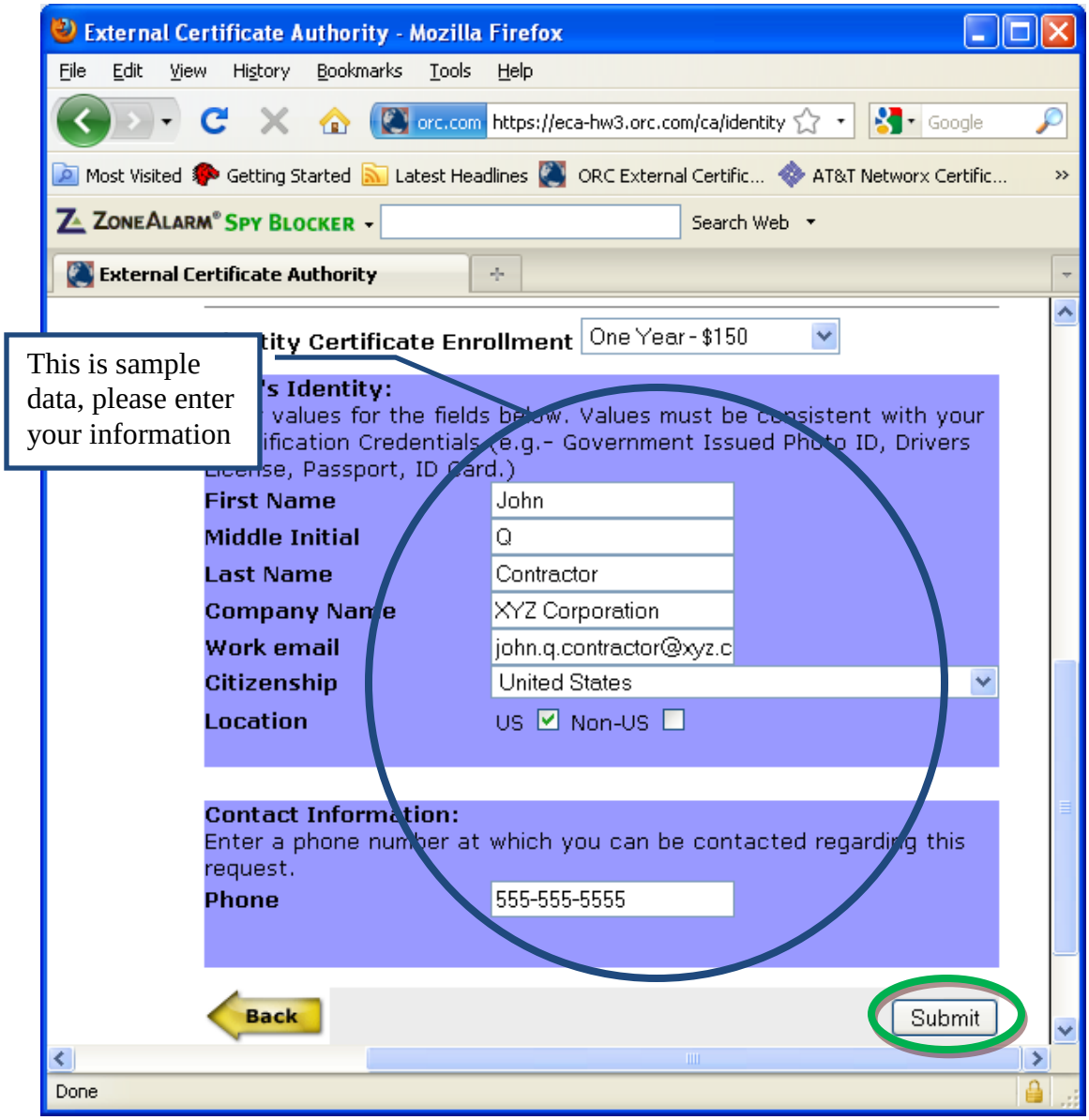
7. On the Medium-Token Assurance Identity/Encryption Certificates page



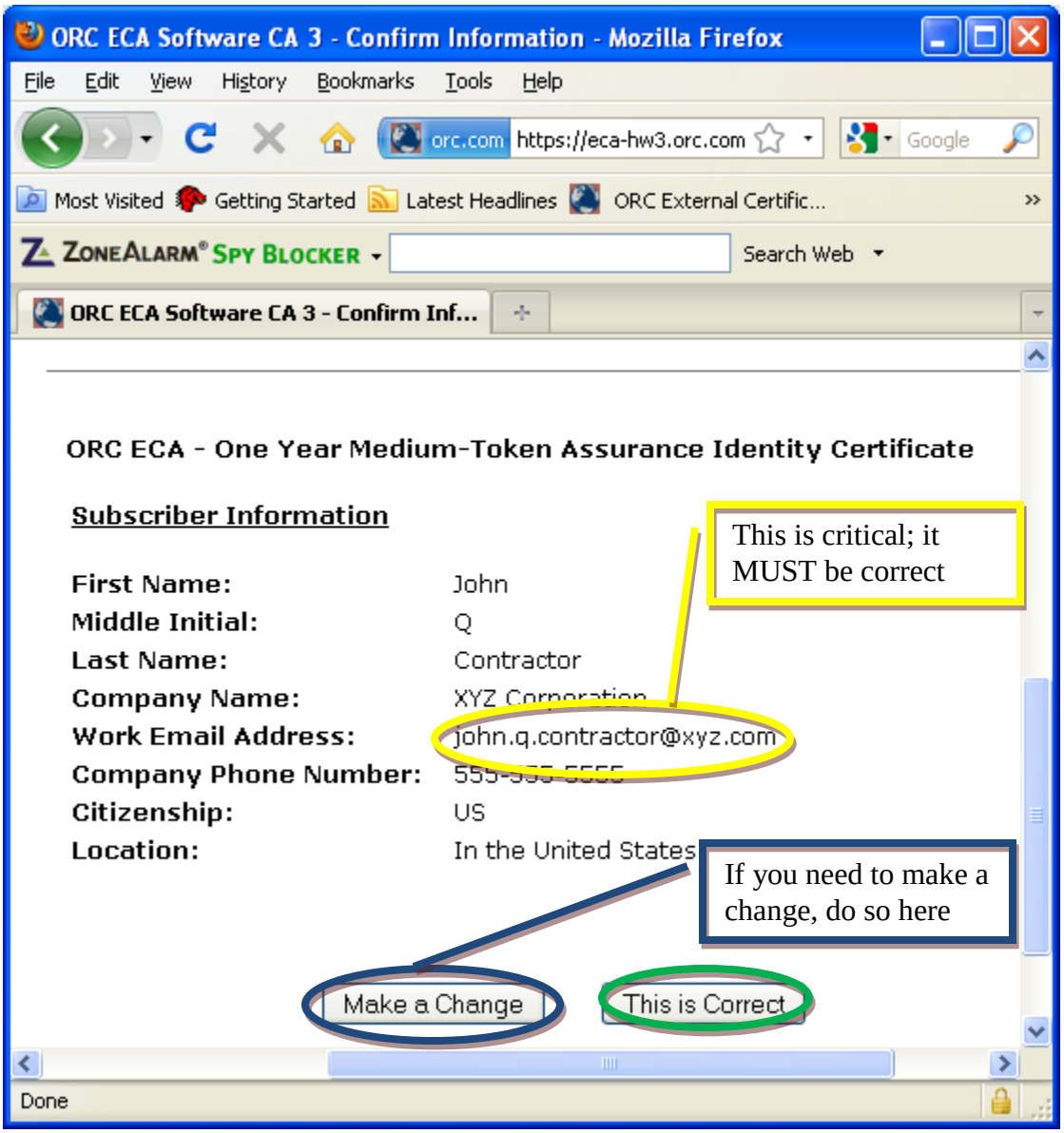
8. On the Medium-Token Assurance Identity/Encryption Certificates Subscriber Obligations page, read the obligations and click **I Agree**. Understand that the most important obligation is <u>that only the named individual is authorized to use the certificate</u>. You may not request a certificate for someone else and you may not allow someone else to use your certificate.



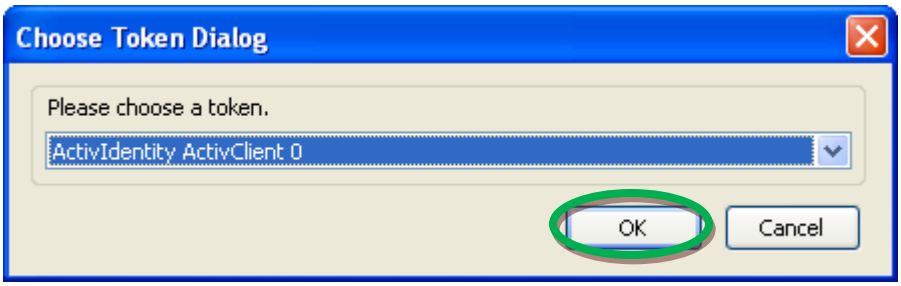
9. On the application page, select the desired Validity Period (1 or 3 Years) enter your name, company name, the email address that you use at work, your citizenship, and your phone number at work. Then click the **Submit** button



10. On the Confirm Information page, double check your information, make any changes if necessary and then click **This is Correct** (NOTE: If you make a mistake and ORC has to re-issue your certificate with at correction; you will be charged again to fix your mistake.)

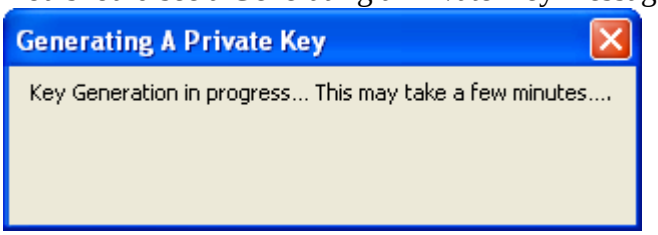


11. When you get the Choose Token Dialog, ensure that it is set to ActivIdentity and click **OK**

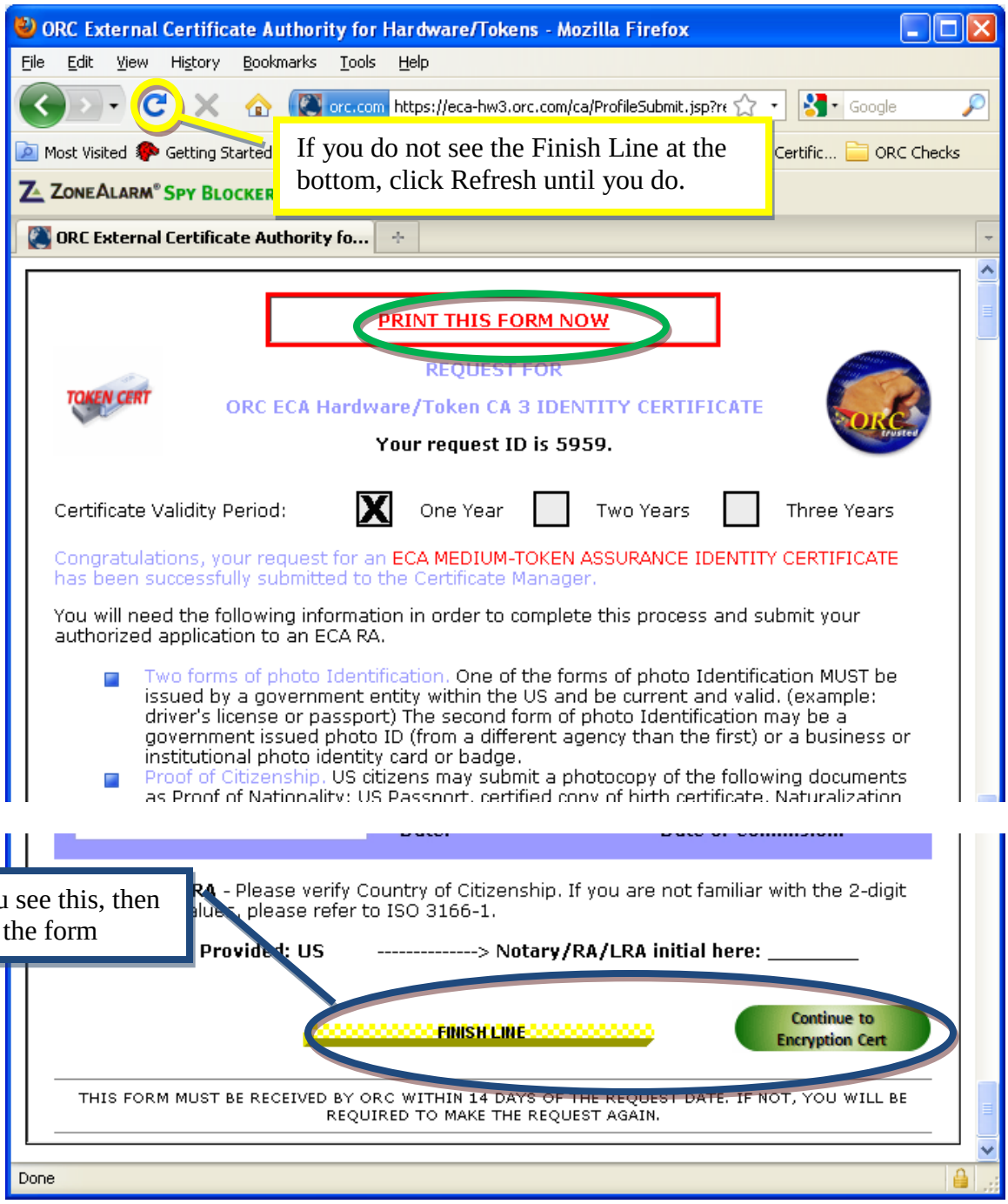


12. ActivClient should then prompt you to enter the PIN for the device. (You might not be prompted if you have entered the PIN within the last few minutes.) Enter the PIN that you have set on the device.

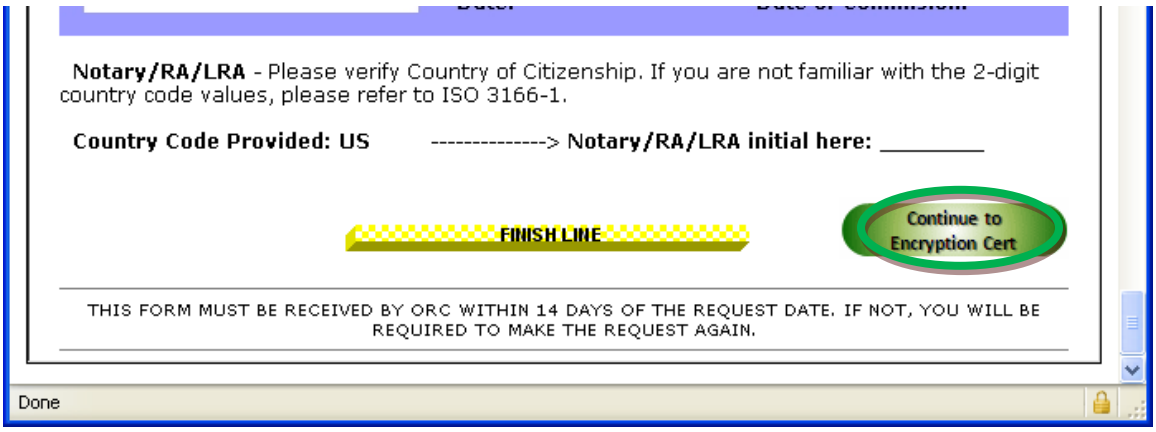
13. You should see a Generating a Private Key message. This will take a few minutes.



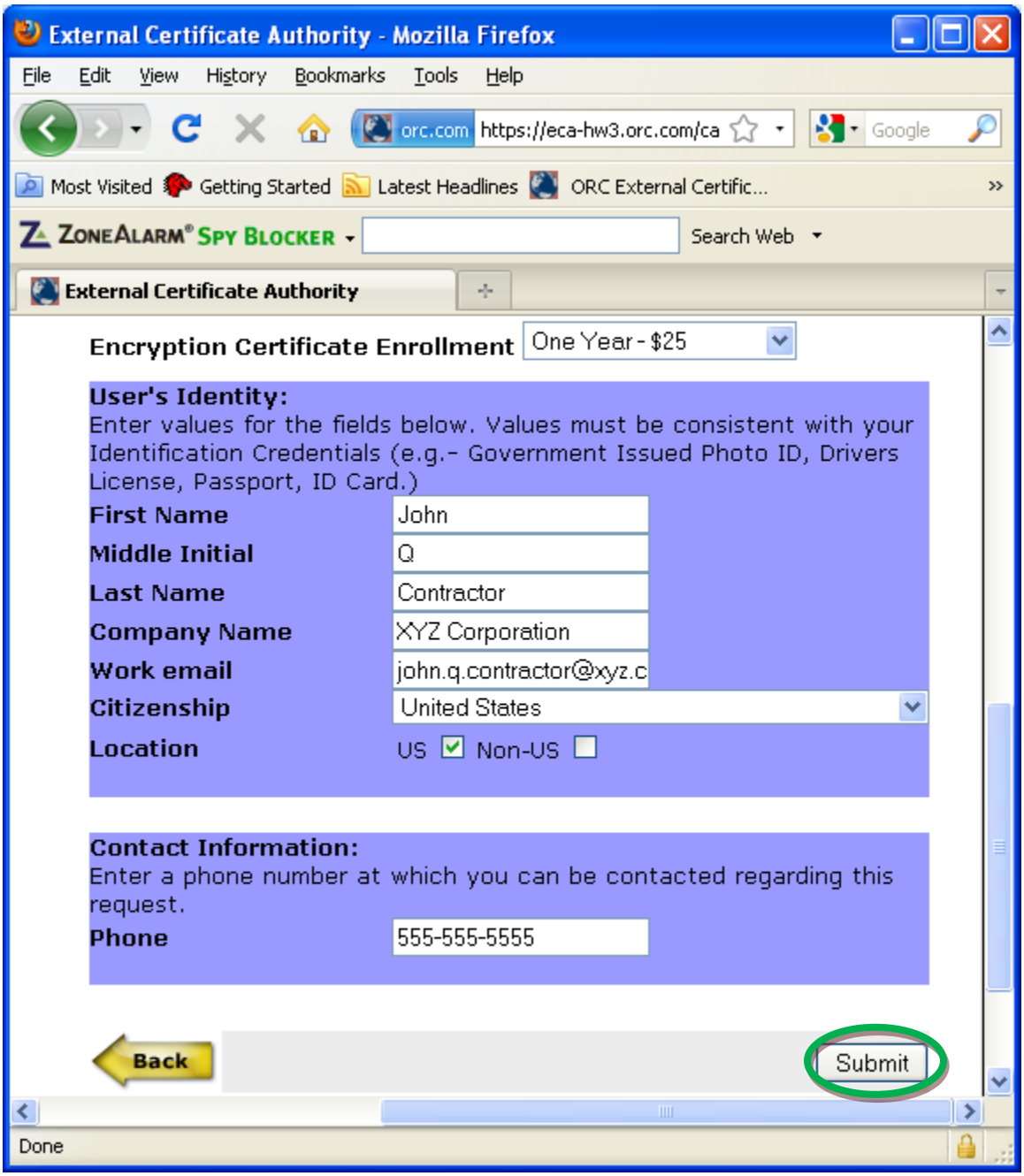
14. When key generation has been successful, you should see a web page that says "PRINT THIS FORM NOW." Print the request form; it should be 4 pages with a Finish Line at the bottom of the form. (If you do not see the Finish Line or a Green button at the bottom, click your refresh/reload button until you do.)



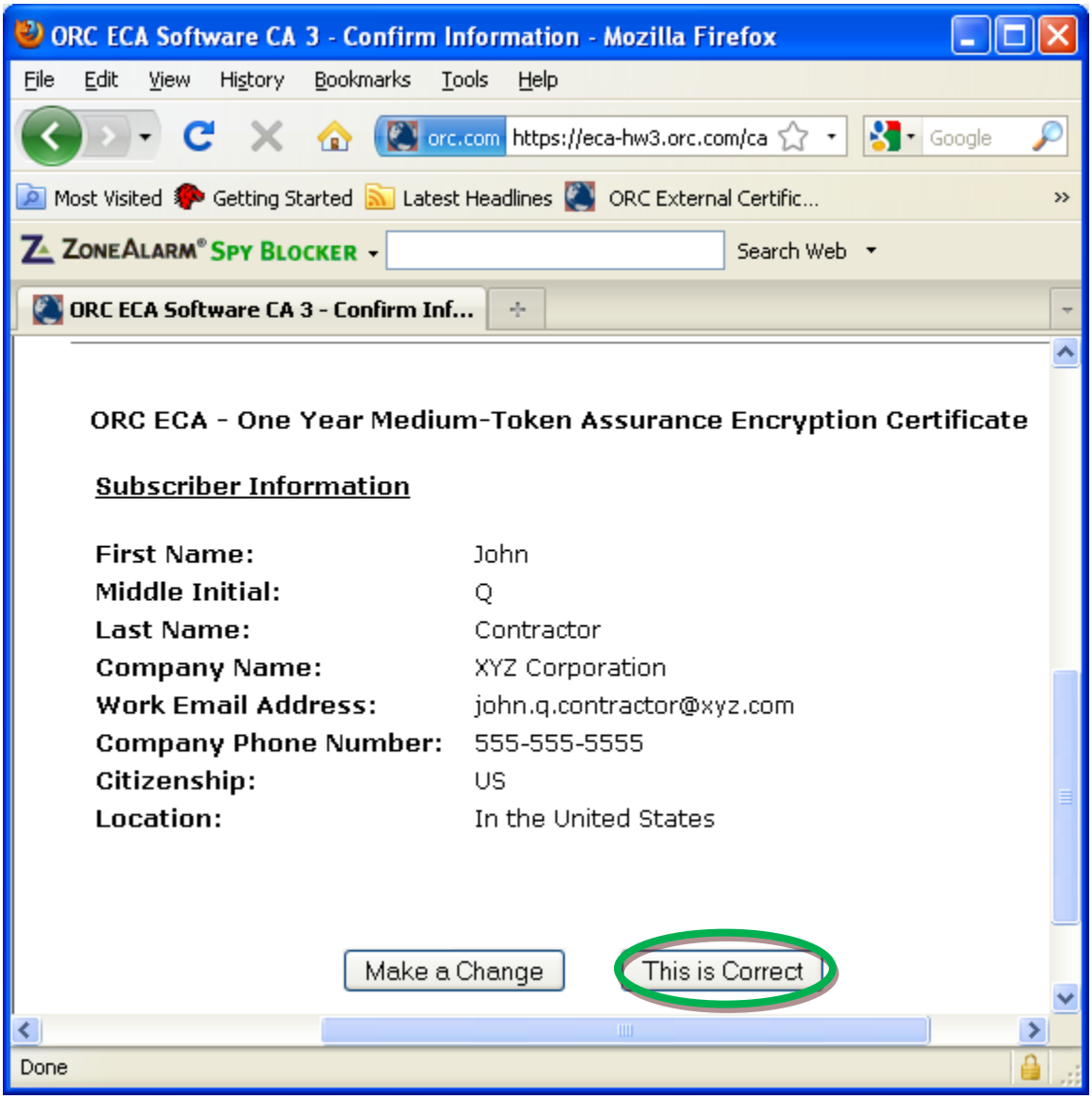
15. After you have printed the form, click the Continue to Encryption Cert button



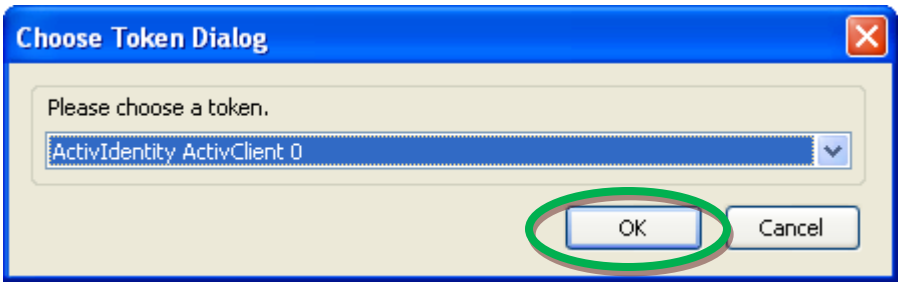
16. On the Encryption Certificate application page, the data should all be the same, click the **Submit** button



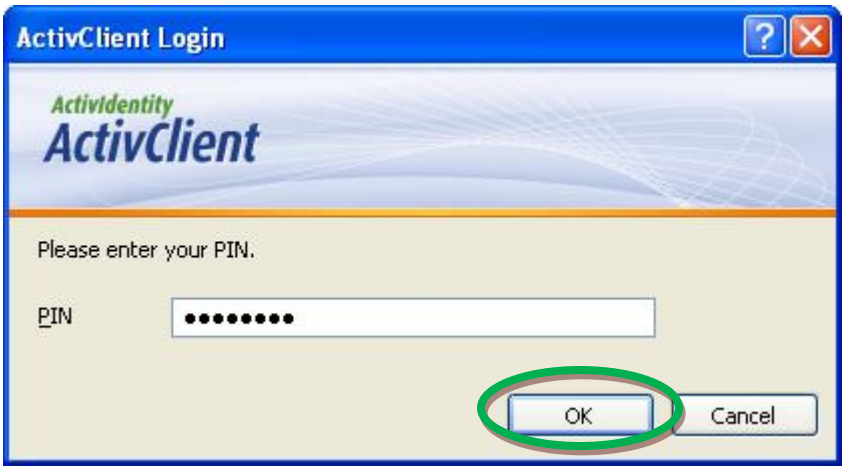
17. On the Confirm Information page, double check your information again. (NOTE: If you see a problem, it means that you made a mistake when you made your Identity Certificate Request; go back and make a new Identity Certificate Request.) Make any changes if necessary and then click **This is Correct** (NOTE: If you make a mistake and ORC has to re-issue your certificate with at correction; you will be charged again to fix your mistake.)



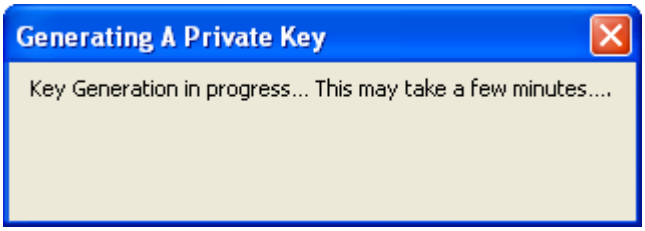
18. When you get another Choose Token Dialog, ensure that it is set to ActivIdentity and click **OK**



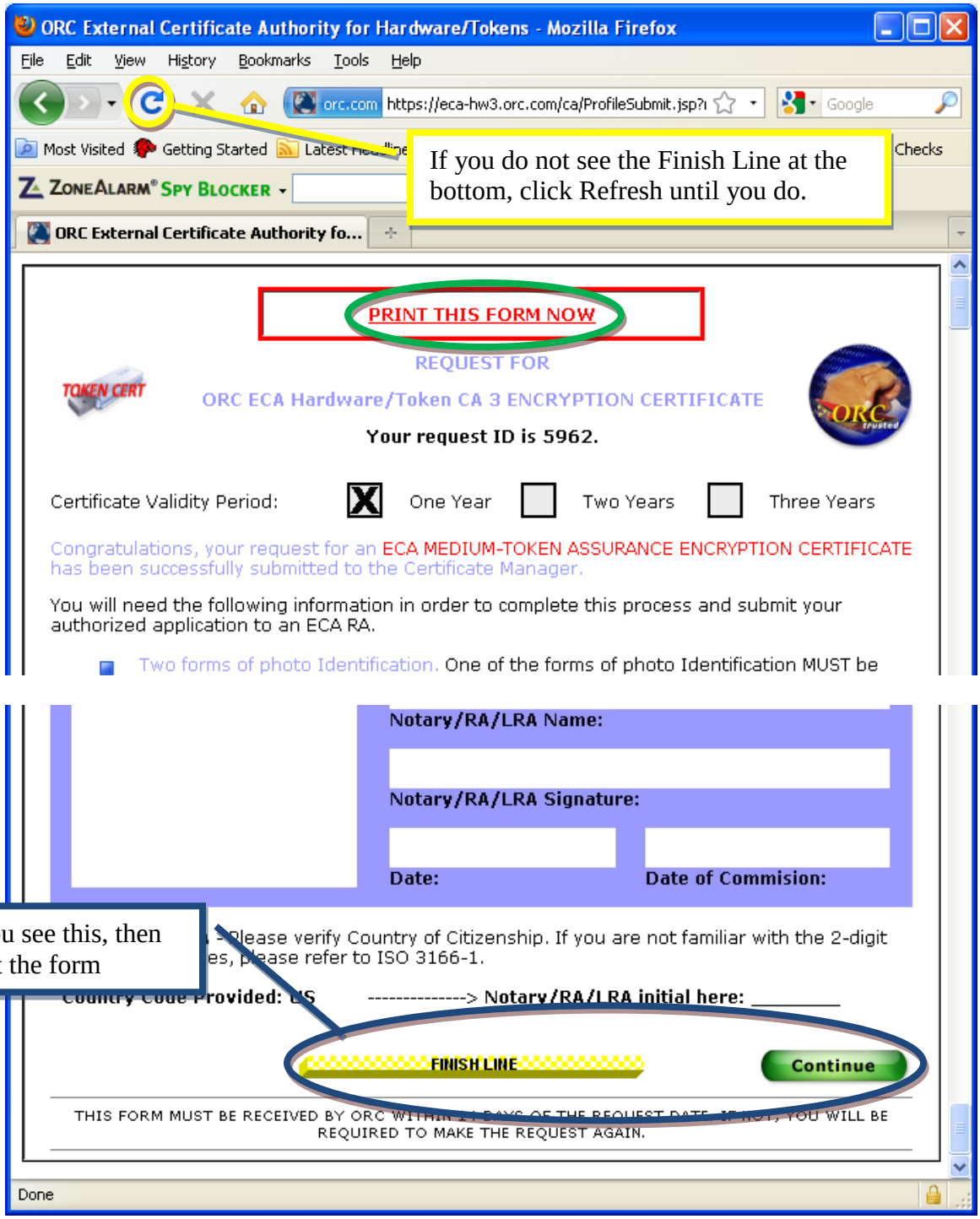
19. ActivClient might (or might not) prompt you to enter the PIN for the device. Enter the PIN



20. You should see another Generating a Private Key message. This will take a few minutes.

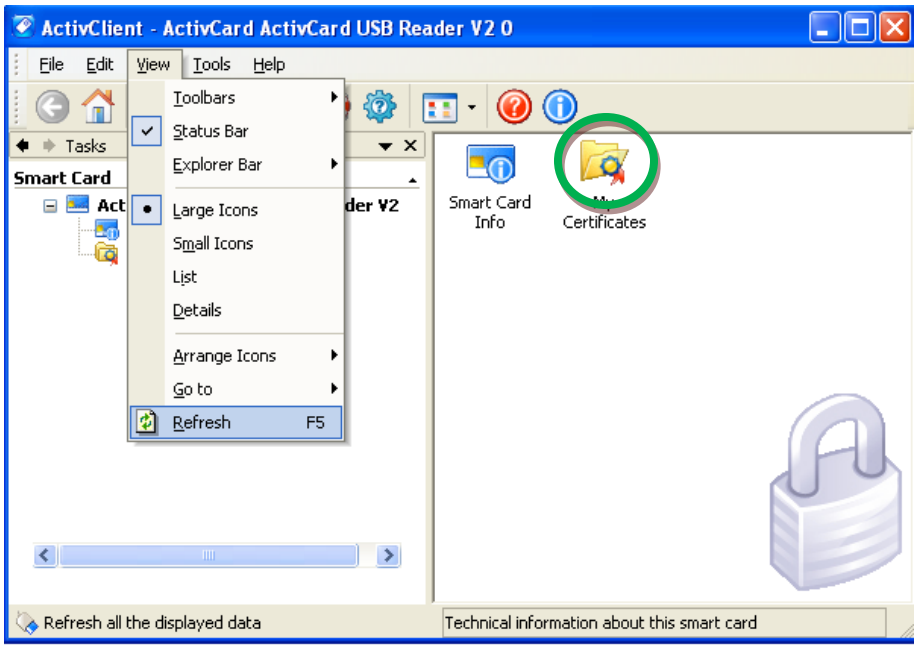


21. When key generation has been successful, you should see a web page that says "PRINT THIS FORM NOW." Print the request form; it should be 4 pages with a Finish Line at the bottom of the form. (If you do not see the Finish Line or a Green button at the bottom, click your refresh/reload button until you do.)

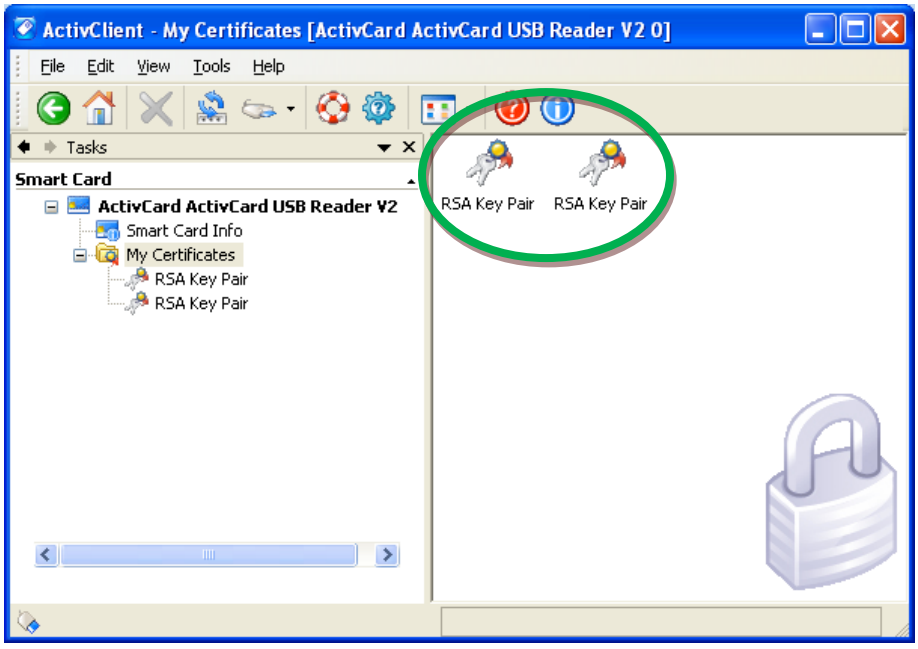


22. IMPORTANT: Confirm that your certificate key pairs were written onto the device.

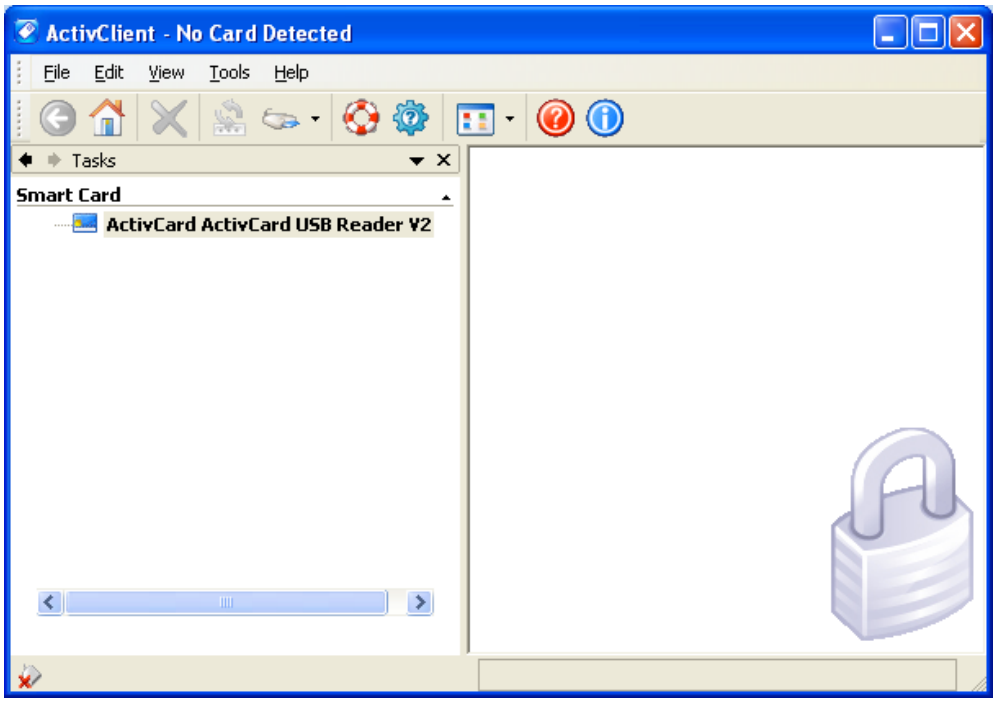
a. Open the ActivClient User Console and then click **View** then **Refresh**, then double-click on the My Certificates folder



b. You should see one (1) RSA Key Pair for each certificate that you are requesting. [Please note that the RSA Key Pairs are not yet certificates. They are the core of a certificate, but will not be finished until you receive a Certificate Issuance Notification email from ORC and you execute the instructions contained in that email.]



c. Pull your card out of the reader [Notice how the display goes blank.]



CRITICAL: If you do not see any Key Pairs on the device; that means that they were not written to the device. If the requests are issued, the resulting certificates will not be functional. Restart your computer and make a new set of requests. If you still get this result, contact ecahelp@orc.com

23. You are now finished on the computer. The printed request forms have detailed instructions on what to do with the forms. You will take to a Notary Public, then send the notarized forms with photo copies of your supporting documents to ORC. In a week or less, you will receive a Certificate Issuance Notification (CIN) email, telling you how to import the certificates and complete the certificate issuance process.

24. CRITICAL: Do not uninstall Firefox. Do not update Firefox until you have imported the finished certificates onto your card.