

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.]

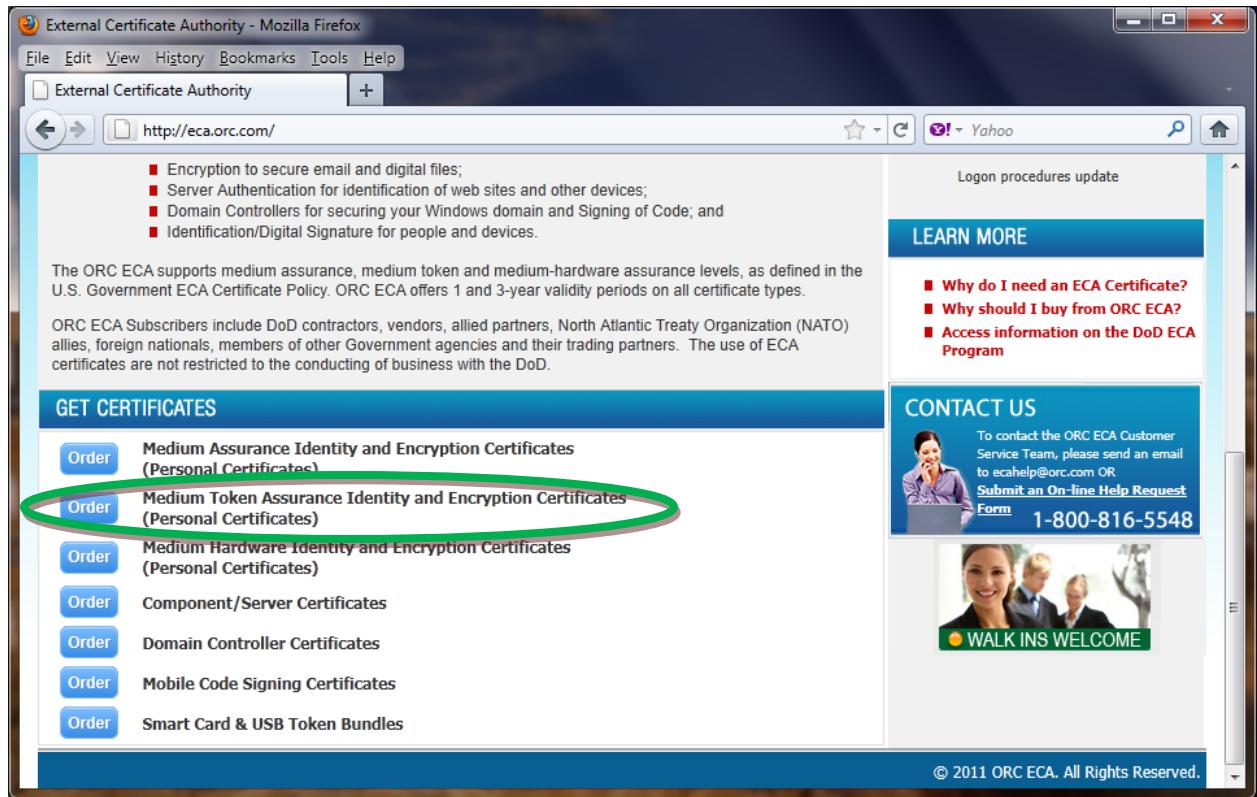
Please Note: Making the certificate request via Mozilla Firefox will not prevent nor impede your use of the certificates in Microsoft Internet Explorer (or other Microsoft application). On the contrary, Firefox generally performs certificate request functions in a ‘cleaner’ manner than the Microsoft 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



External Certificate Authority - Mozilla Firefox

File Edit View History Bookmarks Tools Help

External Certificate Authority

http://eca.orc.com/

Encryption to secure email and digital files;
Server Authentication for identification of web sites and other devices;
Domain Controllers for securing your Windows domain and Signing of Code; and
Identification/Digital Signature for people and devices.

The ORC ECA supports medium assurance, medium token and medium-hardware assurance levels, as defined in the U.S. Government ECA Certificate Policy. ORC ECA offers 1 and 3-year validity periods on all certificate types.

ORC ECA Subscribers include DoD contractors, vendors, allied partners, North Atlantic Treaty Organization (NATO) allies, foreign nationals, members of other Government agencies and their trading partners. The use of ECA certificates are not restricted to the conducting of business with the DoD.

GET CERTIFICATES

- Order** Medium Assurance Identity and Encryption Certificates (Personal Certificates)
- Order** Medium Token Assurance Identity and Encryption Certificates (Personal Certificates)
- Order** Medium Hardware Identity and Encryption Certificates (Personal Certificates)
- Order** Component/Server Certificates
- Order** Domain Controller Certificates
- Order** Mobile Code Signing Certificates
- Order** Smart Card & USB Token Bundles

Logon procedures update

LEARN MORE

- Why do I need an ECA Certificate?
- Why should I buy from ORC ECA?
- Access information on the DoD ECA Program

CONTACT US

To contact the ORC ECA Customer Service Team, please send an email to ecahelp@orc.com OR [Submit an On-line Help Request Form](#) 1-800-816-5548

  **WALK INS WELCOME**

© 2011 ORC ECA. All Rights Reserved.

3. Read the appropriate instructions depending on your citizenship

Order Certificates

Instructions for citizens of the United States, Great Britain, Canada, Australia and New Zealand.

Instructions for citizens of all other countries.

Before you order your certificate, be sure you have gone through all of the above instructions, including Trusting the ECA CAs.

Once you are confident that you understand what is needed to request a certificate, then please make your selection from the certificates below. If you require additional assistance, please contact the ORC ECA Customer Service.

- Medium Assurance Identity/Encryption Certificates
- Medium Token Assurance Identity/Encryption Certificates
- Medium Hardware Assurance Identity/Encryption Certificates
- Server Certificates
- Domain Controller Certificates
- Mobile Code Signing Certificates

Help Desk

ECA Repository

Certificate Tools

Reminders & Tips

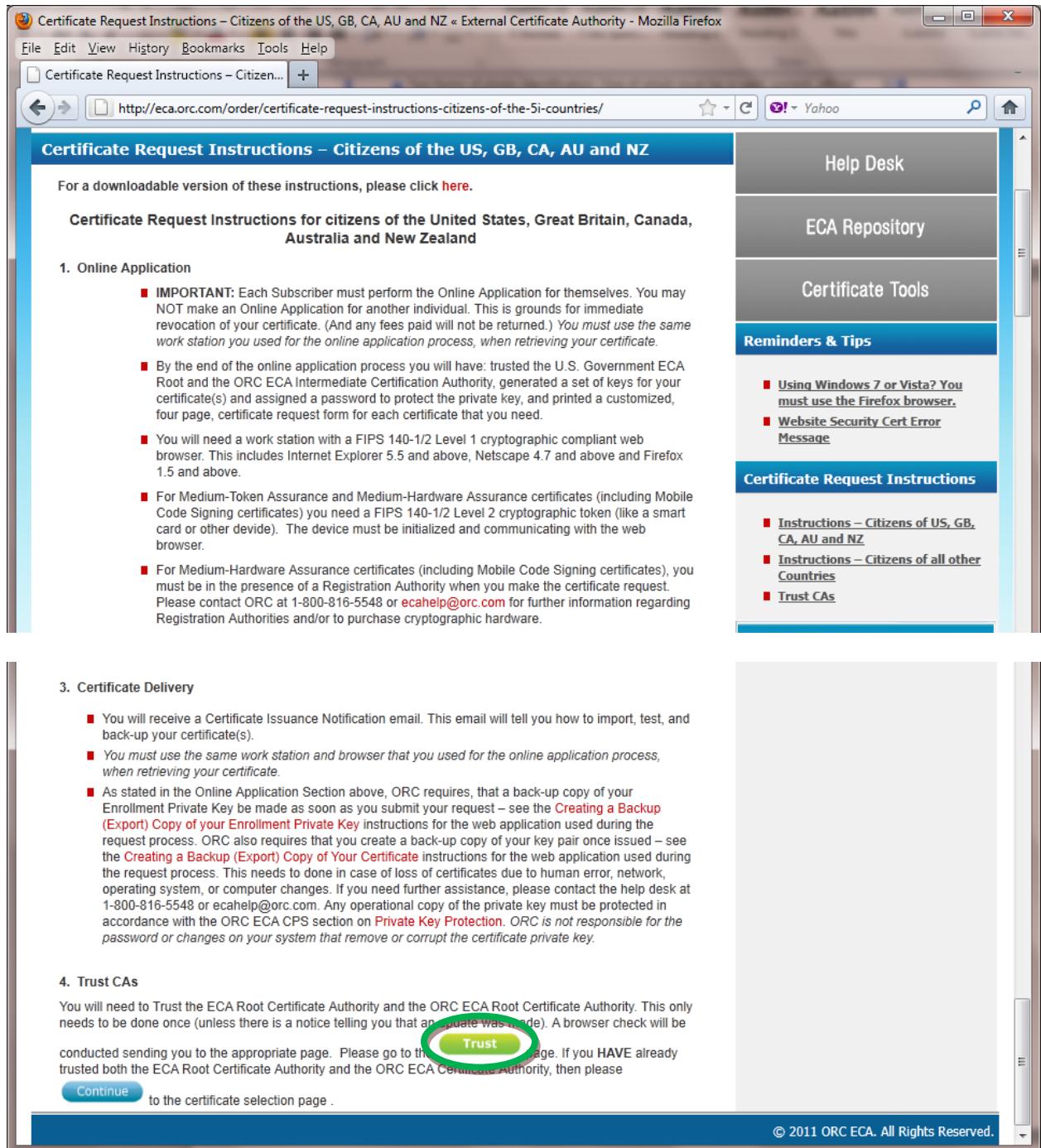
- [Using Windows 7 or Vista? You must use the Firefox browser.](#)
- [Website Security Cert Error Message](#)

Certificate Request Instructions

- [Instructions – Citizens of US, GB, CA, AU and NZ](#)
- [Instructions – Citizens of all other Countries](#)
- [Trust CAs](#)

CONTACT US

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



The screenshot shows a Mozilla Firefox browser window with the following details:

- Title Bar:** Certificate Request Instructions – Citizens of the US, GB, CA, AU and NZ » External Certificate Authority - Mozilla Firefox
- Address Bar:** http://eca.orc.com/order/certificate-request-instructions-citizens-of-the-5i-countries/
- Page Content:**
 - Section 1: Online Application**
 - IMPORTANT:** Each Subscriber must perform the Online Application for themselves. You may NOT make an Online Application for another individual. This is grounds for immediate revocation of your certificate. (And any fees paid will not be returned.) *You must use the same work station you used for the online application process, when retrieving your certificate.*
 - By the end of the online application process you will have: trusted the U.S. Government ECA Root and the ORC ECA Intermediate Certification Authority, generated a set of keys for your certificate(s) and assigned a password to protect the private key, and printed a customized, four page, certificate request form for each certificate that you need.
 - You will need a work station with a FIPS 140-1/2 Level 1 cryptographic compliant web browser. This includes Internet Explorer 5.5 and above, Netscape 4.7 and above and Firefox 1.5 and above.
 - For Medium-Token Assurance and Medium-Hardware Assurance certificates (including Mobile Code Signing certificates) you need a FIPS 140-1/2 Level 2 cryptographic token (like a smart card or other device). The device must be initialized and communicating with the web browser.
 - For Medium-Hardware Assurance certificates (including Mobile Code Signing certificates), you must be in the presence of a Registration Authority when you make the certificate request. Please contact ORC at 1-800-816-5548 or ecahelp@orc.com for further information regarding Registration Authorities and/or to purchase cryptographic hardware.
 - Section 3: Certificate Delivery**
 - You will receive a Certificate Issuance Notification email. This email will tell you how to import, test, and back-up your certificate(s).
 - You must use the same work station and browser that you used for the online application process, when retrieving your certificate.*
 - As stated in the Online Application Section above, ORC requires, that a back-up copy of your Enrollment Private Key be made as soon as you submit your request – see the [Creating a Backup \(Export\) Copy of your Enrollment Private Key](#) instructions for the web application used during the request process. ORC also requires that you create a back-up copy of your key pair once issued – see the [Creating a Backup \(Export\) Copy of Your Certificate](#) instructions for the web application used during the request process. This needs to be done in case of loss of certificates due to human error, network, operating system, or computer changes. If you need further assistance, please contact the help desk at 1-800-816-5548 or ecahelp@orc.com. Any operational copy of the private key must be protected in accordance with the ORC ECA CPS section on [Private Key Protection](#). ORC is not responsible for the password or changes on your system that remove or corrupt the certificate private key.
 - Section 4: Trust CAs**

You will need to Trust the ECA Root Certificate Authority and the ORC ECA Root Certificate Authority. This only needs to be done once (unless there is a notice telling you that an update was made). A browser check will be conducted sending you to the appropriate page. Please go to the [Trust](#) page. If you HAVE already trusted both the ECA Root Certificate Authority and the ORC ECA Certificate Authority, then please [Continue](#) to the certificate selection page.

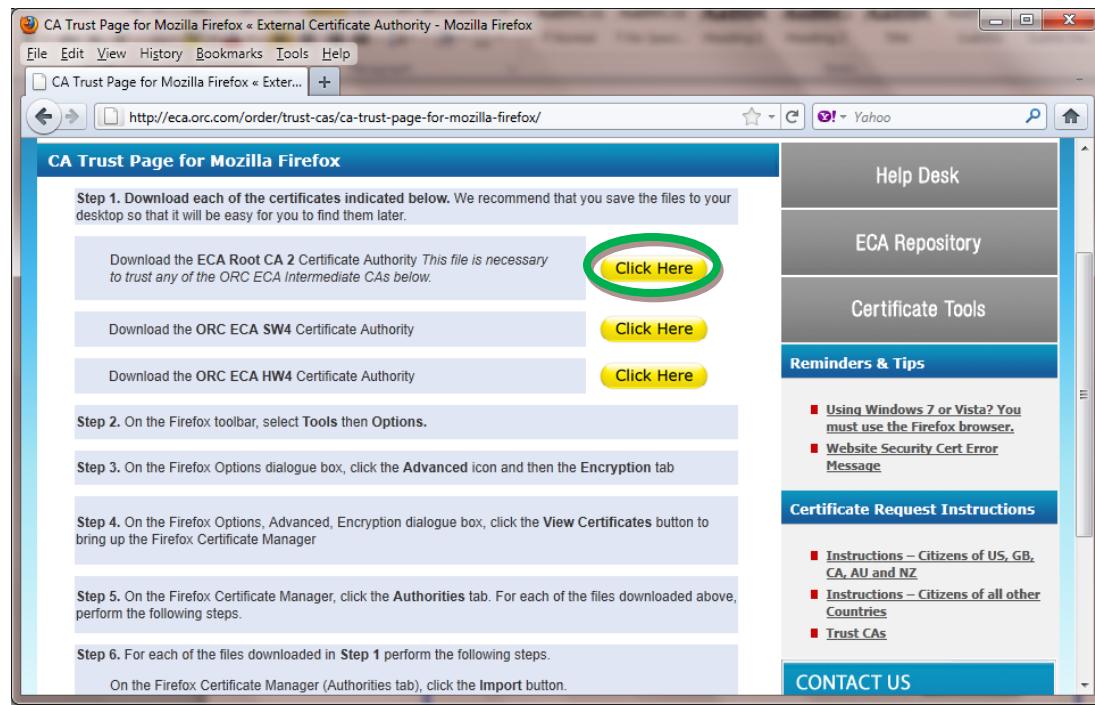
Right Sidebar:

 - Help Desk
 - ECA Repository
 - Certificate Tools
 - Reminders & Tips**
 - [Using Windows 7 or Vista? You must use the Firefox browser.](#)
 - [Website Security Cert Error Message](#)
 - Certificate Request Instructions**
 - [Instructions – Citizens of US, GB, CA, AU and NZ](#)
 - [Instructions – Citizens of all other Countries](#)
 - [Trust CAs](#)

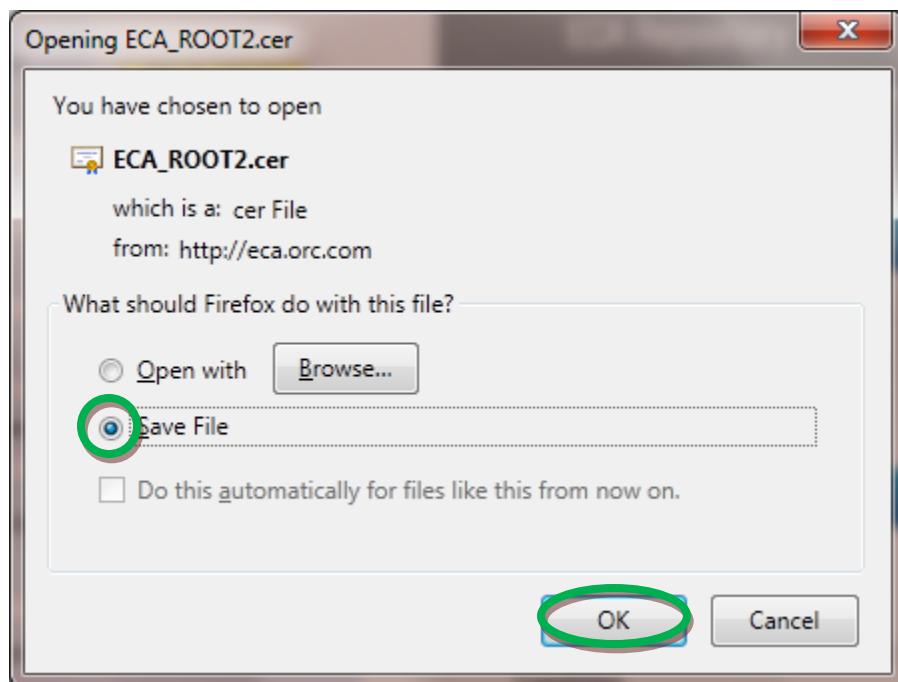
Page Footer: © 2011 ORC ECA. All Rights Reserved.

5. On the CA Trust page for Mozilla Firefox page... (This section executes the instructions as indicated on the web page.)

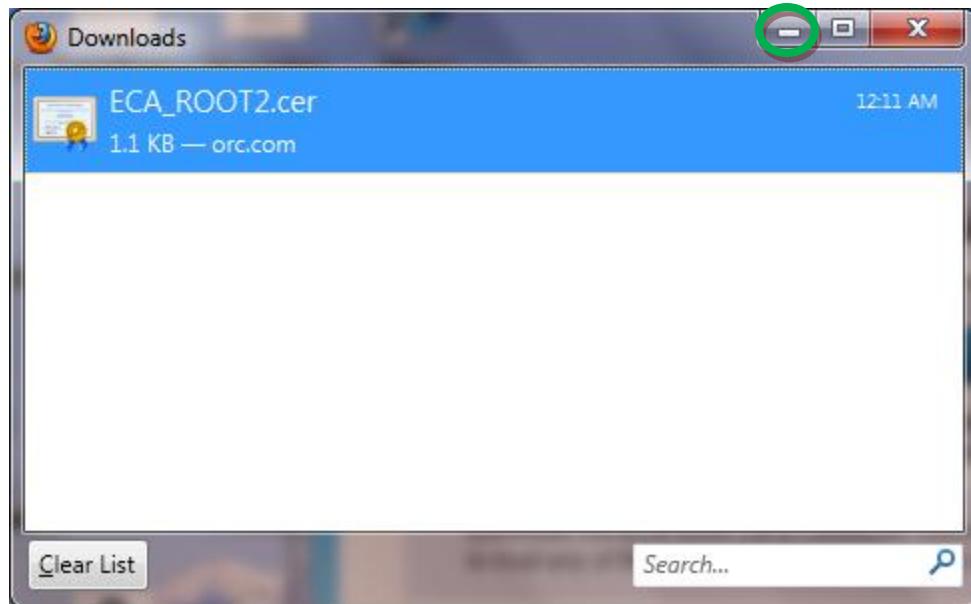
- Download all 3 files indicated in **Step 1** on the page by clicking on the **Click Here** button



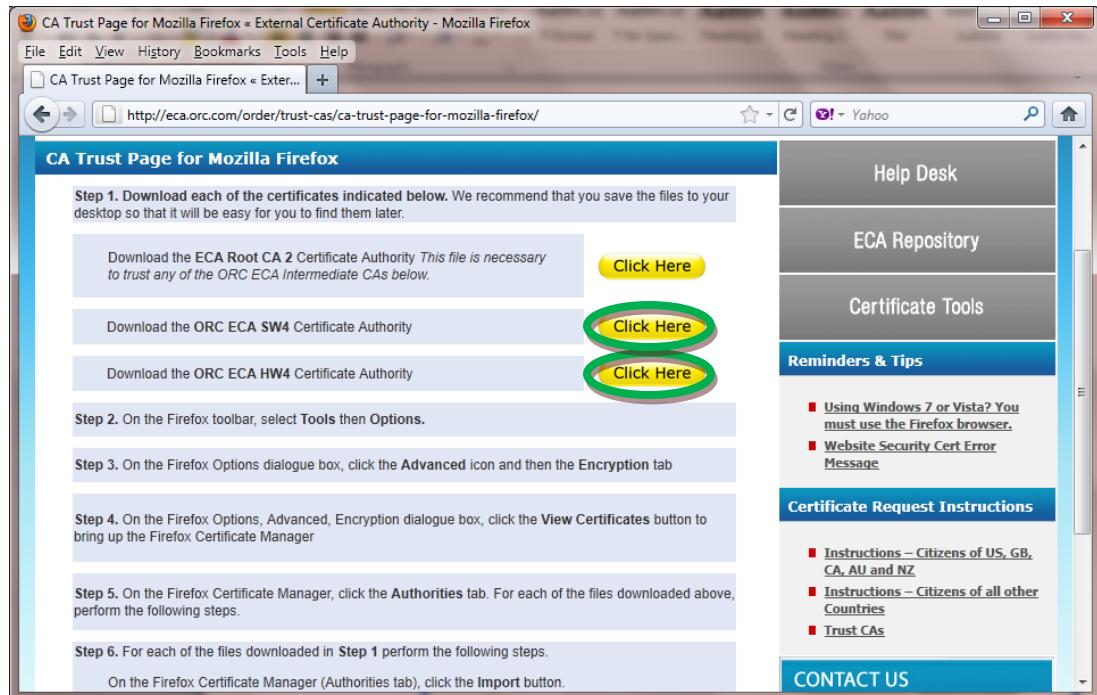
- This should bring up the following dialog box, select **Save File** and click the **OK** button



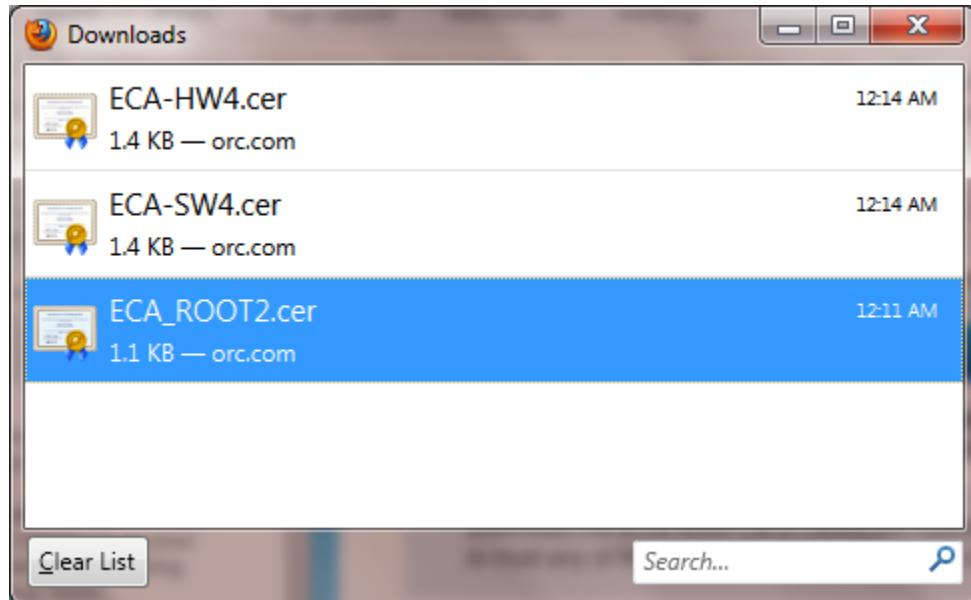
c. This should bring up the Firefox Downloads dialog box. (Note: You do not need to do anything in this box, it is just informing you that Firefox is downloading files.) Minimize the Downloads dialog box.



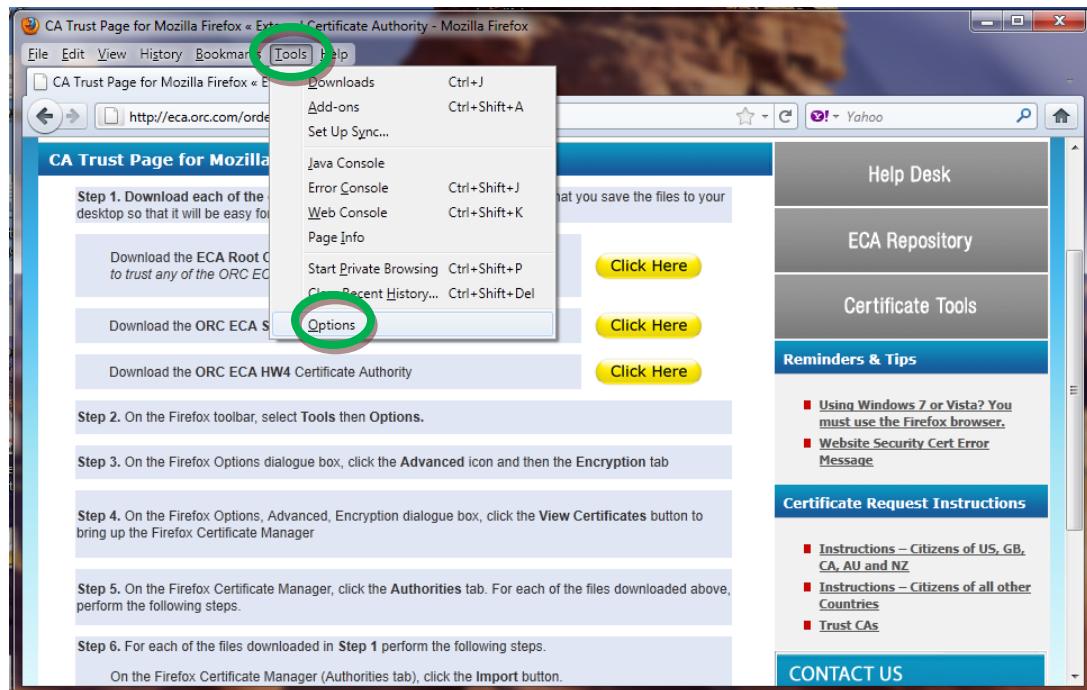
d. Go back to the web page and download the other two files indicated in Step 1.



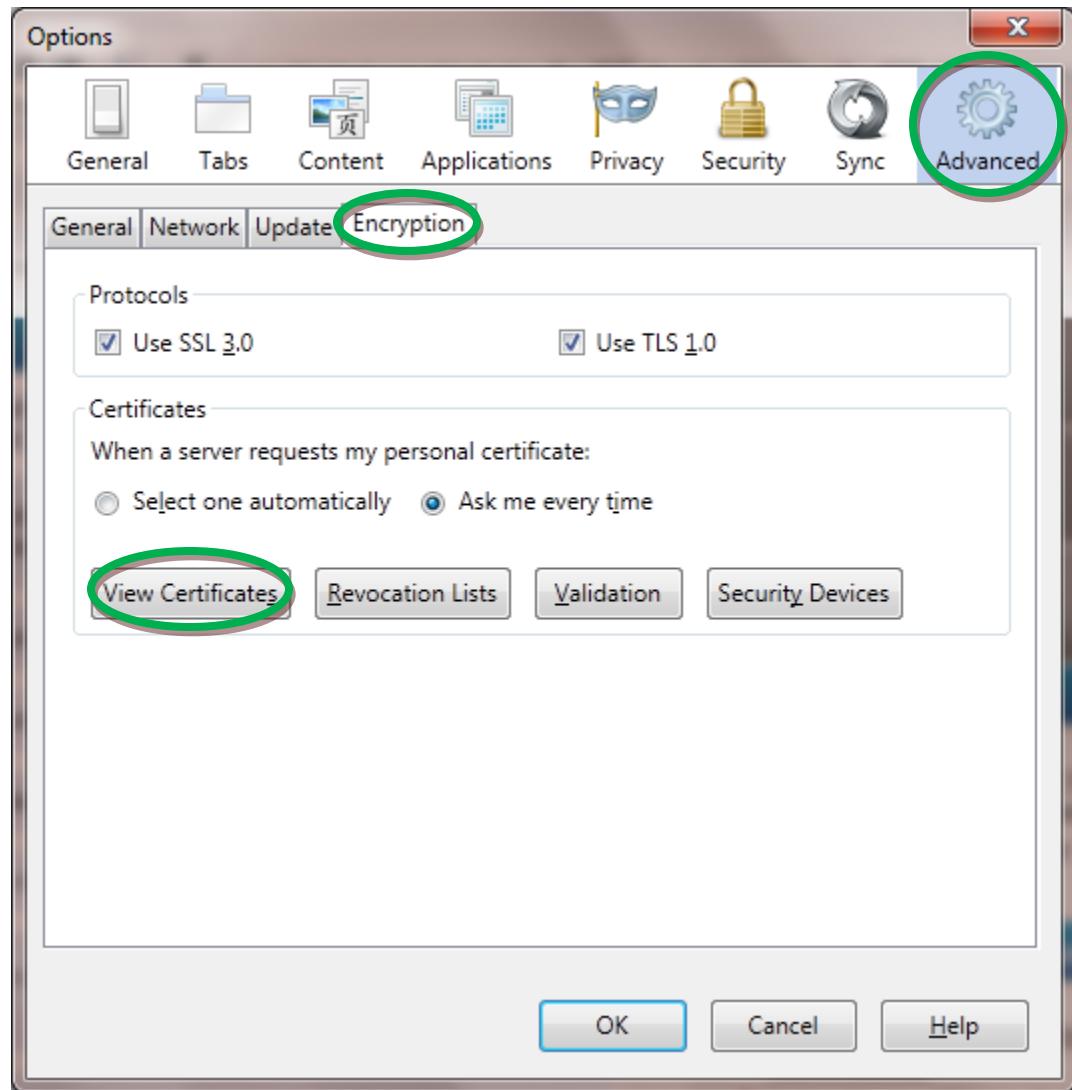
e. Look at the Firefox Downloads dialog box. (It should look something like this.)



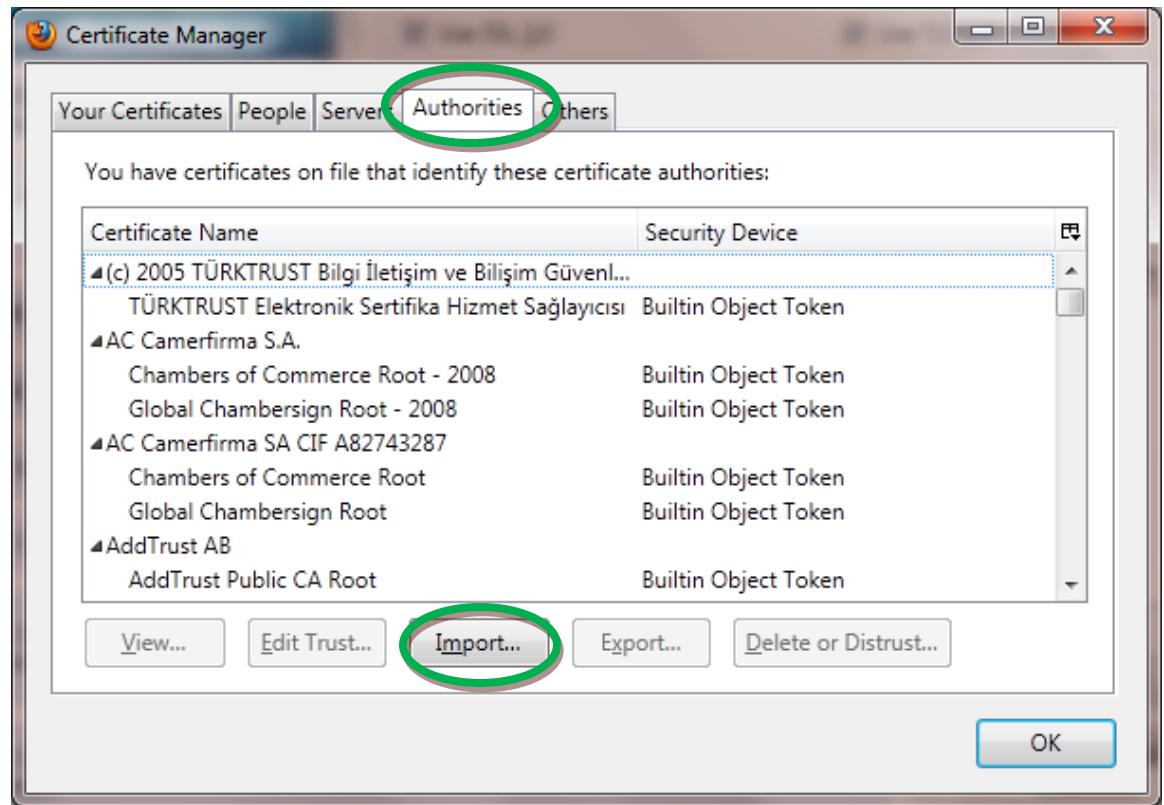
f. On the Firefox toolbar, select **Tools** then **Options...**



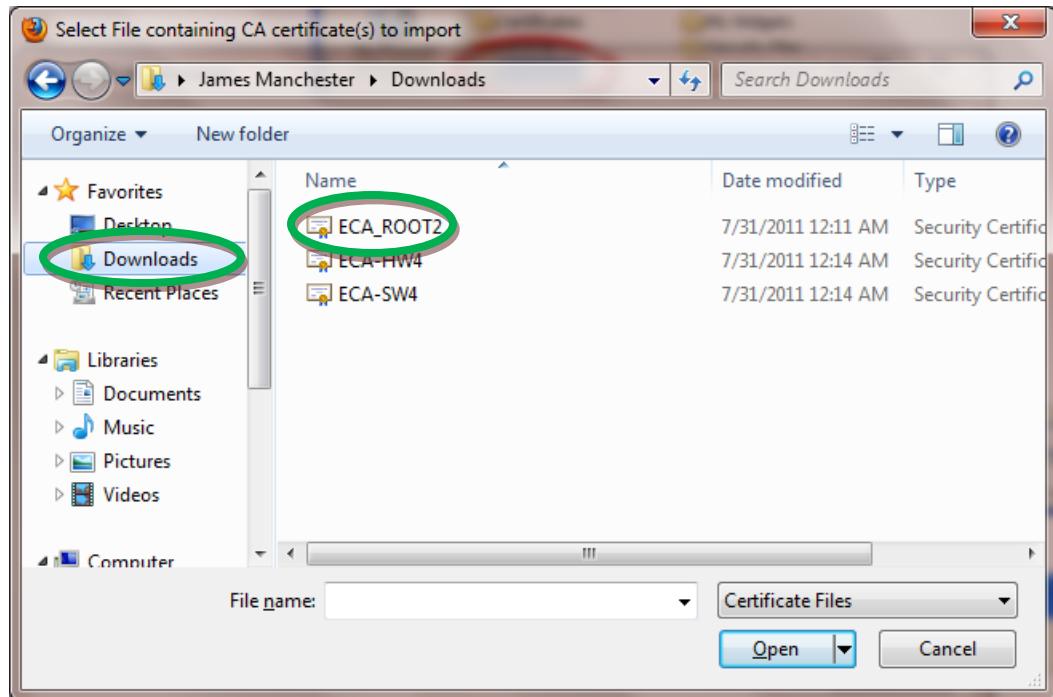
g. On the Firefox Options dialogue box, click the **Advanced** icon and then the **Encryption** tab, then click the **View Certificates** button



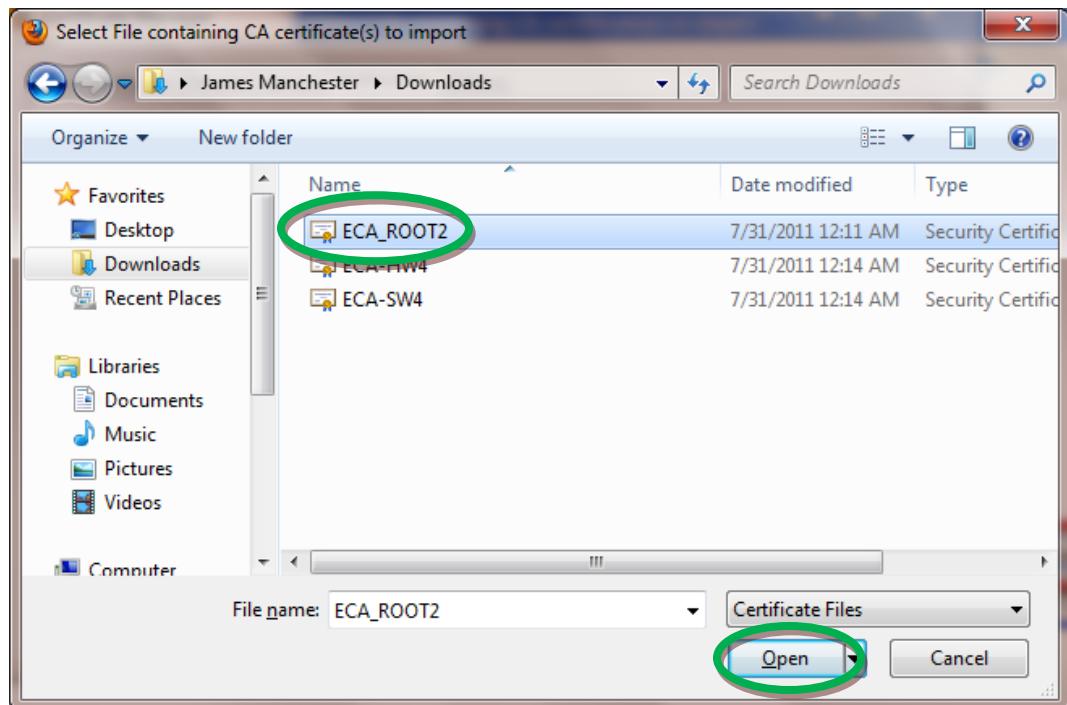
h. In the Firefox Certificate Manager, click the **Authorities** tab, then click the **Import** button



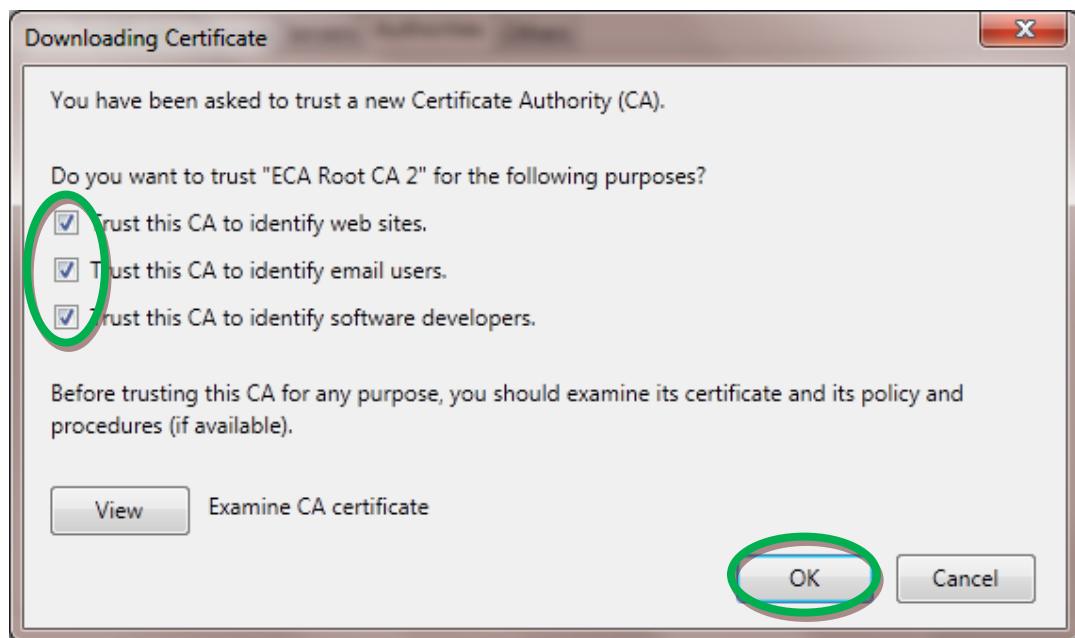
i. In the Select File containing CA certificate(s) to import dialogue box, navigate to the location where you saved the imported “.cer” files from above. (If the files are not in the location shown in the screenshot perform a search on your computer for files named “*.cer” to find out where the files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



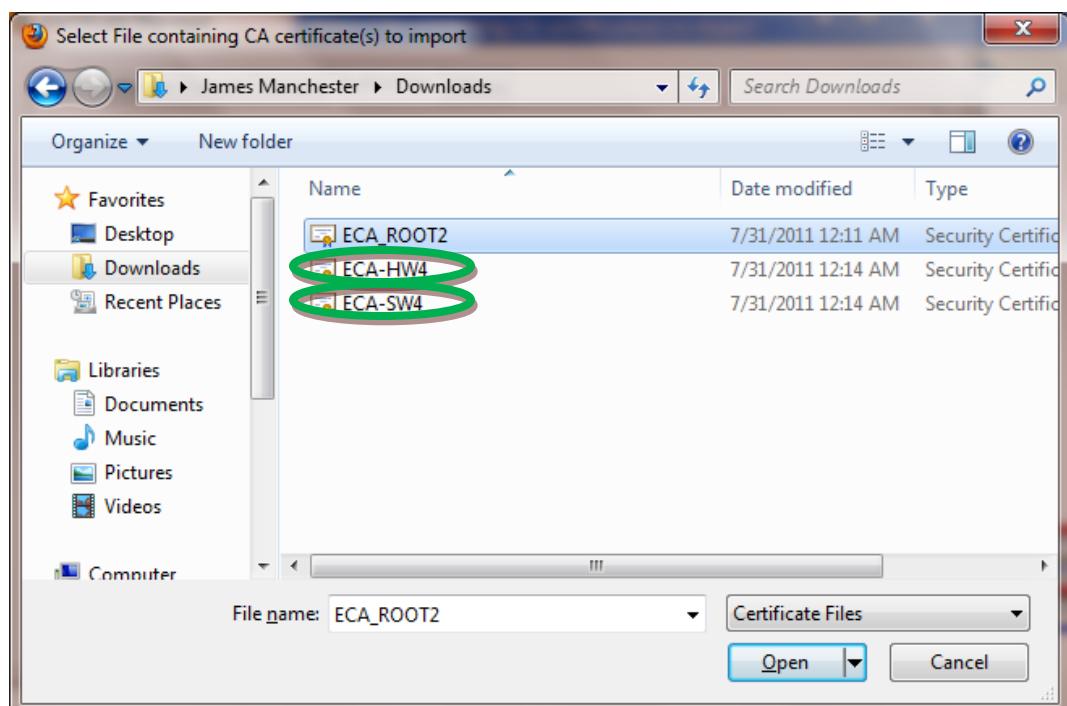
j. Select the file named “ECA-ROOT2.cer” and click the **Open** button



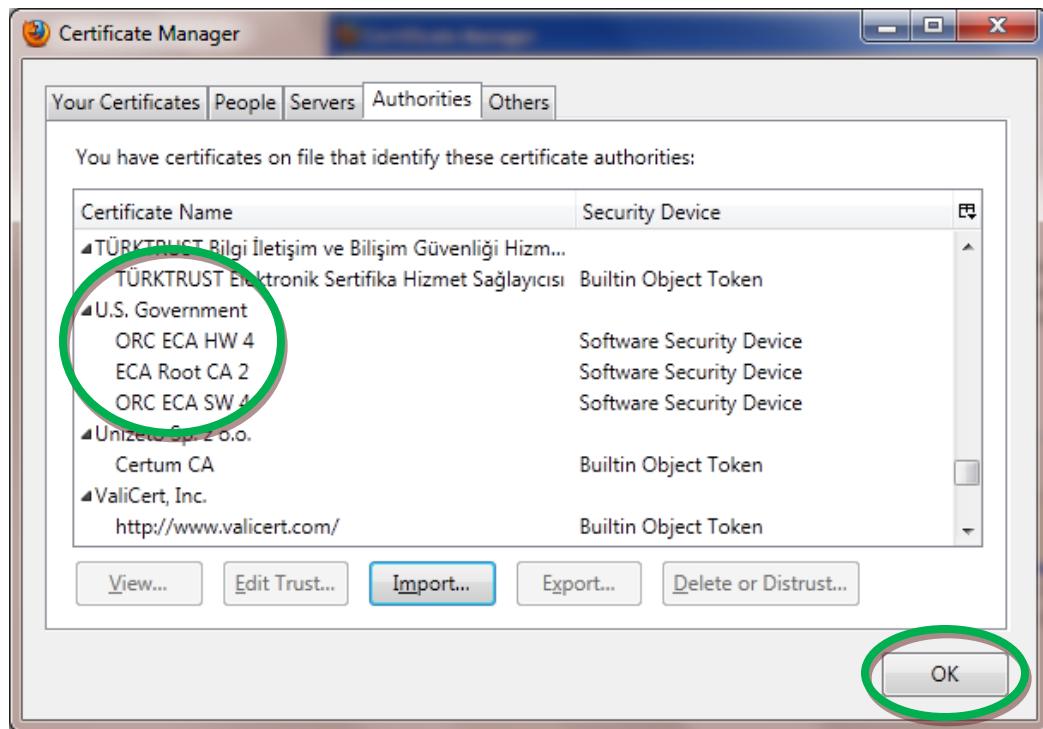
k. Check all three (3) check boxes and click the OK button



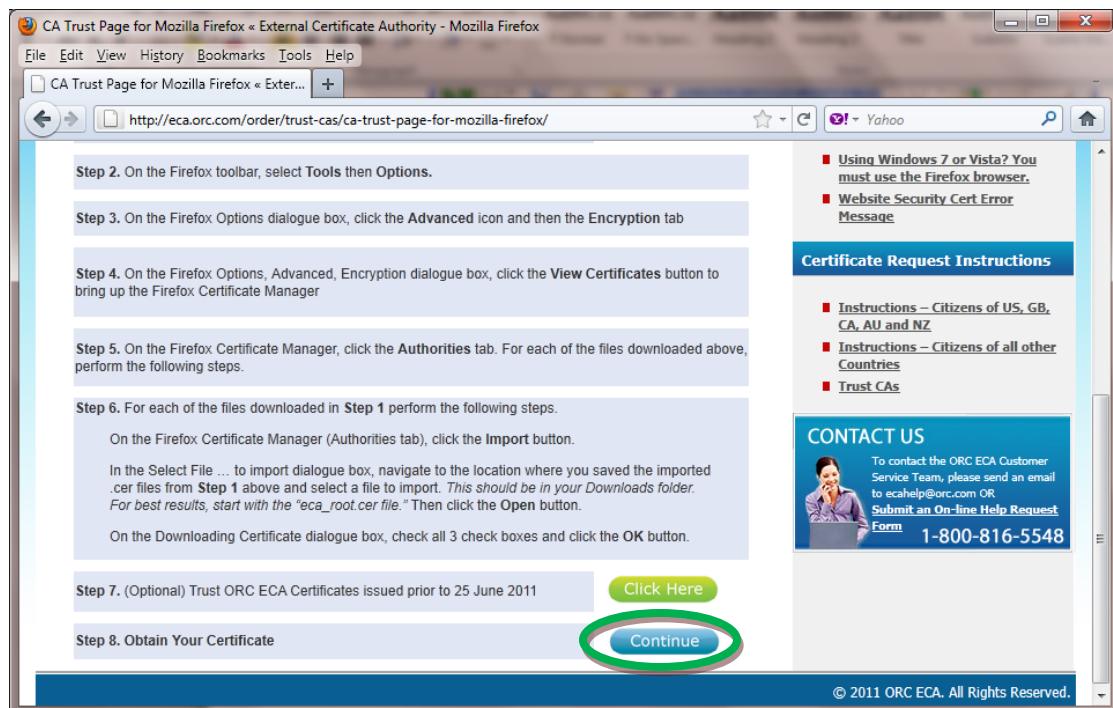
1. Then in the Firefox Certificate Manager, perform the exact same function for the other two files.



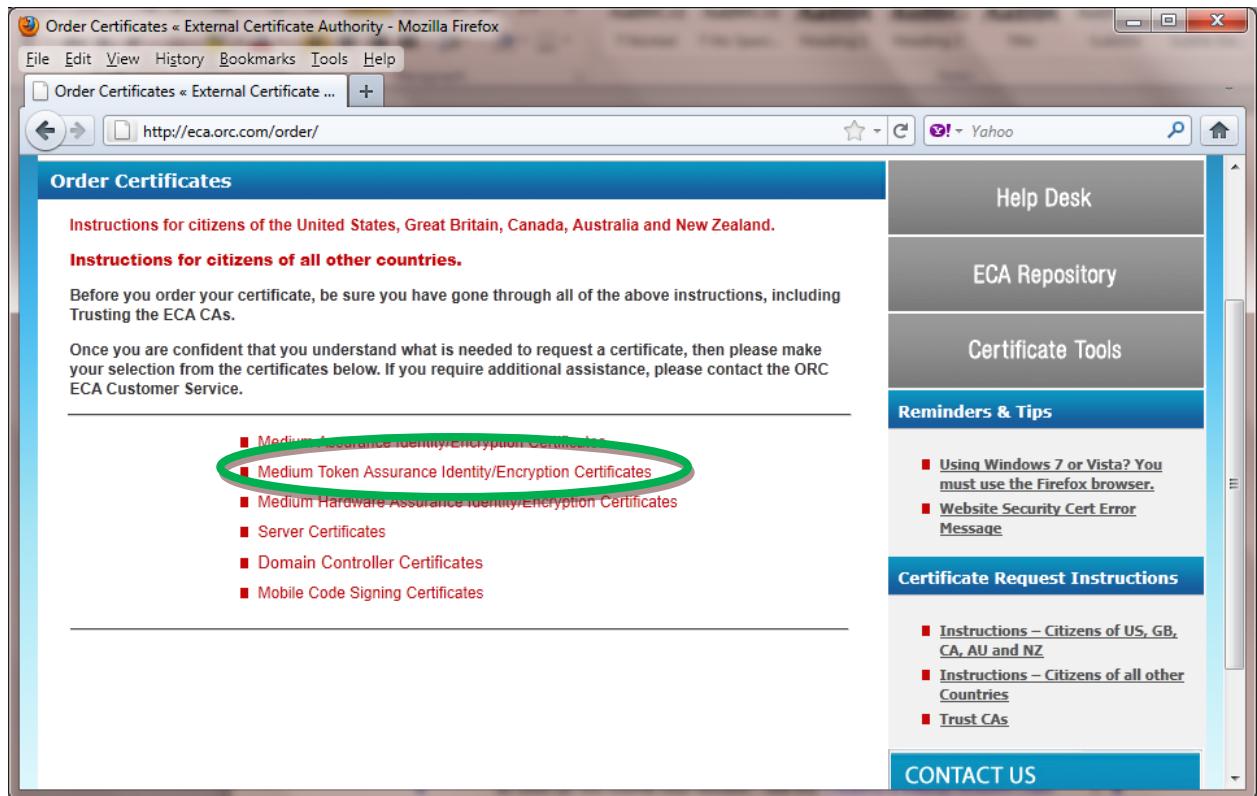
m. When you are done, you should see something like this in the U.S. Government section in the Firefox Certificate Manager – Authorities. Click the **OK** button.



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



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



Order Certificates

Instructions for citizens of the United States, Great Britain, Canada, Australia and New Zealand.

Instructions for citizens of all other countries.

Before you order your certificate, be sure you have gone through all of the above instructions, including Trusting the ECA CAs.

Once you are confident that you understand what is needed to request a certificate, then please make your selection from the certificates below. If you require additional assistance, please contact the ORC ECA Customer Service.

- Medium Assurance Identity/Encryption Certificates
- **Medium Token Assurance Identity/Encryption Certificates**
- Medium Hardware Assurance Identity/Encryption Certificates
- Server Certificates
- Domain Controller Certificates
- Mobile Code Signing Certificates

Help Desk

ECA Repository

Certificate Tools

Reminders & Tips

- [Using Windows 7 or Vista? You must use the Firefox browser.](#)
- [Website Security Cert Error Message](#)

Certificate Request Instructions

- [Instructions – Citizens of US, GB, CA, AU and NZ](#)
- [Instructions – Citizens of all other Countries](#)
- [Trust CAs](#)

CONTACT US

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



Medium Token Assurance Identity/Encryption Certificates

TOKEN CERT

A Medium-Token Assurance Identity Certificate is intended for all applications operating in environments appropriate for medium assurance but which require a higher degree of technical non-repudiation based on the relying party's assessment. A certificate that a person uses to authenticate to a PKI-enabled application, such as a secure web site. Identity certificates may be used for non-repudiation purposes, (i.e., transactions that have been signed by an identity certificate) and may be legally linked to the owner of that certificate. The token certificate may also be used for secure and authenticated email. Some web sites that require Medium-Token Assurance as the minimum acceptable assurance level are DoD eMail and JPAS.

A Medium-Token Assurance Encryption Certificate is intended for all applications operating in environments appropriate for medium assurance but which require a higher degree of technical non-repudiation based on the relying party's assessment. A certificate that may be used for encrypting e-mail. When encrypting e-mail messages, the sender uses the certificate of the recipient(s), and the recipient decrypts the message using his or her private key.

Reminders & Tips

- [Using Windows 7 or Vista? You must use the Firefox browser.](#)
- [Website Security Cert Error Message](#)

Certificate Request Instructions

- [Instructions – Citizens of US, GB, CA, AU and NZ](#)
- [Instructions – Citizens of all other Countries](#)
- [Trust CAs](#)

CONTACT US

To contact the ORC ECA Customer Service Team, please send an email to ecahelp@orc.com OR

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 that only the named individual is authorized to use the certificate. You may not request a certificate for someone else and you may not allow someone else to use your certificate.

Medium Token Assurance Identity/Encryption Obligations « External Certificate Authority - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Medium Token Assurance Identity/Encryption Obligations +

http://eca.orc.com/token-identity-encryption-obligations/

Medium Token Assurance Identity/Encryption Obligations

TOKEN CERT

In order to request and use a Medium-Token Assurance Identity/Encryption Certificates issued under the ORC ECA CPS you (the subscriber) **must make the request using a web browser and a FIPS 140-1/2 Level 2 token** and agree to the following obligations.

- Subscriber shall use cryptographic tokens that have been verified to meet FIPS 140 Level 2 to receive a Medium Token Assurance certificate.
- To accurately represent yourself in all communications with ORC and the PKI.
- To protect the certificate private key from unauthorized access in accordance with the [Private Key Protection](#) section of the ORC ECA CPS. Only the person named in the certificate is authorized to access the private key. The private key is accessed when using the certificate. *(You are the only person allowed to use certificates issued in your name. You may not loan your device to another person nor provide another person with the PIN that protects your device.)*

■ As a result of issuing a certificate that identifies a person as an employee or member of an organization, ORC does not represent that the individual has authority to act for that organization.

■ For Relying Parties: Use of REVOKED certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new Revocation data should be obtained is a determination to be made by the relying party and the system accreditor. If it is temporarily infeasible to obtain Revocation information, then the relying party must either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of the ORC ECA practice statement.

Theft, compromise or misuse of the private key may cause the Subscriber, Relying Party, and their organization local consequences.

I understand that during this process I will be generating my **key pair** and will possess the only copy of my private key on the workstation/computer (or hardware token) from which I am making my request. If lost, damaged, or compromised, I will be responsible for requesting and incurring the costs of a new certificate.

I have read and understand all the certificate instructions listed in the Subscriber Instructions document, as well as Trusted the ECA CAs.

I have read and agree to all of the Subscriber Obligations listed above.

I Agree

Reminders & Tips

- [Using Windows 7 or Vista? You must use the Firefox browser.](#)
- [Website Security Cert Error Message](#)

Certificate Request Instructions

- [Instructions – Citizens of US, GB, CA, AU and NZ](#)
- [Instructions – Citizens of all other Countries](#)
- [Trust CAs](#)

CONTACT US

To contact the ORC ECA Customer Service Team, please send an email

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

This is sample data, please enter your information

Validity Certificate Enrollment One Year - \$150

Identity: Enter values for the fields below. Values must be consistent with your Identification Credentials (e.g.- Government Issued Photo ID, Drivers License, Passport, ID Card.)

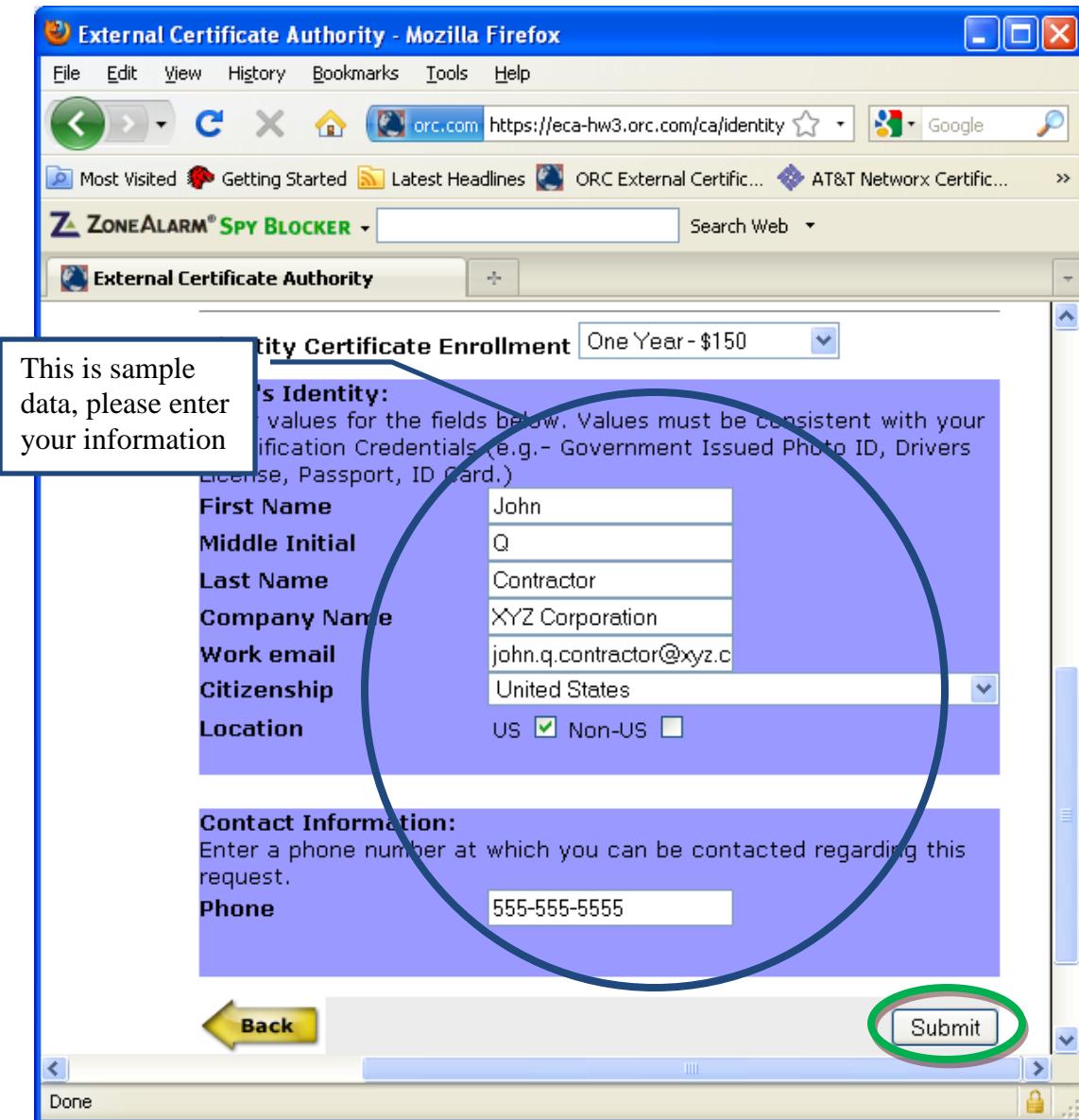
First Name	John
Middle Initial	Q
Last Name	Contractor
Company Name	XYZ Corporation
Work email	john.q.contractor@xyz.c
Citizenship	United States
Location	US <input checked="" type="checkbox"/> Non-US <input type="checkbox"/>

Contact Information:
Enter a phone number at which you can be contacted regarding this request.

Phone 555-555-5555

Back **Submit**

Done



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 a correction; you will be charged again to fix your mistake.)

ORC ECA Software CA 3 - Confirm Information - Mozilla Firefox

File Edit View History Bookmarks Tools Help

orc.com https://eca-hw3.orc.com Google

Most Visited Getting Started Latest Headlines ORC External Certific...

ZONEALARM® SPY BLOCKER Search Web

ORC ECA Software CA 3 - Confirm Inf...

ORC ECA - One Year Medium-Token Assurance Identity Certificate

Subscriber Information

First Name:	John
Middle Initial:	Q
Last Name:	Contractor
Company Name:	XYZ Corporation
Work Email Address:	john.q.contractor@xyz.com
Company Phone Number:	555-555-5555
Citizenship:	US
Location:	In the United States

This is critical; it MUST be correct

If you need to make a change, do so here

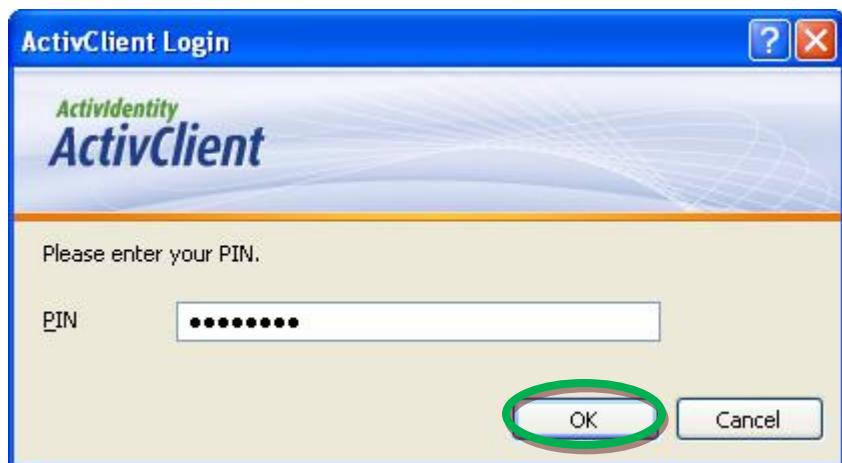
Make a Change This is Correct

Done

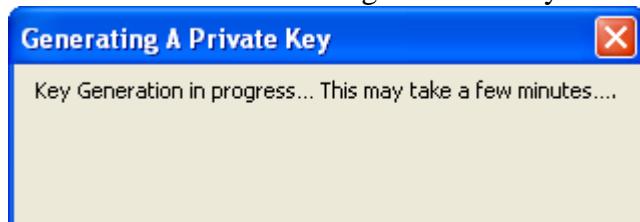
11. When you get the Choose Token Dialog, ensure that it is set to ActivIdentity and click **OK**



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.)

If you do not see the Finish Line at the bottom, click Refresh until you do.

PRINT THIS FORM NOW

REQUEST FOR

ORC ECA Hardware/Token CA 3 IDENTITY CERTIFICATE

Your request ID is 5959.

Certificate Validity Period: One Year Two Years Three Years

Congratulations, your request for an **ECA MEDIUM-TOKEN ASSURANCE IDENTITY CERTIFICATE** has been successfully submitted to the Certificate Manager.

You will need the following information in order to complete this process and submit your authorized application to an ECA RA.

- Two forms of photo Identification. One of the forms of photo Identification MUST be issued by a government entity within the US and be current and valid. (example: driver's license or passport) The second form of photo Identification may be a government issued photo ID (from a different agency than the first) or a business or institutional photo identity card or badge.
- Proof of Citizenship. US citizens may submit a photocopy of the following documents as Proof of Nationality: US Passport, certified copy of birth certificate, Naturalization

RA - Please verify Country of Citizenship. If you are not familiar with the 2-digit values, please refer to ISO 3166-1.

Provided: US -----> Notary/RA/LRA initial here: _____

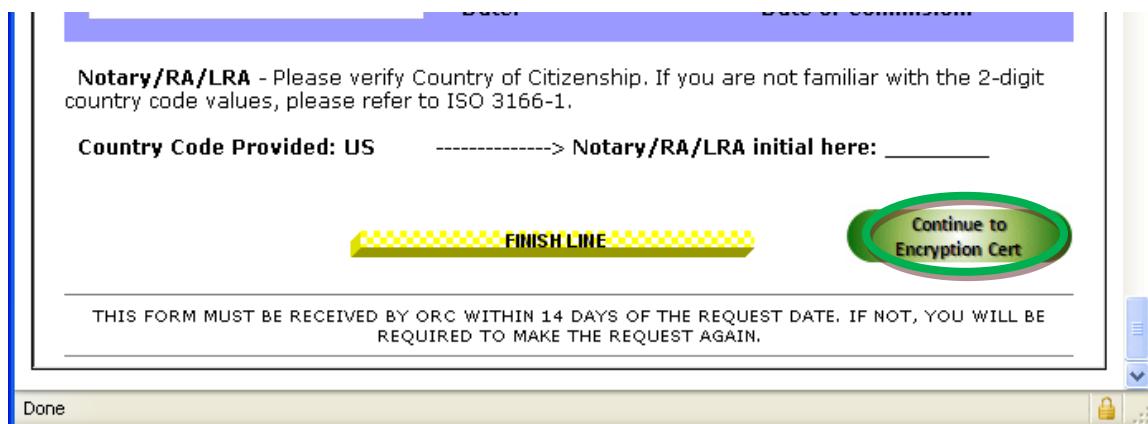
FINISH LINE

Continue to Encryption Cert

THIS FORM MUST BE RECEIVED BY ORC WITHIN 14 DAYS OF THE REQUEST DATE. IF NOT, YOU WILL BE REQUIRED TO MAKE THE REQUEST AGAIN.

Done

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



Notary/RA/LRA - Please verify Country of Citizenship. If you are not familiar with the 2-digit country code values, please refer to ISO 3166-1.

Country Code Provided: US -----> Notary/RA/LRA initial here: _____

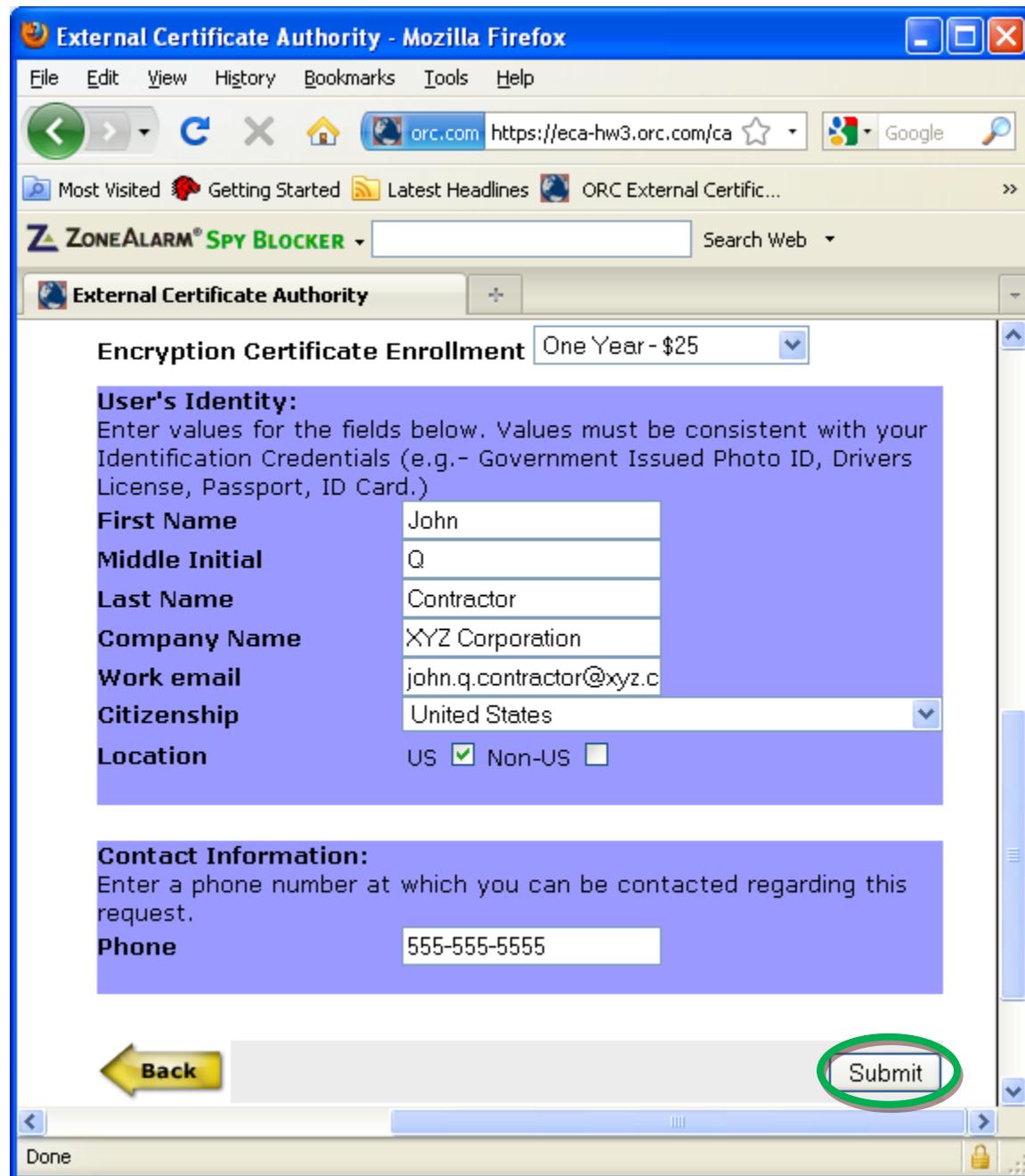
FINISH LINE

Continue to Encryption Cert

THIS FORM MUST BE RECEIVED BY ORC WITHIN 14 DAYS OF THE REQUEST DATE. IF NOT, YOU WILL BE REQUIRED TO MAKE THE REQUEST AGAIN.

Done

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



External Certificate Authority - Mozilla Firefox

File Edit View History Bookmarks Tools Help

orc.com https://eca-hw3.orc.com/ca

Most Visited Getting Started Latest Headlines ORC External Certific...

ZONEALARM® SPY BLOCKER Search Web

External Certificate Authority

Encryption Certificate Enrollment One Year - \$25

User's Identity:
Enter values for the fields below. Values must be consistent with your Identification Credentials (e.g.- Government Issued Photo ID, Drivers License, Passport, ID Card.)

First Name	John
Middle Initial	Q
Last Name	Contractor
Company Name	XYZ Corporation
Work email	john.q.contractor@xyz.c
Citizenship	United States
Location	US <input checked="" type="checkbox"/> Non-US <input type="checkbox"/>

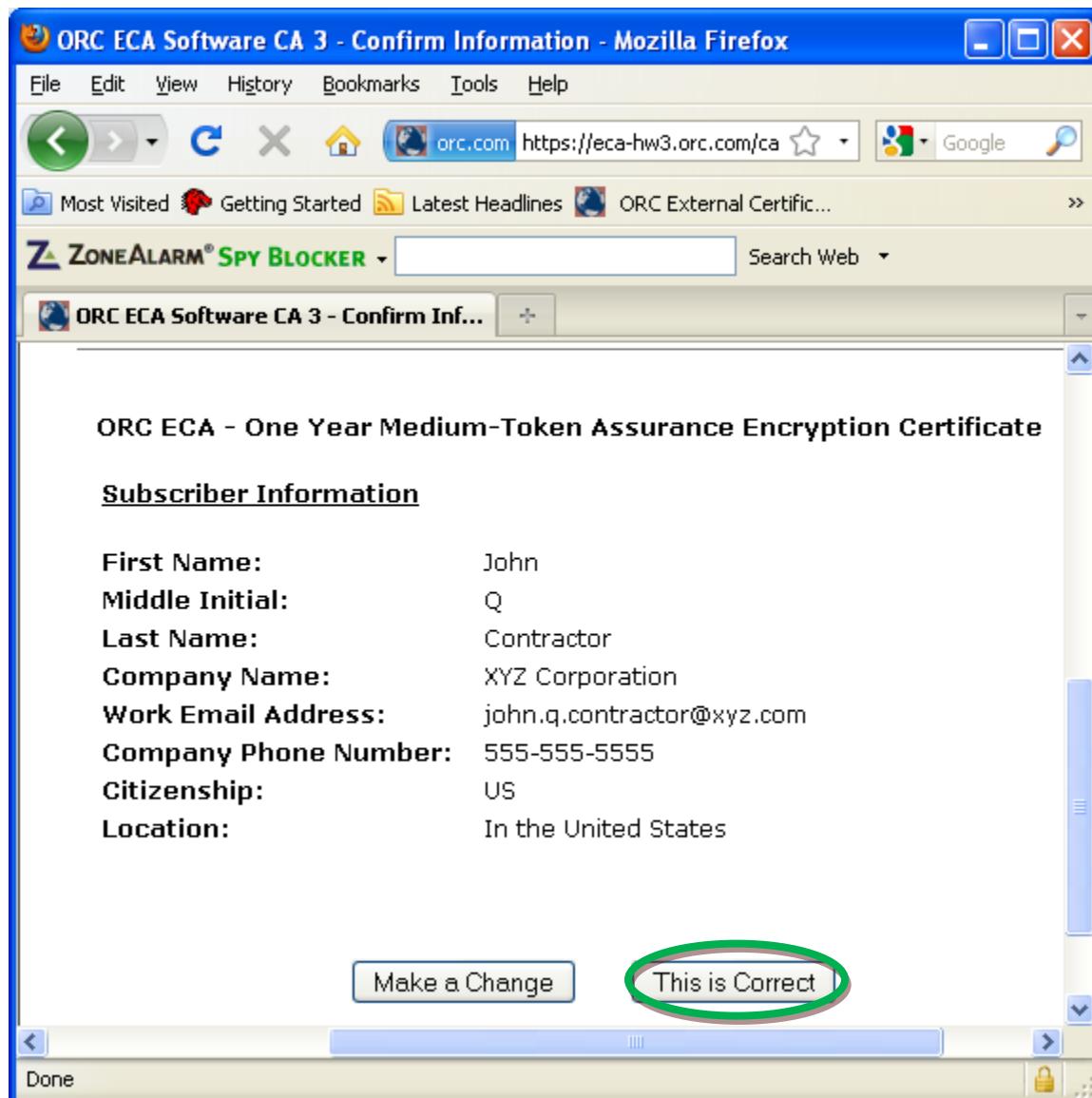
Contact Information:
Enter a phone number at which you can be contacted regarding this request.

Phone	555-555-5555
-------	--------------

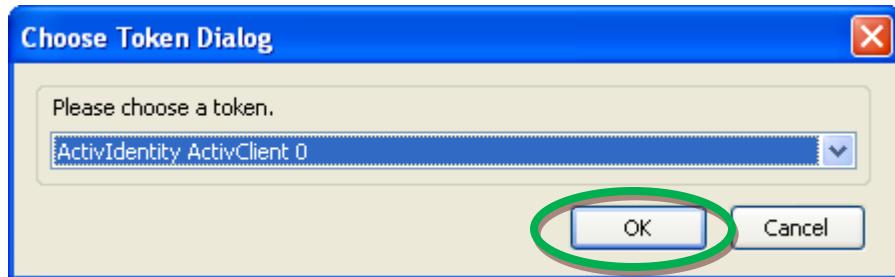
Back **Submit**

Done

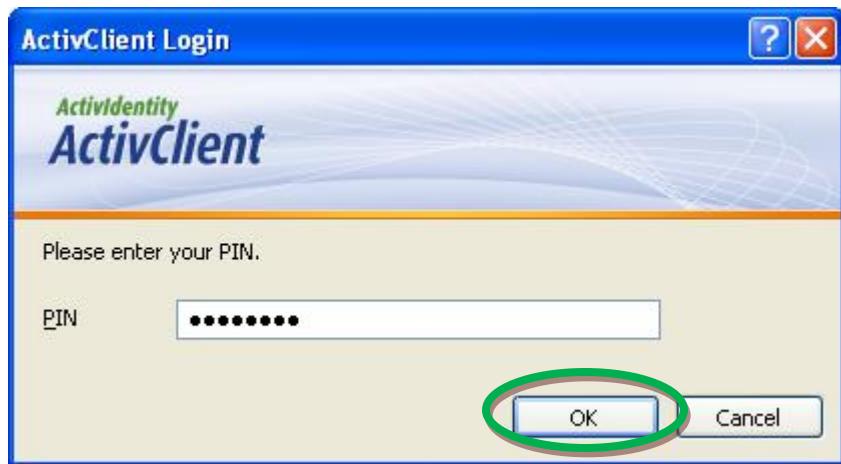
17. On the Confirm Information page, double check your information again. (NOTE: If you see a problem, it means that you made a mistake when you made your Identity Certificate Request; go back and make a new Identity Certificate Request.) Make any changes if necessary and then click **This is Correct**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



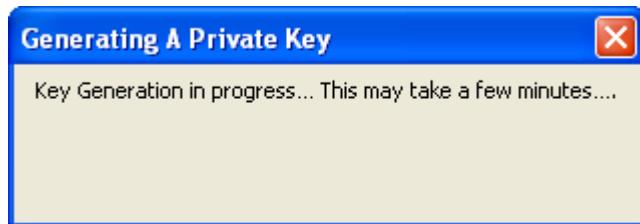
18. When you get another Choose Token Dialog, ensure that it is set to ActivIdentity and click **OK**



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.)

If you do not see the Finish Line at the bottom, click Refresh until you do.

PRINT THIS FORM NOW

REQUEST FOR
ORC ECA Hardware/Token CA 3 ENCRYPTION CERTIFICATE
Your request ID is 5962.

Certificate Validity Period: One Year Two Years Three Years

Congratulations, your request for an **ECA MEDIUM-TOKEN ASSURANCE ENCRYPTION CERTIFICATE** has been successfully submitted to the Certificate Manager.

You will need the following information in order to complete this process and submit your authorized application to an ECA RA.

Two forms of photo Identification. One of the forms of photo Identification MUST be

Notary/RA/LRA Name: _____
Notary/RA/LRA Signature: _____
Date: _____ Date of Commision: _____

If you see this, then
Print the form

Please verify Country of Citizenship. If you are not familiar with the 2-digit
es, please refer to ISO 3166-1.

Country Code Provided: US -----> Notary/RA/LRA initial here: _____

FINISH LINE

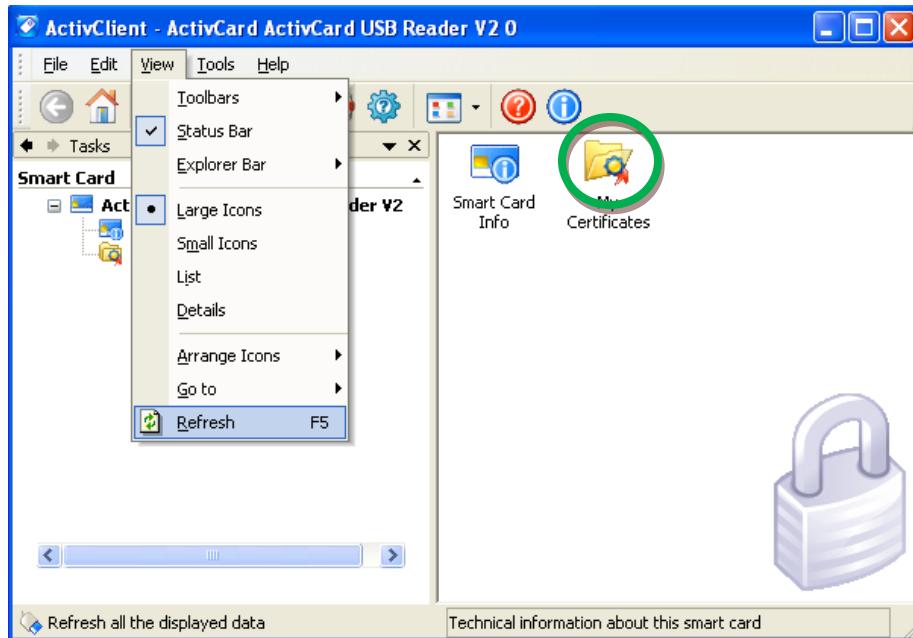
THIS FORM MUST BE RECEIVED BY ORC WITHIN 15 DAYS OF THE REQUEST DATE. IF NOT, YOU WILL BE
REQUIRED TO MAKE THE REQUEST AGAIN.

Continue

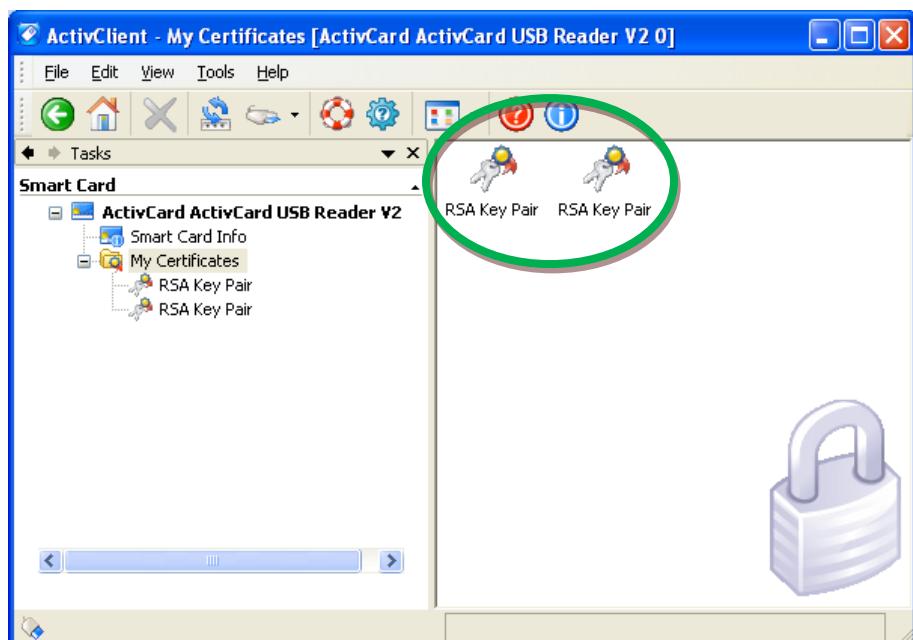
Done

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

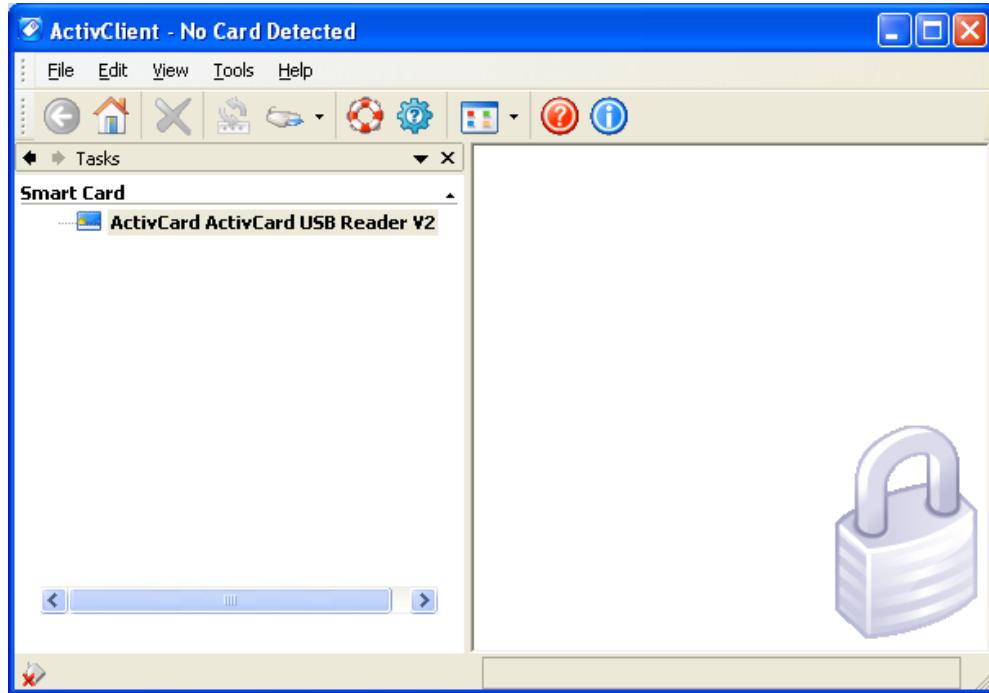
- a. Open the ActivClient User Console and then click **View** then **Refresh**, then double-click on the My Certificates folder



- 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.