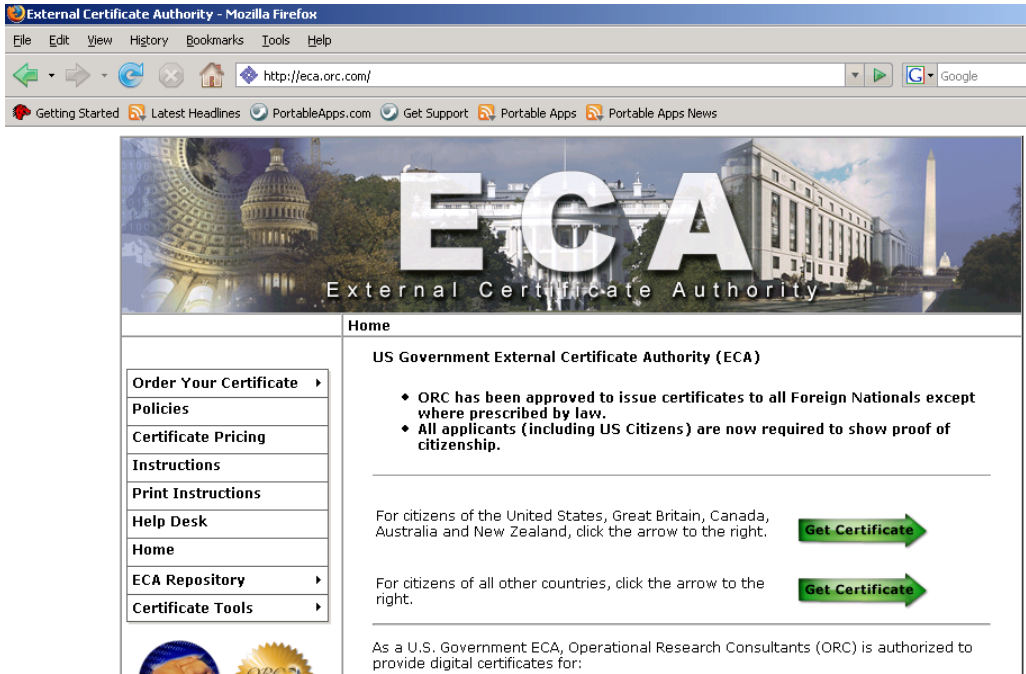
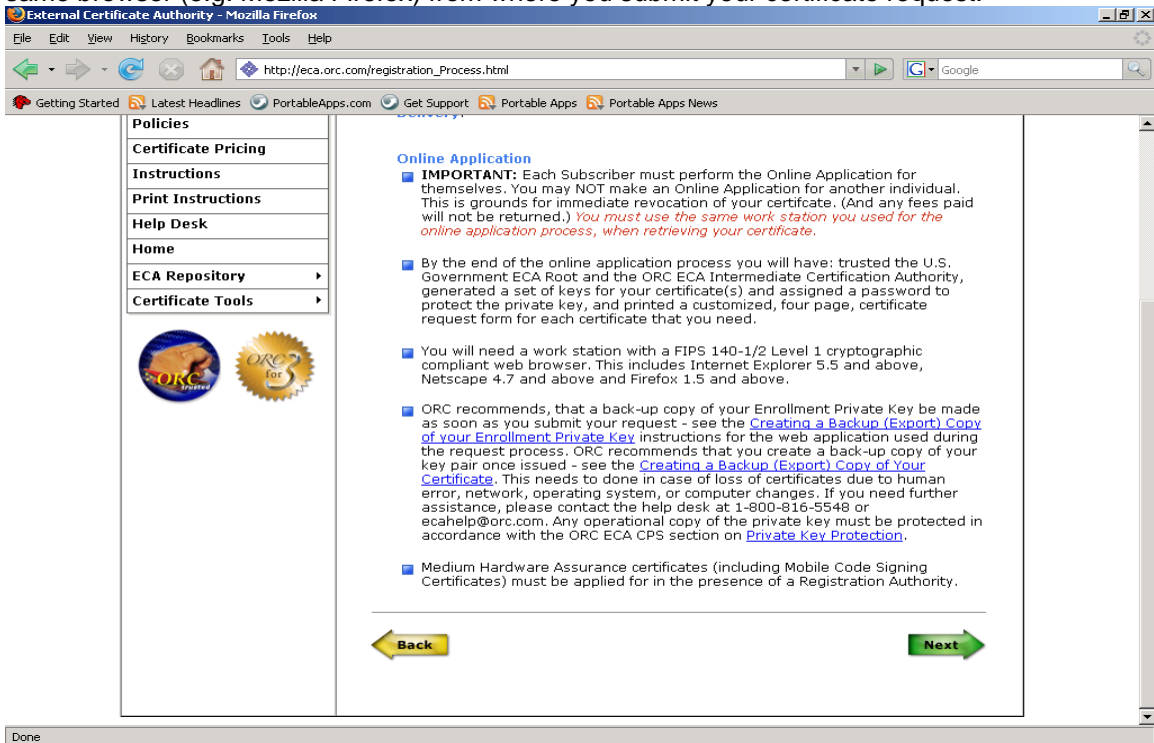


Certificate Request Instructions - Firefox

1. Depending on your citizenship, click the **Get Certificate** arrow that pertains to you to get started.



2. Click the **Next** arrow on the **Online Application** page. Please note that you will have to install your ORC ECA Identity and Encryption Certificates on the same computer and on the same browser (e.g. Mozilla Firefox) from where you submit your certificate request.



3. Click the **Next** arrow on the **Identity Verification** page. Please note that you must provide copies of two photo IDs (the first photo ID must be a valid, current, official government ID such as passport, and the second photo ID can be an official company issued photo identity badge) along with your ORC ECA Identity and Encryption Certificate request forms.

NOTE: Applicant citizenship verification requires individual applicants to provide an official credential issued by a government authority with jurisdiction over the issuance of such credentials to the applicant. For US citizenship, only the following credentials may be accepted:

- U.S. Passport
- Certified birth certificate issued by the city, county, or state of birth, in accordance with applicable local law
- Naturalization Certificate
- Certificate of Citizenship
- FS-240 – Consular Report
- DS-1350 – Certification of Report of Birth

For non US citizens, a photocopy of a passport from their country of citizenship (or nationality)

External Certificate Authority - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://eca.orc.com/registration_Process_Authentication.html

Getting Started Latest Headlines PortableApps.com Get Support Portable Apps Portable Apps News

ECA Repository

Certificate Tools

IDS.)

- **Proof of Nationality**
 - Non-US Citizens must submit a photocopy of a passport from their country of Citizenship (or Nationality)
 - US citizens may submit a photocopy of the following documents as Proof of Nationality: US Passport, birth certificate, Certificate of Naturalization, Certificates of Citizenship, FS-240 Consular Report, or DS-1350 Certification or Report of Birth.
- **Form of payment (Purchase Order Number, Check, Credit Card).**
- **Please provide **Proof of Organizational Affiliation**.** If you are using a company issued ID, as one of your two forms of photo Identification, then this will also work as your Proof of Organizational Affiliation. If you are not submitting a copy of a company issued photo ID, then you will need to submit a letter on company letterhead, signed by a Duly Authorized Company Representative, stating that you are an employee of that organization. (exp. [Individual's Proof of Organizational Affiliation Letter](#).) (NOTE: **A Proof of Organizational Affiliation letter does NOT replace one of the required photo IDs.**)
- For **Component/Server Certificates(including Domain Controller)**, please provide a [Component/Server Authorization](#) letter that designates you as the representative for your company for that certificate.
- For **Medium Hardware Assurance**, Certificate requests must be made in the presence of an ORC RA. Certificates must be requested and issued on a FIPS compliant Cryptographic Token.
- For jurisdictions other than the United States, see Appendix E of the [ORC ECA CPS](#).

Back **Next**

Done

4. Click the **Next** arrow on the **Secure Online Certificate Delivery** page

External Certificate Authority - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://eca.orc.com/registration_Process_Delivery.html

Getting Started Latest Headlines PortableApps.com Get Support Portable Apps Portable Apps News

ECA

External Certificate Authority

Certificate Order Process

Secure Online 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 you used for the online application process, when retrieving your certificate.*
- ORC recommends, 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 recommends that you create a back-up copy of your key pair once issued - see the [Creating a Backup \(Export\) Copy of Your Certificate](#). 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.*

[Back](#) [Next](#)

Done

5. Click the **Trust CA's** button on the **Trust the Certificate Authority** page.

External Certificate Authority - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://eca.orc.com/trustRootPortal.html

Getting Started Latest Headlines PortableApps.com Get Support Portable Apps Portable Apps News

ECA

External Certificate Authority

Trust the Certificate Authority

Trust the Certificate Authority

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.

If you HAVE NOT already trusted both the ECA Root Certificate Authority and the ORC ECA Certificate Authority, then please click the button below.	If you HAVE already trusted both the ECA Root Certificate Authority and the ORC ECA Certificate Authority, then please click the button below.
Trust CA's	Continue

[Back](#)

Done

6. Click on the **Click Here** button for **Step 1. Trust the ECA Root Certificate Authority**.

External Certificate Authority - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://eca.orc.com/trust_navigator.html

Getting Started Latest Headlines PortableApps.com Get Support Portable Apps Portable Apps News

ECA

External Certificate Authority

Trust the Root Certificate Authority

Order Your Certificate ▶
Policies
Certificate Pricing
Instructions
Print Instructions
Help Desk
Home
ECA Repository ▶
Certificate Tools ▶

Print and keep this page for reference. Upon clicking the link for **Step 1** below, your browser will prompt you to open the certificate prior to installing it. Follow the sequence below to trust the ECA Root Certification Authority.

Note: If you take the time to read the popup screens, you will time out. This will most likely occur after screen five. When you restart this process, Screen 6 will be the first to appear.

Screens 1-5: For the first five screens click on **Next**.
Screen 6: That completes the first part of the process, click on **Finish**.
Screen 7: Review the text and click **Next**.
Screen 8: Review the text and click **Next**.
Screen 9: Review the text and click **Next**.
Screen 10: Select all three options presented by clicking in the boxes to the left of the options, then click **Next**.
Screen 11: **Do not** select the "Warn me..." option. Click **Next**.
Screen 12: Click on the "Name" box and type **ORC ECA ROOT CA**, then Click **Finish**.

♦ **Step 1. Trust the ECA Root Certificate Authority** :: [Click Here](#)

♦ **Step 2. Obtain Your Certificate** :: [Click Here](#)

7. Check the three boxes on the **Downloading Certificate** prompt, then click **OK**

Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "ECA Root CA" for the following purposes?

Trust this CA to identify web sites.
 Trust this CA to identify email users.
 Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

[View Examine CA certificate](#)

[OK](#) [Cancel](#)

8. Click on the **Click Here** button for **Click Step 2. Obtain Your Certificate.**

The screenshot shows a Mozilla Firefox browser window with the URL http://eca.orc.com/trust_navigator.html. The page features a header with the ECA logo and the text "External Certificate Authority". A left sidebar contains a menu with items: "Order Your Certificate", "Policies", "Certificate Pricing", "Instructions", "Print Instructions", "Help Desk", "Home", "ECA Repository", and "Certificate Tools". Below the menu are two circular logos for "ORC" and "ORC for 3". The main content area is titled "Trust the Root Certificate Authority" and contains the following text:

Trust the Root Certificate Authority

Print and keep this page for reference. Upon clicking the link for **Step 1** below, your browser will prompt you to open the certificate prior to installing it. Follow the sequence below to trust the ECA Root Certification Authority.

Note: If you take the time to read the popup screens, you will time out. This will most likely occur after screen five. When you restart this process, Screen 6 will be the first to appear.

Screens 1-5: For the first five screens click on **Next**.
Screen 6: That completes the first part of the process, click on **Finish**.
Screen 7: Review the text and click **Next**.
Screen 8: Review the text and click **Next**.
Screen 9: Review the text and click **Next**.
Screen 10: Select all three options presented by clicking in the boxes to the left of the options, then click **Next**.
Screen 11: **Do not** select the "Warn me..." option. Click **Next**.
Screen 12: Click on the "Name" box and type **ORC ECA ROOT CA**, then Click **Finish**.

At the bottom, there are two steps with "Click Here" buttons:

- Step 1. Trust the ECA Root Certificate Authority :: [Click Here](#)
- Step 2. Obtain Your Certificate :: [Click Here](#)

The browser's status bar at the bottom shows the URL: <https://eca-ca-2.orc.com/getCAChain?op=download&mimeType=application/x-x509-ca-cert>

9. On the **Select a Certificate** page, click on **Identity Certificate** option.

The screenshot shows a Mozilla Firefox browser window with the URL <http://eca.orc.com/choose.html>. The page features a header with the ECA logo and the text "External Certificate Authority". A left sidebar contains a menu with items: "Order Your Certificate", "Policies", "Certificate Pricing", "Instructions", "Print Instructions", "Help Desk", "Home", "ECA Repository", and "Certificate Tools". Below the menu are two circular logos for "ORC" and "ORC for 3". The main content area is titled "Select a Certificate" and contains the following text:

Select a Certificate

Select a certificate type below.

Note 1: You must first electronically submit your request for an **Identity Certificate**, prior to requesting an **Encryption or Mobile Code Signing Certificate**.

Identity Certificate

 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 may be legally linked to the owner of that certificate. The certificate may also be used for secure and authenticated email.

For certificate costs please see the [Certificate Pricing](#) link in the left menu.

If you use older versions of Outlook or Netscape for your email client, you may need to have both an Identity and Encryption Certificate in order to be able to digitally sign e-mail.

Encryption Certificate (See NOTE 1 above)

 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.

The browser's status bar at the bottom shows the text "Done".

10. Review the terms and conditions on the **Subscriber Obligations** page, then click **I Agree**

Subscriber Obligations

Online Application → Verification → Certificate Delivery

In order to request and use an **Identity Certificate** issued under the ORC ECA CPS you (the subscriber) must agree to the following obligations.

- 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.
- To immediately report to an RA or LRA and request certificate revocation if [Private Key Compromise](#) is suspected.
- To use the certificate only for authorized applications which have met the requirements of the US Government ECA CP and the ORC ECA CPS.
- To use the certificate only for the purpose for which it was issued, as indicated in the key usage extension.
- To report any changes to information contained in the certificate to the appropriate RA or LRA for certificate reissue processing.
- Abide by all the terms, conditions, and restrictions levied upon the use of private keys and certificates.

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

[Back](#) [I Agree](#)

11. Complete the **Certificate Enrollment Form**, select your **Validity Period** (e.g. One Year - \$99), and then click **Submit**. Please note that if you encounter the Save New DataCard prompt, you should cancel if you do not want to save data in the request form.

The purpose of this enrollment is to request a **Identity Certificate** that may be used for digital signature and digital identity to access websites.

Important: You will need to use the same workstation and the same browser to accept your certificate that you are now using to request it.

Identity Certificate Enrollment: One Year - \$99

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: Mario
Middle Initial: A
Last Name: Salguero - TEST
Company Name: ORC
Country: United States

Contact Information:
Enter an email address and phone number at which you can be contacted regarding this request.

Email: salguerom@orc.com
Phone: 703-246-8537

[Back](#) [Submit](#)

12. Review your information on the **Subscriber Information** page. If you have entered all your information correctly, then click **This Is Correct**.

The screenshot shows a web application interface for the ORC ECA Identity Certificate. On the left, there is a sidebar with 'ECA Repository' and 'Certificate Tools' menus, and two circular logos: 'ORC' and 'ORC for'. The main content area is titled 'ORC ECA - One Year Identity Certificate' and contains a 'Subscriber Information' section with the following details:

- First Name: Mario
- Middle Initial: A
- Last Name: Salguero - TEST
- Company Name: ORC
- Company Email Address: salguerom@orc.com
- Company Phone Number: 703-246-8537
- Company Country: US

Below the information, there is a warning: 'If you chose to submit this form you will need to create a password when setting the security level for the private key. Please be aware that you will be the only person with this password. It is important that you remember this password, as it will not be retrievable by the certificate authority. Do not share your password with anyone.' This is followed by a recommendation: 'ORC recommends, that if you know of a network, operating system, or computer change that will take place from the time you electronically SUBMIT your request (creating your private key on the computer you are using), to when you receive the email notifying you to retrieve your public key, then please see the [Creating an Operational Copy of your Private Key](#) instructions for the web application used during the request process, located under the Instructions tab in the left tool bar on the eca.orc.com web site. If you need further assistance, please contact the help desk at 1-800-816-5548 or 703-246-8536 or pkihelp@orc.com. Any operational copy of the private key must be protected in accordance with the ORC ECA CPS section on Private Key Protection.'

At the bottom, there are two buttons: 'Make a Change' and 'This is Correct'.

13. After clicking **This Is Correct** on the ORC ECA Identity Certificate online application form, the **Master Password** window may appear when submitting through Mozilla Firefox browser. Subscriber must create his/her own private key password. The private key password is case-sensitive, and cannot be restored or reset by ORC if it is lost or forgotten. The password should be between 8 to 10 characters in length and should be alphanumeric.

14. Print out your ORC ECA Identity Certificate request form. If you do not see the yellow **Finish Line** at the bottom of the certificate request form or all pages of the ORC ECA Identity Certificate request form, please click the **Reload** current page.

The screenshot shows a browser window titled 'External Certificate Authority' displaying the 'REQUEST FOR ORC ECA IDENTITY CERTIFICATE' form. At the top, there is a red-bordered button that says 'PRINT THIS FORM NOW'. Below this, the form is titled 'REQUEST FOR ORC ECA IDENTITY CERTIFICATE' and shows 'Your request ID is 54099'. There are radio buttons for 'Certificate Validity Period': 'One Year' (selected), 'Two Years', and 'Three Years'. A message states: 'Congratulations, your request for an ECA 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 which must be a valid, current, official government ID such as a passport, driver's license, and government issued photo identity card or badge. The second photo ID can be an official company, or institutional, issued photo identity card or badge.
- Proof of Organizational Affiliation
 - If you are using a company issued ID, as one of your two forms of Identification, then this will also work as your Proof of Organizational Affiliation.
 - If you are not using a company issued photo ID, then you will need to submit a letter on company letterhead, signed by a Duly Authorized Company Representative, stating that you are an employee of that organization. (A sample letter is provided on our ECA Instructions page).
- Form of payment (Check, Credit Card, Purchase Order)
- A completed and verified copy of this Request Form

A red warning message states: 'To ensure that you have printed and are completing the entire request form, you should see a FINISH LINE at the end of the form. FINISH LINE'. At the bottom, there is a note: 'Please take this form, along with your two official photo IDs, and proof of organizational affiliation (if required, see above), to ORC's Fairfax Branch or a Notary Public for verification of'.

15. If you need to obtain your ORC ECA Encryption Certificate, click on **Continue** and proceed to apply for your ORC ECA Encryption Certificate.