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

1. Online Application

a. **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.*

b. 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.

c. 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.

d. 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 instructions for the web application used during the request process. This needs to 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.

e. Medium Hardware Assurance certificates (including Mobile Code Signing Certificates) must be applied for in the presence of a Registration Authority. Please contact ORC at 1-800-816-5548 or ecahelp@orc.com to make an appointment.

2. Identity Verification

You will need to present the following to a Notary Public **(if you are being processed outside the U.S. you need to see a U.S Consular Notary)**, an ORC Registration Authority (RA) or an authorized Local Registration Authority (LRA):

a. The request form generated during the online application process containing your request ID.

b. **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. **(NOTE: A Proof of Organizational Affiliation letter does NOT replace one of the required photo IDs.)**

c. **Proof of Nationality**

   a. Non-US Citizens must submit a photocopy of a passport from their country of Citizenship (or Nationality)

   b. US citizens may submit a photocopy of the following documents as Proof of Nationality: US Passport, birth certificate, Certificate of Naturalization, Certificate of Citizenship, FS-240 Consular Report, or DS-1350 Certification or Report of Birth.

d. **Form of payment** (Purchase Order Number, Check, Credit Card).

e. **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.)**

f. 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.

g. 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.

h. For jurisdictions other than the United States, see Appendix E of the ORC ECA CPS.

i. Once your paperwork is complete, please send the signed originals, along with payment, copies of your 2 photo IDs, proof of citizenship and proof of affiliation to ORC, Inc.,11250 Waples Mill Rd, South Tower, Suite 210, Fairfax, VA 22030, attn: ECA RA.

3. Certificate Delivery

a. You will receive a Certificate Issuance Notification email. This email will tell you how to import, test, and back-up your certificate(s).

b. You must use the same work station you used for the online application process, when retrieving your certificate.

c. As stated in the Online Application Section above, 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 instructions for the web application used during the request process. This needs to 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.*

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 CAs page at http://eca.orc.com.

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 at http://eca.orc.com.