## What this document is for...

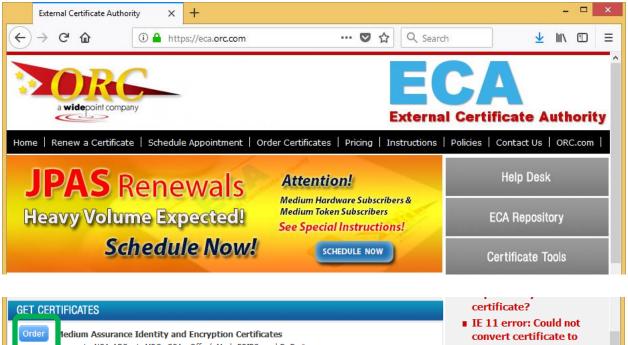
This instruction was created to assist you in making certificate requests for ECA Medium Assurance certificates (browser-based certificates), only. If you require ECA Medium-Token Assurance certificates or ECA Medium-Hardware Assurance certificates (smart card-based certificates) please send an email to <a href="mailto:ecahelp@orc.com">ecahelp@orc.com</a> and request instructions for those assurance levels.

Medium Assurance certificates (browser-based certificates) are the lowest assurance level defined under the DoD ECA Certificate Policy. They are the easiest to obtain. Some DoD activities (like JPAS) require that you use a higher assurance level of certificate to access their site(s). If the web site or activity that you wish to access specifies Medium-Token Assurance or Medium-Hardware Assurance, do not follow these instructions. If the web site or activity that you wish to access does not specify the assurance level or specifies Medium Assurance, then this should be all that you need.

# Why use Mozilla Firefox?

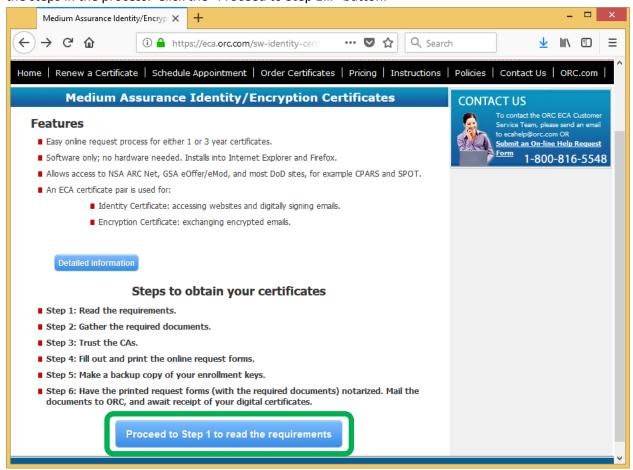
Mozilla Firefox has its own cryptographic module (its own certificate store) so it is often not bound by restrictions that are on the computer's operating system. And Mozilla Firefox works basically the same across all platforms (i.e. it works the same on a PC and a Mac). Some users find many certificate actions to be more straight-forward in Firefox than in other browsers. Additionally, you can pull your certificates out of Mozilla Firefox to install into other browsers and/or to install on other computers. So you can use Firefox as a tool to obtain your certificates and then install them where you wish after you have made back-up files. You can obtain Mozilla Firefox here: <a href="https://www.mozilla.org/en-US/">https://www.mozilla.org/en-US/</a>

1. In the Mozilla Firefox browser, go to <a href="https://eca.orc.com">https://eca.orc.com</a> Scroll down and click the Order button for Medium Assurance Identity and Encryption certificates.

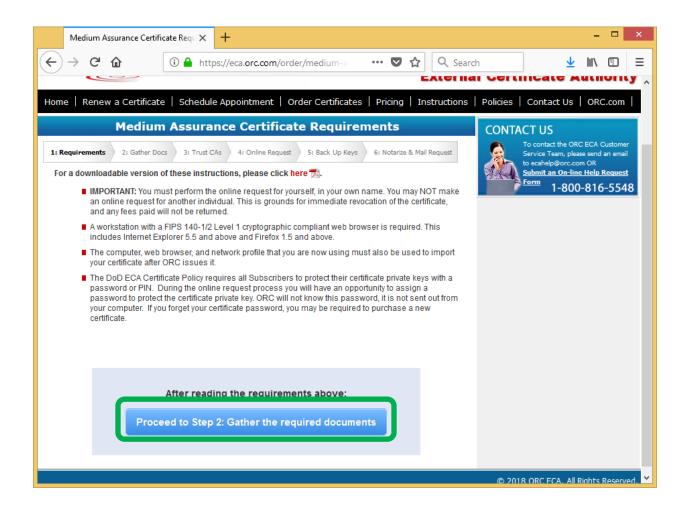




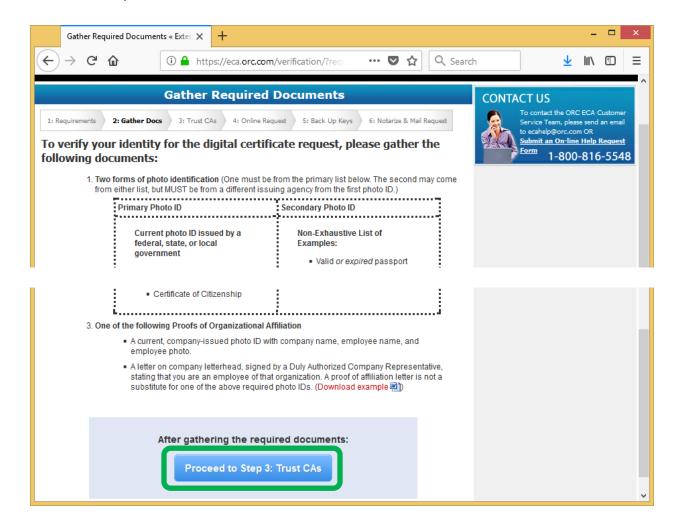
2. This page just gives a description of the features of a Medium Assurance ECA certificate and lays out the steps in the process. Click the "Proceed to Step 1..." button.



3. This page gives basic requirements for Medium Assurance ECA certificates. The pages also states, very clearly, that each individual must do this for themselves. You may not make a certificate request for someone else. Click the "Proceed to Step 2..." button.

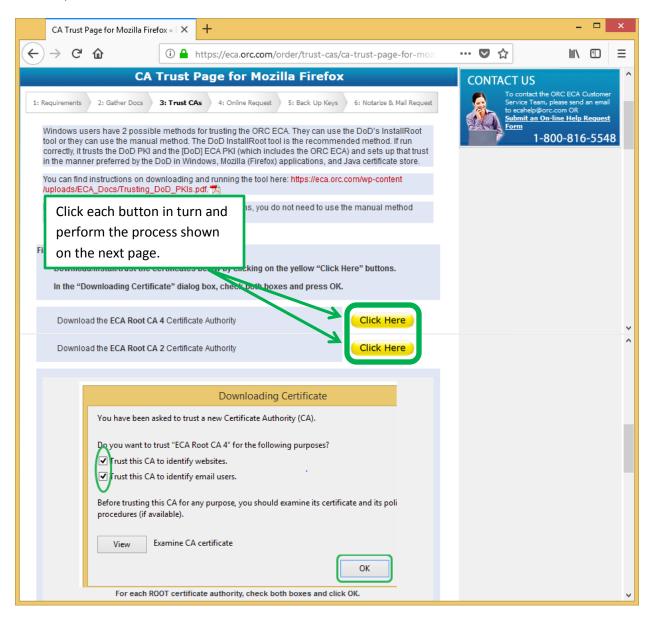


4. This page tells you about the documents you will need to present for Identity Proofing (Identity Verification) later. You don't need them right now, but you will need them later. Click the "Proceed to Step 3..." button.



5. This page tells you to how to manually trust the ORC ECA <u>Certificate Authority (CA)</u> in Mozilla Firefox. Most commercial CAs are 'pre-trusted' in Firefox when you install it. But most of the US Federal Government CAs are not pre-trusted, so you will need to do this following this process.

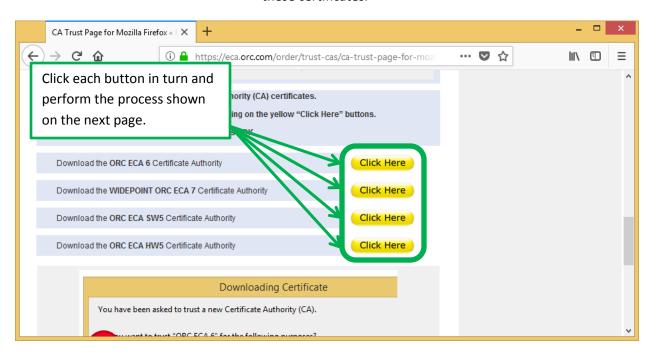
First, we will trust the Root CAs ...



For each yellow "Click Here" button; click the button and then check the check boxes and click the OK button.



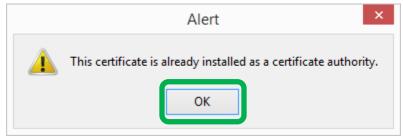
Then we will install the Intermediate CA certificates. You will <u>not</u> check the boxes to specifically trust these certificates. They will have trust inherited from the Root CAs. Scroll down and select these certificates.



For each yellow "Click Here" button; click the button (but <u>do not</u> check the check boxes) and click the OK button.



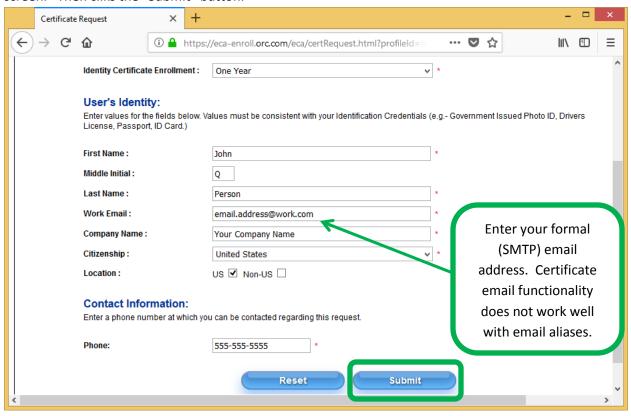
If you click a button and it says that the certificate is already installed, it means that it has already been done, just cick OK and move on to the next yellow "Click Here" button.



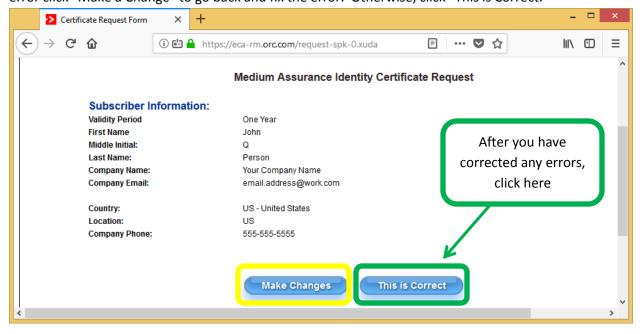
6. When you have trusted all of the CAs, click the "Proceed to Step 4..." button.



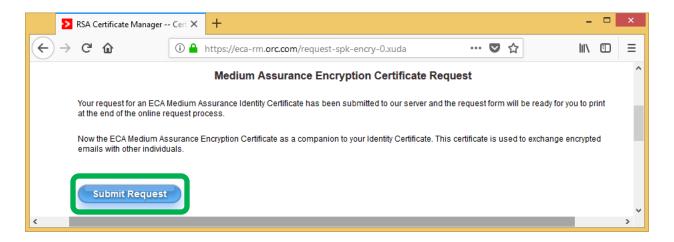
7. Select the validity period that you desire and enter your information into the fields on the screen. Then cliks the "Submit" button.



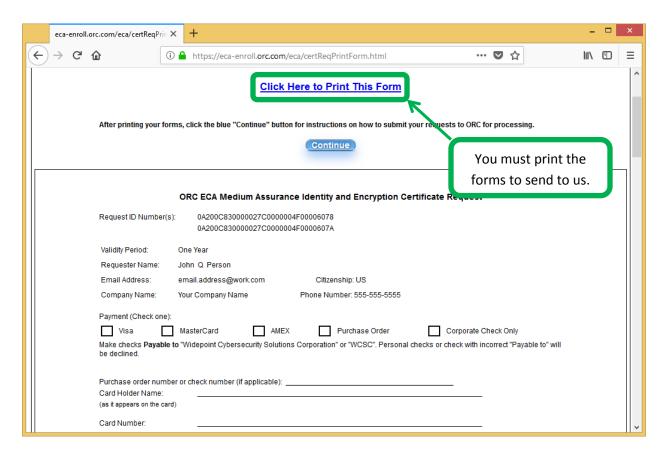
8. Verify the accuracy of the information that you are sending to our server. Be very careful regarding typographical errors, if any part is wrong, the whole thing is wrong. If you find an error click "Make a Change" to go back and fix the error. Otherwise, click "This is Correct."



9. Firefox will generate a private/public key pair (the core of what will become your Identity certificate) and send the public key to our CA server. When the CA server gets that public key, you will get a web page instructing you to Submit the request for the companion Encryption certificate. Click the Submit button to continue.

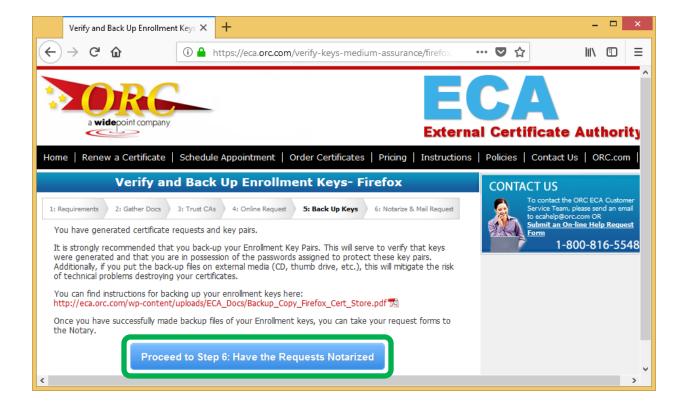


10. Firefox will generate a private/public key pair (the core of what will become your Encryption certificate) and send the public key to our CA server. When the CA server gets that public key, you will get a Certificate Request page on the screen and be instructed to print the form before you continue. The printed form should be about 3 pages long.

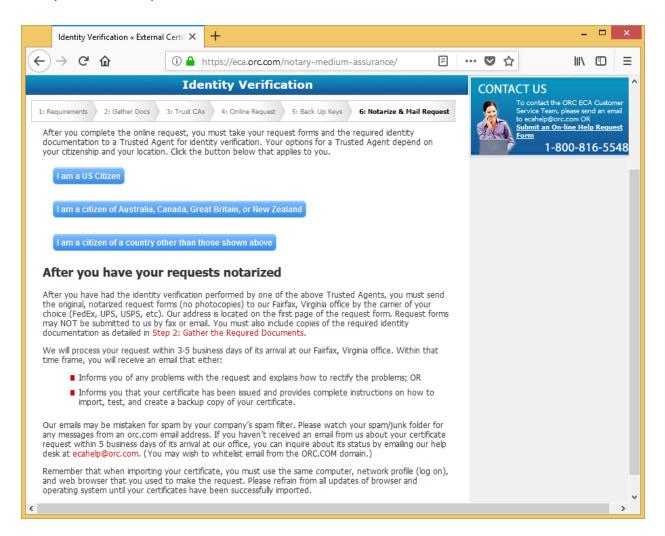


11. After printing the form, you are done making the on-line requests. You may click the Continue button. This page contains a link to instructions on how to make a back-up copy of your entire Firefox profile (which contains the Firefox certificate store). This process is not required, but it can be used to restore a certificate that is 'lost' if Firefox should be un-installed or updated. This process is also <u>not</u> a substitute for making back-up files of you finished certificates after we issue them. Please make back-up files when you are specifically directed to do so.

Click the "Proceed ..." button



12. This last page provides instruction on having Identity verification performed (these instructions are also included on the third page of the printed request forms) and explains what will happen after you send the request forms to us.



This concludes the certificate request process.

Remember that you should always protect your certificate with a password, whether it's stored in your browser or saved as a backup copy. If you haven't already set a master password in Firefox to safeguard your certificate, take a moment to do it now. Here's a link to our instructions on how to do that: https://eca.orc.com/wp-content/uploads/ECA\_Docs/Firefox\_Instructions/Set\_Password\_Firefox.pdf