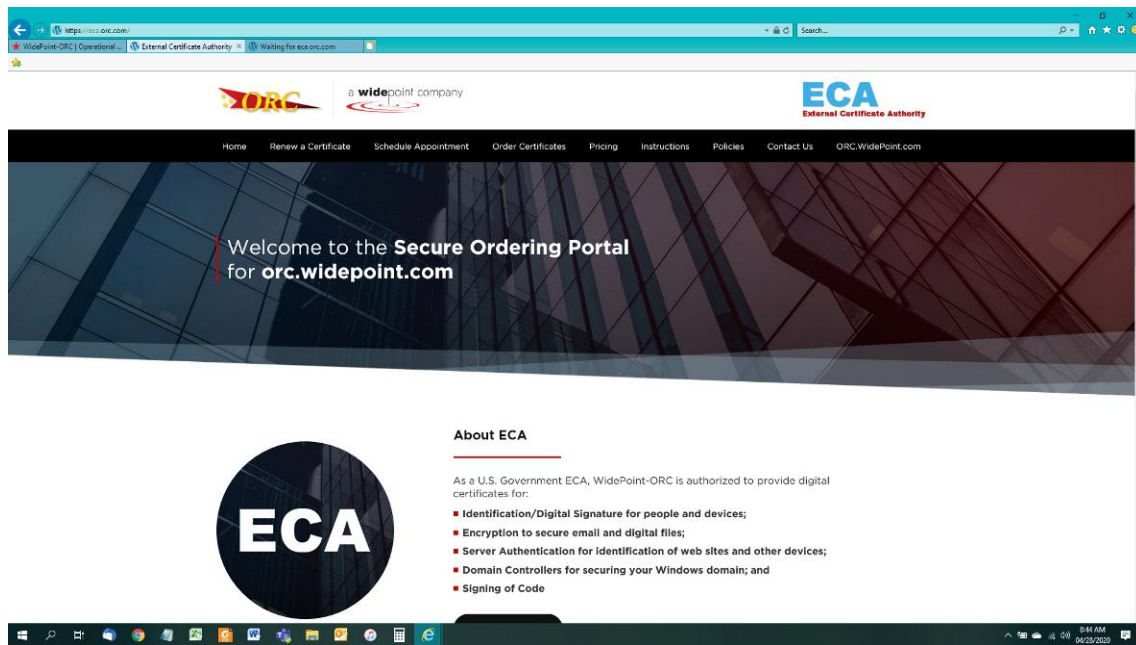


Instructions for requesting ECA Medium Assurance (browser based) certificates via Internet Explorer.

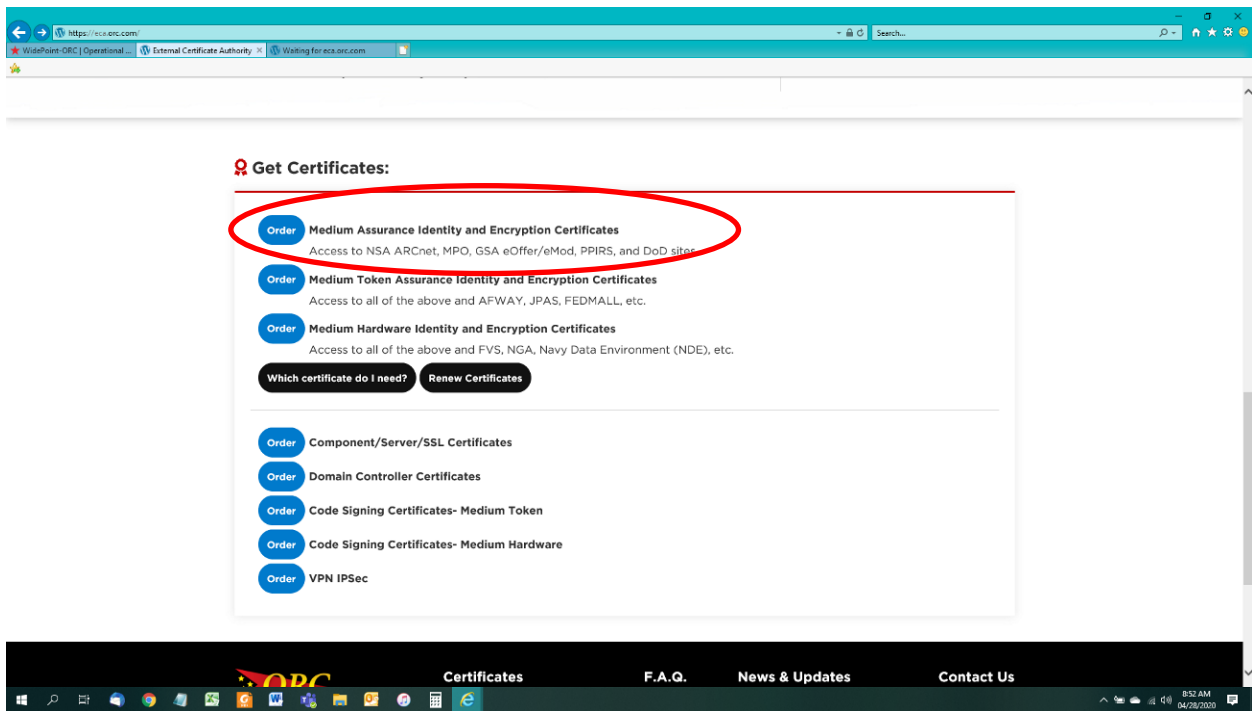
IMPORTANT: These instructions are written step-by-step; do not perform an action before the instructions tell you to do so.

A NOTE TO INTERNET EXPLORER APPLICANTS – Do not try to make certificate requests with the Microsoft Edge browser; open Internet Explorer, instead. When performing certificate functions with Internet Explorer, you are really dealing with the Windows operating system. This means that there can be many Windows configuration variables that ORC cannot anticipate. You *must* be logged on to your computer under your **normal user profile** (or Username) [Sometimes people get help from their IT support personnel. Often, IT support personnel will log-on to the computer as the Administrator; but we want the user logged on now, not the Administrator.]

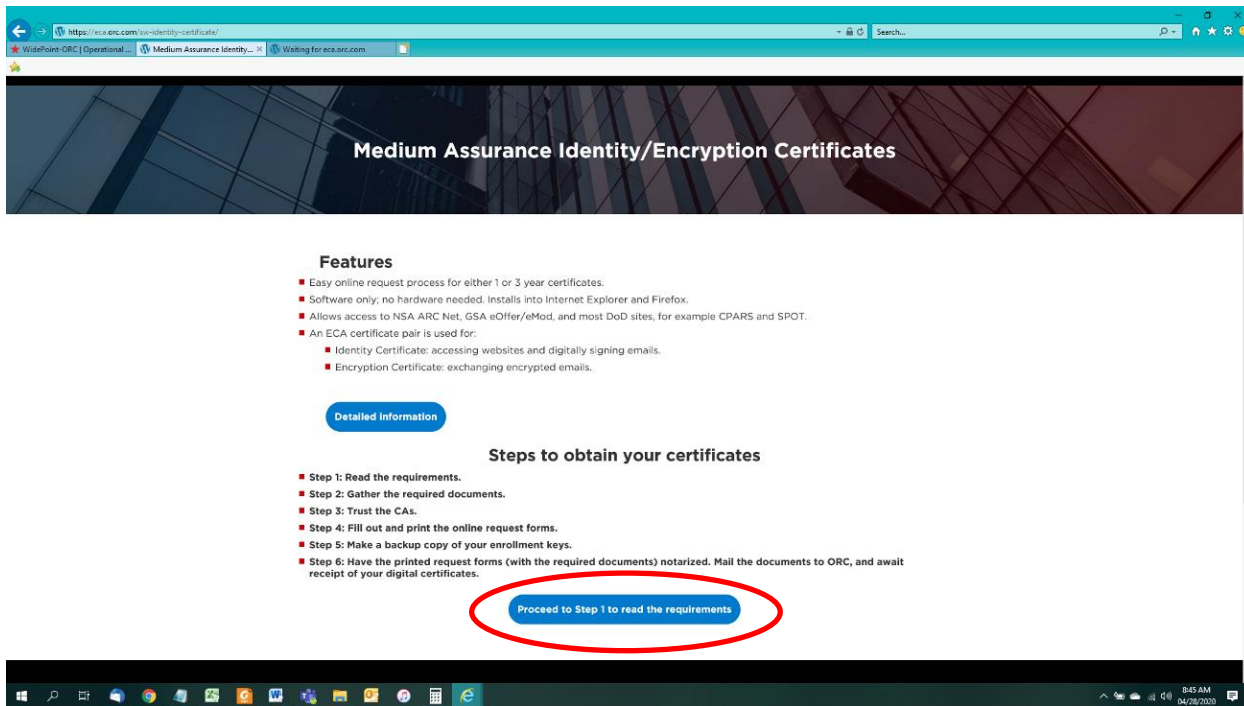
1. In Internet Explorer, go to: <https://eca.orc.com/>.



2. Scroll down and click the “**Order**” button next to Medium Assurance Identity and Encryption Certificates.



3. Click on the link to “Proceed to Step 1 to read the requirements”.



4. Read the requirements, and then click on the “Proceed to Step 2” button.

1: Requirements 2: Gather Docs 3: Trust CAs 4: Online Request 5: Back Up Keys 6: Notarize & Mail Request

For a downloadable version of these instructions, please click [here](#).

- IMPORTANT:** You must perform the online request for yourself, in your own name. You may NOT make an online request for another individual. This is grounds for immediate revocation of the certificate, and any fees paid will not be returned.
- A workstation with a FIPS 140-1/2 Level 1 cryptographic compliant web browser is required. This includes Internet Explorer 5.5 and above and Firefox 1.5 and above.
- The computer, web browser, and network profile that you are now using must also be used to import your certificate after ORC issues it.
- The DoD ECA Certificate Policy requires all Subscribers to protect their certificate private keys with a password or PIN. During the online request process you will have an opportunity to assign a password to protect the certificate private key. ORC will not know this password, it is not sent out from your computer. If you forget your certificate password, you may be required to purchase a new certificate.

After reading the requirements above:

Proceed to Step 2: Gather the required documents

- Read the requirements to present 2 photo IDs, Proof of Citizenship and Proof of Organizational Affiliation when you go through the Identity Verification process. Then click on the “Proceed to Step 3” button.

2. Proof of Citizenship	
<p>Proof of Citizenship for U.S. Citizens</p> <ul style="list-style-type: none"> Current, valid U.S. Passport (also qualifies as one of the required photo IDs) Birth certificate issued by a government entity within the US or its territories Certificate of Naturalization FS-240 Consular Report DS-1350 Certification of Report of Birth Certificate of Citizenship 	<p>Proof of Citizenship for Non-U.S. Citizens</p> <ul style="list-style-type: none"> Current, valid passport from your country (also qualifies as one of the required photo IDs) Unfortunately, Green (Permanent Resident) Cards are NOT authorized for proof of citizenship.

3. One of the following Proofs of Organizational Affiliation

- A current, company-issued photo ID with company name, employee name, and employee photo.
- A letter on company letterhead, signed by a Duly Authorized Company Representative, stating that you are an employee of that organization. A proof of affiliation letter is not a substitute for one of the above required photo IDs. ([Download example](#))

After gathering the required documents:

Proceed to Step 3: Trust CAs

6. At this point you will need to Trust the Certificate Authority (CA).
You can follow the instructions on this page to manually trust all of the ORC ECA Certificate Authority servers. But a more effective method of doing this is to run the DoD InstallRoot tool. The DoD Installroot tool will trust all of the DoD PKI and all of the ECA PKIs very quickly. It is the recommended way to perform this process. You can run the DoD Installroot tool by referencing this instruction: https://eca.orc.com/wp-content/uploads/ECA_Docs/Trusting_DoD_PKIs.pdf When you have trusted the ECA PKI, click the “Proceed to Step 4” button.

Trust the PKIs with InstallRoot (Windows OS only)

Windows users have 2 possible methods for trusting the ORC ECA. They can use the DoD’s InstallRoot tool or they can use the manual method. The DoD InstallRoot tool is the recommended method. If run correctly, it trusts the DoD PKI and the [DoD] ECA PKI (which includes the ORC ECA) and sets up that trust in the manner preferred by the DoD in Windows, Mozilla (Firefox) applications, and Java certificate store.

You can find instructions on downloading and running the tool here: https://eca.orc.com/wp-content/uploads/ECA_Docs/Trusting_DoD_PKIs.pdf.

If you run the InstallRoot tool according to our instructions, you do not need to use the manual method below.

Step A. Trust the ECA Root CA 4 Certificate Authority

[Click Here](#)

Step B. Trust the ECA Root 2 Certificate Authority

[Click Here](#)

Step C. Trust the ECA 6 Certificate Authority

[Click Here](#)

Step D. Trust the ECA 7 Certificate Authority

[Click Here](#)

Step E. Trust the ORC ECA CA SW5 Certificate Authority

[Click Here](#)

Step F. Trust the ORC ECA CA HW5 Certificate Authority

[Click Here](#)

Do this
OR
This
You do not
need to do
both

After installing the Certificate Authorities:

[Proceed to Step 4: Request Your Certificates](#)

You already
did this (and
more) when
you ran the
InstallRoot
files.

7. On the application page, select the desired Validity Period (One or Three 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.

Home Certificate Request Contact Us

Medium Assurance Identity Certificate Request

Identity Certificate Enrollment : Select Validity Period *

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 : *

Middle Initial :

Last Name : *

Work Email : *

Company Name : *

Citizenship : United States *

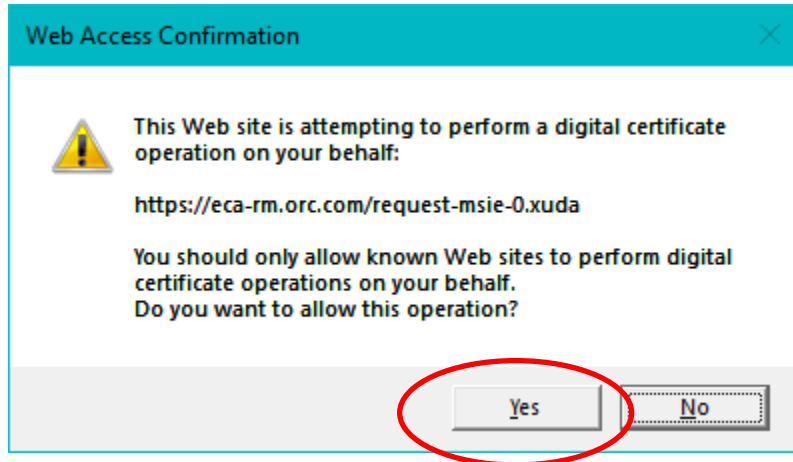
Location : US ☒ Non-US ☐

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

Phone: *

This is sample data, please enter your information

8. If you see a Web Access Confirmation dialogue box, click Yes



9. 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.)

ECA
External Certificate Authority

Home Certificate Request Contact Us

Medium Assurance Identity Certificate Request

Subscriber Information:

Validity Period: One Year
 First Name: John
 Middle Initial: Q
 Last Name: Smith
 Company Name: YourCompanyName
 Company Email: YourEmail@work.com
 Country: US - United States
 Location: US
 Company Phone: 555-555-5555
 Cryptographic Service Provider: Microsoft Enhanced Cryptographic Provider v1.0

Buttons: Make Changes, This is Correct

Annotations:
 - Red box around 'YourEmail@work.com' with text: 'This is critical; it MUST be correct'
 - Red box around 'Make Changes' with text: 'If you need to make a change, do so here'

10. When you get the Creating a new RSA exchange key dialog box, click the Set Security Level button.

Creating a new RSA exchange key

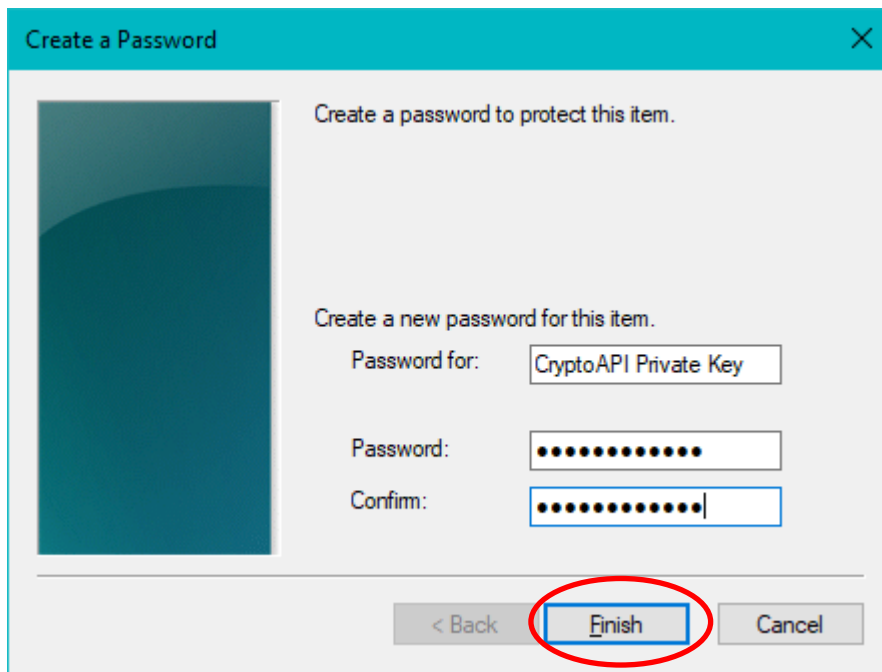
An application is creating a Protected item.

CryptoAPI Private Key

Security level set to High

Buttons: OK, Cancel, Details..., Set Security Level...

11. You must assign a password to protect your Identity certificate (and its private key). This will be your certificate password from here on. Your computer will require you to set a password of the same complexity level as your log on password. Please choose a password that you can remember; ORC will not have your password and cannot reset it for you if you can't remember it later. *(While much of this process happens over the internet, the password assignment is happening only on your computer. The password does not leave your computer and is not sent to ORC.)* After you have assigned a password, click the Finish button.



Create a Password

Create a password to protect this item.

Create a new password for this item.

Password for: CryptoAPI Private Key

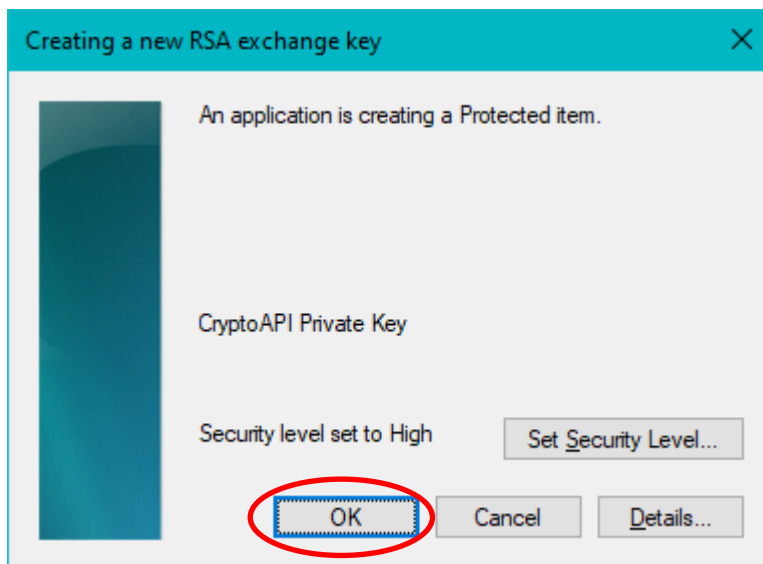
Password:

Confirm:

< Back Finish Cancel

The 'Create a Password' dialog box has a teal header bar with the title 'Create a Password' and a close button. The main area is light gray. On the left is a teal vertical bar. The text 'Create a password to protect this item.' is at the top. Below it, 'Create a new password for this item.' is followed by three input fields: 'Password for:' containing 'CryptoAPI Private Key', 'Password:' with ten dots, and 'Confirm:' with ten dots and a cursor. At the bottom are three buttons: '< Back' (disabled), 'Finish' (active, circled in red), and 'Cancel' (disabled).

12. You may now click the OK button.



Creating a new RSA exchange key

An application is creating a Protected item.

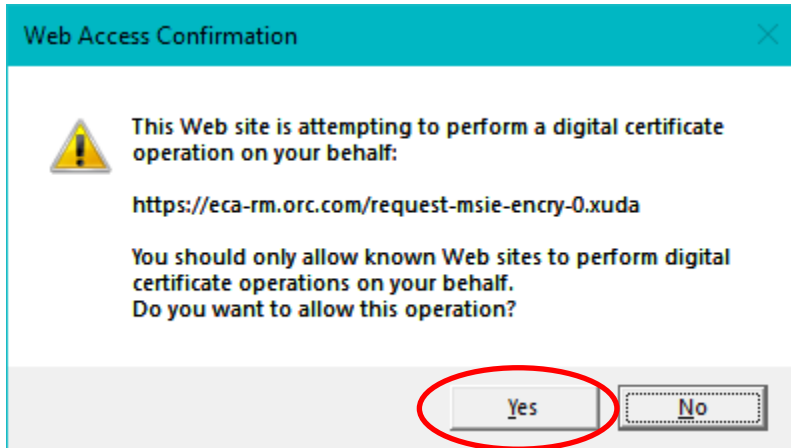
CryptoAPI Private Key

Security level set to High Set Security Level...

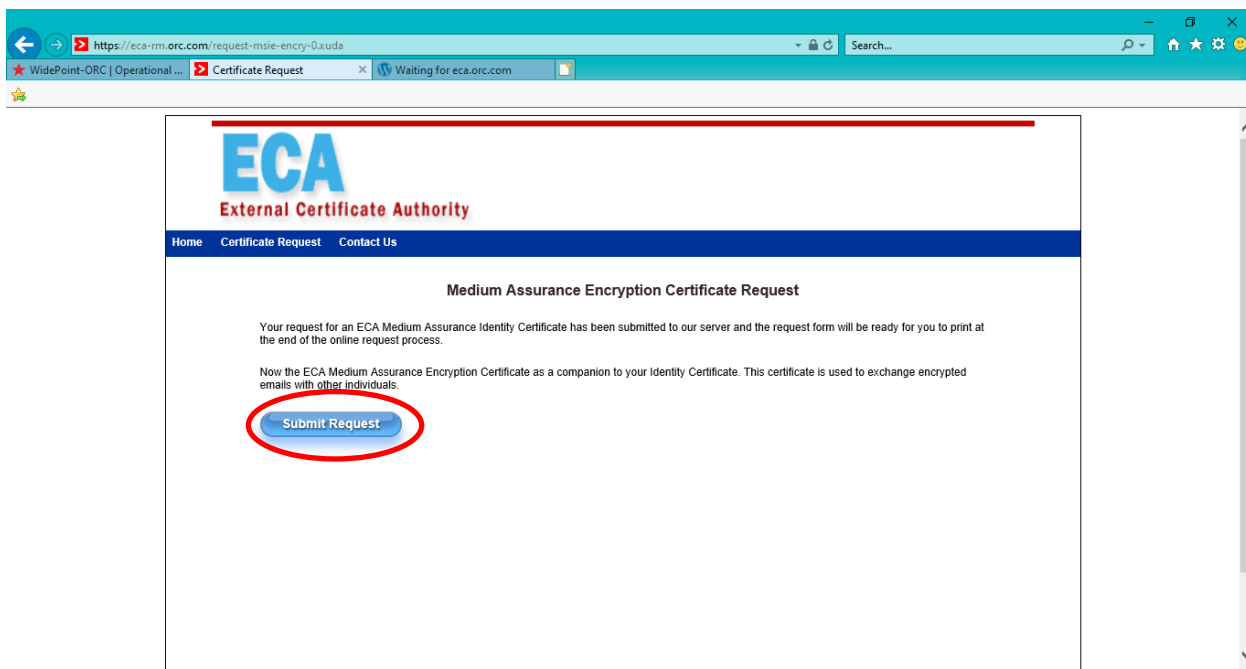
OK Cancel Details...

The 'Creating a new RSA exchange key' dialog box has a teal header bar with the title 'Creating a new RSA exchange key' and a close button. The main area is light gray. On the left is a teal vertical bar. The text 'An application is creating a Protected item.' is at the top. Below it is 'CryptoAPI Private Key'. Then 'Security level set to High' is followed by a 'Set Security Level...' button. At the bottom are three buttons: 'OK' (active, circled in red), 'Cancel' (disabled), and 'Details...' (disabled).

13. If you see a Web Access Confirmation dialogue box, click Yes



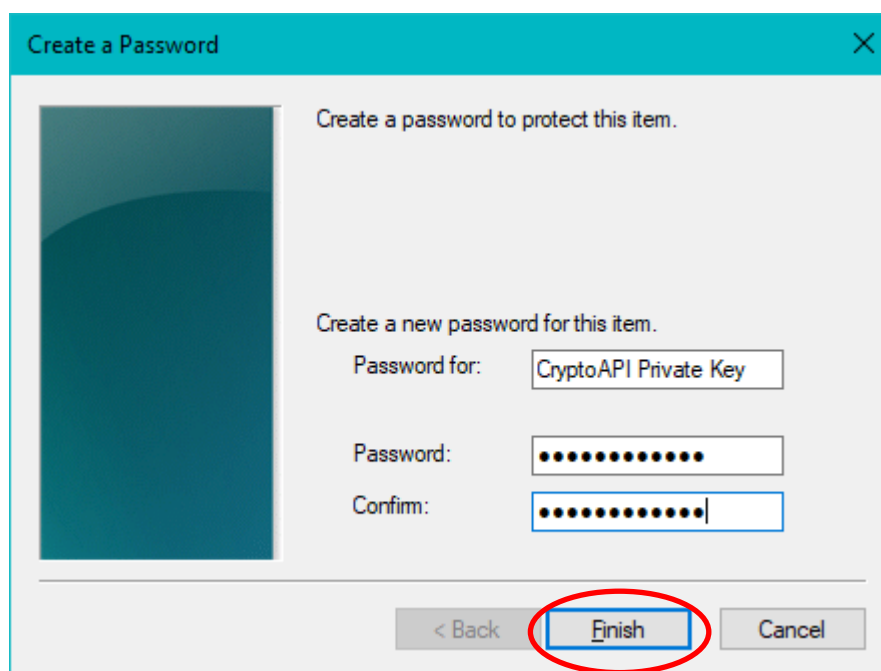
14. Your computer has generated the private/public keys for your Identity certificate. Now click the Submit button to request your Encryption certificate.



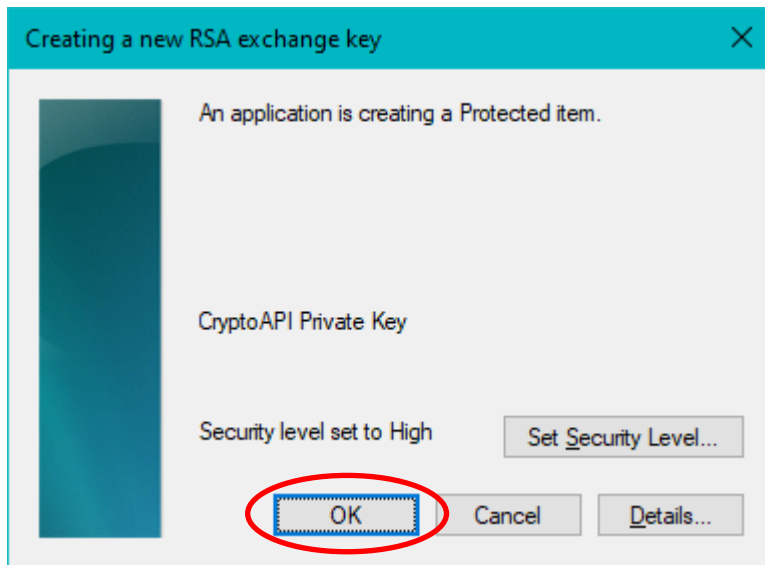
15. When you get the Creating a new RSA exchange key dialog box, click the Set Security Level button.



16. You must assign a password to protect your Encryption certificate (and it's private key). You may use the same password for your Encryption certificate as you used for your Identity certificate. This will be your certificate password from here on. Your computer will require you to set a password of the same complexity level as your log on password. Please choose a password that you can remember; ORC will not have your password and cannot reset it for you if you can't remember it later. *(While much of this process happens over the internet, the password assignment is happening only on your computer. The password does not leave your computer and is not sent to ORC.)* After you have assigned a password, click the Finish button.



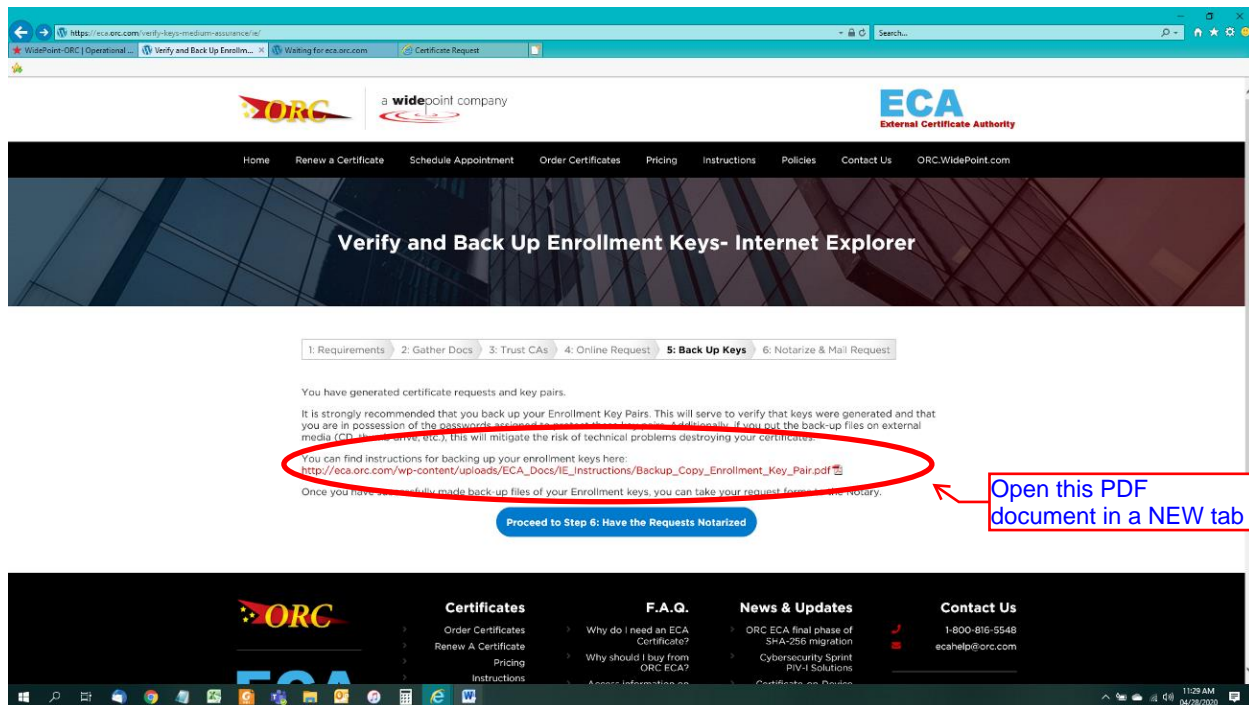
17. You may now click the OK button.



18. The request form is displayed on the screen. Please click the link to print the Request form. The printed request form should be three (3) pages long. The third page is instructions. After the form has printed, click the Continue button.

A screenshot of a web browser window showing the "External Certificate Authority" page. The browser's address bar shows the URL "https://eca-enroll.orc.com/eca/certMsrReqPrintForm.html". The page has a blue header with "Home", "Certificate Request", and "Contact Us" links. Below the header, there is a link "Click Here to Print This Form" circled in red. Below that, there is a blue "Continue" button also circled in red. A red arrow points from the "Continue" button to a text box on the right that says "Please print Then click the continue button". The main content area is titled "ORC ECA Medium Assurance Identity and Encryption Certificate Request" and contains a form with fields for Request ID Number(s), Validity Period, Requester Name, Email Address, Company Name, Citizenship, and Phone Number. There are also checkboxes for Payment (Check one) and a section for Purchase order number or check number.

19. You have completed the Certificate Request process. The next page asks you to verify and back-up your certificate key. This procedure will mitigate the risk of technical problems ‘destroying’ your certificate. Instructions for doing so are referenced on the page.



The RSA Key Pairs are generated in your Windows certificate store. There will be an RSA key for each certificate request that you have made. Your computer will look for this RSA Key Pair when you attempt to import the issued certificate from the certificate server. This RSA Key Pair is NOT YET a certificate; it is, rather, the 'foundation' of the certificate (i.e. - the RSA Key Pair will become the certificate). It has real value prior to your certificate being issued.

20. After backing up your RSA keys, click the button to “Proceed to Step 6”
21. Click the button that corresponds to your citizenship status. Read all of the information provided and follow the instructions on this page to submit your request forms to ORC.

(See following page for screenshot.)

https://eca.orc.com/notary-medium-assurance/

WidePoint-ORC | Operational... Identity Verification - Extern... Waiting for eca.orc.com Certificate Request

Identity Verification

1: Requirements 2: Gather Docs 3: Trust CAs 4: Online Request 5: Back Up Keys 6: Notarize & Mail Request

After you complete the online request, you must take your request forms and the required identity documentation to a Trusted Agent for identity verification. Your options for a Trusted Agent depend on your citizenship and your location. Click the button below that applies to you.

I am a US Citizen

I am a citizen of Australia, Canada, Great Britain, or New Zealand

I am a citizen of a country other than those shown above

After you have your requests notarized

After you have had the identity verification performed by one of the above Trusted Agents, you must send the original, notarized request forms (no photocopies) to our Fairfax, Virginia office by the carrier of your choice (FedEx, UPS, USPS, etc). Our address is

11:25 AM 04/28/2020

22. The application process is complete.