

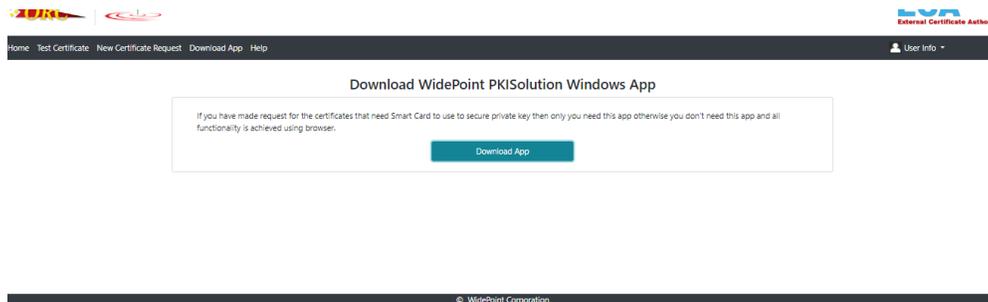
Medium Token Certificates:

Downloading the Widepoint PKI Solutions Application:

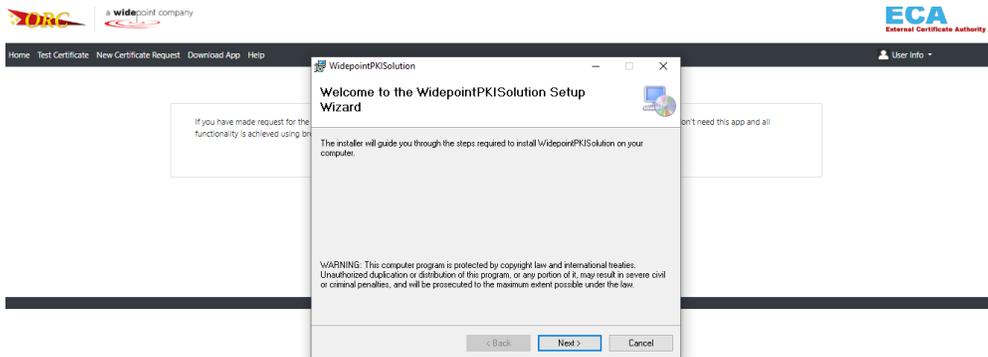
The Widepoint PKI Solutions application is a downloadable application once your certificate has been issued. This is where you will generate your private keys and install your certificates directly onto your smartcard/token.

Note: To install this application on your computer you will need to reach out to your internal IT for permission or you possibly might need Admin permissions in order to install on your machine.

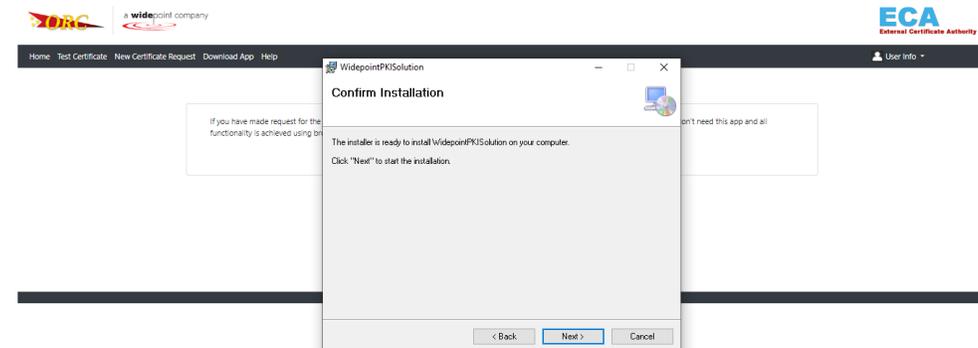
Step 1: Once you finish making your request you can move to the “Download App” tab at the top which will take you to the below screen.



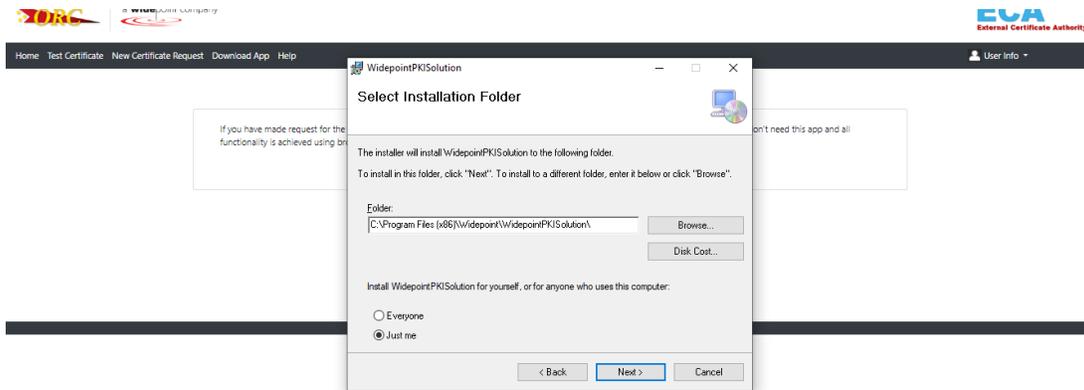
Step 2: Once you hit ‘Download App’ the installer should then populate, you will click ‘Next’.



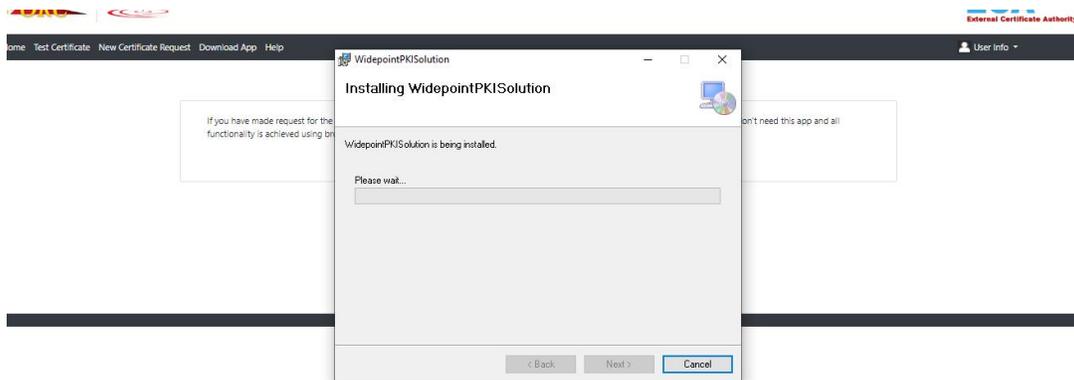
Step 3: You will then leave the settings on the installer as shown below and click ‘Next’.



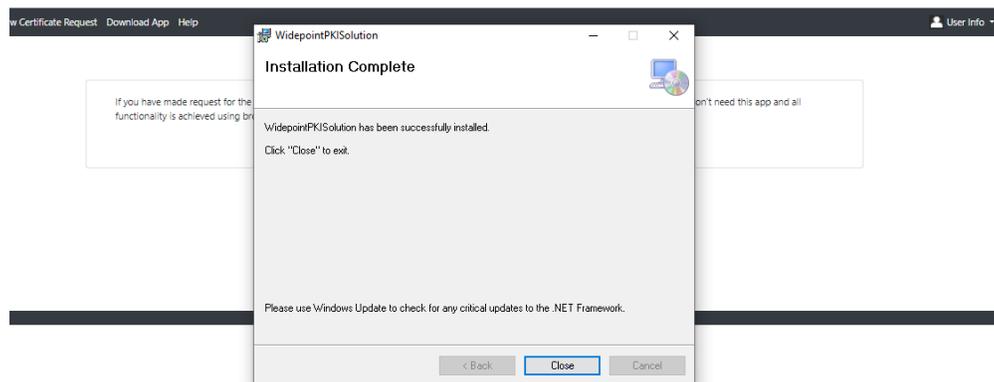
Step 4: To confirm installation you will then click 'Next' – this is where you might need to allow through Microsoft pop-up in order for installation to go through or possibly admin access depending on internal security measures.



Step 5: You will then wait for the downloader to fully load; this process can take up to a few minutes depending on your Wi-Fi connection. If it takes longer than 10 minutes, please consult your local IT/system admin for assistance.



Step 6: Installation should be completed, you can click Close out of the installer.



Step 7: Once your certificates have been processed and issued from Widepoint - ORC you should receive the below email to the email address you utilized when creating your account. Please read the full email and instructions below on how to install your newly issued certificates.

Congratulations! Your WidePoint ECA 8 Medium Assurance Certificates are ready to be downloaded. Contact ecahelp@orc.com if you have any issues with these instructions.

NEVER DELETE/REMOVE YOUR CERTIFICATES FROM THE MICROSOFT MANAGEMENT CONSOLE (MMC) OR WINDOWS CERTIFICATE STORE WITHOUT FIRST CONSULTING THE WIDEPOINT/ORC HELP DESK (ecahelp@orc.com)!!!

NOTE: Import your certificates as soon as possible. If you fail to install both of your certificates within 30 days of making the certificate request, you will be required to reapply and pay for new certificates.

PLEASE READ ALL INSTRUCTIONS CAREFULLY BEFORE IMPORTING CERTIFICATES

You MUST ensure that the trust chain for your certificates is properly installed in the computer prior to attempting to import the certificates; otherwise, you will lose your certificates. Please follow these instructions to check the trust chain (Checking ECA 8 Trust Chain.docx). If it is NOT installed properly, go to our ECA Web Site, click on the Instructions Tab in the black menu bar across the top of the web page, then click on Microsoft Instructions in the list displayed, then open and follow the PDF Instructions entitled 'Trusting the DOD PKI and ECA PKI in IE.' Then, close the MMC Screen if it is still open and access the Current User - MMC again to check if the trust chain installed properly according to the PDF in the second line in this paragraph. If it still is not installed properly, **STOP**. Contact ecahelp@orc.com.

In addition to the Username and Password for your Account with us, you will need to assign a password to your certificates (it should be a different password than your Account Password). We have ways for you to reset your Account Password; however, you CANNOT reset your **certificate** password unless you know the one assigned to your certificates. So, **CAREFULLY follow the instructions on the site for your certificate password to ensure that you do NOT lose it or make a typo error after or when assigning it!!!**

Log into your ECA Account at our web site <https://certificateenroll.orc.com/enroll/sub/login.html> Select the 'Get Cert' Button for your Identity Certificate to download it. Then, select the 'Get Cert' Button for your Encryption Certificate to download it.

To check that both certificates downloaded properly and to install them into the Windows Certificate Store, follow these instructions https://eca.orc.com/wp-content/uploads/ECA_Docs/IE_Instructions/Import_Medium_Assurance_Certs_into_WindowsCertStore.pdf

To test your identity certificate, copy and paste the following URL <https://eca.orc.com/certificate-test/> into one of your browsers, strike the Enter Key, and provide your certificate password (if prompted). You should get the message, "Your client certificate is valid and expires in about --- days, and You presented an ECA Medium Assurance Certificate."

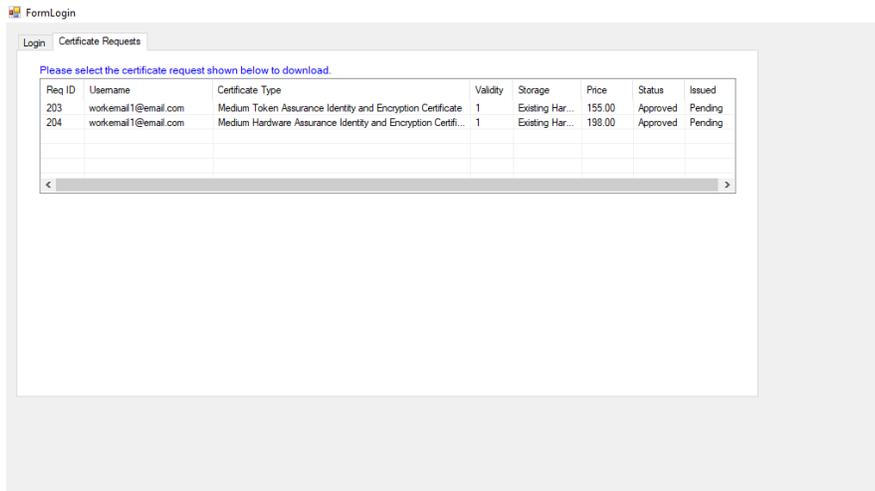
If you should encounter any problems, please contact the ORC ECA PKI Helpdesk at ecahelp@orc.com.

Thank you for choosing WidePoint/ORC!

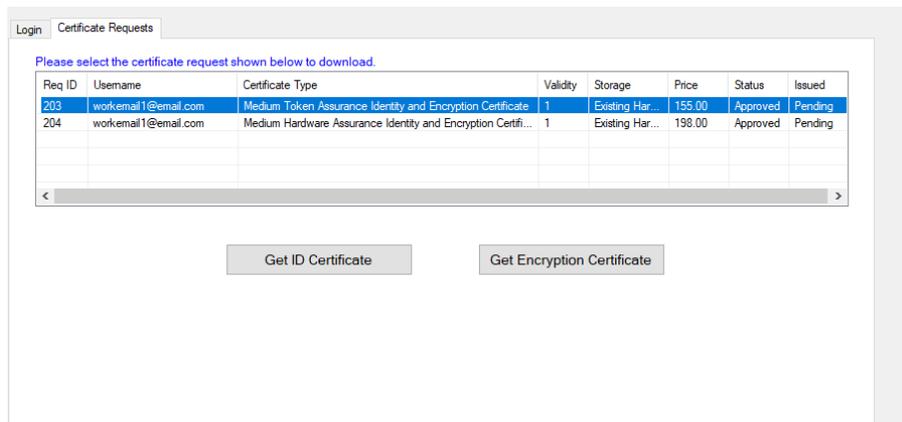
Step 8: You **MUST** have ActivClient Software installed on your PC before attempting to import your certificates and you must leave the token/smartcard inserted into your machine when installing the software. If you do not have a copy of the software license please reach out to your internal IT to see if they have an extra license, if not you can purchase one here: <https://www.scbolutions.com/express/index.php?cPath=32>.

Step 9: You will need to ensure you trusted the Certificate Authorities or CA's by following the attached instructions if you have not done so already https://eca.orc.com/wp-content/uploads/ECA_Docs/IE_Instructions/Checking_ECA_8_Trust_Chain.pdf

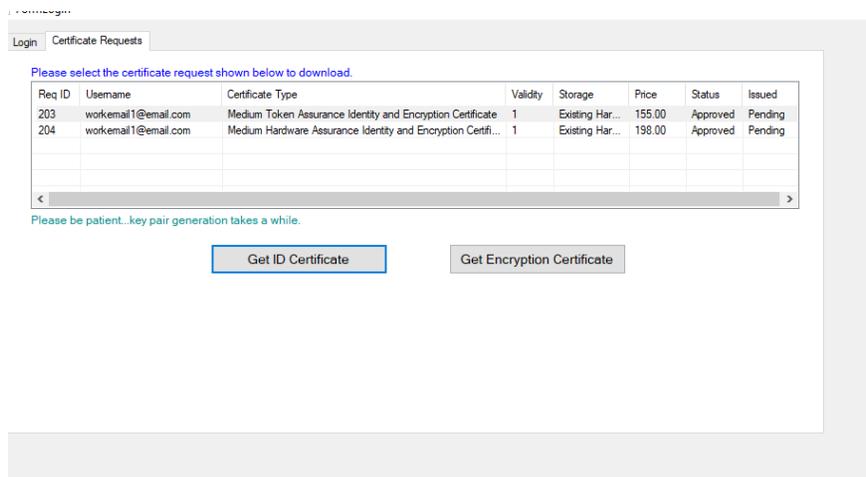
Step 10: You will then open up the WidepointPKI Solutions application by following the attached instructions: https://eca.orc.com/wp-content/uploads/ECA_Docs/IE_Instructions/Opening_WidePoint_Proprietary_App.pdf. Once you open the application and login with your account credentials you created when making the request you should see the below screen. (For reference purposes the above is showing both a set of Medium Token and Medium Hardware certificates being issued, you should only have one line unless you have purchased multiple sets of certificates)



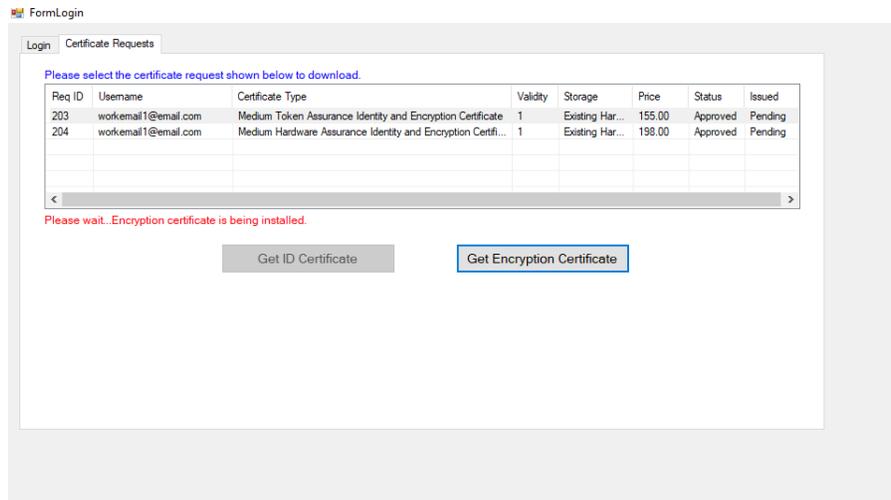
Step 11: You select your certificate and will get two options to install your identity and encryption certificate. **At this point if you do not already you need to ensure your smartcard/token is inserted into your computer or this process will error out or could corrupt the installation process.**



Step 12: Once you click Get ID/EN Certificate you should see the below message populate. At this point Key Pair Generation is occurring let it complete.



Step 13: Once the Key Pair Generation has completed you will then see the below screen of the certificate being installed on the device. At this point is when ActivClient 'User Console' might ask to verify your smartcard/token PIN.



Step 14: Once you've completed the process to install both the Identity and Encryption certificate, you can open the User Console application and see that the certificates have installed. You can also go to: <https://eca.orc.com/certificate-test/> to test your certificate. If for some reason you are getting an error message when installing or your certificate test is showing as "Certificate Not Presented" please email in to our helpdesk support team at ECAHelp@ORC.com for assistance and a representative will get back with you.

Note: Once the certificates have been fully installed they cannot be backed up. The Medium Token & Medium Hardware Certificates are non-exportable and live on the device itself due to the security of the certificate itself. If the smartcard/token has been lost/stolen or the certificates are no longer on the device unfortunately there is no way to retrieve them and will need to make new requests for new certificates.