FAQ`s:

Making an on-line request for a certificate

Why am I getting a Security Alert message that there is a problem with the ORC site's certificate?

You have not properly trusted the ORC ECA Certificate Authority.
Go to the https://eca.orc.com/instructions/ and find the instructions for your browser to Trust the ORC ECA Certificate Authority

I am being asked for a password but haven't created one yet.

This should only occur if you are Firefox which is NOT recommended. This browser uses something called a "Master Password" to protect the certificate store (also called the software security device and the internal cryptographic device). This Master Password also protects the "Password Manager" function in these browsers. So, if you are using the Password Manager feature, you may have set the Master Password at some previous time. If you cannot recall (or cannot discover) the correct Master Password, then you should 'reset' the Master Password BEFORE you make and submit certificate requests.

WARNING: If you reset the Master Password, all information protected by that Master Password (the Password Manager and the certificate store) will be deleted. So this will destroy any certificates currently protected by the Master Password that you are resetting.

IE users:

The private key password (aka CryptoAPI Private Key Password) was created by you when submitting your request for ORC WidePoint (ORC) ECA 7 identity certificate through Internet Explorer.

Please note that ORC cannot restore or reset your password.

Please test your WidePoint (ORC) ECA 7 identity certificate on the WidePoint (ORC) ECA website (http://eca.orc.com/), by clicking on Certificate Tools menu and then clicking on Certificate Test. You should be able to select your WidePoint (ORC) ECA 7 identity certificate. You will be prompted for your private key password.

Please note that you must try to figure out the private key password. Please note also that the private key password is case-sensitive. Please try any and all variations of any passwords that you would use.

If you encounter the Internet Explorer prompt "Request for Permission to use a Key", click "Grant Permission", and type the private key password.

If you receive the message "Your client certificate is valid", you have the correct private key password.

If you cannot figure out your private key password, you must submit requests for new WidePoint (ORC) ECA 7 identity and encryption certificates.

Can I get certificates on my Apple Macintosh computer?

We recommend that you download and install Windows Parallel software and run your MAC as a PC to complete your PKI tasking.

The following is an interim response to the issue of the Catalina OS for a Mac failing to work with ECA Medium Token Assurance or ECA Medium Hardware Assurance Certificates. Apple made a conscious decision to block ActivClient Software from working with a Mac for the Catalina OS. They did it because they want customers to use the card reader software that is part of the Catalina OS. The issue with this is that they designed that card reader software to work for CACs and PIV Cards.

The ECA Medium Token Assurance or ECA Medium Hardware Assurance Certificates that you have on your smartcard/cryptotoken are not designed to work without interaction with the ActivClient Software on the Mac. Because the Catalina OS blocks that interaction, your smartcard/cryptotoken will not work with the keychain access. Therefore, the Chrome, Safari, and other browsers that use the keychain will not work. Also, Outlook for a Mac and Adobe (along with other PDF-Reading Software) will not work with your smartcard/cryptotoken for digitally signing emails, exchanging encrypted emails, and digitally signing PDF Documents with your certificates because the certificates must be seen via the keychain access.

The lowest level of ECA Certificate is the ECA Medium Assurance Certificate, which is a browser-based or software certificate. Those certificates can be imported into the organic keychain of the Catalina OS and should still work with emails and PDF-Reading Software as well as the Chrome and Safari Browser; however, they cannot access the higher level ECA Sites, such as JPAS, SWFT, NGA, FVS, FEDMall, Navy Data Environment, etc.

We have been successful in getting Mozilla Firefox on a Catalina OS to work with the current version of ActivClient Software for a Mac installed on the Mac to access the web sites via Firefox as you may have done all along. The reason Firefox works is that it is a self-contained app/browser that does not require interaction with the Mac keychain. Let us know if you want us to configure Firefox to access the web sites.

Furthermore, because Mozilla Firefox can still work for getting access to web sites with the ActivClient Smartcards/Cryptotokens, Mozilla Thunderbird should be successful in digitally signing emails and exchanging encrypted emails with your certificates on a Mac with the Catalina OS. It is a free download just like Firefox. However, you must get your IT Department to set up Thunderbird on your Mac with the correct settings so that it goes through your mail server; you need to test it to make sure that you can send emails out and receive emails. After that, we can connect via a gotomeeting to configure Thunderbird to digitally sign emails and exchange encrypted emails.

Please note that we are continuing to experiment with the Catalina OS and our NFI PIV-I Cards and our ECA PIV-I Cards (ECA PIV-I is a PIV-I version of the ECA Medium Hardware Assurance Certificate and is issued out of a card managed system) because these certificates are supposed to work with that card reader software for the Catalina OS. We currently are experimenting with these PIV-I Cards because they do NOT require ActivClient Software to work.

HOWEVER, HID/ActivClient has NO plans to develop any further hotfixes (patches of code) to overcome the current issue with their smartcards working other than through Firefox on a Mac Catalina OS BECAUSE the Catalina OS would block it from working.

Accepting a Certificate

I am copying the URL from the email message, but I keep getting an error message.

The URL should look like:

https://ecarm.orc.com/viewcert.xuda?md5=98d4aef0004901169d38c50a8e6884c2&domainID=

or

https://ecarm.orc.com/viewcert.xuda?md5=98d4aef0004901169d38c50a8e6884c2&domainID=

Generally, the problem is that the end of this URL is chopped off. Have the subscriber key the end of the URL into their browser.

When I try to download my issued certificate, I get an "Accept in PKCS7" error message.

If you are still getting the "Error in accept PKCS7" message that means that the Microsoft OS/Internet Explorer can not find the private key(s) for those certificates. *(Please note that this does not necessarily mean that the private key(s) are not there, just that the MS system can not find them.)*
This happens because:

- the request was done under a different log-in profile (you are logged on under a different username/password) than when the request was made
- or the request was made with a different browser (for example, Firefox)
- or the request was made on a different computer than the one you are trying to import it on
- or something was done to the machine (like an update to the operating system - a Windows update, profile change, computer re-imaged, etc.)

You will only be able to import the issued certificate onto the same computer, same log-in profile, and using the same web browser as when you made the on-line request. (i.e. as when you got the "Print this form" web page).

I get the error message that there is no matching private key.

This is the Mozilla Firefox error equivalent to the Microsoft "Accept in PKCS7" error message discussed above.

This happens because:

- the request was done under a different log-in profile (you are logged on under a different username/password) than when the request was made
- or the request was made with a different browser (for example, Internet Explorer)
- or the request was made on a different computer than the one you are trying to import it on

- or something was done to the machine (like an update to the operating system - a Windows update, profile change, computer re-imaged, etc.)

You will only be able to import the issued certificate onto the same computer, same log-in profile, and using the same web browser as when you made the on-line request. (i.e. as when you got the “Print this form” web page).

I am using a different workstation.

If you have switched workstations, or are trying to accept the certificate from home, you will be unable to retrieve the certificate. Go back to the original workstation that was used to request the certificate. Once the certificate has been accepted, it can be exported and imported into other workstations.

If you have proper back-up copies of your enrollment key pairs contact our help desk at ecahelp@orc.com

My workstation has been upgraded since the request was made.

If your workstation has been upgraded ie new operating system the private key that goes with the certificate may have been inadvertently deleted. If so, it cannot be recovered. You will have to delete the certificate database file, request a new certificate, and request that the current certificate be revoked.

If you have proper back-up copies of your enrollment key pairs contact our help desk at ecahelp@orc.com

My password is not working.

Passwords are case sensitive.

The private key password (aka CryptoAPI Private Key Password) was created by you when submitting your request for ORC WidePoint (ORC) ECA 7 identity certificate through Internet Explorer.

Please note that ORC cannot restore or reset your password.

Please test your WidePoint (ORC) ECA 7 identity certificate on the WidePoint (ORC) ECA website (http://eca.orc.com/), by clicking on Certificate Tools menu and then clicking on Certificate Test. You should be able to select your WidePoint (ORC) ECA 7 identity certificate. You will be prompted for your private key password.

Please note that you must try to figure out the private key password. Please note also that the private key password is case-sensitive. Please try any and all variations of any passwords that you would use.

If you encounter the Internet Explorer prompt "Request for Permission to use a Key", click "Grant Permission", and type the private key password.

If you receive the message "Your client certificate is valid", you have the correct private key password.

If you cannot figure out your private key password, you must submit requests for new WidePoint (ORC) ECA 7 identity and encryption certificates.

If the subscriber cannot remember his or her password, it cannot be recovered. He or she will have to request a new certificate, and request that the current certificate be revoked. (See https://eca.orc.com/wp-content/uploads/ECA_Docs/IE_Instructions/Password_Tips.pdf.)

How do I take my certificate to a new workstation?

See the subscriber instructions for your browser type at *https://eca.orc.com/instructions/*.

I have a certificate, but I cannot access the application.

If a certificate is rejected from the application, either the application requires additional access approval beyond holding an ECA PKI certificate, or the certificate is not properly loaded into the directory that the application is using.

Run a test at our website and you receive a valid test response please contact the system directly as they run/maintain themselves therefore they will need to offer further trouble shooting assistance.

If the test fails please contact our help desk at ecahelp@orc.com.