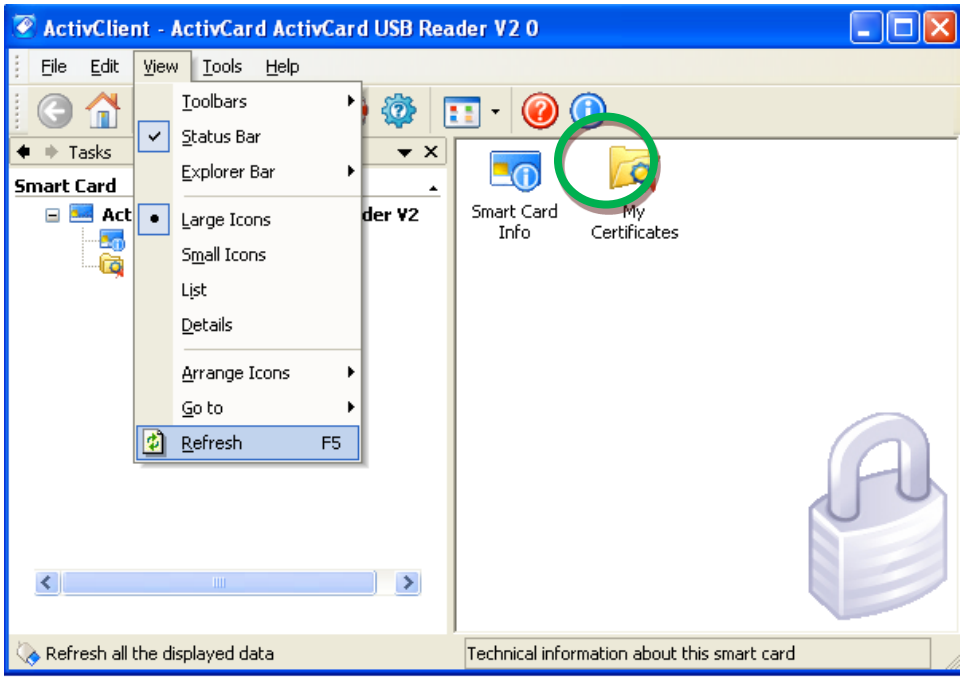
The RSA Key Pair is written to your cryptographic token when you have successfully made an on-line request for certificates. There will be an RSA key for each certificate request that you have made. Your computer will look for this RSA Key Pair on your cryptographic token when you attempt to import the 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. Verification of the RSA Key Pair will confirm that the RSA Key for your future certificate is fully functional.

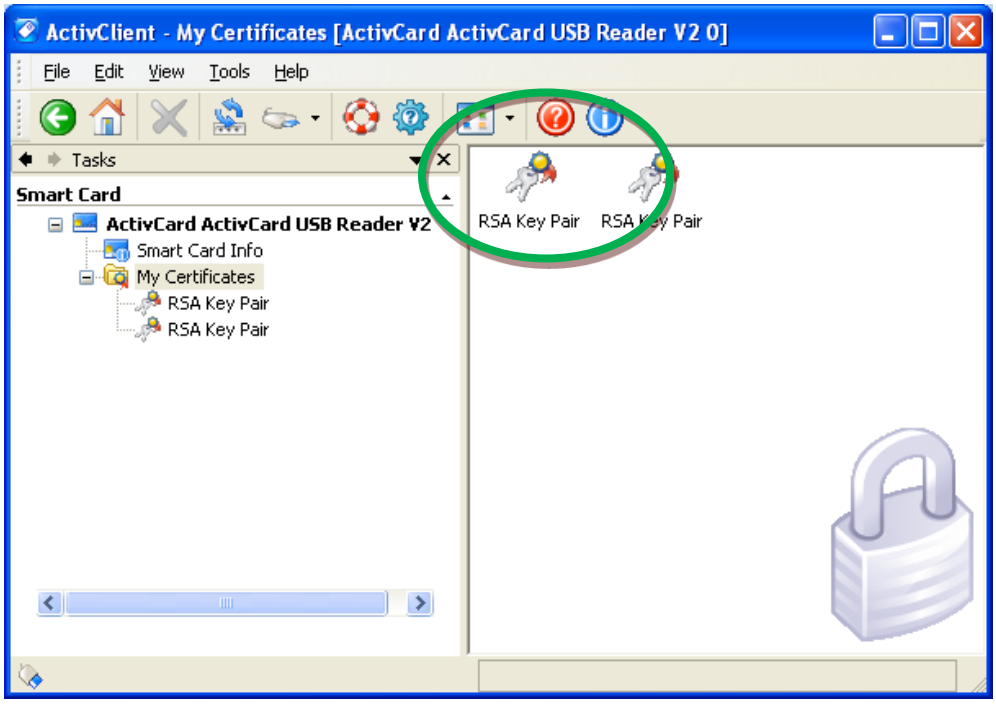
To ensure that the RSA Key Pair has successfully written to your cryptographic token, please follow the steps below.

CRITICAL: DO NOT at any time delete an RSA key from your cryptographic token.

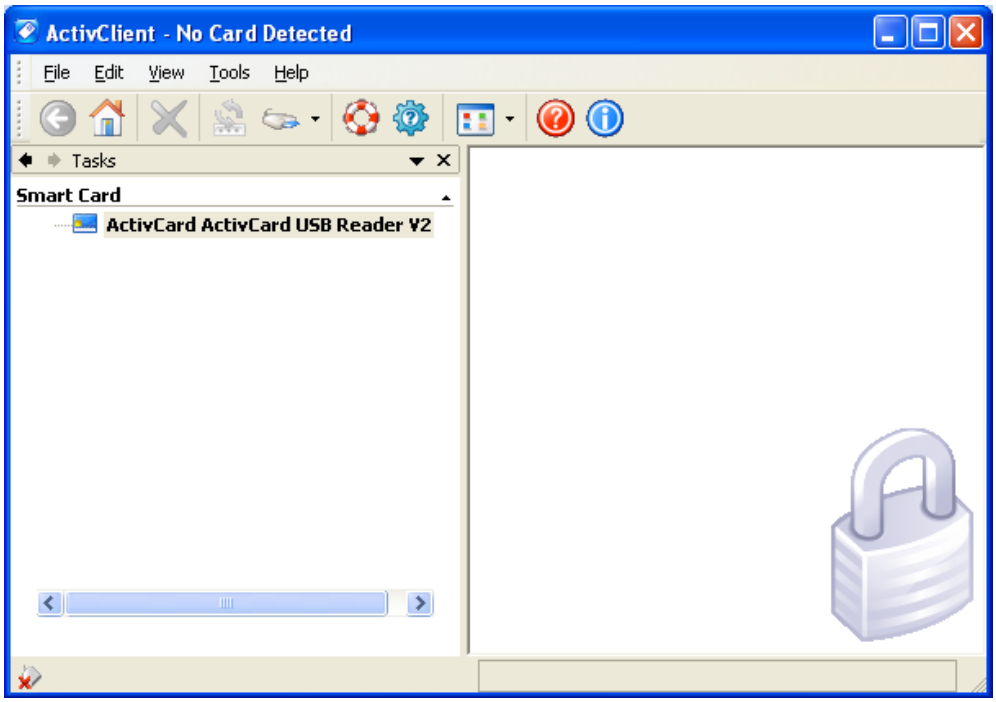
1. Open the ActivClient User Console and then click **View** then **Refresh**, then double-click on the My Certificates folder.



   a. You should see one (1) RSA Key Pair for each certificate that you are requesting. [Please note that the RSA Key Pairs are not yet certificates. They are the core of a certificate, but will not be finished until you receive a Certificate Issuance Notification email from ORC and you execute the instructions contained in that email.]



b. Pull your card out of the reader. If you have a USB token, follow the process to “Safely Remove Hardware”. [Notice how the display goes blank.]



CRITICAL: If you do NOT see an RSA Key Pair on your cryptographic token, you have not made a successful request. Also, if you see more than two (2) RSA keys on your cryptographic token, this means that you have generated more than two on-line requests. These are problems for the following reasons:

1. If you do not see your RSA Key Pair on the cryptographic token, then you will not be able to successfully complete the import process when you receive the certificate issuance notification email.
2. If you see more than two (2) RSA Keys on your cryptographic token, then you have generated more than two on-line requests. It is impossible to tell which RSA Key is associated with a particular request number that you generated during the on-line request process. If you were to send in paperwork for the wrong RSA Key Pair, then you would not be able to complete the import process when you receive the certificate issuance notification email.

If you find that you fall into either one of these categories, and were to send us the request forms anyway, then your certificate will NOT work when issued, and you will be solely responsible for the cost of purchasing a new certificate.

To fix the problem:

1. DO NOT at any time delete an RSA Key from your cryptographic token.
2. If your RSA Key Pair is not on your cryptographic token and you are using Mozilla Firefox, please follow the instructions for ensuring that Firefox is talking to the smartcard/token (http://eca.orc.com/wp-content/uploads/ECA_Docs/Adding_ActivClient_to_Firefox.pdf). Restart your computer and make a new set of requests. If you still get this result, contact ecahelp@orc.com.
3. If your RSA Key Pair is not on your cryptographic token and you are using Internet Explorer, the above fix for Firefox does not apply. Please contact ecahelp@orc.com for assistance.
4. If you have generated multiple requests and have more than two (2) RSA Keys on your cryptographic token, DO NOT delete any of the RSA Keys, and please contact ecahelp@orc.com for assistance.