Setup Guide

GLP Server and Client Certificates

17th January 2022

Overview

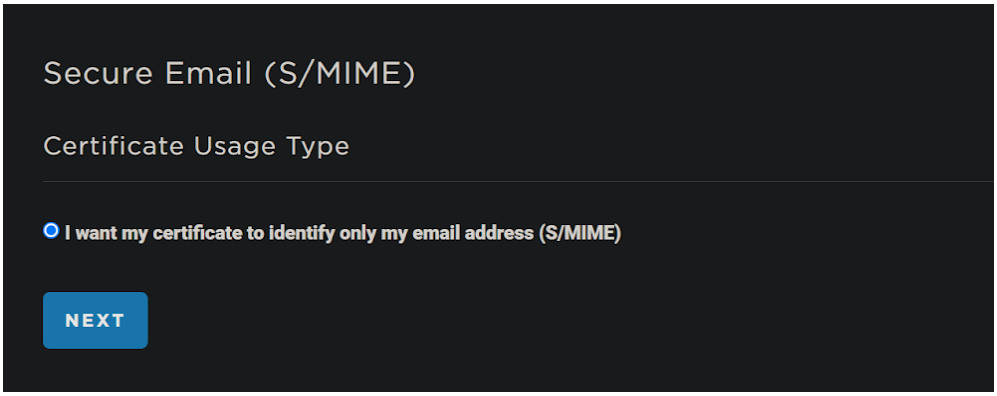
GLP uses certificates for signing and authoring GLP documents in LabChart. To increase the security of GLP systems and infrastructure for both ADInstruments and customers, we changed how certificates were issued in 2018. Instead of using ADInstruments issued certificates, customers now need to obtain a Client Authentication Certificate from a trusted certification authority. We recommend that ADInstruments customers purchase certificates from IdenTrust. This guide will outline the steps necessary to obtain a certificate from IdenTrust and configure it with GLP Client. The steps taken by the Lab Administrators when installing the client's public certificate remain unchanged.

Guide

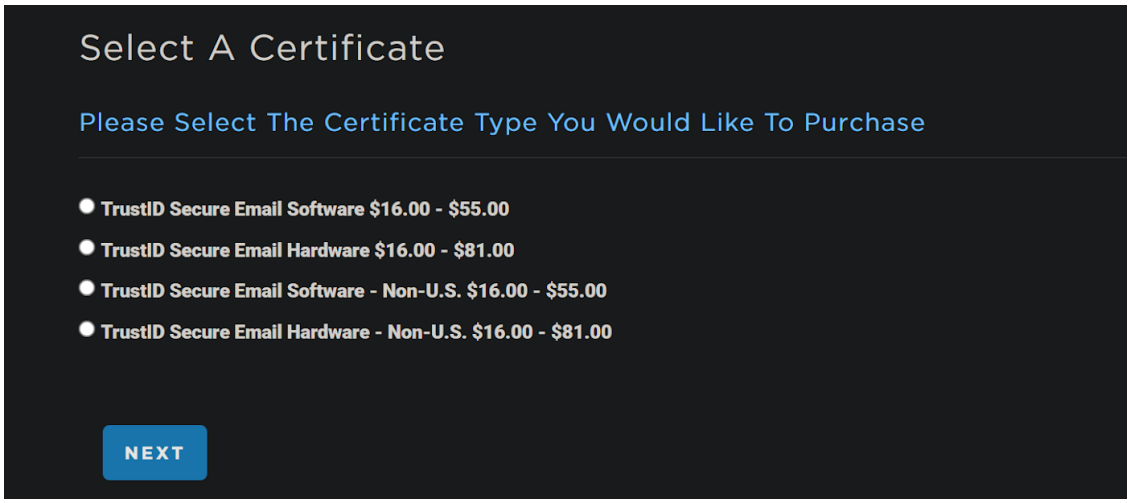
The steps below are to be performed by each 'Client' that wishes to be able to save GLP documents and communicate with the laboratory's GLP server. You cannot issue multiple client certificates under one email address with IdenTrust. The email is used to identify the person's certificate, and the certificate is issued to that email address.

Part 1 – Obtain Client Authentication Certificate

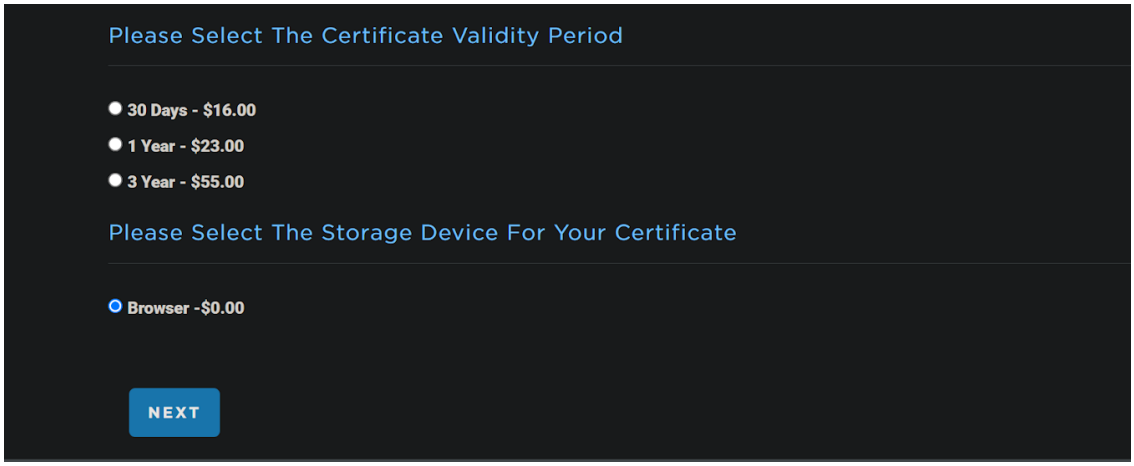
1) Navigate to https://www.identrust.com/wizard?nid=180 to purchase an S/MIME certificate from IdenTrust. Select the option, **'I want my certificate to identify only my email address (S/MIME)'** and click **'NEXT'**.



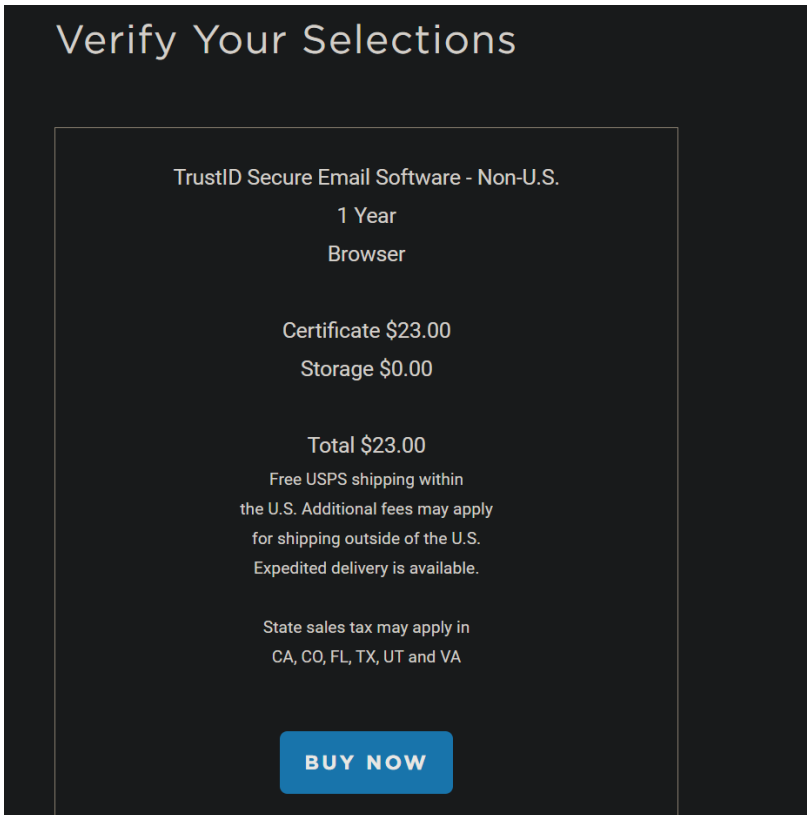
2) Now select your certificate type. If you are in the U.S., select **‘TrustID Secure Email Software’**. If you are outside the U.S., select **‘TrustID Secure Email Software - Non-U.S’**. Then click **‘NEXT’**.



3) Now you can select the validity period of your certificate. We recommend selecting a validity period of at least one year, and we used the **‘1 Year’** certificate for our testing. After selecting your validity period, click **‘NEXT’**.

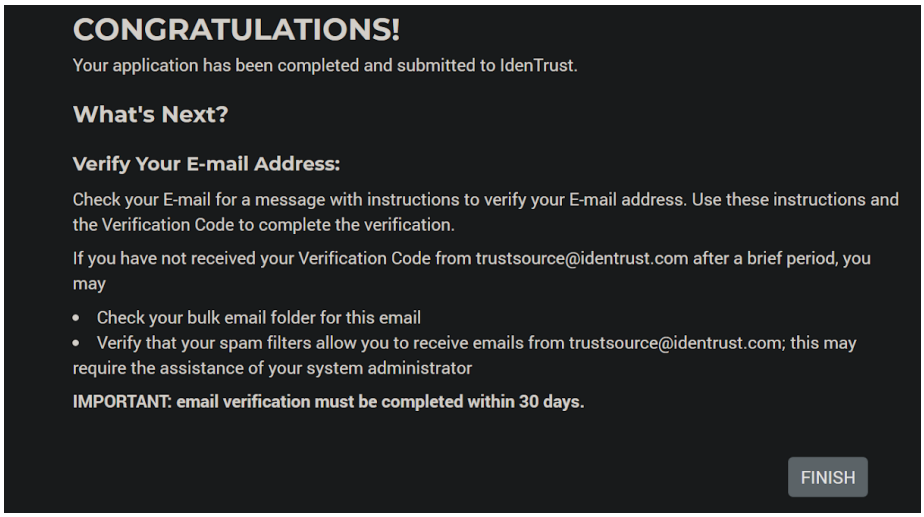


4) Now you will confirm the details of your certificate. If the details are correct, click **'BUY NOW**'. Then on the next page, click **'NEXT'**.



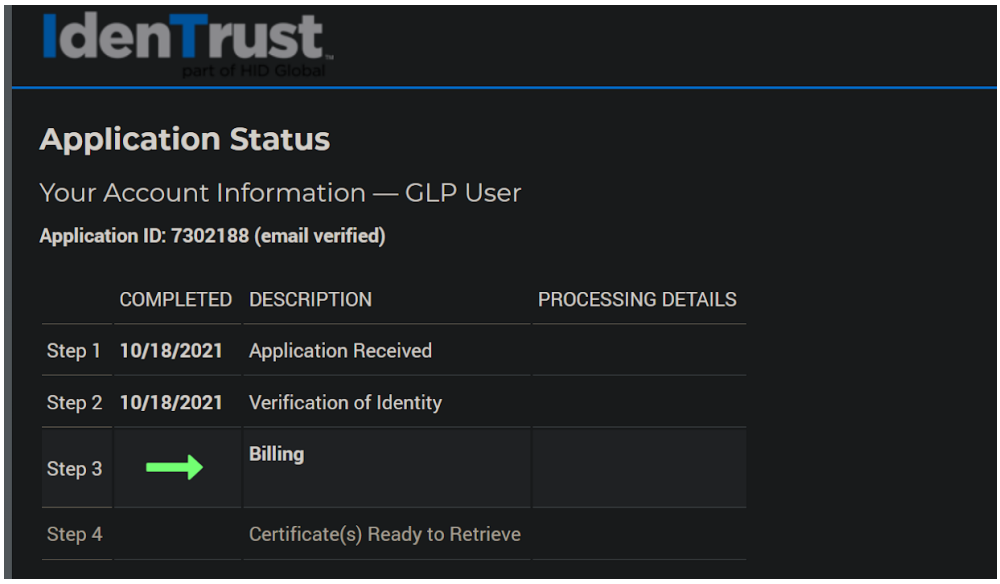
5) Enter your account set up details, including the name and email address for the person the certificate will be issued to, and set up the account password. **Ensure that the email address you enter is the email address you will use for your GLP work.**
Once you have finished entering your details, click **'NEXT'**.

6) Read the instructions and click '**FINISH**'.

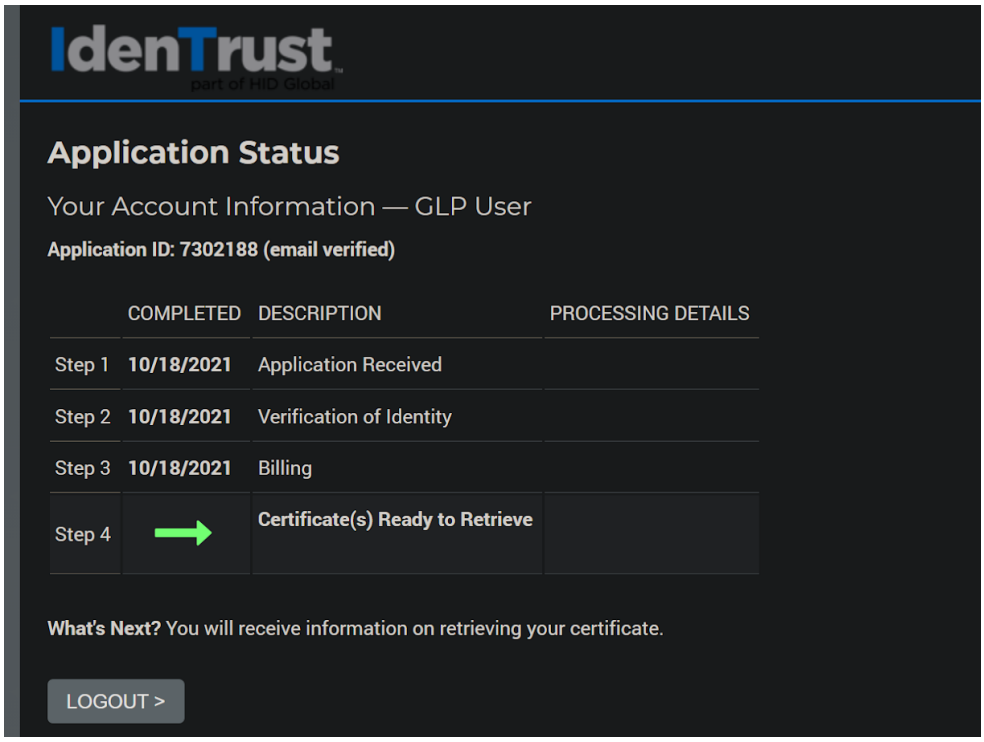


7) Check your inbox for an email from IdenTrust. If you can't find this email, check your spam folder. Click the verification link in the email and follow the instructions to verify your email address.

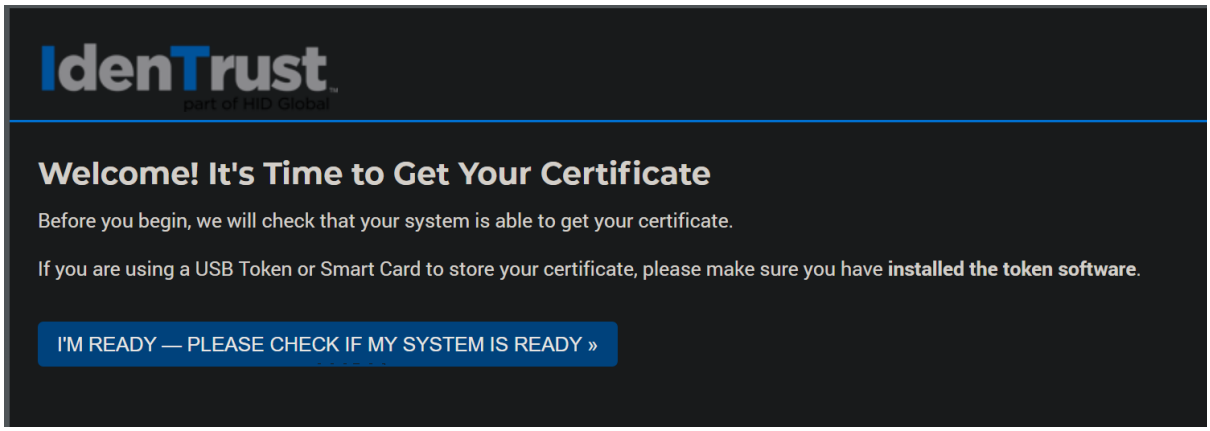
8) Once you have verified your email address, some users might see that their request is still being processed. If you see this, please wait a short time for your certificate to be ready (when we tested this, we waited less than 10 minutes).



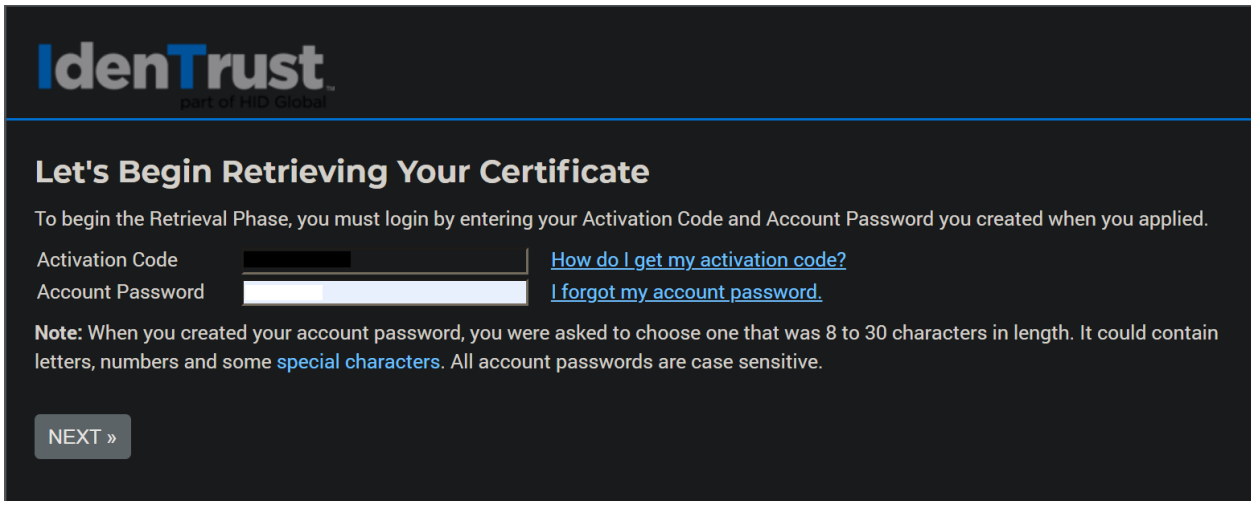
Once your certificate is ready, you will see this:



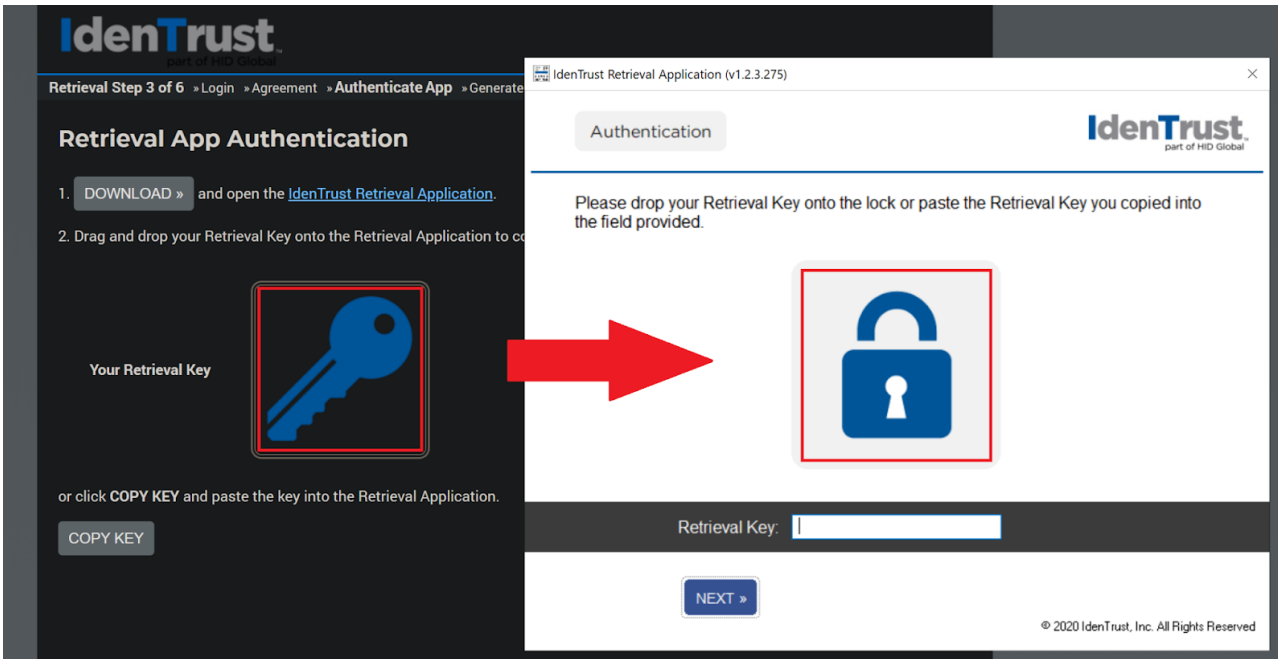
9) Once your certificate is ready you will receive a confirmation email. If you can't find this email, check your spam folder. This email includes your activation code. **You will use this activation code in the next step to install the certificate.**
In the email, click on *www.identrust.com/install* to install your certificate on your computer. Then click the **'I'M READY'** button:



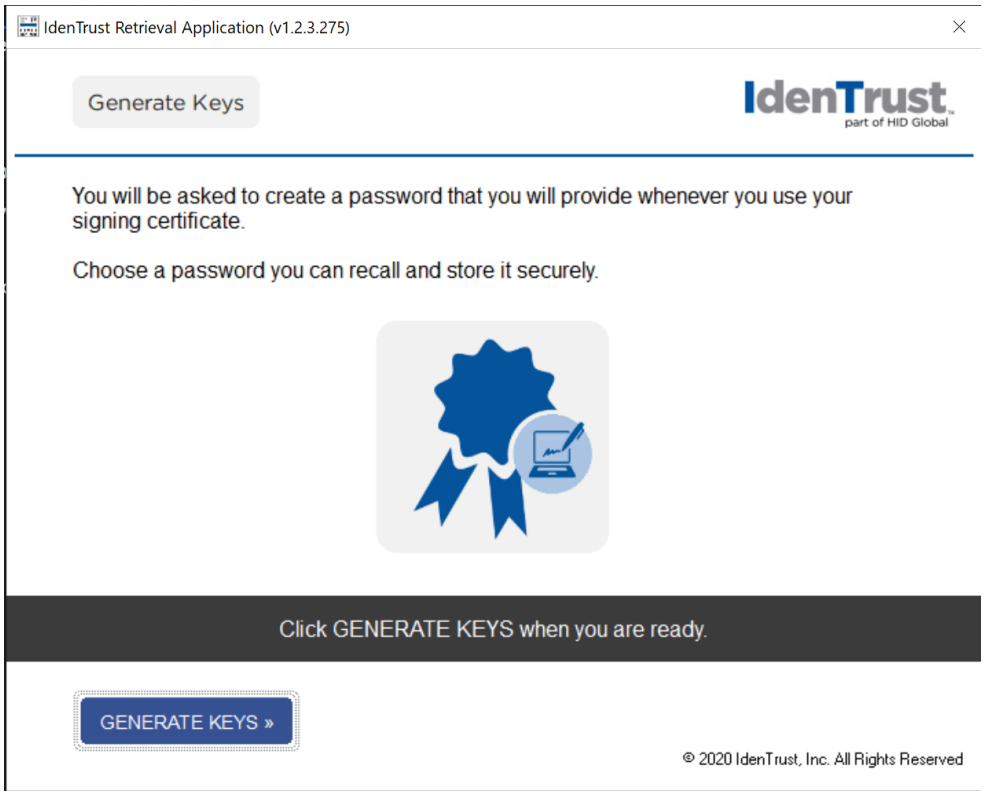
10) Enter the activation code from your confirmation email, and the account password you set up earlier, then click '**NEXT**'.



11) The certificate is installed to your computer using the IdenTrust Retrieval Application. Save the Retrieval Application to your computer.
Once the Retrieval Application has opened, click and drag the the large key icon onto the large padlock icon in the Retrieval Application:



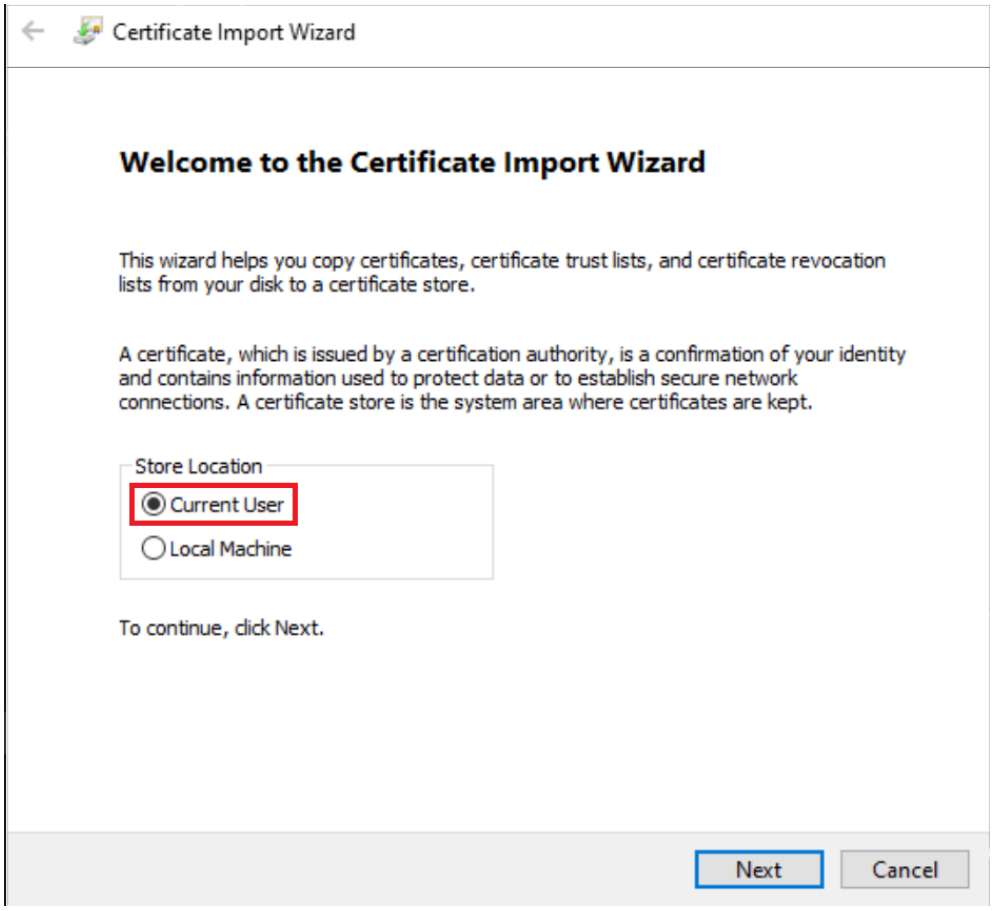
12) In the Retrieval Application, click on '**GENERATE KEYS**'.



13) Your certificate purchase and download are now complete. At this point you can make a back-up if you wish.

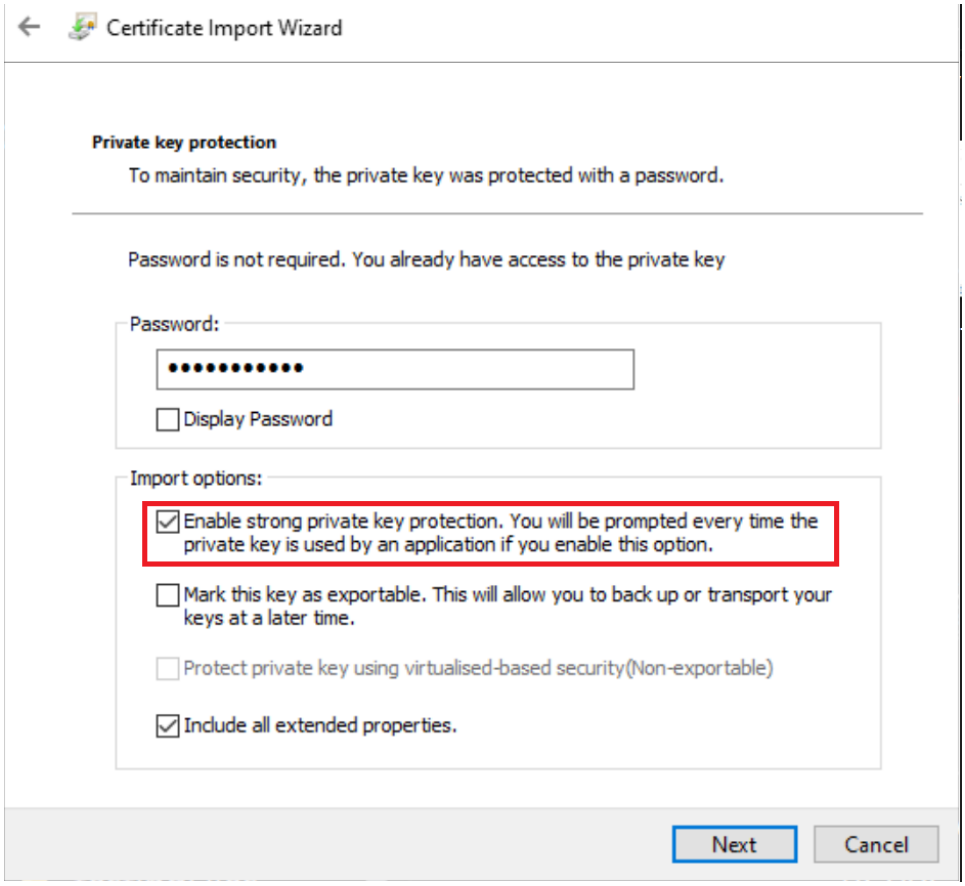
Part 2 - Import Client Authentication Certificate

1) Right click on the certificate you have downloaded to open the Certificate Import Wizard. Select **'Current User'** and click **'Next'**.

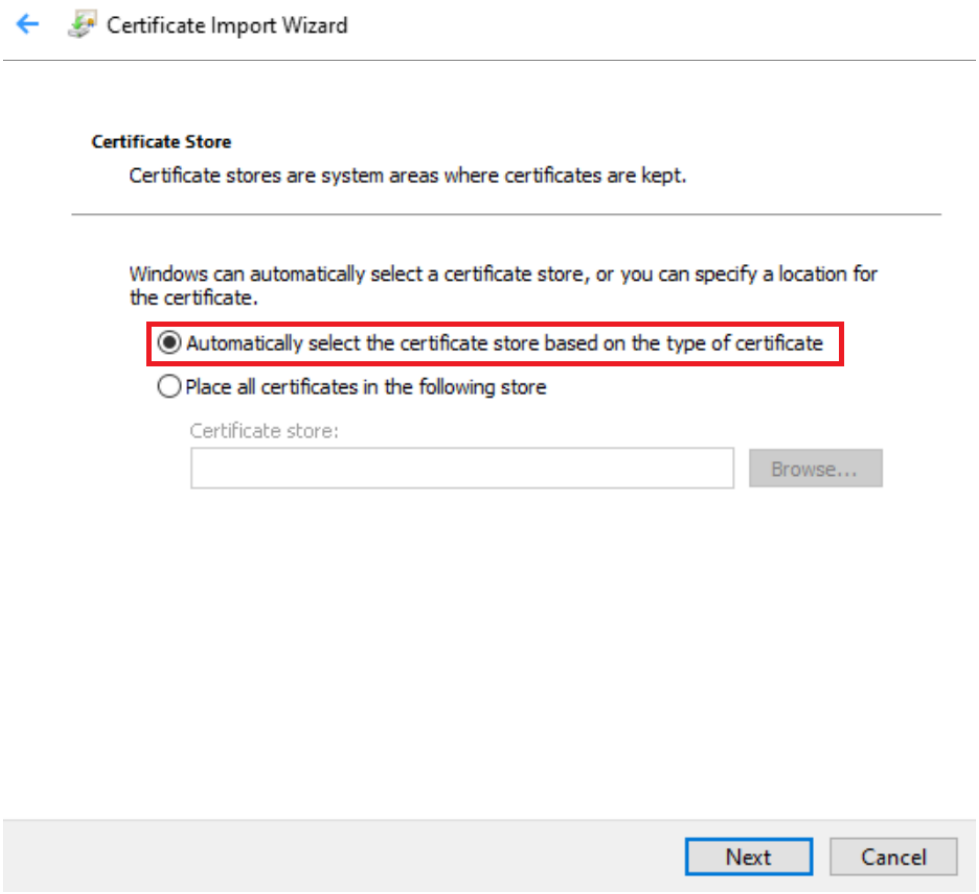


2) Select your certificate file, and click **'Next'**.

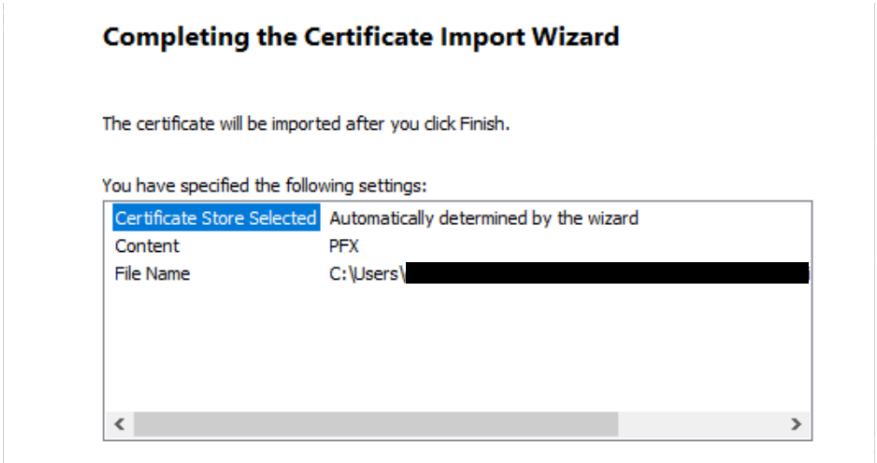
3) Now you can set your import options for the certificate. It is important that you select **'Enable strong private key protection'**. Strong protection is required to be able to save GLP documents in LabChart. Once you have selected this option, click **'Next'**.



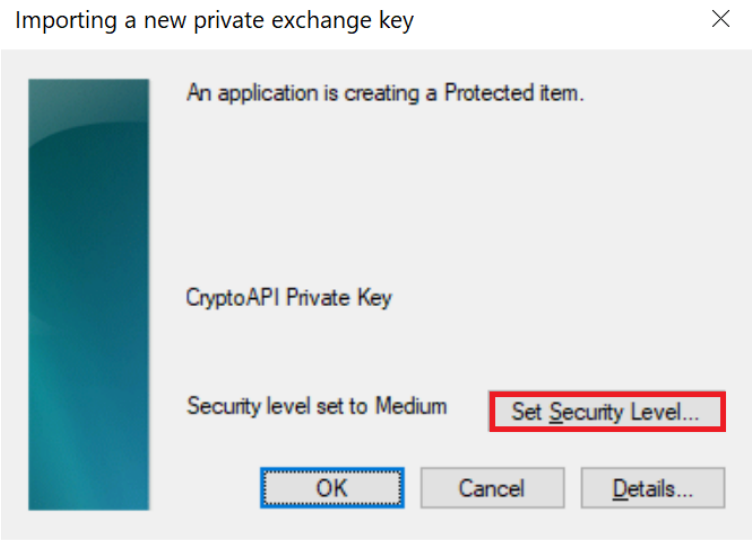
4) Now you have the option to select your certificate store. We want Windows to automatically do this for us, so click **'Automatically select the certificate store based on the type of certificate'** then click **'Next'**.



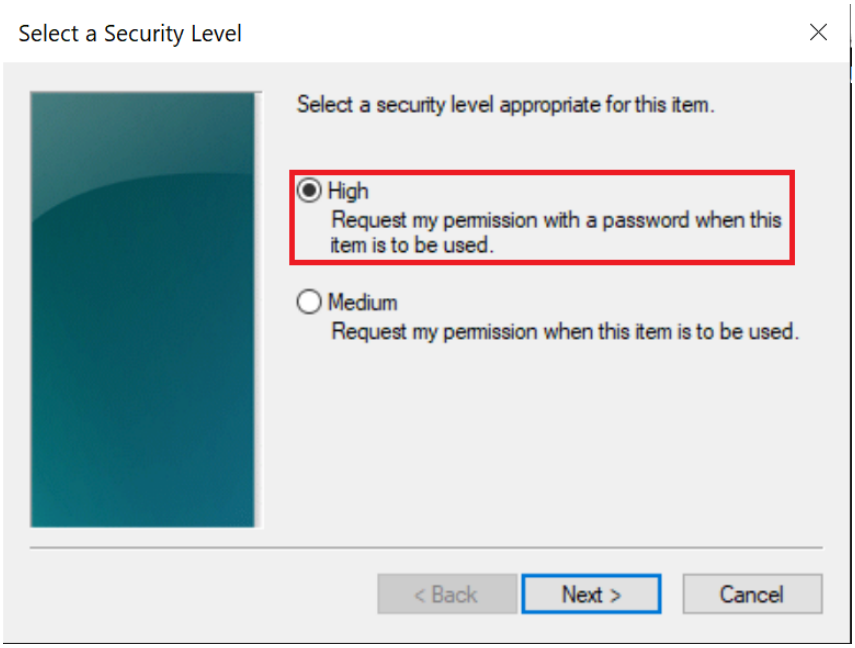
5) Review your settings and click **'Finish'**.



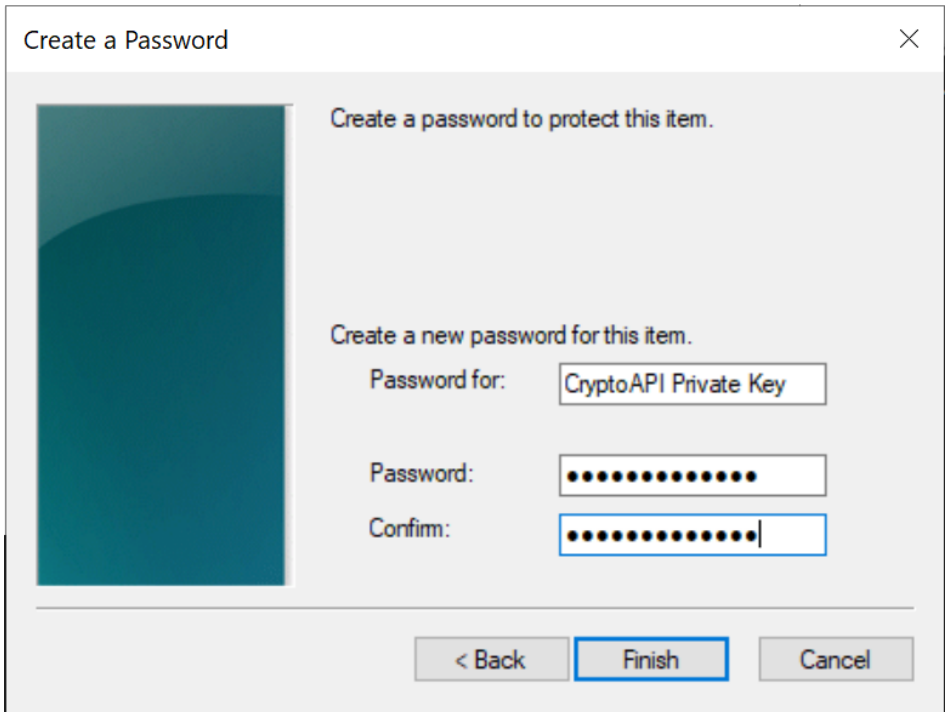
6) The Certificate Import Wizard will now start importing your certificate. You will be asked to set your security level. High security is required to be able to save GLP documents in LabChart, so click **'Set Security Level…'**.



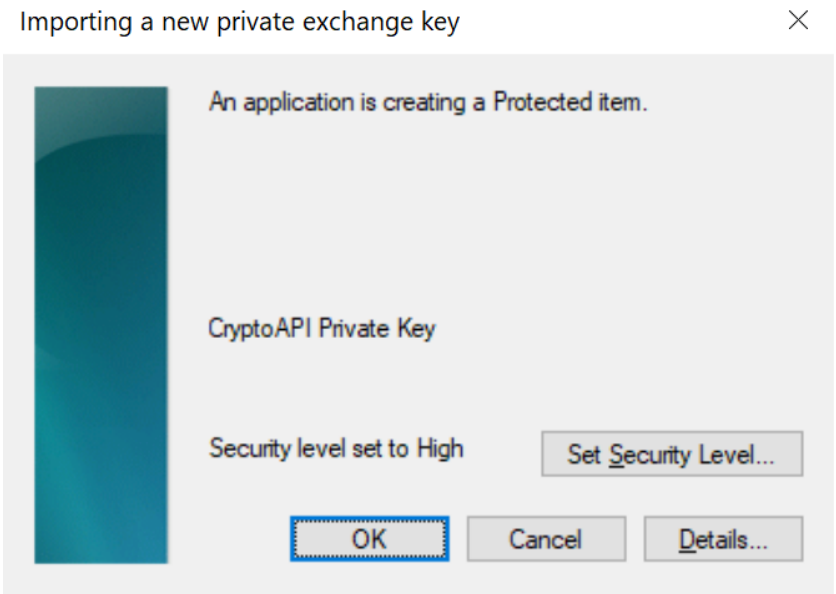
Select the **'High'** security level and click **'Next'**.



7) Now you need to add a password for your certificate. Ensure you remember your password, because **you will be required to enter this password in LabChart when saving a GLP file**. Click **'Finish'**.



8) Now click **'OK'**. Your private authentication certificate has now been successfully installed.

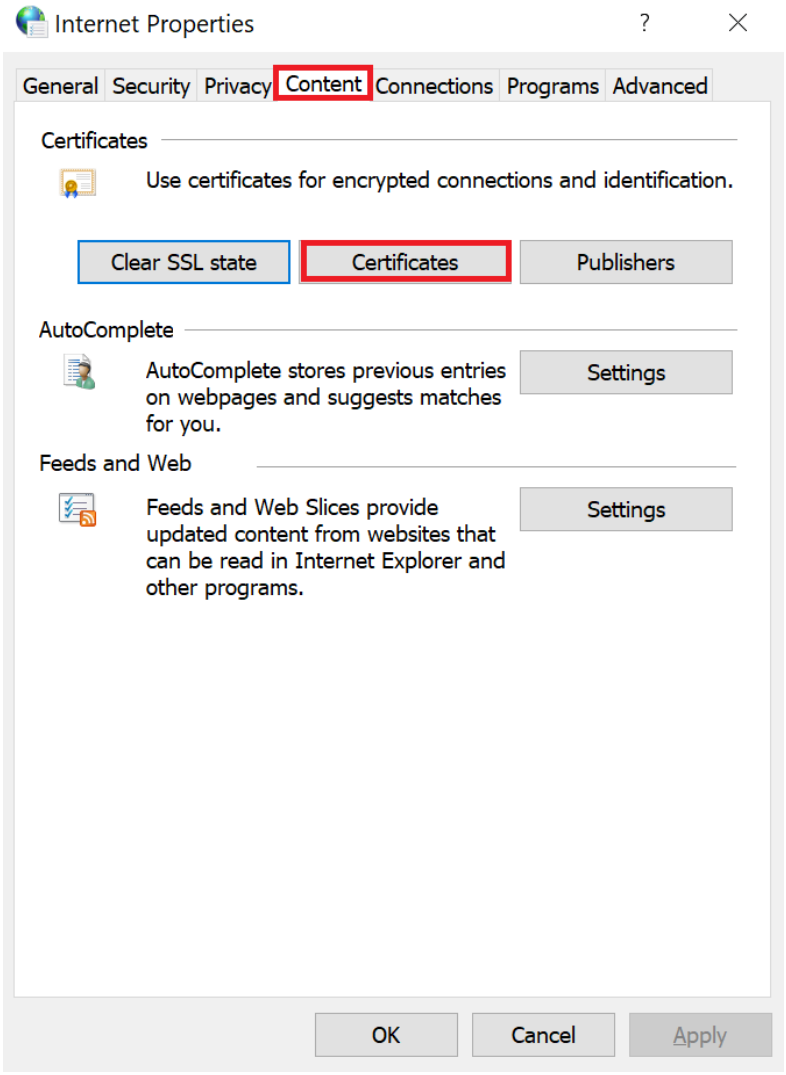


Part 3 - Export Client Public Certificate

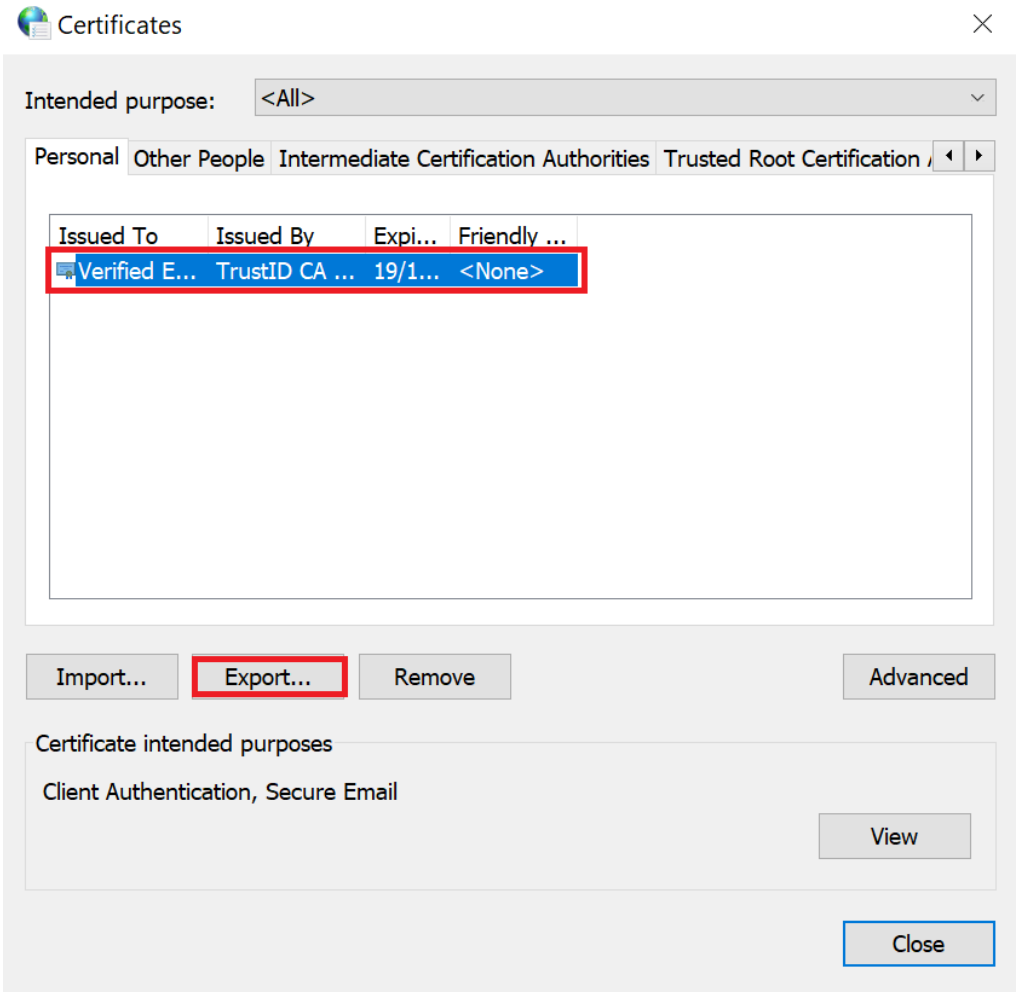
We will now run through the steps required to export the client's ***public certificate***, which will be given to a Lab Administrator to install on their GLP server. Without this public certificate installed on the GLP server, the Client will not be able to save GLP documents.

1) Click on the windows key and search for 'Internet options'. Choose the 'Internet Options' option that should appear at the top of your search results.

   Click the content tab, and then click the 'Certificates' button.

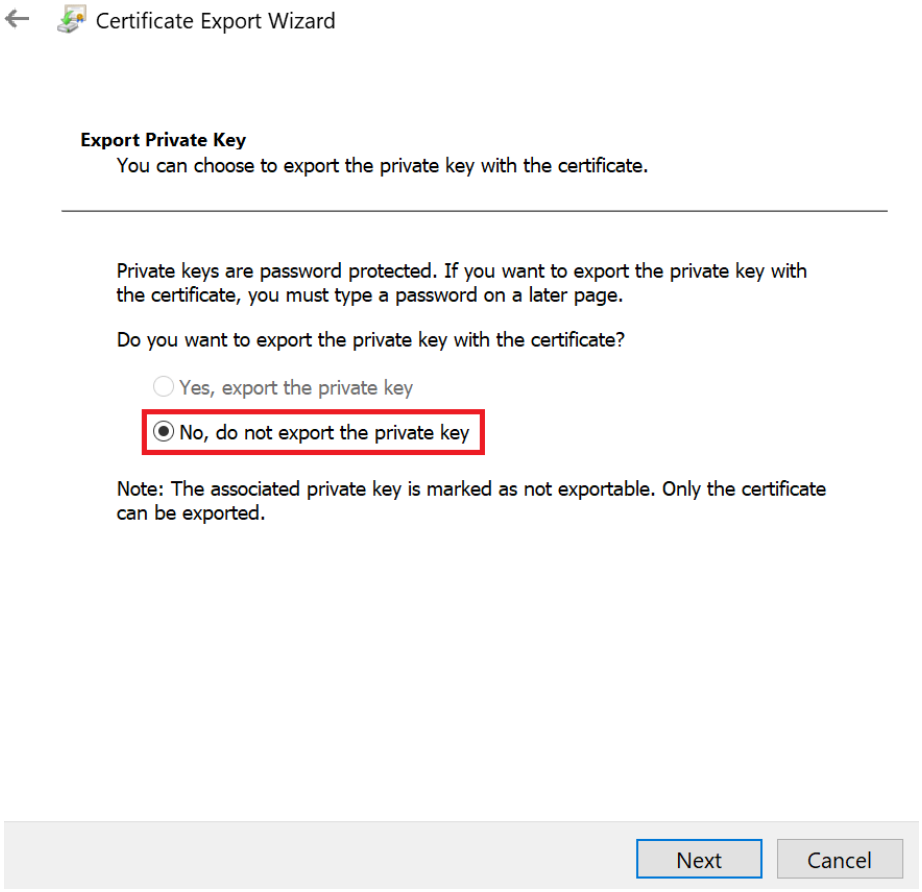


2) Click on your certificate to highlight it and click '***Export…***'.

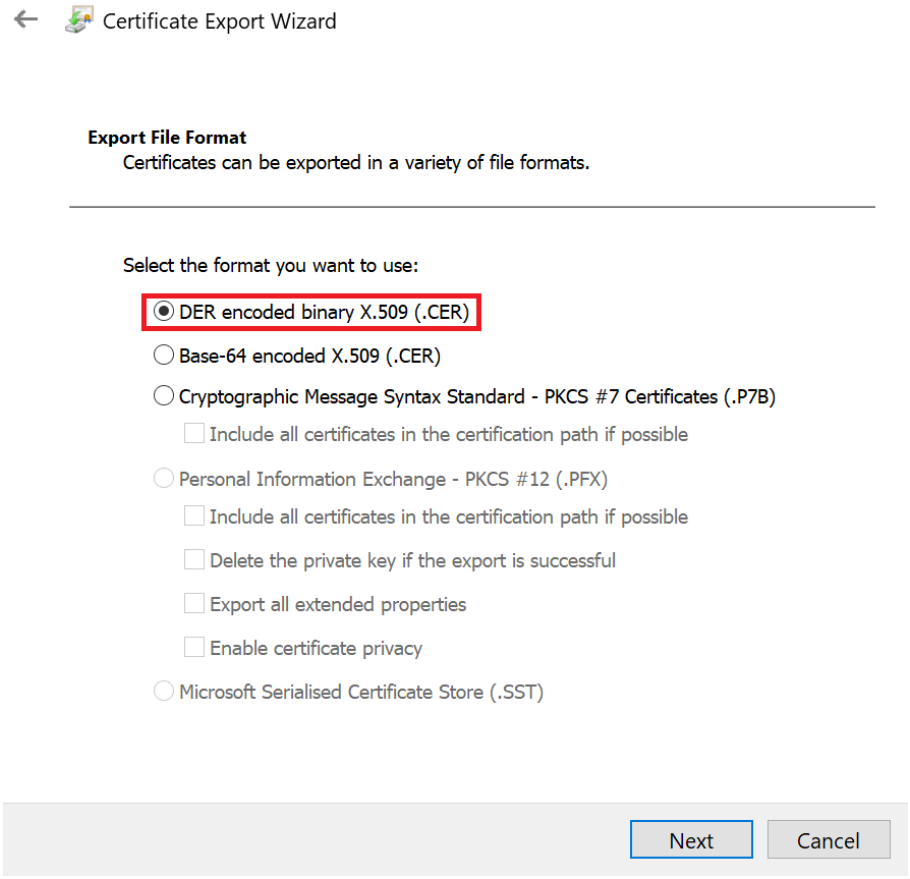


3) This will open the Certificate Export Wizard. Click **'Next'** to begin.

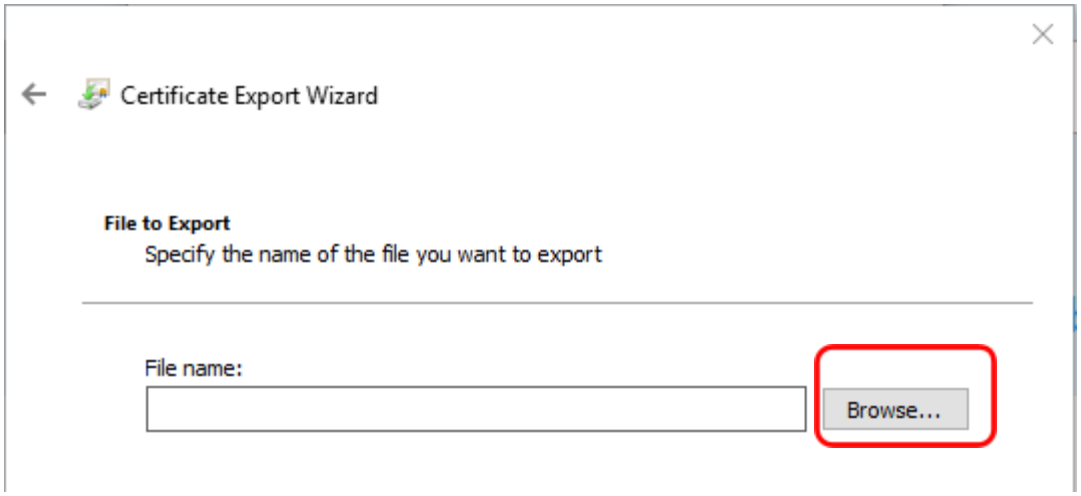
4) On the next screen you will be asked if you would like to export the private key. We do not want to do this so ensure the checkbox is selected with the option '**No, do not export the private key**' and click **'Next'**.



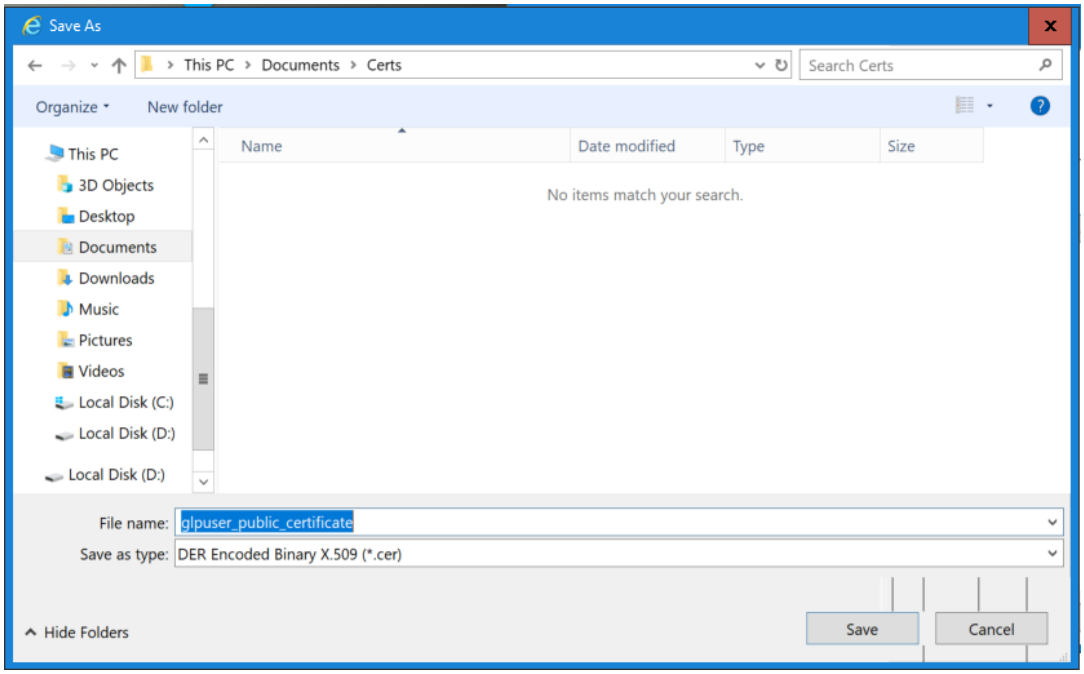
5) The next section lets us select a file format. Select '**DER encoded binary X.509 (CER)**' and click **'Next'** to continue.



6) Now we will specify the folder location and filename that we want to save our certificate to. First click the browse button to open the save file dialog.

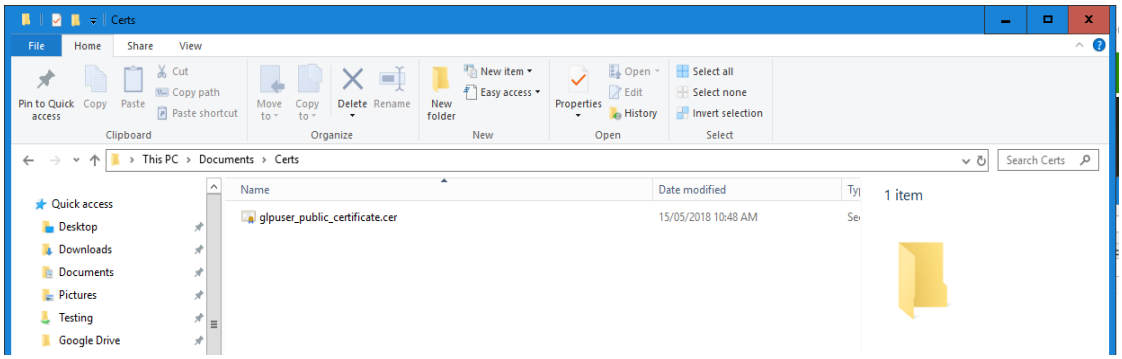


7) Using the file browser that opens, navigate to the folder where you want the certificate to be saved. In the '***File name***' text box enter the name you want the public certificate file to have. I've named mine '*glpuser_public_certificate*' as you can see below.



8) Click 'Save'. This will return you to the previous dialog seen in step 6, but with the file path in the text box to the left of the Browse button. You may now click Next.

9) The certificate export wizard review screen will now show. When ready click Finish to complete the wizard. If successful, a dialog box will display notifying you. The public certificate will now be in the folder you specified in step 7.



10) To be able to save GLP files in LabChart, you must send this public certificate to your Lab Administrator. They can then add your certificate to the GLP Server, allowing you to save GLP files in LabChart.

FAQ

Q) What password do I enter when saving the GLP document in LabChart?

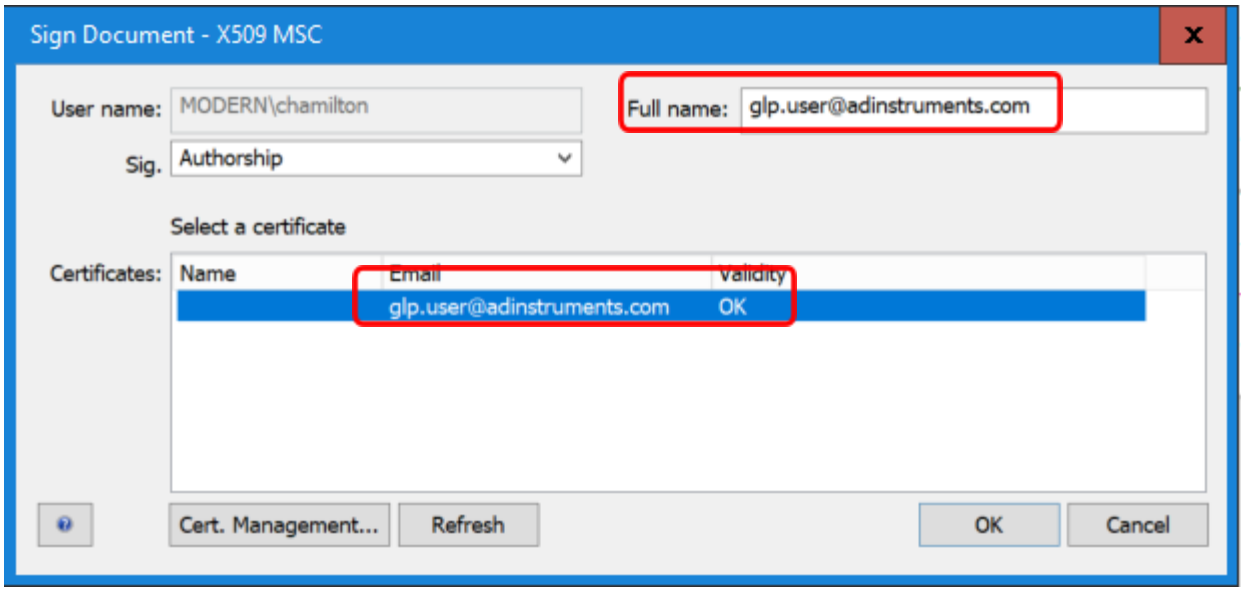
A) In Part 2 – Step 7 when the client private certificate was imported, you were prompted to enter a password to protect the private certificate. You must use this password when saving GLP documents in LabChart, so LabChart can access the client certificate and sign the GLP document.

Q) Can a Lab Administrator create client certificates on behalf of clients for them to use?

A) No they cannot. While this is technically possible, they need to perform the generation process on the machine they will be using and in doing so they are required to enter a private password to protect the certificate. No one else but the client is allowed to know this password.

Q) Entering my real Full Name when signing (saving) the GLP document in LabChart isn't working.

A) You may recall that when signing up for the client certificate we had to enter an email address. You must enter this email address in the Full name field, as that is who the certificate is issued to. Failure to do so will result in the certificate being marked as Invalid in the dialog.



Q) Do I have to install a root certificate on the GLP Server PC and the GLP Client PC?

A) If the customer is using IdenTrust certificates to sign their files, a root certificate is not needed. This is because IdenTrust is already trusted by the Windows operating system.

Q) Do users need their administrator's permission to apply for and create a certificate with IdenTrust?

A) No, they do not. Users can create a certificate without the administrator's permission. The administrator will still need to install the certificate on the GLP server.

Q) How do existing GLP customers switch to IdenTrust certificates?

A) Existing customers do not need to switch certificates. Their existing certificate will continue to work until it expires. Existing documents that were signed using ADInstruments certificates will continue to be valid, provided the customer has the appropriate public keys installed on their GLP server. They will need to retain all public keys that correspond to private keys that were used to sign files. Once the customer's ADInstruments certificate expires, they will have to follow the workflow described in the Setup Guide to use a certificate from a trusted third party supplier such as Sectigo.