

Setup Guide

GLP Server and Client Certificates

17th January 2022

Overview

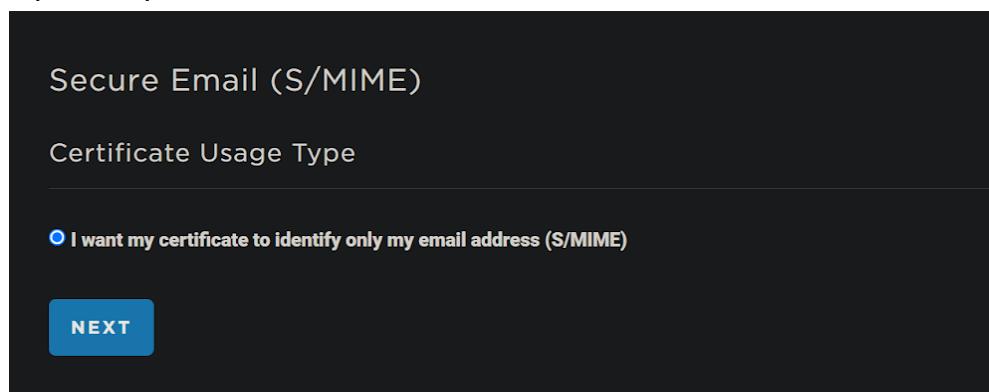
GLP uses certificates for signing and authoring GLP documents in LabChart. To increase the security of GLP systems and infrastructure for both ADInstruments and customers, we changed how certificates were issued in 2018. Instead of using ADInstruments issued certificates, customers now need to obtain 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**'.



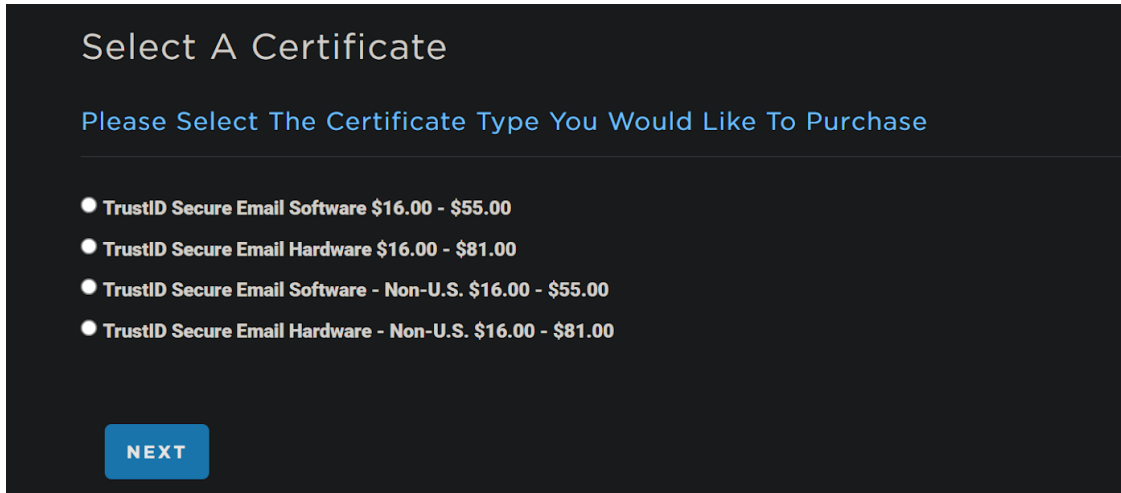
Secure Email (S/MIME)

Certificate Usage Type

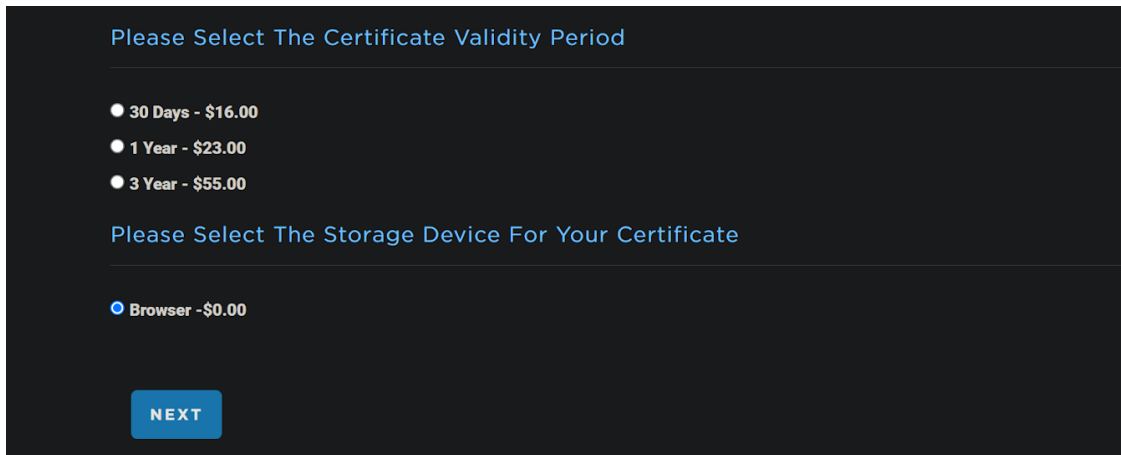
☒ I want my certificate to identify only my email address (S/MIME)

NEXT

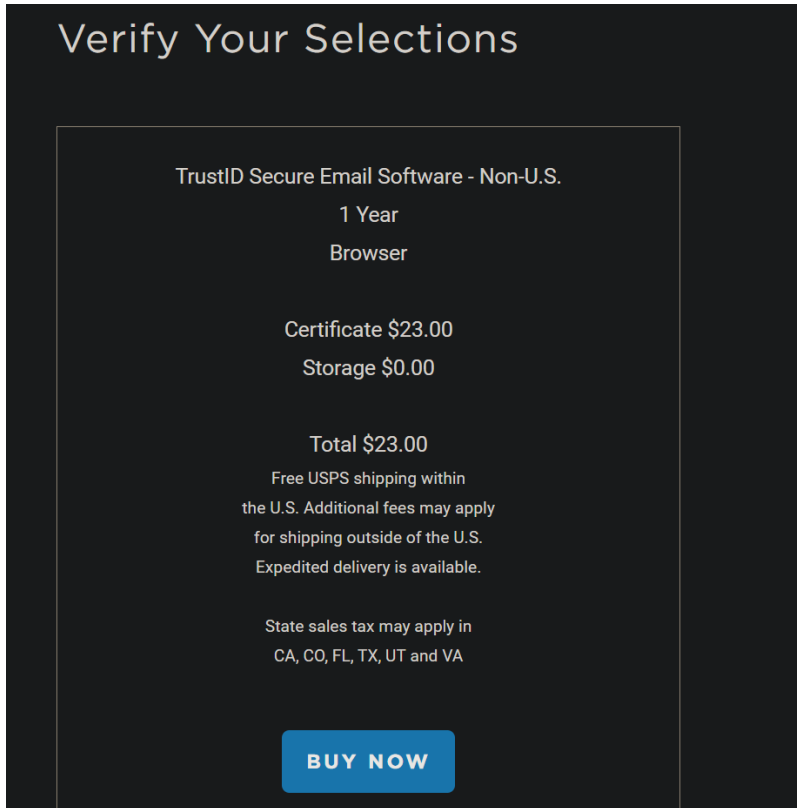
- 2) Now select your certificate type. If you are in the U.S., select '**TrustID Secure Email Software**'. If you are outside the U.S., select '**TrustID Secure Email Software - Non-U.S.**'. Then click '**NEXT**'.



- 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**'.



Verify Your Selections

TrustID Secure Email Software - Non-U.S.

1 Year
Browser

Certificate \$23.00
Storage \$0.00

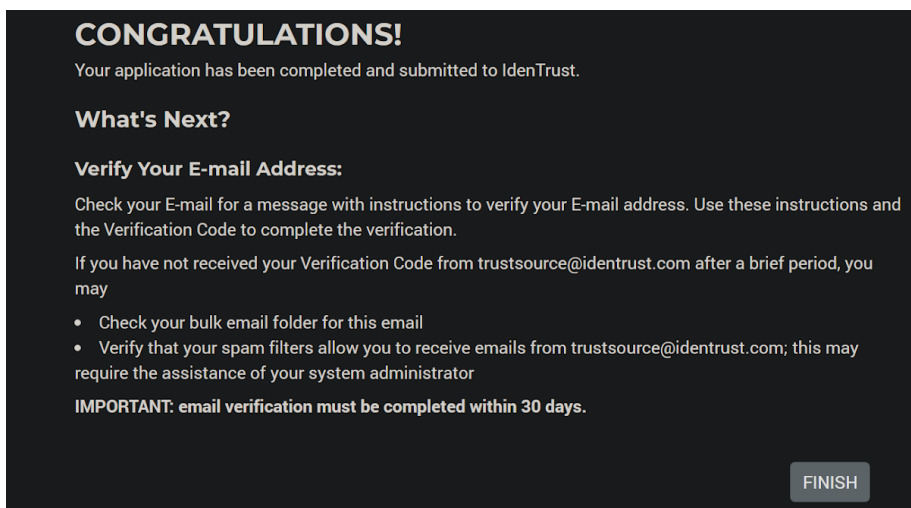
Total \$23.00

Free USPS shipping within
the U.S. Additional fees may apply
for shipping outside of the U.S.
Expedited delivery is available.

State sales tax may apply in
CA, CO, FL, TX, UT and VA

BUY NOW

- 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**'.



CONGRATULATIONS!

Your application has been completed and submitted to IdenTrust.

What's Next?

Verify Your E-mail Address:

Check your E-mail for a message with instructions to verify your E-mail address. Use these instructions and the Verification Code to complete the verification.

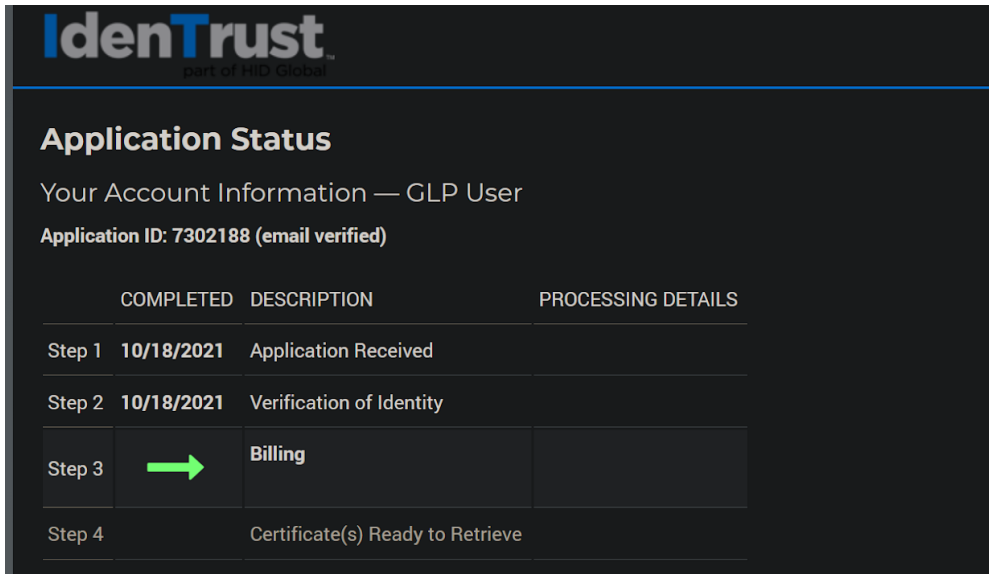
If you have not received your Verification Code from trustsource@identrust.com after a brief period, you may

- Check your bulk email folder for this email
- Verify that your spam filters allow you to receive emails from trustsource@identrust.com; this may require the assistance of your system administrator

IMPORTANT: email verification must be completed within 30 days.

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).




IdenTrust
part of HID Global

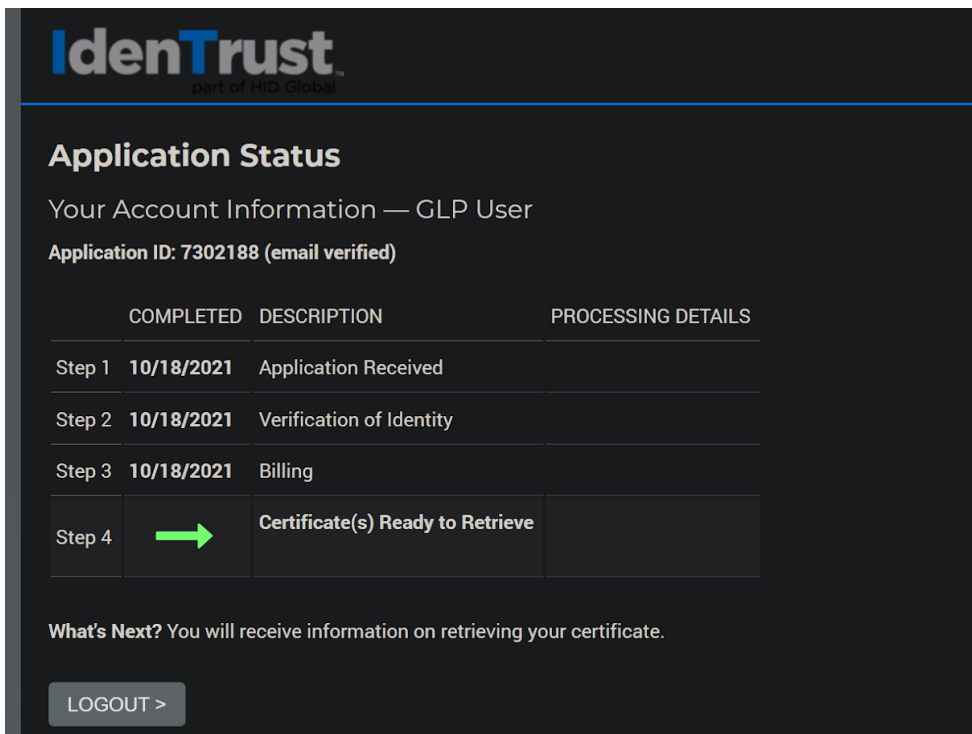
Application Status

Your Account Information — GLP User

Application ID: 7302188 (email verified)

	COMPLETED	DESCRIPTION	PROCESSING DETAILS
Step 1	10/18/2021	Application Received	
Step 2	10/18/2021	Verification of Identity	
Step 3		Billing	
Step 4		Certificate(s) Ready to Retrieve	

Once your certificate is ready, you will see this:




IdenTrust
part of HID Global

Application Status

Your Account Information — GLP User

Application ID: 7302188 (email verified)

	COMPLETED	DESCRIPTION	PROCESSING DETAILS
Step 1	10/18/2021	Application Received	
Step 2	10/18/2021	Verification of Identity	
Step 3	10/18/2021	Billing	
Step 4		Certificate(s) Ready to Retrieve	

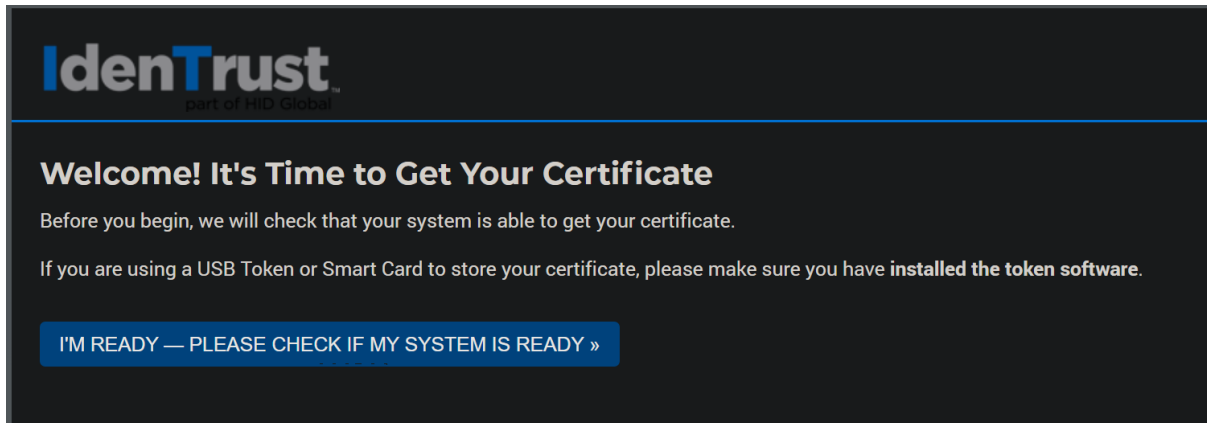
What's Next? You will receive information on retrieving your certificate.

LOGOUT >

- 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.**

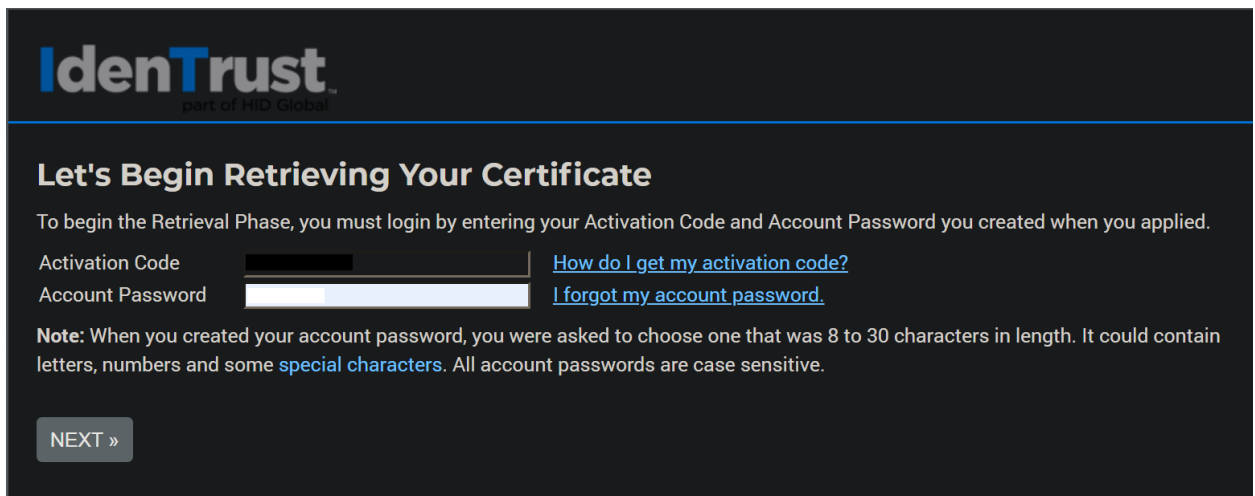
In the email, click on www.identrust.com/install to install your certificate on your computer.

Then click the 'I'M READY' button:



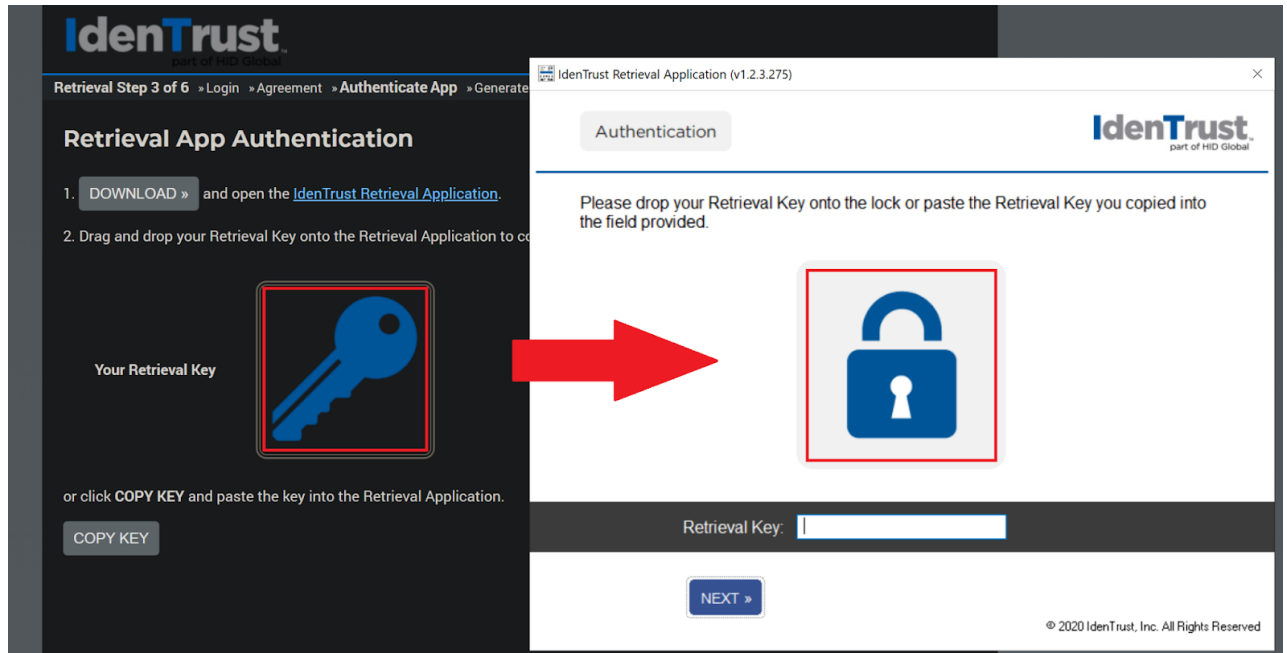
The screenshot shows the IdenTrust website interface. At the top is the IdenTrust logo with the tagline 'part of HID Global'. Below the logo, the heading 'Welcome! It's Time to Get Your Certificate' is displayed. Underneath, there are two lines of text: 'Before you begin, we will check that your system is able to get your certificate.' and 'If you are using a USB Token or Smart Card to store your certificate, please make sure you have installed the token software.' At the bottom of this section is a blue button with the text 'I'M READY — PLEASE CHECK IF MY SYSTEM IS READY »'.

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

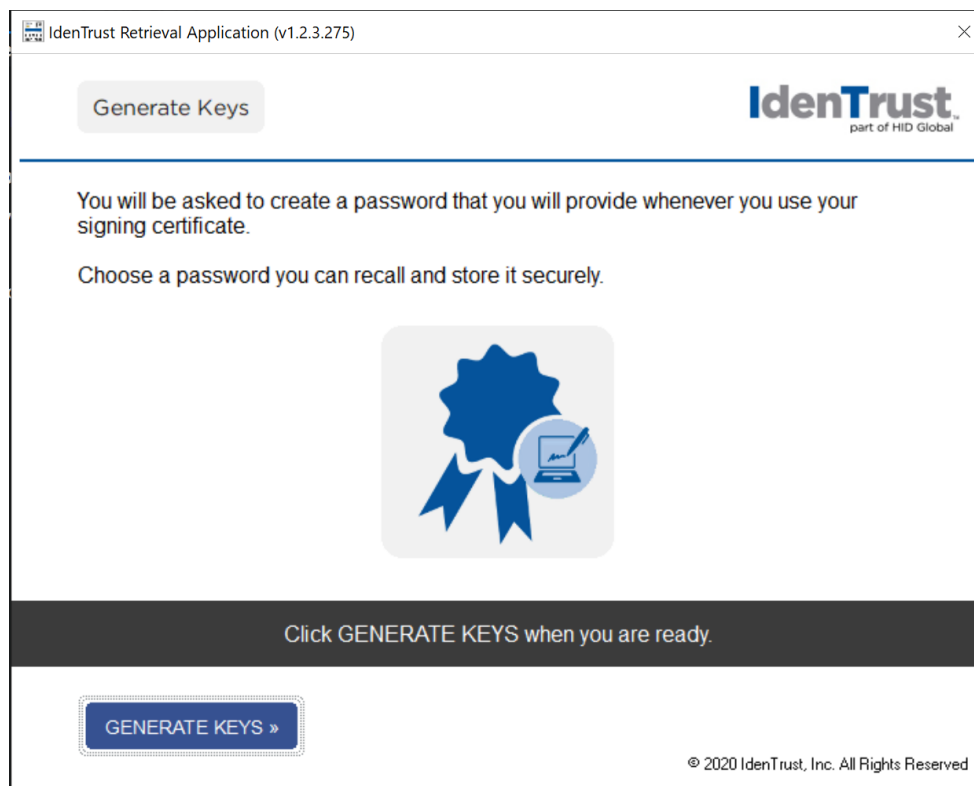


The screenshot shows the IdenTrust website interface for the next step. At the top is the IdenTrust logo with the tagline 'part of HID Global'. Below the logo, the heading 'Let's Begin Retrieving Your Certificate' is displayed. Underneath, there is a line of text: 'To begin the Retrieval Phase, you must login by entering your Activation Code and Account Password you created when you applied.' Below this text are two input fields: 'Activation Code' and 'Account Password'. To the right of the 'Activation Code' field is a link: 'How do I get my activation code?'. To the right of the 'Account Password' field is a link: 'I forgot my account password.' Below these fields is a 'Note' section: 'Note: When you created your account password, you were asked to choose one that was 8 to 30 characters in length. It could contain letters, numbers and some special characters. All account passwords are case sensitive.' At the bottom of this section is a grey button with the text '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:



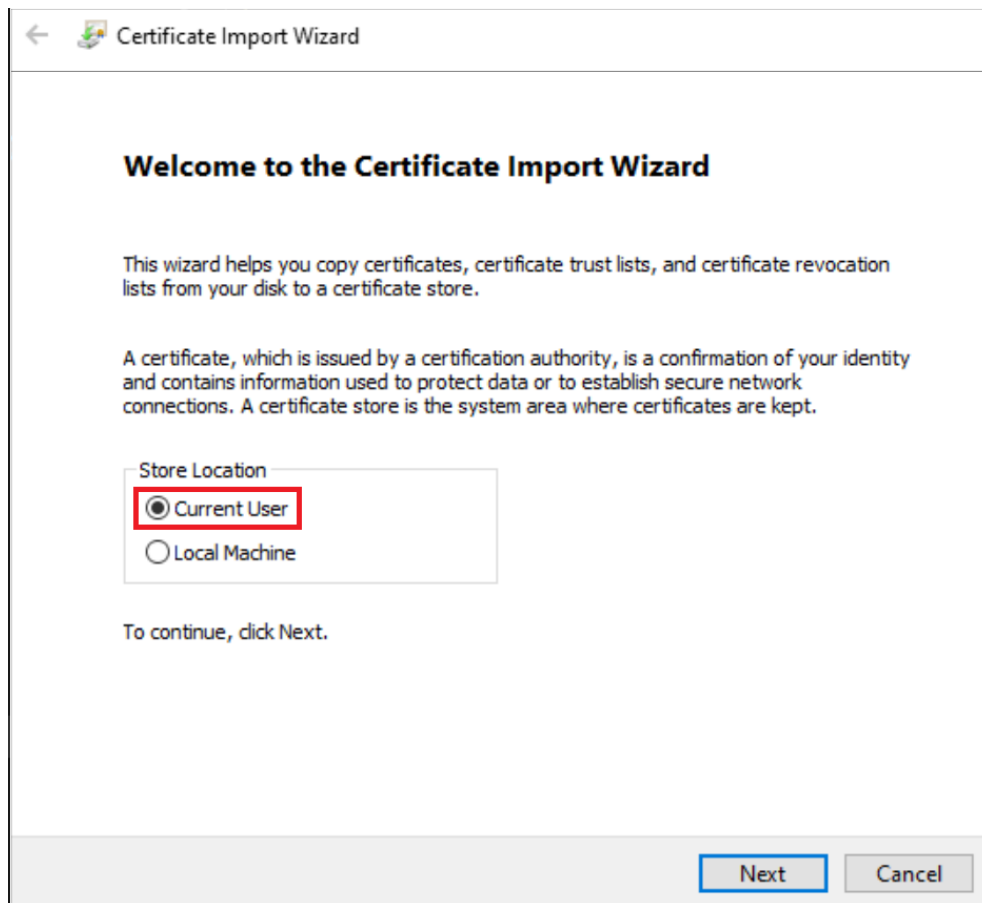
- 12) In the Retrieval Application, click on '**GENERATE KEYS**'.



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

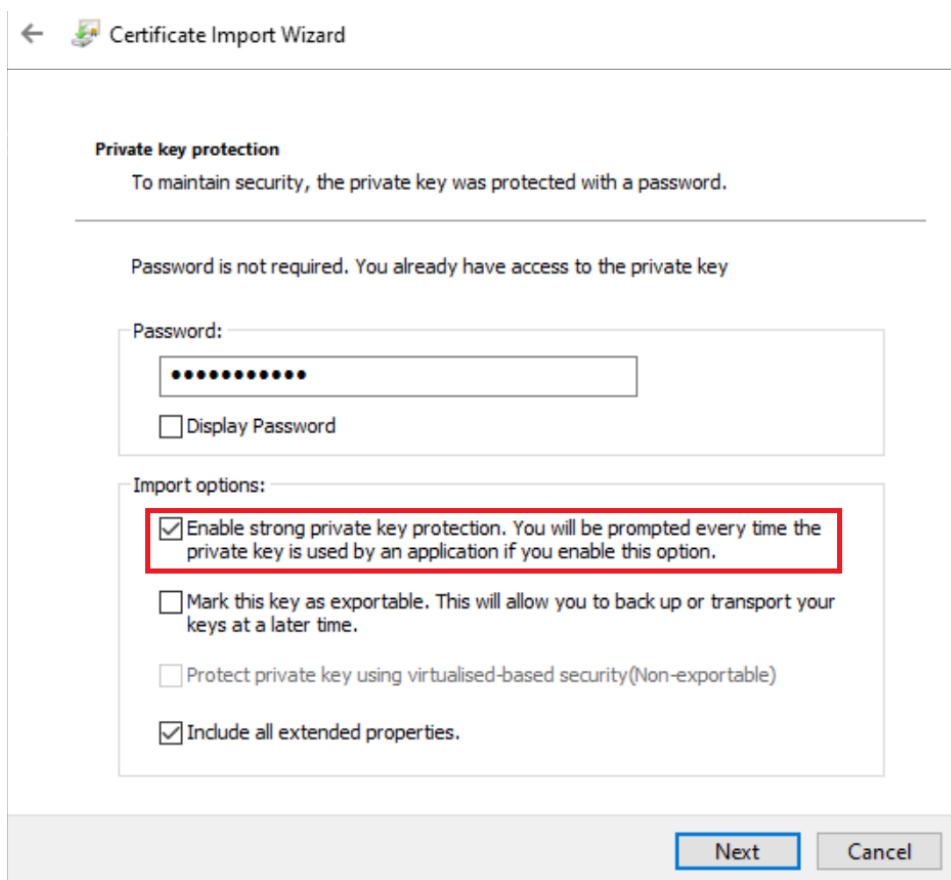
Part 2 - Import Client Authentication Certificate

- 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'**.



The image shows a 'Certificate Import Wizard' dialog box. At the top, there is a back arrow and the title 'Certificate Import Wizard'. Below this, the section 'Private key protection' is displayed. It contains the text 'To maintain security, the private key was protected with a password.' followed by a horizontal line and then 'Password is not required. You already have access to the private key'. Below this is a 'Password:' label and a text box containing ten dots. A checkbox labeled 'Display Password' is located below the text box. The 'Import options:' section follows, containing four checkboxes. The first checkbox, 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.', is checked and highlighted with a red rectangular border. The other three checkboxes are unchecked: 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.', 'Protect private key using virtualised-based security(Non-exportable)', and 'Include all extended properties.' (which is checked). At the bottom right, there are 'Next' and 'Cancel' buttons.

← Certificate Import Wizard

Private key protection
To maintain security, the private key was protected with a password.

Password is not required. You already have access to the private key

Password:

.....

☐ Display Password

Import options:

☒ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.


☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☐ Protect private key using virtualised-based security(Non-exportable)

☒ Include all extended properties.

Next Cancel

- 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'**.

←  Certificate Import Wizard

Certificate Store
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

☒ Automatically select the certificate store based on the type of certificate

☐ Place all certificates in the following store

Certificate store:

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

Completing the Certificate Import Wizard

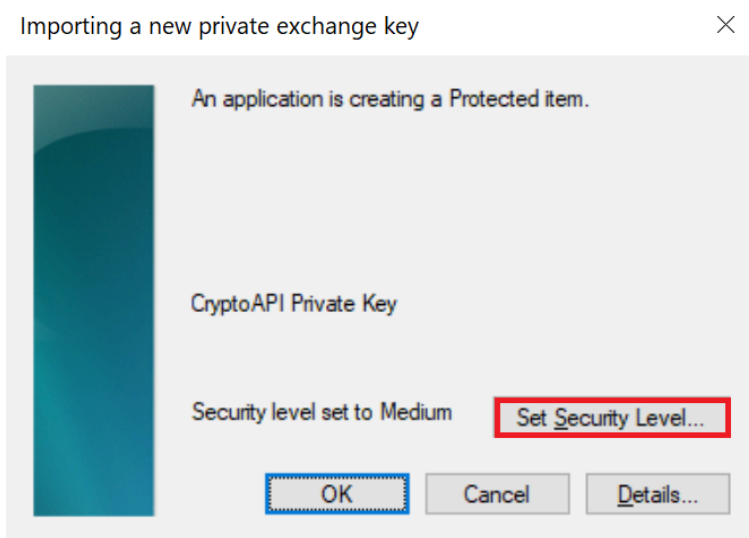
The certificate will be imported after you click Finish.

You have specified the following settings:

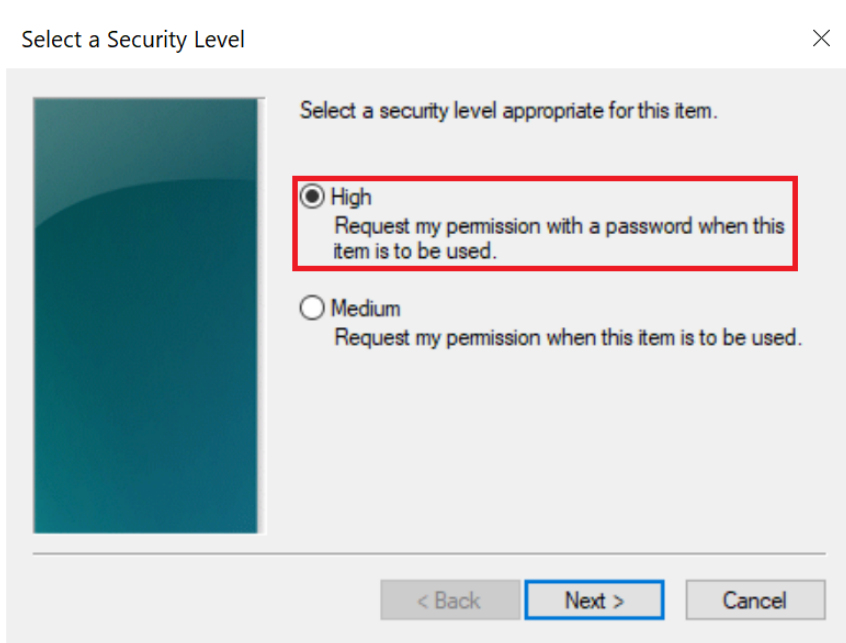
Certificate Store Selected	Automatically determined by the wizard
Content	PFX
File Name	C:\Users\ [REDACTED]

< >

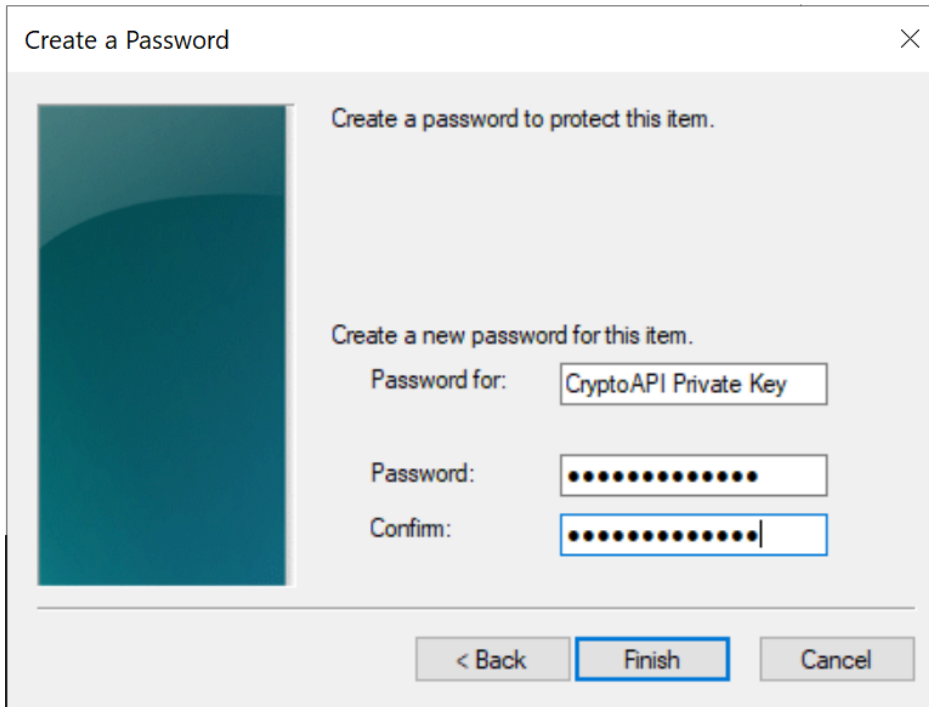
- 6) The Certificate Import Wizard will now start importing your certificate. You will be asked to set your security level. High security is required to be able to save GLP documents in LabChart, so click '**Set Security Level...**'.



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'**.



Create a Password

Create a password to protect this item.

Create a new password for this item.

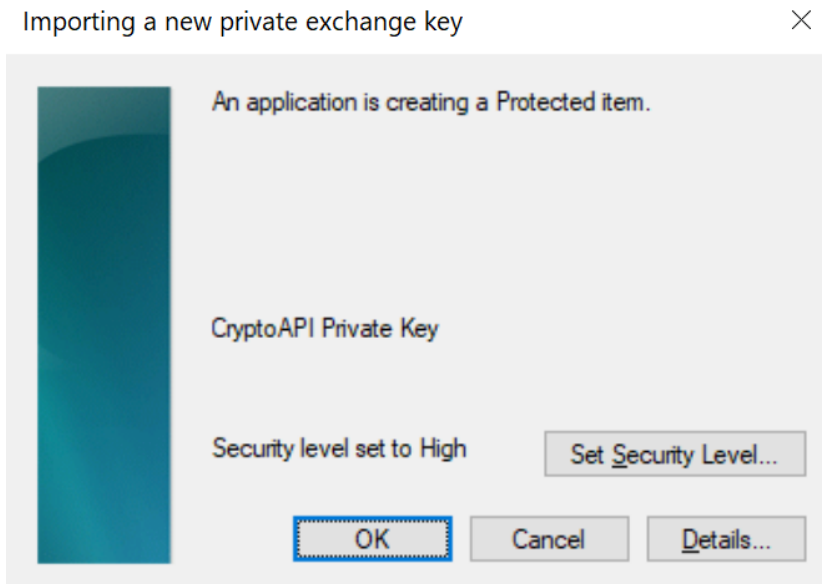
Password for: CryptoAPI Private Key

Password:

Confirm:

< Back Finish Cancel

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



Importing a new private exchange key

An application is creating a Protected item.

CryptoAPI Private Key

Security level set to High

Set Security Level...

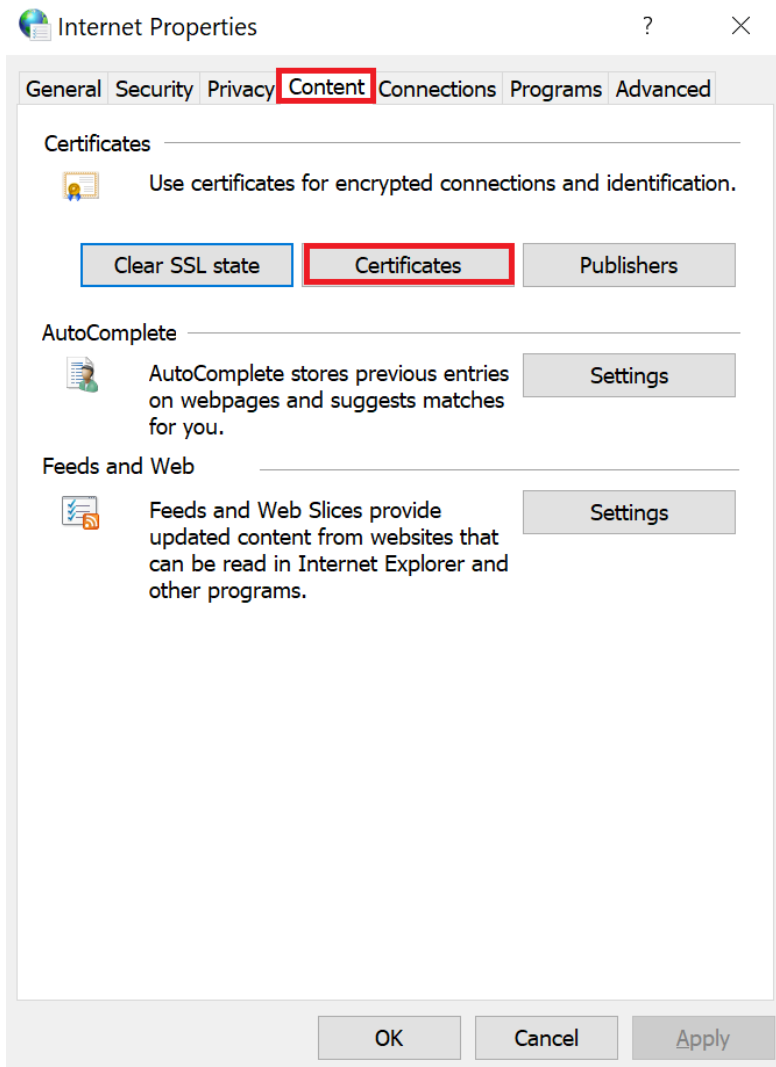
OK Cancel Details...

Part 3 - Export Client Public Certificate

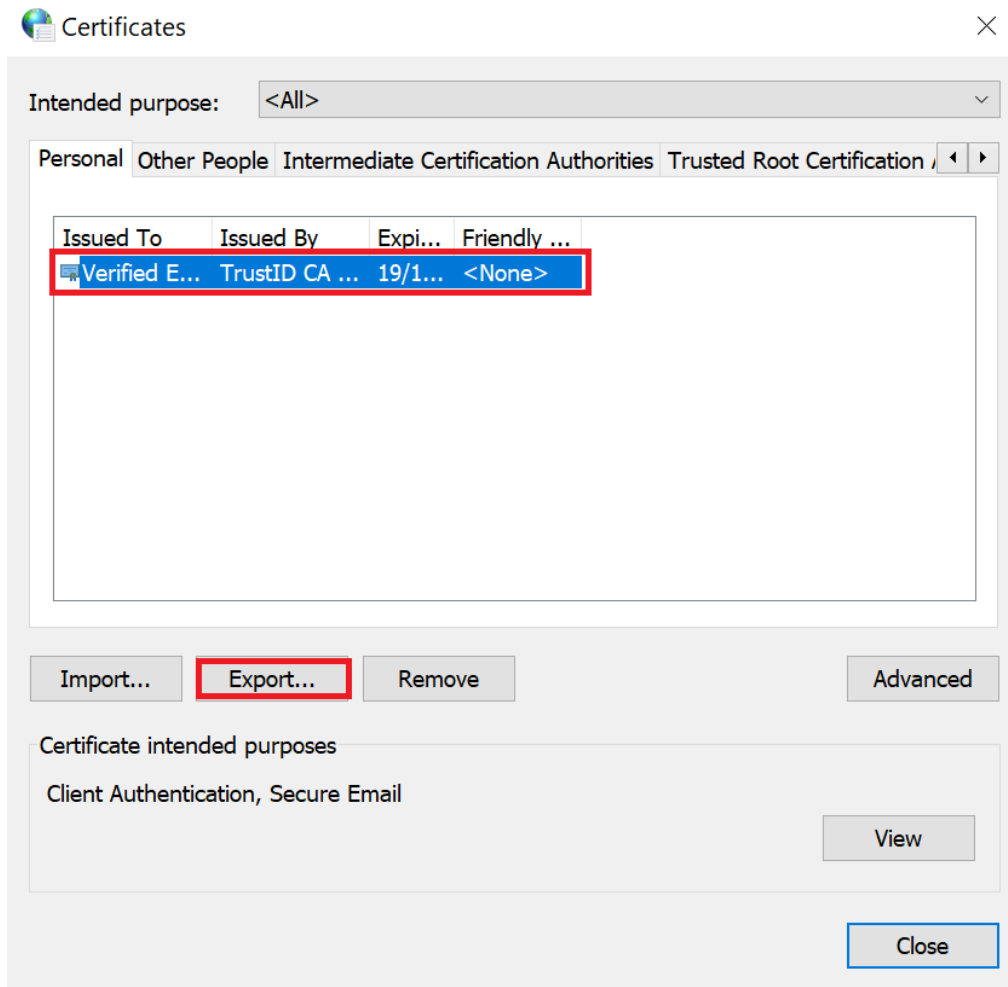
We will now run through the steps required to export the client's **public certificate**, which will be given to a Lab Administrator to install on their GLP server. Without this public certificate installed on the GLP server, the Client will not be able to save GLP documents.

- 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**'.

←  Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

☐ Yes, export the private key

☒ No, do not export the private key

Note: The associated private key is marked as not exportable. Only the certificate can be exported.

Next

Cancel

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

←  Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.


Select the format you want to use:

- ☒ **DER encoded binary X.509 (.CER)**
- ☐ Base-64 encoded X.509 (.CER)
- ☐ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
- ☐ Include all certificates in the certification path if possible
- ☐ Personal Information Exchange - PKCS #12 (.PFX)
- ☐ Include all certificates in the certification path if possible
- ☐ Delete the private key if the export is successful
- ☐ Export all extended properties
- ☐ Enable certificate privacy
- ☐ Microsoft Serialised Certificate Store (.SST)

Next

Cancel

- 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.

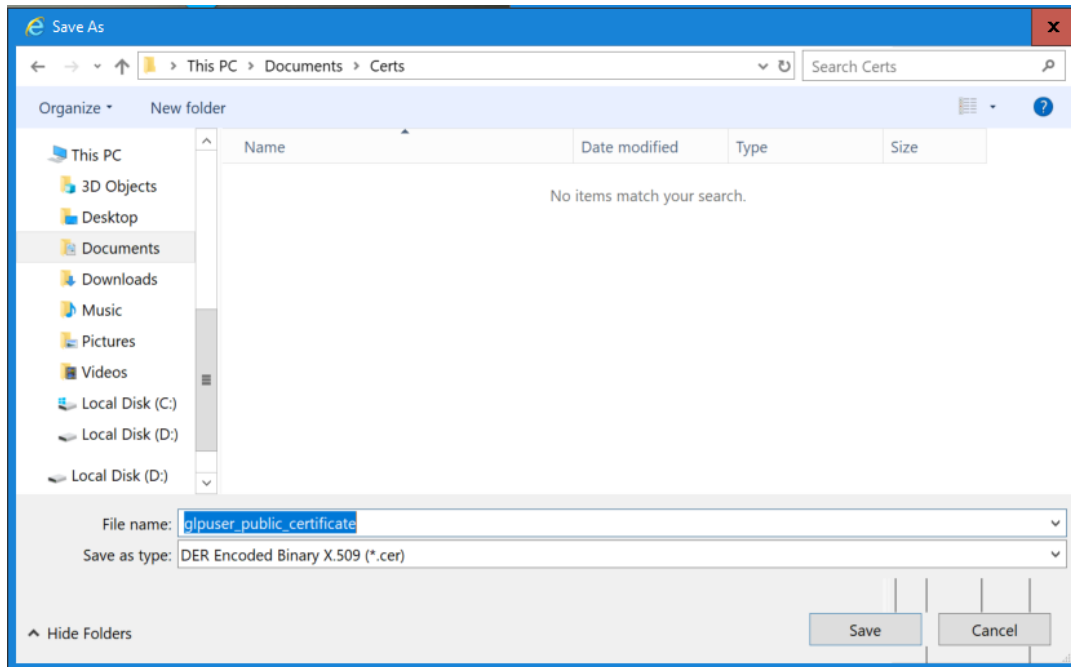
←  Certificate Export Wizard

File to Export
Specify the name of the file you want to export

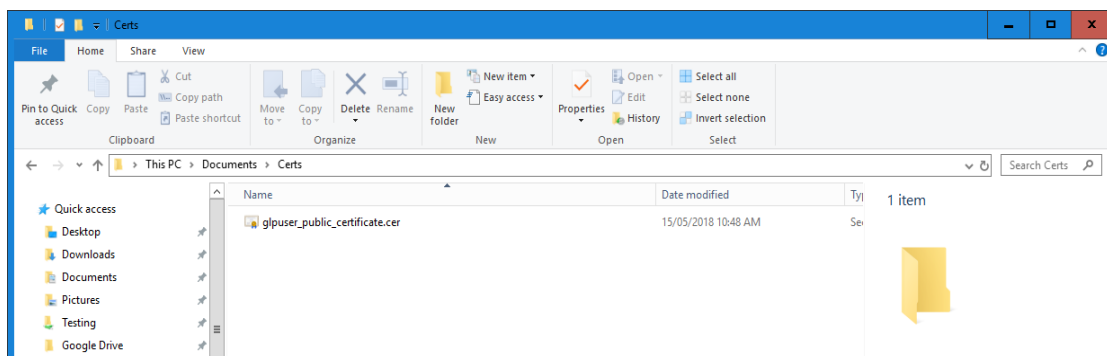
File name:

Browse...

- 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?

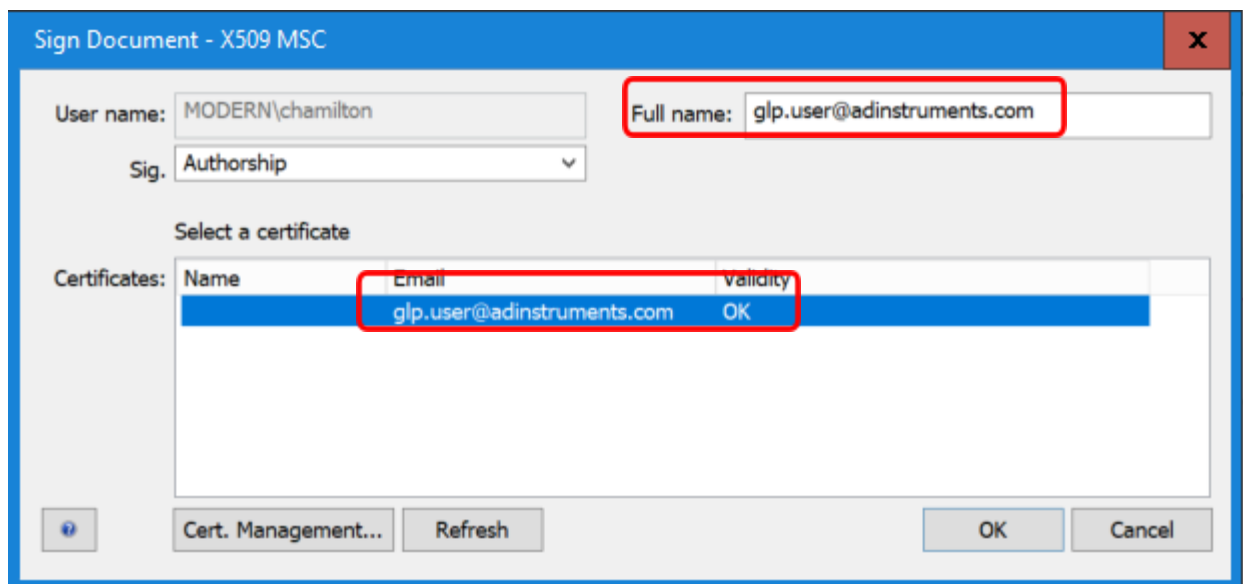
A) In Part 2 – Step 7 when the client private certificate was imported, you were prompted to enter a password to protect the private certificate. You must use this password when saving GLP documents in LabChart, so LabChart can access the client certificate and sign the GLP document.

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.