Netrust User Setup Guide

Version 1.7

Authored by: Netrust Customer Support

Identification

Document Author:	Customer Service
Document Version:	1.7

Revision History

Version	Effective Date	Summary of Changes	Author
1.0	April 2020	Initial Release	Jasmine Leong
1.1	April 2020	Updated changes	Kirti Raj
1.2	May 2020	Addition of EESP features	Kirti Raj
1.3	May 2020	EESP admin usage	Jasmine Leong
1.4	Dec 2020	Email and fax update	Kirti Raj
1.5	Aug 2021	Logo, address and software version update	Isaac Zainal
1.6	July 2023	Update of Software Information – Entrust Certificate Agent (ECA)	Susan Ler
1.7	Feb 2024	Update of Software Information – Safenet Authentication Client (SAC)	Susan Ler

Table of Contents

1. About this Document

This document is an overview of the software installation and usages of the eToken device on multiple platforms.

2. How To Install Safenet Authentication Client Tools

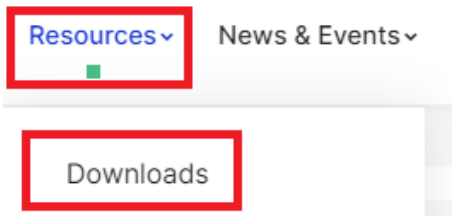
The Safenet client has to be installed in order for the token to be detected in the machine, kindly follow the steps below to complete the installation.

NOTE:

***For CORENET users: Skip this step and download Netrust Digital Signer v4.1.3*.**

- **STEP 1**

Go to Netrust website https://www.netrust.net/ > click on Resources and select Downloads.

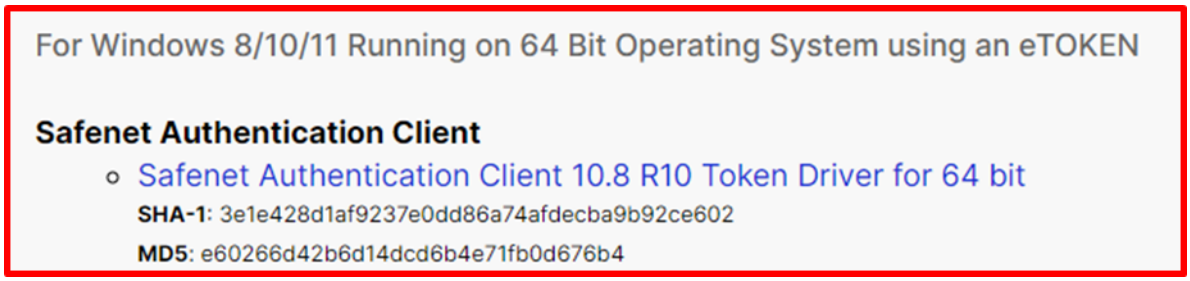


Under Netrust Downloadable Software, select the software depending on what is the version of your PC's Operating System and Windows Version.

Example: I am using a Windows 10 PC running on 64 Bit Operating System

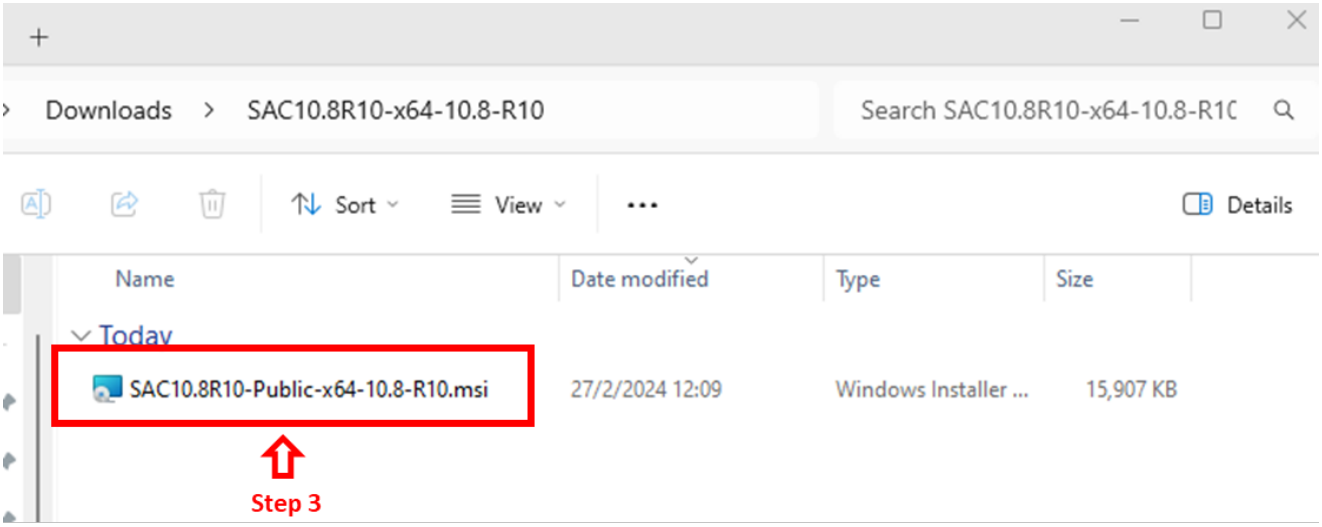
- **STEP 2**

Select and run the file accordingly.



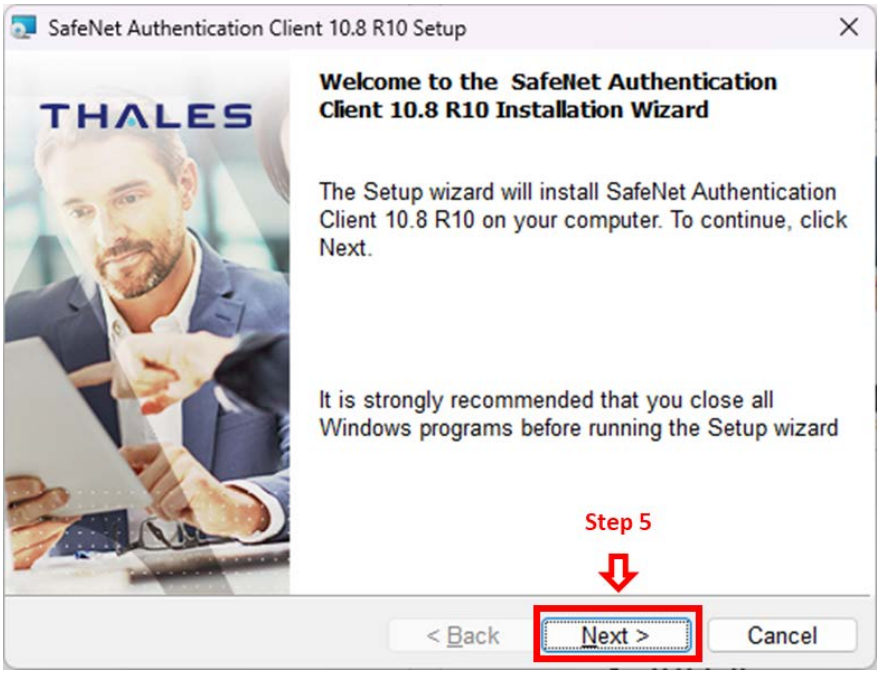
- **STEP 3**

Open the software folder, extract the ZIP file and double click on SAC 10.8 X64-10.8.msi file to run the installation

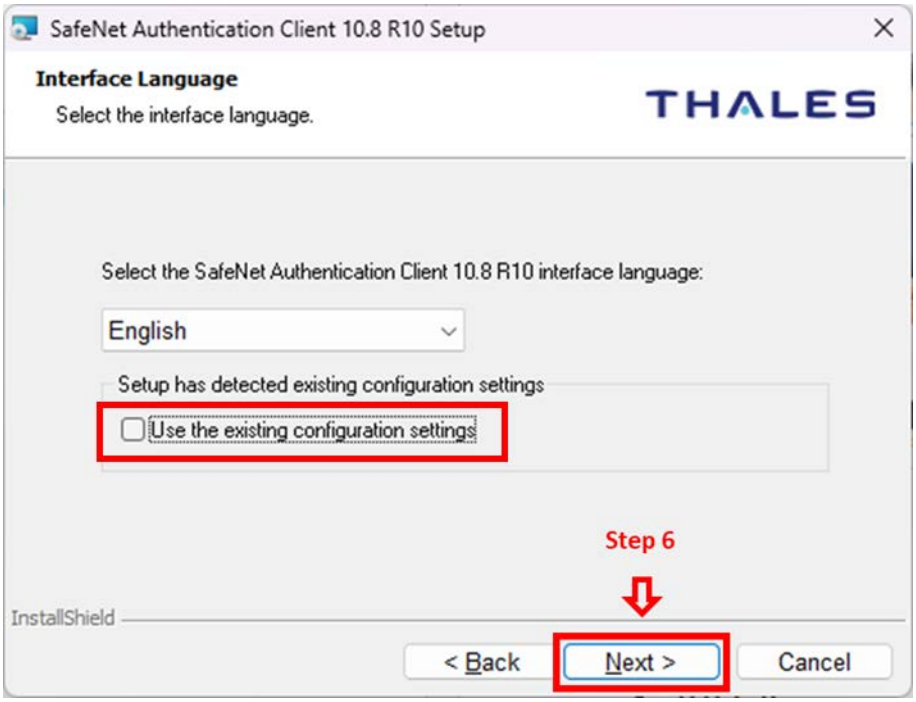


- **STEP 4**
  Click on 'More Info' and 'Run anyway' to proceed

- **STEP 5**
  Click on 'Next' to proceed.

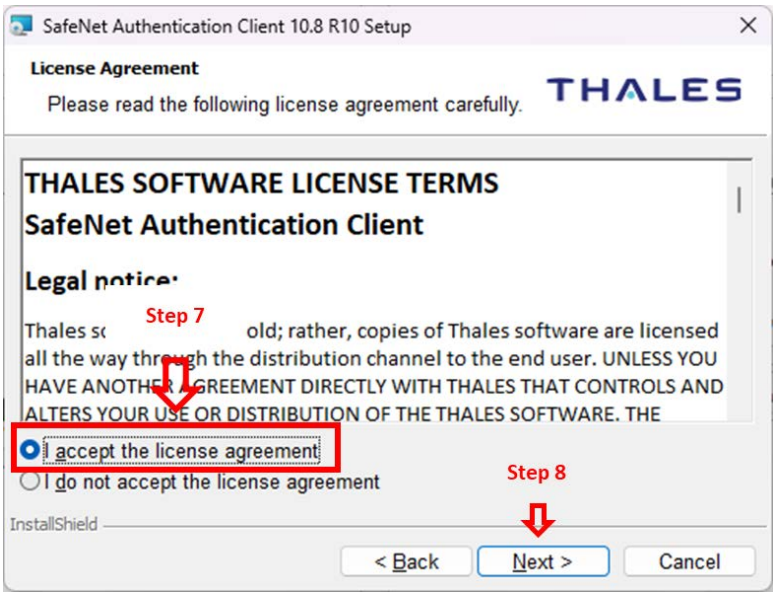


- **STEP 6**
  Uncheck "Use the existing configuration settings" and click on 'Next' to proceed.

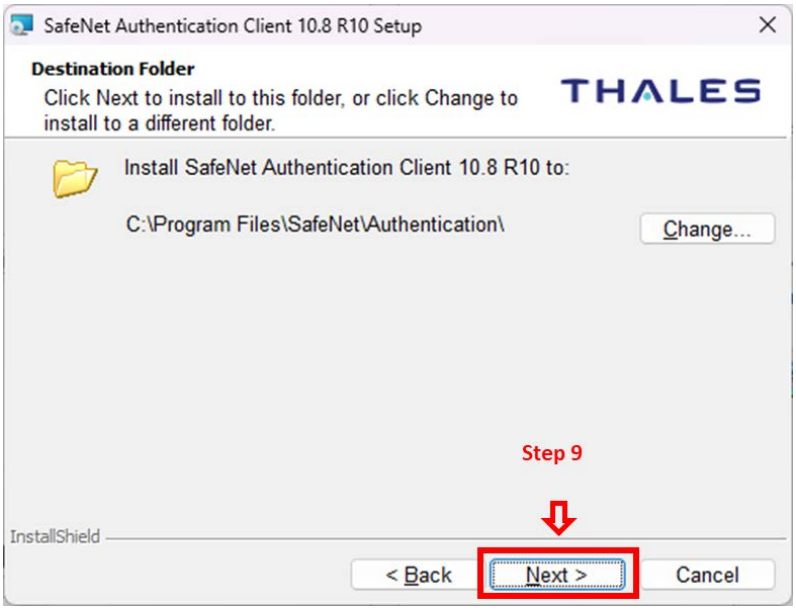


- **STEP 7**
  Select 'I accept the license agreement'

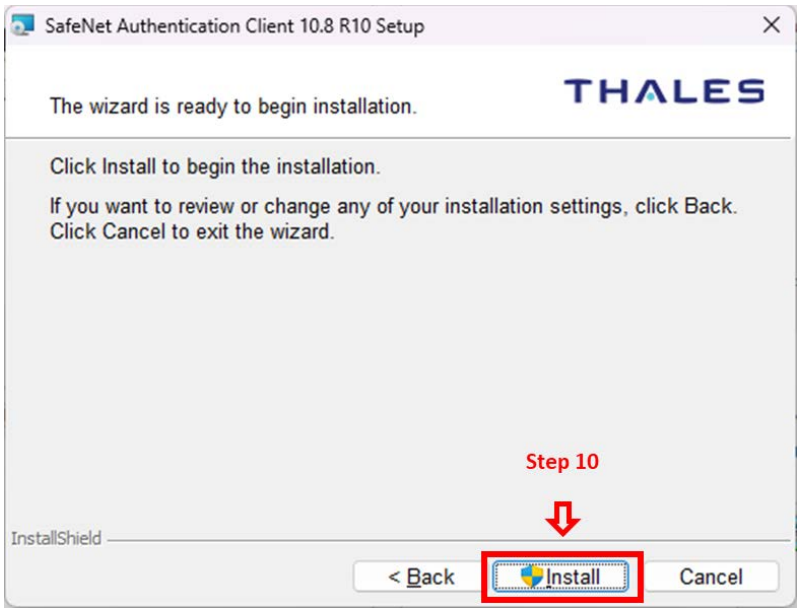
- **STEP 8**
  Click on 'Next' to proceed.

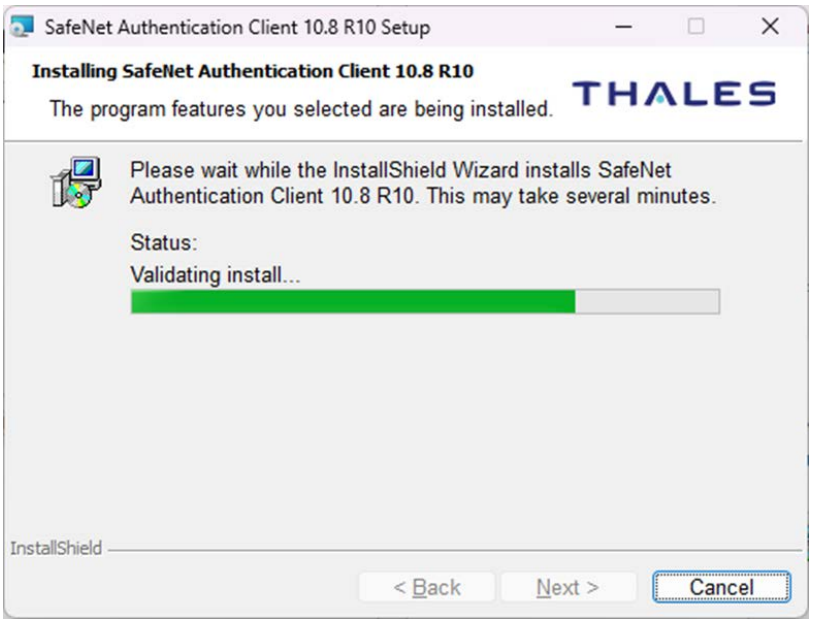


- **STEP 9**
  Click on 'Next' to proceed.



- **STEP 10**
  Click on 'Install' to proceed.





- **STEP 11**
  Click on ‘Finish’ after the installation have been completed.

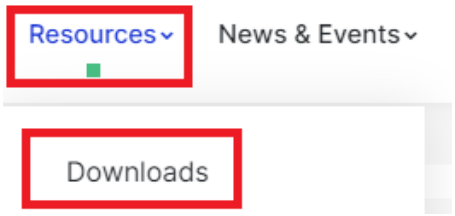
3. How To Install Entrust Certificate Agent (ECA)

Note: If you currently have Entrust Entelligence Security Provider installed, please uninstall first before installing Entrust Certificate Agent.

- **STEP 1**

Go to Netrust website https://www.netrust.net/

Click on Resources, then click on Downloads.



Under Netrust Downloadable Software, select the software depending on what is the version of your PC's Operating System and Windows Version.

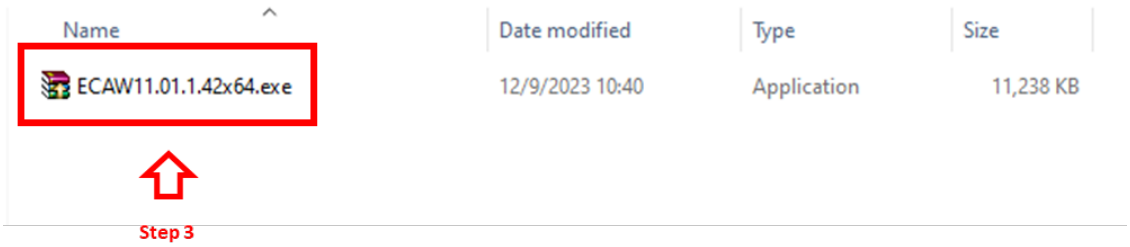
Example: I am using a Windows 10 PC running on 64 Bit Operating System

- **STEP 2**

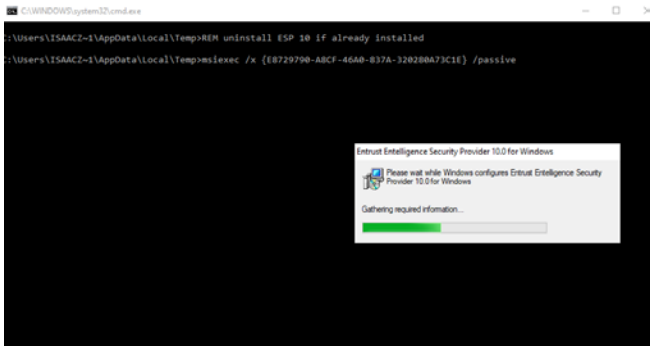
Select and download the file under Entrust Certificate Agent 11 for eToken

- **STEP 3**

Open the software folder, extract the ZIP file, and double click on ECAW11.01.1.42x64.exe file to run the installation



- **STEP 4**
  The installation will proceed automatically.



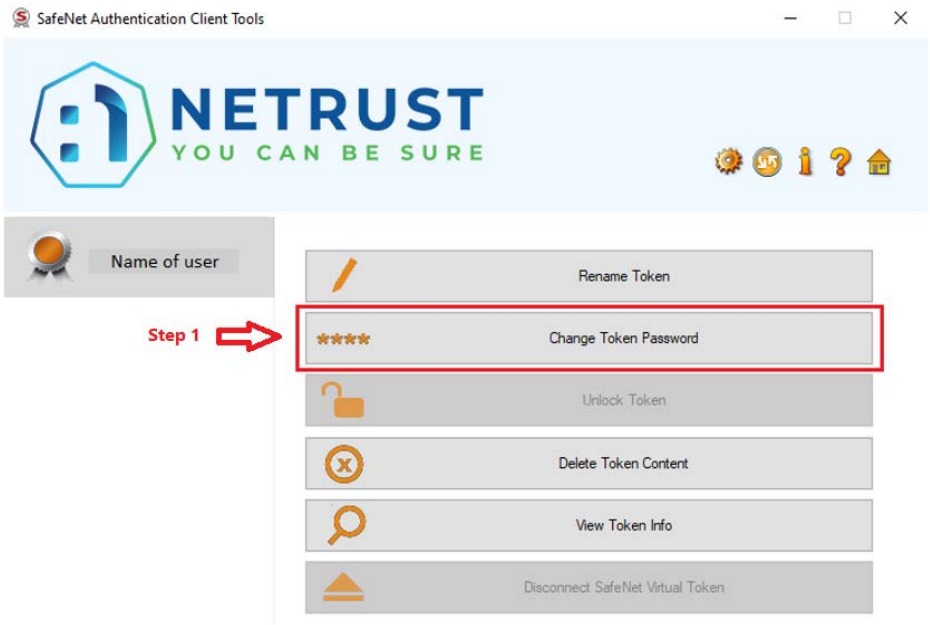
- **STEP 5**
  After installation the icon will appear at the Windows taskbar.

4. How To Change eToken Password via Safenet Authentication Client Tools

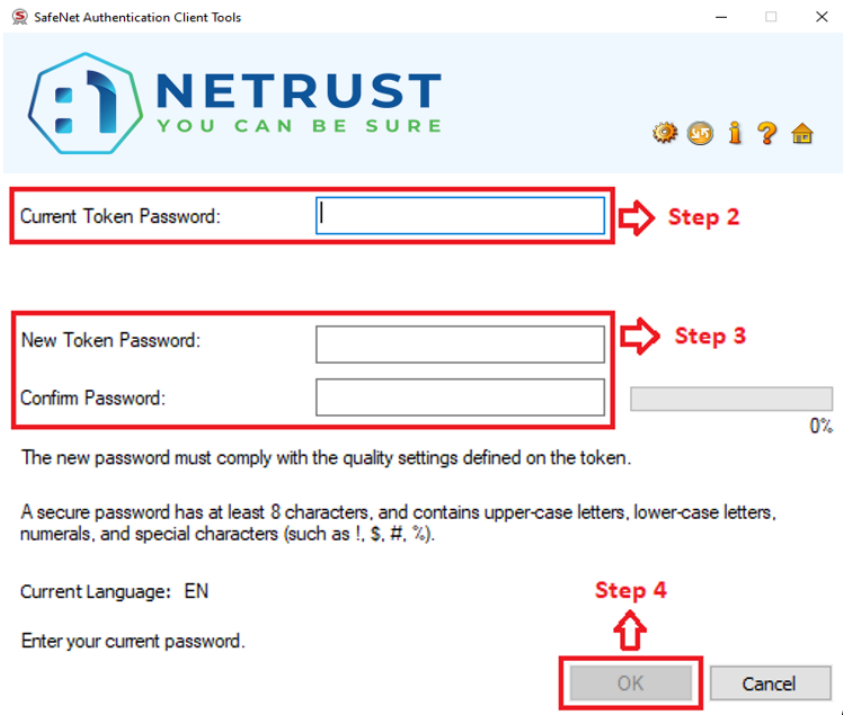
- **STEP 1**
  Open SafeNet Authentication Client Tools

  Ensure that your eToken is plugged in

  Click on ‘Change Token Password’



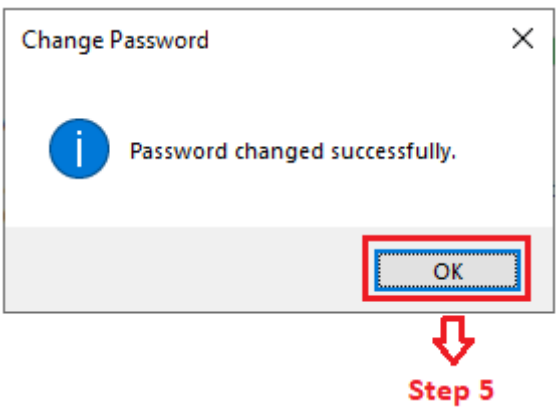
- **STEP 2**
  Enter Current Token Password
  NOTE: This instruction will not be applicable for users that has forgotten the current token password. If you have not set a password at Netrust office, please enter the default token password: 1234567890



- **STEP 3**
  Enter your preferred New Token Password

- **STEP 4**
  Click ‘OK’ to proceed

- **STEP 5**
  Password is changed successfully when you received this prompt.
  Click ‘OK’ to proceed.



5. Online Certificate Renewal via Entrust Certificate Agent (ECA)

1. What is the function of ECA?

Entrust Certificate Agent (ECA) is a client software which monitors user's certificate expiry status. When the certificate is expiring soon, ECA will prompt users to renew their certificate for user's certificate to be always active and no disruption during day-to-day operation.

It also can encrypt and digitally sign files for safeguarding of files.

2. How to check if your ECA is properly configured

The auto-renewal of Netrust Certificate requires an internet connection to Netrust servers. For the auto update to facilitate users need to make sure the following firewall ports are configured to allow internet connection from user's terminal to Netrust servers:

Port 829 – This port will be used by the ECA program to poll and retrieve available updates/renewal for the certificate

Port 389 – This port is used by ECA to connect to Netrust directory if users need to access the address book using ldap21.netrust.net or for other reasons require access to our LDAP (e.g. secure email)

To test if the ports are configured correctly, on your PC go to command prompt and type:

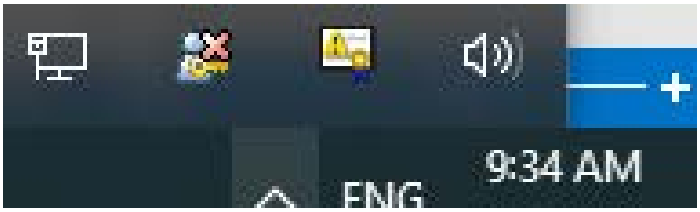
- telnet authority21.netrust.net 829
- telnet ldap21.netrust.net 389

If the ports are not configured correctly, you will receive the message, "*Could not open connection to the host, on port 829: Connection failed"*

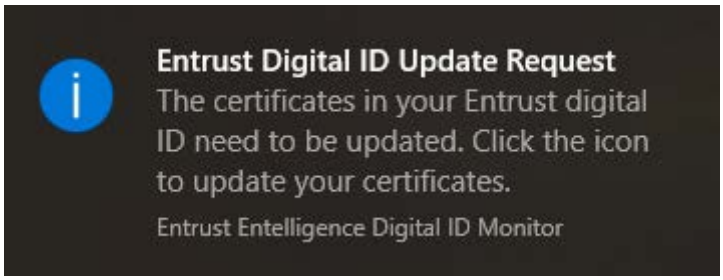
NOTE: You may contact Netrust for assistance or guidance

3. When will I know that my certificate is due for renewal or about to expire?

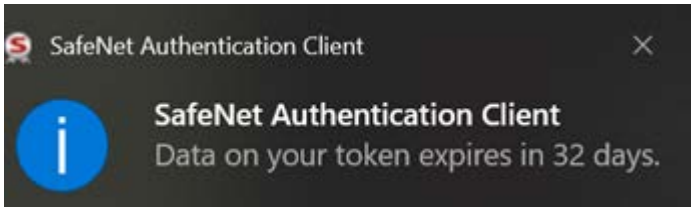
A prompt / notification will be shown at the bottom right of the taskbar where the ECA is installed



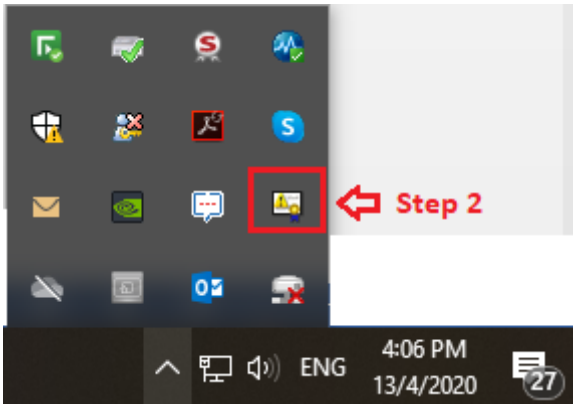
- **STEP 1**
  A pop up message will appear on the bottom right hand corner of the PC, from Entrust Certificate Agent:



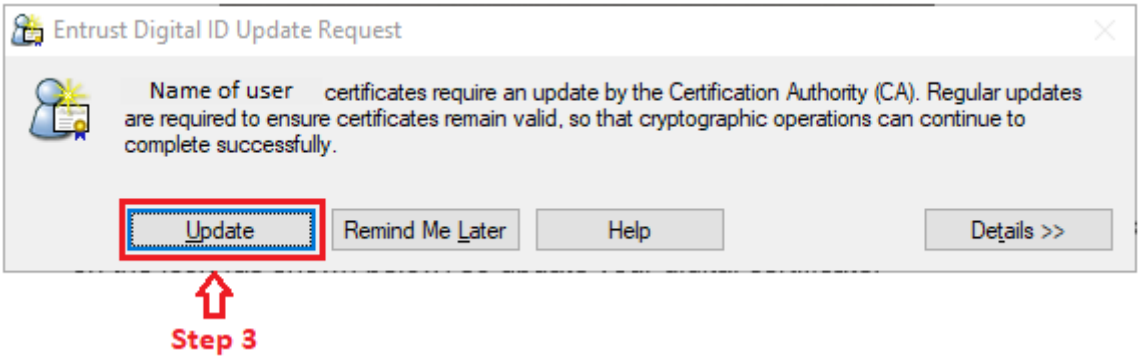
  There will also be a prompt from Safenet Authentication Client (token driver) as below. Please follow from Step 2 to update the token.



- **STEP 2**
  Open up all the hidden icons from the bottom right hand corner of the PC and click on the icon (as shown below) so update your digital certificate

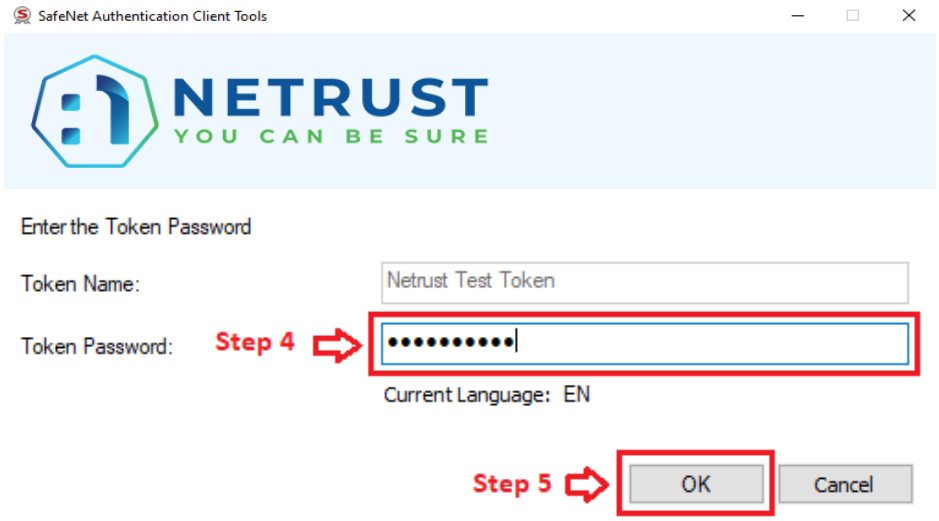


- **STEP 3**
  Click on 'Update' to proceed.

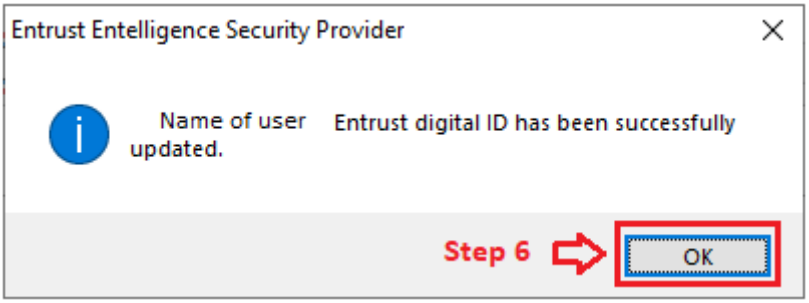


- **STEP 4**
  Enter token password

- **STEP 5**
  Click on 'OK' to proceed



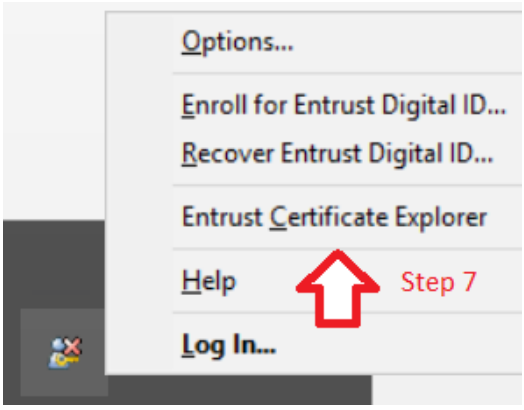
- **STEP 6**
  Click on 'OK' after the certificate has been updated successfully.



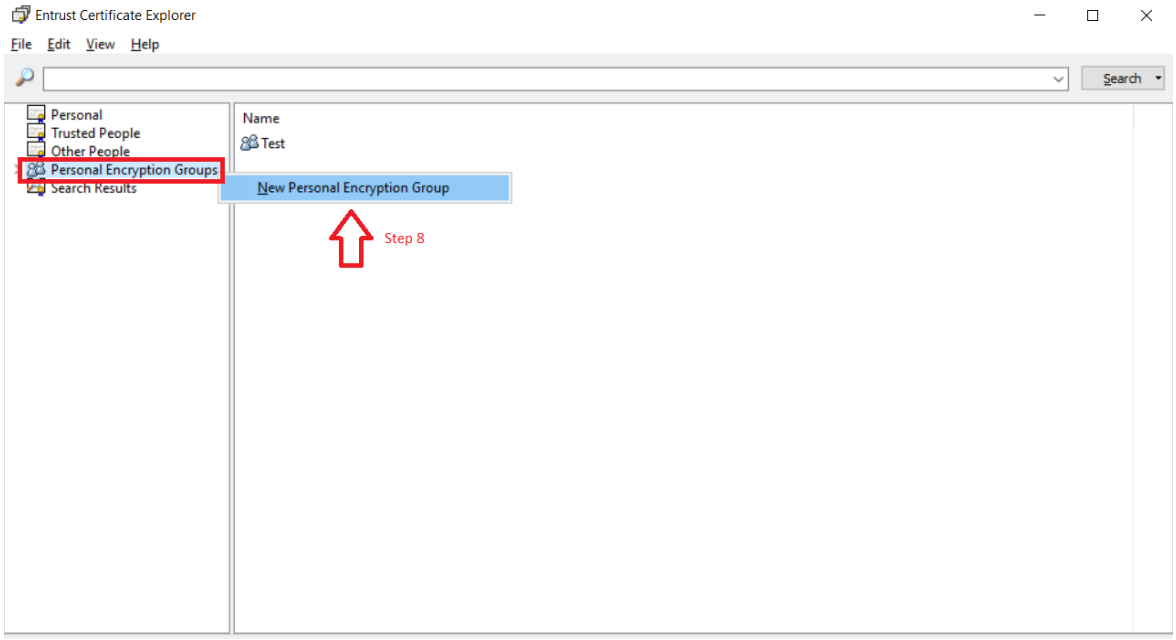
- **STEP 7**
  The ECA is able to create a personal encryption group for file encryption and digital signing for users that frequently communicate

  This personal encryption group can contain recipients from Netrust and other users with a public certificate saved locally

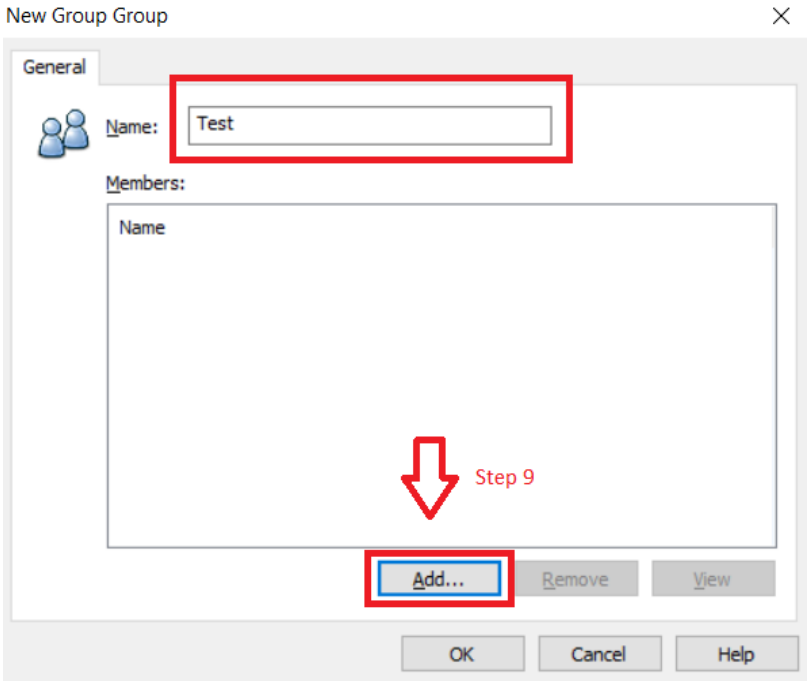
  Right click on the  select the option Entrust certificate explorer



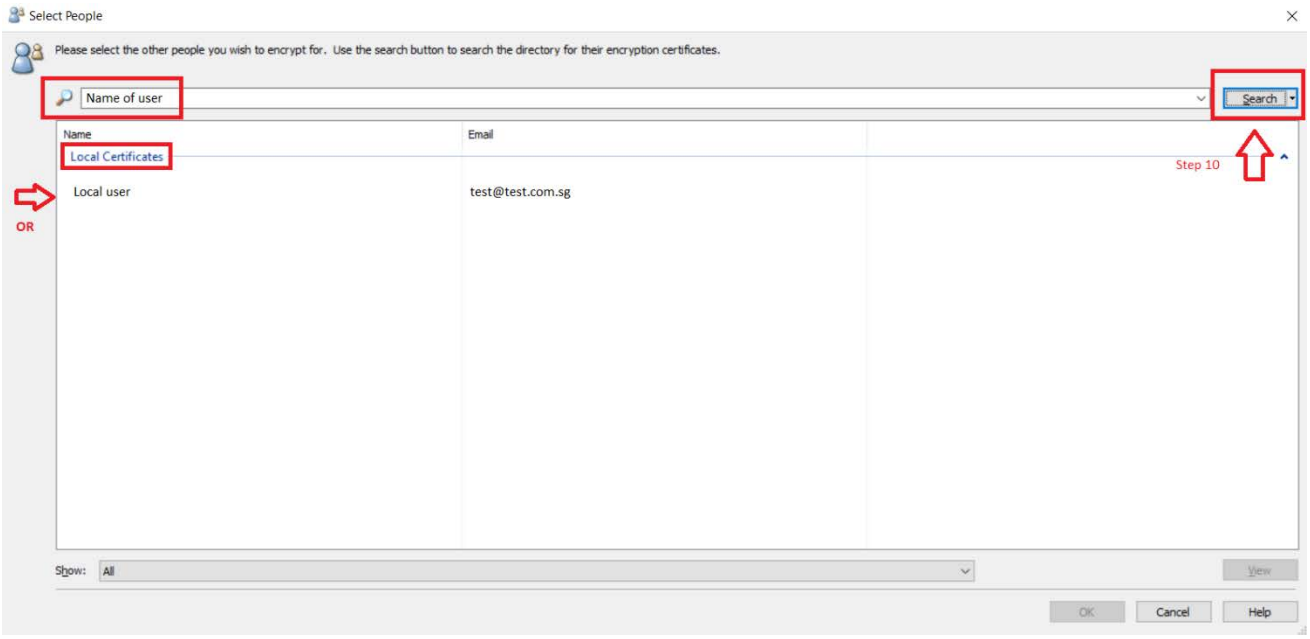
- **STEP 8**
  A pop up window will appear, right click and select New Personal Encryption Group



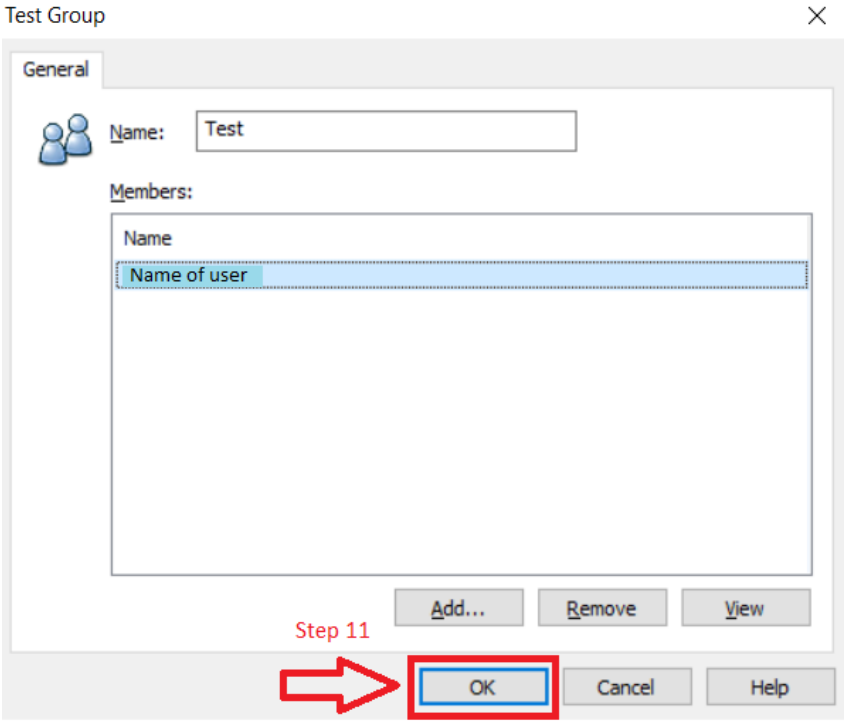
- **STEP 9**
  From the pop up window type to set a group name and click add to choose certificates from the certificate store or Netrust LDAP

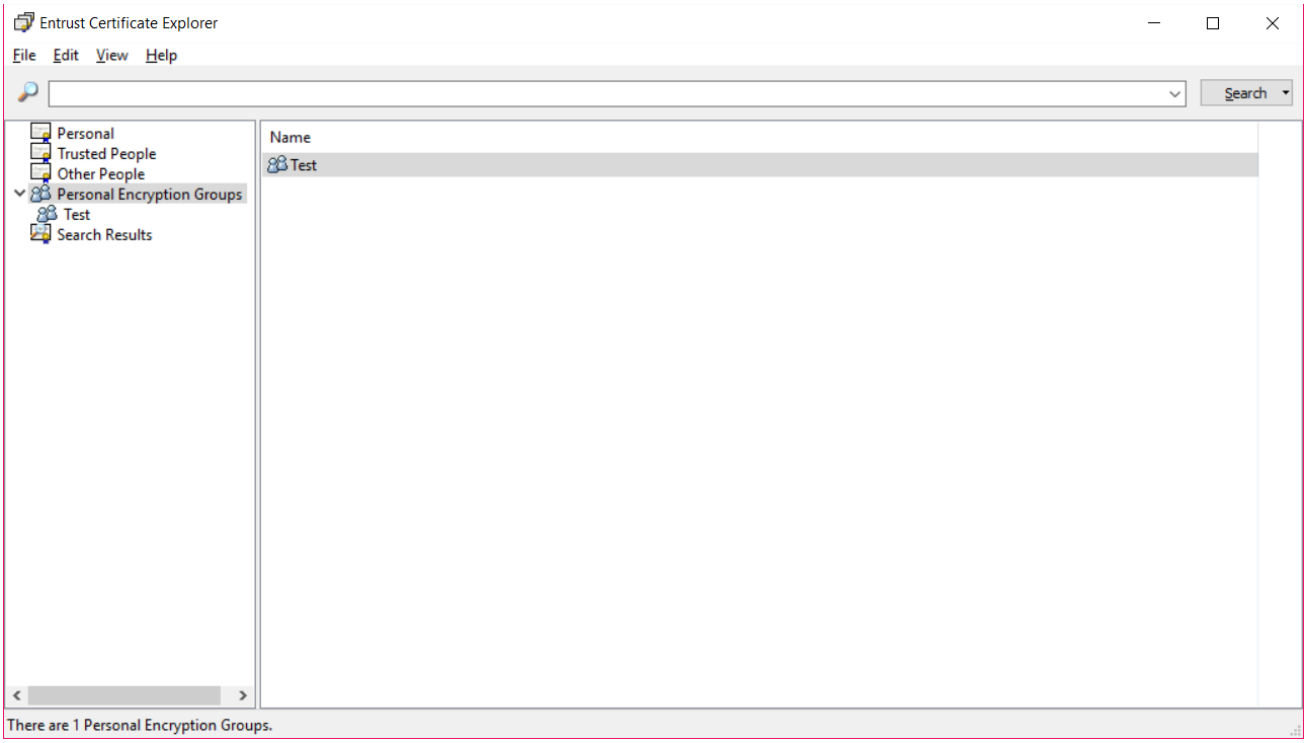


- **STEP 10**
  Type in search user name to find from Netrust LDAP **or** select certificate from local certificate store to add to the Personal Encryption Group



- **STEP 11**
  Click ‘OK’ once all certificates selected to finalize group

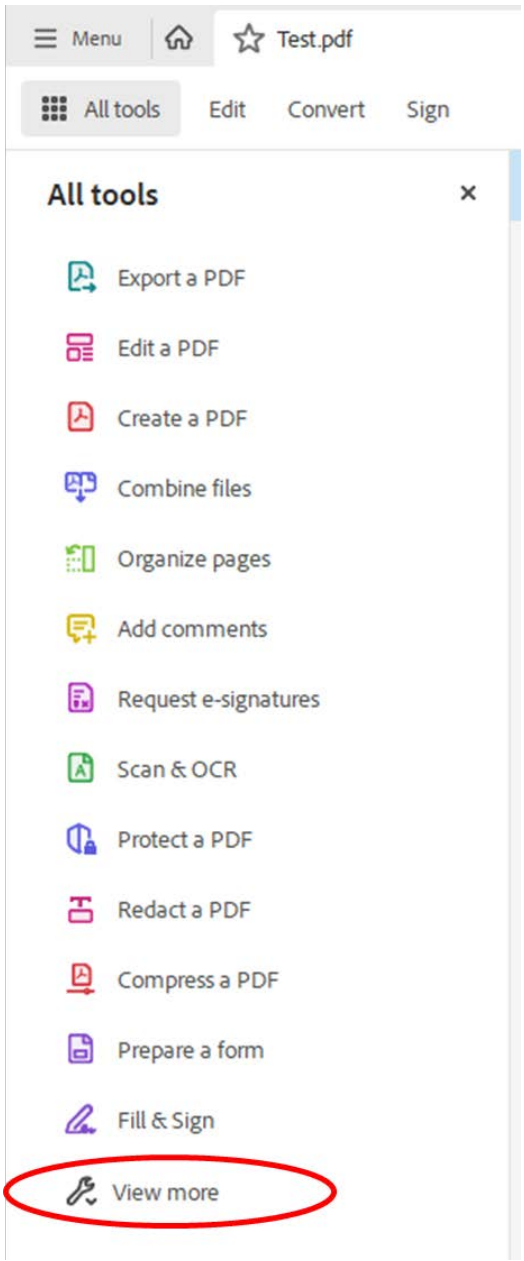


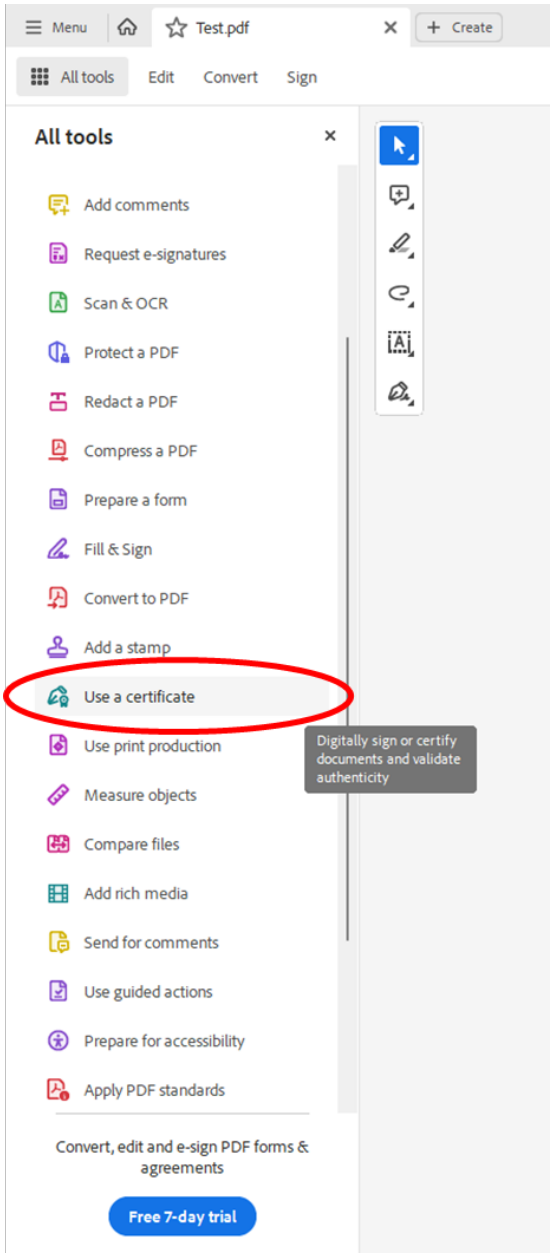


The group name will appear in Entrust Certificate Explorer.

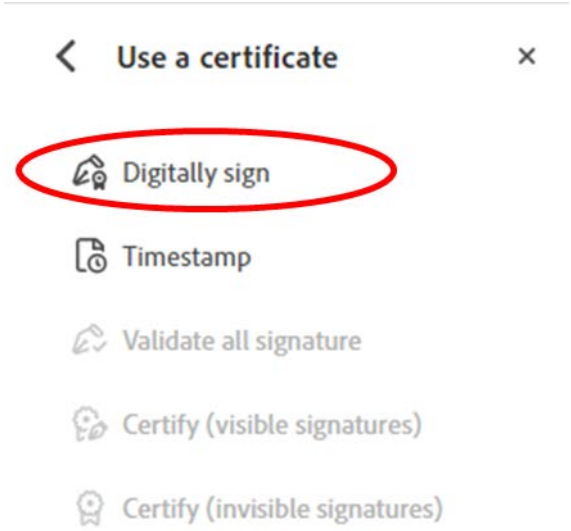
6. How To Sign Documents Digitally with Adobe

1. Prepare a document file
2. Print & save as PDF format
3. Insert token
4. Open file now as .pdf
5. Click " View more " then " Use a certificate " under All tools

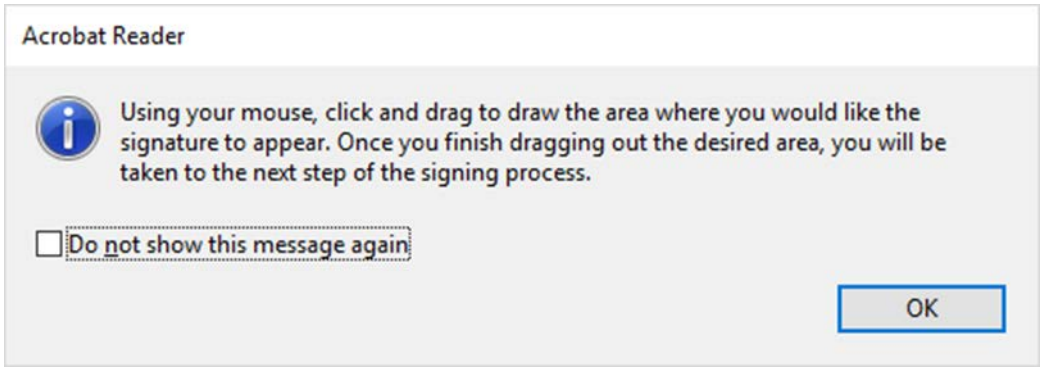




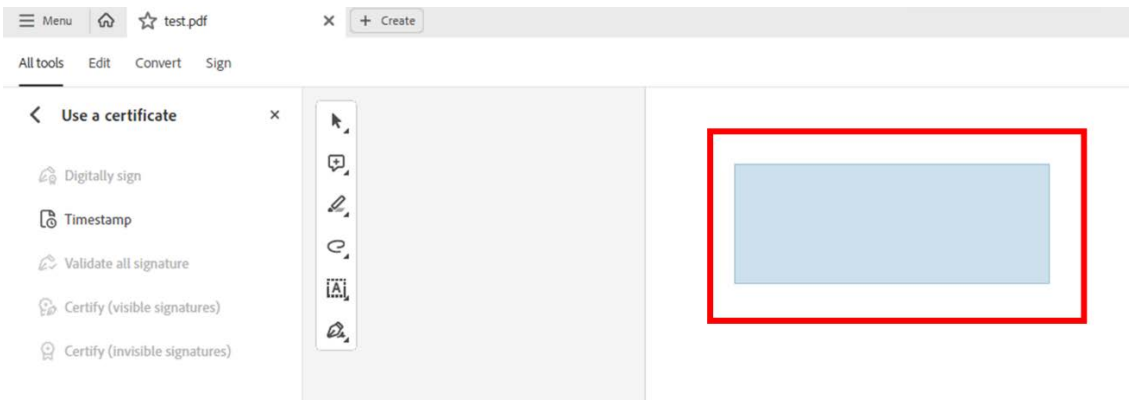
6. Click " Digitally Sign "



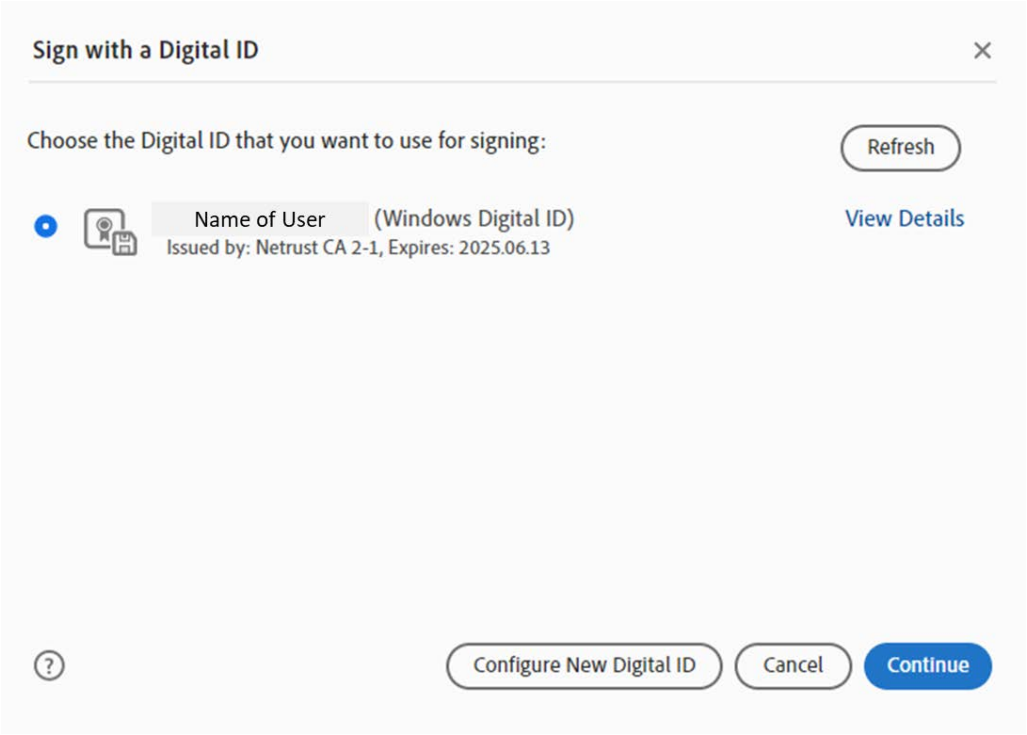
7. Click " OK "



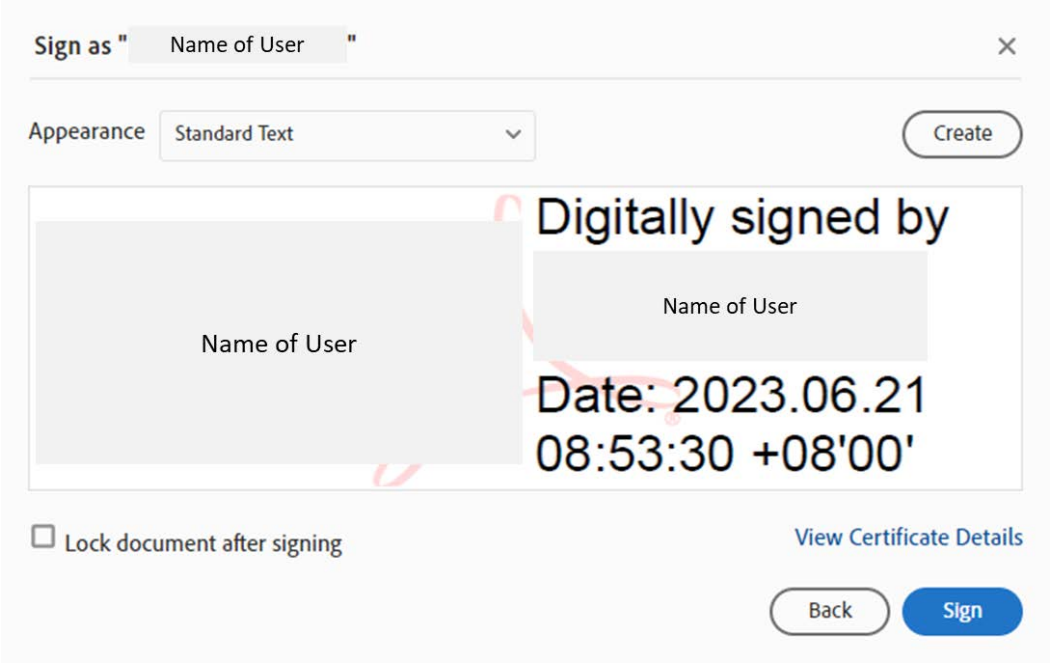
8. Drag & draw at any area that you want to digitally sign



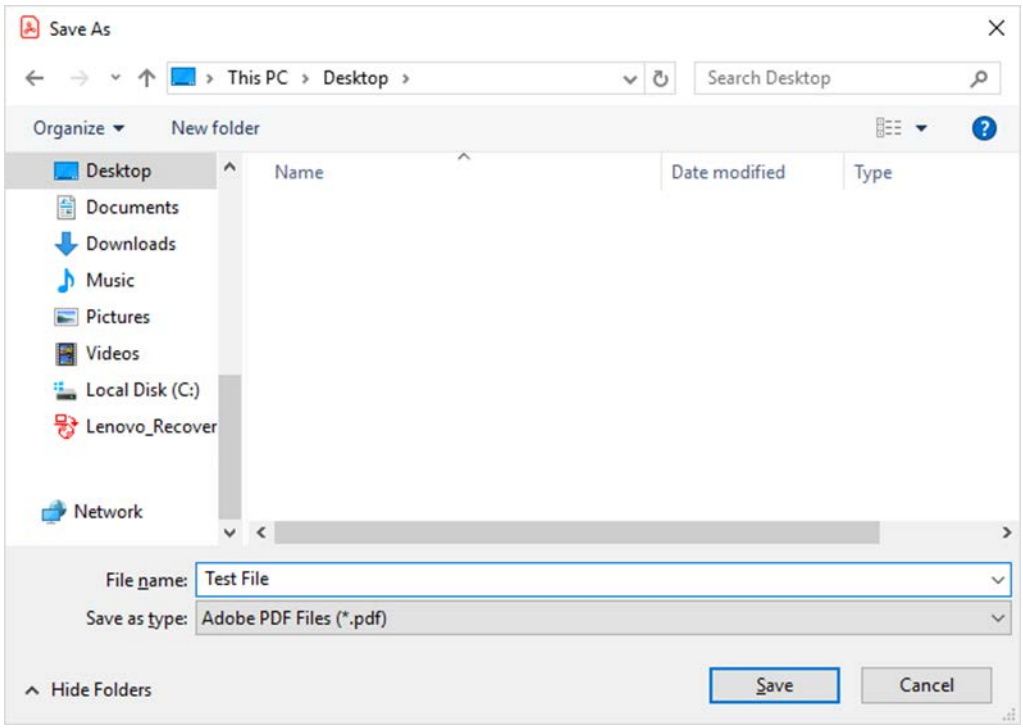
9. Choose the Digital ID (certificate from token) that you want to use for signing



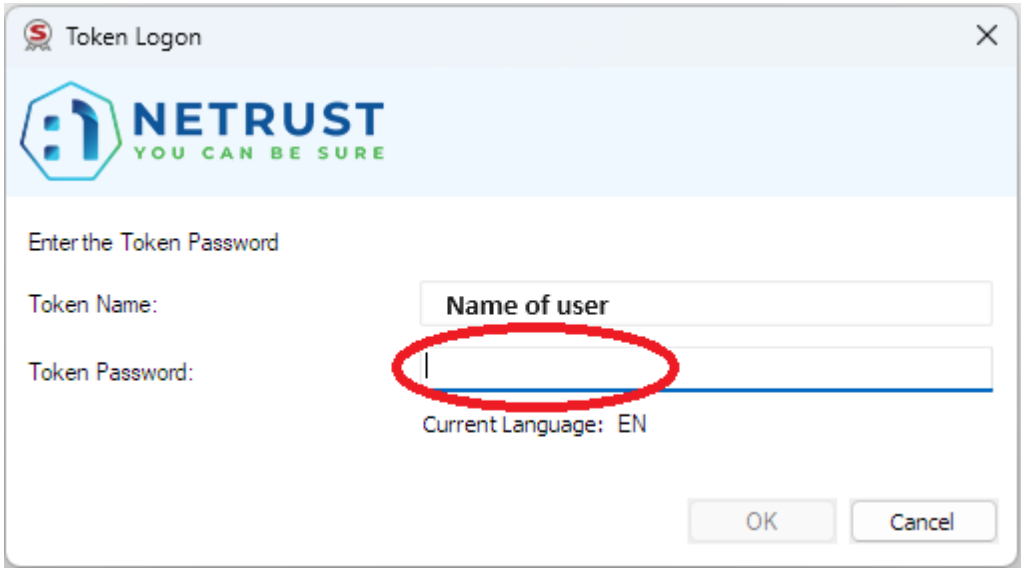
10. Click " Continue " and your certificate will be prompted to be confirmed
11. Click " Sign "



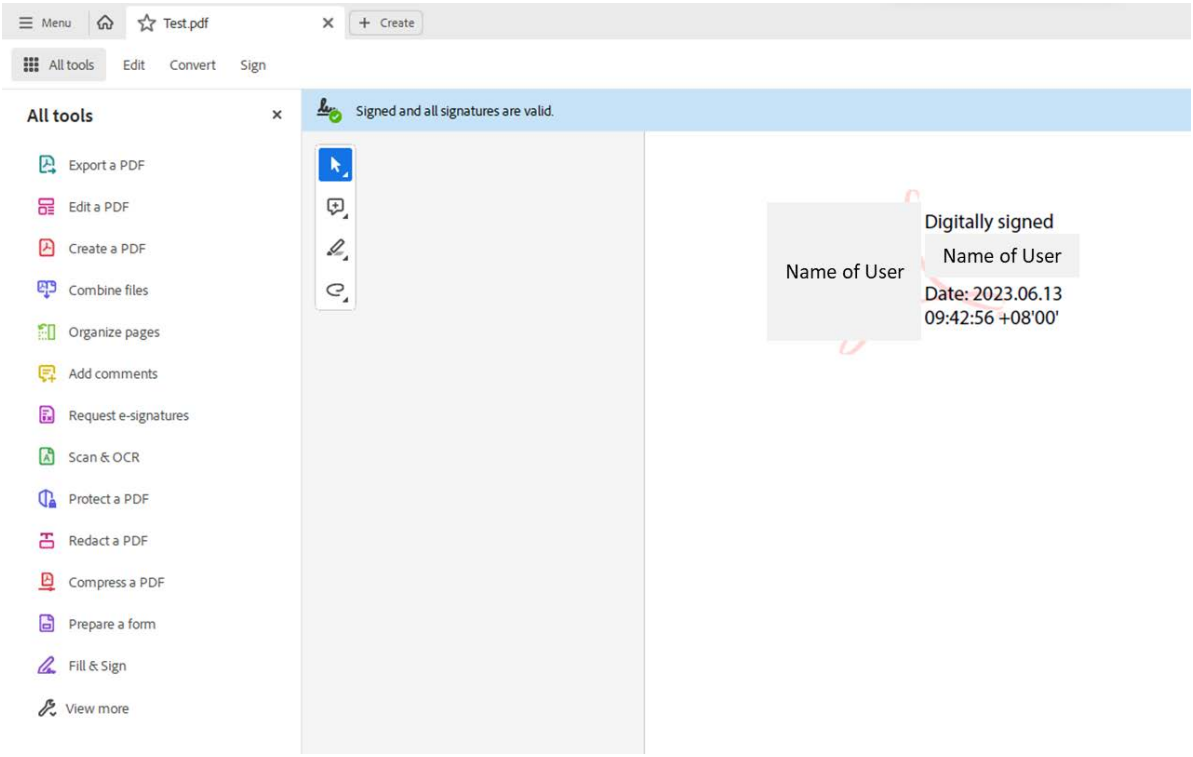
12. A pop up window will open to save the digitally signed PDF file, select the destination to save the file and click save



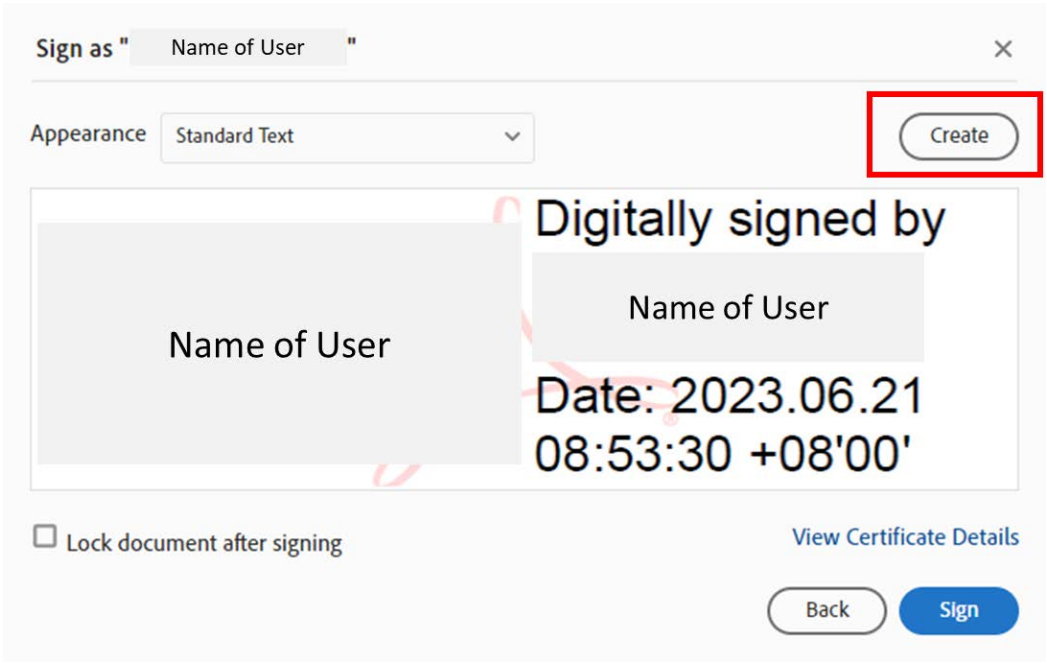
13. Enter your token password to digitally sign



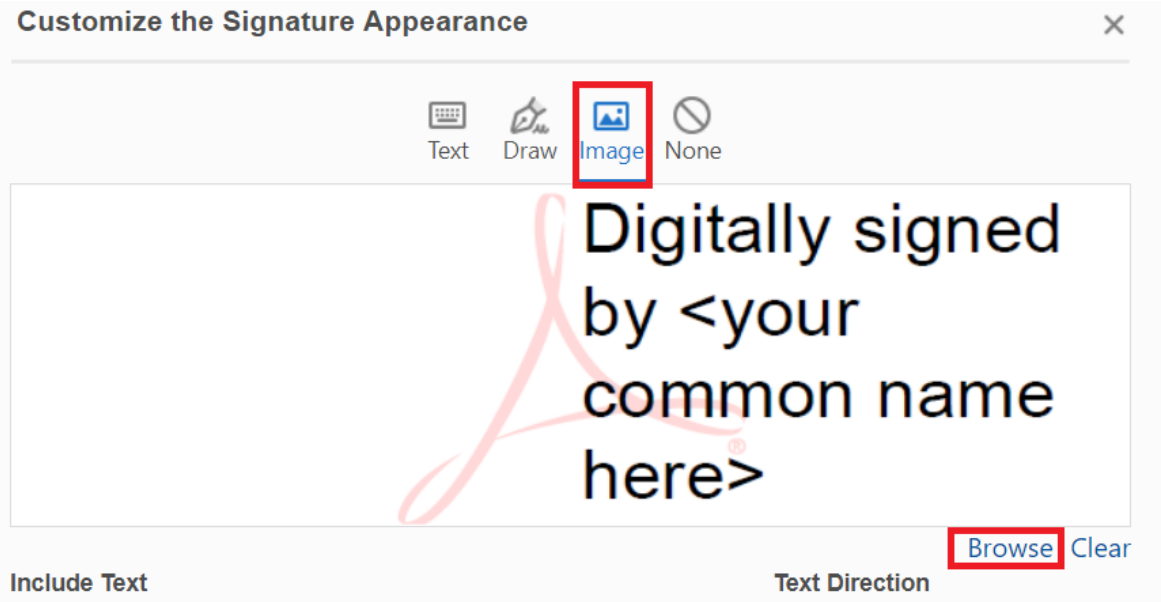
14. Your digital signature will be reflected in the PDF document after it is being sign successfully.



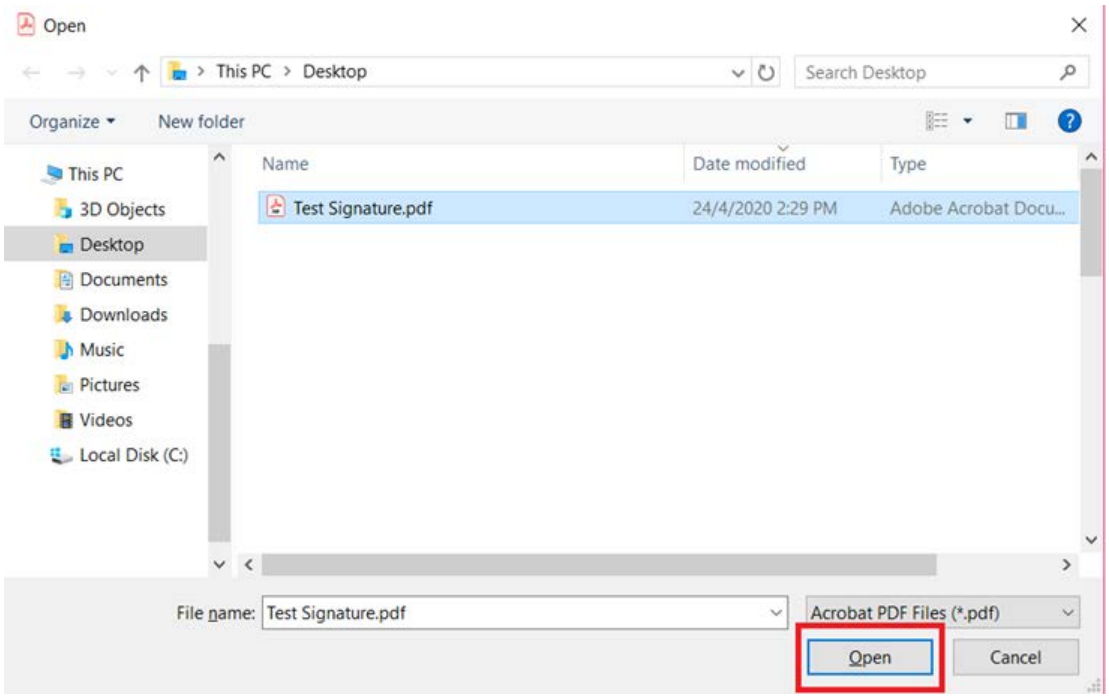
****<u>ALTERNATE STEP</u>: If you need an image of the digital signature you can create one**



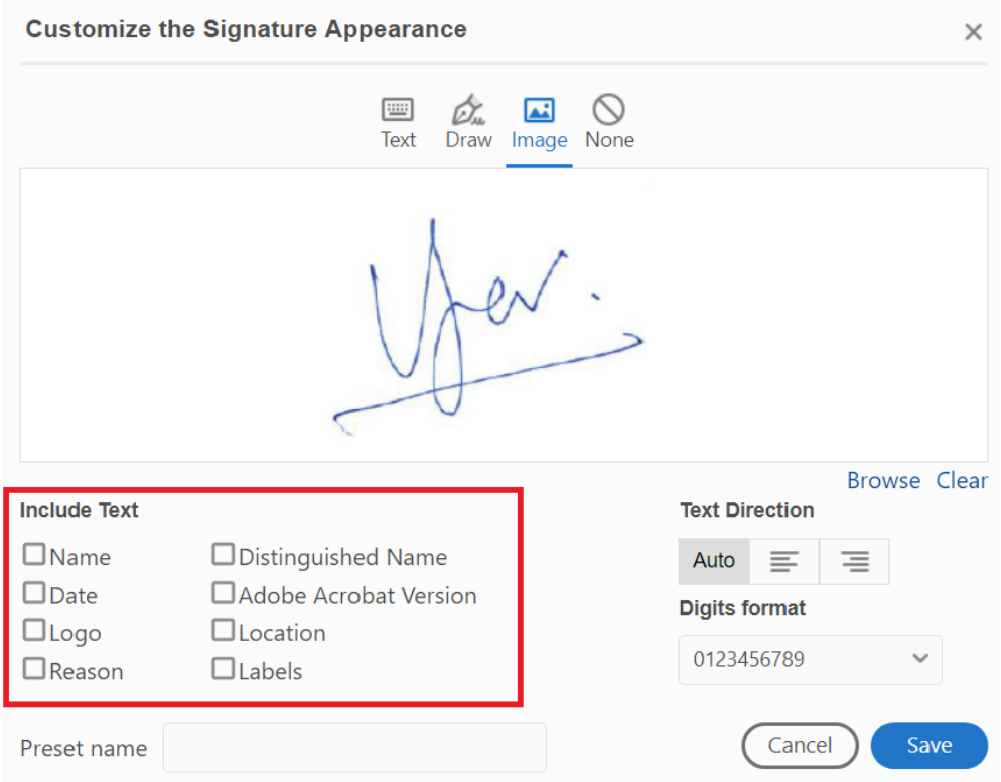
I. Select Image and click Browse



II. Select a scanned image of the signature



III. The image can be customized to the preference required and save



IV. The image will be available during signing

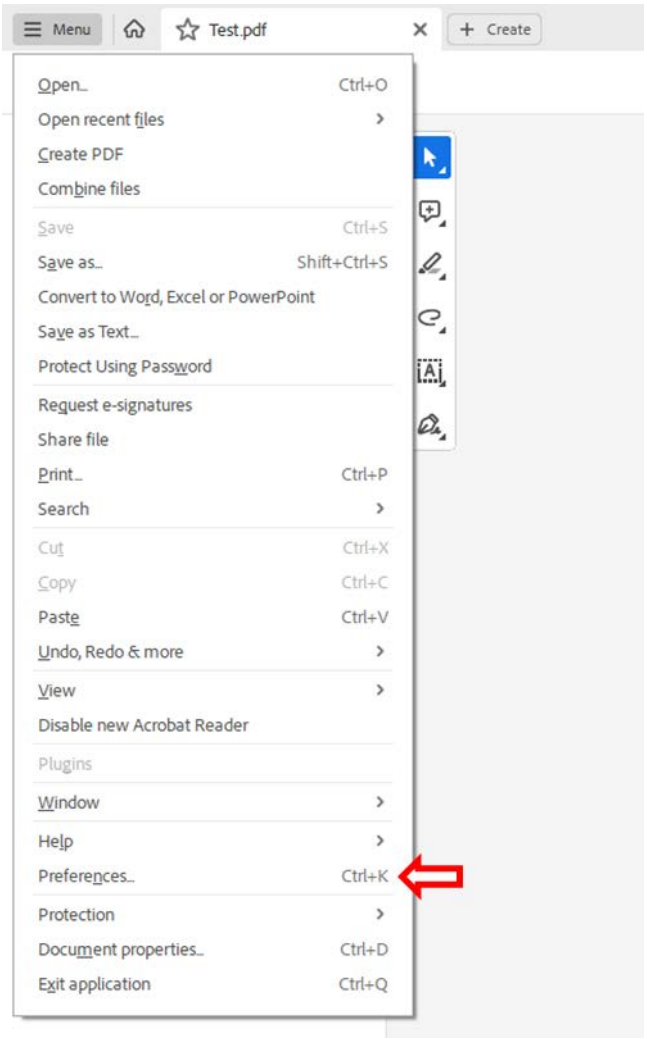
V. Signed with image

7. How To Ensure Digital Signature is Automatically Trusted (AATL)

These steps will be required if you are using an intranet PC or Adobe Acrobat Reader software that has not been updated.

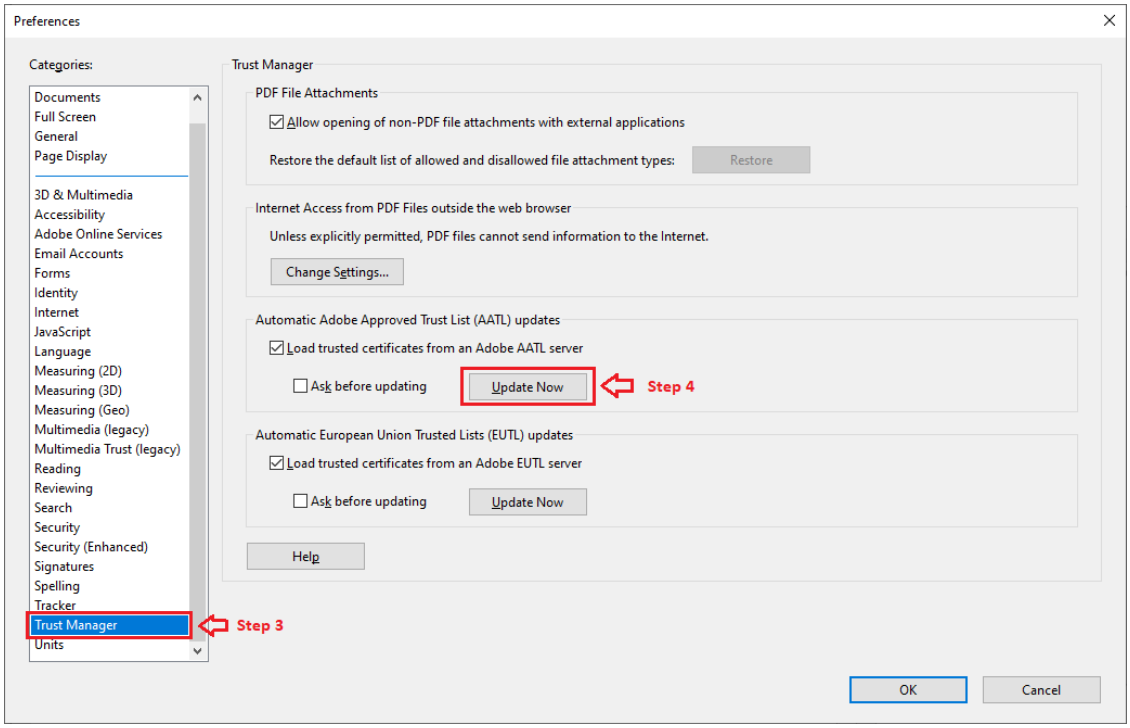
- **STEP 1**
  Open any PDF Document
  Click on the 'Menu' (at the top left)

- **STEP 2**
  Click on 'Preferences…'

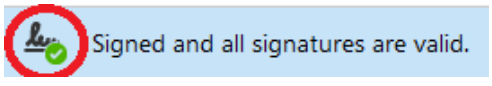


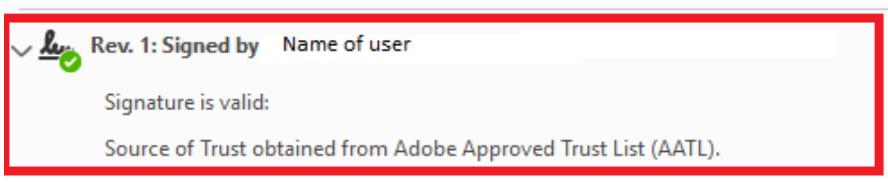
- **STEP 3**
  Select Trust Manager

- **STEP 4**
  Under Automatic Adobe Approved Trust List (AATL) updates, click 'Update Now'



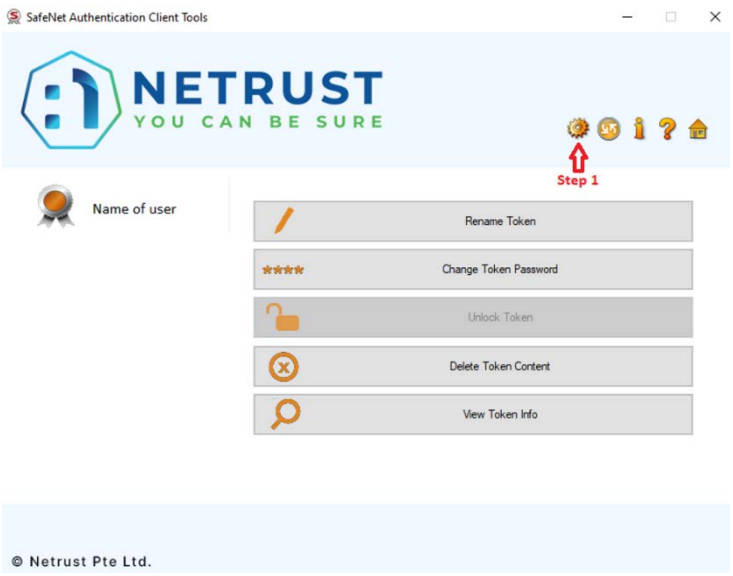
- **STEP 5**
  After updating the AATL updates, you'll notice that your digital signature is trusted automatically when you see the green tick (as per below)





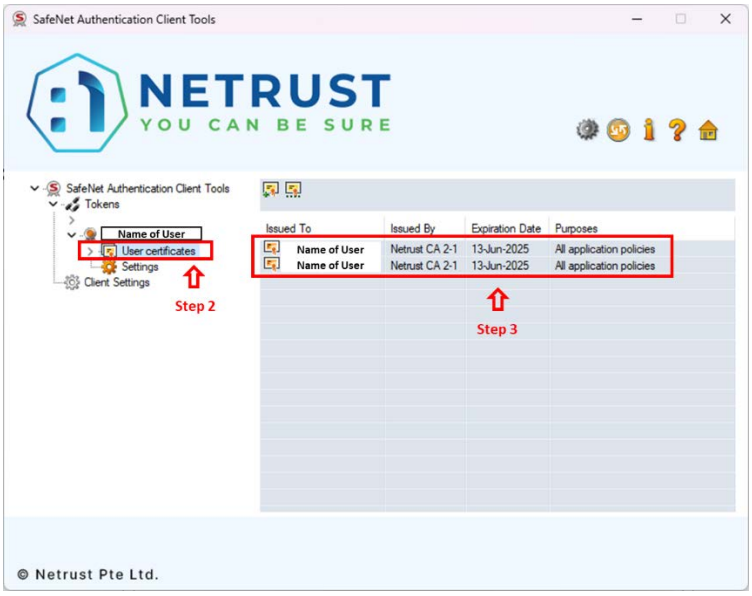
8. How To Check Certificate Details on eToken

- **STEP 1**
  Open SafeNet Authentication Client Tools
  Click on the Advanced View icon



- **STEP 2**
  Under the Token drop down list, select ‘User Certificates’

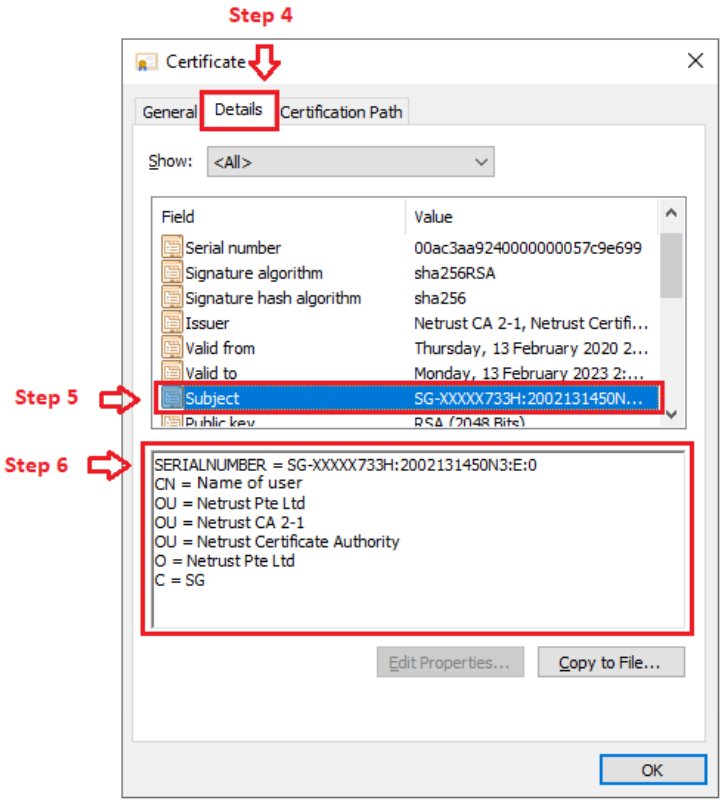
- **STEP 3**
  Double click on the certificate on the right hand side to view more information



- **STEP 4**
  Click on the ‘Details’ tab

- **STEP 5**
  Click on ‘Subject’

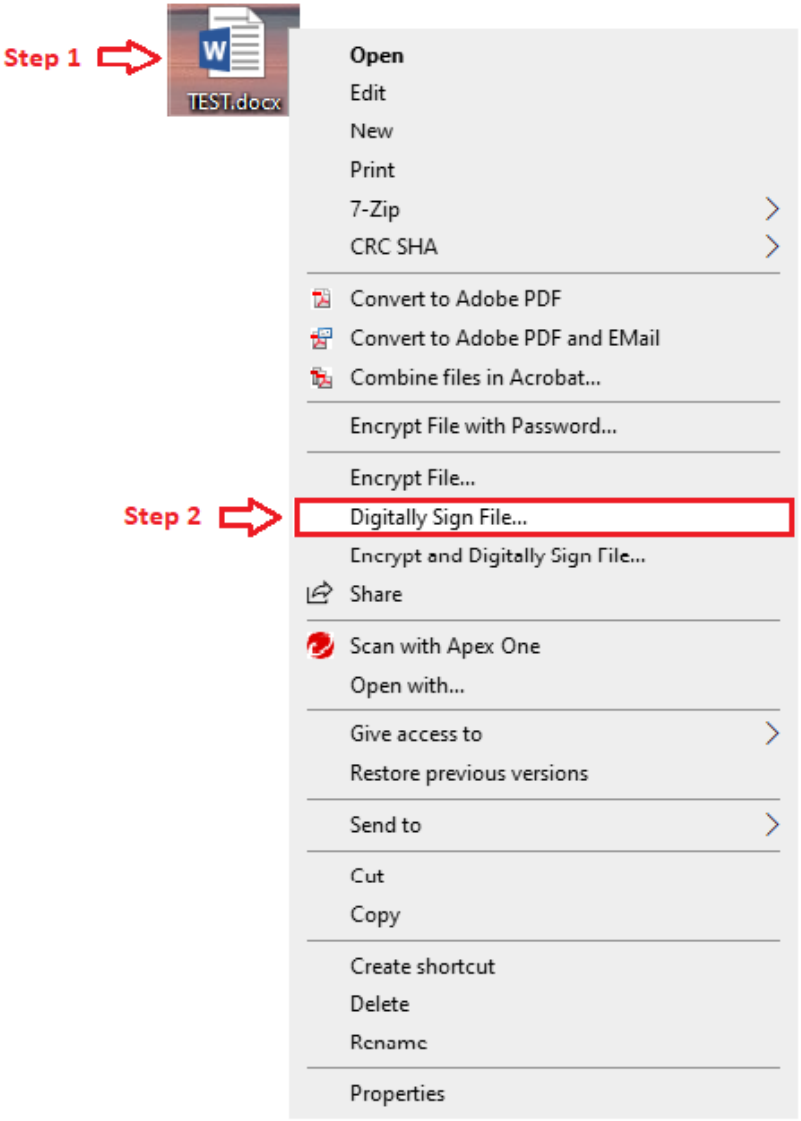
- **STEP 6**
  The certificate details will be shown in the box below



9. How To Digitally Sign/Encrypt Files Using Entrust Certificate Agent (ECA) using Microsoft Office Applications

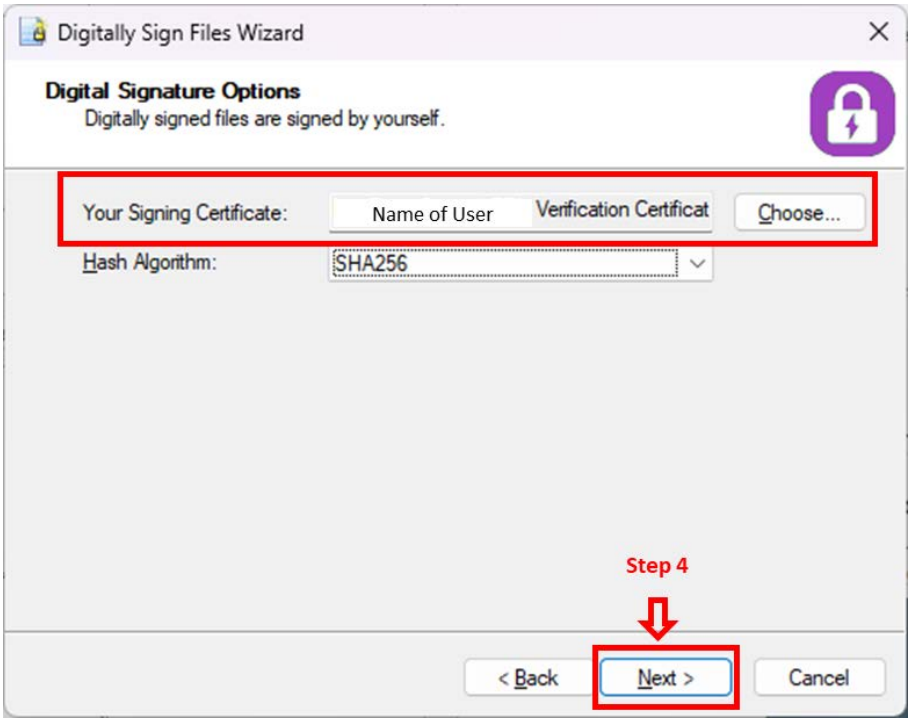
- **STEP 1**
  Select any Microsoft Word, Excel or PowerPoint file individually to sign digitally

- **STEP 2**
  Right click on the file and select 'Digitally Sign File…' to proceed next

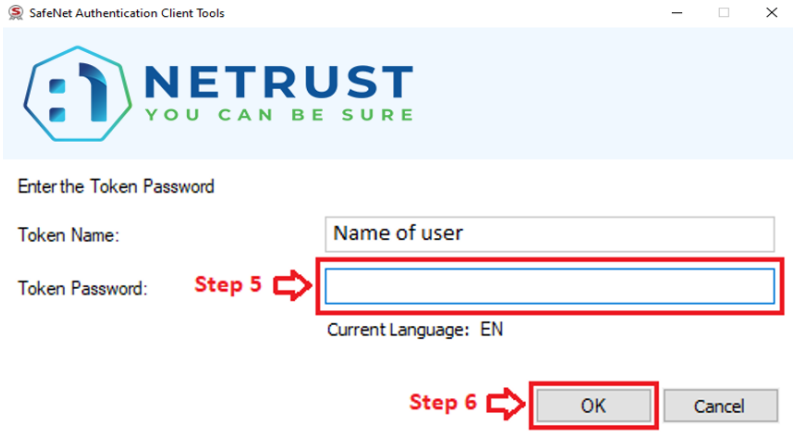


- **STEP 3**
  A pop up window will appear from 'Digitally Sign Files Wizard'
  Click on 'Next' to proceed

- **STEP 4**
  Check if the information is correct under 'Your Signing Certificate'
  Click on 'Next' to proceed



- **STEP 5**
  A pop up window will appear from ‘SafeNet Authentication Client Tools - Token Logon’
  Enter Token Password

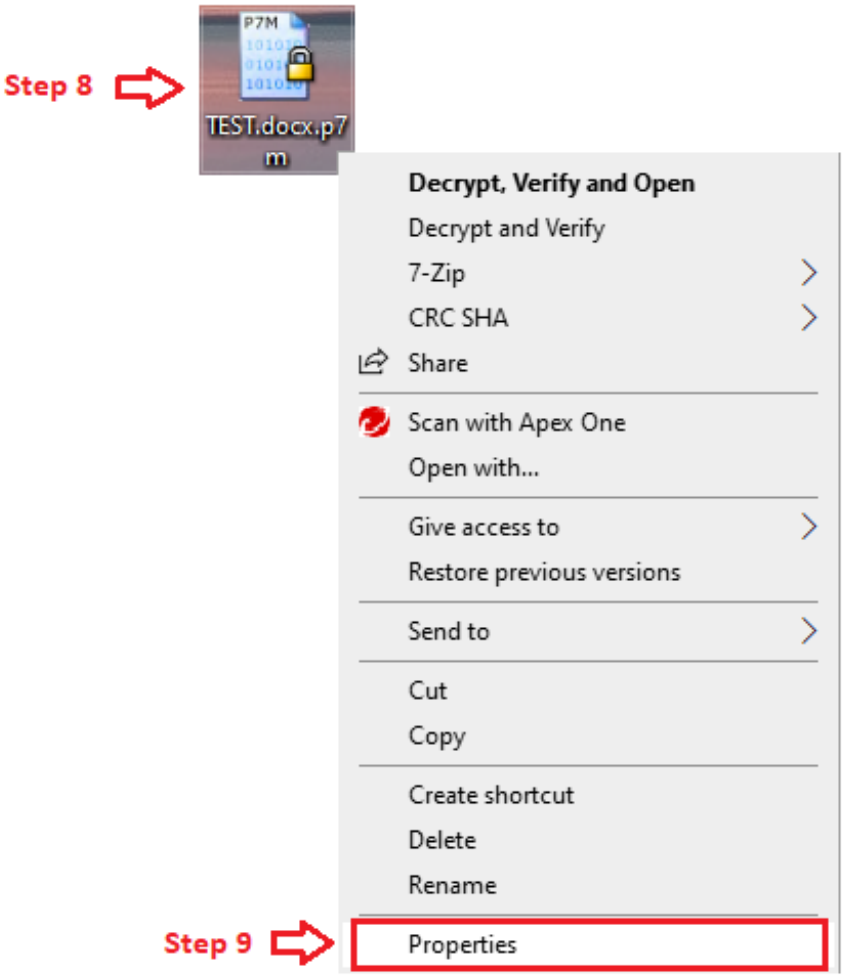


- **STEP 6**
  Click ‘OK’ to proceed

- **STEP 7**
  Document is digitally signed successfully after receiving the following message from the pop up window
  Click on ‘Finish’ to proceed

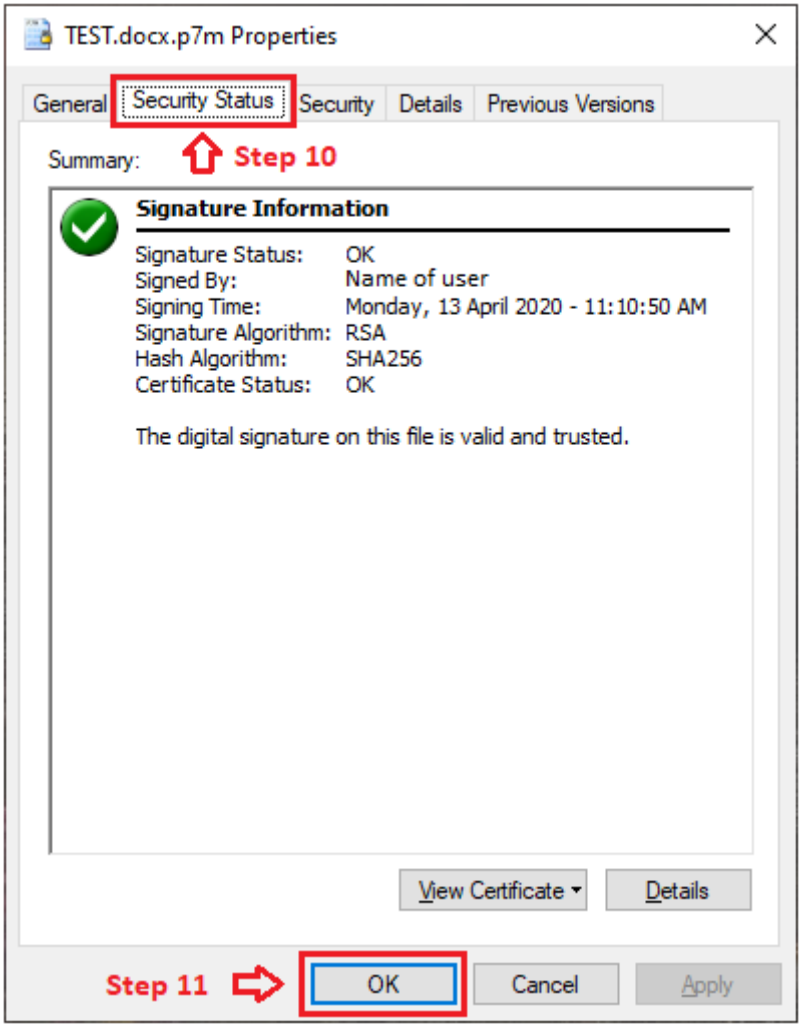
- **STEP 8**
  The digitally signed file will be saved automatically in the file location as a .p7m file extension
  NOTE: ECA will be required to view the file

- **STEP 9**
  Right click on the file and select 'Properties' to check on signature information



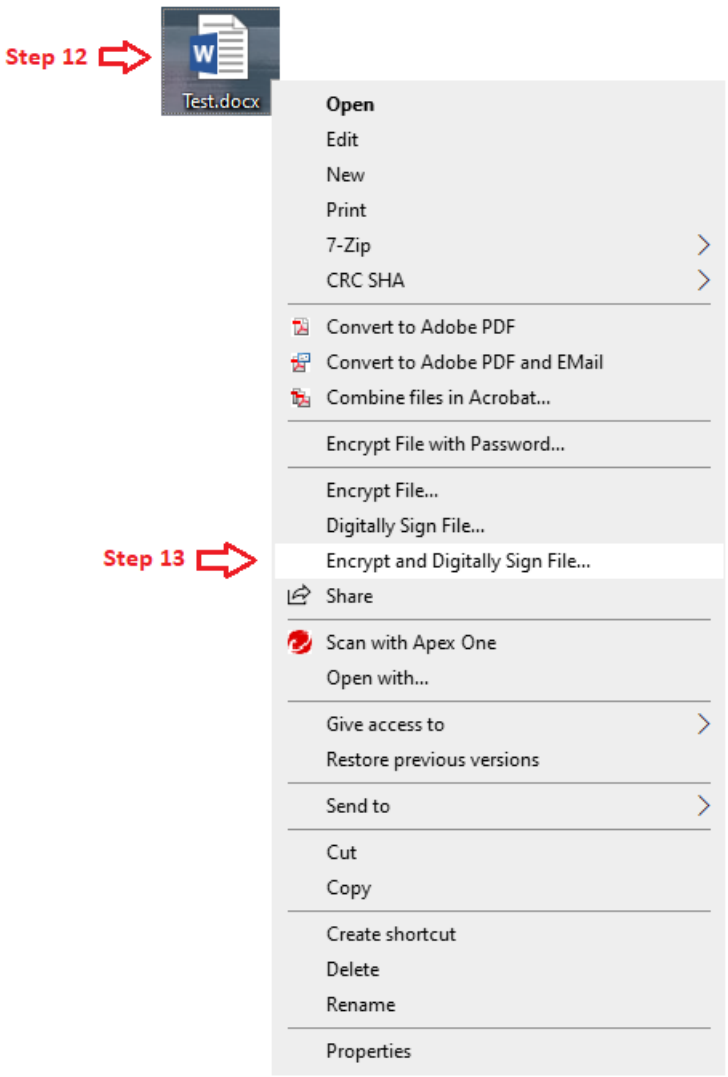
- **STEP 10**
  A pop up window will appear, click on ‘Security Status tab’
  A summary of the signature information will be shown in the box below

- **STEP 11**
  Click ‘OK’ to proceed



- **STEP 12 – How to Encrypt and Digitally Sign a file**

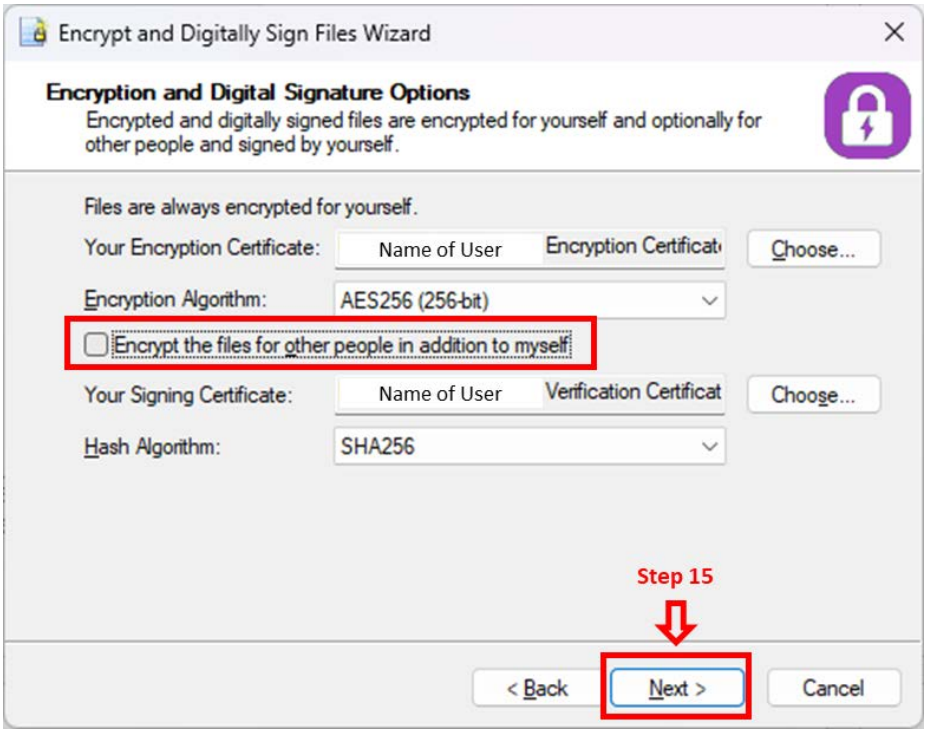
- **STEP 13**
  Right click on the file and select ‘Encrypt and Digitally Sign’ to proceed next



- **STEP 14**
  A pop up window will appear from 'Encrypt and Digitally Sign Files Wizard'
  Click on 'Next' to proceed

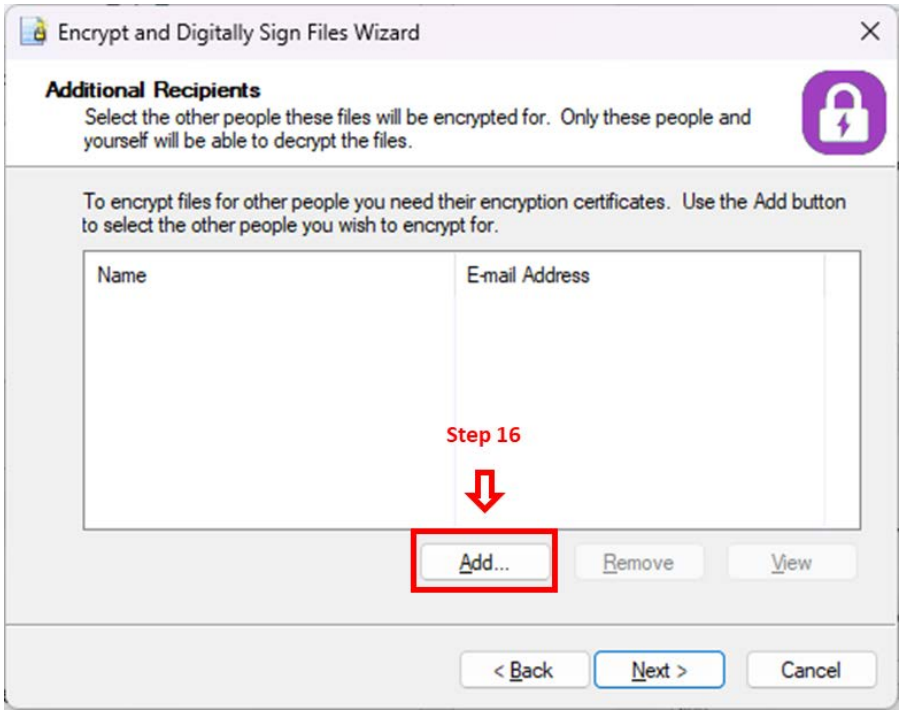
- **STEP 15**

  Check if the information is correct under 'Your Encryption & Signing Certificate'
  Click on 'Encrypt the files for other people in addition to myself' and click 'Next' to proceed



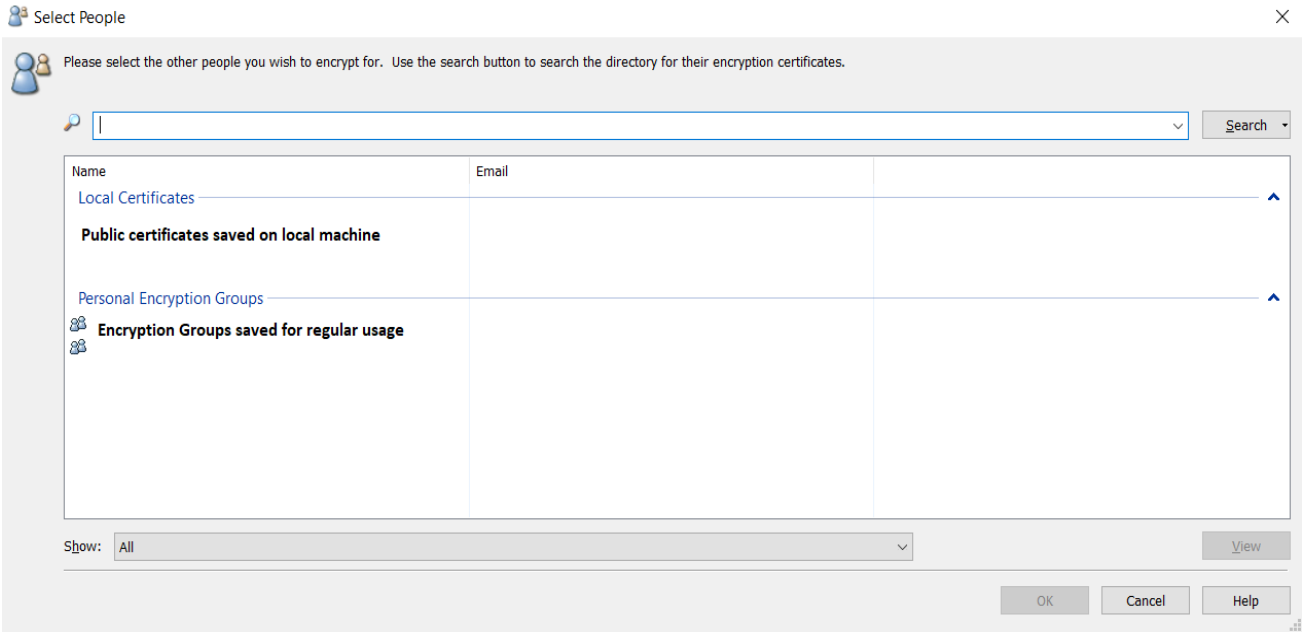
- **STEP 16**

  Click ‘Add’ to search for the recipients in the Netrust LDAP directory or you can add user public certificates which have been saved in your machine

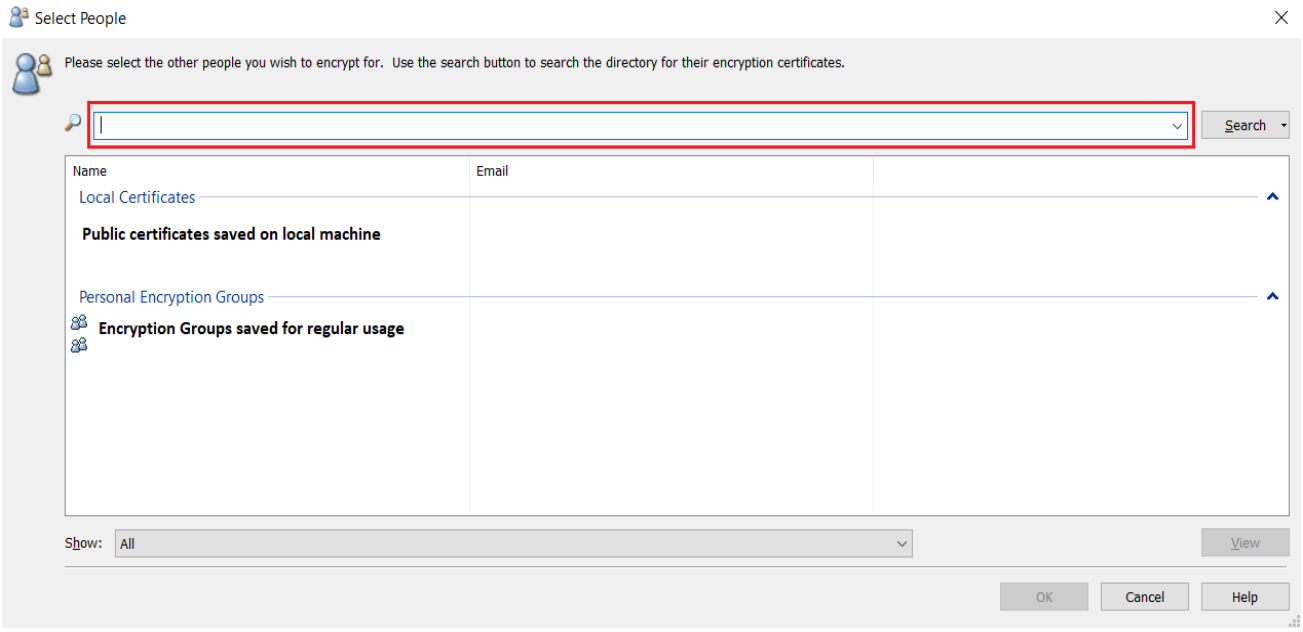


- **STEP 17**

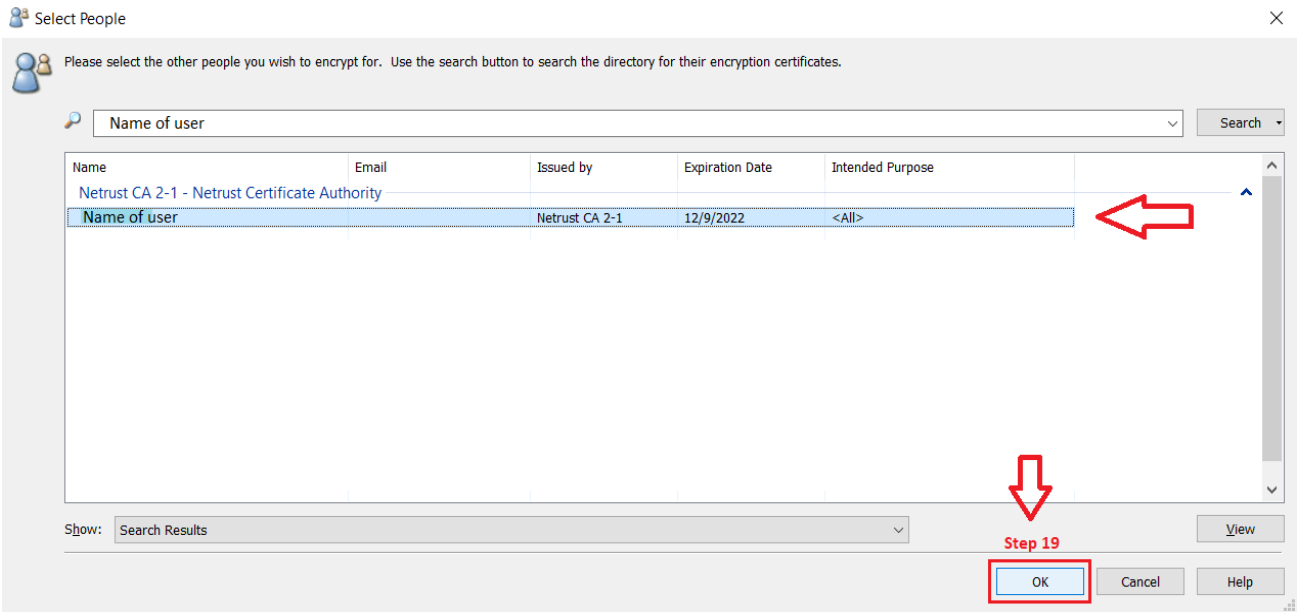
  You can view the certificates from local certificate store or personal encryption groups which can be saved from the ‘ECA certificate explorer



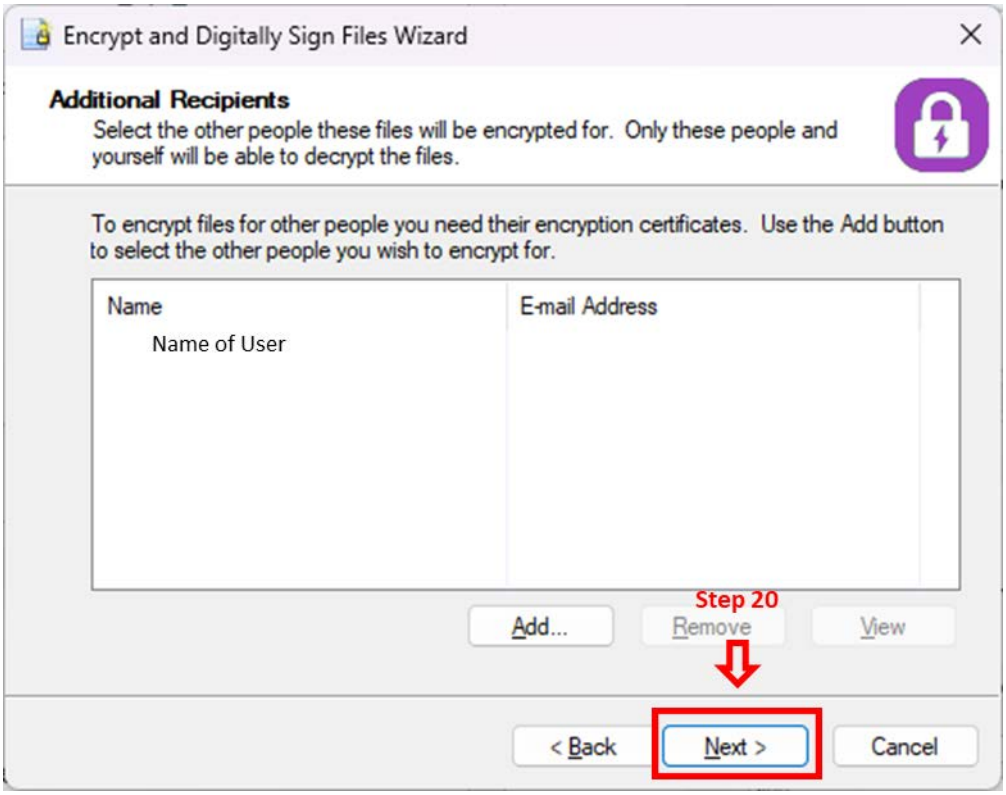
- **STEP 18**
  Click on ‘search’ after typing in name/email of user to encrypt file to



- **STEP 19**
  Select name of user searched and click ok

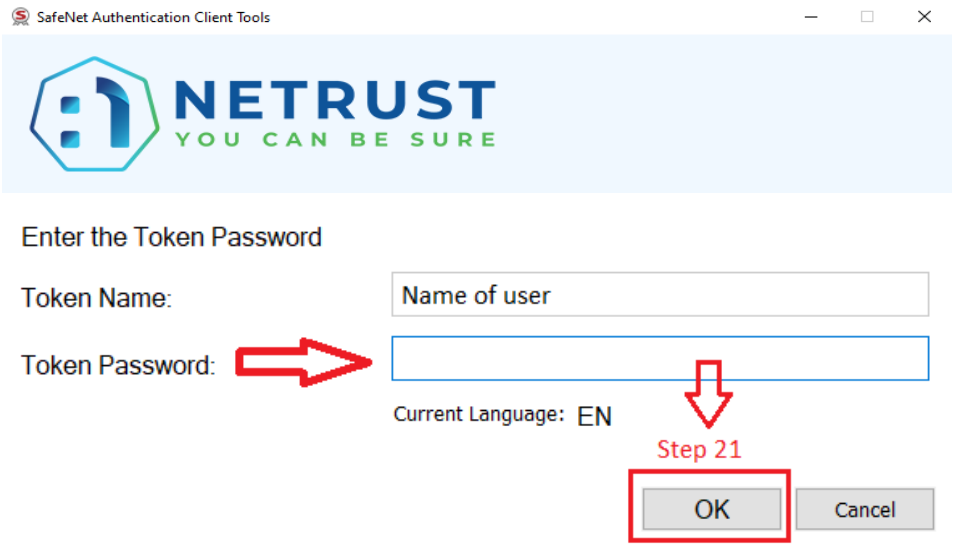


- **STEP 20**
  Click 'Next' and you will be prompted to key in token password

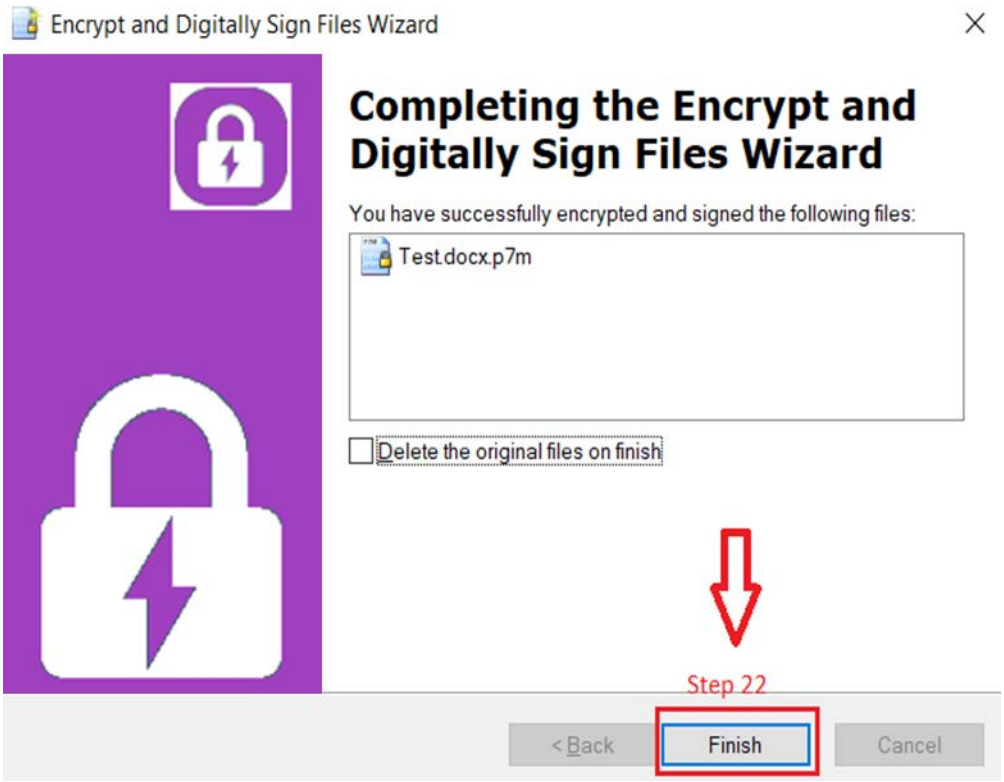


- **STEP 21**

  Click OK

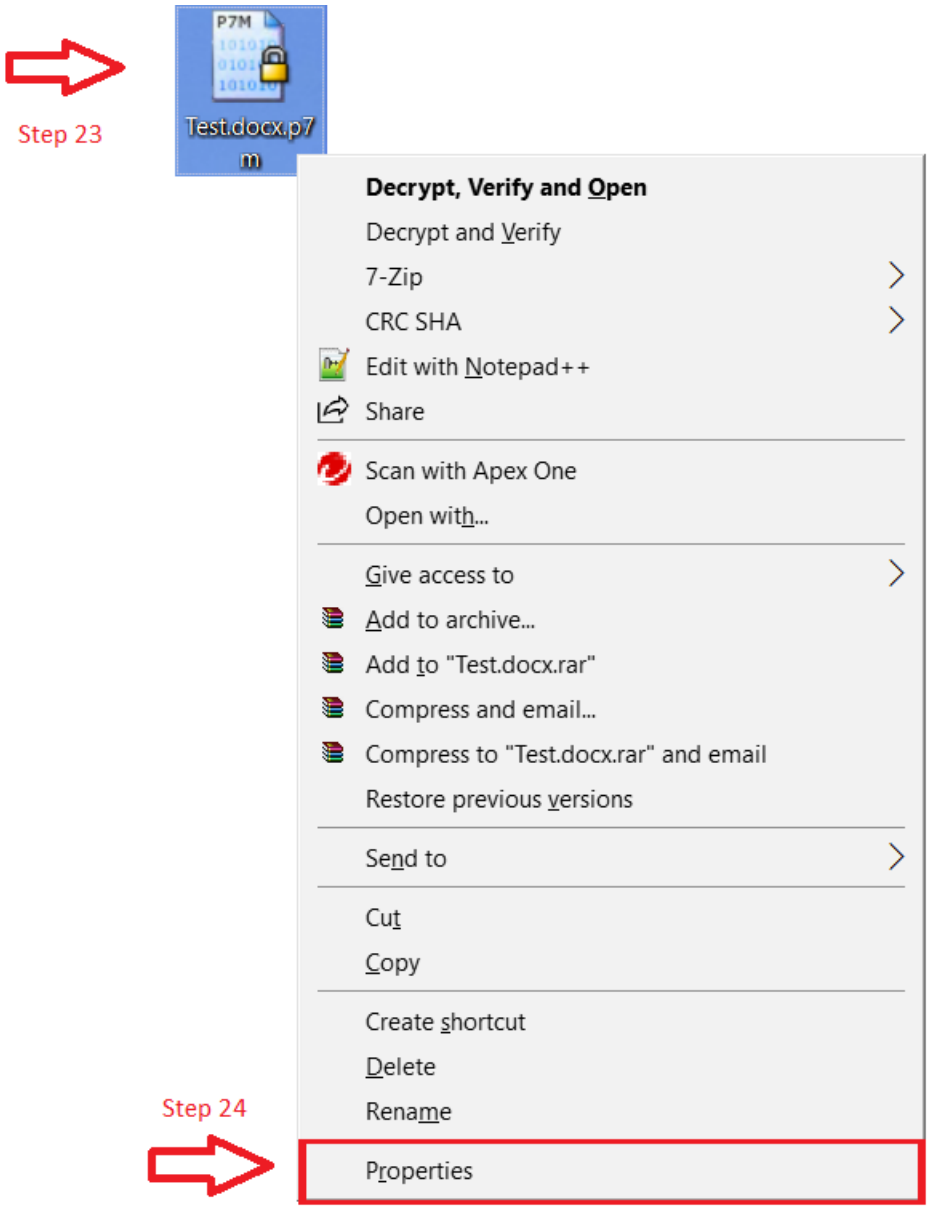


- **STEP 22**
  Click ‘Finish’ to complete encryption



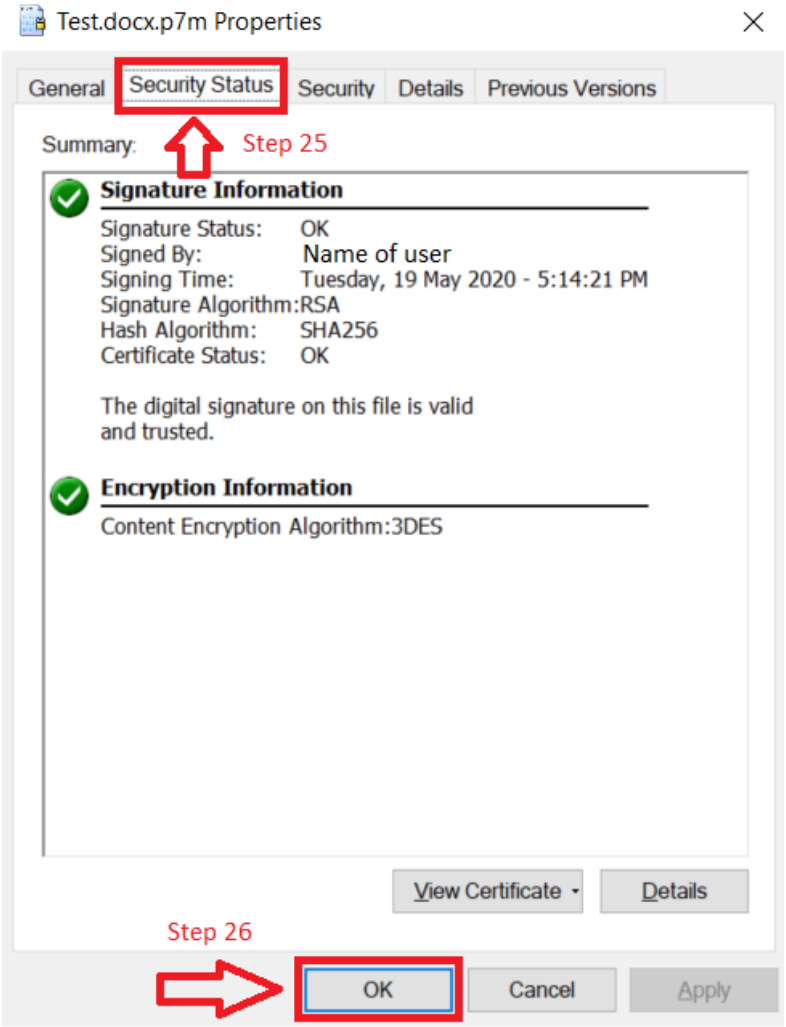
- **STEP 23**
  The encrypted and digitally signed file will be saved automatically in the same file location as .p7m extension
  NOTE: ECA will be required to view the file

- **STEP 24**
  Right click on the file and select 'Properties' to check on signature information



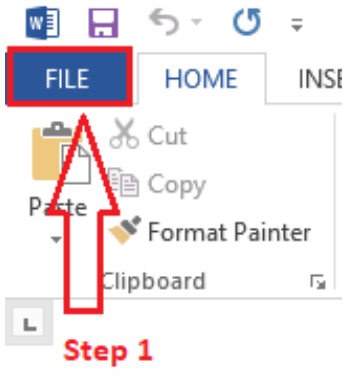
- **STEP 25**
  A pop up window will appear, click on 'Security Status tab'
  A summary of the signature information will be shown in the box below

- **STEP 26**
  Click 'OK' to proceed



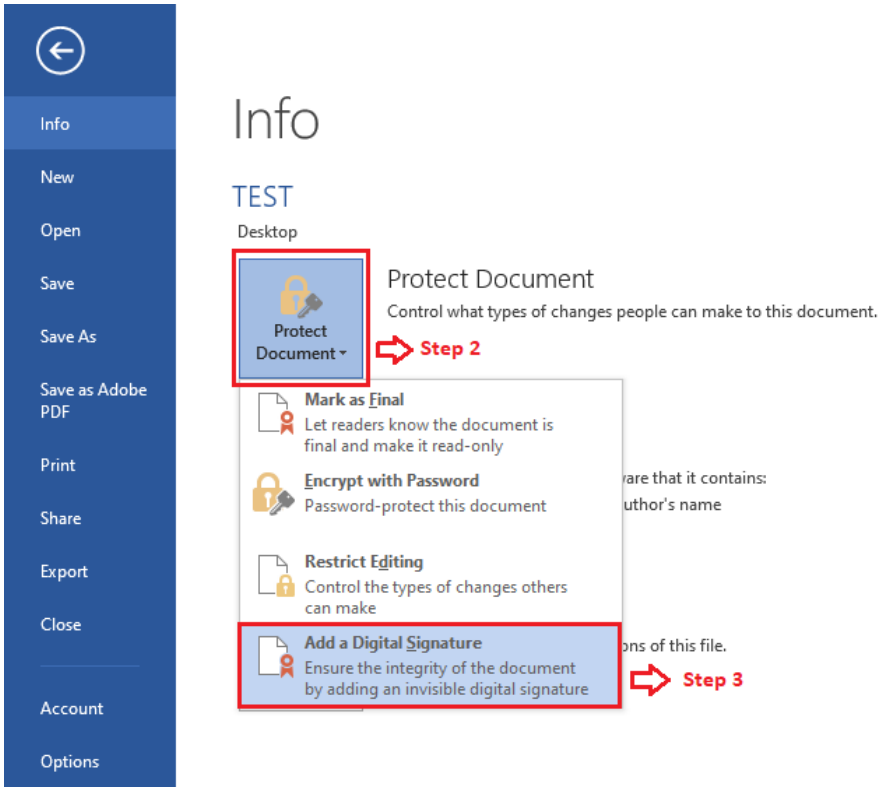
10. How To Digitally Sign using Microsoft Office Word

- **STEP 1**
  Open up a document that you wish to digitally sign directly on it
  Click on 'File'

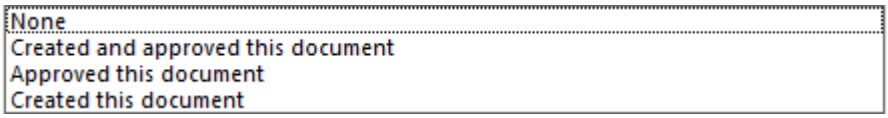


- **STEP 2**
  Under Info, click on 'Protect Document'

- **STEP 3**
  Select 'Add a Digital Signature'

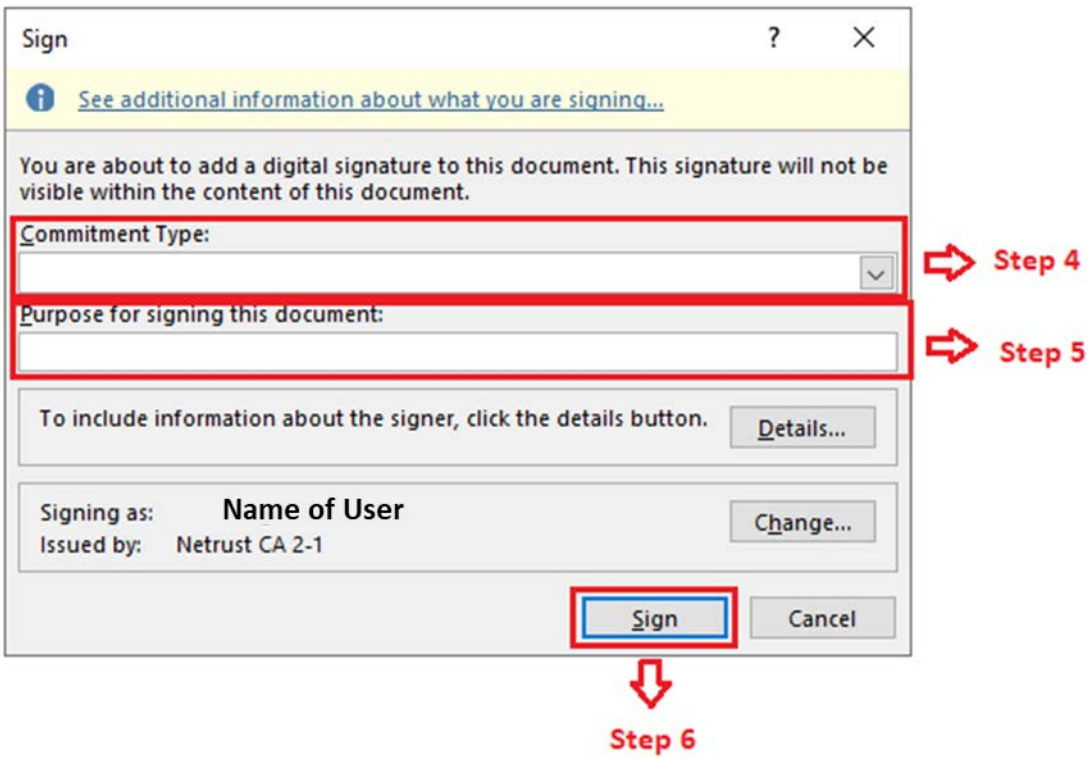


- **STEP 4**
  Select a Commitment Type from the drop down list

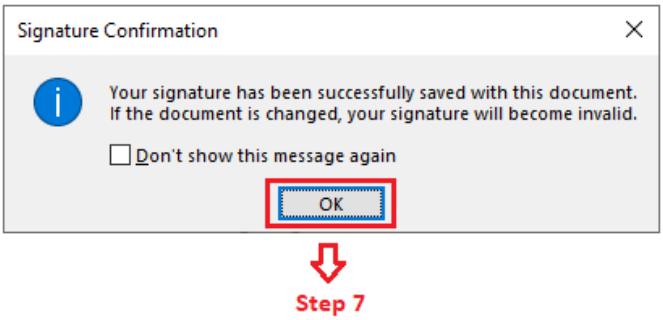


- **STEP 5**
  Enter a content under 'Purpose for signing this document'

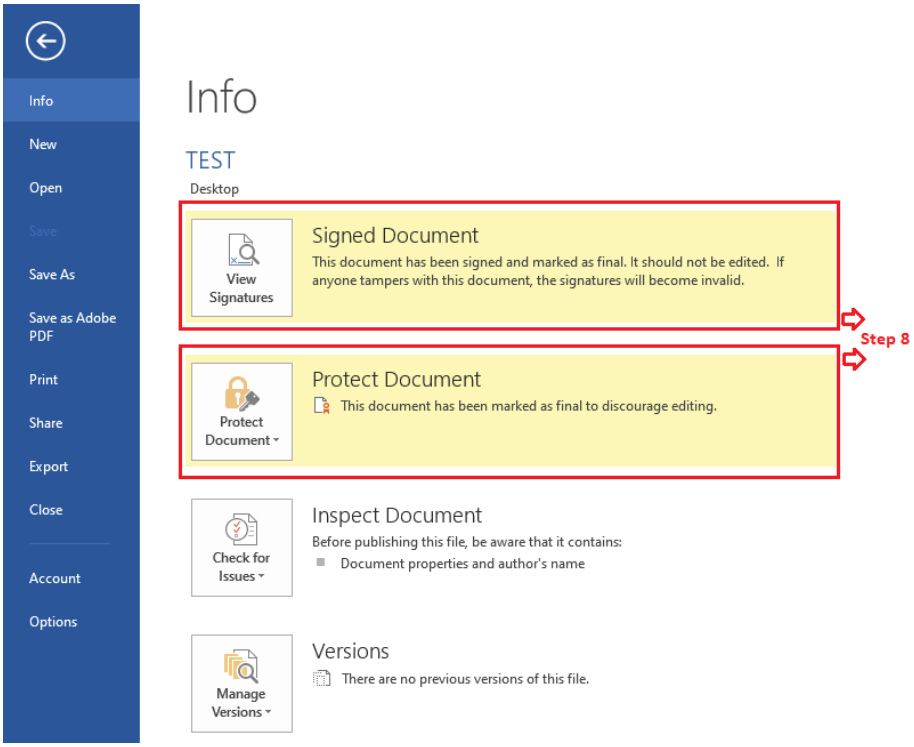
- **STEP 6**
  Click on 'Sign' to proceed



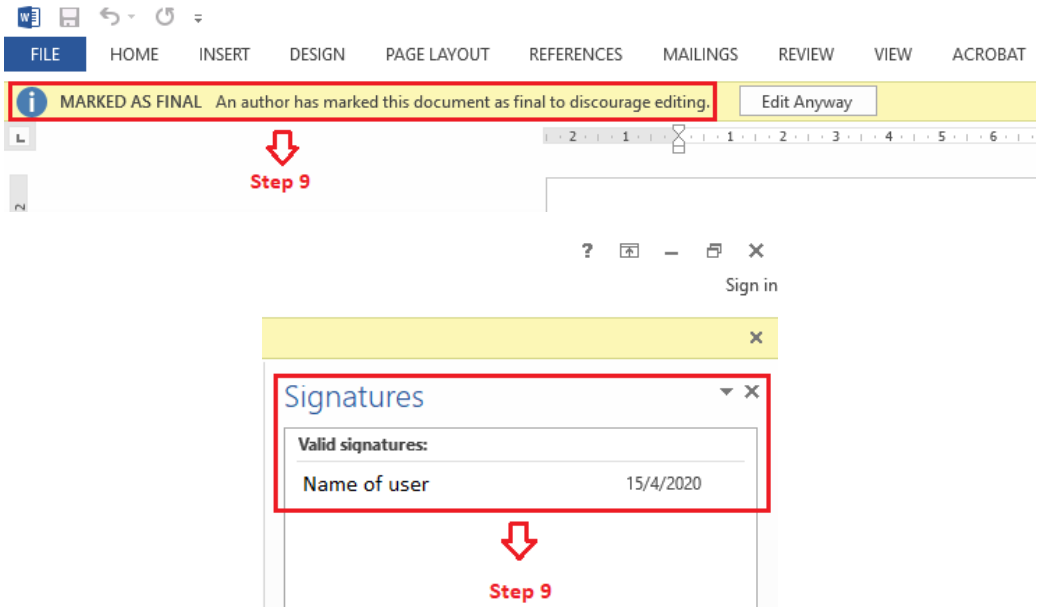
- **STEP 7**
  Click on 'OK' to proceed



- **STEP 8**
  After digitally signing successfully, you will notice that the document is signed and protected

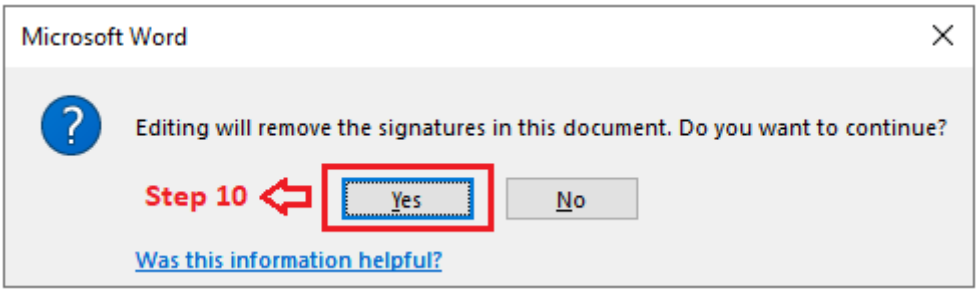


- **STEP 9**
  Within the document, you will see the following information reflected after it is sign successfully



- **STEP 10**
  You may still edit the document after it is being signed on it
  Click 'Yes' to proceed next

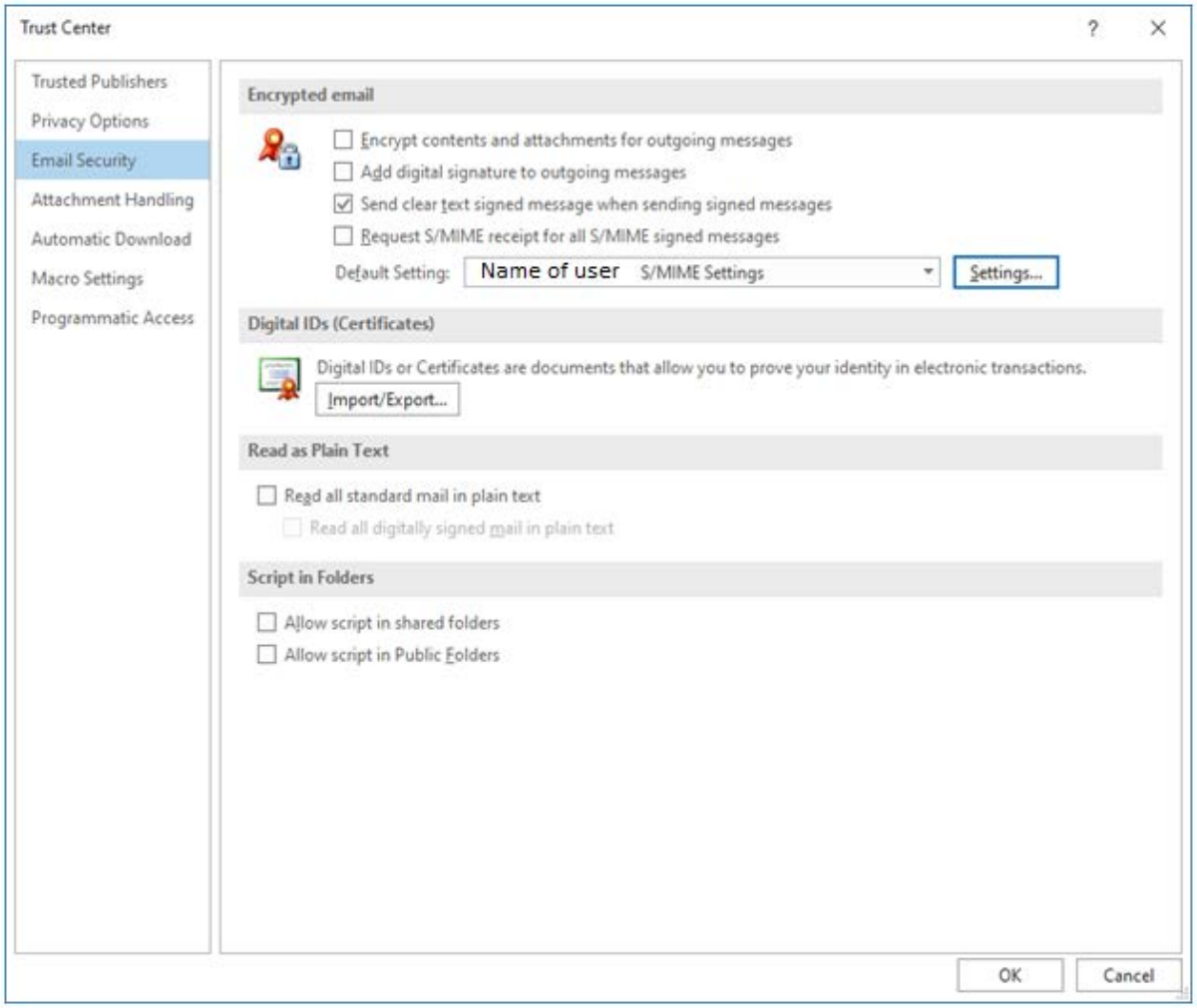
  NOTE: The signature will be removed if there amendments on the signed document. You will need to sign on the document again after you have edited it.



11. Configuration of Secure Email on Microsoft Outlook

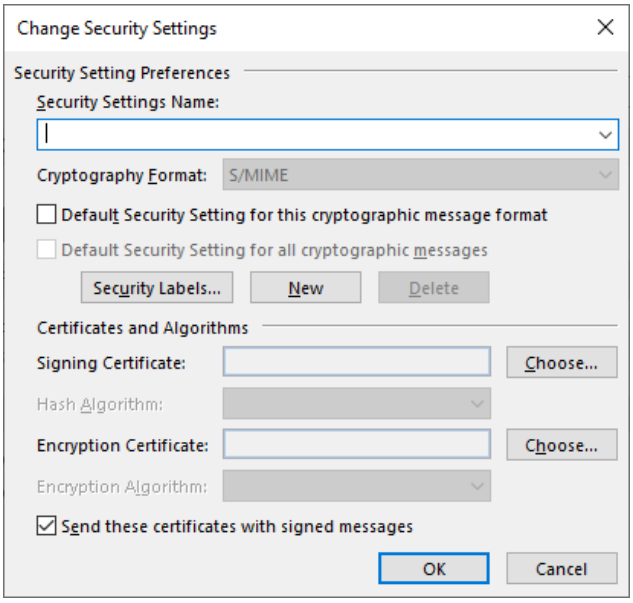
- **STEP 1**
  Upon installation of the certificate to configure the Outlook, refer to the STEPs below:

  - Click "Files" on the Outlook menu bar
  - Click “Options”
  - Click “Trust Center”
  - Click “Email Security”



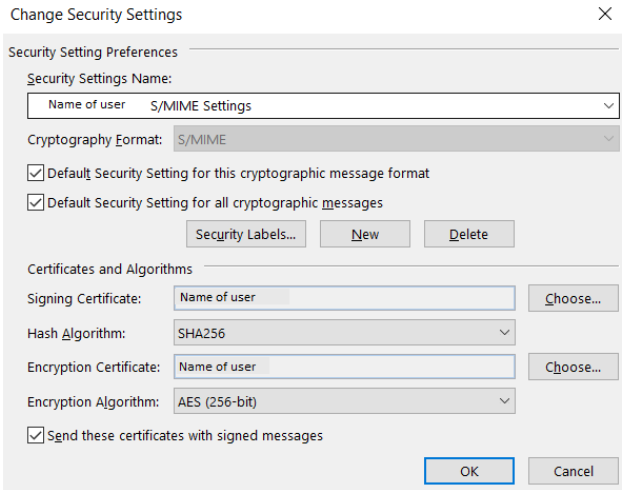
- **STEP 2**

To define the security settings, specify which certificate will be required. Click on "Settings..." button as shown below:



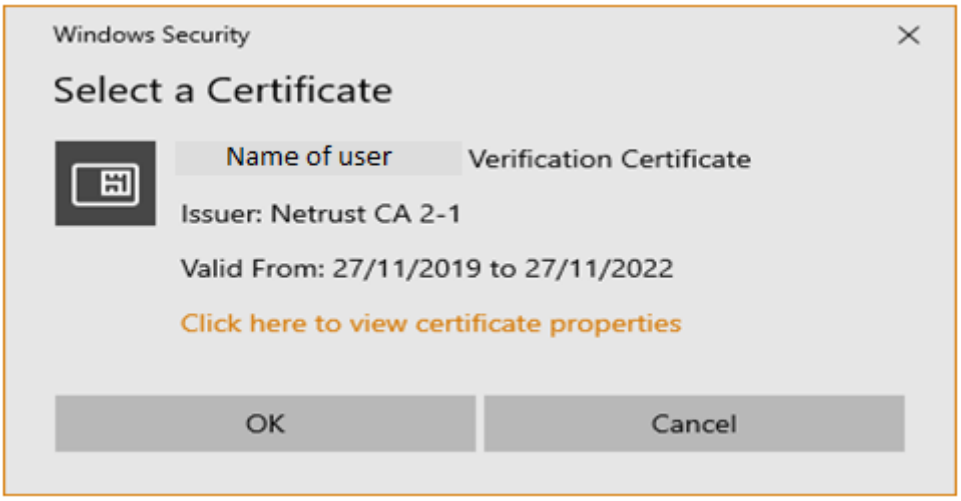
The security settings can be categorized under each required individual and named accordingly:

- Secure Message Format (type of e-mail)
- Digital Signature Settings
- Encryption Settings
- Security Setting Preferences (setting defaults)



- Hash Algorithm should be "**SHA256**"
- Encryption Algorithm should be "**AES (256-bit)"**

- **STEP 3**
  Then proceed to choose the Signing Certificate and Encryption Certificate

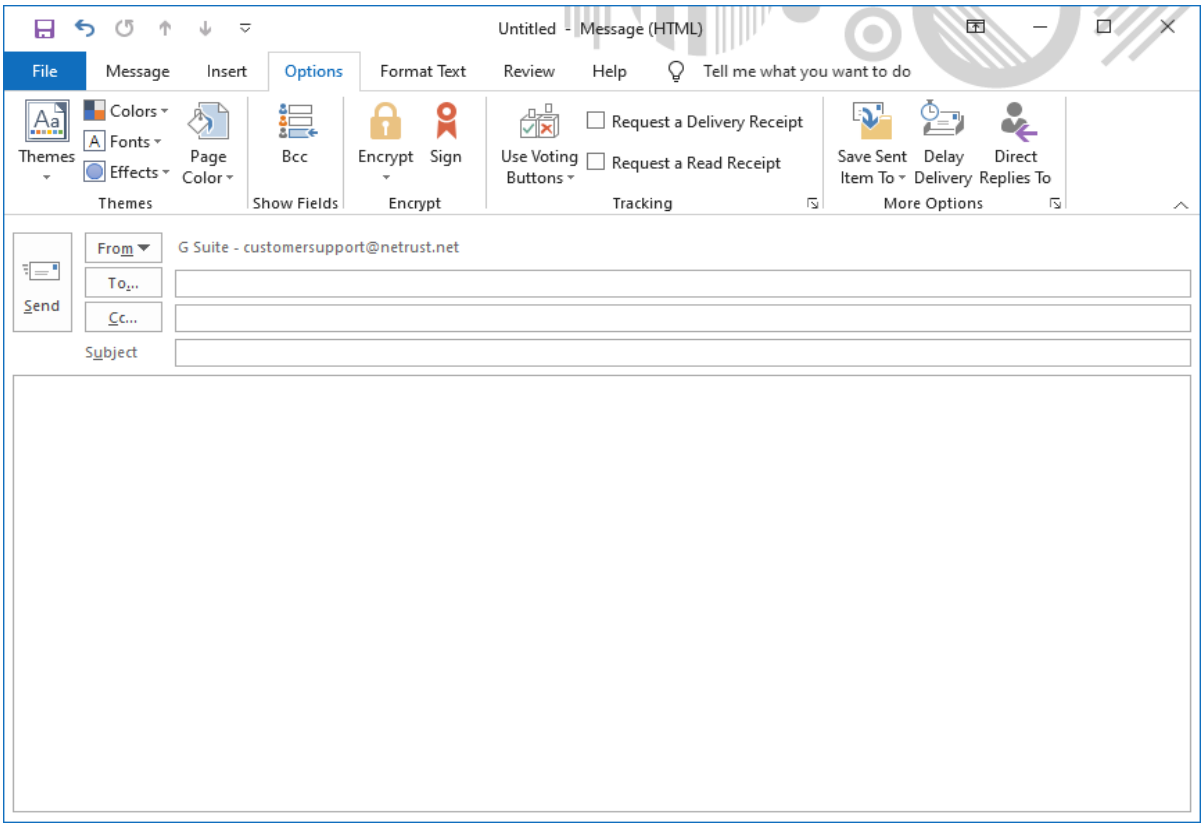


- **STEP 4**
  Digitally signing your e-mail messages with Microsoft Outlook

  The first STEP to secure the e-mail messages is to sign them using the digital certificate.

  Follow the STEPs below to successfully sign an email:

  a) Open a new email window:



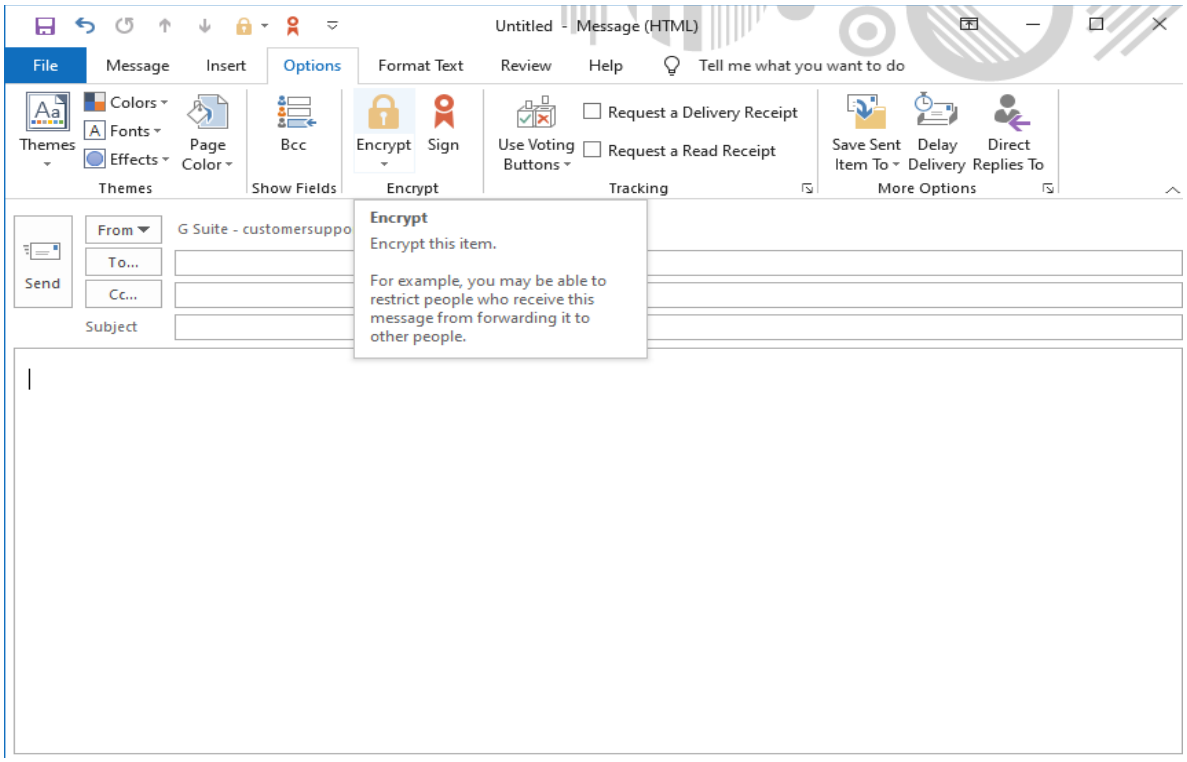
- In the Message ribbon in the Options section displayed are the two Mail Security icons, the first is the signing icon and selecting this will sign the email with the chosen certificate, the second is the encrypting icon and selecting it will encrypt the email

Signing Icon ***Encrypting Icon***

- **STEP 5**

  Encrypting the e-mail messages with Outlook

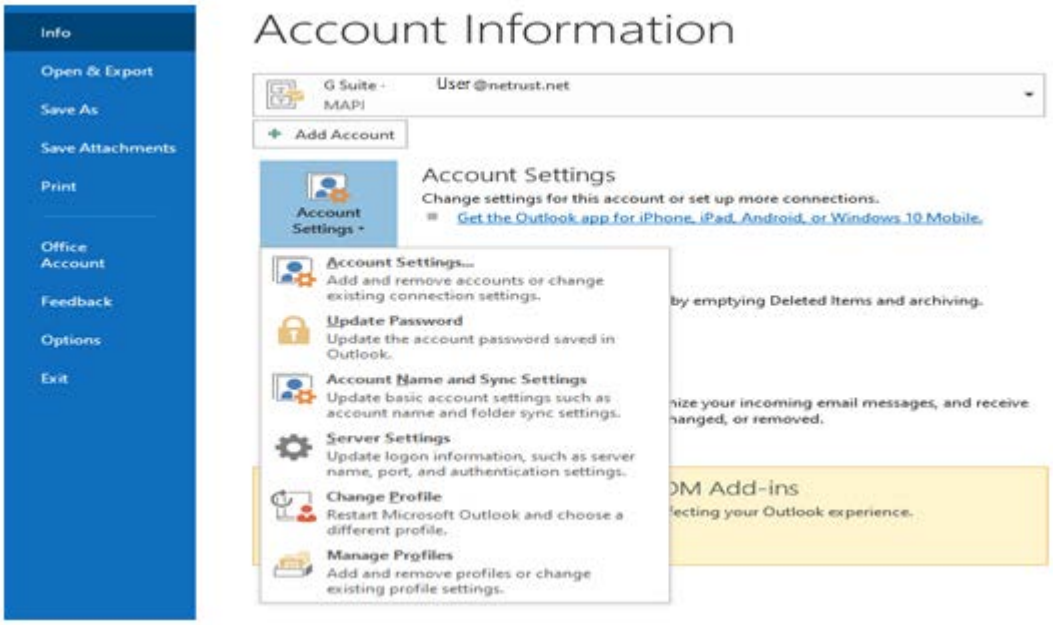
  Signing a message does not affect the contents of the message in any way or protect the message from being intercepted and read by someone other than the intended recipient. To ensure that only the recipient can read a message, you must also encrypt the message.



- **STEP 6**

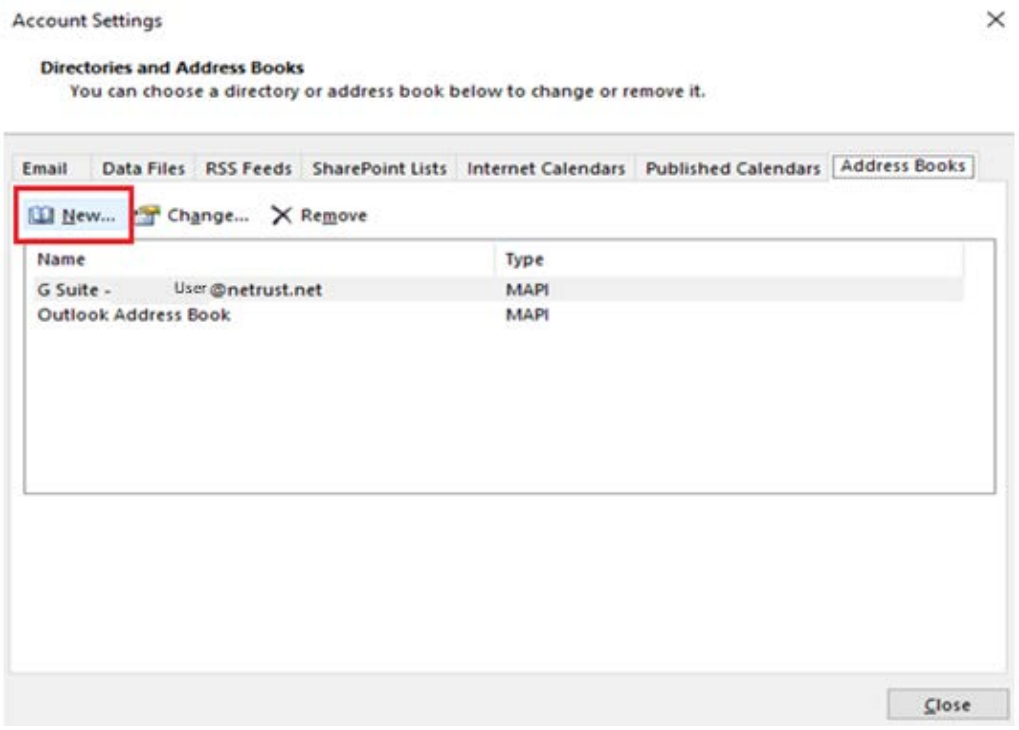
  To encrypt your message, add the online directory of the certification authority (ldap21.netrust.net). To do so, follow the STEPs below:

  Click on “Account Settings…”



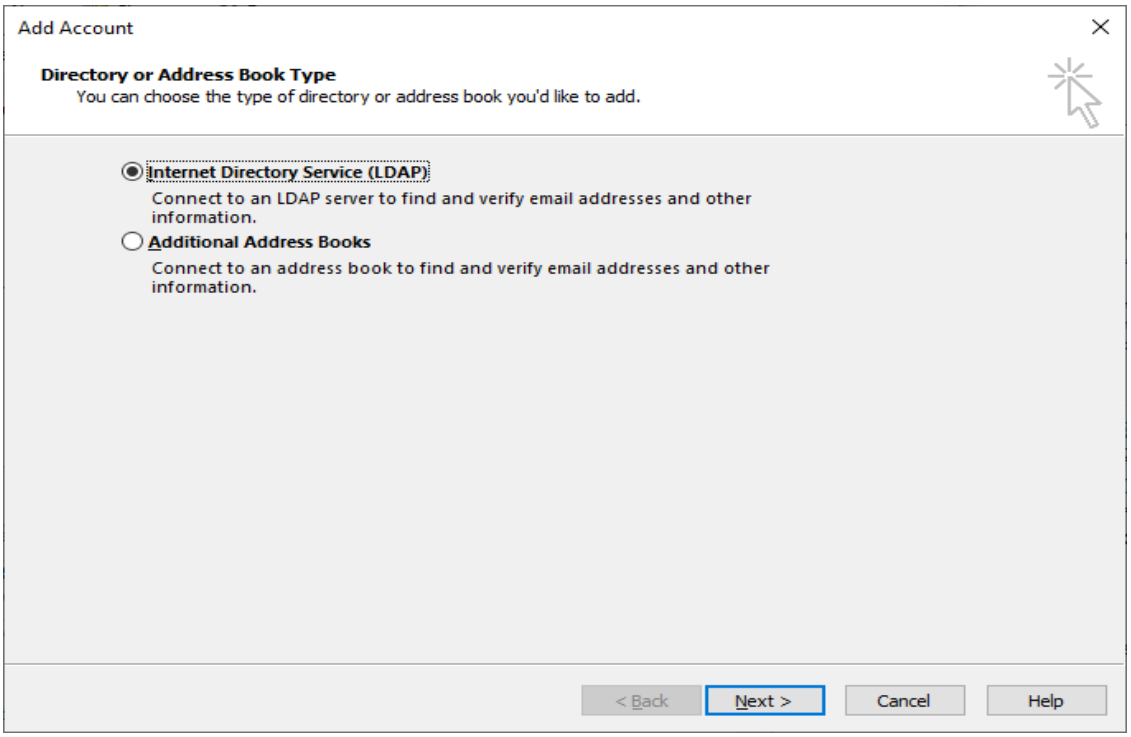
- **STEP 7**

  Select “New” to add the server name

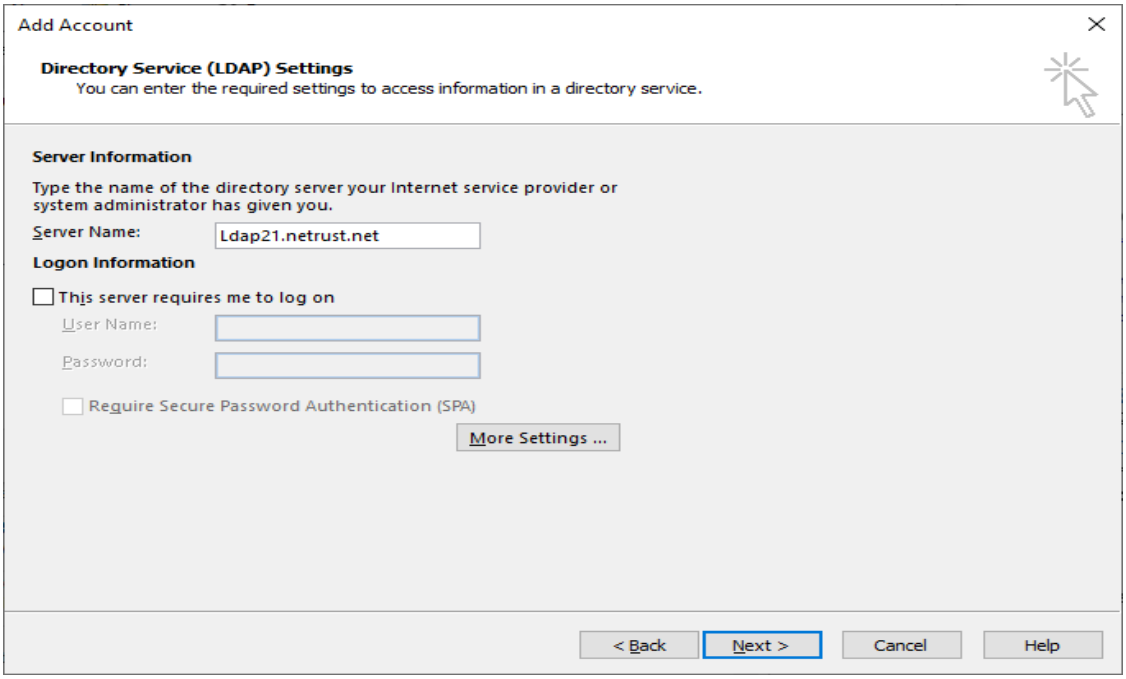


- **STEP 8**

  Select “Internet Directory Service (LDAP), click “Next”

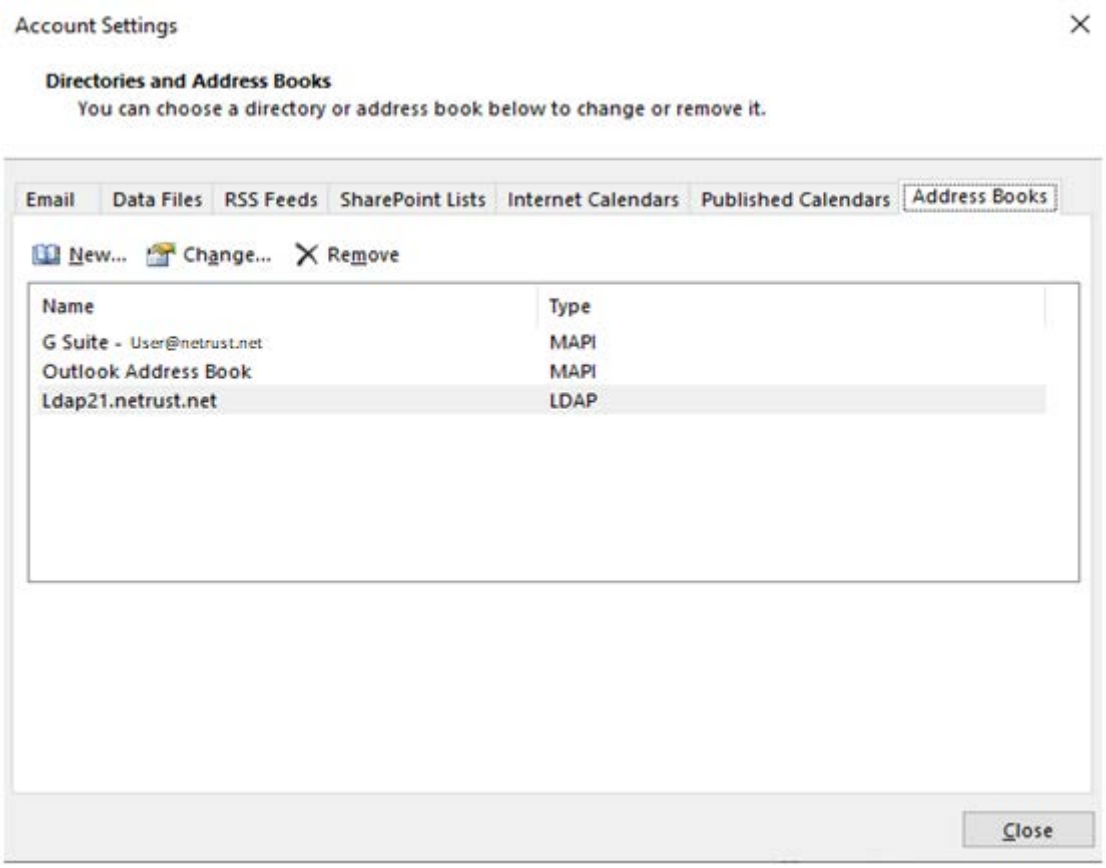


Add Server Name as: Ldap21.netrust.net



- **STEP 9**

  Upon adding the **Server Name**, proceed to **Restart** the Outlook



12. How to Enrol/Recover Certificate via Entrust Certificate Agent

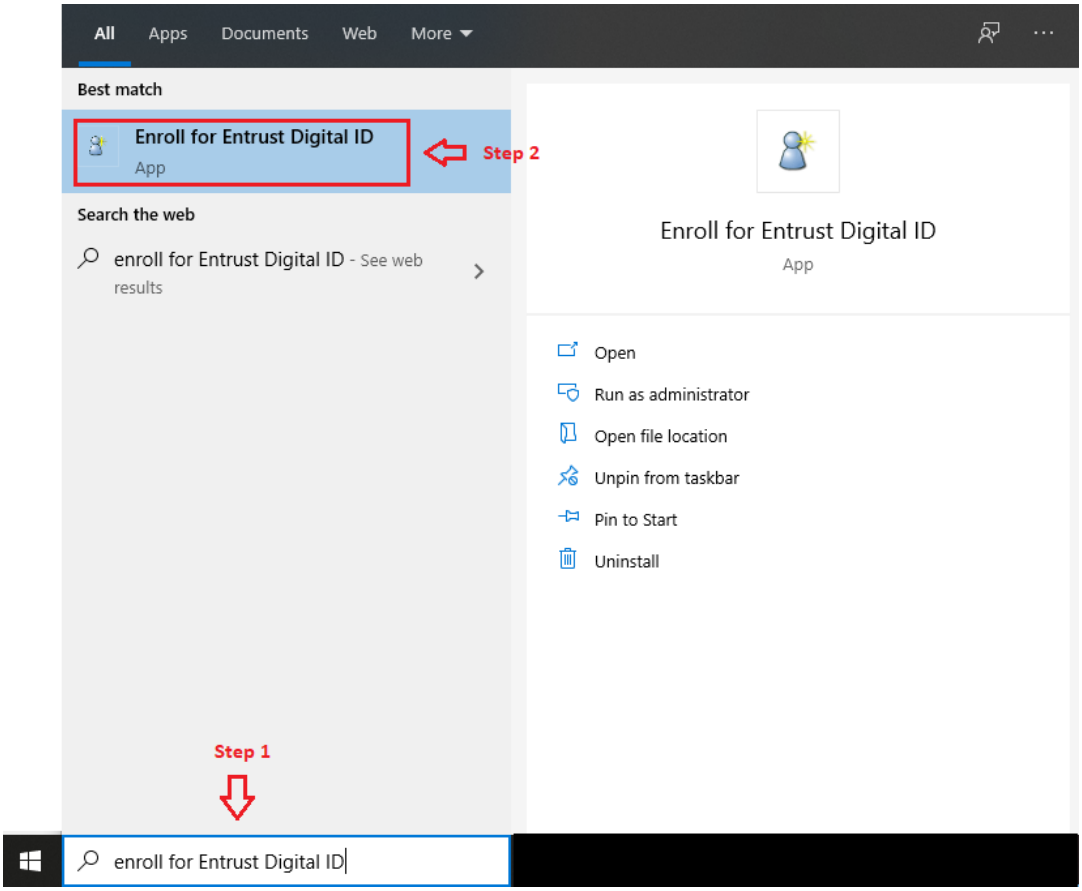
Enrolment

- **STEP 1**

  Search for Enroll for Entrust Digital ID

- **STEP 2**

  Select Enroll for Entrust Digital ID App



- **STEP 3**

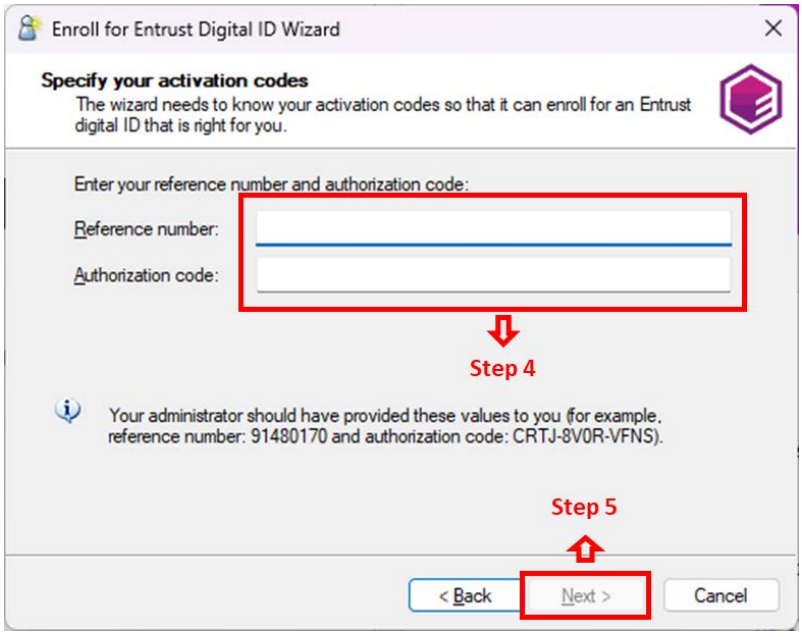
  Select 'Next' to proceed

- **STEP 4**

  Enter the Reference number and Authorization code

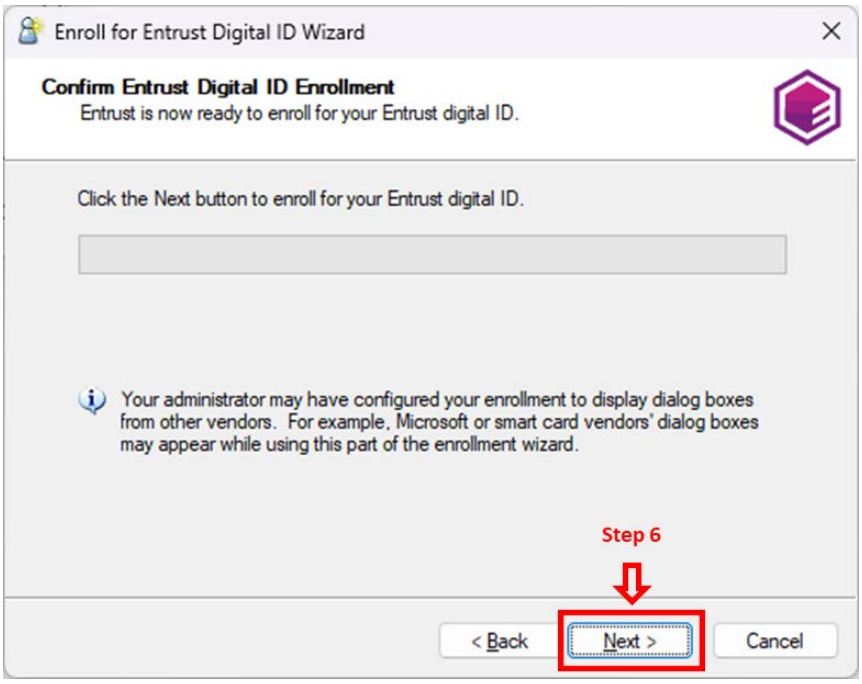
- **STEP 5**

  Select 'Next' to proceed



- **STEP 6**

  Select ‘Next’ to proceed

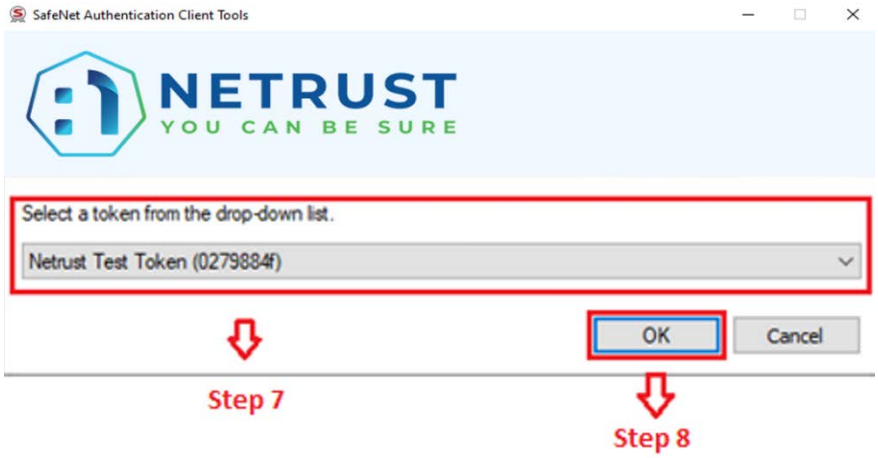


- **STEP 7**

  Ensure the correct token is selected from the drop down list

- **STEP 8**

  Select ‘OK’ to proceed

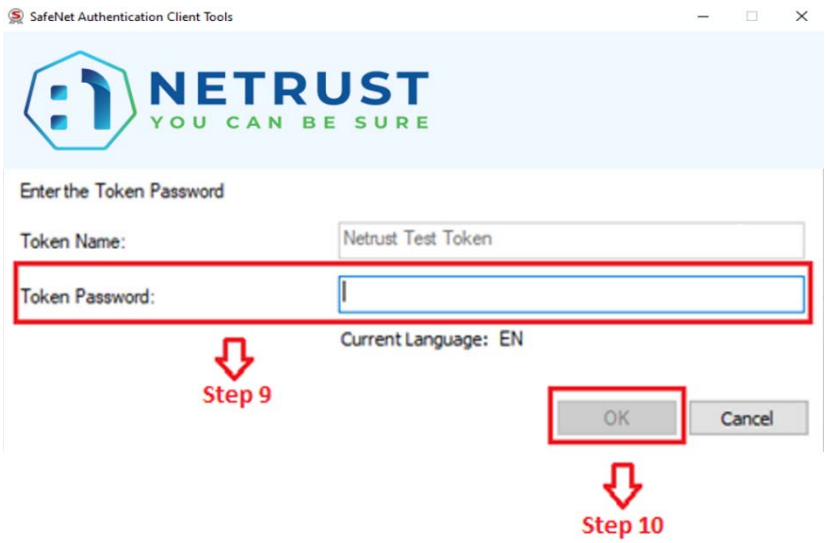


- **STEP 9**

  Select ‘OK’ to proceed

- **STEP 10**

  Select ‘OK’ to proceed

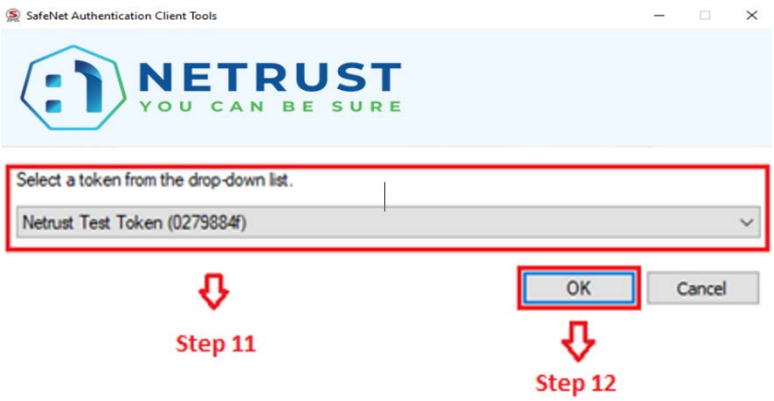


- **STEP 11**

  Ensure the correct token is selected from the drop down list again

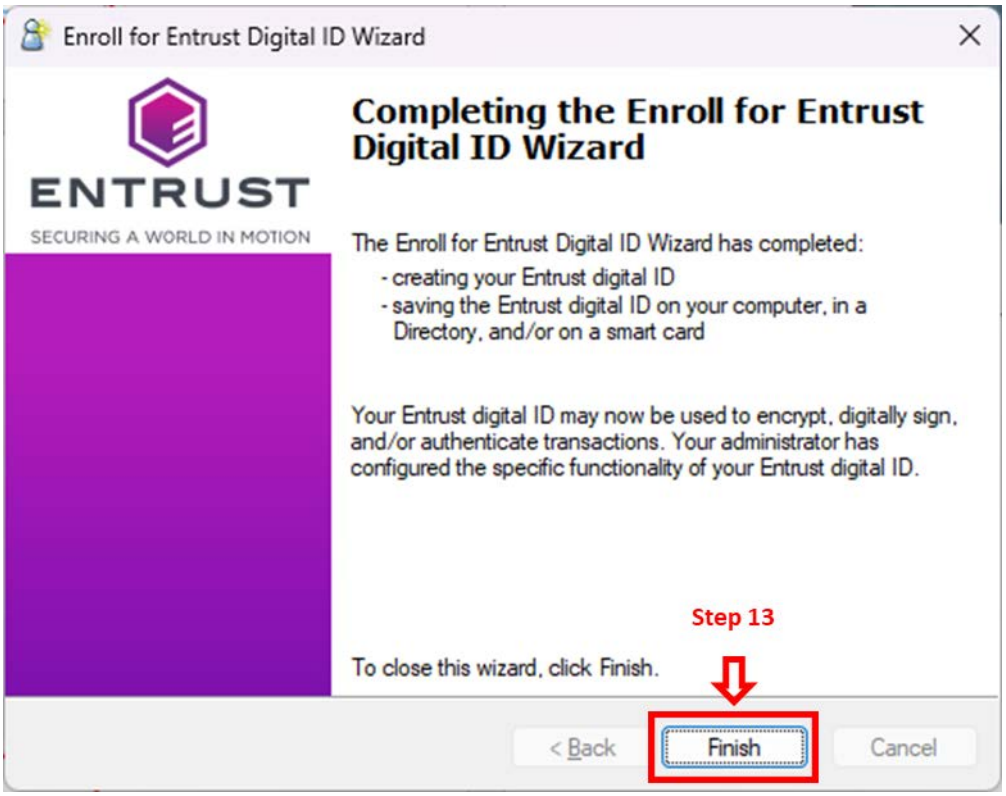
- **STEP 12**

  Select ‘OK’ to proceed



- **STEP 13**

  Click on 'Finish' once the enrolment is completed



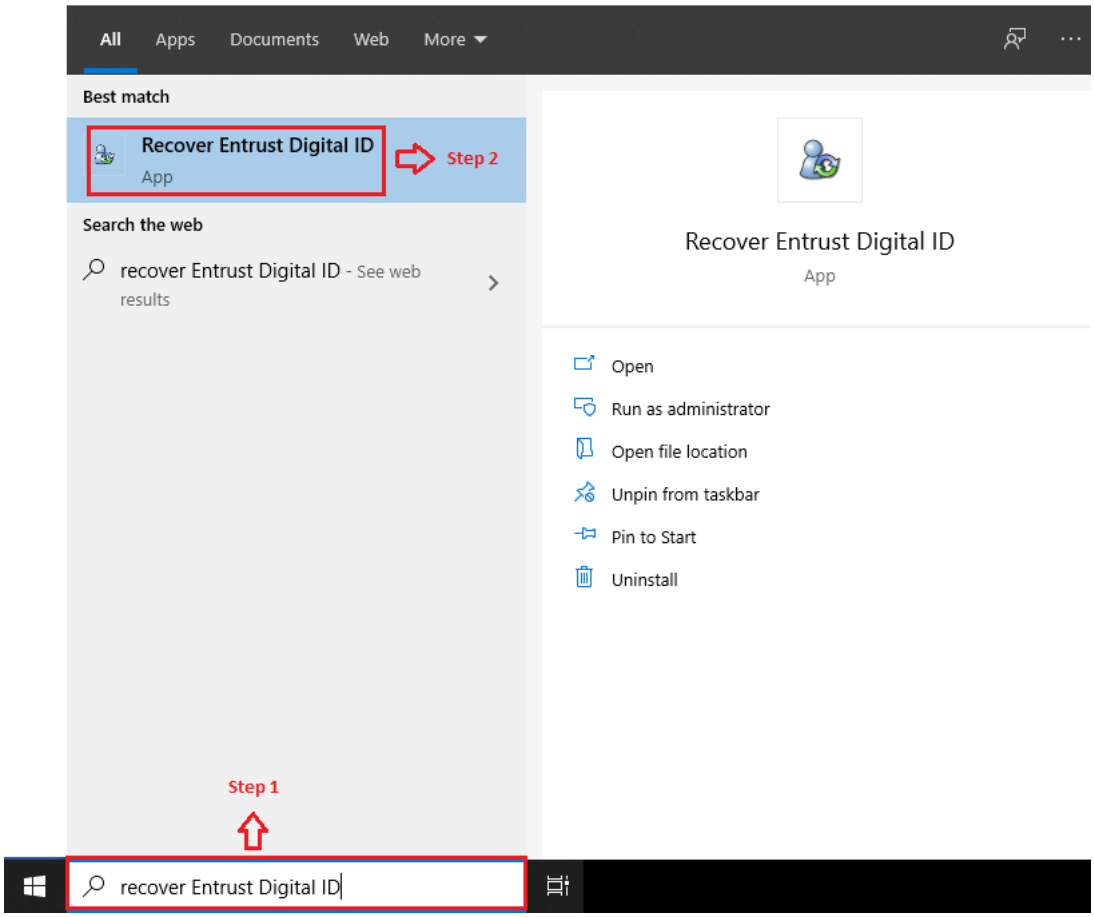
Recovery

- **STEP 1**

  Search for Recover Entrust Digital ID

- **STEP 2**

  Select Recover Entrust Digital ID App



- **STEP 3**

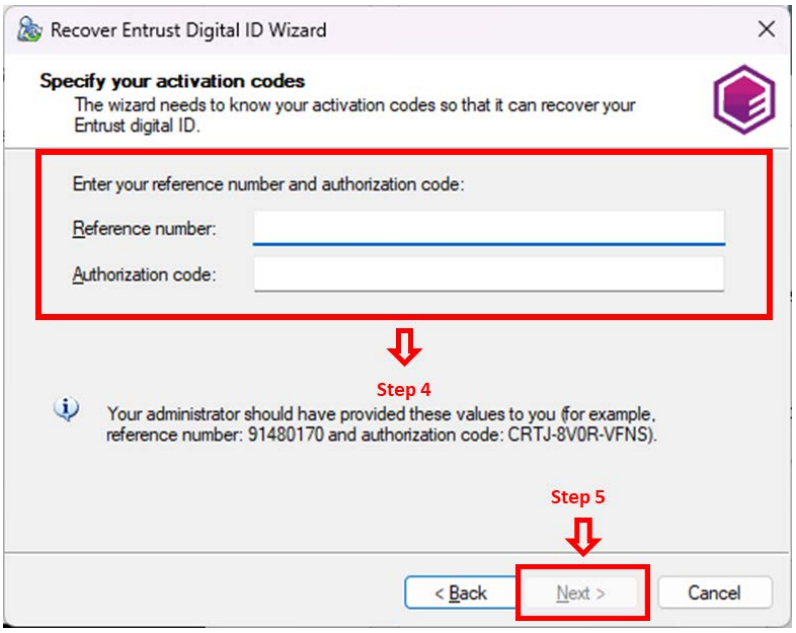
  Select 'Next' to proceed

- **STEP 4**

  Enter the Reference number and Authorization code

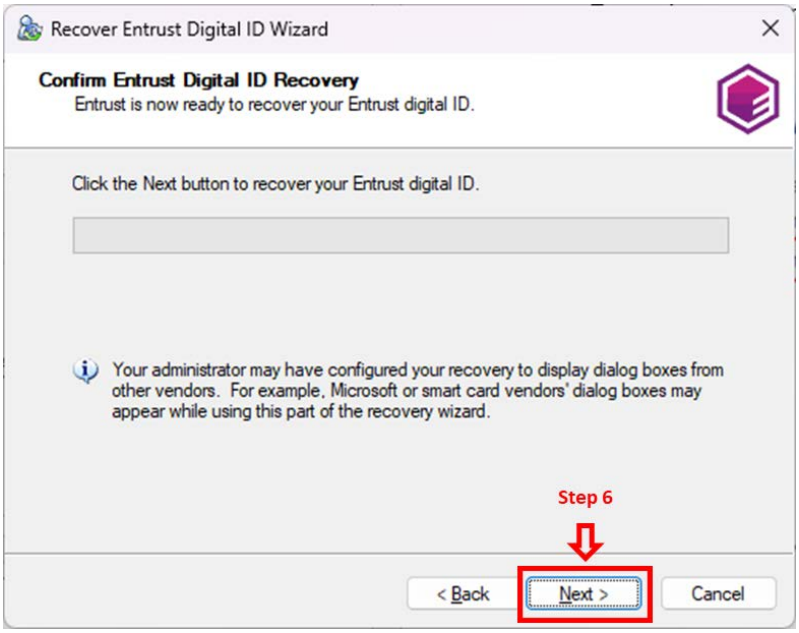
- **STEP 5**

  Select 'Next' to proceed



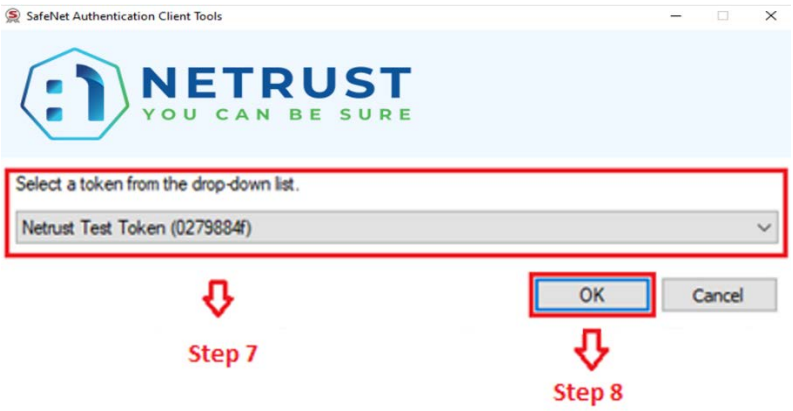
- **STEP 6**

  Select 'Next' to proceed



- **STEP 7**

  Ensure the correct token is selected from the drop down list

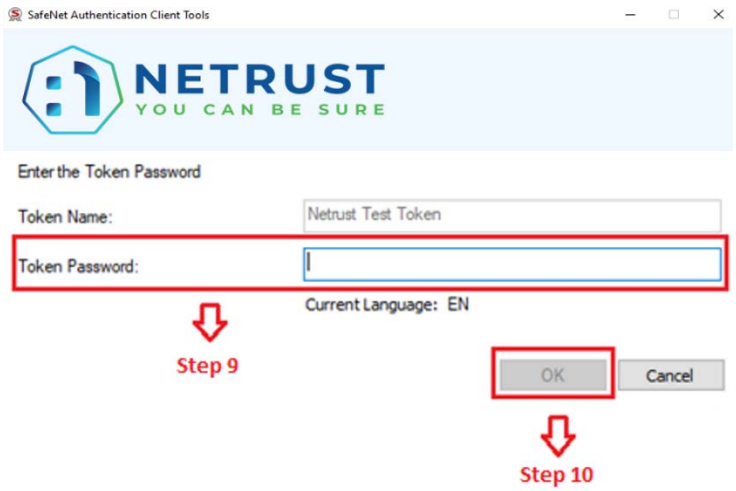


- **STEP 8**

  Select 'OK' to proceed

- **STEP 9**

  Type token password when prompted



- **STEP 10**

  Select ‘OK’ to proceed

- **STEP 11**

  Click on ‘Finish’ once the recovery is completed

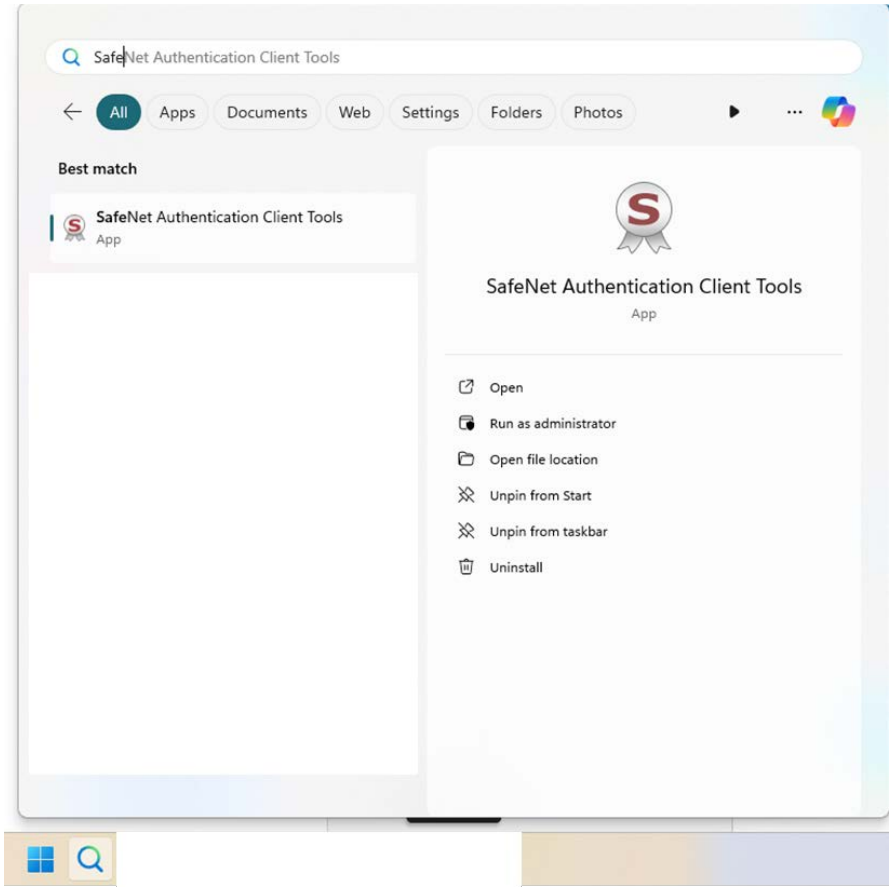
13. How to Initialize eToken via SafeNet Authentication Client Tools

WARNING: The token initialization process will delete all token content and reset all token parameters. DO NOT perform this unless Recovery codes are issued by Netrust

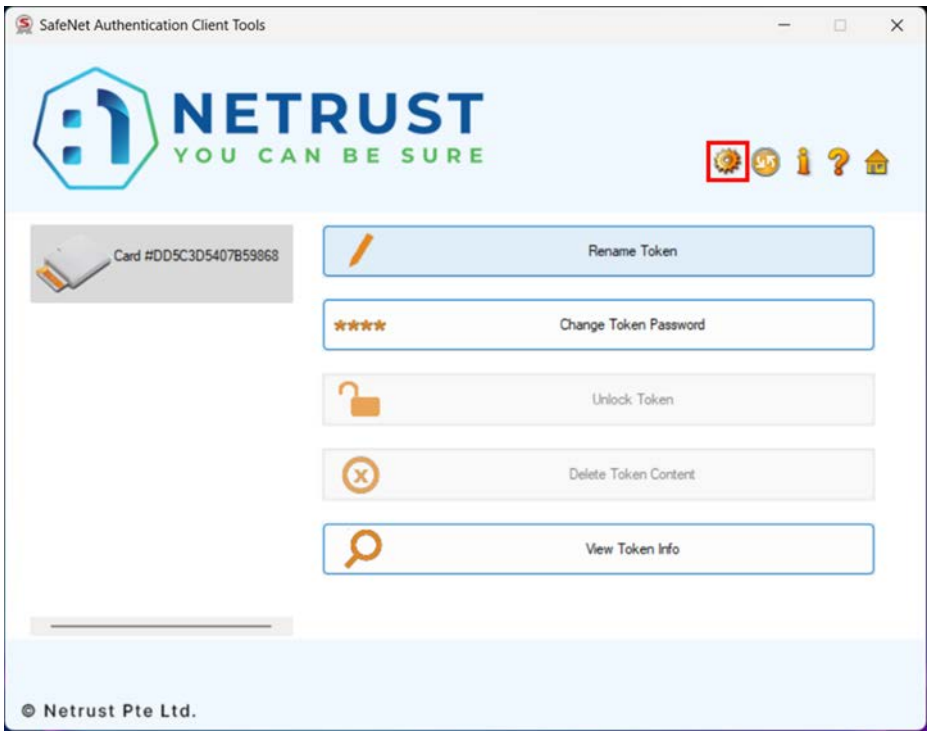
Please ensure that Safenet Authentication Client version 10.8 R10 has been installed.

- **STEP 1**
  Search for SafeNet Authentication Client Tools

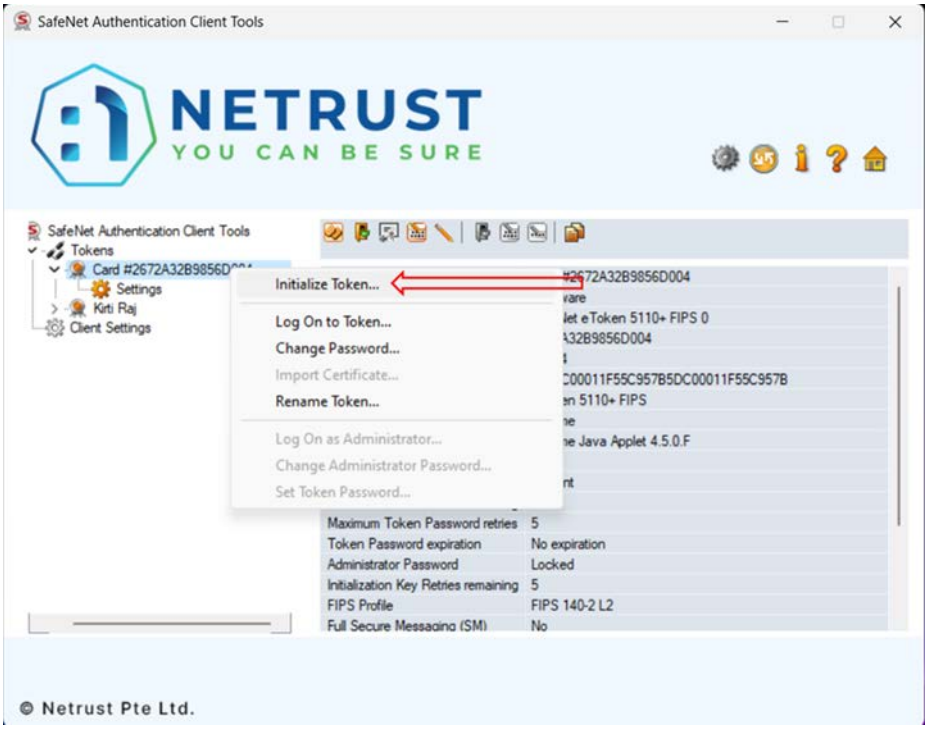
- **STEP 2**
  Select SafeNet Authentication Client Tools Application



- **STEP 3**
  Select Advanced View icon

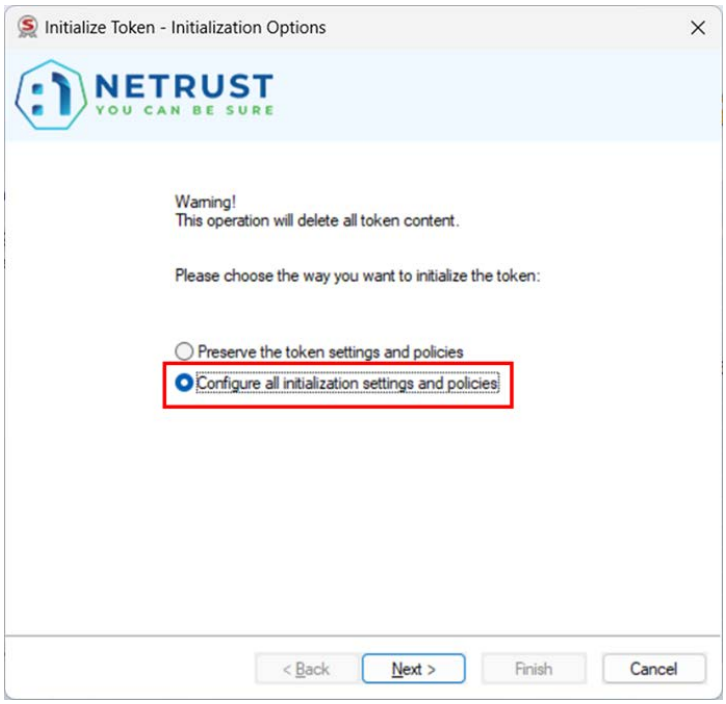


- **STEP 4**
  Right click on the user's token and select 'Initialize Token…'

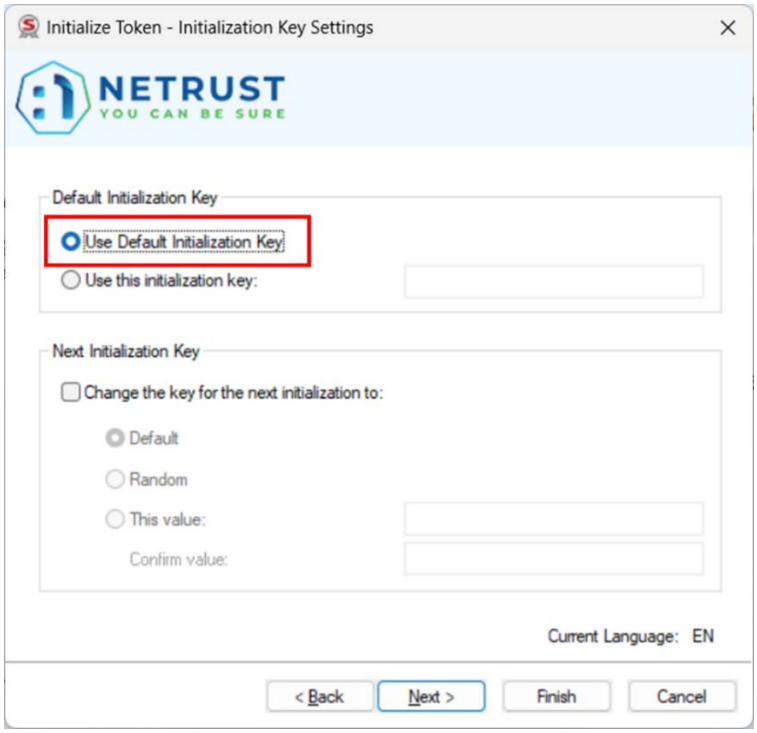


- **STEP 5**
  Select ‘Configure all initialization settings and policies’

- **STEP 6**
  Click ‘Next’ to proceed



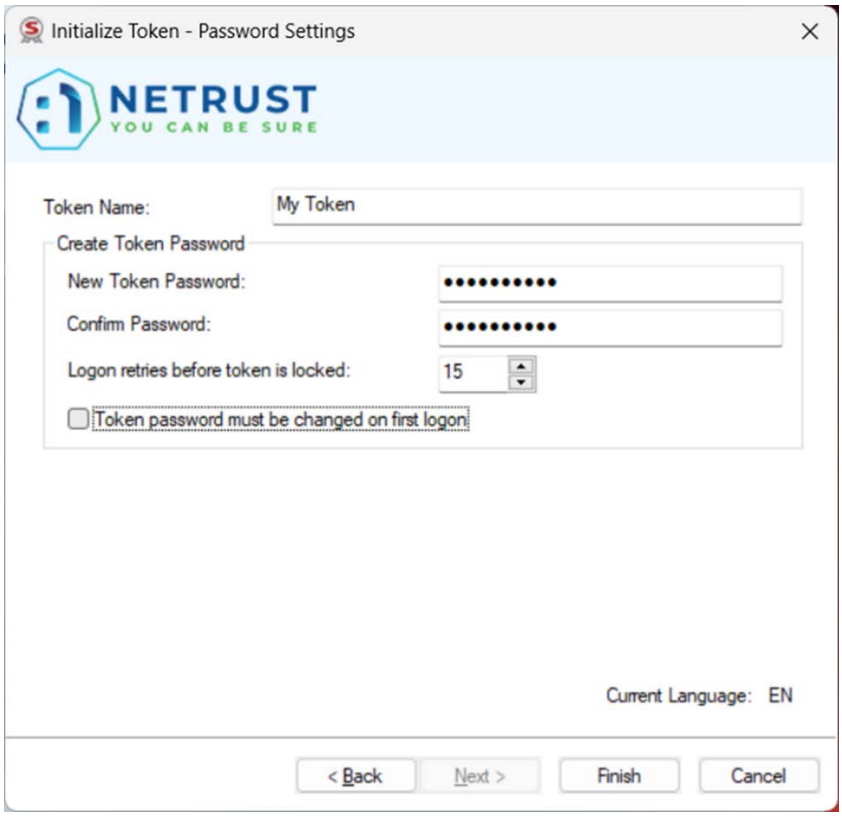
- **STEP 7**
  Click ‘Use Default Initialization Key’ and click ‘Next’



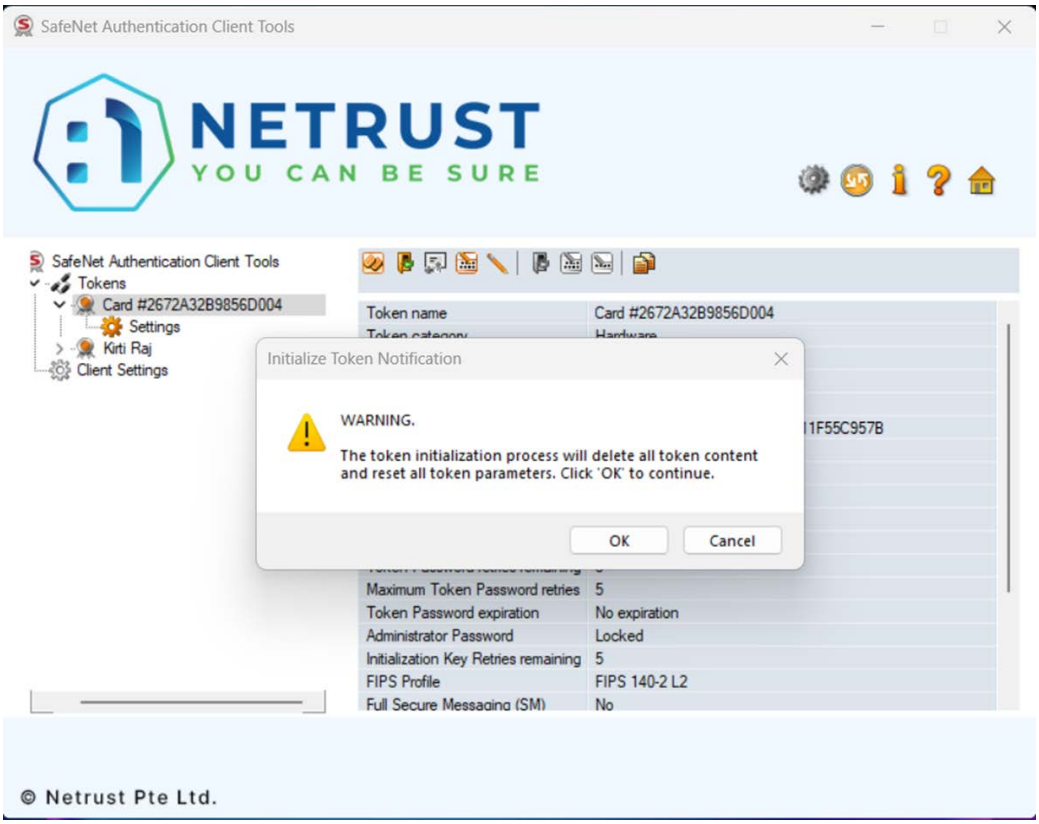
- **STEP 8**
  Type in the desired token name

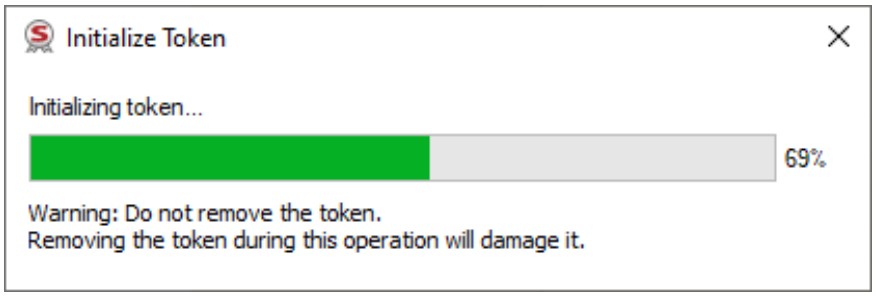
- **STEP 9**
  Uncheck “Token Password must be changed on first logon” and click “Finish”

- **STEP 10**
  Click ‘Finish’ to proceed

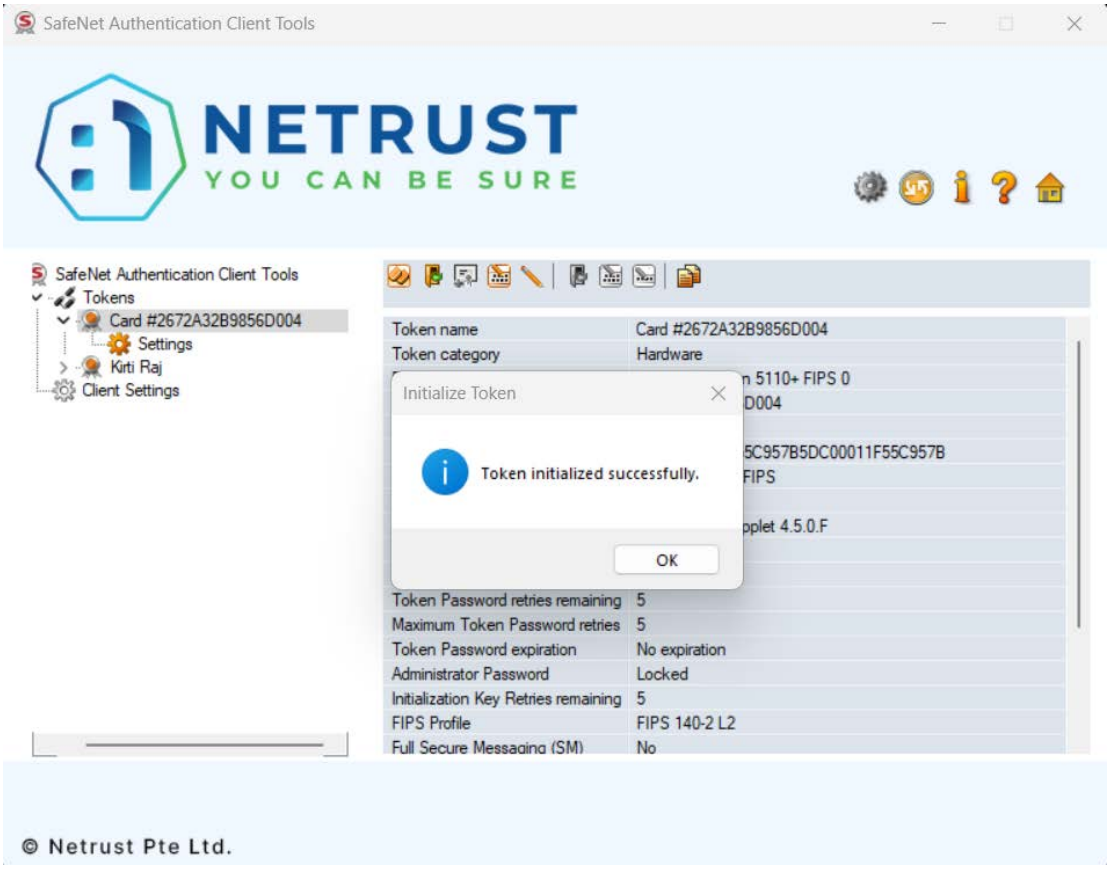


- **STEP 11**
  Click ‘OK’ to proceed





- **STEP 12**
  Click ‘OK’ once the initialization is completed



We thank you for engaging Netrust as your trusted partner

NETRUST PTE LTD

19 Tai Seng Avenue #05-01

Singapore 534054

Tel: +65 6212 1388

www.netrust.net

customersupport@netrust.net