



**NETRUST**  
YOU CAN BE SURE

## Netrust User Setup Guide

Version 1.5

Authored by: Netrust Customer Support



Netrust logo is registered trademark of Netrust Pte Ltd.

All other trademarks belong to their respective companies.

Netrust Pte Ltd considers information included in this documentation to be proprietary and restricted.

Permission to use, duplicate, or disclose document is granted by Netrust Pte Ltd, provided that the copyright notice appears in all copies and that both the copyright notice and this permission notice appear.

Use of this document should not be copied or posted on any network computer or broadcast in any media, and no modifications of the document are to be made without prior approval.

Use for any unauthorized purpose is expressly prohibited by law, and may result in severe civil and criminal penalties. Violators will be prosecuted to the maximum extent possible.

## Identification

<b>Document Author:</b>	Jasmine Leong, Customer Service Officer
<b>Document Version:</b>	1.5
<b>Updated by:</b>	Kirti Raj, Customer Service Manager

## Revision History

<b>Version</b>	<b>Effective Date</b>	<b>Summary of Changes</b>	<b>Author</b>
1.0	15 April 2020	Initial Release	Jasmine Leong
1.1	22 April 2020	Updated changes	Kirti Raj
1.2	20 May 2020	Addition of EESP features	Kirti Raj
1.3	27 May 2020	EESP admin usage	Jasmine Leong
1.4	23 Dec 2020	Email and fax update	Kirti Raj
1.5	25 Aug 2021	Logo, address and software version update	Isaac Zainal

## Table of Contents

1. About this Document .....	5
2. How To Install Safenet Authentication Client Tools.....	6
3. How To Install Entrust Entelligence Security Provider (EESP) .....	12
4. How To Change eToken Password via Safenet Authentication Client Tools .....	14
5. Online Certificate Renewal via Entrust Entelligence Security Provider (EESP) .....	16
6. How To Sign Documents Digitally with Adobe .....	22
7. How To Ensure Digital Signature is Automatically Trusted (AATL) .....	30
8. How To Check Certificate Details on eToken.....	32
9. How To Digitally Sign/Encrypt Files Using Entrust Entelligence Security Provider (EESP) using Microsoft Office Applications.....	34
10. How To Digitally Sign using Microsoft Office Word.....	47
11. Configuration of Secure Email on Microsoft Outlook .....	51
12. How to Enrol/Recover Certificate via Entrust Entelligence Security Provider .....	59
13. How to Initialize eToken via SafeNet Authentication Client Tools .....	68

## 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.

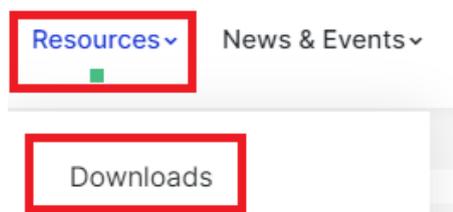
### **NOTE:**

**For STARS (eLodgment) users: Install Safenet Authentication Client 10.7 Token Driver.**

**For CORENET users: Skip this step and download Netrust Digital Signer 3.3 Full Package 2017.**

### ▪ **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 under Safenet Authentication Client 10.8 Token Driver for 64 Bit

For Windows 7/8/10 Running on 64 Bit Operating System using an eTOKEN

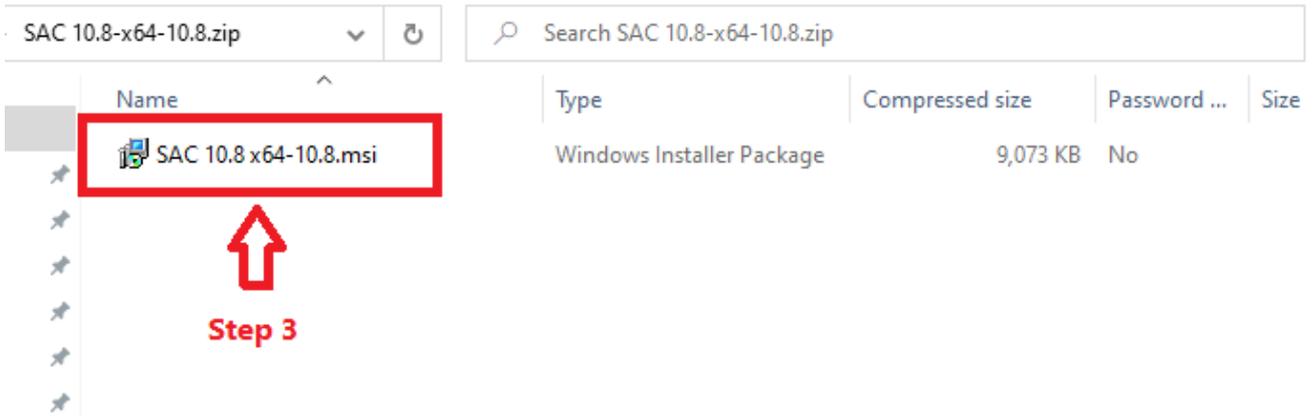
- [Safenet Authentication Client 10.8 Token Driver for 64 bit](#)

SHA-1: dff855d324f1be3139123369c3b05ac7f7c2d2fa

MD5: fcdb243b542b66a5dceb5a6150a8a61f

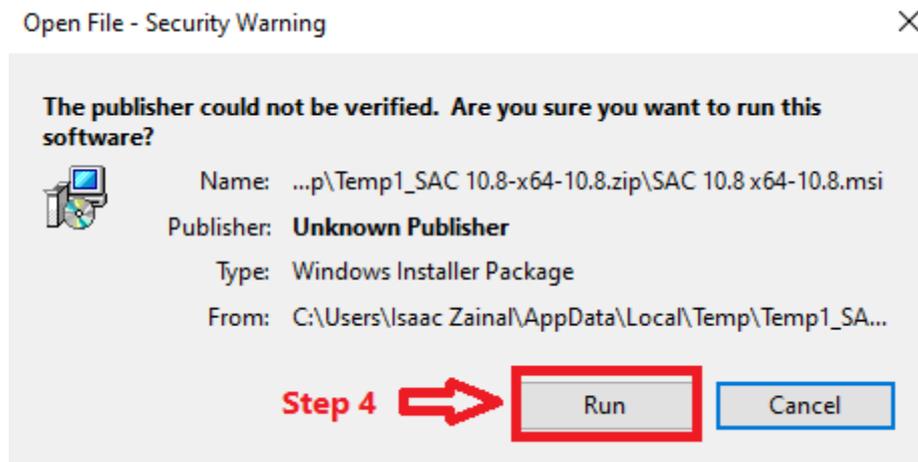
▪ **STEP 3**

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 'Run' to proceed



▪ **STEP 5**

Click on 'Next' to proceed.



▪ **STEP 6**

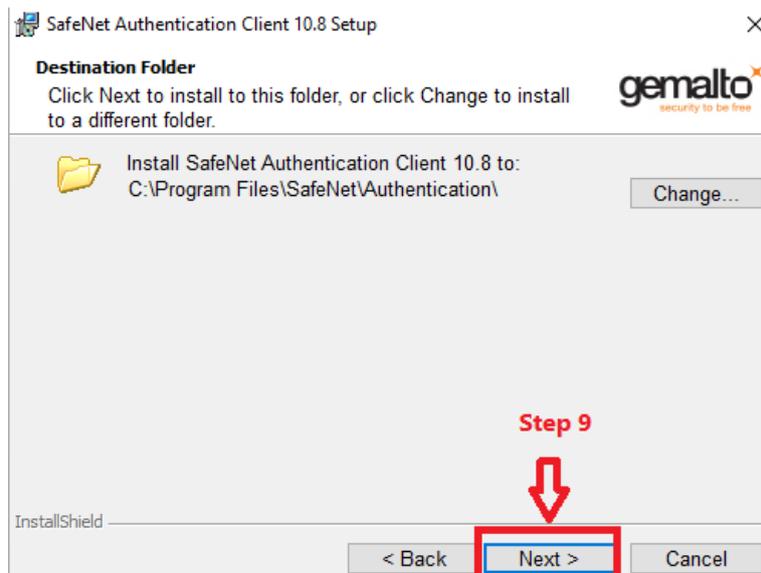
Click on 'Next' to proceed.



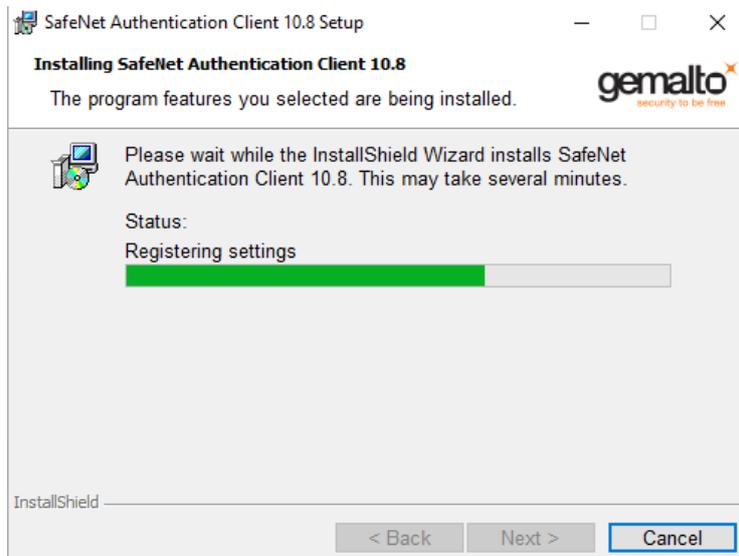
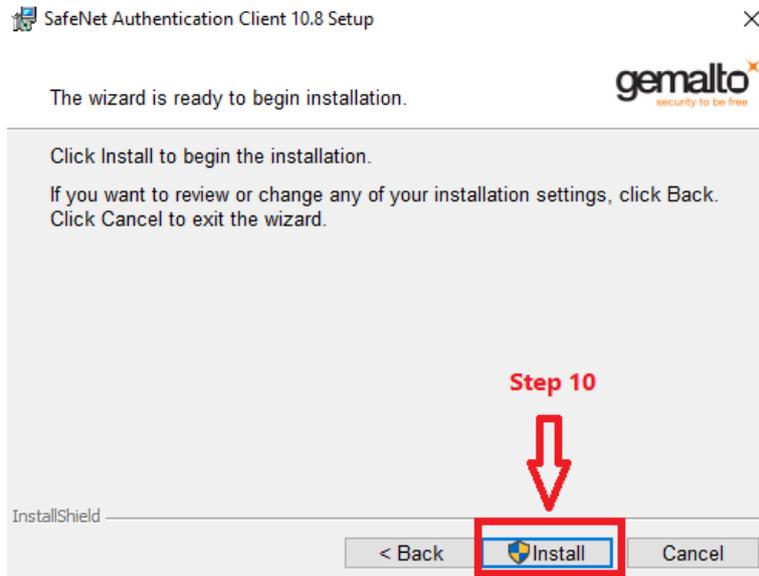
- **STEP 7**  
Select 'I accept the license agreement'
- **STEP 8**  
Click on 'Next' to proceed.



- **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.

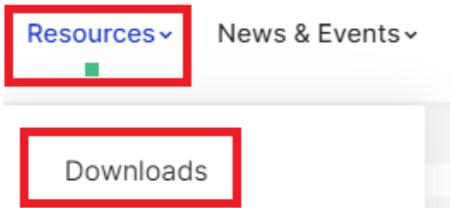


### 3. How To Install Entrust Entelligence Security Provider (EESP)

▪ **STEP 1**

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

Click on Resources, then click on Downloads.

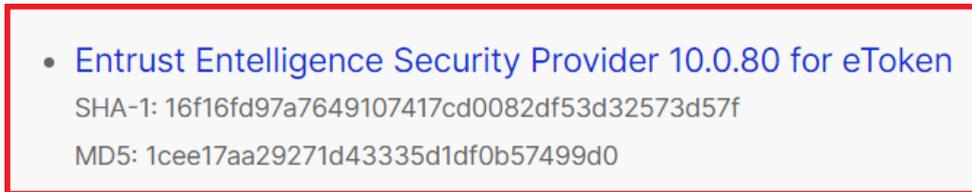


Under Netrust Downloadable Software, select the software depending on what is the version of your PC's Operating System and Windows Version.

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

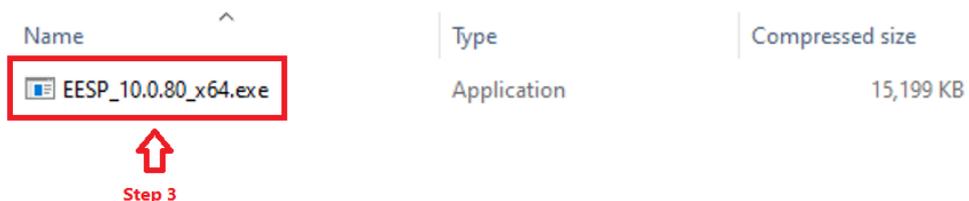
▪ **STEP 2**

Select and download the file under Entrust Entelligence Security Provider 10.0.8 for eToken



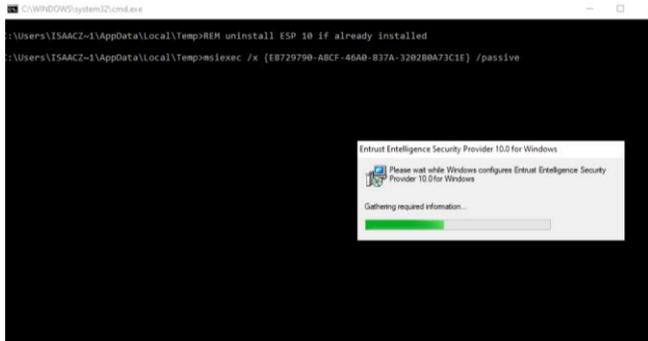
▪ **STEP 3**

Open the software folder, extract the ZIP file, and double click on EESP 10.0.80.exe file to run the installation



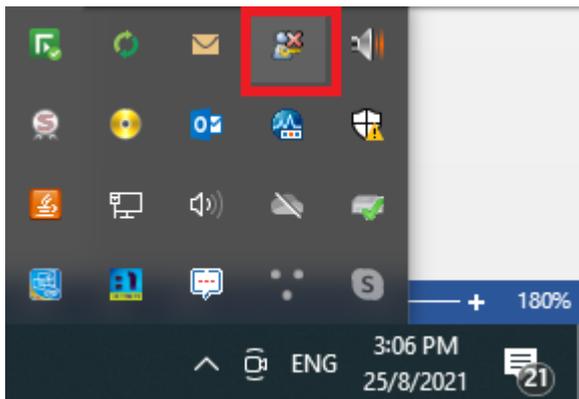
- **STEP 4**

The installation will proceed automatically.



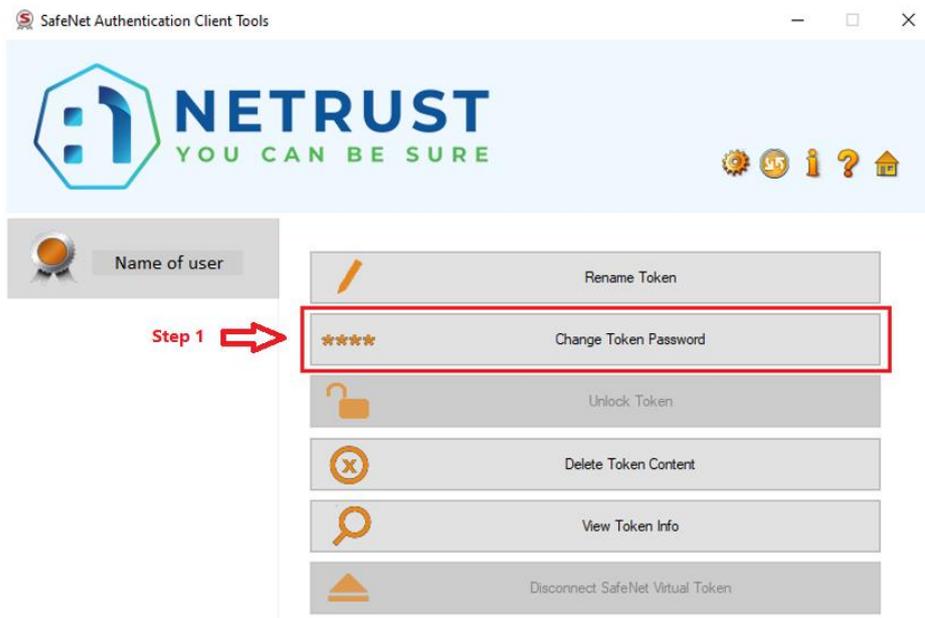
- **STEP 5**

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**

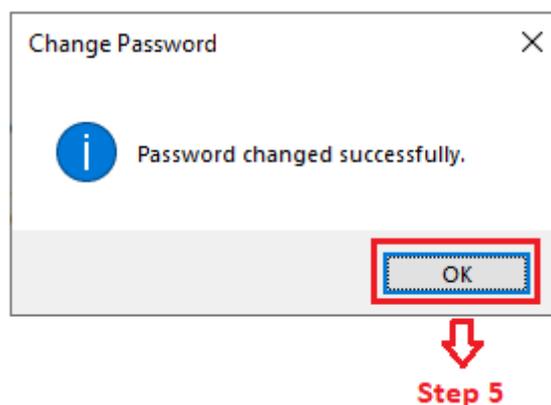
Enter your preferred New Token Password

**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 Entelligence Security Provider (EESP)

### 1. What is the function of EESP?

Entrust Entelligence Security Provider (EESP) is a client software which monitors user's certificate expiry status. When certificate is expiring soon, EESP will prompt users to renew their certificate in order 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 EESP is properly configured

The auto renewal of Netrust Certificate requires 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 EESP program to poll and retrieve available updates/renewal for the certificate

Port 389 – This port is used by EESP 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:

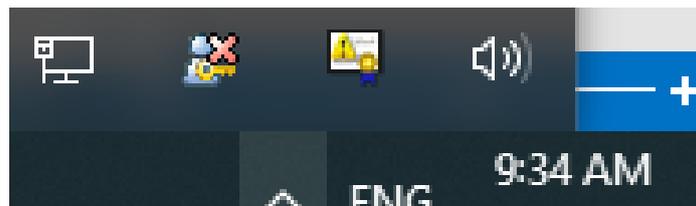
- telnet authority21.netrust.net 829
- telnet ldap21.netrust.net 389

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**

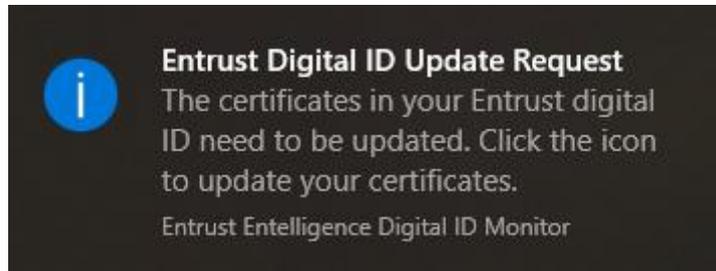
### 3. When will I know that my certificate is due for renewal or about to expire?

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

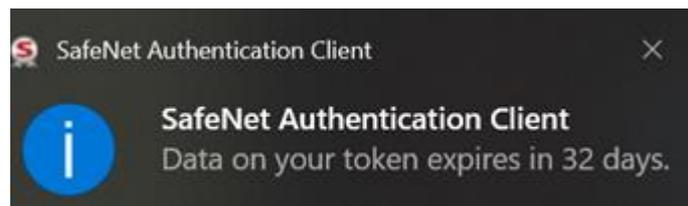


▪ **STEP 1**

A pop up message will appear on the bottom right hand corner of the PC, from Entrust Entelligence Security Provider:

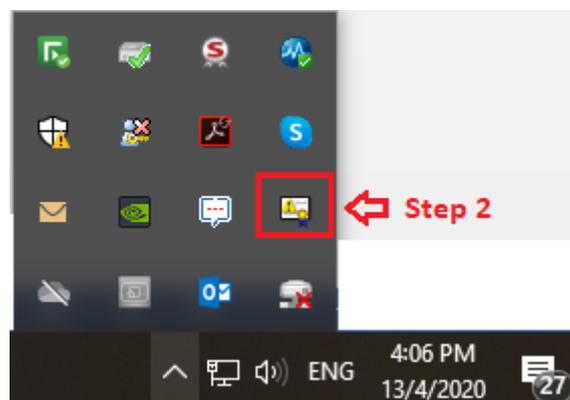


There will also be a prompt from Safenet Authentication Client (token driver) as below. Please follow from Step 2 to update the token.

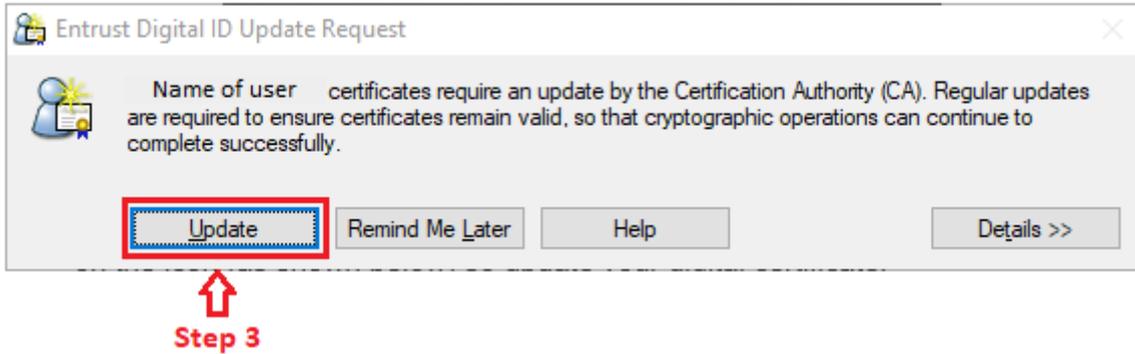


▪ **STEP 2**

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



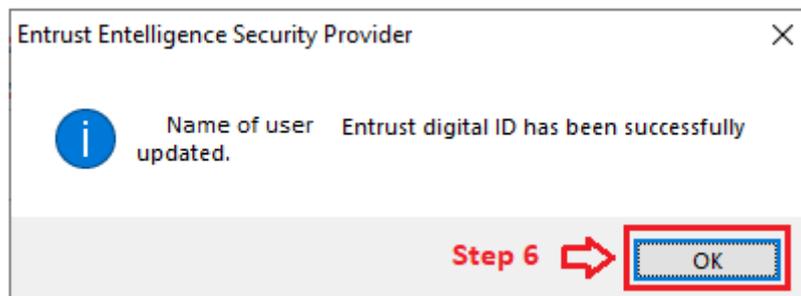
- **STEP 3**  
Click on 'Update' to proceed.



- **STEP 4**  
Enter token password
- **STEP 5**  
Click on 'OK' to proceed



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

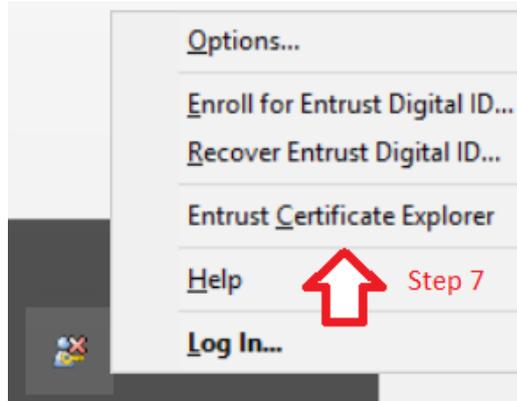


▪ **STEP 7**

The 'EESP' is able to create a personal encryption group for file encryption and digital signing for users that frequently communicate

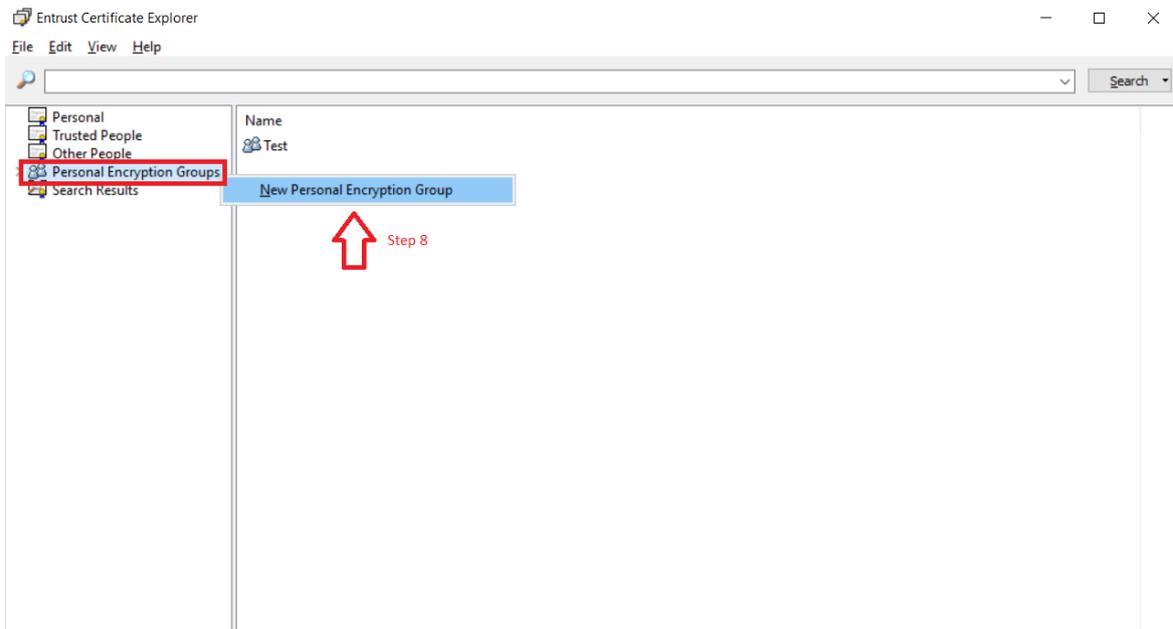
This personal encryption group can contain recipients from Netrust and other users with a public certificate saved locally

Right click on the  select the option Entrust certificate explorer



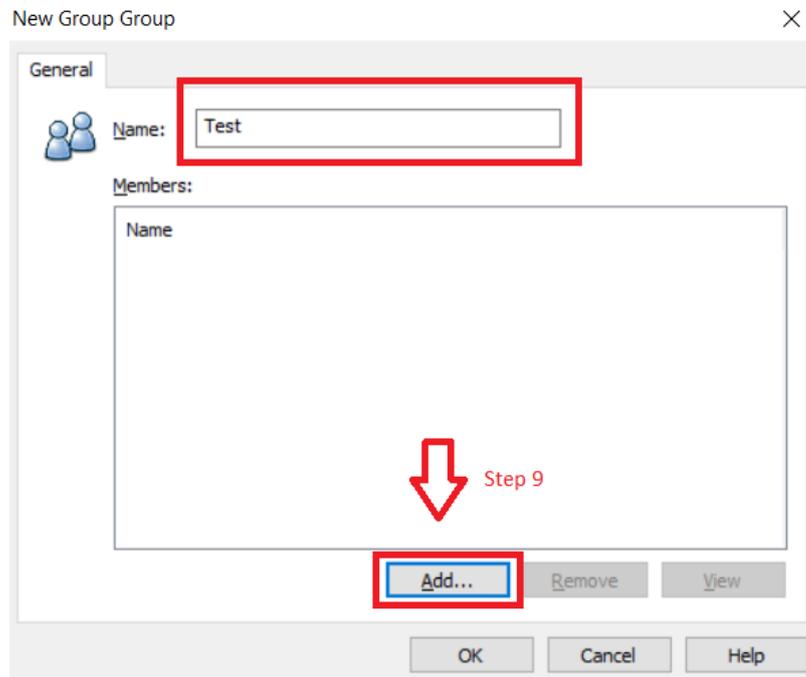
▪ **STEP 8**

A pop up window will appear, right click and select New Personal Encryption Group



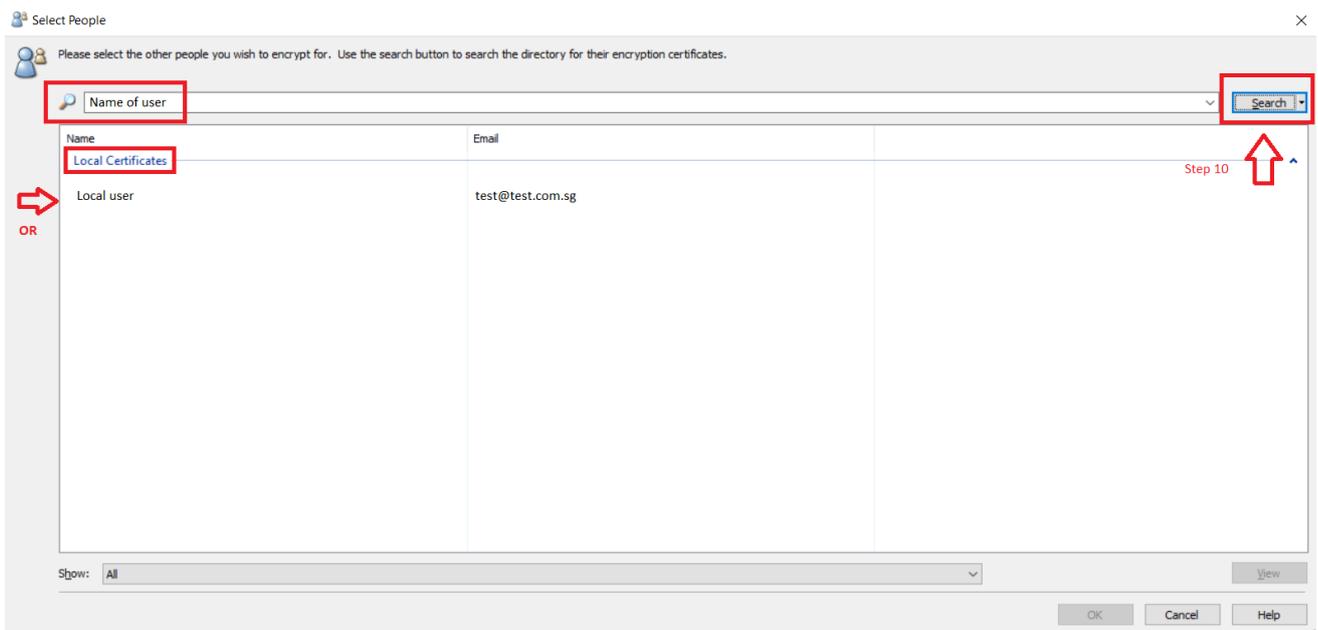
▪ **STEP 9**

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



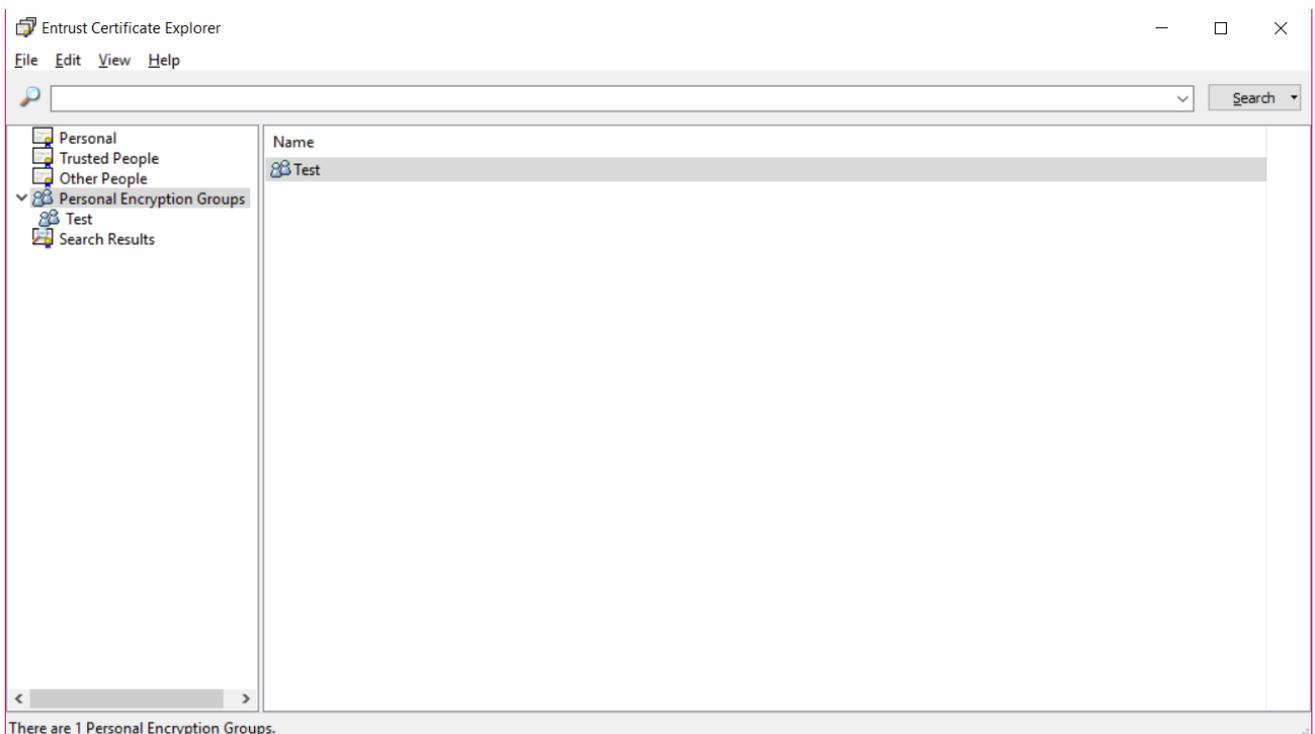
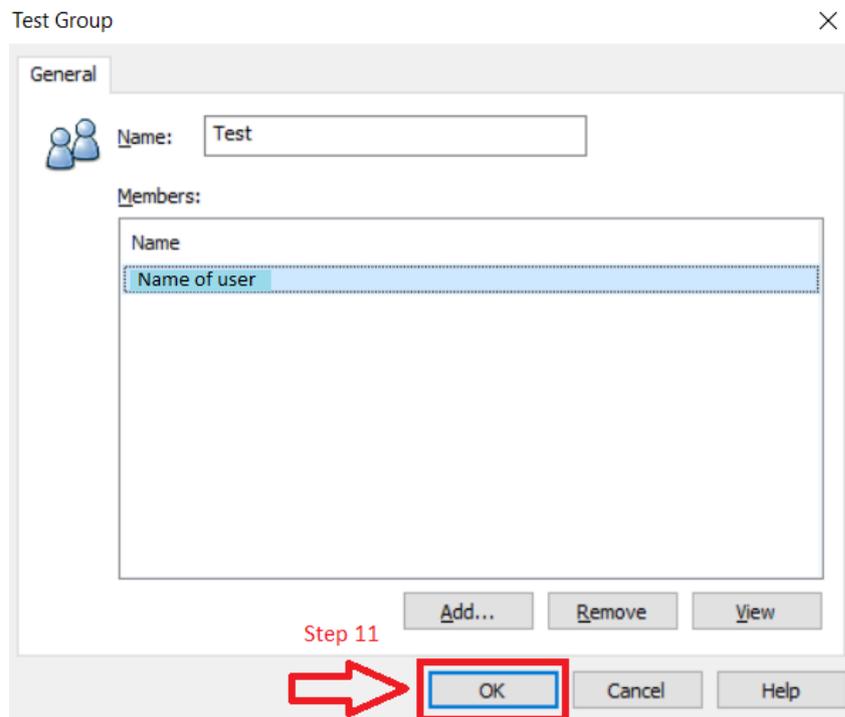
▪ **STEP 10**

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**

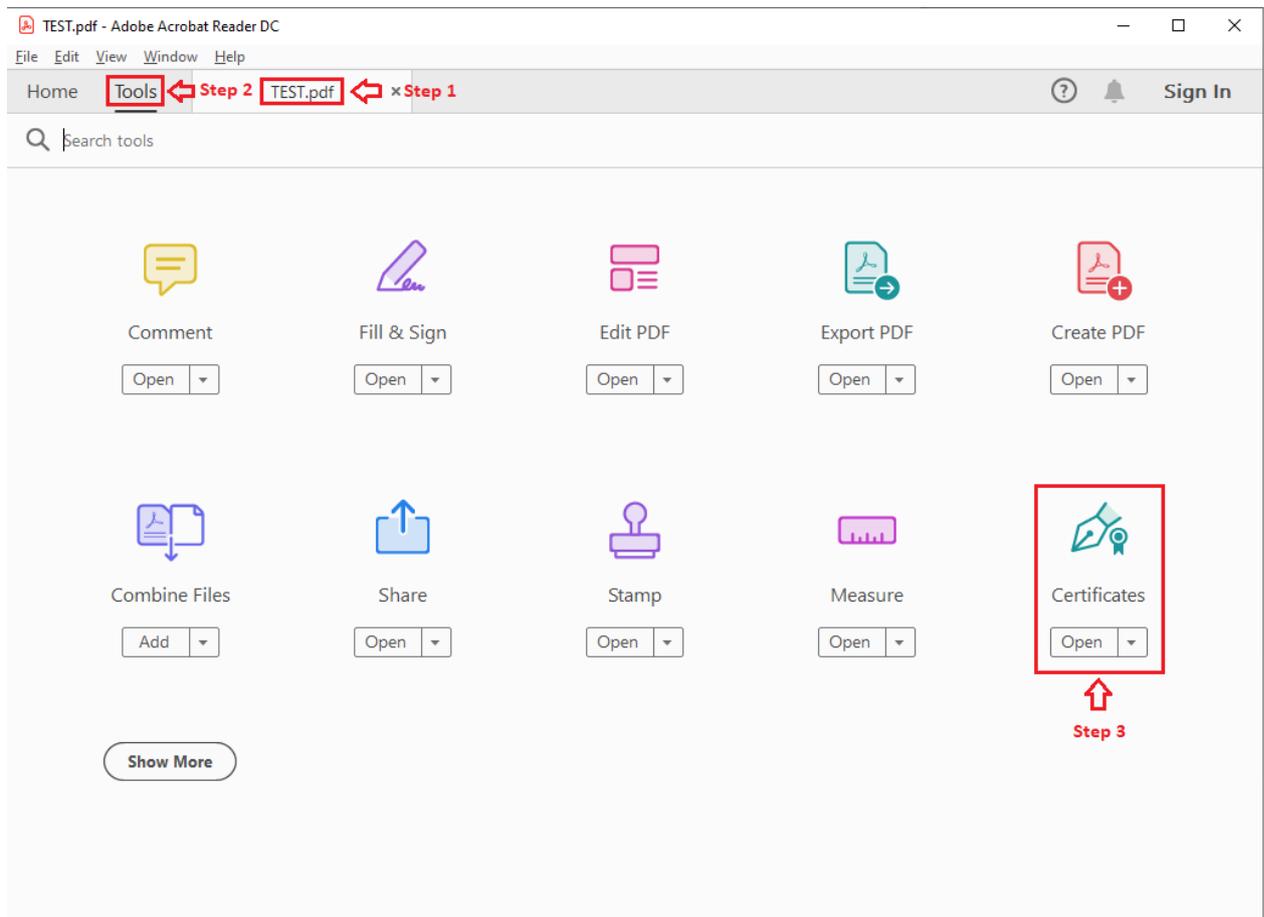
Click 'OK' once all certificates selected to finalize group



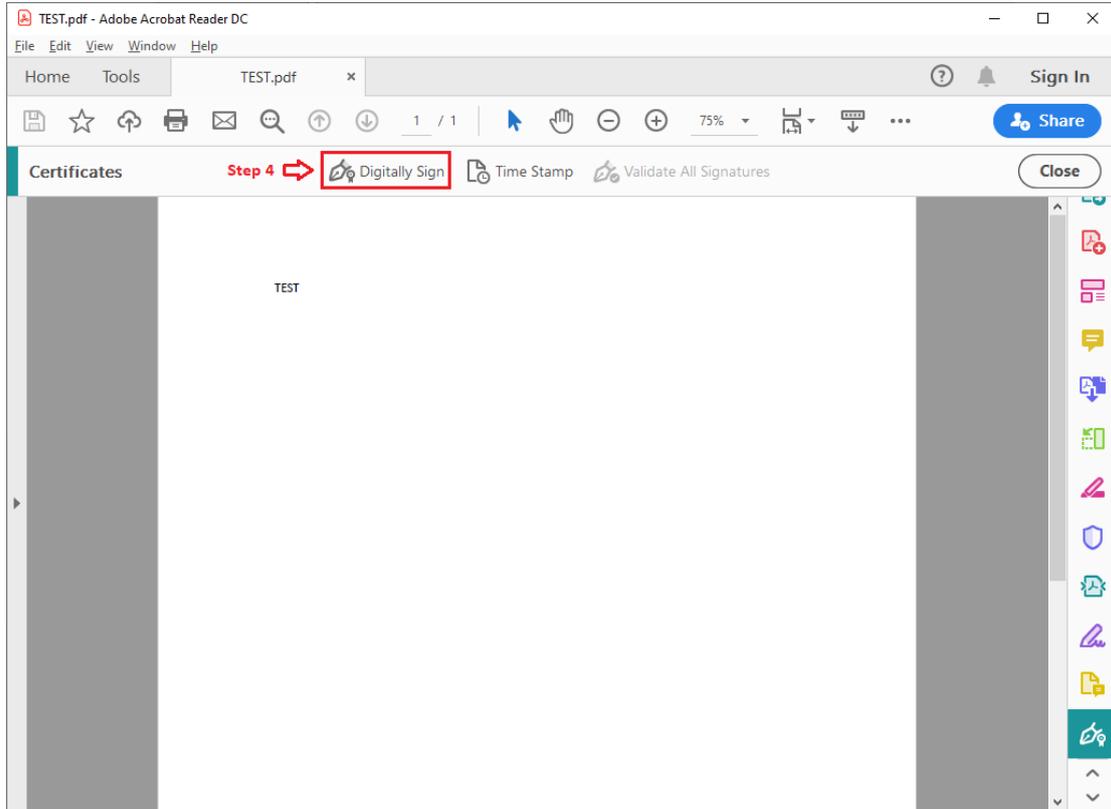
The group name will appear in Entrust Certificate Explorer.

## 6. How To Sign Documents Digitally with Adobe

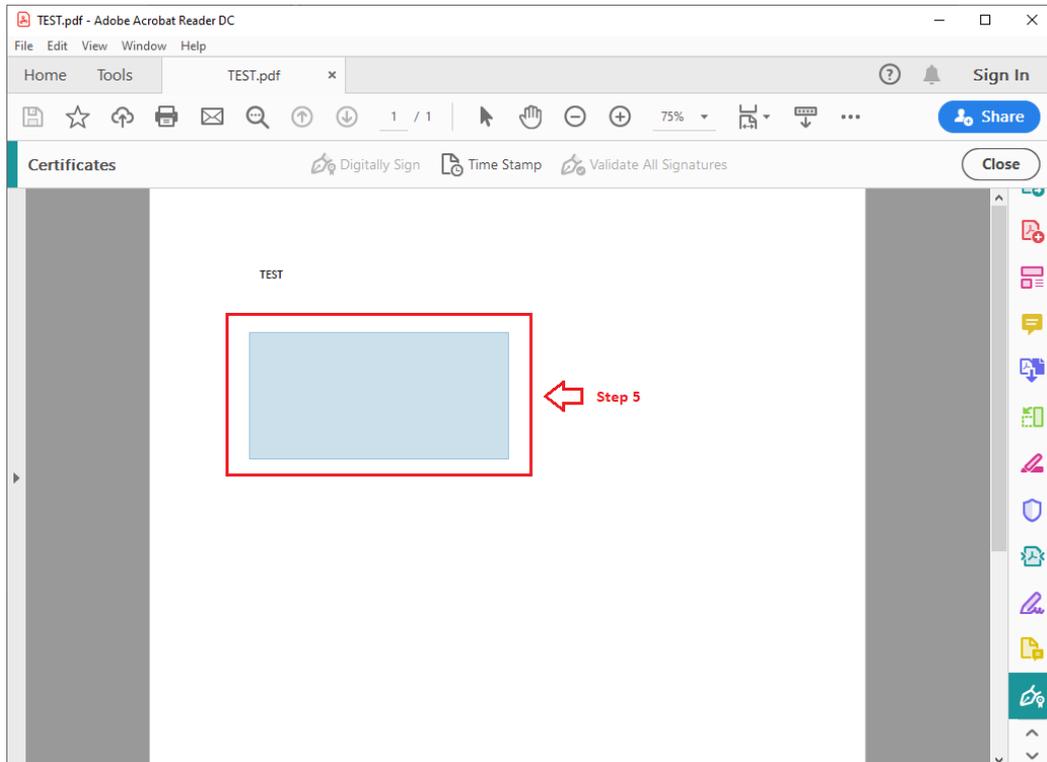
- **STEP 1**  
Open a PDF Document
- **STEP 2**  
Click on 'Tools'
- **STEP 3**  
Click on 'Certificates'



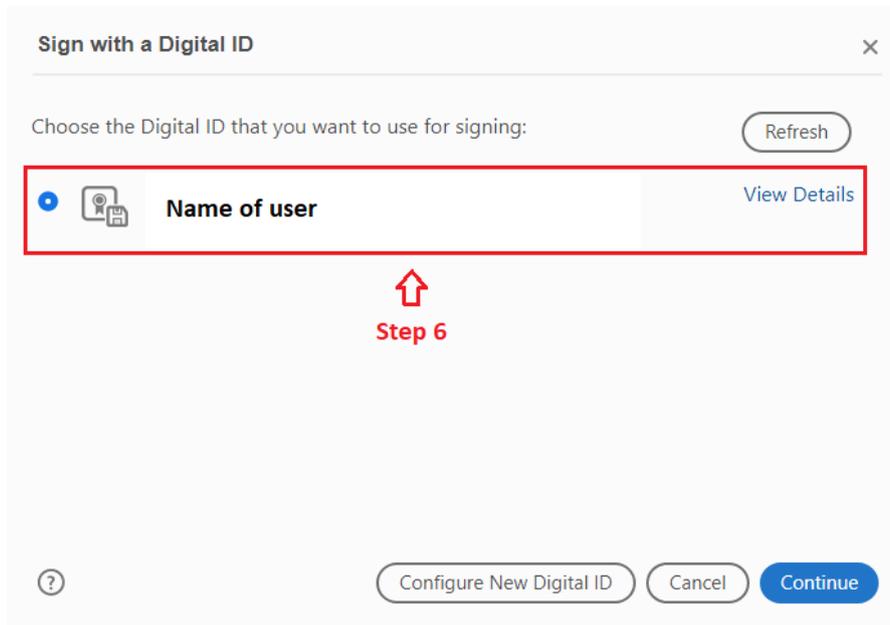
- **STEP 4**  
Click on 'Digitally Sign'



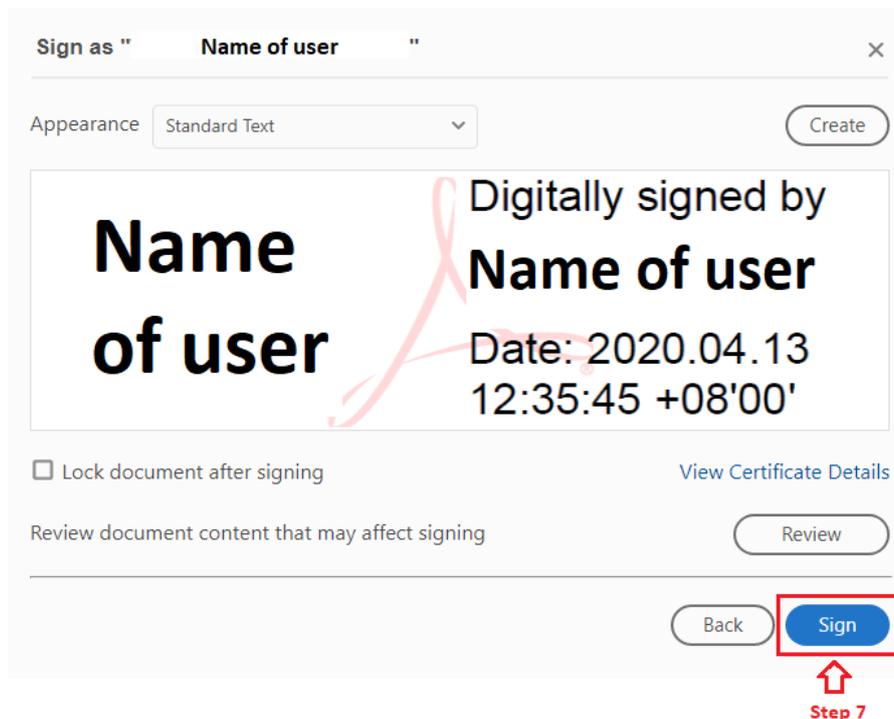
- **STEP 5**  
Draw and drag a box where you want your signature to be placed



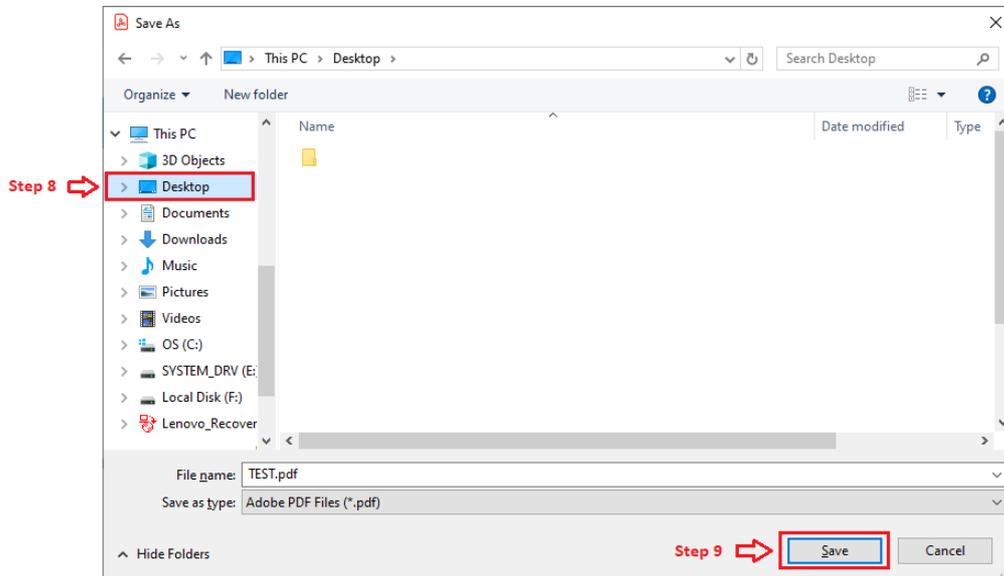
- **STEP 6**  
Select the user's certificate to digitally sign



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



- **STEP 8**  
Save the file in your Desktop or your preferred file location
- **STEP 9**  
Click on 'Save' to proceed



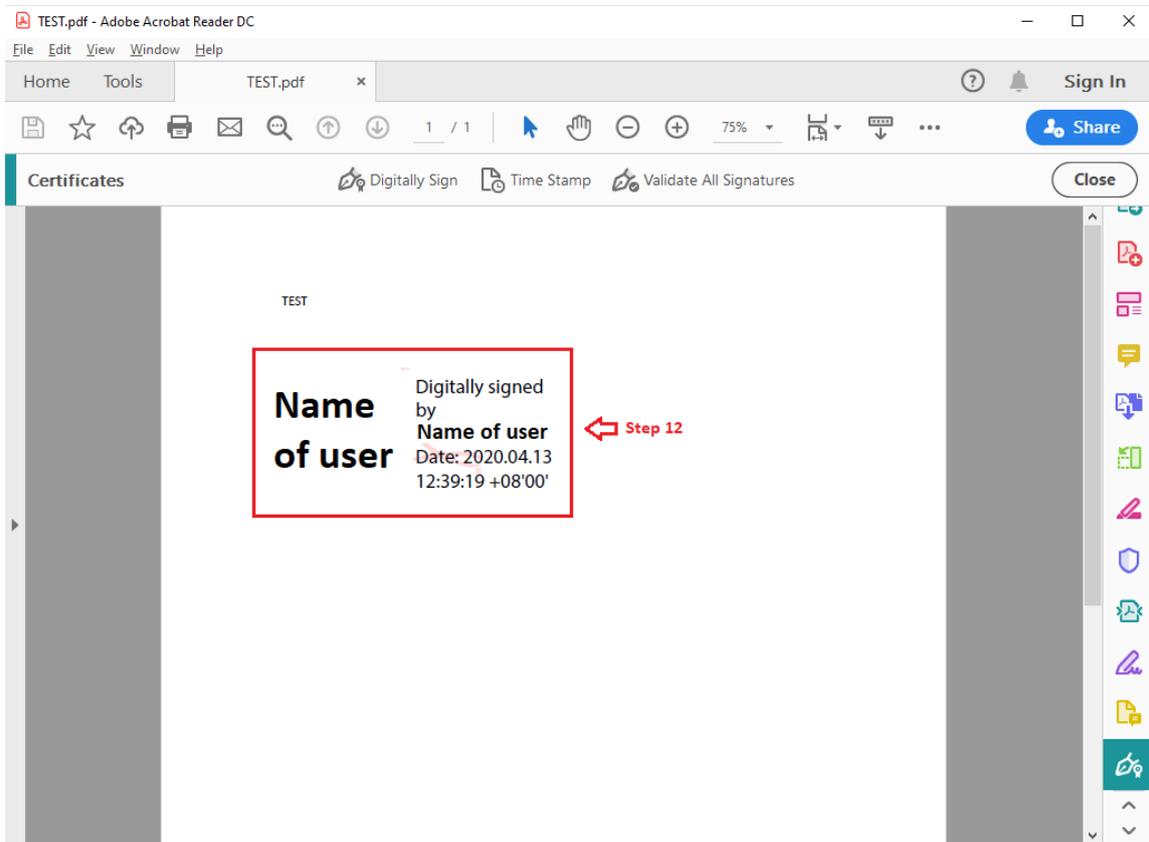
- **STEP 10**  
A pop up window will appear from 'SafeNet Authentication Client Tools - Token Logon'. Enter Token Password



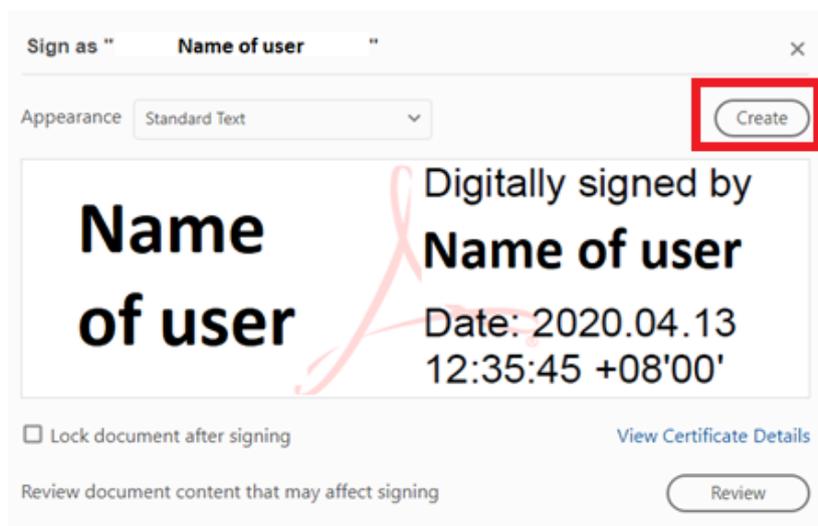
- **STEP 11**  
Click 'OK' to proceed

▪ **STEP 12**

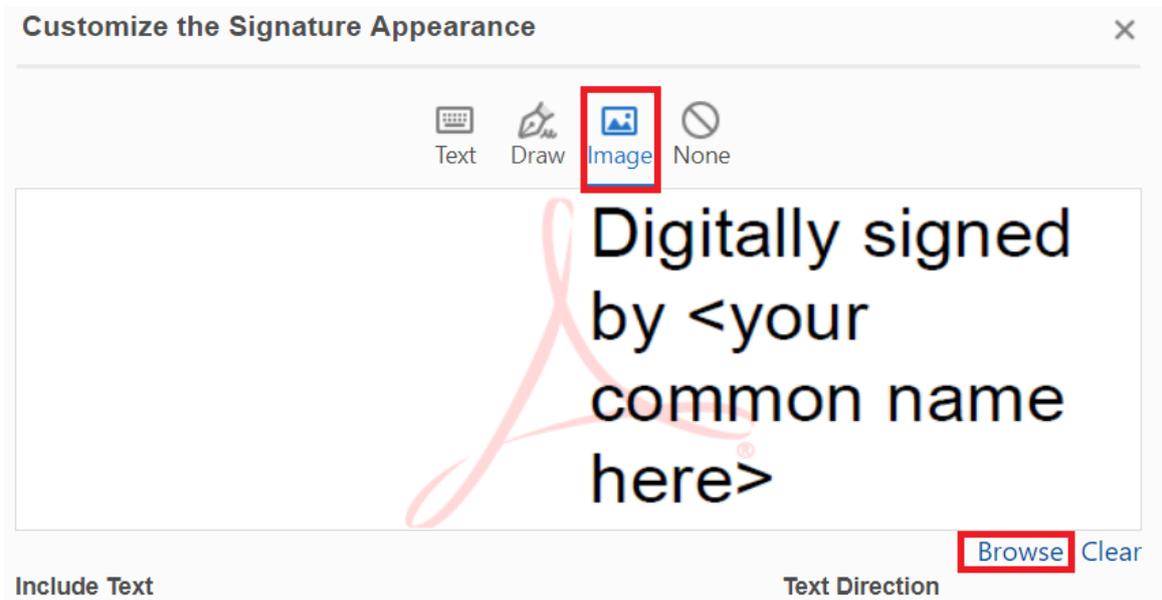
Your digital signature will be reflected in the PDF document after being signed successfully



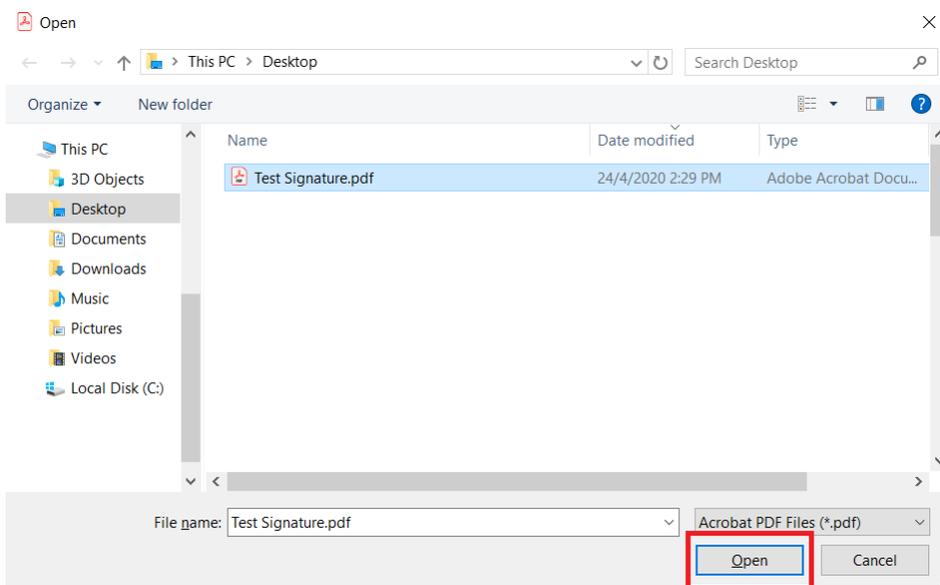
**\*\*ALTERNATE STEP:** If you need an image of the digital signature you can create one



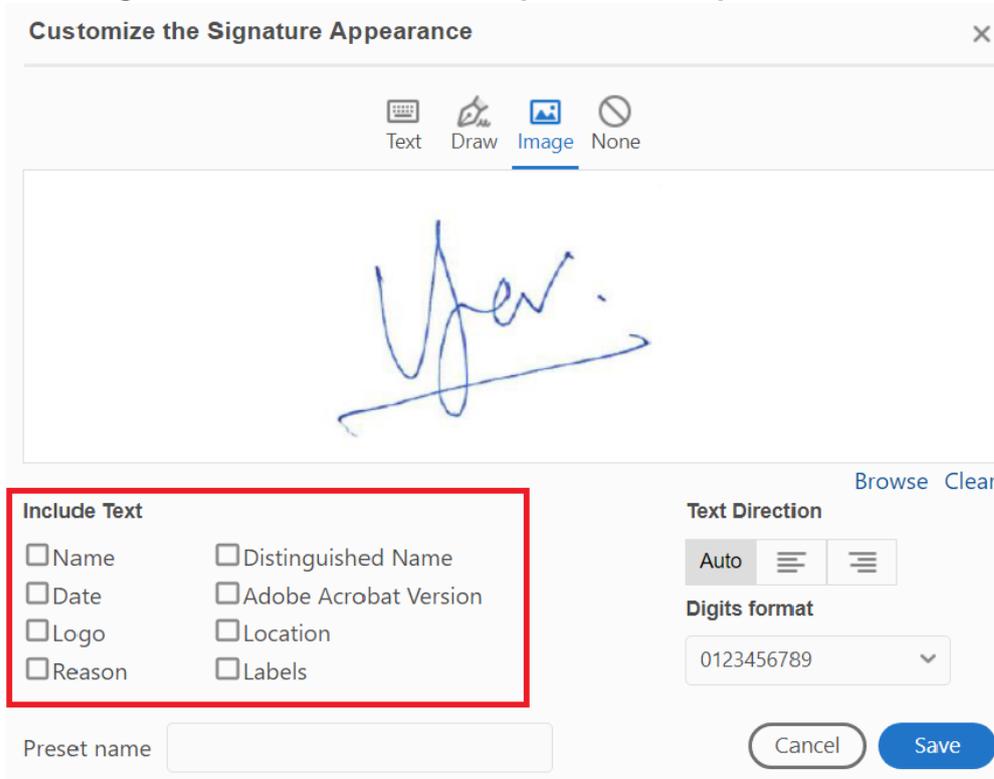
I. Select Image and click Browse



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

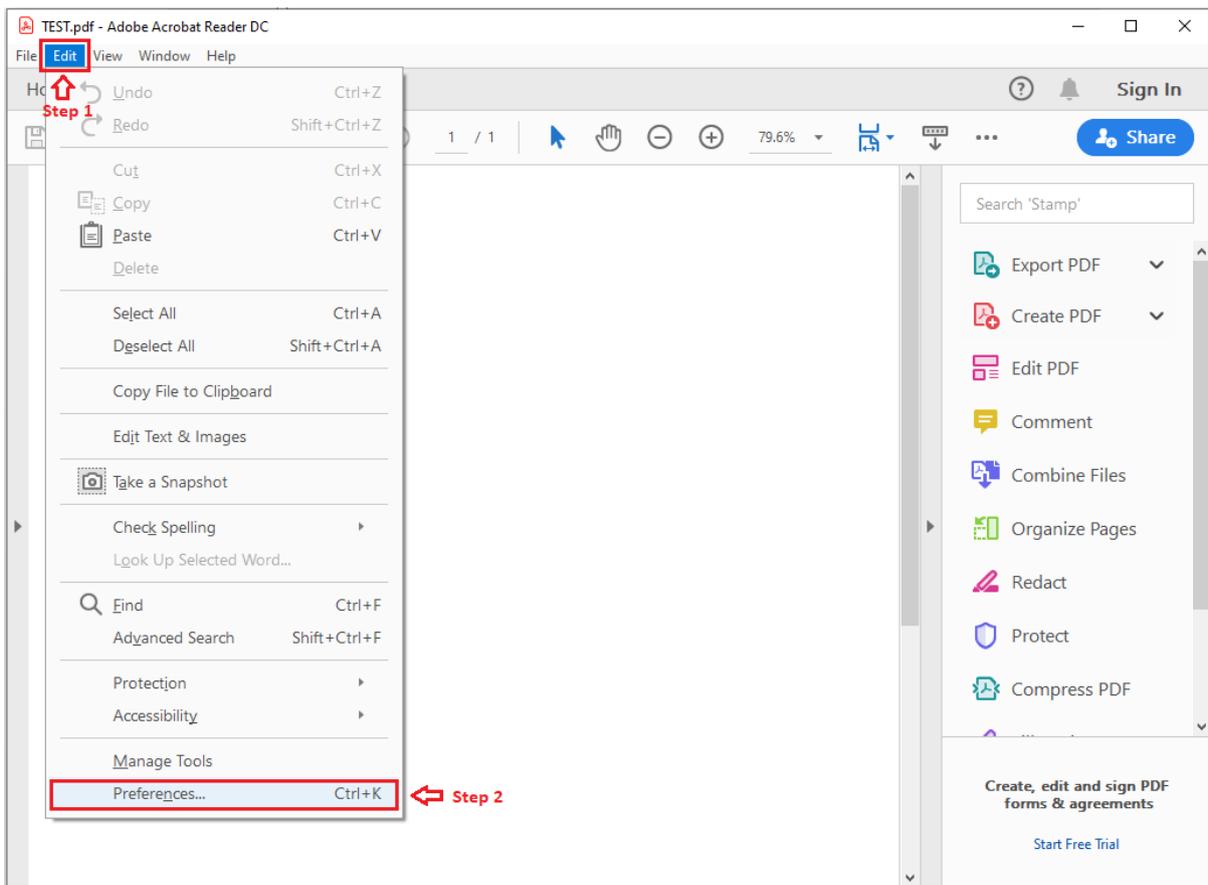


V. Signed with image



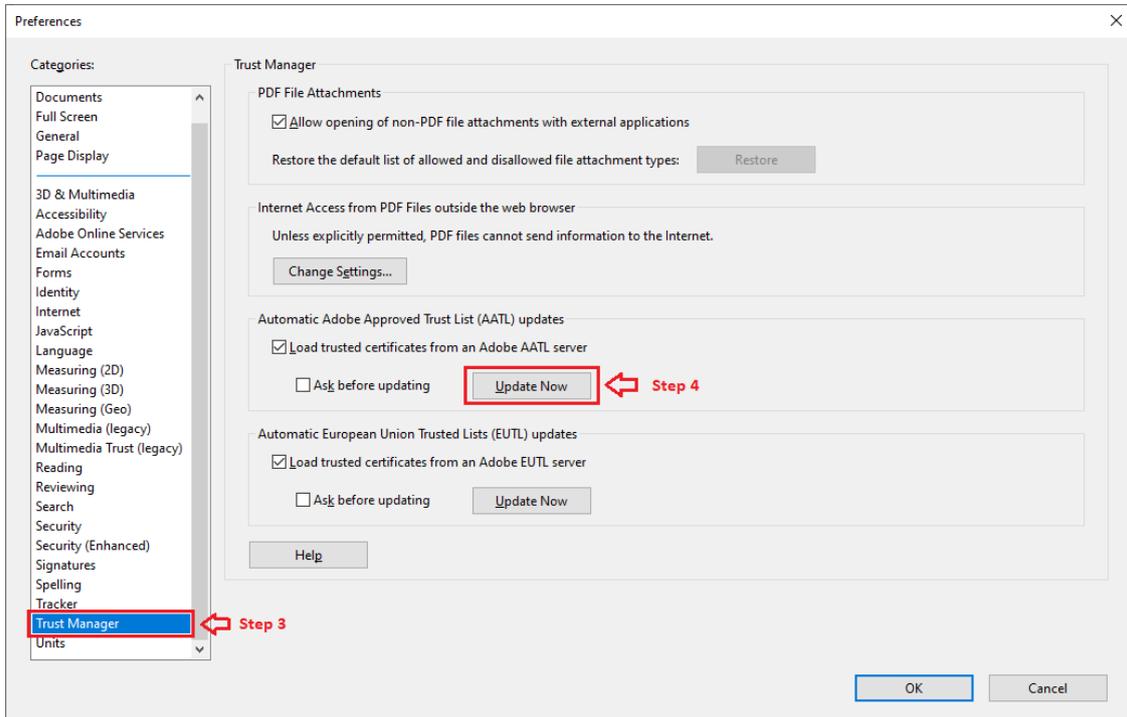
## 7. How To Ensure Digital Signature is Automatically Trusted (AATL)

- **STEP 1**  
Open any PDF Document  
Click on the 'Edit'
- **STEP 2**  
Click on 'Preferences...'

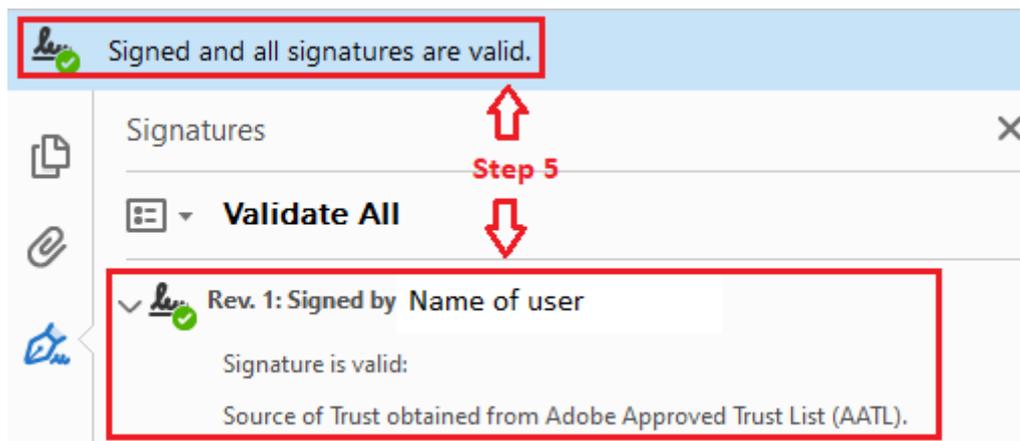


- **STEP 3**  
Select Trust Manager

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

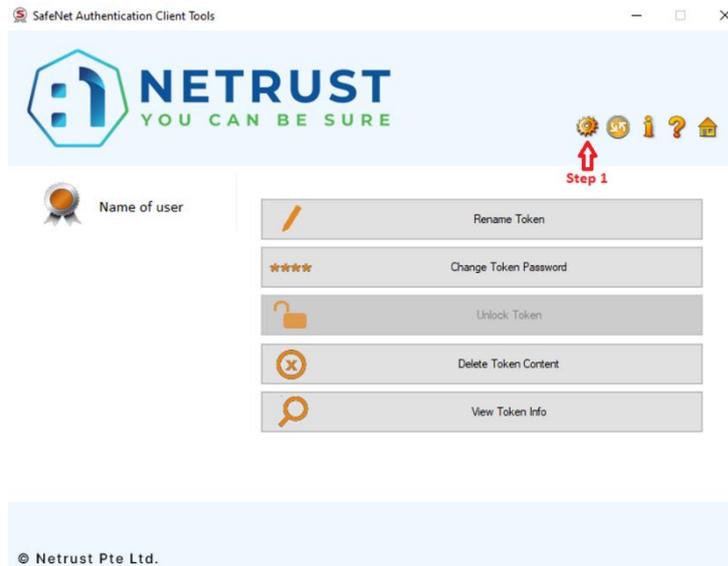


- STEP 5**  
 After updating the AATL updates, you'll notice that your digital signature is trusted automatically when you see the green tick (as per below)

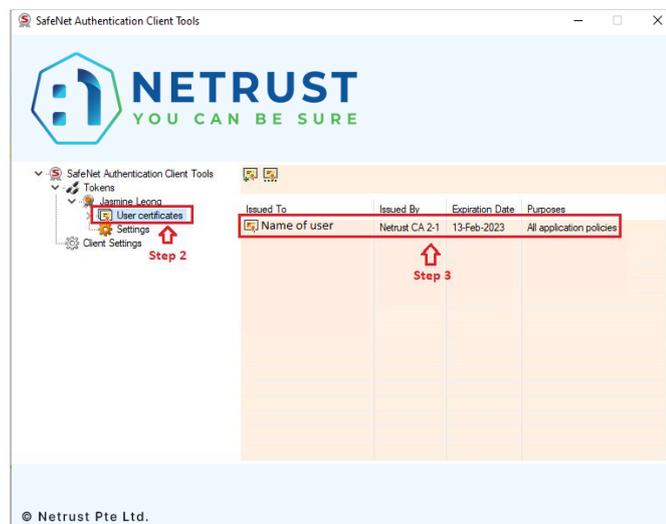


## 8. How To Check Certificate Details on eToken

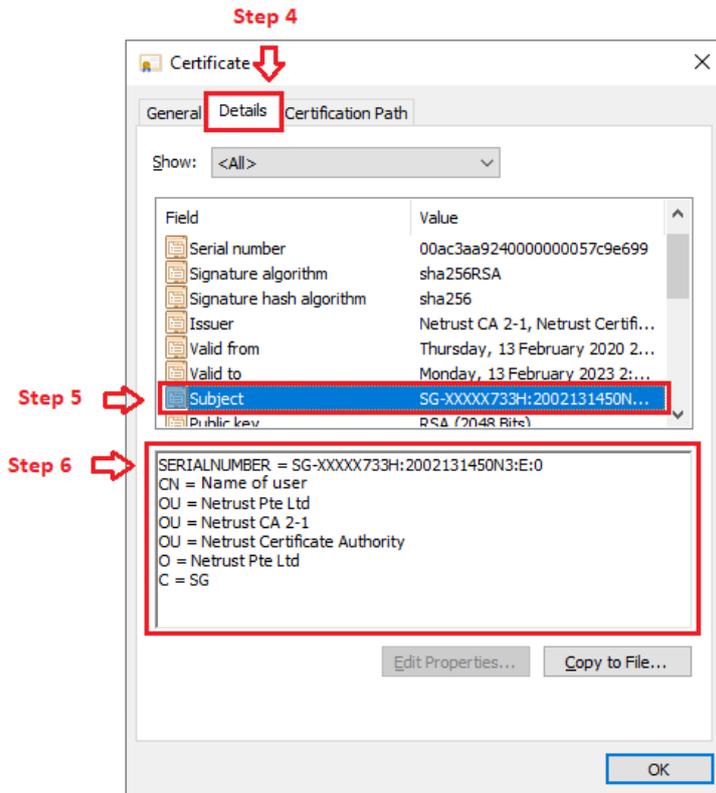
- **STEP 1**  
Open SafeNet Authentication Client Tools  
Click on the Advanced View icon



- **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



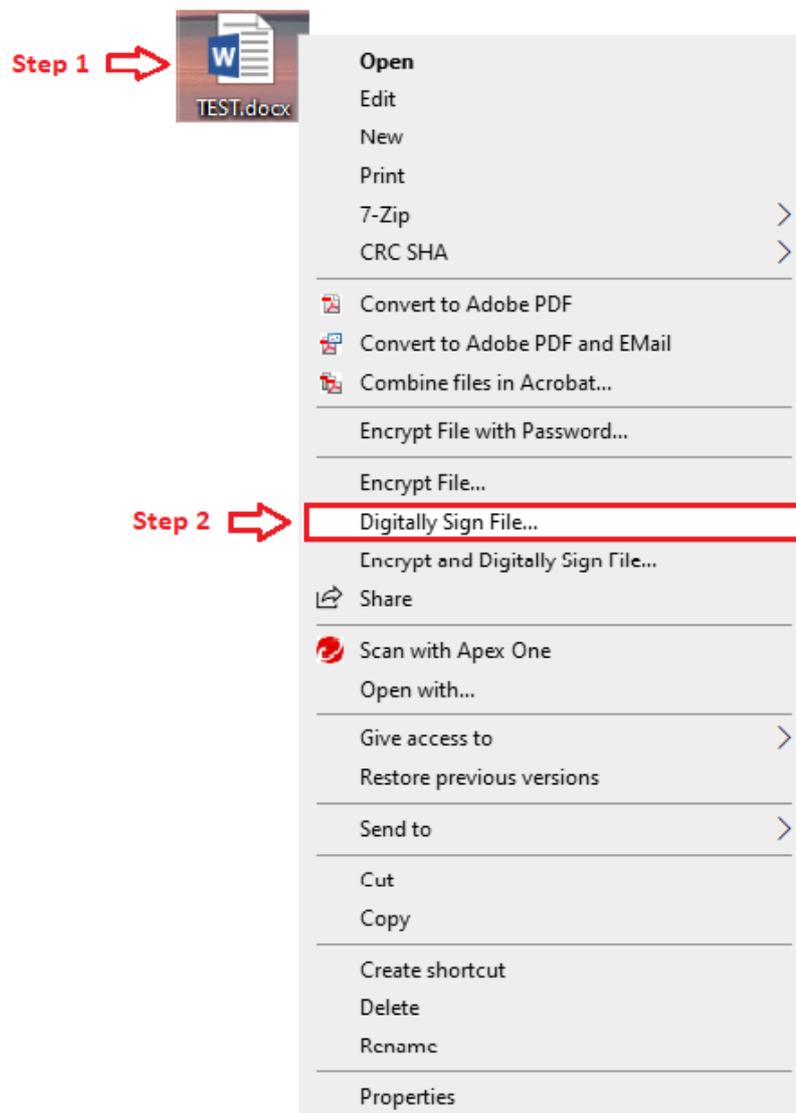
## 9. How To Digitally Sign/Encrypt Files Using Entrust Intelligence Security Provider (EESP) using Microsoft Office Applications

### 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



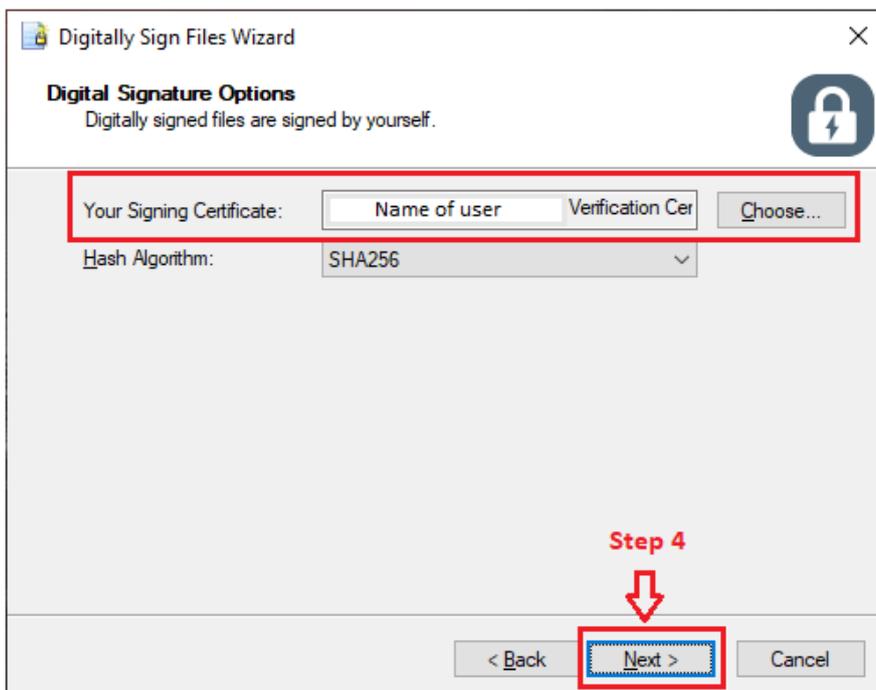
▪ **STEP 3**

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



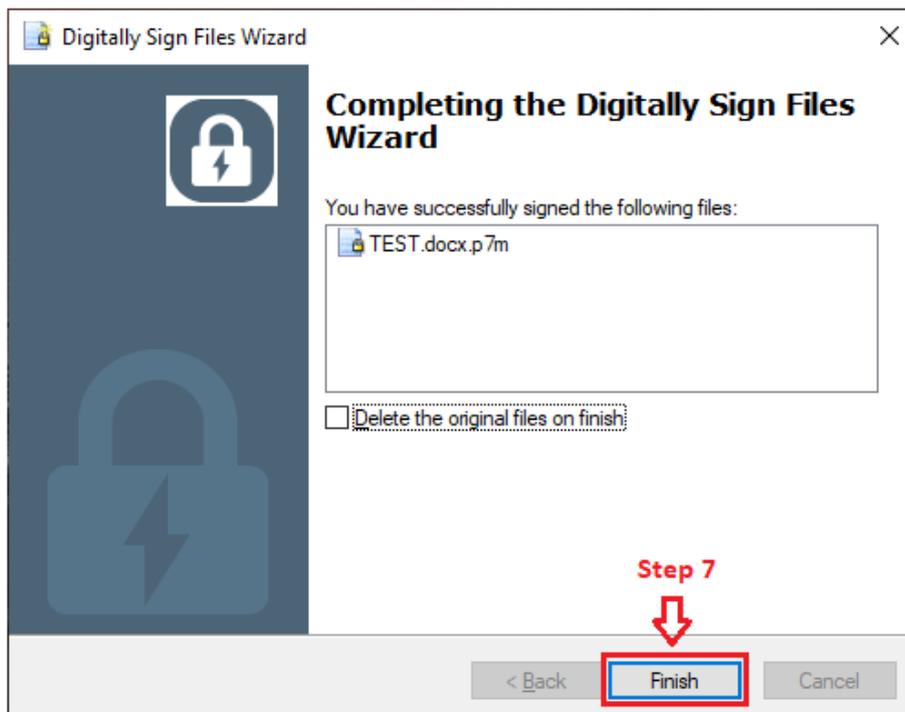
▪ **STEP 6**

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

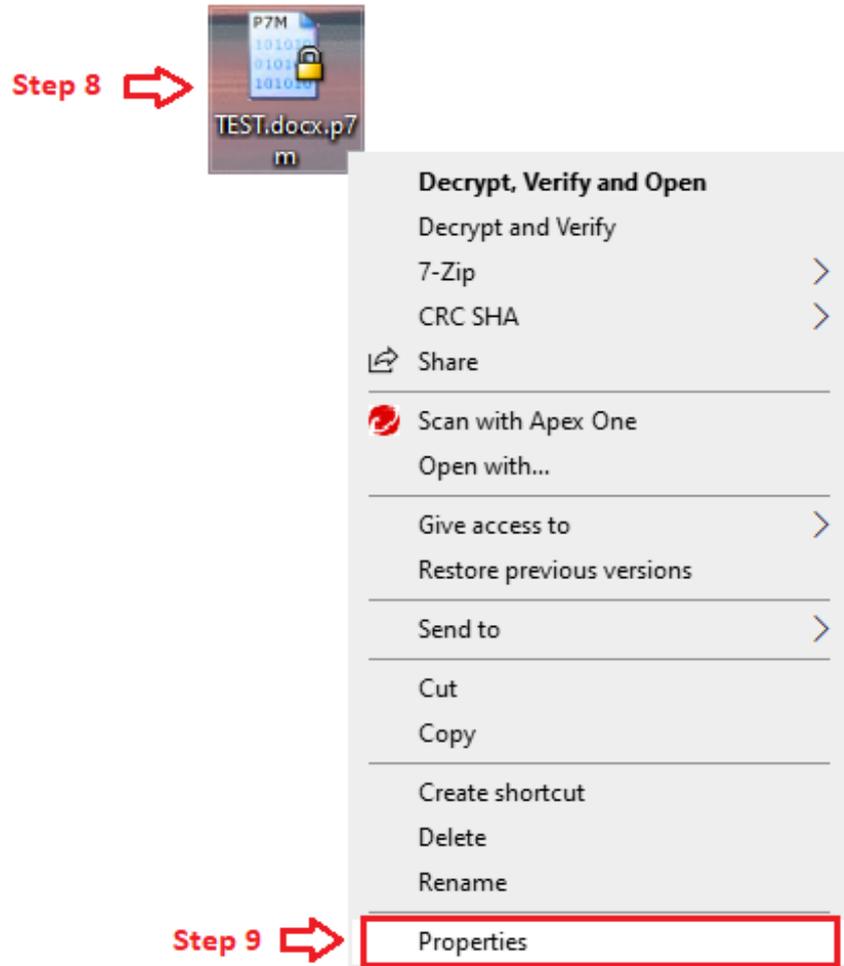


- **STEP 8**

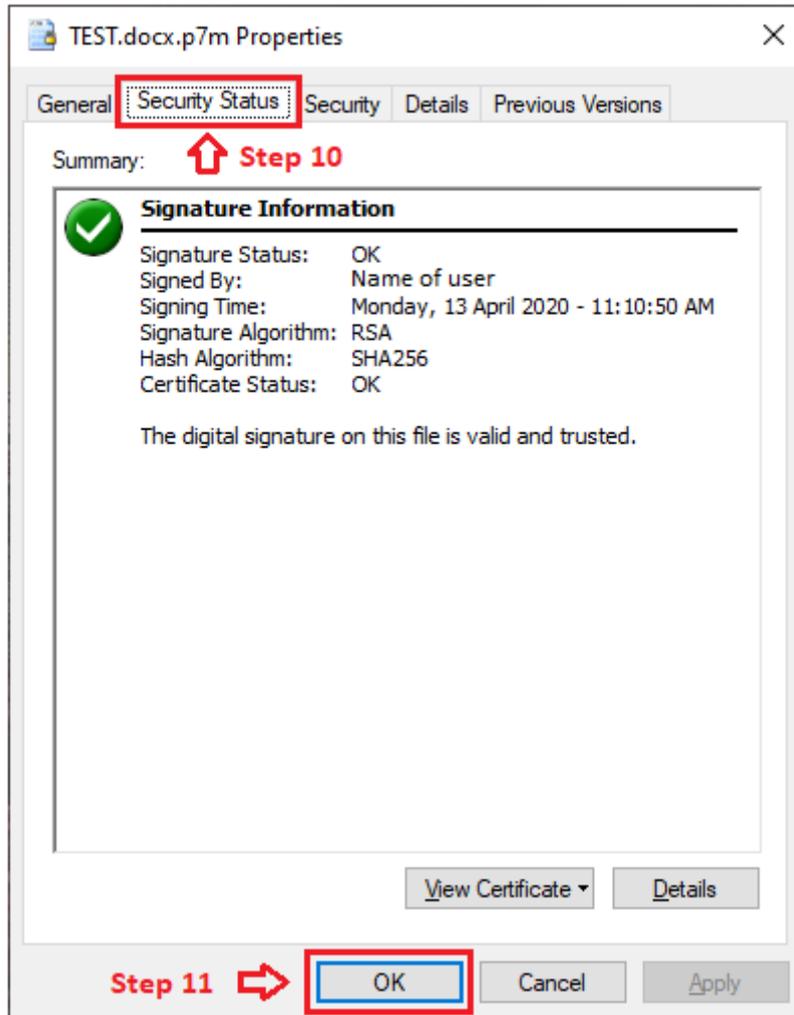
The digitally signed file will be saved automatically in the file location as a .p7m file extension  
*NOTE: EESP will be required to view the file*

- **STEP 9**

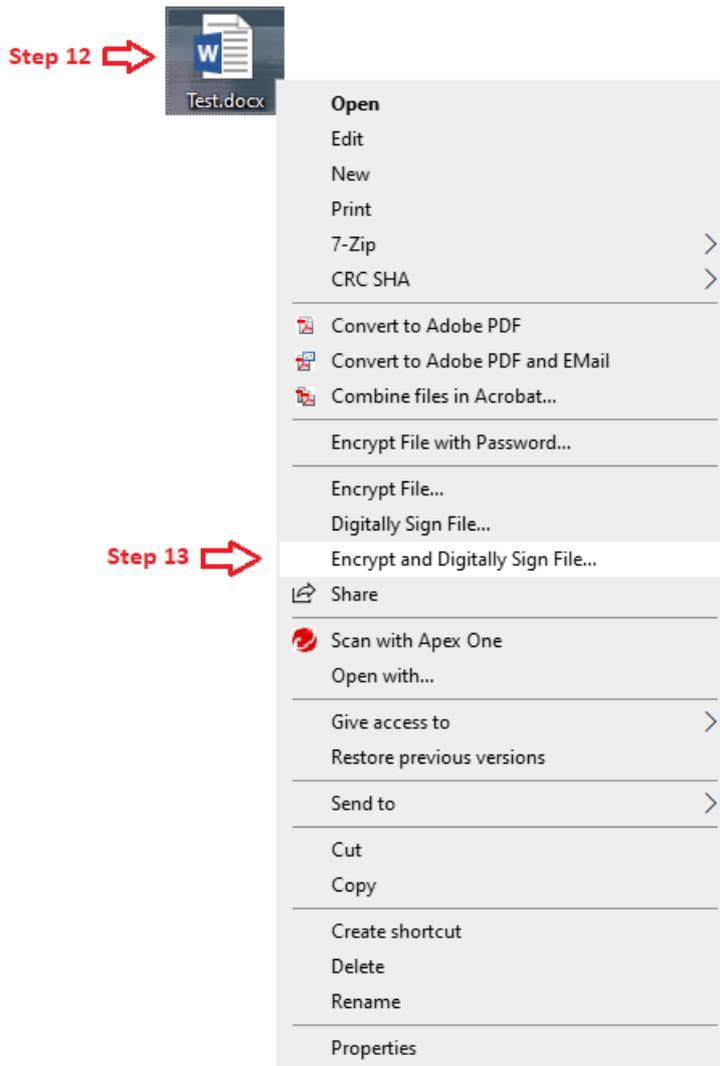
Right click on the file and select 'Properties' to check on signature information



- **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



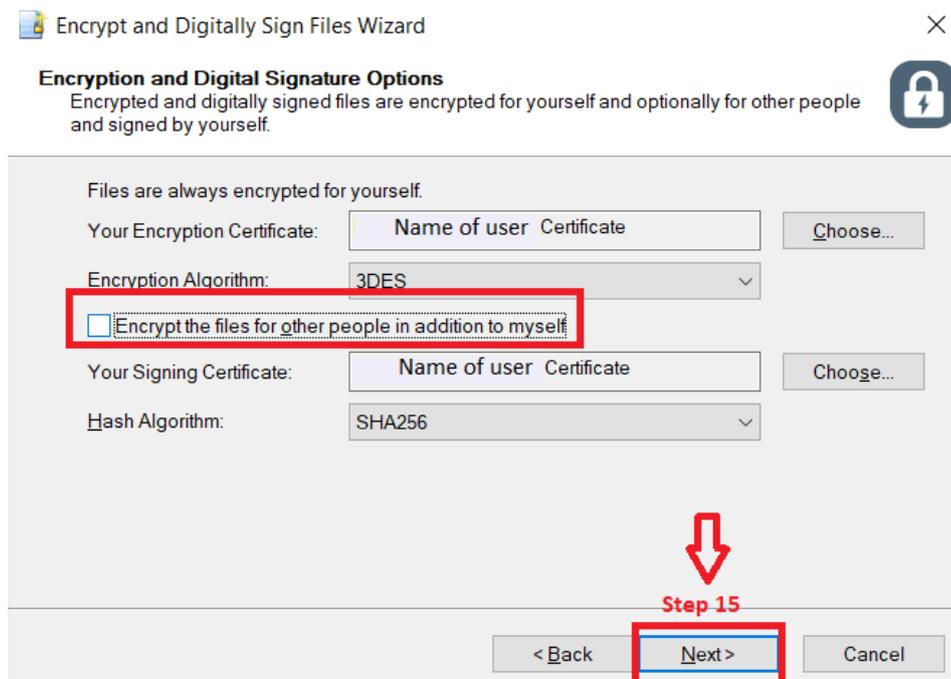
▪ **STEP 14**

A pop up window will appear from ‘Encrypt and Digitally Sign Files Wizard’  
Click on ‘Next’ to proceed



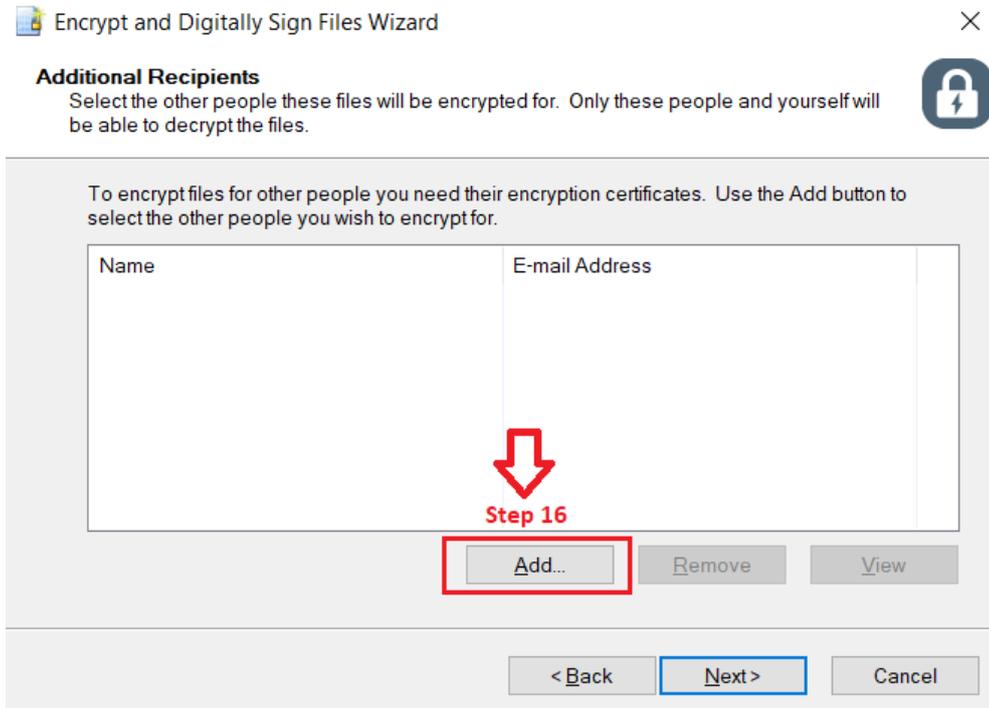
▪ **STEP 15**

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



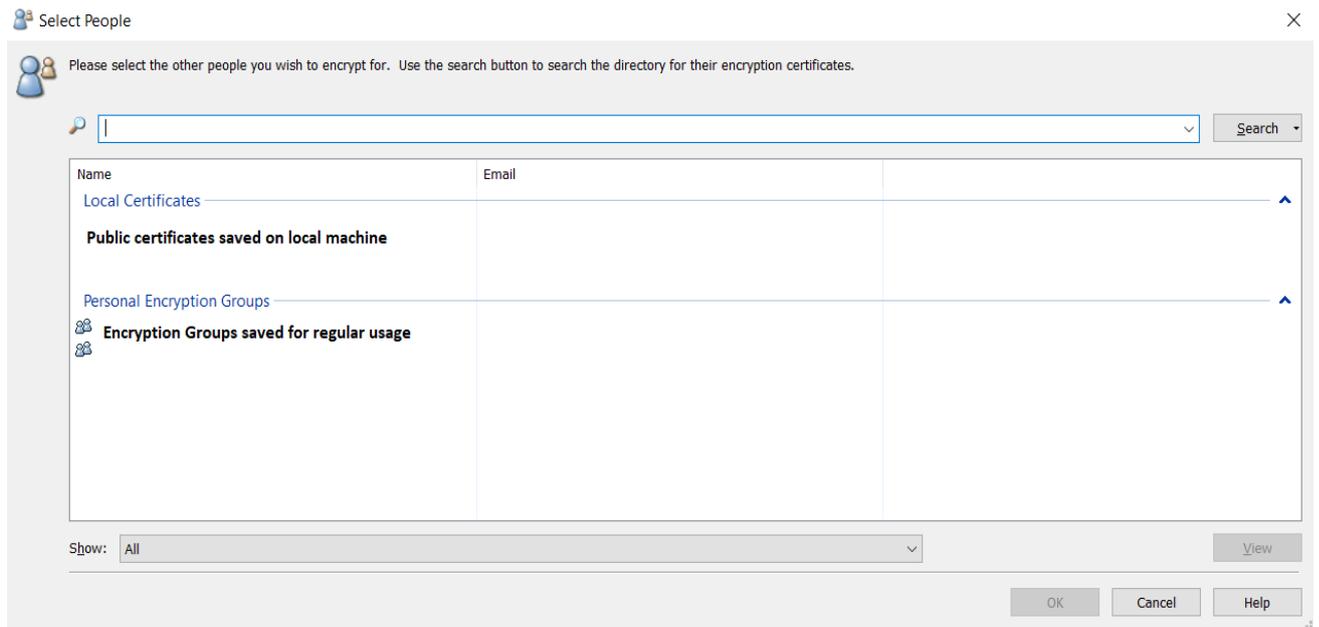
▪ **STEP 16**

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



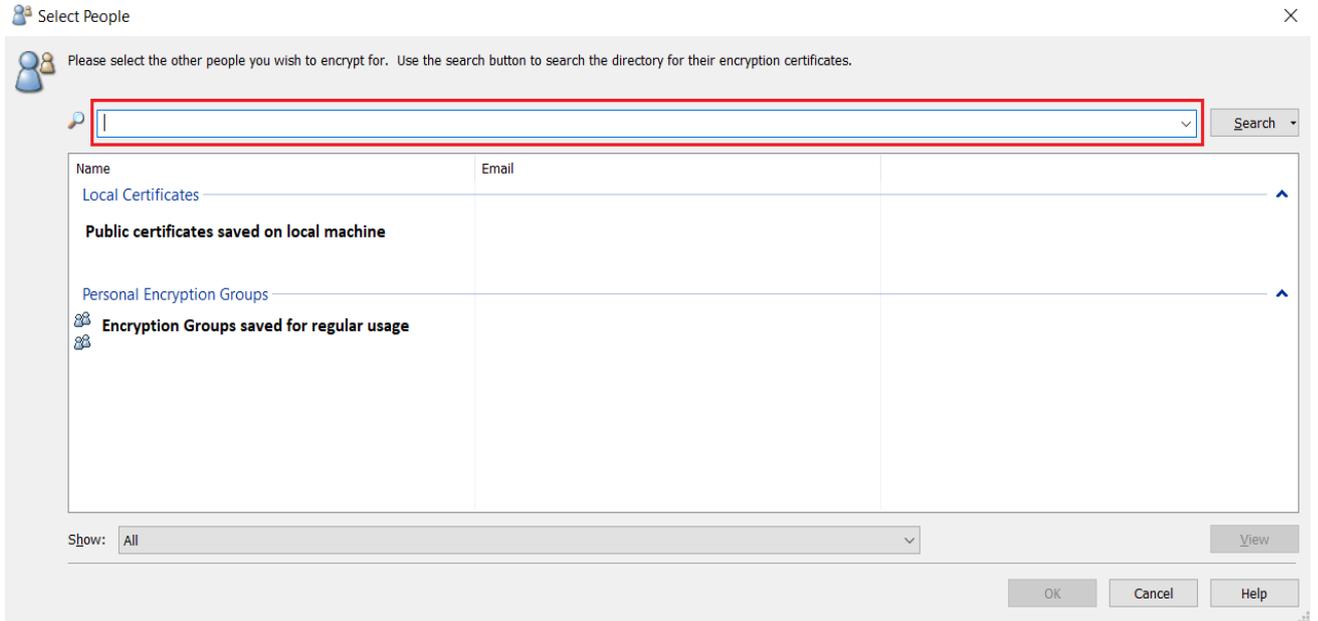
▪ **STEP 17**

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



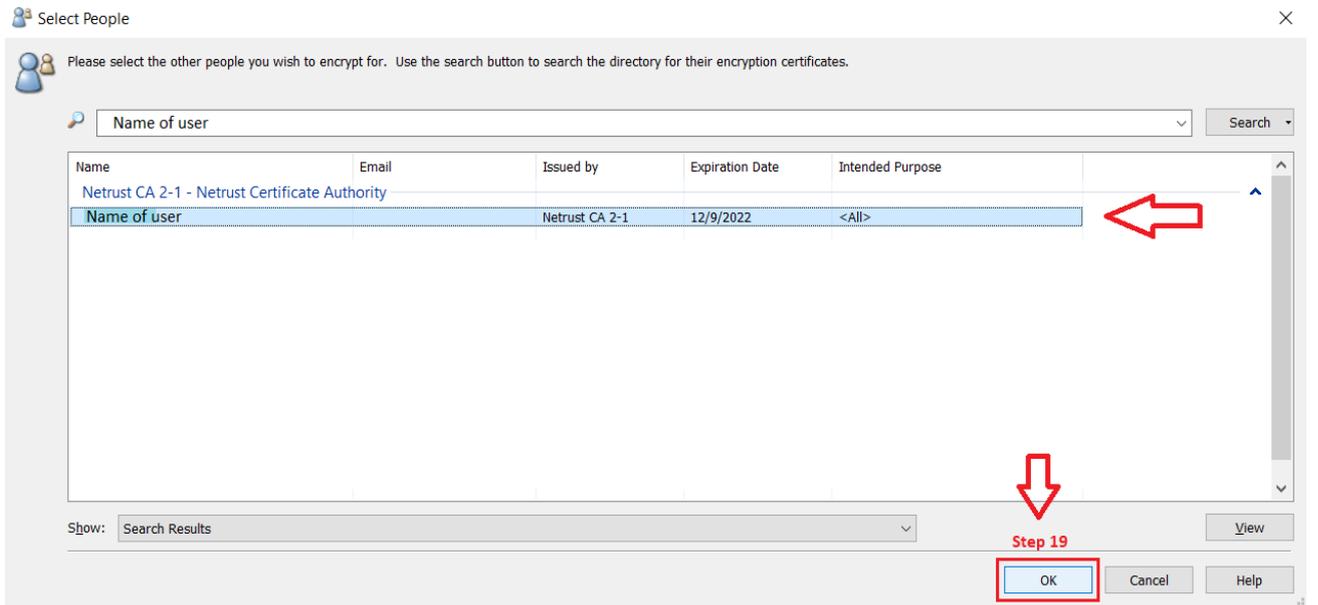
▪ **STEP 18**

Click on 'search' after typing in name/email of user to encrypt file to



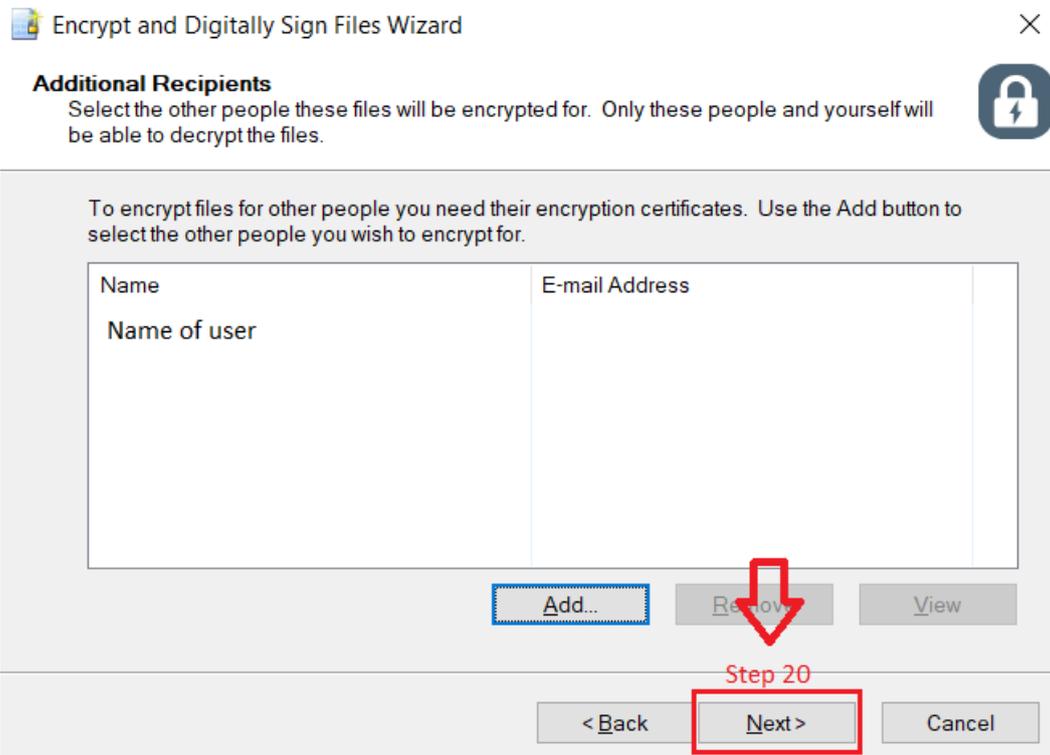
▪ **STEP 19**

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



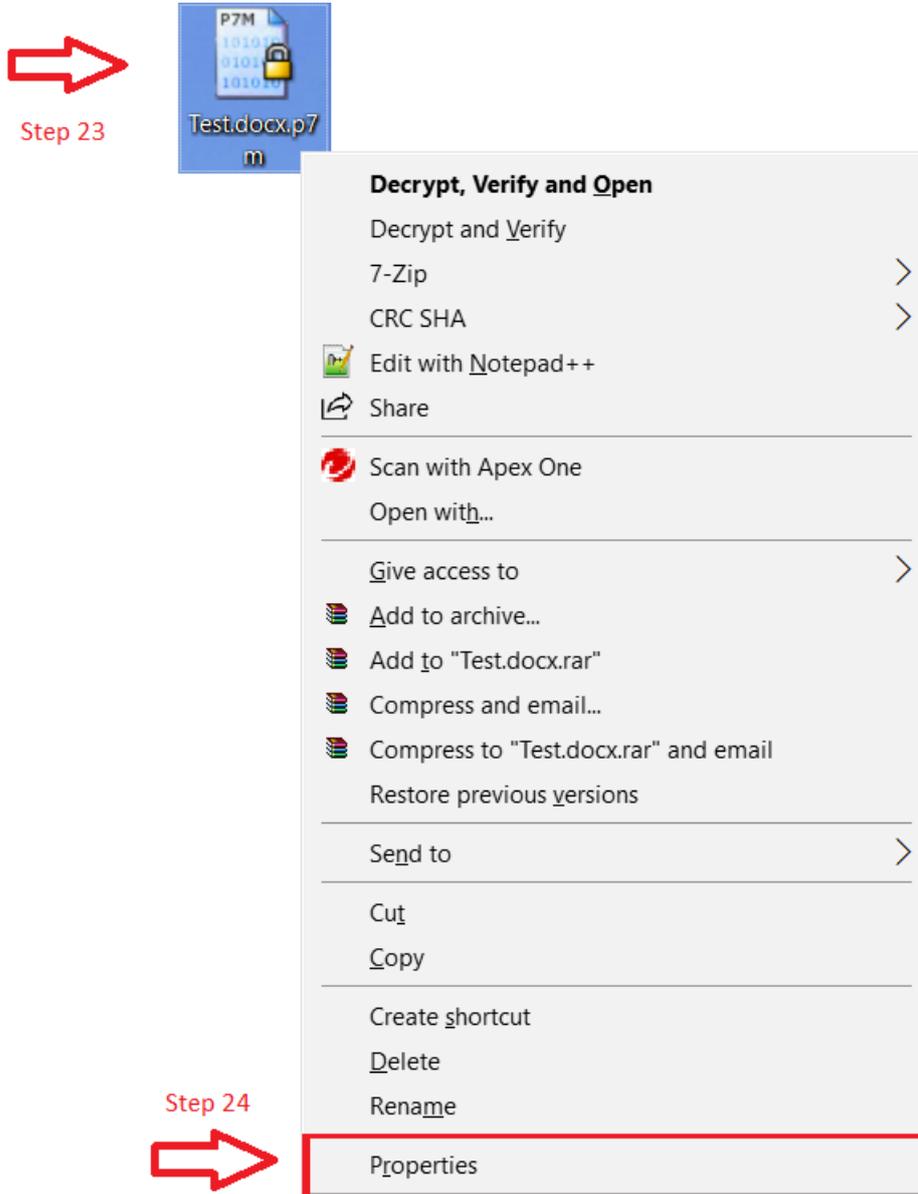
▪ **STEP 23**

The encrypted and digitally signed file will be saved automatically in the same file location as .p7m extension

**NOTE: EESP will be required to view the file**

▪ **STEP 24**

Right click on the file and select 'Properties' to check on signature information

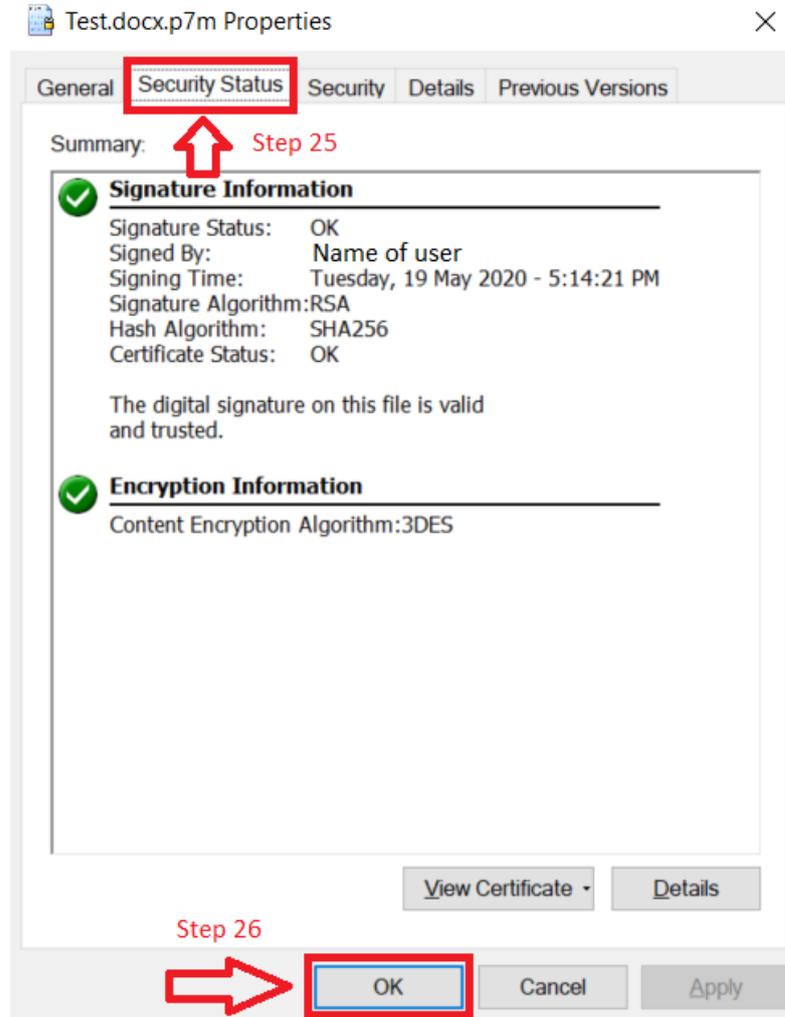


▪ **STEP 25**

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**

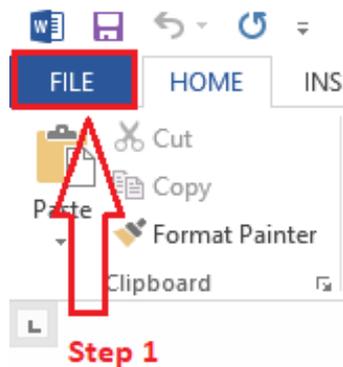
Click 'OK' to proceed



## 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'

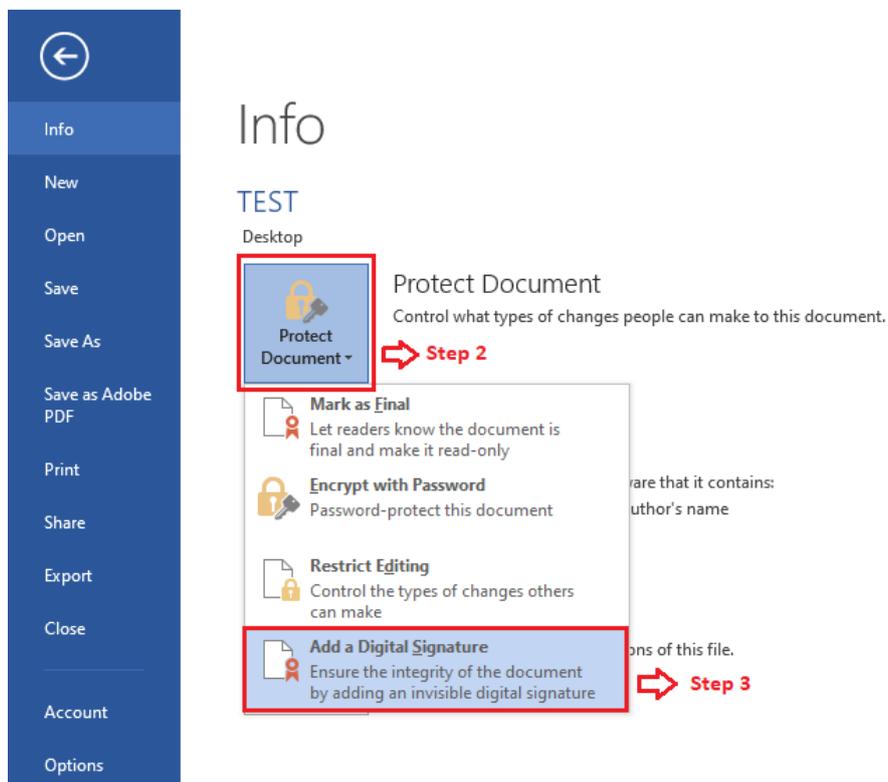


- **STEP 2**

Under Info, click on 'Protect Document'

- **STEP 3**

Select 'Add a Digital Signature'

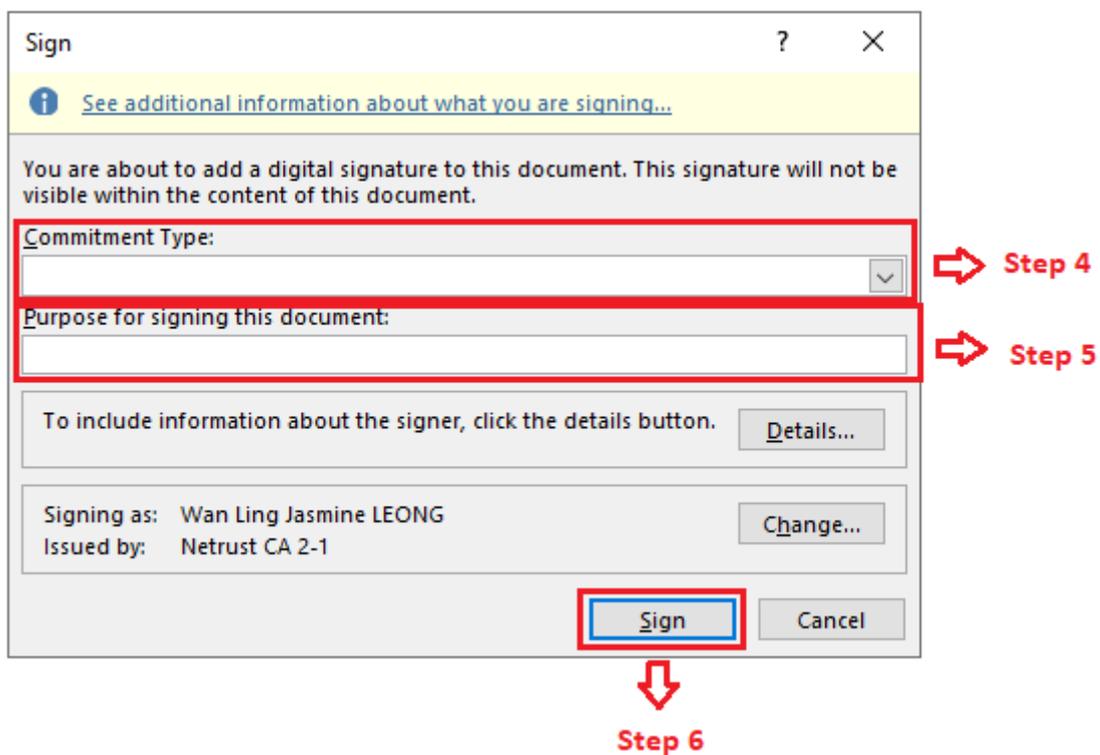


- **STEP 4**  
Select a Commitment Type from the drop down list



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

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

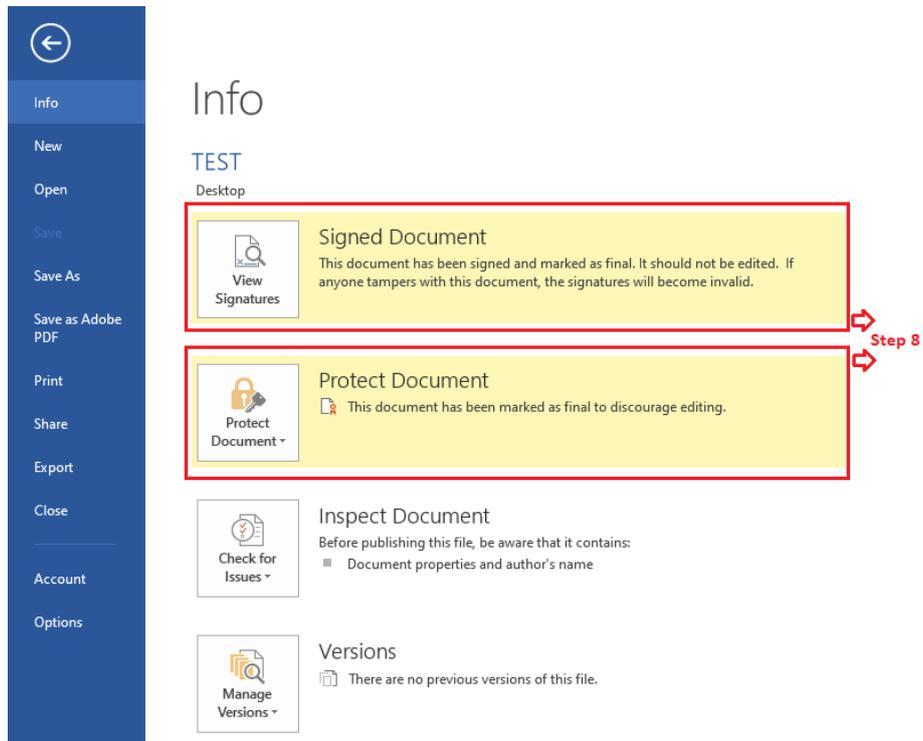


- **STEP 7**  
Click on 'OK' to proceed



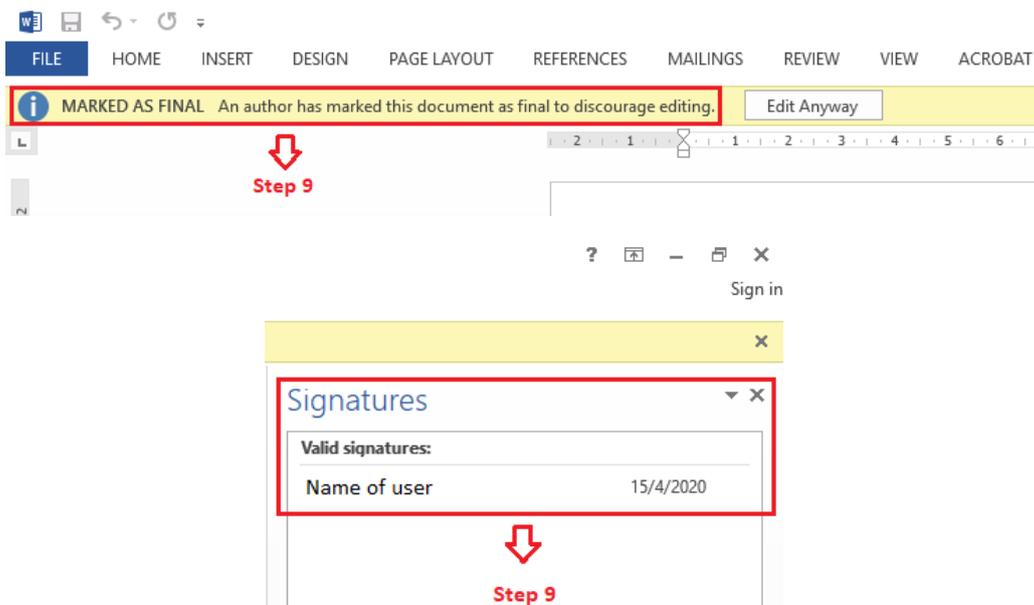
▪ **STEP 8**

After digitally signing successfully, you will notice that the document is signed and protected



▪ **STEP 9**

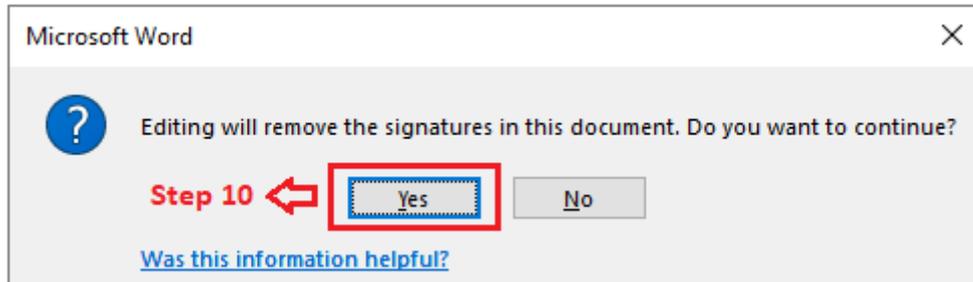
Within the document, you will see the following information reflected after it is sign successfully



- **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.**

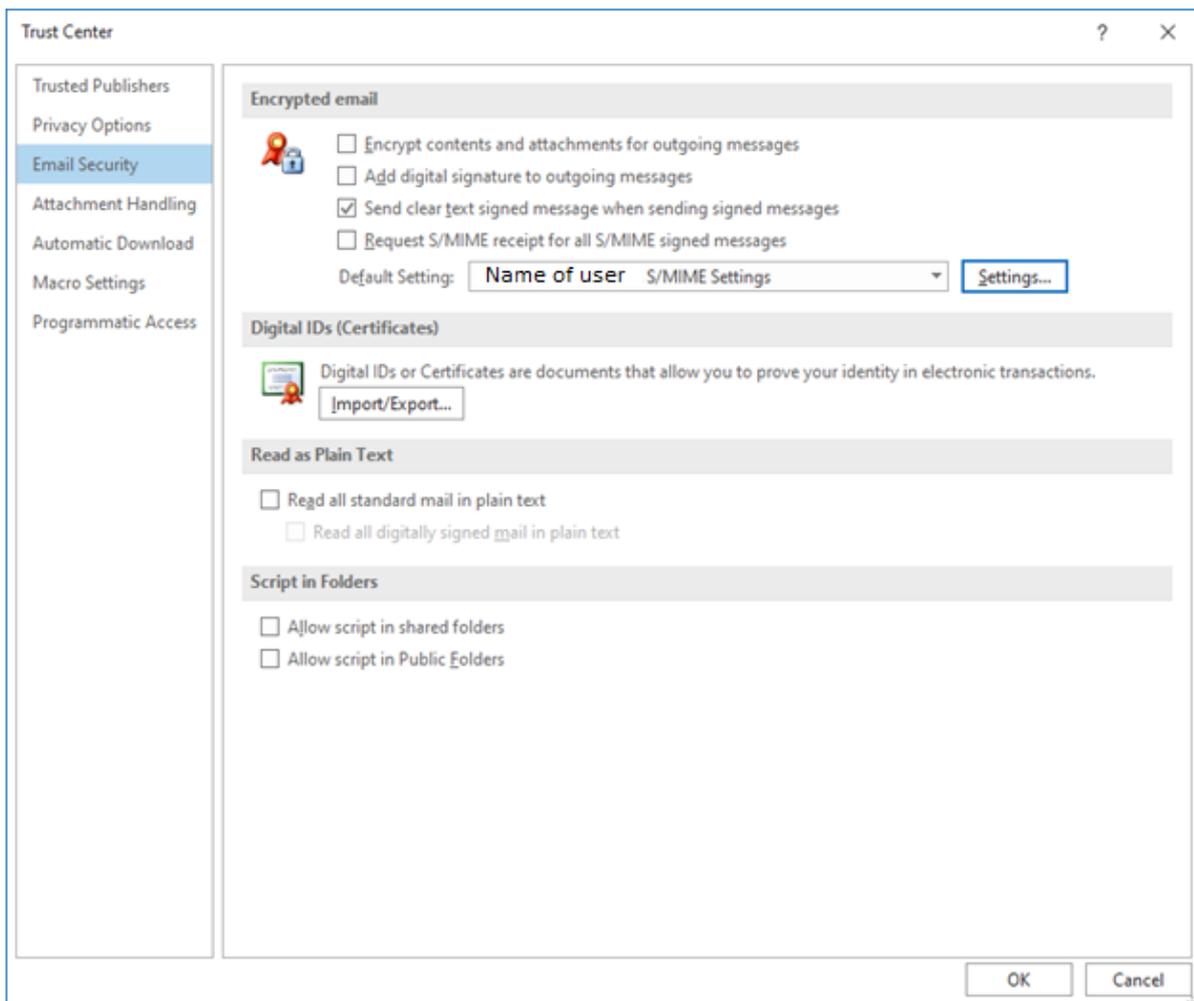


## 11. Configuration of Secure Email on Microsoft Outlook

### STEP 1

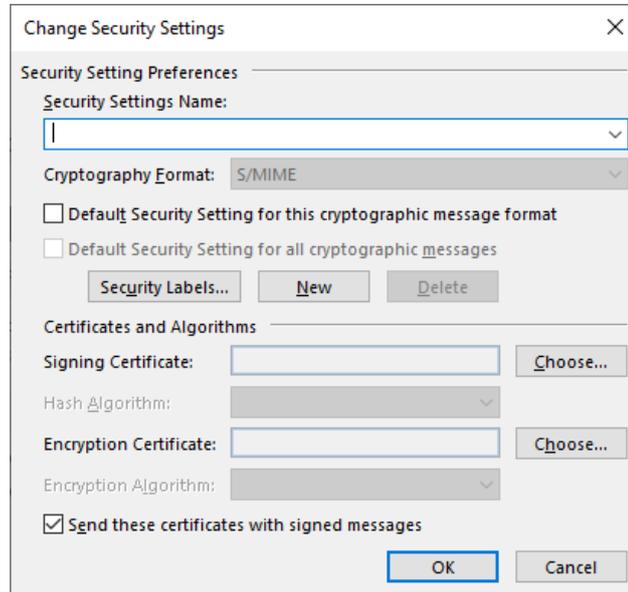
Upon installation of the certificate to configure the Outlook, refer to the STEPs below:

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



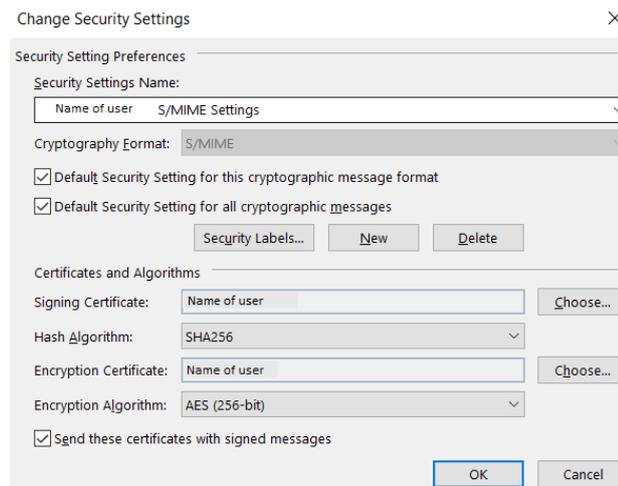
▪ **STEP 2**

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:

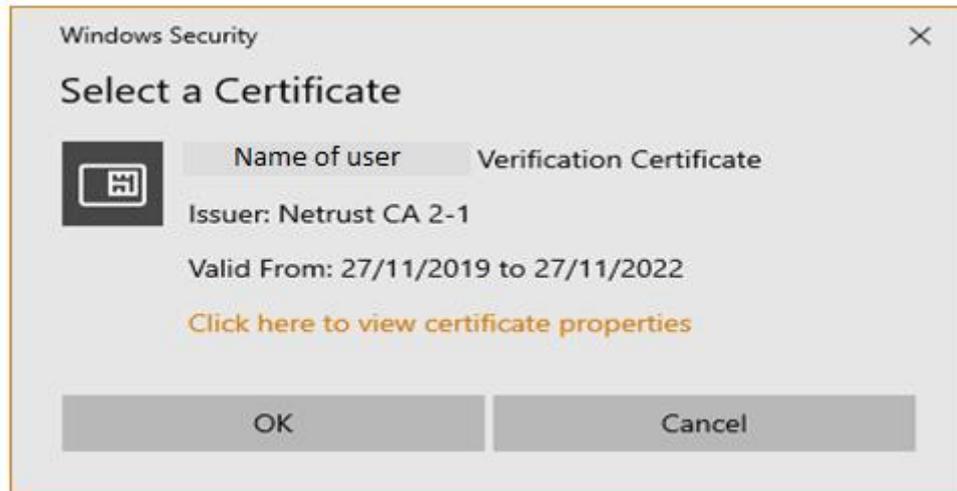
- Secure Message Format (type of e-mail)
- Digital Signature Settings
- Encryption Settings
- Security Setting Preferences (setting defaults)



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

- **STEP 3**

Then proceed to choose the Signing Certificate and Encryption Certificate



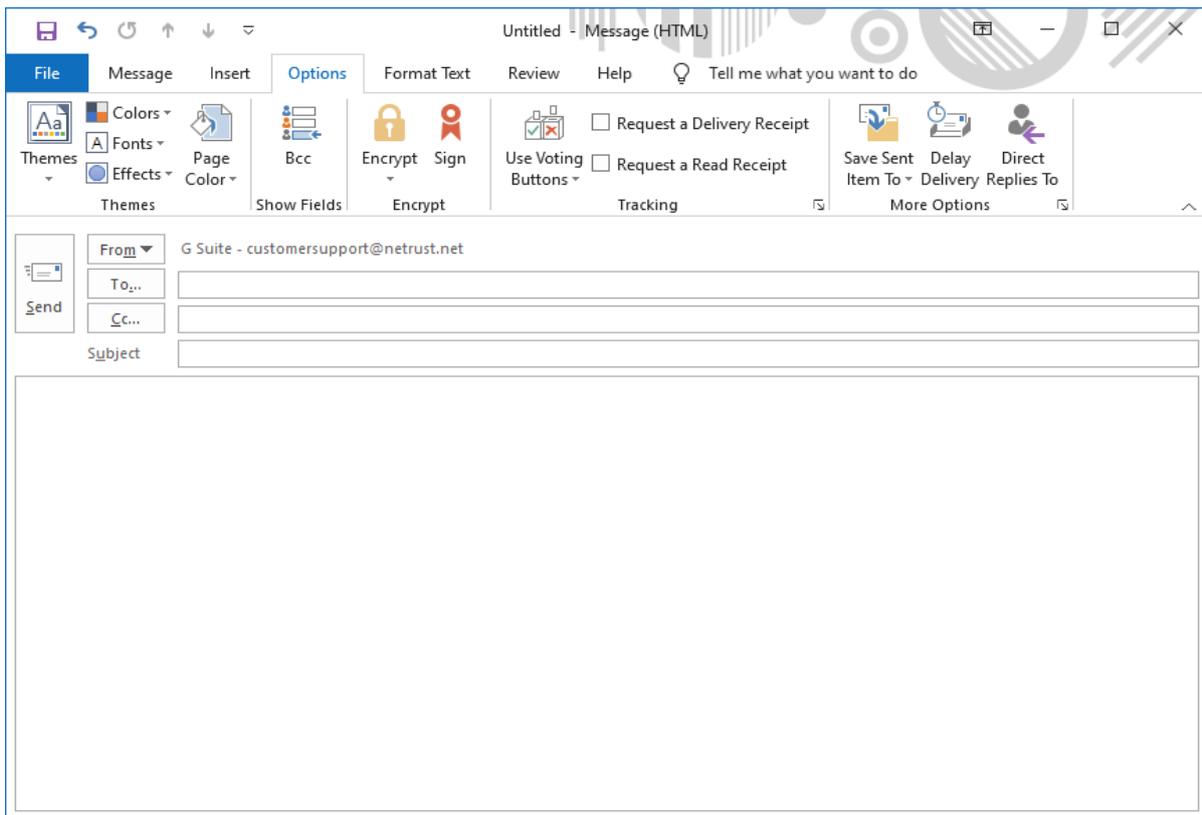
▪ **STEP 4**

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

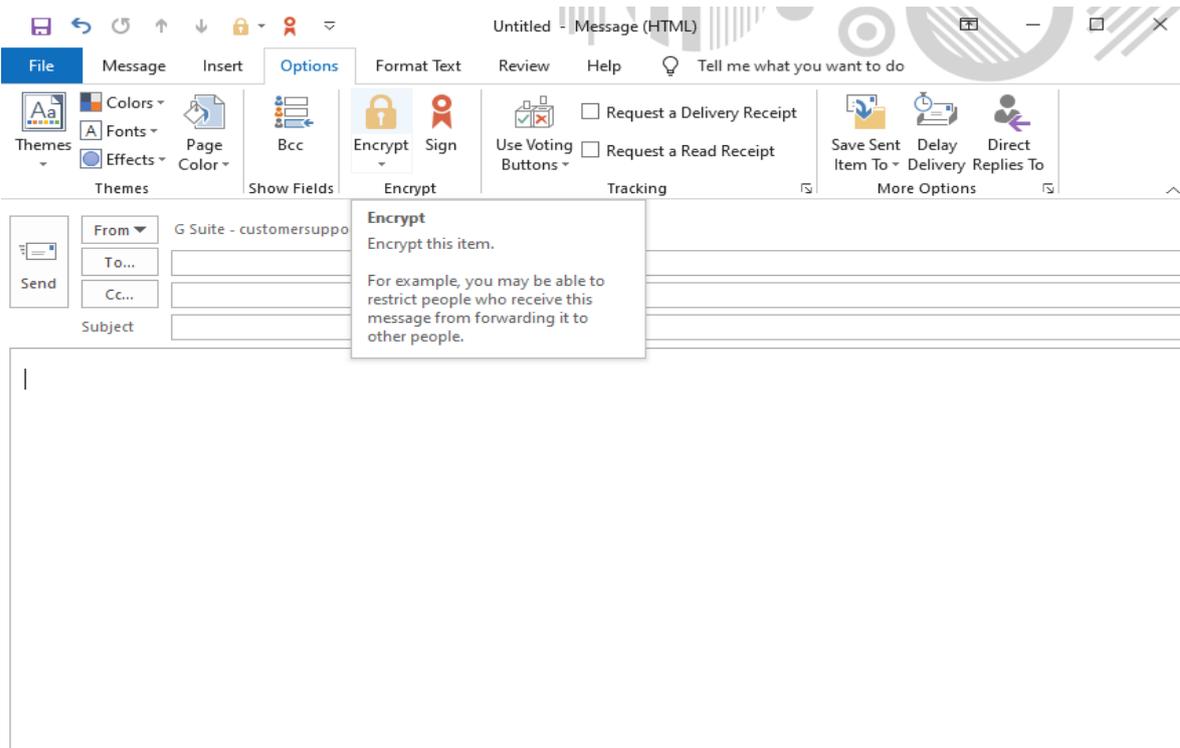
**Signing Icon**      **Encrypting Icon**



▪ **STEP 5**

Encrypting the e-mail messages with Outlook

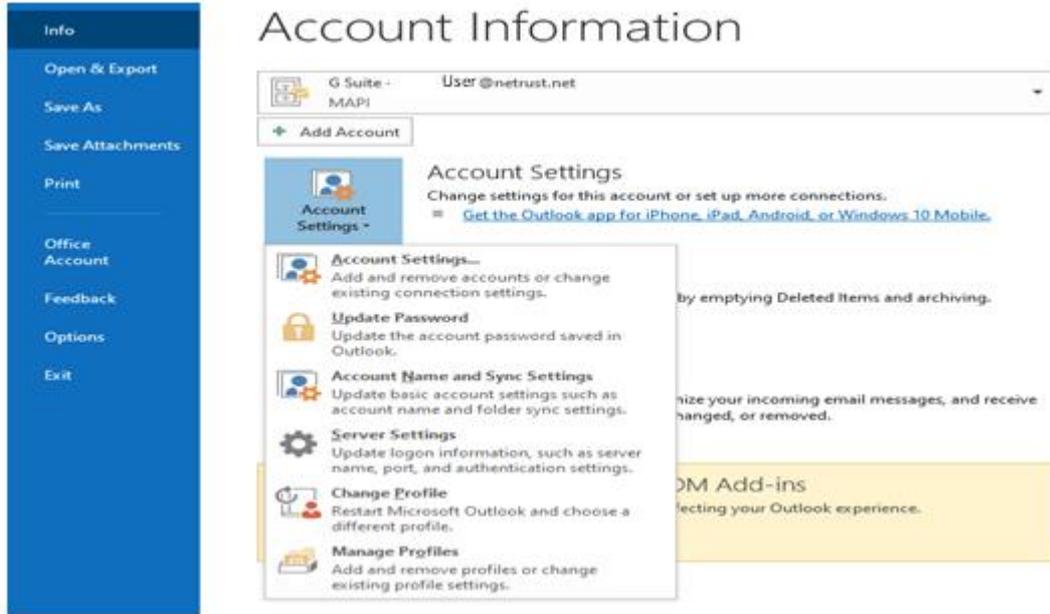
Signing a message does not affect the contents of the message in any way or protect the message from being intercepted and read by someone other than the intended recipient. To ensure that only the recipient can read a message, you must also encrypt the message.



▪ **STEP 6**

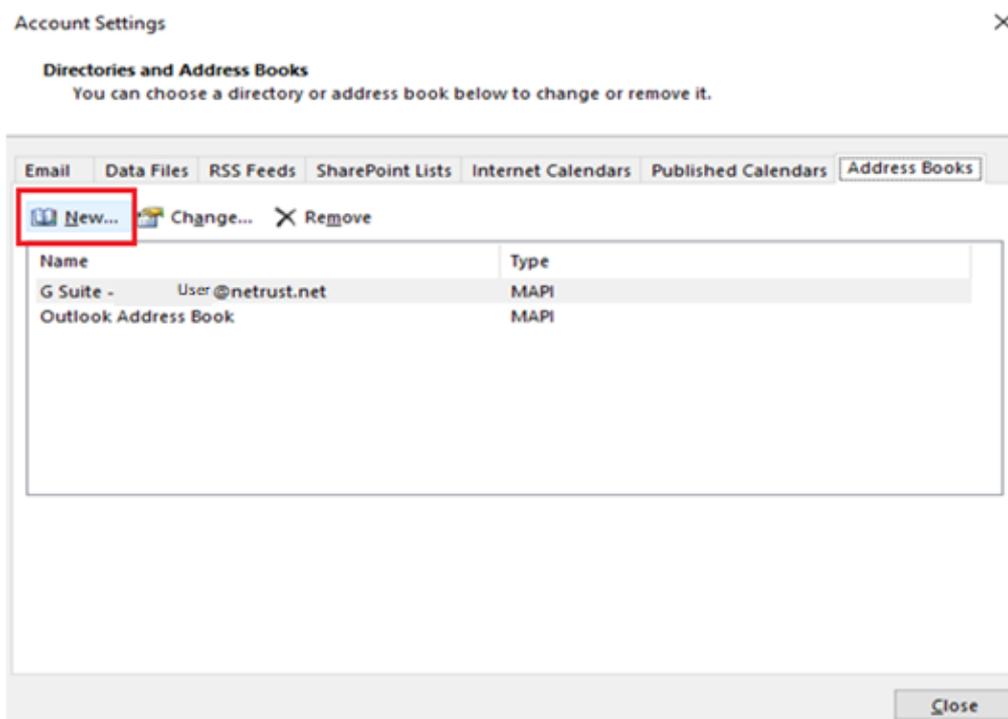
To encrypt your message, add the online directory of the certification authority (ldap21.netrust.net). To do so, follow the STEPs below:

Click on “Account Settings...”



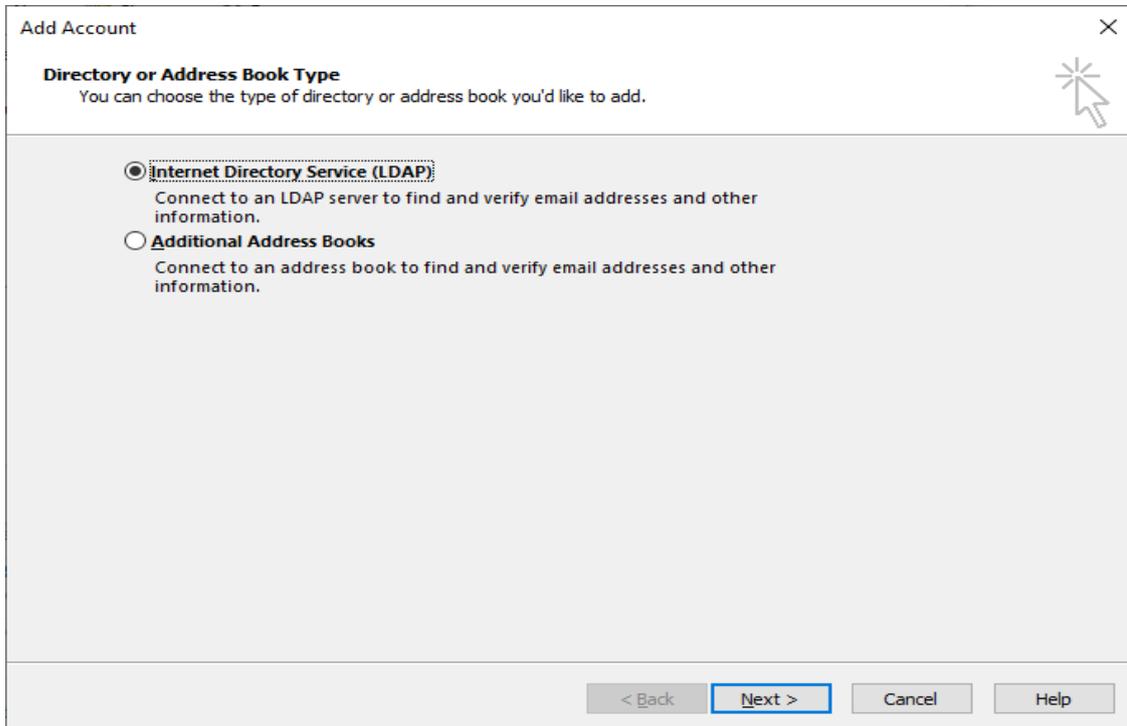
▪ **STEP 7**

Select “New” to add the server name

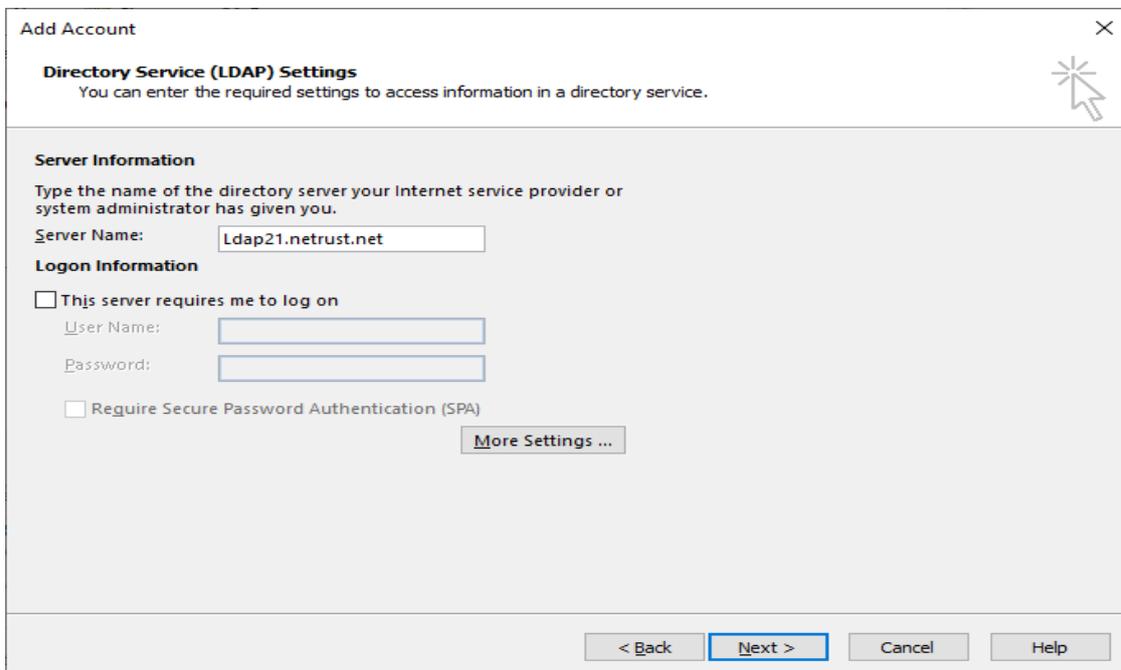


▪ **STEP 8**

Select "Internet Directory Service (LDAP)", click "Next"

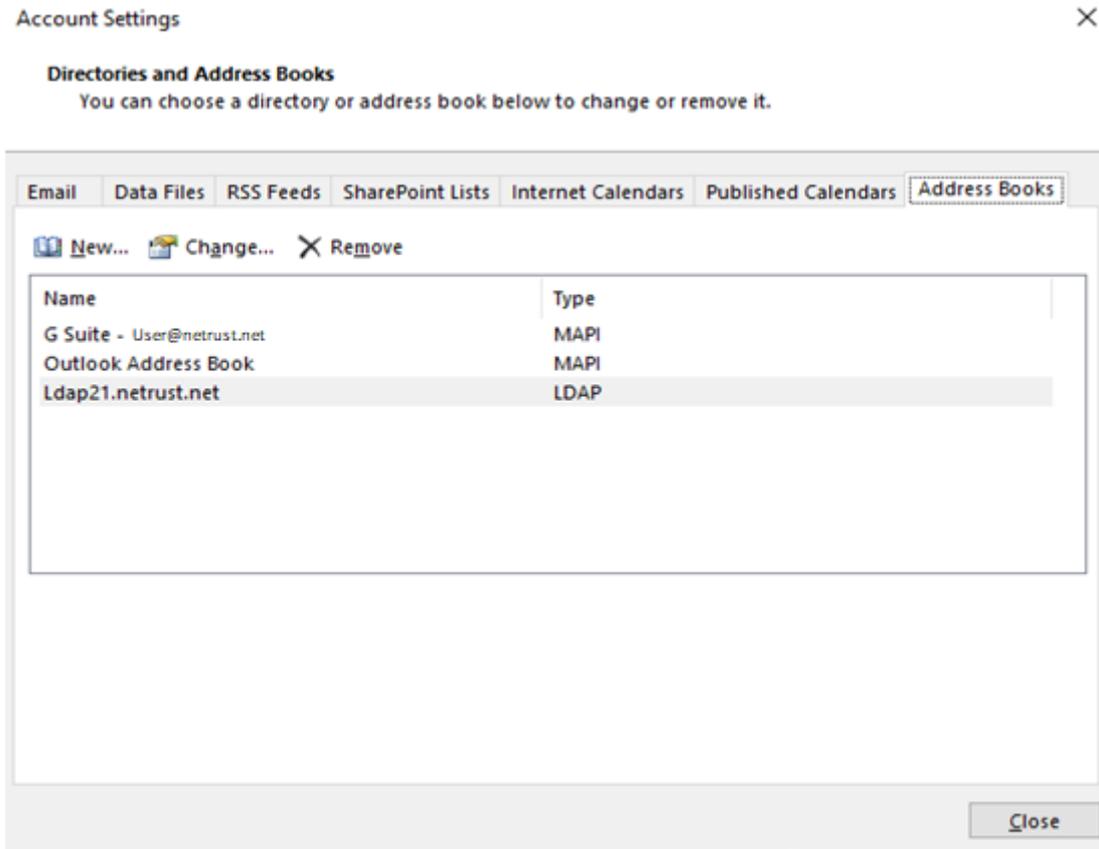


Add Server Name as: Ldap21.netrust.net



- **STEP 9**

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



## 12. How to Enrol/Recover Certificate via Entrust Entelligence Security Provider

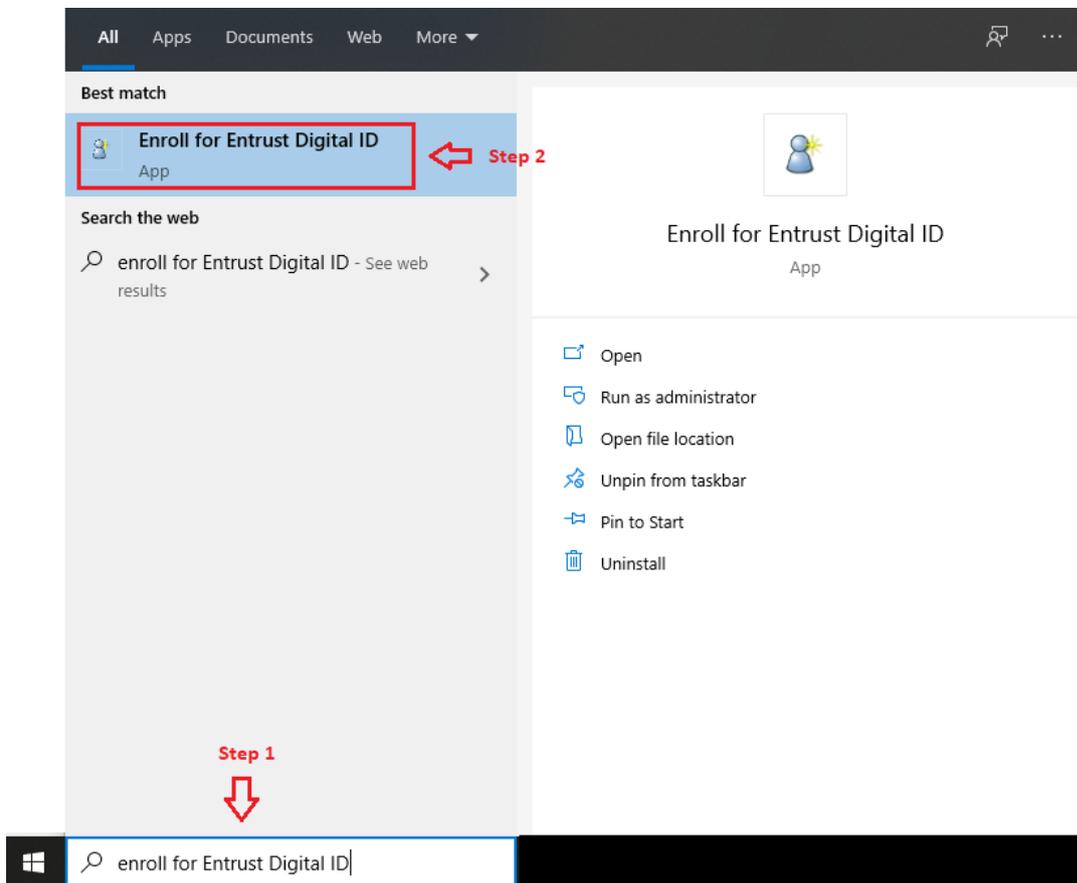
### Enrolment

- **STEP 1**

Search for Enroll for Entrust Digital ID

- **STEP 2**

Select Enroll for Entrust Digital ID App



▪ **STEP 3**

Select 'Next' to proceed

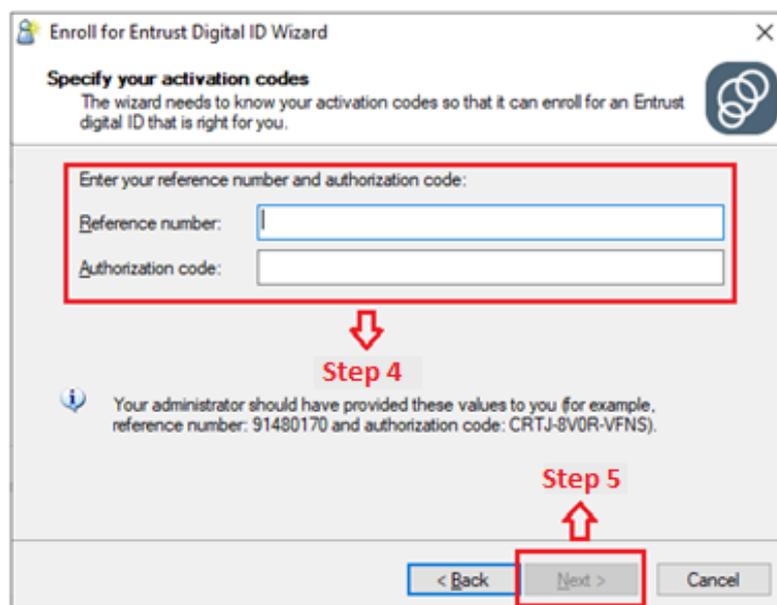


▪ **STEP 4**

Enter the Reference number and Authorization code

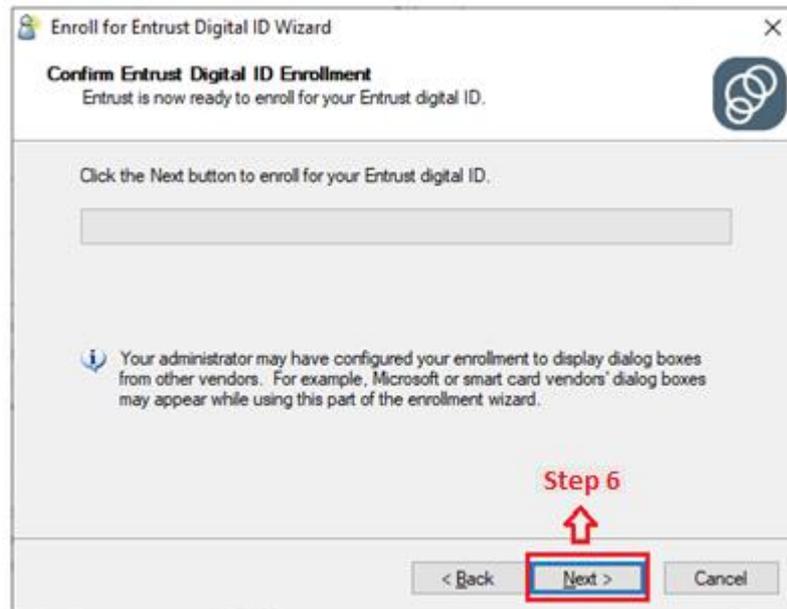
▪ **STEP 5**

Select 'Next' to proceed



- **STEP 6**

Select 'Next' to proceed

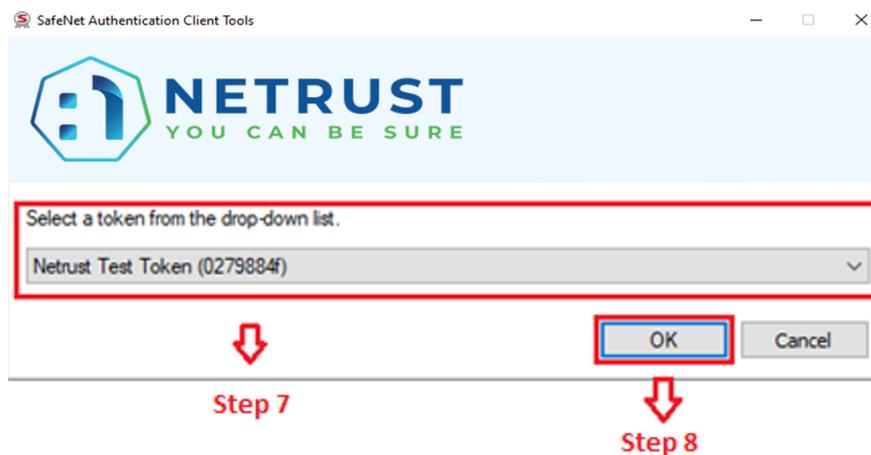


- **STEP 7**

Ensure the correct token is selected from the drop down list

- **STEP 8**

Select 'OK' to proceed

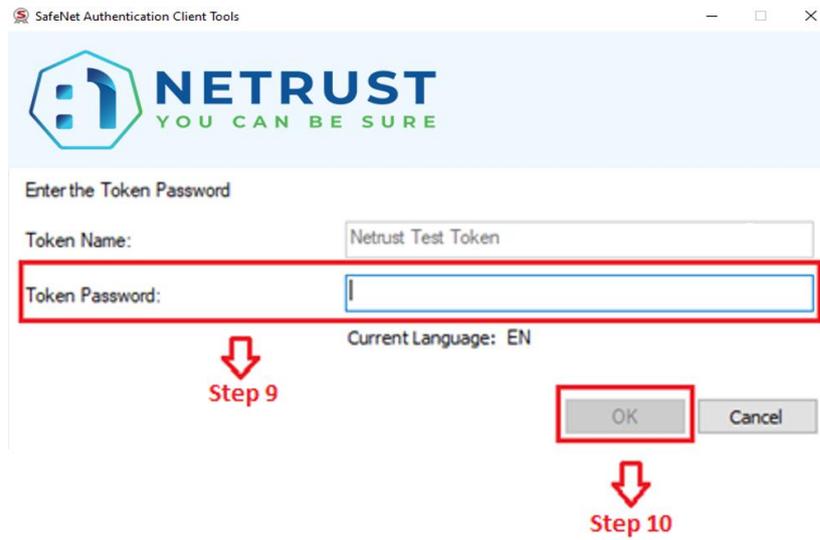


- **STEP 9**

Select 'OK' to proceed

- **STEP 10**

Select 'OK' to proceed

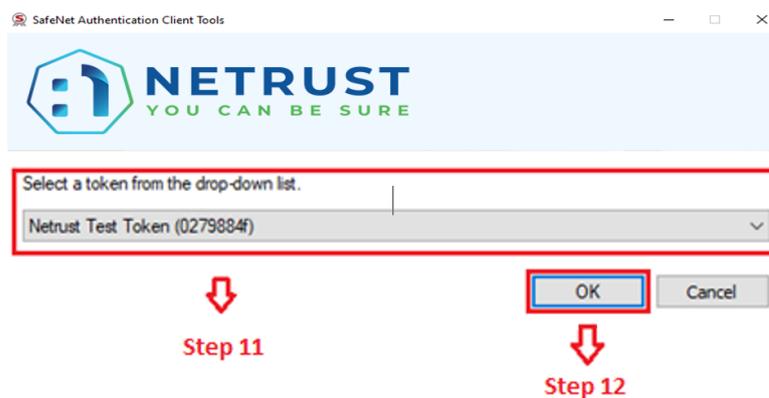


- **STEP 11**

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



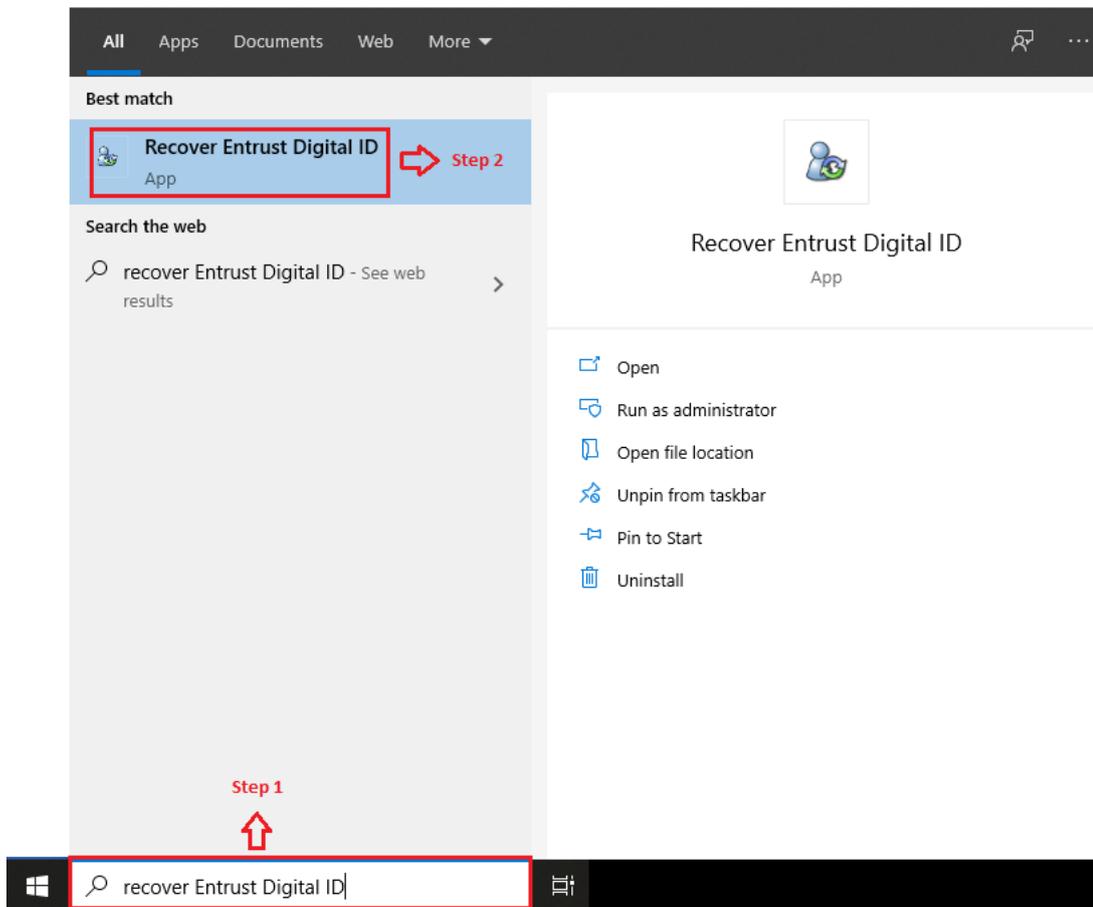
**Recovery**

▪ **STEP 1**

Search for Recover Entrust Digital ID

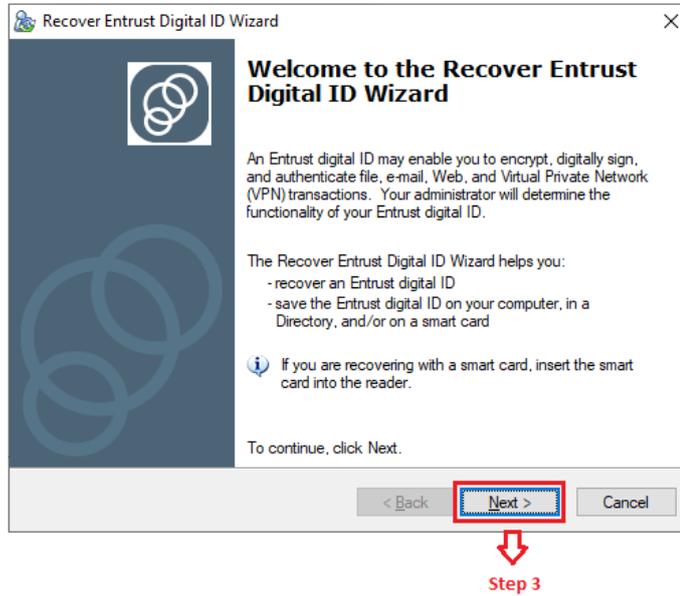
▪ **STEP 2**

Select Recover Entrust Digital ID App



- **STEP 3**

Select 'Next' to proceed

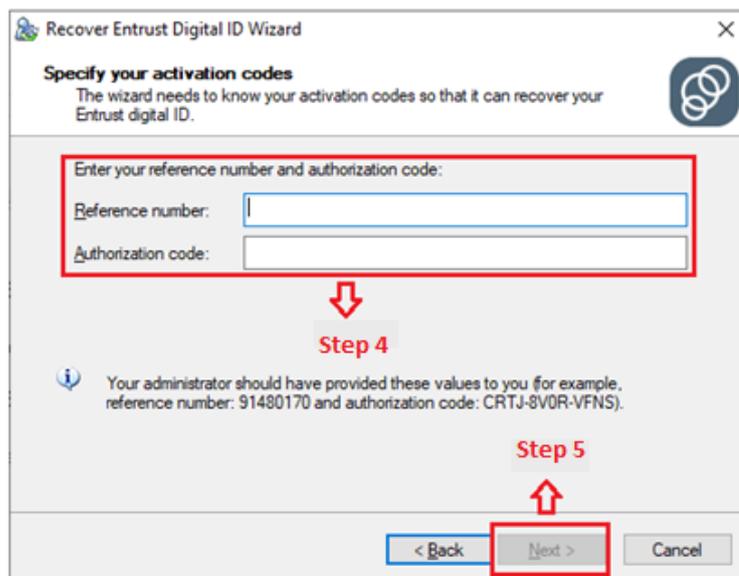


- **STEP 4**

Enter the Reference number and Authorization code

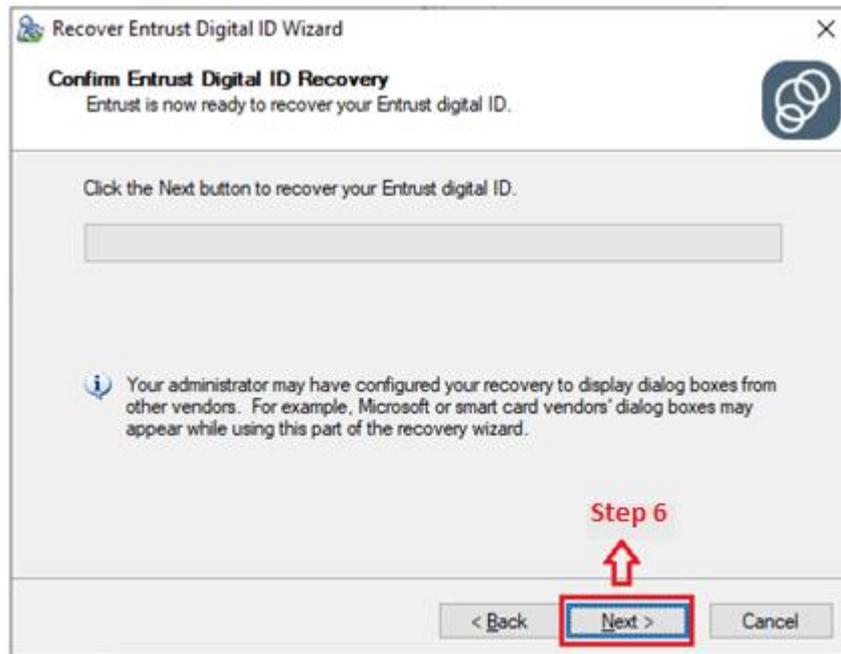
- **STEP 5**

Select 'Next' to proceed



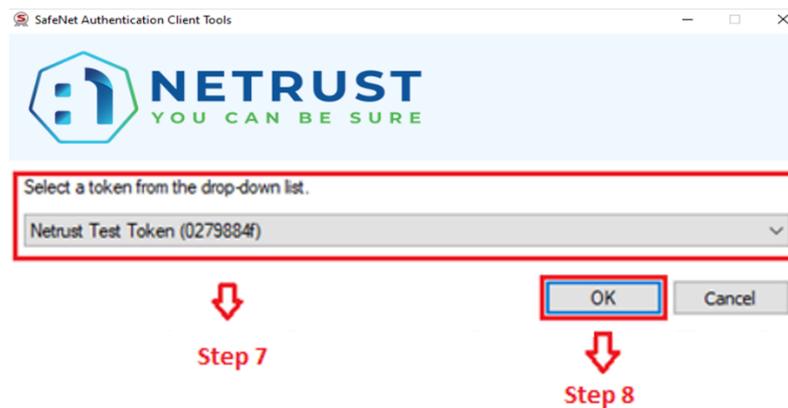
- **STEP 6**

Select 'Next' to proceed



- **STEP 7**

Ensure the correct token is selected from the drop down list

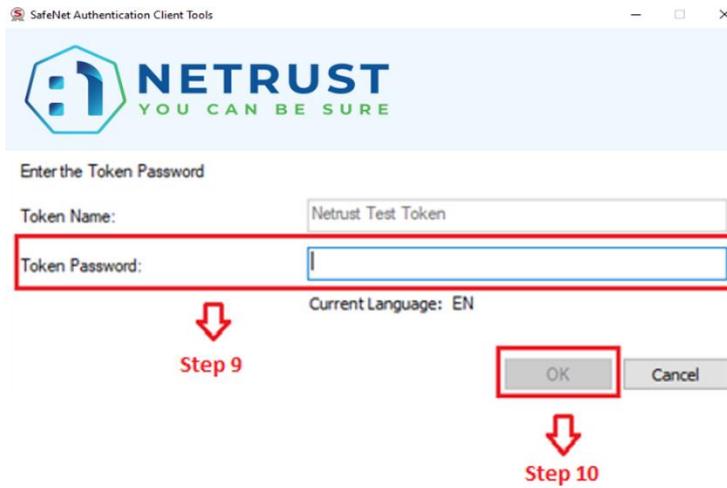


- **STEP 8**

Select 'OK' to proceed

- **STEP 9**

Type token password when prompted



- **STEP 10**

Select 'OK' to proceed

- **STEP 11**

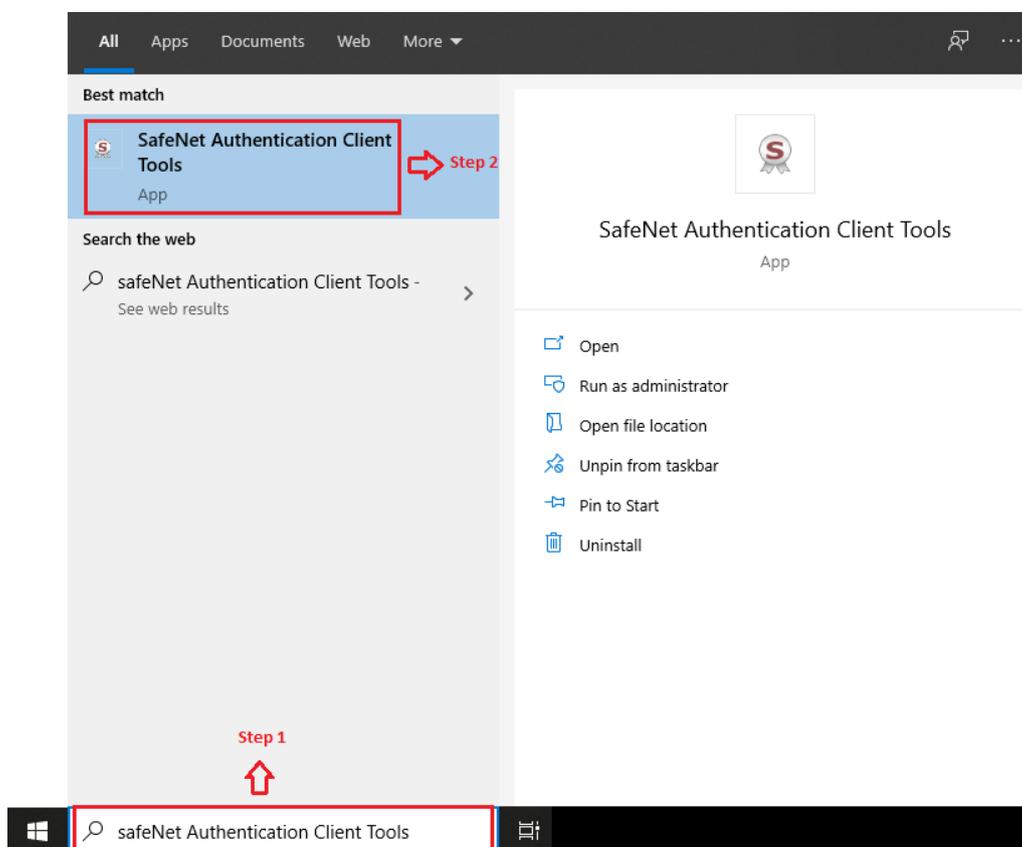
Click on 'Finish' once the enrolment is completed



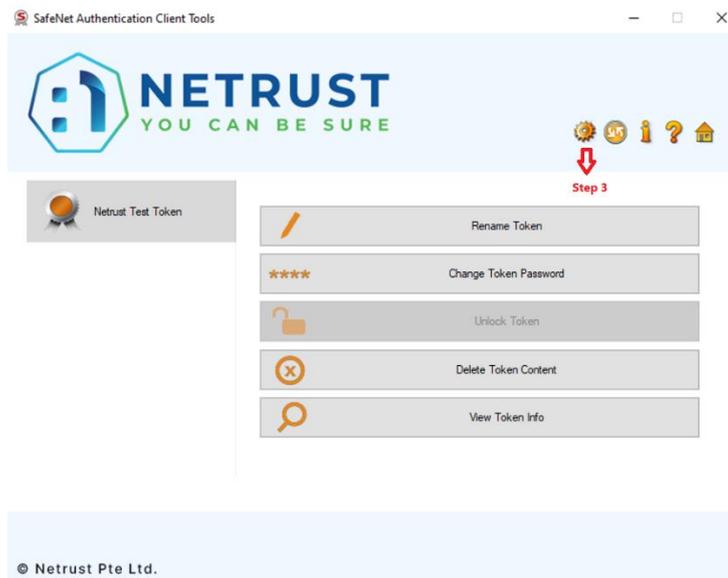
### 13. How to Initialize eToken via SafeNet Authentication Client Tools

**Warning: The token initialization process will delete all token content and reset all token parameters. Do Not Do this unless performing Recovery by administrator.**

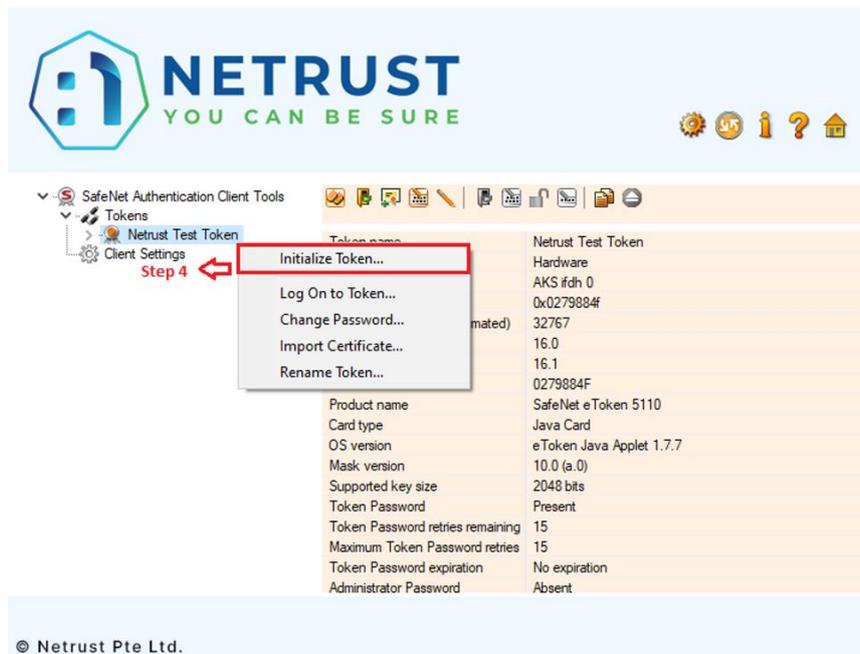
- **STEP 1**  
Search for SafeNet Authentication Client Tools
  
- **STEP 2**  
Select SafeNet Authentication Client Tools Application



- 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**  
Enter a preferred token name
- **STEP 8**  
Enter a preferred token password
- **STEP 9**  
Ensure the box under 'Create Administrator Password' is NOT ticked
- **STEP 10**  
Click 'Finish' to proceed

SafeNet Authentication Client Tools

**NETRUST**  
YOU CAN BE SURE

Token Name:  → Step 7

Create Token Password

New Token Password:  → Step 8

Confirm Password:

Logon retries before token is locked: 15

Token password must be changed on first logon

Create Administrator Password

Create Administrator Password → Step 9

Confirm Password:

Logon retries before token is locked: 10

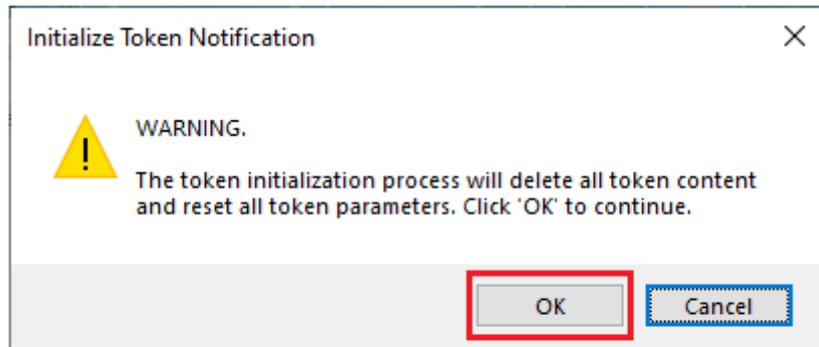
Current Language: EN

One-factor logon

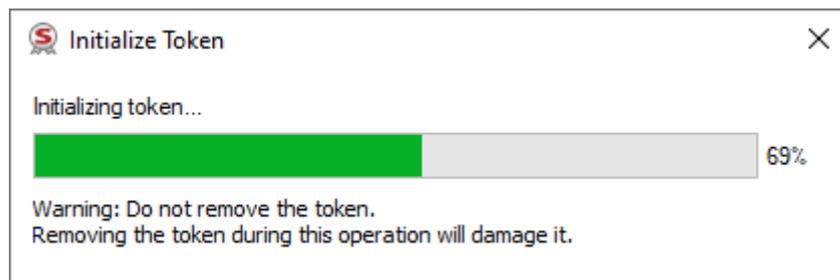
< Back   Next >   **Finish**   Cancel

↑ Step 10

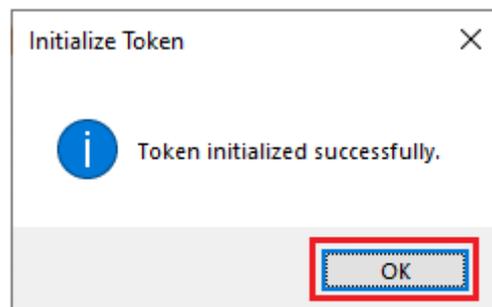
- **STEP 11**  
Click 'OK' to proceed



↓  
**Step 11**



- **STEP 12**  
Click 'OK' to once the initialization is completed



↓  
**Step 12**



**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](http://www.netrust.net)

[customersupport@netrust.net](mailto:customersupport@netrust.net)