

ECA Software Activation Guide v1.0

These steps will help you complete the retrieval on your software certificate.

Highly recommend you read through all instructions first, before starting the actual process.

Instructional video: <https://youtu.be/BZMJgrVplsc>



Instructions

1. **Open the email with** the subject line “Your IdenTrust Certificate Has Been Approved!”

Your IdenTrust Certificate has been Approved!

Account Number
12345678-12

Dear Jane Doe,

Congratulations! Your IdenTrust certificate application has been approved. With your certificate, you can use the Internet with confidence for your secure online transactions.

Your account number is **12345678-12**
Your activation code is **1234567891**

To retrieve the certificate, go to the following URL:

- **Open browser** and go to www.identrust.com/install
- You will be prompted to enter your **Activation Code** listed above, and the **Account Password** set up during the online registration or renewal process
- Follow the prompts to retrieve the certificate.

Remember: You have **90 days** from the date your application is approved to retrieve your certificate. If it is not retrieved in time, a new application will have to be purchased.

If you paid with a credit card, you may request a copy of your receipt by logging into the Certificate Management Center and selecting "receipt" from the dropdown menu: https://www.identrust.com/certificates/cert_management_center.html

If you have questions regarding your digital certificate or need customer support, please view our support website: www.identrust.com/support.

Thank you again for choosing IdenTrust as your trusted source in identity verification.

Sincerely,

IdenTrust Registration Department
www.identrust.com

2. **Look for the activation code** listed in the email. Copy or write down the activation code.
3. **Follow the link** in the Email to www.IdenTrust.com/install.
4. **"Welcome! It's Time to Get Your Certificate."**



Welcome! It's Time to Get Your Certificate

Before you begin, we will check that your system is able to get your certificate.

If you are using a USB Token or Smart Card to store your certificate, please make sure you have **installed the token software**.

I'M READY — PLEASE CHECK IF MY SYSTEM IS READY »

Customer Support

- Toll Free U.S.:
1 (888) 339-8906
- Outside U.S.:
1 (801) 384-3482
- Email:
Support@IdenTrust.com
- Monday thru Friday
from
5:00 a.m. to 5:00 p.m.
MST
1:00 p.m. to 1:00 a.m.
CET

© 2023 IdenTrust, Inc. All Rights Reserved

5. **Enter the activation code** from the email, and the account password you created during your online application.

Let's Begin Retrieving Your Certificate

To begin the Retrieval Phase, you must login by entering your Activation Code and Account Password you created when you applied.

Activation Code [How do I get my activation code?](#)
Account Password [I forgot my account password.](#)

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.

NEXT »

Customer Support

- Toll Free U.S.:
1 (888) 339-8906
- Outside U.S.:
1 (801) 384-3482
- Email:
Support@IdenTrust.com
- Monday thru Friday
from
5:00 a.m. to 5:00 p.m.
MST
1:00 p.m. to 1:00 a.m.
CET

6. **Click “Next”.**
7. **Download and open** the retrieval application.

← → ↻ secure.identrust.com/tsapp/ret-app.jsp?defaultlogo=1 🔑 📄 ☆ 🏠 🌐

New Tab Imported



part of HID Global

Retrieval Step 3 of 6 » Login » Agreement » **Authenticate App** » Generate Keys » Certificate Information » Done

Retrieval App Authentication

- DOWNLOAD »** and open the [IdenTrust Retrieval Application](#).
- Drag and drop your Retrieval Key onto the Retrieval Application to continue.

Your Retrieval Key



or click **COPY KEY** and paste the key into the Retrieval Application.

COPY KEY

Customer Support

- Toll Free U.S.:
1 (888) 339-8906
- Outside U.S.:
1 (801) 384-3482
- Email:
Support@IdenTrust.com
- Monday thru Friday
from
5:00 a.m. to 5:00 p.m.
MST
1:00 p.m. to 1:00 a.m.

IdenTrustRetrieval....exe ^ Show all X

Open File - Security Warning

Do you want to run this file?



Name: ...\\Users\\yourname\\Download\\IdenTrustRetrievalApp(4).exe
Publisher: [IdenTrust, Inc.](#)
Type: Application
From: C: \\Users\\yourname\\Download\\IdenTrustRetrievalApp(4).exe

☒ Always ask before opening this file



While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust.
[What's the risk?](#)

8. **After you run the** retrieval application you will see a "Copy key" button, click that button, then click on the text box next to "Retrieval key" in the retrieval application, and click "ctrl + v" on your keyboard to paste the key.

IdenTrust Retrieval Application (v1.2.3.275)

Authentication

IdenTrust
part of HID Global

Please drop your Retrieval Key onto the lock or paste the Retrieval Key you copied into the field provided.



Retrieval Key:

NEXT »

© 2020 IdenTrust, Inc. All Rights Reserved

Retrieval App Authentication

1. **DOWNLOAD »** and open the [IdenTrust Retrieval Application](#).
2. Drag and drop your Retrieval Key onto the Retrieval Application to continue.

Your Retrieval Key



or click **COPY KEY** and paste the key into the Retrieval Application

COPY KEY

IdenTrust Retrieval Application (v1.2.3.275)

Authentication

Please drop your Retrieval Key onto the lock or paste the Retrieval Key you copied into the field provided.



Retrieval Key:

NEXT »

Retrieval App Authentication

1. **DOWNLOAD** and open the [IdenTrust Retrieval Application](#).
2. Drag and drop your Retrieval Key onto the Retrieval Application to continue.

Your Retrieval Key



or click **COPY KEY** and paste the key into the Retrieval Application.

COPY KEY

Customer Support

- Toll Free U.S.:
1 (888) 339-8906
- Outside U.S.:
1 (801) 384-3482
- Email:
Support@IdenTrust.com
- Monday thru Friday
8:00 a.m. to 5:00 p.m.
MST
1:00 p.m. to 1:00 a.m.
CET



9. **After the key** is on the lock or it's copied/pasted, the retrieval application will say "Welcome," then it will load while it verifies the retrieval key. The original window in your web browser may change a few times during this process - do not move from the screen or close anything.
10. **Leave the drop-down** menus on the default options, then click on the blue "Generate keys" button at the bottom of the window.

IdenTrust Retrieval Application (v1.2.3.275) ✕

Generate Keys

IdenTrust
part of HID Global

You will be asked to create a password that you will provide whenever you use your signing certificate.

Choose a password you can recall and store it securely.

Microsoft Enhanced Cryptographic Provider v1.0

RSA 2048



Click GENERATE KEYS when you are ready.

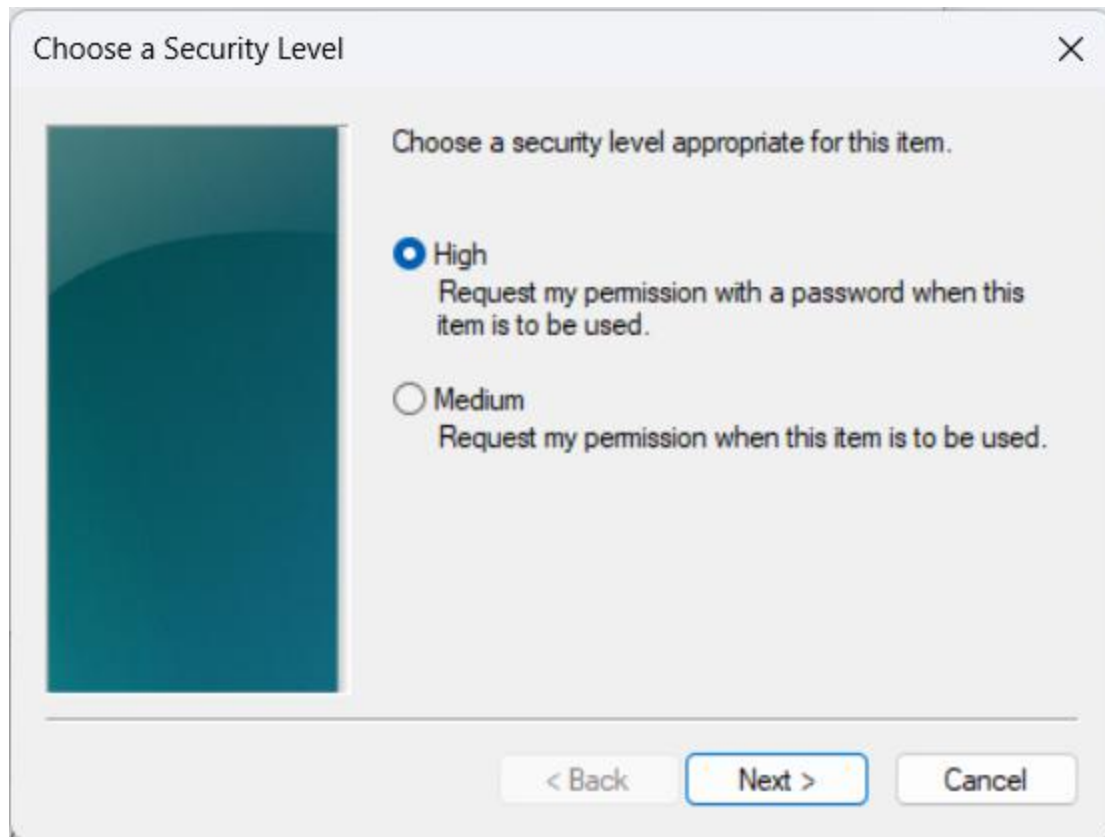
GENERATE KEYS »

© 2020 IdenTrust, Inc. All Rights Reserved

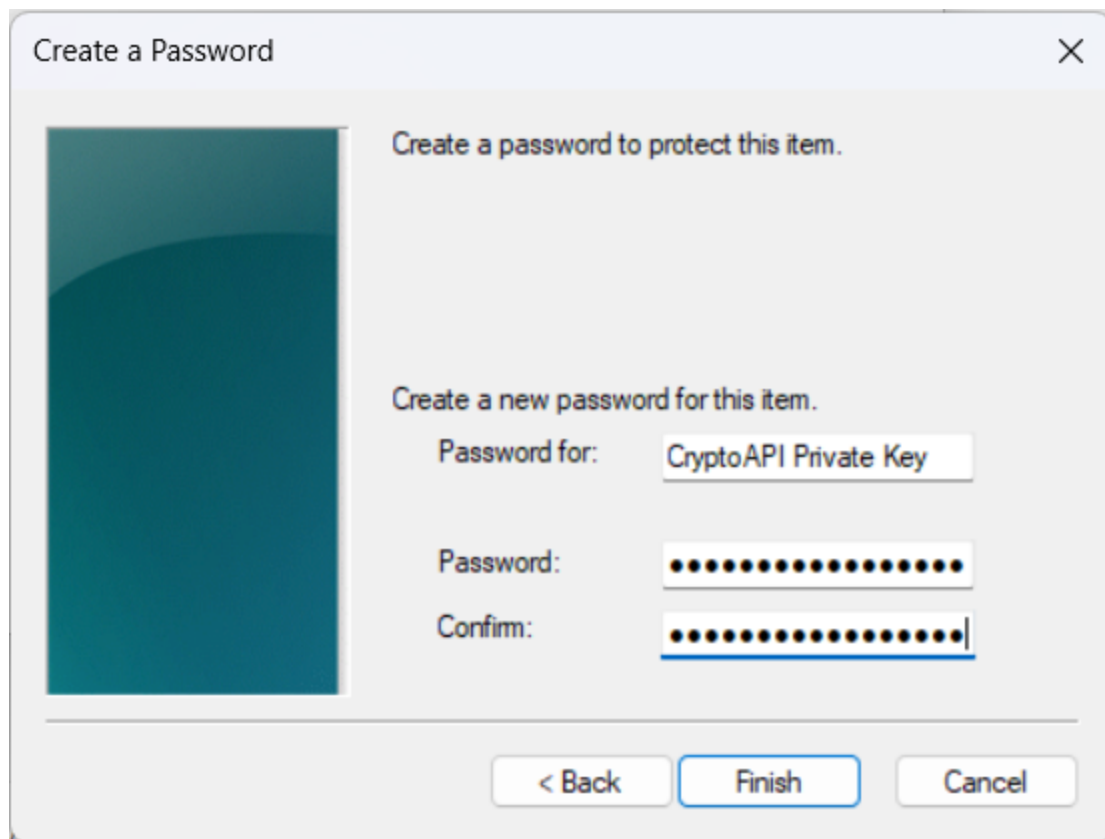
Click “Set Security Level”.

”High” request permission with a password. ***High security is strongly recommended. Implementing strong security controls is critical to ensuring sole access to your credential. This certificate carries non-repudiation, meaning you hold full responsibility for all usage.**

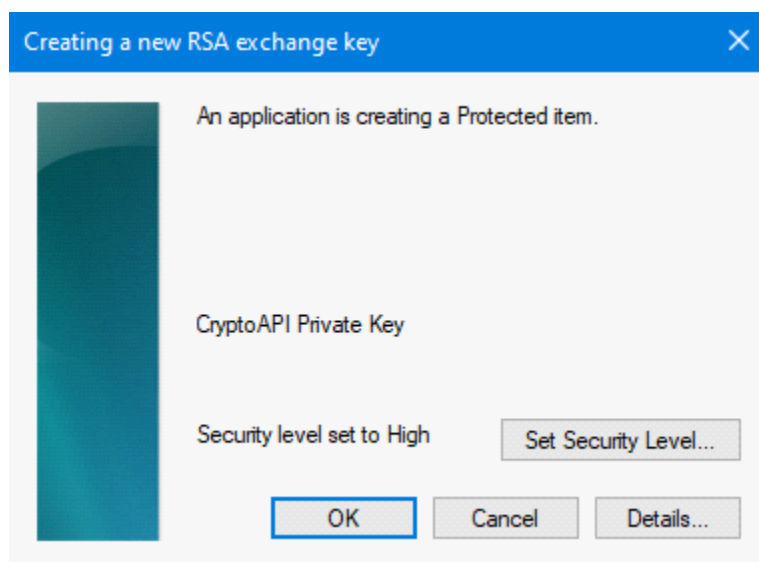
”Medium” requests my permission when this item is being used. ***This does NOT prompt for any kind of PIN or password to use. Not recommended.**



11. **High security** you will be prompted to Enter and Confirm the “CryptoAPI Private Key” certificate password.



12. The **"Creating a new RSA exchange key"** window will pop back up, click on "OK" to continue.



13. **The retrieval application** will go back to a "Generate keys" window. This is to generate the keys for your encryption certificate. Click on the blue "Generate keys" button again at the bottom of the window.

Generate Keys

IdenTrust
part of HID Global

Now you will be asked to create a password that you will provide whenever you use your encryption certificate.

Choose a password you can recall and store it securely.



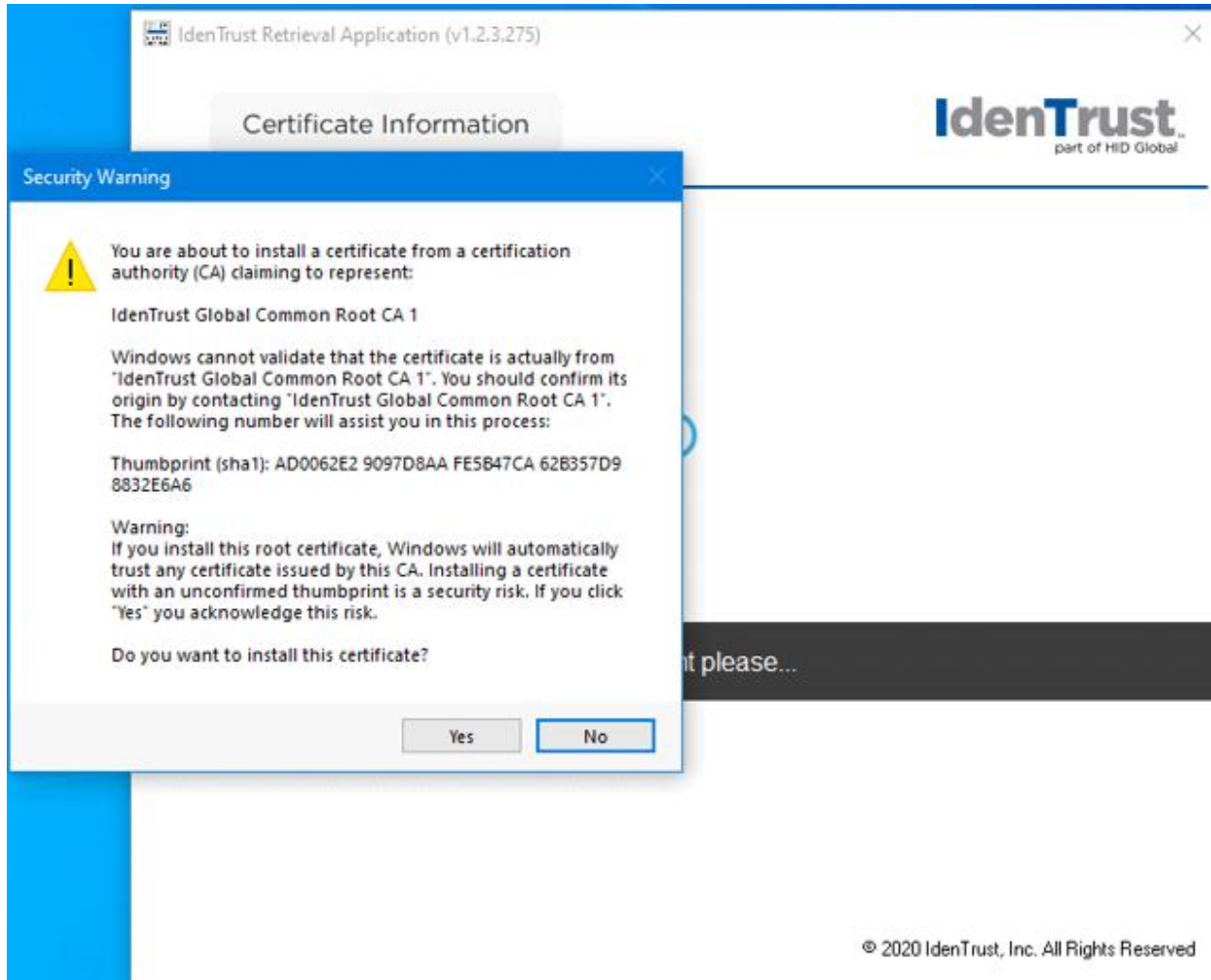
Click GENERATE KEYS when you are ready.

GENERATE KEYS »

© 2020 IdenTrust, Inc. All Rights Reserved

14. **"Choose a Security Level"** window, set the security level, then click Next.
15. **"Create a password"** window, type and confirm the same password you set for the signing certificate.
16. **Click "Finish."**
17. **The "Creating a new RSA exchange key"** window will pop back up, click on "OK" to continue.
18. **The retrieval application** will finish generating the certificates.

During this step, you may see a "Security Warning" window pop up, with a message that starts with "You are about to install a certificate from a certification authority (CA) claiming to represent..." If that window pops up, click on "Yes" at the bottom to install the certificate.



20. **At the end** of the certificate installation, the retrieval application will bring up a window that says "Would you like to back up your certificates now?" Click "Yes."

Certificate Information



Making a backup now is very quick and easy.

Please consider making a backup now.



Would you like to back up your certificates now?

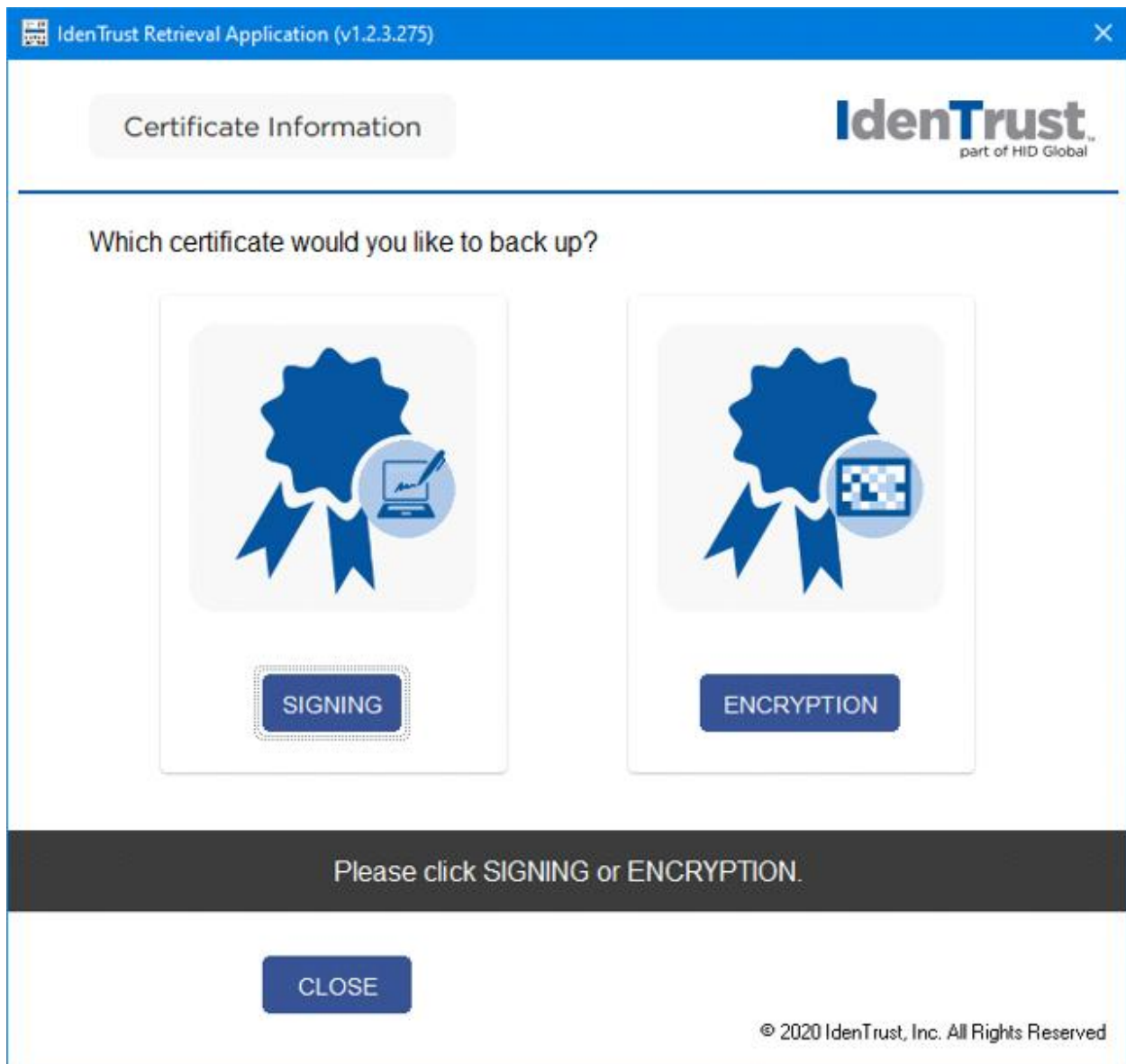
YES

NO

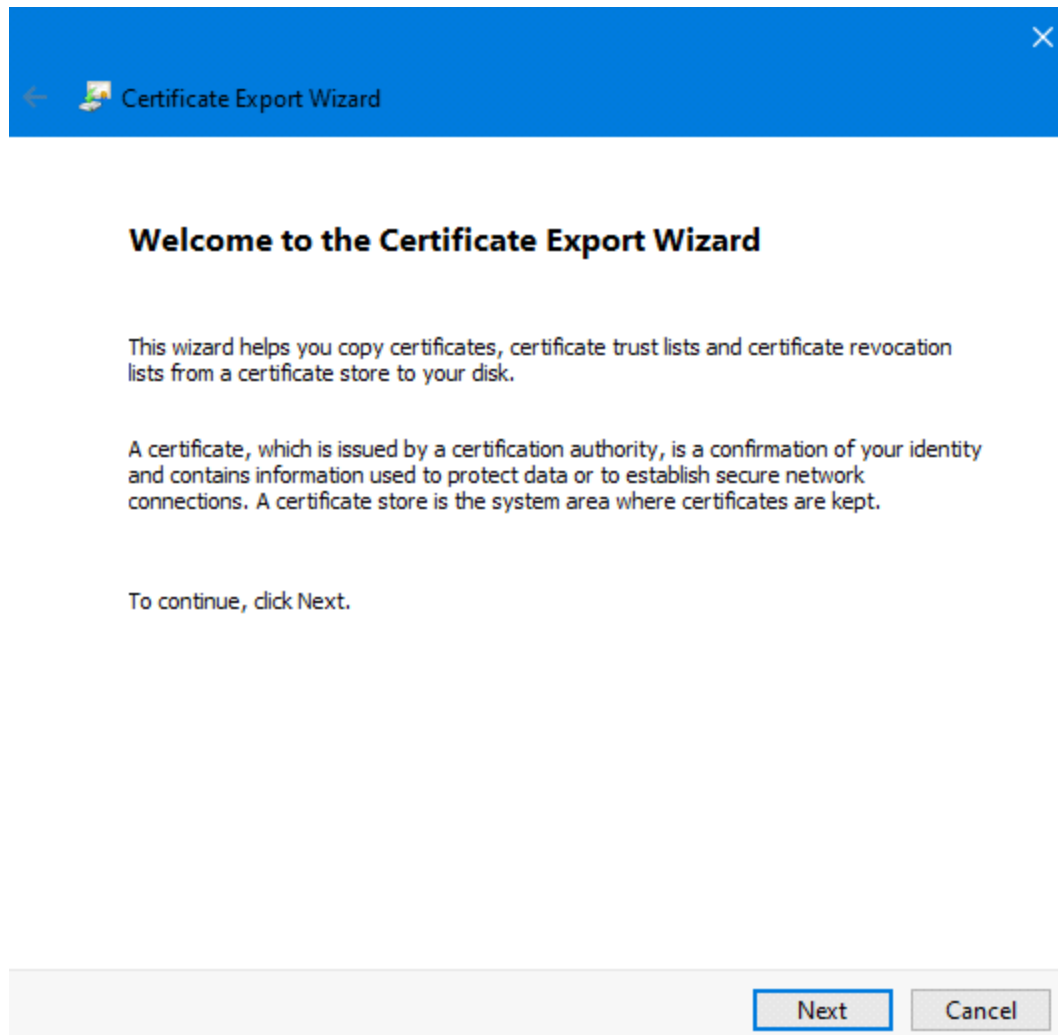
© 2020 IdenTrust, Inc. All Rights Reserved

21. **After you click "Yes,"** it will ask which certificate you would like to back up. The signing certificate is the one which you will use to sign documents or log into websites. Click "Signing" to start backing up the signing certificate.

Back up only the **signing** certificate since these ECA's are not intended and built for encryption. If you do get an ECA that will be using the encryption certificate, please back up both certificates.



22. After you click "Signing," the Certificate Export Wizard will pop up. On the first page, when "Welcome to the Certificate Export Wizard" appears, click Next.



23. **Export File Format.**" Leave the file format on the default, Personal Information Exchange, then click Next.

24. **Check the boxes**

- a. "Include all certificates in the certification path if possible"
- b. "Export all Extended Properties"
- c. Click "Next"

 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

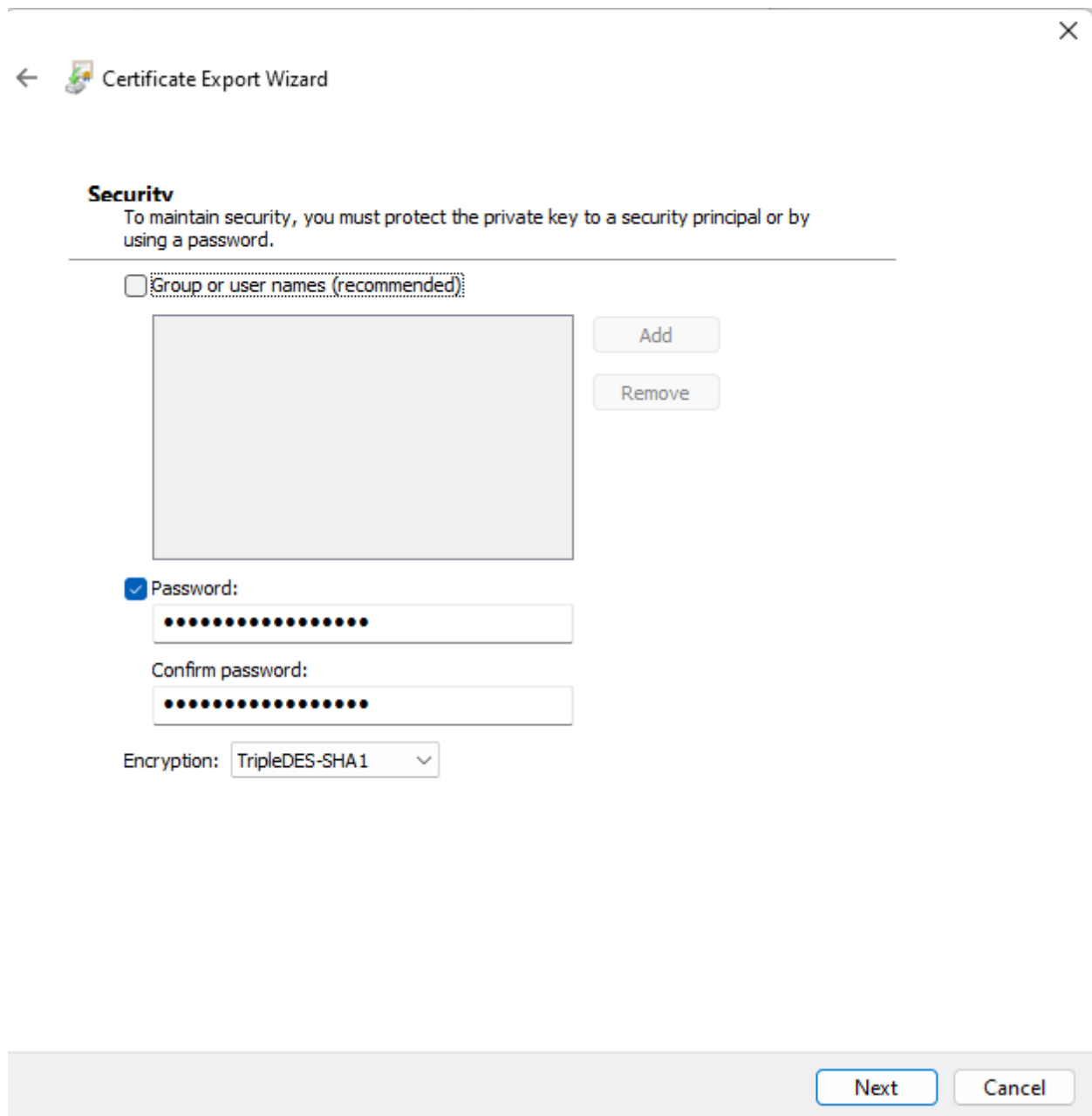
☒ Enable certificate privacy

☐ Microsoft Serialized Certificate Store (.SST)

Next

Cancel

25. **On the Security page**, check the box next to password, then type and confirm the same password you created for your certificates.



The image shows a screenshot of the 'Certificate Export Wizard' window, specifically the 'Security' page. The window has a title bar with a back arrow, a small icon, and the text 'Certificate Export Wizard', and a close button (X) in the top right corner. The 'Security' section is highlighted with a bold title. Below the title, a message states: 'To maintain security, you must protect the private key to a security principal or by using a password.' There are two main options: 'Group or user names (recommended)' which is currently unchecked, and 'Password' which is checked. The 'Group or user names' option includes a large empty list box and 'Add' and 'Remove' buttons. The 'Password' option includes two password input fields, one for 'Password:' and one for 'Confirm password:', both filled with dots. Below the password fields is an 'Encryption:' dropdown menu currently set to 'TripleDES-SHA1'. At the bottom right of the window are 'Next' and 'Cancel' buttons.

← Certificate Export Wizard

Security

To maintain security, you must protect the private key to a security principal or by using a password.

☐ Group or user names (recommended)

☒ Password:

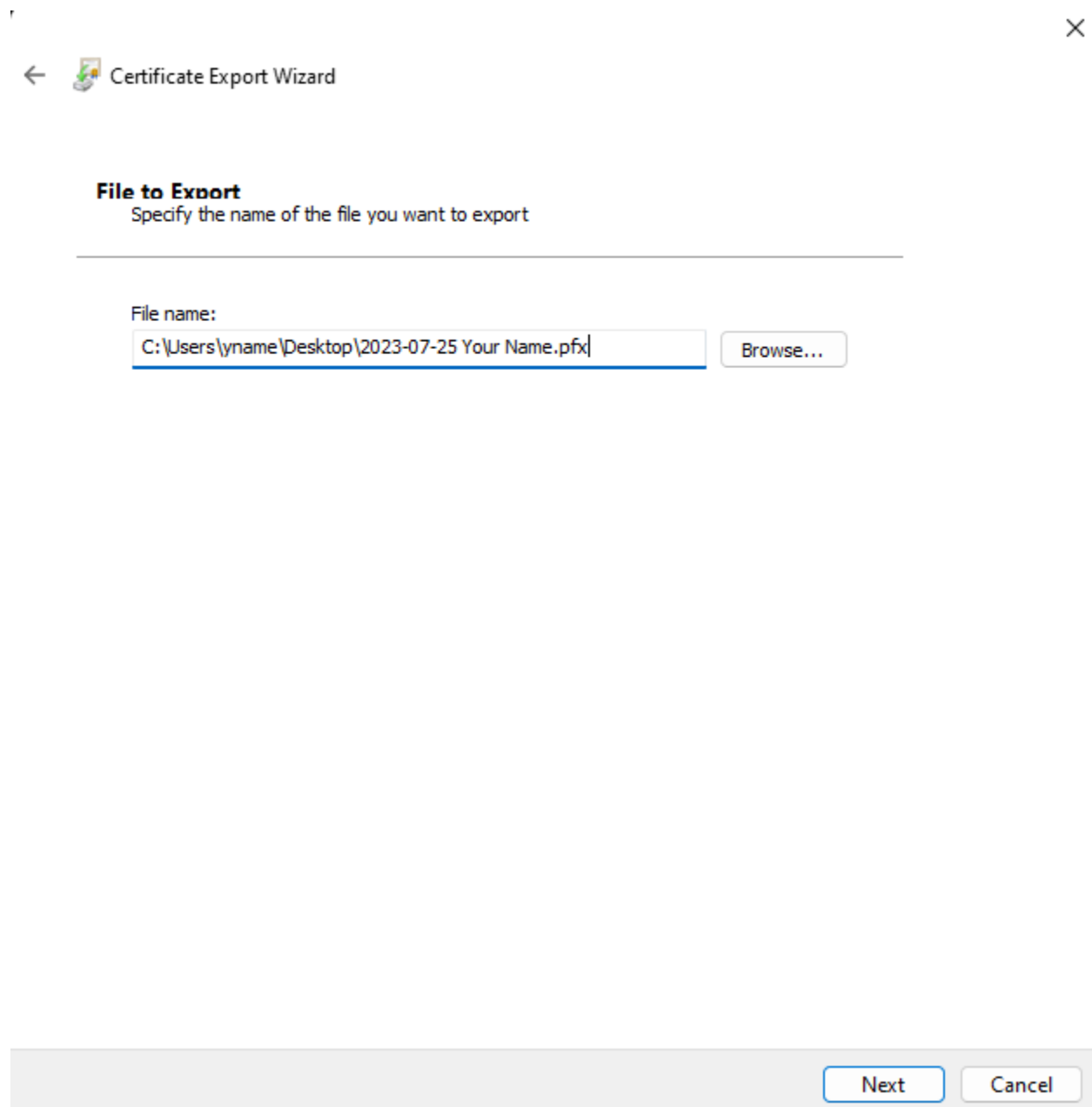
Confirm password:

Encryption: TripleDES-SHA1

Next Cancel

26. **File to Export" page**, you may name the file and where to save it. By default, the backup file will be saved to your desktop, with the current date and your name as the file name. The encryption certificate backup also saves onto your desktop with the date and your name, but with "_encr" at the end of the file name.
27. **If you want to** save the file somewhere other than your desktop and/or give it a different name, click on "Browse" to choose the folder to save it to and the name you'd like to give it. Then, click Next.

If you want to leave the default file location and name, simply click Next.



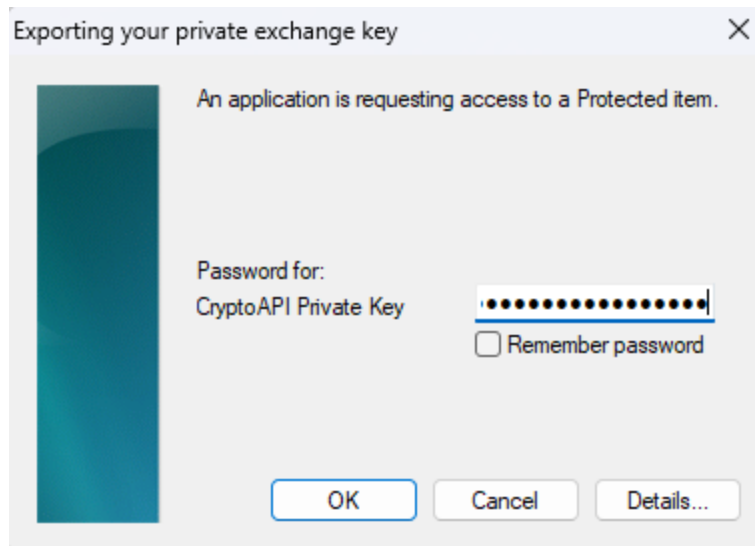
The image shows a screenshot of the 'Certificate Export Wizard' dialog box. At the top right is a close button (X). Below the title bar, there is a back arrow and the text 'Certificate Export Wizard'. The main section is titled 'File to Export' with the instruction 'Specify the name of the file you want to export'. Below this is a 'File name:' label followed by a text input field containing 'C:\Users\yname\Desktop\2023-07-25 Your Name.pfx' and a 'Browse...' button. At the bottom right, there are 'Next' and 'Cancel' buttons.

File name:
C:\Users\yname\Desktop\2023-07-25 Your Name.pfx

Browse...

Next Cancel

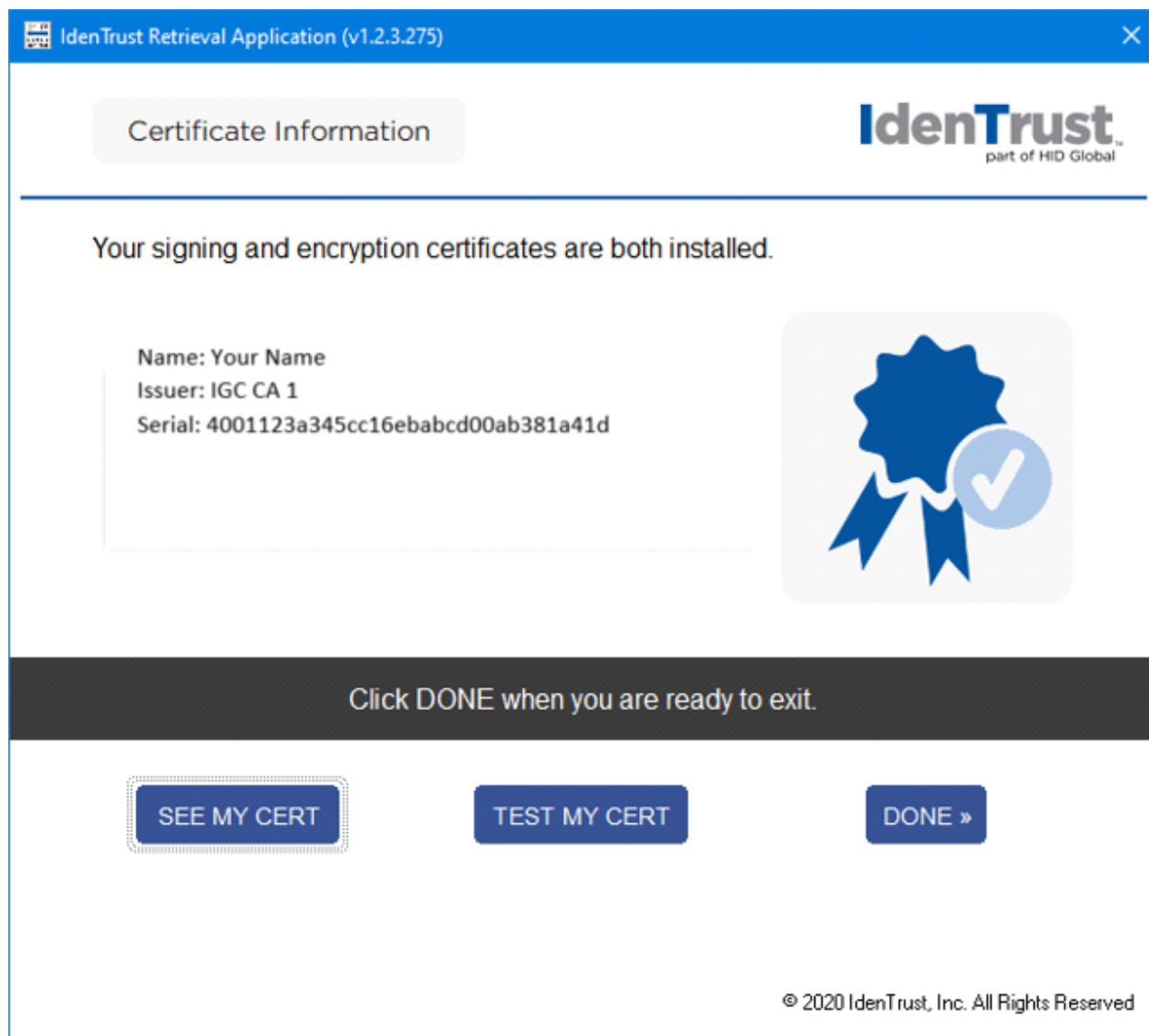
28. **"Completing the Certificate Export Wizard"** page, click Finish. A window will pop up asking for the password for your CryptoAPI Private Key. That is the password you set for your certificate. Type the password, then click "OK".



29. **A window** will pop up saying that the export was successful. Click "OK".

You will repeat these steps to back up your Encryption certificate.

30. **The retrieval application** will say "Your signing and encryption certificates are both installed."



31. **"See My Certificate."** Will allow you to view the information on your certificate.

32. **"Test My Certificate"** will help you to test the certificate in a web browser. If you choose this option, a window will pop up asking you which web browser you would like to use. **We recommend** using Google Chrome or Microsoft Edge.

Close any windows and tabs you have open in your web browser before selecting it for the test. The test works best if there are no windows open.

33. **Click "Done"** to close the retrieval application.

34. **Once you close** the retrieval application, your web browser will ask you to click Next to verify the information on your certificate. Make sure that the certificate information is correct, then click Next.

Let's Verify the Information in Your Certificate

The contents of your certificate are presented below. You are responsible for reviewing the certificate information for accuracy. IdenTrust records the act of digital certificate acceptance.

Notify IdenTrust immediately of any errors, defects or any other problems with your digital certificate at 1-888-248-4447. If you do not, you will be deemed to have accepted it. Click **"Next"** below, after you have reviewed your certificate information.

Your Certificate information

SUBJECT INFORMATION:

Common Name: Your Name

Organization Name: Your Company

Country Name: US

dnQualifier: A01410C000001234D345D7C000B12F0

NEXT »

Customer Support

- Toll Free U.S.:
1 (888) 339-8906
- Outside U.S.:
1 (801) 384-3482
- Email:
Support@IdenTrust.com
- Monday thru Friday
from
5:00 a.m. to 5:00 p.m.
MST
1:00 p.m. to 1:00 a.m.
CET

35. **You will be** given instructions to test your certificate. If you've already done the test in the retrieval application, you can skip this step and close the window. Click Next, and a window should pop up asking you to select a certificate.

Instructions for Verifying Certificate Retrieval

Now that you have retrieved your certificate, follow these instructions to verify that it has been downloaded properly. These instructions will help you navigate through a series of windows. [Print these instructions.](#) then follow them as you go through the process online.

1. Click **"Next"**. The **Select a Certificate** window appears.
2. In the list, select the certificate you just retrieved, then click **OK**.
3. You may be prompted to provide your Microsoft Crypto API password (only if you chose High Protection when you retrieved your certificate). If prompted, [provide the password for your certificate.](#)

In the event that the certificate cannot be verified, due to selecting the wrong certificate, or clicking **Cancel** instead of **OK** at the **Select a Certificate** window, close any browser windows that are open, then restart your browser and return to the following URL to begin the verification process again:

<https://www.identrust.com/test/?AT=273&CT=1420016>

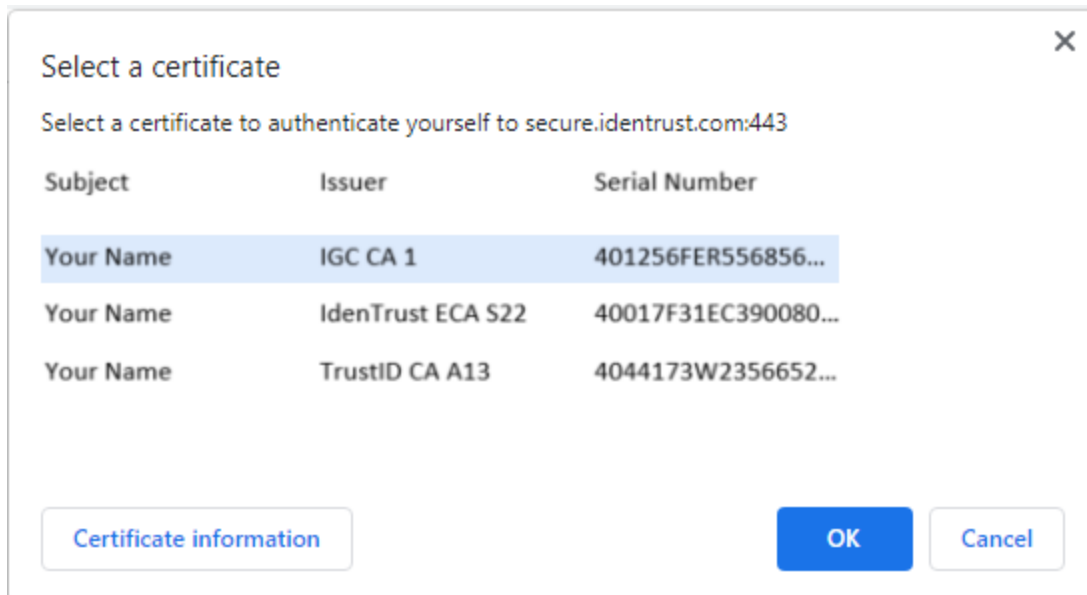
If the **Congratulations** page appears, your certificate has been successfully retrieved and downloaded. The process is complete.



Customer Support

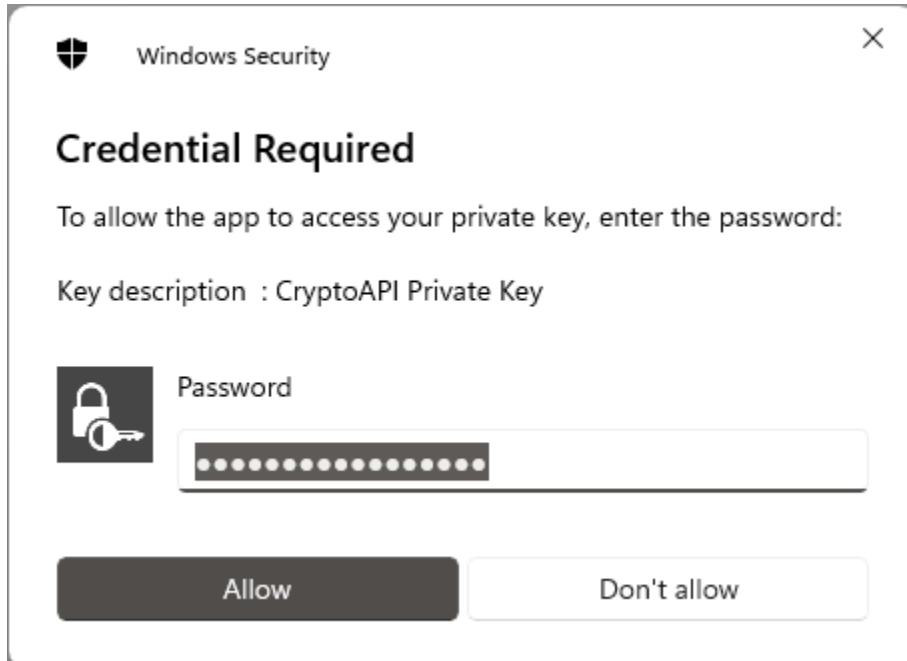
- Toll Free U.S.:
1 (888) 339-8906
- Outside U.S.:
1 (801) 384-3482
- Email:
Support@IdenTrust.com
- Monday thru Friday
from
5:00 a.m. to 5:00 p.m.
MST
1:00 p.m. to 1:00 a.m.
CET

36. **Click on** your certificate issued by IGC CA 1.



37. Click "OK".

38. A window will pop up from Windows Security that says "Credentials Required" and ask for your CryptoAPI Private Key password.



39. Enter the password you set for your certificate.

40. **Click** "Allow."

41. **Congratulations**, Certificate Retrieval Completed.