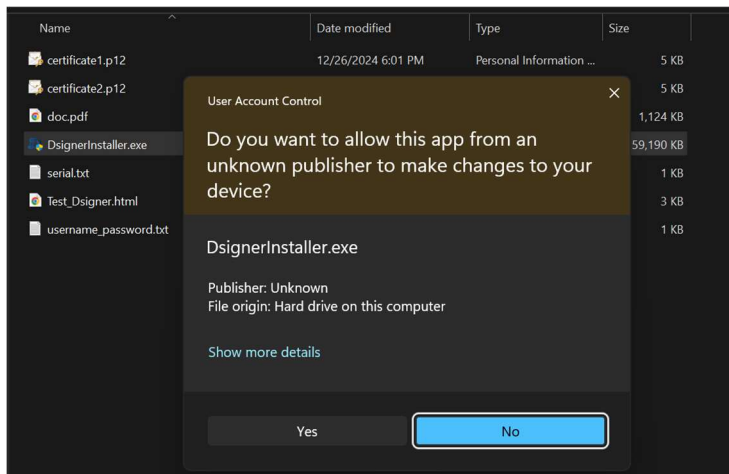


# Dsigner Installation Process

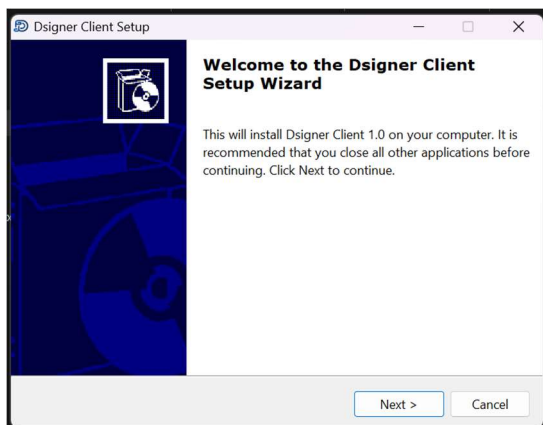
- 1) When you extract the zipped Dsigner folder, you will see these files.

| Name                  | Date modified       | Type                     | Size       |
|-----------------------|---------------------|--------------------------|------------|
| certificate1.p12      | 12/26/2024 6:01 PM  | Personal Information ... | 5 KB       |
| certificate2.p12      | 12/26/2024 11:35 AM | Personal Information ... | 5 KB       |
| doc.pdf               | 4/17/2025 4:00 PM   | Chrome HTML Docu...      | 1,124 KB   |
| DsignerInstaller.exe  | 6/6/2025 1:10 PM    | Application              | 159,190 KB |
| serial.txt            | 3/31/2025 12:16 PM  | Text Document            | 1 KB       |
| Test_Dsigner.html     | 3/30/2025 5:04 PM   | Chrome HTML Docu...      | 3 KB       |
| username_password.txt | 6/9/2025 3:17 PM    | Text Document            | 1 KB       |

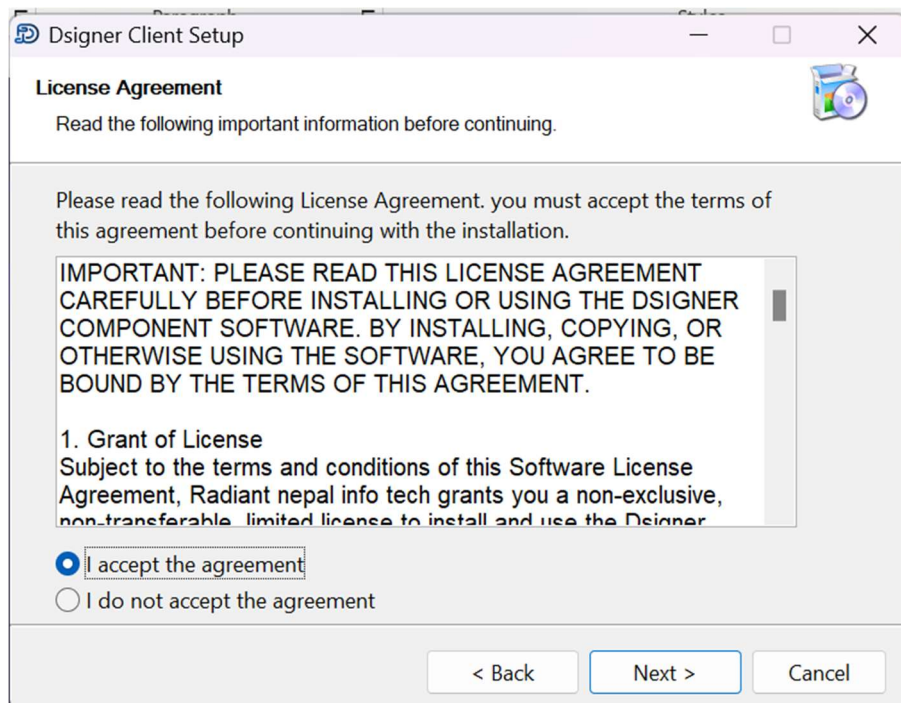
- 2) Double-click on *DsignerInstaller* and click 'Yes' when prompted.



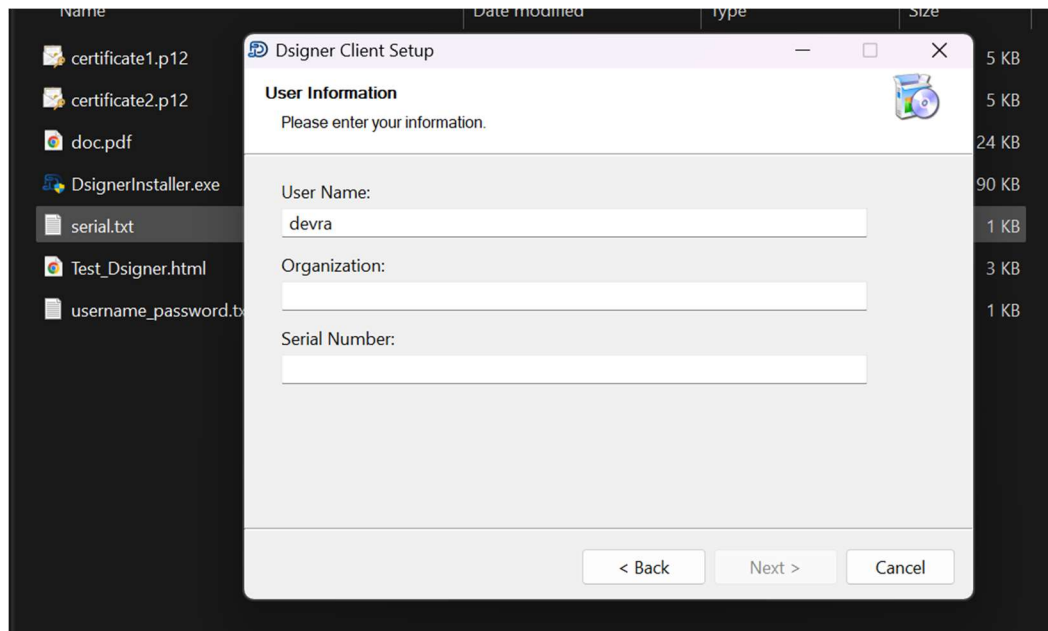
- 3) Click on the 'Next' button.



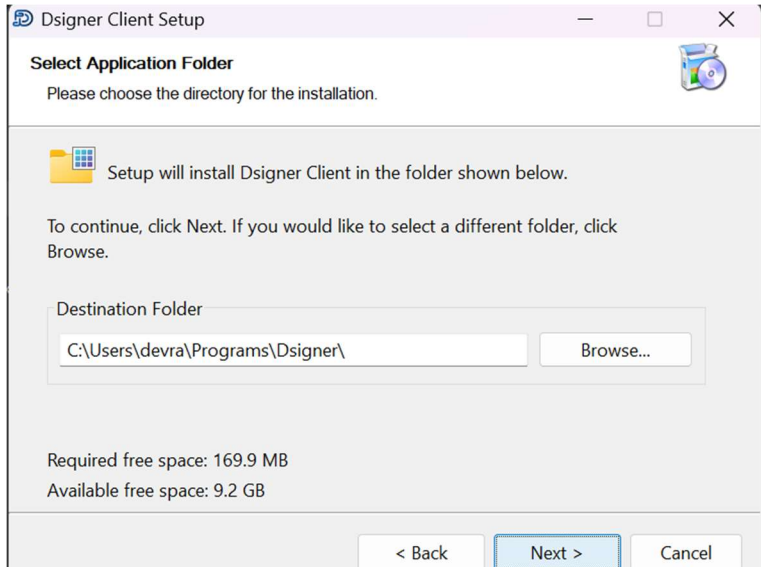
- 4) Now select 'I accept the agreement' and click 'Next'.



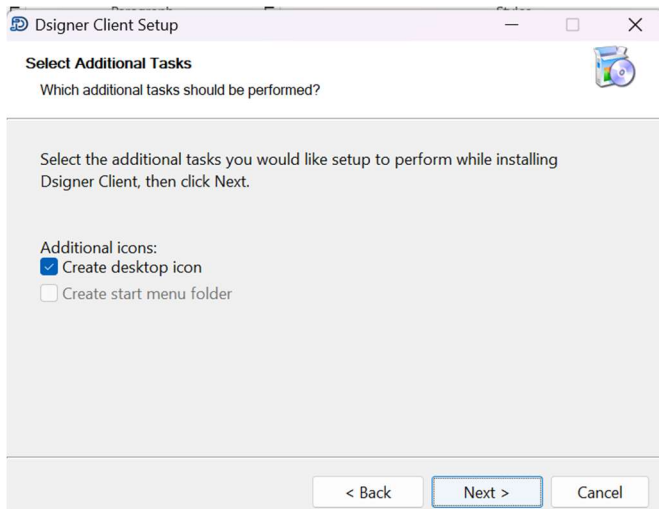
- 5) User Name and Organization are optional, but you may enter your own if you like. For the Serial Number field, open the *serial.txt* file that you extracted earlier and copy the serial number from there. Once the serial number is validated, the 'Next' button will be enabled—then click it.



- 6) If you want to change the destination folder, you can do so now. Then click 'Next'. This is the folder where the required Dsigner files will be installed.



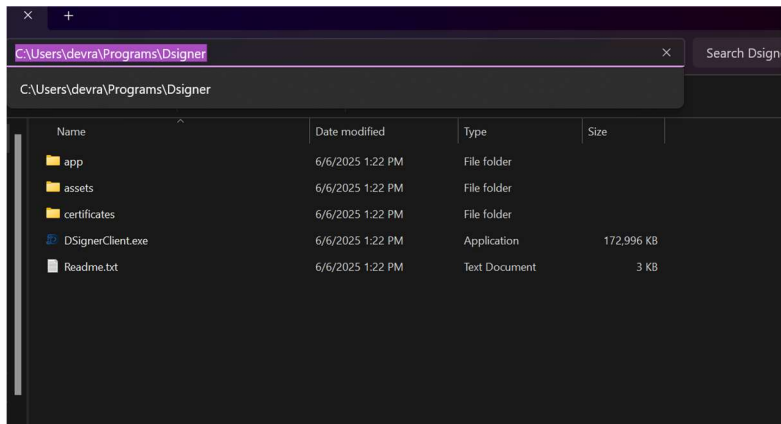
- 7) Click on the 'Next' button.



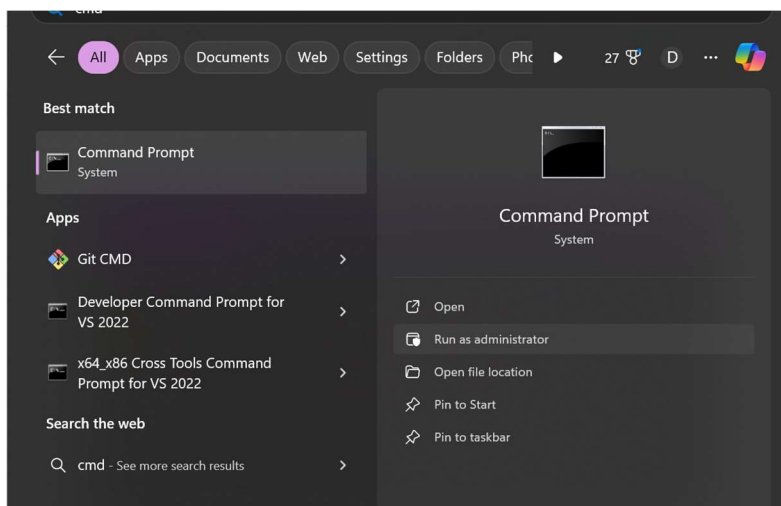
- 8) Once the installation is complete, the *readme.txt* file will open. When you click 'Run', it will show the instructions on how to install the root certificate required for the WSS (WebSocket Secure) connection. You can follow the steps mentioned there. Alternatively, you can right-click the Dsigner shortcut on your desktop, select 'Open file location'.



9) Copy the destination folder path from there.



10) Search for cmd in the search option in the taskbar and Select "Run as administrator."



11) In the Command Prompt, type the following command and press Enter:

- a. `certutil -addstore -f -enterprise -user root <paste location here>\certificates\certificate.crt`

Note:- Replace <paste location here> with the folder path you copied earlier  
(e.g., C:\Users\username\Programs\Dsigner).

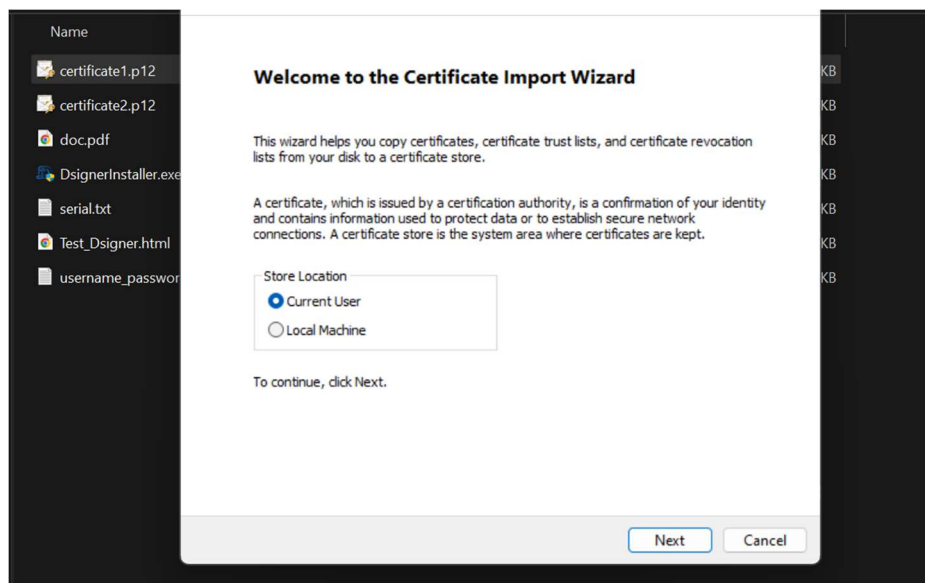
```
C:\Windows\System32>certutil -addstore -f -enterprise -user root C:\Users\devra\Programs\Dsigner\certificates\certificate.crt
root "Trusted Root Certification Authorities"
Signature matches Public Key
Related Certificates:

Exact match:
Element 0:
Serial Number: 707b993c266ebcf168ce95937da05ba763febe12
Issuer: CN=localhost, O=Radiant infotech nepal, L=Kathmandu, S=Bagmati, C=NP
NotBefore: 2/2/2025 2:07 PM
NotAfter: 1/31/2035 2:07 PM
Subject: CN=localhost, O=Radiant infotech nepal, L=Kathmandu, S=Bagmati, C=NP
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): f2c699e6cf8d54dca55d01c2dbebb1431fde620b

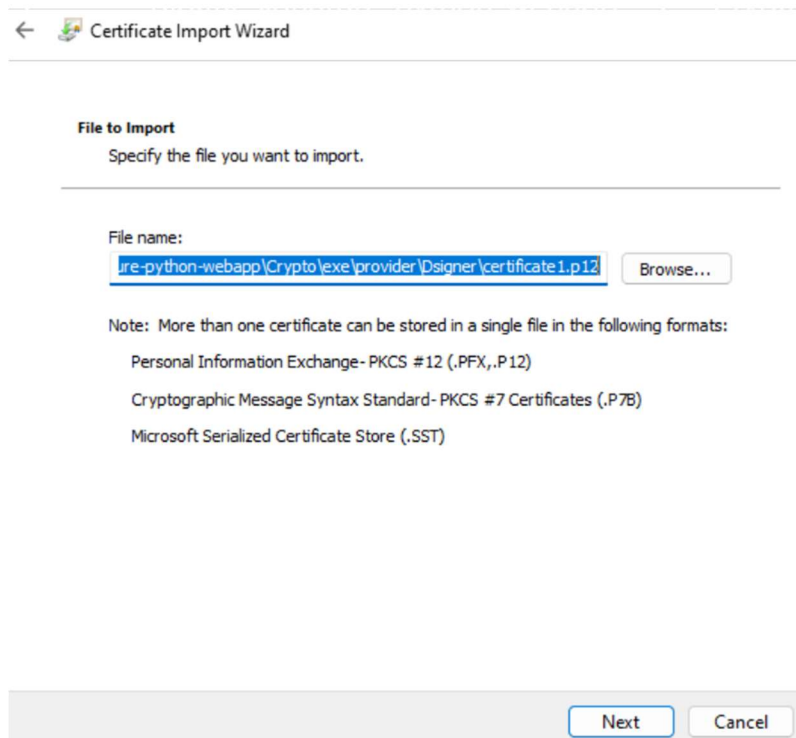
Certificate "localhost" already in store.
CertUtil: -addstore command completed successfully.

C:\Windows\System32>
```

12) Now you need to install the Soft Token, also known as the Digital Certificate. You will find it in the folder you extracted earlier. Double-click the file to begin the installation.



13) Click on the 'Next' button.



← Certificate Import Wizard

**File to Import**  
Specify the file you want to import.

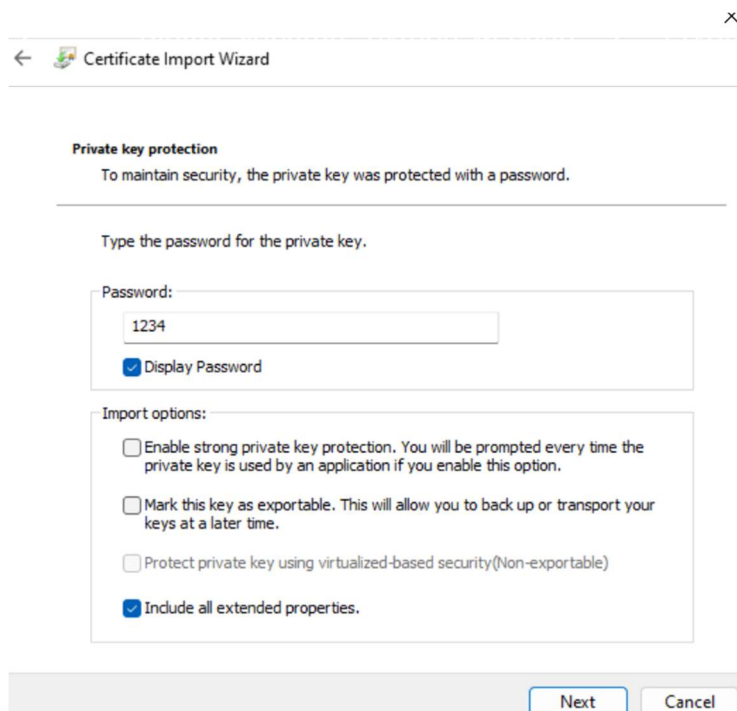
File name:  
ire-python-webapp\Crypto\exe\provider\Designer\certificate1.p12 Browse...

Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

Next Cancel

14) Enter the password '1234'. If you want a password prompt each time you sign a PDF or use this certificate, enable 'Strong private key protection'. Then click 'Next'.



×

← Certificate Import Wizard

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

Type the password for the private key.

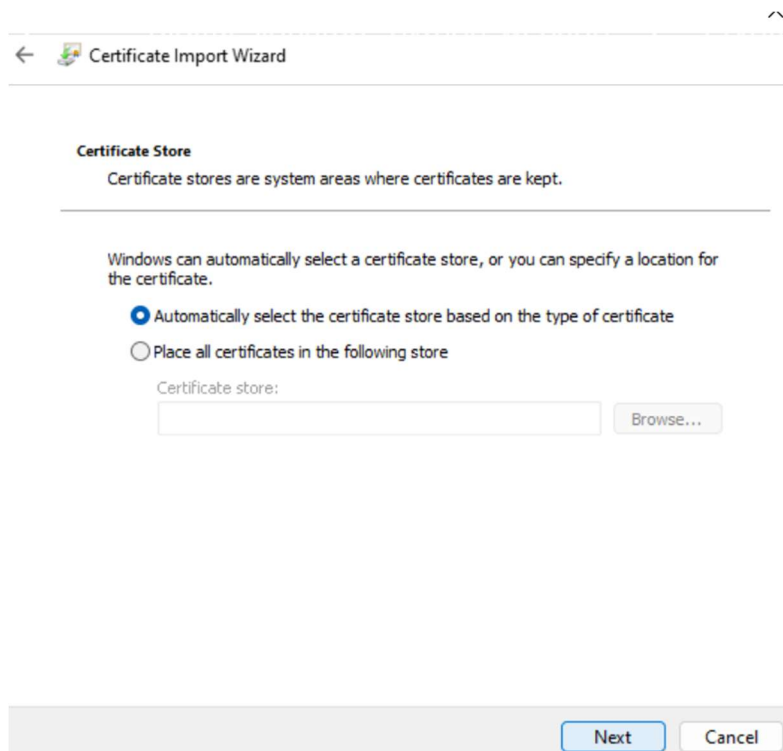
Password:  
1234  
☒ Display Password

Import options:

- ☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
- ☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
- ☐ Protect private key using virtualized-based security(Non-exportable)
- ☒ Include all extended properties.

Next Cancel

15) Click on the 'Next' button.



← Certificate Import Wizard

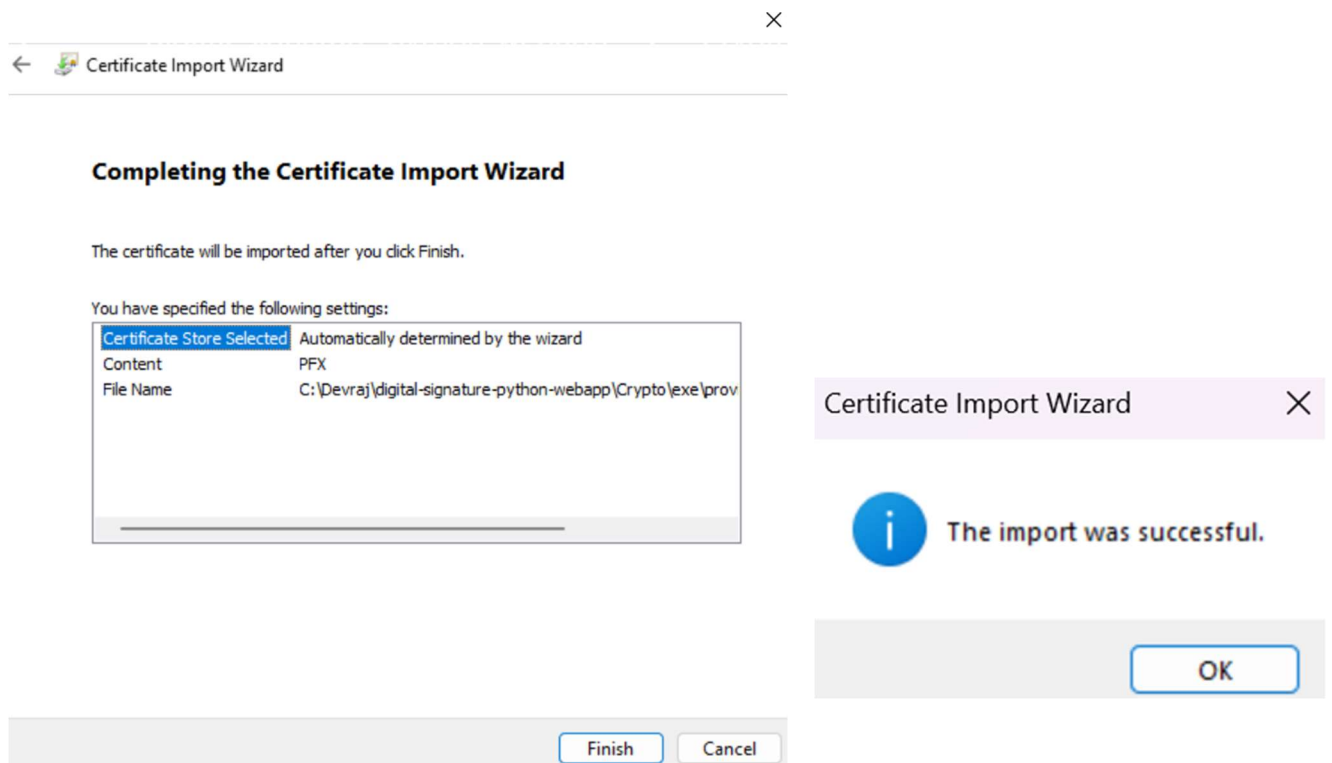
**Certificate Store**  
Certificate stores are system areas where certificates are kept.

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

☒ Automatically select the certificate store based on the type of certificate  
☐ Place all certificates in the following store

Certificate store:

16) Click on the 'Finish' button.



×

← Certificate Import Wizard

**Completing the Certificate Import Wizard**

The certificate will be imported after you click Finish.

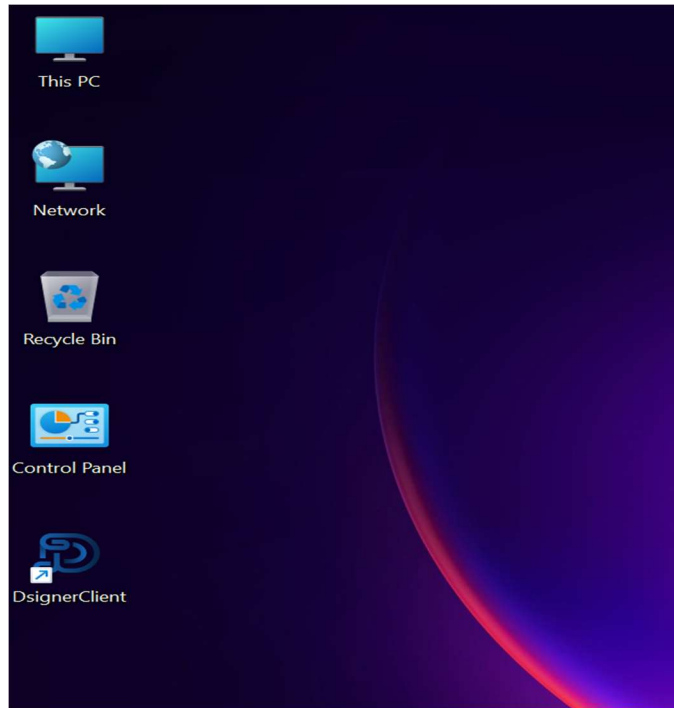
You have specified the following settings:

|                            |                                                           |
|----------------------------|-----------------------------------------------------------|
| Certificate Store Selected | Automatically determined by the wizard                    |
| Content                    | PFX                                                       |
| File Name                  | C:\Devraj\digital-signature-python-webapp\Crypto\exe\prov |

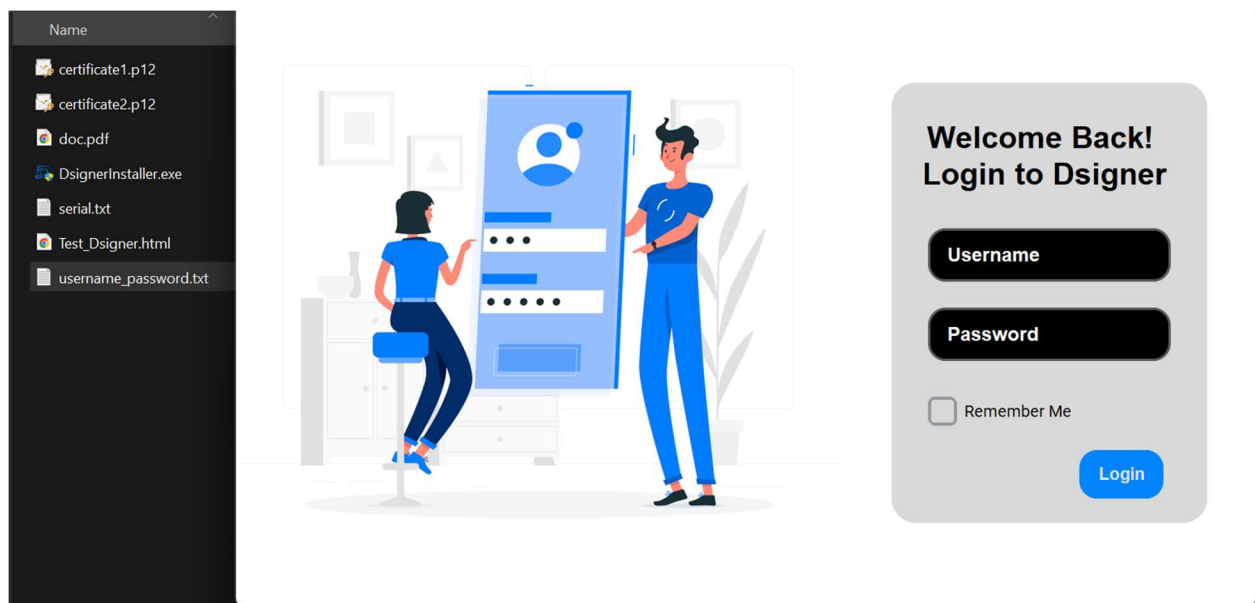
**Certificate Import Wizard** ×

 The import was successful.

17) Now you're ready to run Dsigner. Click on the desktop shortcut to open it.

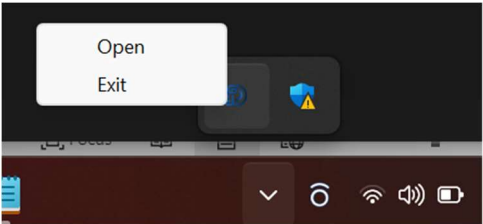


18) You will now be prompted to enter your username and password. You can find them in the extracted folder, inside the *username\_password.txt* file. The validity depends on your subscription plan. Enter the credentials and click 'Login'.

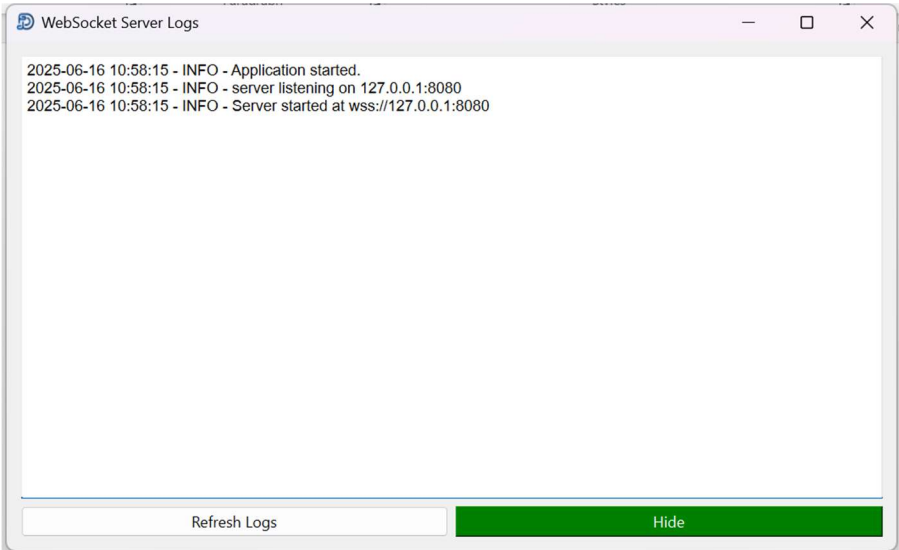




19) Once your login is validated, Dsigner will start running. You will see the Dsigner icon in the taskbar tray. Right-click the icon and select 'Open'.



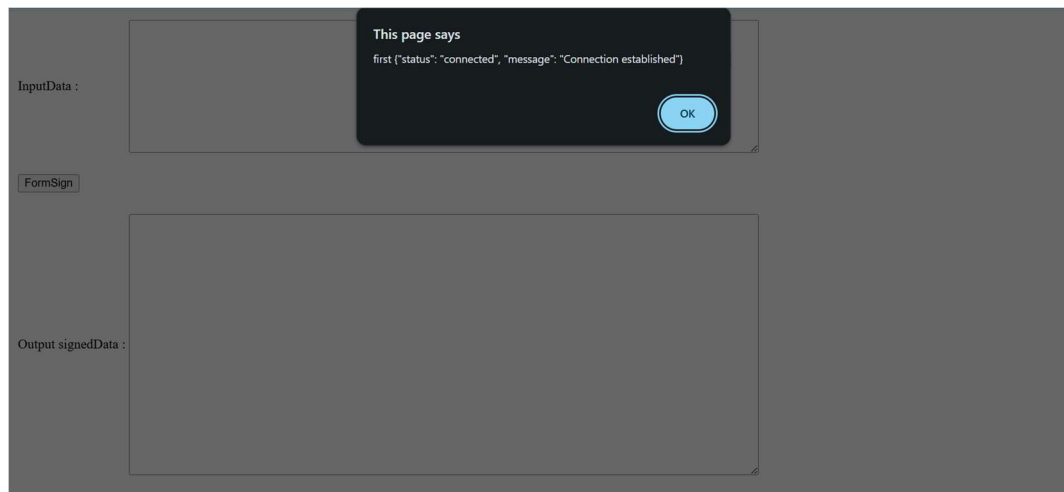
20) Here, you will see that Dsigner is ready to accept connections on the specified port using the WSS protocol.



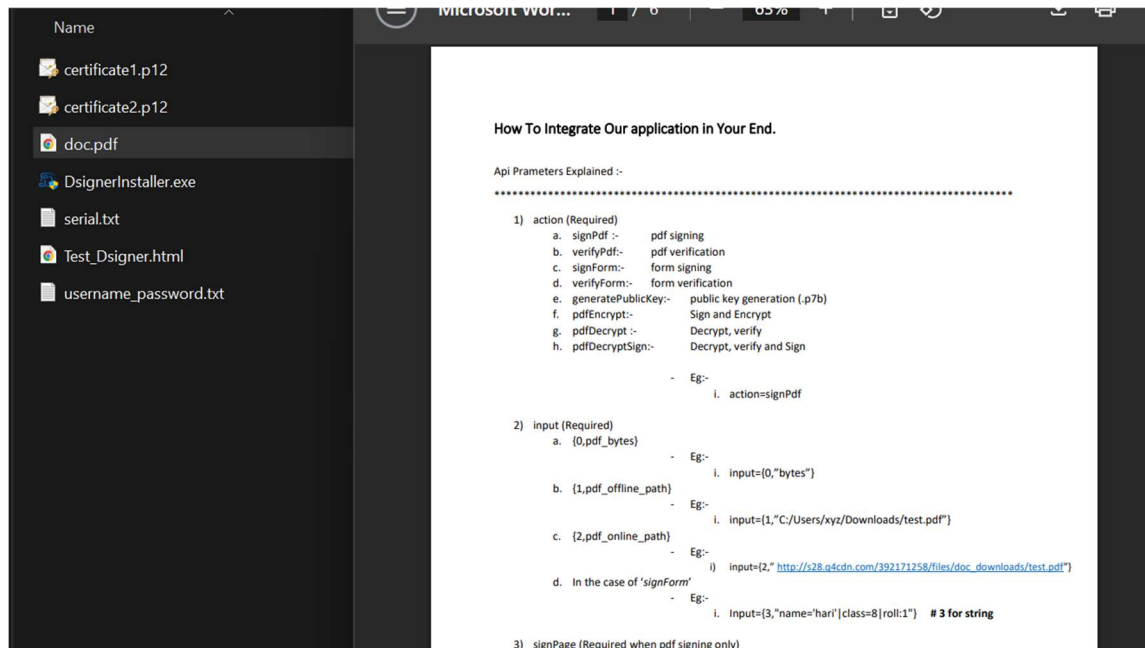
21) Now open the extracted folder. There is a file named *Test\_Dsigner.html* which you can use to test and sign files offline. You can also use its code as a reference to integrate Dsigner with your application.

| Name                  | Date modified       | Type                     | Size       |
|-----------------------|---------------------|--------------------------|------------|
| certificate1.p12      | 12/26/2024 6:01 PM  | Personal Information ... | 5 KB       |
| certificate2.p12      | 12/26/2024 11:35 AM | Personal Information ... | 5 KB       |
| doc.pdf               | 4/17/2025 4:00 PM   | Chrome HTML Docu...      | 1,124 KB   |
| DsignerInstaller.exe  | 6/6/2025 1:10 PM    | Application              | 159,190 KB |
| serial.txt            | 3/31/2025 12:16 PM  | Text Document            | 1 KB       |
| Test_Dsigner.html     | 3/30/2025 5:04 PM   | Chrome HTML Docu...      | 3 KB       |
| username_password.txt | 6/9/2025 3:17 PM    | Text Document            | 1 KB       |

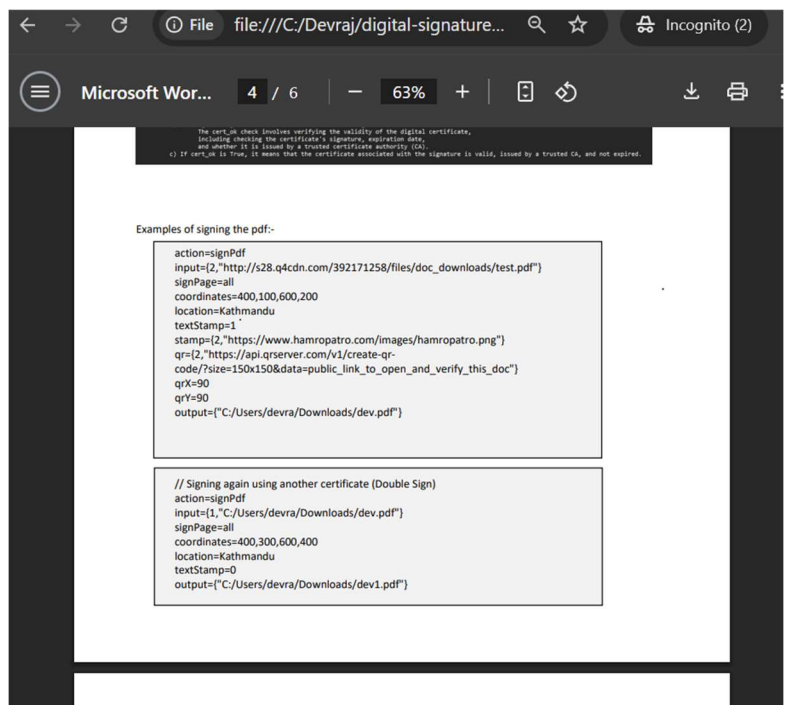
22) Once you open the HTML file, you will see that the connection is successful.



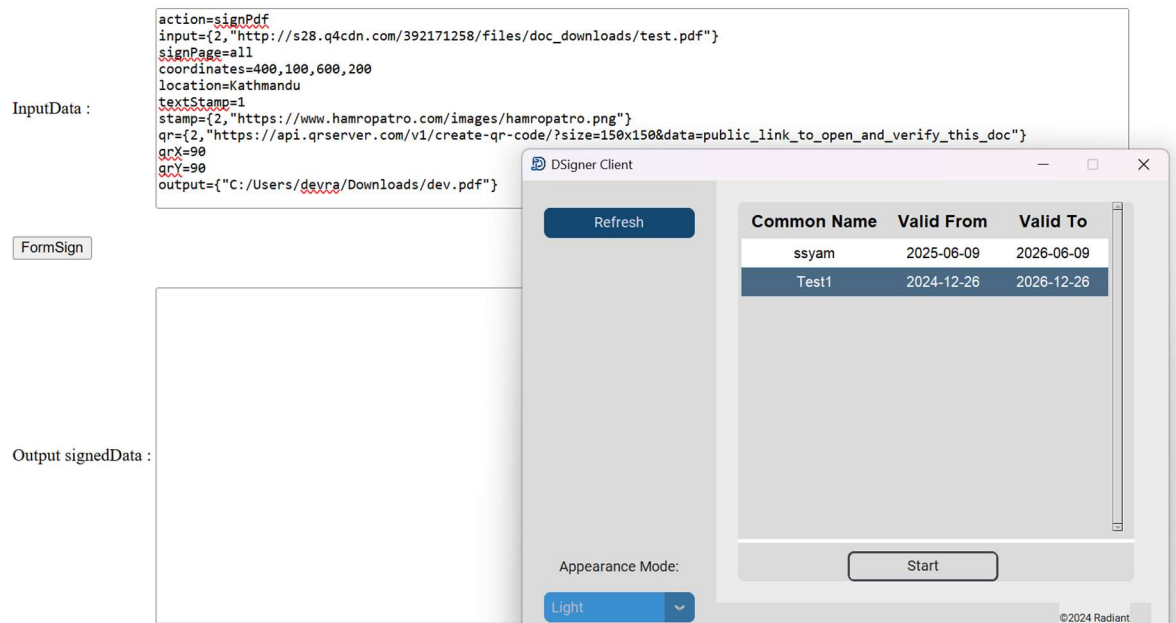
23) For the API documentation, there is a file named *doc.pdf* in the extracted folder. Open and read it to learn how to use the API for signing PDFs, validating signatures, or signing and validating forms.



24) Below are examples demonstrating how to sign a PDF.



25) Here, we have used the above example to sign a PDF using the *Test\_Dsigner.html* file. When you enter all the API parameters correctly and click the 'Sign' button, the Dsigner popup will appear showing the certificates you previously installed. If the popup does not appear, you can check the logs by opening the Dsigner icon in the system tray to identify the problem.



InputData :

FormSign

Output signedData :

# Thank You.