

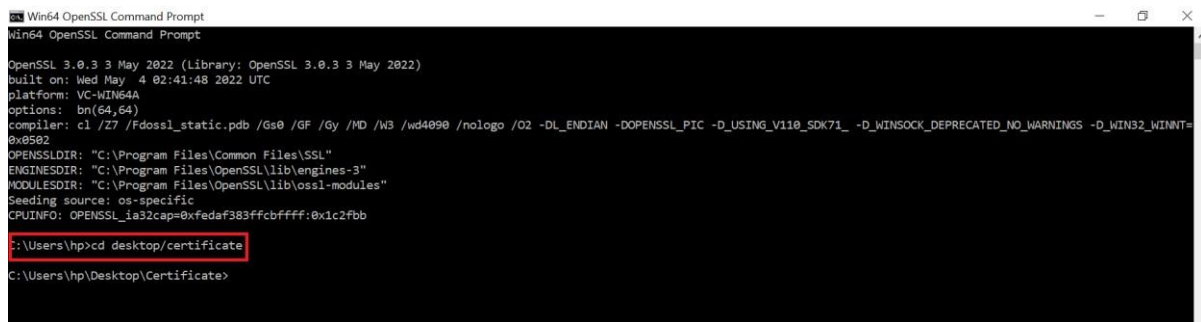
Certificate Creation for accessing SDR API

Certificate can be created by using any one of the below two options.

- PowerShell
- Open SSL

Option 1: Certificate generation with Open SSL

1. Install the Open SSL.
2. Run the OpenSSL Command Prompt and set the directory to the folder where certificate to be stored.



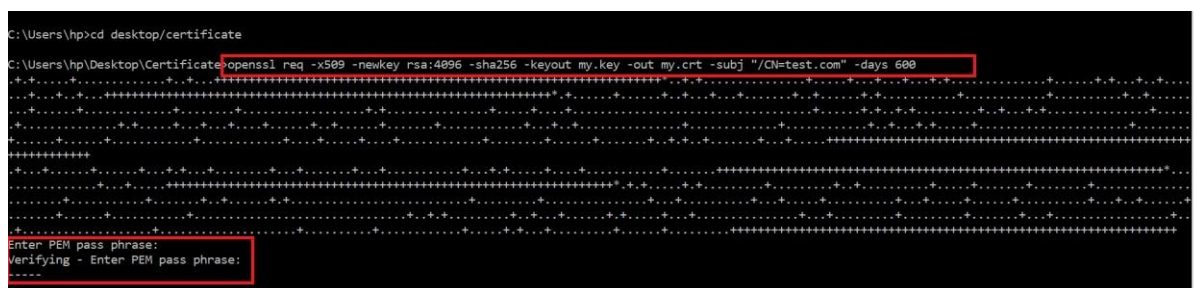
```
Win64 OpenSSL Command Prompt
Win64 OpenSSL Command Prompt

OpenSSL 3.0.3 3 May 2022 (Library: OpenSSL 3.0.3 3 May 2022)
built on: Wed May  4 02:41:48 2022 UTC
platform: VC-WIN64A
options: bn(64,64)
compiler: cl /Z7 /Fdssl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nologo /O2 -DL_ENDIAN -DOPENSSL_PIC -DUSING_V110_SDK71_ -D_WINSOCK_DEPRECATED_NO_WARNINGS -D_WINS32_WINNT=0x0502
OPENSSLDIR: "C:\Program Files\Common Files\SSL"
ENGINESDIR: "C:\Program Files\OpenSSL\lib\engines-3"
MODULESDIR: "C:\Program Files\OpenSSL\lib\openssl-modules"
Seeding source: os-specific
CPUINFO: OpenSSL_1a32cap=0xfedaf383ffcbffff:0x1c2fbb

C:\Users\hp>cd desktop/certificate
C:\Users\hp\Desktop\Certificate>
```

3. Run the below command ⑦ provide **Enter PEM pass phrase** and save the pass phrase to provide it on the command to generate .pfx certificate.

```
openssl req -x509 -newkey rsa:4096 -sha256 -keyout my.key -out my.crt -subj
"/CN=test.com" -days 600
```



```
C:\Users\hp>cd desktop/certificate
C:\Users\hp\Desktop\Certificate>openssl req -x509 -newkey rsa:4096 -sha256 -keyout my.key -out my.crt -subj "/CN=test.com" -days 600
.....
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
```

4. Run the below command to generate the .pfx certificate.

```
openssl pkcs12 -export -name "test.com" -out my.pfx -inkey my.key -in my.crt
```

Provide the below details:

Disclaimer

These materials and information, as well as the underlying code/application they relate to, are provided by TransCelerate Biopharma Inc. AS IS. Any party using or relying on this information, these materials, and/or the underlying code/application do so entirely at their own risk. Neither TransCelerate nor its members will bear any responsibility or liability for any harm, including indirect or consequential harm, that a user may incur from use or misuse of this information, materials, or underlying code/application. TransCelerate does not endorse any particular software, system, or service.

- Enter pass phrase for my.key: Provide the pass phrase passed on step 3
- Enter Export Password: Provide the password for .pfx certificate and save it for later use.

```
C:\Users\hp\Desktop\Certificate>openssl req -x509 -newkey rsa:4096 -sha256 -keyout my.key -out my.crt -subj "/CN=test.com" -days 600
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
C:\Users\hp\Desktop\Certificate>openssl pkcs12 -export -name "test.com" -out my.pfx -inkey my.key -in my.crt
Enter pass phrase for my.key:
Enter Export Password:
Verifying - Enter Export Password:
```

5. Exported .pfx certificate will be stored in the directory where OpenSSL was installed.

MacOS users can generate the client certificate using OpenSSL option mentioned above. Since MacOS comes with OpenSSL pre-installed, users can skip step 1 and follow the rest to create a client certificate.

Note: Share the .pfx certificate and the export password to SDR Support Team to get access to SDR API's on Demo Environment.

Option 2: Certificate generation with PowerShell

1. Open PowerShell and run the below command to generate the self-signed certificate

New-SelfSignedCertificate -certstorelocation cert:\CurrentUser\My\ -dnsname example.com

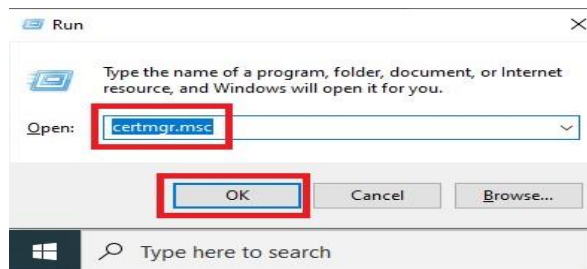
```
Windows PowerShell
PS C:\> New-SelfSignedCertificate -certstorelocation cert:\CurrentUser\My\ -dnsname example.com

PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

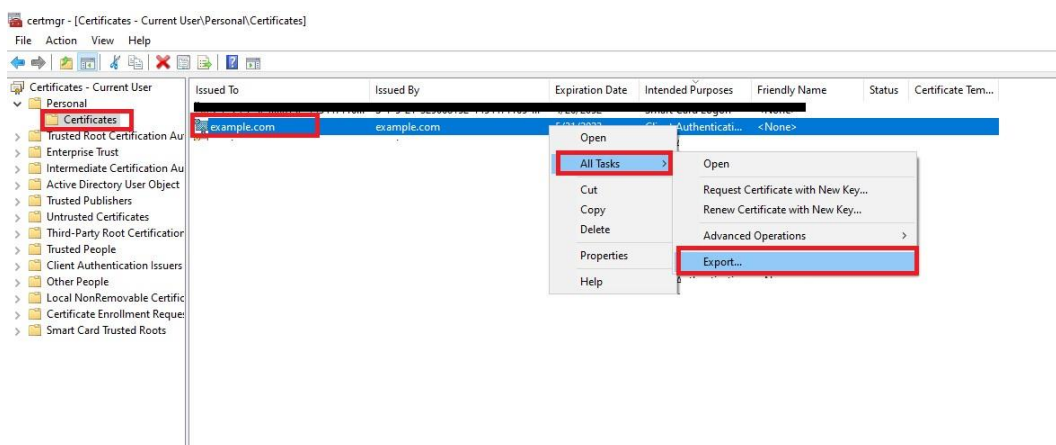
Thumbprint                               Subject
-----
6627DBCEEAB7A9AF558009FC04FF5CA1FFFBC1B  CN=example.com

PS C:\>
```

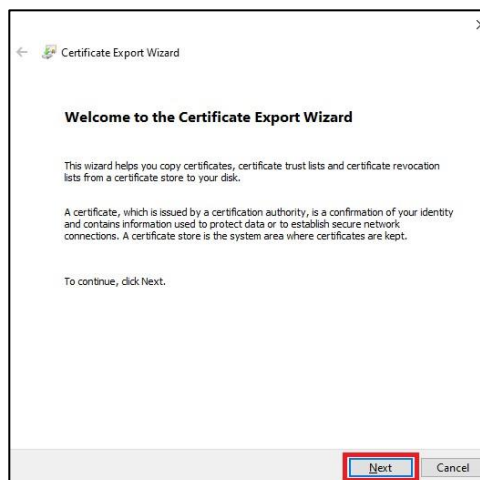
2. To Export the certificate in .pfx format, go to run → type certmgr.msc and click ok



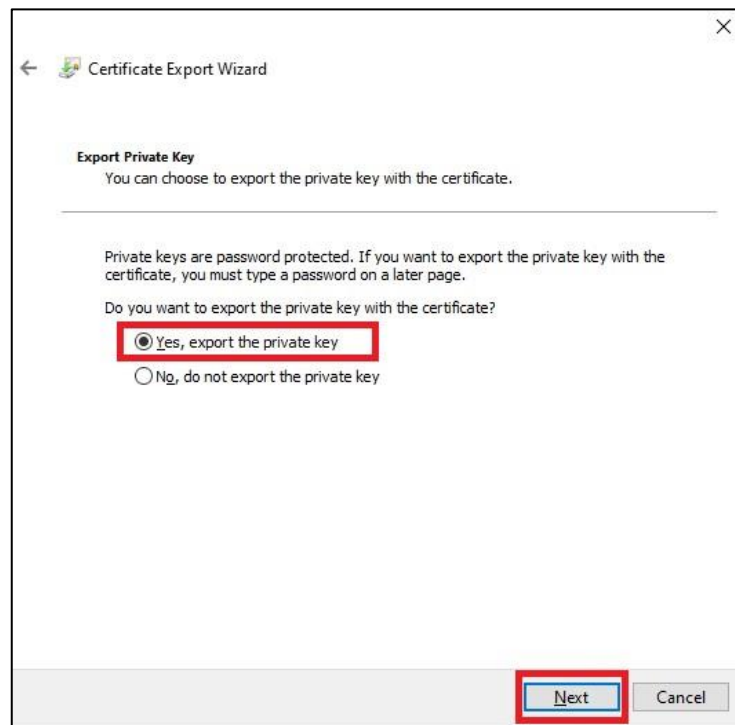
3. In certificate manager go to personal → certificates → select the generated certificate and right click select All Tasks → Select Export.



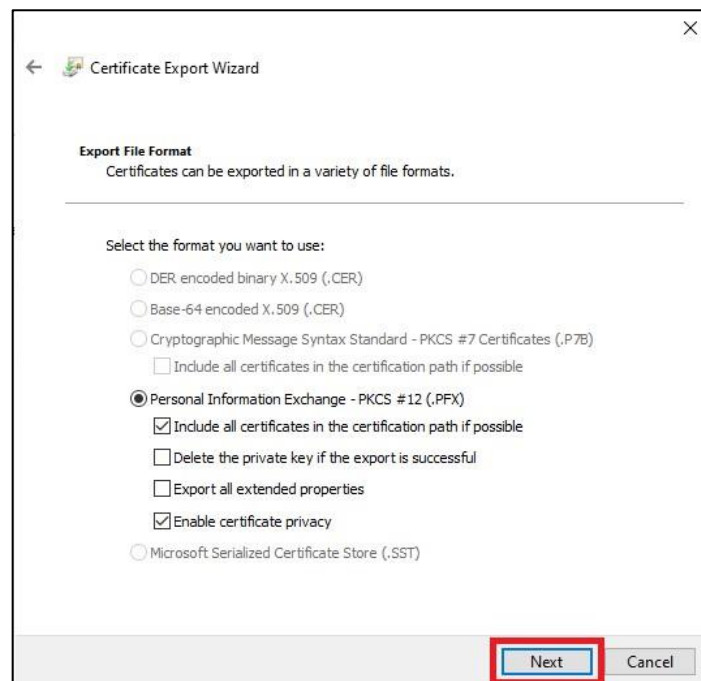
4. In Certificate Export Wizard click Next to continue.



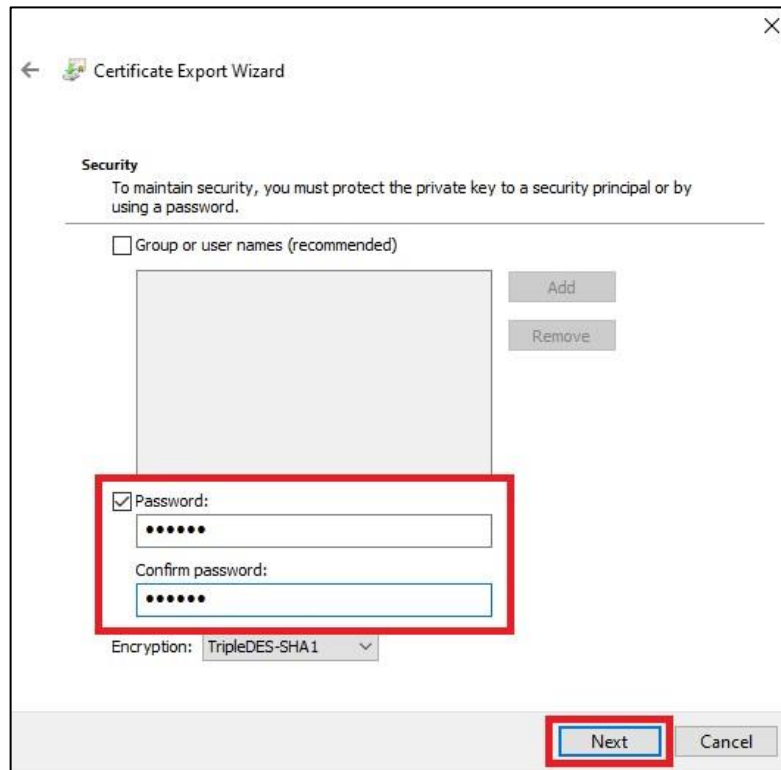
5. Select export the private key option and click next.



6. Leave the defaults and click next.

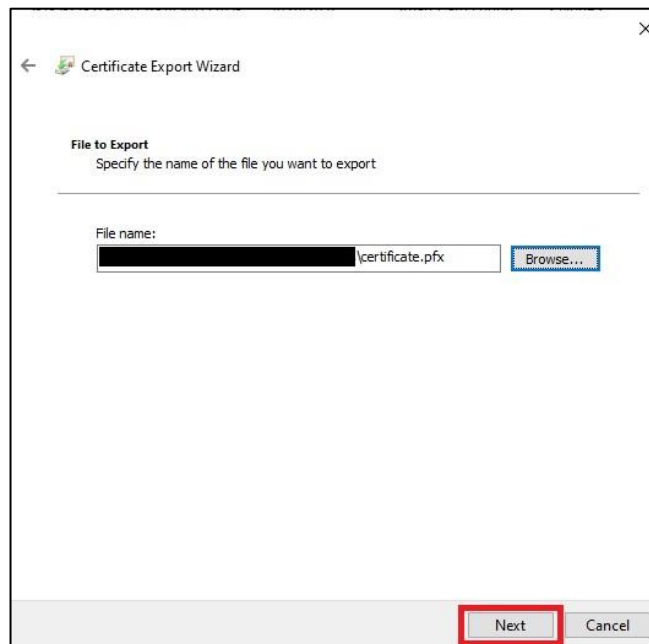


7. Provide the password for certificate and click next.



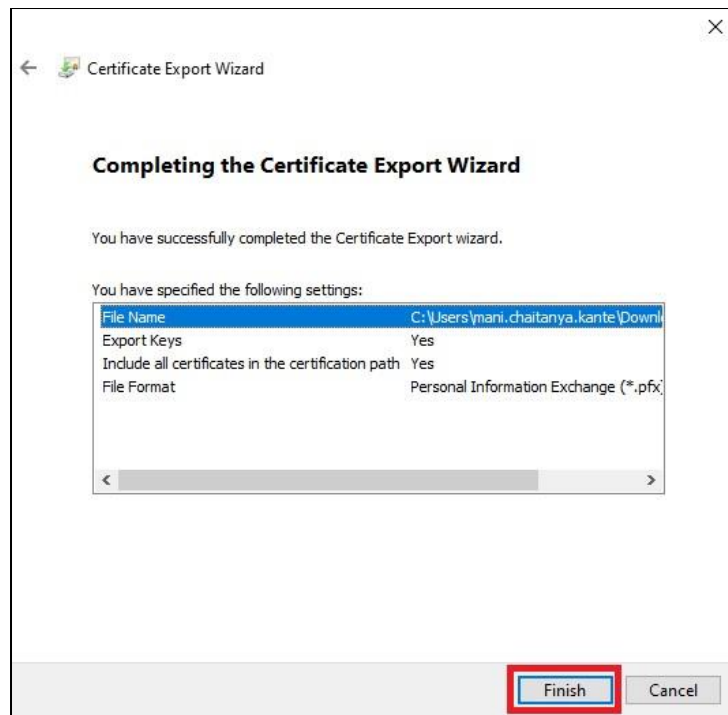
The screenshot shows the 'Security' step of the 'Certificate Export Wizard'. The window title is 'Certificate Export Wizard'. Below the title bar, there is a back arrow and a small icon. The main heading is 'Security'. Below it, a text box states: 'To maintain security, you must protect the private key to a security principal or by using a password.' There are two options: 'Group or user names (recommended)' with an unchecked checkbox, and 'Password' with a checked checkbox. The 'Password' option is highlighted with a red rectangle. Below the 'Password' checkbox, there are two text boxes: 'Password:' and 'Confirm password:', both containing six dots. Below these, there is a dropdown menu for 'Encryption:' set to 'TripleDES-SHA1'. To the right of the list box, there are 'Add' and 'Remove' buttons. At the bottom right, there are 'Next' and 'Cancel' buttons, with the 'Next' button highlighted by a red rectangle.

8. Select the path and provide certificate name to save the certificate.



The screenshot shows the 'File to Export' step of the 'Certificate Export Wizard'. The window title is 'Certificate Export Wizard'. Below the title bar, there is a back arrow and a small icon. The main heading is 'File to Export'. Below it, a text box states: 'Specify the name of the file you want to export.' There is a 'File name:' label followed by a text box containing 'certificate.pfx'. To the right of the text box is a 'Browse...' button. At the bottom right, there are 'Next' and 'Cancel' buttons, with the 'Next' button highlighted by a red rectangle.

9. Click on Finish.



10. Exported .pfx certificate will be stored on the folder path provided on step 8.

Note: Share the .pfx certificate and the password to SDR Support team to get access to SDR APIs .