Guide to generate Certificate Signing Request for Netrust Certificates - Singpass/Myinfo/Verify/SafeEntry

Version 1.1
Authored by: Netrust Support

Identification

Document Name:	Singpass/Myinfo/SafeEntry Certificate
Document Author:	Netrust Support
Document Version:	1.1
This update is by:	

Revision History

Version	Effective Date	Summary of Changes	Author
1.0		Initial Release	Netrust Support
1.1	18 Jan 2023	Update Netrust Logo	Customer Support – Shalini

Table of Contents

1. Introduction

Netrust offers x509 seSrver certificates for Singpass applications, such as Singpass/Corppass Login, Myinfo, SafeEntry and Verify, for both the government and private sectors. Being the only local compatible Certificate Authority in Singapore, Netrust fully understands Singpass requirements and is well-positioned to support your organization's integration with Singpass. Apart from providing digital certificates for Singpass applications, Netrust has developed authentication modules that allow ease of integration with Singpass/CorpPass, Singpass Login, Verify and Myinfo.

Notes: Netrust x509 server certificates for Singpass applications are not use for hosting website.

Website Certificate is using SSL Certificate.

2. What is Singpass Certificate

Login with Singpass enables residents' easy access to government and private sector digital services. Using the Singpass Mobile app, residents can securely log in to digital services, without the need of a password.

This service provides businesses with an accessible and established login platform for all their digital services.

3. What is Myinfo Certificate

Designed by the Government, Myinfo is a service that enables citizens and residents to manage the use of their personal data for simpler online transactions. Users control and consent to the sharing of their data, and can view a record of past usage.

4. What is SafeEntry Certificate

SafeEntry is a national digital check-in system which logs visits by individuals to hotspots and venues providing essential services, as well as employees of essential services.

Individuals visiting these premises are required to provide key information (e.g. NRIC and mobile number). After scanning the location's QR code, they will need to key in their details

5. What is Certificate Signing Request (CSR)

A certificate signing request (also CSR or certification request) is a message sent from an applicant to a registration authority of the public key infrastructure in order to apply for a digital identity certificate. It usually contains the public key for which the certificate should be issued, identifying information (such as a domain name) and integrity protection (e.g., a digital signature). The most common format for CSRs is the PKCS #10 specification; another is the Signed Public Key and Challenge SPKAC format generated by some web browsers.

6. How to generate X509 Certificate Signing Request (CSR)

There are a few option for you to generate an x509 Certificate. The following any Option below will help able to generate the CSR for Netrust to sign an x509 Certificate

6.1. Option 1: OpenSSL

Complete the following steps to create your CSR.

The process below will guide you through the steps of creating a Private Key and CSR.

IMPORTANT: The private key is not to be shared by anyone, sharing of the private key is against best practice. If you require to share the private key it is best to transfer in a secure manner and not through open communication such as unencrypted email. DO NOT provide NETRUST with the private key.

1. Launch the OS Terminal or Command Prompt:
   SHA-2 signing algorithm:
   Type the following command: openssl req -new -newkey rsa:2048 –sha256 -nodes -keyout server.key -out server.csr
   PLEASE NOTE: Replace "server.key" and "server.csr" with your own values

2. Once prompted for a "Common Name" enter the Fully Qualified Domain Name (FQDN) that you wish to secure in the certificate
   For Wildcard: If you are going to be requesting a Wildcard Certificate you will need to place an asterisk * in front of the domain (e.g. *.entrust.com)
   You will also be prompted for the following information:

Attribute	Prefix	Description	Example
Country/Region	C	Business Location - Country	SG
State/Province	ST	Business Location - State/Province	Singapore
City/Locality	L	Business Location - City	Singapore
Organization Unit	OU	Organization Unit if required to be listed*	***Optional****
Organization	O	Organization's legal business name	My Company Name
Common Name	CN	Domain to be secured by certificate	www.mydomain.com

PLEASE NOTE: Do not use a Challenge Password

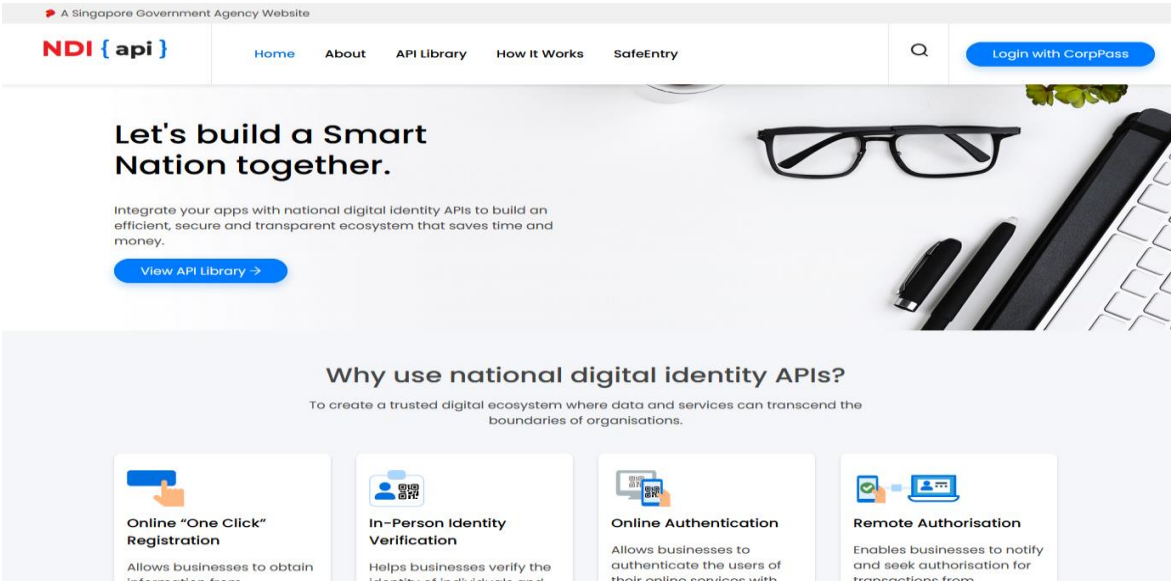
Command Output Sample:

```
[User@localhost ~]$ openssl req -new -newkey rsa:2048 -nodes -keyout server.key -
out server.csr
Generating a 2048 bit RSA private key
.....................................................................+++
.....................................+++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:SG
State or Province Name (full name) []:Singapore
Locality Name (eg, city) [Default City]: Singapore
Organization Name (eg, company) [Default Company Ltd]:MyCompany
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:www.mydomain.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

3. You will now have a Private Key and CSR, the CSR contents are used to submit the request to Entrust to issue the certificate. You can view the contents of the CSR by opening the file within a basic text editor, to confirm the information is correct use the Entrust CSR viewer to parse the information within the CSR: http://www.entrust.net/ssl-technical/csr-viewer.cfm

4. Once Netrust Sign the x509 Certificate (Sample of x509 file extension commonname.der, commonname.cer or commonname.crt), please Login to https://www.ndi-api.gov.sg/ with CorpPass login.



5. Upload the Netrust Sign x509 Certificate to ndi-api Portal.

For more Technical Queries on ndi-api please email: support@Myinfo.gov.sg

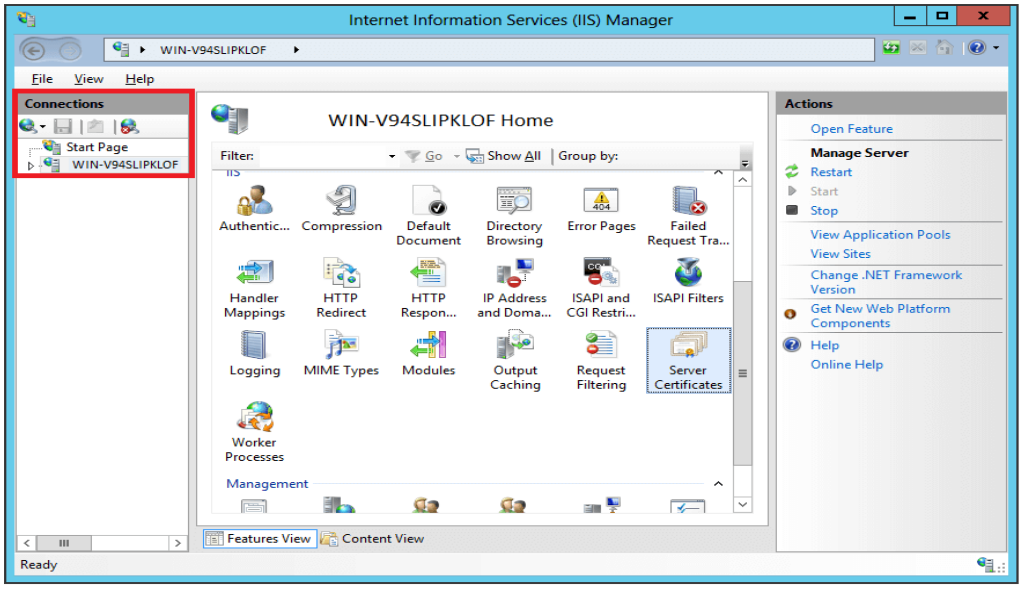
6.2. Option 2: Microsoft IIS 8/8.5

Complete the following steps to create your CSR.

1. Open Internet Information Services (IIS) Manager

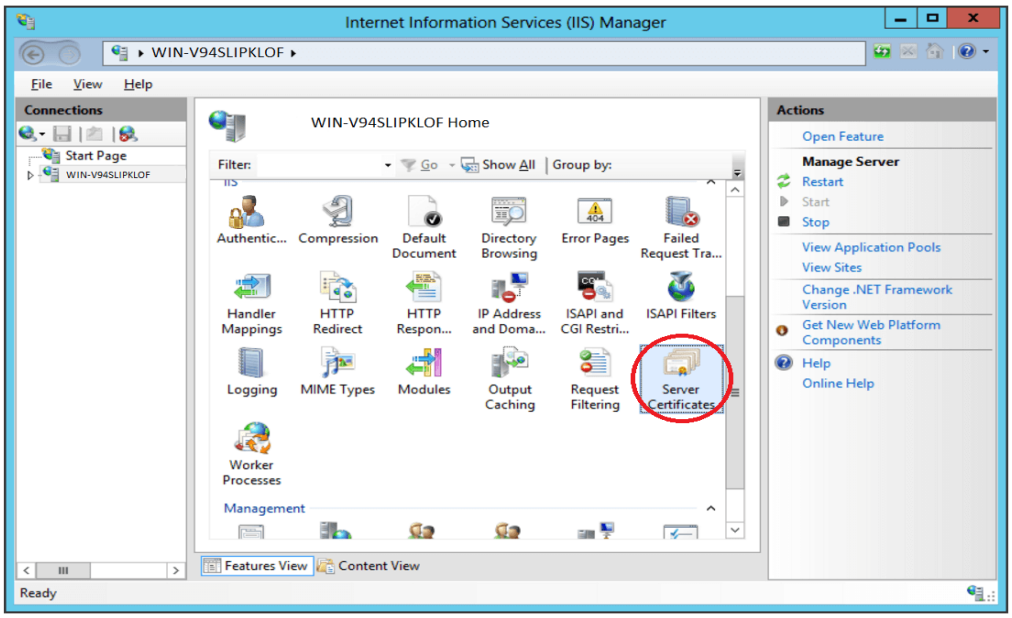
   Click Start, Control Panel, System and Security, Administrative Tools, and then select Internet Information Services (IIS) Manager.

2. Select the server where you want to generate the certificate
   In the left Connections menu, select the server name (host) where you want to generate the request.



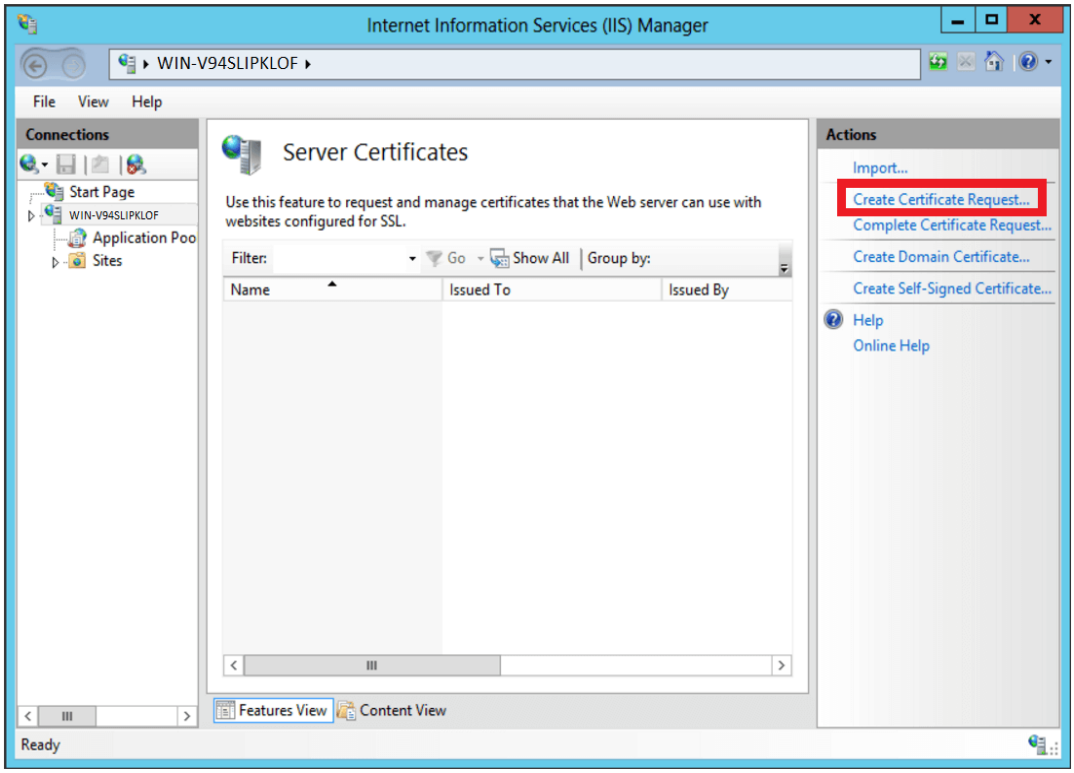
3. Navigate to Server Certificates

   In the center menu, click the Server Certificates icon under the Security section near the bottom.



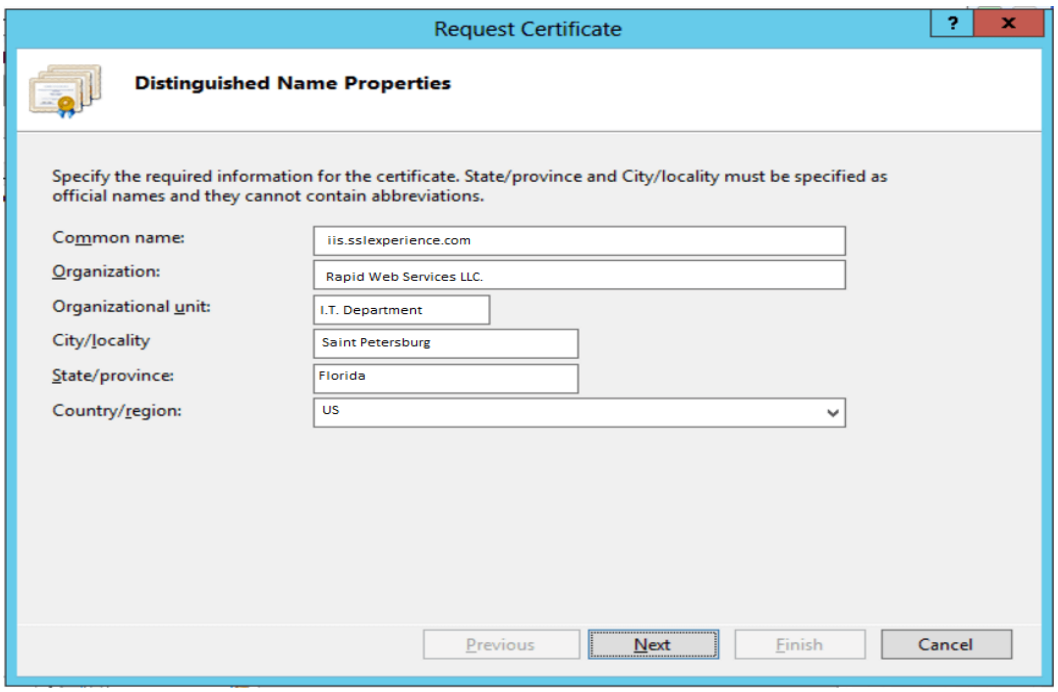
4. Select Create a New Certificate

   In the right Actions menu, click Create Certificate Request.



5. Enter your CSR details

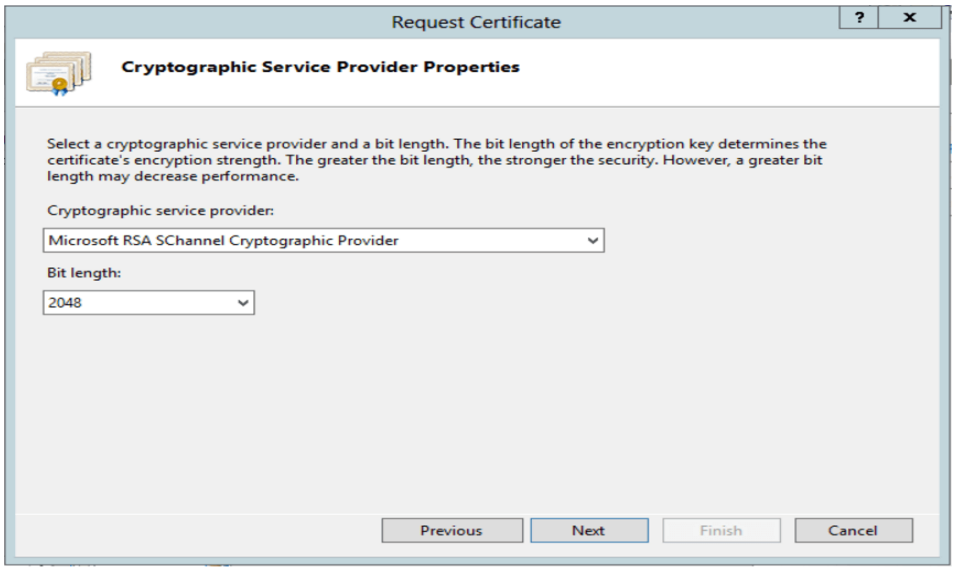
   In the Distinguished Name Properties window, enter in the required CSR details and then click Next.



Note: *To avoid common mistakes when filling out your CSR details, reference our Overview of Certificate Signing Request article.*

6. Select a cryptographic service provider and bit length

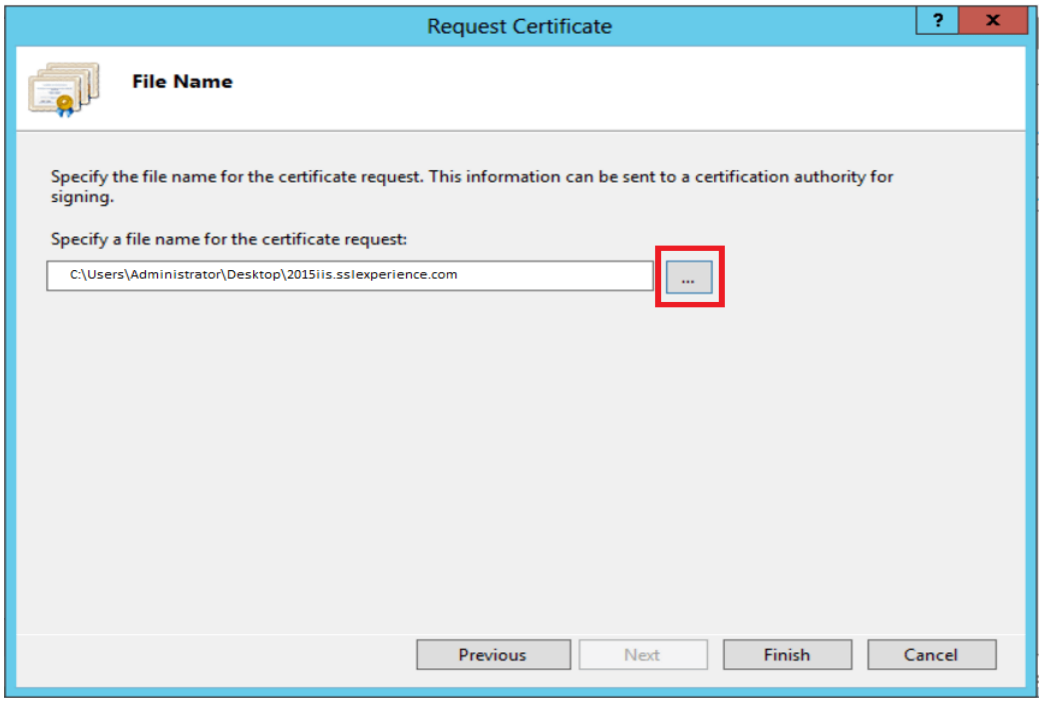
   In the Cryptographic Service Provider Properties window, select Microsoft RSA SChannel Cryptographic Provider and Bit Length of 2048, then click Next.



Note*: Bit Length: 2048 is the current industry standard. You may choose a larger key size, but only if you have a requirement to do so, as longer key lengths increase latency and may reduce compatibility.*

7. Save the CSR

   Click Browse to specify the location where you want to save the CSR as a ".txt" file and click Finish.



8. Generate the Order

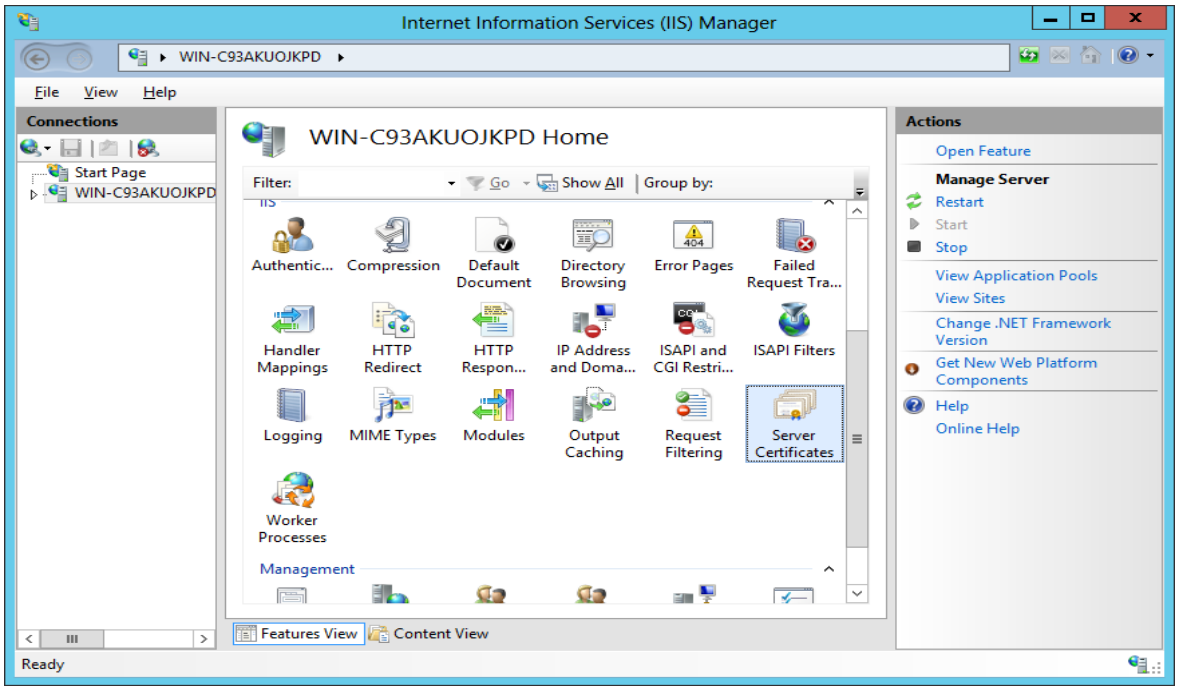
   Locate and open the newly created CSR from the specified location you choose in a text editor such as Notepad and copy all the text including:

   -----BEGIN CERTIFICATE REQUEST-----
   And
   -----END CERTIFICATE REQUEST-----

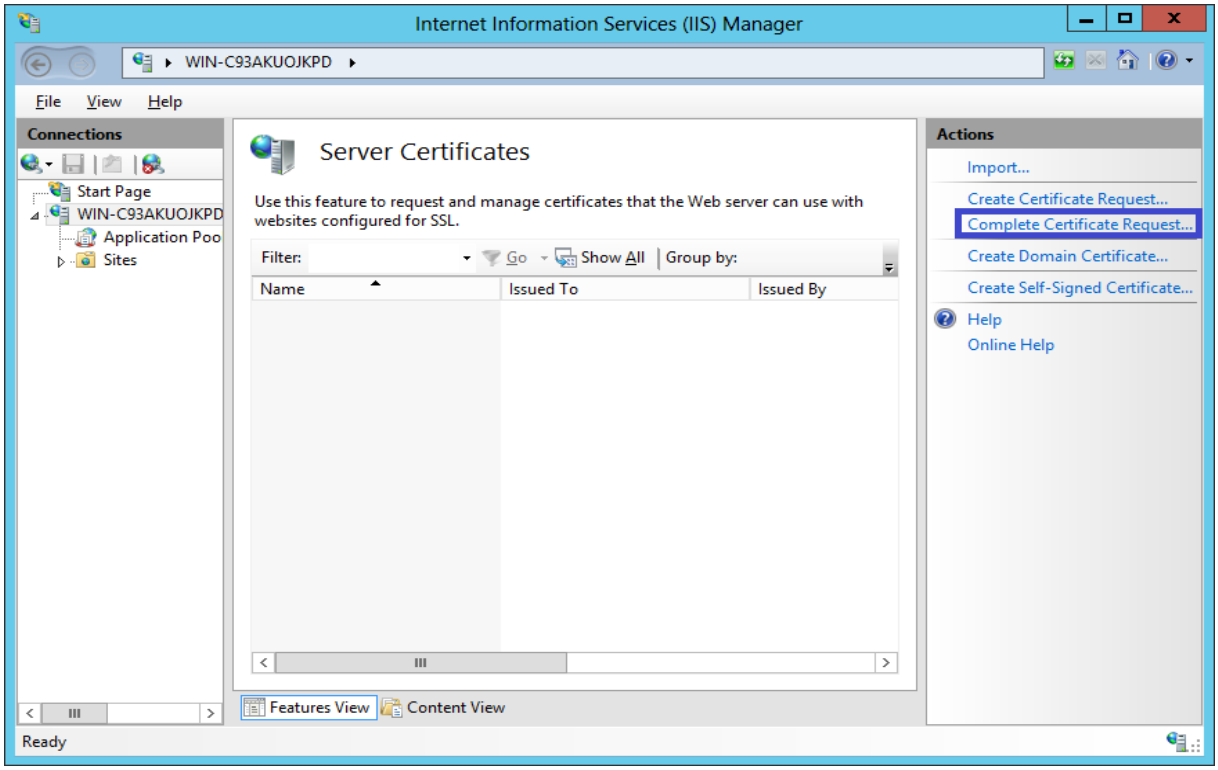
9. Install Your Certificate

   On the server where you created the CSR, save the SSL certificate .cer file (e.g., your_domain_com.cer) that you received from Netrust.
   From the Start screen, find Internet Information Services (IIS) Manager and open it.
   In the Connections pane, locate and click the server.

In the server Home page (center pane) under the IIS section, double-click Server Certificates.



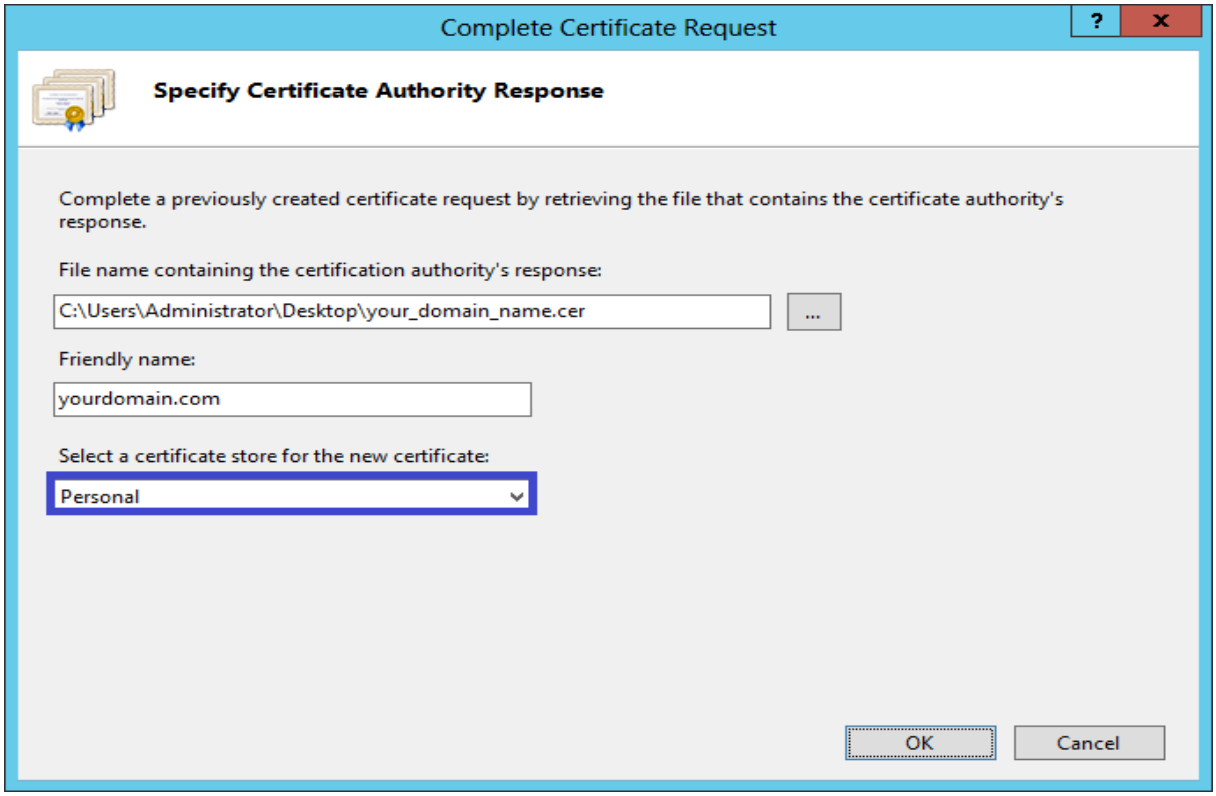
10. In the Actions menu (right pane), click Complete Certificate Request.



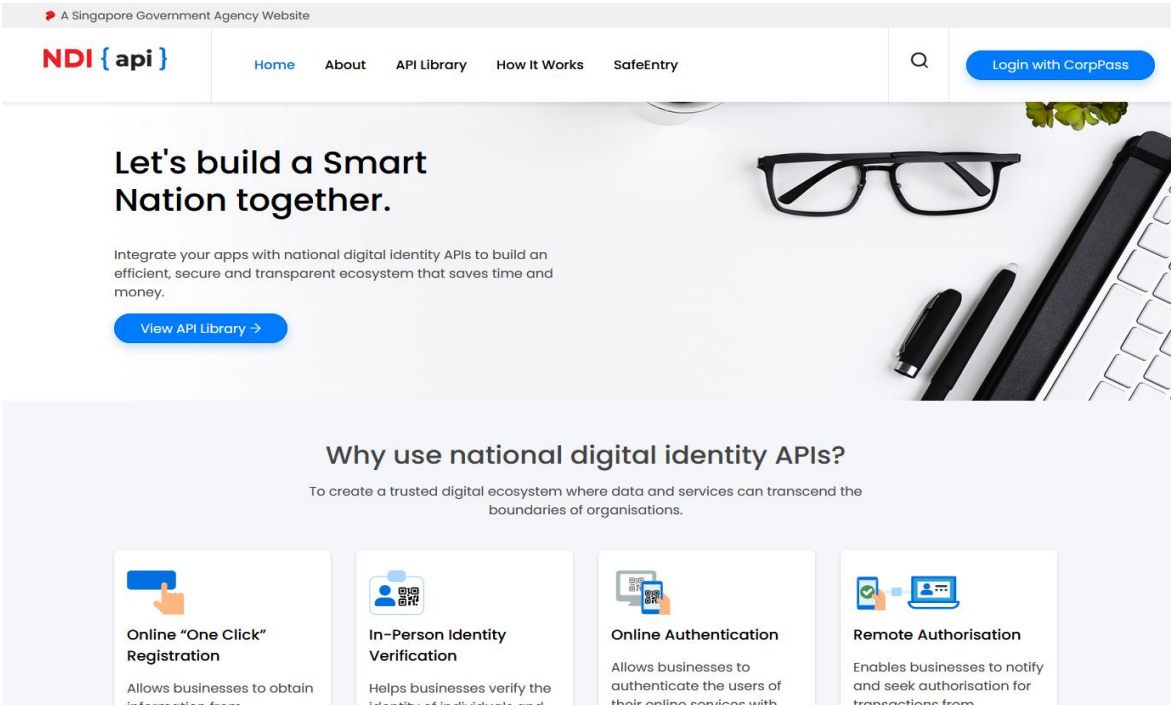
11. In the Complete Certificate Request wizard, on the Specify Certificate Authority Response page, provide the following information:

File name containing the certificate authority's response:	Click the … button to locate the .cer file you received from Netrust

	(e.g., your_domain_com.cer).
Friendly name:	Type a friendly name for the certificate. This is not part of the certificate; instead, it is used to identify the certificate.
Select a certificate store for the new certificate:	In the drop-down list, select Personal.



12. Click OK to install the certificate.
13. Now that you've successfully installed your certificate.
    DO not bind the Netrust x509 Certificate on your website for testing.
14. Once Netrust Sign the x509 Certificate (Sample of x509 file extension commonname.der, commonname.cer or commonname.crt), please Login to https://www.ndi-api.gov.sg/ with CropPass login.



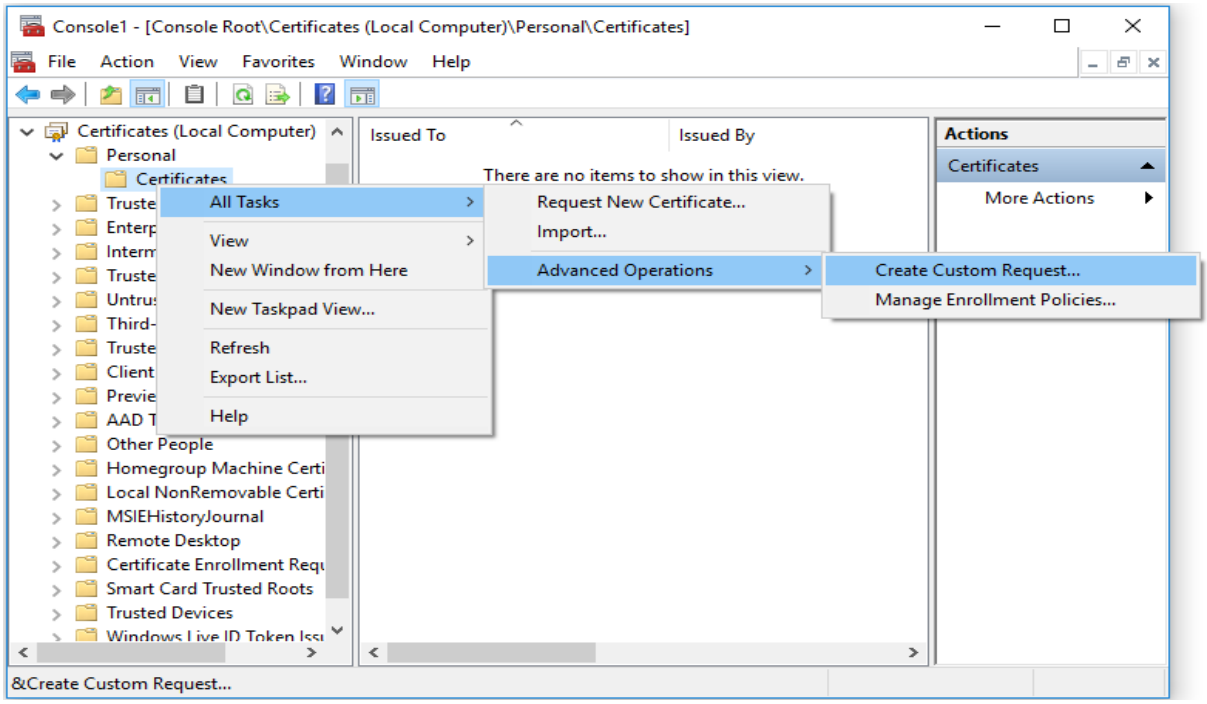
15. Upload the Netrust Sign x509 Certificate to ndi-api Portal.

For more Technical Queries on ndi-api please email: support@Myinfo.gov.sg

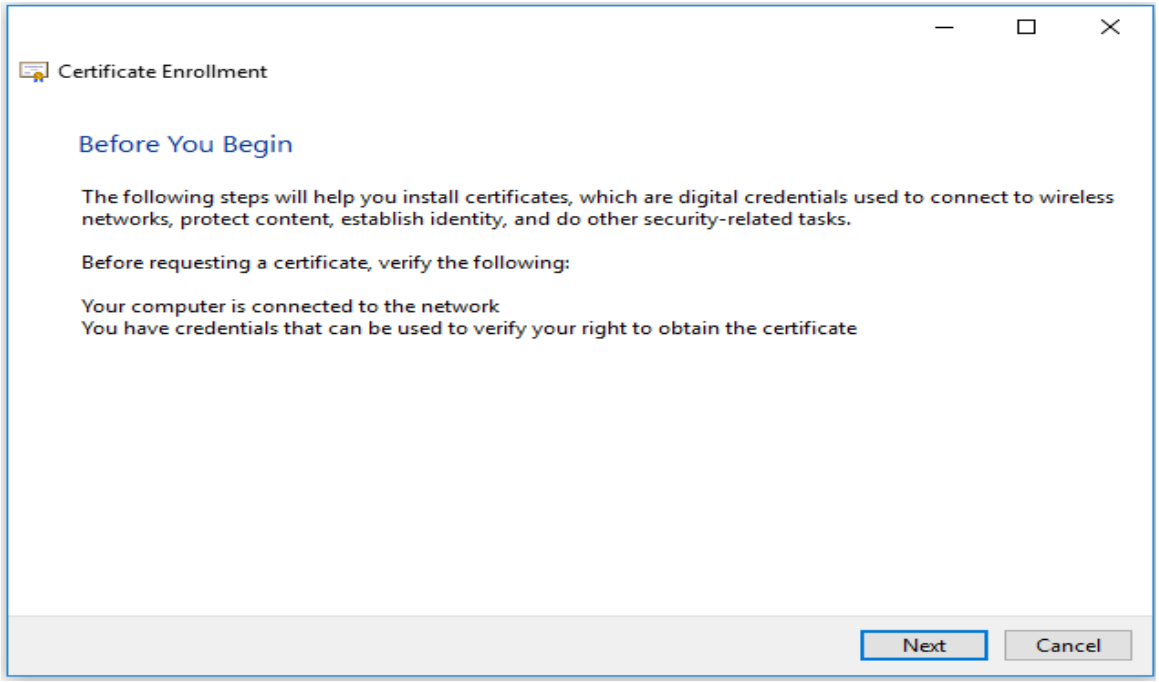
16. Optional: Export PFX Please refer to Section 7.1 Windows

6.3. Option 3: Generate CSR with MMC

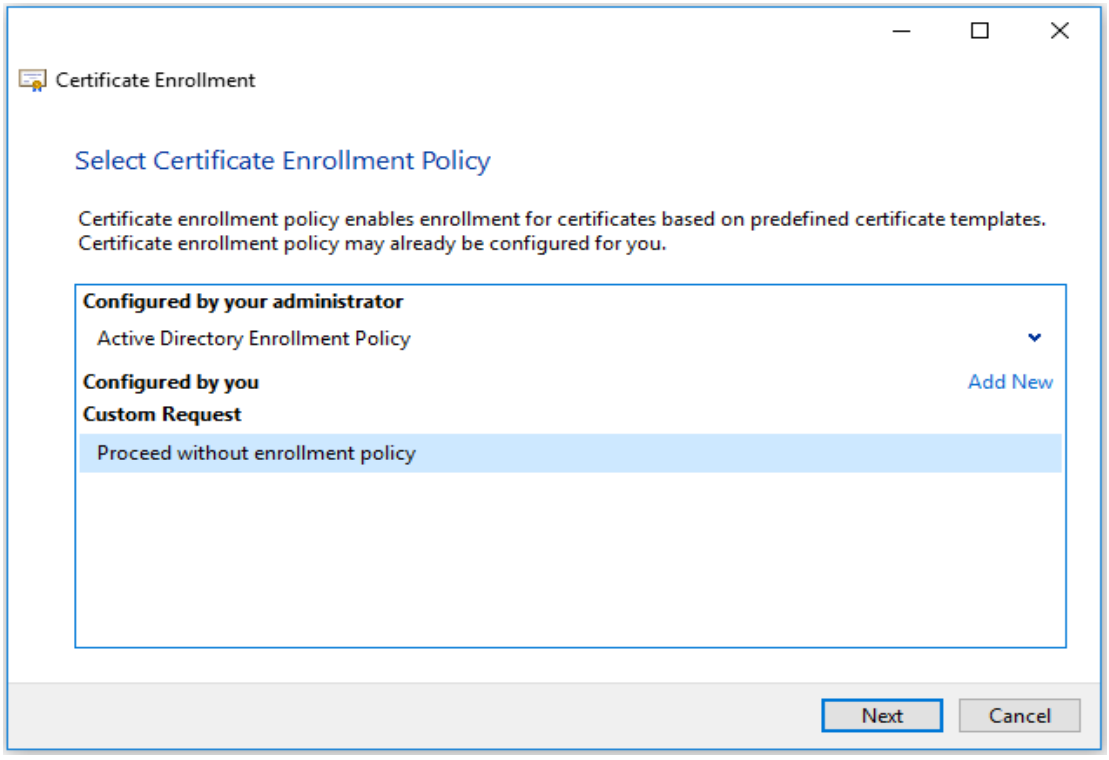
1. Open the Local Machine Certificate Store via the MMC.
2. Right-click with your mouse on **Personal** and select **All tasks → Advanced operations → Create custom request**



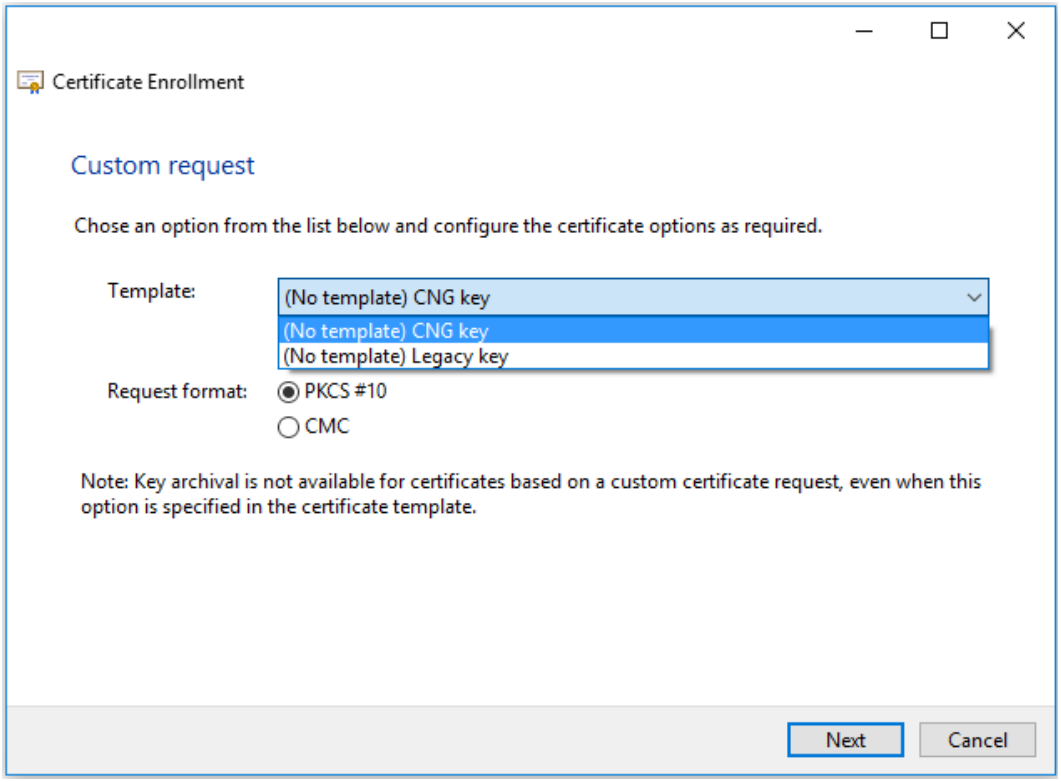
3. A new screen with the title "Certificate Enrollment" appears. Click on **Next**



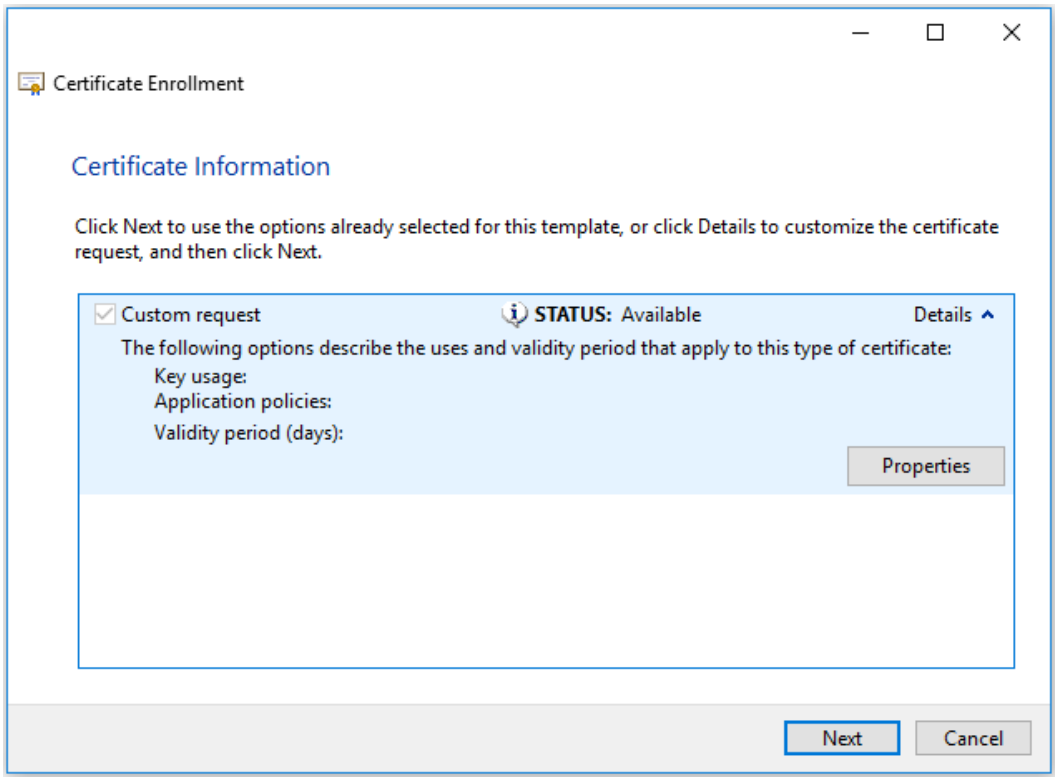
4. Select Custom Request -> Proceed without enrollment policy



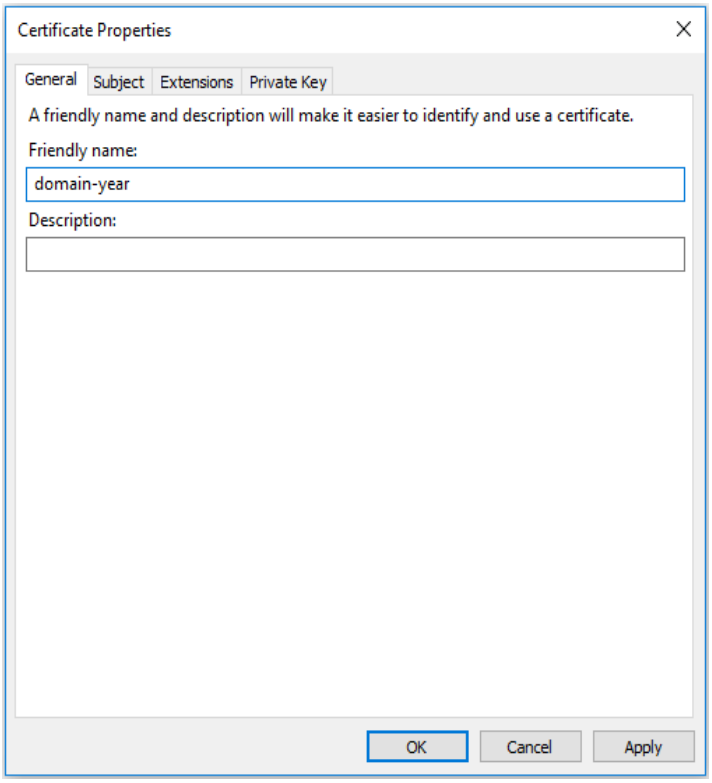
5. For usage with Microsoft TMG, RDP, or ADFS on Azure You need to select **(No template) Legacy key** as template, for all other usages you can leave the settings on default. Click **Next**



6. Click on the down-arrow next to Details and then on Properties



7. On the tab General you enter a Friendly name to use for the certificate and go to the next tab



8. On the tab Subject you need to enter the request details:

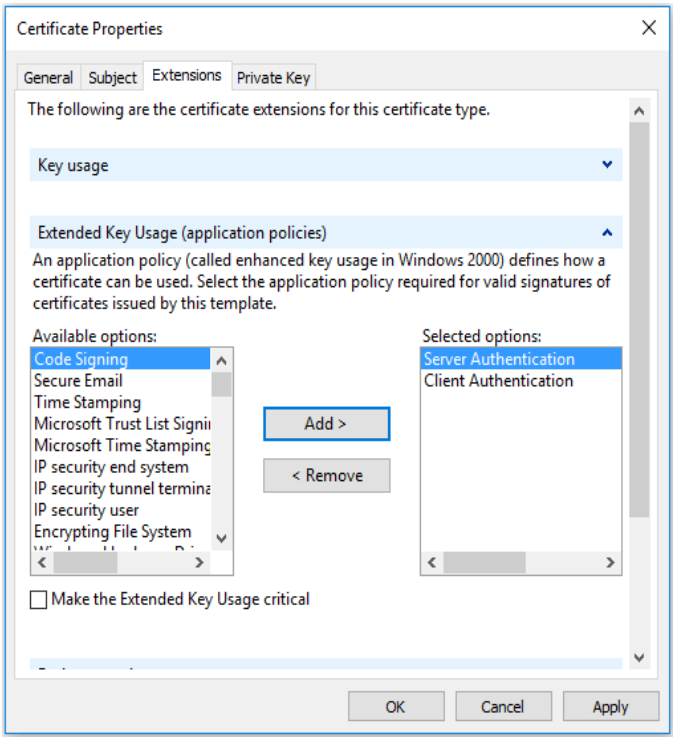
- Common name
- Country
- Locality
- Organization
- Organization unit
- State

Every field can be added by clicking **Add** before selecting the next field. When all required details have been added, you can navigate to the next tab.

9. On the tab **Extensions** click on the arrow next to **Extended Key usage**. Select for **Available options** the options **server authentication** and click on **Add**.

   Repeat these steps for **client authentication**.

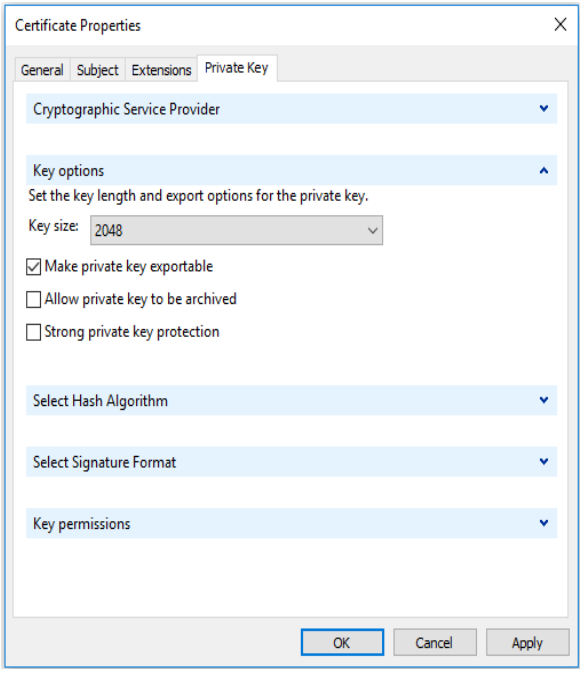
   Then navigate to the last tab.



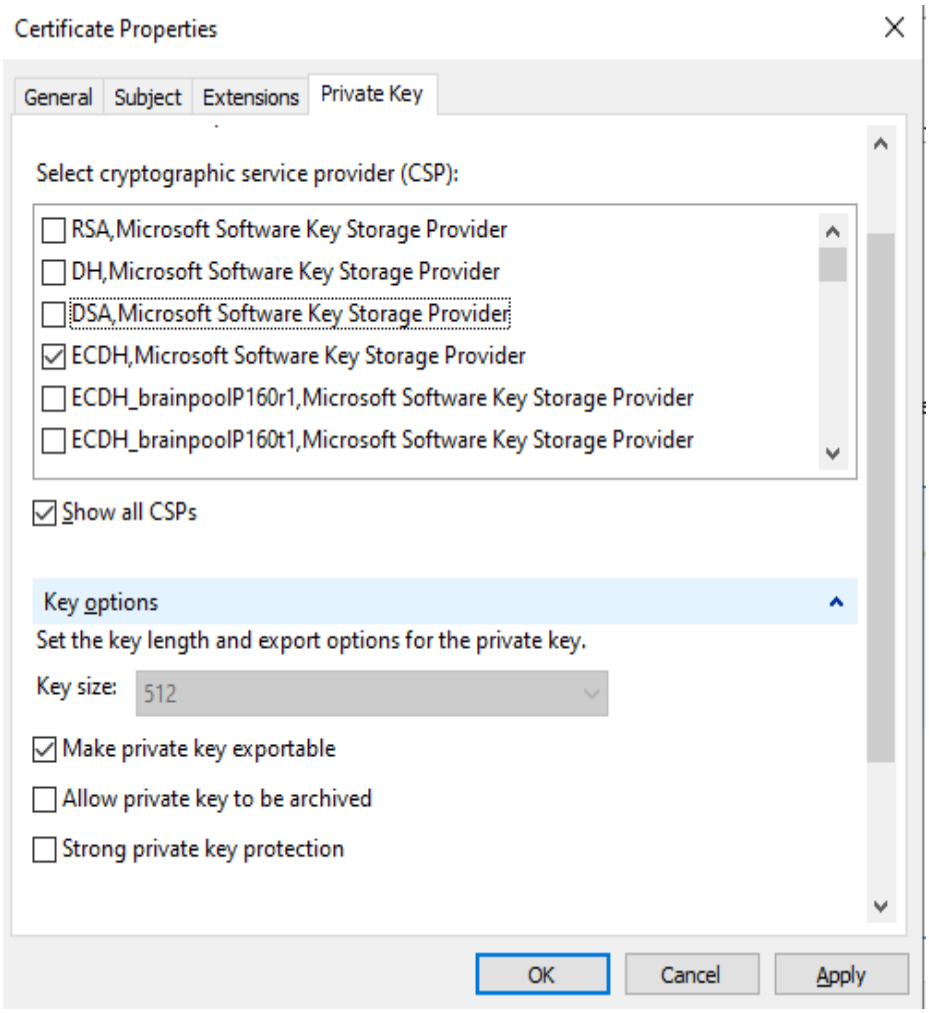
10. On the tab **Private key**, click on the arrow-button next to **Cryptographic service provider**.

    When you want to use a **RSA key**, select the **RSA, Microsoft software key storage provider**

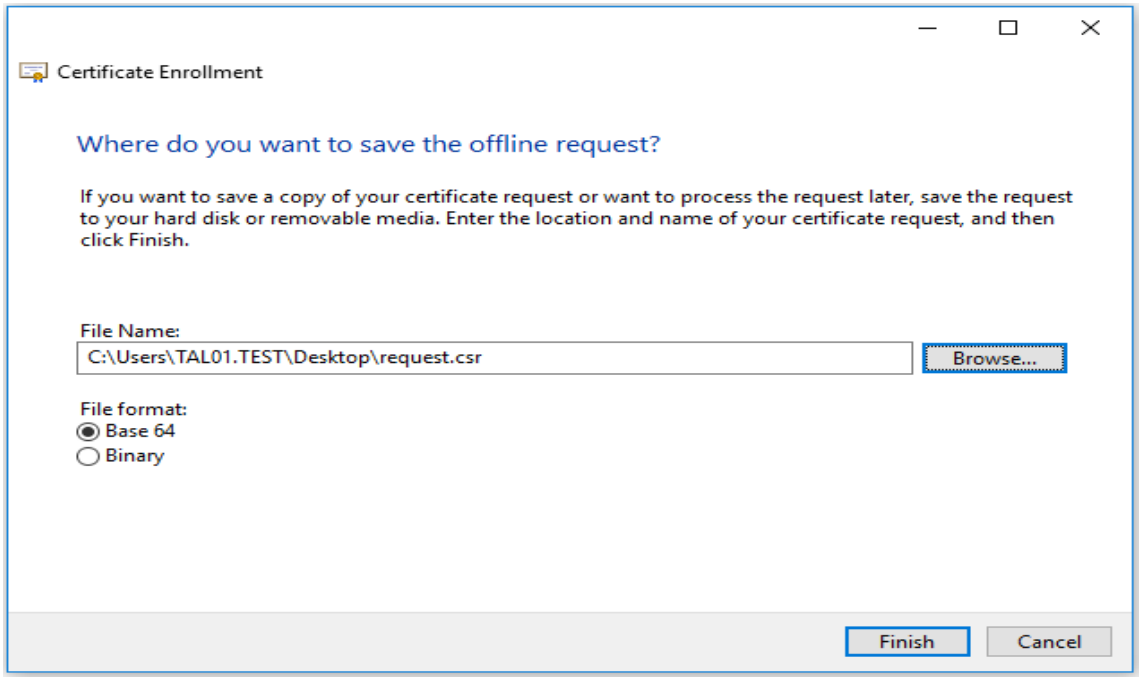
    Select **Microsoft RSA SChannel Cryptographic Provider** and then under **Key options** select as key size: **2048**.



Select Private key **Cryptographic service provider** for ECC algorithm



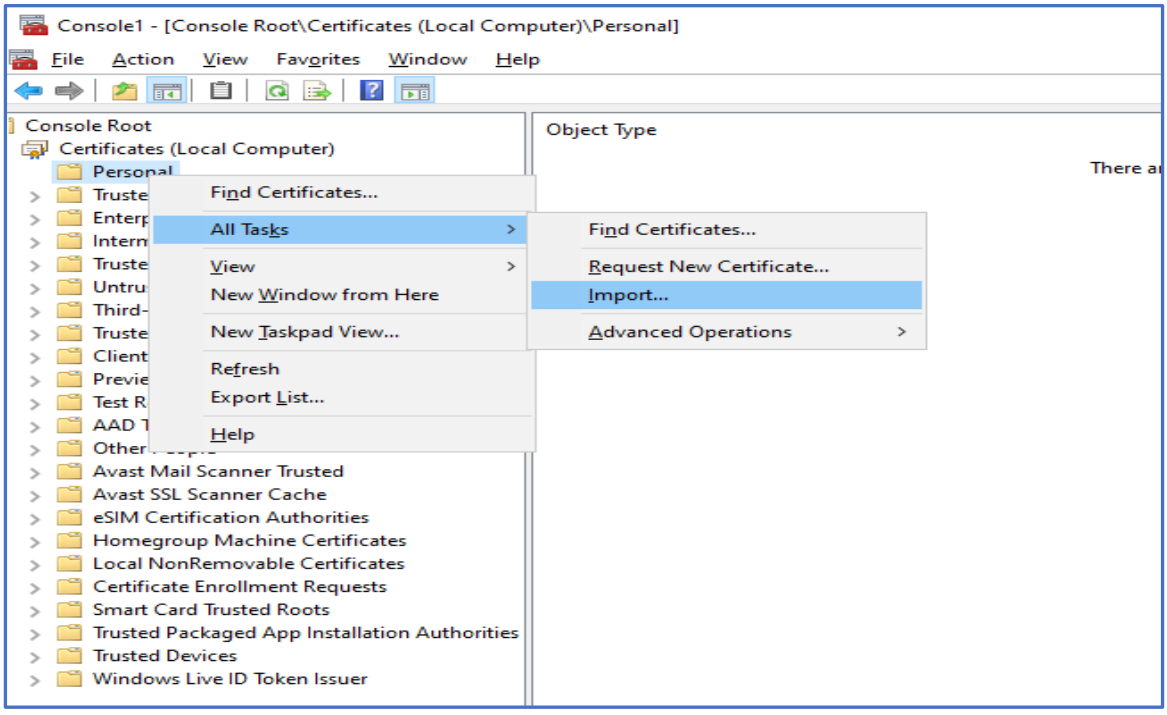
11. Check the option **Make private key exportable** when you want to export the certificate later on to a .pfx be stand.
12. Click on **Apply** and then **Ok**
13. Click on **Next**. In the following screen click on **Browse**... to select where you want to store the CSR, then name it (like: CSR) and click **Save**.



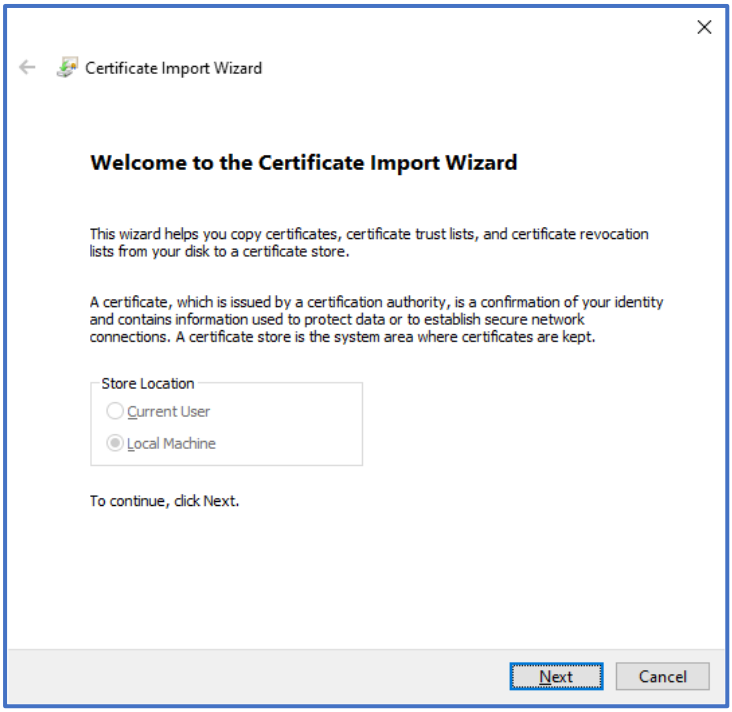
14. Click on **Finish**

Install the Sign Certificate

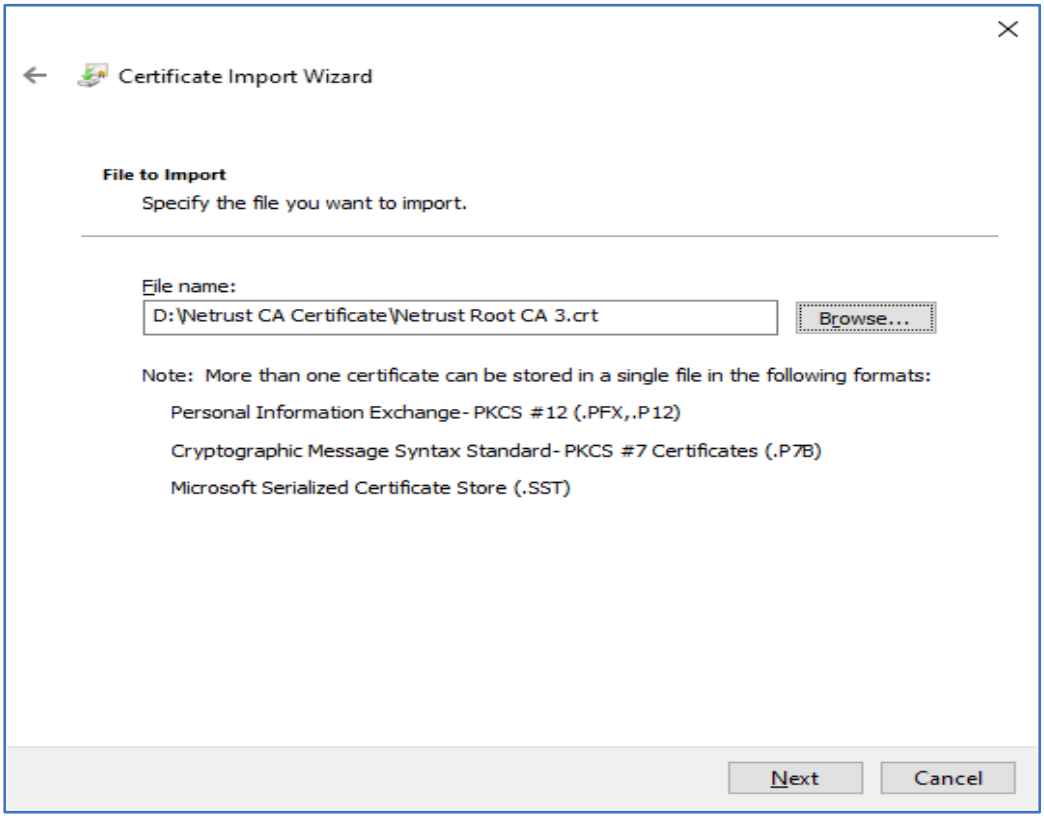
1. Open the Local Machine Certificate Store via the MMC.
2. Right-click with your mouse on **Personal** and select **All tasks → Import**



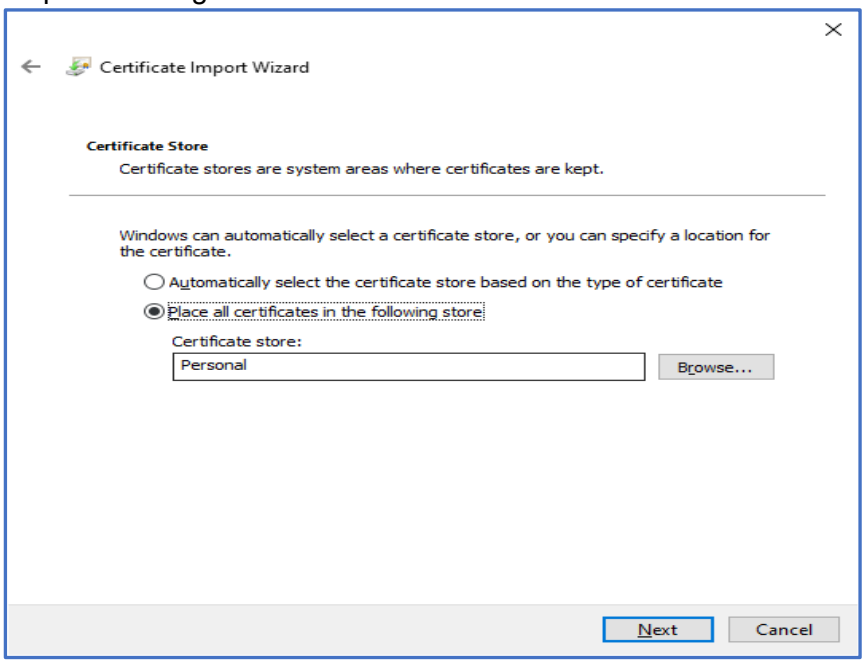
3. Click **Next**



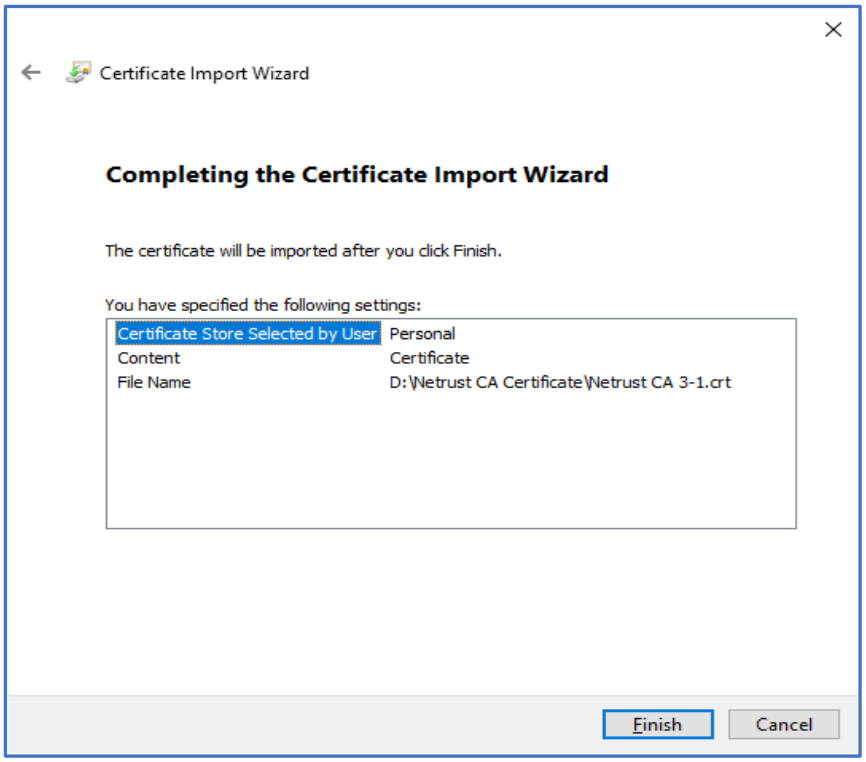
4. Browse to the location of the Signed Certificate -> Click “Next”



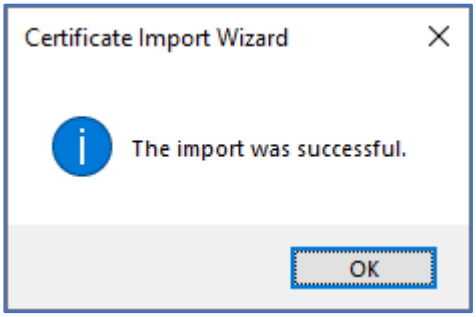
5. Keep the Setting as follow and Click “Next”



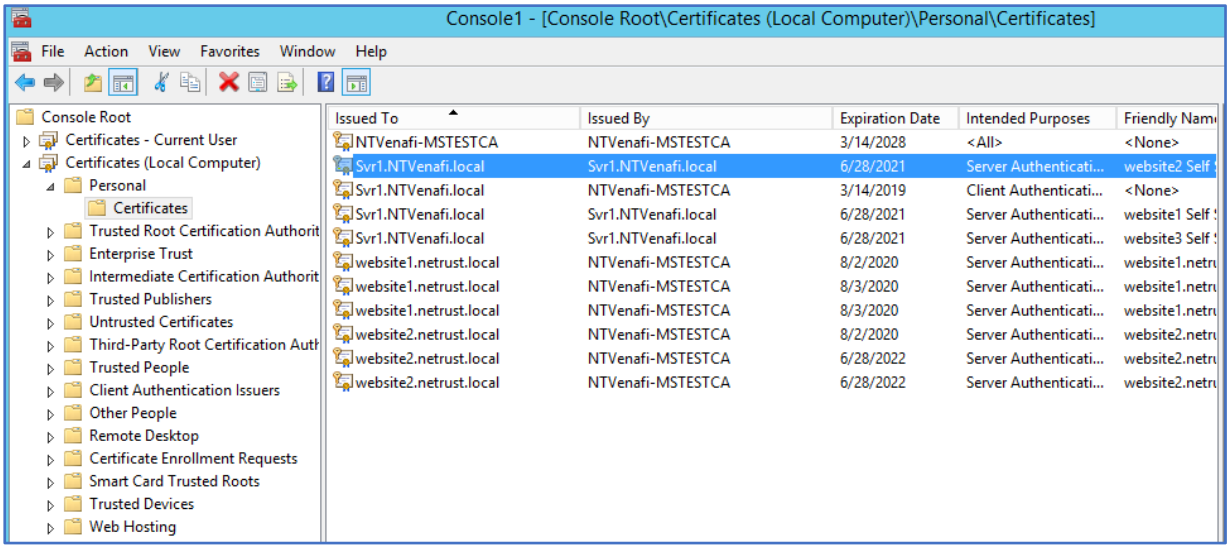
6. Click “Finish”



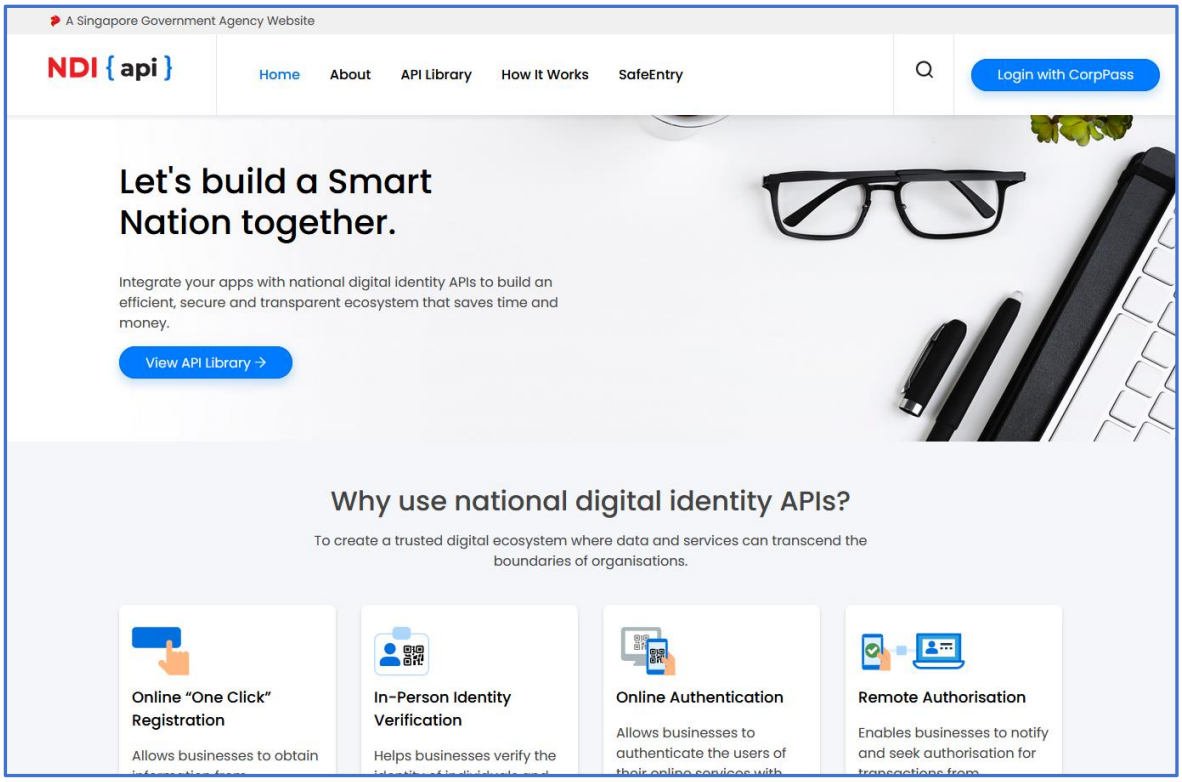
7. Click “Ok” once it import wizard prompt on successful



8. Verify the Certificate on MMC, Make sure the Icon of the certificate on the top have a key icon.  This Show that the Certificate have private key.



9. Once Netrust Sign the x509 Certificate (Sample of x509 file extension commonname.der, commonname.cer or commonname.crt), please Login to https://www.ndi-api.gov.sg/ with CropPass login.



10. Upload the Netrust Sign x509 Certificate to ndi-api Portal.

    For more Technical Queries on ndi-api please email: support@Myinfo.gov.sg

11. Optional: Export PFX Please refer to Section 7.1 Windows

7. Export Certificate

This is the Guide on how to export the Certificate with private key to PFX/PKCS#12 format so that you can deploy to your application.

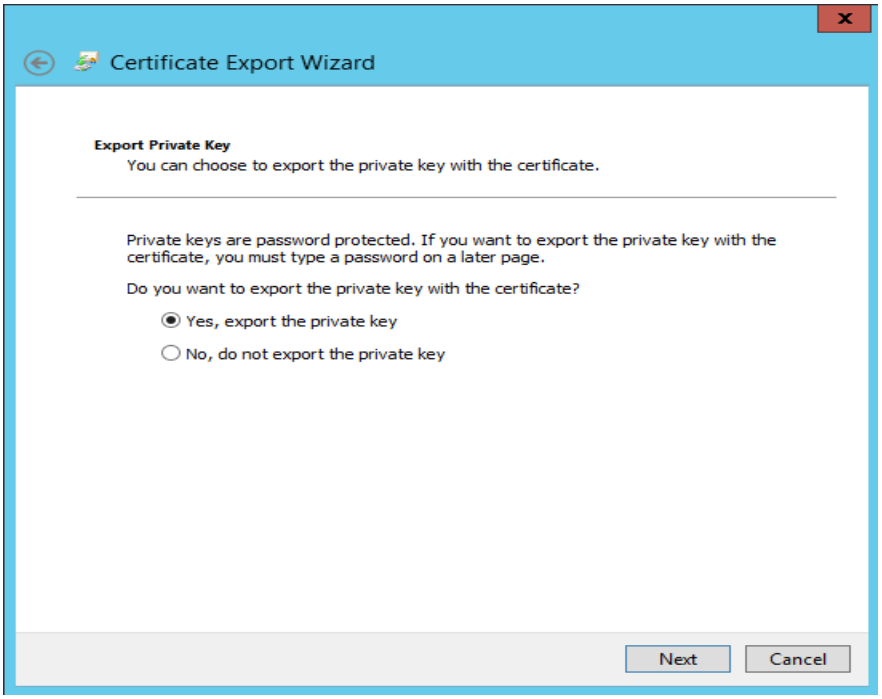
Notes: You **Do Not Need** to convert the certificate to PFX/PKCS#12. It depending on how your application ingrate with the certificate.

7.1. Windows

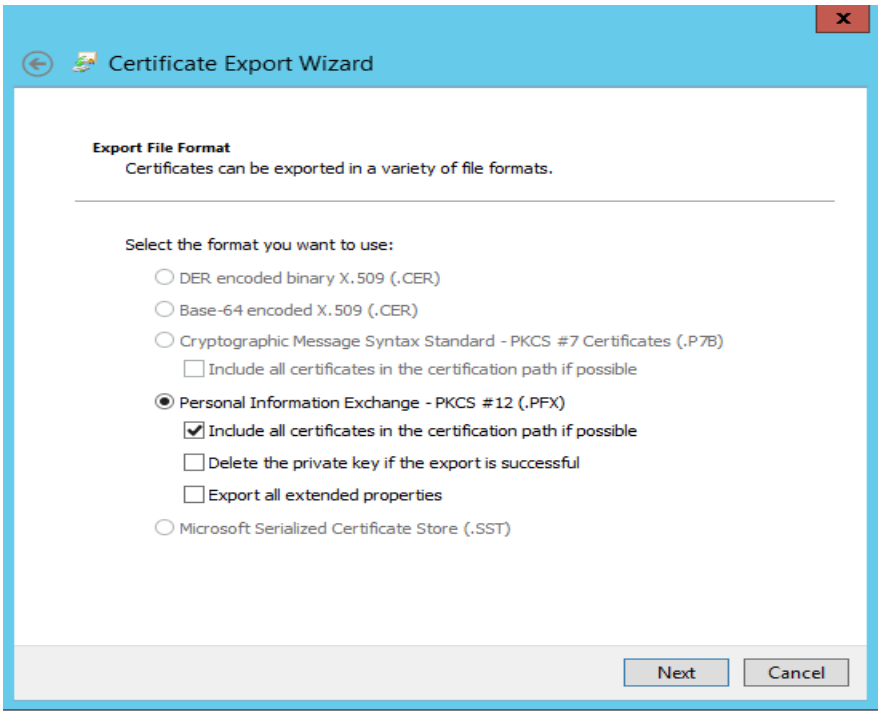
Exporting the x509 Certificate from your server for your application to integrate for Singpass/Corppass Login, Myinfo, SafeEntry use case.

This apply for Option 2 and Option 3 on how you generate the CSR.

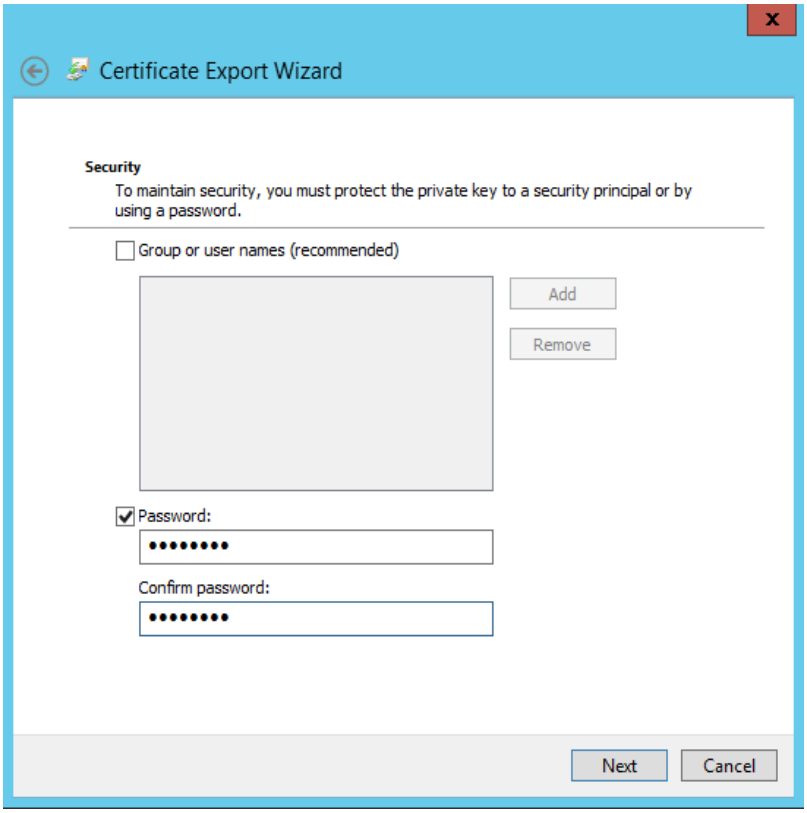
1. Open the Local Machine Certificate Store via the MMC.
2. Right-click with your mouse on **Personal** and select **Certificate → Right click the certificate → All Tasks → Export**
3. Click **Next**
4. Select Yes, Export the Private key → Click **Next**



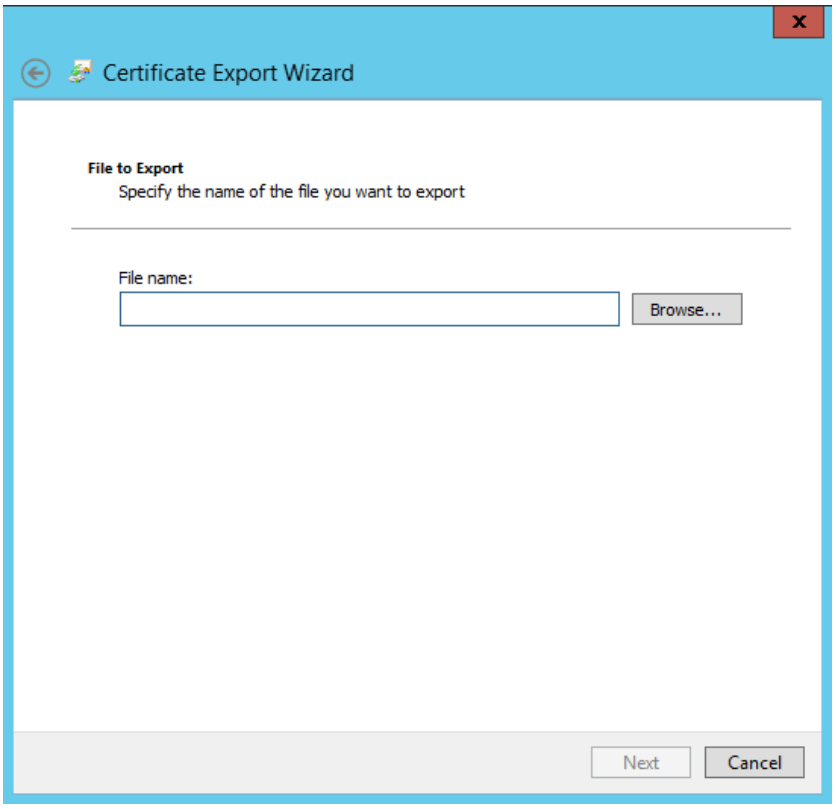
5. Select as follows → Click **Next**



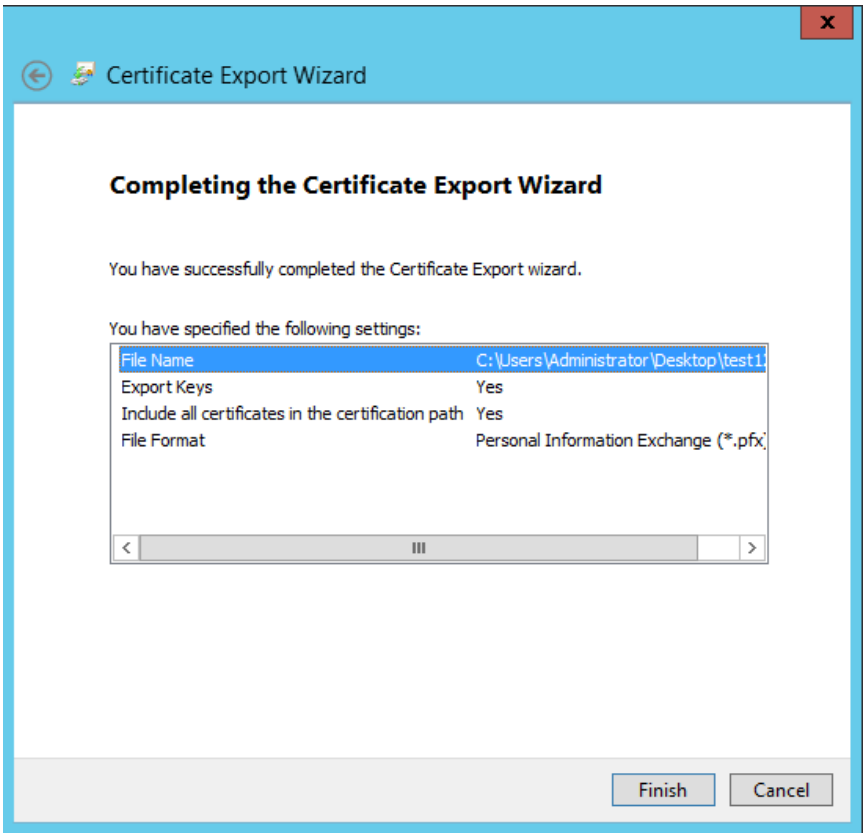
6. Enter Your Password the PKCS#12 → Click **Next**



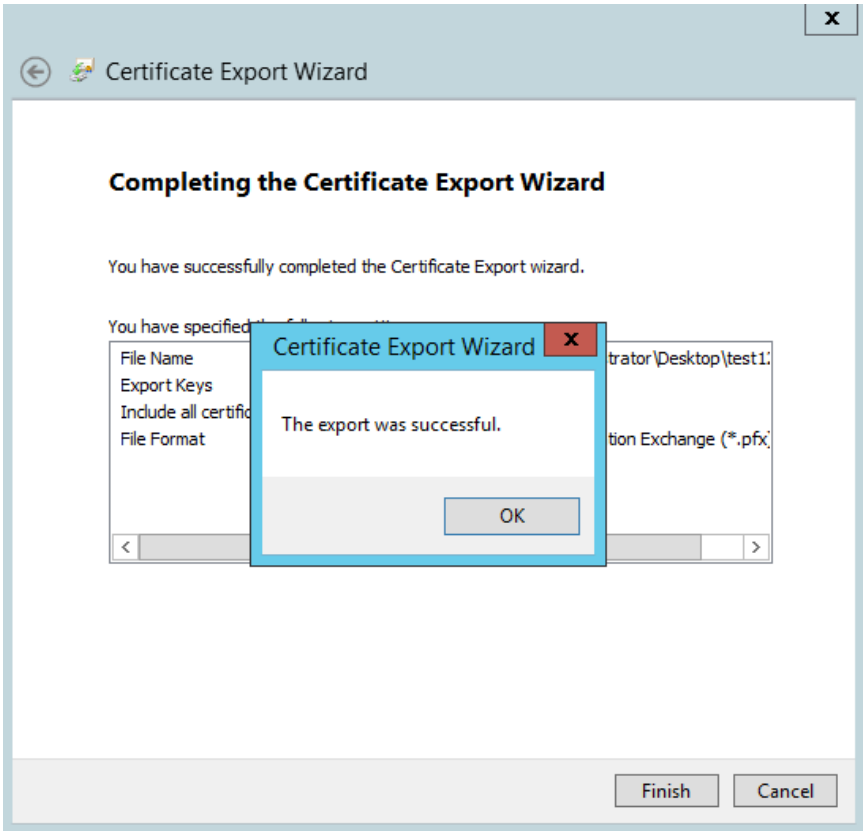
7. Select the location to save the x509 Certificate with private key to your system. → Click **Next**



8. Click Finish



9. Click “Ok”



7.2. PEM (.pem, .crt, .cer) to PFX (OpenSSL)

The commands below demonstrate examples of how to create a .pfx/.p12 file in the command line using OpenSSL:

openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -certfile more.crt

Breaking down the command:

Command	Description
openssl	the command for executing OpenSSL
pkcs12	the file utility for PKCS#12 files in OpenSSL
-export -out certificate.pfx	export and save the PFX file as certificate.pfx
-inkey privateKey.key	use the private key file privateKey.key as the private key to combine with the certificate.
-in certificate.crt	use certificate.crt as the certificate the private key will be combined with.
-certfile more.crt	This is optional, this is if you have any additional certificates you would like to include in the PFX file.

The End of the Document