

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

Version 1.1 Authored by: Netrust 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

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	5
2.	٧	What is Singpass Certificate	5
3.	٧	What is Myinfo Certificate	5
4.	٧	What is SafeEntry Certificate	5
5.	٧	What is Certificate Signing Request (CSR)	5
6.	ŀ	How to generate X509 Certificate Signing Request (CSR)	6
6	5.1	1. Option 1: OpenSSL	6
6	6.2	2. Option 2: Microsoft IIS 8/8.5	9
6	6.3	3. Option 3: Generate CSR with MMC10	6
7.	E	Export Certificate from Windows MMC24	8
8.	F	PEM (.pem, .crt, .cer) to PFX (OpenSSL)	2

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 <u>authentication</u> <u>modules</u> that allow ease of integration with Singpass/CorpPass, Singpass Login, Verify and Myinfo.

<u>Notes: Netrust x509 server certificates for Singpass</u> 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)

Attribute	Prefix	Description	Example		
Country/Region	С	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	0	Organization's legal business name	My Company Name		
Common Name	CN	Domain to be secured by certificate	www.mydomain.com		

You will also be prompted for the following information:

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 (eq, 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.

V 3		Interr	net Informa	ation Service	es (IIS) Man	ager			- 🗆 X
E WIN-	V94SLIPKLOF								🔤 🖂 🟠 🕡 🗸
<u>F</u> ile <u>V</u> iew <u>H</u> elp								_	
Connections		WIN-V	94SLIPKL	OF Home				Act	tions Open Feature
Start Page ▶ 🔮 WIN-V94SLIPKLOF	Filter:		• \$\$ <u>G</u> o • \$	Show <u>A</u> ll	Group by:	^	Ŧ	2	Manage Server Restart
	<u></u>	9			404			₽	Start Stop
	Authentic	Compression	Document	Browsing	Error Pages	Request Tra			View Application Pools View Sites
	Handler				ISADI and				Change .NET Framework Version
	Mappings	Redirect	Respon	and Doma	CGI Restri	ISAFI FILLEIS		0	Get New Web Platform Components
		1			8	P		0	Help
	Logging	MIME Types	Modules	Output Caching	Request Filtering	Server Certificates	=		Online Help
	Worker Processes								
	Managemen	nt				^			
			<u>, </u>	<u>, , , , , , , , , , , , , , , , , , , </u>	an 🛓	_	~		
< III >	Features Vie	w 📑 Conten	t View						
Ready									€ 1.:

3. Navigate to Server Certificates

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

V		Interr	net Informa	tion Service	s (IIS) Man	ager		_ 🗆 X
💽 🖣 🖣 WIN-V	94SLIPKLOF >							🕶 🛛 🟠 I 🕖 -
<u>F</u> ile <u>V</u> iew <u>H</u> elp								
Connections		WIN-V94S	LIPKLOF Ho	me			A	Actions
Start Dags								Open Feature
♦ • WIN-V94SLIPKLOF	Filter:		- <u>G</u> o - (Show <u>A</u> ll	Group by:		-	Manage Server
			2				- I I	Start
	Authentic			Directory	404	Eniled.		Stop
	Addrende C	ompression	Document	Browsing	EnorPages	Request Tra		View Application Pools View Sites
	Handler							Change .NET Framework Version
	Mappings	Redirect	Respon	and Doma	CGI Restri	ISAFIFICEIS	•	Get New Web Platform Components
		325	*		8			Help
	Logging N	VIME Types	Modules	Output Caching	Request Filtering	Server Certificates		Online Help
	2					\smile		
	Worker Processes							
	Management					^		
			<u>,</u>	<u> 2</u>		_	~	
< III >	Features View	/ 💦 Content	View					
Ready								• <u>1</u> .:

4. Select Create a New Certificate

In the right Actions menu, click Create Certificate Request.

8	Internet Information Services (IIS) Manager	_ □ X
€ WIN-V	94SLIPKLOF >	😰 🛛 🟠 🔞 🗸
File View Help		
Connections Connections Start Page Start Page WIN-V94SLIPRIOF Application Poo b-Sites	Server Certificates Use this feature to request and manage certificates that the Web server can use with websites configured for SSL. Filter: • @ Go • @ Show All Group by: # Name Issued To Issued By	Actions Import Create Certificate Request Complete Certificate Request Create Domain Certificate Create Self-Signed Certificate Help Online Help
< III > Ready	< Ⅲ >	

5. Enter your CSR details

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

	Request Certificate ? ×									
Distinguished Name Properties										
Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.										
Co <u>m</u> mon name:	iis.sslexperience.com									
Organization:	Rapid Web Services LLC.									
Organizational <u>u</u> nit:	I.T. Department									
City/locality	Saint Petersburg									
<u>State/province:</u>	Florida									
Country/ <u>r</u> egion:	Us									
	Previous Next Einish Cancel									

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.

Request Certificate	?	x
Cryptographic Service Provider Properties		
Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance. Cryptographic service provider:		
Microsoft RSA SChannel Cryptographic Provider		
Bit length: 2048 v		
Previous Next Finish	Cancel	

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.

Request Certificate	? ×
File Name	
Specify the file name for the certificate request. This information can be sent to a certification authority for signing.	
Specify a file name for the certificate request:	
C:\Users\Administrator\Desktop\2015iis.ssiexperience.com	
Previous Next Finish 0	Cancel

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-----

2015 lis.sslexperience.com csr - Notepad	
File Edit Format View Help	
BEGIN NEW CERTIFICATE REQUEST	*
MIIEhjCCA24CAQAwgYsxCzAJBgNVBAYTAlVTMRAwDgYDVQQIDAdGbG9yawRhMQ4w	
GDAWDGNVDASMDUK UVC4 GRGVWYAS UDDWVUDDEWDWGALDEAWWW AW IZE INVDGV4 GGVY	
KZ3cgrgzJSour6goD3vtc1gAdct1H8kn/MBBnx6kWooz1suAgISb+2Jgrg5/e6xm	
xNnjqZsOKoDk]]iI2n1RxF0Wtj4Z]jQ+7jmEIK99eIeqY5vq61+hatTGYk6IbHQh	
QQNFEyvg630CXnabAFtnxY5X5/Nn6AFurxuAgtrFXzici5Ggxe59XJh9psVNkbH/	
XG9yUVGE99ATAOLOHICUZSIAJCOU6LMGK2XDON3PARFC9ZDU99MGFJCG6OTC4TLT	
awnabscildav.Roticiaas Banchactexitaatinaacoose philiptaabini ita	
Twy JKwy BBAGCNXUUMUI WOAI BBOWPVO I OLVEZMIQ3UK 91VK NWDBLXSU4t UTMVNDdS	
T0hWQ1ZcQWRtaW5pc3RyYxRvcgwLSW5ldE1nci5leGUwcgYKKwYBBAGCNw0CAjFk	
MGICAQEeWgBNAGkAYwBYAG8AcWBYAGYAdAAgAFIAUwBBACAAUwBDAGgAYQBUAG4A	
ZQBSACAAQWBYAHKACABUAGSAZWBYAGEACABDAGKAYWAGAFAACGBYAHYAAQBKAGUA	
CGMDADCESTUSTOSTICUTUS CNAQKOMY NDMIGHMAAASIDOWEDY WQEANIEDDAI DQINYNSUE	
Bagadki G9w0DBAICAIAwCWYJYIZIAWUDBAECMASGCWCGSAF JAW0BLTALBQ J QKAB	
ZQMEAQIWCWYJYIZIAWUDBAEFMACGBSSOAWIHMAQGCCQGSIb3DQMHMB0GALUdDgQW	
BBTbhtbVdwt3Pc+K9bYwsVK4d3wGFjANBgkqhk1G9w0BAQUFAAOCAQEARkMImjFO	
S4 JWCTANBLFF6GF+ZAX/IZ2EW0Z20FbU93NpSMGmAUTTY/IT4/J/IJAK+N42mFV4De	
L Chyfachasyddiad yn ar	
tvEW1P72YtLvaa09yPz7UuFtohPJzzmv0kd7oTv06vsuv4UmKubooL7EtK06Aup	
EXaaofcjF4LJhd5wGYNbdrustUlNlgxbdMzLHrw0JognuGeqxP0hVPSMyAehJM80	
Oierf3mnqQuBuA==	
END NEW 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.

2]		Interr	net Informa	ation Service	es (IIS) Man	ager		_ D X
 (€) ● (€) ● (€) ● (€) ● (€) ● (€) ● 								
<u>F</u> ile <u>V</u> iew <u>H</u> elp								
Connections	Sim Wi	N-C93AKI		Home			- 15	Actions
Start Page			5 0514 2					Open Feature
NIN-C93AKUOJKPD	Filter:		• 🦻 <u>G</u> o 🐨	Show <u>A</u> ll	Group by:		Ŧ	Manage Server
		9					<u>-</u>	Start
	Authentic	Compression	Default	Directory	404	Eniled		Stop
	Authentic	Compression	Document	Browsing		Request Tra		View Application Pools View Sites
	and lar							Change .NET Framework Version
	Mappings	Redirect	Respon	and Doma	CGI Restri	ISAPI FILLEIS		 Get New Web Platform Components
		1	a		8	D		😢 Help
	Logging	MIME Types	Modules	Output Caching	Request Filtering	Server Certificates	=	Online Help
	2							
	Worker Processes							
	Manageme	nt				~		
			<u> </u>	<u>, (</u>	i 🖩 🍷	y -	~	
< III >	Features Vie	ew 📑 Conten	t View					
Ready								¶:

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.

🛐 Internet Information Services (IIS) Manager 📃 🗖 🗙					
€ WIN-C	C93AKUOJKPD >	🛂 🛛 🟠 😥 🕶			
<u>F</u> ile <u>V</u> iew <u>H</u> elp					
Connections Start Page WIN-C93AKUOJKPD Application Poo Sites	Server Certificates Use this feature to request and manage certificates that the Web server can use with websites configured for SSL. Filter: • • • • • • • • • • • • • • • • • • •	Actions Import Create Certificate Request Create Domain Certificate Create Self-Signed Certificate We Help Online Help			
	۲ الله الله الله الله الله الله الله الل				
< III >	🛅 Features View 🕼 Content View				
Ready		•1.:			

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	In the drop-down list, select Personal.
new certificate:	

Complete Certificate Request ? ×
Specify Certificate Authority Response
Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.
File name containing the certification authority's response:
C:\Users\Administrator\Desktop\your_domain_name.cer
Friendly name:
yourdomain.com
Select a certificate store for the new certificate: Personal
OK Cancel

- 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

		—		\times
🔄 C	ertificate Enrollment			
	Before You Begin			
	The following steps will help you install certificates, which are digital credentials used networks, protect content, establish identity, and do other security-related tasks.	to conne	ct to wire	less
	Before requesting a certificate, verify the following:			
	Your computer is connected to the network You have credentials that can be used to verify your right to obtain the certificate			
		Next	Cano	:el

4. Select Custom Request -> Proceed without enrollment policy

	_		×
Certificate Enrollment			
Select Certificate Enrollment Policy			
Certificate enrollment policy enables enrollment for certificates based on p Certificate enrollment policy may already be configured for you.	predefined certificate	template	<u>is</u> .
Configured by your administrator			
Active Directory Enrollment Policy			~
Configured by you		Add N	ew
Custom Request			
Proceed without enrollment policy			
	Next	Can	cel

 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

		—		×
🔄 Certificate Enrollment				
Custom request				
Chose an option from	the list below and configure the certificate options as required.			
Template:	(No template) CNG key		~	
	(No template) CNG key			
	(No template) Legacy key			1
Request format:	PKCS #10			
	⊖ cmc			
Note: Key archival is	not available for certificates based on a custom certificate request	, even w	hen this	
option is specified in	the certificate template.			
	Ν	ext	Cano	el:

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

			_		×
🔄 Ce	rtificate Enrollment				
(Certificate Information				
1	Click Next to use the options already selected request, and then click Next.	for this template, or click Details to	customize th	ne certifica	ite
	Custom request	③ STATUS: Available		Details	~
	The following options describe the uses Key usage: Application policies: Validity period (days):	and validity period that apply to th	is type of cert	ificate: roperties	
			Next	Can	cel

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

Certificate Properties	×
General Subject Extensions Private Key	
A friendly name and description will make it easier to identify and use a certificate.	
Friendly name:	
domain-year	
Description:	
OK Cancel App	ly

- 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.

Certificate Properties				×	
General Subject Extensions	Private Key				
The subject of a certificate is can enter information about can be used in a certificate.	the user or con the types of sul	nputer to whi oject name a	ich the certificate is nd alternative name	issued. You e values that	
Subject of certificate					
The user or computer that is	receiving the ce	ertificate			
Subject name:	_		CN		
Туре:	0.4	d s	C=I		
State v	/ Ad	u >	L=F		
Value:	< Re	move	00: S=N		
Alternative name:					
Туре:					
Directory name 🔷 🗸	,				
Value:	Ad	d >			
	< Re	move			
		ОК	Cancel	Apply	

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.

Certificate Properties	×
General Subject Extensions Private Key	
The following are the certificate extensions for this certificate type.	^
Key usage	•
Extended Key Usage (application policies)	~
An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures o certificates issued by this template.	f
Available options: Selected options:	
Code Signing 🔨 Server Authentication	
Secure Email Client Authentication	
Time Stamping	
Microsoft Time Stamping	
IP security end system	
IP security tunnel termina	
IP security user	
Encrypting File System	
< >> <	>
Make the Extended Key Usage critical	
• · ·	
OK Cancel A	pply

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**.

Certificate Properties	×
General Subject Extensions Private Key	
Cryptographic Service Provider	*
Key options	^
Set the key length and export options for the private key.	
Key size: 2048 🗸	
Make private key exportable	
Allow private key to be archived	
Strong private key protection	
Select Hash Algorithm	•
Select Signature Format	*
Key permissions	*
OK Consel	Apply
OK Cancel	Арріу

Select Private key	Cryptographic	service provider	for ECC algorithm

Certificate Properties		×
General Subject Extensions Private Key		
Select cryptographic service provider (CSP):		^
RSA, Microsoft Software Key Storage Provider	^	
DH, Microsoft Software Key Storage Provider		
CIECDH Microsoft Software Key Storage Provider		
ECDH brainpoolP160r1 Microsoft Software Key Storage Provider		
ECDH_brainpoolP160t1,Microsoft Software Key Storage Provider	~	
Show all CSPs		
Key options	^	
Set the key length and export options for the private key.		
Key size: 512		
☑ Make private key exportable		
Allow private key to be archived		
Strong private key protection		
		~
OK Cancel	<u>A</u> pply	

- 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**.

	_		\times
Certificate Enrollment			
Where do you want to save the offline request?			
If you want to save a copy of your certificate request or want to process the request late to your hard disk or removable media. Enter the location and name of your certificate re click Finish.	r, save t equest, a	he reques and then	st
File Name:			
C:\Users\TAL01.TEST\Desktop\request.csr	Br	owse	
File format:			
O Binary			
Fir	nish	Cano	:el

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** \rightarrow **Import**



3. Click Next

Г

🗧 😺 Certificate Import Wizard	×
Welcome to the Certificate Import Wizard	
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
Local Machine	
To continue, click Next.	
Next Cance	el

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

pecify the file you want to import.
ile name:
D:\Vetrust CA Certificate\Vetrust Root CA 3.crt Browse
ote: 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)

5. Keep the Setting as follow and Click "Next"

Contribute C	h
Certificate S	iore Ite stores are system areas where certificates are kept.
Window the cert	s can automatically select a certificate store, or you can specify a location for ificate.
	utomatically select the certificate store based on the type of certificate
OP	ace all certificates in the following store
c	Certificate store:
[Personal Browse
	Nevt

6. Click "Finish"

← 🛛 & Certificate Import Wizard	×
Completing the Certific	ate Import Wizard
The certificate will be imported after	you click Finish.
You have specified the following setti	ings:
Certificate Store Selected by User	Personal
Content	Certificate
File Name	D: Wetrust CA Certificate Wetrust CA 3-1.crt
	<u>F</u> inish Cancel

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

a .	Console1 - [Console Root\Certificates (Lo	ocal Computer)\Pers	onal\Certificates]	
File Action View Favorites Windo Image: state of the state	w Help	Issued By	Expiration Date	Intended Purposes	Friendly Name
 Certificates - Current User Certificates (Local Computer) Personal Certificates Trusted Root Certification Authorit Enterprise Trust Intermediate Certification Authorit Trusted Publishers Untrusted Certificates Trusted People Client Authentication Issuers Client Authentication Issuers Certificate Enrollment Requests Smart Card Trusted Roots Trusted Devices 	INTVenafi-MSTESTCA Svr1.NTVenafi.local Svebsite1.netrust.local website1.netrust.local website2.netrust.local website2.netrust.local website2.netrust.local website2.netrust.local website2.netrust.local	NTVenafi-MSTESTCA Svr1.NTVenafi.local NTVenafi-MSTESTCA Svr1.NTVenafi.local Svr1.NTVenafi.local NTVenafi-MSTESTCA NTVenafi-MSTESTCA NTVenafi-MSTESTCA NTVenafi-MSTESTCA NTVenafi-MSTESTCA	3/14/2028 6/28/2021 3/14/2019 6/28/2021 6/28/2021 8/2/2020 8/3/2020 8/3/2020 8/2/2020 6/28/2022 6/28/2022	<all> Server Authenticati Client Authenticati Server Authenticati Server Authenticati Server Authenticati Server Authenticati Server Authenticati Server Authenticati Server Authenticati</all>	<none> website2 Self : <none> website1 Self : website1.netri website1.netri website1.netri website2.netri website2.netri website2.netri</none></none>

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.

<u>Notes:</u> You <u>Do Not Need</u> 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.
- 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

	×
📀 🍠 Certificate Export Wizard	
	_
Export Private Key You can choose to export the private key with the certificate	
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.	
Do you want to export the private key with the certificate?	
 Yes, export the private key 	
\bigcirc No, do not export the private key	
Next Can	cel

5. Select as follows → 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:
O DER encoded binary X.509 (.CER)
O 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
 Microsoft Serialized Certificate Store (.SST)
Next Cancel

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

~ -	
🔄 🐓 Certificate Export Wizard	
Security To maintain security, you must protect t using a password.	the private key to a security principal or by Add Remove
Password:	
Confirm password:	
•••••	
	Next Cancel

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

📀 😼 Certificate Export Wizard	×
File to Export Specify the name of the file you want to export	
File name:	
Next	el

8. Click Finish

	Certificate Exp	ort Wizard
	Completing	the Certificate Export Wizard
,	You have successfu	Illy completed the Certificate Export wizard.
	You have specified t File Name Export Keys Include all certifica File Format	the following settings: C:\Users\Administrator\Desktop\test1; Yes ates in the certification path Yes Personal Information Exchange (*.pfx;
	<	III >
		Finish Cancel
Click "Ol	K"	
\sim -		ort Wizard
(4) 🐖 (Certificate Evn	
(e) 🥩 (Certificate Exp	
(e) 🔮 (Certificate Exp	the Certificate Export Wizard
(e) 🐓 (Certificate Exp Completing	the Certificate Export Wizard
	Certificate Exp Completing You have successfu	the Certificate Export Wizard
	Certificate Exp Completing You have successful You have specified File Name Export Keys Include all certific File Format	the Certificate Export Wizard Illy completed the Certificate Export wizard. Certificate Export Wizard The export was successful.
	Certificate Exp Completing You have successfu You have specified File Name Export Keys Include all certific File Format	the Certificate Export Wizard Illy completed the Certificate Export wizard. Certificate Export Wizard The export was successful. The export was successful.
	Certificate Exp Completing You have successfu You have specified File Name Export Keys Include all certific File Format	the Certificate Export Wizard Illy completed the Certificate Export wizard. Certificate Export Wizard The export was successful. OK
	Certificate Exp Completing You have successful You have specified File Name Export Keys Include all certific File Format	the Certificate Export Wizard Illy completed the Certificate Export wizard. Certificate Export Wizard The export was successful. OK
	Certificate Exp Completing You have successful You have specified File Name Export Keys Include all certific File Format	the Certificate Export Wizard Ally completed the Certificate Export wizard. Certificate Export Wizard The export was successful. OK OK
	Certificate Exp Completing You have successfu You have specified File Name Export Keys Include all certific File Format	the Certificate Export Wizard Ily completed the Certificate Export wizard. Certificate Export Wizard The export was successful. OK 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