

# Step by step, how to generate certificate file

## Table of Contents

Generate certificate file for web server (use external root CA for sign request): .....	1
Create Request (step) .....	2
Create Signed Certificate (step) .....	5
Generate pfx file (when you got signed certificate file from external CA root authority e.g. GoDaddy) .....	5
Generate certificate file for web server (use internal CA(s) for sign request).....	6
Create Request (step) .....	7
CA Certificate (step).....	10
Variant I – „Sign locally-Don’t have CA cert “ .....	10
Variant II – „Sign locally-Have CA cert“ .....	13
Issue Certificate (step) .....	16
Create Signed Certificate (step) .....	18
Import certificate from generated pfx file to web server .....	19
Import certificate from generated pfx file to client computer for web server .....	24
Import three level CA certificate (issuer CA).....	26
Import two level CA certificate (intermediate CA) .....	27
Import one level CA certificate (master CA) .....	29

## Generate certificate file for web server (use external root CA for sign request):

Done	Menu option (step)	Comment
<input type="checkbox"/>	Create Request	<p>Fill all data on the form. When you click on the "Generate" button, the application will generate two files in the folder whose path is listed in the "Path to store generate files:" field.</p> <p>The first file with a .key extension is a private certificate key file. Another file with the .csr extension is the certificate request file, that need to be send to CA server for sign.</p> <p><b>NOTE:</b></p> <p>If files with the same names already exist on selected folder (field "Path to store generate files"), you need to delete these files and click "Generate" button again.</p> <p>When the external CA authority signs the .csr file, it should return the signed generated file as well as the .cer file with public key of the root CA (and if the signing is done by the intermediate CA, then it is necessary to send us the .cer file with public key of that intermediate CA).</p> <p>If signing is done with some of the public CAs (whose certificates came with the Windows installation), then these certificates from root CA (and intermediate CA) need not be sent, but ONLY the generated file.</p>
<input type="checkbox"/>	Create Signed Certificate	<p>On the form, enter the path for the .cer file that was obtained after signing with external CA and the .key file containing the private key certificate for which we sent the .csr file to the external CA authority.</p> <p>It is necessary to select a folder in which the signed certificate file with a private key will be generated (file with .pfx extension).</p>

**NOTE:**

If a file with the same name already exists in the selected location, it is necessary to delete this file and click "Generate" button again.

## Create Request (step)

**GENERATE CERTIFICATE - APPLICATION** Theme Accent

Create Request Create Certificate Create SelfSign Cert. Issue Certificate CA Certificate

Main **Create Request**

Common Name:  **Gen.Alternative Names**

Subject Alternative Names:

Is this CA certificate:

Key Length:

Signature Algorithm:

Country Code:

State or Province Name:

Locality Name:

Organization:

Choose Key Usage:

Choose Extended Key Usage:

Path to store generate files:  **Browse**

Private Key File Name:  **.key**

Request Key File Name:  **.csr**

**Generate**

**Continue**

Generate Request and Certificate Application | Menu option: Create Request

**GENERATE CERTIFICATE - APPLICATION** Theme Accent

Create Request Create Certificate Create SelfSign Cert. Issue Certificate CA Certificate

Main **Create Request**

Common Name:  **Gen.Alternative Names**

Subject Alternative Names:

Is this CA certificate:

Key Length:

Signature Algorithm:

Country Code:

State or Province Name:

Locality Name:

Organization:

Choose Key Usage:

Choose Extended Key Usage:

Path to store generate files:  **Browse**

Private Key File Name:  **.key**

Request Key File Name:  **.csr**

**Generate**

**Continue**

Generate Request and Certificate Application | Menu option: Create Request

GENERATE CERTIFICATE - APPLICATION Theme Accent

Create Request Create Certificate Create SelfSign Cert. Issue Certificate

Main Create Request

Common Name: Test Local Gen.Alternative Names

Subject Alternative Names: s1.test.local s2.test.local s3.test.local s4.test.local

Key Length: 1024 X

Signature Algorithm: SHA1WITHRSA X

Country Code: For example "RS" X

State or Province Name: For example "Serbia" X

Locality Name: For example "Novi Sad" X

Organization: For example "Company123" X

Choose Key Usage:

Choose Extended Key Usage: ServerAuthentification

Path to store generate files: G:\PKI\GenCert\out X Browse

Private Key File Name: Name for private key file without extension X .key

Request Key File Name: Name for cert. request key file without extension X .csr

Generate

Continue

Generate Request and Certificate Application | Menu option: Create Request

GENERATE CERTIFICATE - APPLICATION Theme Accent

Create Request Create Certificate Create SelfSign Cert. Issue Certificate CA Certificate

Main Create Request

Common Name: webserver.local Gen.Alternative Names

Subject Alternative Names: webserver.local s1.webserver.local s2.webserver.local s3.webserver.local s4.webserver.local

Is this CA certificate: No

Key Length: 1024 X

Signature Algorithm: SHA512WITHRSA X

Country Code: RS X

State or Province Name: Serbia X

Locality Name: Novi Sad X

Organization: Company ABC X

Choose Key Usage:

Choose Extended Key Usage: ServerAuthentification

Path to store generate files: G:\PKI\GenCert\out\webserver X Browse

Private Key File Name: webserver\_private X .key

Request Key File Name: webserver\_request X .csr

Generate

Continue

Generate Request and Certificate Application | Menu option: Create Request

GENERATE CERTIFICATE - APPLICATION Theme Accent

Create Request Create Certificate Create SelfSign Cert. Issue Certificate CA Certificate

Main Create Request

Common Name: webserver.local Gen.Alternative Names

Subject Alternative Names: webserver.local s1.webserver.local s2.webserver.local s3.webserver.local s4.webserver.local

Is this CA certificate: No

Key Length: 1024 X

Signature Algorithm: SHA512WITHRSA X

Country Code: RS X

State or Province Name: Serbia X

Locality Name: Novi Sad X

Organization: Company ABC X

Choose Key Usage:

Choose Extended Key Usage: ServerAuthentification

Path to store generate files: G:\PKI\GenCert\out\webserver X Browse

Private Key File Name: webserver\_private X .key

Request Key File Name: webserver\_request X .csr

File with private key: G:\PKI\GenCert\out\webserver\webserver\_private.key successfully generated and saved.

Generate

Continue

Generate Request and Certificate Application | Menu option: Create Request

GENERATE CERTIFICATE - APPLICATION

Theme Accent

Create Request Create Certificate Create SelfSign Cert. Issue Certificate CA Certificate

Main Create Request

Common Name: webserver.local

Subject Alternative Names: webserver.local, s1.webserver.local, s2.webserver.local, s3.webserver.local, s4.webserver.local

Is this CA certificate: No

Key Length: 1024

Signature Algorithm: SHA512WITHRSA

Country Code: RS

State or Province Name: Serbia

Locality Name: Novi Sad

Organization: Company ABC

Choose Key Usage: Server Authentication

Path to store generate files: G:\PKI\GenCert\out\webserver

Private Key File Name: webserver\_private

Request Key File Name: webserver\_request

Generate Continue

File with private key: G:\PKI\GenCert\out\webserver\webserver\_private.key successfully generated and saved.  
File with certificate request: G:\PKI\GenCert\out\webserver\webserver\_request.csr successfully generated.  
File with certificate request: G:\PKI\GenCert\out\webserver\webserver\_request.csr successfully saved.

Generate Request and Certificate Application Menu option: Create Request

Tip:  
When files with request and private keys successfully created on

**NOTE:**  
To test if a request file is well created, you can use the certificates in the following folders:  
masterCA – master CA authority certificate files (demo root CA)  
intermediateCA – intermediate CA authority certificate files (demo intermediate CA)  
issuerCA – issuer CA authority certificate files (demo issuer CA)

If you wish to test request file with one level (only master CA) CA file use masterCA.pfx file from masterCA folder inside menu option "Issue Certificate".  
If you wish to test request file only two levels (root CA + intermediate CA) CA files use intermediateCA.pfx file from intermediateCA folder inside menu option "Issue Certificate".  
If you wish to test request file only with levels (root CA + intermediate CA + issuer CA) CA files use issuerCA.pfx file from issuerCA folder inside menu option "Issue Certificate".

To do this, click Continue and select the option "Sign locally-Have Ca cert" (data from the rootCA folder).

On the form, you receive (use described in the Issue Certificate section), issue the certificate issuance based on the request of the generated file (.csr) and when you generate a signed public certificate file (.cer), open it and check that all the attributes look right within that certificate.

Certificate

General Details Certification Path

Show: <All>

Field	Value
Valid from	petak, 15. mart 2019. 01:00:00
Valid to	nedelja, 15. mart 2020. 01:00:00
Subject	Company ABC, Novi Sad, Serb...
Public key	RSA (1024 Bits)
Public key parameters	05 00
Enhanced Key Usage	Server Authentication (1.3.6...
Subject Alternative Name	DNS Name=webserver.local, ...
Subject Key Identifier	07e34d1937698401baaa9094r5

DNS Name=webserver.local  
DNS Name=s1.webserver.local  
DNS Name=s2.webserver.local  
DNS Name=s3.webserver.local  
DNS Name=s4.webserver.local

Edit Properties... Copy to File...

OK

If in the "Subject Alternative Name" section everything looks OK, then the request file for the certificate is properly created and you can continue.

## Create Signed Certificate (step)

Generate pfx file (when you got signed certificate file from external CA root authority e.g. GoDaddy)

Variant I – without CA public keys -> “Path for Master CA file”, “Path for Intermediate CA file”, “Path for Issuer CA file” is empty

GENERATE CERTIFICATE - APPLICATION

Create Request Create Certificate Create SelfSign Cert. Issue Certificate CA Certificate

Main Create Request CA Certificate Issue Certificate **Create Certificate**

Certificate Friendly name: Certificate Friendly name

Path for signed request file (.cer): G:\PKI\GenCert\out\webserver\webserver.cer

Path for private key file (.key): G:\PKI\GenCert\out\webserver\webserver\_private.key

Path for generate certificate file (.pfx): G:\PKI\GenCert\out\webserver

Certificate File Name: Name for certificate file without extension .pfx

Password for export private key: Password

Path for Master CA file (.cer) (Optional): Select Master CA .cer file path

Path for Intermediate CA file (.cer) (Optional): Select Intermediate CA .cer file path

Path for Issuer CA file (.cer) (Optional): Select Issuer CA .cer file path

Generate

Generate Request and Certificate Application | Menu option: Create Certificate

You need inside fields:

“Path for Master CA file”, “Path for Intermediate CA file”, “Path for Issuer CA file” to enter file path for appropriate CA certificate.

GENERATE CERTIFICATE - APPLICATION

Create Request Create Certificate Create SelfSign Cert. Issue Certificate CA Certificate

Main Create Request CA Certificate Issue Certificate **Create Certificate**

Certificate Friendly name: Certificate Friendly name

Path for signed request file (.cer): G:\PKI\GenCert\out\webserver\webserver.cer

Path for private key file (.key): G:\PKI\GenCert\out\webserver\webserver\_private.key

Path for generate certificate file (.pfx): G:\PKI\GenCert\out\webserver

Certificate File Name: Name for certificate file without extension .pfx

Password for export private key: Password

Path for Master CA file (.cer) (Optional): Select Master CA .cer file path

Path for Intermediate CA file (.cer) (Optional): Select Intermediate CA .cer file path

Path for Issuer CA file (.cer) (Optional): Select Issuer CA .cer file path

Generate

Generate Request and Certificate Application | Menu option: Create Certificate

Enter file path and click Generate button.

GENERATE CERTIFICATE - APPLICATION

Create Request Create Certificate Create SelfSign Cert. Issue Certificate CA Certificate

Main Create Request CA Certificate Issue Certificate **Create Certificate**

Certificate Friendly name: ABC WebServer

Path for signed request file (.cer): G:\PKI\GenCert\out\webserver\webserver.cer

Path for private key file (.key): G:\PKI\GenCert\out\webserver\webserver\_private.key

Path for generate certificate file (.pfx): G:\PKI\GenCert\out\webserver

Certificate File Name: webserver .pfx

Password for export private key: ●●●●

Path for Master CA file (.cer) (Optional): G:\PKI\GenCert\out\masterCA\masterCA\_public.cer

Path for Intermediate CA file (.cer) (Optional): G:\PKI\GenCert\out\intermediateCA\intermediateCA\_public.cer

Path for Issuer CA file (.cer) (Optional): G:\PKI\GenCert\out\issuerCA\issuerCA\_public.cer

Generate

Certificate file with private key: G:\PKI\GenCert\out\webserver\webserver.pfx and Master, Intermediate, Issuer CA public key successfully generated.

Generate Request and Certificate Application | Menu option: Create Certificate

Variant II – with CA public keys -> “Path for Master CA file”, “Path for Intermediate CA file”, “Path for Issuer CA file” – enter path for public certificate files for CA server(s)

The screenshot shows the 'GENERATE CERTIFICATE - APPLICATION' window. The 'Create Certificate' tab is selected. The form contains the following fields and values:

- Certificate Friendly name: ABC WebServer
- Path for signed request file (.cer): G:\\_PKI\GenCert\out\webserver\webserver.cer
- Path for private key file (.key): G:\\_PKI\GenCert\out\webserver\webserver\_private.key
- Path for generate certificate file (.pfx): G:\\_PKI\GenCert\out\webserver
- Certificate File Name: webserver
- Password for export private key: [masked]
- Path for Master CA file (.cer) (Optional): G:\\_PKI\GenCert\out\masterCA\masterCA\_public.cer
- Path for Intermediate CA file (.cer) (Optional): G:\\_PKI\GenCert\out\intermediateCA\intermediateCA\_public.cer
- Path for Issuer CA file (.cer) (Optional): G:\\_PKI\GenCert\out\issuerCA\issuerCA\_public.cer

A red box highlights the three optional CA file paths. A green box at the bottom of the form area contains the message: "Certificate file with private key: G:\\_PKI\GenCert\out\webserver\webserver.pfx and Master, Intermediate, Issuer CA public key successfully generated." The 'Generate' button at the bottom left is highlighted with an orange box.

Go to „[Import certificate from generated pfx file](#)“

### Generate certificate file for web server (use internal CA(s) for sign request)

Done	Menu option (step)	Comment
<input type="checkbox"/>	Create Request	<p>Fill in all the information in the form. When you click on the "Generate" button, the application will be in a folder whose path is listed in the "Path to store generate files:" field, generate two files.</p> <p>The first file with a .key extension is a private certificate key file. Another file with the .csr extension is a certificate request file that will be signed by the internal root CA (which already exists or can be generated -&gt; option: "Create SelfSign Cert.")</p> <p><b>NOTE:</b></p> <p>If there are already files in the selected location with the same name, you need to delete these files and start generating again.</p> <p>On the form, click the "Continue" button switches to the next "step"</p>
<input type="checkbox"/>	CA Certificate	<p>Fill in all the information in the form, or click on the "Test Data" button to fill all form fields with test data.</p> <p>When the "Generate" button is clicked, the application will generate 3 folders and generate 2 files in each folder.</p> <ul style="list-style-type: none"> <li>-The first file with the .csr extension is a public key certificate for the (master / intermediate / issuer) CA server.</li> <li>-The other file with the extension .pfx is a certificate that contains a private + public key for the (master / intermediate / issuer) CA server.</li> </ul> <p><b>NOTICE for Test Data:</b></p> <p>If, for example, we want to generate only MasterCA and intermediateCA certificates, you need to leave the "Common Name:" field in the Issuer CA section blank.</p> <p>If, for example, we want to generate only the masterCA certificate, we need to leave the "Common Name:" field in the Issuer CA and Intermediate CA section blank.</p> <p><b>NOTE for Continue:</b></p> <p>On the form, there are 3 x Continue buttons on each part of the form (master / intermediate / issuer).</p> <p>Depending on which Continue button is pressed, the form for the "Issue Certificate" with the automatic certificate field for the CA certificate path file (.pfx) is called. However, depending on that, the certificate's request file will be signed as with the (master / intermediate / issuer) certificate.</p>

		<p><b>NOTE:</b> If there are already files in the selected location with the same name, you need to delete these files and start generating again.</p> <p>On this form, click the "Continue" button switches to the next "step"</p>
<input type="checkbox"/>	Issue Certificate	<p>Fill in all the information in the form. When the "Generate" button is clicked, the application will be in a folder whose path is specified in the "Path for generate signed cert.file (.cer)" field: "generate two filenames with the name specified in the" Signed request File Name ".</p> <p><b>NOTE:</b> If there are already files in the selected location with the same name, you need to delete these files and start generating again.</p> <p>From this form, clicking the "Continue" button switches to the next "step"</p>
<input type="checkbox"/>	Create Signed Certificate	<p>On the form, enter the path to the .cer file obtained from root CA and the .key file containing the private key certificate for which we sent the .csr file to the client. It is necessary to select a folder in which a signed certificate file with a private key will be generated (file with .pfx extension).</p> <p><b>NOTE:</b> Depending on whether they are in the fields:          "Path for Master CA file (.cer) (Optional):"          "Path for Intermediate CA file (.cer) (Optional):"          "Path for Issuer CA file (.cer) (Optional):"          entered path to public key from (master / intermediate / issuer) CA authority that signed the request file, in the generated .pfx file the chain of the mentioned certificates will be located or not.</p>

## Create Request (step)

**GENERATE CERTIFICATE - APPLICATION**

Theme Accent

[Create Request](#)
[Create Certificate](#)
[Create SelfSign Cert.](#)
[Issue Certificate](#)
[CA Certificate](#)

Main

Create Request

Common Name:

Subject Alternative Names:

Is this CA certificate:

No

Key Length:

1024

Signature Algorithm:

SHA512WITHRSA

Country Code:

For example "RS"

State or Province Name:

For example "Serbia"

Locality Name:

For example "Novi Sad"

Organization:

For example "Company123"

Choose Key Usage:

Choose Extended Key Usage:

ServerAuthetification

Path to store generate files:

G:\\_PKI\GenCert\out

Private Key File Name:

Name for private key file without extension

Request Key File Name:

Name for cert. request key file without extension

Generate

Continue

Gen.Alternative Names

Browse

.key

.csr

Generate Request and Certificate Application | Menu option: Create Request

GENERATE CERTIFICATE - APPLICATION

ThemeAccent

Create RequestCreate CertificateCreate SelfSign Cert. Issue CertificateCA Certificate

MainCreate Request

Common Name:webserver.local

Gen.Alternative Names

Subject Alternative Names:

webserver.locals1.webserver.locals2.webserver.local  
s3.webserver.local  
s4.webserver.local

Is this CA certificate:No

Key Length:1024

Signature Algorithm:SHA512WITHRSA

Country Code:For example "RS"

State or Province Name:For example "Serbia"

Locality Name:For example "Novi Sad"

Organization:For example "Company123"

Choose Key Usage:

Choose Extended Key Usage:ServerAuthetification

Path to store generate files :G:\PKI\GenCert\outBrowse

Private Key File Name:Name for private key file without extension.key

Request Key File Name:Name for cert. request key file without extension.csr

Generate

Continue

Generate Request and Certificate Application | Menu option: Create Request

GENERATE CERTIFICATE - APPLICATION

ThemeAccent

Create RequestCreate CertificateCreate SelfSign Cert. Issue Certificate

MainCreate Request

Common Name:Test Local

Gen.Alternative Names

Subject Alternative Names:

s1.test.locals2.test.local  
s3.test.local  
s4.test.local

Key Length:1024

Signature Algorithm:SHA1WITHRSA

Country Code:For example "RS"

State or Province Name:For example "Serbia"

Locality Name:For example "Novi Sad"

Organization:For example "Company123"

Choose Key Usage:

Choose Extended Key Usage:ServerAuthetification

Path to store generate files :G:\PKI\GenCert\outBrowse

Private Key File Name:Name for private key file without extension.key

Request Key File Name:Name for cert. request key file without extension.csr

Generate

Continue

Generate Request and Certificate Application | Menu option: Create Request



GENERATE CERTIFICATE - APPLICATION Theme Accent

Create Request Create Certificate Create SelfSign Cert. Issue Certificate CA Certificate

Main Create Request

Common Name: webserver.local Gen Alternative Names

Subject Alternative Names: webserver.local  
s1.webserver.local  
s2.webserver.local  
s3.webserver.local  
s4.webserver.local

Is this CA certificate: No

Key Length: 1024

Signature Algorithm: SHA512WITHRSA

Country Code: RS

State or Province Name: Serbia

Locality Name: Novi Sad

Organization: Company ABC

Choose Key Usage:

Choose Extended Key Usage: ServerAuthetification

Path to store generate files: G:\PKI\GenCert\out\webserver Browse

Private Key File Name: webserver\_private .key

Request Key File Name: webserver\_request .csr

Generate

Generate Request and Certificate Application | Menu option: Create Request

GENERATE CERTIFICATE - APPLICATION Theme Accent

Create Request Create Certificate Create SelfSign Cert. Issue Certificate CA Certificate

Main Create Request

Common Name: webserver.local Gen Alternative Names

Subject Alternative Names: webserver.local  
s1.webserver.local  
s2.webserver.local  
s3.webserver.local  
s4.webserver.local

Is this CA certificate: No

Key Length: 1024

Signature Algorithm: SHA512WITHRSA

Country Code: RS

State or Province Name: Serbia

Locality Name: Novi Sad

Organization: Company ABC

Choose Key Usage:

Choose Extended Key Usage: ServerAuthetification

Path to store generate files: G:\PKI\GenCert\out\webserver Browse

Private Key File Name: webserver\_private .key

Request Key File Name: webserver\_request .csr

File with private key: G:\PKI\GenCert\out\webserver\webserver\_private.key sucessfully generated and saved.

Generate

Generate Request and Certificate Application | Menu option: Create Request

GENERATE CERTIFICATE - APPLICATION Theme Accent

Create Request Create Certificate Create SelfSign Cert. Issue Certificate CA Certificate

Main Create Request

Common Name: webserver.local Gen Alternative Names

Subject Alternative Names: webserver.local  
s1.webserver.local  
s2.webserver.local  
s3.webserver.local  
s4.webserver.local

Is this CA certificate: No

Key Length: 1024

Signature Algorithm: SHA512WITHRSA

Country Code: RS

State or Province Name: Serbia

Locality Name: Novi Sad

Organization: Company ABC

Choose Key Usage:

Choose Extended Key Usage: ServerAuthetification

Path to store generate files: G:\PKI\GenCert\out\webserver Browse

Private Key File Name: webserver\_private .key

Request Key File Name: webserver\_request .csr

File with private key: G:\PKI\GenCert\out\webserver\webserver\_private.key sucessfully generated and saved.  
File with certificate request : G:\PKI\GenCert\out\webserver\webserver\_request.csr sucessfully generated.  
File with certificate request : G:\PKI\GenCert\out\webserver\webserver\_request.csr sucessfully saved.

Generate

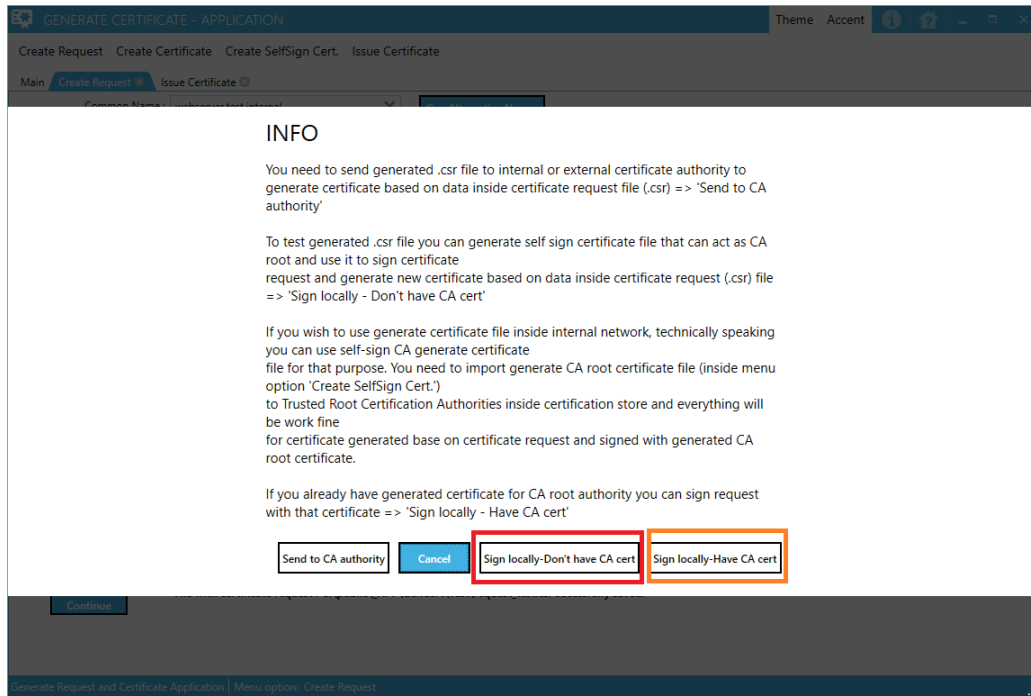
Continue

Generate Request and Certificate Application | Menu option: Create Request

Tip:

When files with request and private keys successfully created on Continue button will be enabled.

Click Continue button



Depending on whether you already have a generic root certificate that you will use to sign (orange) or there is no root certificate that you will use for signing (red), click on the appropriate button.

## CA Certificate (step)

Variant I – „Sign locally-Don't have CA cert “

When click “Test Data L1” or “Test Data L2” or “Test Data L3”, new form for fill CA Parameters will be open.

GENERATE CERTIFICATE - APPLICATION

Theme Accent

Create RequestCreate CertificateCreate SelfSign Cert. Issue CertificateCA Certificate

MainCA Certificate

Expand / Collapse master CA

Master CA :

Common Name : For example masterCA.test.local

Key Length: 4096

Signature Algorithm: SHA512WITHRSA

Country Code: For example "RS"

State or Province Name: For example "Serbia"

Locality Name: For example "Novi Sad"

Organization: For example "ABC"

Start Date: 15.3.2019

End Date: 15.3.2029

Path for generate files : G:\PKI

Public Key File Name: Name

Signed Key File Name: Name

Password for export: Password

Certificate Friendly name: Master CA

Test Data L1

Test Data L2

Test Data L3

Generate

Continue

Clean data

Collapse Intermediate CA

Collapse Issuer CA

CA PARAMETERS

Organization : ABC

Domain name : test.local

Country Code : RS

State or Province name : Serbia

Locality Name : Novi Sad

Password :

Ok

Cancel

Generate Request and Certificate Application | Menu option: CA Certificate

GENERATE CERTIFICATE - APPLICATION

Theme Accent

Create RequestCreate CertificateCreate SelfSign Cert. Issue CertificateCA Certificate

MainCA Certificate

Expand / Collapse master CA

Master CA :

Common Name : ABC masterCA.test.local

Key Length: 4096

Signature Algorithm: SHA512WITHRSA

Country Code: RS

State or Province Name: Serbia

Locality Name: Novi Sad

Organization: Master CA CO

Start Date: 12.3.2019

End Date: 15.3.2029

Path for generate files : G:\PKI\GenCert\out\masterCA

Public Key File Name: masterCA\_public

Signed Key File Name: masterCA

Password for export:

Certificate Friendly name: ABC Master CA

Test Data L1

Test Data L2

Test Data L3

Generate

Continue

Clean data

Expand / Collapse Intermediate CA

Intermediate CA :

Common Name : ABC intermediateCA.test.local

Key Length: 2048

Signature Algorithm: SHA512WITHRSA

Country Code: RS

State or Province Name: Serbia

Locality Name: Novi Sad

Organization: Intermediate CA CO

Start Date: 13.3.2019

End Date: 15.3.2028

Path for generate files : G:\PKI\GenCert\out\intermediateCA

Public Key File Name: intermediateCA\_public

Signed Key File Name: intermediateCA

Password for export:

Certificate Friendly name: ABC Intermediate CA

Continue

Clean data

Expand / Collapse Issuer CA

Issuer CA :

Common Name : ABC issuerCA.test.local

Key Length: 1024

Signature Algorithm: SHA512WITHRSA

Country Code: RS

State or Province Name: Serbia

Locality Name: Novi Sad

Organization: Issuer CA CO

Start Date: 14.3.2019

End Date: 15.3.2027

Path for generate files : G:\PKI\GenCert\out\issuerCA

Public Key File Name: issuerCA\_public

Signed Key File Name: issuerCA

Password for export:

Certificate Friendly name: ABC Issuer CA

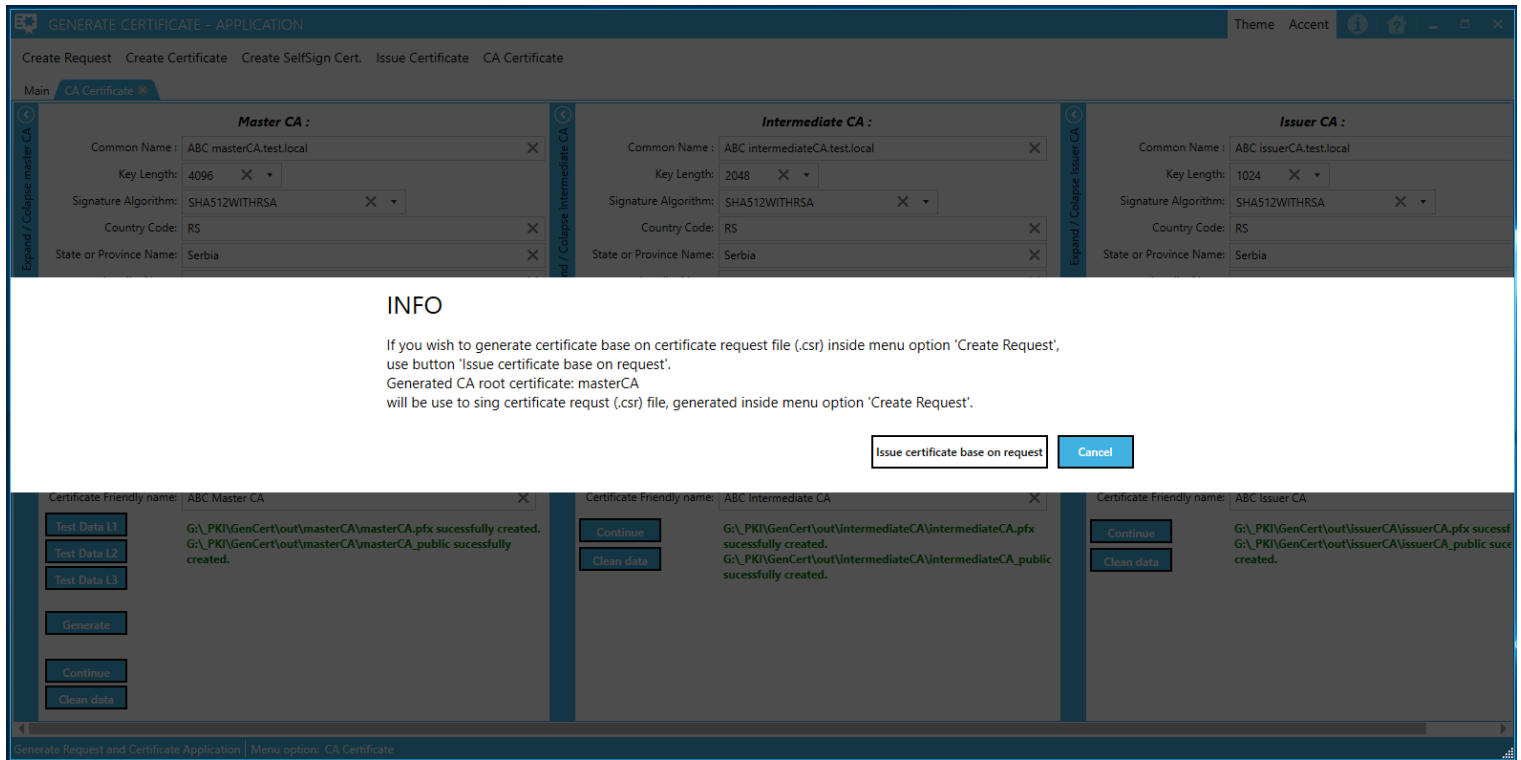
Continue

Clean data

Generate Request and Certificate Application | Menu option: CA Certificate

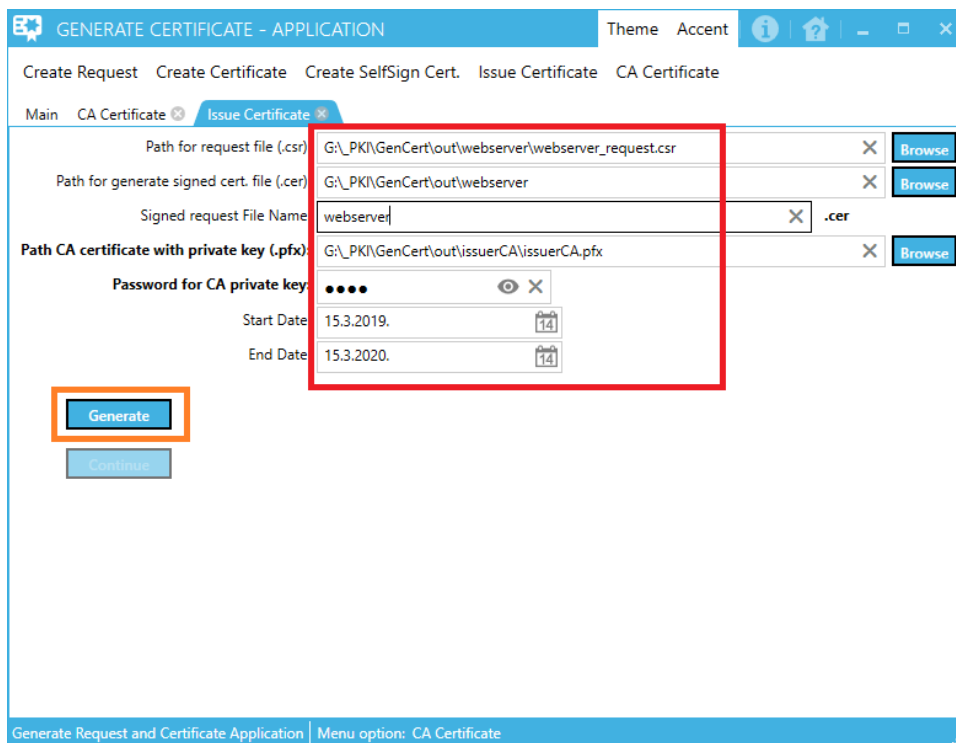
OK

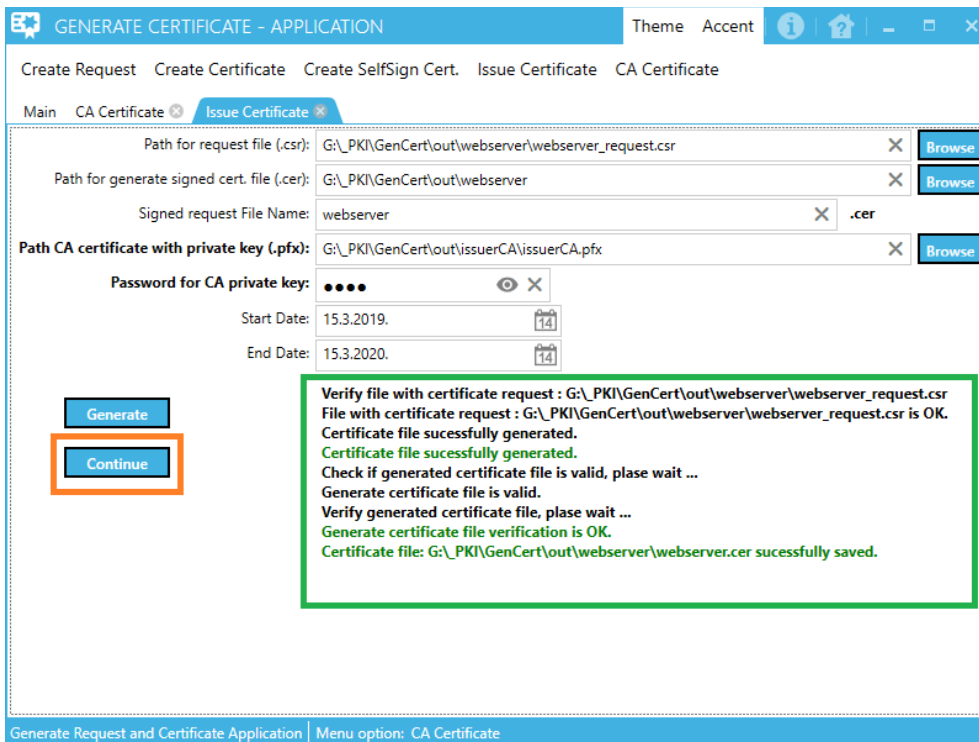
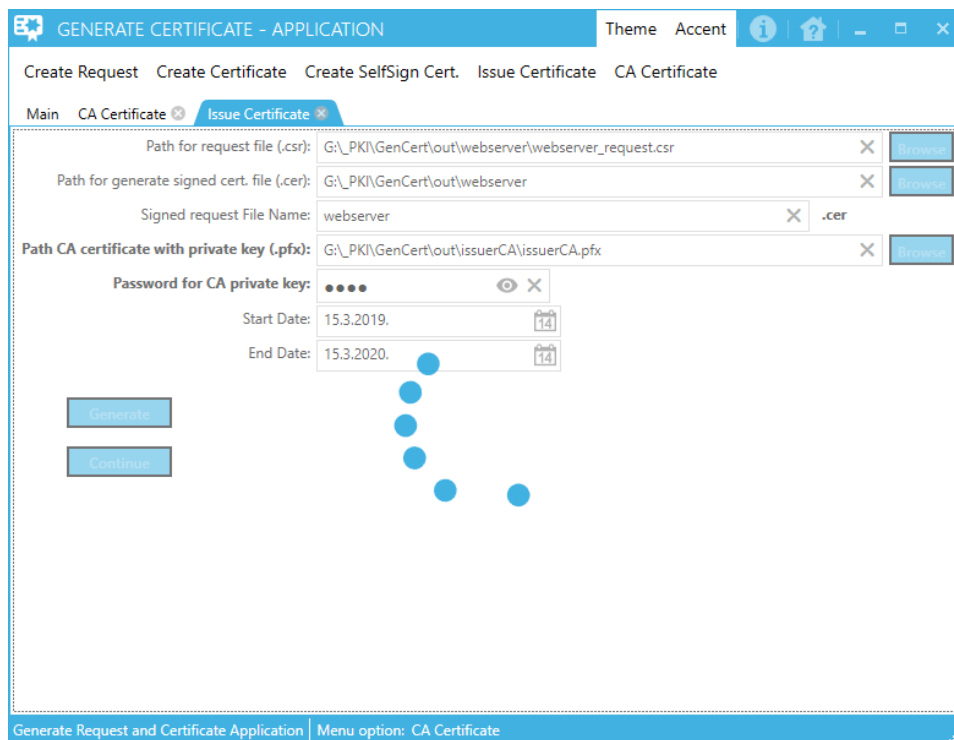
Generate Request and Certificate Application | Menu option: CA CertificateGenerate Request and Certificate Application | Menu option: CA Certificate



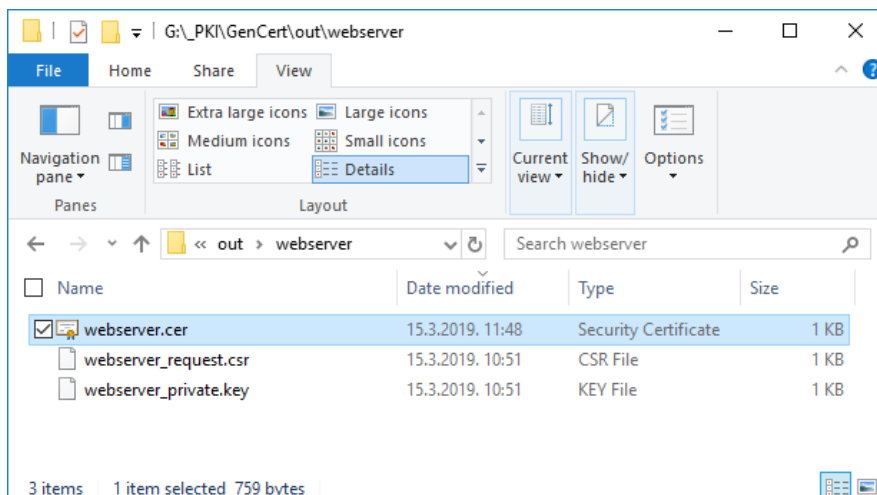
## Variant II – „Sign locally-Have CA cert“

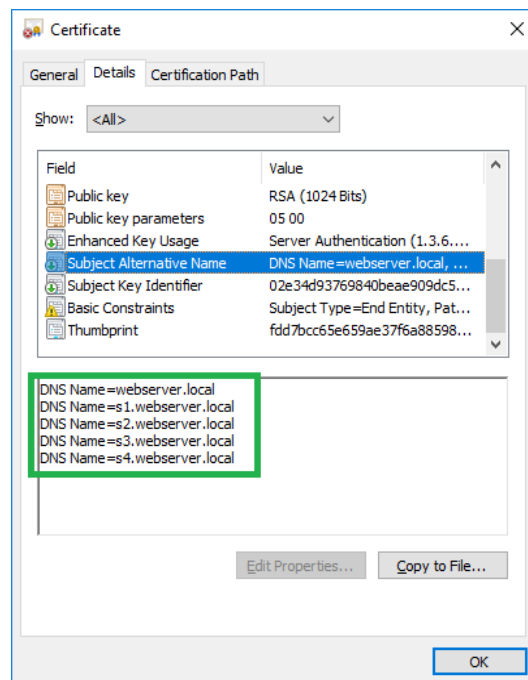
**NOTE:** If you use the root certificate from the rootCA subfolder, in the cert\_password.txt file in that folder there is a password that needs to be entered in the form.





To verify that the signed certificate is successfully generated, perform a check

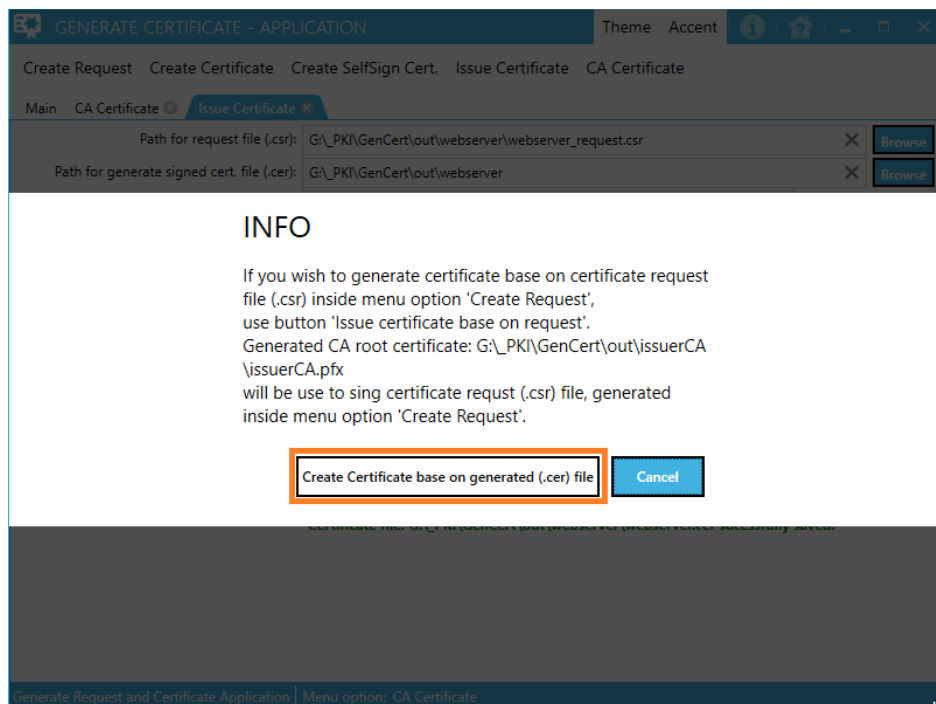




An alternate name certificate is OK.

Click "Continue".

We continue to generate a file that will contain public + private key (.pfx), from a signed file (.cer) to a private key (.key)



Issue Certificate (step)

GENERATE CERTIFICATE - APPLICATION

ThemeAccent

Create RequestCreate CertificateCreate SelfSign Cert. Issue CertificateCA Certificate

MainCA CertificateIssue Certificate

Path for request file (.csr):G:\\_PKI\GenCert\out\webserver\webserver\_request.csr

Path for generate signed cert. file (.cer):G:\\_PKI\GenCert\out\webserver

Signed request File Name:webserver.cer

Path CA certificate with private key (.pfx):G:\\_PKI\GenCert\out\issuerCA\issuerCA.pfx

Password for CA private key:.....

Start Date:15.3.2019.

End Date:15.3.2020.

Generate

Continue

Generate Request and Certificate Application | Menu option: CA Certificate

GENERATE CERTIFICATE - APPLICATION

ThemeAccent

Create RequestCreate CertificateCreate SelfSign Cert. Issue CertificateCA Certificate

MainCA CertificateIssue Certificate

Path for request file (.csr):G:\\_PKI\GenCert\out\webserver\webserver\_request.csr

Path for generate signed cert. file (.cer):G:\\_PKI\GenCert\out\webserver

Signed request File Name:webserver.cer

Path CA certificate with private key (.pfx):G:\\_PKI\GenCert\out\issuerCA\issuerCA.pfx

Password for CA private key:.....

Start Date:15.3.2019.

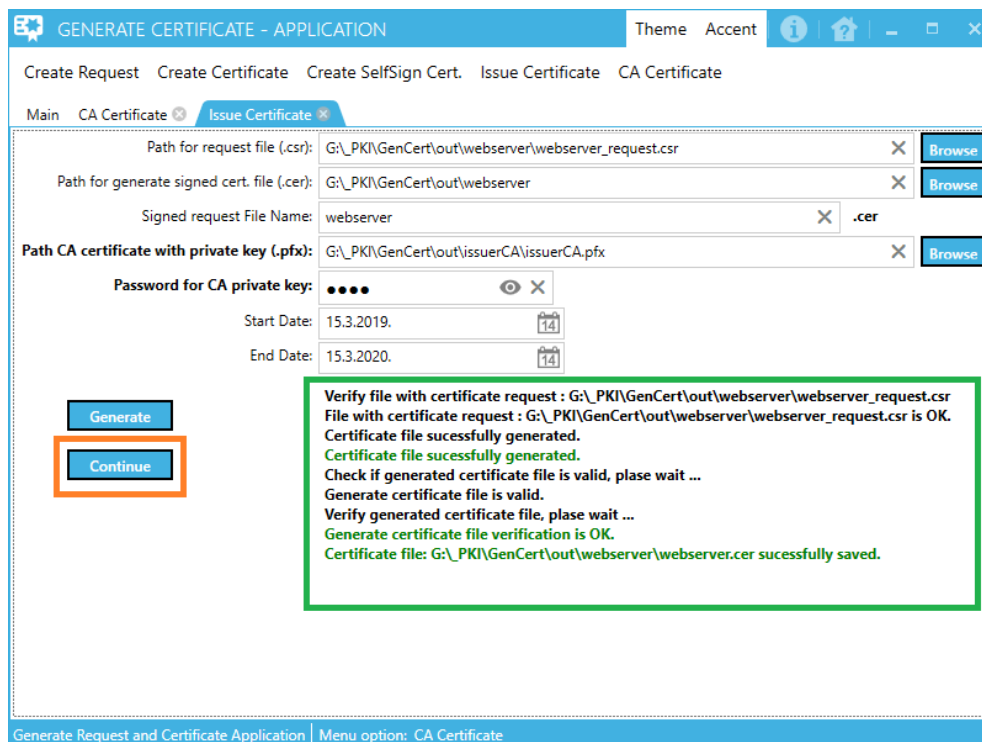
End Date:15.3.2020.

Generate

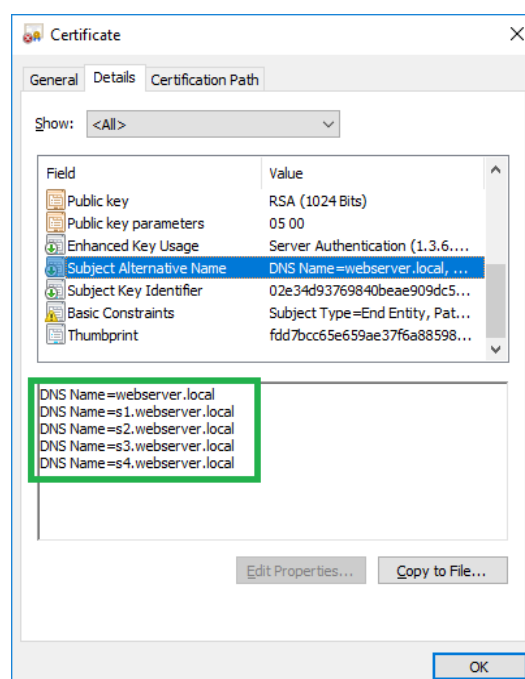
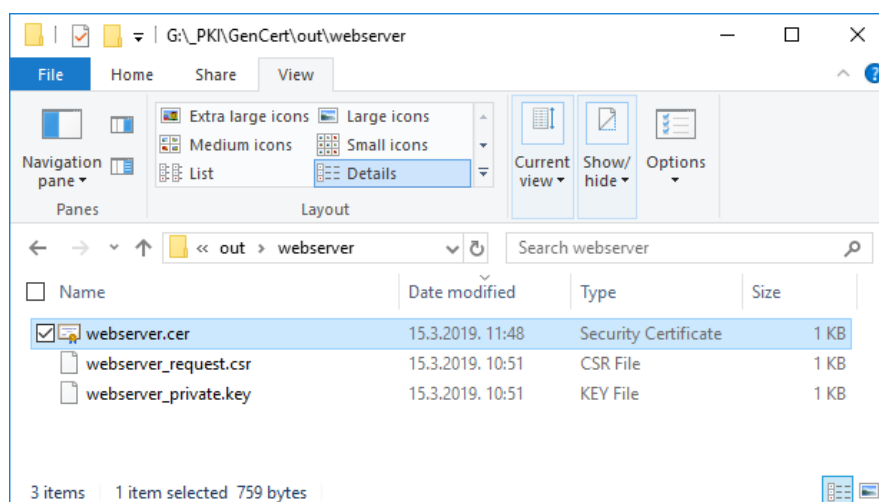
Continue

Generate Request and Certificate Application | Menu option: CA Certificate





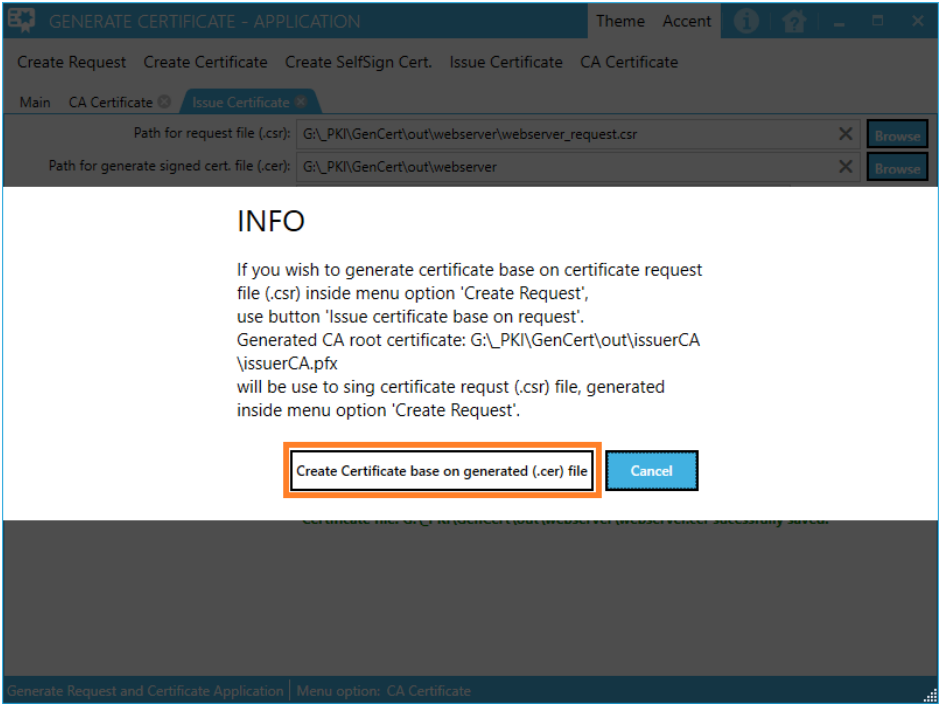
To verify that the signed certificate is successfully generated, perform a check



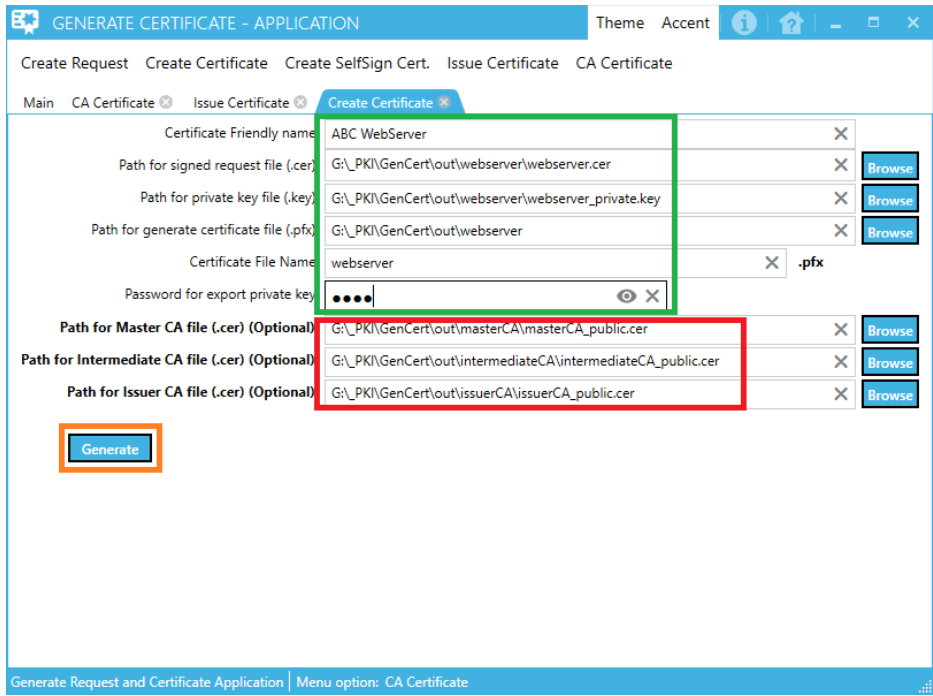
An alternate name certificate is OK.

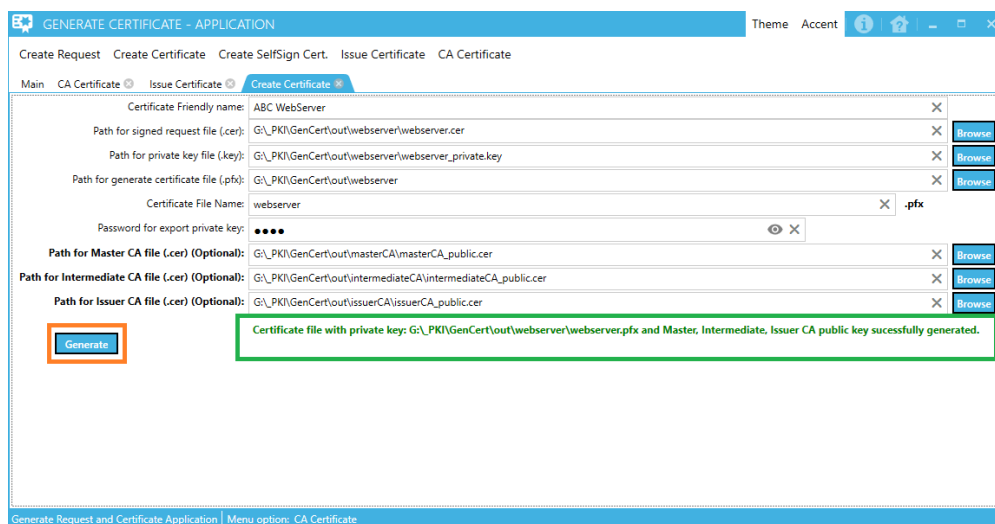
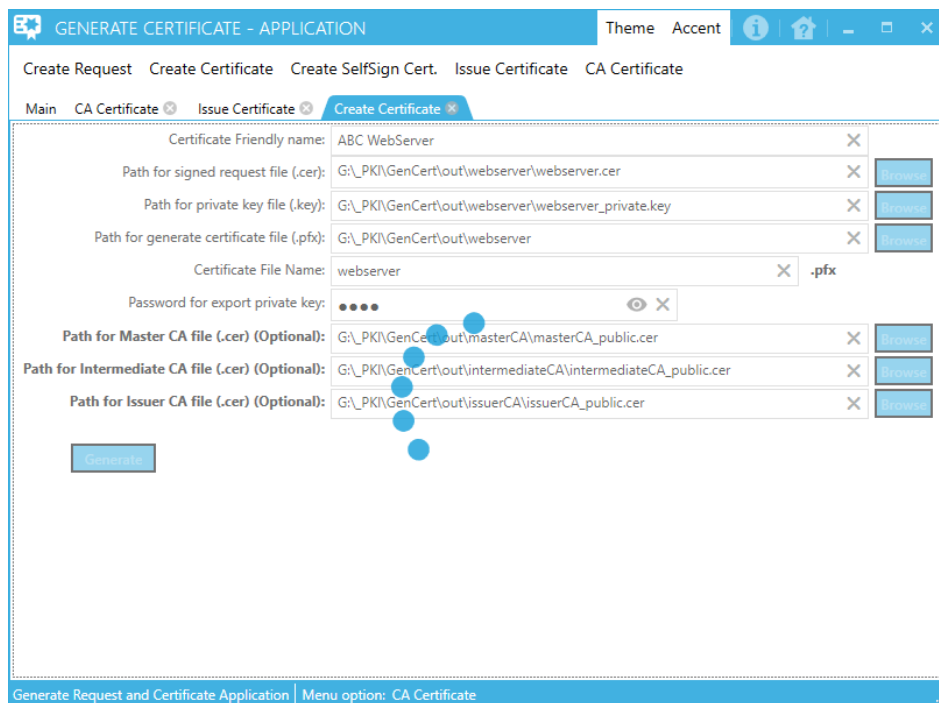
Click "Continue".

We continue to generate a file that will contain public + private key (.pfx), from a signed file (.cer) to a private key (.key)



Create Signed Certificate (step)

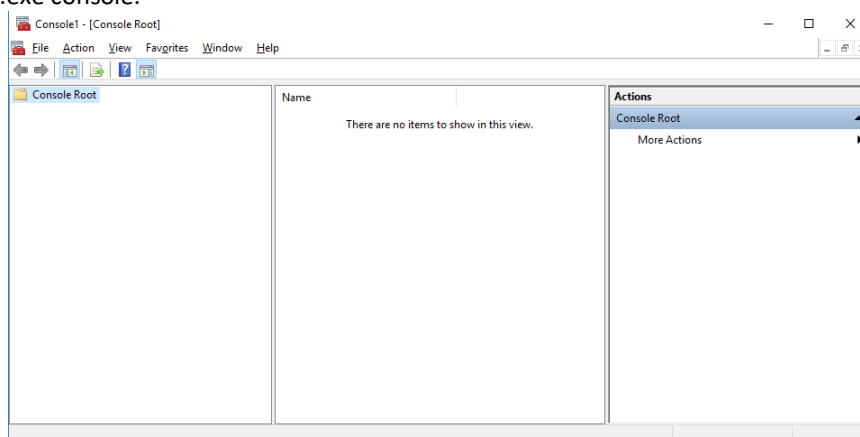




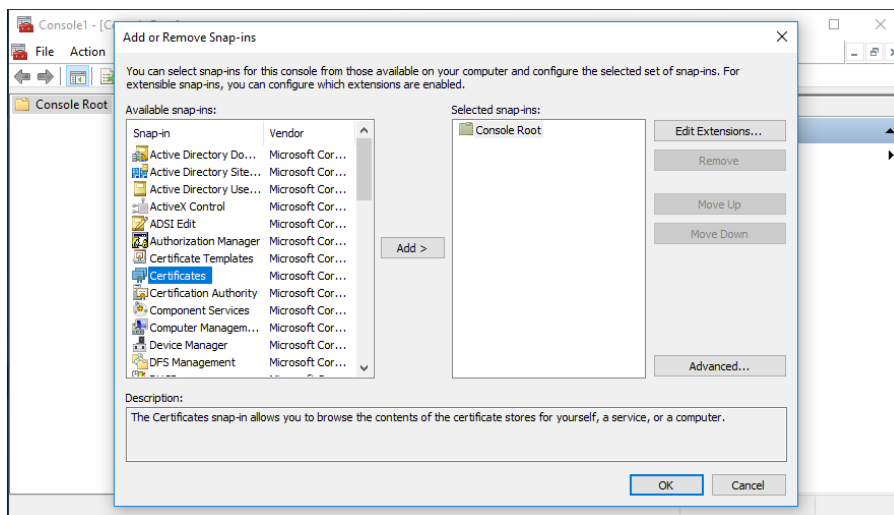
Go to „[Import certificate from generated pfx file](#)“

Import certificate from generated pfx file to web server

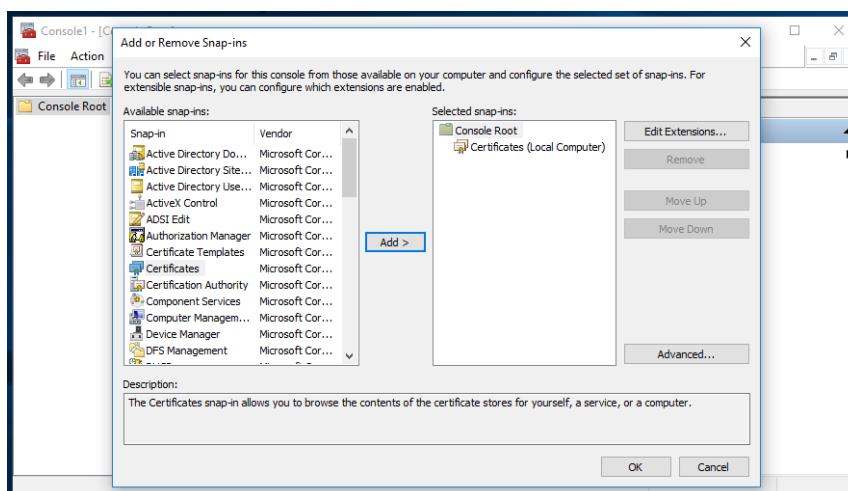
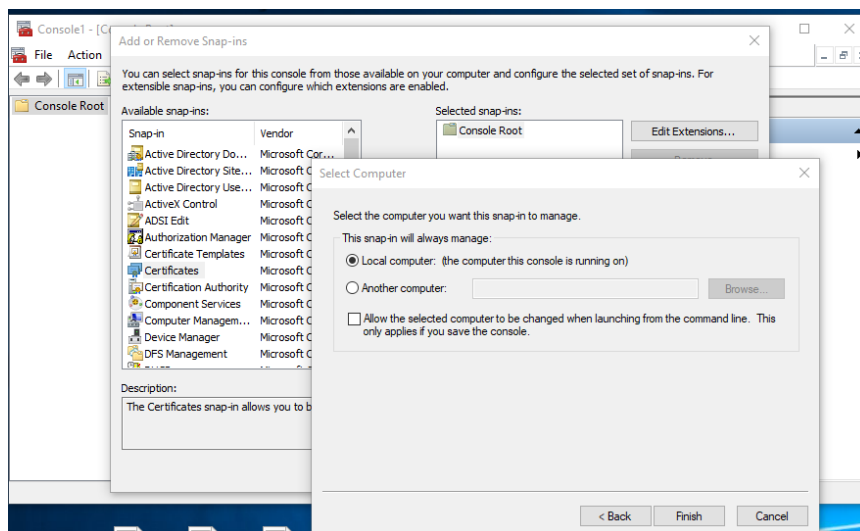
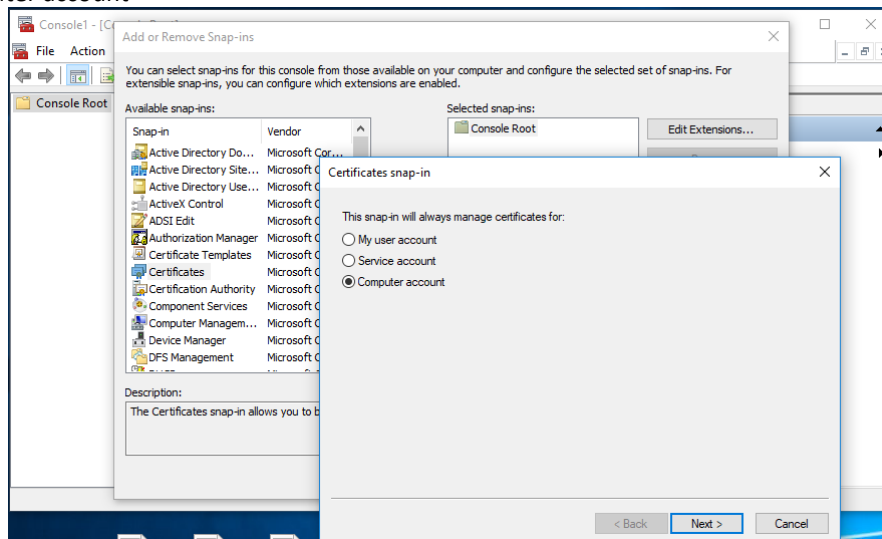
On the computer, open mmc.exe console.

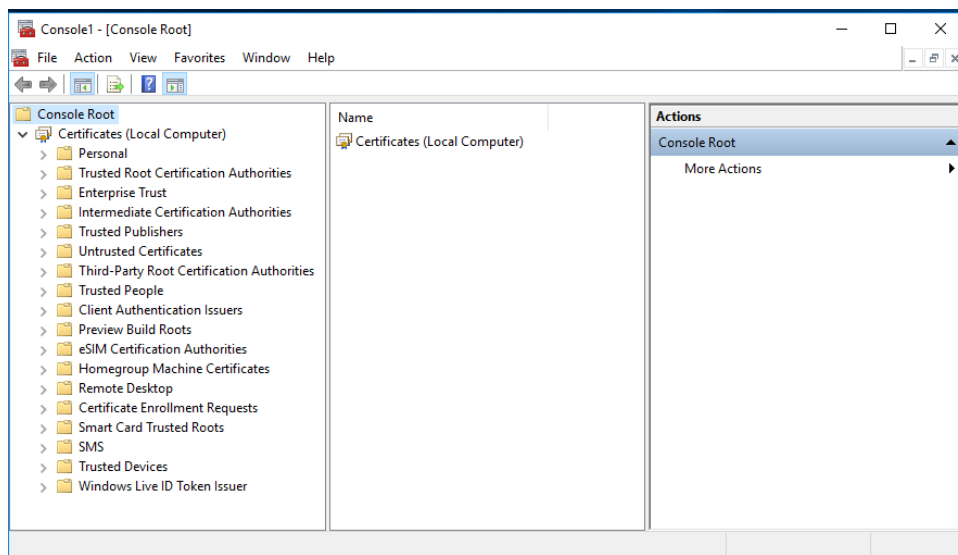


Add Certificate Snap-in



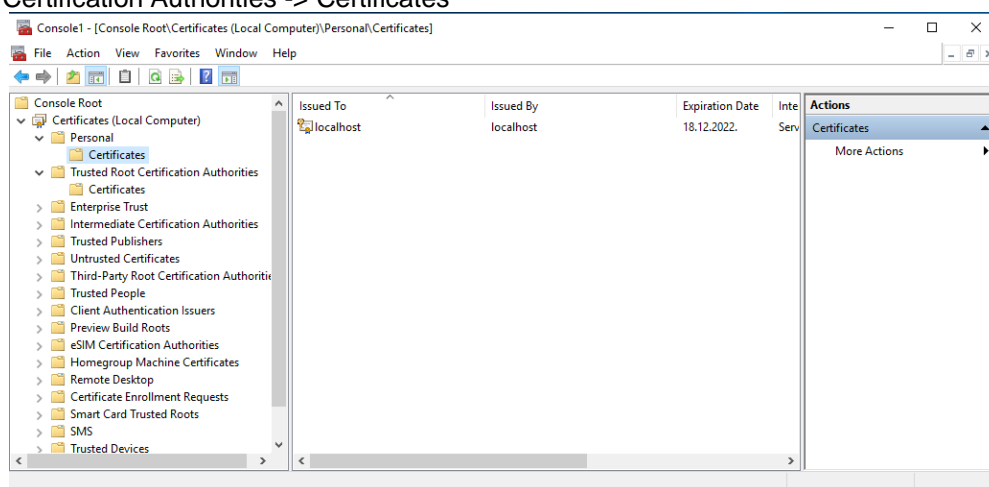
Add, Choose option “Computer account”



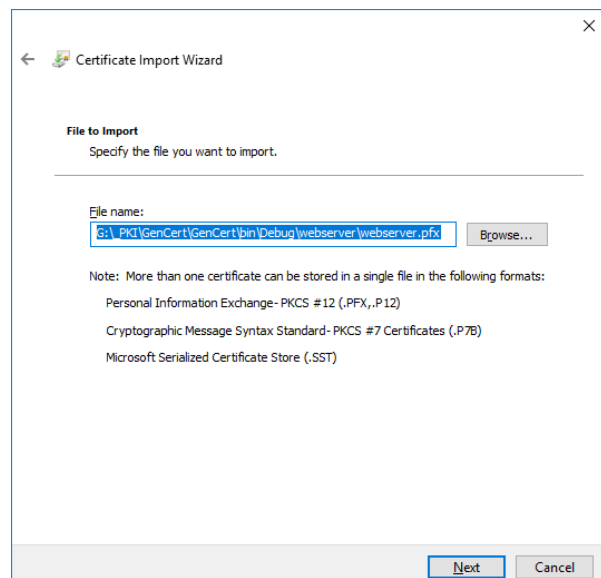
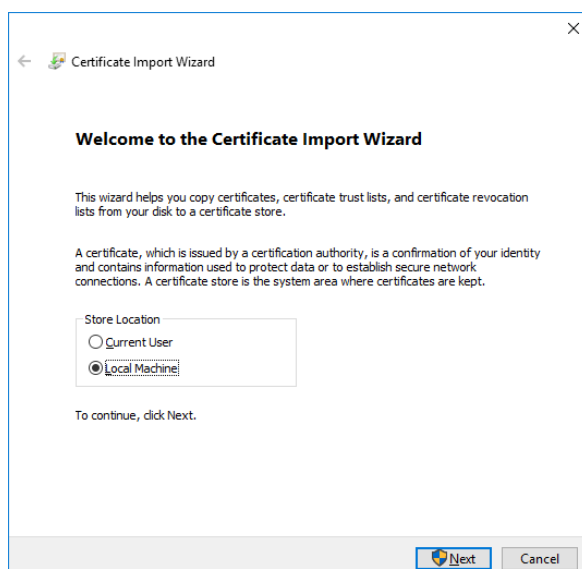


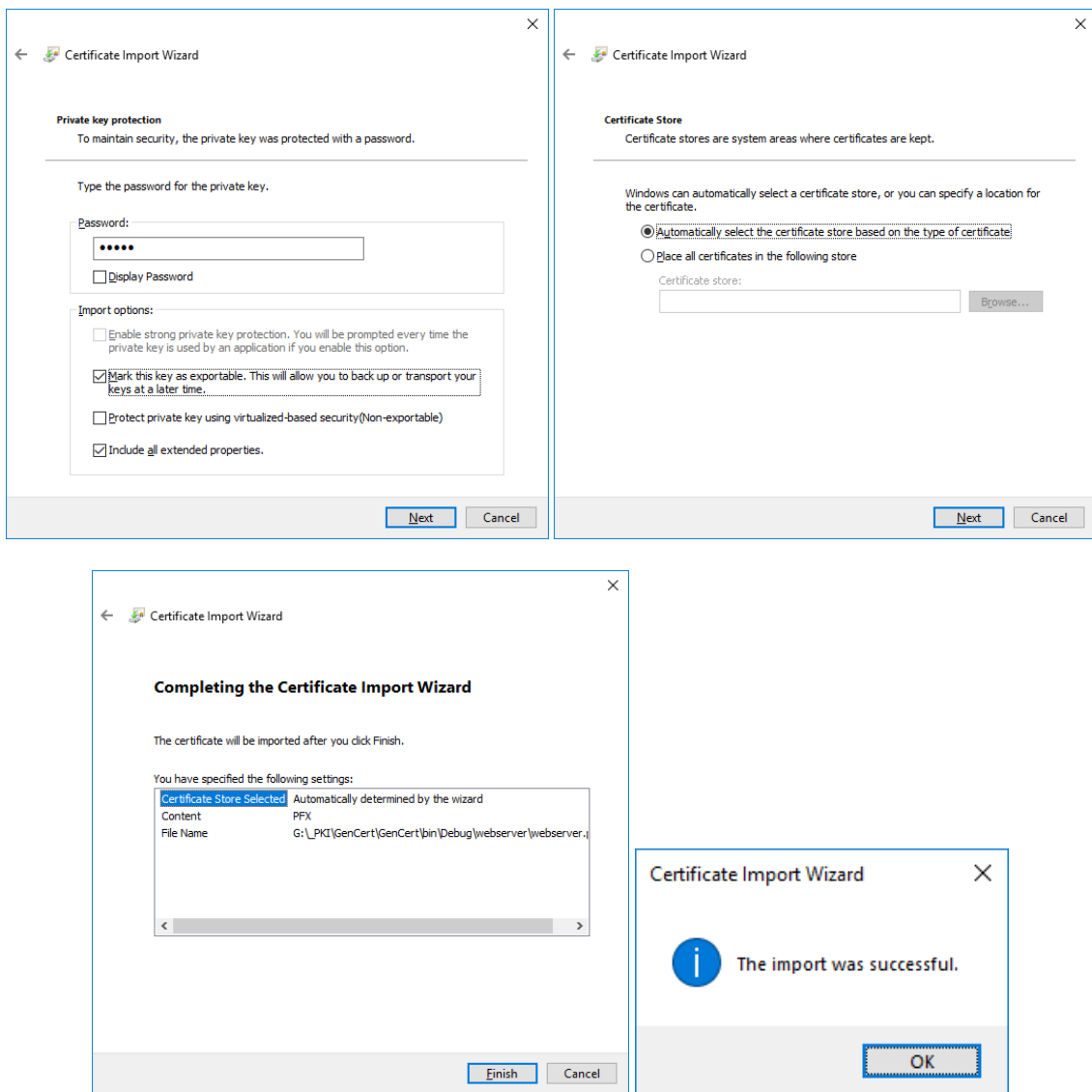
Parts of local computer Certificate store for interest are:

1. Personal -> Certificates
2. Trusted Root Certification Authorities -> Certificates
3. Intermediate Certification Authorities -> Certificates

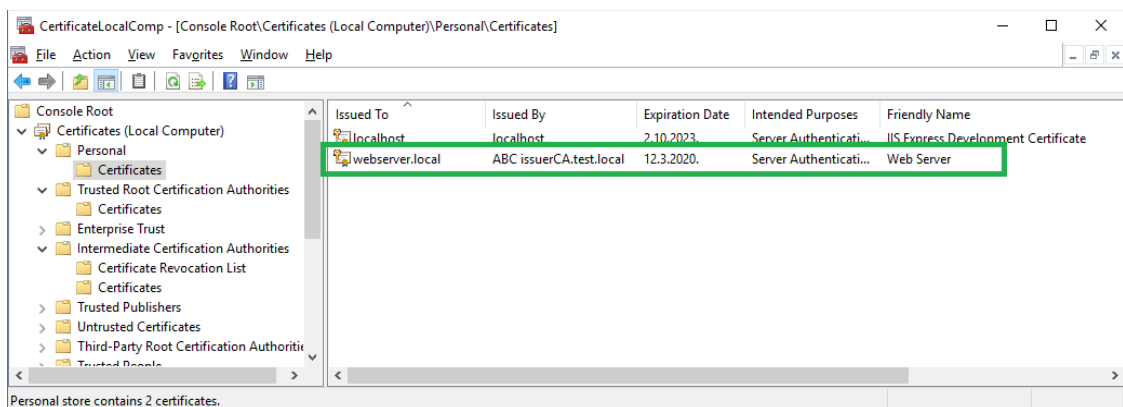
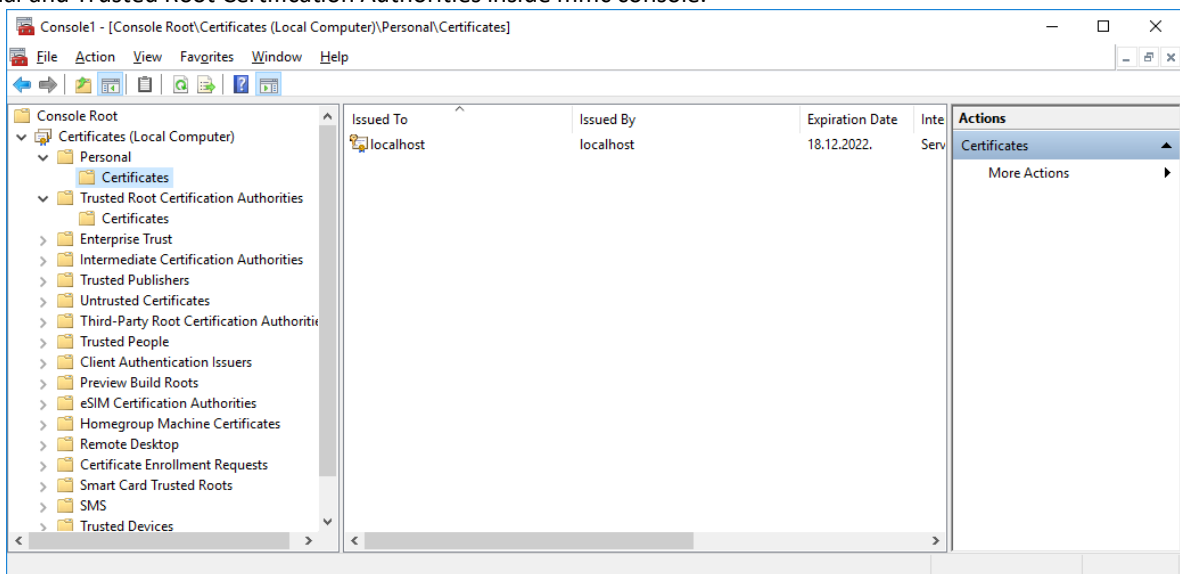


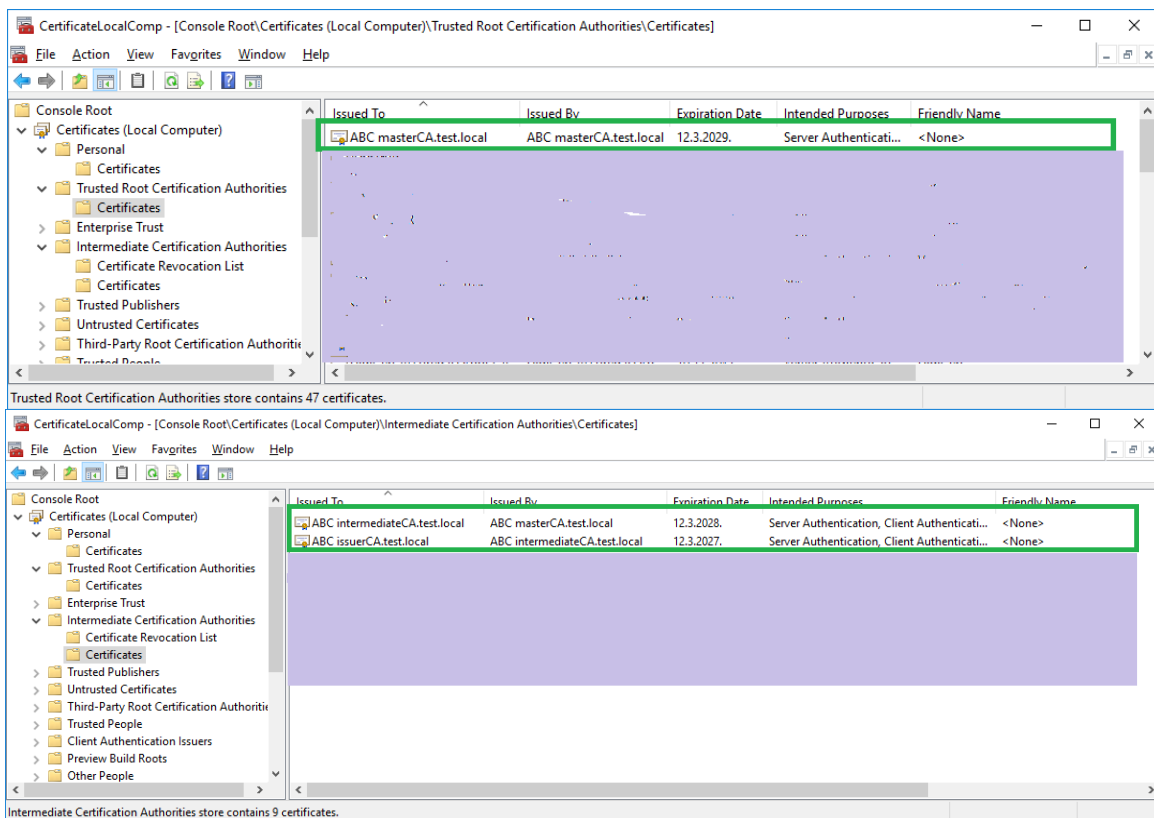
Double click on generated signed certificate request file with .pfx extension will open Certificate Import Wizard. Select Store location -> Local Machine



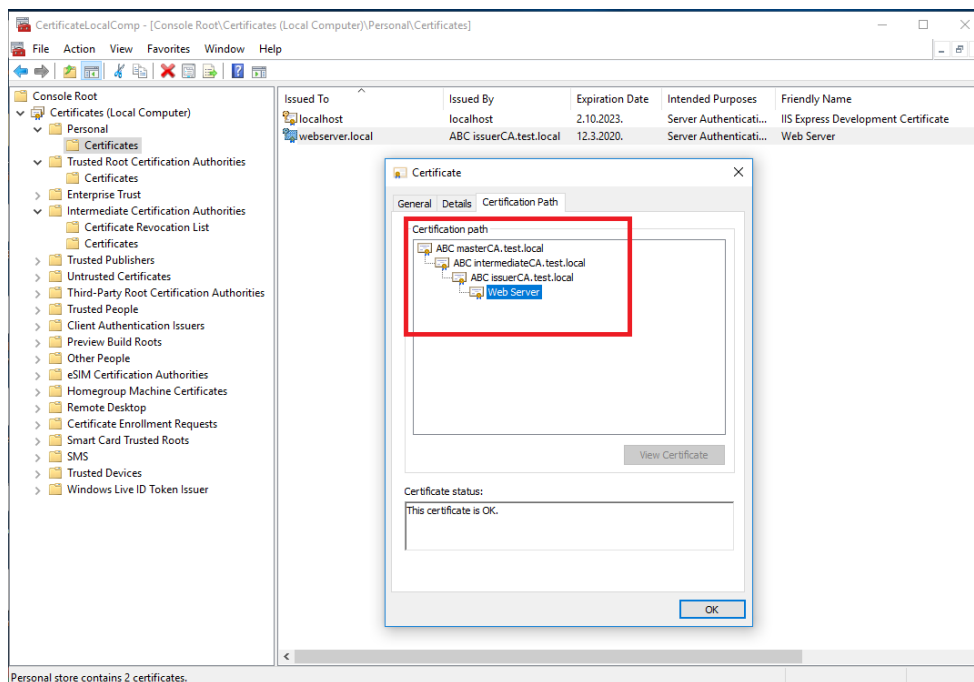


Refresh Personal and Trusted Root Certification Authorities inside mmc console.

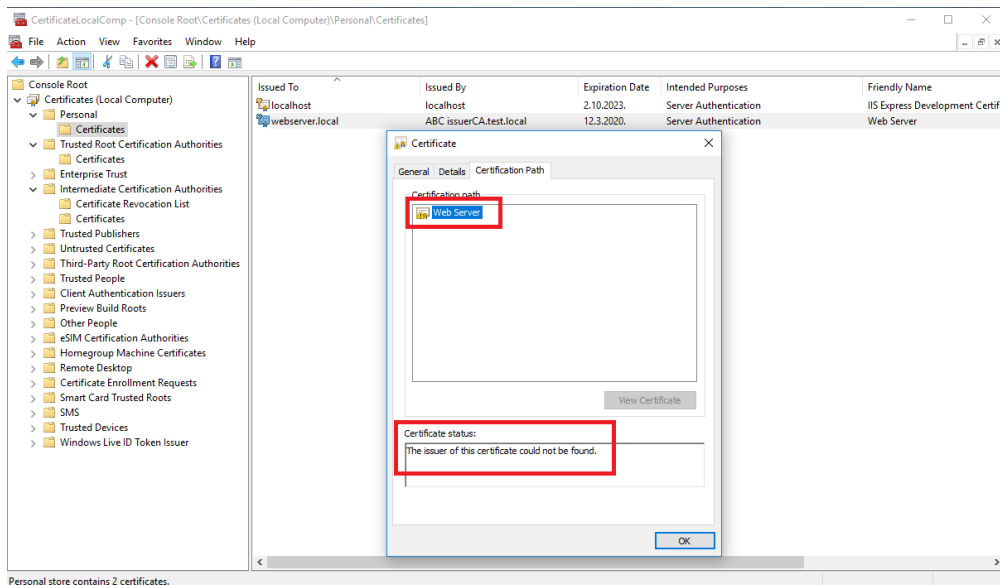




Valid certificate:

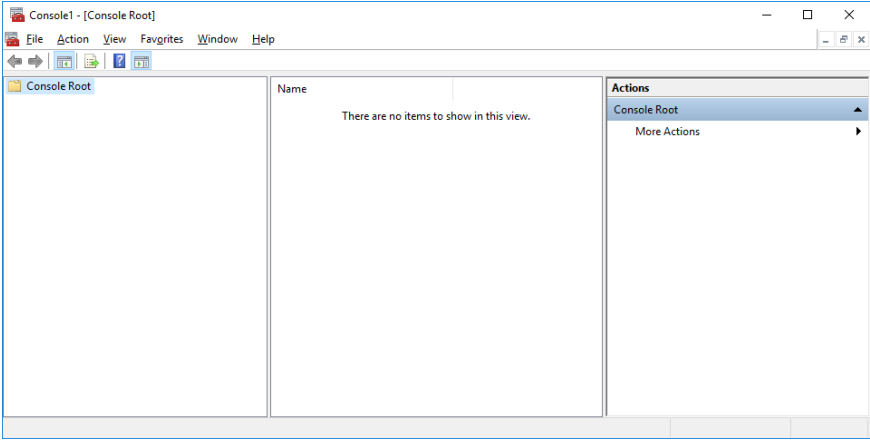


Wrong certificate:

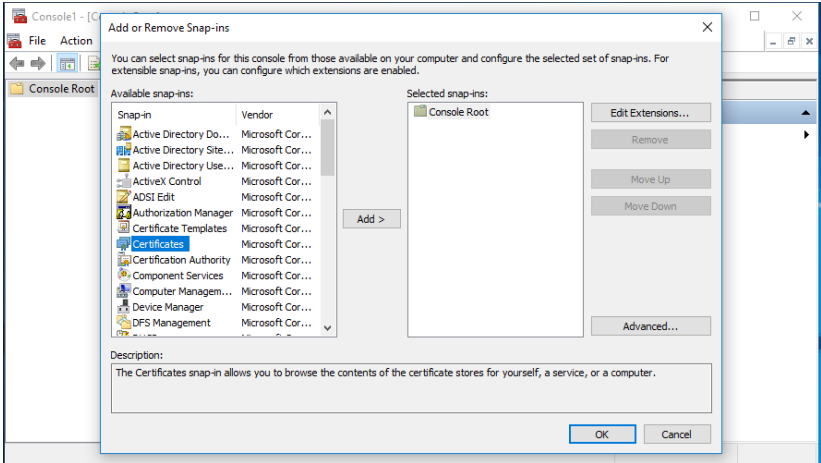


Import certificate from generated pfx file to client computer for web server

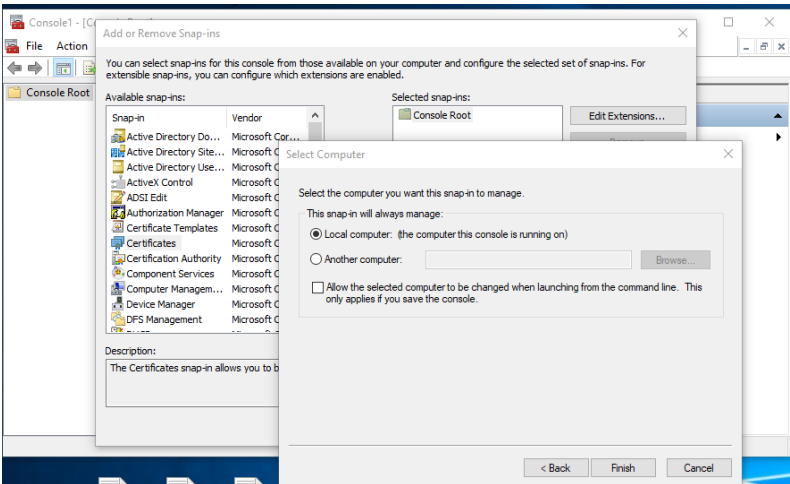
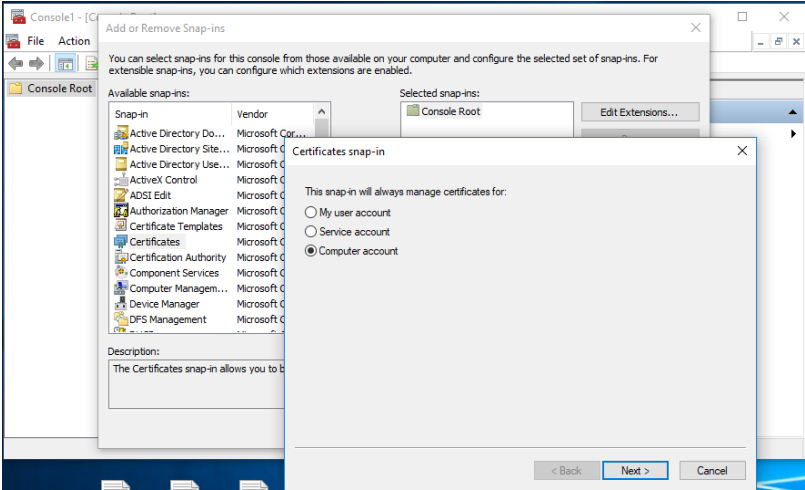
On the client computer, open mmc.exe console.



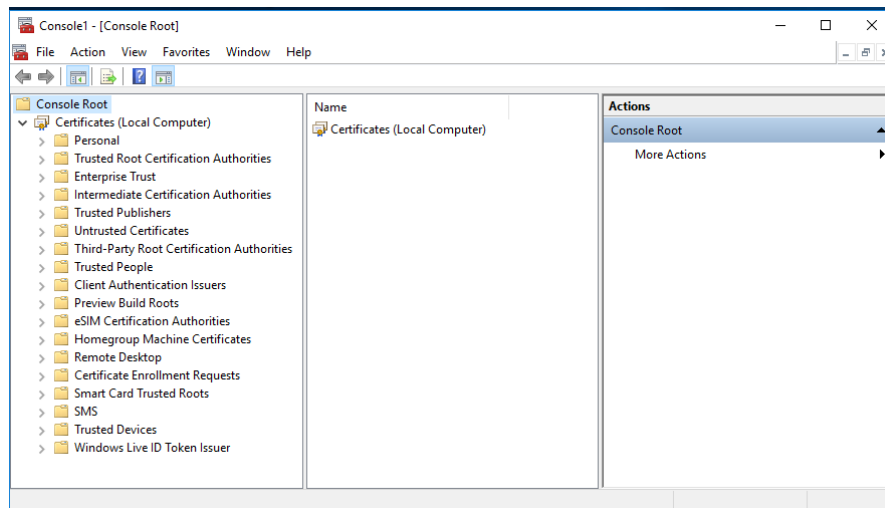
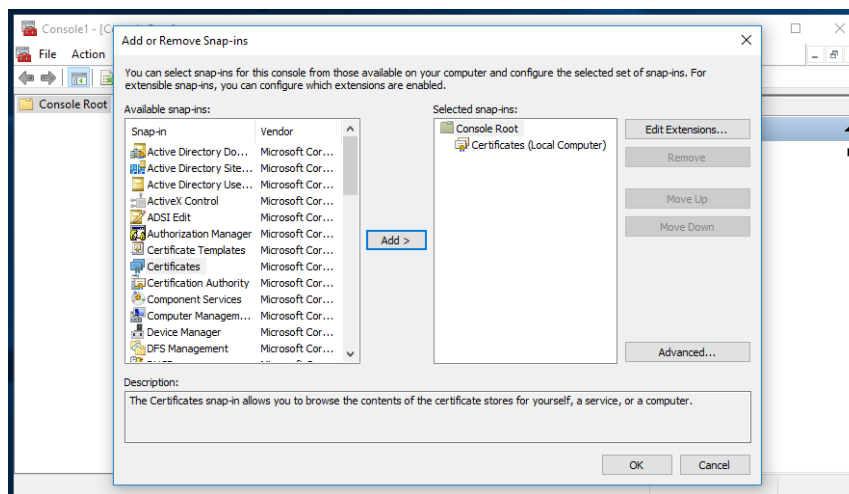
Add Certificate Snap-in



Add, Choose option "Computer account"

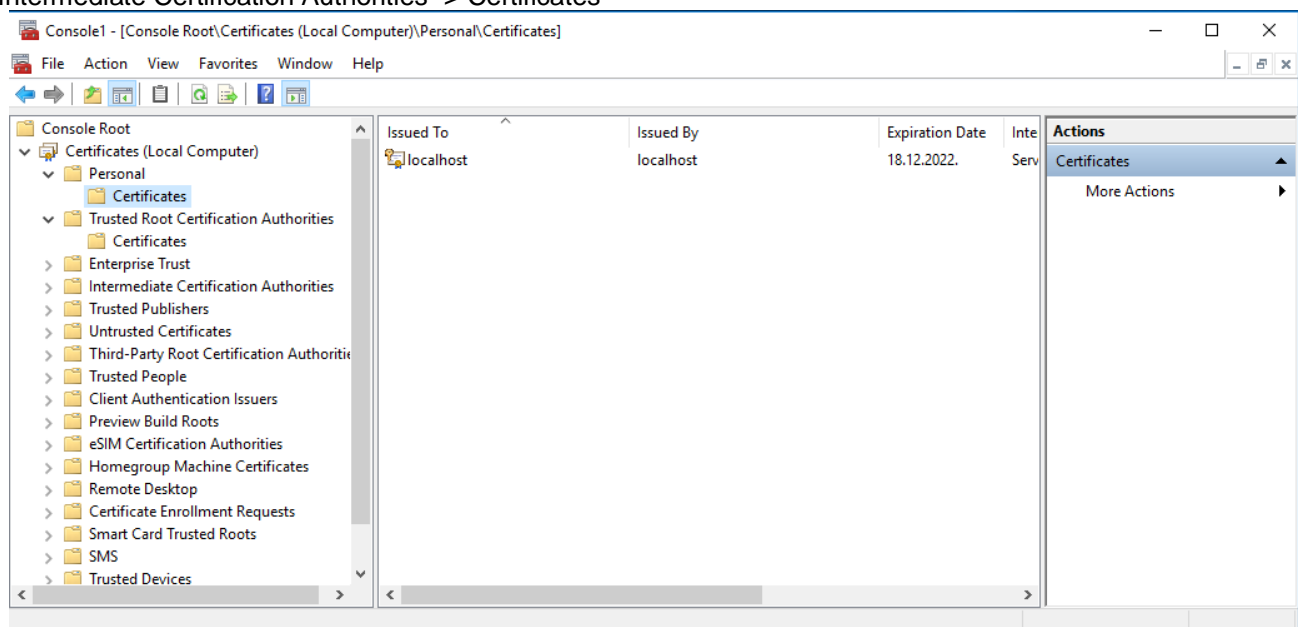






Parts of local computer Certificate store for interest are:

1. Personal -> Certificates
2. Trusted Root Certification Authorities -> Certificates
3. Intermediate Certification Authorities -> Certificates



### NOTE:

Always use CA file that was used when issuing certificate for server.

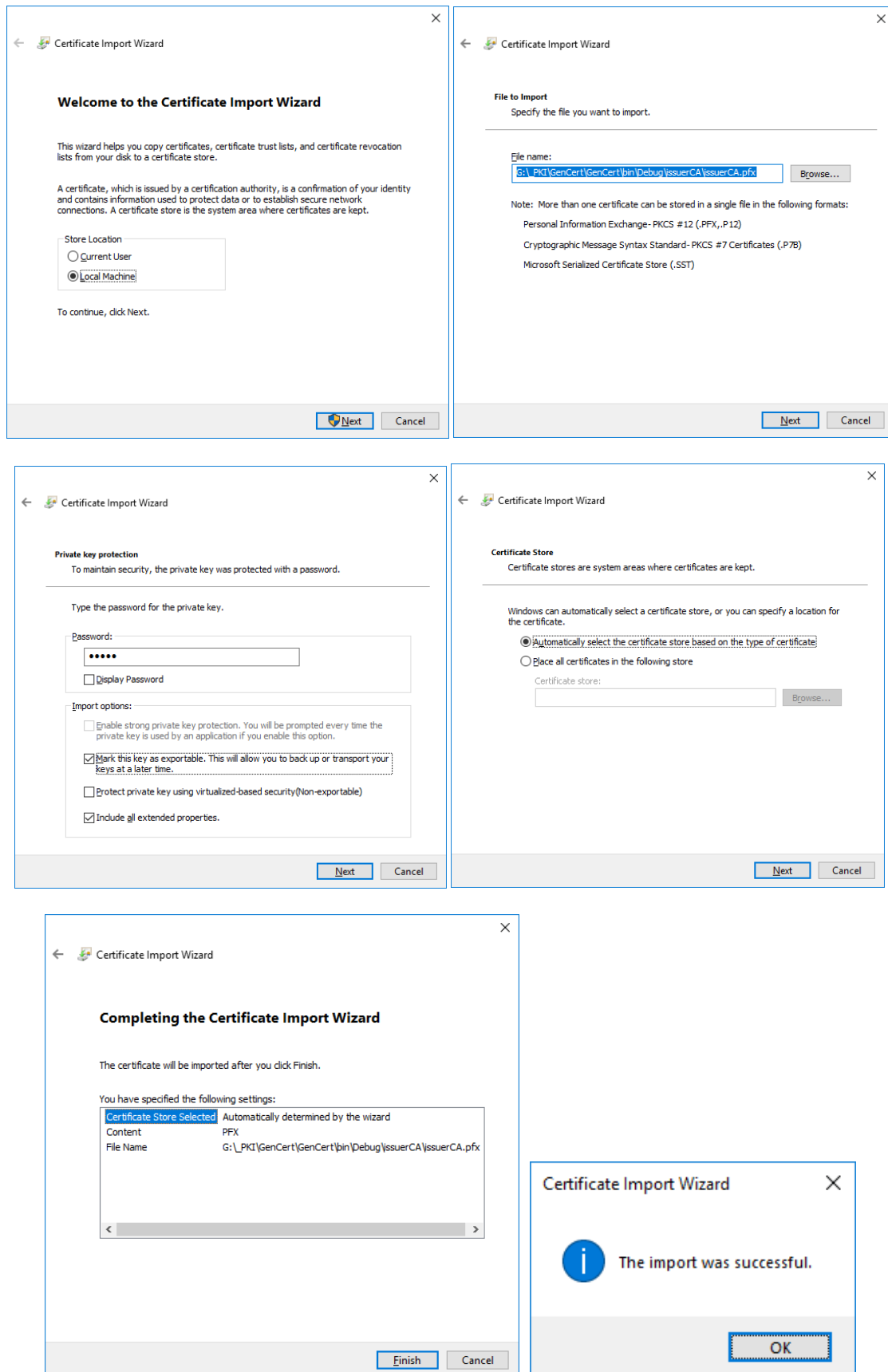
If you use one level CA (only master CA) to issue certificate for server use master CA .pfx file.

If you use two level CA (master CA + intermediate CA) to issue certificate for server use intermediate CA .pfx file.

If you use three level CA (master CA + intermediate CA + issuer CA) to issue certificate for server use issuer CA .pfx file.

## Import three level CA certificate (issuer CA)

Double click on generated CA file with .pfx extension will open Certificate Import Wizard. Select Store location -> Local Machine



**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.

Store Location

☐ Current User

☒ Local Machine

To continue, click Next.

**File to Import**

Specify the file you want to import.

File name:  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)

**Private key protection**

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

Type the password for the private key.

Password:  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.

**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:  Browse...

**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	G:\_PKI\GenCert\GenCert\bin\Debug\issuerCA\issuerCA.pfx

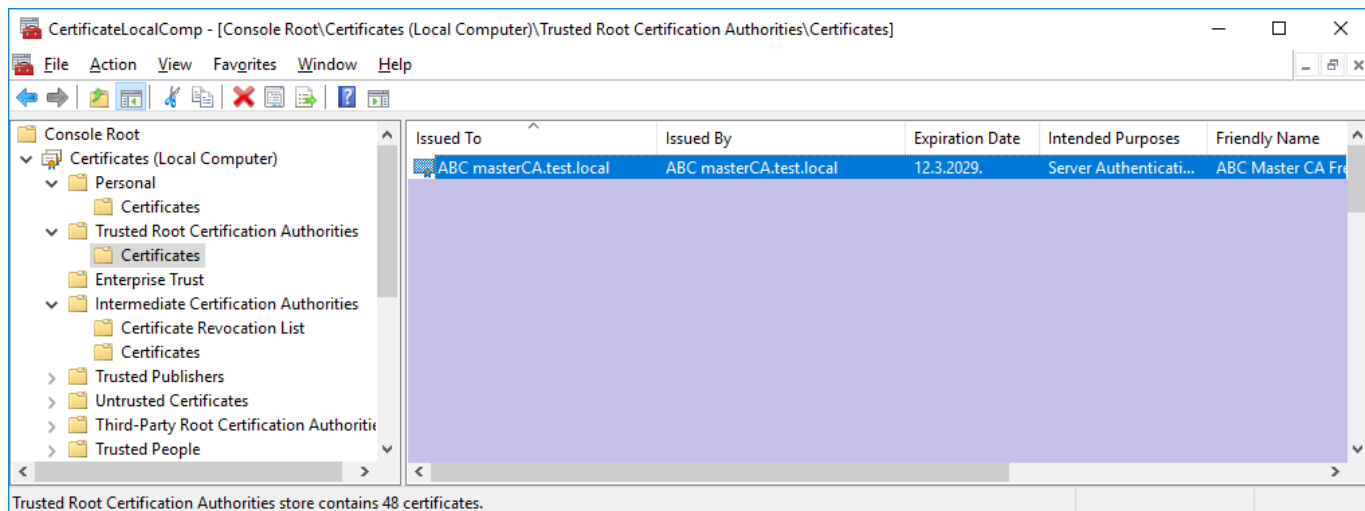
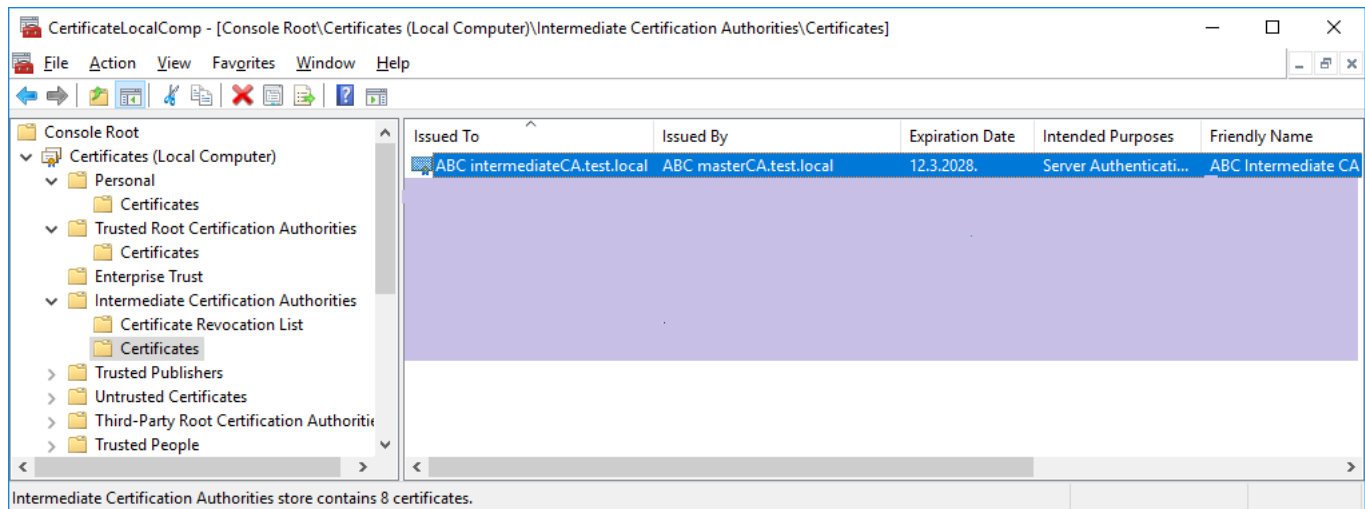
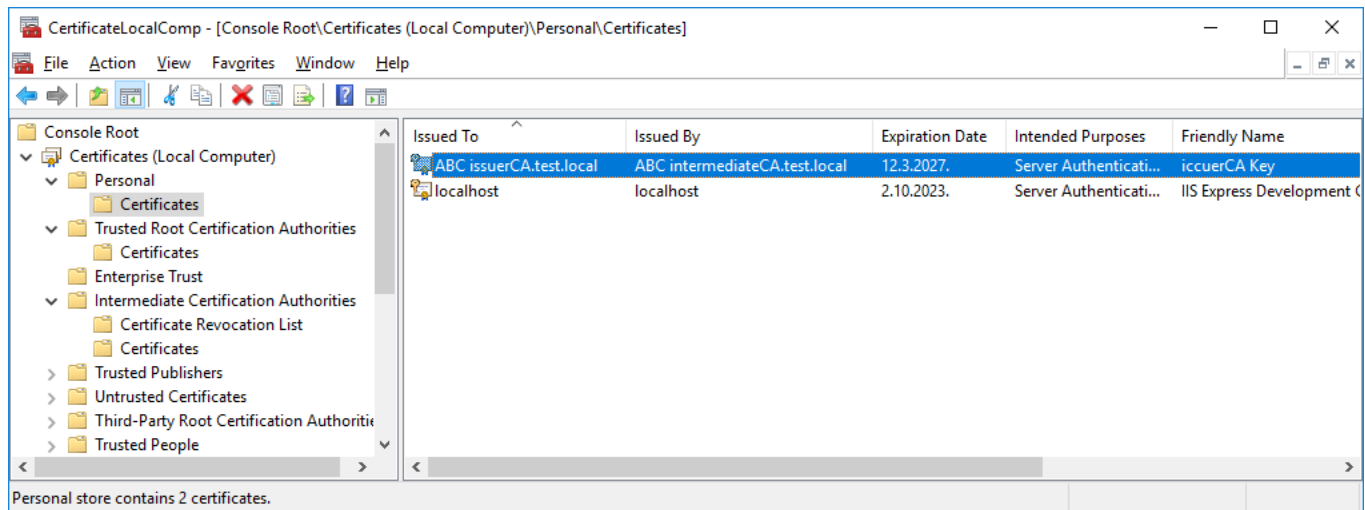
**Certificate Import Wizard**

The import was successful.

OK

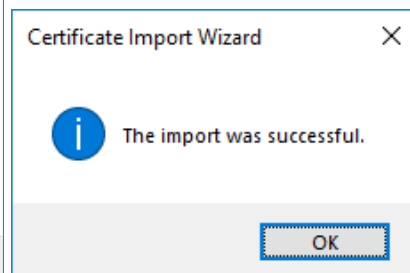
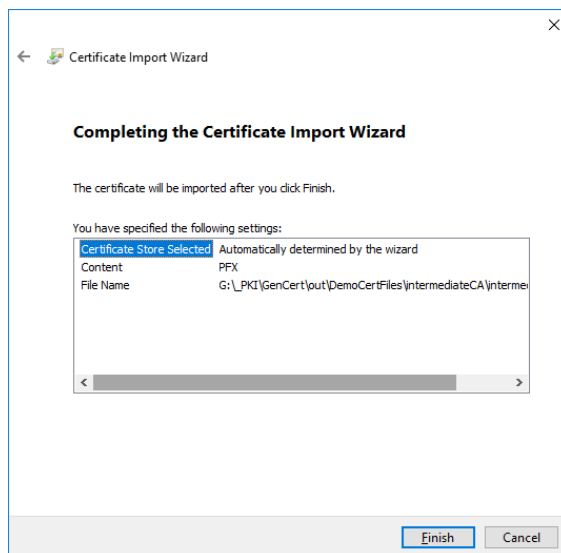
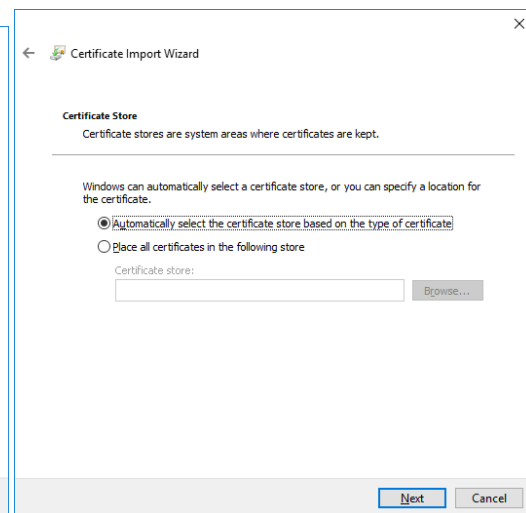
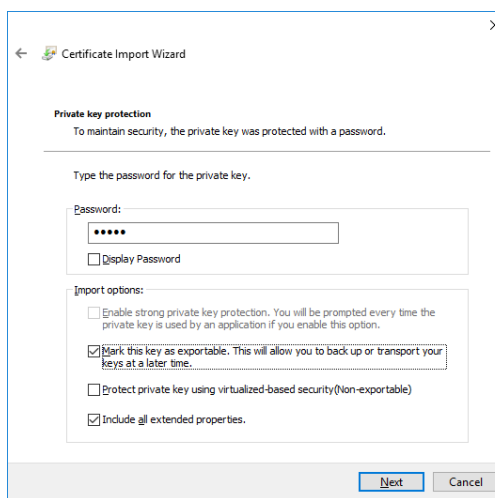
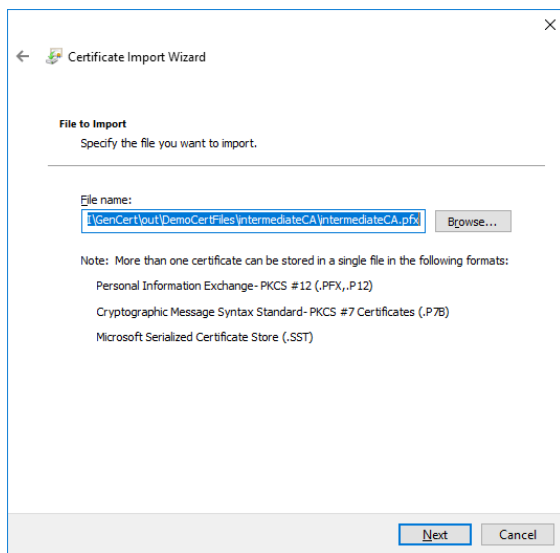
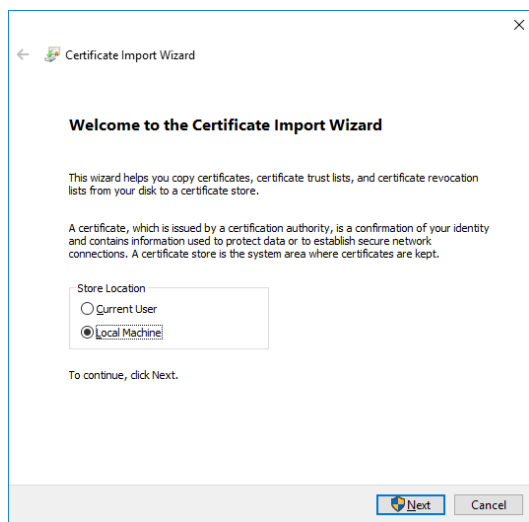
If you import three level certificate (issuer CA) you need to refresh Personal, Trusted Root Certification Authorities and Intermediate Certification Authorities inside mmc console to see new imported certificates.

- issuer CA certificate will be found inside Personal->Certificates store.
- intermediate CA certificate will be found inside Intermediate Certification Authorities ->Certificates store.
- master CA certificate will be found inside Trusted Root Certification Authorities ->Certificates store.

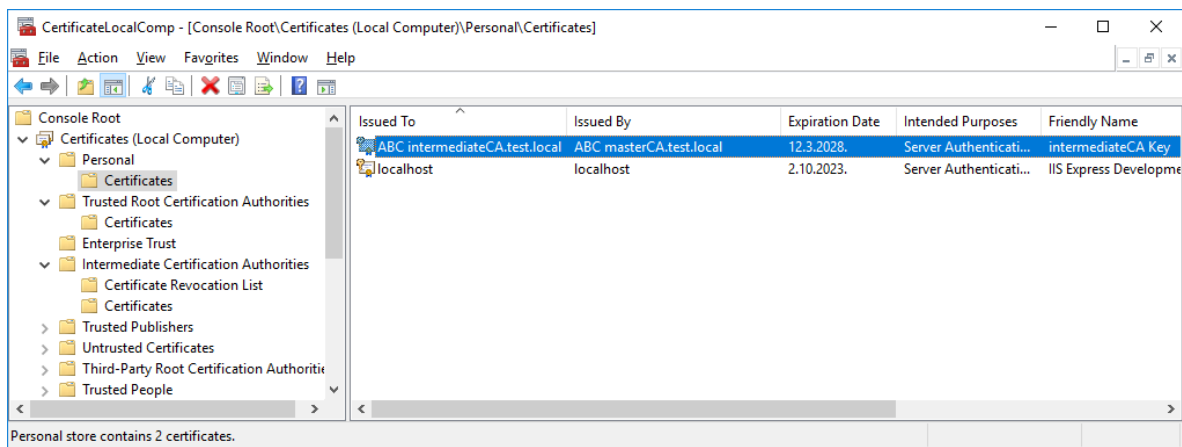


## Import two level CA certificate (intermediate CA)

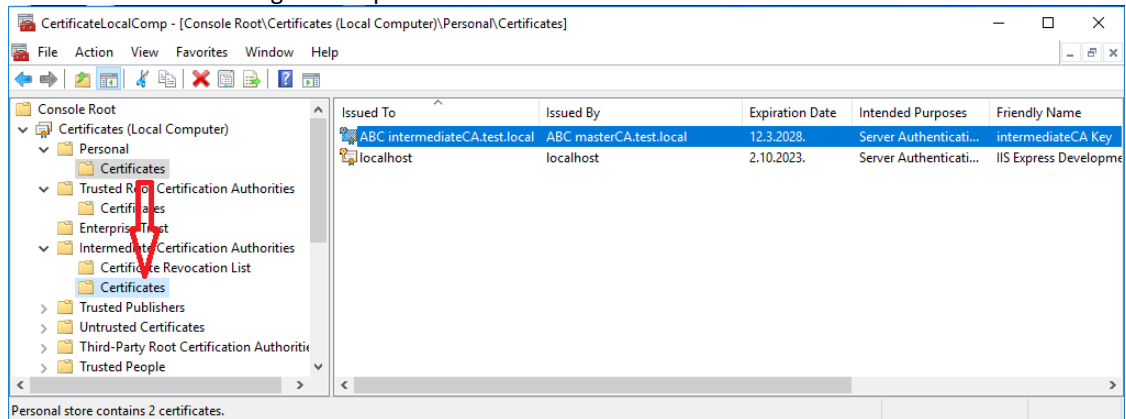
Double click on generated CA file with .pfx extension will open Certificate Import Wizard. Select Store location -> Local Machine



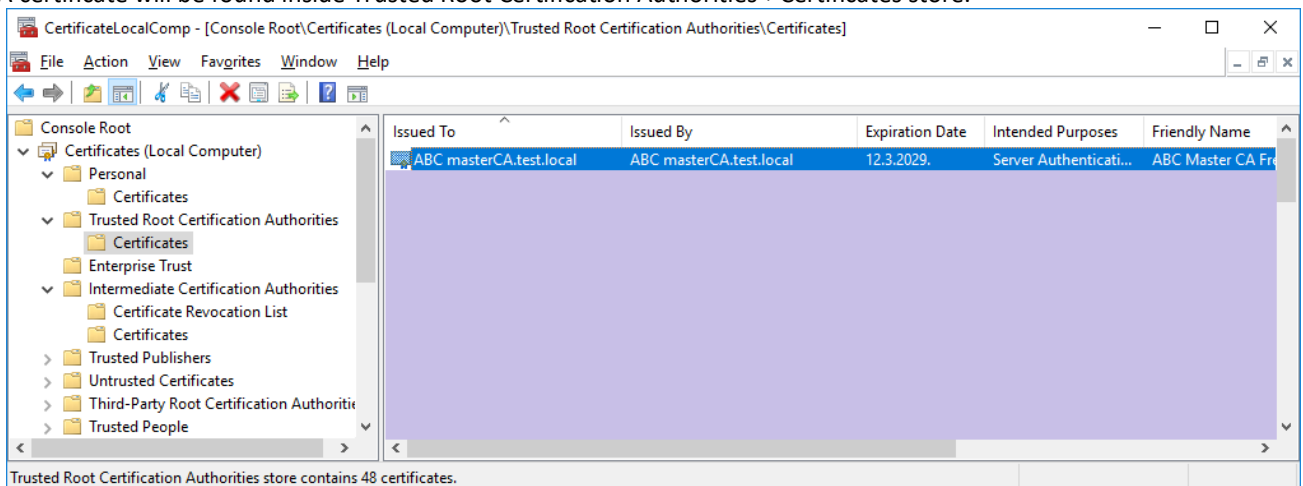
If you import two level certificate (intermediate CA) you need to refresh Personal, Trusted Root Certification Authorities. Intermediate CA certificate will be found inside Personal->Certificates store.



This certificate need to be moved to Intermediate Certification Authorities->Certificates store. Select imported intermediate certificate inside Personal->Certificates store and drag and drop that certificate to Intermediate Certification Authorities ->Certificates store.

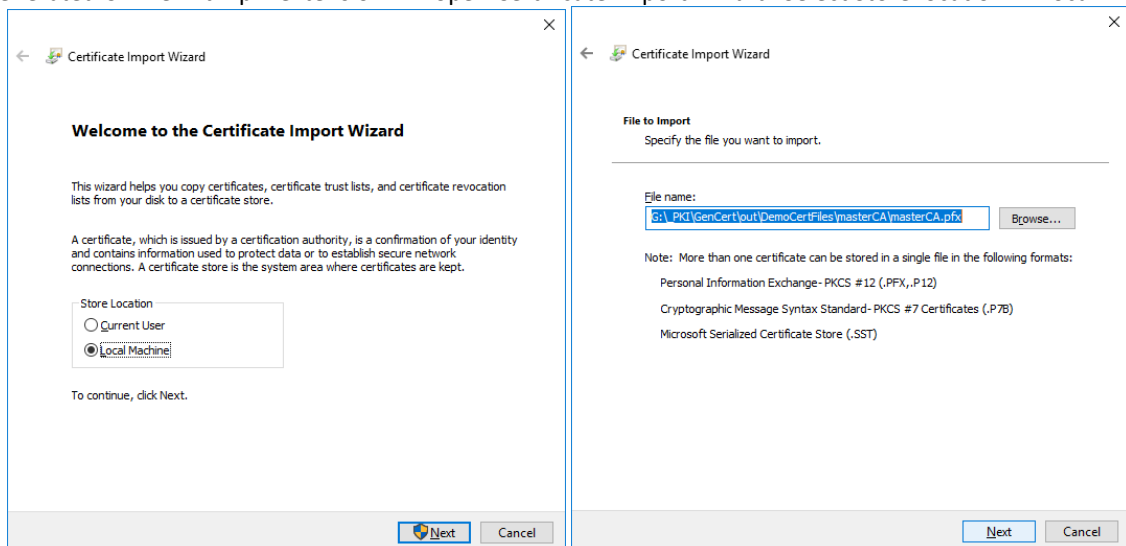


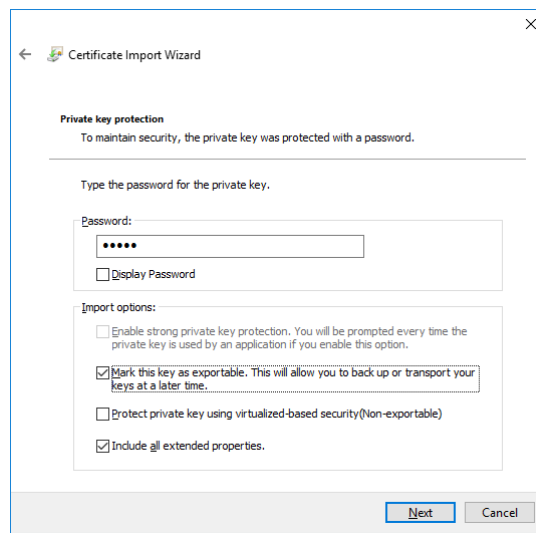
Master CA certificate will be found inside Trusted Root Certification Authorities->Certificates store.



Import one level CA certificate (master CA)

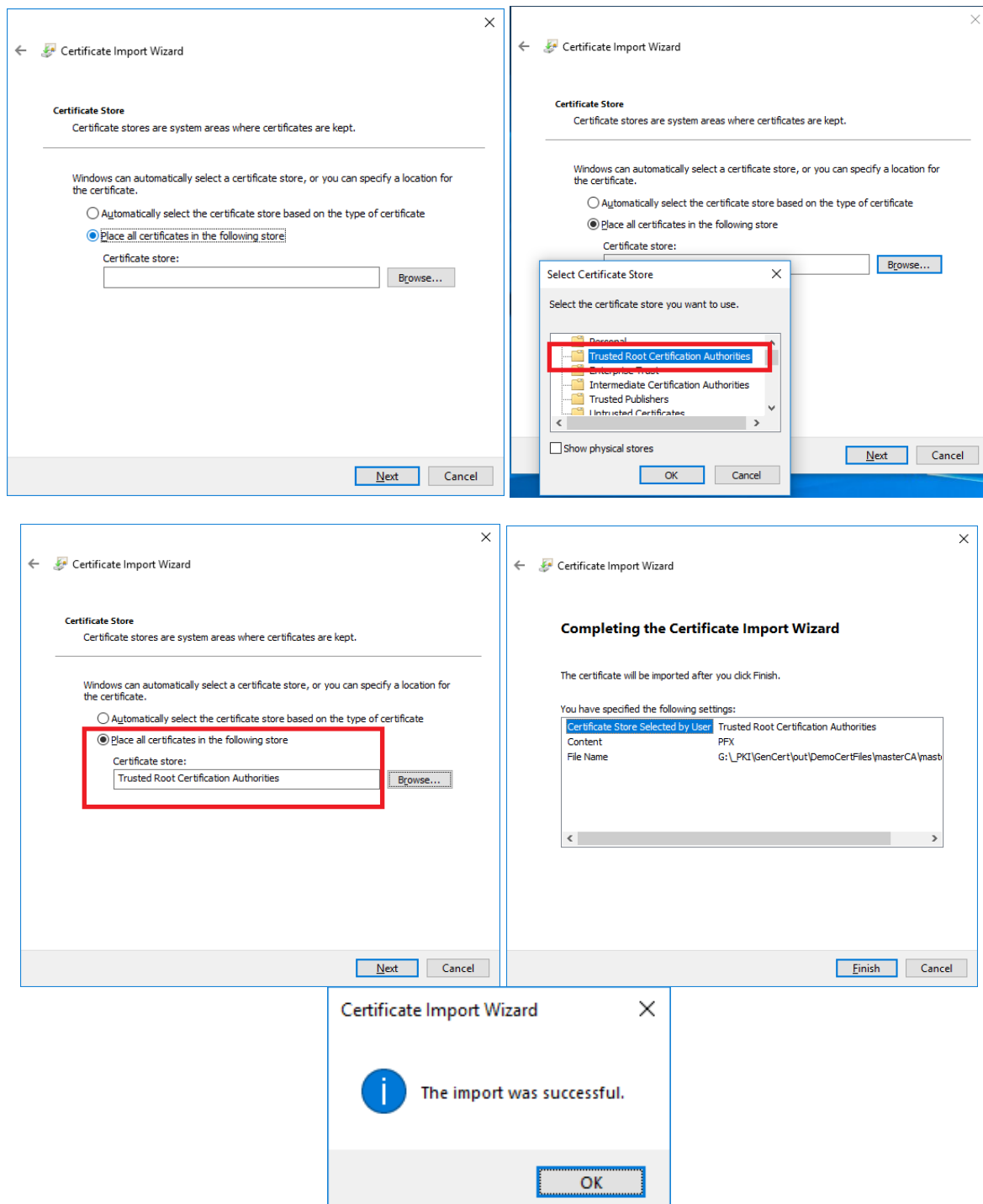
Double click on generated CA file with .pfx extension will open Certificate Import Wizard. Select Store location -> Local Machine





**NOTE:**

In next step be careful, use option “Place all certificates in the following store” and use certificate store “Trusted Root Certification Authorities”



If you import one level certificate (master CA) you need to refresh master CA certificate will be found inside Trusted Root Certification Authorities->Certificates store.

CertificateLocalComp - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

FileActionViewFavgritesWindowHelp

Console Root

Certificates (Local Computer)

Personal

Certificates

Trusted Root Certification Authorities

Certificates

Enterprise Trust

Intermediate Certification Authorities

Certificate Revocation List

Certificates

Trusted Publishers

Untrusted Certificates

Third-Party Root Certification Authorities

Trusted People

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
ABC masterCA.test.local	ABC masterCA.test.local	12.3.2029.	Server Authenticati...	ABC Master CA Fr

Trusted Root Certification Authorities store contains 48 certificates.