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](#_Toc3544358)

[Create Request (step) 2](#_Toc3544359)

[Create Signed Certificate (step) 5](#_Toc3544360)

[Generate pfx file (when you got signed certificate file from external CA root authority e.g. GoDaddy) 5](#_Toc3544361)

[Generate certificate file for web server (use internal CA(s) for sign request) 6](#_Toc3544362)

[Create Request (step) 7](#_Toc3544363)

[CA Certificate (step) 10](#_Toc3544364)

[Variant I –„Sign locally-Don’t have CA cert “ 10](#_Toc3544365)

[Variant II –„Sign locally-Have CA cert“ 13](#_Toc3544366)

[Issue Certificate (step) 16](#_Toc3544367)

[Create Signed Certificate (step) 18](#_Toc3544368)

[Import certificate from generated pfx file to web server 19](#_Toc3544369)

[Import certificate from generated pfx file to client computer for web server 24](#_Toc3544370)

[Import three level CA certificate (issuer CA) 26](#_Toc3544371)

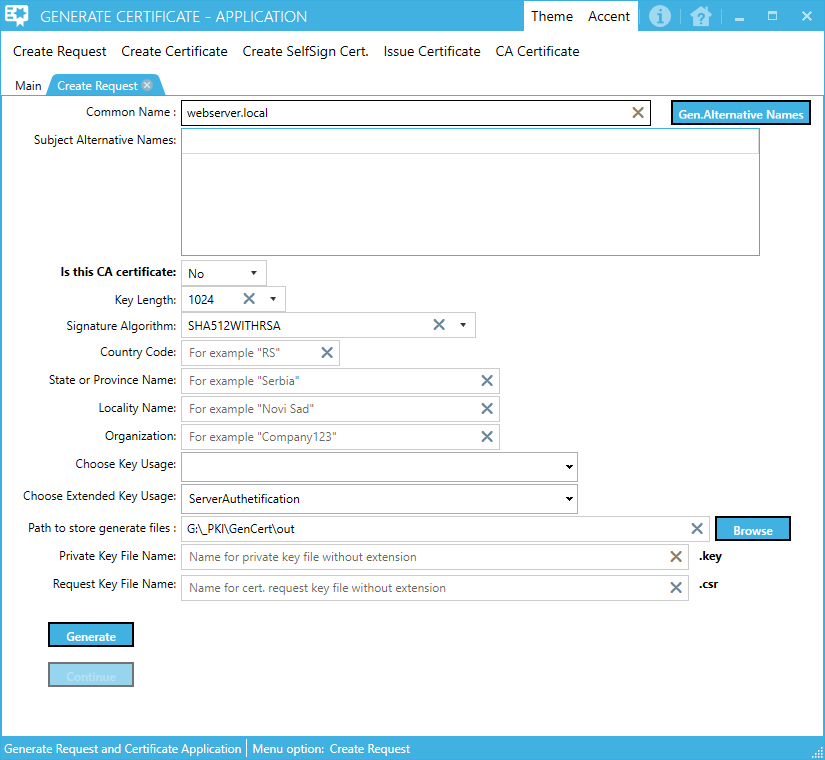
[Import two level CA certificate (intermediate CA) 27](#_Toc3544372)

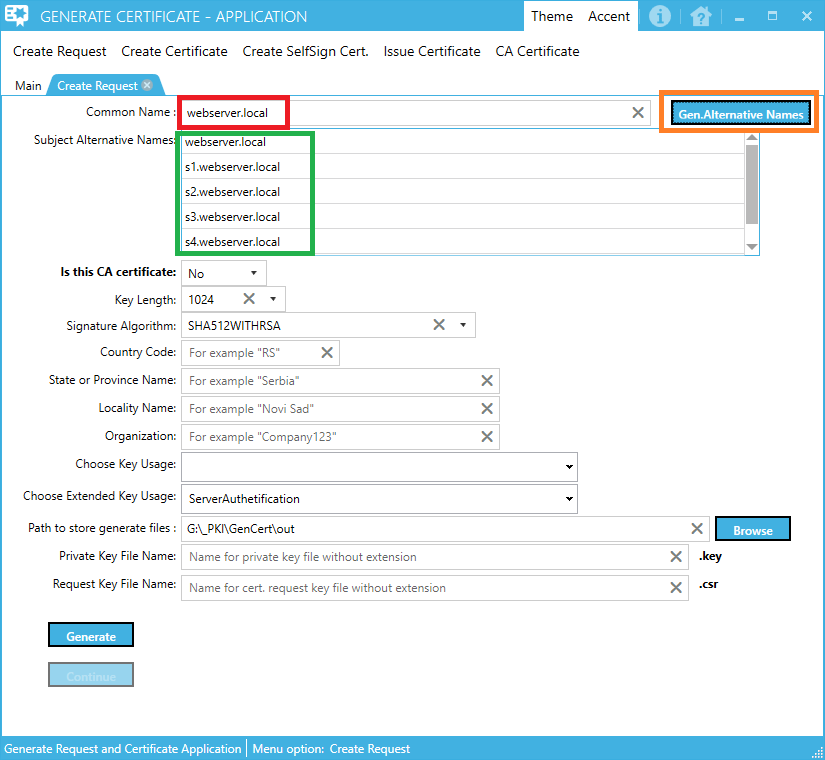
[Import one level CA certificate (master CA) 29](#_Toc3544373)

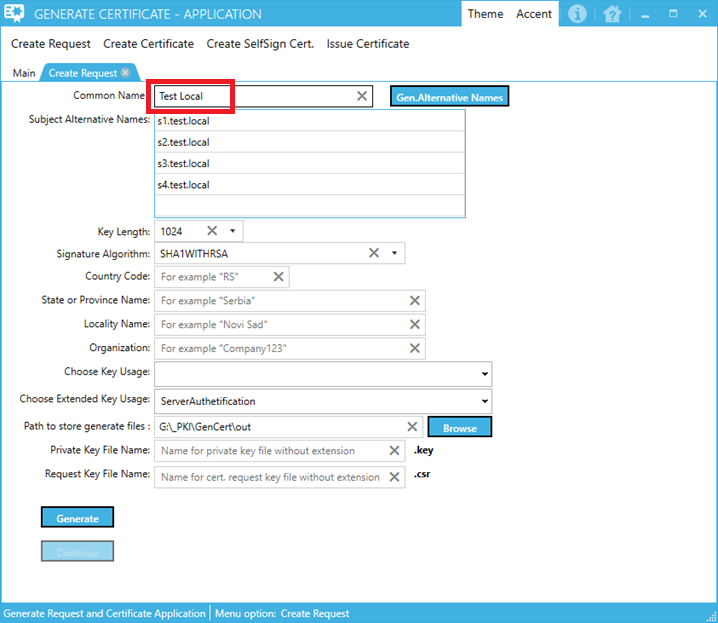
# Generate certificate file for web server (use external root CA for sign request):

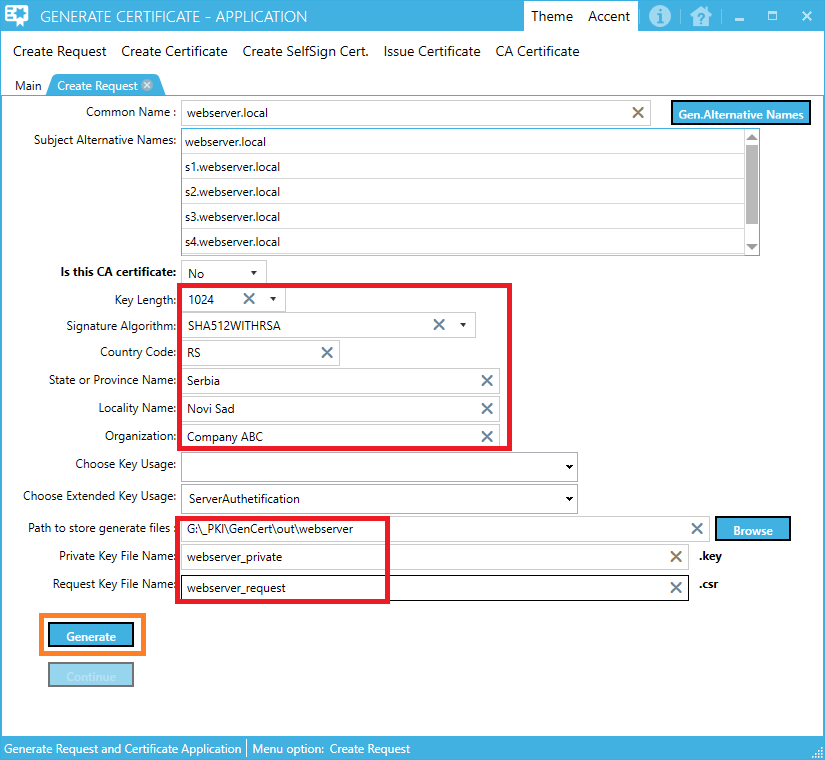
|  |  |  |
| --- | --- | --- |
| **Done** | **Menu option (step)** | **Comment** |
|  | Create Request | Fill all data on the form. When you click on the "Generate" button, the application will generate two files in the folder whose path is listed in the "Path to store generate files:" field.  The first 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.  **NOTE:**  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.  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).  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. |
|  | Create Signed Certificate | 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.  It is necessary to select a folder in which the signed certificate file with a private key will be generated (file with .pfx extension).  **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. |

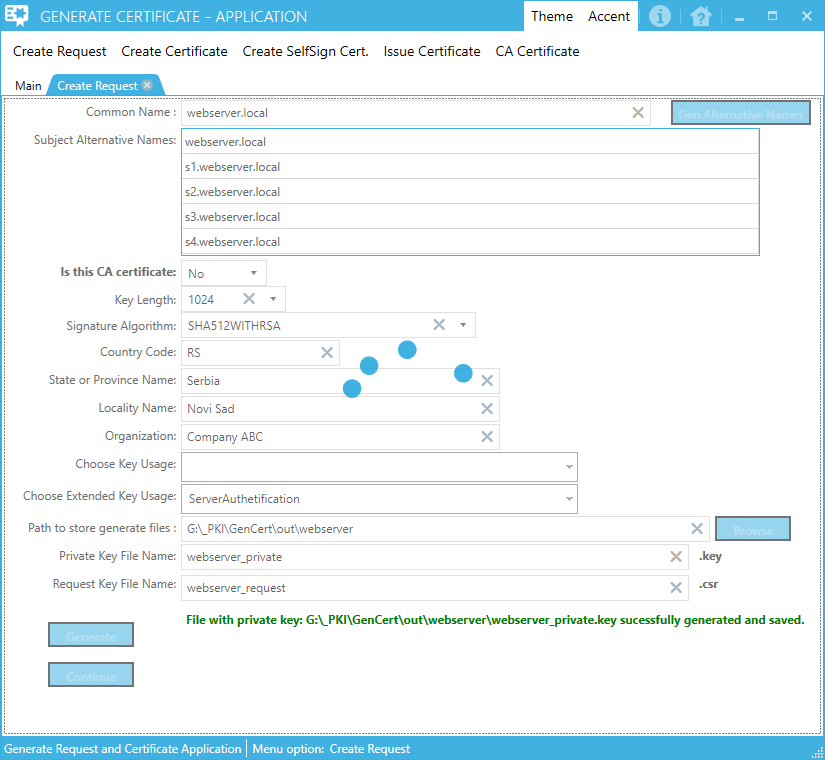
## Create Request (step)

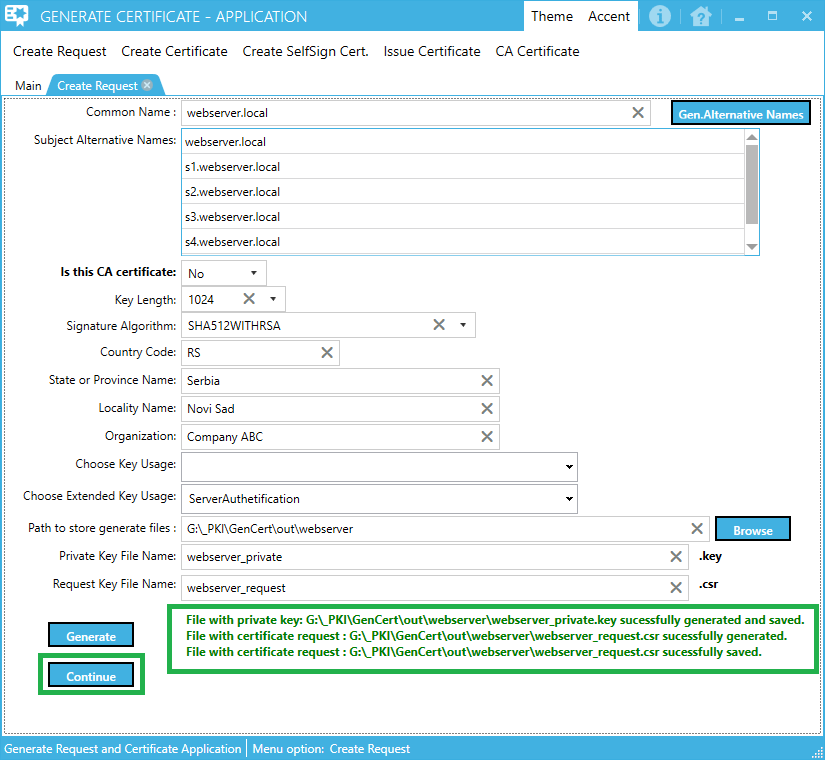












Tip:

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).

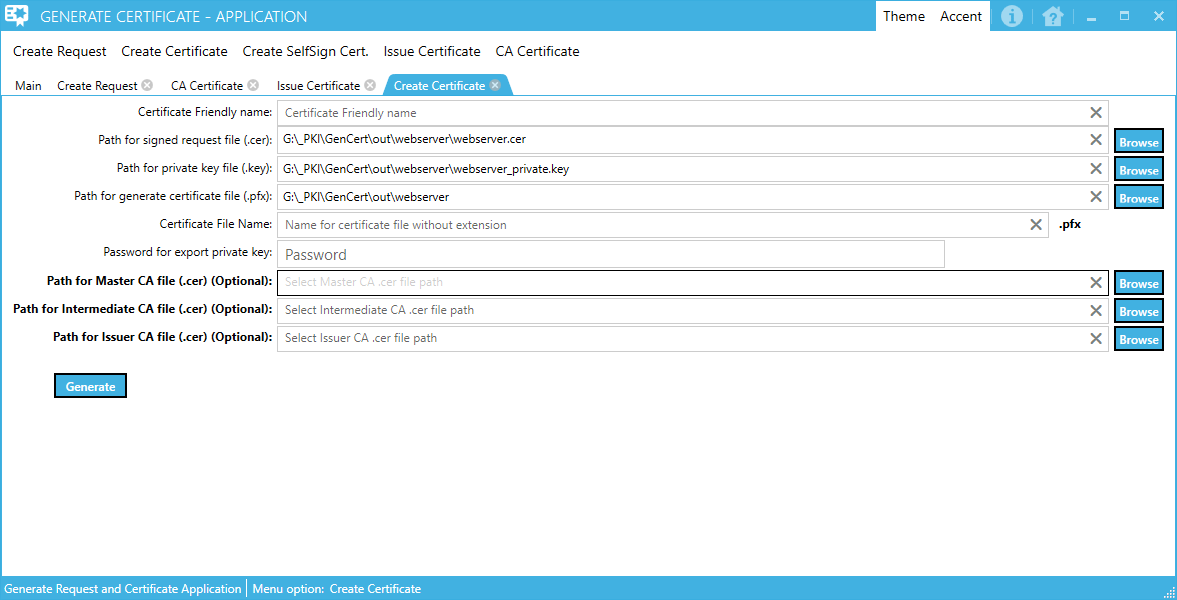
On the form, you receive (use described in the Issue Certificate section), issue the certificate issuance based on the request of the generated file (.csr) and when you generate a signed public certificate file (.cer), open it and check that all the attributes look right within that certificate.

|  |  |
| --- | --- |
|  | 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)

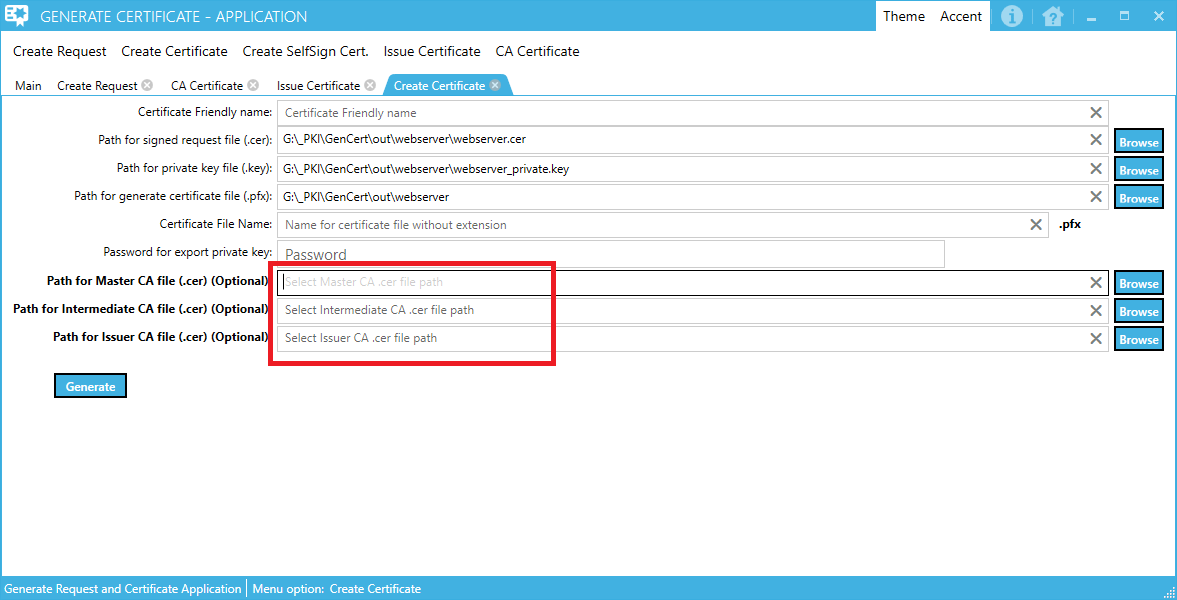
### Generate pfx file (when you got signed certificate file from external CA root authority e.g. GoDaddy)

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

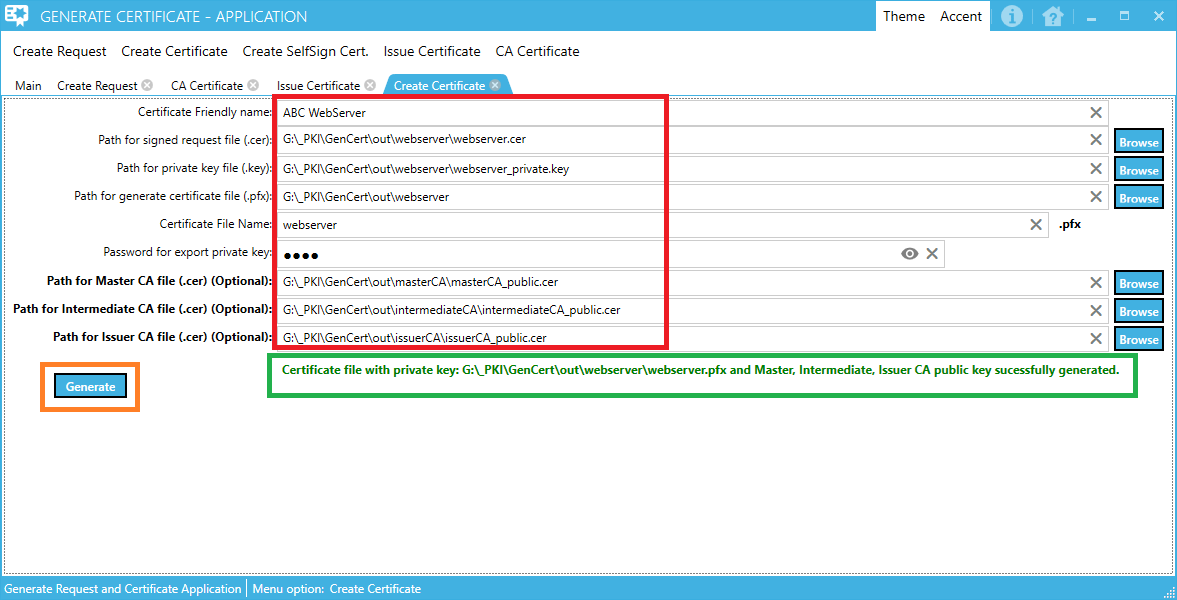


You need inside fields:

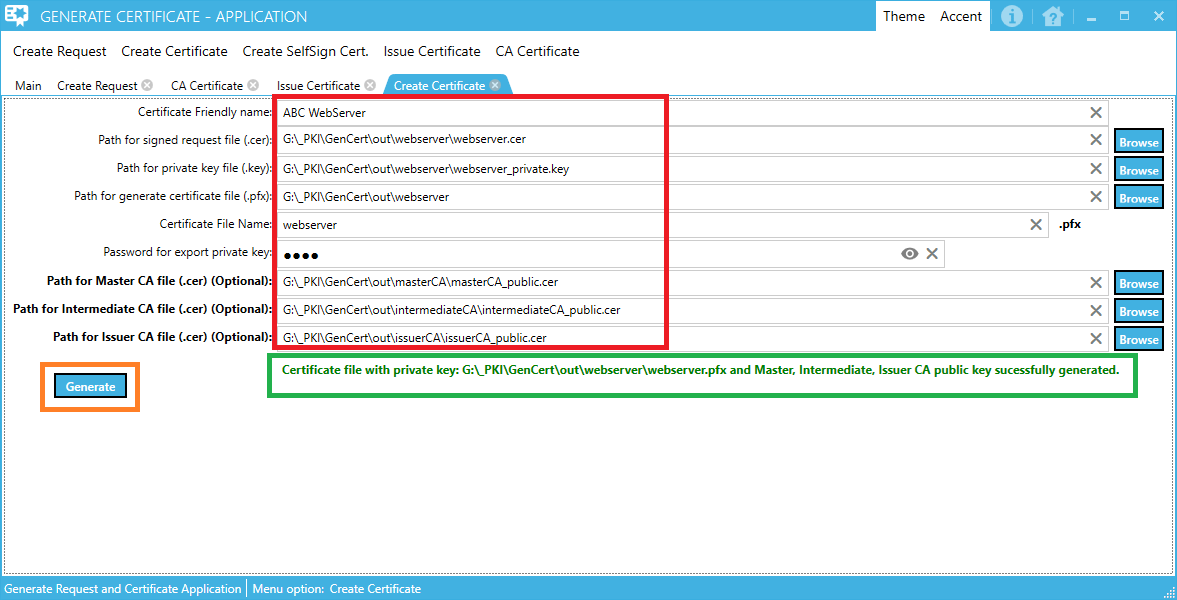
“Path for Master CA file”, “Path for Intermediate CA file”, “Path for Issuer CA file” to enter file path for appropriate CA certificate.



Enter file path and click Generate button.



#### 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)

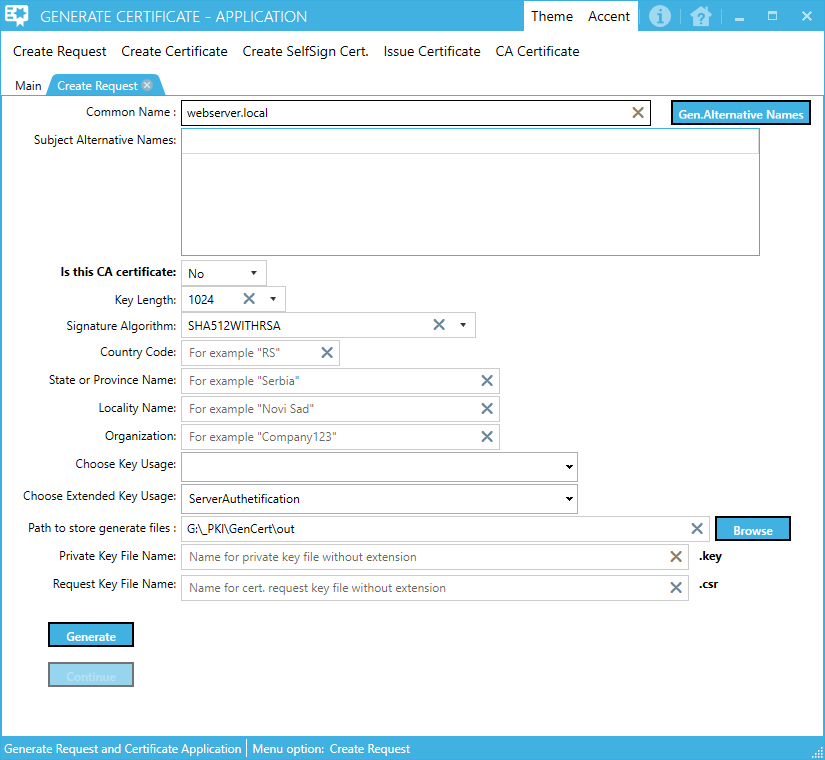


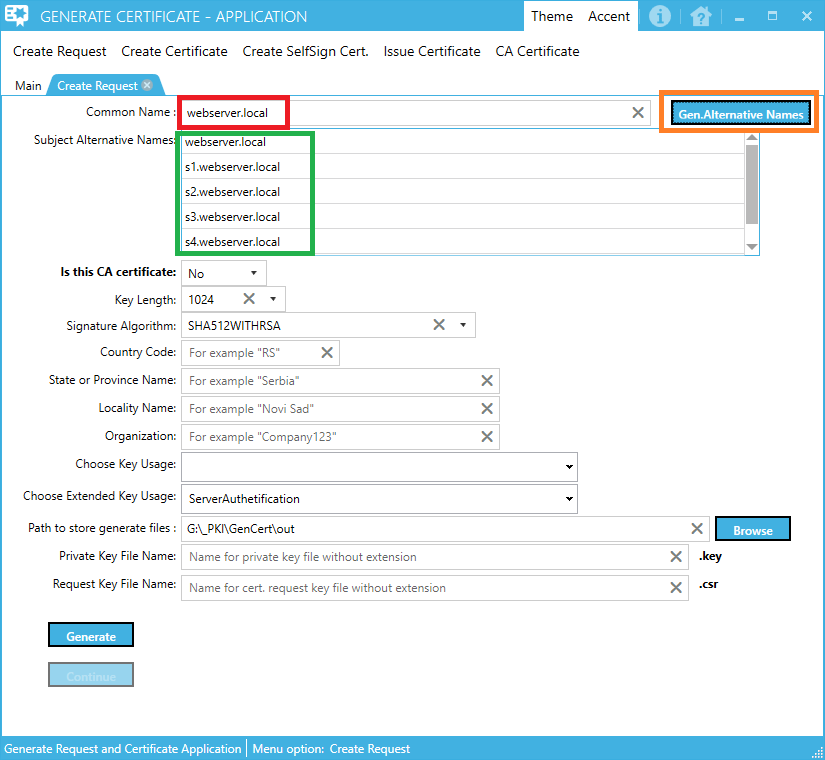
Go to „[Import certificate from generated pfx file](#_Import_certifikata_iz)“

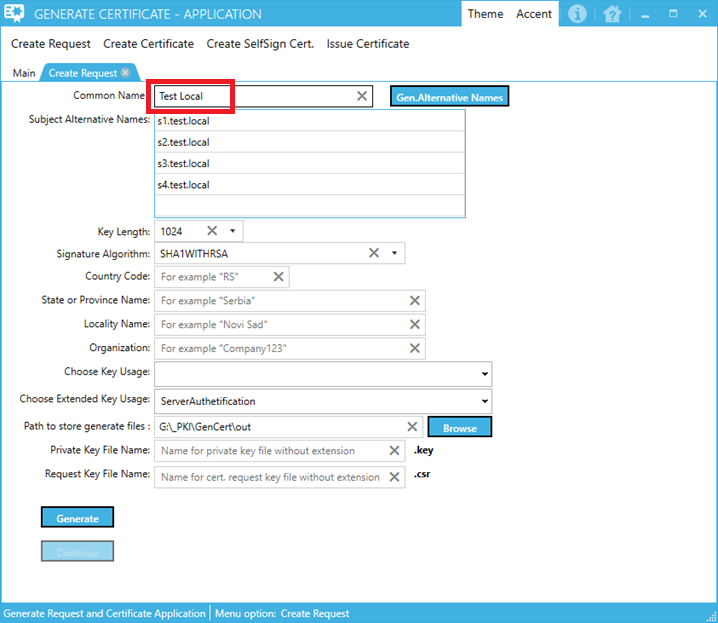
# Generate certificate file for web server (use internal CA(s) for sign request)

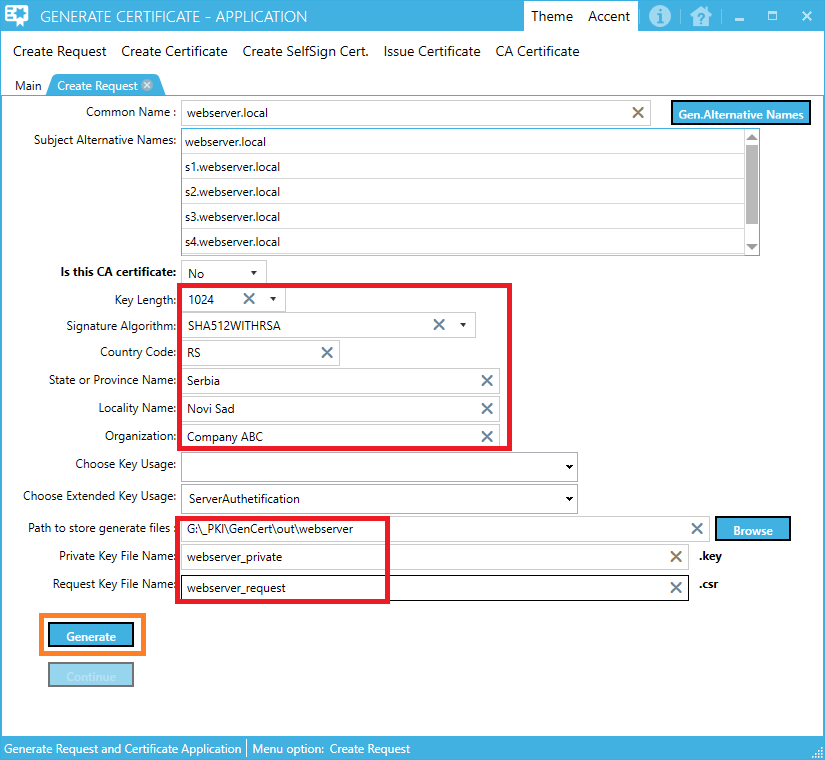
|  |  |  |
| --- | --- | --- |
| **Done** | **Menu option (step)** | **Comment** |
|  | Create Request | Fill in all the information in the form. When you click on the "Generate" button, the application will be in a folder whose path is listed in the "Path to store generate files:" field, generate two files.  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 -> option: "Create SelfSign Cert.")  **NOTE:**  If there are already files in the selected location with the same name, you need to delete these files and start generating again.  On the form, click the "Continue" button switches to the next "step" |
|  | CA Certificate | Fill in all the information in the form, or click on the "Test Data" button to fill all form fields with test data.  When the "Generate" button is clicked, the application will generate 3 folders and generate 2 files in each folder.  -The first file with the .csr extension is a public key certificate for the (master / intermediate / issuer) CA server.  -The other file with the extension .pfx is a certificate that contains a private + public key for the (master / intermediate / issuer) CA server.  NOTICE for Test Data:  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.  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.  NOTE for Continue:  On the form, there are 3 x Continue buttons on each part of the form (master / intermediate / issuer).  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.  **NOTE:**  If there are already files in the selected location with the same name, you need to delete these files and start generating again.  On this form, click the "Continue" button switches to the next "step" |
|  | Issue Certificate | 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 ".  **NOTE:**  If there are already files in the selected location with the same name, you need to delete these files and start generating again.  From this form, clicking the "Continue" button switches to the next "step" |
|  | Create Signed Certificate | 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).  **NOTE:**  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. |

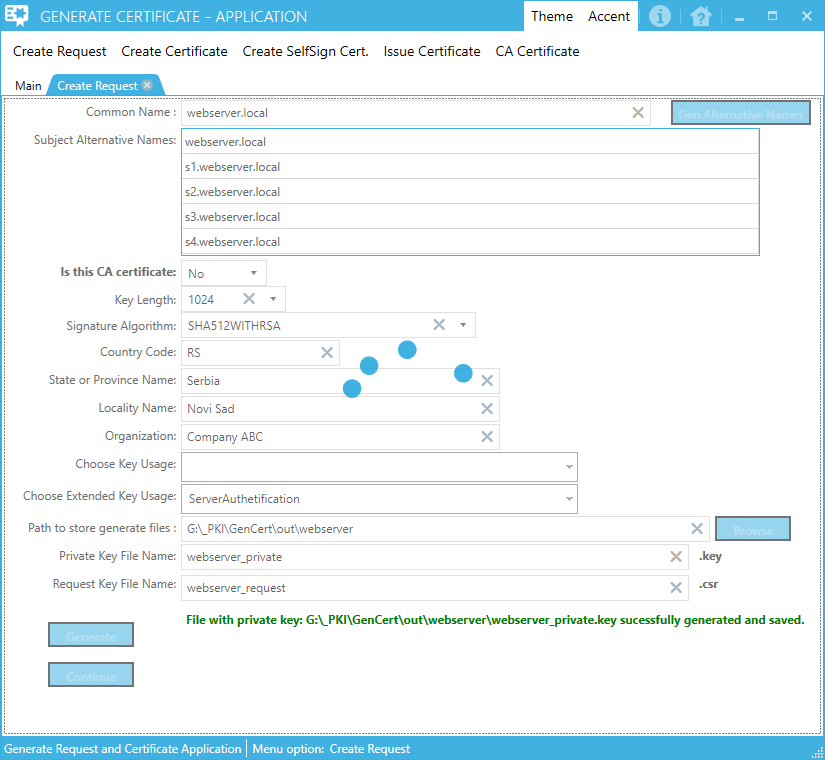
## Create Request (step)

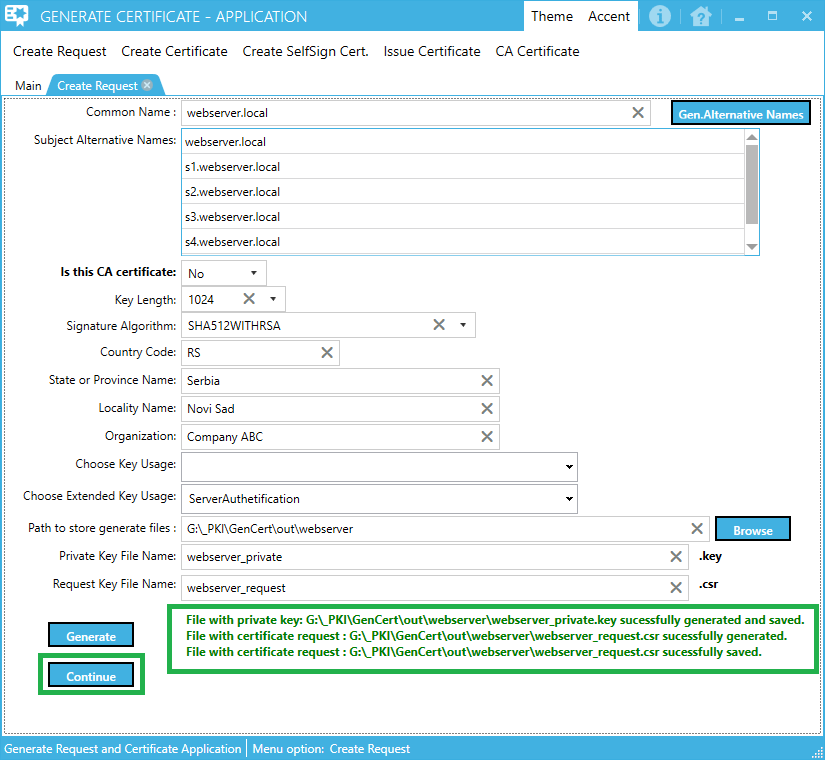








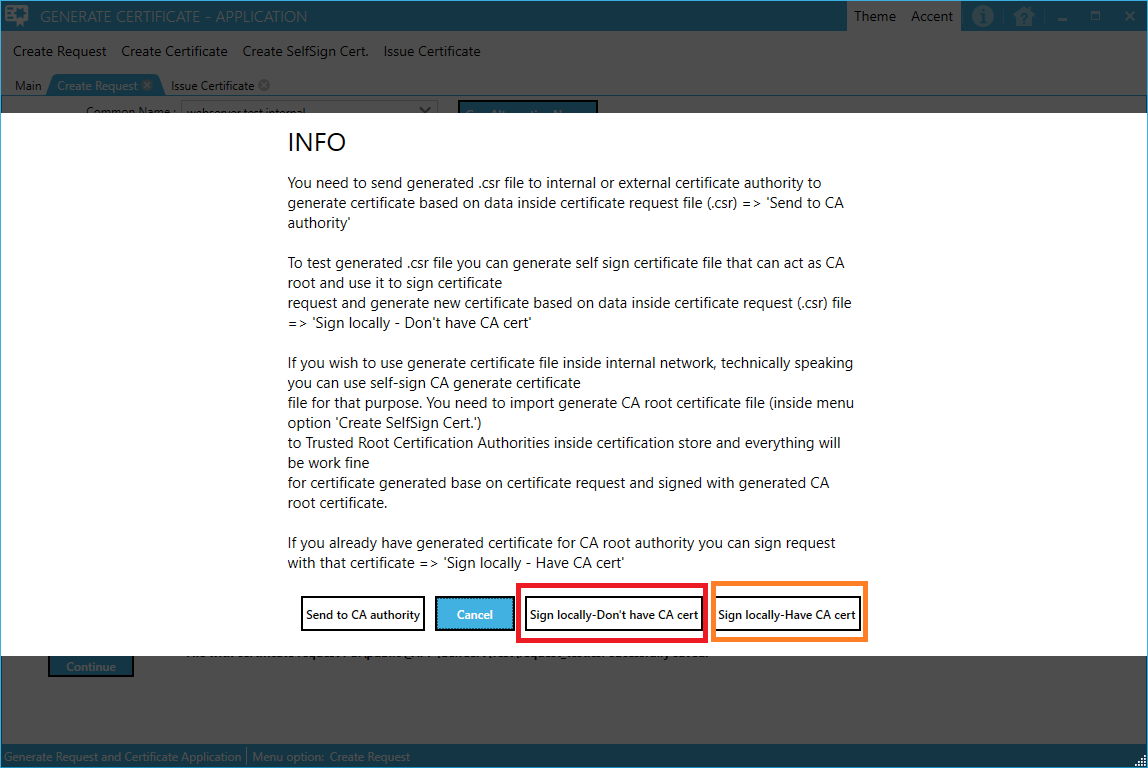




Tip:

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

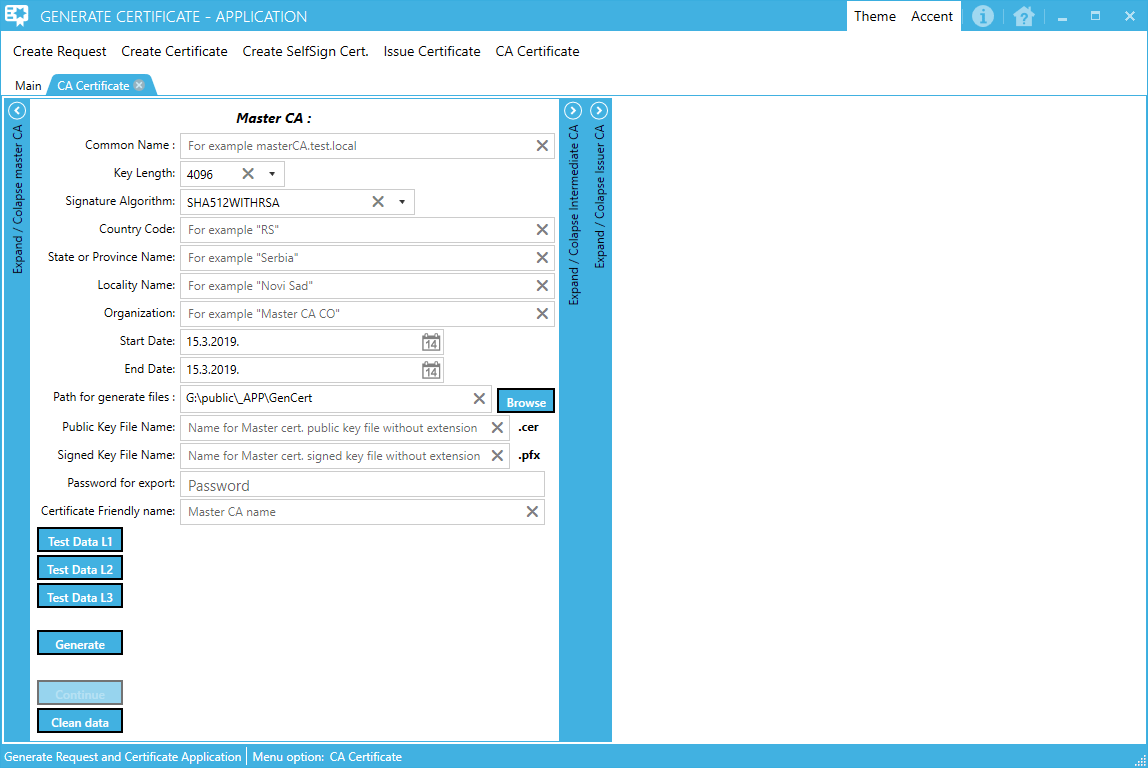
Click Continue button



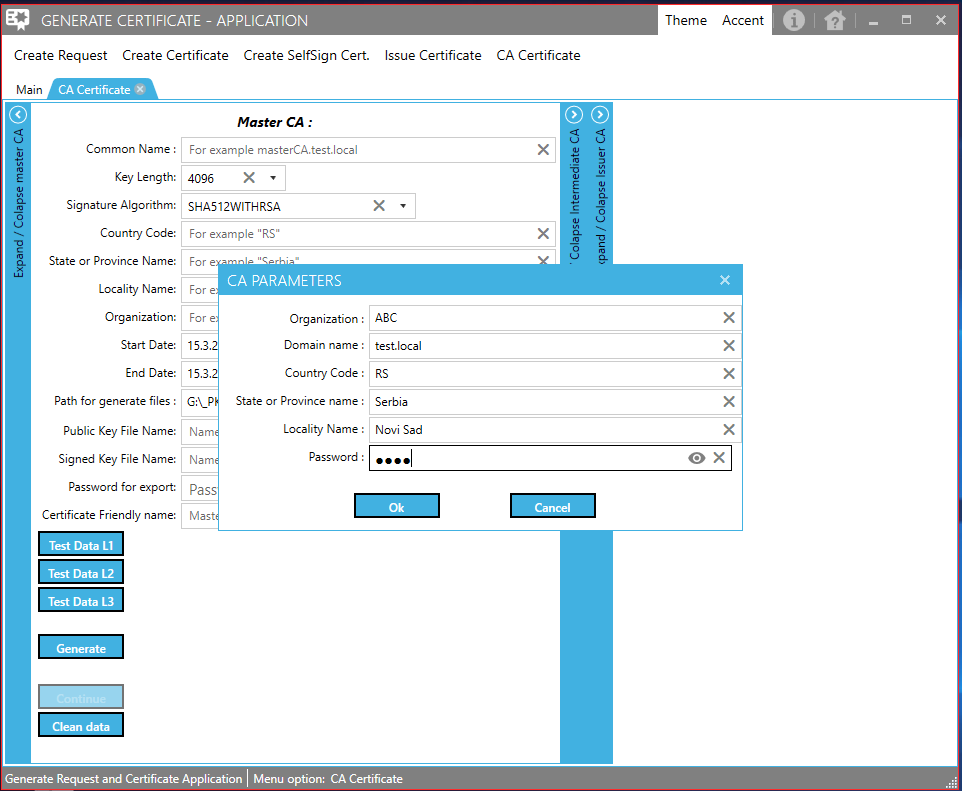
Depending on whether you already have a generic root certificate that you will use to sign (orange) or there is no root certificate that you will use for signing (red), click on the appropriate button.

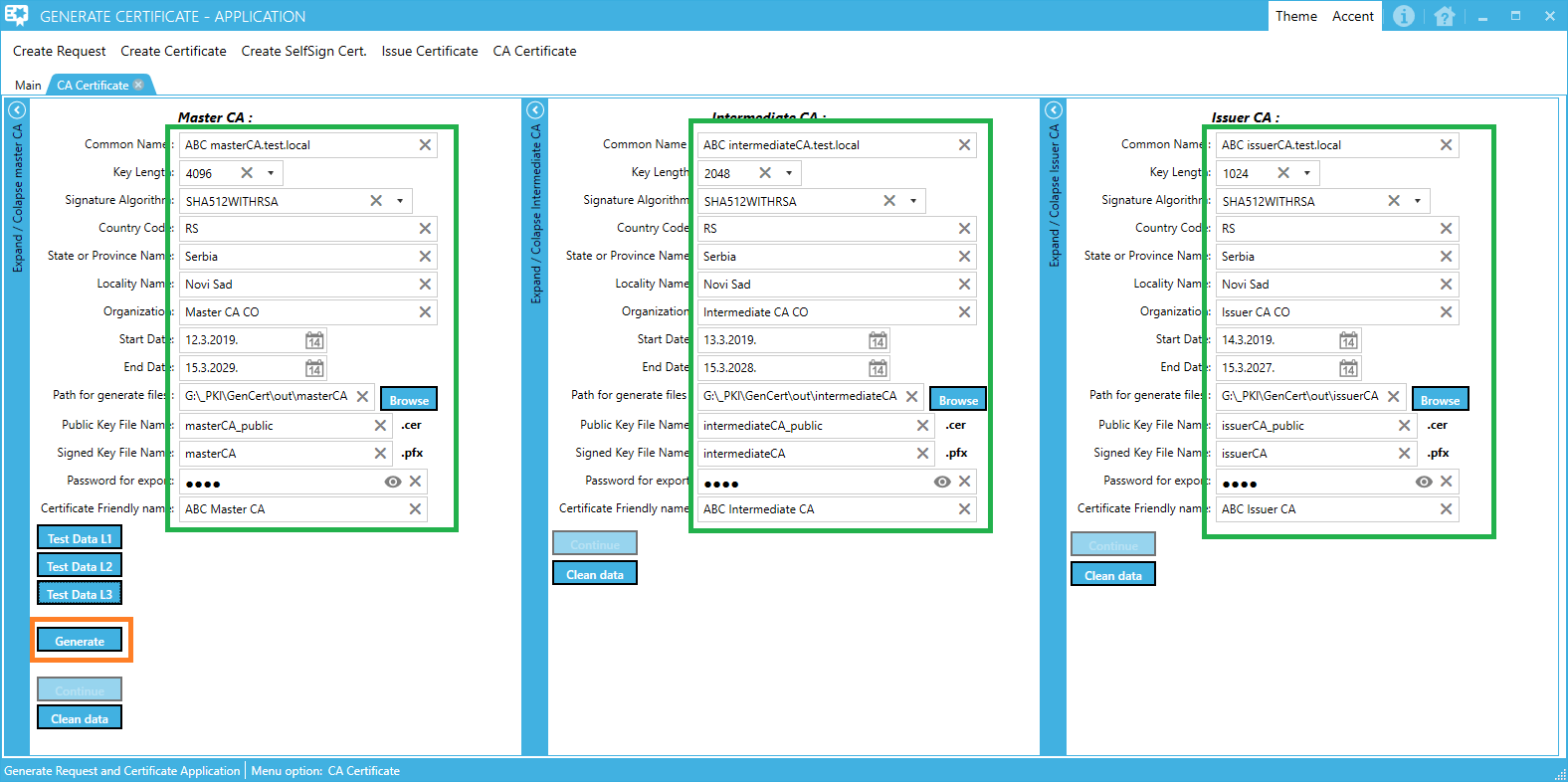
## CA Certificate (step)

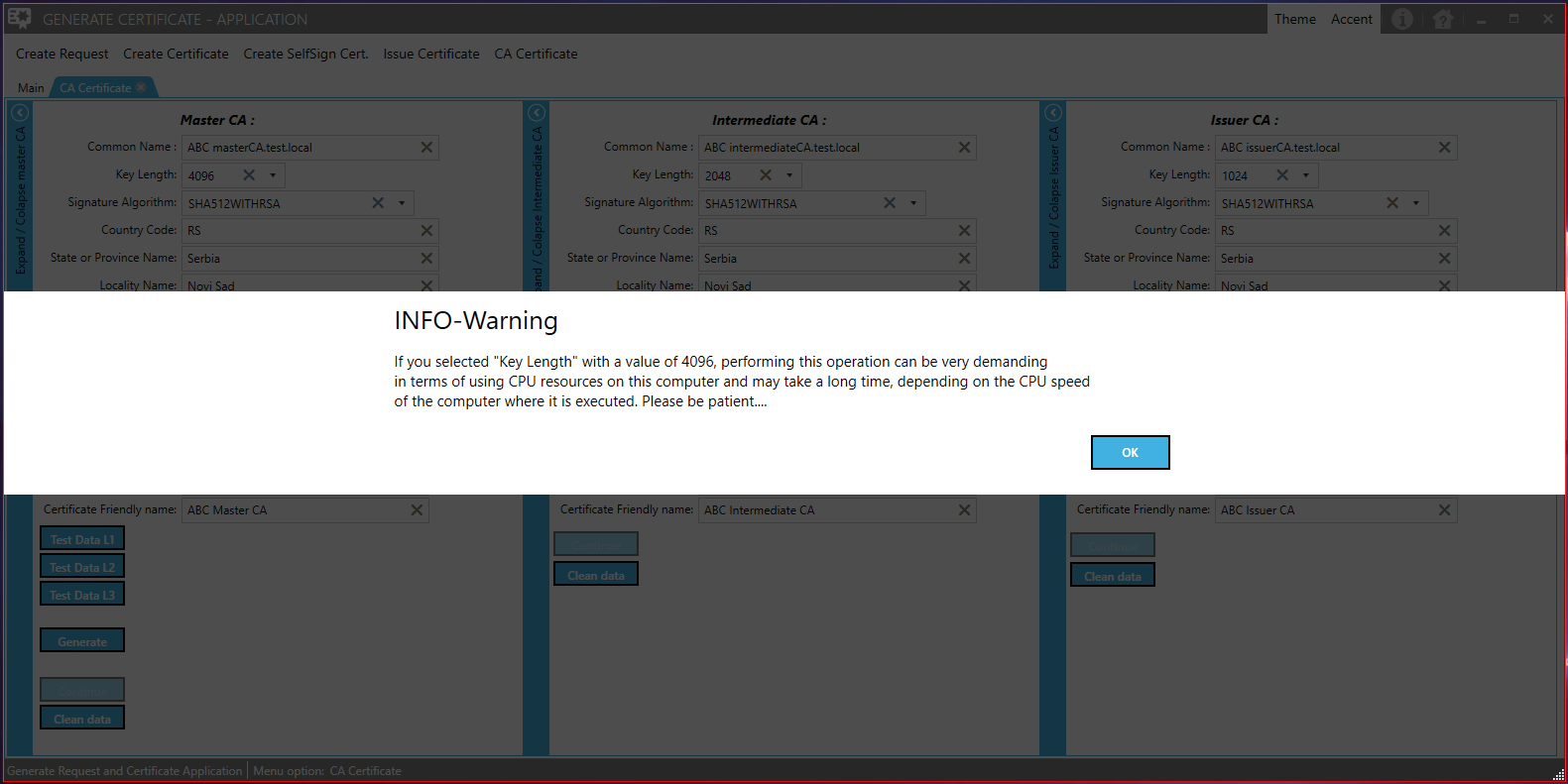
### Variant I –„Sign locally-Don’t have CA cert “

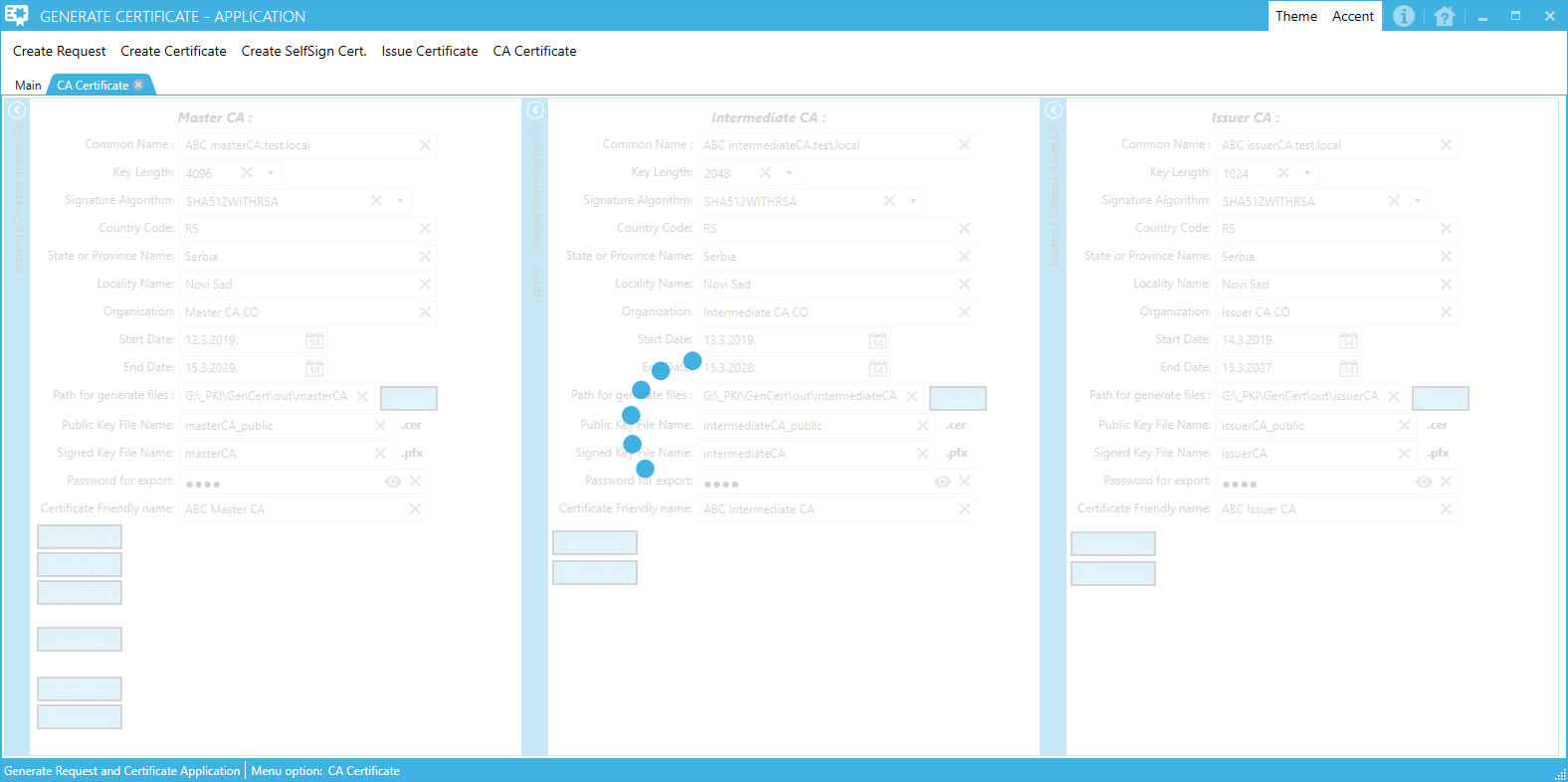


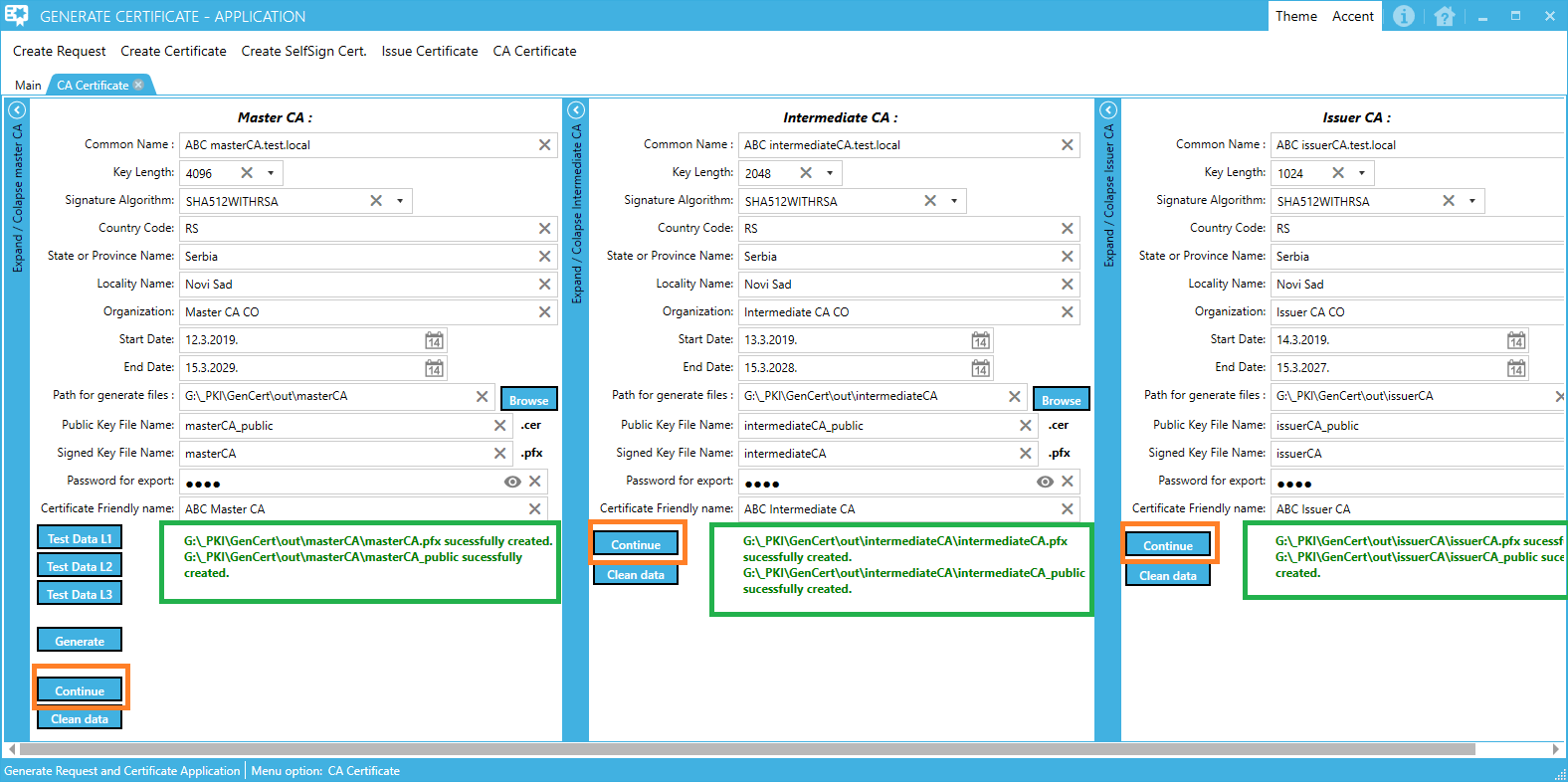
When click “Test Data L1” or “Test Data L2” or “Test Data L3”, new form for fill CA Parameters will be open.

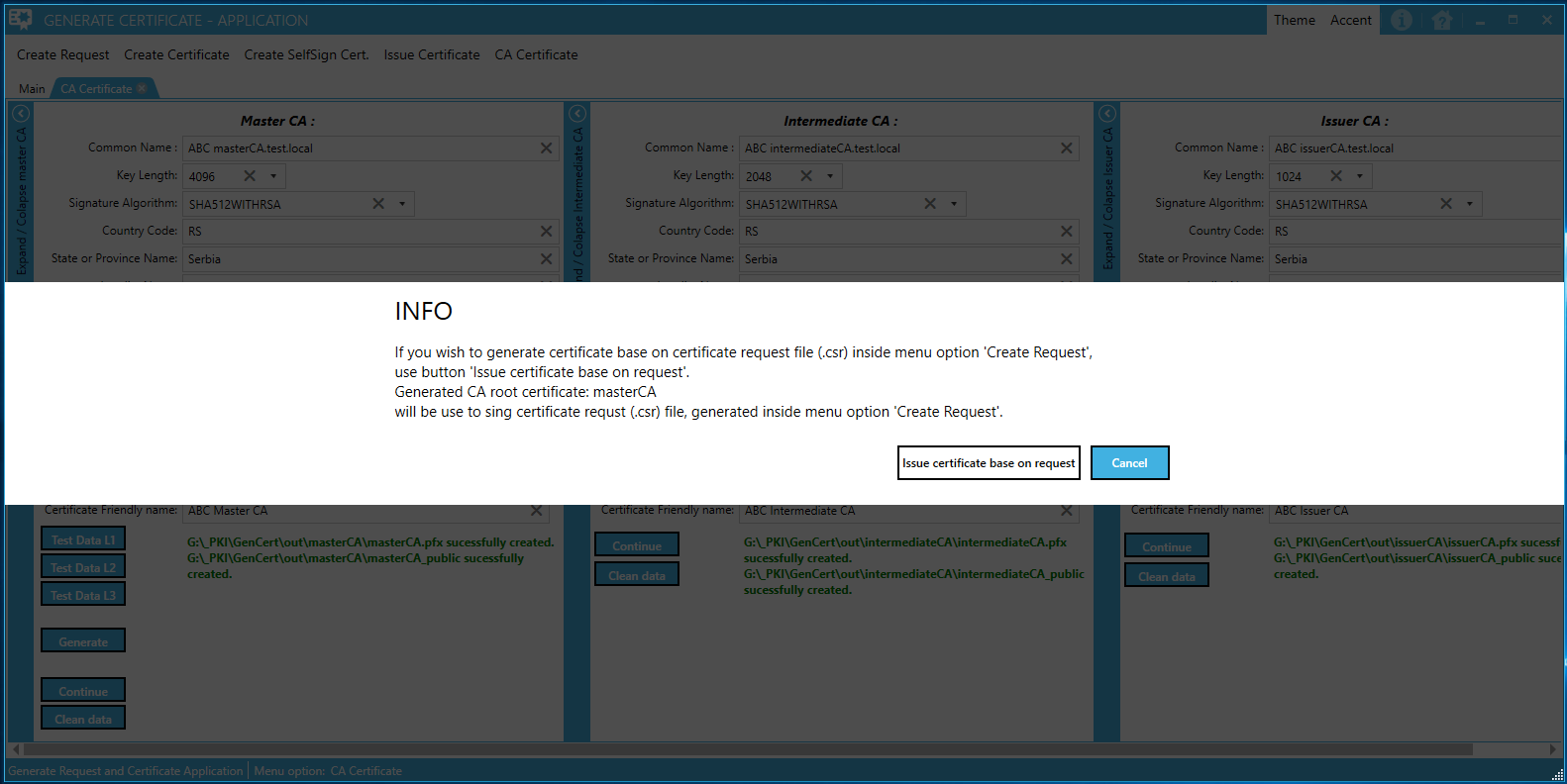






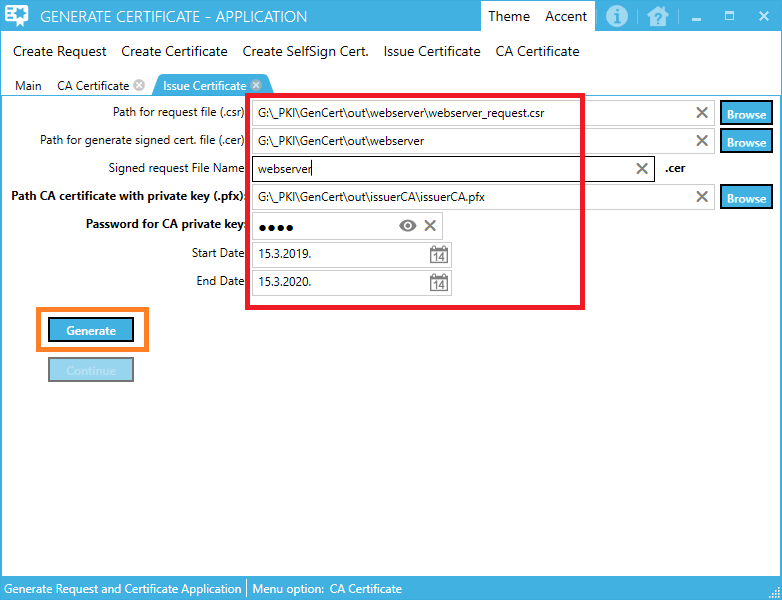


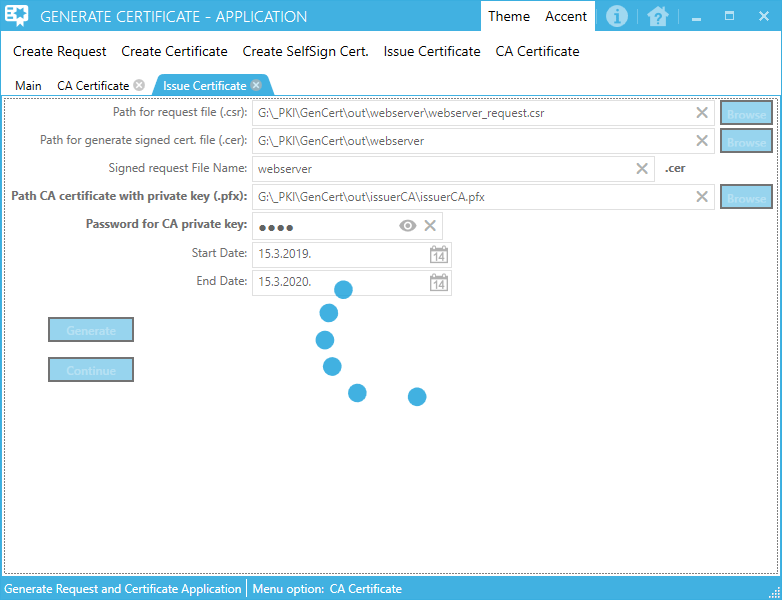


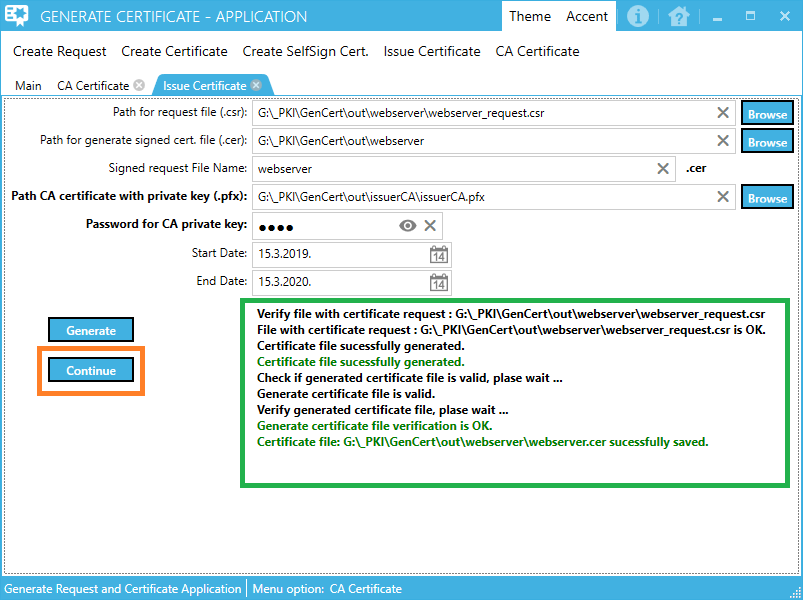


### Variant II –„Sign locally-Have CA cert“

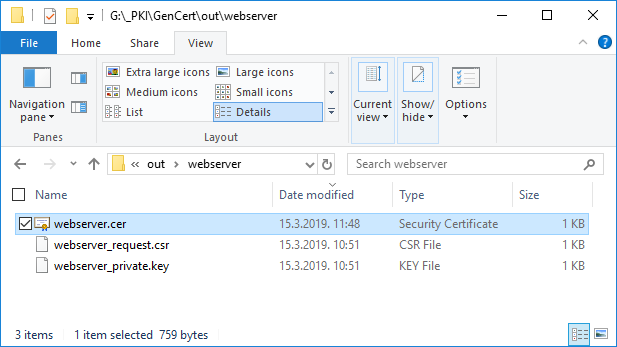
**NOTE:** If you use the root certificate from the rootCA subfolder, in the cert\_password.txt file in that folder there is a password that needs to be entered in the form.

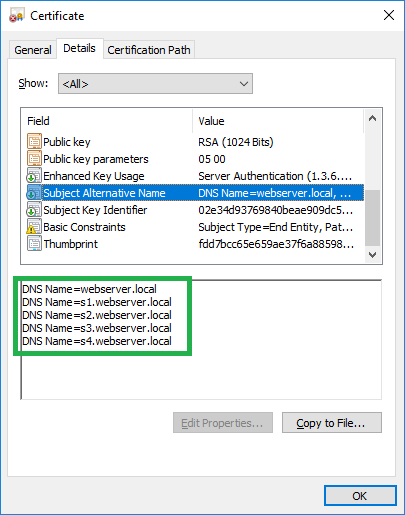






To verify that the signed certificate is successfully generated, perform a check

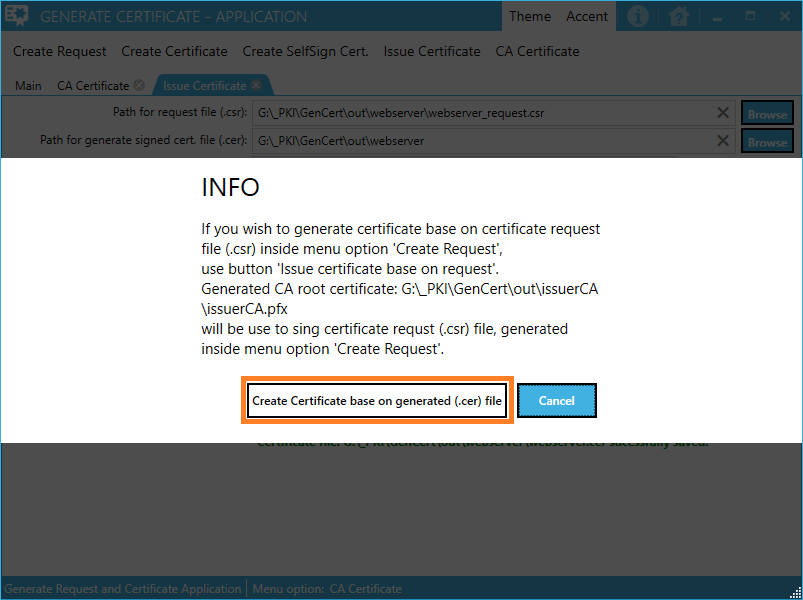




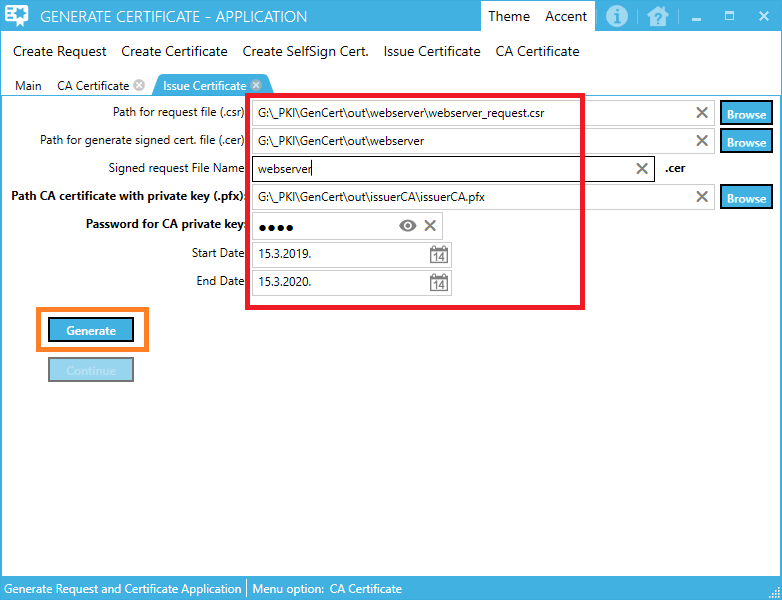
An alternate name certificate is OK.

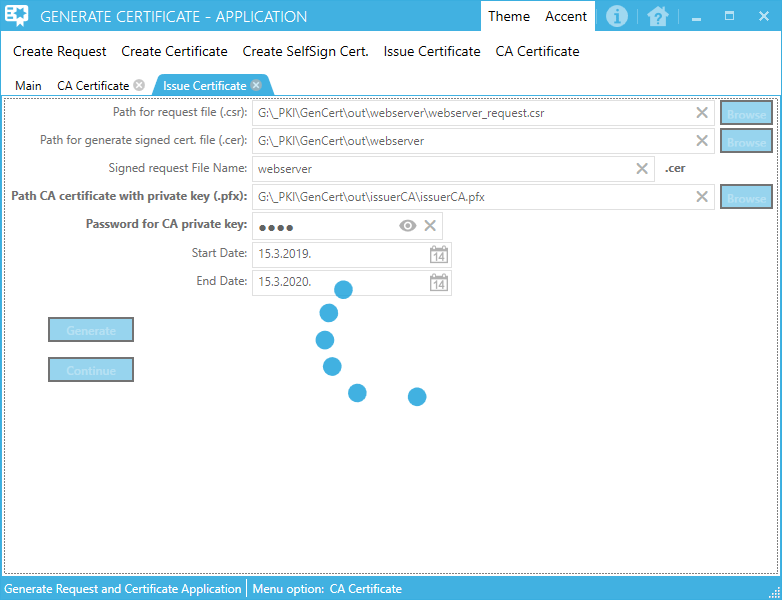
Click “Continue”.

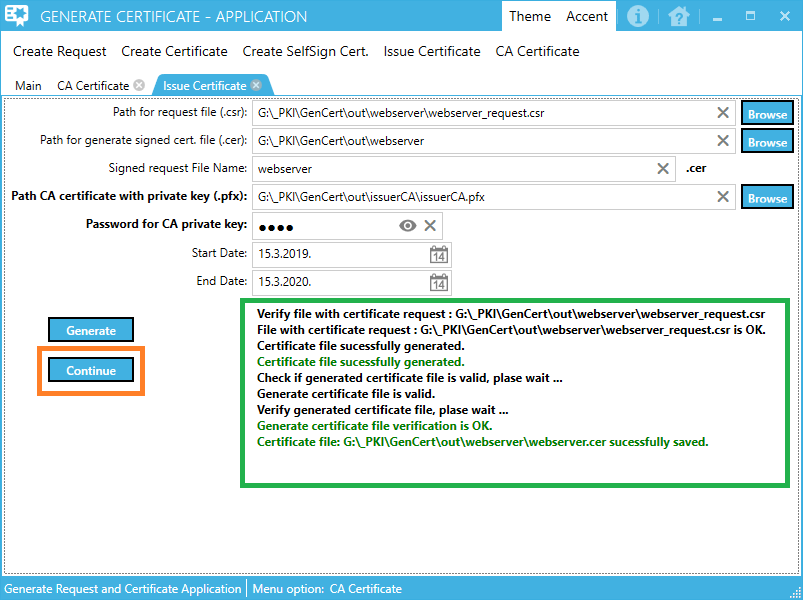
We continue to generate a file that will contain public + private key (.pfx), from a signed file (.cer) to a private key (.key)



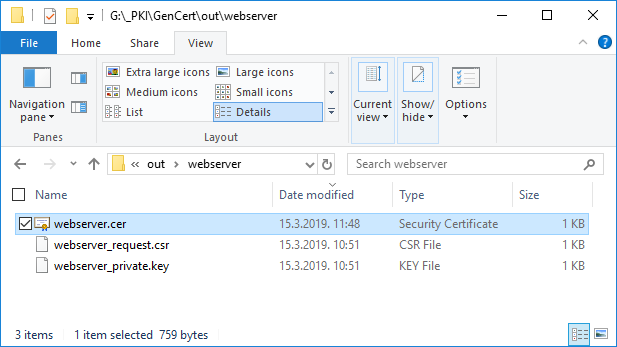
## Issue Certificate (step)

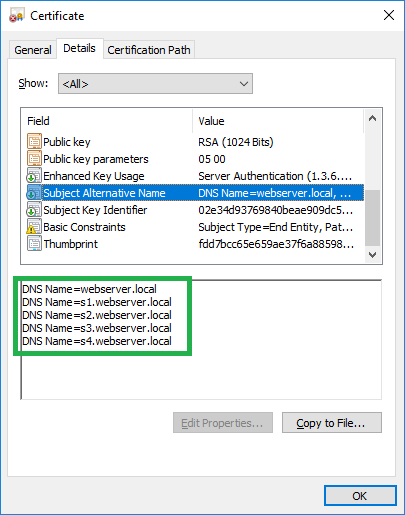






To verify that the signed certificate is successfully generated, perform a check

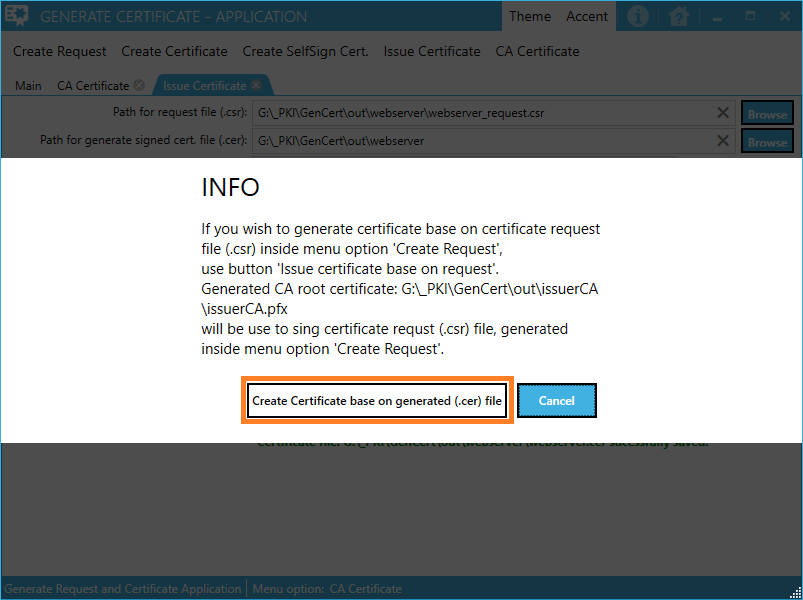




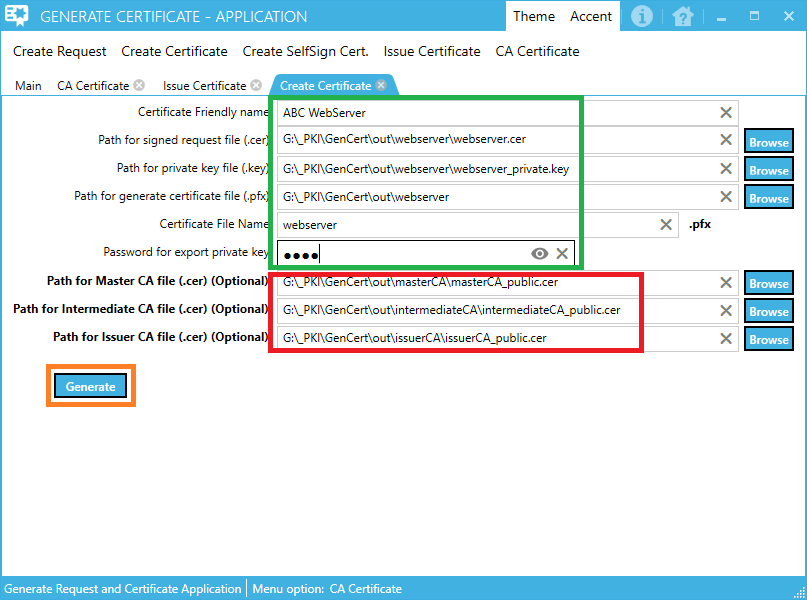
An alternate name certificate is OK.

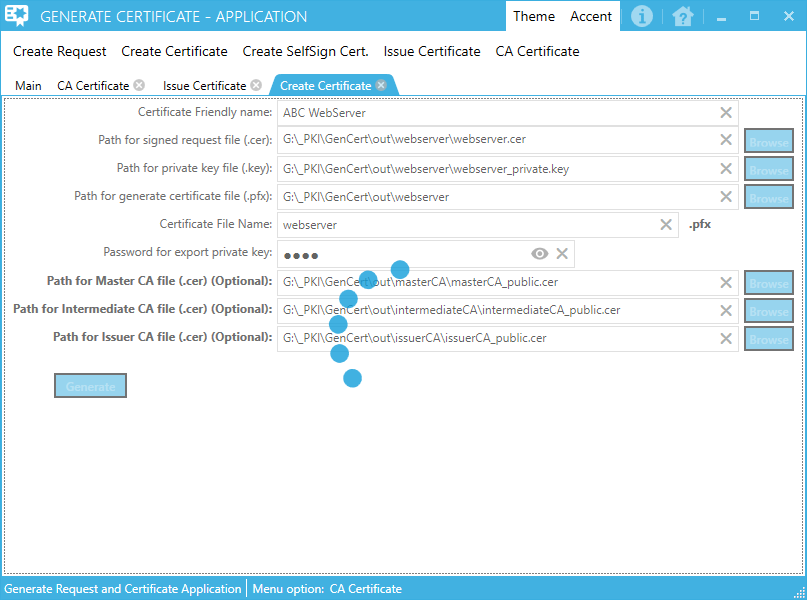
Click “Continue”.

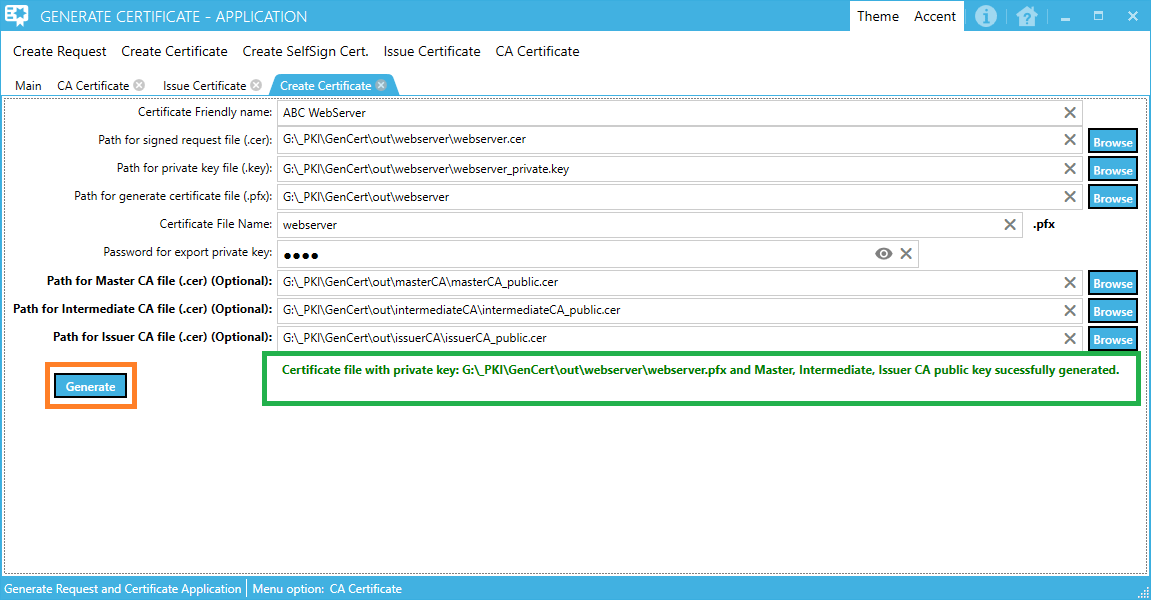
We continue to generate a file that will contain public + private key (.pfx), from a signed file (.cer) to a private key (.key)



## Create Signed Certificate (step)



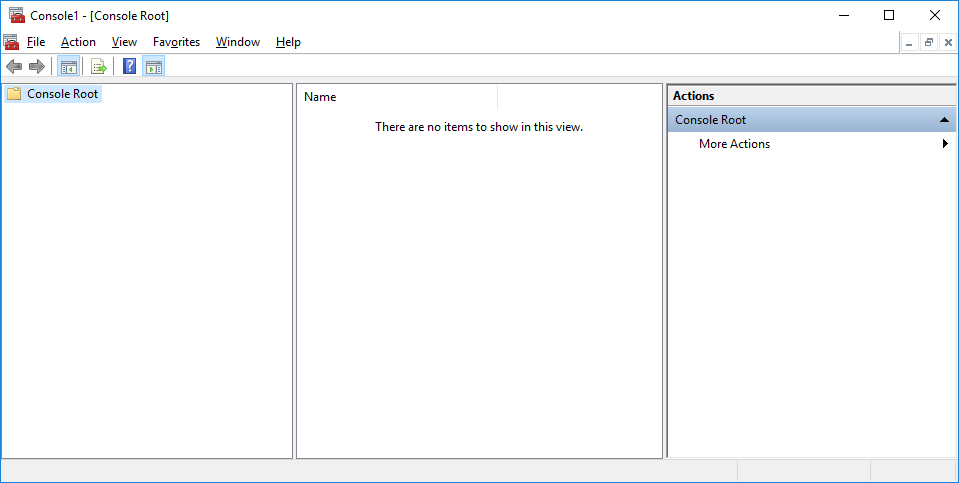




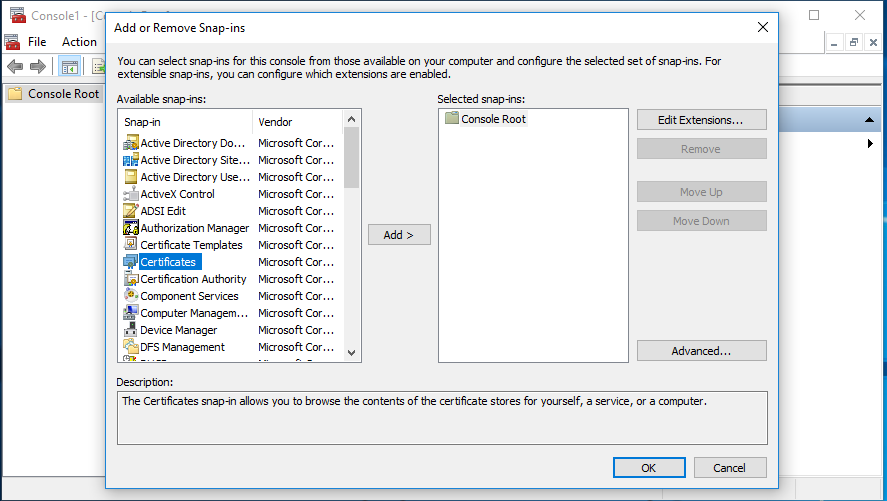
Go to „[Import certificate from generated pfx file](#_Import_certifikata_iz)“

### Import certificate from generated pfx file to web server

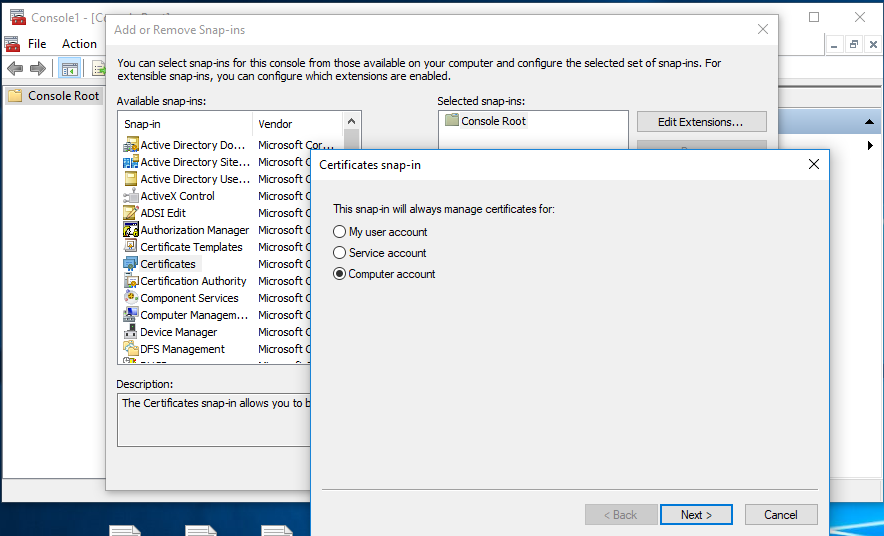
On the computer, open mmc.exe console.

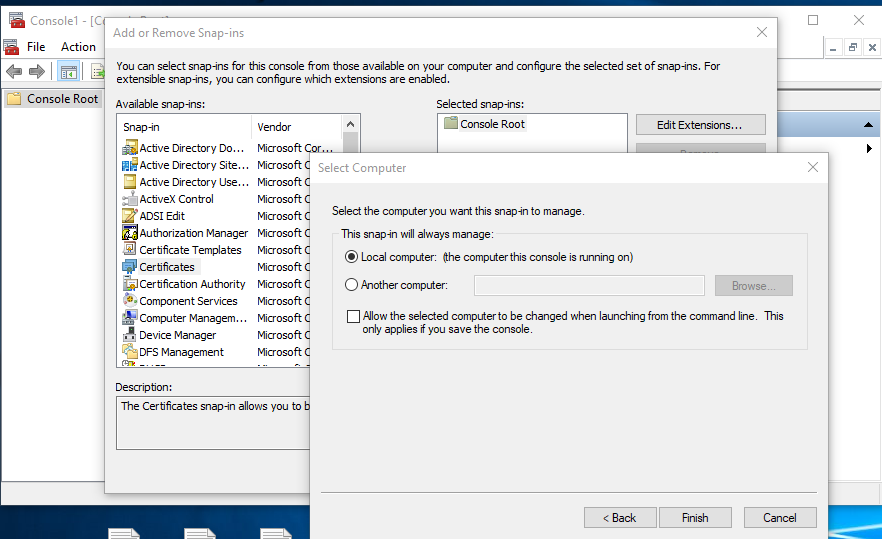


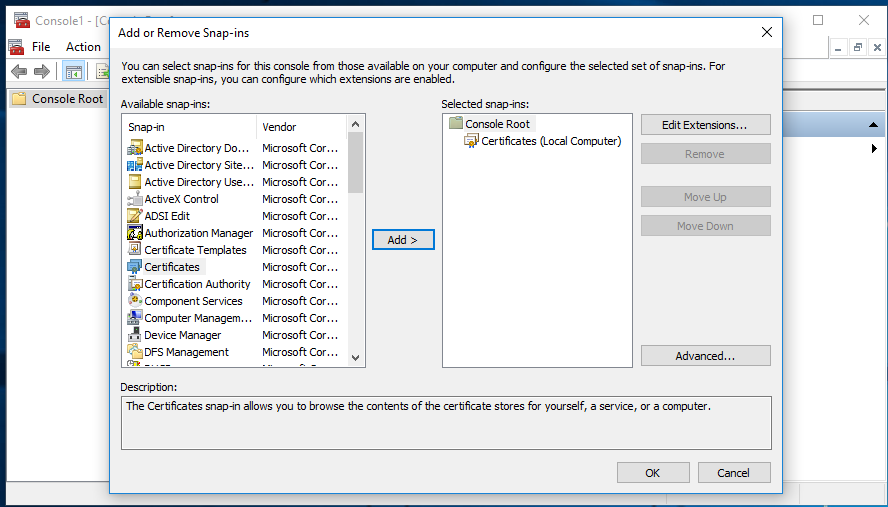
Add Certificate Snap-in

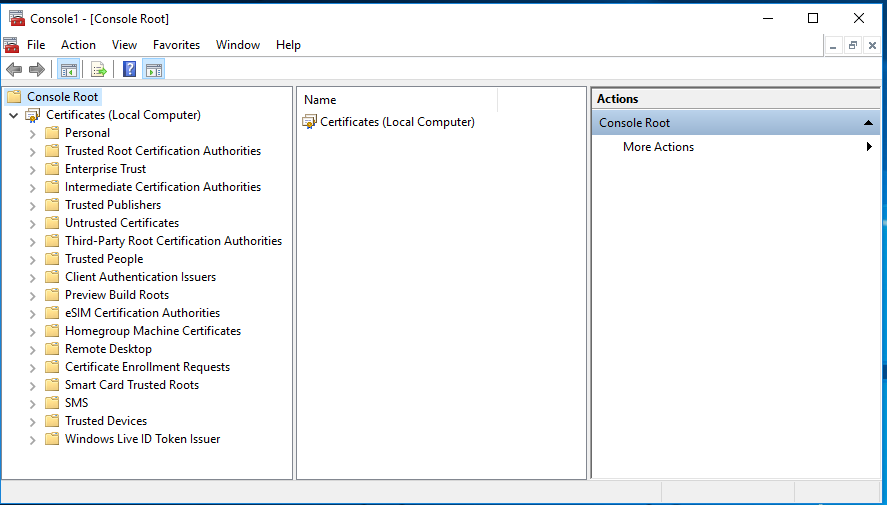


Add, Choose option “Computer account”



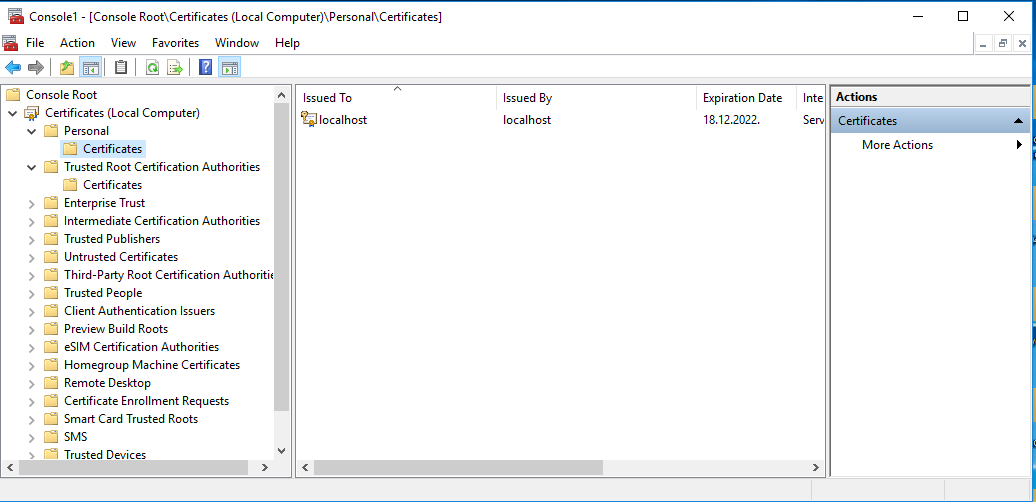




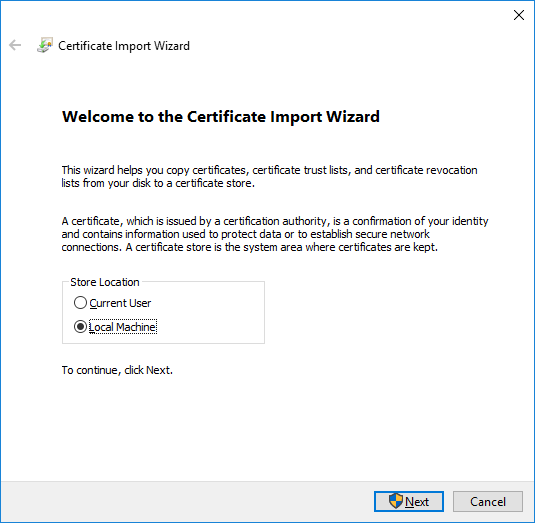
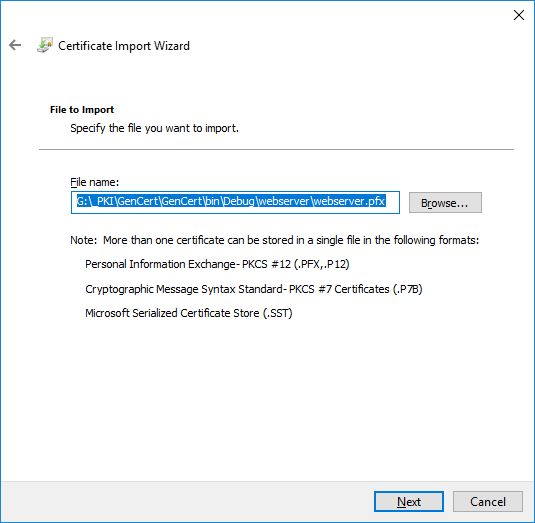


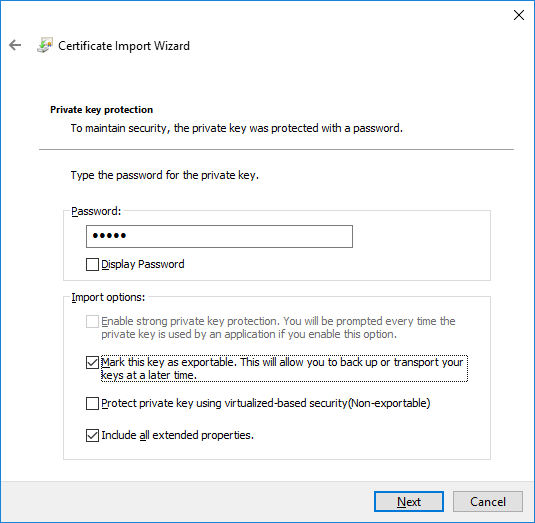
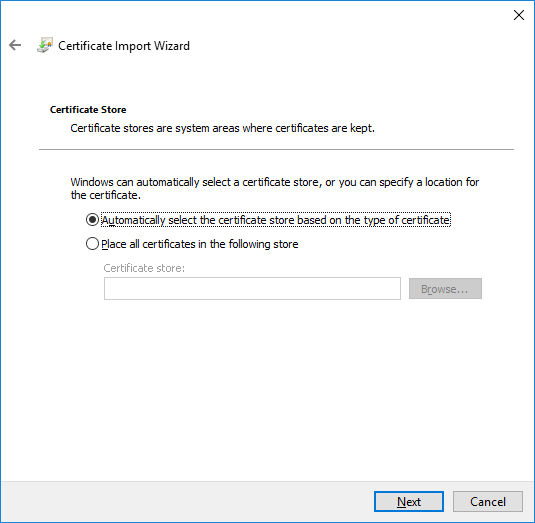
Parts of local computer Certificate store for interest are:

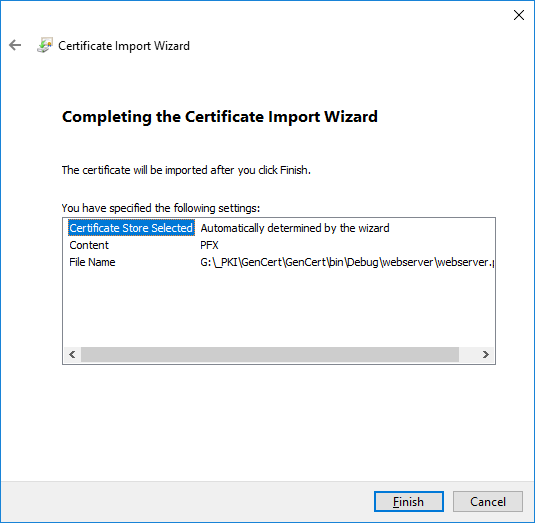
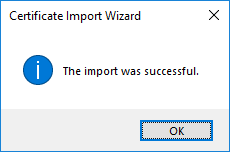
1. Personal -> Certificates
2. Trusted Root Certification Authorities -> Certificates
3. Intermediate Certification Authorities -> Certificates



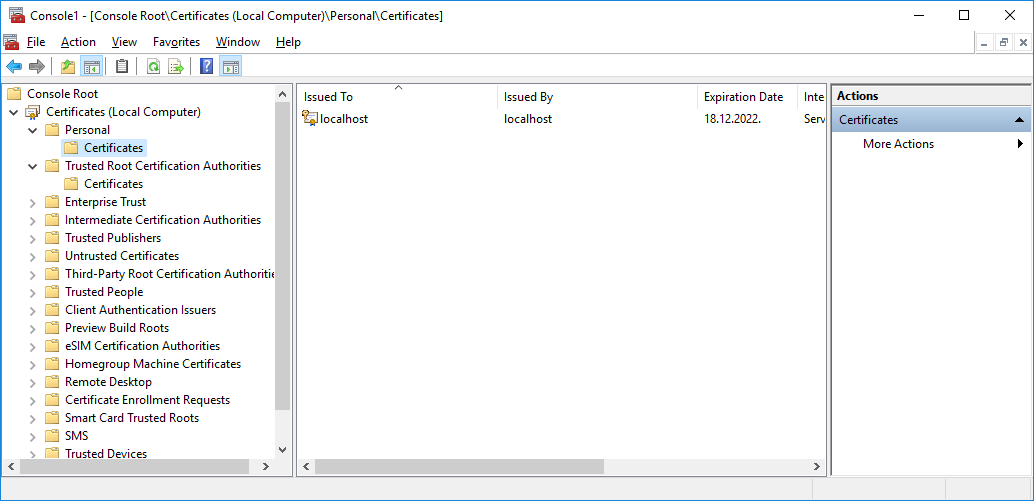
Double click on generated signed certificate request file with .pfx extension will open Certificate Import Wizard. Select Store location -> Local Machine

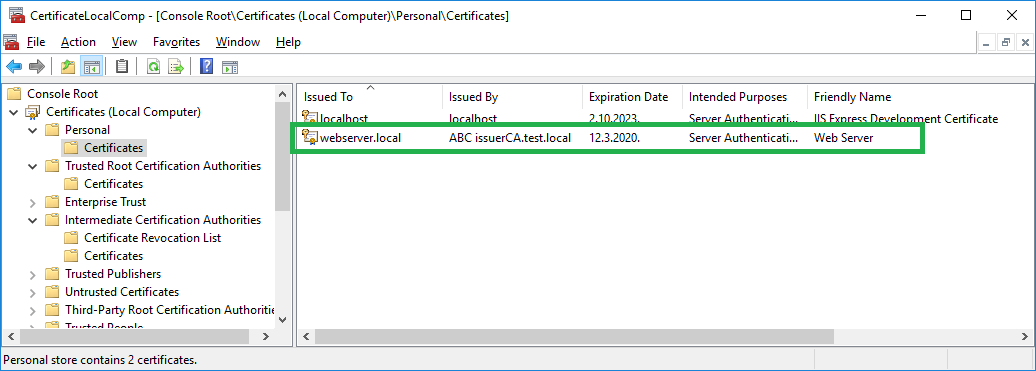
 

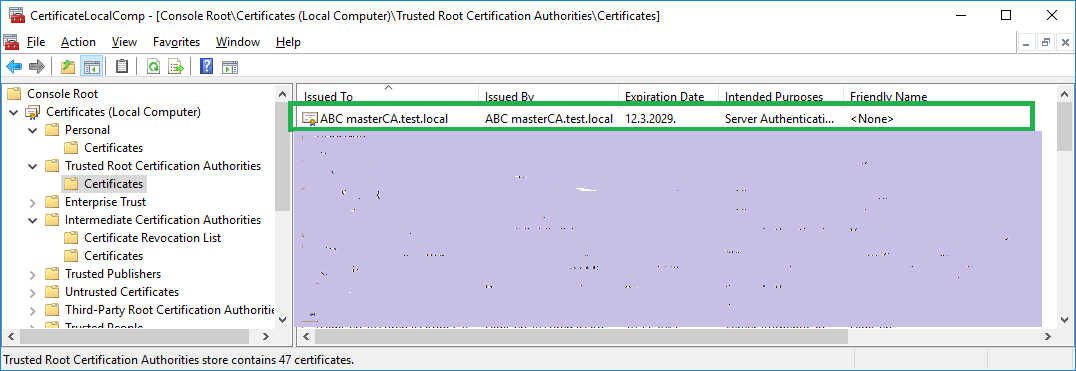
 

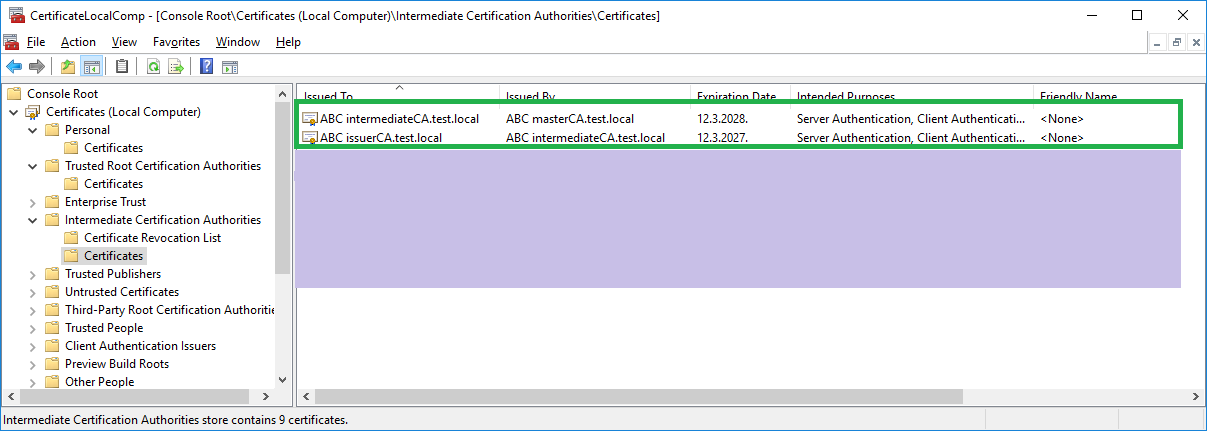
 

Refresh Personal and Trusted Root Certification Authorities inside mmc console.

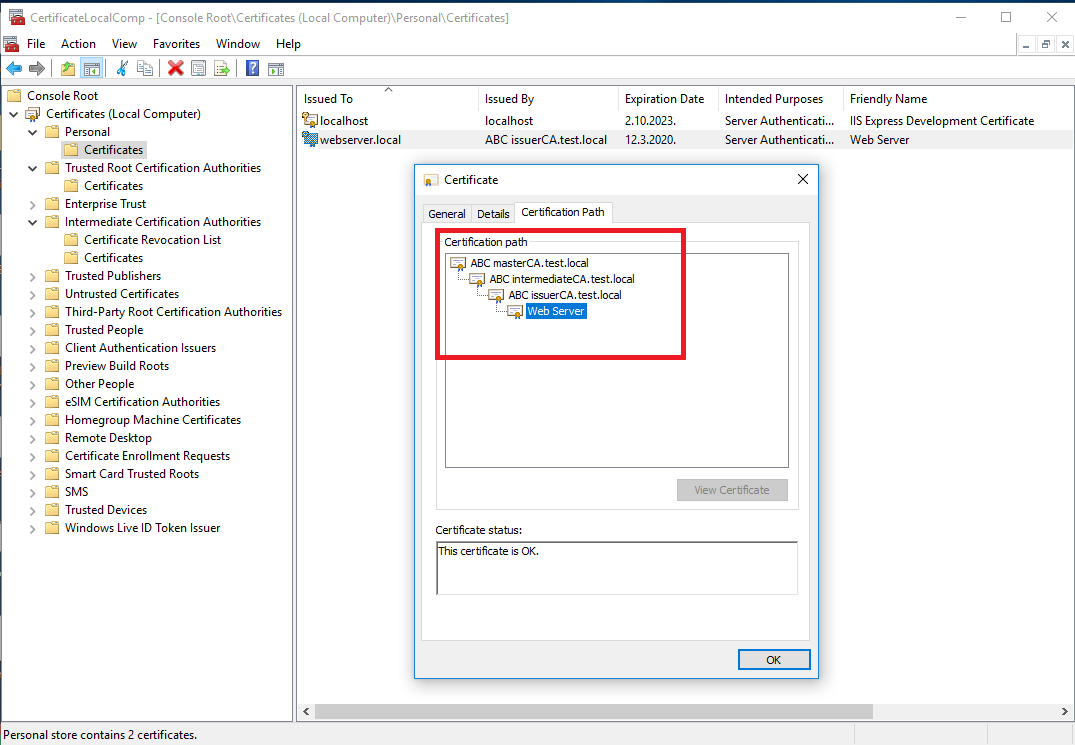




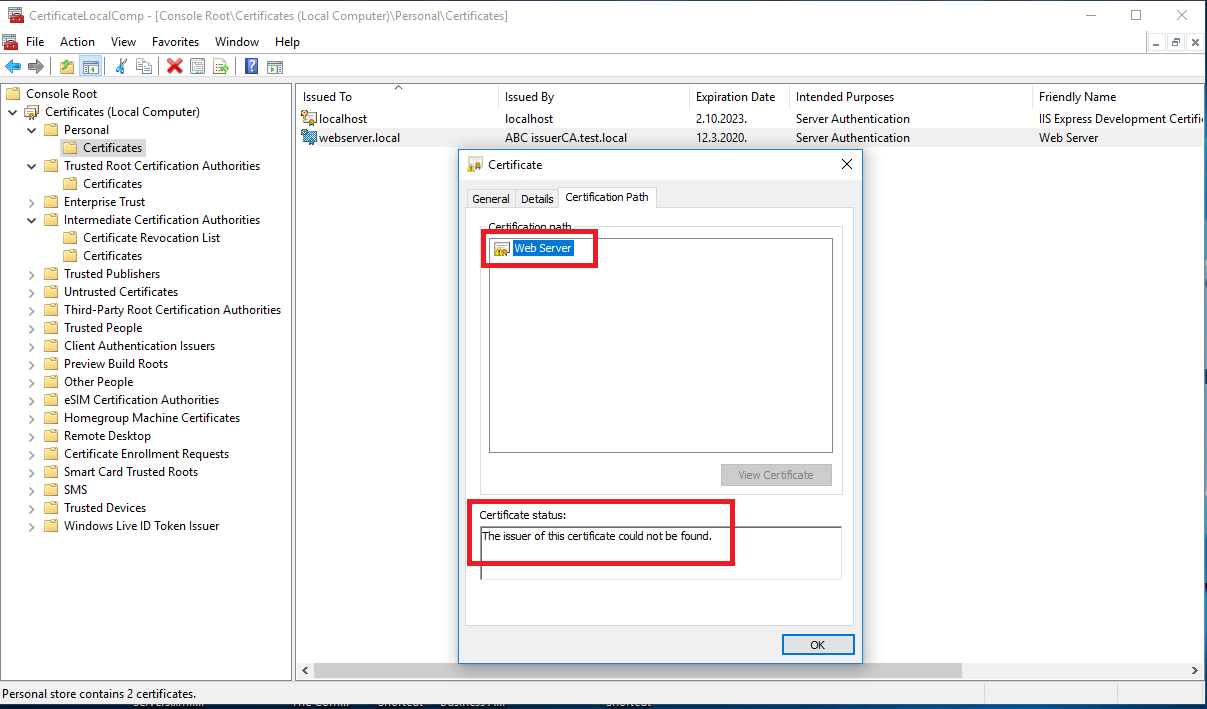




Valid certificate:

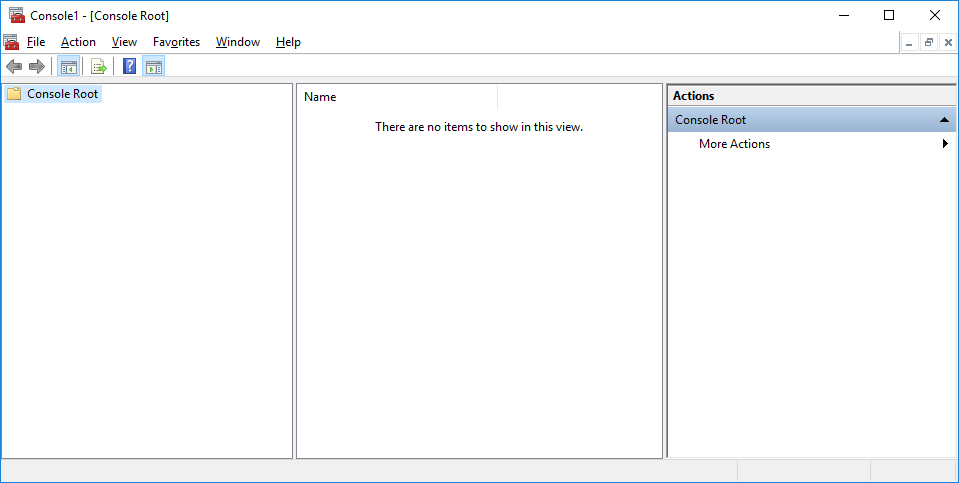


Wrong certificate:

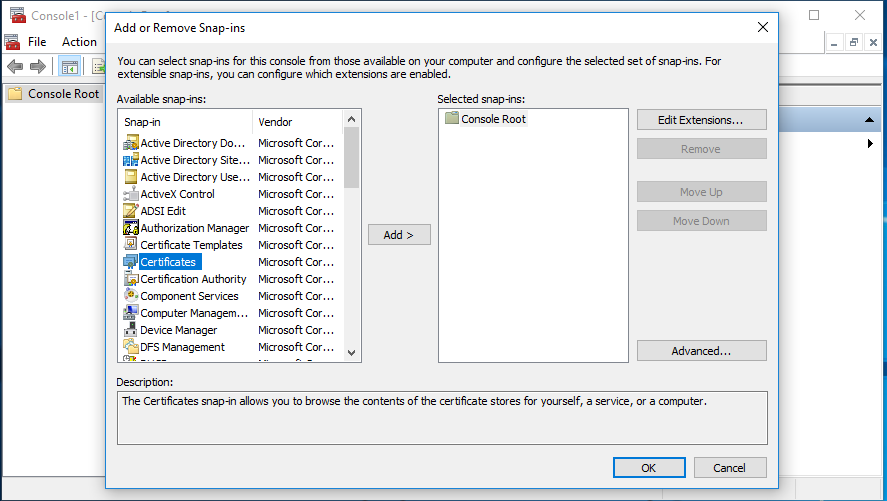


### Import certificate from generated pfx file to client computer for web server

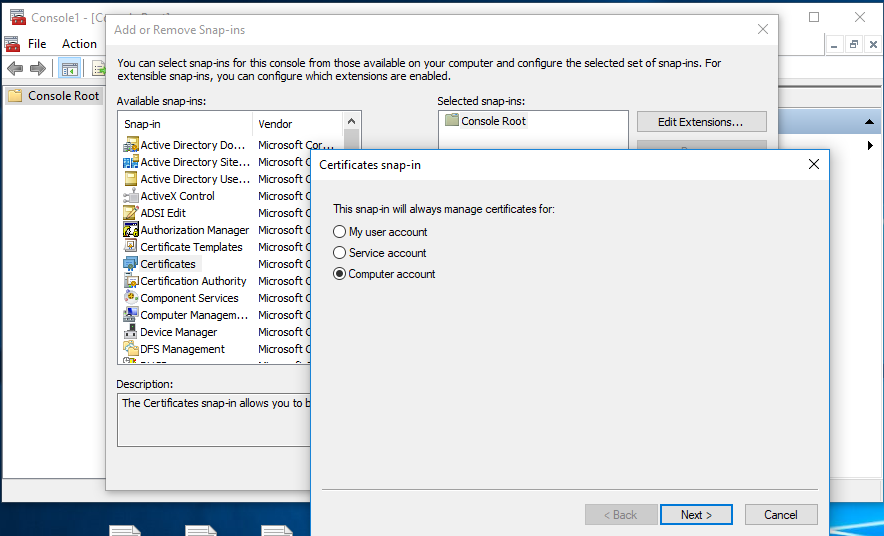
On the client computer, open mmc.exe console.

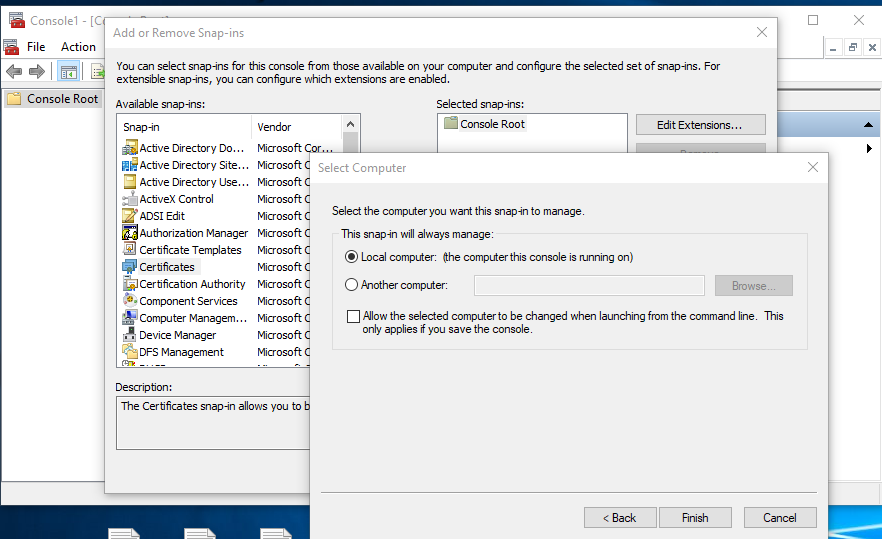


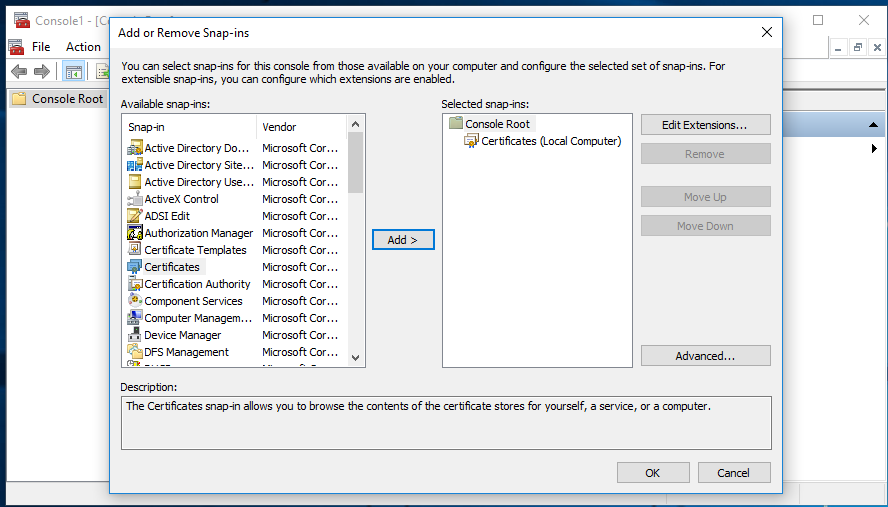
Add Certificate Snap-in

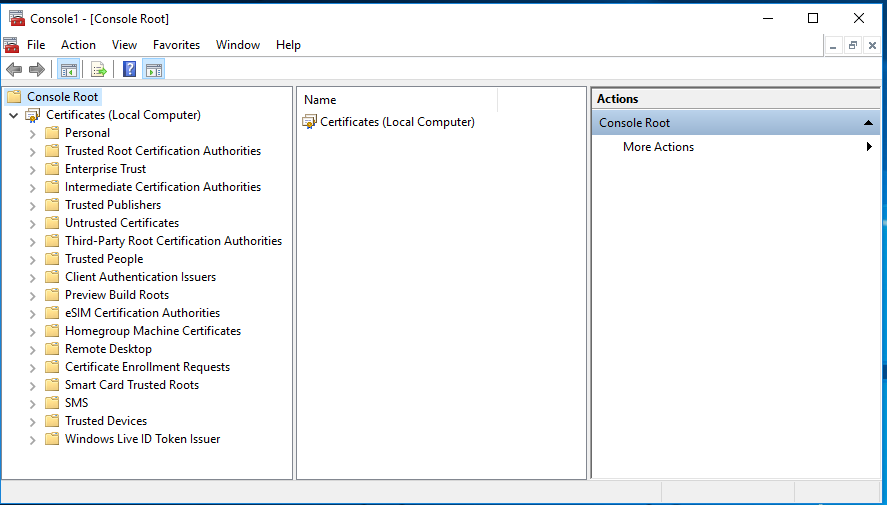


Add, Choose option “Computer account”



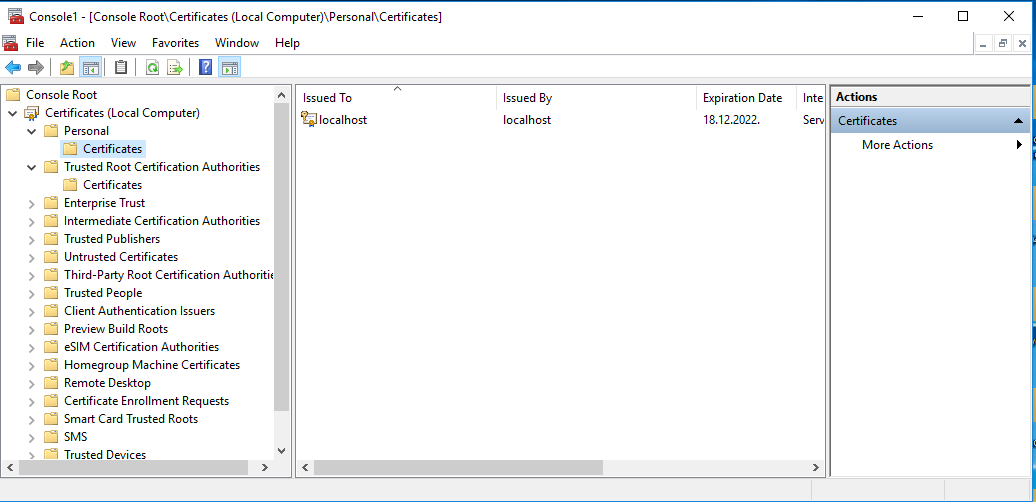






Parts of local computer Certificate store for interest are:

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.

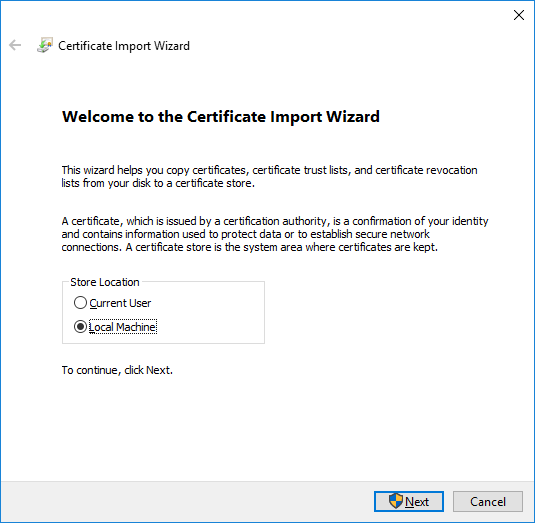
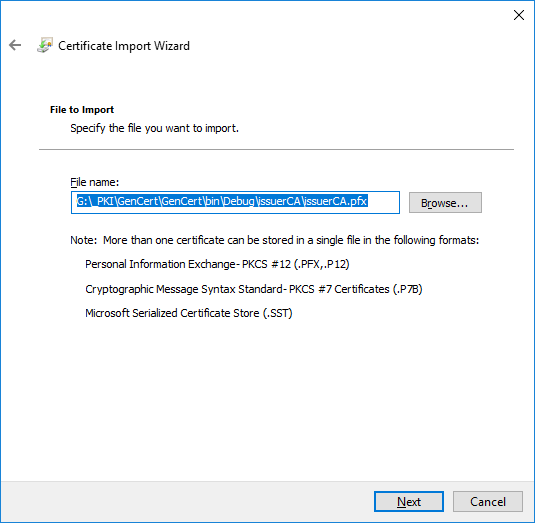
If you use one level CA (only master CA) to issue certificate for server use master CA .pfx file.

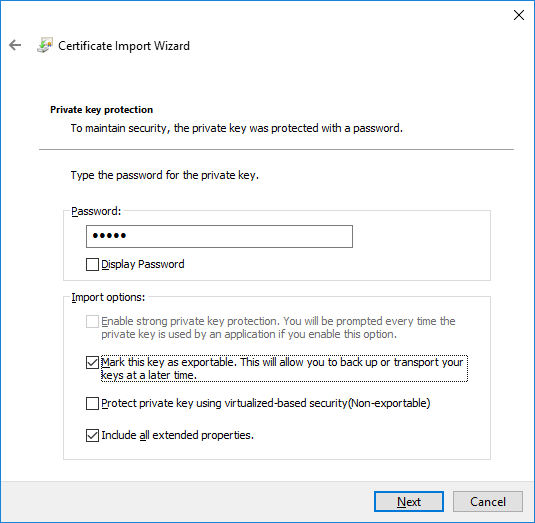
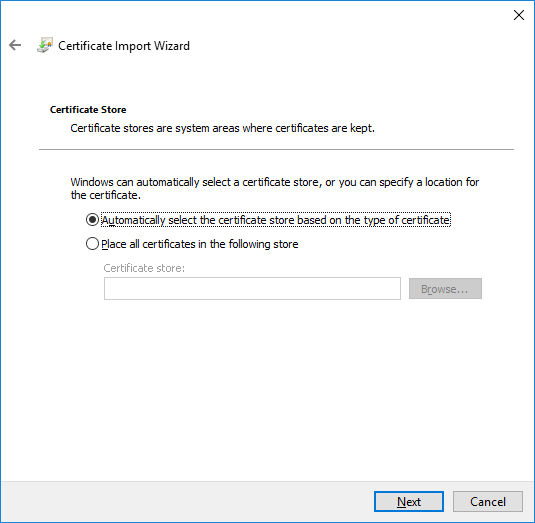
If you use two level CA (master CA + intermediate CA) to issue certificate for server use intermediate CA .pfx file.

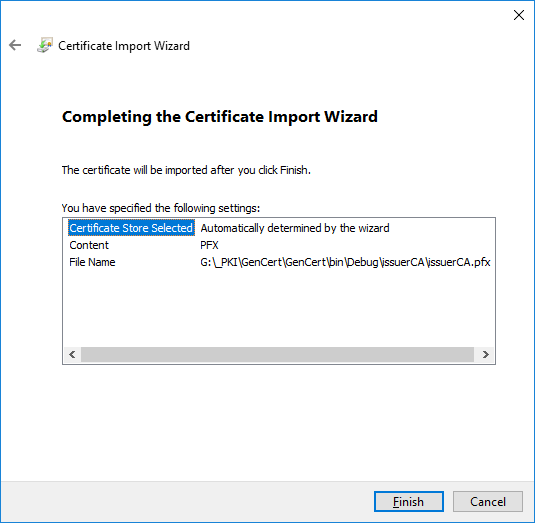
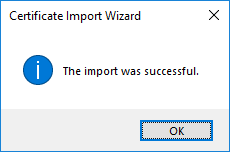
If you use three level CA (master CA + intermediate CA + issuer CA) to issue certificate for server use issuer CA .pfx file.

## 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

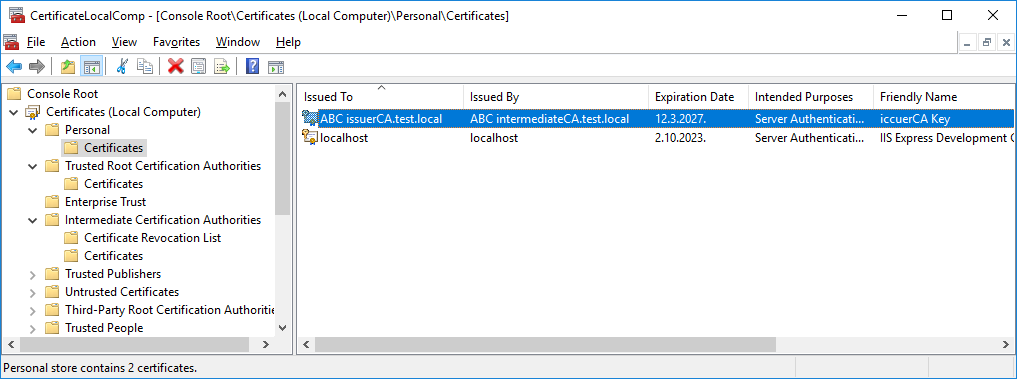
 

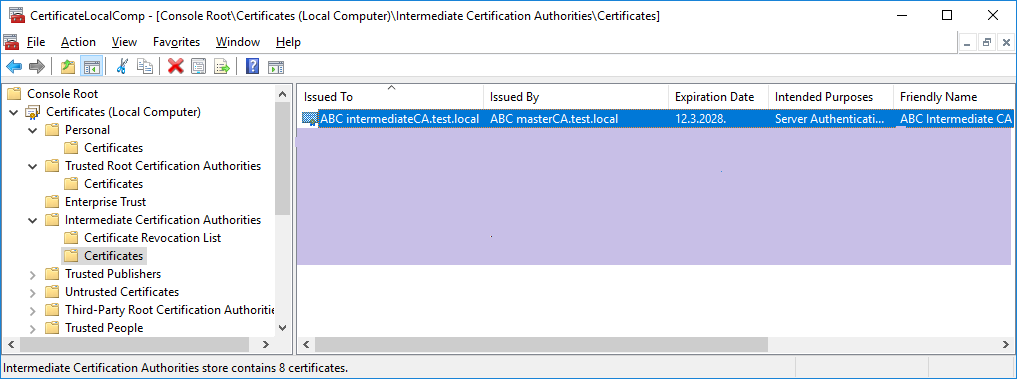
If you import three level certificate (issuer CA) you need to refresh Personal, Trusted Root Certification Authorities and Intermediate Certification Authorities inside mmc console to see new imported certificates.

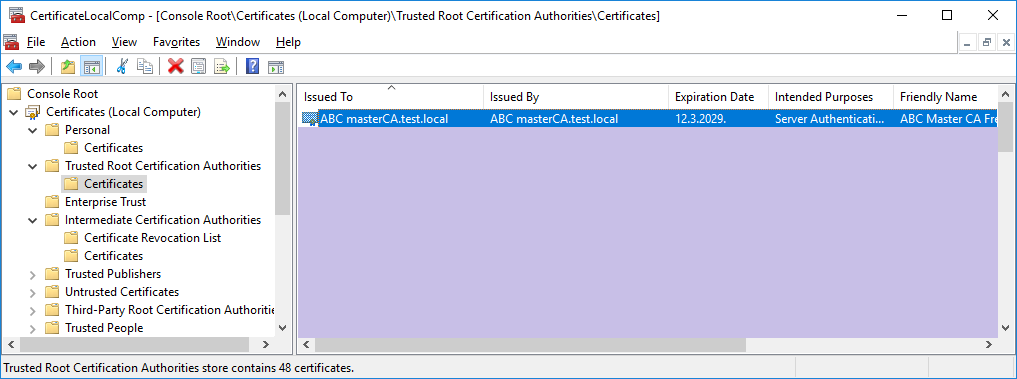
-issuer CA certificate will be found inside Personal->Certificates store.

-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.

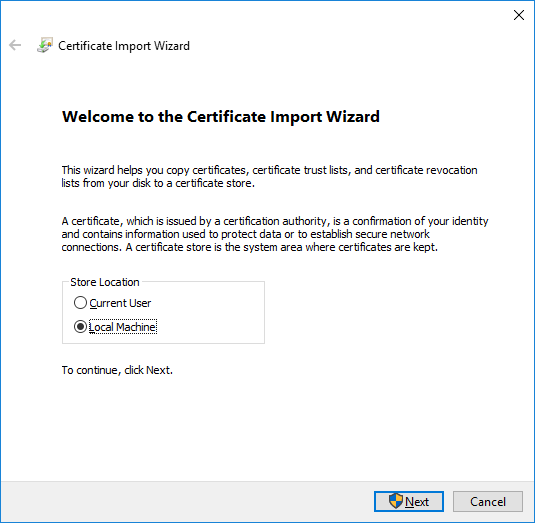
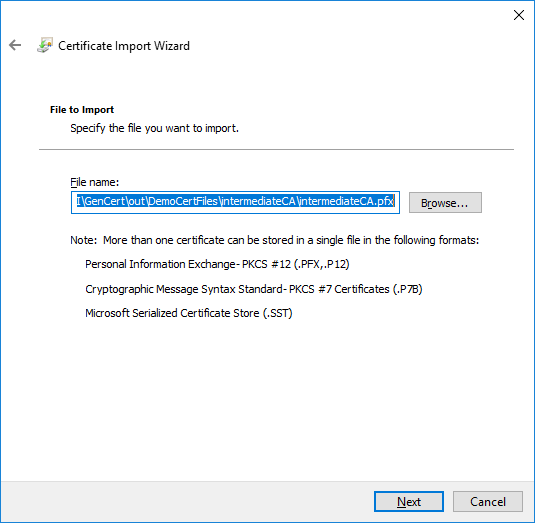


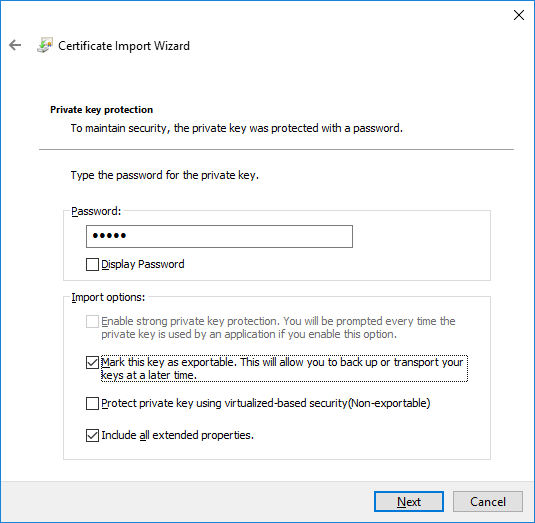
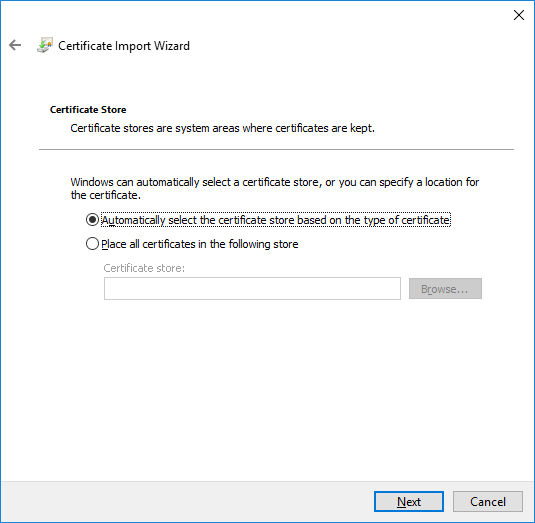


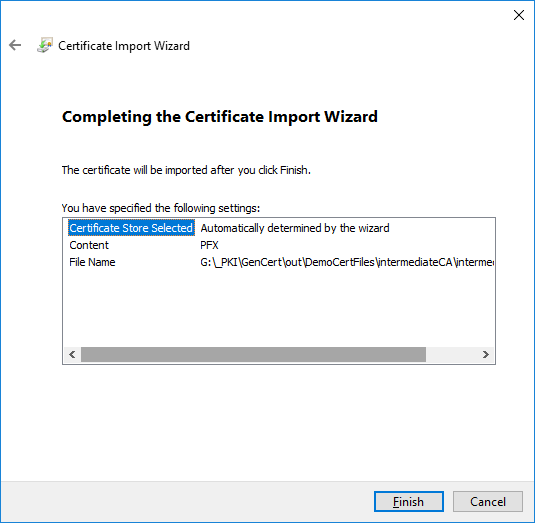
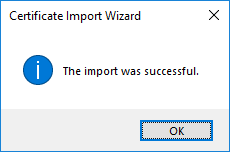


## Import two level CA certificate (intermediate CA)

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

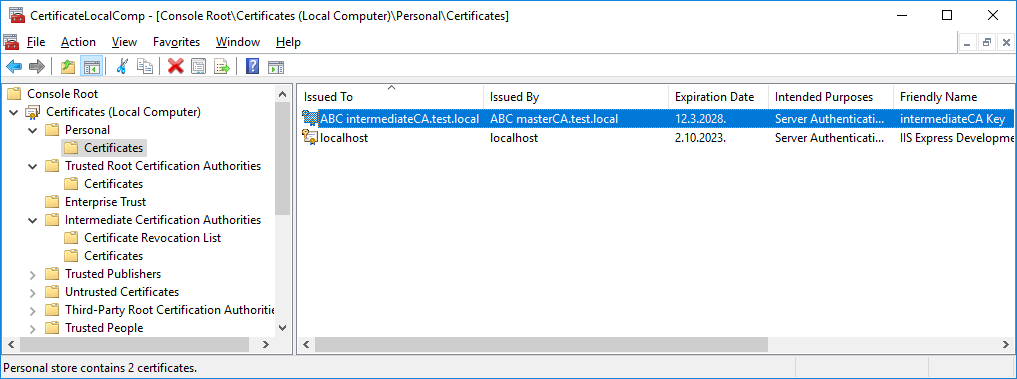
 

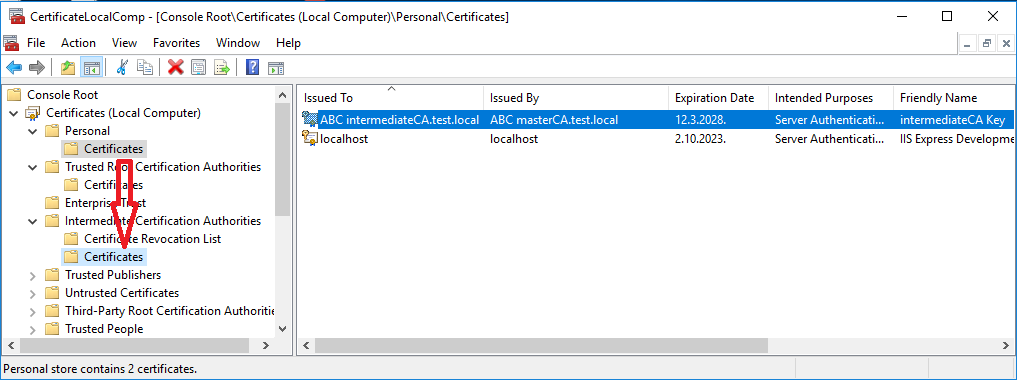
 

If you import two level certificate (intermediate CA) you need to refresh Personal, Trusted Root Certification Authorities.

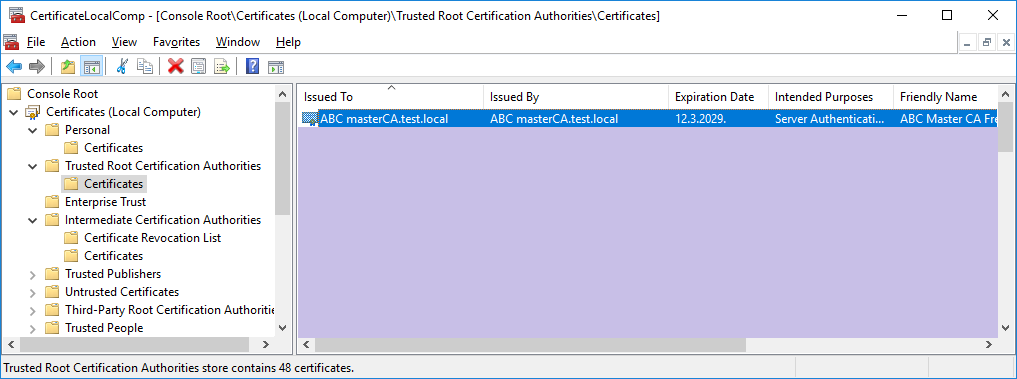
Intermediate CA certificate will be found inside Personal->Certificates store.



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.

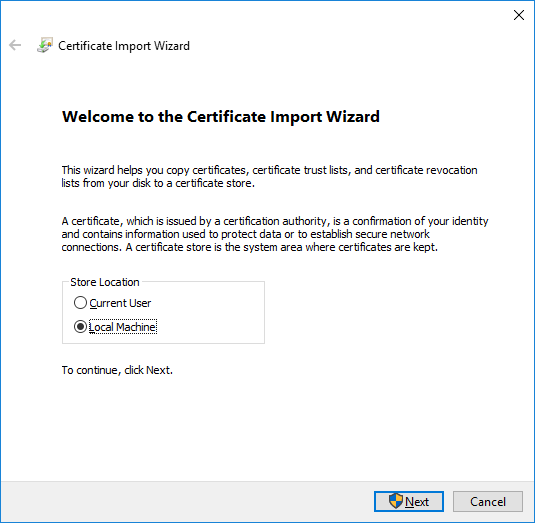
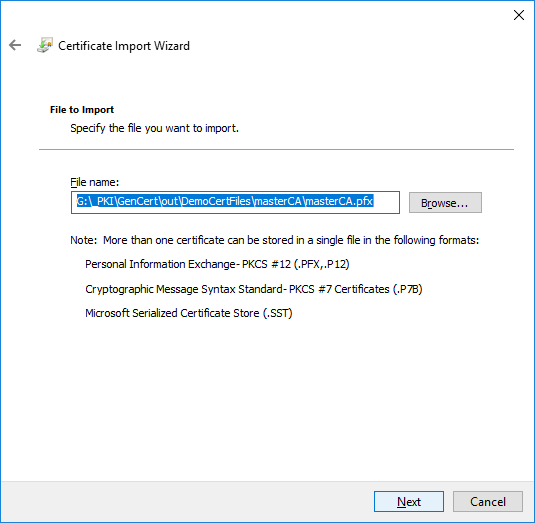


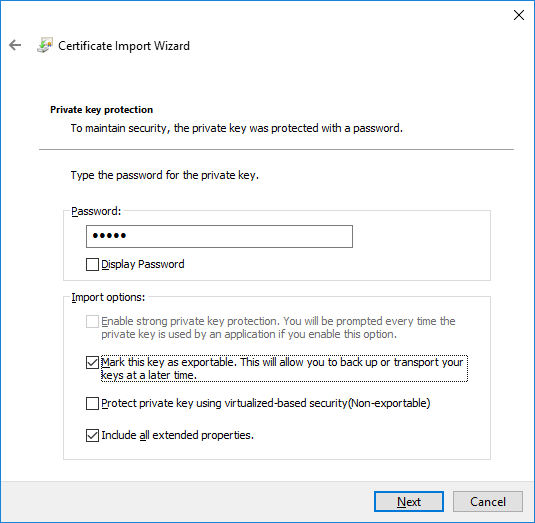
Master CA certificate will be found inside Trusted Root Certification Authorities->Certificates store.



## Import one level CA certificate (master CA)

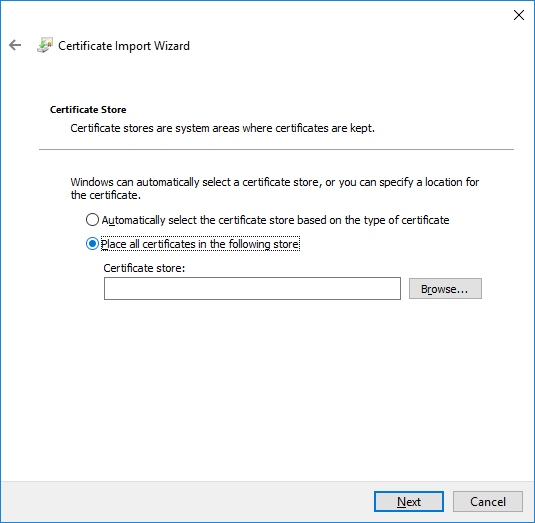
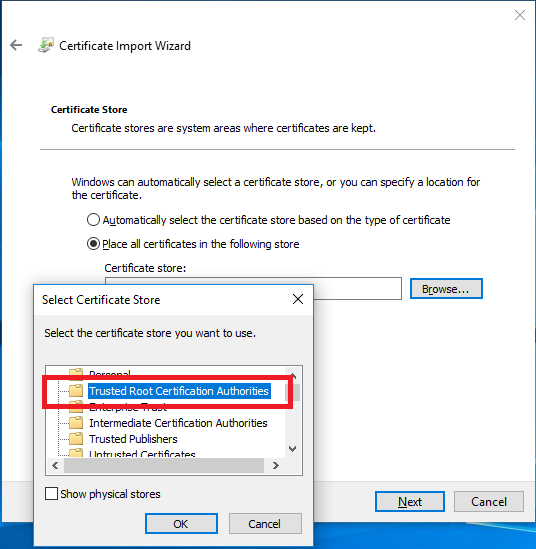
Double click on generated CA file with .pfx extension will open Certificate Import Wizard. Select Store location -> Local Machine

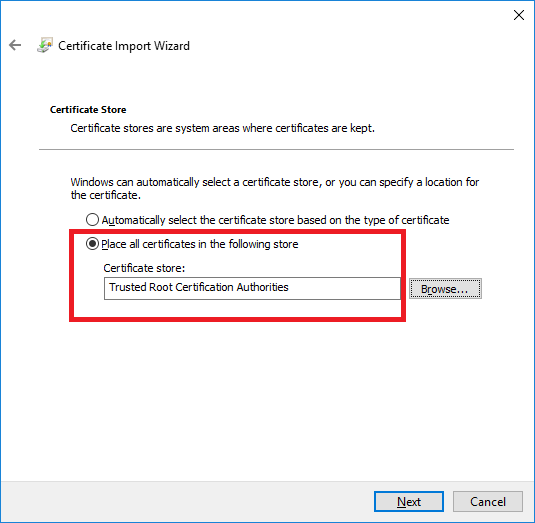
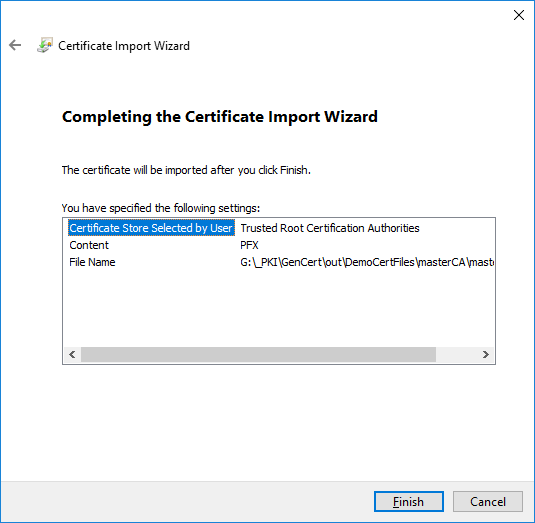
 

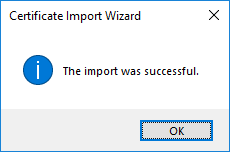


**NOTE:**

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.

