Generate Request and Certificate PKI Application

Table of Contents

[1. Introduction 1](#_Toc3808683)

[1.1. User Interface 2](#_Toc3808684)

[2. Create Request 11](#_Toc3808685)

[3. Create Certificate 17](#_Toc3808686)

[4. Create SelfSign Cert. 21](#_Toc3808687)

[5. Issue Certificate 24](#_Toc3808688)

[6. CA Certificate 27](#_Toc3808689)

[7. Import data from generated signed certificate file to SERVER certificate store 34](#_Toc3808690)

[8. Import data from generated CA certificate file(s) to client certificate store 41](#_Toc3808691)

[8.1. Import three level CA certificate (issuer CA) 43](#_Toc3808692)

[8.2. Import two level CA certificate (intermediate CA) 46](#_Toc3808693)

[8.3. Import one level CA certificate (master CA) 49](#_Toc3808694)

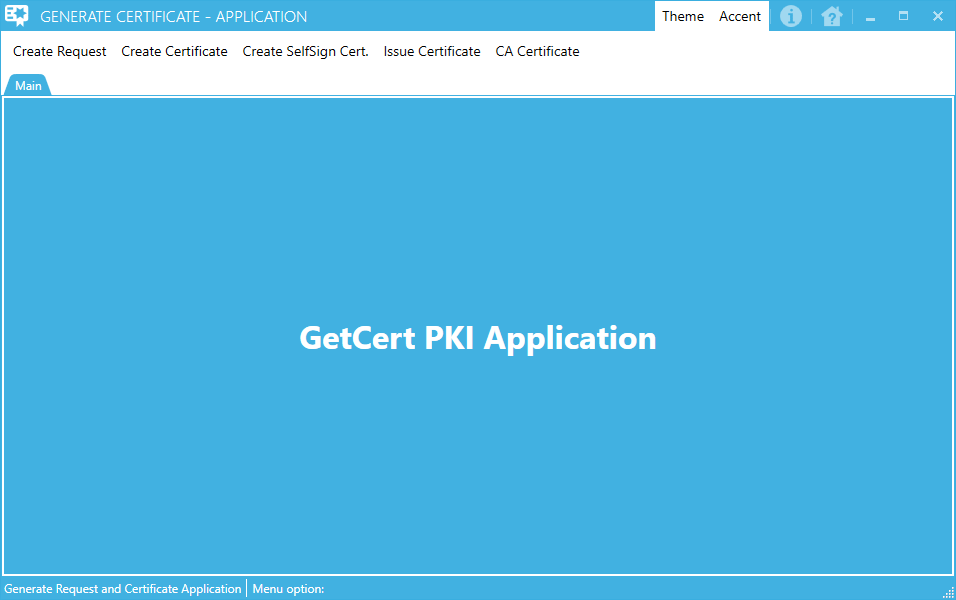
[9. Application requirements 53](#_Toc3808695)

# Introduction

This document describes how to use Generate Request and Certificate PKI Application (GenCert) application.

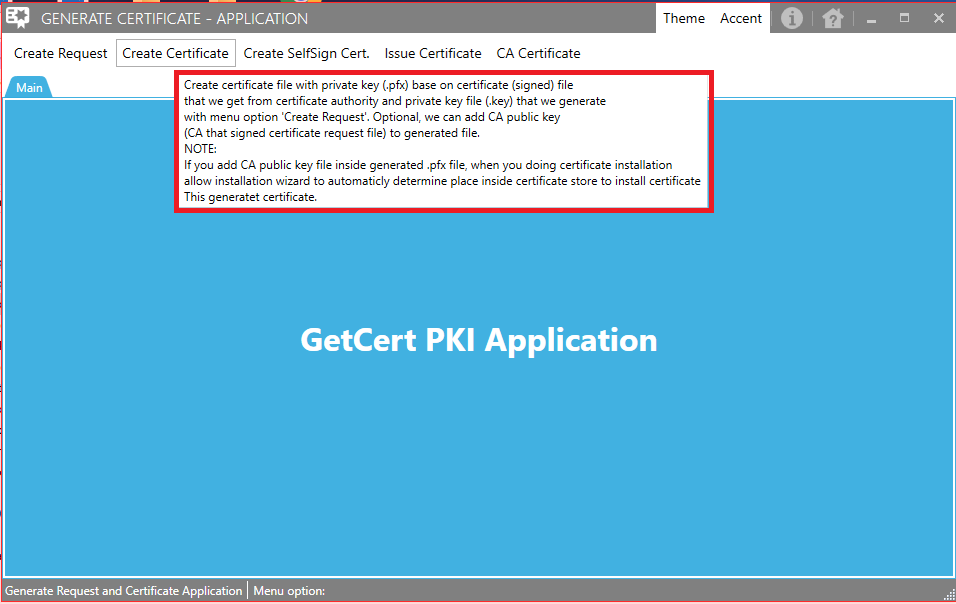
The application consists of 5 menu options:

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

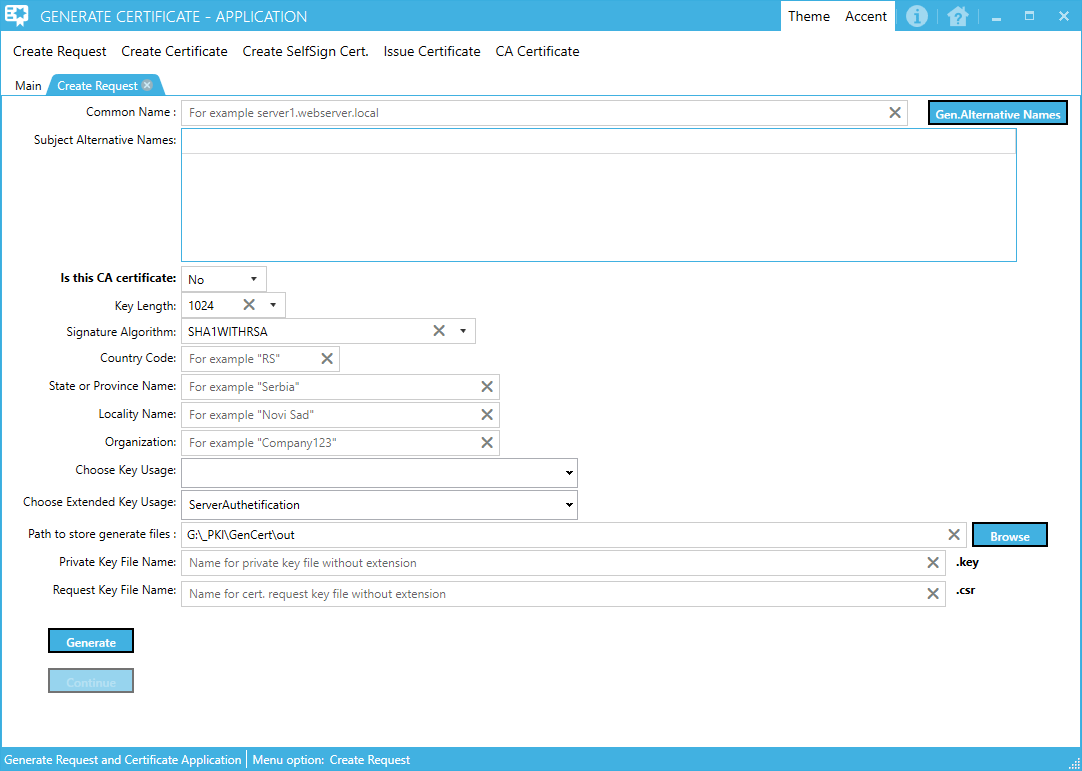


## User Interface

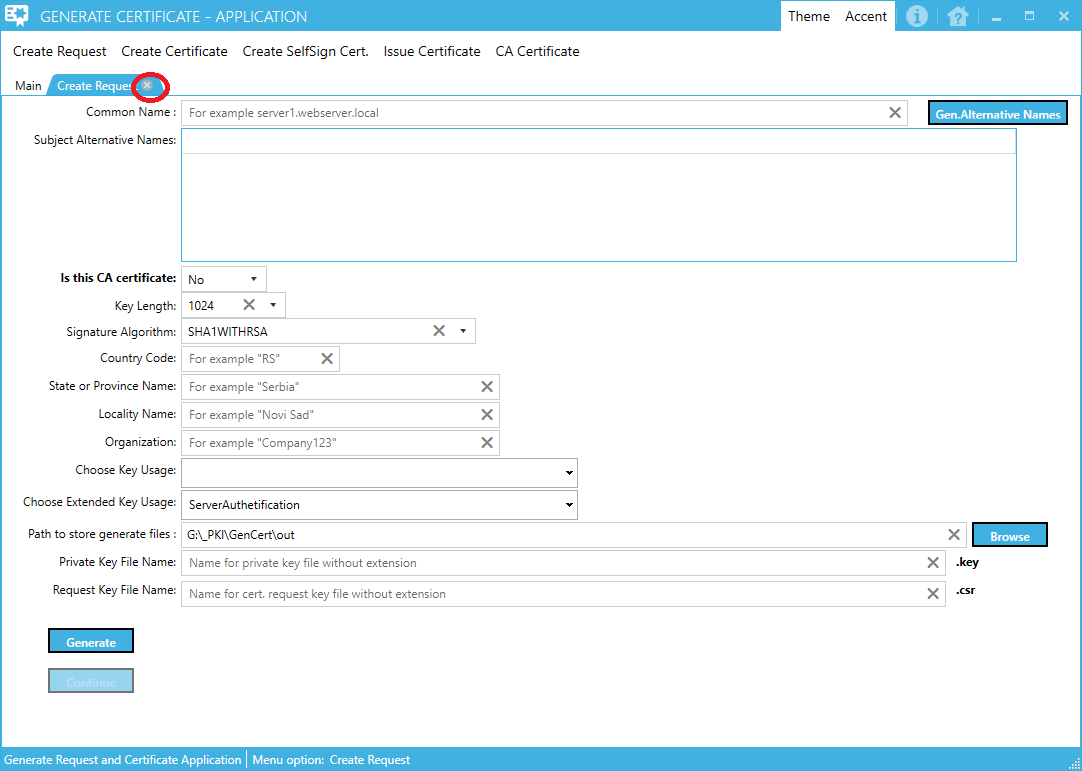
If you position mouse pointer over each menu option, you can get ToolTip help, what does that menu option do.



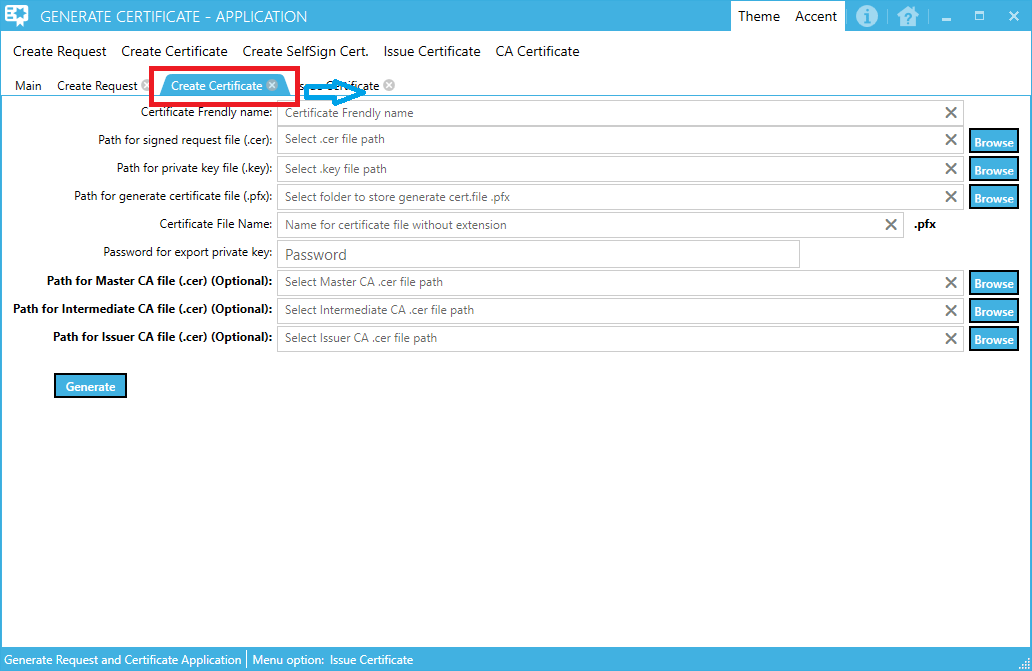
When you click on any menu option at the top of the window inside, appropriate form will be open inside new tab.

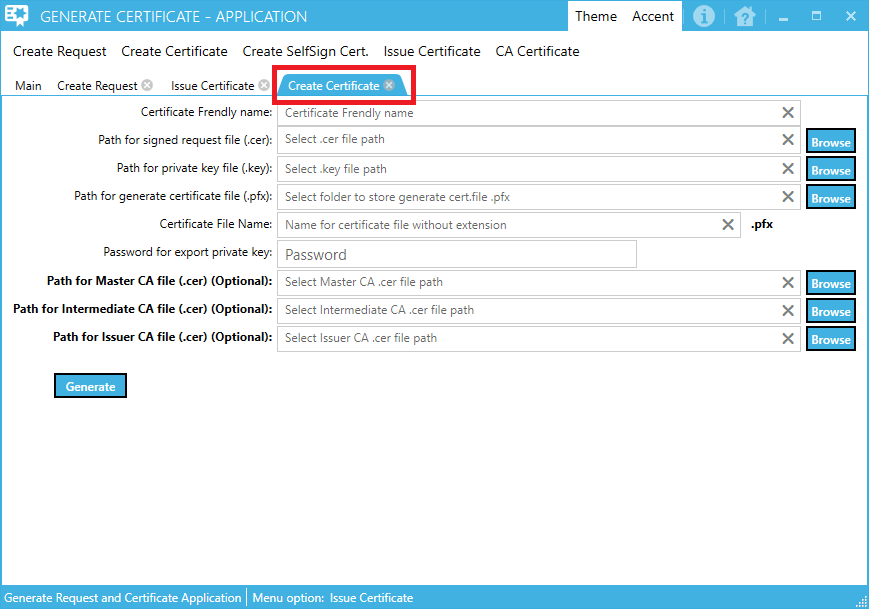


To close new opened tab, you can use ‘x’ circle inside each opened tab

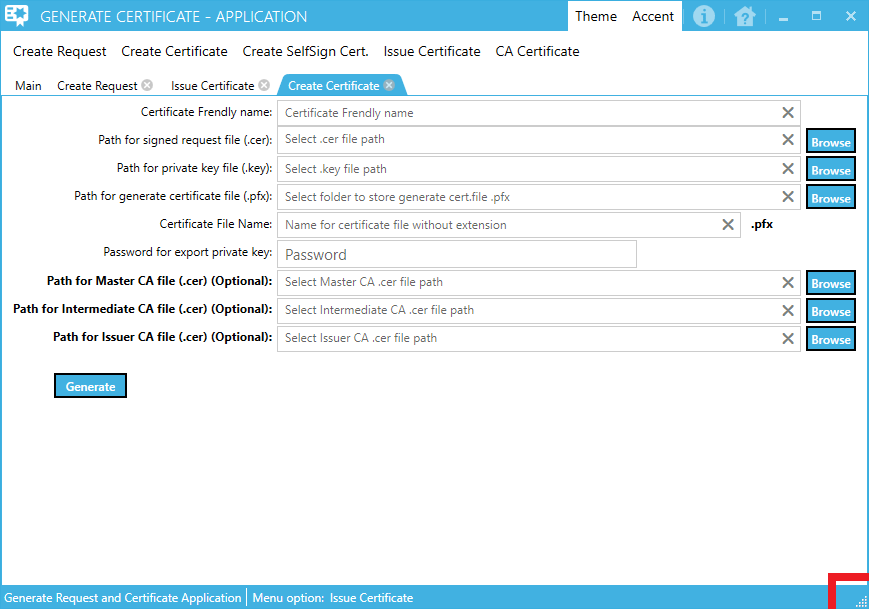


If you wish to reorder opened tab you can drag, move and drop each opened tab

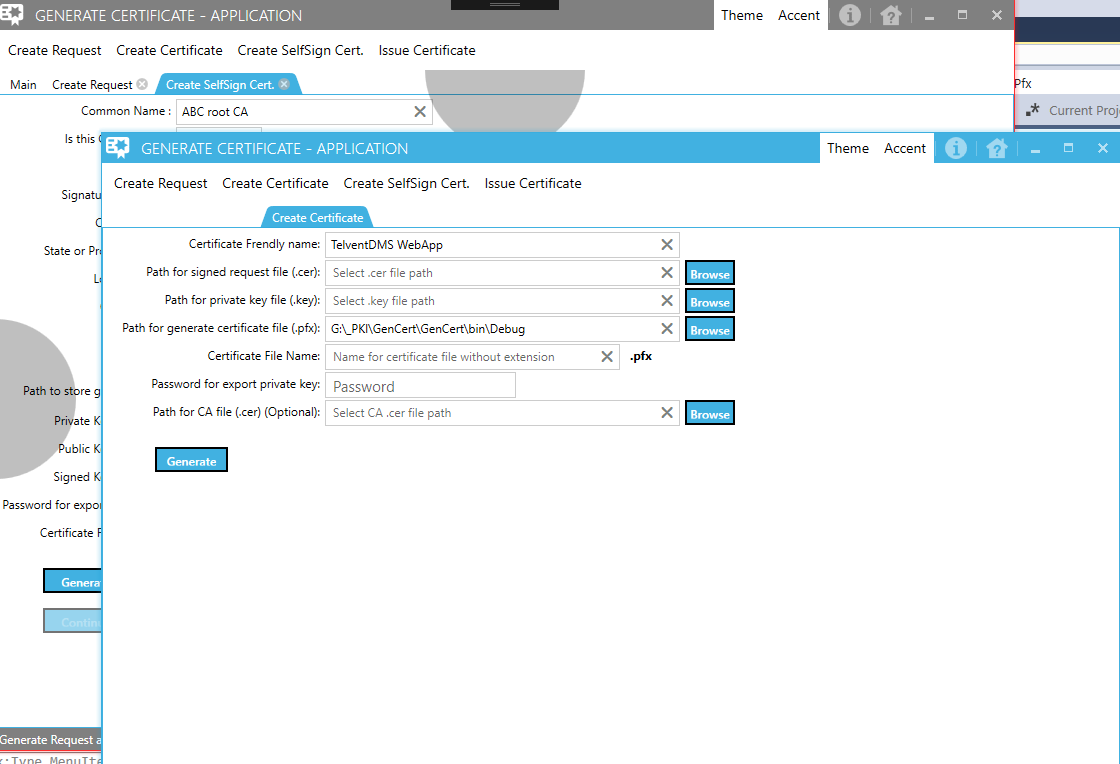


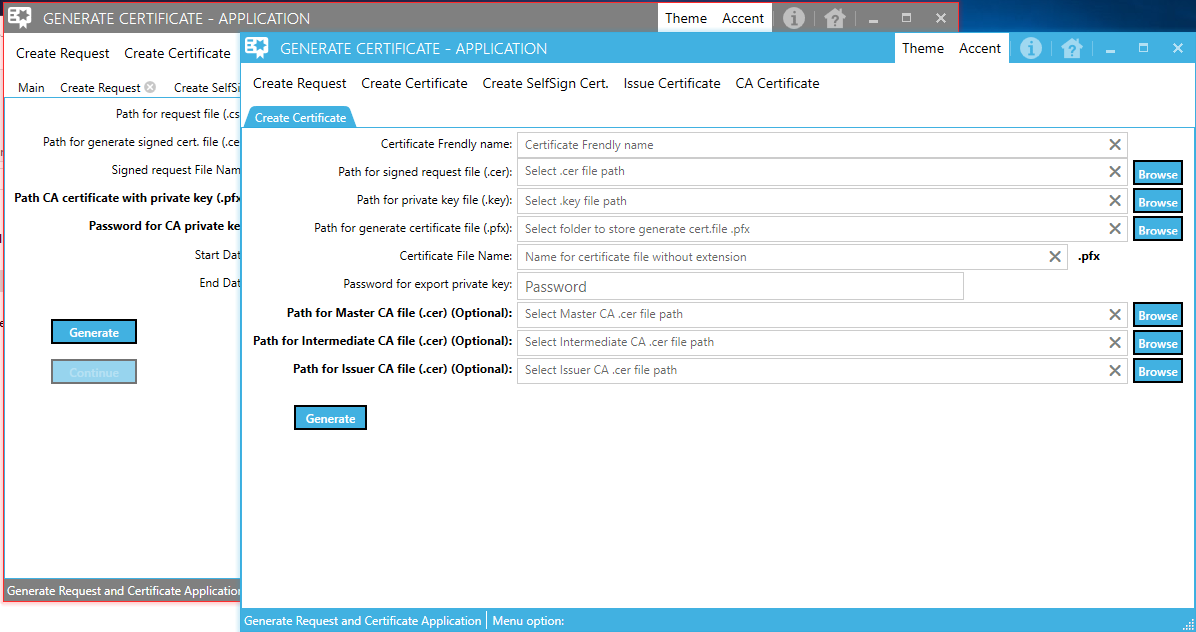


To resize application window, you can use grip inside down right corner of application window



You can drag and drop each opened tab inside main application window to totally new window by clicking on any tab, press left mouse button, hold and move tab outside the main application window.

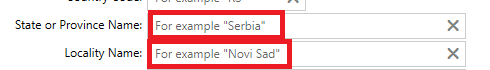




But, be careful, if you close any application window, all created application windows also will be closed.

On the open form for any menu option you will found different UI elements (textboxes, comboboxes, checkcomboboxes, passwords, ... etc.).

When textbox is empty, you will see watermark message as help, what you need to enter inside that textbox (picture below).



At the end of each textbox you will find “X” mark. If you enter some value inside textbox and after that you click on “X” mark at the end of that textbox, entered value inside textbox will be deleted (picture below).





When you click on textboxes that use to store value from Browse button, all content of that textboxes will be automatically selected (picture below)



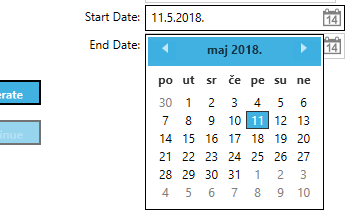
When you are entering value inside password box, you will see dot character instead of character you entered (picture below)



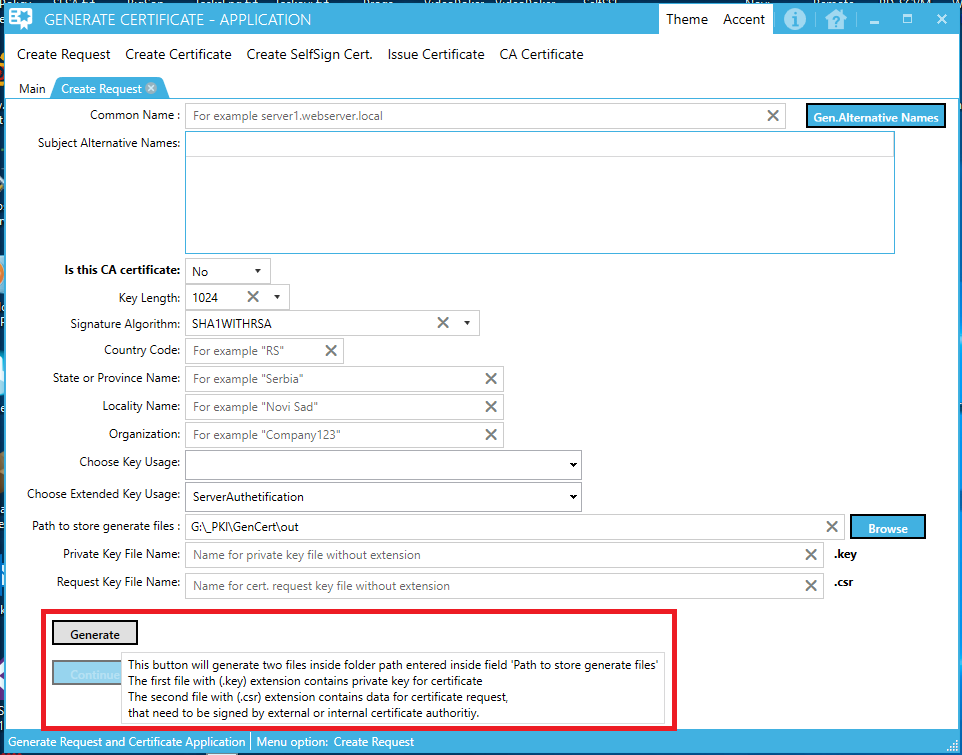
When password box has some value, at the end of password box you will see new mark “eye” . When you click on “eye” you will see real content inside password box (picture below)



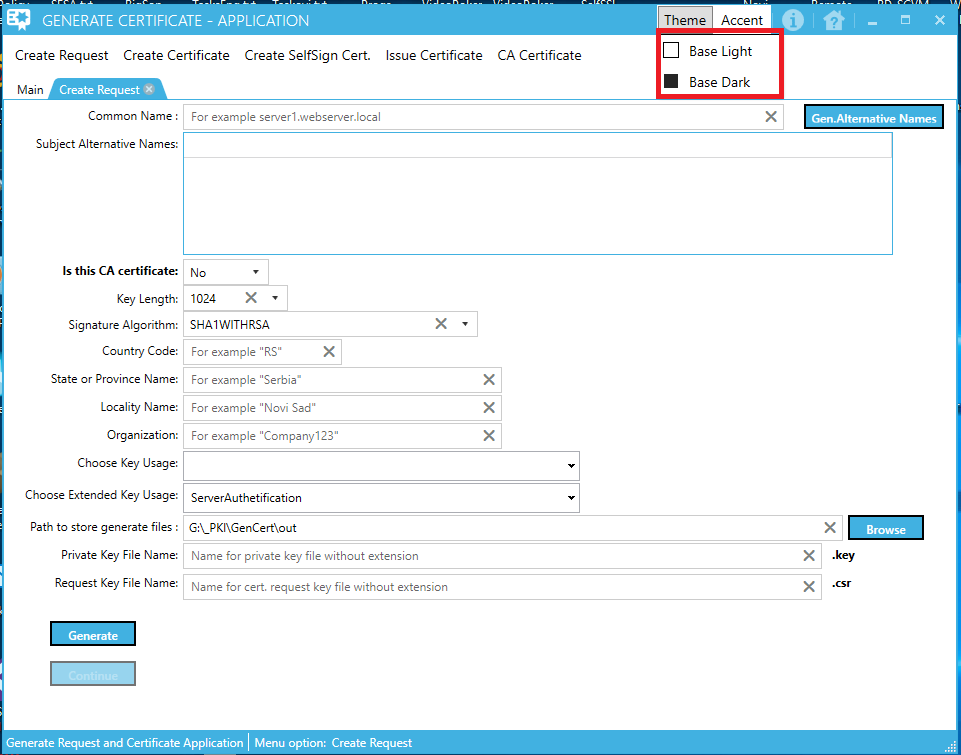
When you need to enter value for date field on the form, you can enter that value manually or click on calendar symbol at the end of date field and choose value (picture below)



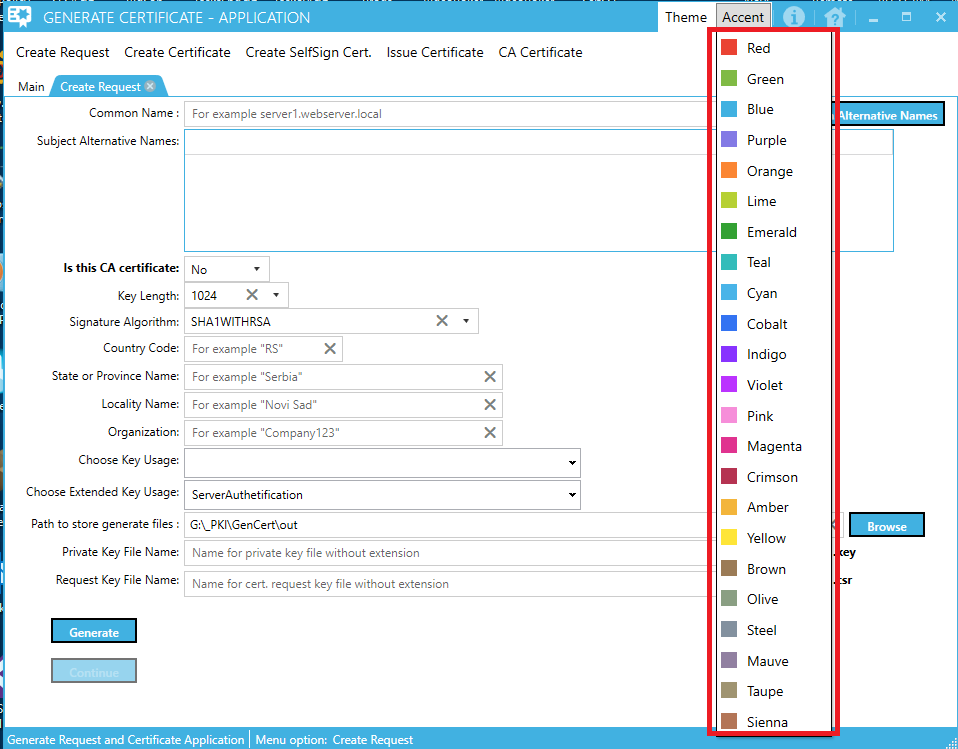
If you position mouse pointer over each button inside opened form, you will get help for current button under the mouse pointer. For example, mouse pointer located over button “Generate”, picture below:



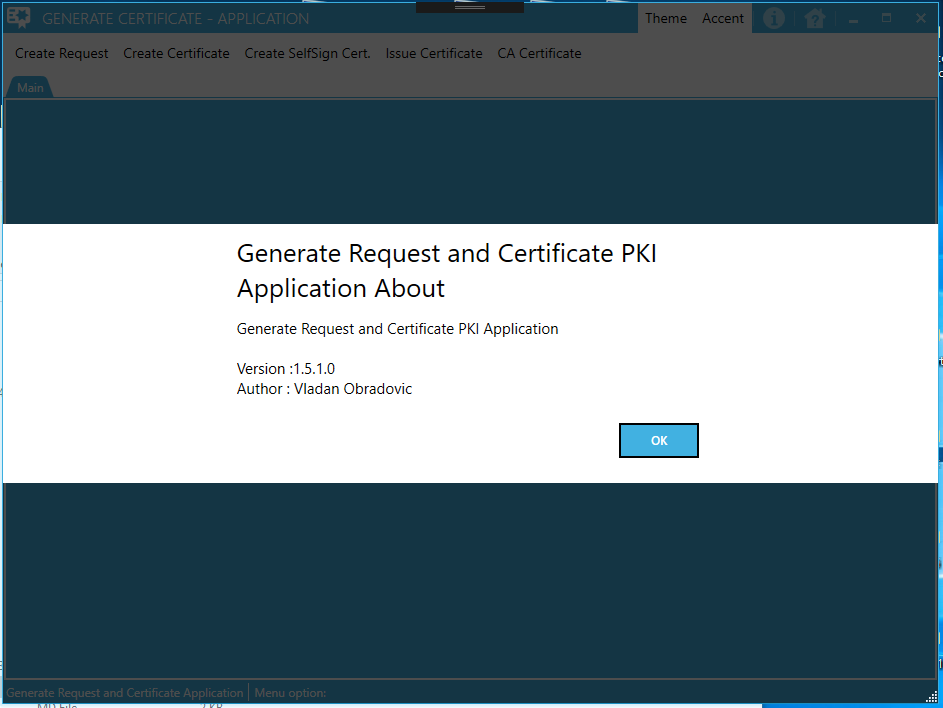
When you click on the Theme button on the application title bar, menu options for application themes will be open. You can choose between “Base Light” (see picture under) and “Base Dark” theme.



When you click on the Accent button on the application title bar, menu options for application color theme will be open. You can choose between 23 color themes.



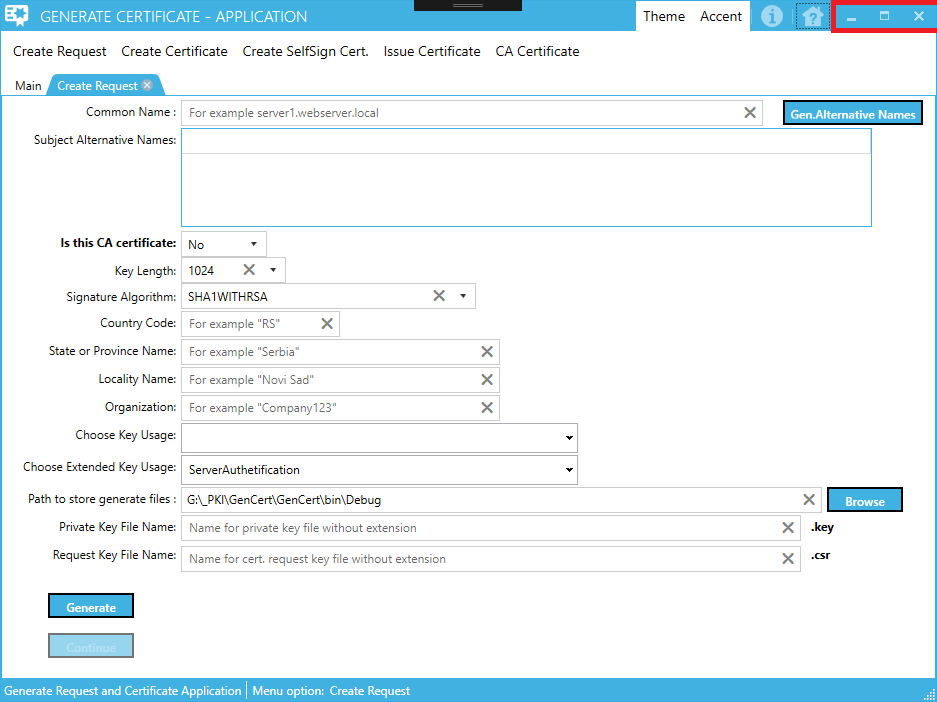
When you click on the Application Info button on the application title bar, application info will be open.



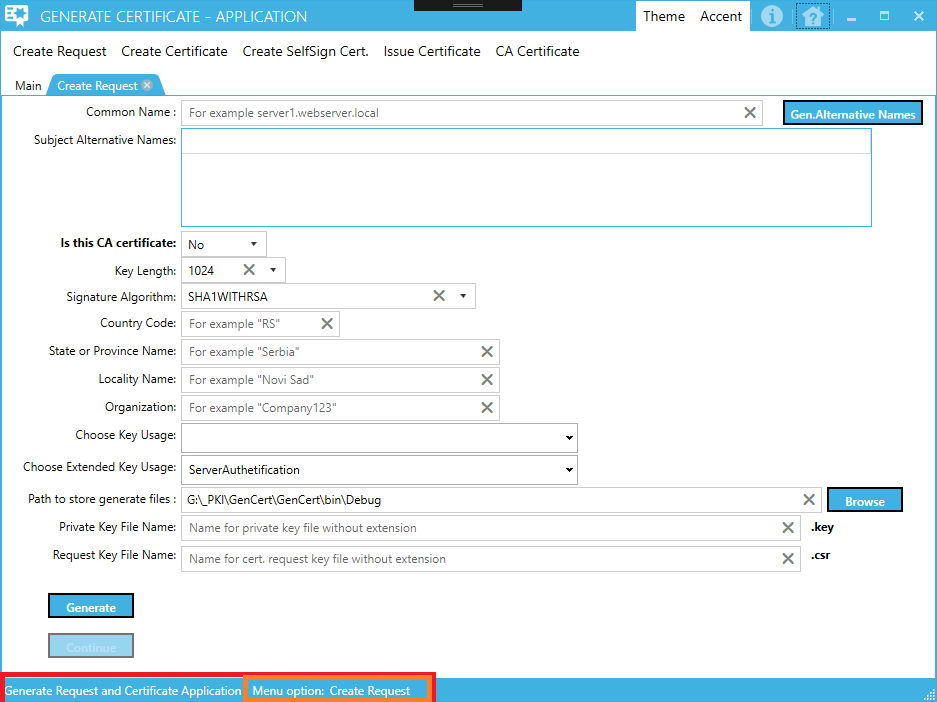
When you click on the Get Application Help button on the application title bar, application help in .chm format will be open.



When click on the main window command buttons (upper red rectangle in the picture below), you can minimize, maximize and close (exit) application.



Inside application status bar, you can see name of currently activated menu option (see picture below)



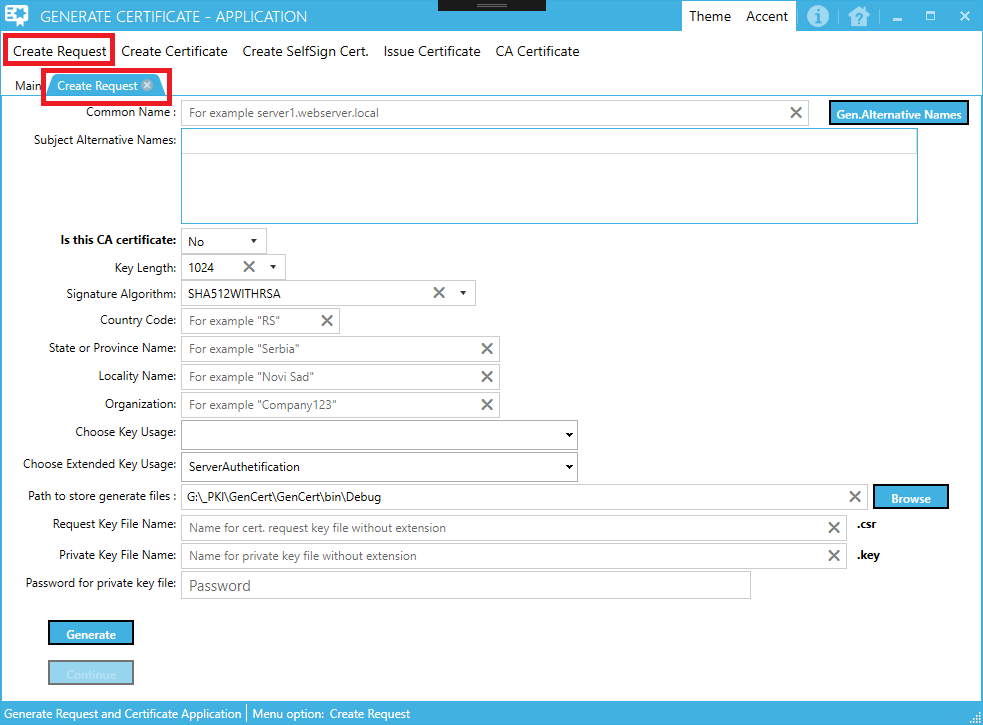
Inside windows task bar you can see application icon (see picture below)



# Create Request

This option is used to create certificate request file, that will be send to external certificate authority to be signed .

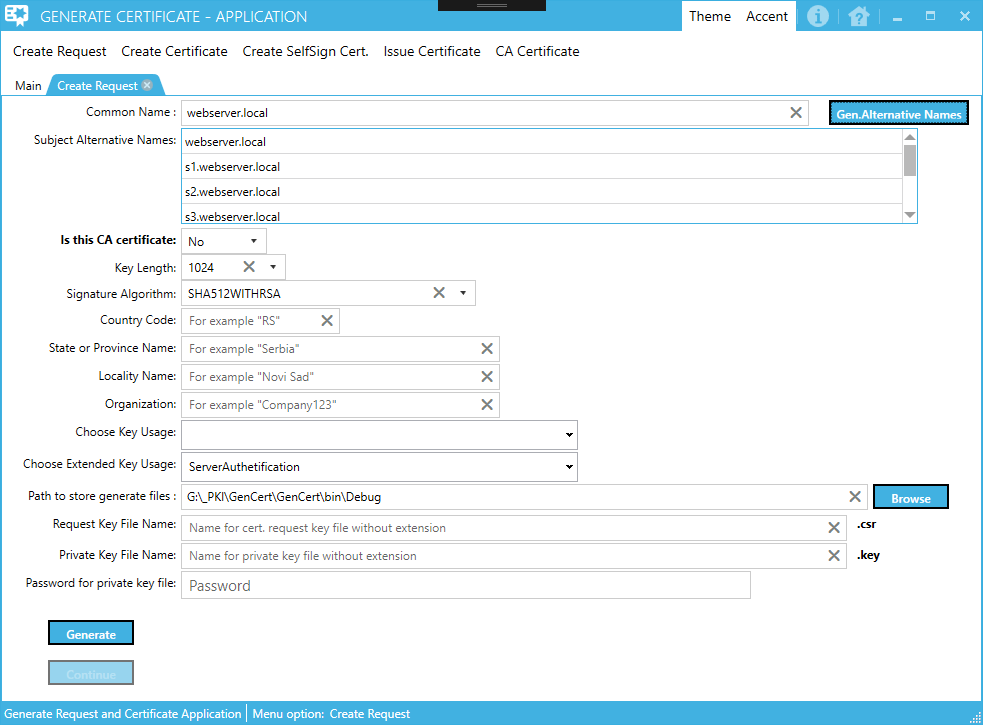
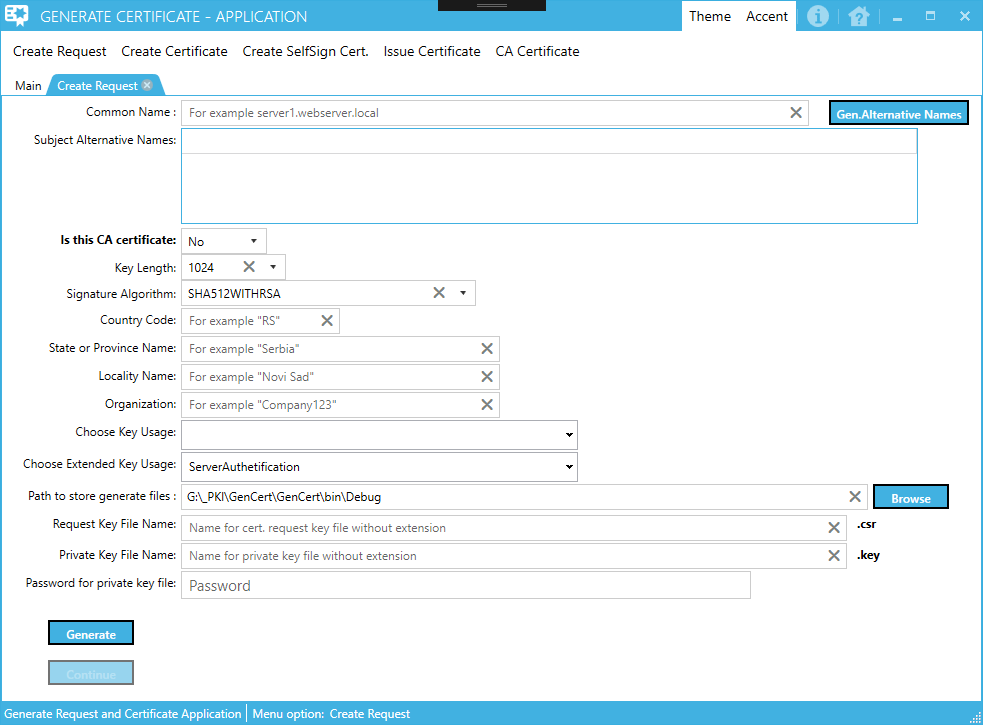




You need to fill all displayed fields on the form under before generate certificate request file. Some fields offer default value that can be changed. Another fields need to be fill with appropriate value(s).

Watermark inside fields that need to be fill with value(s) show example value for each field.

When enter value inside field "Common Name:" you can click on the button "Gen.Alternative Names" to generate alternative web server names to fill "Subject Alternative Names:" table or you can fill this table with alternative names manually. Or you can generate and then change names of generated alternative names.



**Tip:**

In field “Common Name:” you can enter value for field “Issued To”. This is what you can see when you open Certificate mmc console and look for certificate



When you fill all fields inside form click on the button “Generate” to create following files:

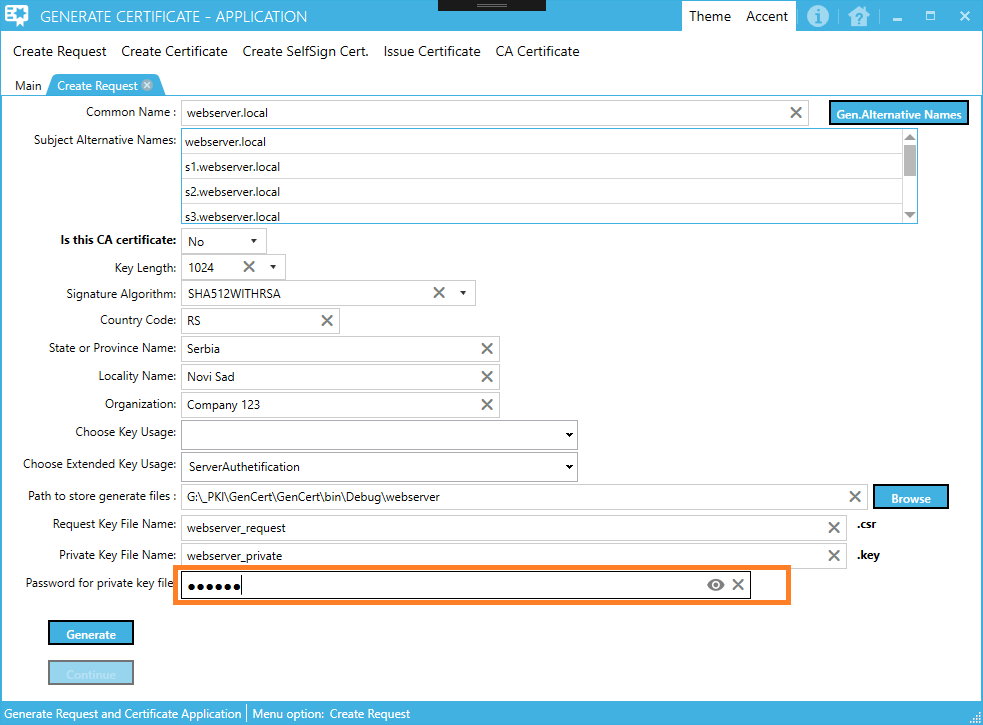
1.File with certificate private key (.key)

2.File with certificate request (.csr)

If everting is OK, form will be generated 2 files. Inside directory path entered inside field "Path to store generate files:", you will find two files. First file with .key extension (certificate private key file) and the second file with .csr extension (certificate request file).

**Tip:**

If you wish to add additional security to generated private key file, you can enter password inside field “Password for private key file” and that password will be used to encrypt data inside generated private key file. See the picture below (orange rectangle). This field is optional.

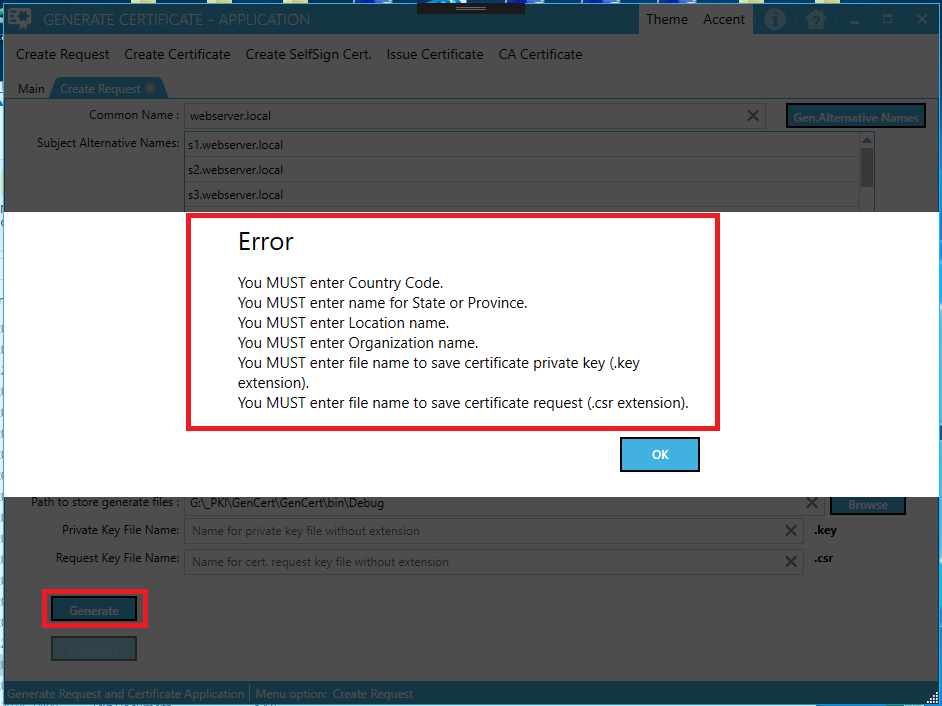


File with .csr extension need to be send to external certificate authority for signing and generate file with .cer extension. This file will be use lately to generate signed certificate file with private key (file with .pfx extension).

Also, you can generate own CA root authority certificate and sign certificate request file with generated CA root certificate (menu option "Create SelfSign Cert."), or if you already have generated CA root certificate file you immediately can proceed with sign certificate file with that root CA certificate (menu option "Issue Certificate").

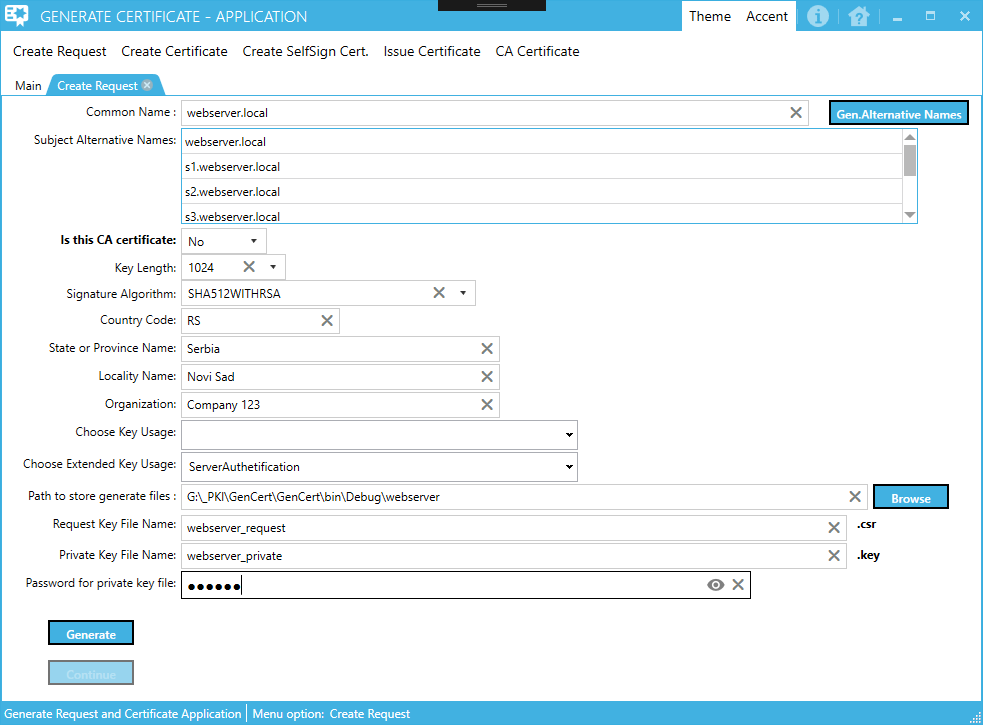
**NOTE:**

If data inside form not filled as need, you will get error screen, for example:

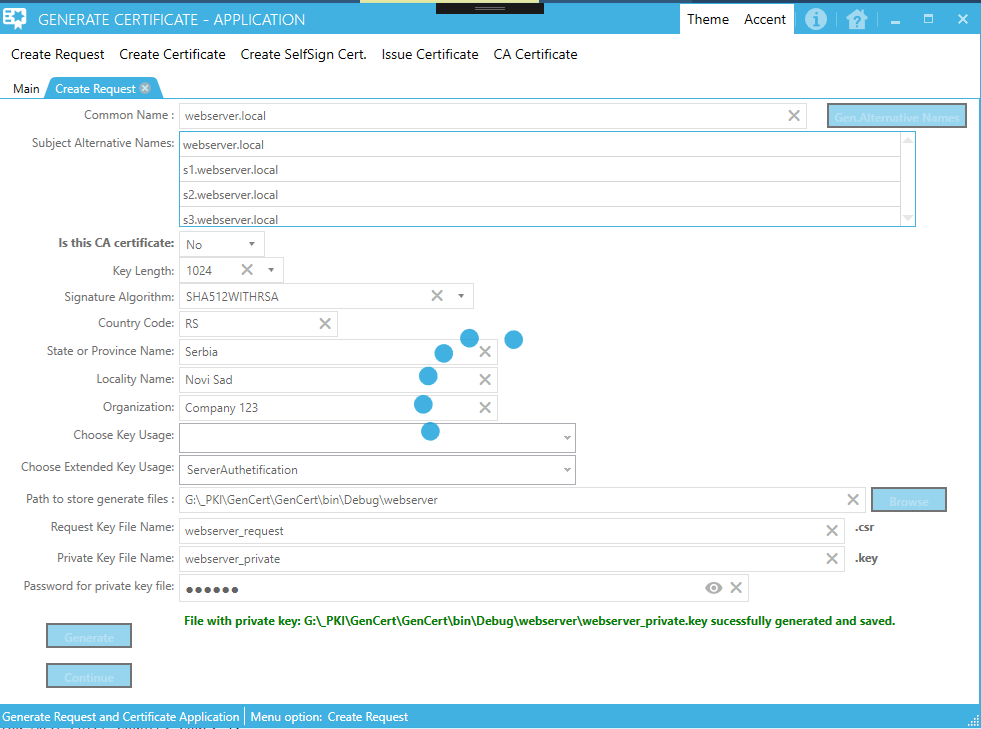


You need to fix all error messages and then try to generate certificate request file again.

If everything fills correctly on the form, when you press Generate button, two files (.key and .csr) will be generate and button “Continue” on the form will be enabled.



Click Generate





Messages shown upper, inside green rectangle, informing you that .key and .csr files has been generated.

**Tip:**

You can use Browse button to locate folder where generated files will be stored or you can enter path manually and if path not exist, that folders path will be created.

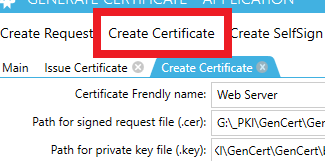
If you click on button Continue, new wizard dialog will be open.

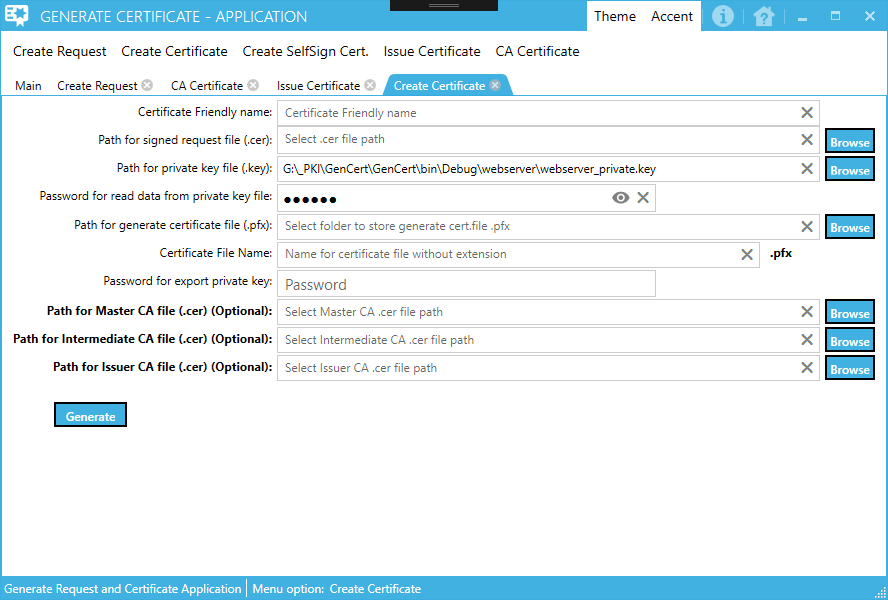


1. Option “Send to CA authority” will be use if you wish to send generated .csr file to internal or external CA authority for issuing
2. Option “Cancel” will close current dialog and return you to previous screen
3. Option "Sign locally-Don't have CA cert" will activate menu option "Create SelfSign Cert." and set value inside opened form "Is this CA certificate:"=Yes. We can use this option if we wish to generate certificate for CA root authority that we will use to sign certificate request (.csr) file
4. Option "Sign locally-Have CA cert" will activate menu option "Issue Certificate" to sign certificate request file (.csr) with previously generated CA root authority certificate (option "Create SelfSign Cert.").

# Create Certificate

This option is used to create certificate request file, that will be send to external certificate authority to be signed.





You need to fill all displayed fields on the form under before generate file signed certificate file with private key.

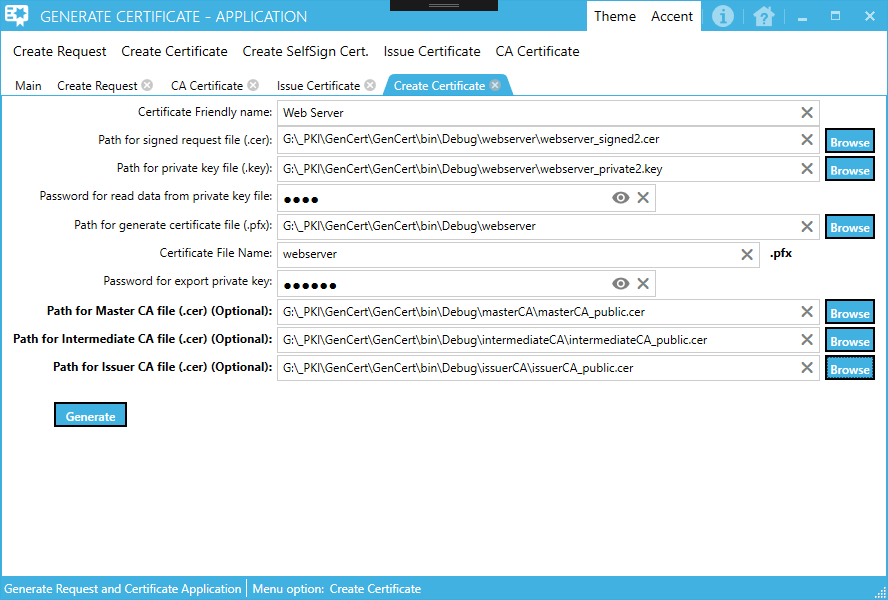
You can enter data manually or click on the “Browse” buttons to select appropriate files and output directory where generate file (.pfx extension) will be generate.

Inside field "Password for export private key:" you need to enter password that will be use when import data for generated certificate file to computer store. When enter data inside this field, you will see black dots. When click on the right icon on right inside this field, you will see what you typed.

Watermark inside fields show help message what kind of data need to be enter to each field.

**Tip:**

You can use Browse button to locate folder where generated files will be stored or you can enter path manually and if path not exist, that folders path will be created.



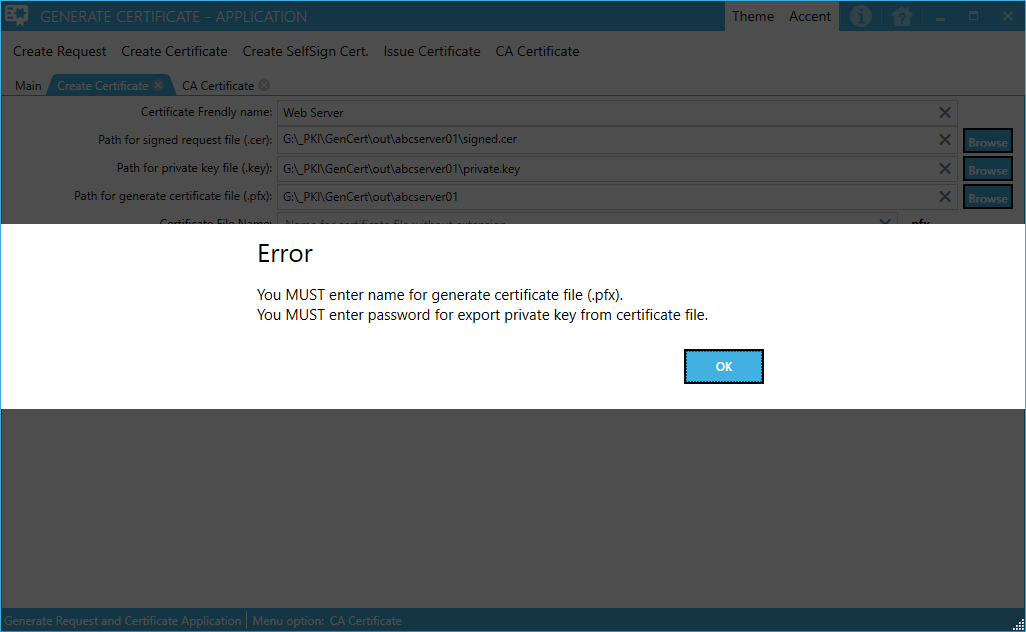
When you fill all fields inside form click on the button “Generate” to create files.

If everting is OK, form will generate certificate file with private key Inside directory path entered inside field "Path for generate certificate file (.pfx):".

This file and external CA public key file need to be installed inside computer store on each computer that will access web server.

**NOTE:**

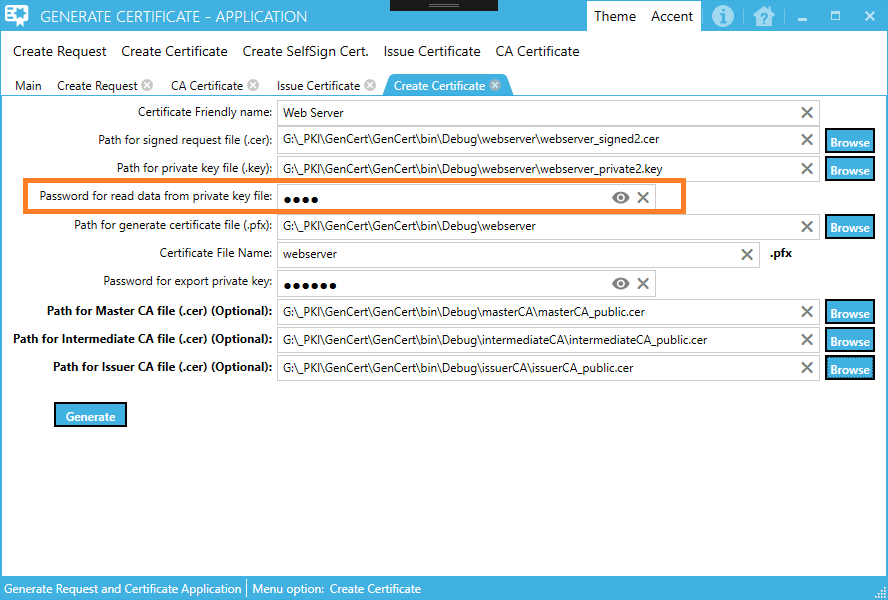
If data inside form not filled as need, you will get error screen, for example:



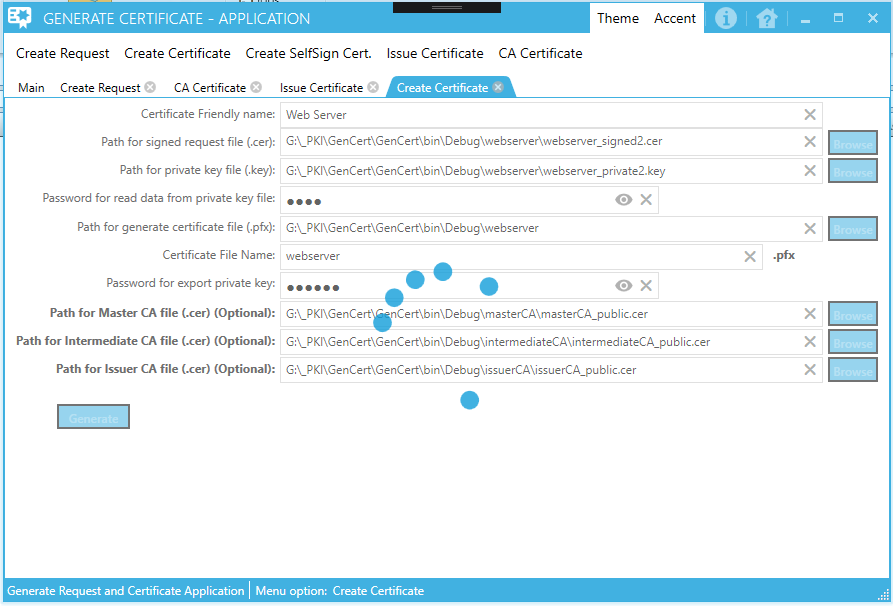
You need to fix all error messages and then try to generate certificate request file again.

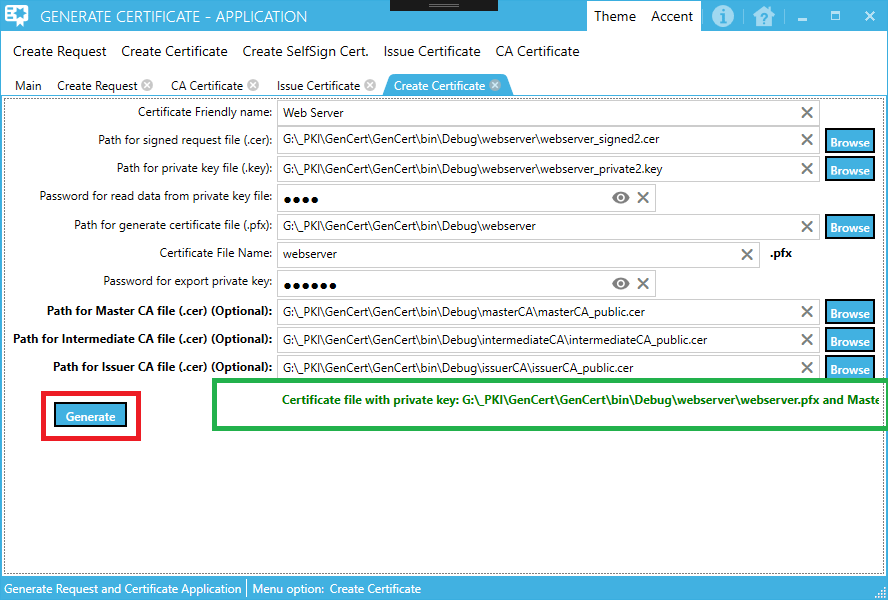
**Tip:**

If you previously generated private key file and protected it with password, you must enter that password inside field “Password for read data from private key file”. See picture below (orange rectangle).



You can use Browse button to locate folder where generated files will be stored or you can enter path manually and if path not exist, that folders path will be created.



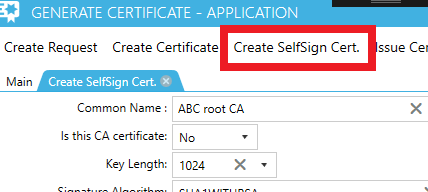


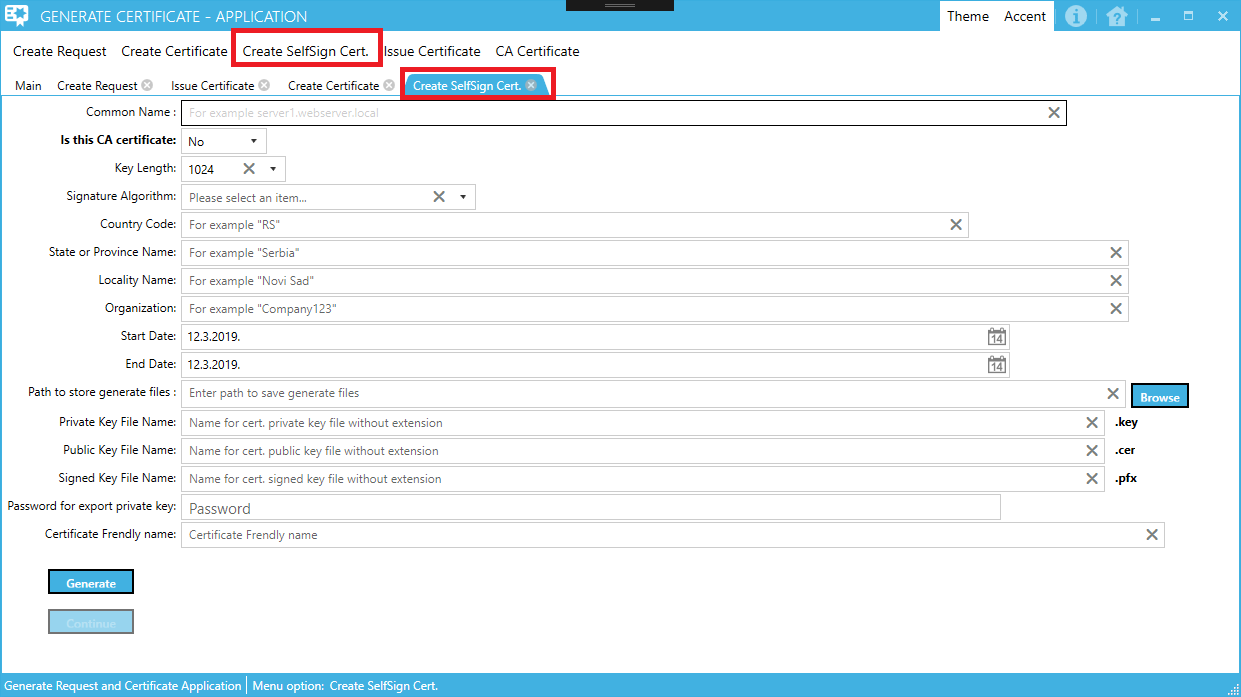
Generated .pfx file, now can be import to appropriate computer certificate store.

See chapter 7, how to import data from generated certificate file to computer certificate store.

# Create SelfSign Cert.

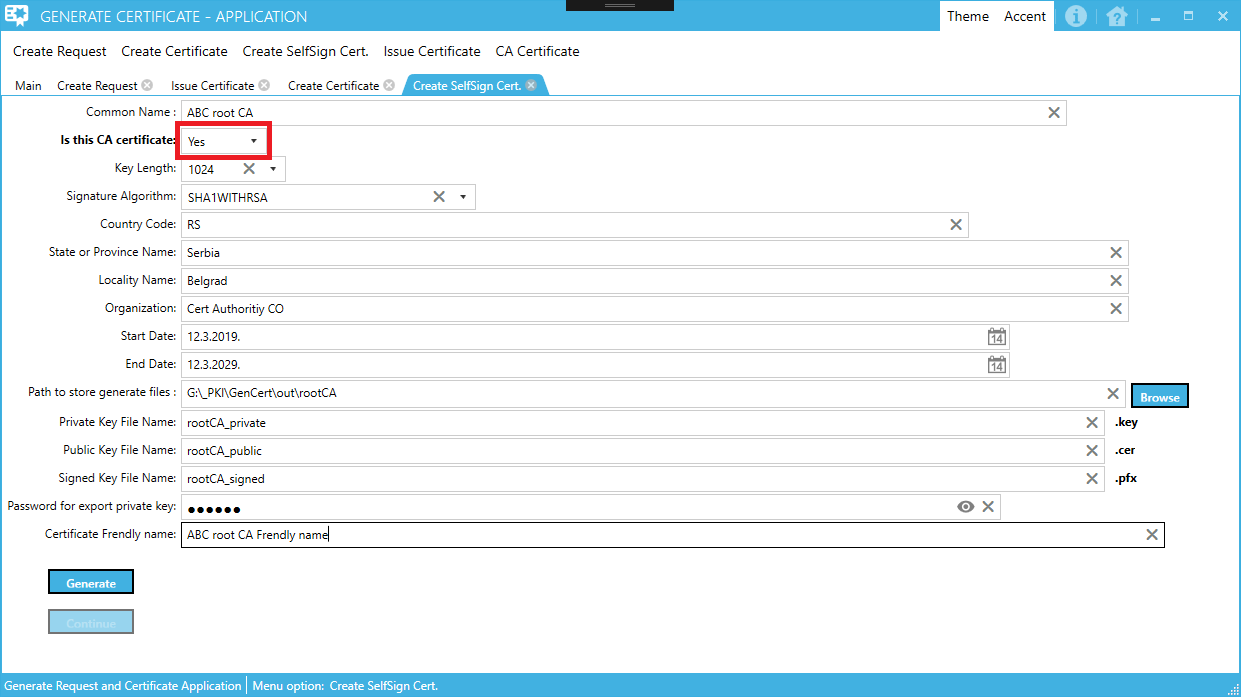
This option is used to create self-sign certificate or create self-sign certificate for CA root.





You need to fill all displayed fields on the form over before generating self-sign certificate file.

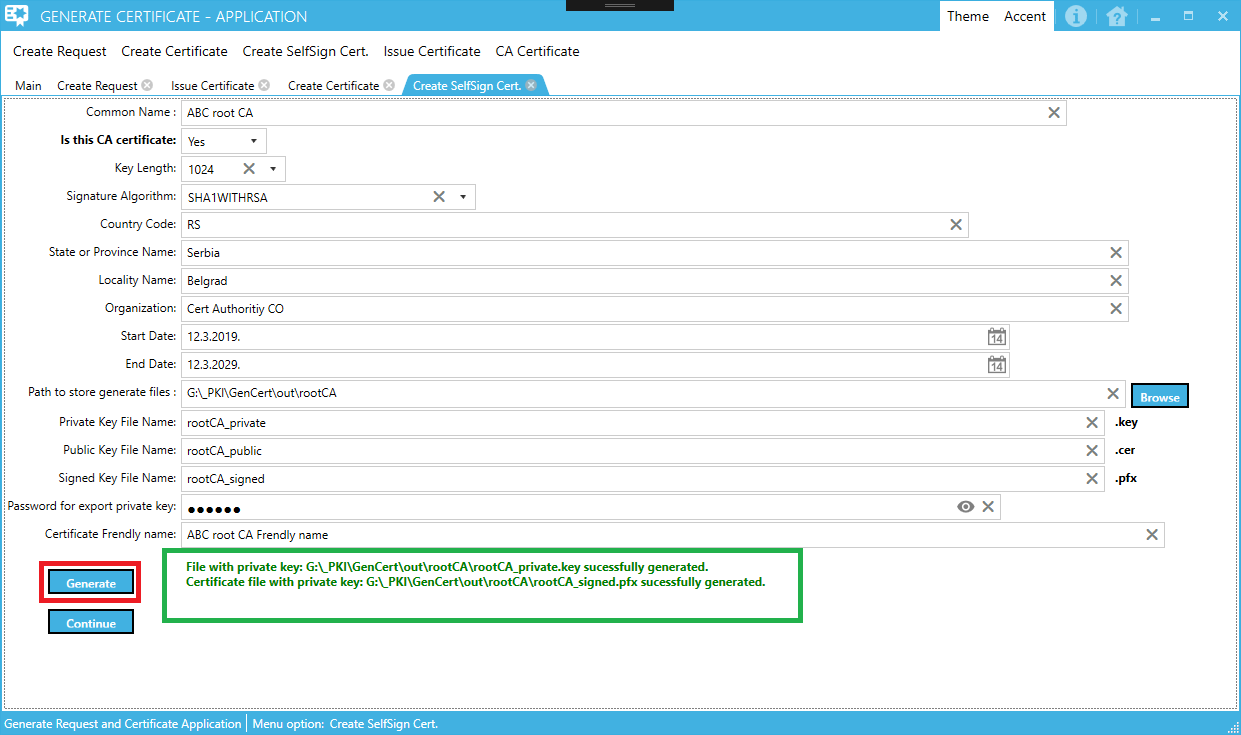
If you use option “Is this CA certificate”=Yes, generated certificate file can be use as CA root certificate.



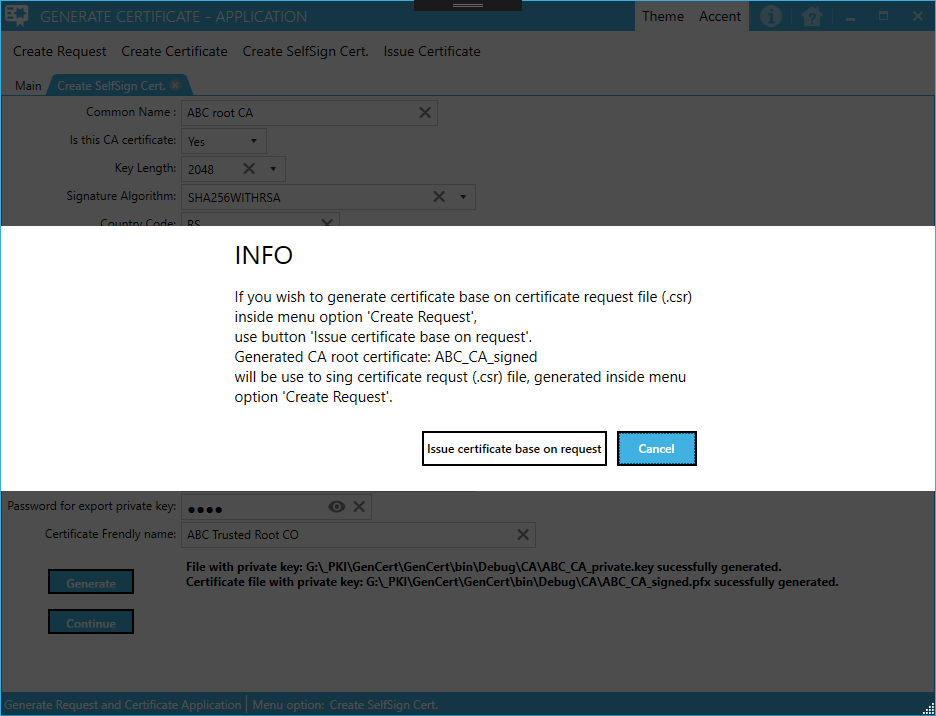
When you click on Generate, application will generate 3 files:

1. File with certificate private key (.key)
2. File with certificate public key (.cer)
3. File with private and public key (.pfx)

If all files successfully generated and you choose Yes value for field "Is this CA certificate", button Continue will be enabled.



If you click Continue button, you will get dialog wizard to explain what to do next.



If you use option "Create Certificate base on generated (.cer) file", this will activate menu option "Create Certificate" and automatically fill all fields with appropriate value:

"Path for signed request file (.cer):"

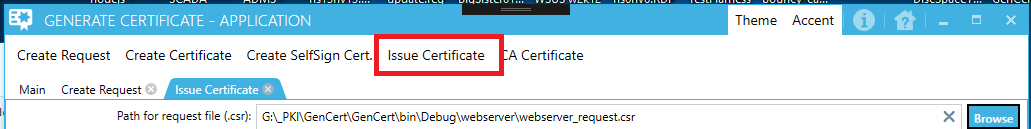
"Path for private key file (.key):"

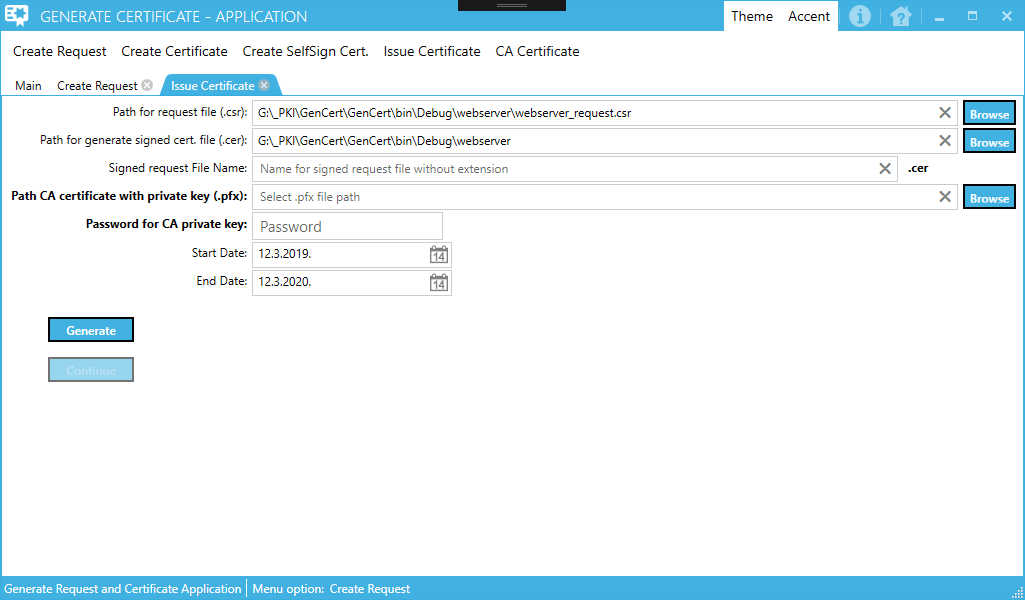
"Path for generate certificate file (.pfx):"

"Path for CA file (.cer) (Optional):"

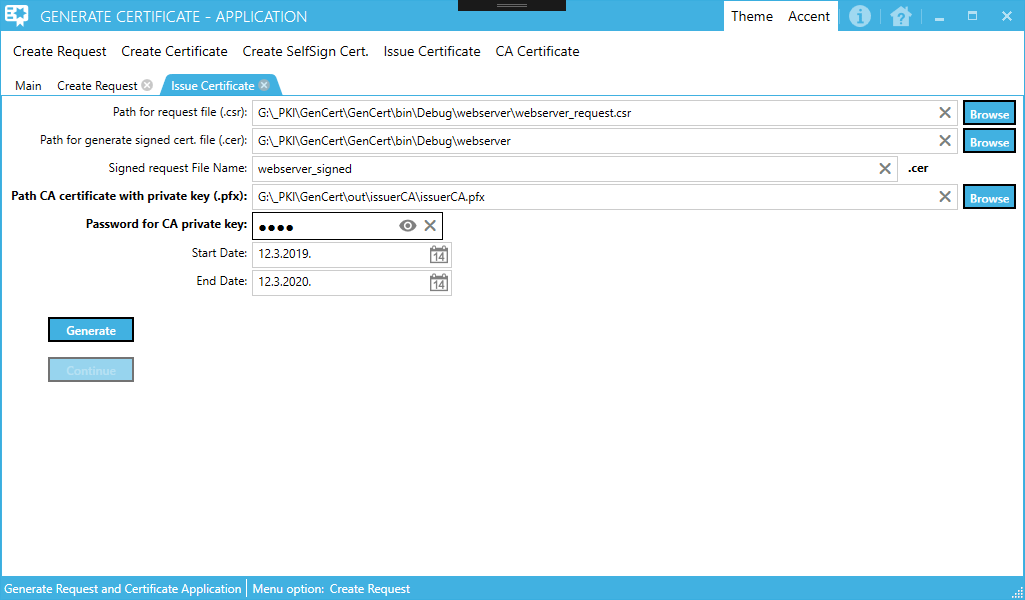
# Issue Certificate

This option is used to create signed certificate file base on request certificate file which will be signed by generated CA root certificate file inside menu option "Create SelfSign Cert.".



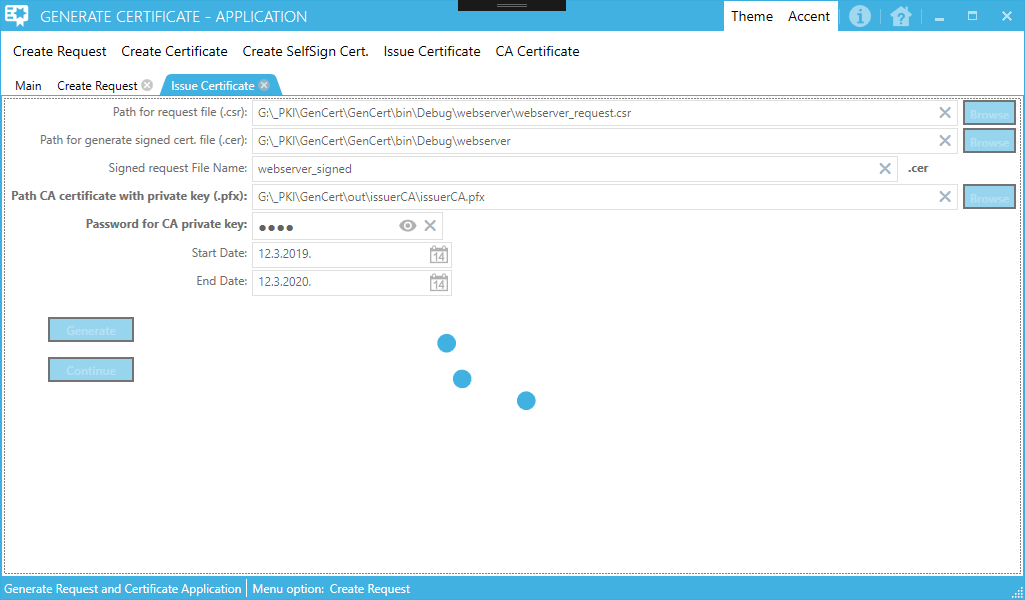


You need to fill all displayed fields on the form over before generating certificate signed file.

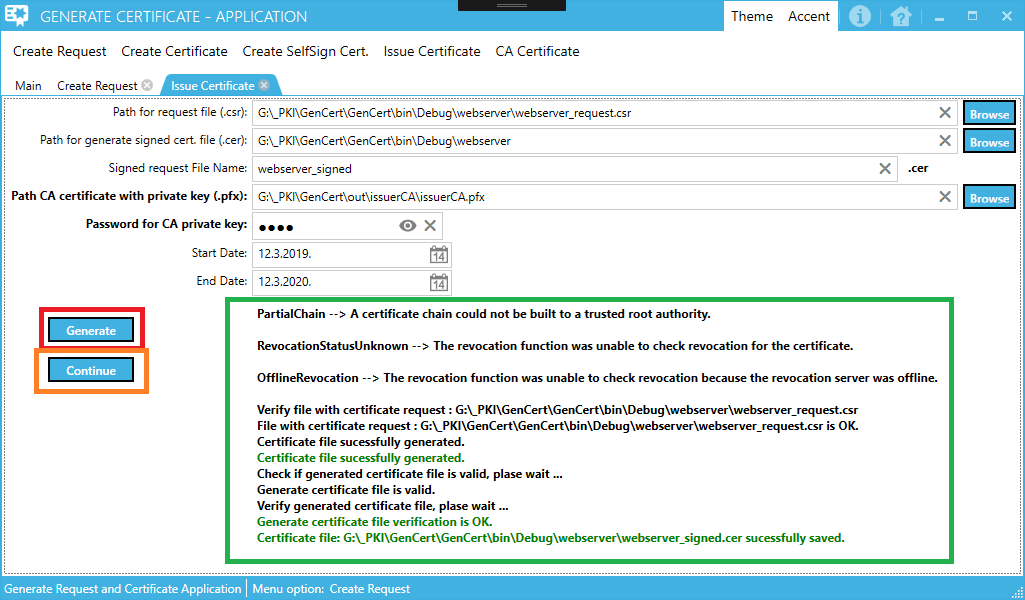


When you click on Generate, application will generate file:

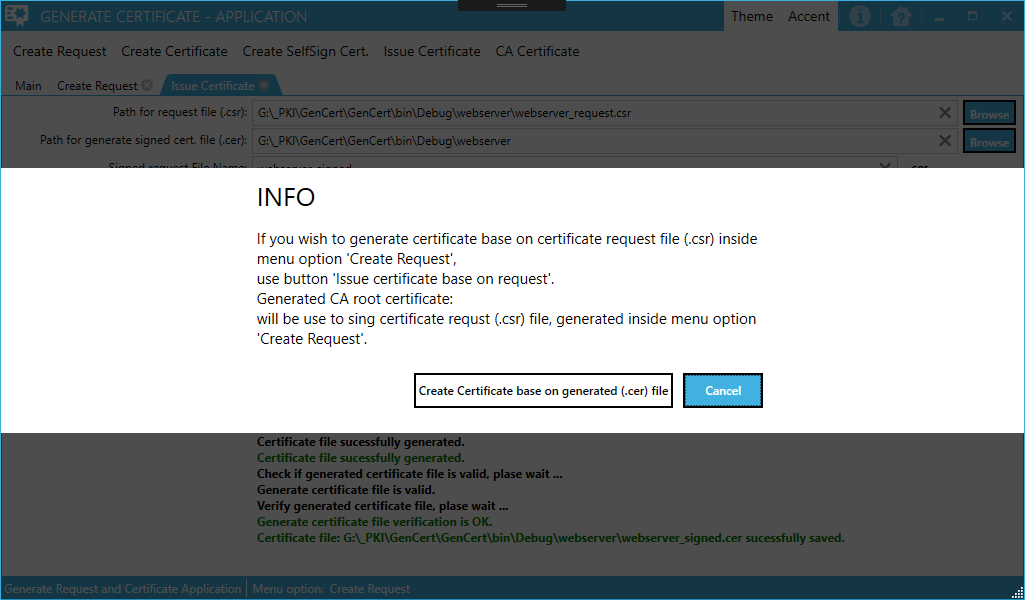
File with certificate public key (.cer)



If all files successfully generated, button Continue will be enabled.

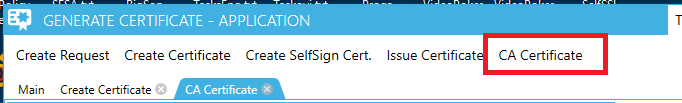


If you click Continue button, you will get dialog wizard to explain what to do next.



# CA Certificate

This option is used to create signed certificate file base on request certificate file which will be signed by generated CA root certificate file inside menu option "Create SelfSign Cert.".



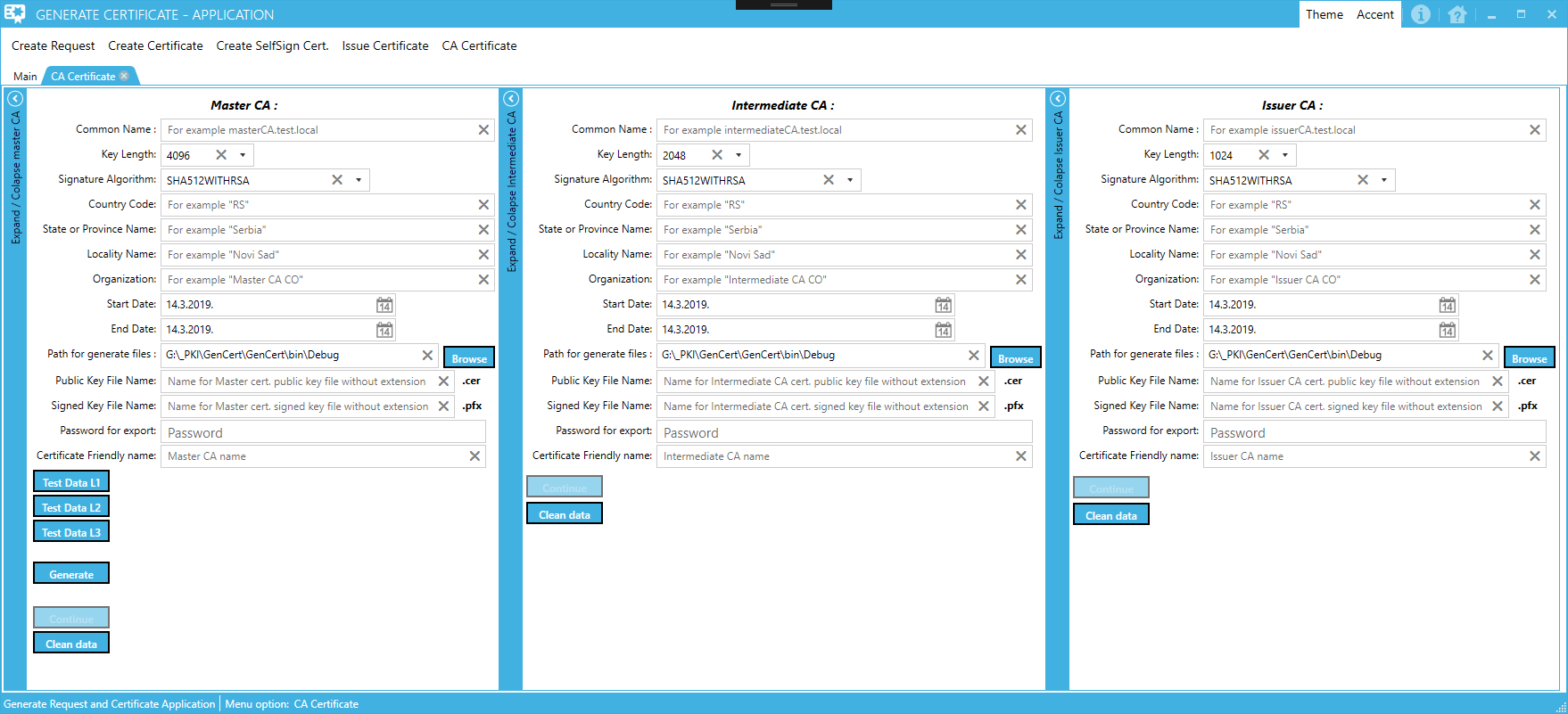


This form has tree expander form parts.

The first expander form can be used to enter data for master CA (usually this is workgroup computer, keep as offline).

The second expander form can be used to enter data for intermediate CA (usually this computer is part of some Active Directory domain, always online – for II level CA infrastructure, use to issue certificate for computers and users, for III level CA infrastructure, use to issue certificate for issuer CA server).

The third expander form can be used to enter data for issuer CA (usually this computer is part of some Active Directory domain, always online – for III level CA infrastructure, use to issue certificate for computers and users).



Buttons:

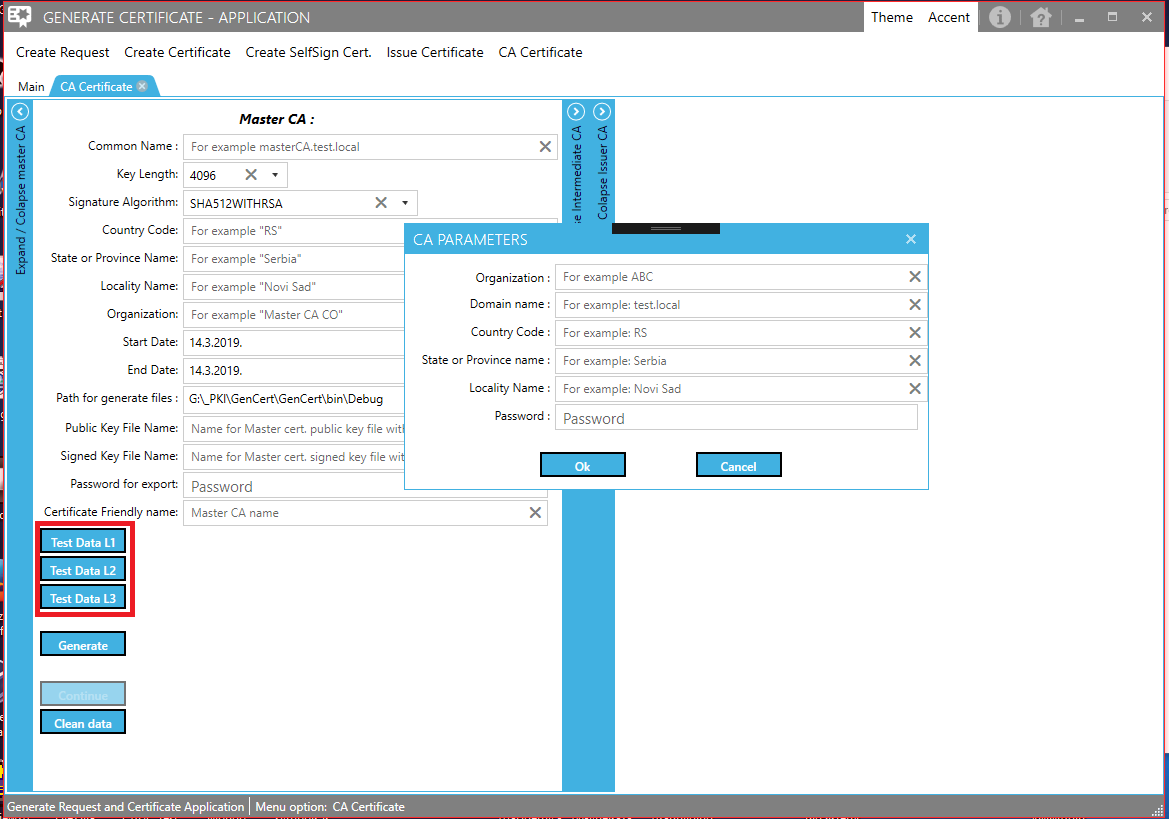
"Test Data L1" - This button will fill master CA form with entered data. Use this button if you generate only mater CA certificate to sign certificate request

"Test Data L2" - This button will fill master CA + intermediate CA forms with entered data. Use this button if you generate mater CA + intermediate CA certificates to sign certificate request

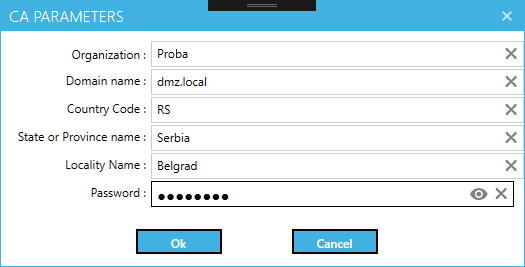
"Test Data L3" - This button will fill master CA + intermediate CA + issuer CA forms with entered data. Use this button if you generate mater CA + intermediate CA + issuer CA certificates to sign certificate request

"Clean data" - This button will clean entered data on current form

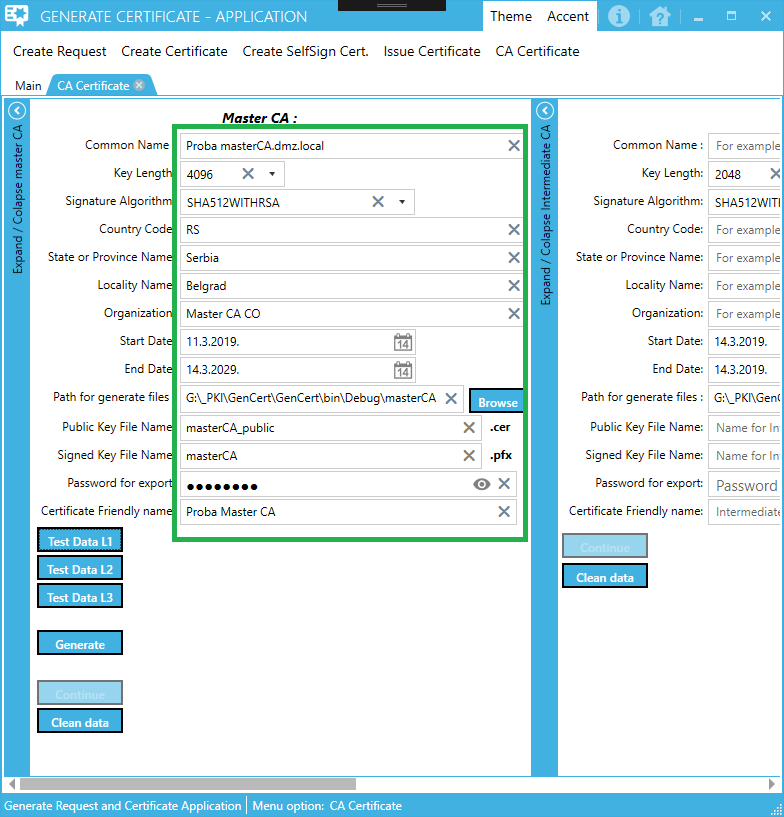
When click one of “Test Data” buttons, application will open new form to enter data that will be used to automatically generate data these need to generate appropriate certificates files.

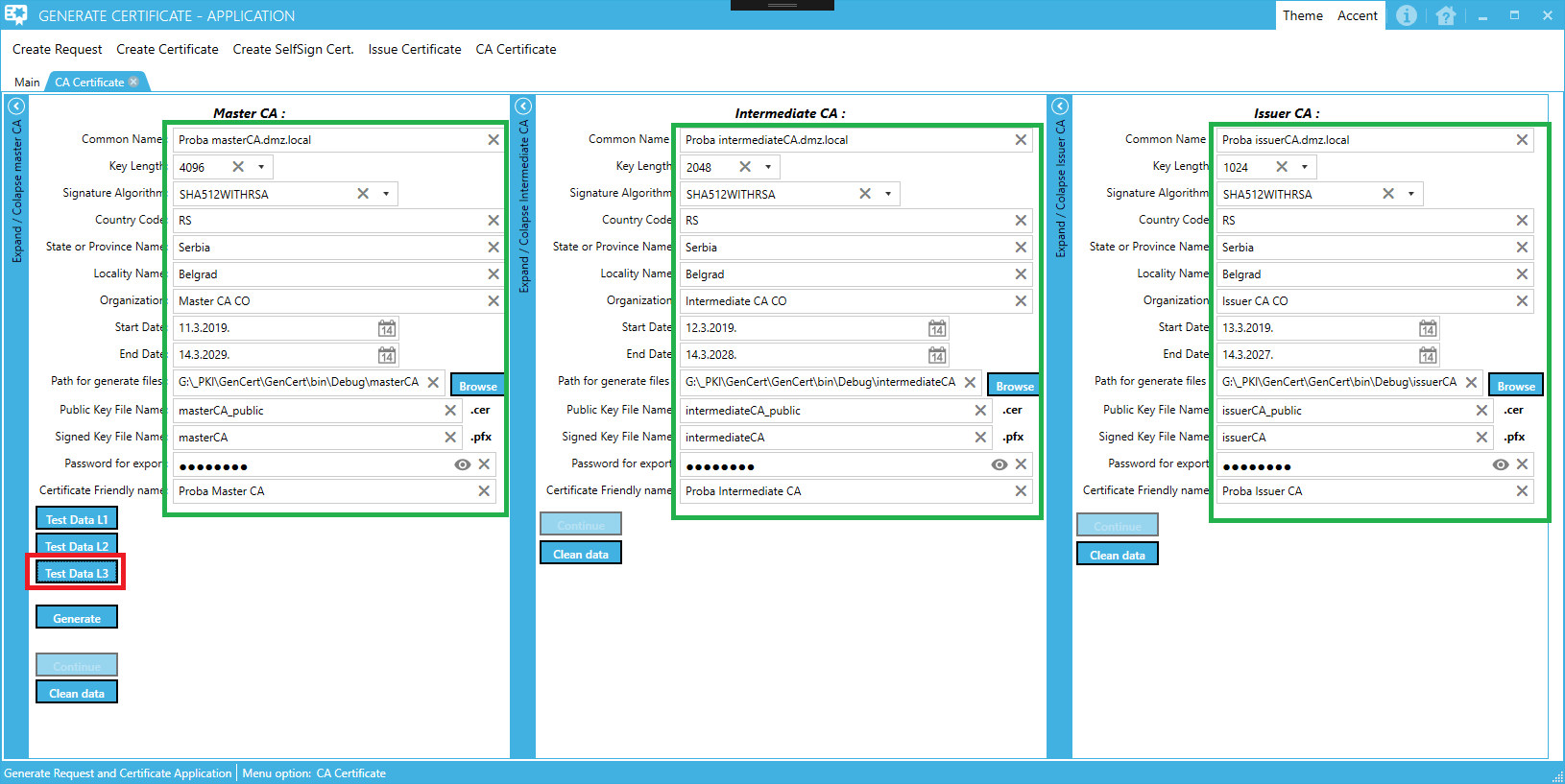


On opened form for “CA PARAMETERS”, enter data and press “Ok” button to continue.

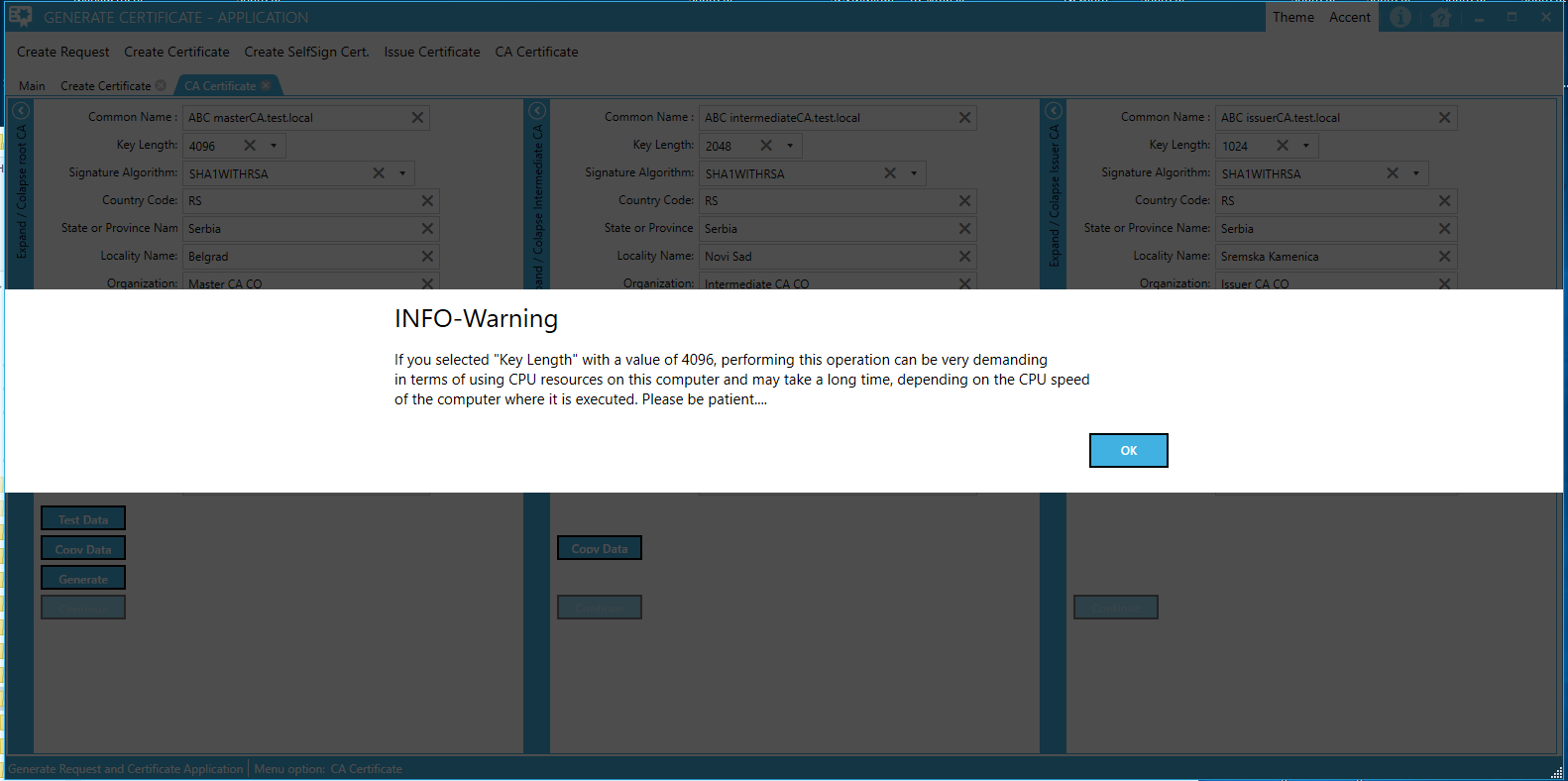


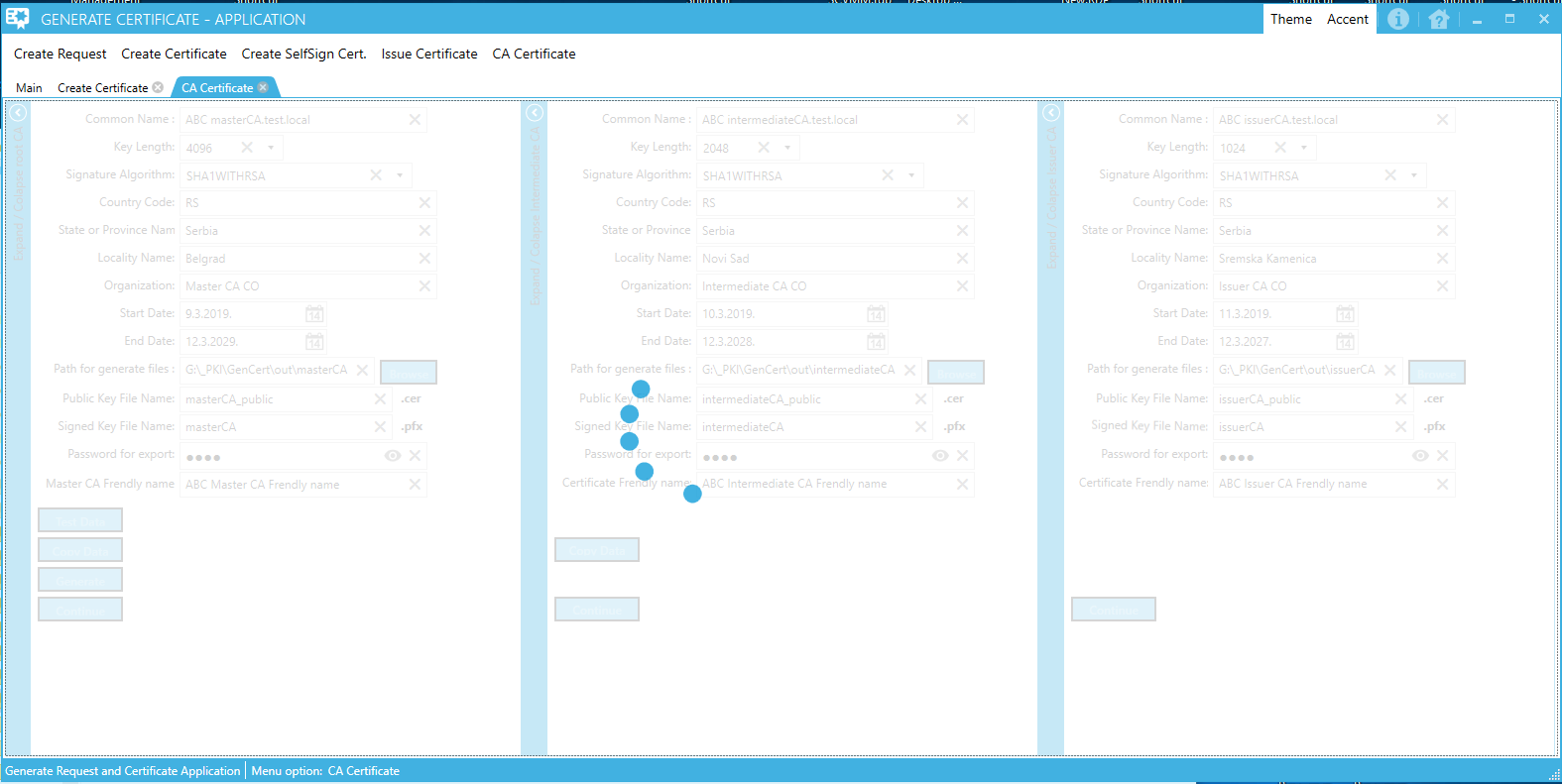
If data entered correctly, application will automatically generate and fill form(s) with appropriate data.

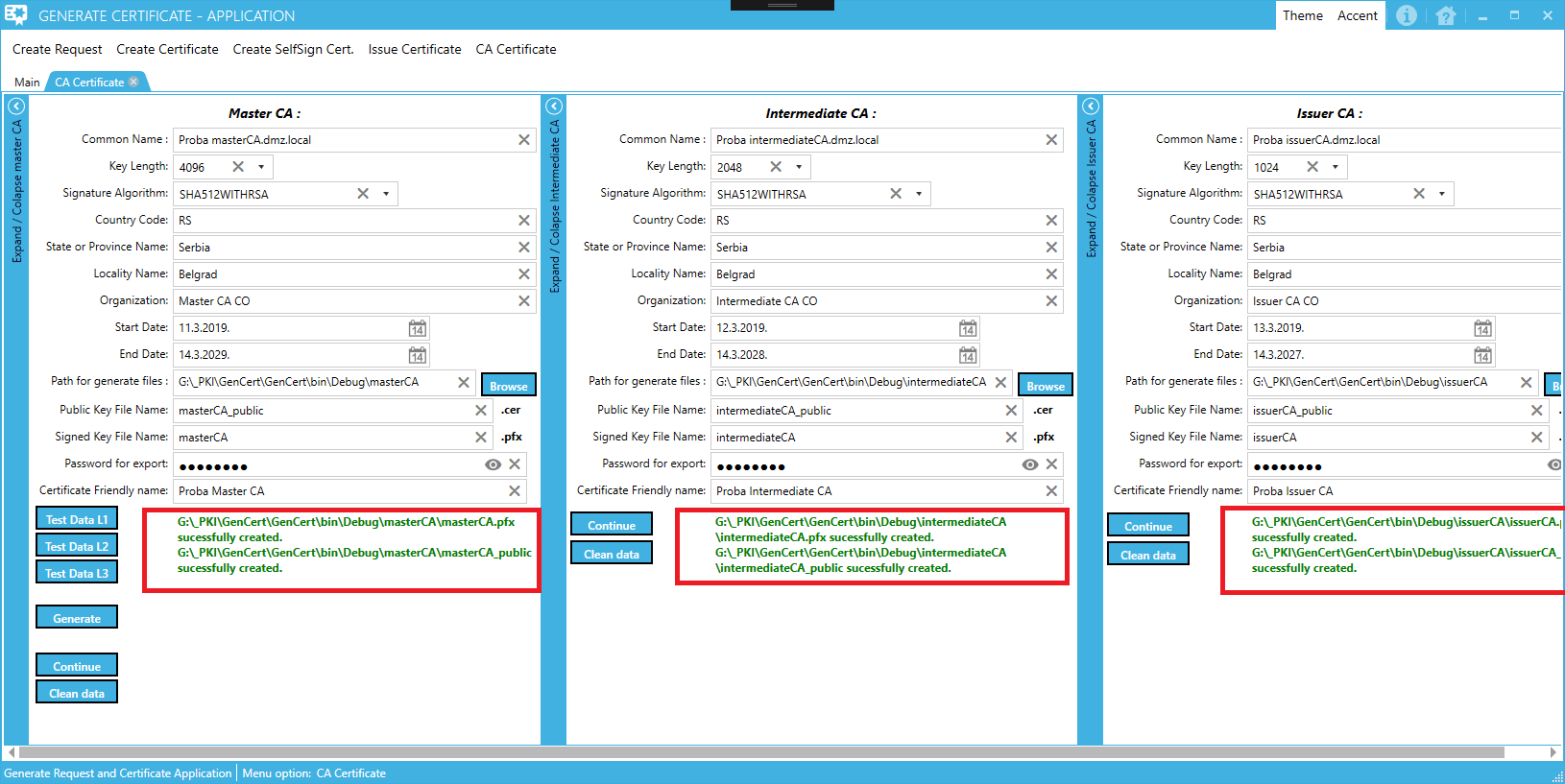




When you click “Generate” button you will get next message

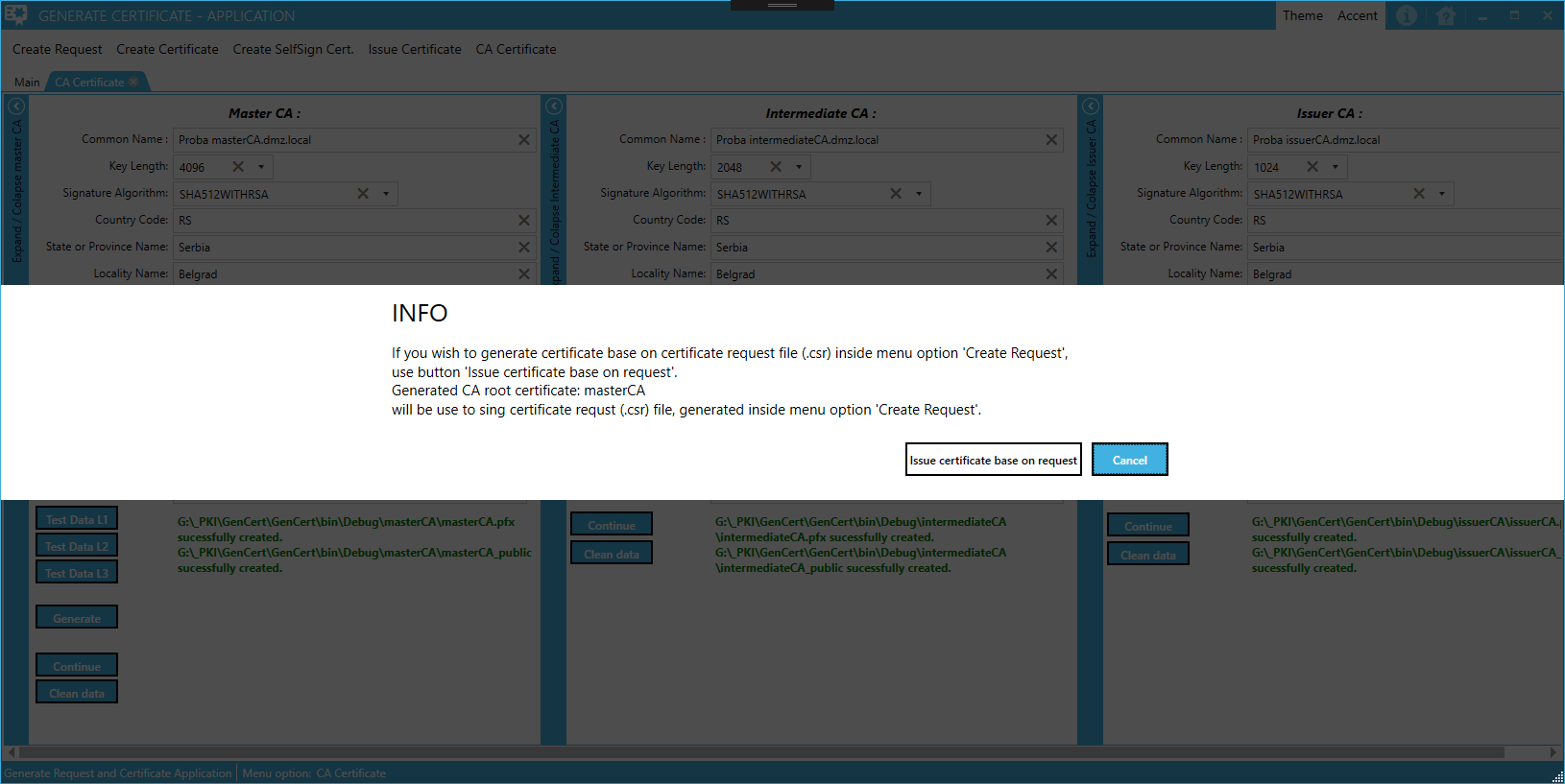




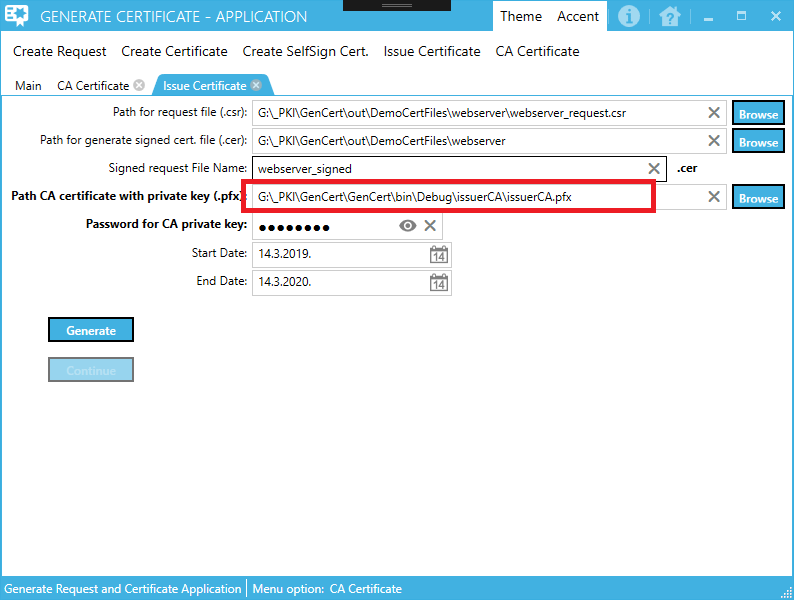


When you successfully generate appropriate CA certificate file(s), button “Continue” will be enabled.

If you click on “Continue” button, you will get next dialog:



If click Cancel you will stay on current form or if you click button “Issue certificate base on request”, application will open new form for issuing (sign) certificate file, based on created request file.



Base on generated certificate file(s), (masterCA / intermediateCA / issuerCA) new form for issue certificate will be automatically fill field “Path CA certificate with private key (.pfx)” with appropriate generated certificate file.

This means, if you generate only certificate for masterCA and click Continue button, field “Path CA certificate with private key (.pfx)” will be filled with materCA file path.

If you generate masterCA and intermediateCA and click Continue button, field “Path CA certificate with private key (.pfx)” will be filled with intermediateCA file path.

If you generate masterCA, intermediateCA and issuerCA and click Continue button, field “Path CA certificate with private key (.pfx)” will be filled with issuerCA file path.

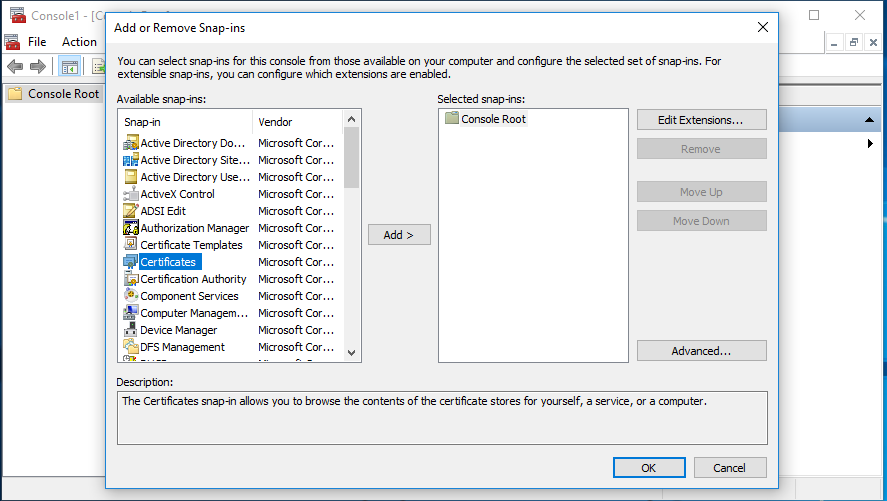
Field “Path CA certificate with private key (.pfx)” always will be filled with last generated certificate file path inside certificates CA chain.

# Import data from generated signed certificate file to SERVER certificate store

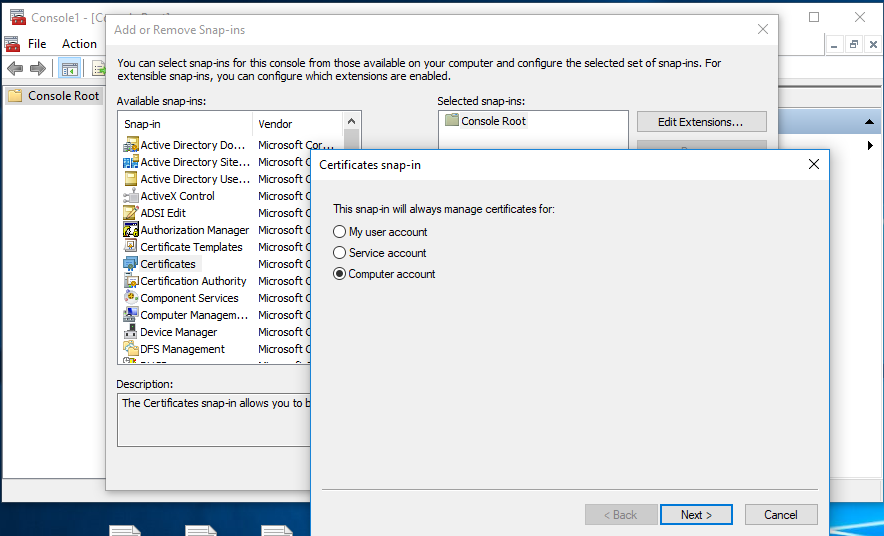
On the computer, open mmc.exe console.



Add Certificate Snap-in



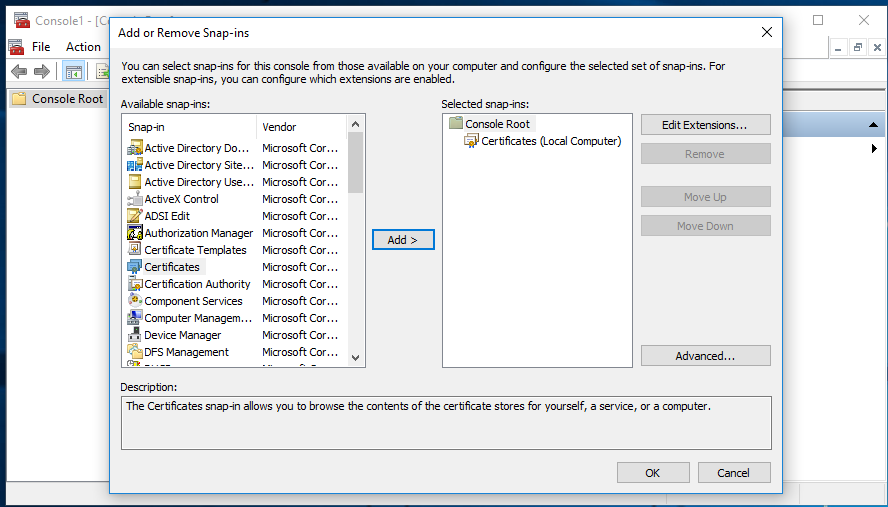
Add, Choose option “Computer account”



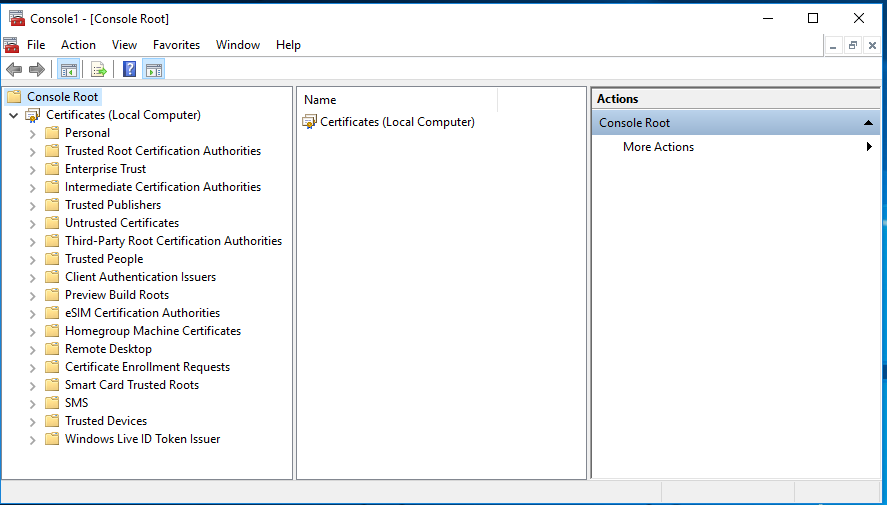
Next



Finish

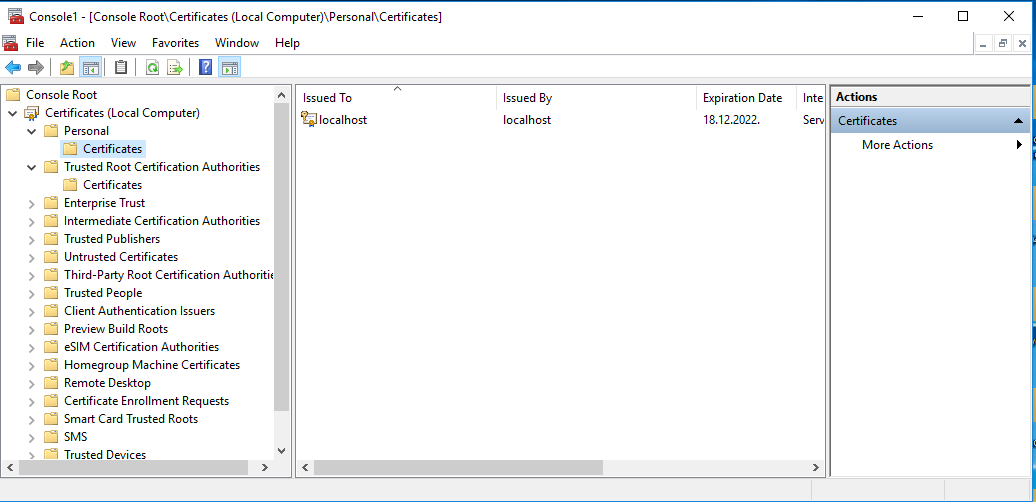


OK

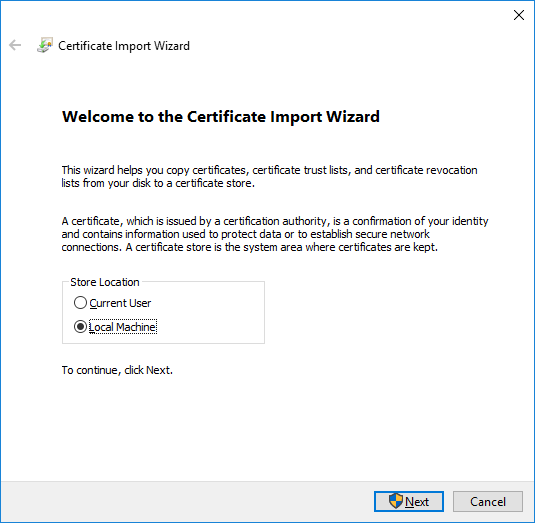


Parts of local computer Certificate store for interest are:

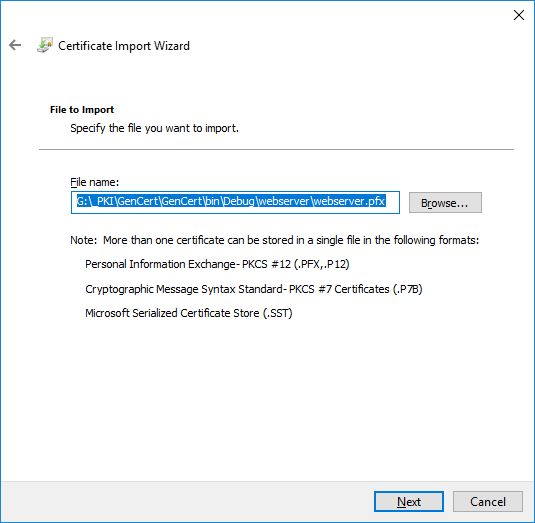
1. Personal -> Certificates
2. Trusted Root Certification Authorities -> Certificates
3. Intermediate Certification Authorities -> Certificates



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

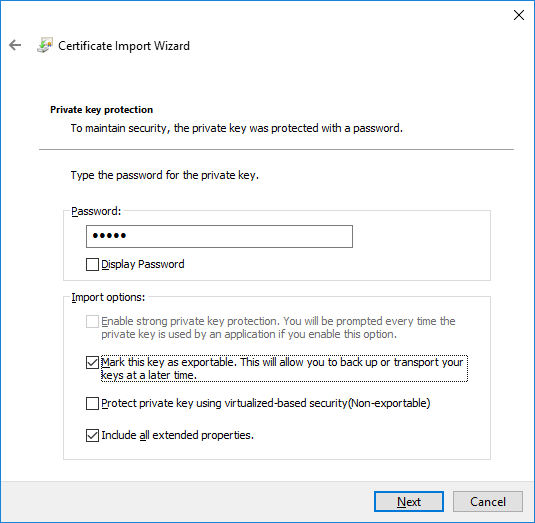


Next

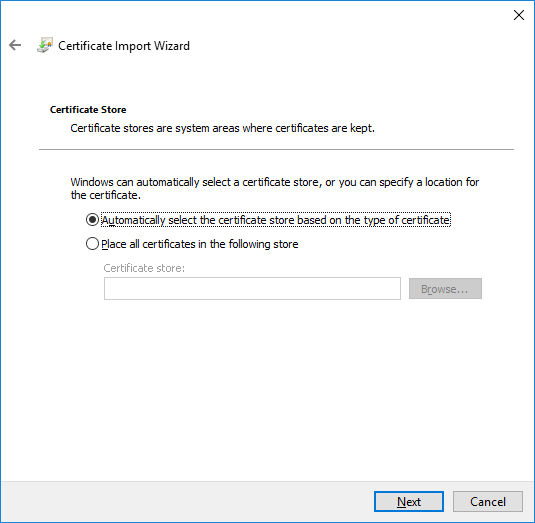


Next

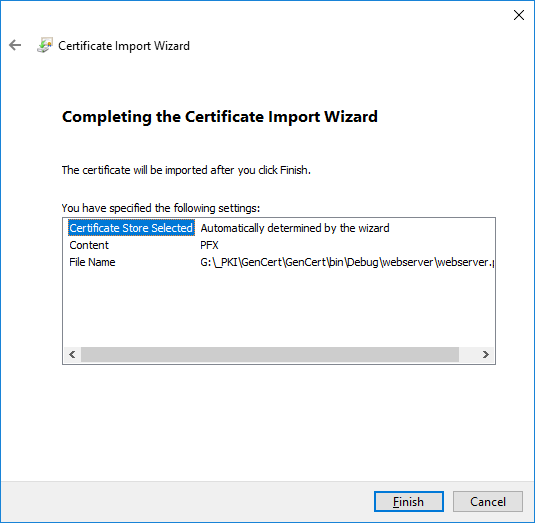
Enter password you set when generated .pfx file. Optionally you can allow that this certificate can by exportable from certificate store by checking option “Mark this key as exportable.”



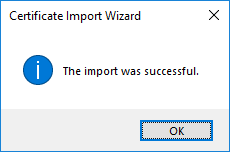
Next



Next



Finish

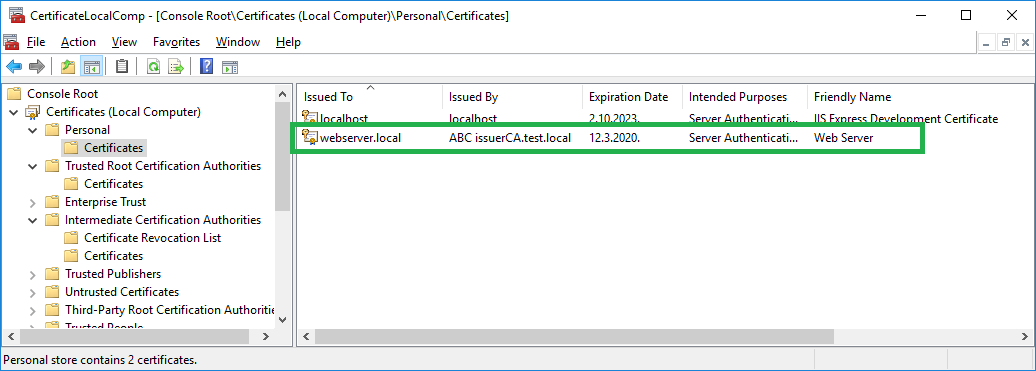


OK

Refresh Personal and Trusted Root Certification Authorities inside mmc console.



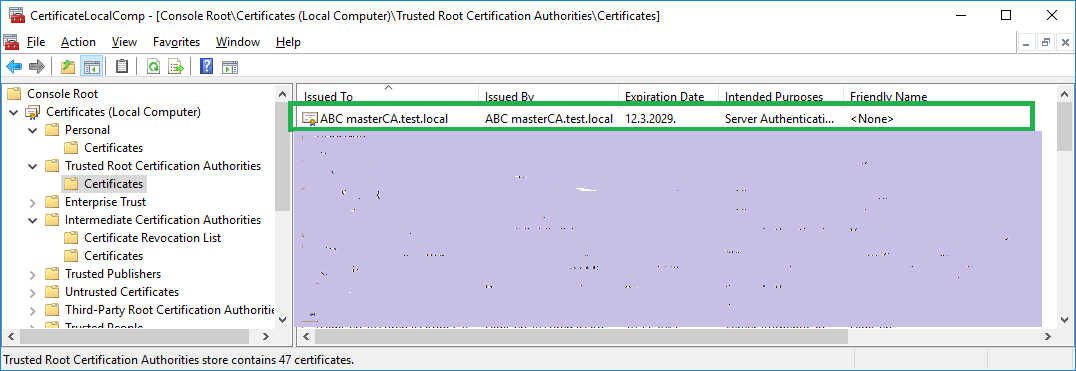
After refresh



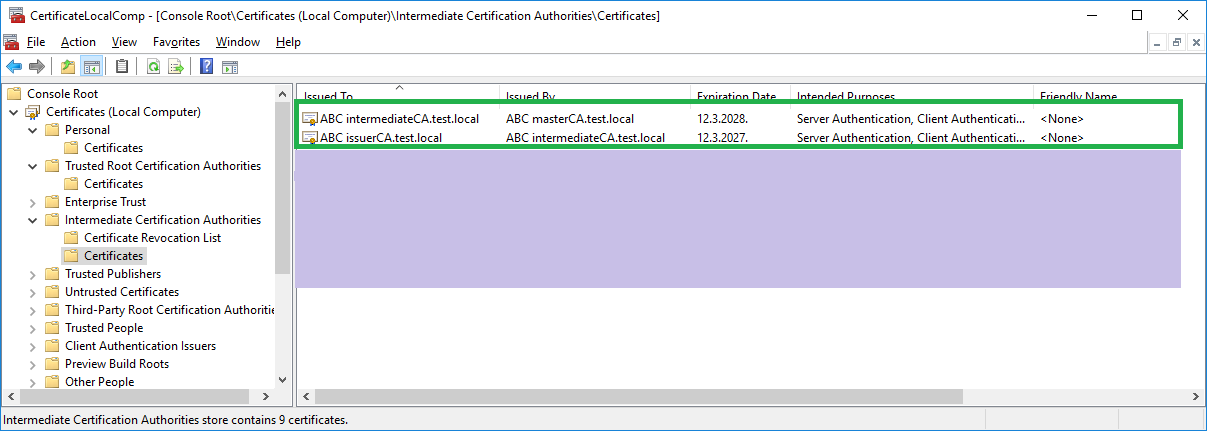
You can see data from imported certificate file inside Personal, Certificate store.

On the picture, you can see that certificate issued to webserver.local by CA root name “ABC issuerCA.test.local”, expiration day for imported certificate and purpose (Server Authentication)

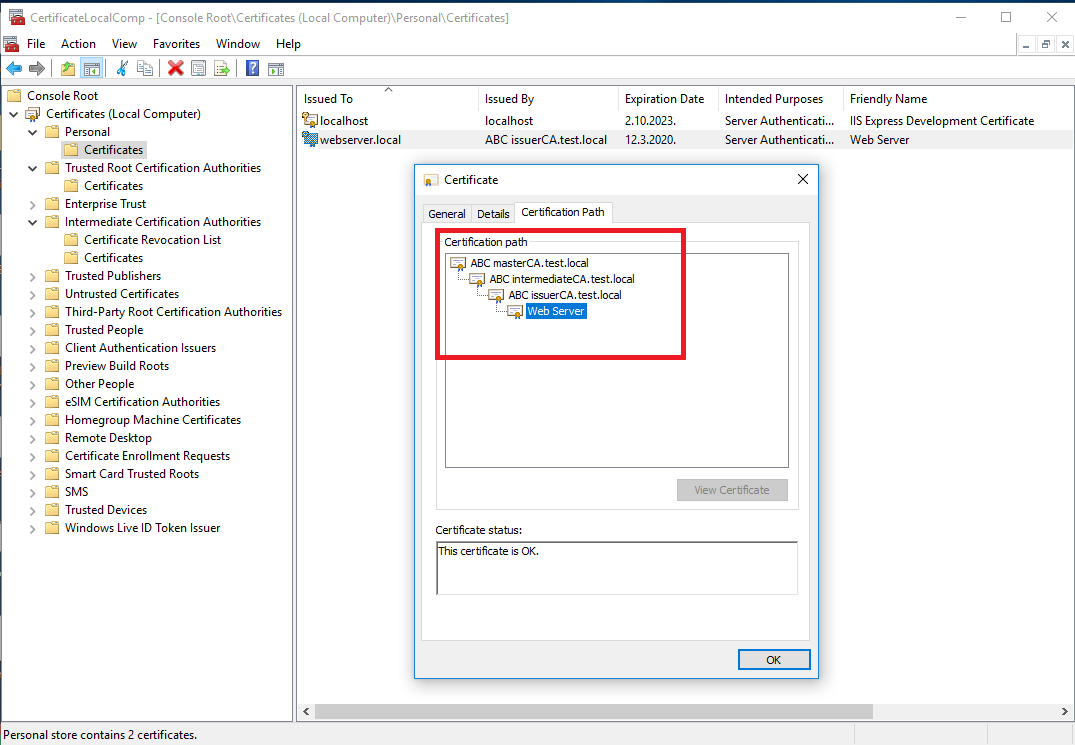
If Refresh “Trusted Root Certification Authorities” -> “Certificates” you can see certificate for root CA that signed our generated certificate file, that we imported when generate our certificate file. In our case, that is certificate named “ABC masterCA.test.local”



If Refresh “Intermediate Certification Authorities” -> “Certificates” you can see certificate for intermediate CA and issuer CA that signed our generated certificate file, that we imported when generate our certificate file. In our case, that is certificate named “ABC intermediateCA.test.local” and “ABC issuerCA.test.local”.

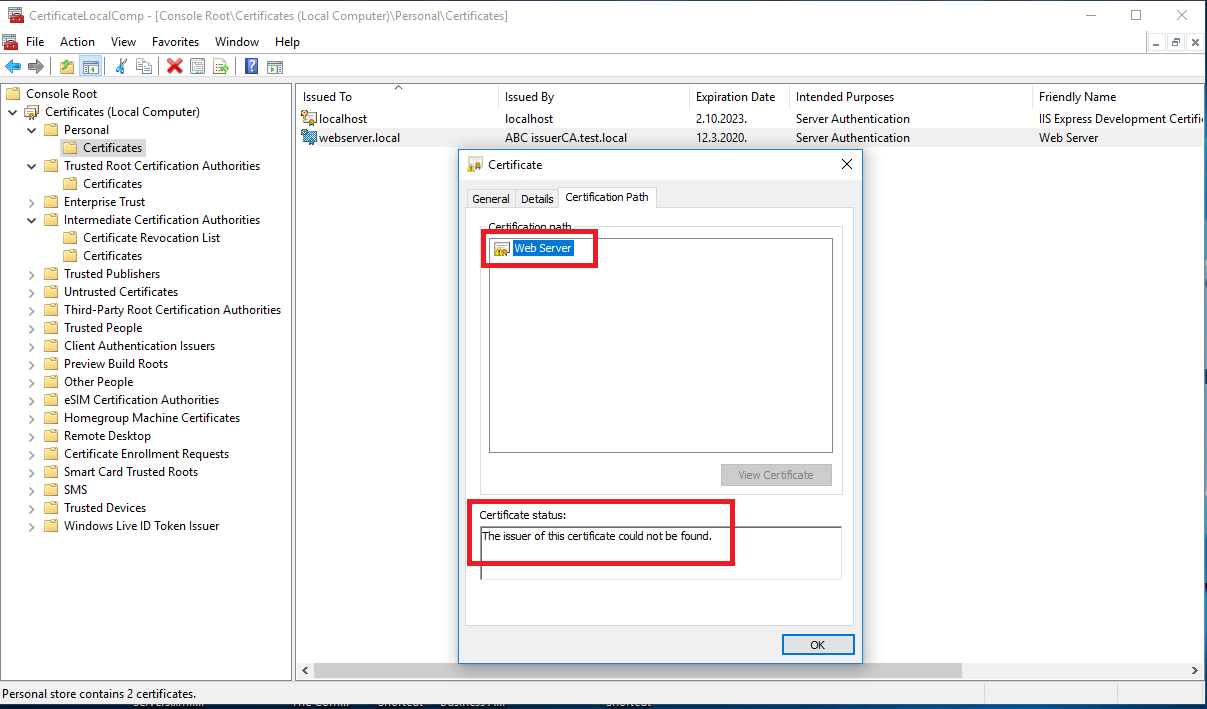


If you sign your certificate request file by some internal or external certificate authorities, you need to import data from that CA certificate authorities to “Trusted Root Certification Authorities” and if need also import appropriate certificate inside “Intermediate Certification Authorities”, otherwise imported generated certificate don’t be valid.



Valid imported certificate look.

If you didn’t import data for CA root public key to certificate store, certificate look like this:

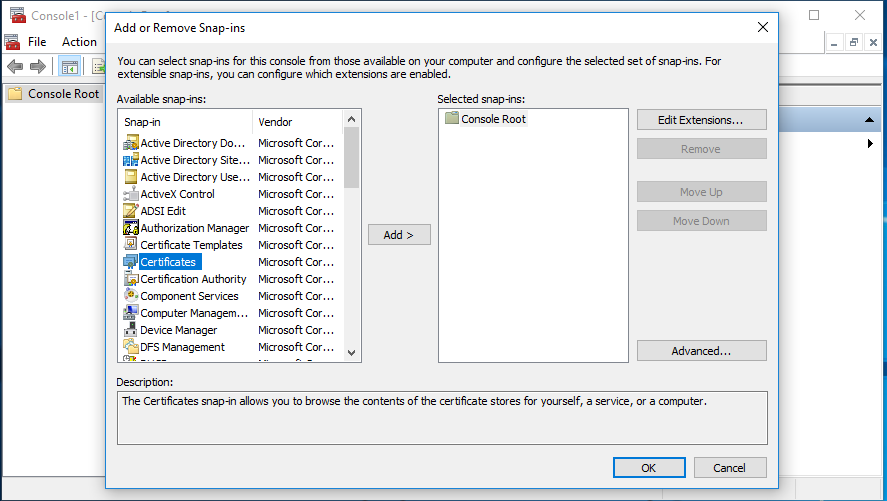


# Import data from generated CA certificate file(s) to client certificate store

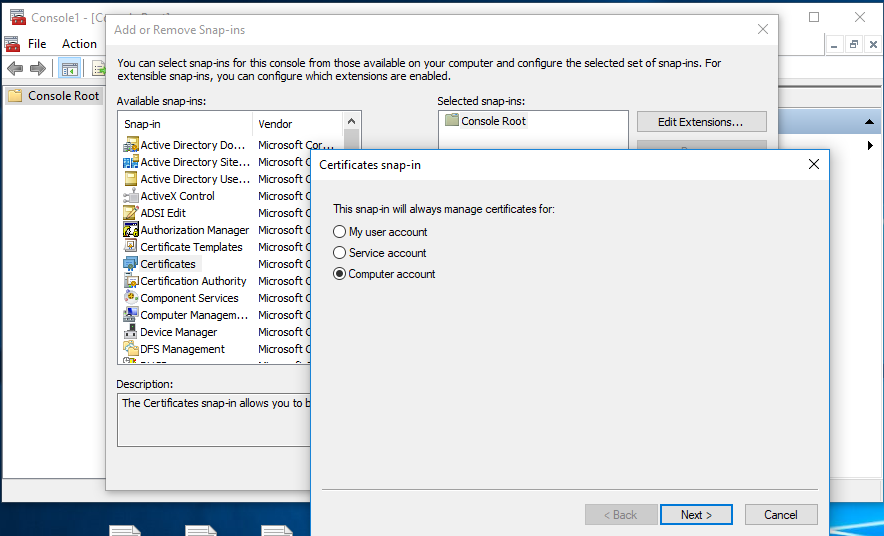
On the client computer, open mmc.exe console.



Add Certificate Snap-in



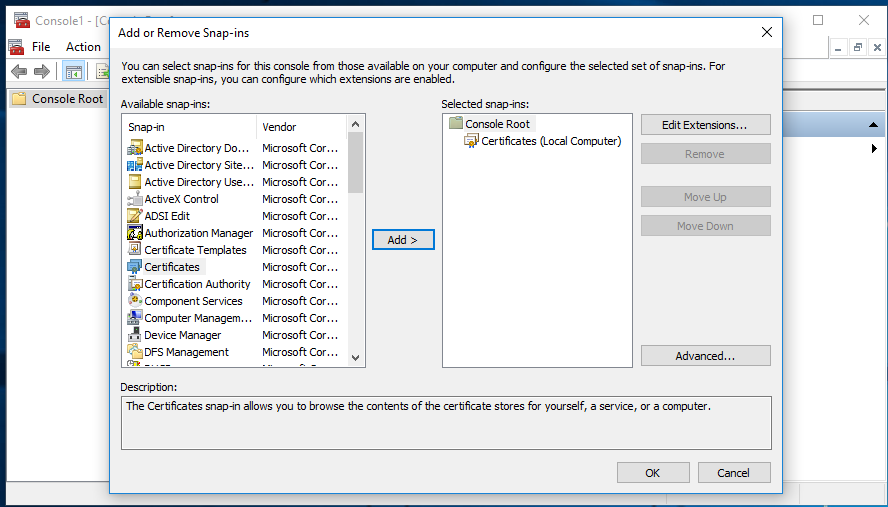
Add, Choose option “Computer account”



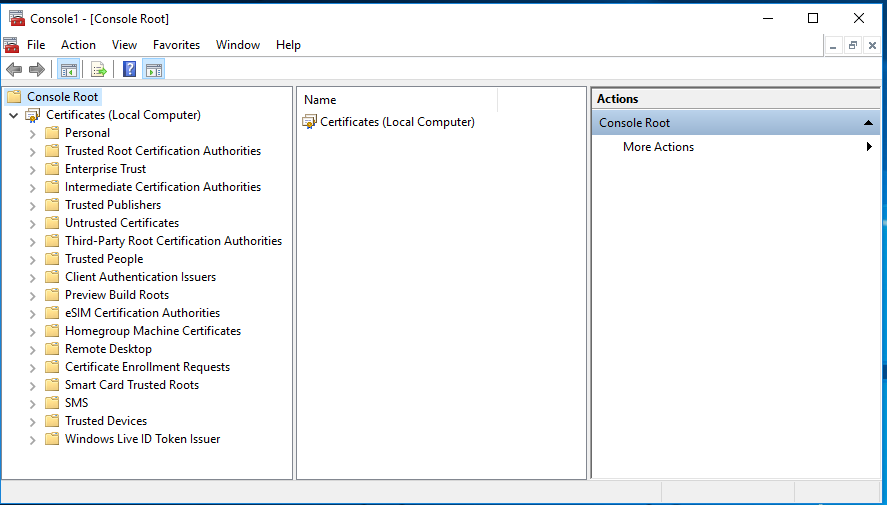
Next



Finish

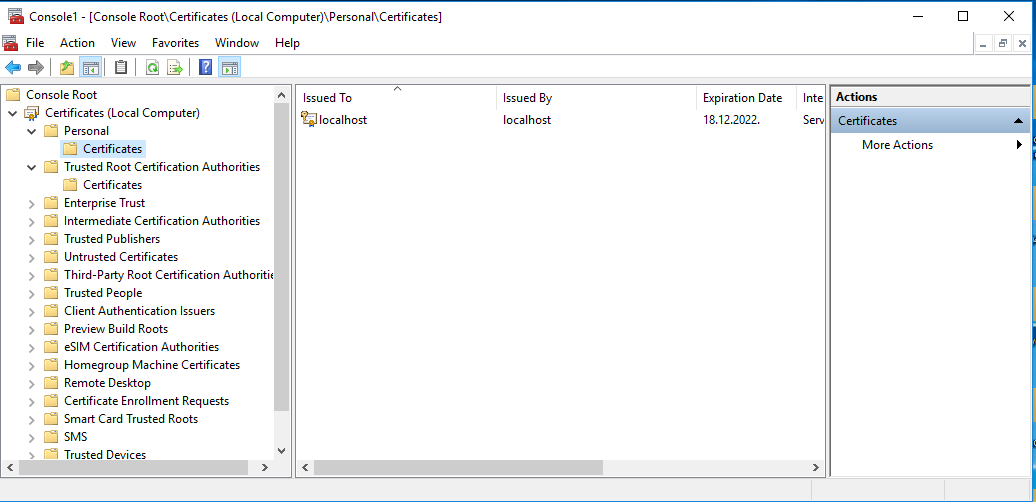


OK



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.

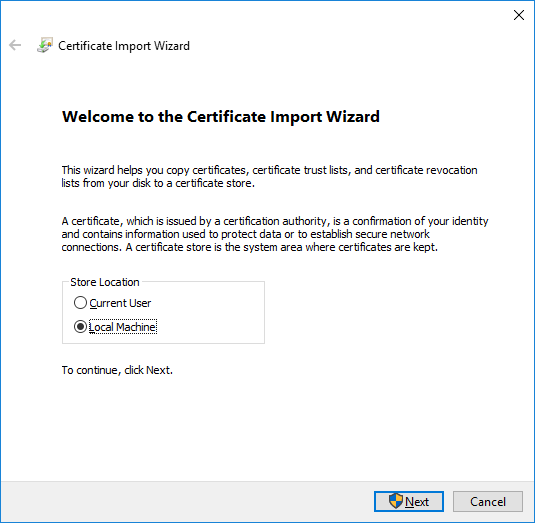
If you use one level CA (only master CA) to issue certificate for server use master CA .pfx file.

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

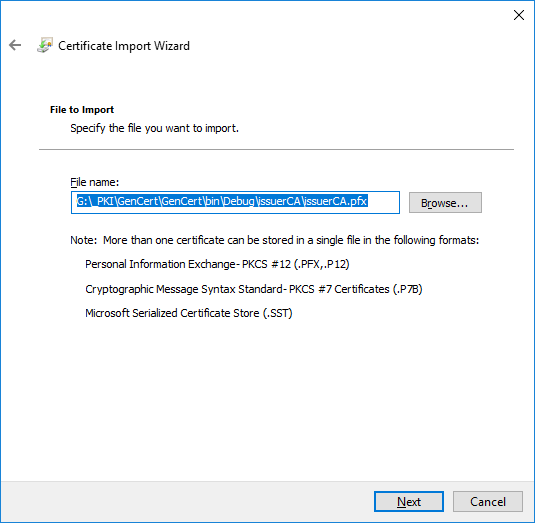
If you use three level CA (master CA + intermediate CA + issuer CA) to issue certificate for server use issuer CA .pfx file.

## 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

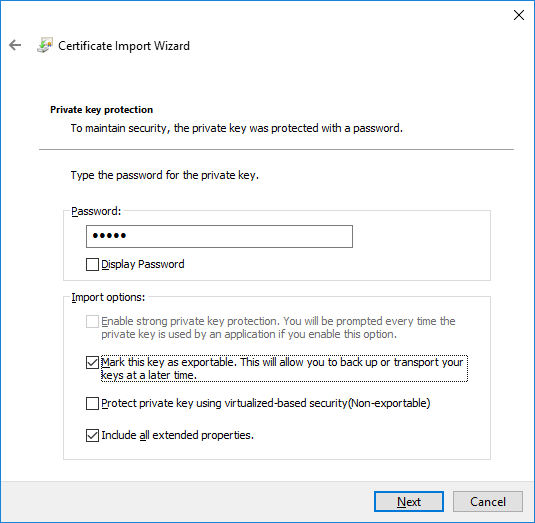


Next

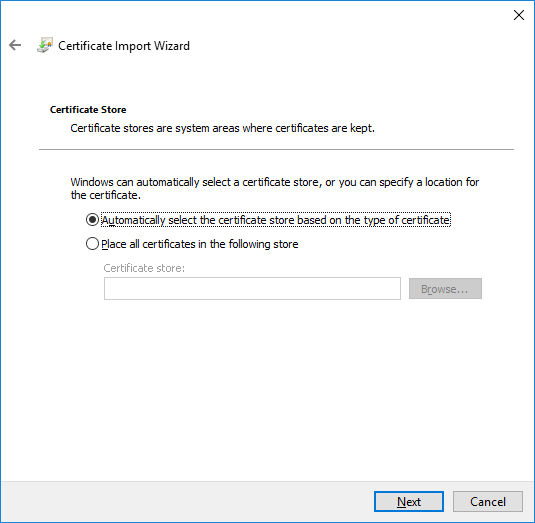


Next

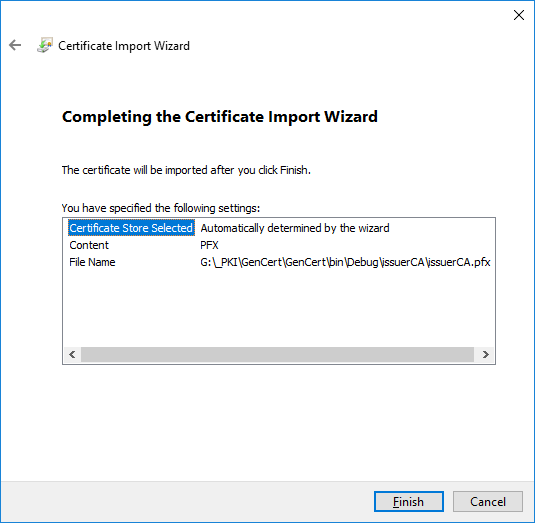
Enter password you set when generated .pfx file. Optionally you can allow that this certificate can by exportable from certificate store by checking option “Mark this key as exportable.”



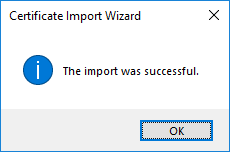
Next



Next



Finish



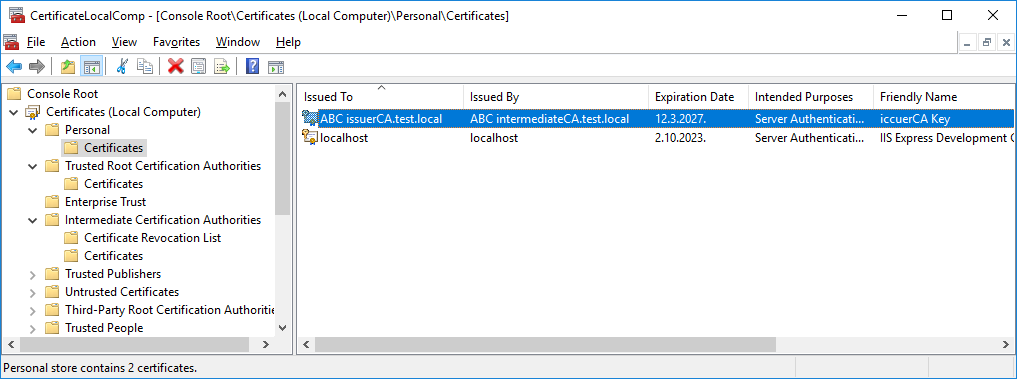
OK

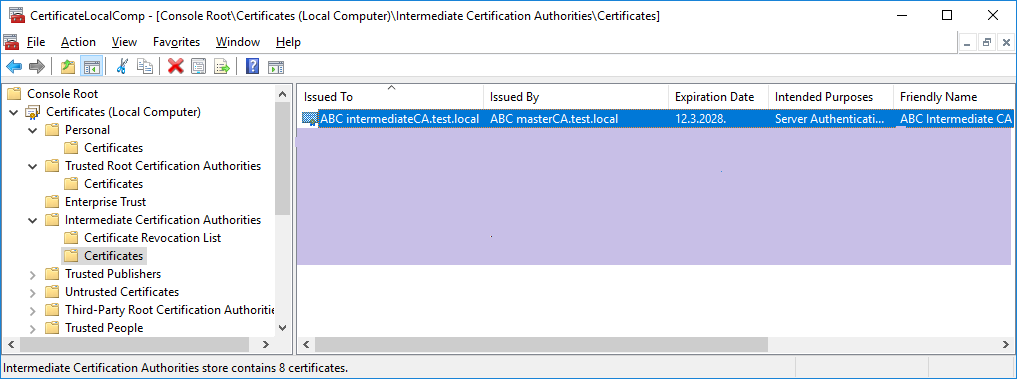
If you import three level certificate (issuer CA) you need to refresh Personal, Trusted Root Certification Authorities and Intermediate Certification Authorities inside mmc console to see new imported certificates.

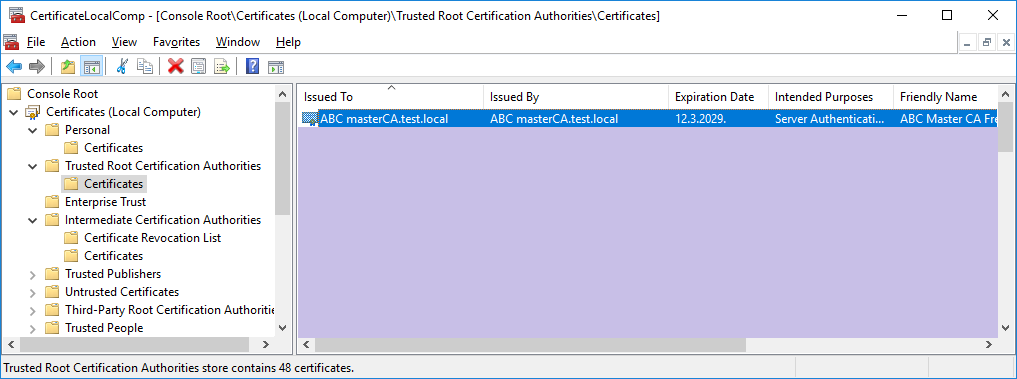
-issuer CA certificate will be found inside Personal->Certificates store.

-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.

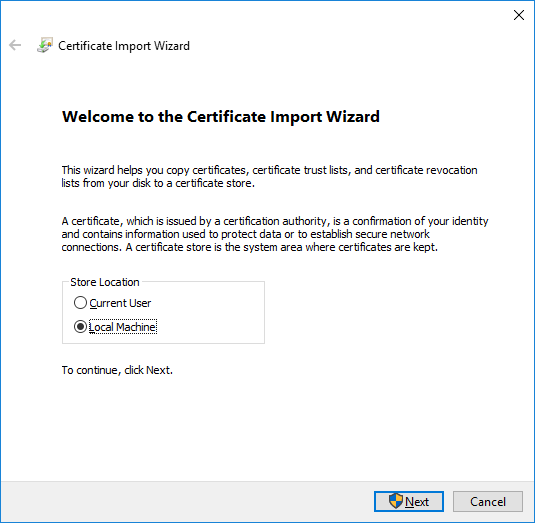




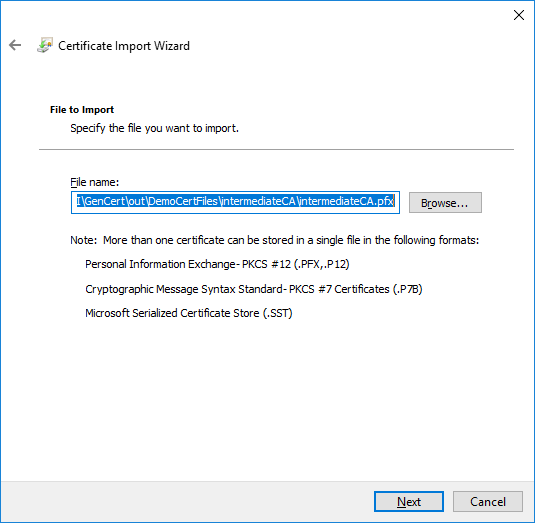


## Import two level CA certificate (intermediate CA)

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

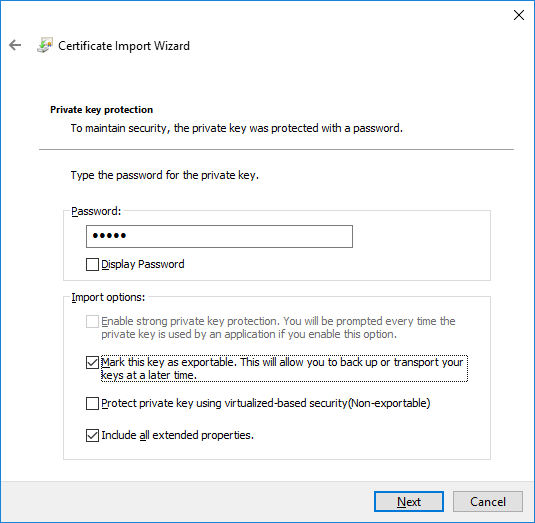


Next

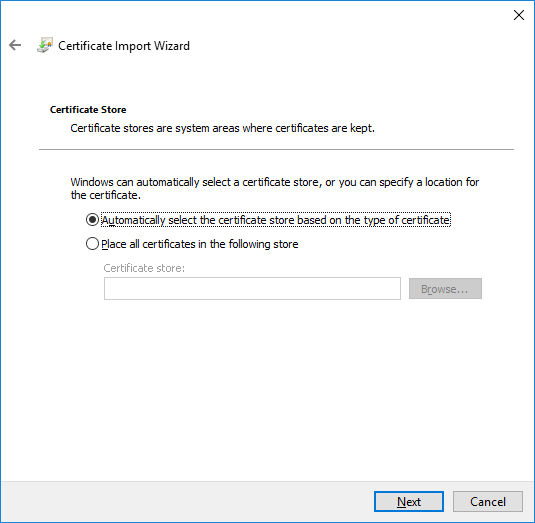


Next

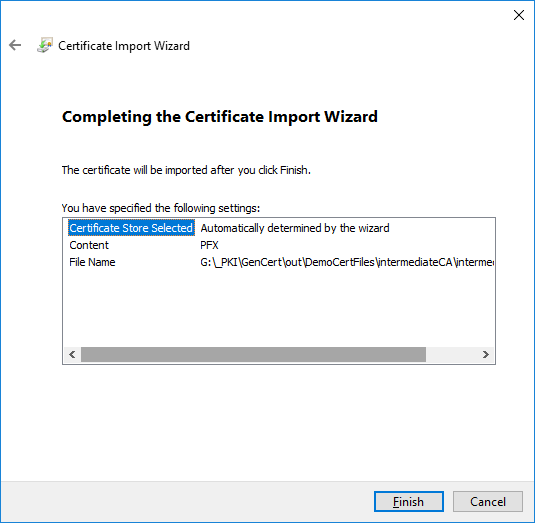
Enter password you set when generated .pfx file. Optionally you can allow that this certificate can by exportable from certificate store by checking option “Mark this key as exportable.”



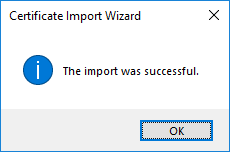
Next



Next



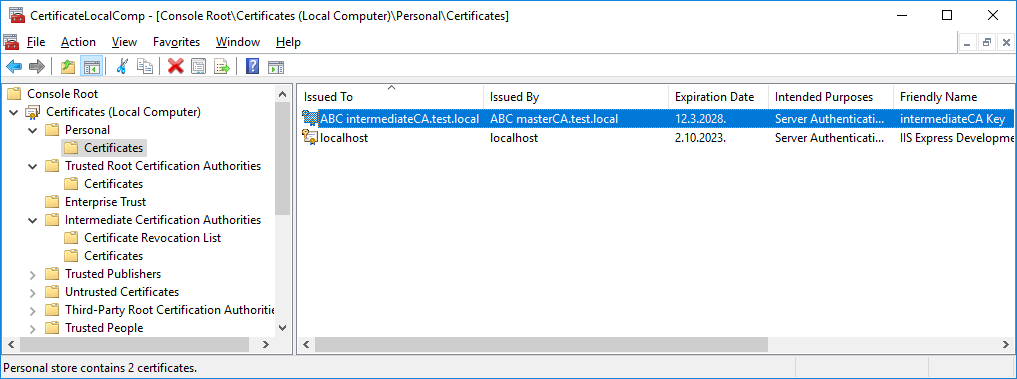
Finish



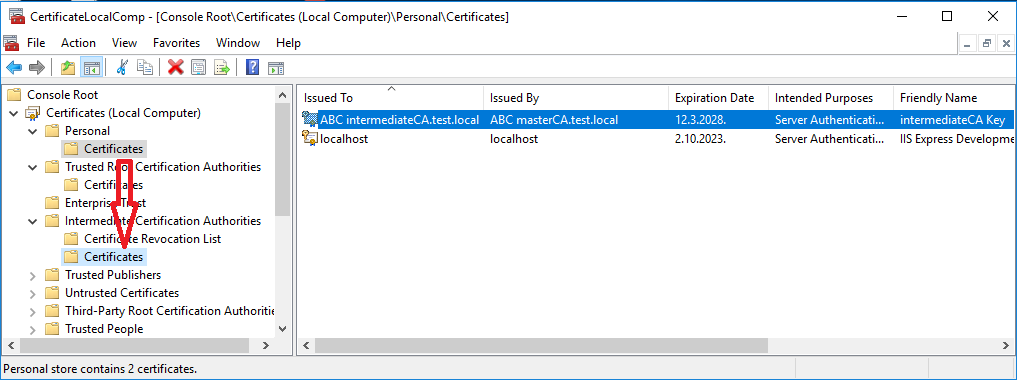
OK

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

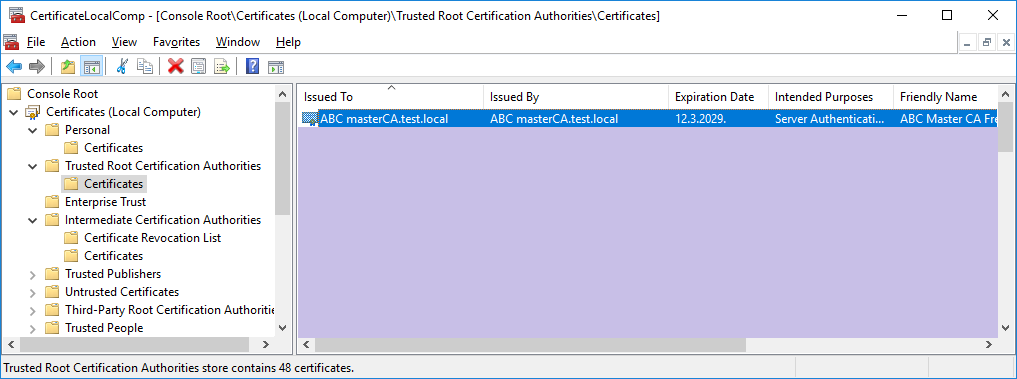
Intermediate CA certificate will be found inside Personal->Certificates store.



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.

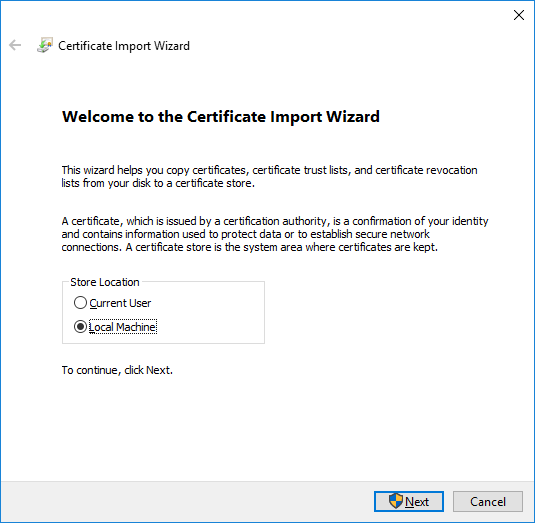


Master CA certificate will be found inside Trusted Root Certification Authorities->Certificates store.

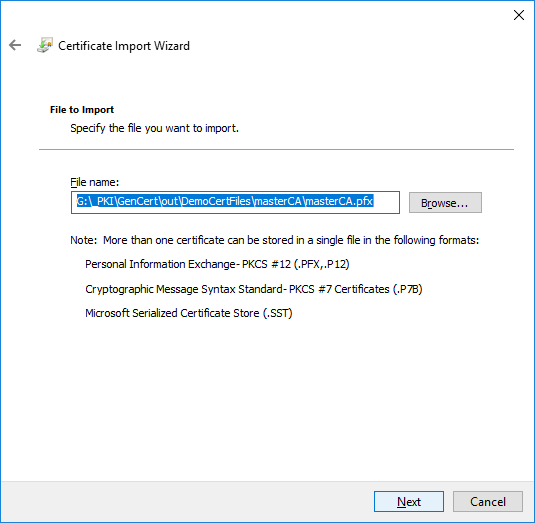


## Import one level CA certificate (master CA)

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

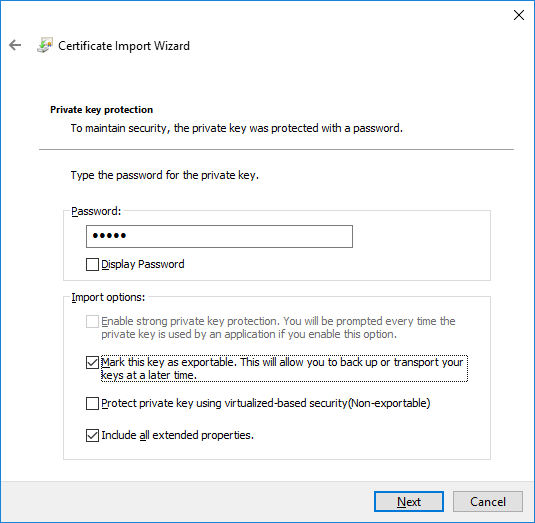


Next



Next

Enter password you set when generated .pfx file. Optionally you can allow that this certificate can by exportable from certificate store by checking option “Mark this key as exportable.”

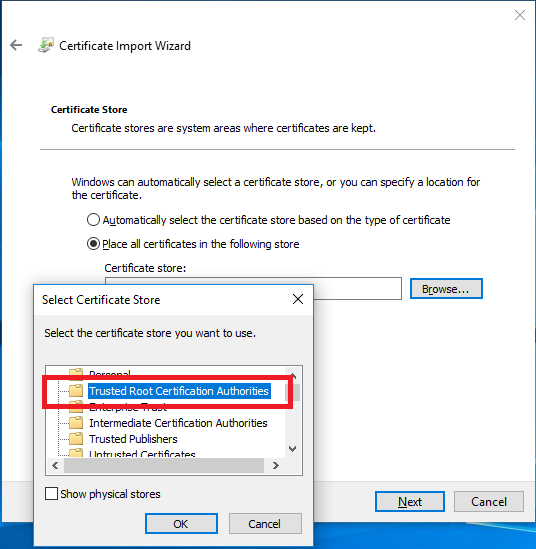


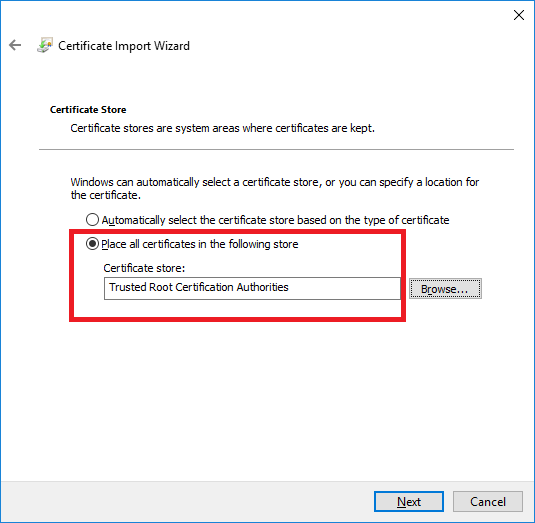
Next

**NOTE:**

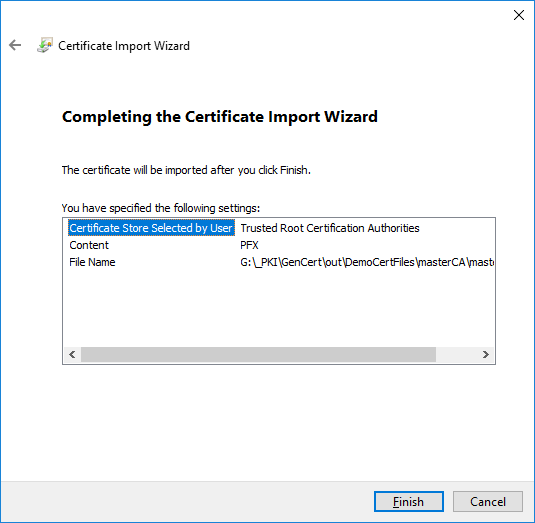
In next step be careful, use option “Place all certificates in the following store” and use certificate store “Trusted Root Certification Authorities”



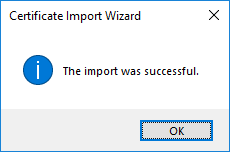




Next

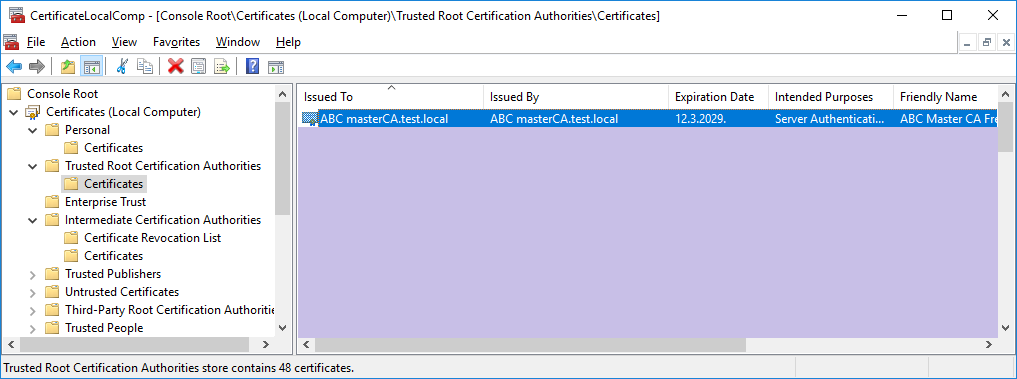


Finish



OK

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.



# Application requirements

To successfully start application, you need .NET Framework 4.x installed on computer where application need to be started.

For minimal configuration, you ONLY need a file GenCert.exe to run application.

Inside Help folder you can find generated application user manual in different file formats: pdf, chm, xps, html.

For complete configuration, you need following files:

GenCert.exe

GenCert.chm

config.ini

File GenCert.chm extension is help file for application. If you put GenCert.chm file inside the same folder where you start

application, this help will be open when you click on Home button

When you start application for the first time 3 new files will be created:

Log4NetApplicationLog.log – log4net application log file in txt format

Log4NetApplicationLog.xml – log4net application log file in xml format

config.ini – application configuration file

Inside config.ini file, you can configure default value for option Certificate Friendly Name which is used inside application on different menu options.