Generate Request and Certificate PKI Application

User Guide

Last update: May, 2018

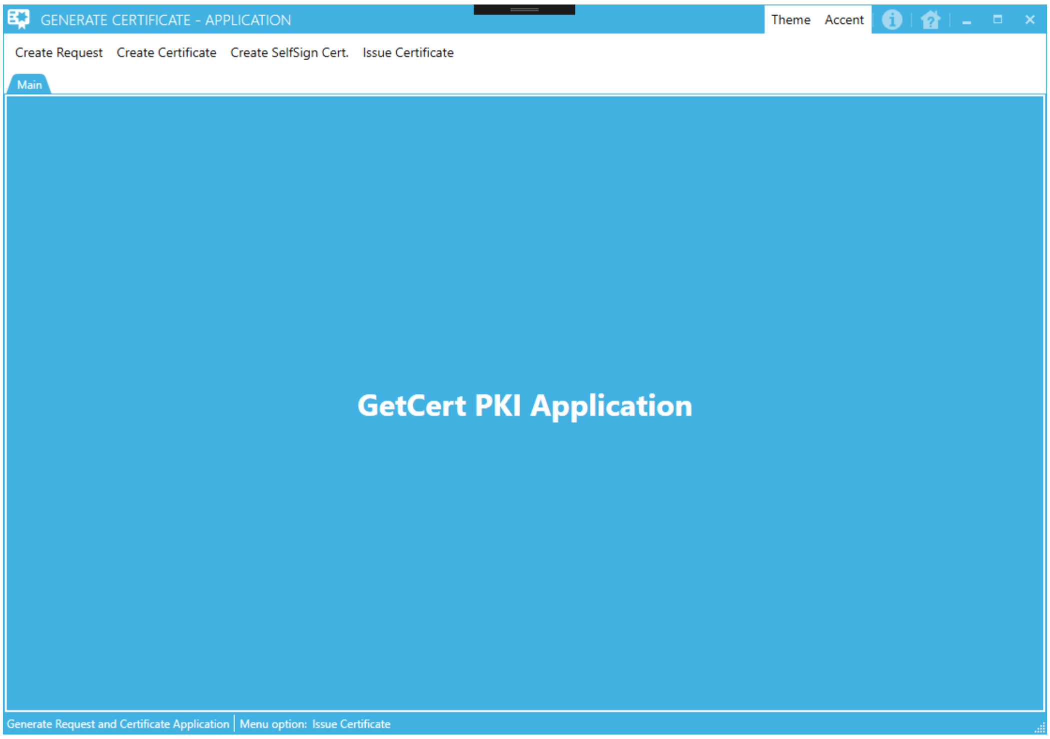
Table of Contents

1. INTRODUCTION

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

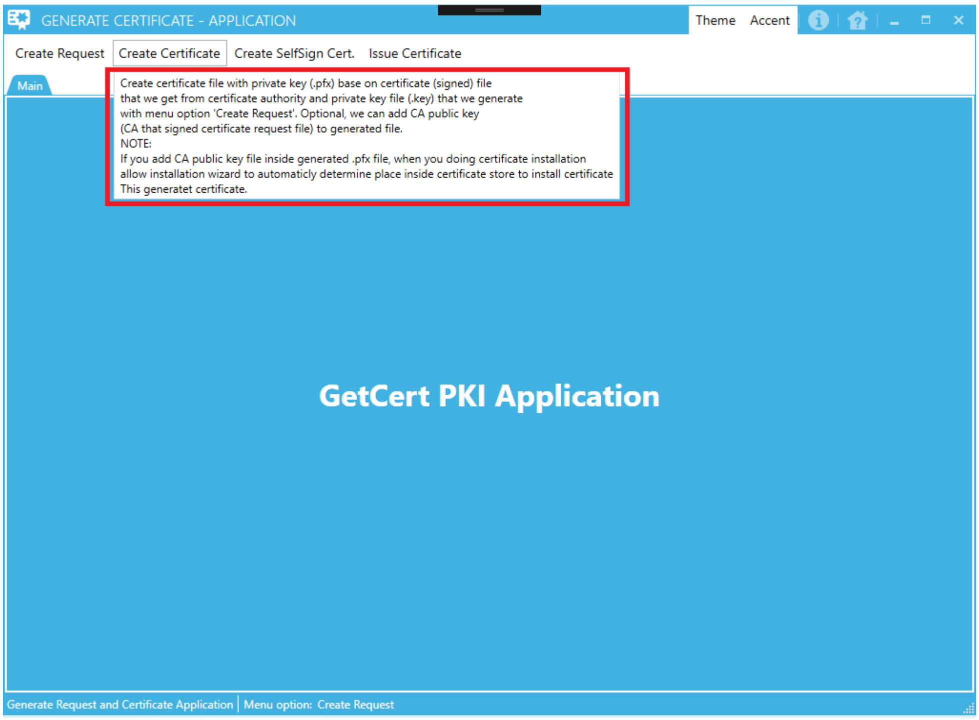
The application consists of 4 menu options:

- Create Request
- Create Certificate
- Create SelfSign Cert.
- Issue Certificate


GENERATE CERTIFICATE - APPLICATION
Theme
Accent
Create Request
Create Certificate
Create SelfSign Cert.
Issue Certificate
Main
GetCert PKI Application
Generate Request and Certificate Application
Menu option: Issue Certificate

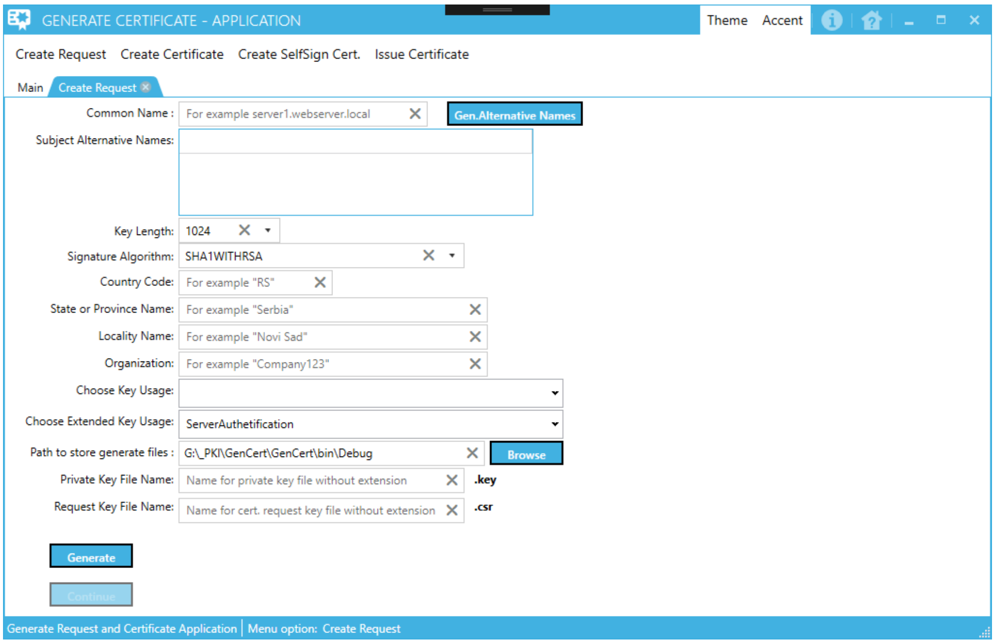
1.1. User Interface

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



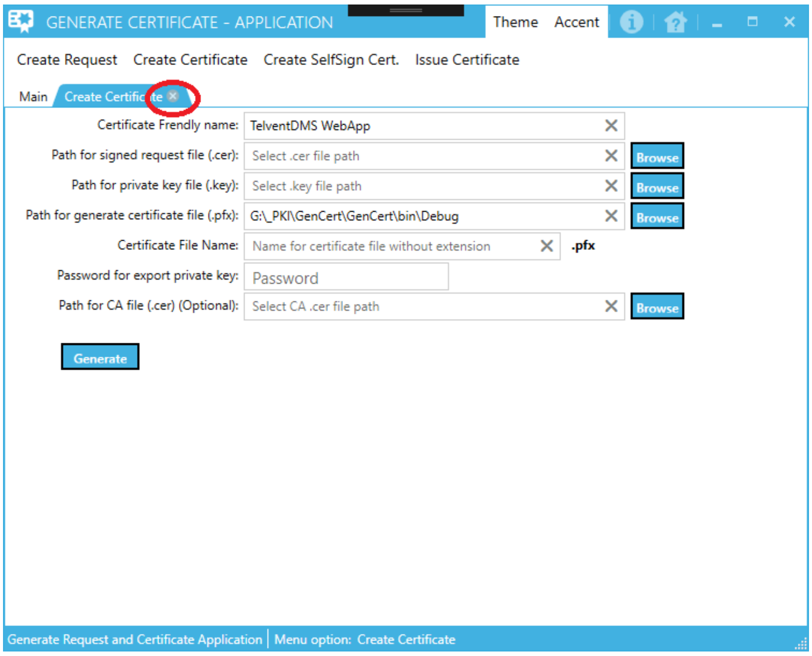
Create certificate file with private key (.pfx) base on certificate (signed) file
that we get from certificate authority and private key file (.key) that we generate
with menu option 'Create Request'. Optional, we can add CA public key
(CA that signed certificate request file) to generated file.
NOTE:
If you add CA public key file inside generated .pfx file, when you doing certificate installation
allow installation wizard to automaticly determine place inside certificate store to install certificate
This generatet certificate.

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



Common Name : For example server1.webserver.local
Subject Alternative Names:
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\GenCert\bin\Debug
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

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



Certificate Frendly name: TelventDMS WebApp

Path for signed request file (.cer): Select .cer file path

Path for private key file (.key): Select .key file path

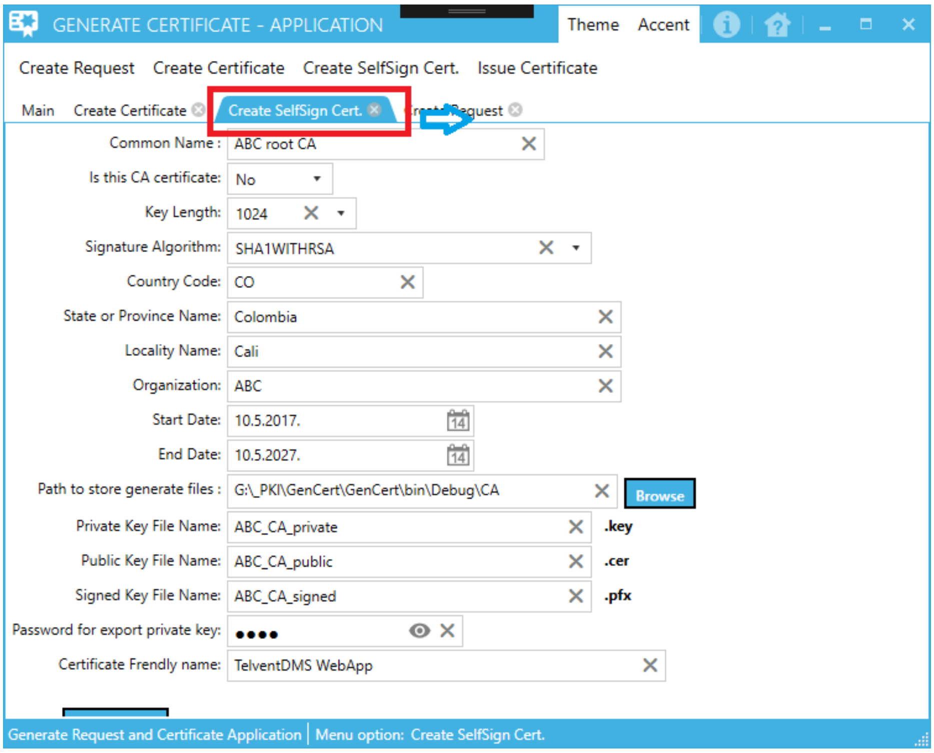
Path for generate certificate file (.pfx): G:_PKI\GenCert\GenCert\bin\Debug

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

Password for export private key: Password

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

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



Common Name : ABC root CA

Is this CA certificate: No

Key Length: 1024

Signature Algorithm: SHA1WITHRSA

Country Code: CO

State or Province Name: Colombia

Locality Name: Cali

Organization: ABC

Start Date: 10.5.2017.

End Date: 10.5.2027.

Path to store generate files : G:_PKI\GenCert\GenCert\bin\Debug\CA

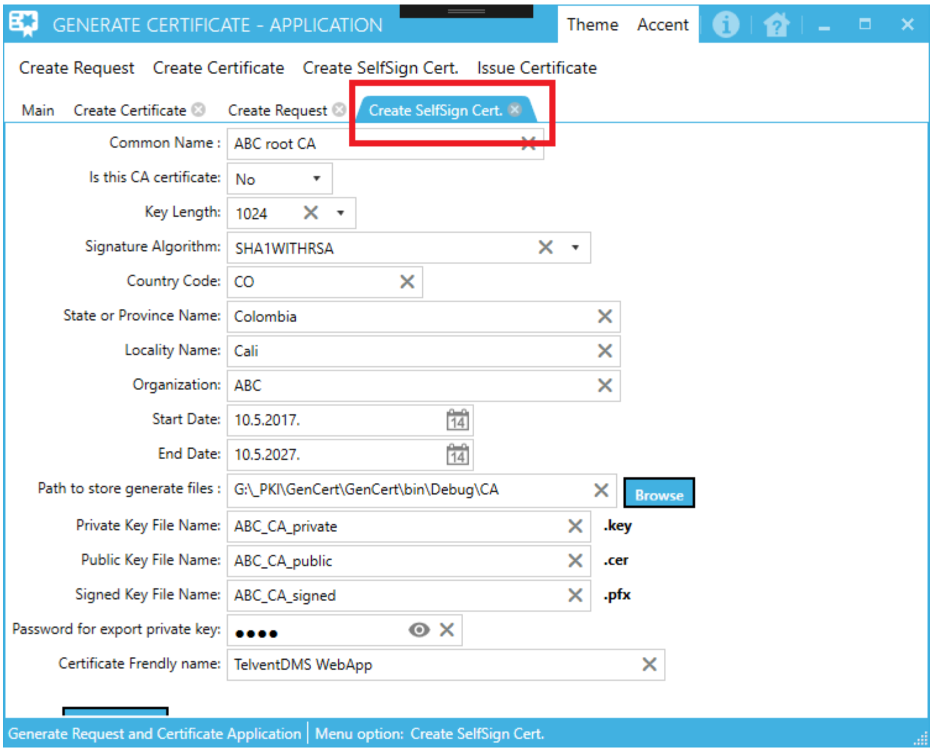
Private Key File Name: ABC_CA_private .key

Public Key File Name: ABC_CA_public .cer

Signed Key File Name: ABC_CA_signed .pfx

Password for export private key: ●●●●

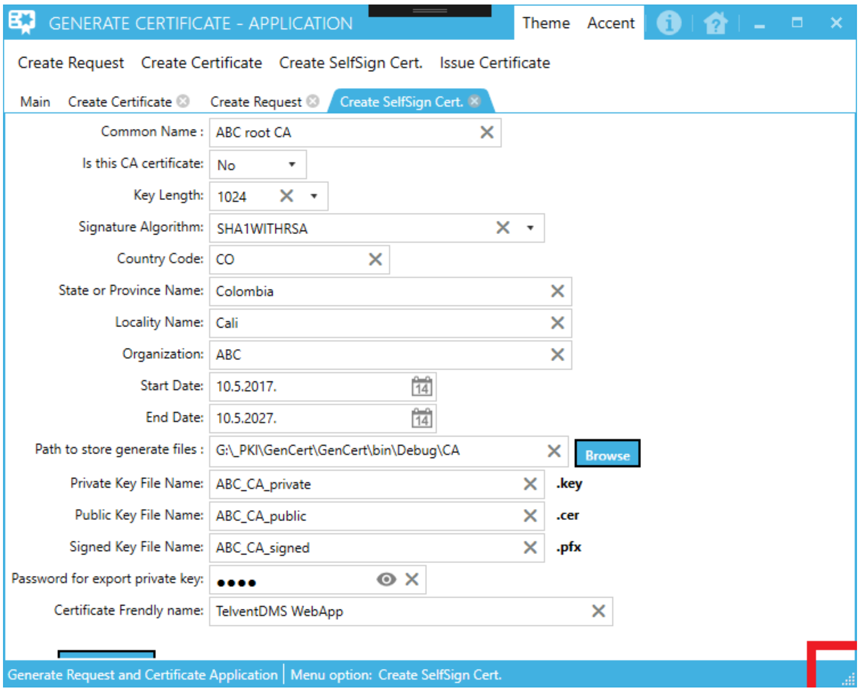
Certificate Frendly name: TelventDMS WebApp



Common Name : ABC root CA
Is this CA certificate: No
Key Length: 1024
Signature Algorithm: SHA1WITHRSA
Country Code: CO
State or Province Name: Colombia
Locality Name: Cali
Organization: ABC
Start Date: 10.5.2017.
End Date: 10.5.2027.
Path to store generate files : G:_PKI\GenCert\GenCert\bin\Debug\CA
Private Key File Name: ABC_CA_private .key
Public Key File Name: ABC_CA_public .cer
Signed Key File Name: ABC_CA_signed .pfx
Password for export private key: ●●●●
Certificate Frendly name: TelventDMS WebApp

Generate Request and Certificate Application | Menu option: Create SelfSign Cert.

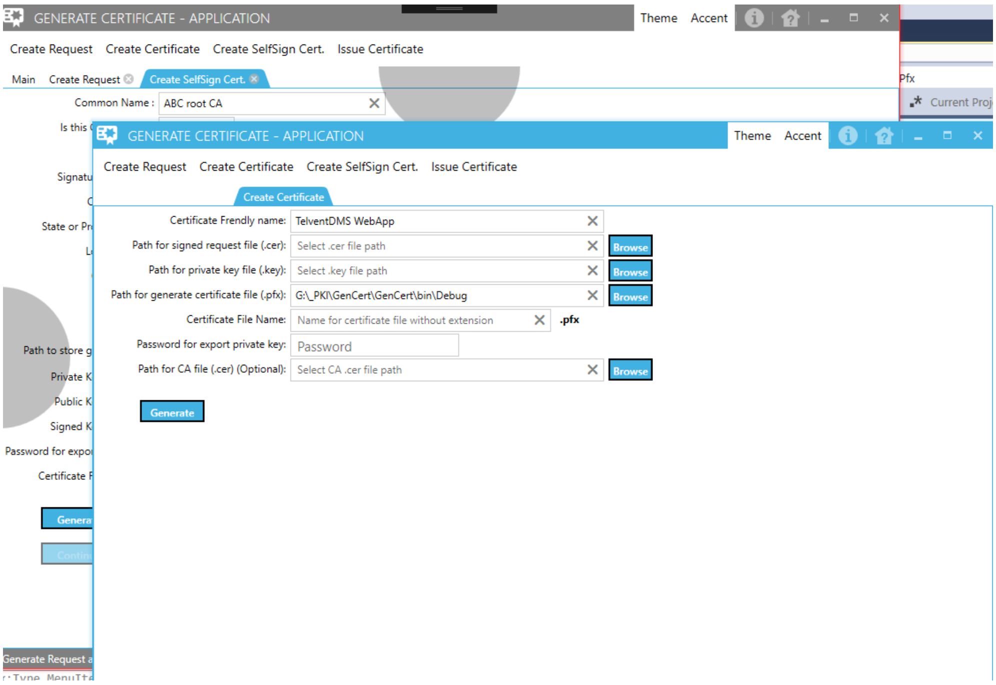
To resize application window, you can use grip inside down right corner of application window



Common Name : ABC root CA
Is this CA certificate: No
Key Length: 1024
Signature Algorithm: SHA1WITHRSA
Country Code: CO
State or Province Name: Colombia
Locality Name: Cali
Organization: ABC
Start Date: 10.5.2017.
End Date: 10.5.2027.
Path to store generate files : G:_PKI\GenCert\GenCert\bin\Debug\CA
Private Key File Name: ABC_CA_private .key
Public Key File Name: ABC_CA_public .cer
Signed Key File Name: ABC_CA_signed .pfx
Password for export private key: ●●●●
Certificate Frendly name: TelventDMS WebApp

Generate Request and Certificate Application | Menu option: Create SelfSign Cert.

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.



GENERATE CERTIFICATE - APPLICATION

Common Name : ABC root CA

Certificate Frendly name: TelventDMS WebApp

Path for signed request file (.cer): Select .cer file path [Browse]

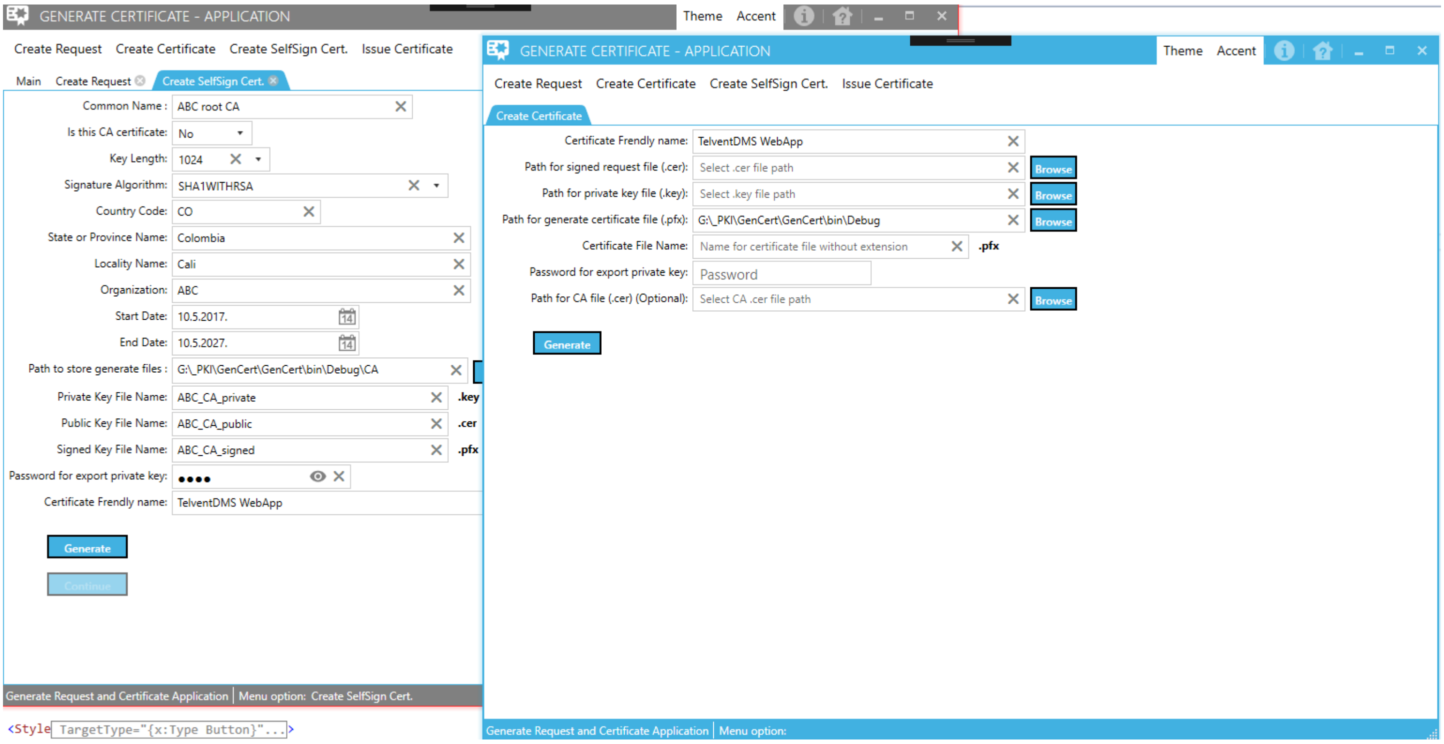
Path for private key file (.key): Select .key file path [Browse]

Path for generate certificate file (.pfx): G:_PKI\GenCert\GenCert\bin\Debug [Browse]

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

Password for export private key: Password

Path for CA file (.cer) (Optional): Select CA .cer file path [Browse]



GENERATE CERTIFICATE - APPLICATION

Common Name : ABC root CA

Is this CA certificate: No

Key Length: 1024

Signature Algorithm: SHA1WITHRSA

Country Code: CO

State or Province Name: Colombia

Locality Name: Cali

Organization: ABC

Start Date: 10.5.2017.

End Date: 10.5.2027.

Path to store generate files : G:_PKI\GenCert\GenCert\bin\Debug\CA

Private Key File Name: ABC_CA_private .key

Public Key File Name: ABC_CA_public .cer

Signed Key File Name: ABC_CA_signed .pfx

Password for export private key: ••••

Certificate Frendly name: TelventDMS WebApp

Generate Request and Certificate Application | Menu option: Create SelfSign Cert.

<Style TargetType="{x:Type Button}"...>

GENERATE CERTIFICATE - APPLICATION

Certificate Frendly name: TelventDMS WebApp

Path for signed request file (.cer): Select .cer file path [Browse]

Path for private key file (.key): Select .key file path [Browse]

Path for generate certificate file (.pfx): G:_PKI\GenCert\GenCert\bin\Debug [Browse]

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

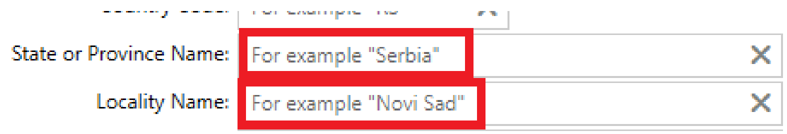
Password for export private key: Password

Path for CA file (.cer) (Optional): Select CA .cer file path [Browse]

Generate Request and Certificate Application | Menu option:

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

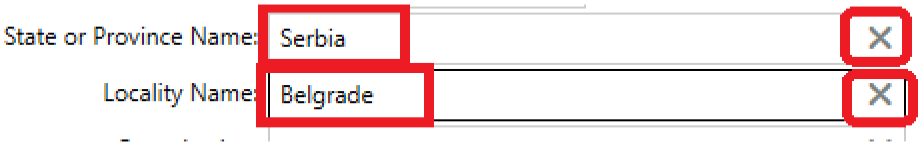
On the open form for any menu option you will found different UI elements (textboxes, comboboxes, checkcomboboxes, passwords, ... etc.).
When textbox is empty, you will see watermark message as help, what you need to enter inside that textbox (picture below).



State or Province Name: For example "Serbia"

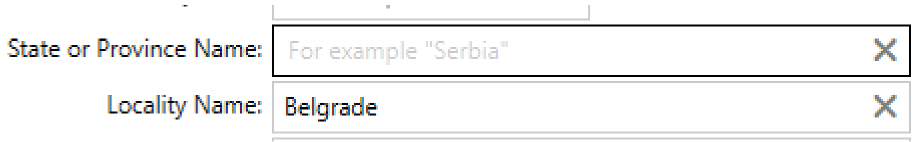
Locality Name: For example "Novi Sad"

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).



State or Province Name: Serbia

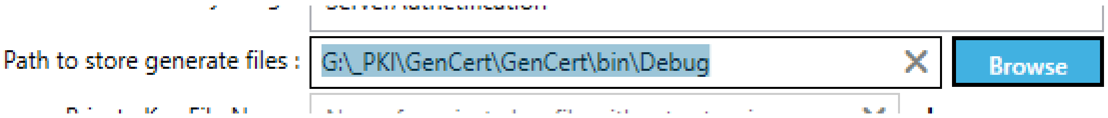
Locality Name: Belgrade



State or Province Name: For example "Serbia"

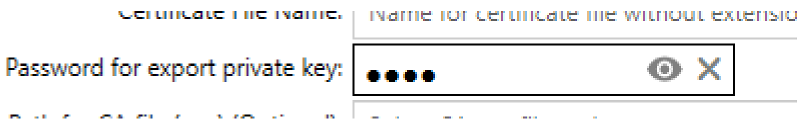
Locality Name: Belgrade

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



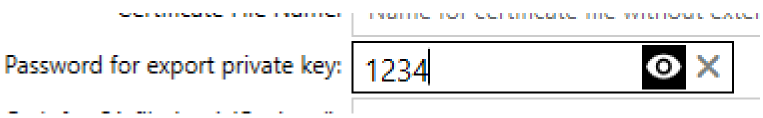
Path to store generate files : G:_PKI\GenCert\GenCert\bin\Debug

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



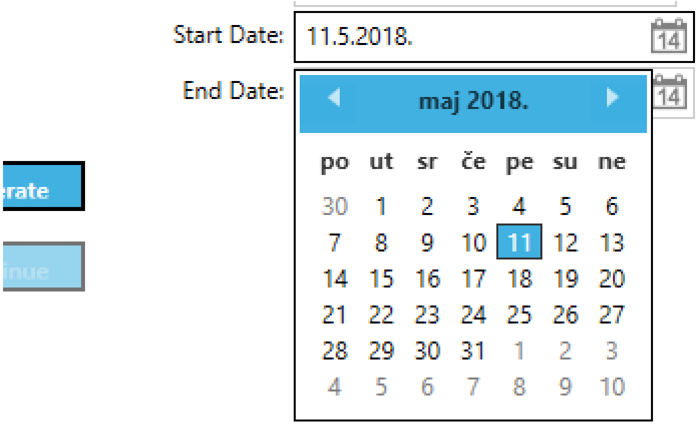
Password for export private key: ●●●●

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)



Password for export private key: 1234

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)



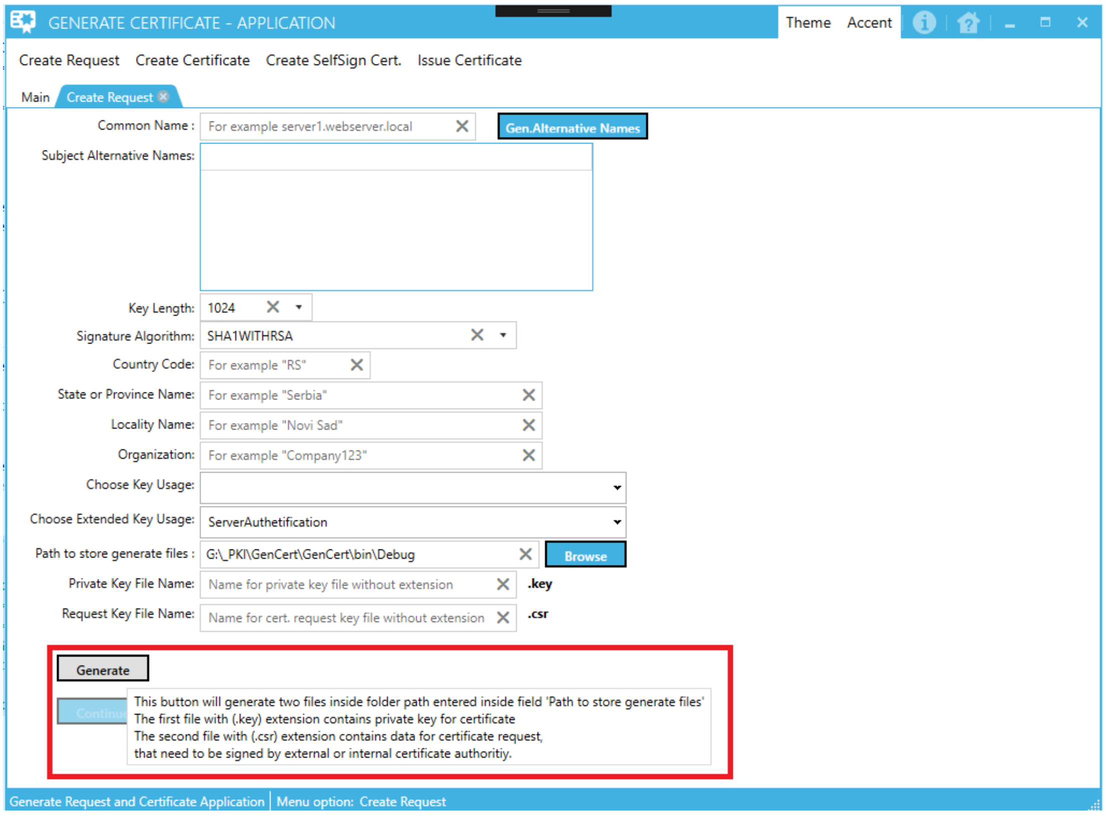
Start Date: 11.5.2018.

End Date:

maj 2018.

po	ut	sr	če	pe	su	ne
30	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

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:



Common Name : For example server1.webserver.local

Subject Alternative Names:

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\GenCert\bin\Debug

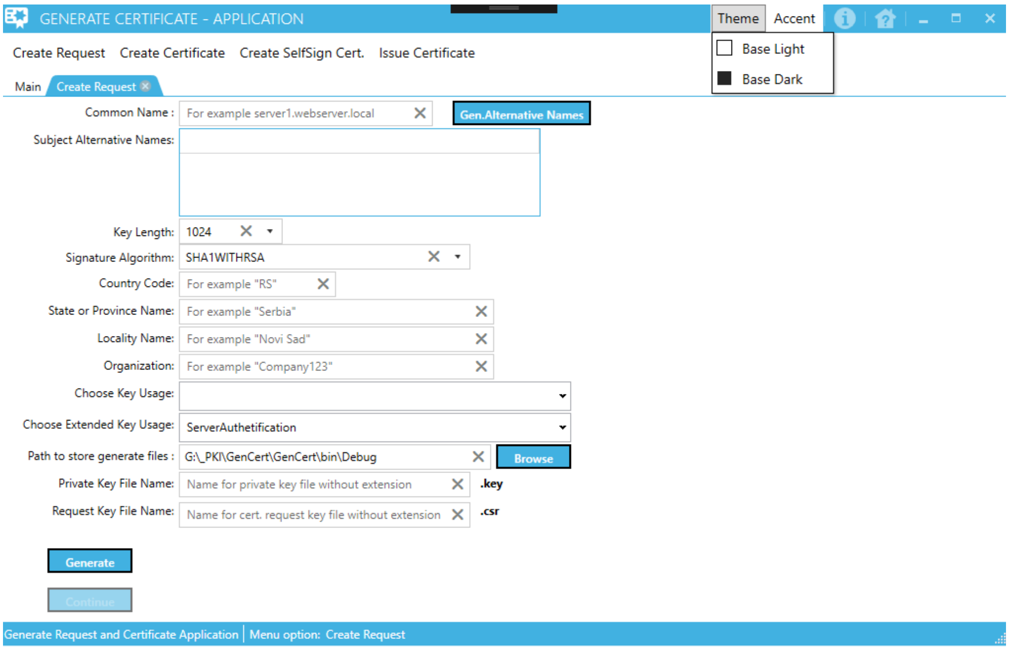
Private Key File Name: Name for private key file without extension .key

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

This button will generate two files inside folder path entered inside field 'Path to store generate files'
The first file with (.key) extension contains private key for certificate
The second file with (.csr) extension contains data for certificate request,
that need to be signed by external or internal certificate authoritiy.

Generate Request and Certificate Application | Menu option: Create Request

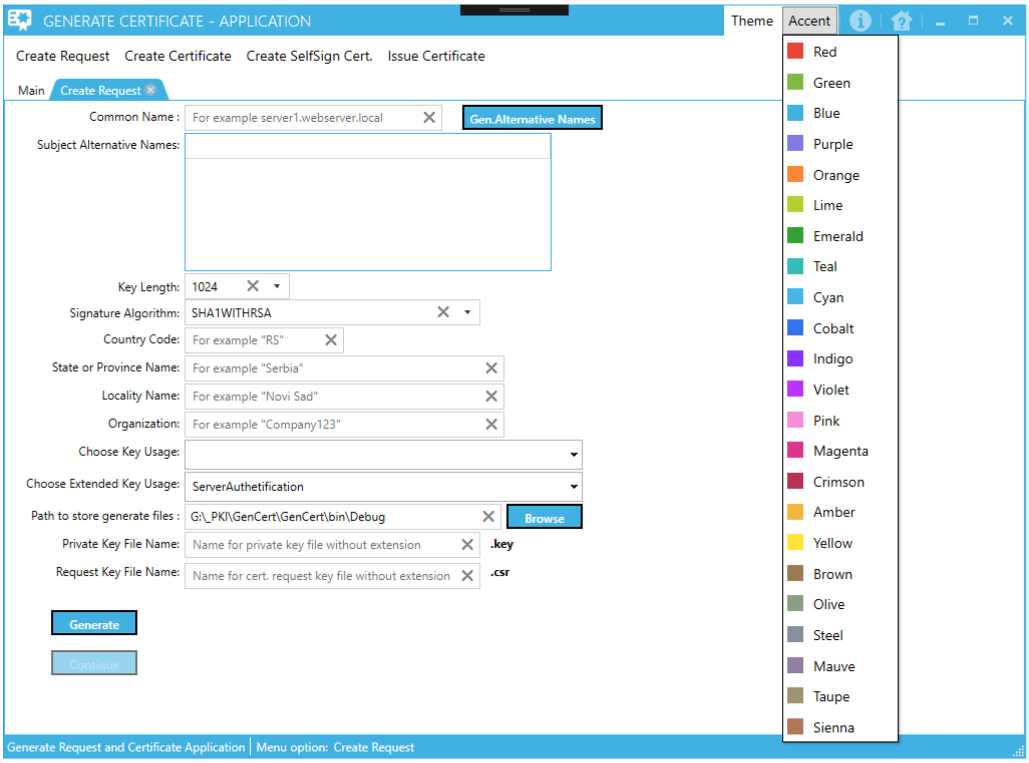
When you click on the Theme button on the application title bar, menu options for application themes will be open. You can choose between “Base Light” (see picture under) and “Base Dark” theme.



Common Name : For example server1.webserver.local
Subject Alternative Names:
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\GenCert\bin\Debug
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 Request and Certificate Application | Menu option: Create Request

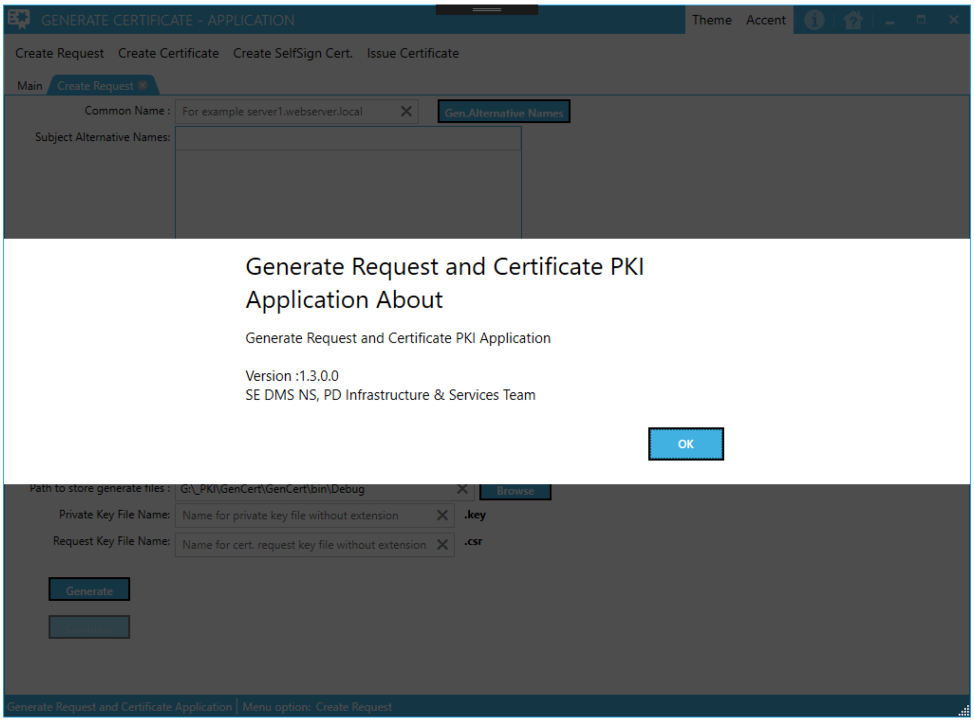
When you click on the Accent button on the application title bar, menu options for application color theme will be open. You can choose between 23 color themes.



Common Name : For example server1.webserver.local
Subject Alternative Names:
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\GenCert\bin\Debug
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 Request and Certificate Application | Menu option: Create Request

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



Common Name : For example server1.webserver.local

Subject Alternative Names:

Generate Request and Certificate PKI Application About

Generate Request and Certificate PKI Application

Version :1.3.0.0
SE DMS NS, PD Infrastructure & Services Team

OK

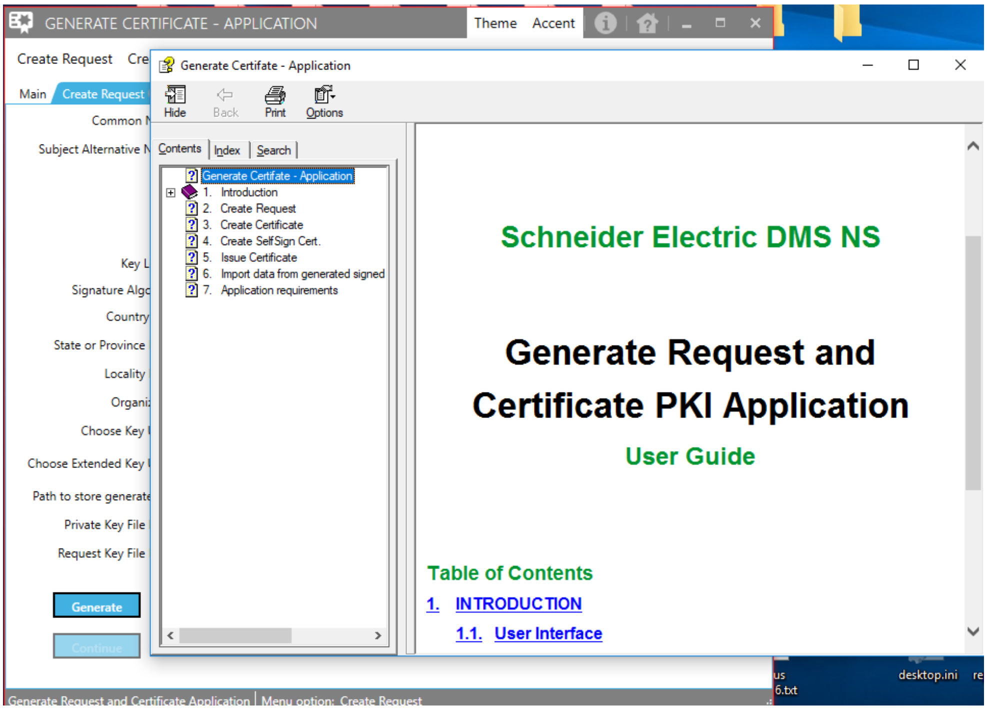
Path to store generate files : G:_PKI\GenCert\GenCert\bin\Debug

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 Request and Certificate Application | Menu option: Create Request

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



Generate Certifate - Application
1. Introduction
2. Create Request
3. Create Certificate
4. Create SelfSign Cert.
5. Issue Certificate
6. Import data from generated signed
7. Application requirements

Schneider Electric DMS NS

Generate Request and Certificate PKI Application

User Guide

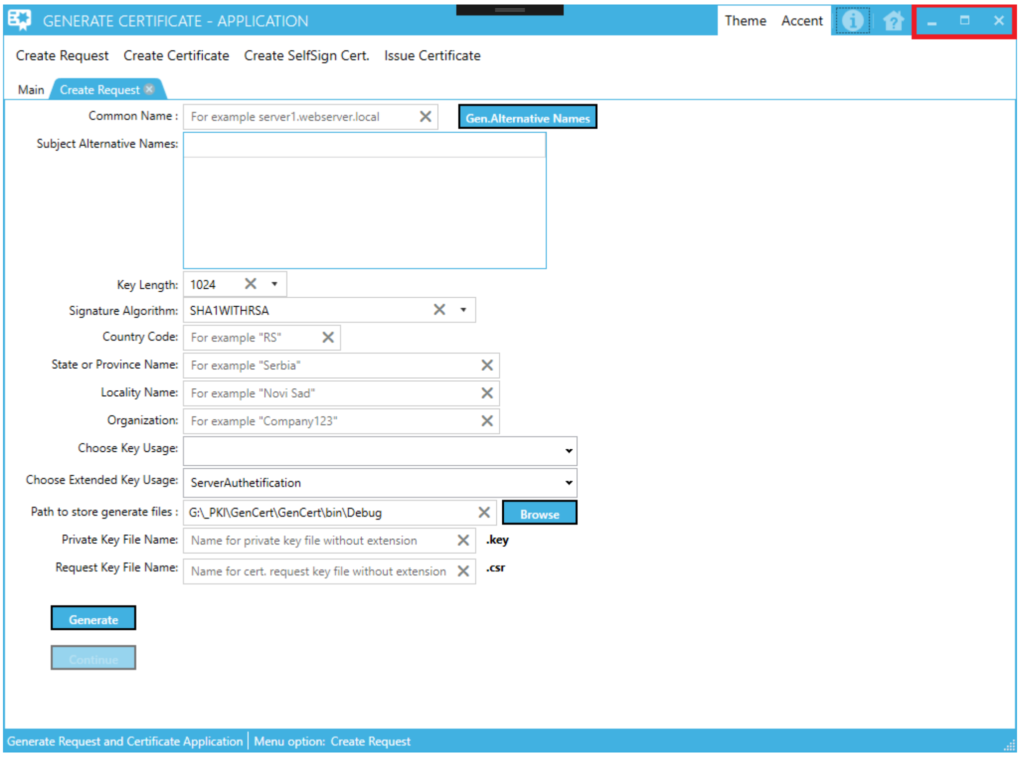
Table of Contents

1. INTRODUCTION

1.1. User Interface

Generate Request and Certificate Application | Menu option: Create Request

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



Common Name : For example server1.webserver.local

Subject Alternative Names:

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

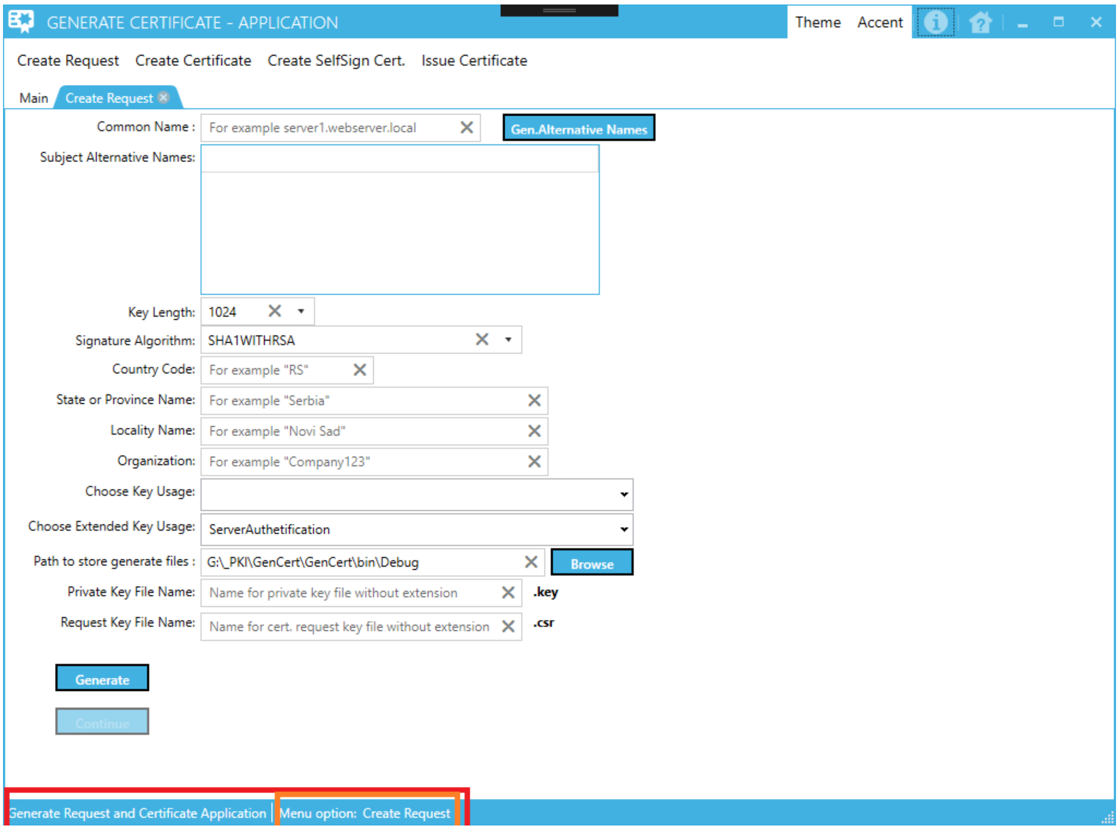
Path to store generate files : G:_PKI\GenCert\GenCert\bin\Debug

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 Request and Certificate Application | Menu option: Create Request

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



Common Name : For example server1.webserver.local

Subject Alternative Names:

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

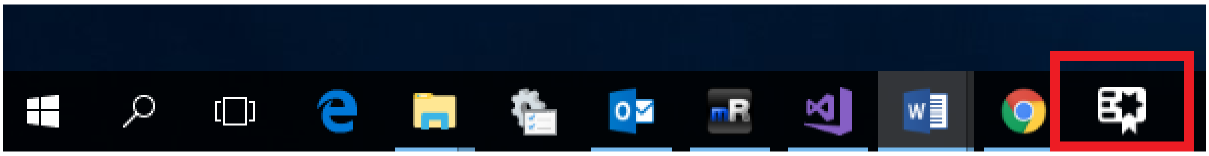
Path to store generate files : G:_PKI\GenCert\GenCert\bin\Debug

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

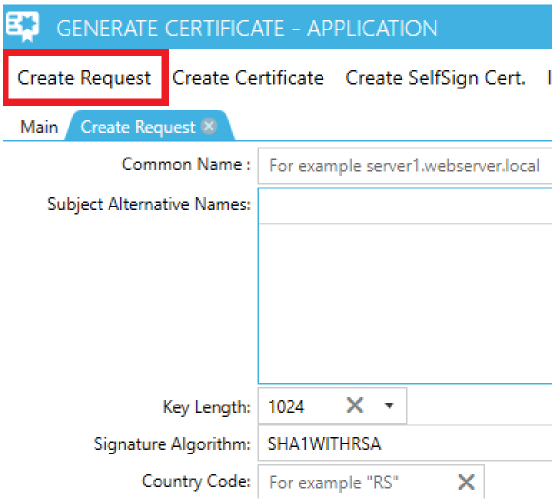
Generate Request and Certificate Application | Menu option: Create Request

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



2. CREATE REQUEST

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



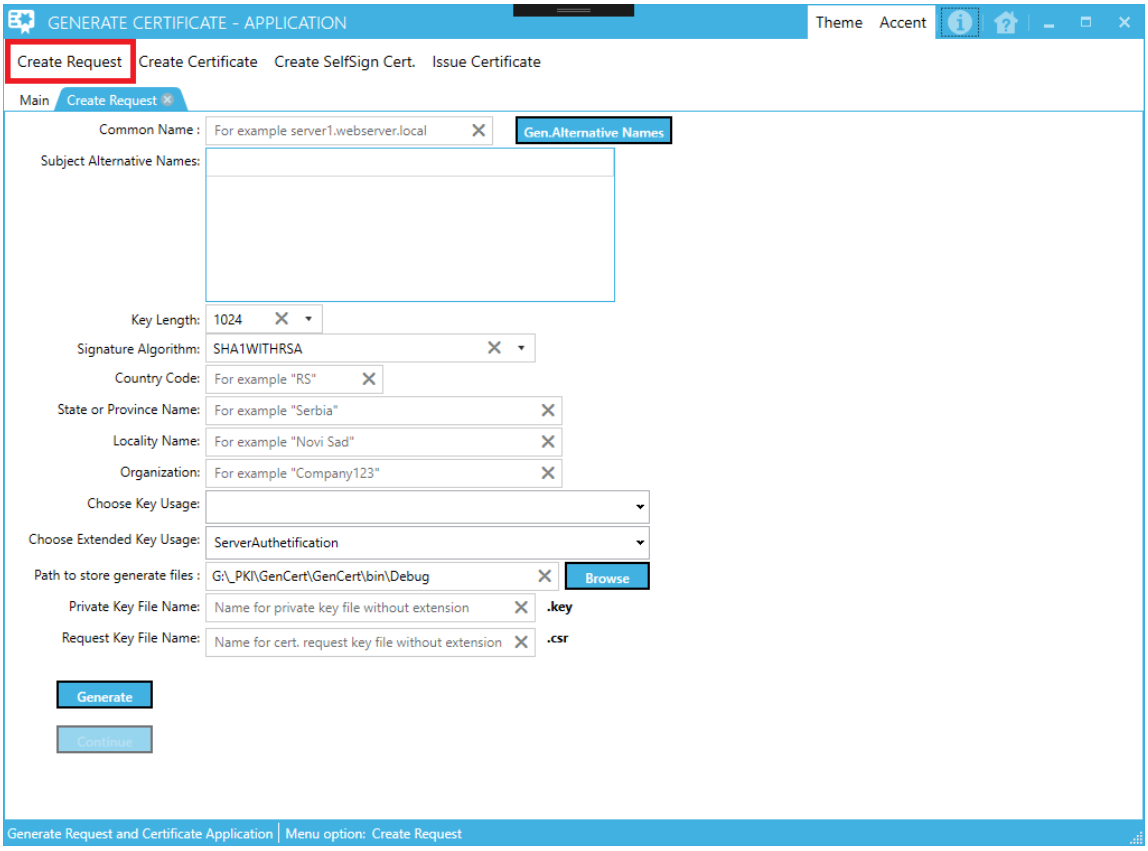
Common Name : For example server1.webserver.local

Subject Alternative Names:

Key Length: 1024

Signature Algorithm: SHA1WITHRSA

Country Code: For example "RS"



Common Name : For example server1.webserver.local

Subject Alternative Names:

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\GenCert\bin\Debug

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

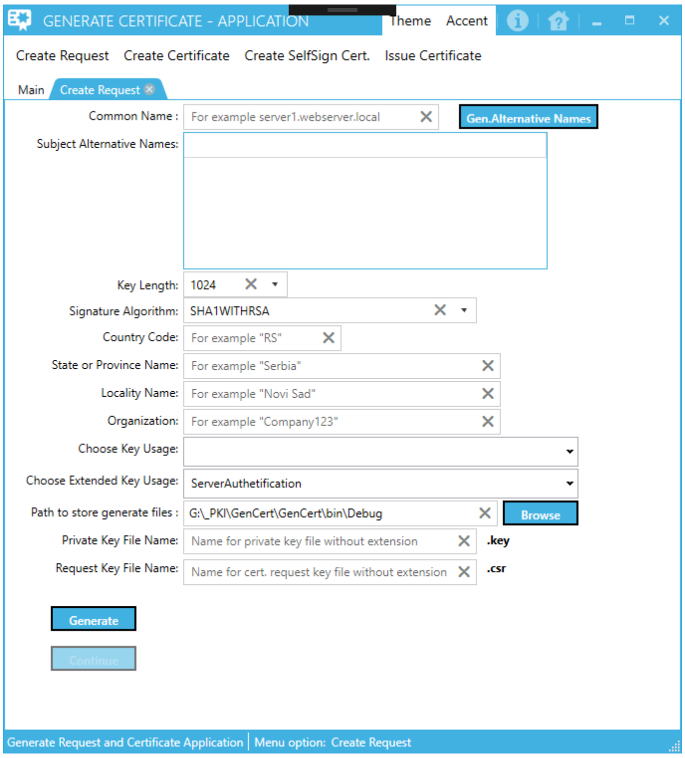
Request Key File Name: Name for cert. request key file without extension .csr

Generate Request and Certificate Application | Menu option: Create Request

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.



Common Name : For example server1.webserver.local

Subject Alternative Names:

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:

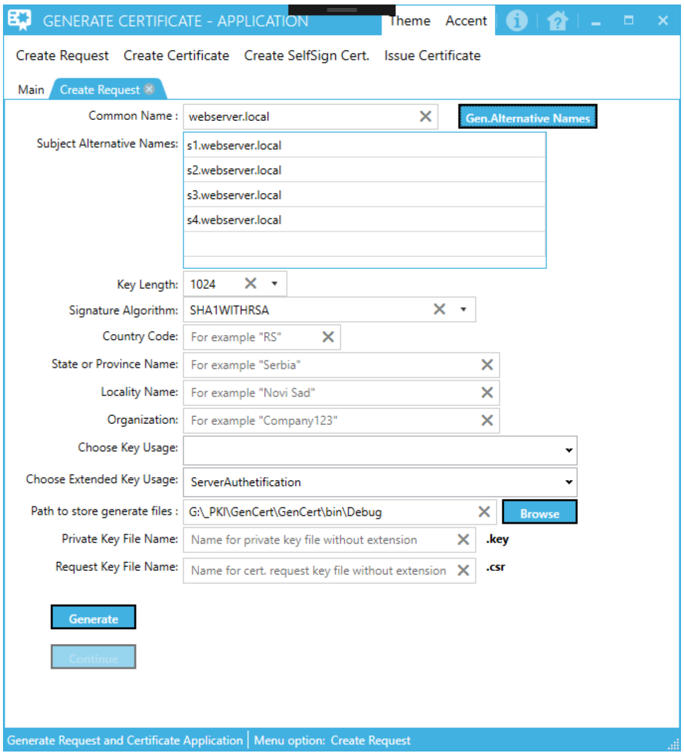
Choose Extended Key Usage: ServerAuthetification

Path to store generate files : G:_PKI\GenCert\GenCert\bin\Debug

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 Request and Certificate Application | Menu option: Create Request



Common Name : webserver.local

Subject Alternative Names:

s1.webserver.local
s2.webserver.local
s3.webserver.local
s4.webserver.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\GenCert\bin\Debug

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 Request and Certificate Application | Menu option: Create Request

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)

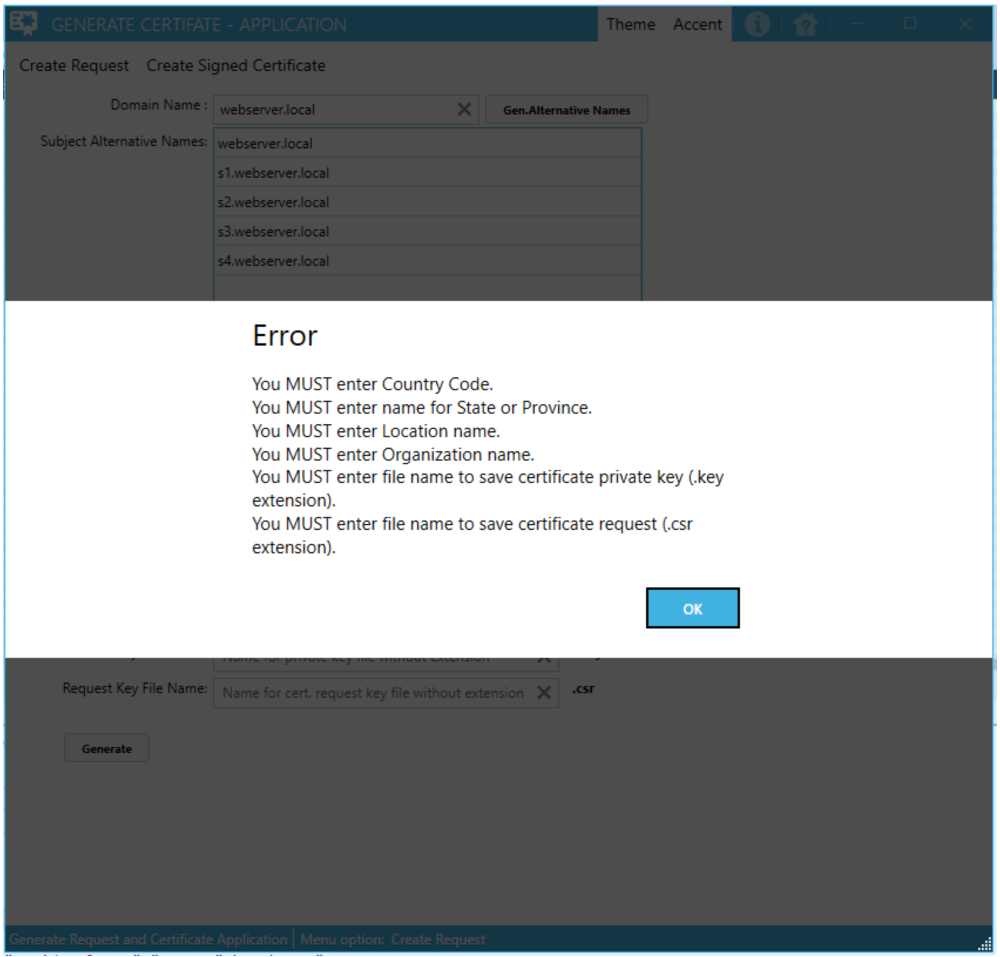
If everting is OK, form will be generated 2 files. Inside directory path entered inside field "Path to store generate files:", you will find two files. First file with .key extension (certificate private key file) and the second file with .csr extension (certificate request file).

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:



Domain Name : webserver.local

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

Error

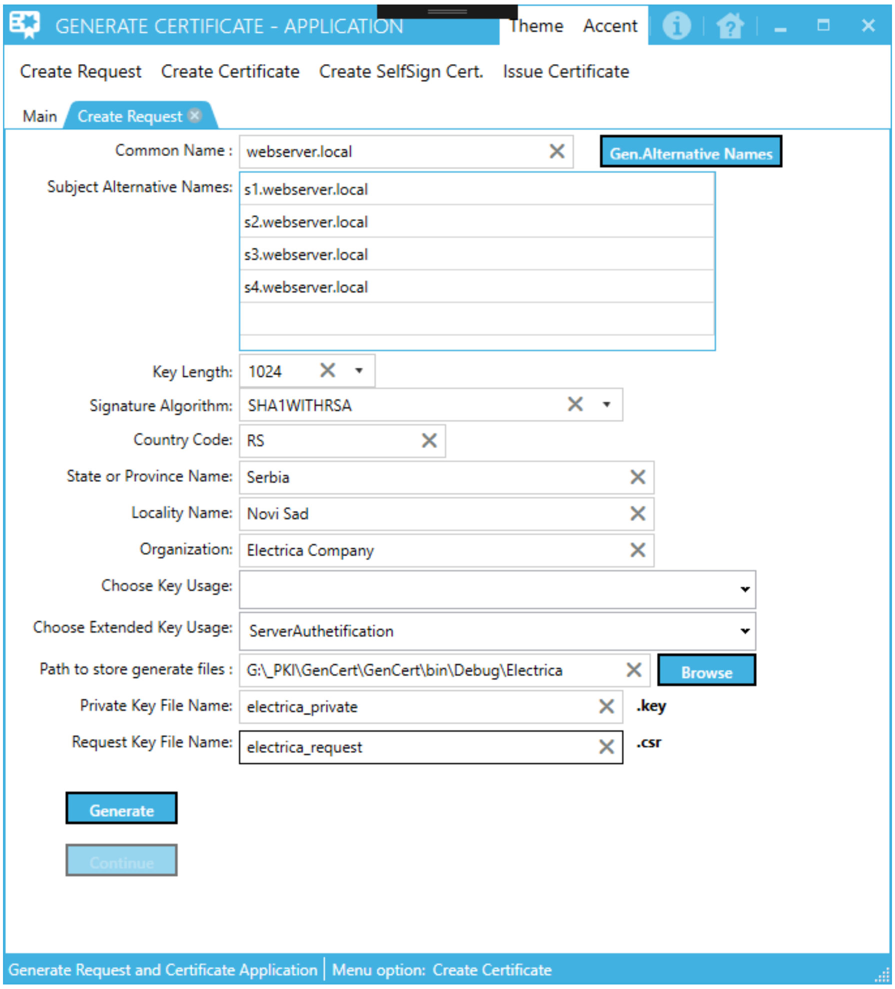
You MUST enter Country Code.
You MUST enter name for State or Province.
You MUST enter Location name.
You MUST enter Organization name.
You MUST enter file name to save certificate private key (.key extension).
You MUST enter file name to save certificate request (.csr extension).

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

Generate Request and Certificate Application | Menu option: Create Request

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.



Common Name : webserver.local

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

Key Length: 1024

Signature Algorithm: SHA1WITHRSA

Country Code: RS

State or Province Name: Serbia

Locality Name: Novi Sad

Organization: Electrica Company

Choose Key Usage:

Choose Extended Key Usage: ServerAuthetification

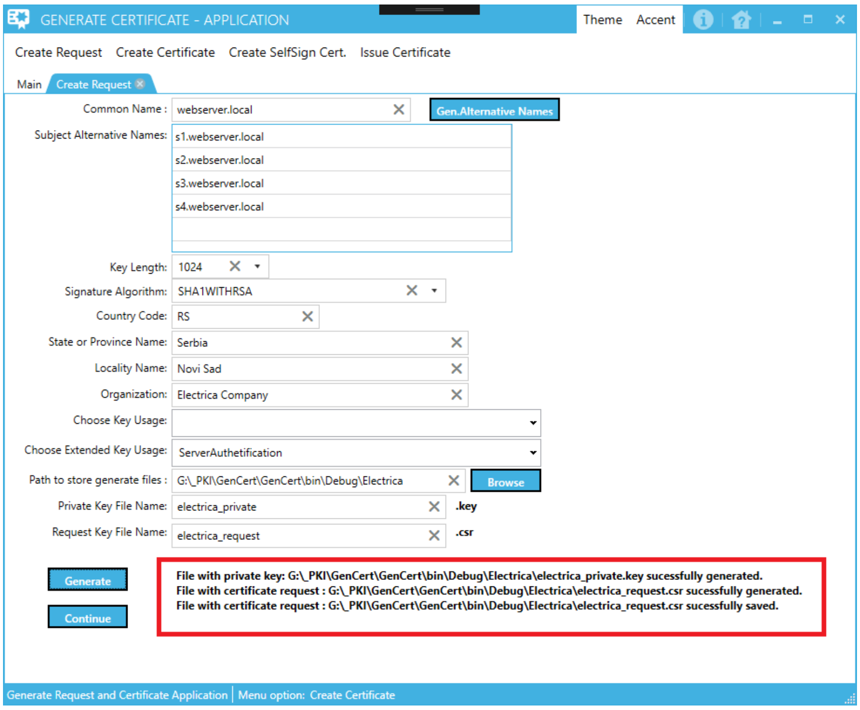
Path to store generate files : G:_PKI\GenCert\GenCert\bin\Debug\Electrica

Private Key File Name: electrica_private .key

Request Key File Name: electrica_request .csr

Generate Request and Certificate Application | Menu option: Create Certificate

Click Generate



Common Name : webserver.local

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

Key Length: 1024

Signature Algorithm: SHA1WITHRSA

Country Code: RS

State or Province Name: Serbia

Locality Name: Novi Sad

Organization: Electrica Company

Choose Key Usage:

Choose Extended Key Usage: ServerAuthetification

Path to store generate files : G:_PKI\GenCert\GenCert\bin\Debug\Electrica

Private Key File Name: electrica_private .key

Request Key File Name: electrica_request .csr

```
File with private key: G:\_PKI\GenCert\GenCert\bin\Debug\Electrica\electrica_private.key sucessfully generated.
File with certificate request : G:\_PKI\GenCert\GenCert\bin\Debug\Electrica\electrica_request.csr sucessfully generated.
File with certificate request : G:\_PKI\GenCert\GenCert\bin\Debug\Electrica\electrica_request.csr sucessfully saved.
```

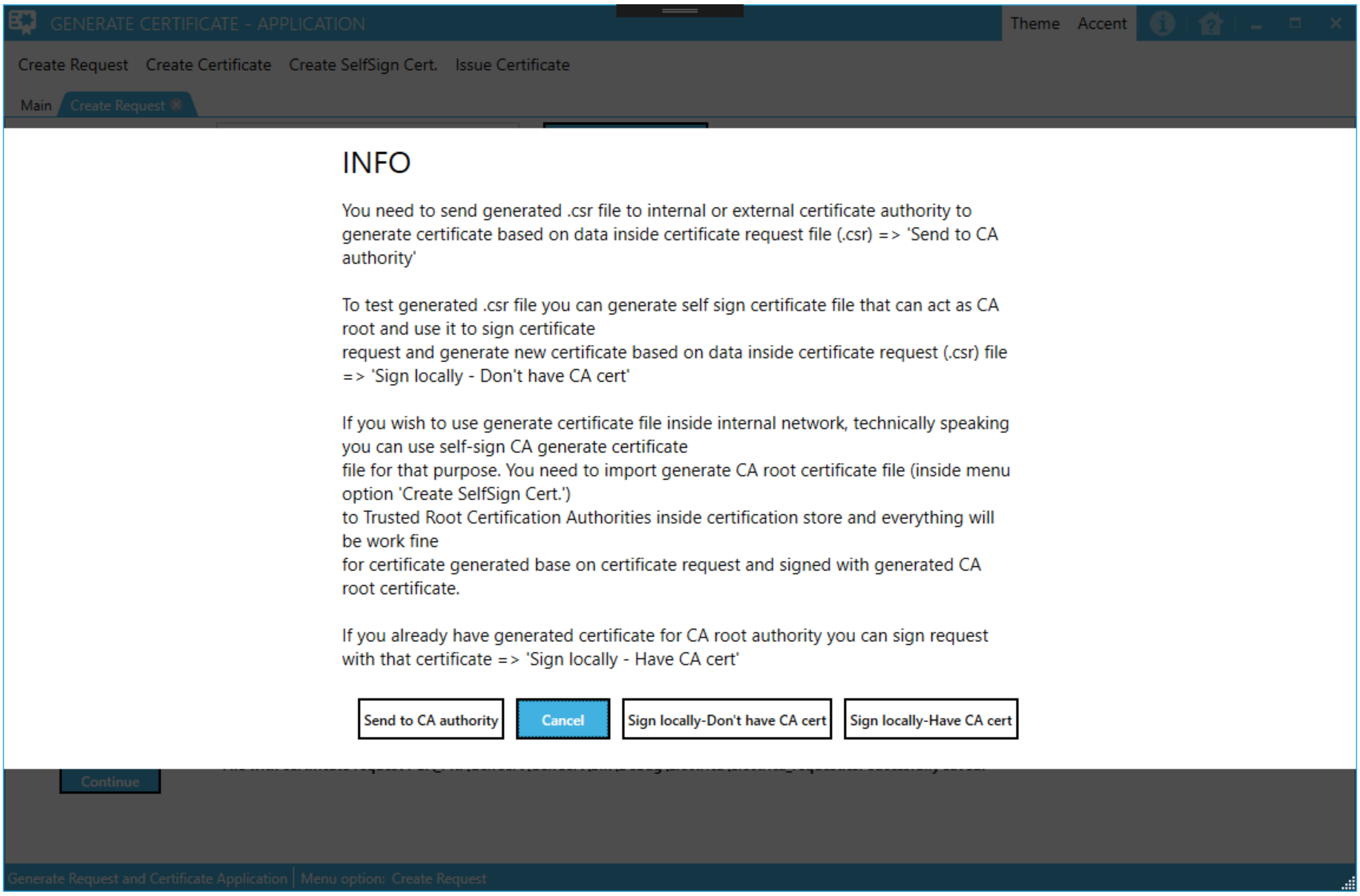
Generate Request and Certificate Application | Menu option: Create Certificate

Messages shown upper inside red square 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.



INFO

You need to send generated .csr file to internal or external certificate authority to generate certificate based on data inside certificate request file (.csr) => 'Send to CA authority'

To test generated .csr file you can generate self sign certificate file that can act as CA root and use it to sign certificate
request and generate new certificate based on data inside certificate request (.csr) file => 'Sign locally - Don't have CA cert'

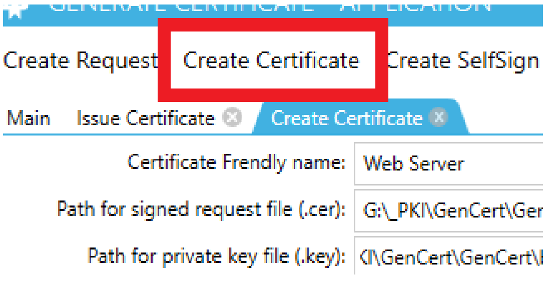
If you wish to use generate certificate file inside internal network, technically speaking you can use self-sign CA generate certificate
file for that purpose. You need to import generate CA root certificate file (inside menu option 'Create SelfSign Cert.')
to Trusted Root Certification Authorities inside certification store and everything will be work fine
for certificate generated base on certificate request and signed with generated CA root certificate.

If you already have generated certificate for CA root authority you can sign request with that certificate => 'Sign locally - Have CA cert'

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.").

3. CREATE CERTIFICATE

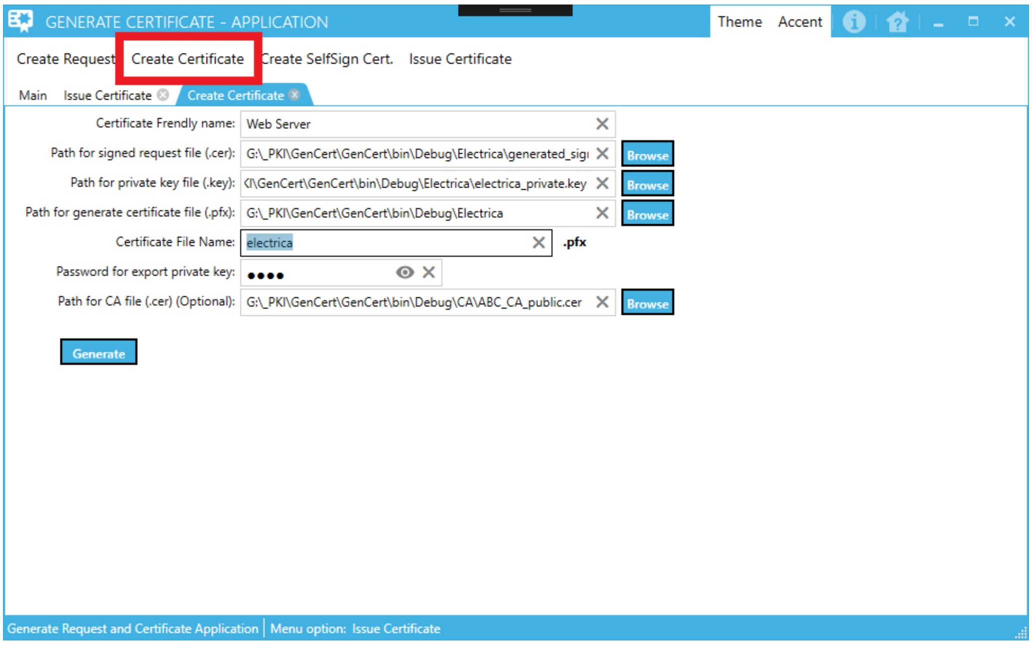
This option is used to create certificate request file, that will be send to external certificate authority to be signed .



Certificate Frendly name: Web Server

Path for signed request file (.cer): G:_PKI\GenCert\Ger

Path for private key file (.key): (I\GenCert\GenCert\I



Certificate Frendly name: Web Server

Path for signed request file (.cer): G:_PKI\GenCert\GenCert\bin\Debug\Electrica\generated_sig

Path for private key file (.key): (I\GenCert\GenCert\bin\Debug\Electrica\electrica_private.key

Path for generate certificate file (.pfx): G:_PKI\GenCert\GenCert\bin\Debug\Electrica

Certificate File Name: electrica .pfx

Password for export private key: ●●●●

Path for CA file (.cer) (Optional): G:_PKI\GenCert\GenCert\bin\Debug\CA\ABC_CA_public.cer

Generate Request and Certificate Application | Menu option: Issue Certificate

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

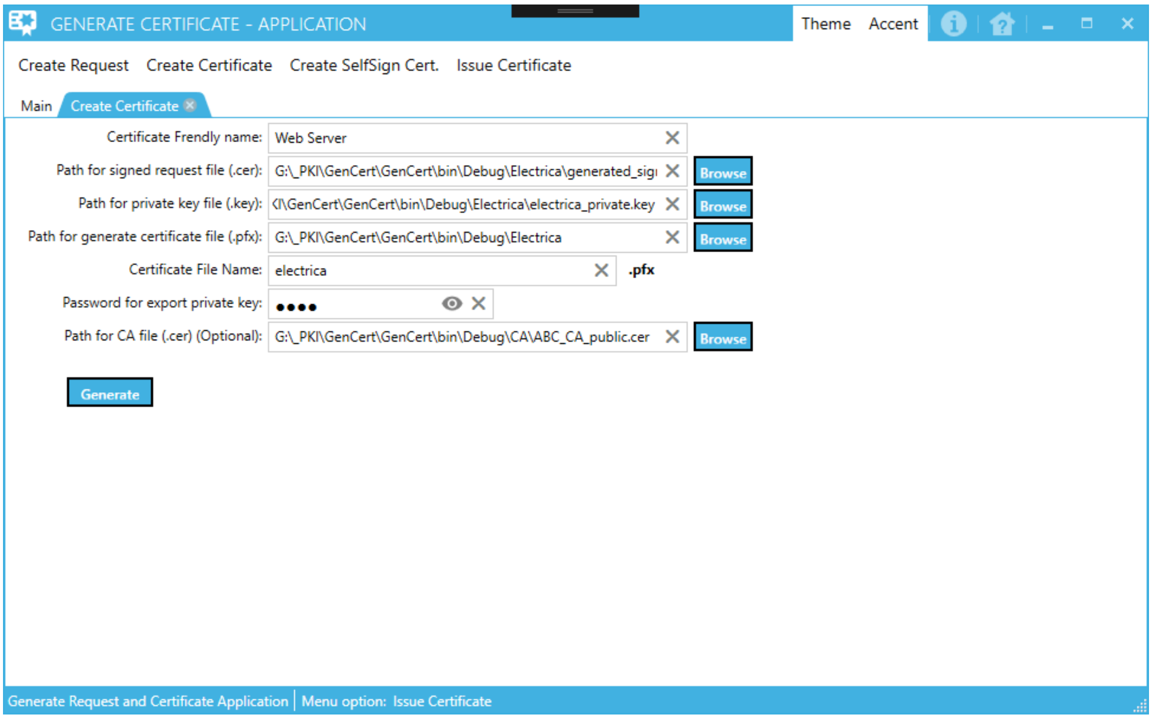
You can enter data manually or click on the “Browse” buttons to select appropriate files and output directory where generate file (.pfx extension) will be generate.

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.



Certificate Frendly name: Web Server

Path for signed request file (.cer): G:_PKI\GenCert\GenCert\bin\Debug\Electrica\generated_sigı

Path for private key file (.key): <I\GenCert\GenCert\bin\Debug\Electrica\electrica_private.key

Path for generate certificate file (.pfx): G:_PKI\GenCert\GenCert\bin\Debug\Electrica

Certificate File Name: electrica .pfx

Password for export private key: ●●●●

Path for CA file (.cer) (Optional): G:_PKI\GenCert\GenCert\bin\Debug\CA\ABC_CA_public.cer

Generate Request and Certificate Application | Menu option: Issue Certificate

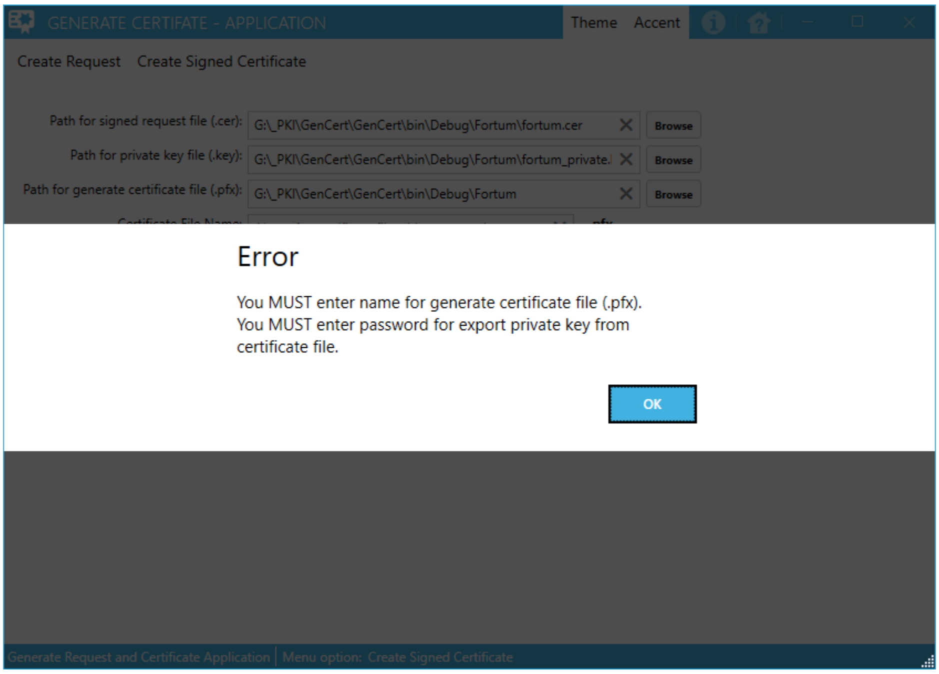
When you fill all fields inside form click on the button “Generate” to create files.

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:



Path for signed request file (.cer): G:_PKI\GenCert\GenCert\bin\Debug\Fortum\fortum.cer

Path for private key file (.key): G:_PKI\GenCert\GenCert\bin\Debug\Fortum\fortum_private.

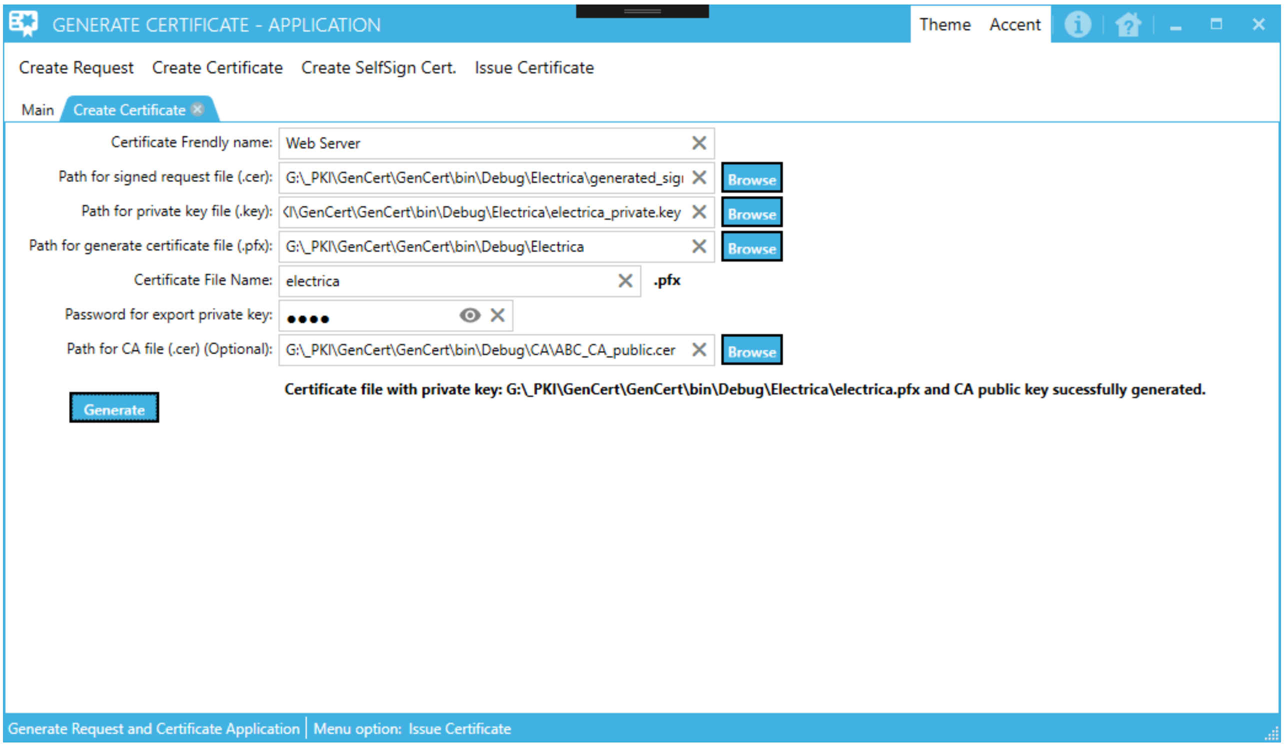
Path for generate certificate file (.pfx): G:_PKI\GenCert\GenCert\bin\Debug\Fortum

Error

You MUST enter name for generate certificate file (.pfx).
You MUST enter password for export private key from certificate file.

Generate Request and Certificate Application | Menu option: Create Signed Certificate

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



Certificate Frendly name: Web Server

Path for signed request file (.cer): G:_PKI\GenCert\GenCert\bin\Debug\Electrica\generated_sig

Path for private key file (.key): \GenCert\GenCert\bin\Debug\Electrica\electrica_private.key

Path for generate certificate file (.pfx): G:_PKI\GenCert\GenCert\bin\Debug\Electrica

Certificate File Name: electrica .pfx

Password for export private key: ••••

Path for CA file (.cer) (Optional): G:_PKI\GenCert\GenCert\bin\Debug\CA\ABC_CA_public.cer

Certificate file with private key: G:_PKI\GenCert\GenCert\bin\Debug\Electrica\electrica.pfx and CA public key sucessfully generated.

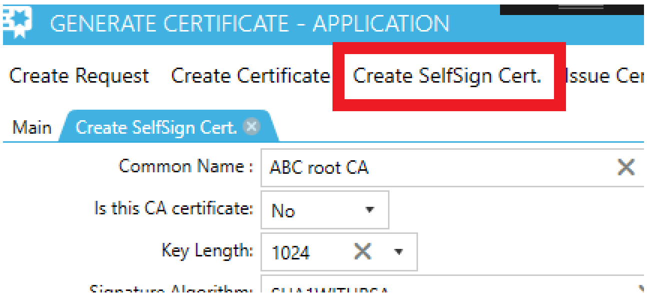
Generate Request and Certificate Application | Menu option: Issue Certificate

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

See chapter 6, how to import data from generated certificate file to computer certificate store.

4. CREATE SELFSIGN CERT.

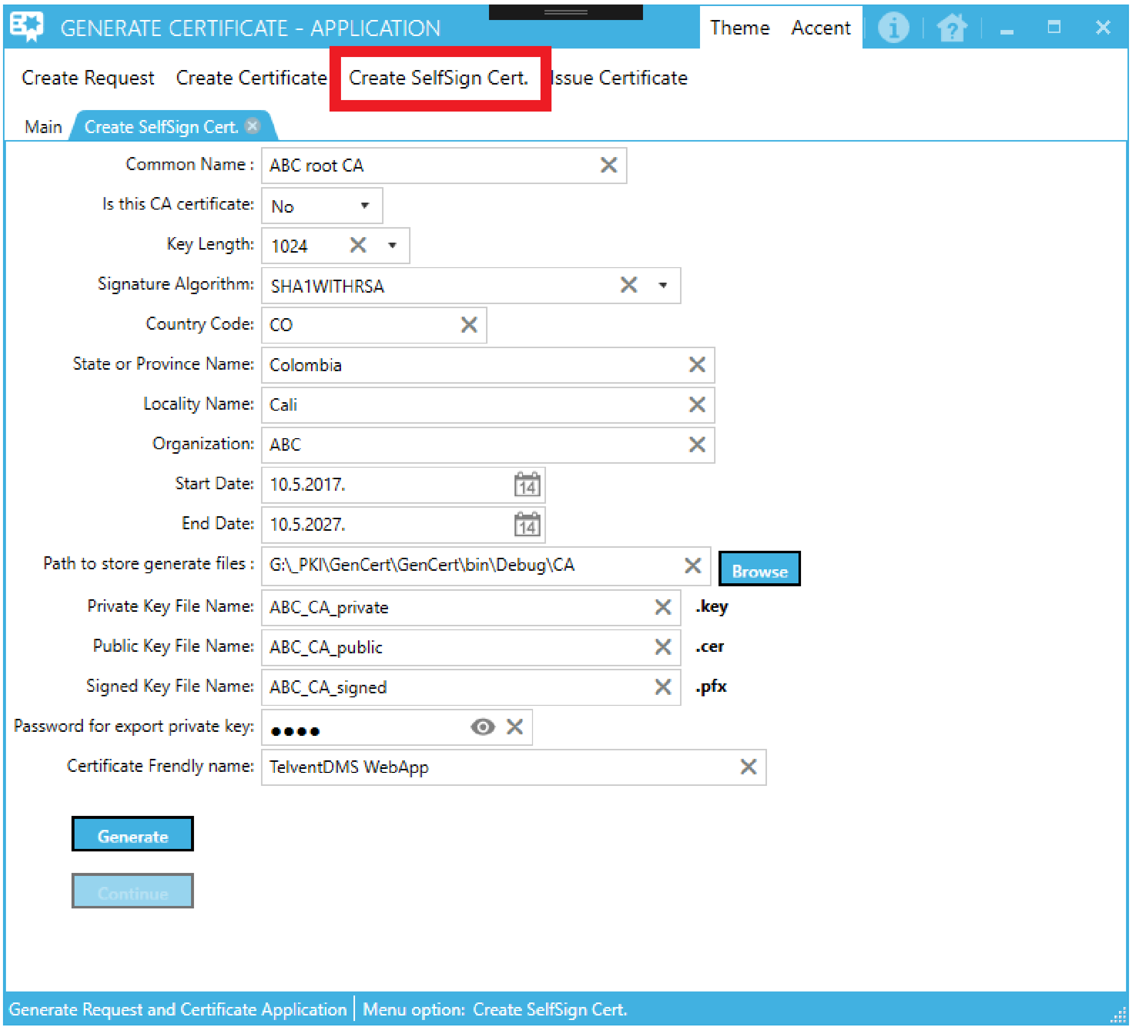
This option is used to create self-sign certificate or create self-sign certificate for CA root .



Common Name : ABC root CA

Is this CA certificate: No

Key Length: 1024



Common Name : ABC root CA

Is this CA certificate: No

Key Length: 1024

Signature Algorithm: SHA1WITHRSA

Country Code: CO

State or Province Name: Colombia

Locality Name: Cali

Organization: ABC

Start Date: 10.5.2017.

End Date: 10.5.2027.

Path to store generate files : G:_PKI\GenCert\GenCert\bin\Debug\CA

Private Key File Name: ABC_CA_private .key

Public Key File Name: ABC_CA_public .cer

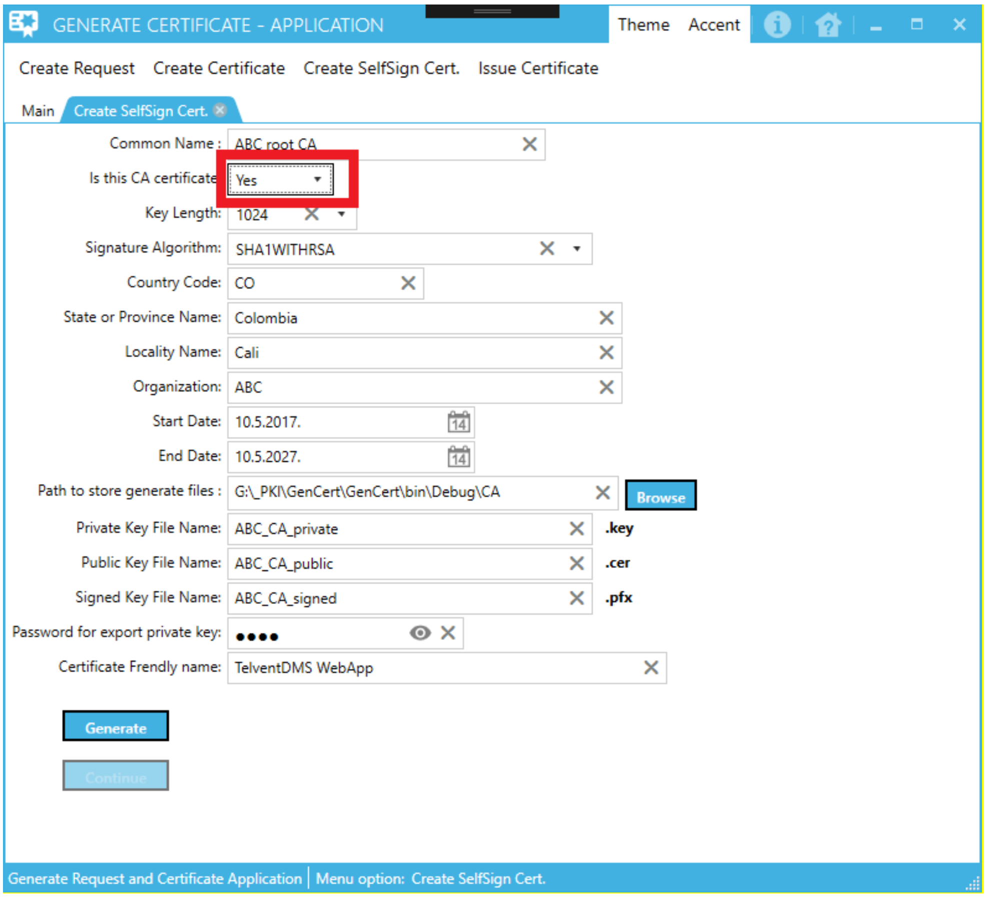
Signed Key File Name: ABC_CA_signed .pfx

Password for export private key: ●●●●

Certificate Frendly name: TelventDMS WebApp

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.



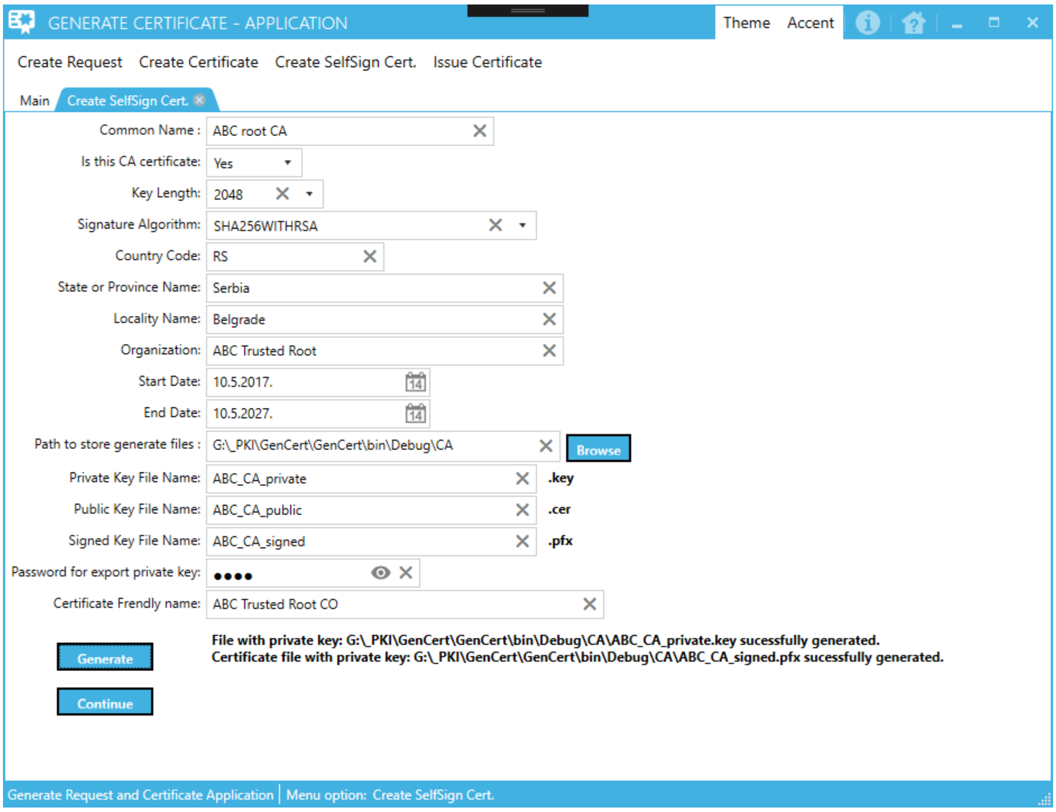
Common Name :	ABC root CA	
Is this CA certificate	Yes	
Key Length:	1024	
Signature Algorithm:	SHA1WITHRSA	
Country Code:	CO	
State or Province Name:	Colombia	
Locality Name:	Cali	
Organization:	ABC	
Start Date:	10.5.2017.	
End Date:	10.5.2027.	
Path to store generate files :	G:_PKI\GenCert\GenCert\bin\Debug\CA	
Private Key File Name:	ABC_CA_private	.key
Public Key File Name:	ABC_CA_public	.cer
Signed Key File Name:	ABC_CA_signed	.pfx
Password for export private key:	••••	
Certificate Frendly name:	TelventDMS WebApp	

Generate Request and Certificate Application | Menu option: Create SelfSign Cert.

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.

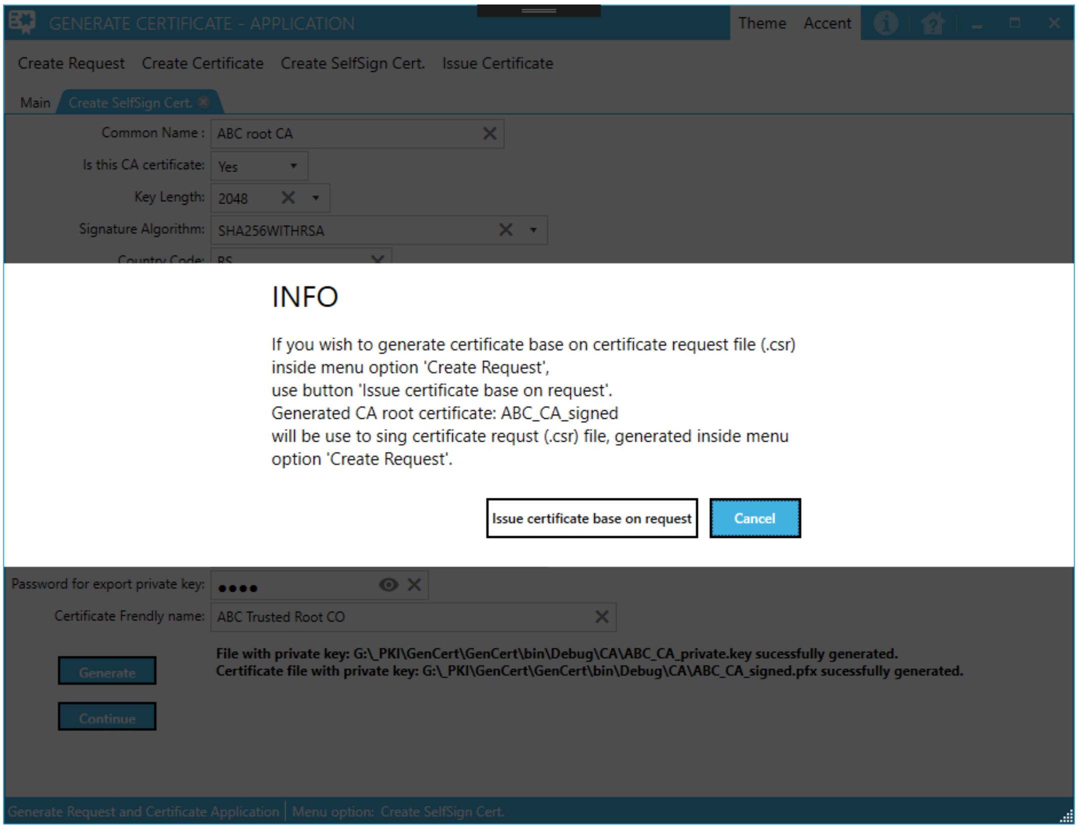


Common Name : ABC root CA
Is this CA certificate: Yes
Key Length: 2048
Signature Algorithm: SHA256WITHRSA
Country Code: RS
State or Province Name: Serbia
Locality Name: Belgrade
Organization: ABC Trusted Root
Start Date: 10.5.2017.
End Date: 10.5.2027.
Path to store generate files : G:_PKI\GenCert\GenCert\bin\Debug\CA
Private Key File Name: ABC_CA_private .key
Public Key File Name: ABC_CA_public .cer
Signed Key File Name: ABC_CA_signed .pfx
Password for export private key: ●●●●
Certificate Frendly name: ABC Trusted Root CO

File with private key: G:_PKI\GenCert\GenCert\bin\Debug\CA\ABC_CA_private.key sucessfully generated.
Certificate file with private key: G:_PKI\GenCert\GenCert\bin\Debug\CA\ABC_CA_signed.pfx sucessfully generated.

Generate Request and Certificate Application | Menu option: Create SelfSign Cert.

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



Common Name : ABC root CA
Is this CA certificate: Yes
Key Length: 2048
Signature Algorithm: SHA256WITHRSA

INFO

If you wish to generate certificate base on certificate request file (.csr)
inside menu option 'Create Request',
use button 'Issue certificate base on request'.
Generated CA root certificate: ABC_CA_signed
will be use to sing certificate requst (.csr) file, generated inside menu
option 'Create Request'.

Password for export private key: ●●●●
Certificate Frendly name: ABC Trusted Root CO

File with private key: G:_PKI\GenCert\GenCert\bin\Debug\CA\ABC_CA_private.key sucessfully generated.
Certificate file with private key: G:_PKI\GenCert\GenCert\bin\Debug\CA\ABC_CA_signed.pfx sucessfully generated.

Generate Request and Certificate Application | Menu option: Create SelfSign Cert.

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):"

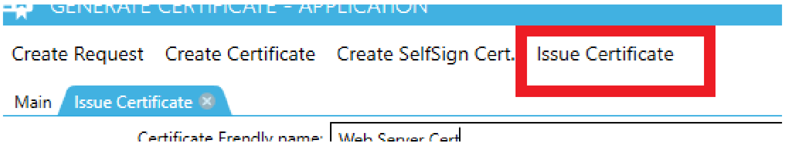
"Path for private key file (.key):"

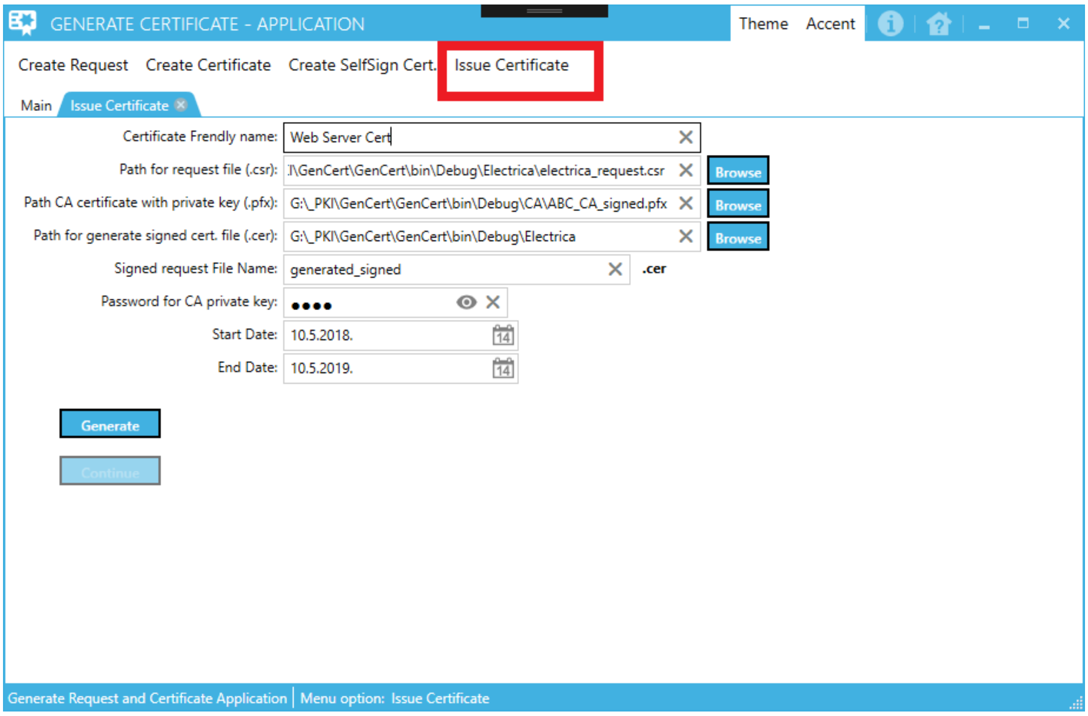
"Path for generate certificate file (.pfx):"

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

5. 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.".





Certificate Frendly name: Web Server Cert

Path for request file (.csr): :\\GenCert\GenCert\bin\Debug\Electrica\electrica_request.csr

Path CA certificate with private key (.pfx): G:_PKI\GenCert\GenCert\bin\Debug\CA\ABC_CA_signed.pfx

Path for generate signed cert. file (.cer): G:_PKI\GenCert\GenCert\bin\Debug\Electrica

Signed request File Name: generated_signed .cer

Password for CA private key: ●●●●

Start Date: 10.5.2018.

End Date: 10.5.2019.

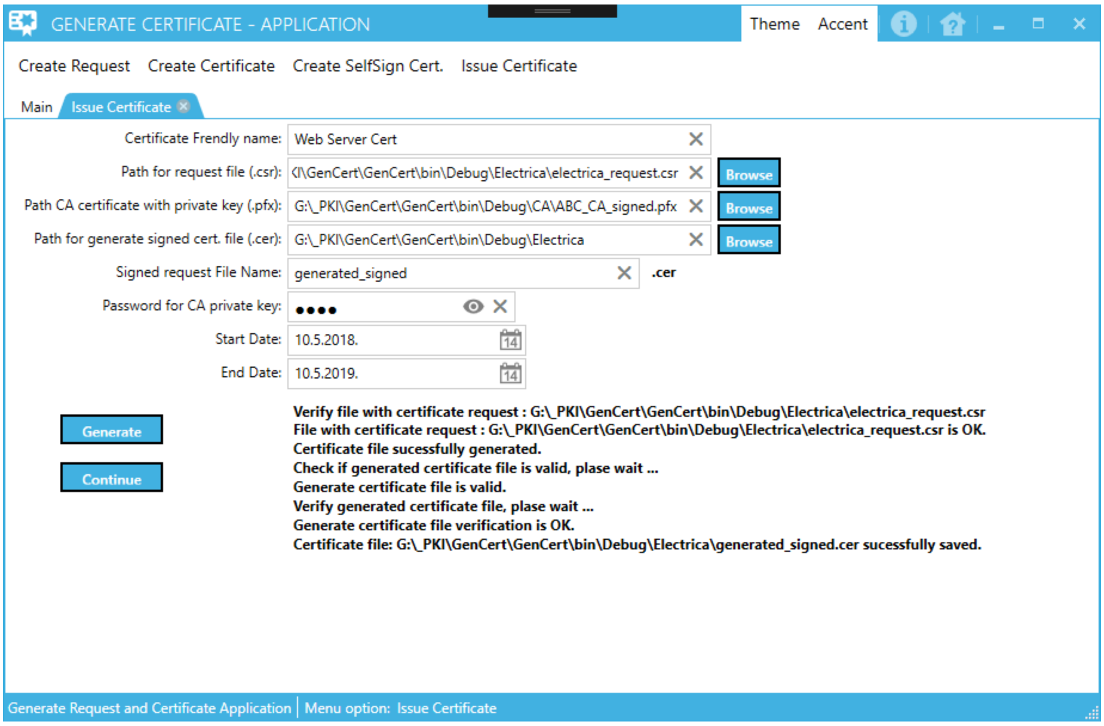
Generate Request and Certificate Application | Menu option: Issue Certificate

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:

1. File with certificate public key (.cer)

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



Certificate Frendly name: Web Server Cert

Path for request file (.csr): :I\GenCert\GenCert\bin\Debug\Electrica\electrica_request.csr

Path CA certificate with private key (.pfx): G:_PKI\GenCert\GenCert\bin\Debug\CA\ABC_CA_signed.pfx

Path for generate signed cert. file (.cer): G:_PKI\GenCert\GenCert\bin\Debug\Electrica

Signed request File Name: generated_signed .cer

Password for CA private key: ●●●●

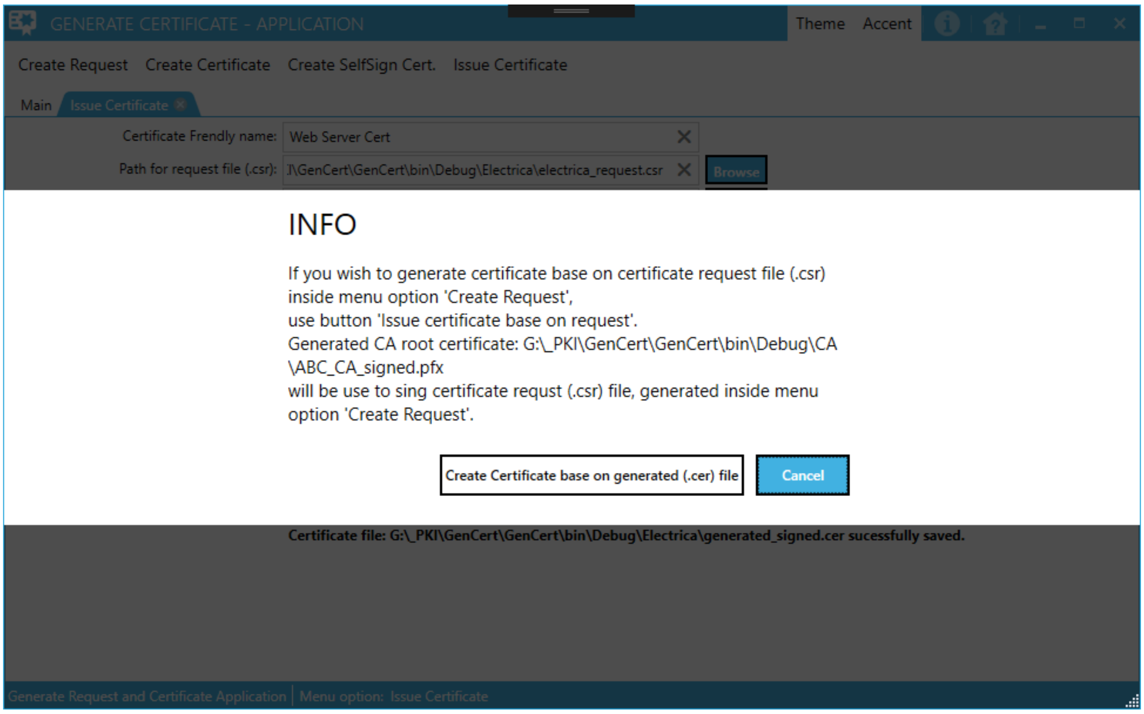
Start Date: 10.5.2018.

End Date: 10.5.2019.

Verify file with certificate request : G:_PKI\GenCert\GenCert\bin\Debug\Electrica\electrica_request.csr
File with certificate request : G:_PKI\GenCert\GenCert\bin\Debug\Electrica\electrica_request.csr is OK.
Certificate file sucessfully generated.
Check if generated certificate file is valid, plase wait ...
Generate certificate file is valid.
Verify generated certificate file, plase wait ...
Generate certificate file verification is OK.
Certificate file: G:_PKI\GenCert\GenCert\bin\Debug\Electrica\generated_signed.cer sucessfully saved.

Generate Request and Certificate Application | Menu option: Issue Certificate

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



Certificate Frendly name: Web Server Cert

Path for request file (.csr):]\GenCert\GenCert\bin\Debug\Electrica\electrica_request.csr

INFO

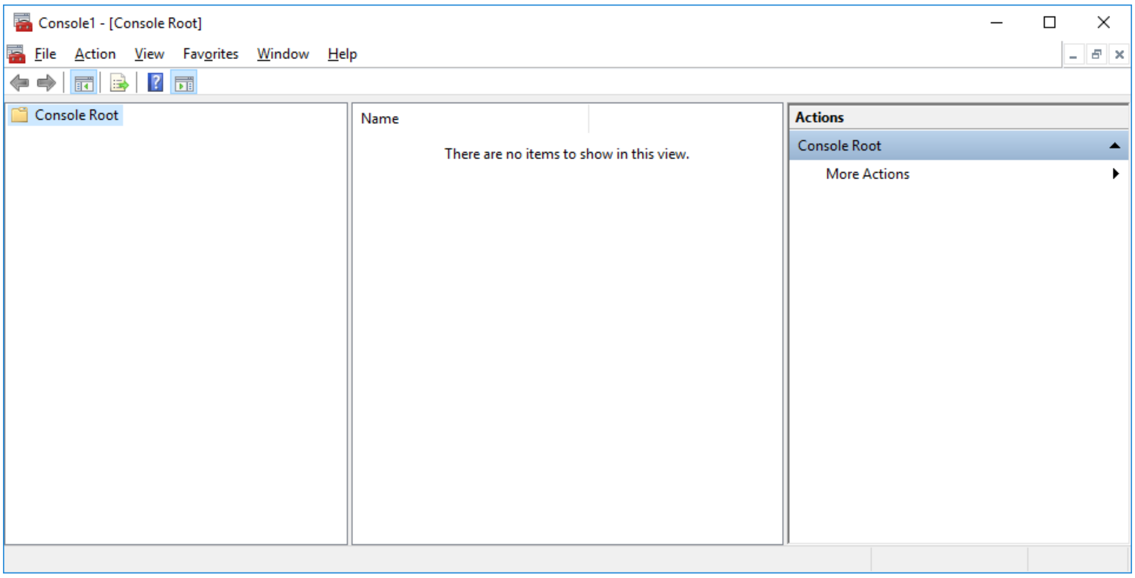
If you wish to generate certificate base on certificate request file (.csr)
inside menu option 'Create Request',
use button 'Issue certificate base on request'.
Generated CA root certificate: G:_PKI\GenCert\GenCert\bin\Debug\CA
\ABC_CA_signed.pfx
will be use to sing certificate requst (.csr) file, generated inside menu
option 'Create Request'.

Certificate file: G:_PKI\GenCert\GenCert\bin\Debug\Electrica\generated_signed.cer sucessfully saved.

Generate Request and Certificate Application | Menu option: Issue Certificate

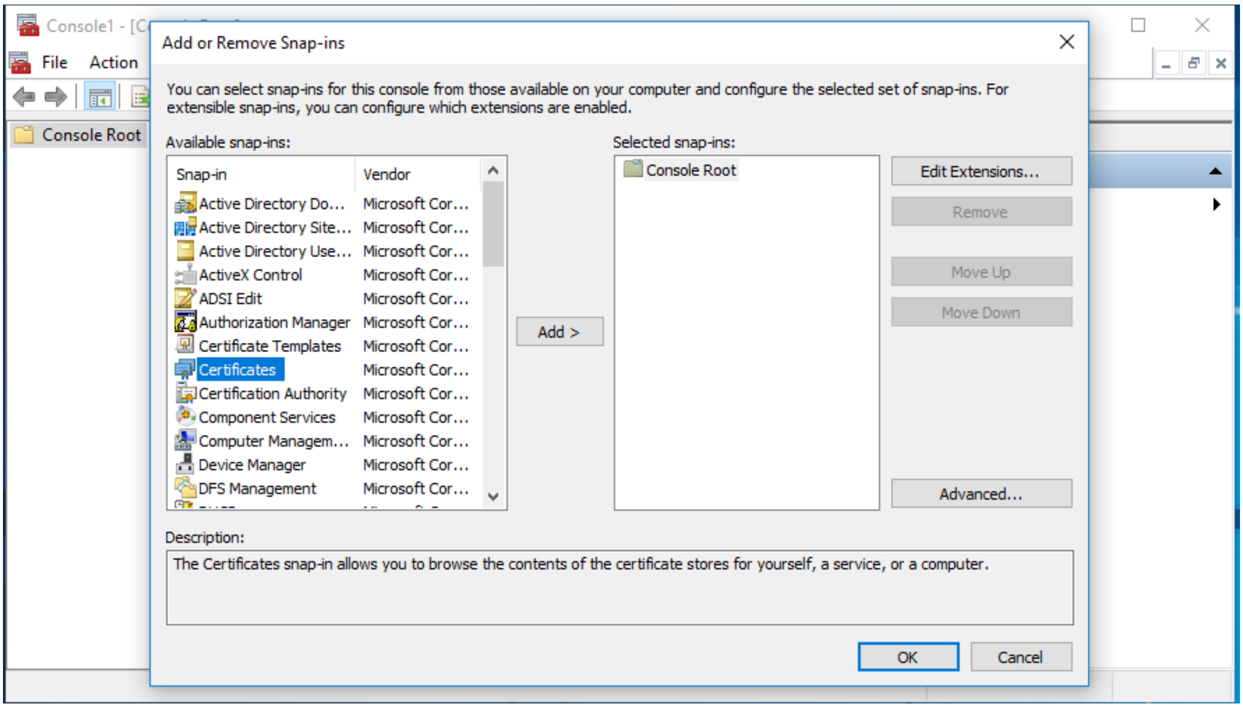
6. IMPORT DATA FROM GENERATED SIGNED CERTIFICATE FILE TO CERTIFICATE STORE

On the computer, open mmc.exe console.


Console1 - [Console Root]
File Action View Favorites Window Help
Console Root
Name
Actions
Console Root
More Actions

There are no items to show in this view.

Add Certificate Snap-in

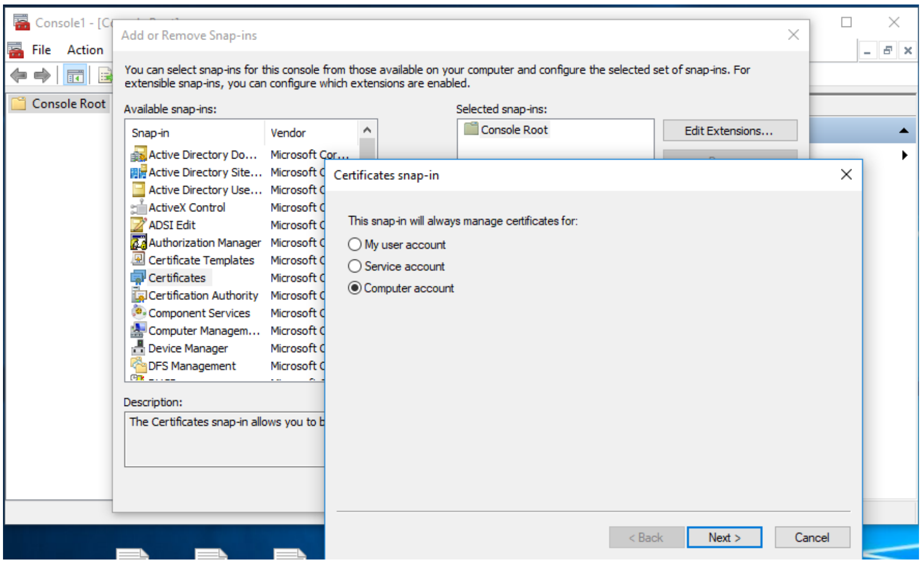


You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
DFS Management	Microsoft Cor...

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Add, Choose option “Computer account”



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Certificates snap-in

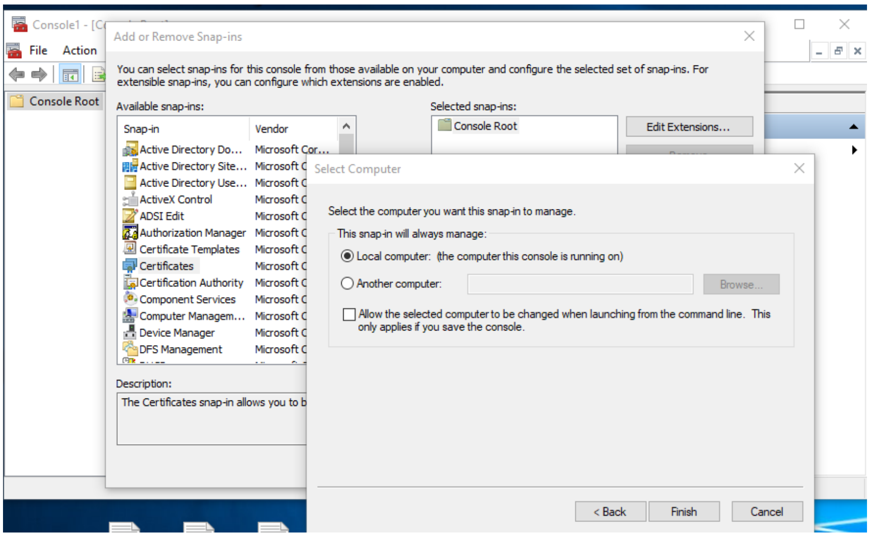
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

Next



Select Computer

Select the computer you want this snap-in to manage.

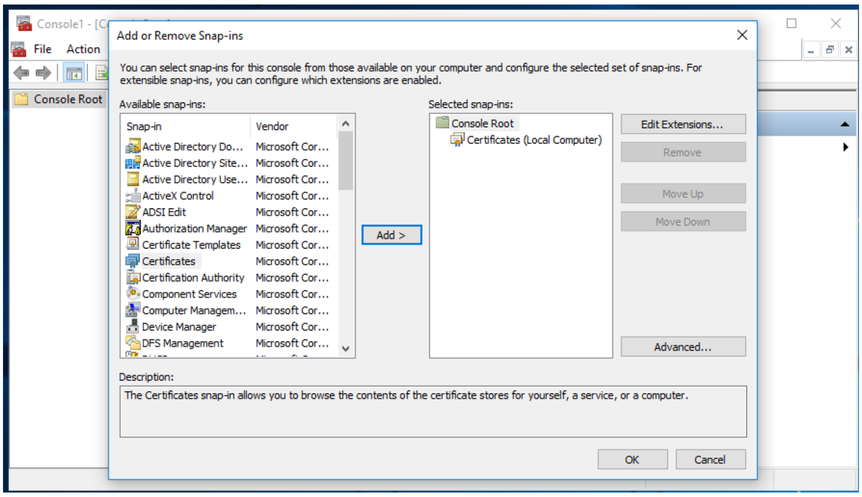
This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

Finish



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
DFS Management	Microsoft Cor...

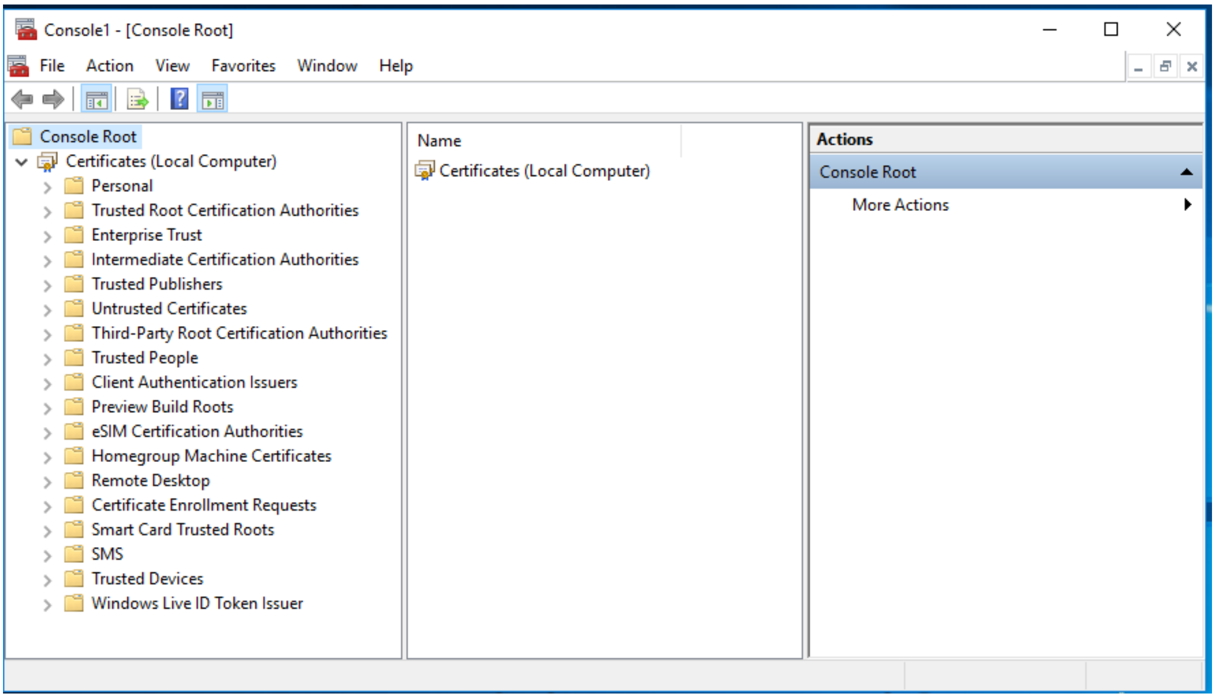
Selected snap-ins:

Console Root
- Certificates (Local Computer)

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

OK

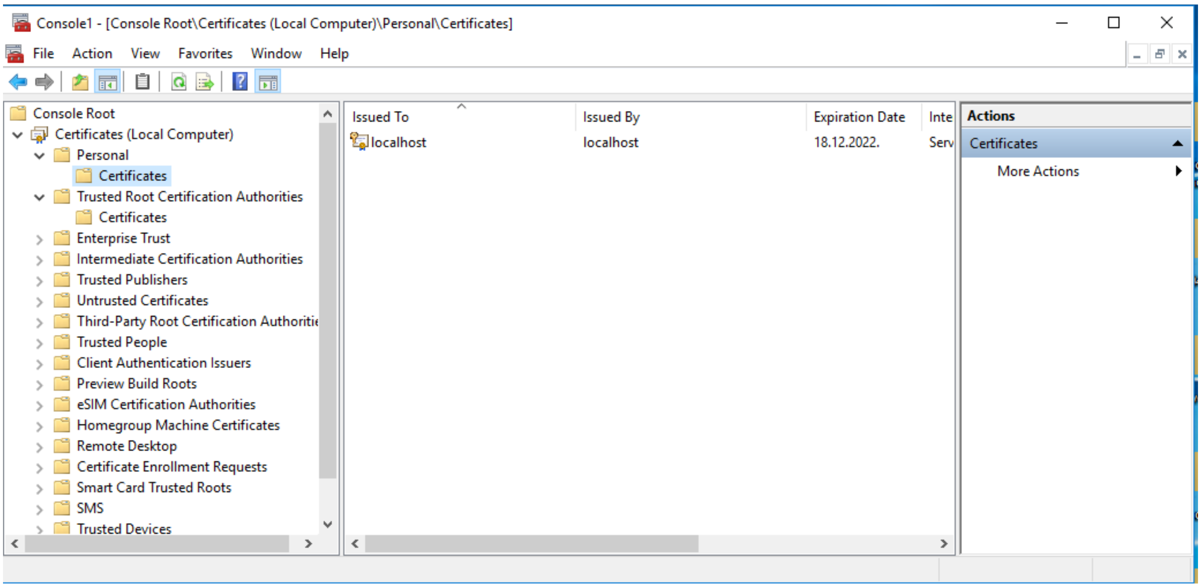

Console1 - [Console Root]
File Action View Favorites Window Help
Name
Actions
Console Root
More Actions

- Console Root
  - Certificates (Local Computer)
    - Personal
    - Trusted Root Certification Authorities
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Client Authentication Issuers
    - Preview Build Roots
    - eSIM Certification Authorities
    - Homegroup Machine Certificates
    - Remote Desktop
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots
    - SMS
    - Trusted Devices
    - Windows Live ID Token Issuer

Certificates (Local Computer)

Parts of local computer Certificate store for interest are:

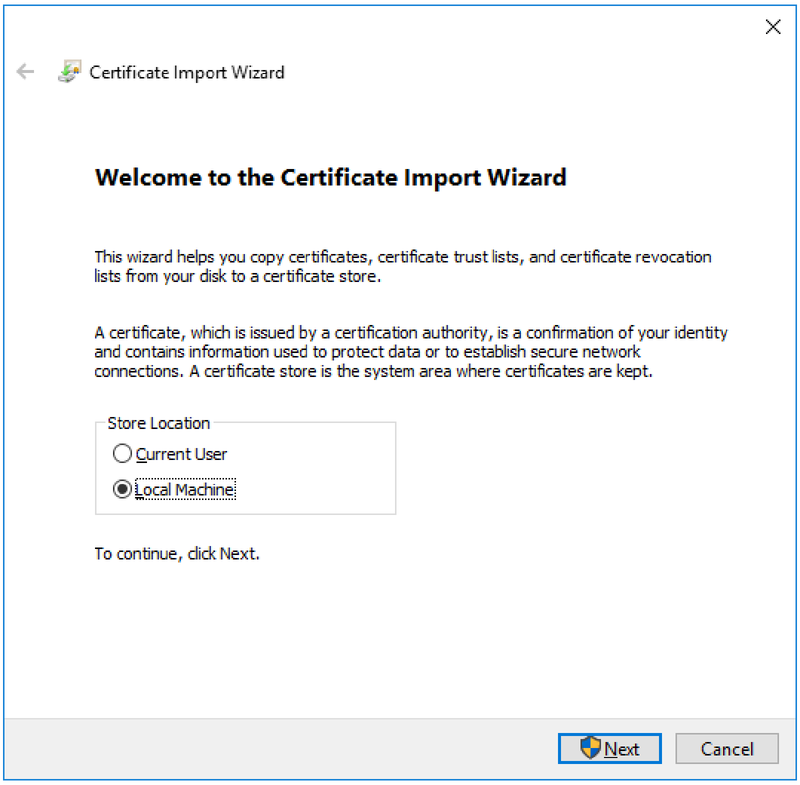
1. Personal, Certificates
2. Trusted Root Certification Authorities


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
Actions
Certificates
More Actions

- Console Root
  - Certificates (Local Computer)
    - Personal
      - Certificates
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authoritie
    - Trusted People
    - Client Authentication Issuers
    - Preview Build Roots
    - eSIM Certification Authorities
    - Homegroup Machine Certificates
    - Remote Desktop
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots
    - SMS
    - Trusted Devices

Issued To	Issued By	Expiration Date	Inte
localhost	localhost	18.12.2022.	Serv

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



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

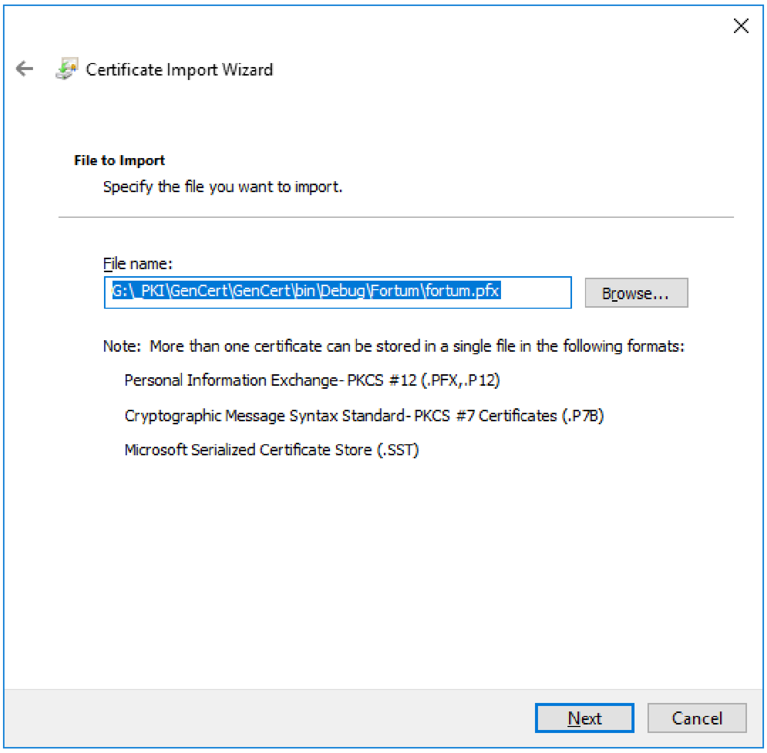
Store Location

○ Current User

● Local Machine

To continue, click Next.

Next



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

G:_PKI\GenCert\GenCert\bin\Debug\Fortum\fortum.pfx

Note: More than one certificate can be stored in a single file in the following formats:

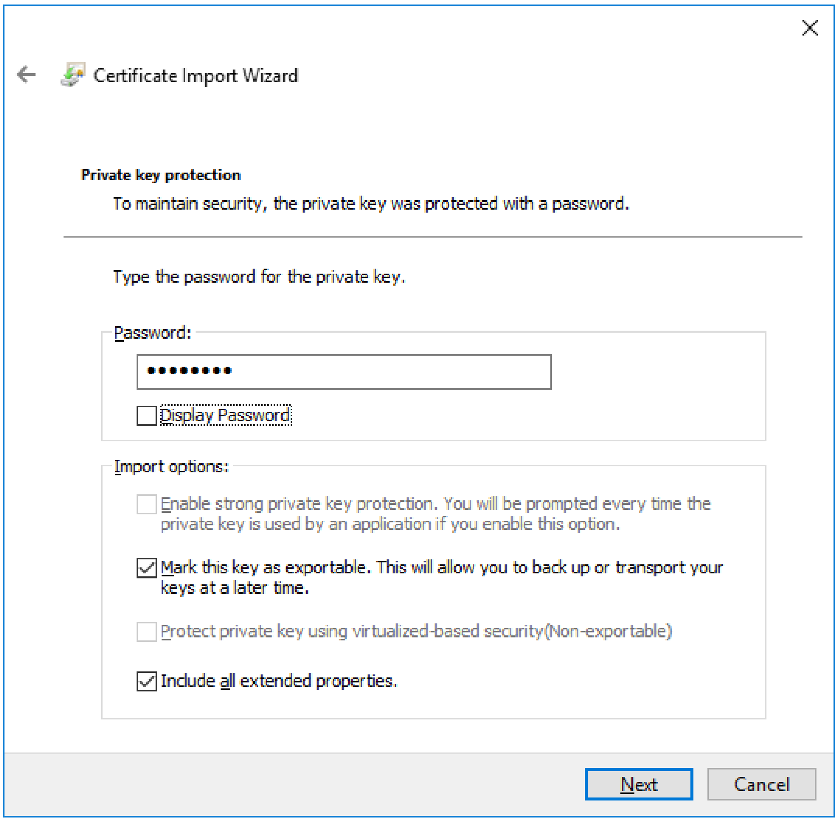
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

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.”



Certificate Import Wizard

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:

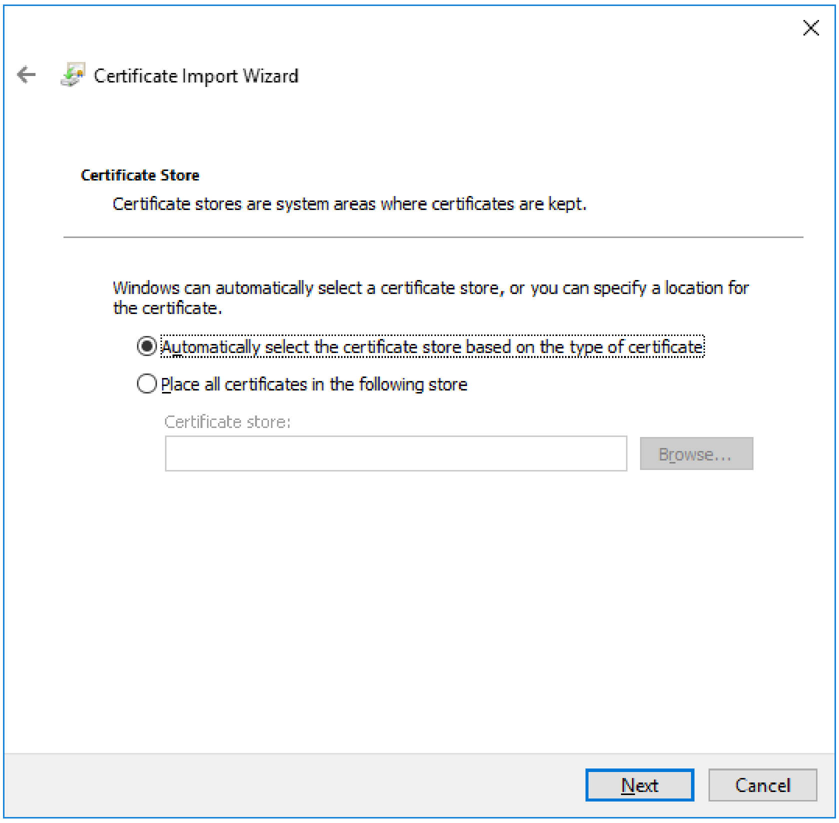
□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☑ 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.

Next



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

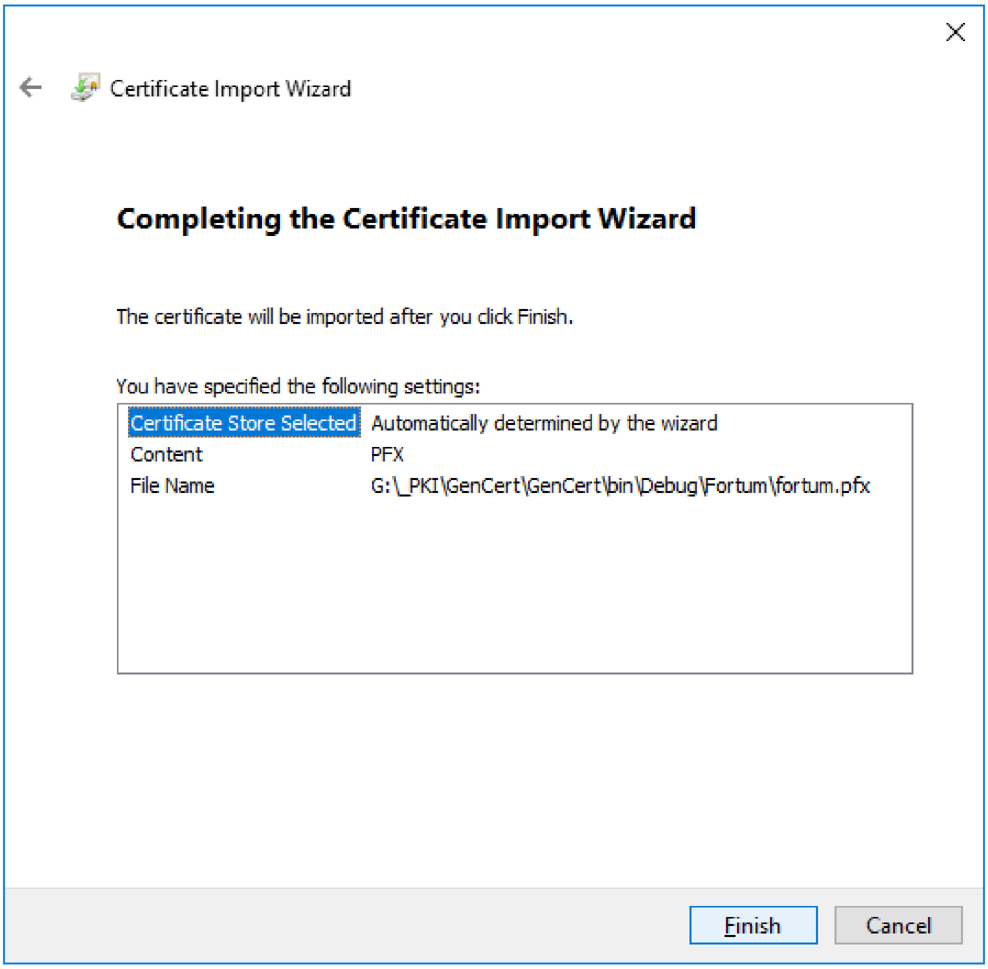
Windows can automatically select a certificate store, or you can specify a location for the certificate.

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

Next



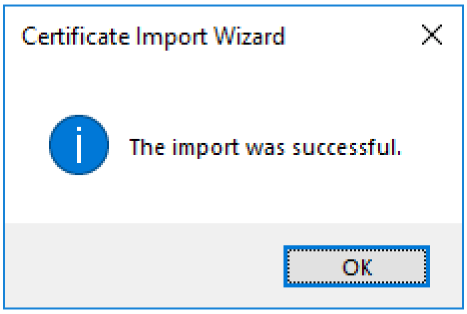
Completing the Certificate Import Wizard

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\Fortum\fortum.pfx

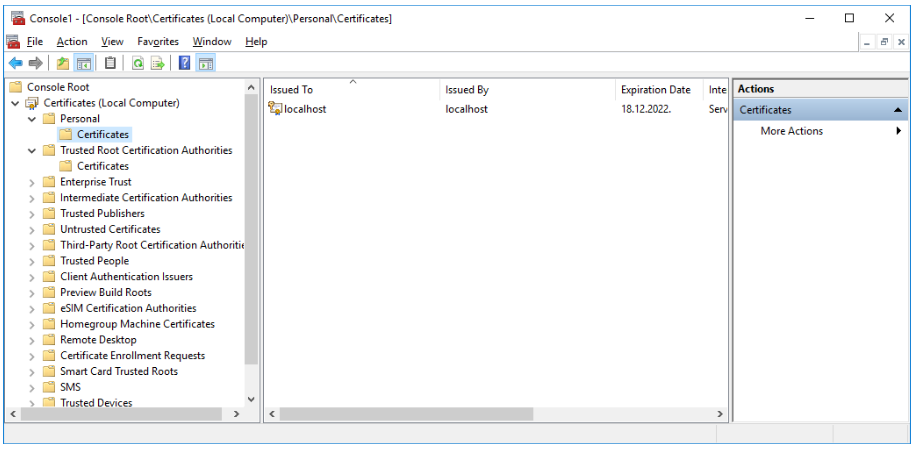
Finish



The import was successful.

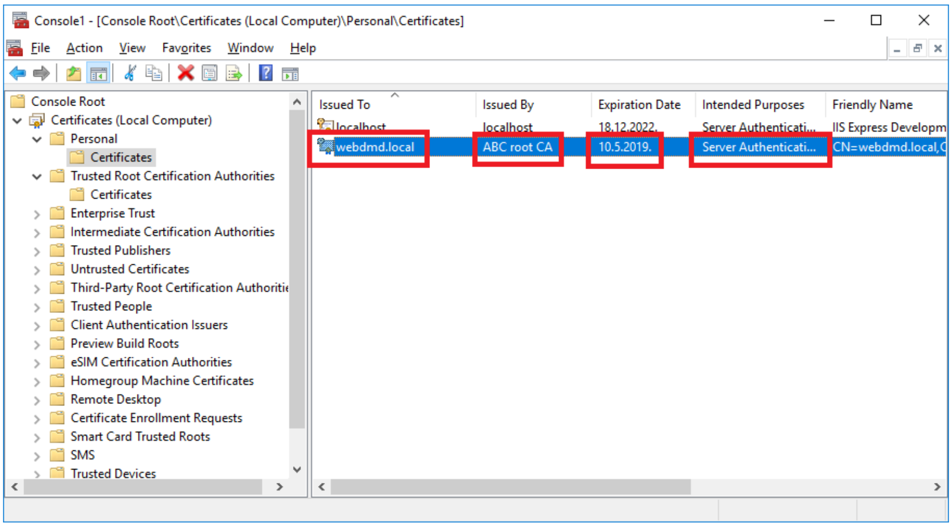
OK

Refresh Personal and Trusted Root Certification Authorities inside mmc console.


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authoritie
Trusted People
Client Authentication Issuers
Preview Build Roots
eSIM Certification Authorities
Homegroup Machine Certificates
Remote Desktop
Certificate Enrollment Requests
Smart Card Trusted Roots
SMS
Trusted Devices
Actions
Certificates
More Actions

Issued To	Issued By	Expiration Date	Inte
localhost	localhost	18.12.2022.	Serv

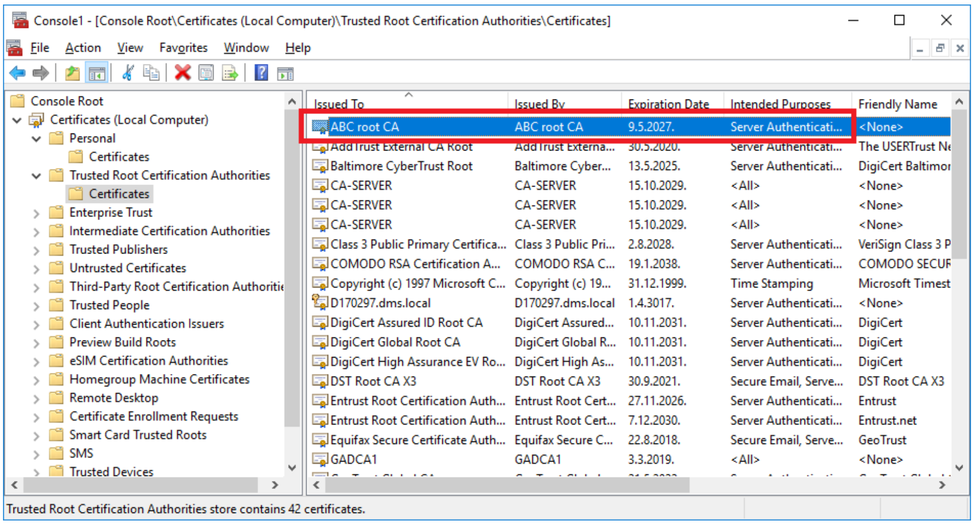
After refresh


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authoritie
Trusted People
Client Authentication Issuers
Preview Build Roots
eSIM Certification Authorities
Homegroup Machine Certificates
Remote Desktop
Certificate Enrollment Requests
Smart Card Trusted Roots
SMS
Trusted Devices

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
localhost	localhost	18.12.2022.	Server Authenticati...	IIS Express Developm
webdmd.local	ABC root CA	10.5.2019.	Server Authenticati...	CN=webdmd.local,C

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

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

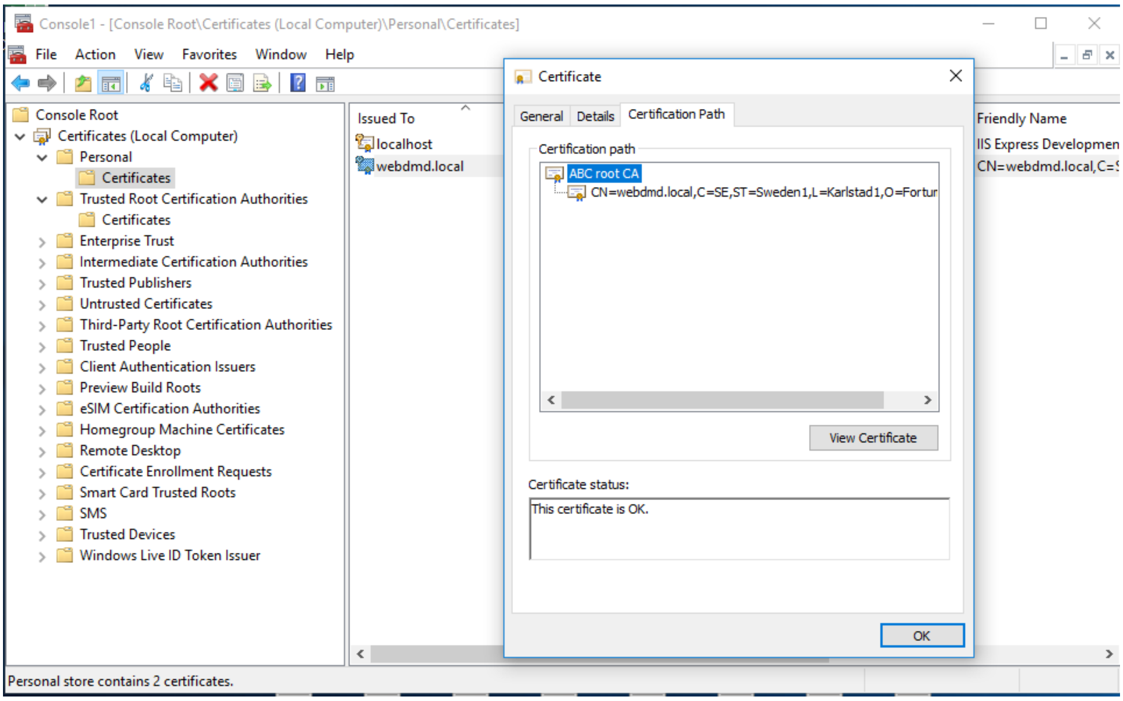

Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authoritie
Trusted People
Client Authentication Issuers
Preview Build Roots
eSIM Certification Authorities
Homegroup Machine Certificates
Remote Desktop
Certificate Enrollment Requests
Smart Card Trusted Roots
SMS
Trusted Devices

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
ABC root CA	ABC root CA	9.5.2027.	Server Authenticati...	<None>
AddTrust External CA Root	AddTrust Externa...	30.5.2020.	Server Authenticati...	The USERTrust Ne
Baltimore CyberTrust Root	Baltimore Cyber...	13.5.2025.	Server Authenticati...	DigiCert Baltimor
CA-SERVER	CA-SERVER	15.10.2029.	<All>	<None>
CA-SERVER	CA-SERVER	15.10.2029.	<All>	<None>
CA-SERVER	CA-SERVER	15.10.2029.	<All>	<None>
Class 3 Public Primary Certifica...	Class 3 Public Pri...	2.8.2028.	Server Authenticati...	VeriSign Class 3 P
COMODO RSA Certification A...	COMODO RSA C...	19.1.2038.	Server Authenticati...	COMODO SECUR
Copyright (c) 1997 Microsoft C...	Copyright (c) 19...	31.12.1999.	Time Stamping	Microsoft Timest
D170297.dms.local	D170297.dms.local	1.4.3017.	Server Authenticati...	<None>
DigiCert Assured ID Root CA	DigiCert Assured...	10.11.2031.	Server Authenticati...	DigiCert
DigiCert Global Root CA	DigiCert Global R...	10.11.2031.	Server Authenticati...	DigiCert
DigiCert High Assurance EV Ro...	DigiCert High As...	10.11.2031.	Server Authenticati...	DigiCert
DST Root CA X3	DST Root CA X3	30.9.2021.	Secure Email, Serve...	DST Root CA X3
Entrust Root Certification Auth...	Entrust Root Cert...	27.11.2026.	Server Authenticati...	Entrust
Entrust Root Certification Auth...	Entrust Root Cert...	7.12.2030.	Server Authenticati...	Entrust.net
Equifax Secure Certificate Auth...	Equifax Secure C...	22.8.2018.	Secure Email, Serve...	GeoTrust
GADCA1	GADCA1	3.3.2019.	<All>	<None>

Trusted Root Certification Authorities store contains 42 certificates.

If Refresh “Trusted Root Certification Authorities” 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 root CA”

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”, otherwise imported generated certificate don’t be valid.



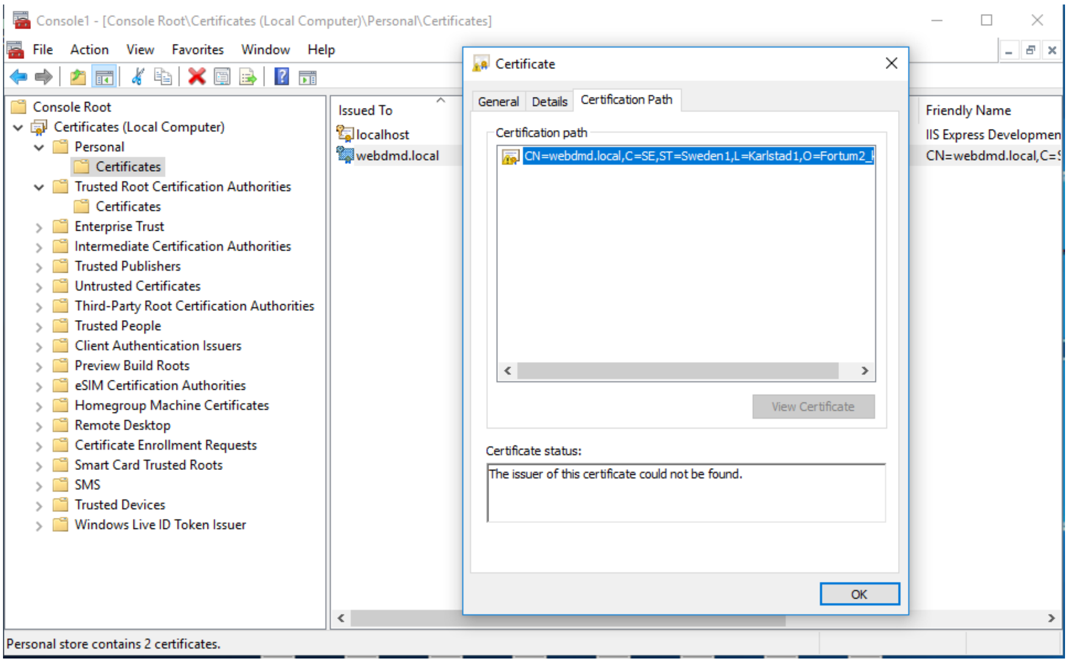
ABC root CA
CN=webdmd.local,C=SE,ST=Sweden1,L=Karlstad1,O=Fortur

This certificate is OK.

Personal store contains 2 certificates.

Valid imported certificate look.

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



CN=webdmd.local,C=SE,ST=Sweden1,L=Karlstad1,O=Fortum2_

The issuer of this certificate could not be found.

Personal store contains 2 certificates.

7. 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.