MUITINĖS DEPARTAMENTAS PRIE LIETUVOS RESPUBLIKOS FINANSŲ MINISTERIJOS

BENDRO NAUDOTOJŲ VALDYMO SISTEMOS, ATITINKANČIOS EUROPOS KOMISIJOS REIKALAVIMUS, SUKŪRIMO PASLAUGŲ PROJEKTAS

CERTIFICATE GENERATION INSTRUCTIONS

VERSION:2.21

Vilnius 2023

CONTENT

1 INTRODUCTION

To login to BAP using a certificate, you must first prepare a certificate signing request. With this request, a certificate is generated which must be installed on your computer. Below are instructions on how to generate a certificate signing request on each operating system, how to download the certificate, install it, and transfer it to another computer.

2 MANAGING CERTIFICATES IN WINDOWS ENVIRONMENT

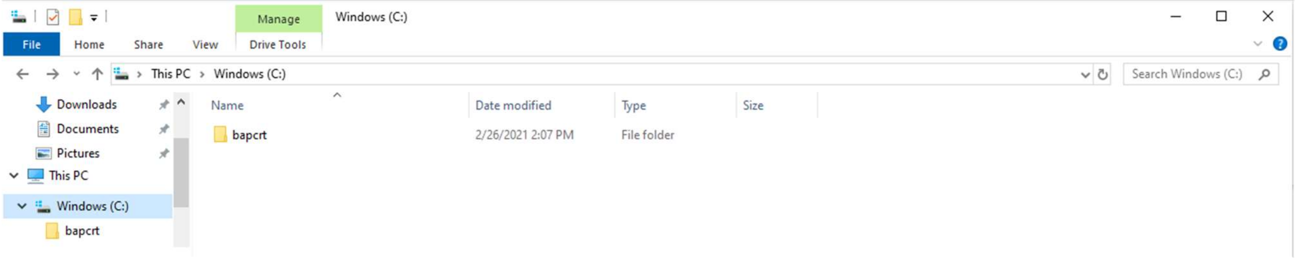
2.1 Creating a certificate signing request

In Windows environment, there are two ways to do this in the following sections. Choose the one that suits you best and follow the steps below.

2.1.1 Using the Microsoft Management Console

1. First, prepare a location on your computer where you can later save the certificate request created in the next steps of these instructions. We recommend that you create a folder named "bapcrt" *at Computer → Local Disc (C :).* The example below shows the folder "bapcrt" created in an *analogous location at This PC → Windows (C :).*

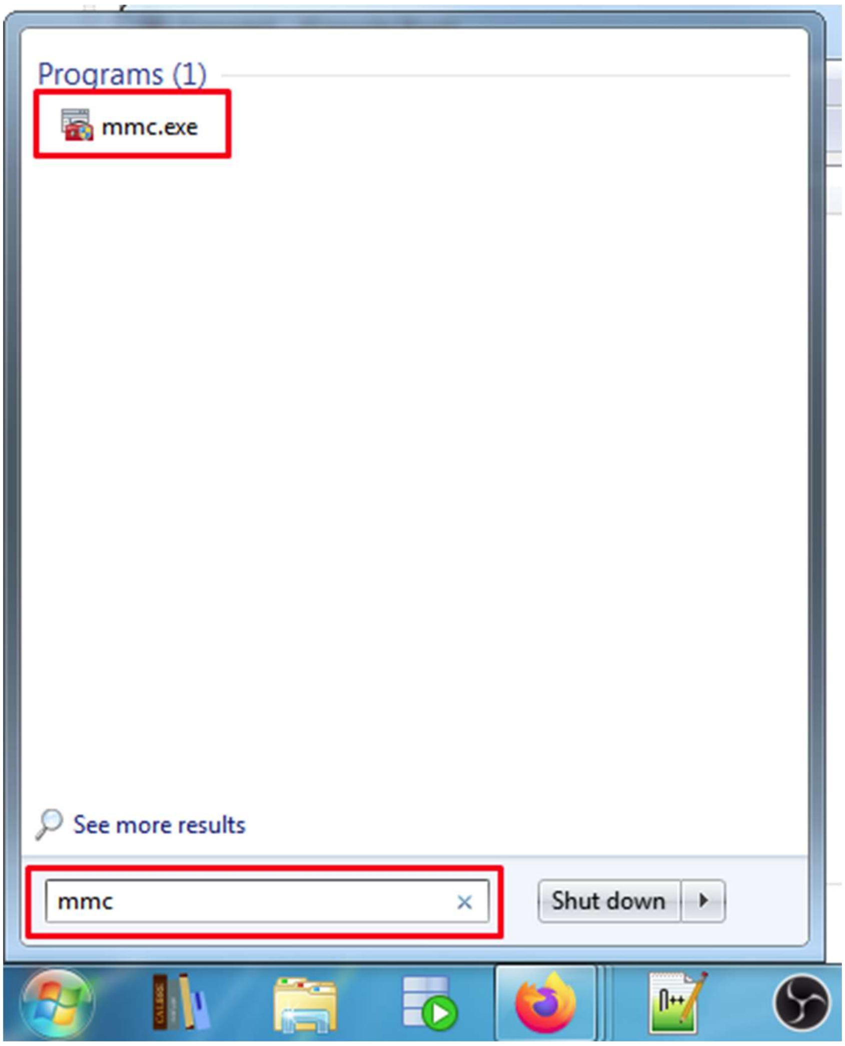
Figure 1 Creating the bapcrt folder



Name	Date modified	Type	Size
bapcrt	2/26/2021 2:07 PM	File folder	

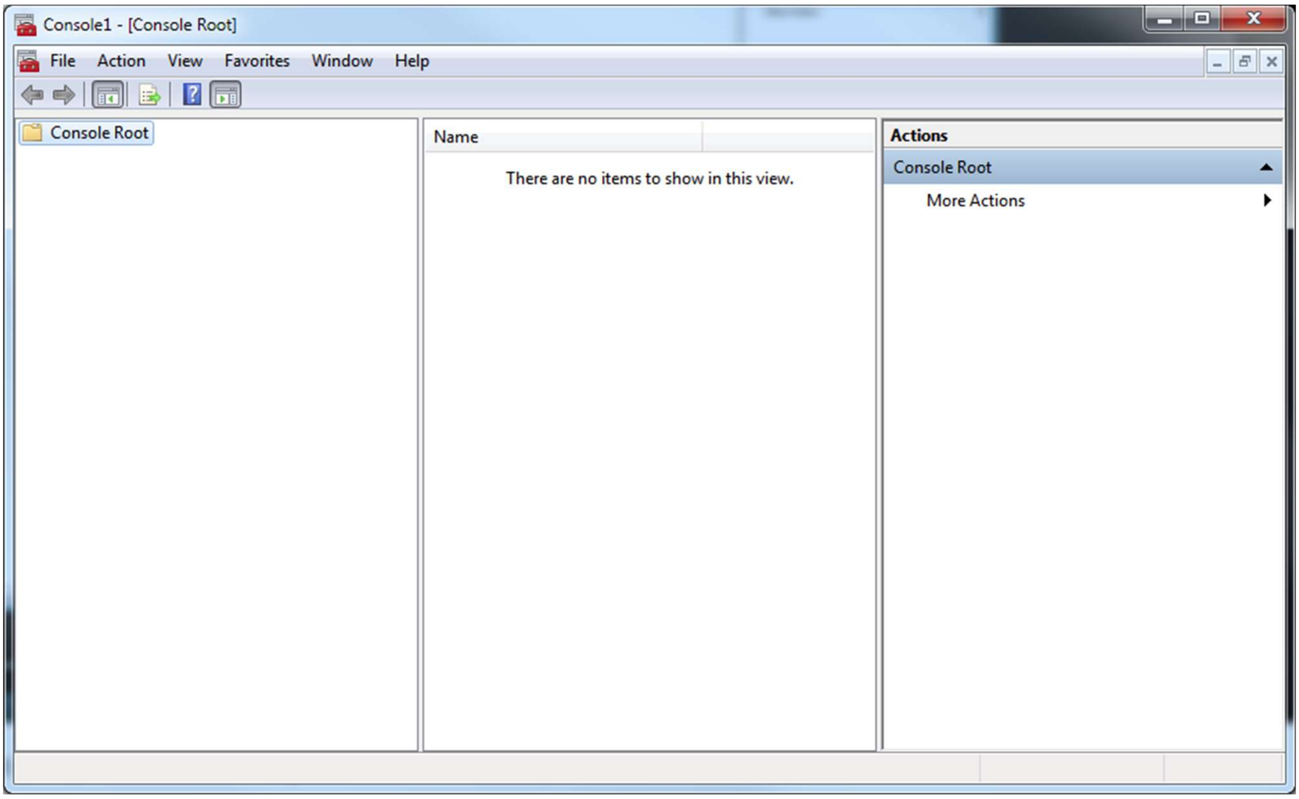
2. To open the *Microsoft Management Console,* type "mmc" in the *Windows Start* bar to search for and run the application that you found.

Figure 2 Search in Windows Start bar



mmc

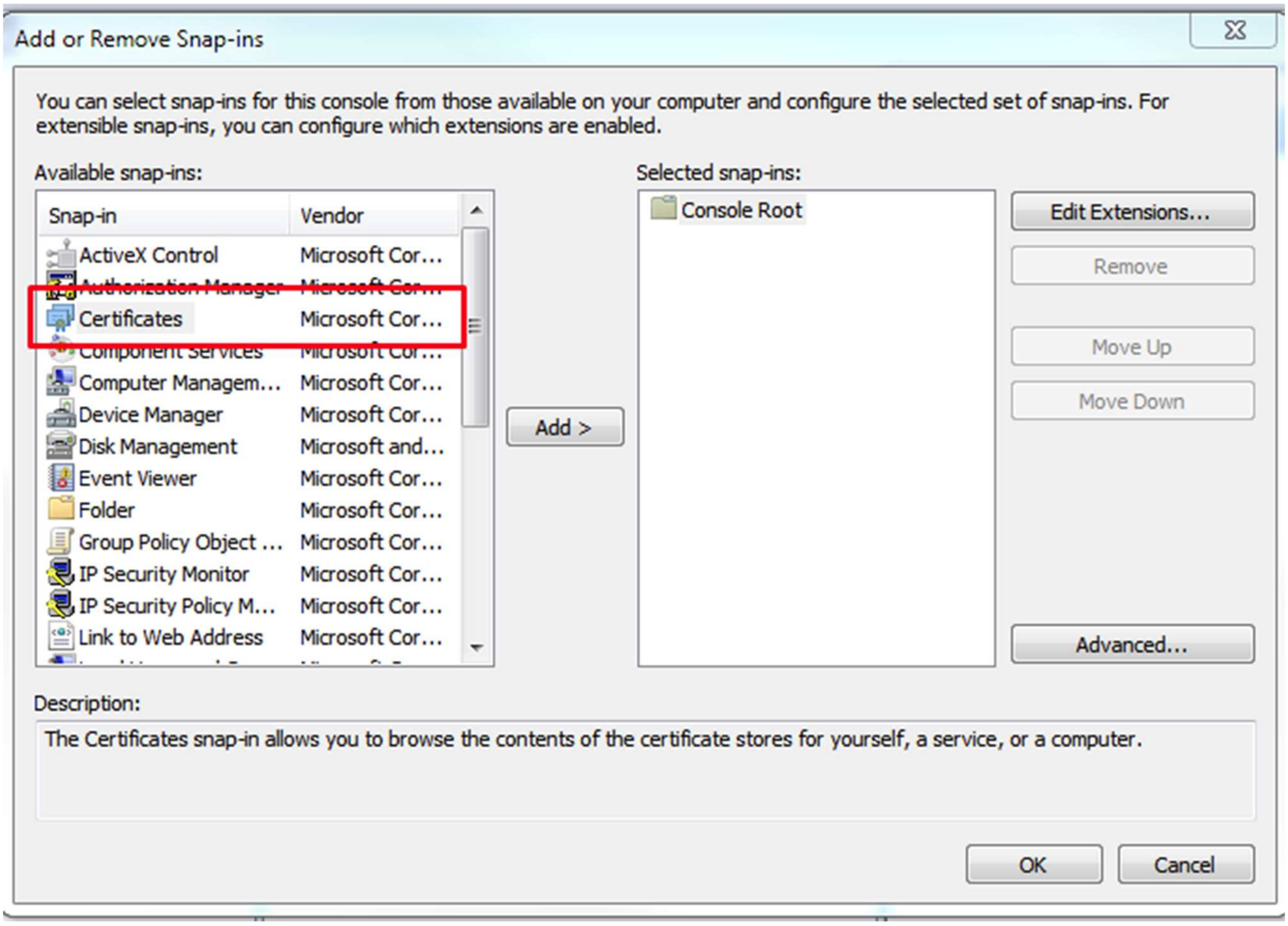
Figure 3 Microsoft Management Console window



There are no items to show in this view.

3. Select *File → Add / Remove Snap-in* in an opened window. In the pop-up window, select *Certificates* option.

Figure 4 Certificates section selection



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
ActiveX Control	Microsoft Cor…
Authorization Manager	Microsoft Cor…
Certificates	Microsoft Cor…
Component Services	Microsoft Cor…
Computer Managem…	Microsoft Cor…
Device Manager	Microsoft Cor…
Disk Management	Microsoft and…
Event Viewer	Microsoft Cor…
Folder	Microsoft Cor…
Group Policy Object …	Microsoft Cor…
IP Security Monitor	Microsoft Cor…
IP Security Policy M…	Microsoft Cor…
Link to Web Address	Microsoft Cor…

Selected snap-ins:

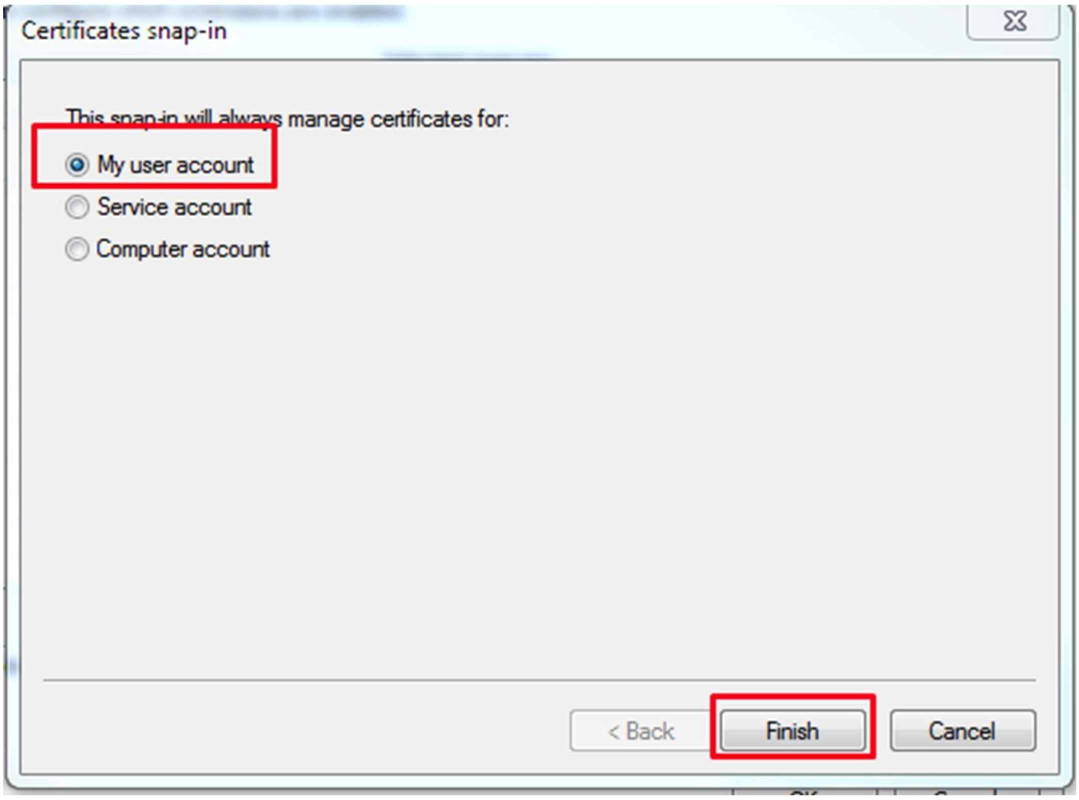
Console Root

Description:

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

4. Click *Add>* button to the right side of the selection. In the new window, select the *My user account* option and click the *Finish* button at the bottom of the window.

Figure 5 My user account selection



Certificates snap-in

This snap-in will always manage certificates for:

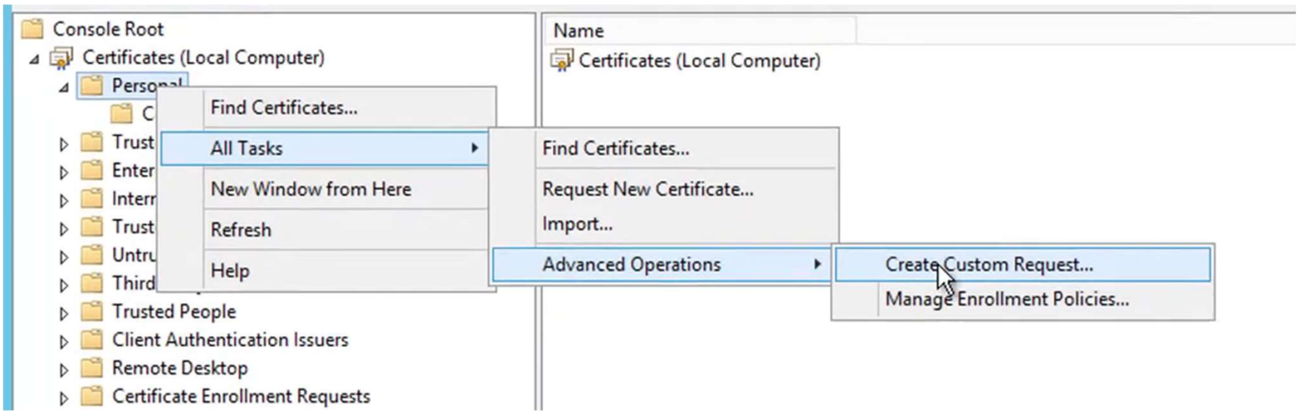
● My user account

○ Service account

○ Computer account

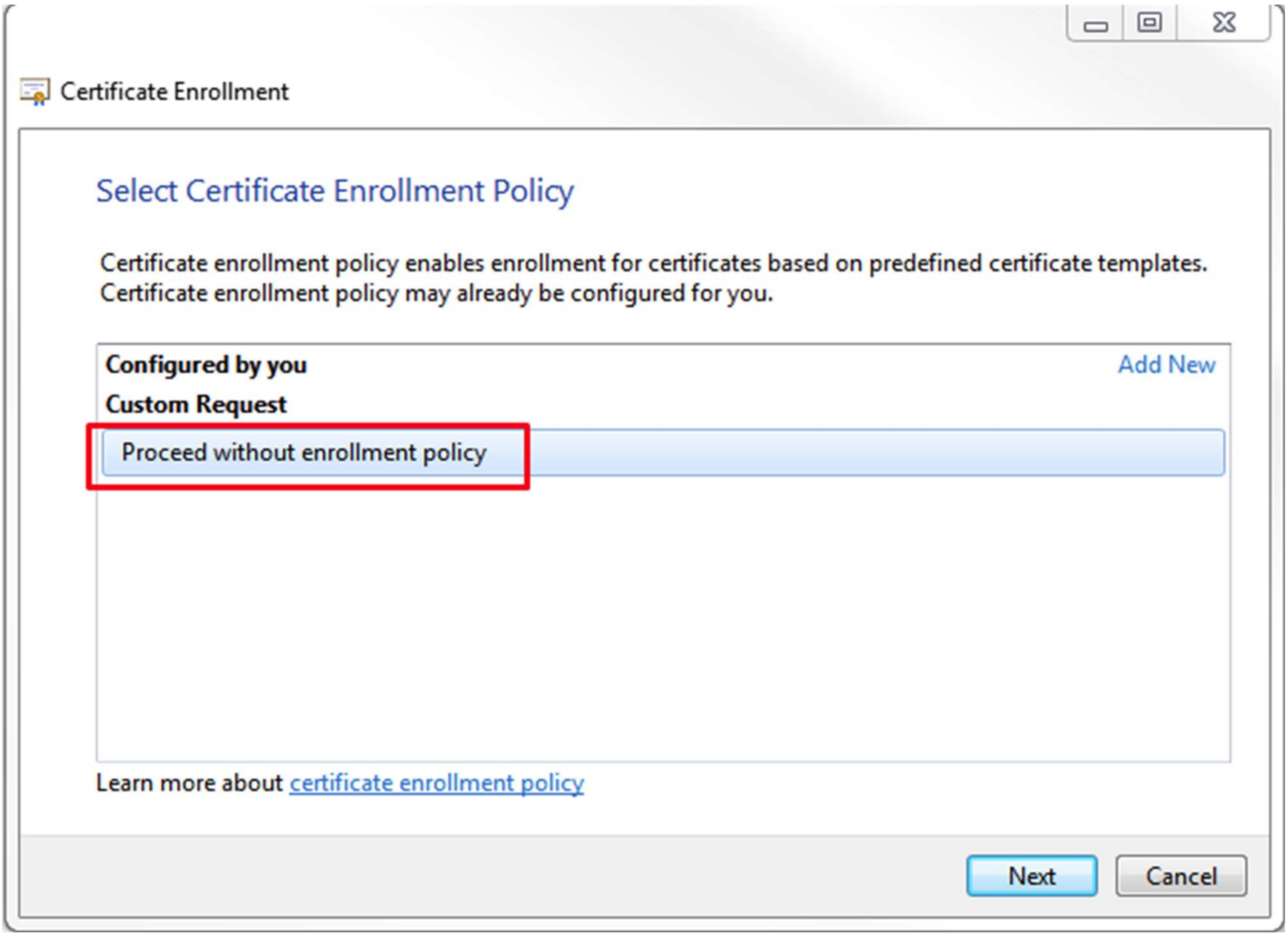
5. Click *OK* to close the *Snap-in* window.

6. Expand *Certificates* and find *Personal* section. Right-click on it to bring up the internal menu. From this menu, select *All Tasks → Advanced Operations → Create custom request.*



7. Click *Next* in an opened window. The next window will suggest a strategy for applying the certificate - here you need to select *Proceed without enrollment policy* and click *Next.*

Figure 6 Strategy selection window



Certificate Enrollment

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by you Add New

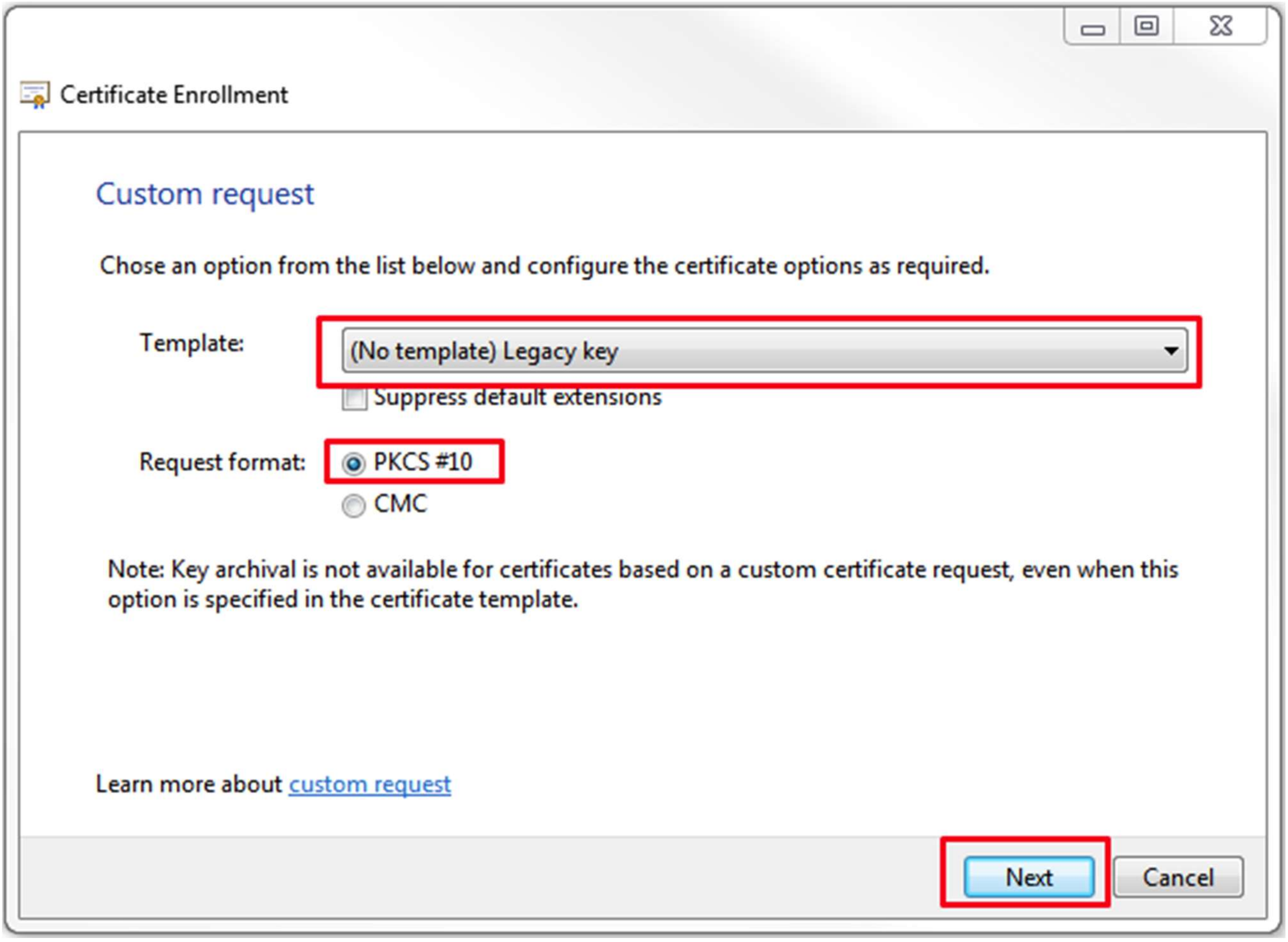
Custom Request

Proceed without enrollment policy

Learn more about certificate enrollment policy

8. In the third window we will be asked to specify a template. Expand the menu and select *(No template) Legacy key.* Note the format *PKS # 10*. After selecting these options, click *Next.*

Figure 7 Template selection



Certificate Enrollment

Custom request

Chose an option from the list below and configure the certificate options as required.

Template: (No template) Legacy key

□ Suppress default extensions

Request format: ● PKCS #10

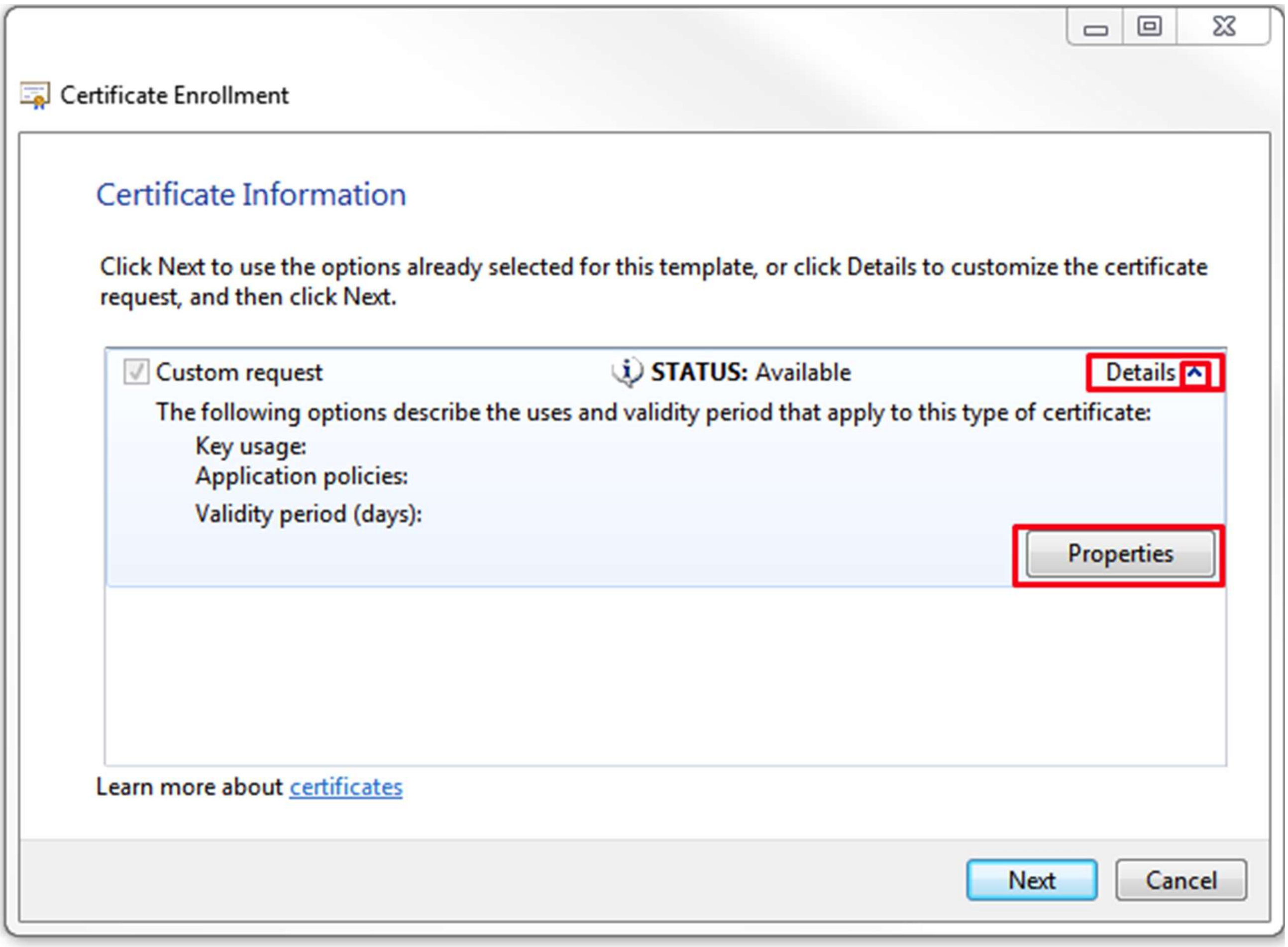
○ CMC

Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template.

Learn more about custom request

9. In the certificate information window, expand the details and click the *Properties* button.

Figure 8 Certificate Information Window



Certificate Enrollment

Certificate Information

Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

☑ Custom request STATUS: Available Details ^

The following options describe the uses and validity period that apply to this type of certificate:

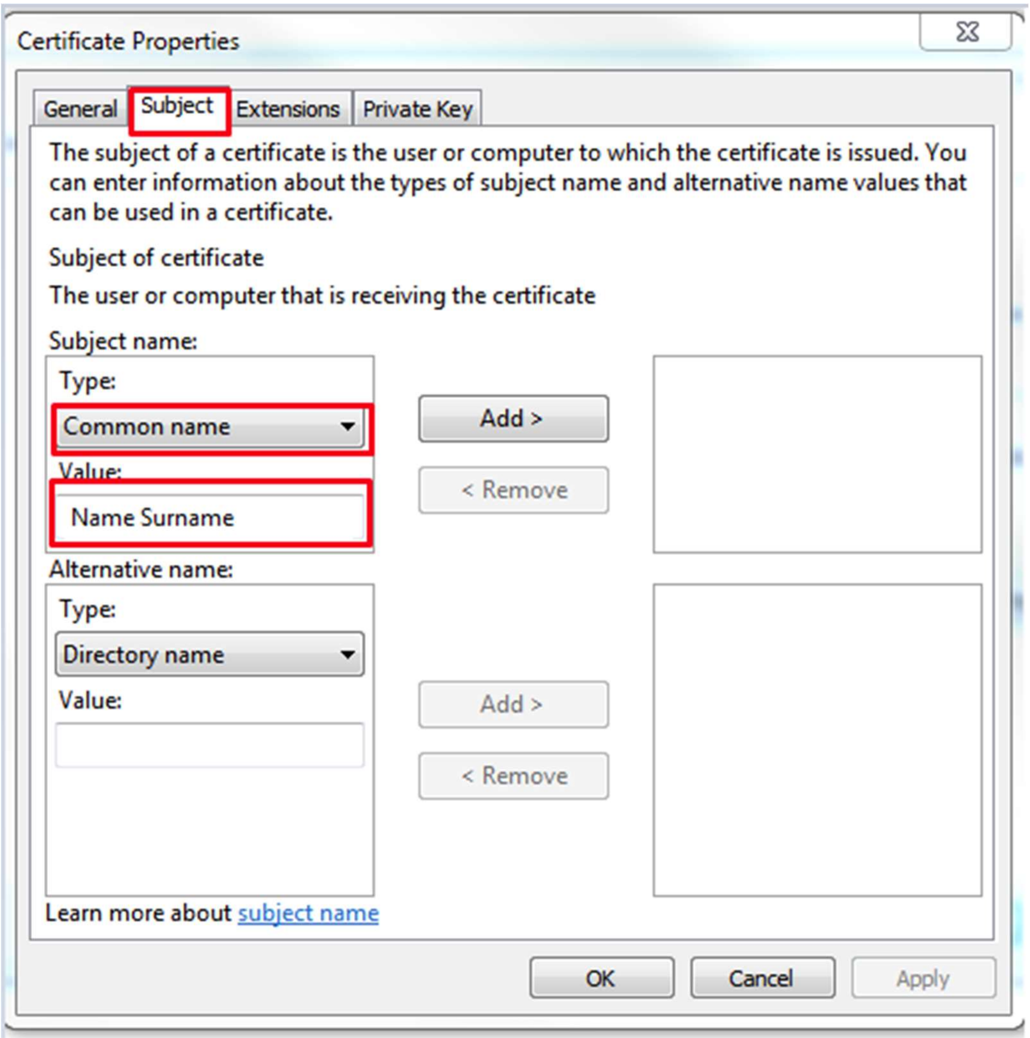
Key usage:

Application policies:

Validity period (days):

10. Select the *Subject* section in an opened window. In the *Type* field, select *Common name* and in the *Value* field, enter your Name and Surname.

Figure 9 Subject cartilage



Certificate Properties

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type: Common name

Value: Name Surname

Alternative name:

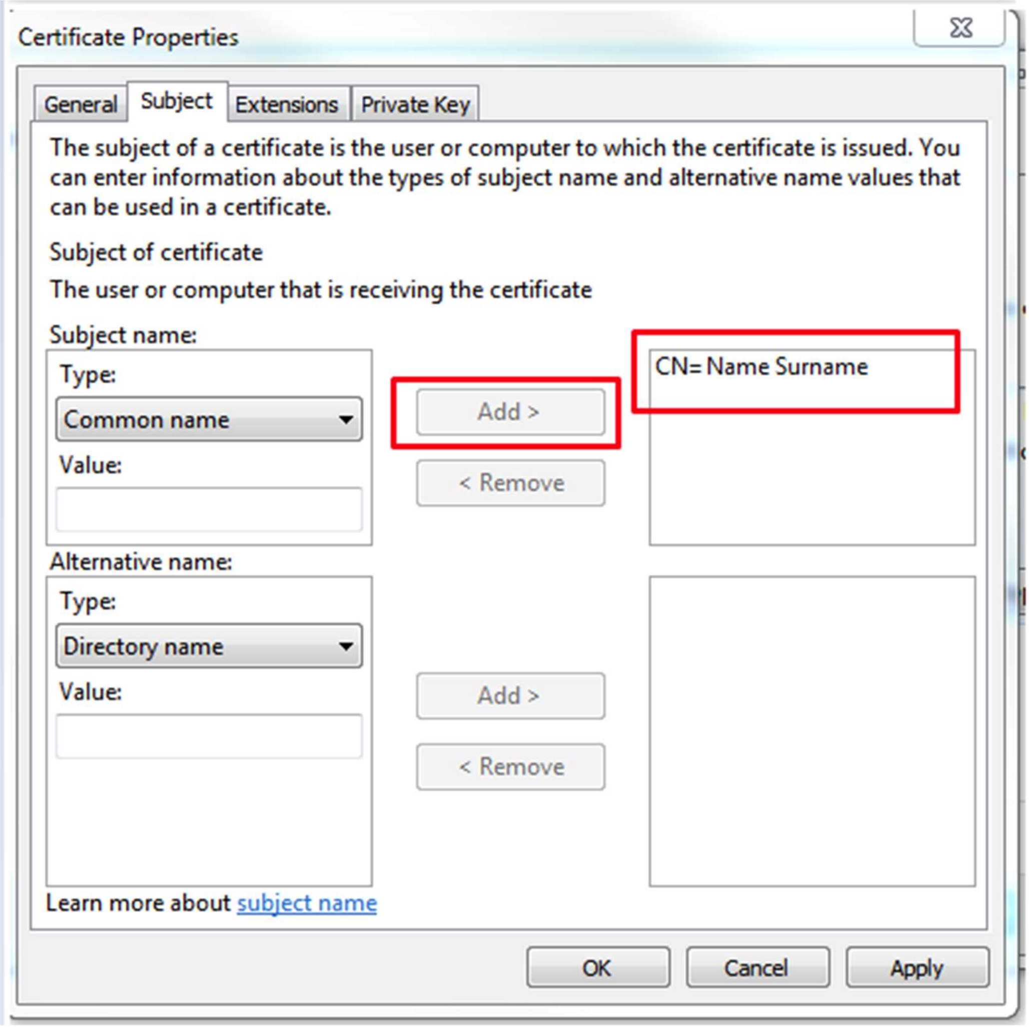
Type: Directory name

Value:

Learn more about subject name

11. When the values are filled in, click the *Add>* button on the right.

Figure 10 Filling in subject data



Certificate Properties

General | Subject | Extensions | Private Key

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type: Common name

Value:

CN= Name Surname

Alternative name:

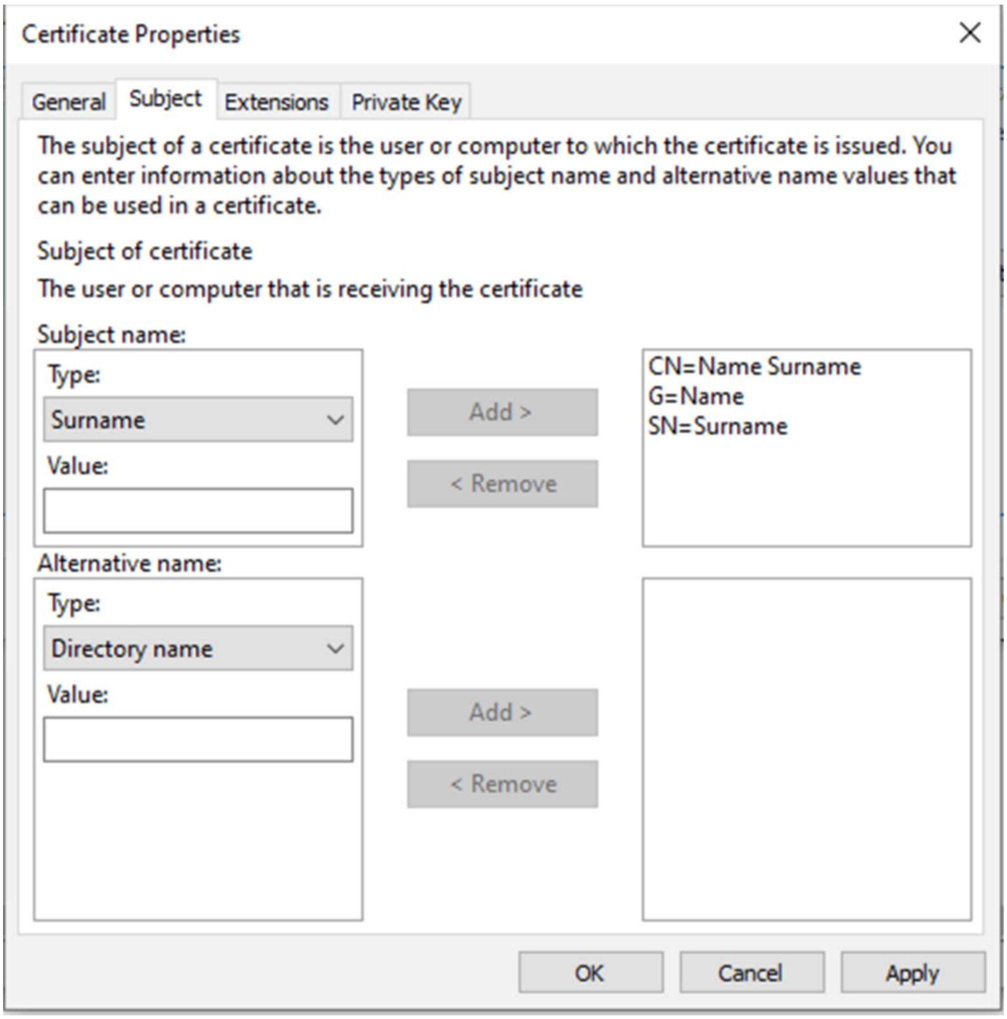
Type: Directory name

Value:

Learn more about subject name

12. Fill out Given name and Surname as in previous step, when attributes are present they should show up in the right pane.

Figure 11 Subject rezultatas



Certificate Properties

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type: Surname

Value:

CN=Name Surname
G=Name
SN=Surname

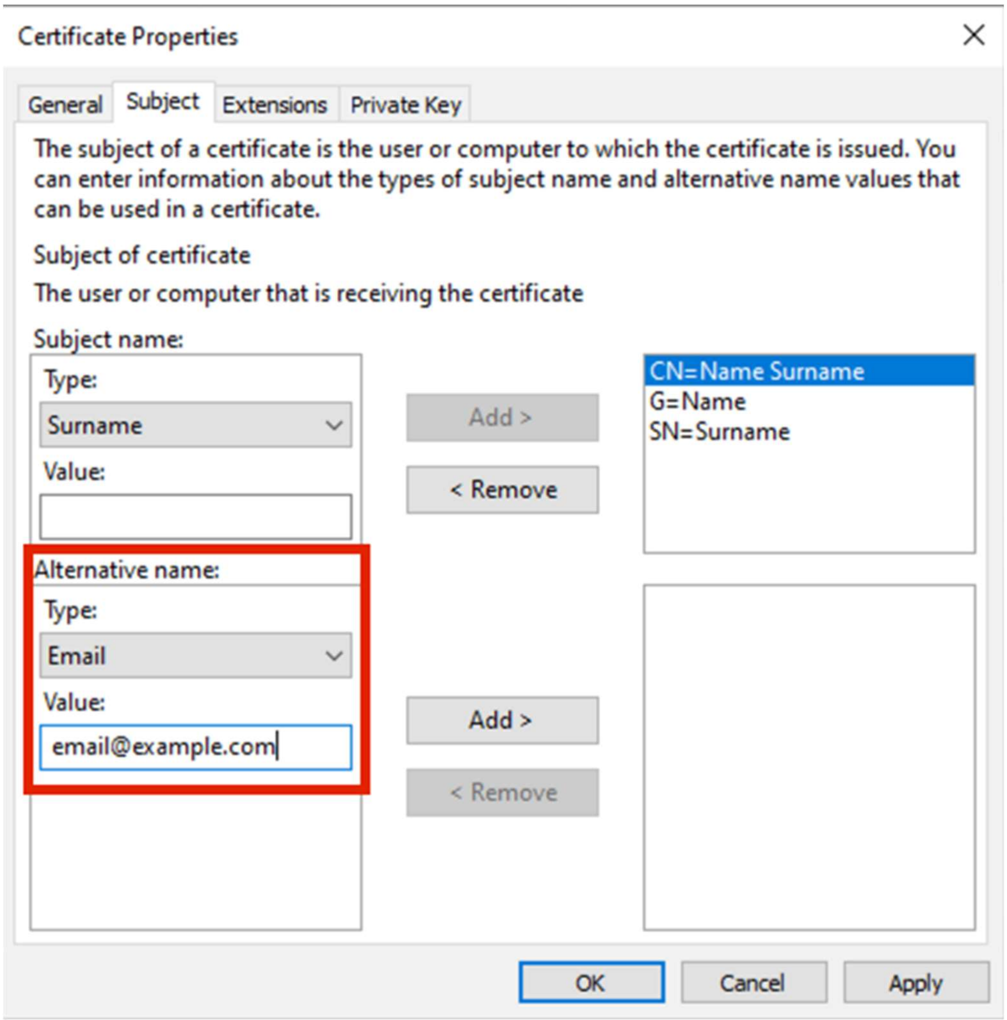
Alternative name:

Type: Directory name

Value:

13. In the Alternative name section, fill out your email address.

Figure 12 Alternative name



Certificate Properties

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type: Surname

Value:

Alternative name:

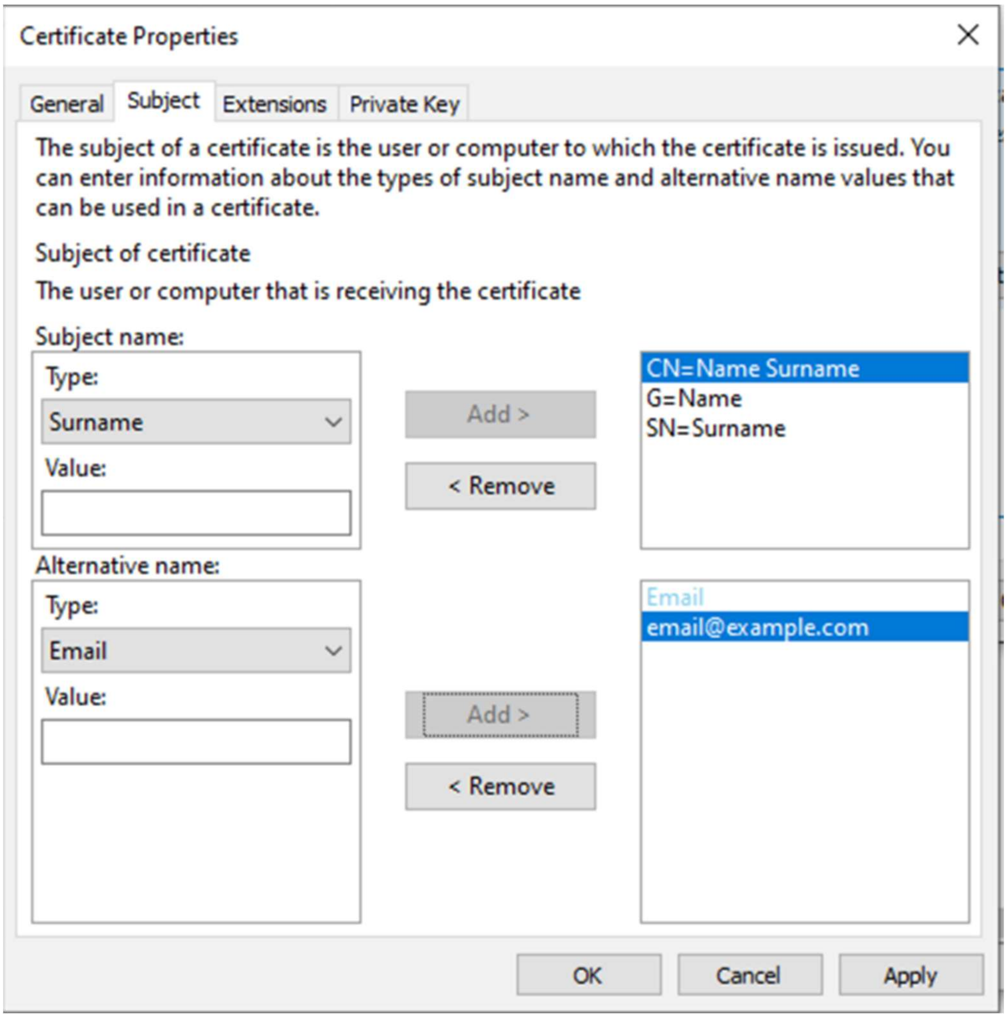
Type: Email

Value: email@example.com

CN=Name Surname
G=Name
SN=Surname

14. After clicking *„Add >“* button subject window should show your email address in the right pane.

Figure 13 Užpildytas subject



The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type: Surname

Value:

CN=Name Surname
G=Name
SN=Surname

Alternative name:

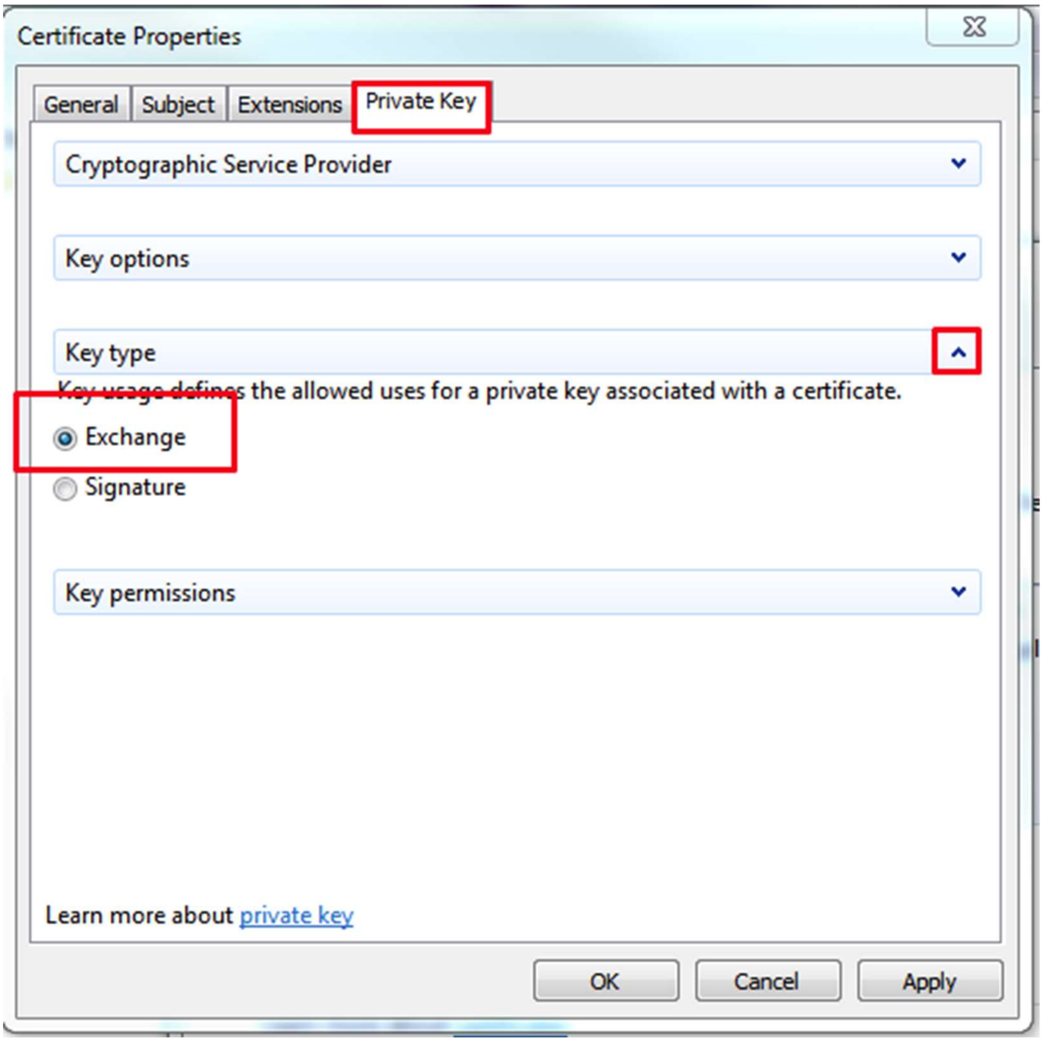
Type: Email

Value:

Email
email@example.com

15. Follow the steps in the *Private Key* section. Expand the *Key type* area and select the *Exchange* option.

Figure 14 Key type selection



Certificate Properties

General | Subject | Extensions | Private Key

Cryptographic Service Provider

Key options

Key type

Key usage defines the allowed uses for a private key associated with a certificate.

● Exchange

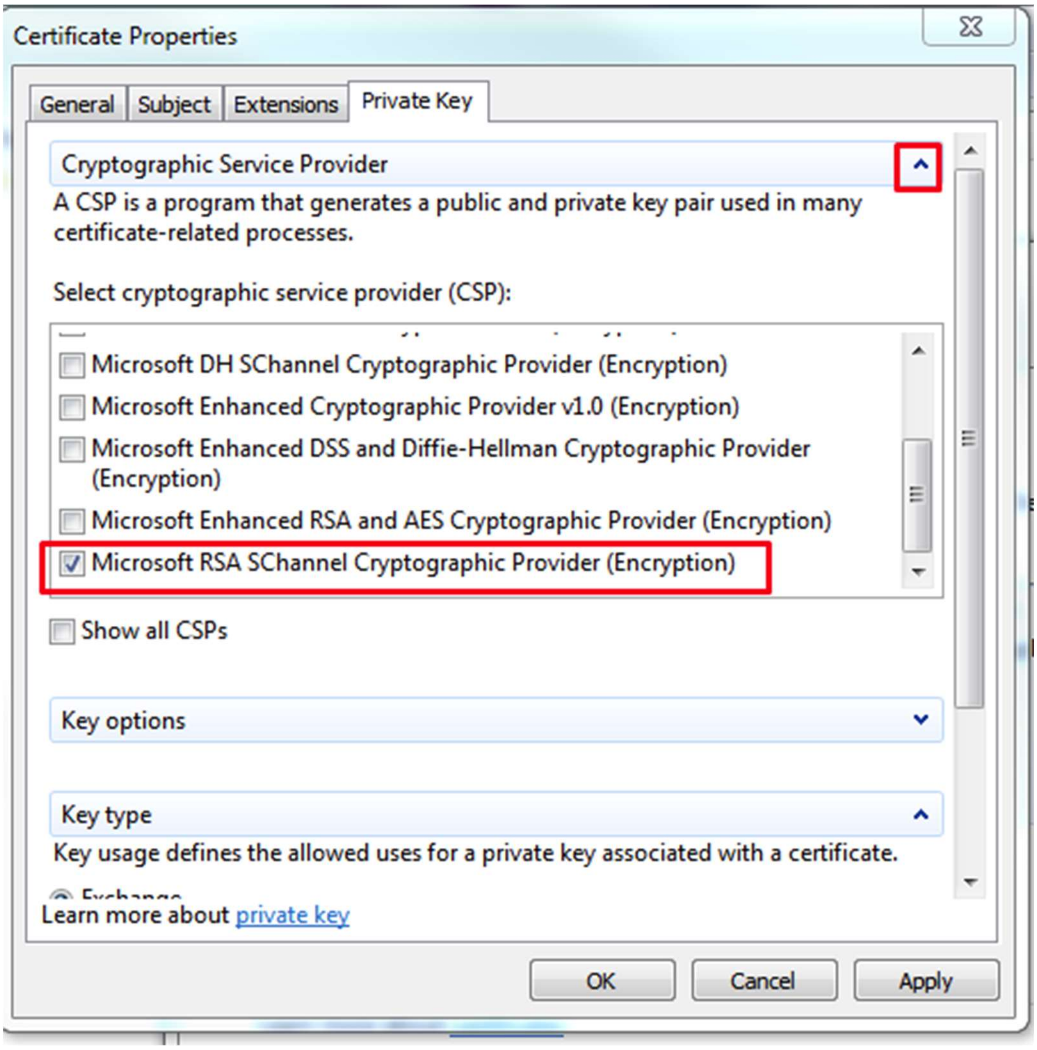
○ Signature

Key permissions

Learn more about private key

16. Once you have selected the key type, you need to choose which algorithm is used to encrypt the data. To do this, expand the *Cryptographic Service Providers* section and make sure that only one option is selected, *Microsoft RSA SChannel Cryptographic Provider (Encryption).*

Figure 15 Choice of encryption algorithm



Certificate Properties

Cryptographic Service Provider

A CSP is a program that generates a public and private key pair used in many certificate-related processes.

Select cryptographic service provider (CSP):

□ Microsoft DH SChannel Cryptographic Provider (Encryption)
□ Microsoft Enhanced Cryptographic Provider v1.0 (Encryption)
□ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider (Encryption)
□ Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)
☑ Microsoft RSA SChannel Cryptographic Provider (Encryption)

□ Show all CSPs

Key options

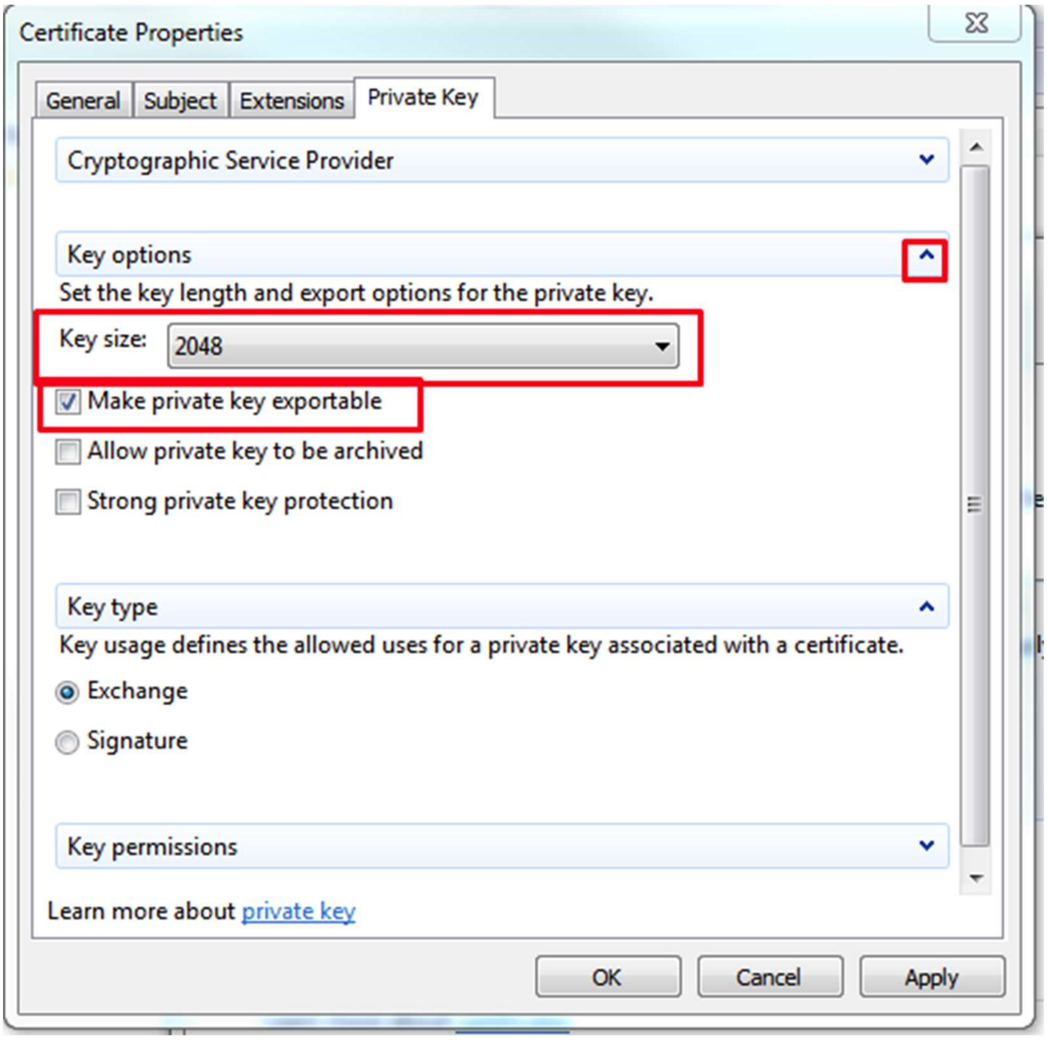
Key type

Key usage defines the allowed uses for a private key associated with a certificate.

Learn more about private key

17. Finally, you need to specify the key size by expanding the *Key options* section, selecting *2048* next to *Key size,* and selecting the *Make private key exportable* checkbox.

Figure 16 Key size selection



Key options

Set the key length and export options for the private key.

Key size: 2048

☑ Make private key exportable

□ Allow private key to be archived

□ Strong private key protection

Key type

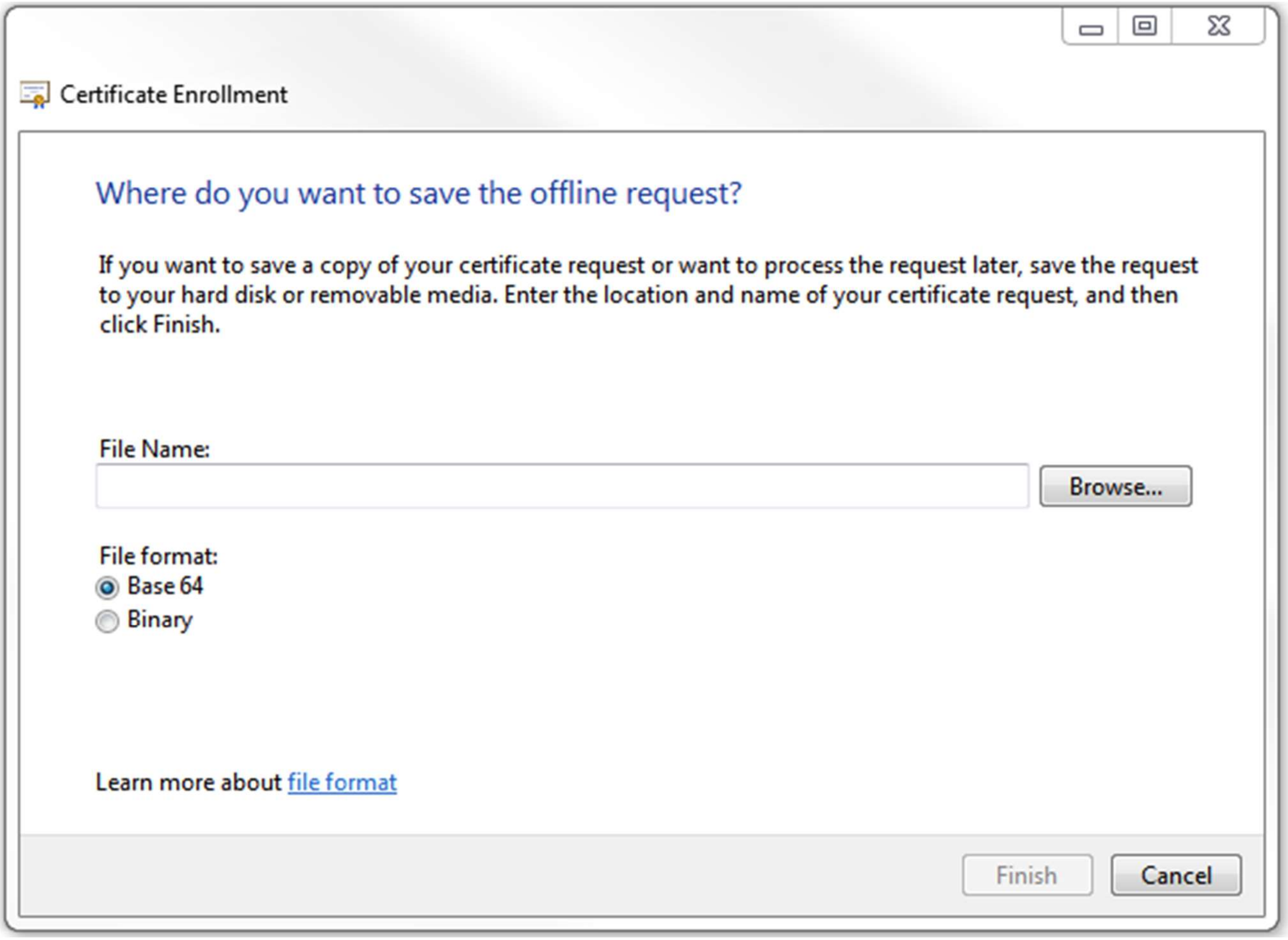
Key usage defines the allowed uses for a private key associated with a certificate.

● Exchange

○ Signature

18. After completing all the above steps, click *OK* - this will close the pop-up window and return to the wizard. In the wizard, click *Next*. You will be asked to specify the disk location where you want to save the certificate request.

Figure 17 Query save dialog



Certificate Enrollment

Where do you want to save the offline request?

If you want to save a copy of your certificate request or want to process the request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish.

File Name:

Browse...

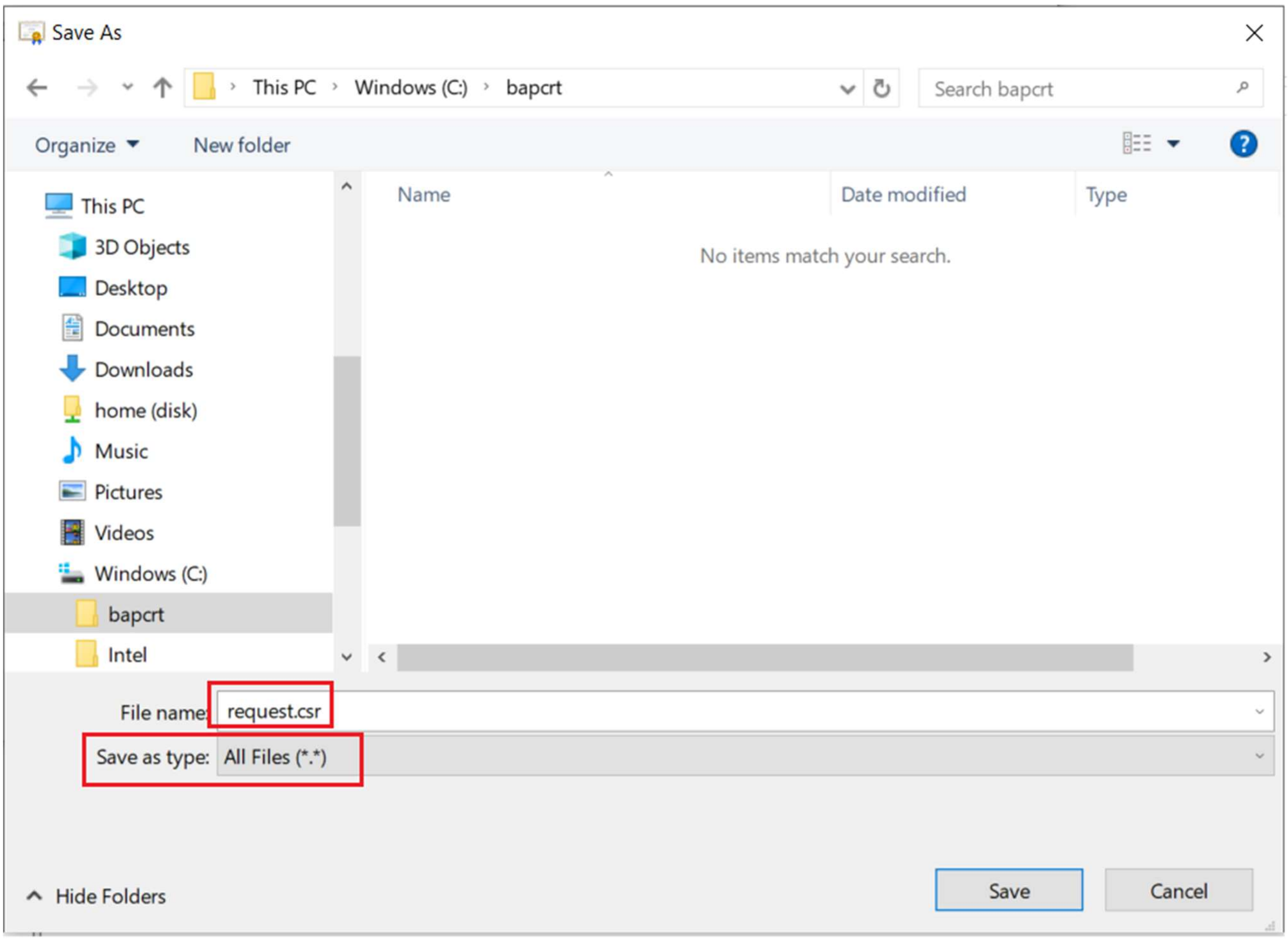
File format:
● Base 64
○ Binary

Learn more about file format

Finish Cancel

19. Click the *Browse ...* button and choose where you want to save the file. It is recommended that you store the file in the *"bapcrt"* folder created at the address in step 1. It's important to save a file with a "*csr"* extension - to do this, add *".csr"* ending to the file name and specify *All files (*. *)* option in the *Save as type* field. Click *Save* in the dialog box after completing all the steps.

Figure 18 File save dialog

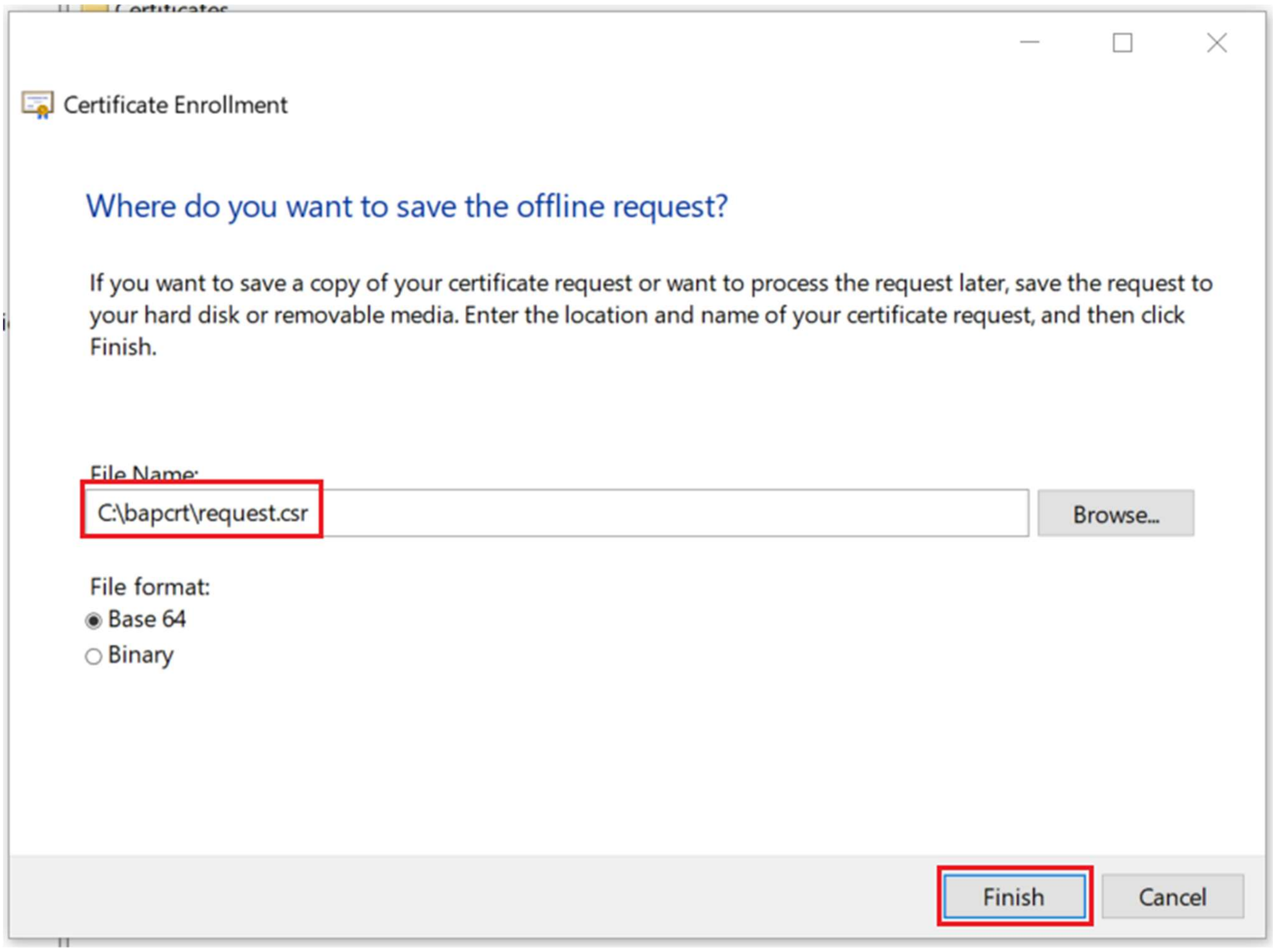


File name: request.csr

Save as type: All Files (*.*)

20. You will be returned to the wizard where you click *Finish.* CSR generated successfully and saved to a file you specified. Continue generating the certificate from the *Download and install the certificate* section.

Figure 19 End of the wizard



Certificate Enrollment

Where do you want to save the offline request?

If you want to save a copy of your certificate request or want to process the request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish.

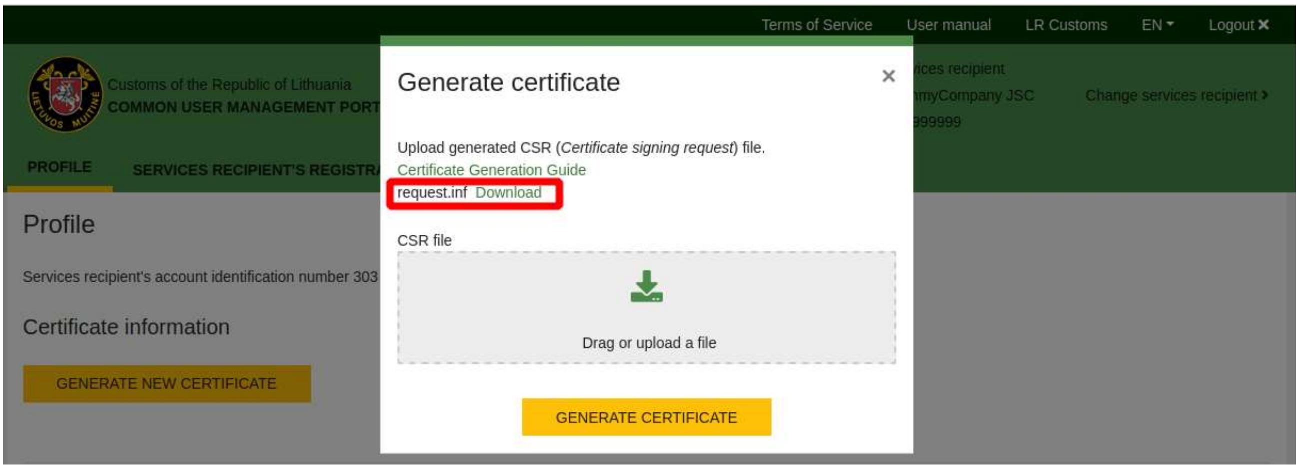
File Name: C:\bapcrt\request.csr

File format:
● Base 64
○ Binary

2.1.2 *Using Command Prompt*

1. Create a *"request.inf"* file. The contents of the file are listed below. **Note:** You can download the prepared *"request.inf"* file in the certificate generation window or on the login page. After downloading the file, enter your first and last name in the Subject line instead of *Name Surname*.

Figure 20 Download of the request.inf file for a logged-in BAP user



Terms of Service
User manual
LR Customs
EN ▾
Logout ✕
Customs of the Republic of Lithuania
COMMON USER MANAGEMENT PORT
PROFILE
SERVICES RECIPIENT'S REGISTR
ices recipient
myCompany JSC
999999
Change services recipient ›

Profile

Services recipient's account identification number 303

Certificate information

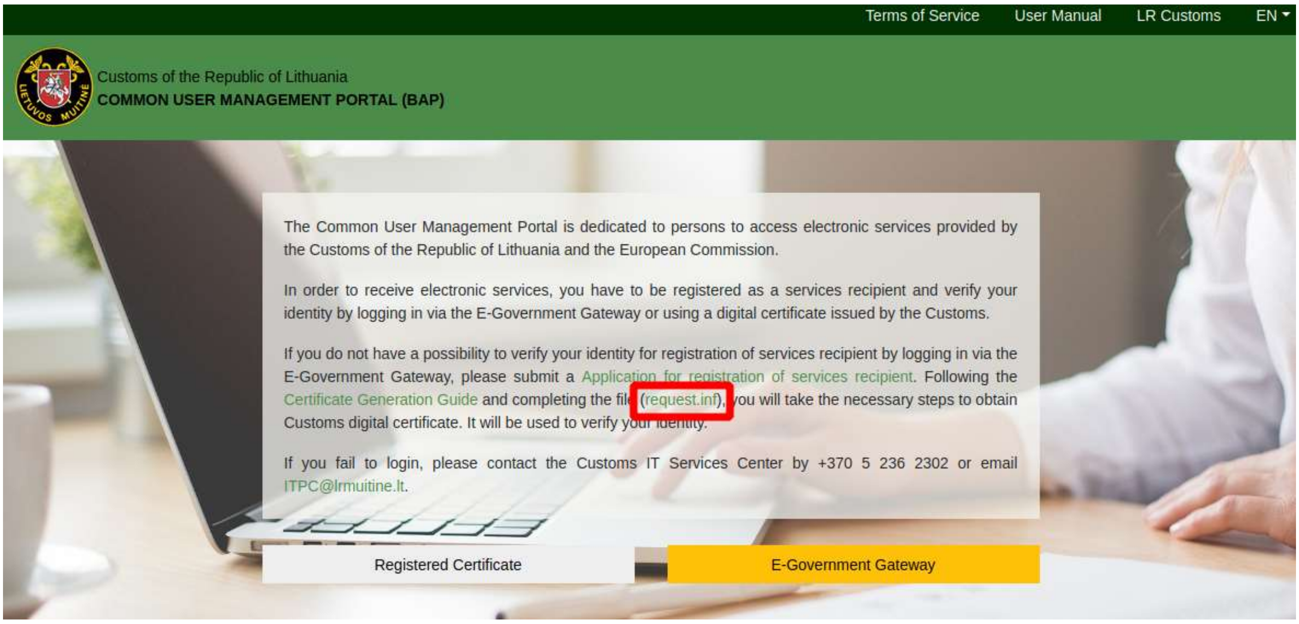
Generate certificate ×

Upload generated CSR (*Certificate signing request*) file.
Certificate Generation Guide
request.inf Download

CSR file

Drag or upload a file

Figure 21 Download the request.inf file for an offline user



Terms of Service
User Manual
LR Customs
EN
Customs of the Republic of Lithuania
COMMON USER MANAGEMENT PORTAL (BAP)

The Common User Management Portal is dedicated to persons to access electronic services provided by the Customs of the Republic of Lithuania and the European Commission.

In order to receive electronic services, you have to be registered as a services recipient and verify your identity by logging in via the E-Government Gateway or using a digital certificate issued by the Customs.

If you do not have a possibility to verify your identity for registration of services recipient by logging in via the E-Government Gateway, please submit a Application for registration of services recipient. Following the Certificate Generation Guide and completing the file (request.inf), you will take the necessary steps to obtain Customs digital certificate. It will be used to verify your identity.

If you fail to login, please contact the Customs IT Services Center by +370 5 236 2302 or email ITPC@lrmuitine.lt.

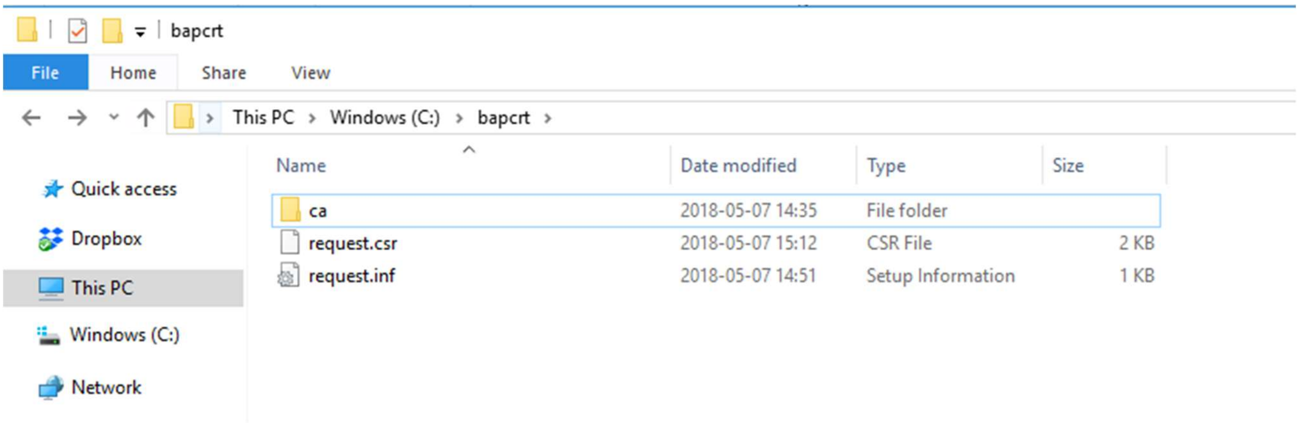
```
;----------------- request.inf -----------------
[Version]
Signature="$Windows NT$"

[NewRequest]
Subject = "CN=Name Surname, G=Name, SN=Surname"
KeySpec = 1
KeyLength = 2048
Exportable = True
MachineKeySet = False
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

[Extensions]
2.5.29.17 = "{text}"
_continue_ = "email=email@example.com"

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1
;-----------------------------------------------
```

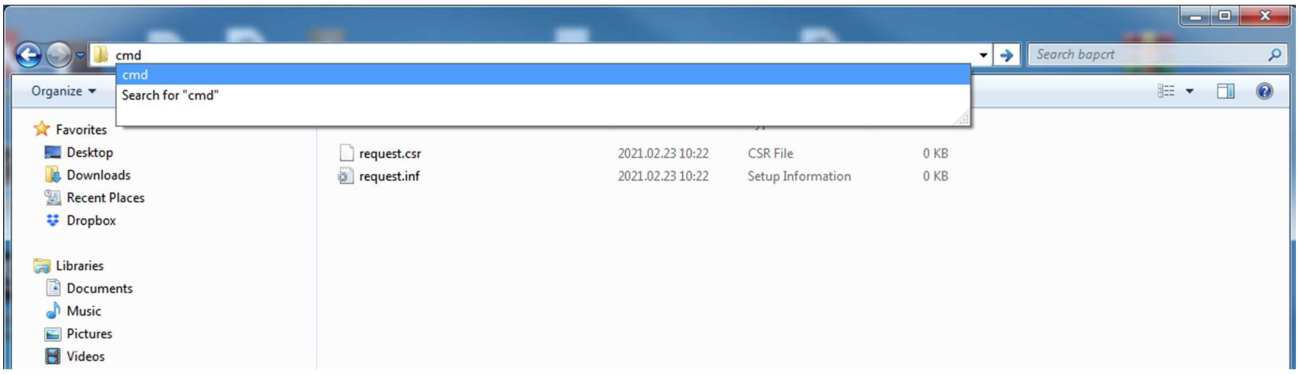
Figure 22 Creating a file request.inf



Name	Date modified	Type	Size
ca	2018-05-07 14:35	File folder	
request.csr	2018-05-07 15:12	CSR File	2 KB
request.inf	2018-05-07 14:51	Setup Information	1 KB

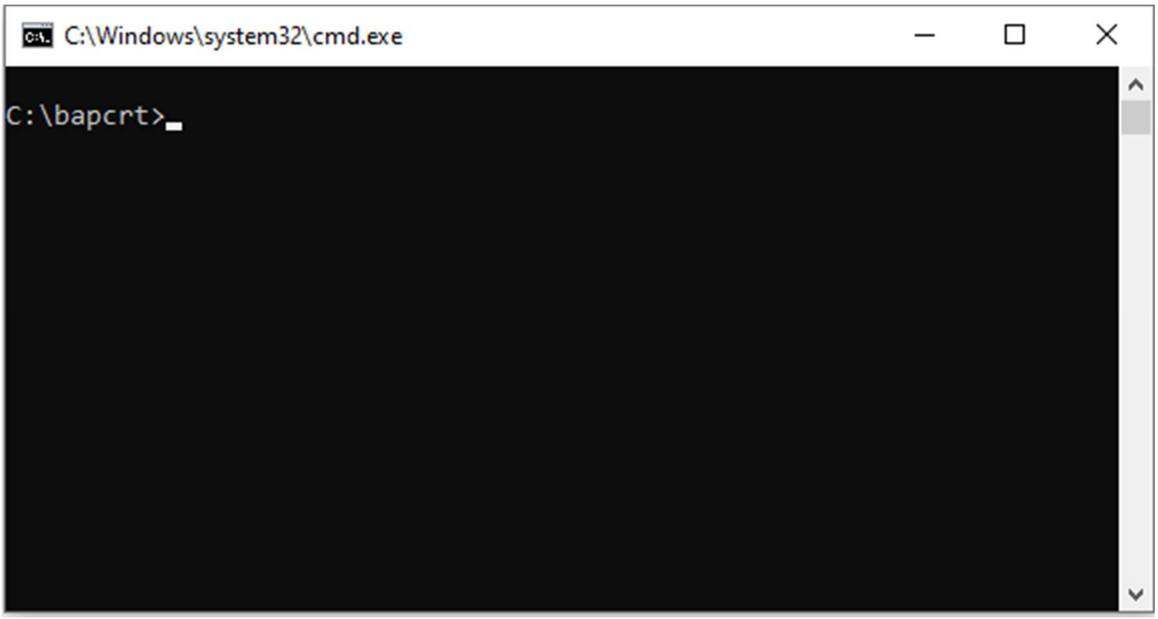
2. Open the *cmd command line*. To do this, type "cmd" in the address bar of the current *"bapcrt"* folder and press the *Enter* key on your keyboard.

Figure 23 opening cmd through the address bar



request.csr	2021.02.23 10:22	CSR File	0 KB
request.inf	2021.02.23 10:22	Setup Information	0 KB

Figure 24 cmd line window



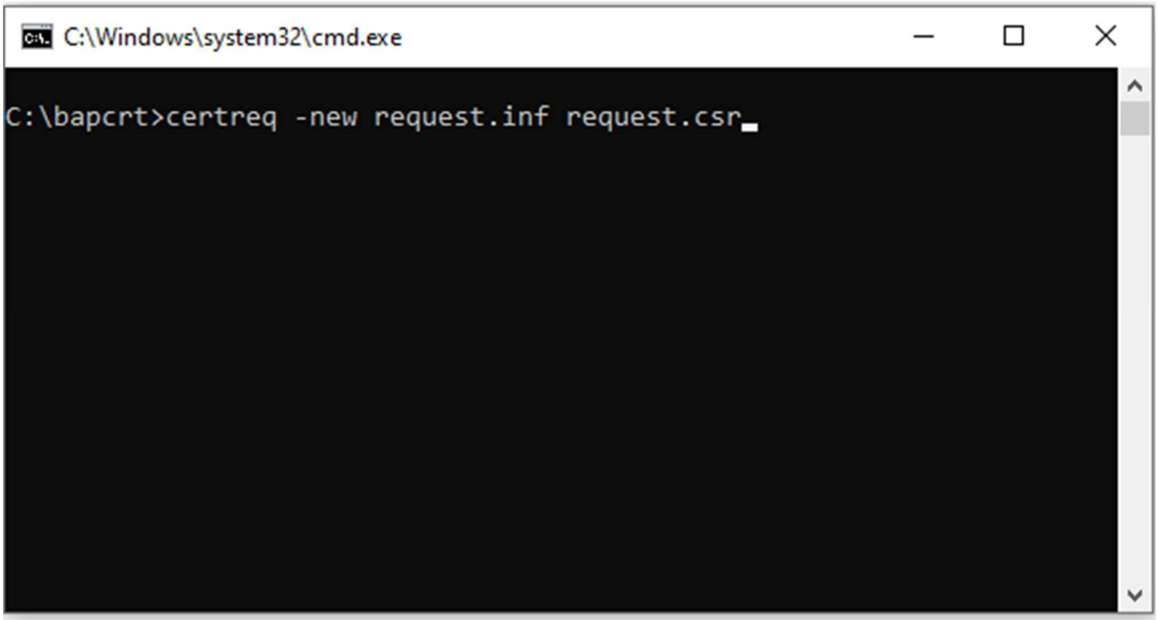
C:\Windows\system32\cmd.exe

```
C:\bapcrt>_
```

3. In the opened window, enter the following command:

```
C:\bapcrt> certreq -new request.inf request.csr
```

Figure 25 Example of command entry



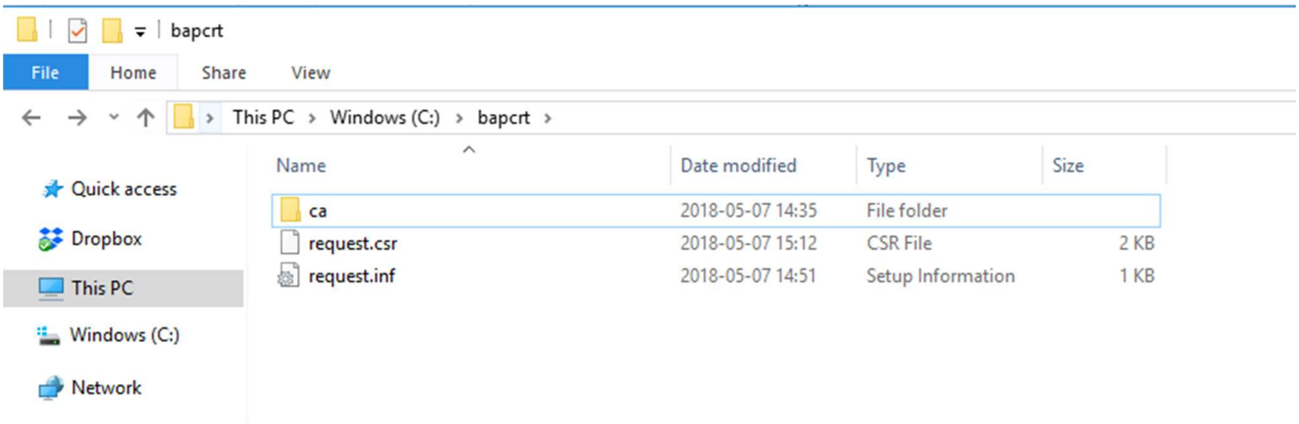
C:\Windows\system32\cmd.exe

```
C:\bapcrt>certreq -new request.inf request.csr_
```

After successfully creating *"request.csr"*, you will receive a response from the command line:

```
CertReq: Request Created
```

Figure 26 Creating a file request.csr



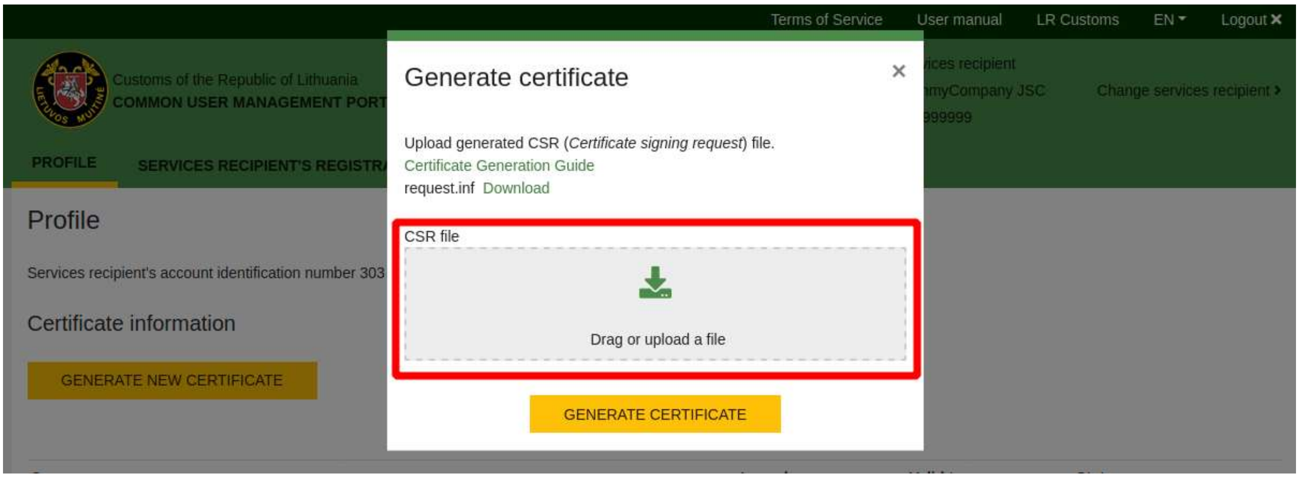
Name	Date modified	Type	Size
ca	2018-05-07 14:35	File folder	
request.csr	2018-05-07 15:12	CSR File	2 KB
request.inf	2018-05-07 14:51	Setup Information	1 KB

2.2 Certificate download and installation

1. If you have not used the BAP system until now and cannot log in via the Electronic Government Gateway, send the prepared *"request.csr"* file by e-mail to customs when requested. You will receive a response with "*certificate.crt"*, which we will save in created folder *"bapcrt"*.

If you can log in to the BAP using the authentication service provided by the Electronic Government Gateway or you have already used the BAP system and are able to login to it, then attach the file *"request.csr"* in the *Profile* section by clicking the *Generate new certificate* button. Download the *"certificate.crt"* file by clicking the *Download* button in the modal window or in the certificate data table. Save the downloaded file to the *"bapcrt"* folder.

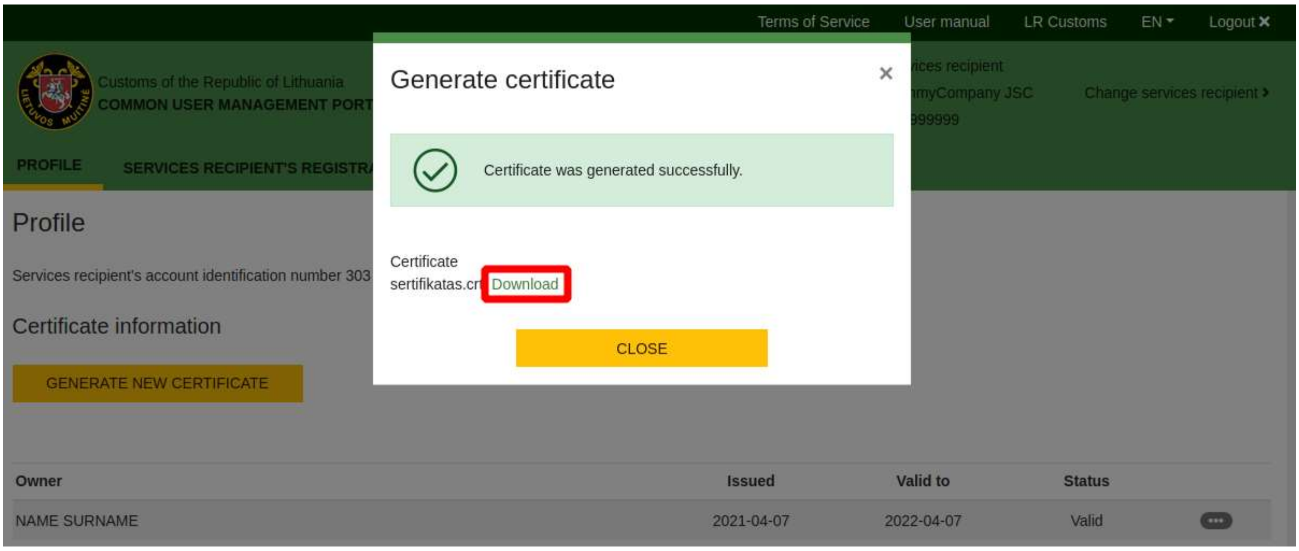
Figure 27 CSR file upload location



Services recipient's account identification number 303

Upload generated CSR (*Certificate signing request*) file.
Certificate Generation Guide
request.inf Download

Figure 28 CRT file download


Terms of Service
User manual
LR Customs
EN
Logout ✕
Customs of the Republic of Lithuania
COMMON USER MANAGEMENT PORT
...ices recipient
...myCompany JSC
...999999
Change services recipient ›
PROFILE
SERVICES RECIPIENT'S REGISTR

Profile

Services recipient's account identification number 303

Certificate information

GENERATE NEW CERTIFICATE

Owner	Issued	Valid to	Status	
NAME SURNAME	2021-04-07	2022-04-07	Valid	•••

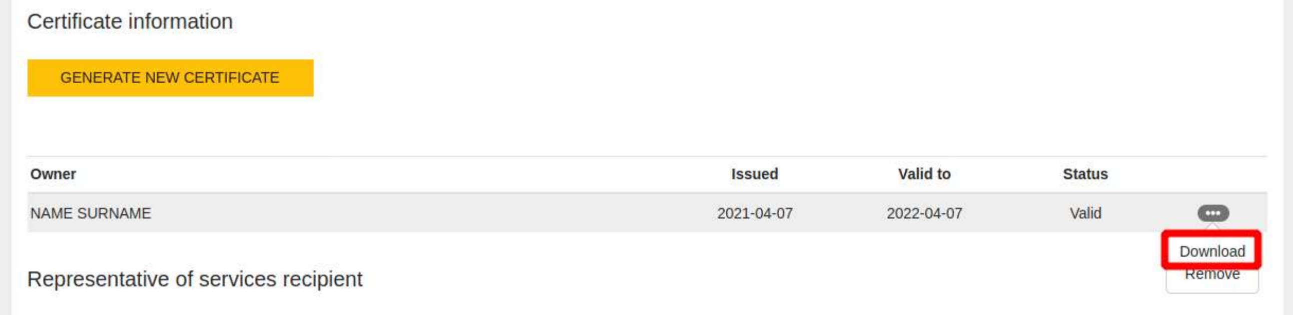
Generate certificate ×

Certificate was generated successfully.

Certificate
sertifikatas.crt Download

CLOSE

Figure 29 Download of a CRT certificate from a certificate data table



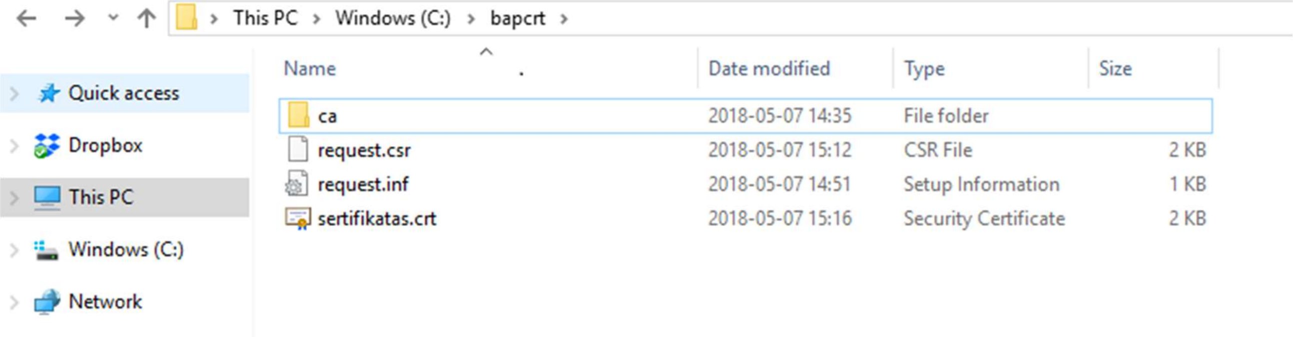
Certificate information

GENERATE NEW CERTIFICATE

Owner	Issued	Valid to	Status	
NAME SURNAME	2021-04-07	2022-04-07	Valid	•••

Representative of services recipient

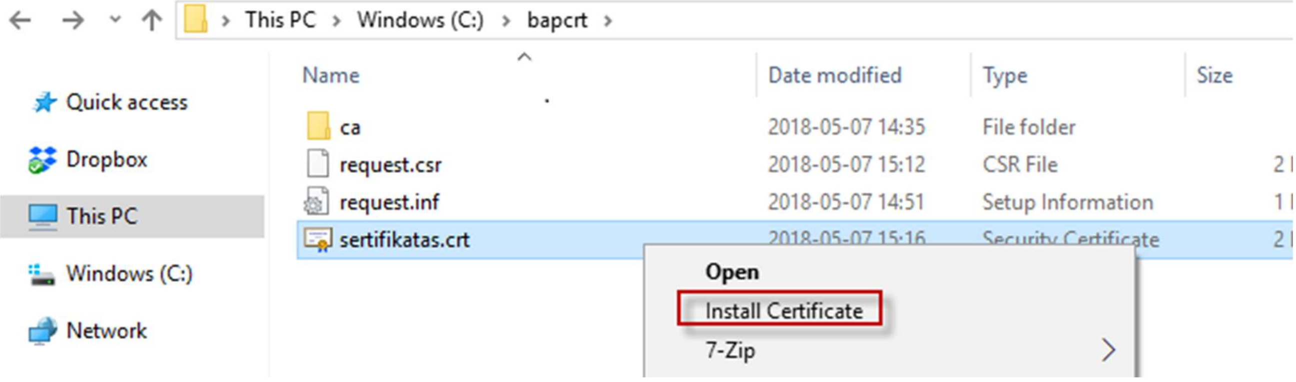
Figure 30 Creating the sertifikatas.crt file



Name	Date modified	Type	Size
ca	2018-05-07 14:35	File folder	
request.csr	2018-05-07 15:12	CSR File	2 KB
request.inf	2018-05-07 14:51	Setup Information	1 KB
sertifikatas.crt	2018-05-07 15:16	Security Certificate	2 KB

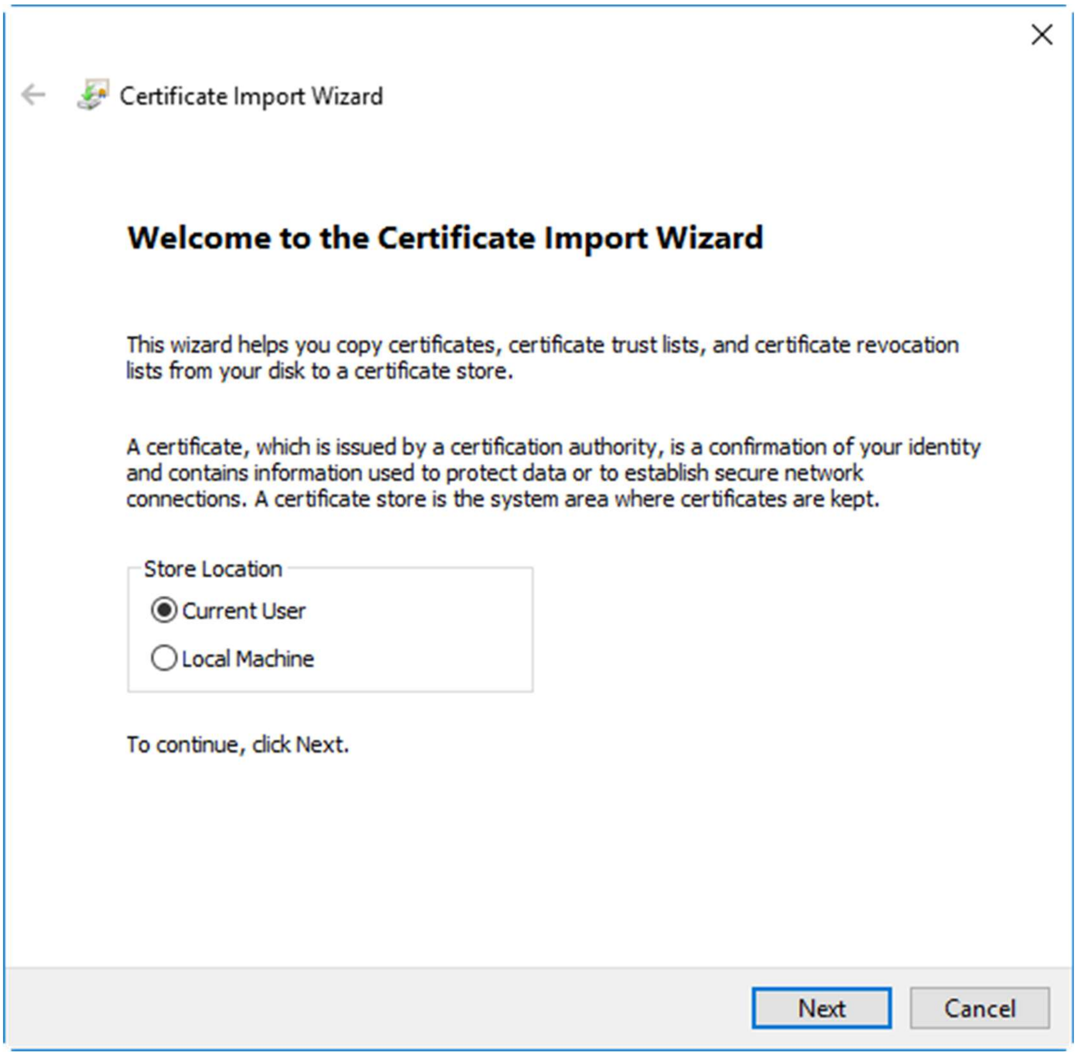
2. Import the certificate into the user certificate cache. Right-click on the "*sertifikatas.crt"* file and select *Install Certificate* in the pop-up window that opens.

Figure 31 Importing a certificate into the user certificate cache



Name	Date modified	Type	Size
ca	2018-05-07 14:35	File folder	
request.csr	2018-05-07 15:12	CSR File	2
request.inf	2018-05-07 14:51	Setup Information	1
sertifikatas.crt	2018-05-07 15:16	Security Certificate	2

Figure 32 Certificate Import Wizard: placement location selection



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.

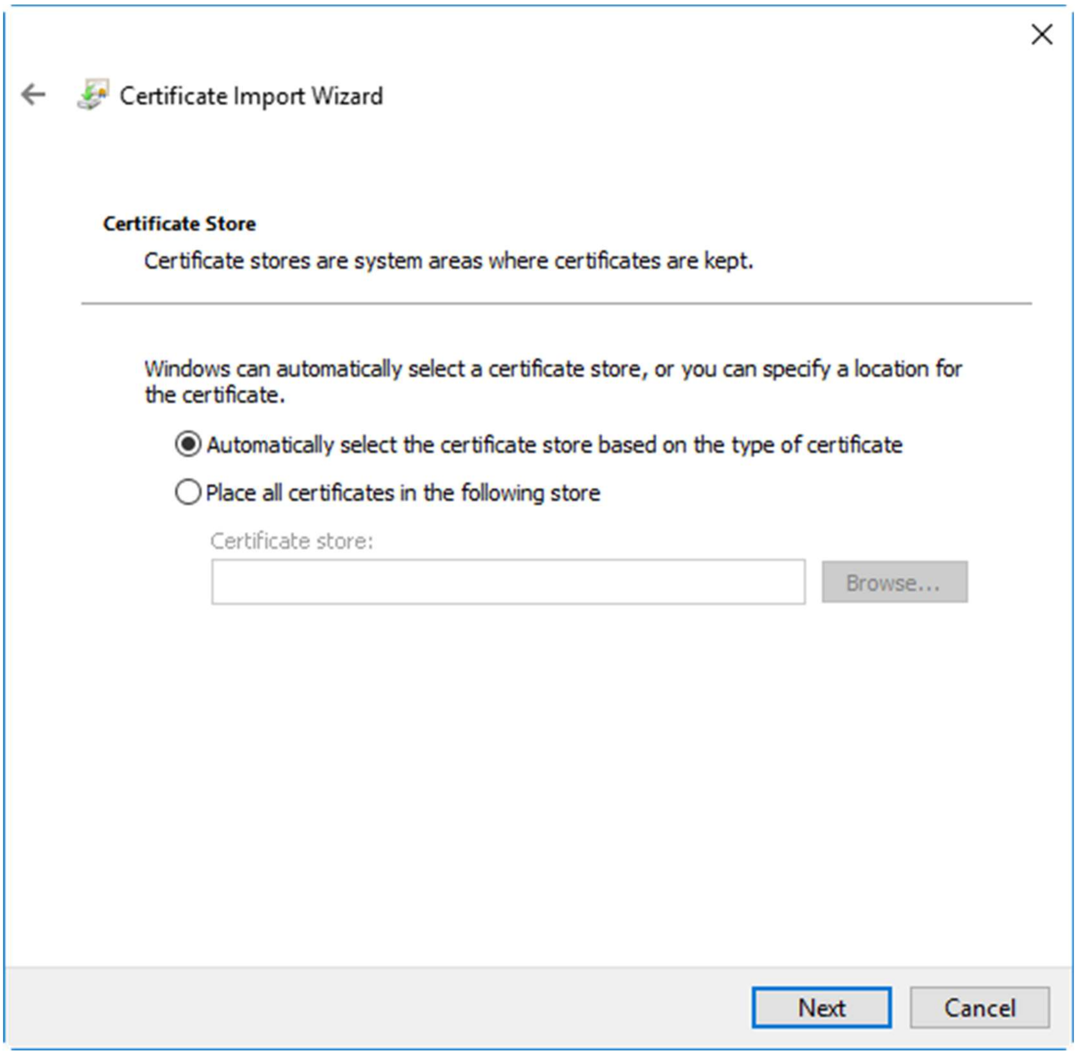
Store Location

● Current User

○ Local Machine

To continue, click Next.

Figure 33 Certificate Import Wizard: specifying the location



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

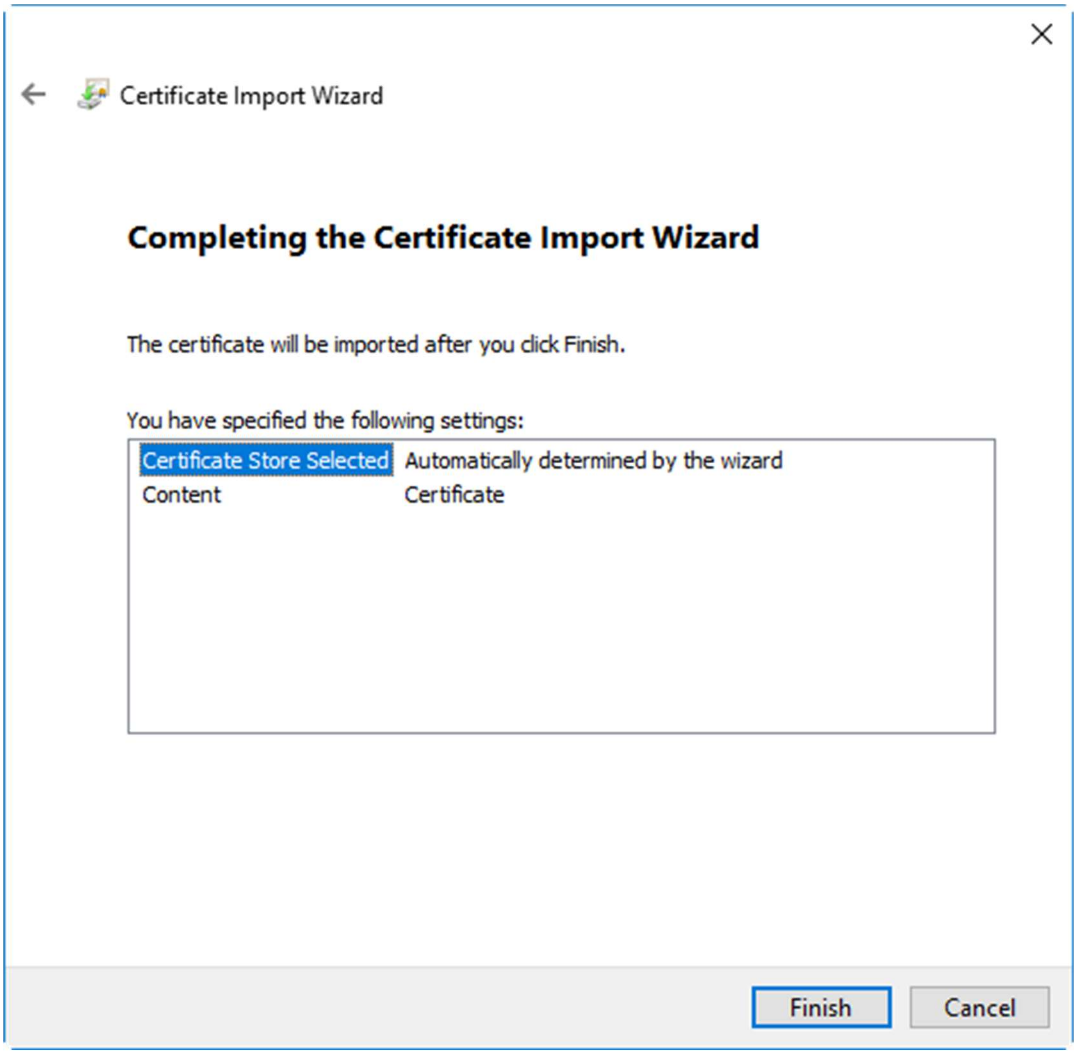
Windows can automatically select a certificate store, or you can specify a location for the certificate.

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

○ Place all certificates in the following store

Certificate store:

Figure 34 Certificate Import Wizard: Reviewing settings



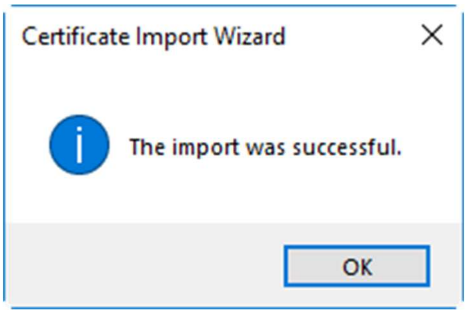
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by the wizard
Content	Certificate

Figure 35 Certificate Import Wizard: notification of the successful completion of a certificate import



The import was successful.

2.3 Preparing the certificate to work on another computer

1. To open the *Microsoft Management Console,* type "mmc" in the search field in the *Windows Start* bar and start the application that you found.

Figure 36 Search in the Windows Start bar

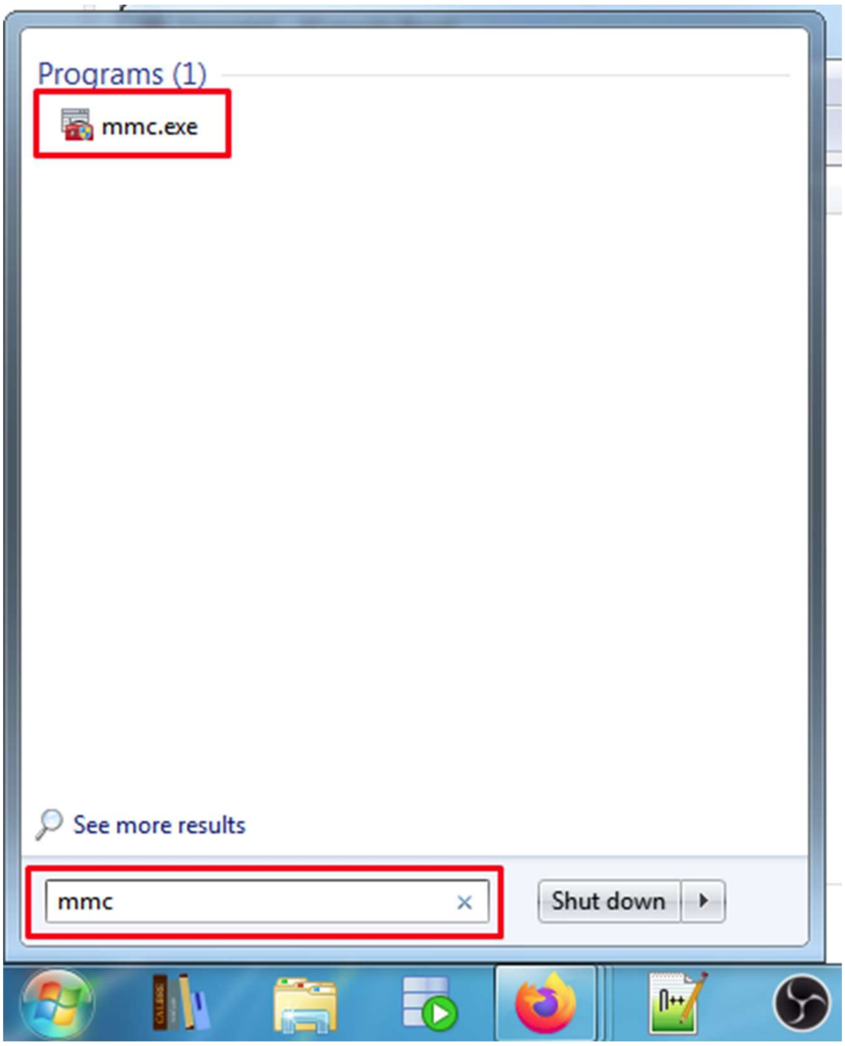
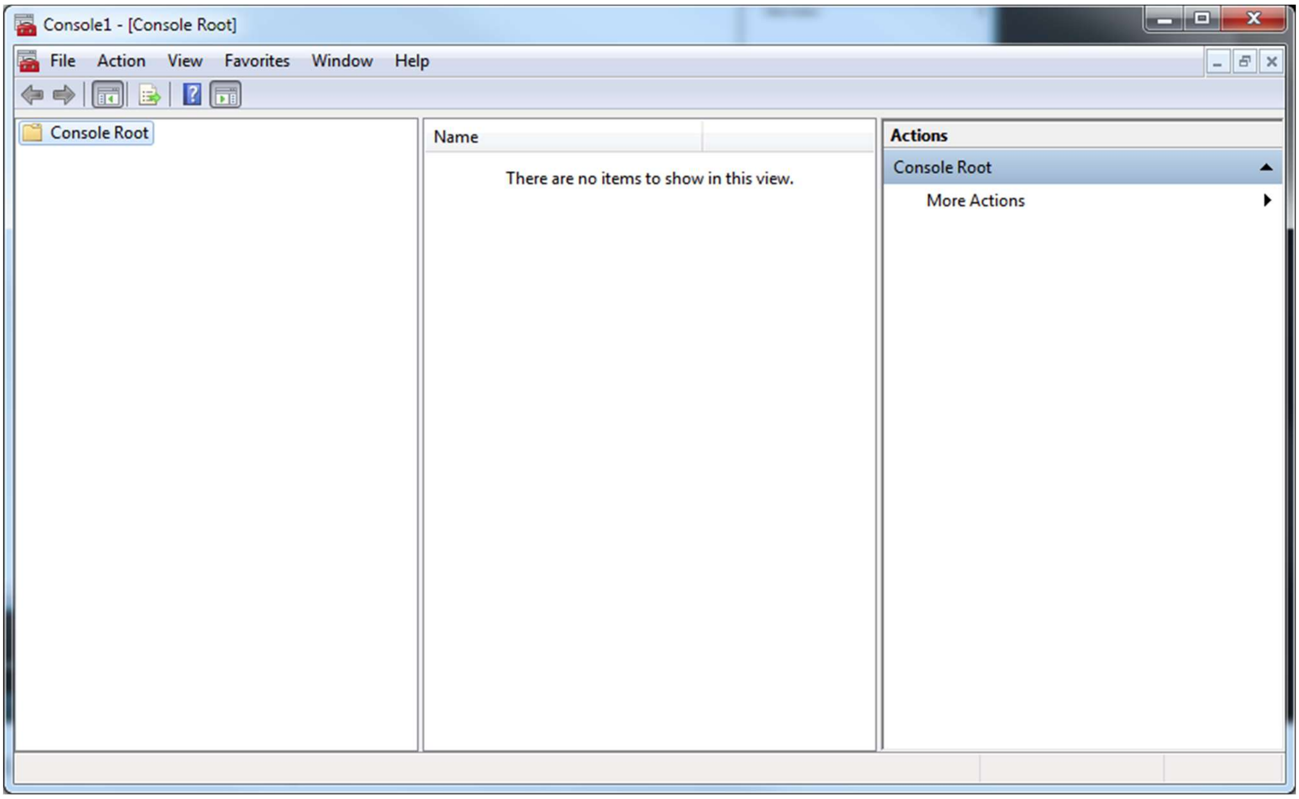


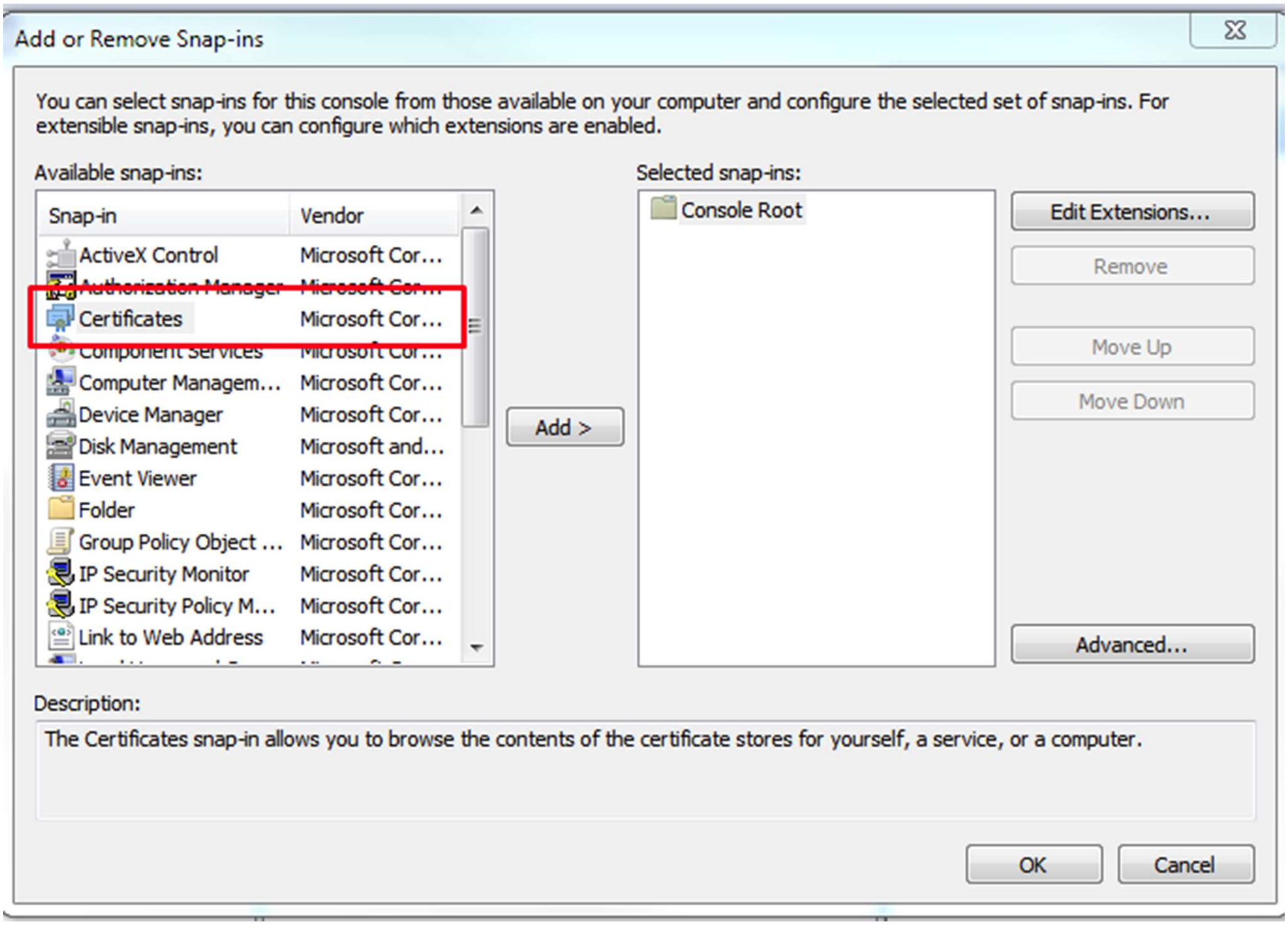
Figure 37 Microsoft Management Console window



There are no items to show in this view.

2. Select *File → Add / Remove Snap-in* in an opened window. In the popup window, select *Certificates* option.

Figure 38 Certificates section selection



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
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

Selected snap-ins:

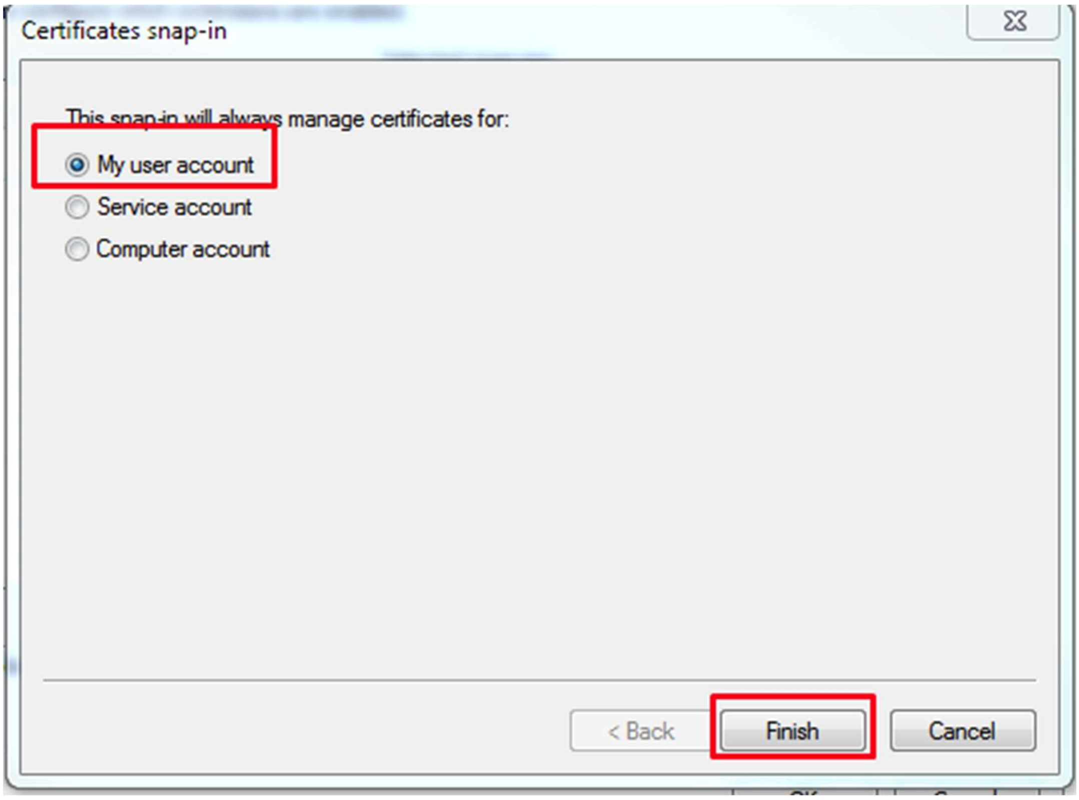
Console Root

Description:

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

3. Click *Add>* button to the right side of the selection. In the new window, select the *My user account* option and click the *Finish* button at the bottom of the window.

Figure 39 My user account selection



Certificates snap-in

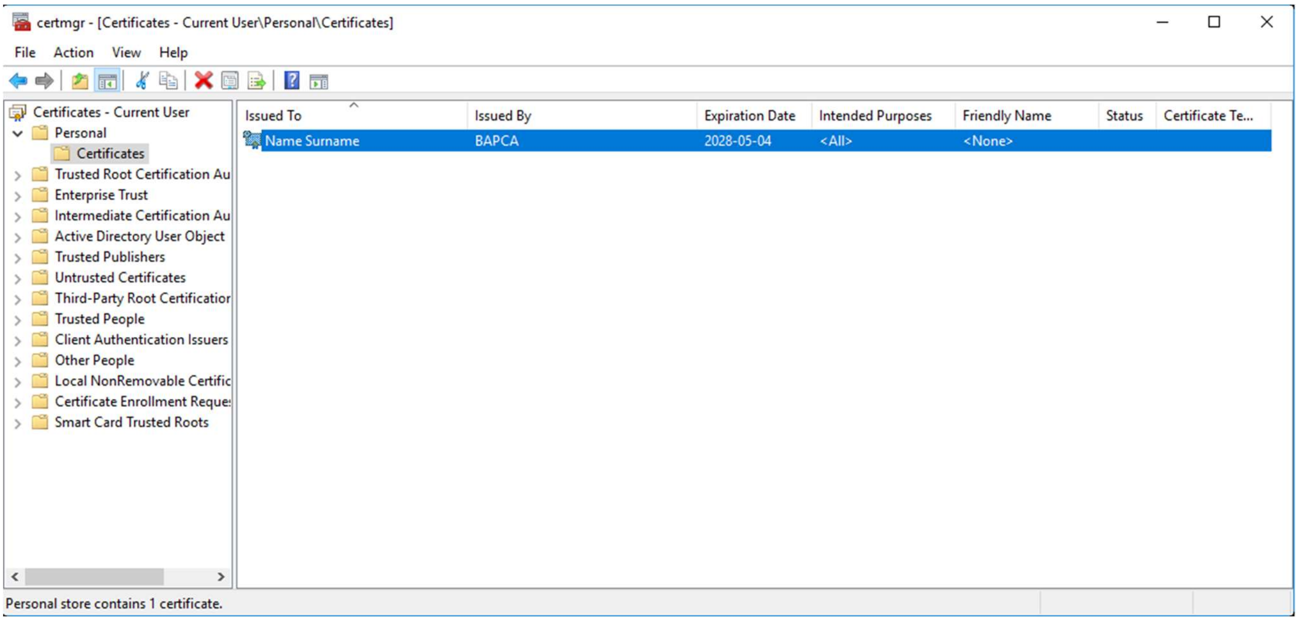
This snap-in will always manage certificates for:

● My user account
○ Service account
○ Computer account

4. Click *Finish* to close the *Snap-in* window.

You should see the imported certificate in an opened window.

Figure 40 View the imported certificate



certmgr - [Certificates - Current User\Personal\Certificates]

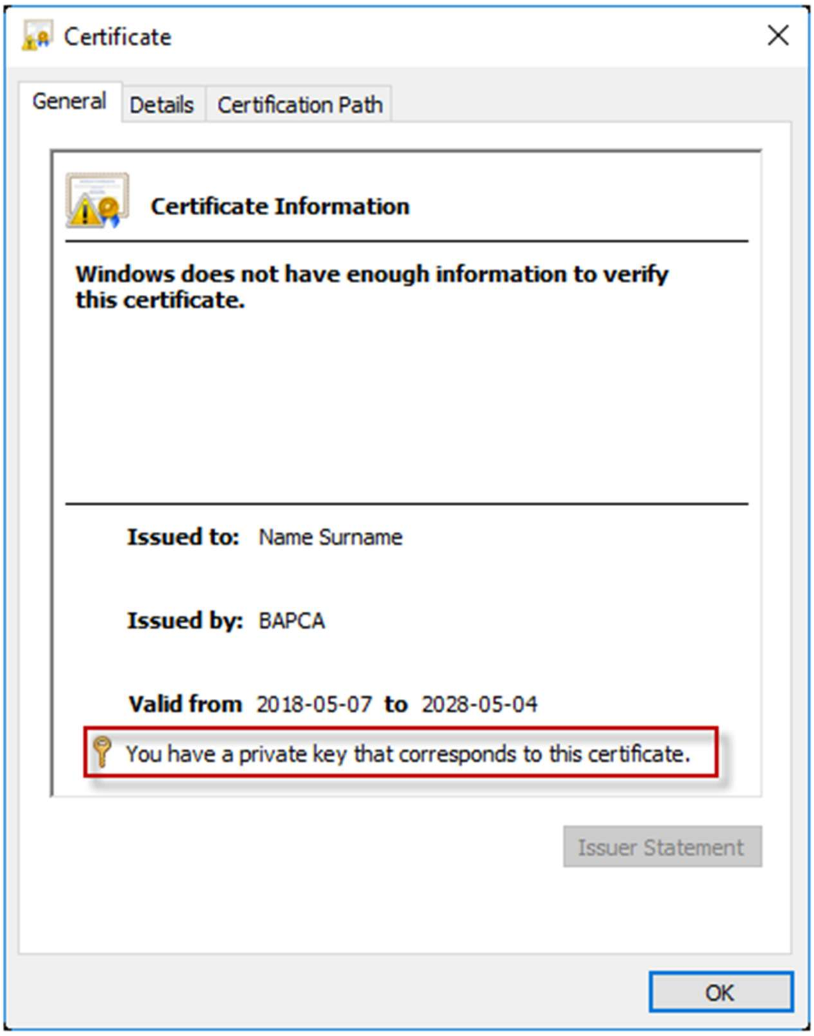
File
Action
View
Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
Other People
Local NonRemovable Certific
Certificate Enrollment Reque:
Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
Name Surname	BAPCA	2028-05-04	<All>	<None>		

Personal store contains 1 certificate.

5. Verify that the certificate has the appropriate private key. After double-clicking on the certificate, you should see the message *You have a private key that corresponds to this certificate*.

Figure 41 Certificate private key verification



Certificate Information

Windows does not have enough information to verify this certificate.

Issued to: Name Surname

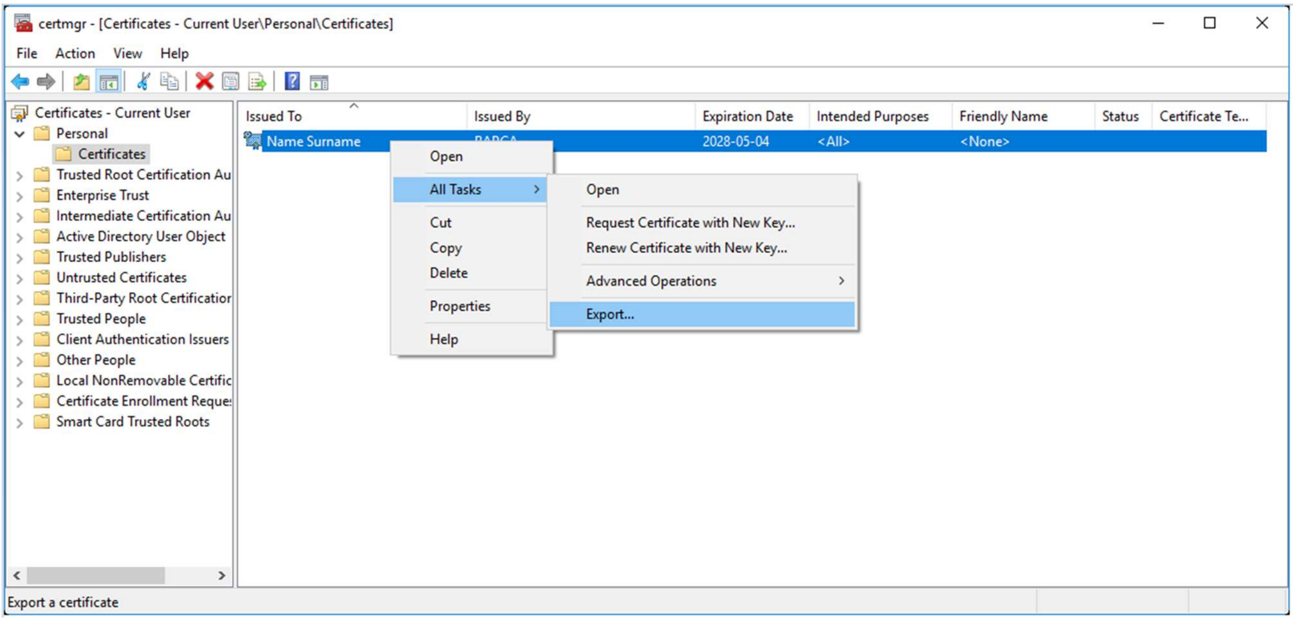
Issued by: BAPCA

Valid from 2018-05-07 **to** 2028-05-04

You have a private key that corresponds to this certificate.

6. Export the certificate along with the private key to a file for use on other computers and to have a backup:

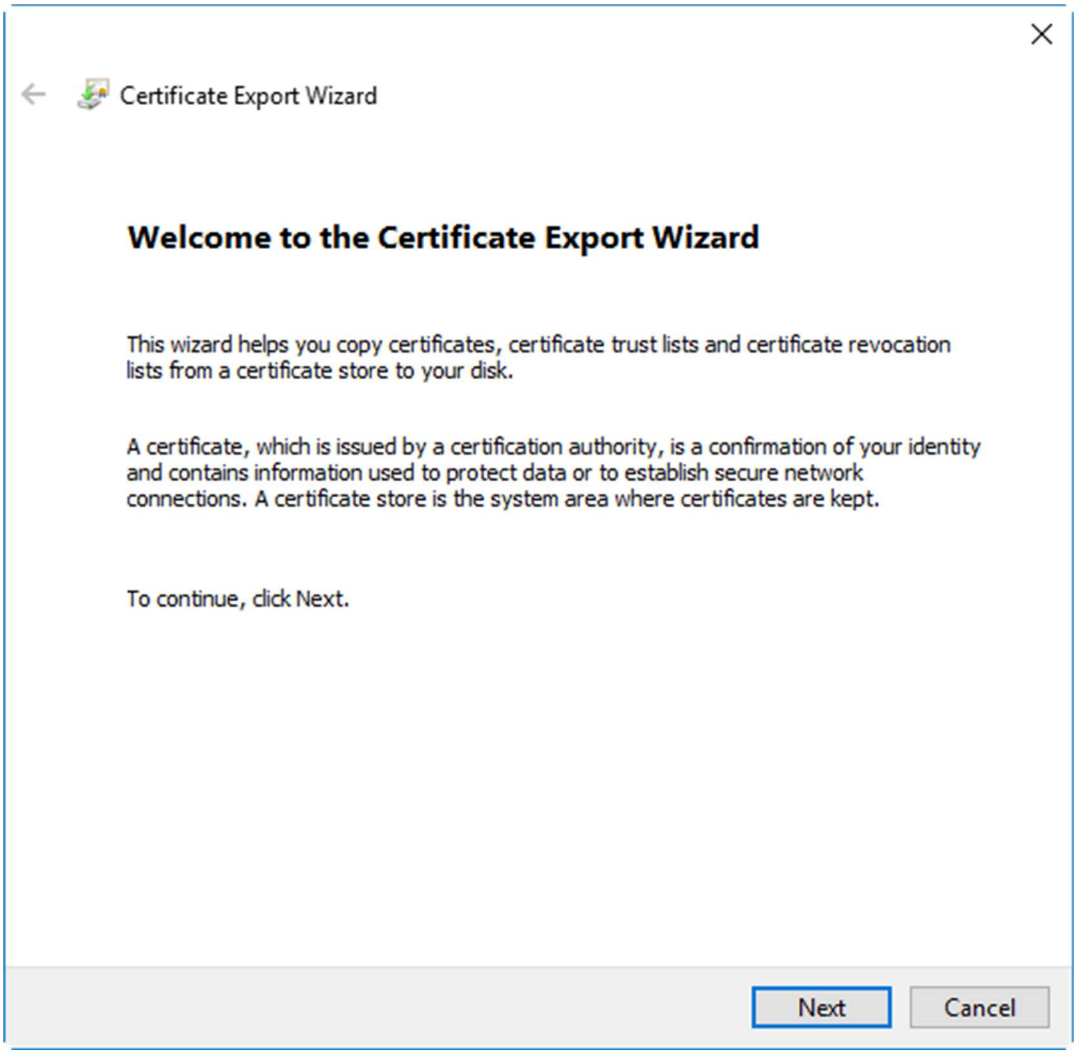
Figure 42 Certificate Export



certmgr - [Certificates - Current User\Personal\Certificates]
File
Action
View
Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
Other People
Local NonRemovable Certific
Certificate Enrollment Reque:
Smart Card Trusted Roots
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Advanced Operations
Export...
Export a certificate

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
Name Surname	BAPCA	2028-05-04	<All>	<None>		

Figure 43 Certificate Export Wizard



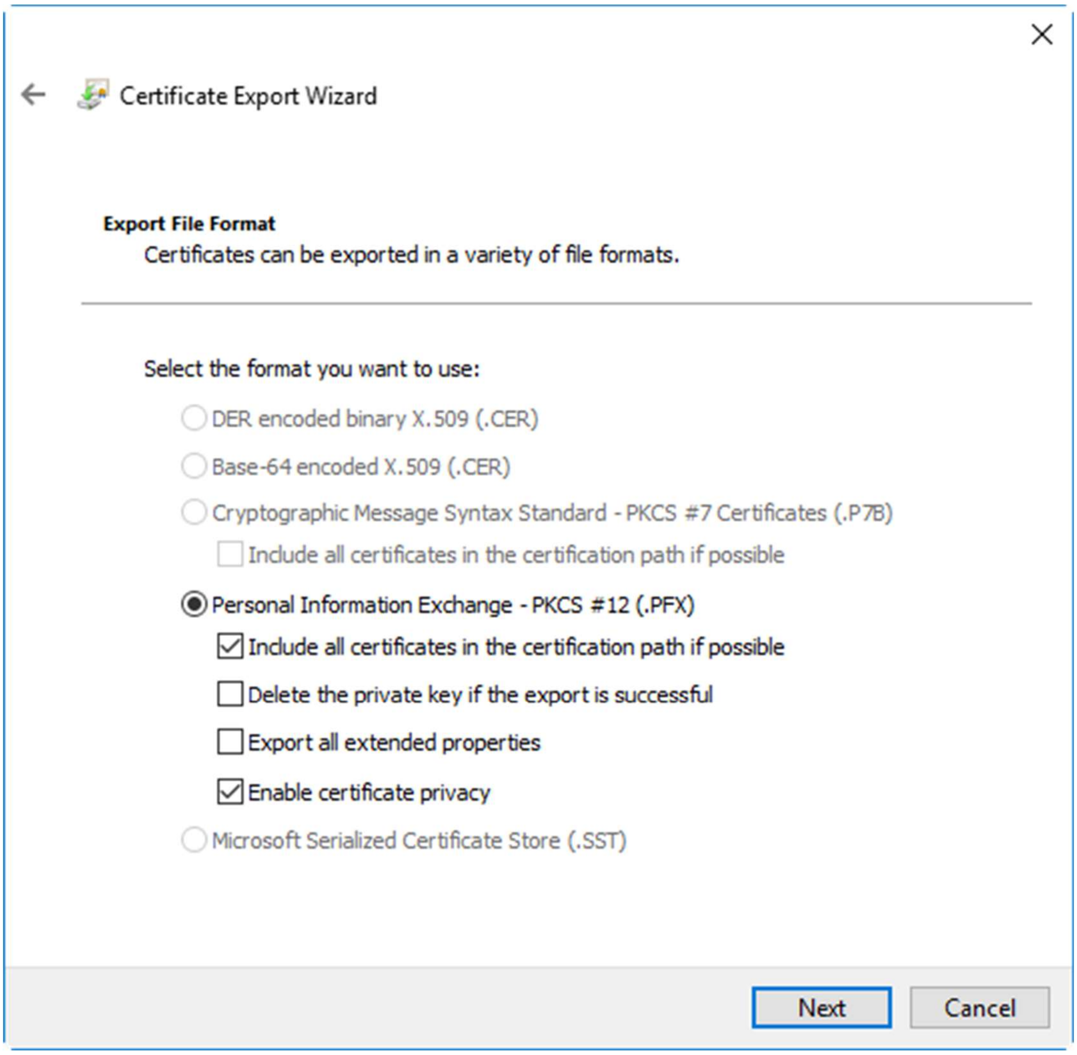
Welcome to the Certificate Export Wizard

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

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.

To continue, click Next.

Figure 44 Certificate Export Wizard: Format selection



Certificate Export Wizard

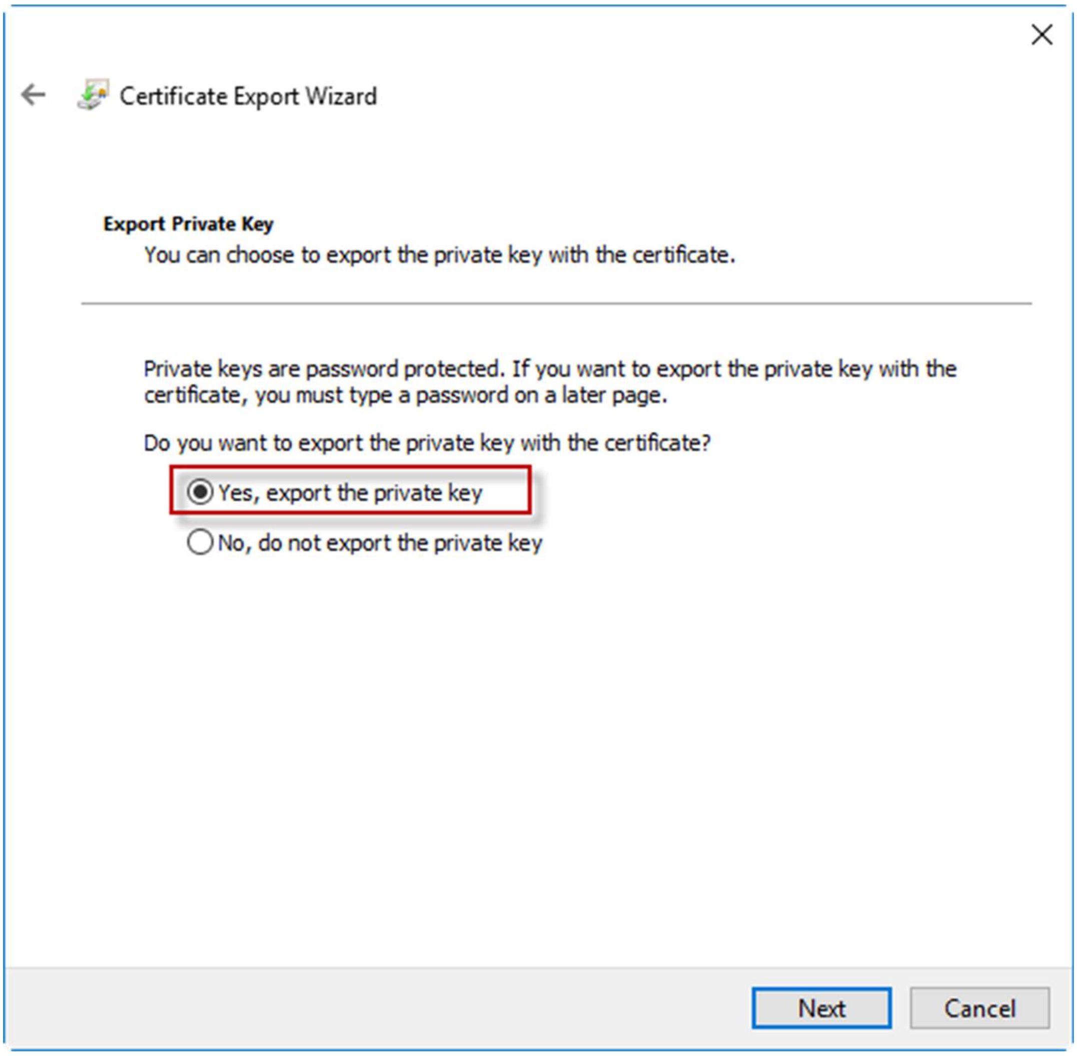
Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ○ DER encoded binary X.509 (.CER)
- ○ Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ● Personal Information Exchange - PKCS #12 (.PFX)
  - ☑ Include all certificates in the certification path if possible
  - □ Delete the private key if the export is successful
  - □ Export all extended properties
  - ☑ Enable certificate privacy
- ○ Microsoft Serialized Certificate Store (.SST)

7. Select to export the private key together with the certificate.

Figure 45 Certificate Export Wizard: Exporting a private key



Certificate Export Wizard

Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

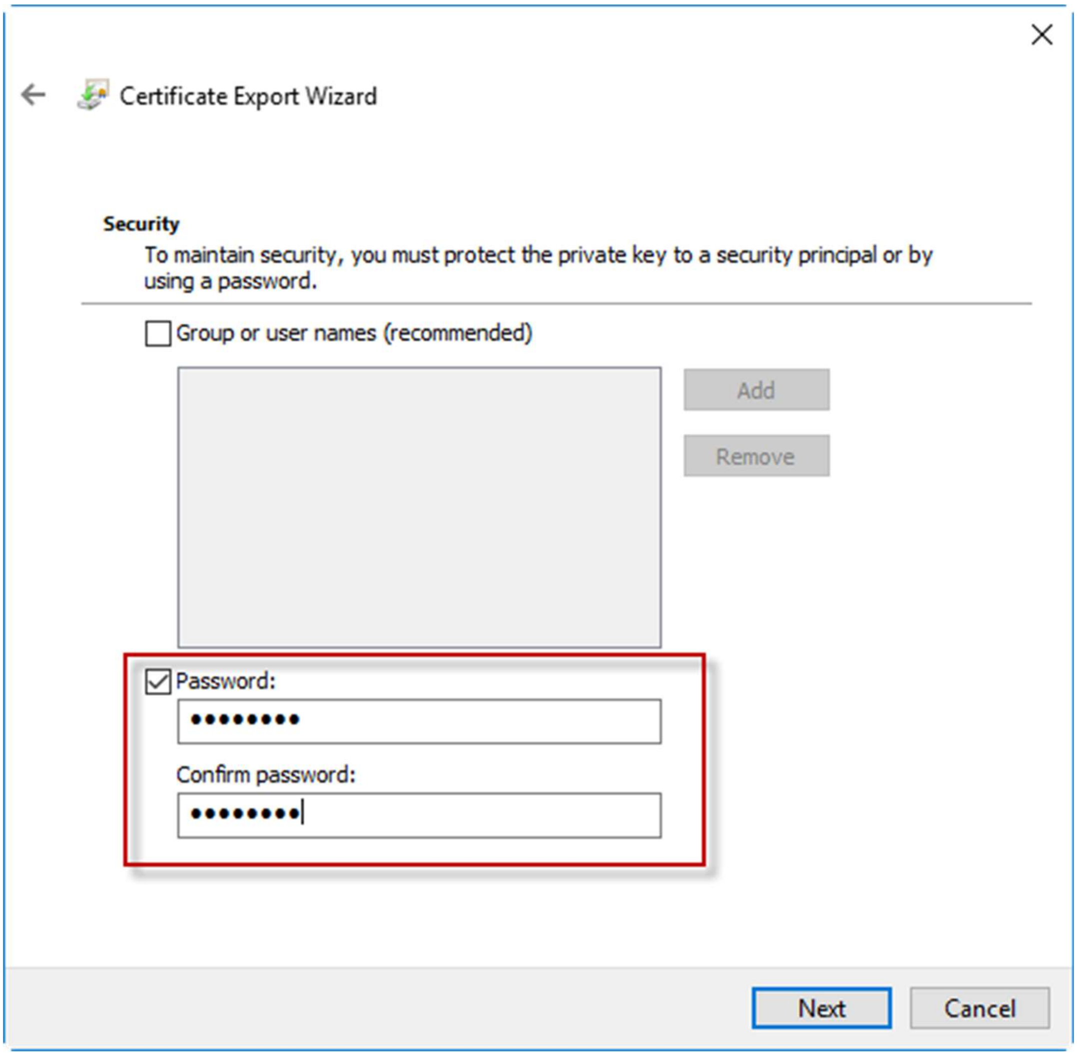
Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

8. Create a password that will protect the private key of the certificate.

Figure 46 Certificate Export Wizard: Creating a password



Certificate Export Wizard

Security

To maintain security, you must protect the private key to a security principal or by using a password.

□ Group or user names (recommended)

☑ Password:

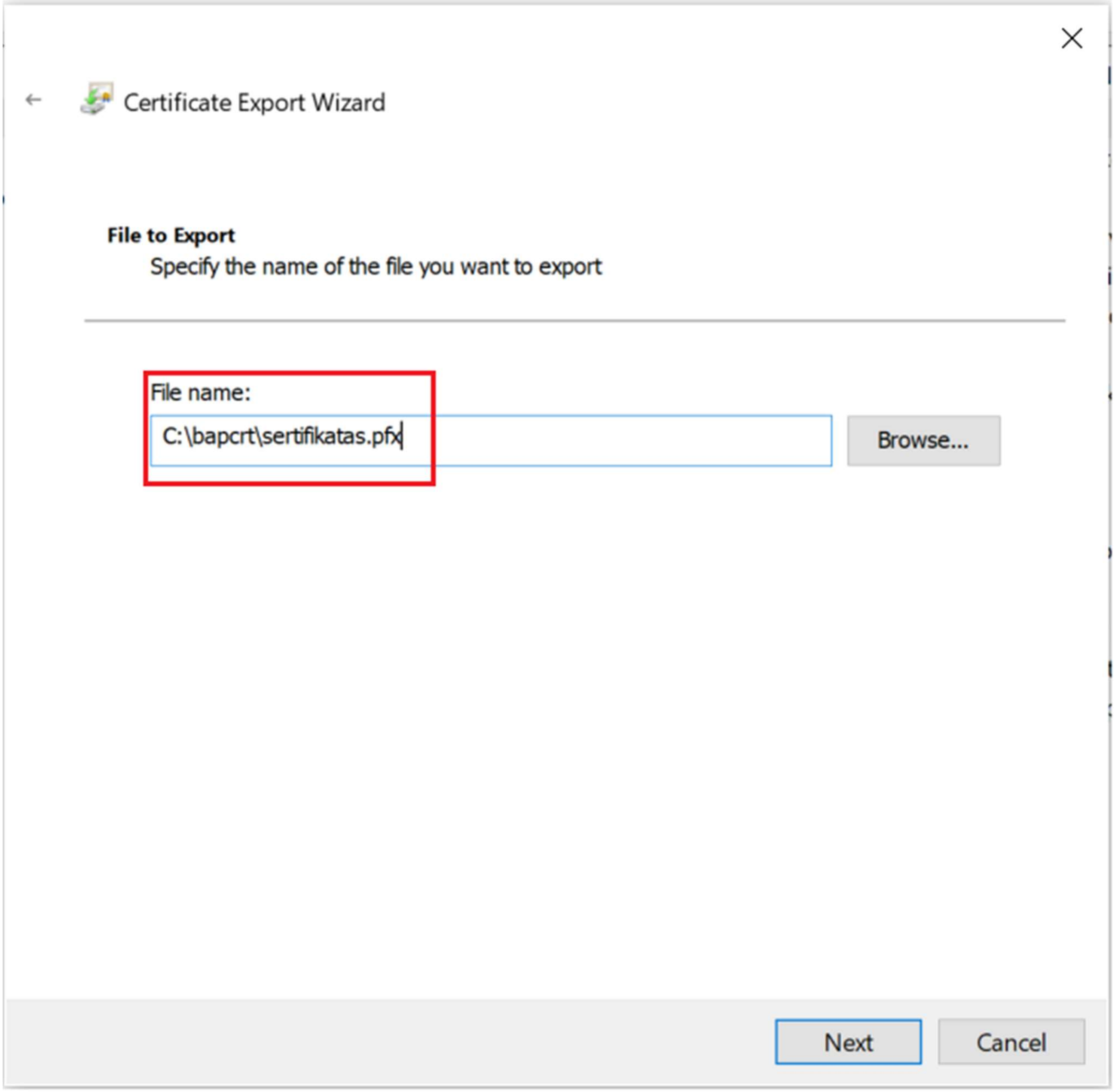
••••••••

Confirm password:

••••••••

Clicking *Next* will take you to a window where you will need to specify the export location and file name.

Figure 47 Certificate Export Wizard: Creating file name



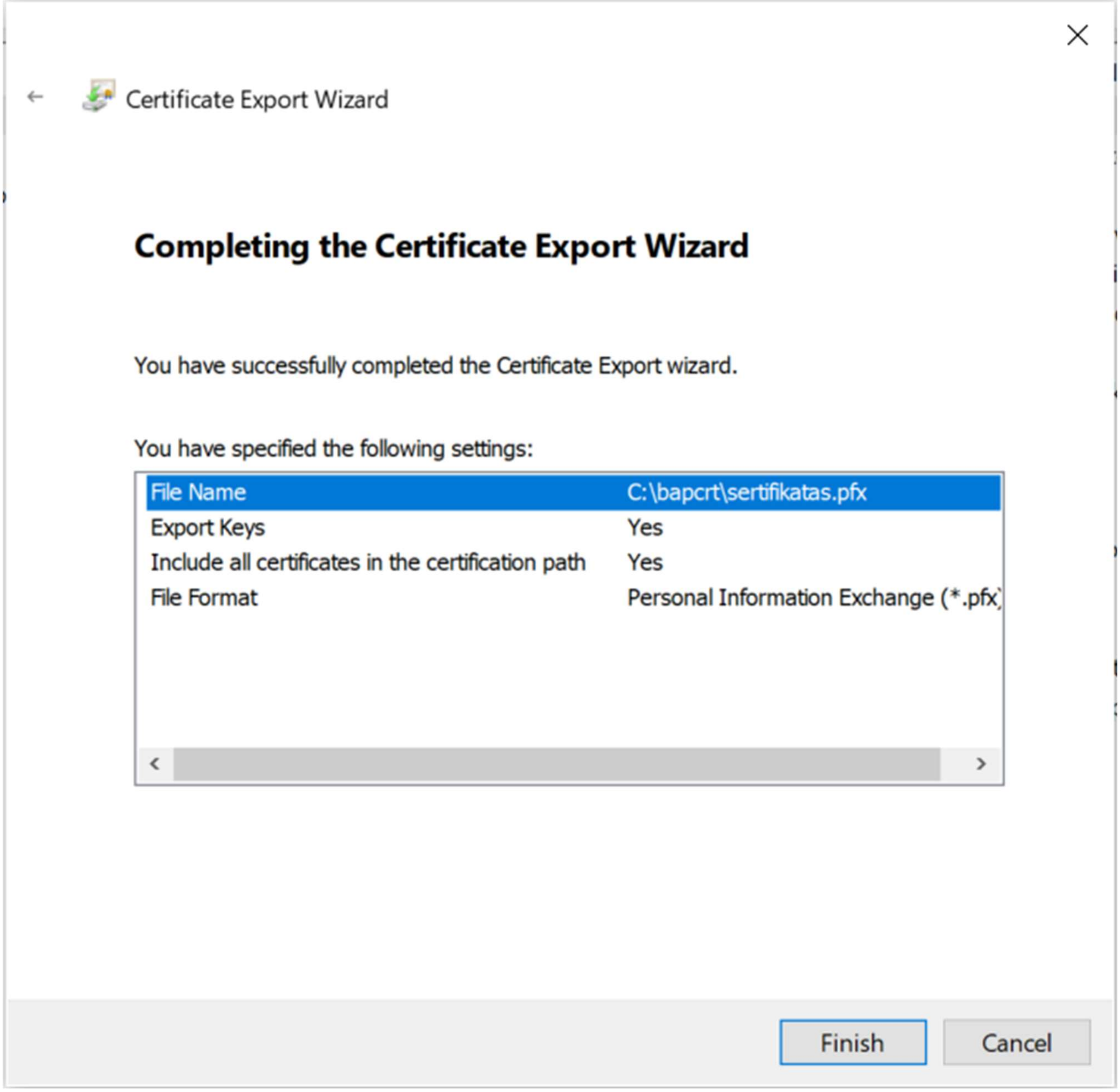
Certificate Export Wizard

File to Export
Specify the name of the file you want to export

File name: C:\bapcrt\sertifikatas.pfx

Clicking *Next* will open a window for reviewing the settings and completing the export operation. After viewing the information, click *Finish*.

Figure 48 Certificate Export Wizard: Settings review



Completing the Certificate Export Wizard

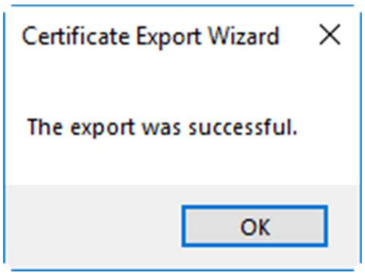
You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\bapcrt\sertifikatas.pfx
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Personal Information Exchange (*.pfx)

After completing this step, you will be notified of the successful completion of the export.

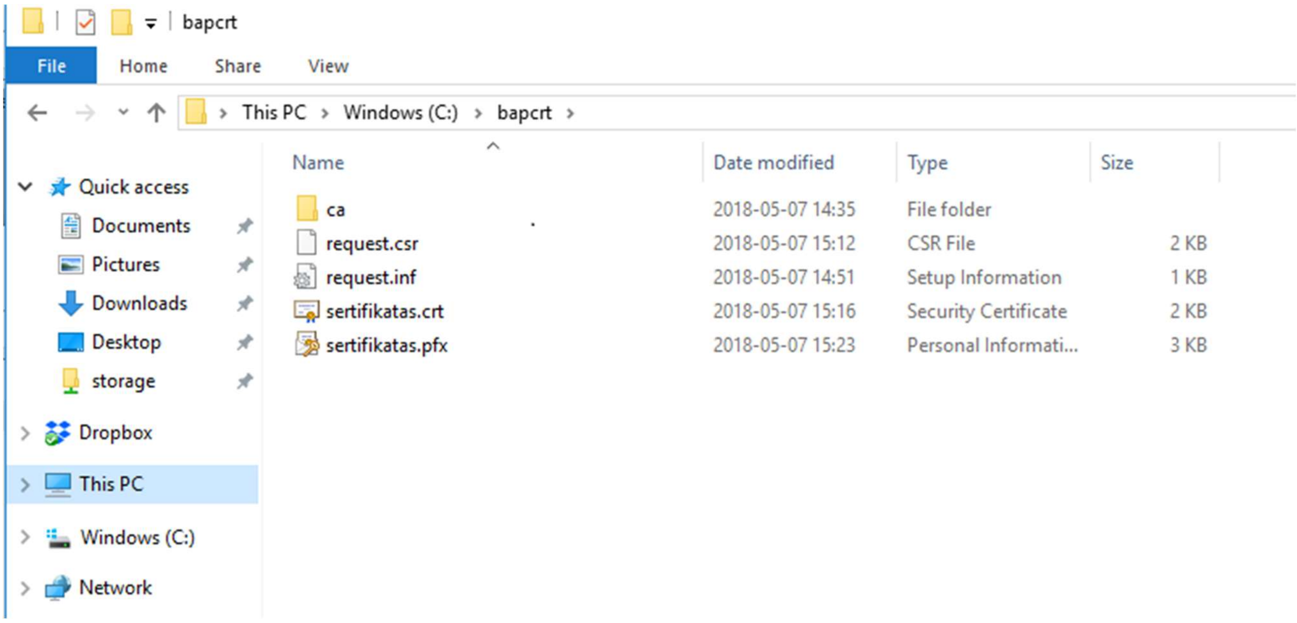
Figure 49 Certificate Export Wizard: Notification of the successful completion of a certificate export



The export was successful.

9. The resulting "*sertifikatas.pfx*" file contains your certificate and its private key. You can easily import it to another computer.

Figure 50 Display of the exported sertifikatas.pfx file



Name	Date modified	Type	Size
ca	2018-05-07 14:35	File folder	
request.csr	2018-05-07 15:12	CSR File	2 KB
request.inf	2018-05-07 14:51	Setup Information	1 KB
sertifikatas.crt	2018-05-07 15:16	Security Certificate	2 KB
sertifikatas.pfx	2018-05-07 15:23	Personal Informati...	3 KB

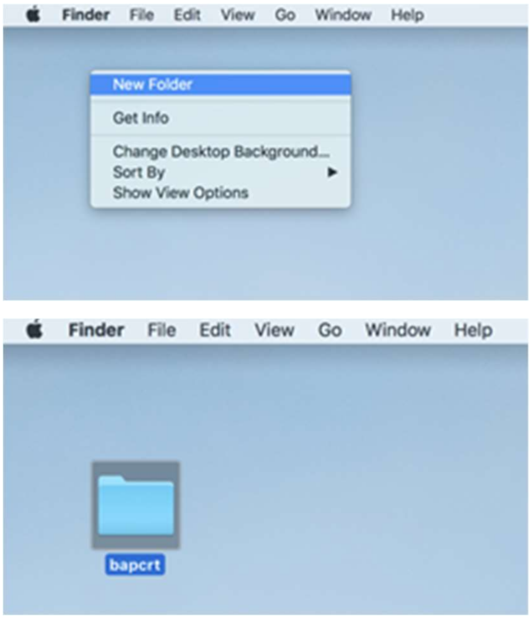
3 CERTIFICATE MANAGEMENT IN MACOS ENVIRONMENT

3.1 Creating a certificate signing request

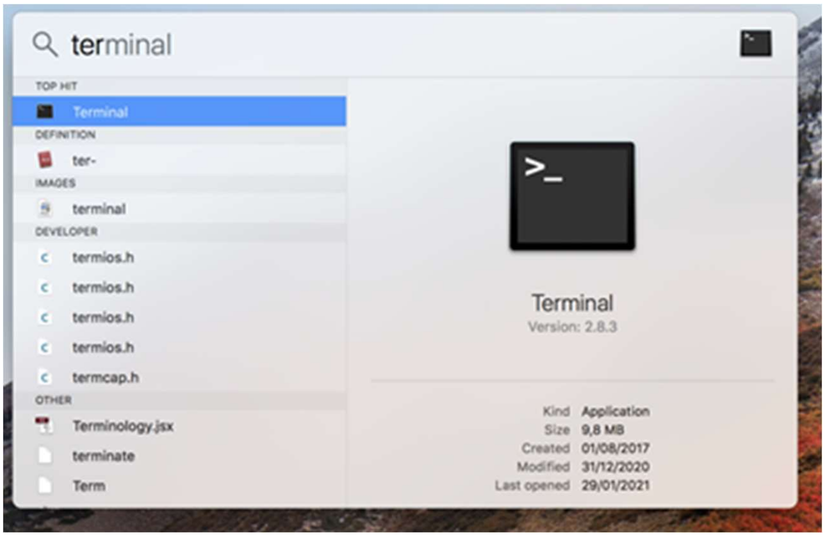
If you are using *macOS* , you can generate a certificate request using the "*openssl*" command via a terminal.

1. For your convenience, we recommend that you create a new folder (such as *"bapcrt"*) on your desktop.

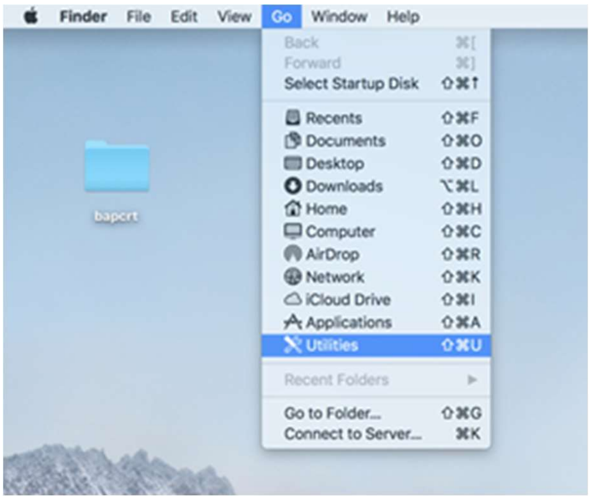
Figure 51 Folder creation

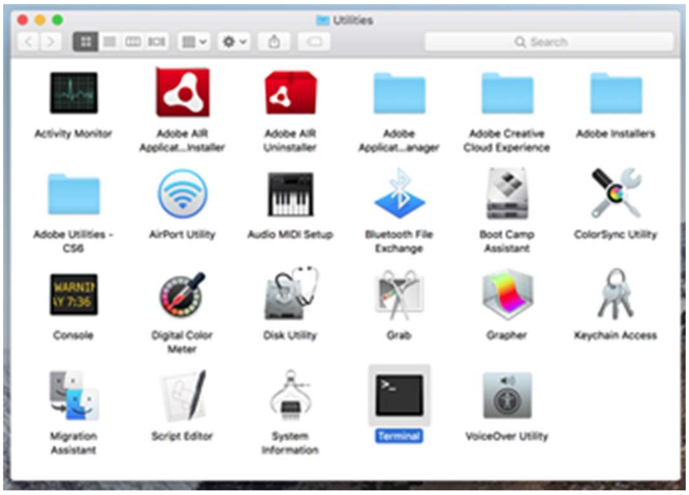


2. Launch the Terminal application. You can use the search by clicking Command-Space bar and typing "terminal" in the search field:



or by selecting *Go* → *Utilities* in the Finder menu





3. In the terminal go to the created folder *"bapcrt"* by entering the command (press the *Enter* key to execute the command)

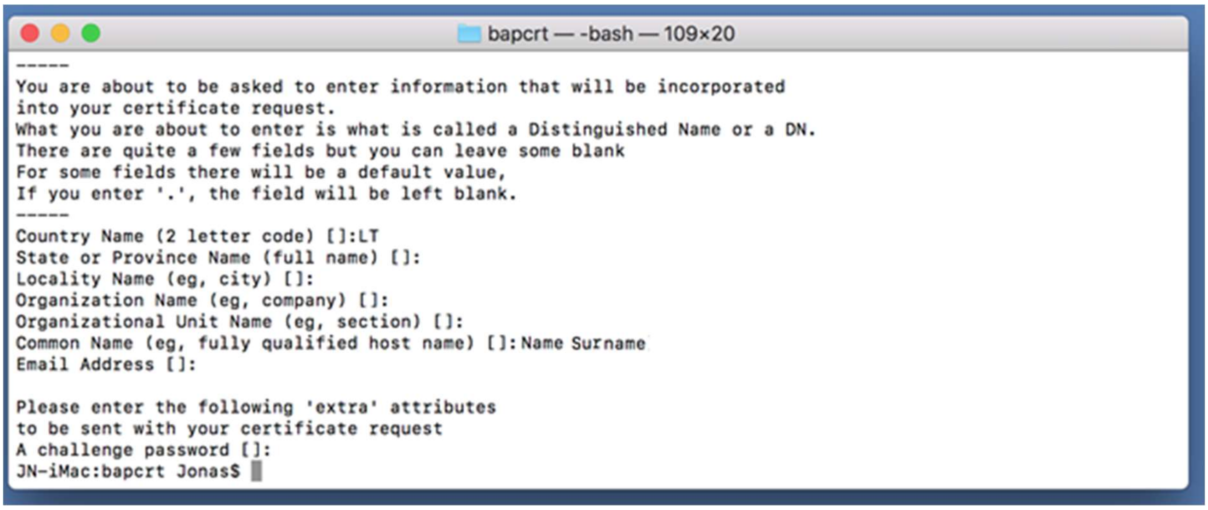
```
cd Desktop/bapcrt
```

4. Generate a certificate request using the "openssl" command:

```
openssl req -out request.csr -utf8 -new -newkey rsa:2048 -nodes -keyout certificate.key \
    -subj "/GN=Vardas/SN=Pavarde/CN=Vardas Pavarde" \
    -reqexts SAN \
    -config <(cat /etc/ssl/openssl.cnf \
          <(printf "\n[SAN]\nsubjectAltName=email:el.pastas@pastas.lt"))
```

Country Name (2 letter code) [AU]:**LT**
State or Province Name (full name) [Some-State]:**n/a**
Locality Name (eg, city) []:**n/a**
Organization Name (eg, company) [Internet Widgits Pty Ltd]:**n/a**
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:**Name Surname**

Figure 52 Certificate request generation



```
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:LT
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, fully qualified host name) []:Name Surname
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
JN-iMac:bapcrt Jonas$
```

5. Check available files:

```
JN-iMac:bapcrt Jonas$ ls -l
total 16
-rw-r--r--  1 Jonas  staff  1704 Sau 29 21:29 certificate.key
-rw-r--r--  1 Jonas  staff   915 Sau 29 21:29 request.csr
```

3.2 Certificate download and installation

1. If you have not used the BAP system until now and cannot log in via the Electronic Government Gateway, send the prepared *"request.csr"* file by e-mail to customs when requested. You will receive a response with *"certificate.crt"*, which we save in the *"bapcrt"* folder.

If you can log in to the BAP using the authentication service provided by the Electronic Government Gateway or you have used the BAP system before and can log in to it, attach the file *"request.csr"* in the *Profile* section by clicking the *Generate new certificate* button. Download the *"certificate.crt"* file by clicking the *Download* button in the modal window or in the certificate data table. Move the downloaded file to the *"bapcrt"* folder.

Figure 53 CSR file upload location

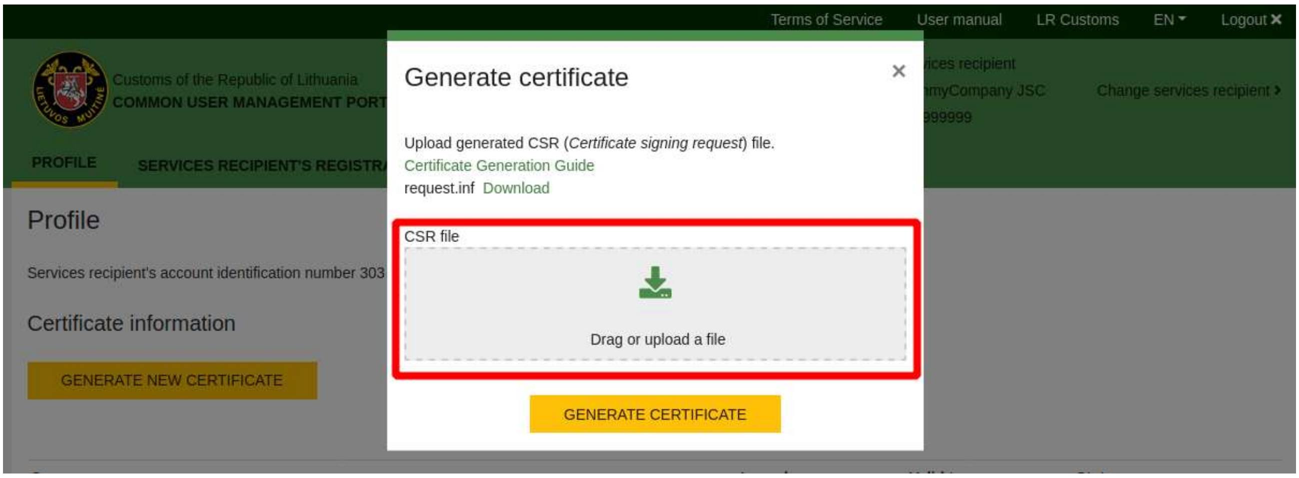
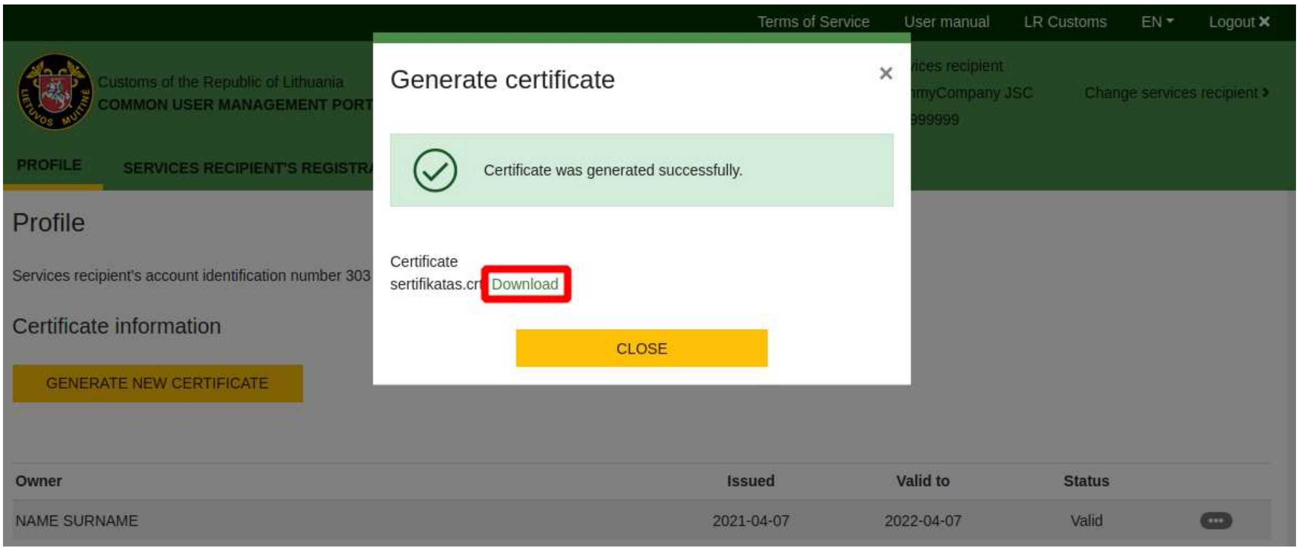

Terms of Service
User manual
LR Customs
EN
Logout
Customs of the Republic of Lithuania
COMMON USER MANAGEMENT PORT
PROFILE
SERVICES RECIPIENT'S REGISTR
ices recipient
myCompany JSC
999999
Change services recipient
Profile
Services recipient's account identification number 303
Certificate information
GENERATE NEW CERTIFICATE
Generate certificate
×
Upload generated CSR (Certificate signing request) file.
Certificate Generation Guide
request.inf Download
CSR file
Drag or upload a file
GENERATE CERTIFICATE

Figure 54 CRT file download



Terms of Service
User manual
LR Customs
EN
Logout
Customs of the Republic of Lithuania
COMMON USER MANAGEMENT PORT
PROFILE
SERVICES RECIPIENT'S REGISTR
ices recipient
myCompany JSC
999999
Change services recipient ›

Generate certificate

Certificate was generated successfully.

Certificate
sertifikatas.crt Download

CLOSE

Profile

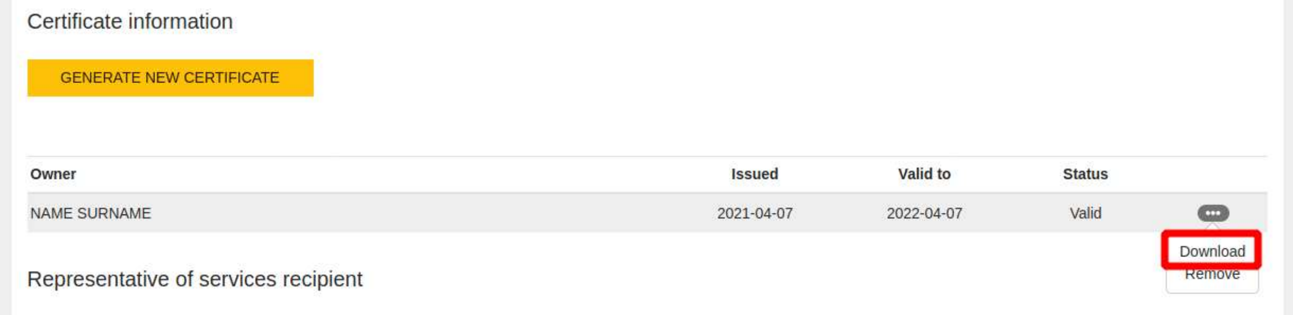
Services recipient's account identification number 303

Certificate information

GENERATE NEW CERTIFICATE

Owner	Issued	Valid to	Status
NAME SURNAME	2021-04-07	2022-04-07	Valid

Figure 55 Download of a CRT certificate from a certificate data table



Certificate information

GENERATE NEW CERTIFICATE

Owner	Issued	Valid to	Status
NAME SURNAME	2021-04-07	2022-04-07	Valid

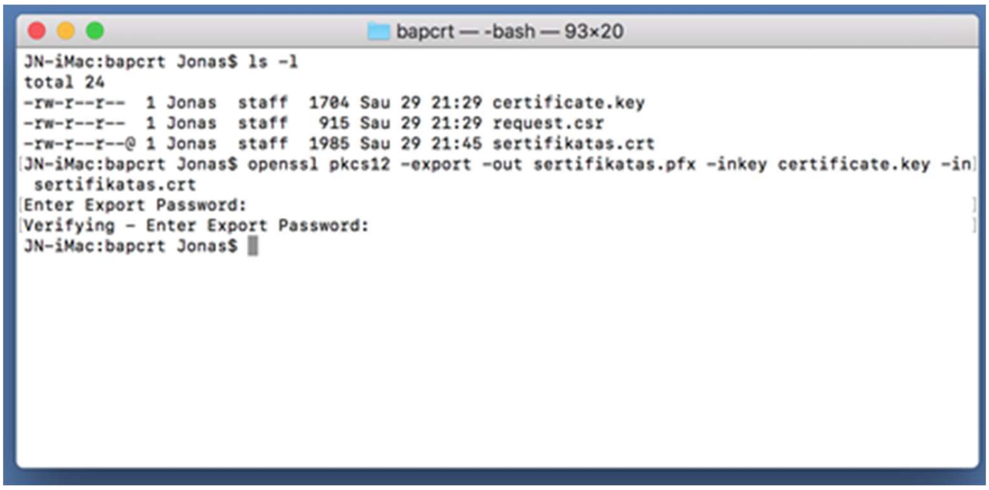
Representative of services recipient

```
JN-iMac:bapcrt Jonas$ ls -l
total 12
-rw-r--r--  1 Jonas  staff  1704 Sau 29 21:29 certificate.key
-rw-r--r--  1 Jonas  staff   915 Sau 29 21:29 request.csr
-rw-r---r--  1 Jonas  staff   915 Sau 29 21:29 sertifikatas.crt
```

2. Generate a PFX file from the certificate and key files. Create a password that will protect the private key.

```
openssl pkcs12 -export -out sertifikatas.pfx -inkey certificate.key -in
sertifikatas.crt
```

Figure 56 Example of export



```
JN-iMac:bapcrt Jonas$ ls -l
total 24
-rw-r--r--  1 Jonas  staff  1704 Sau 29 21:29 certificate.key
-rw-r--r--  1 Jonas  staff   915 Sau 29 21:29 request.csr
-rw-r--r--@ 1 Jonas  staff  1985 Sau 29 21:45 sertifikatas.crt
JN-iMac:bapcrt Jonas$ openssl pkcs12 -export -out sertifikatas.pfx -inkey certificate.key -in
 sertifikatas.crt
Enter Export Password:
Verifying - Enter Export Password:
JN-iMac:bapcrt Jonas$ 
```

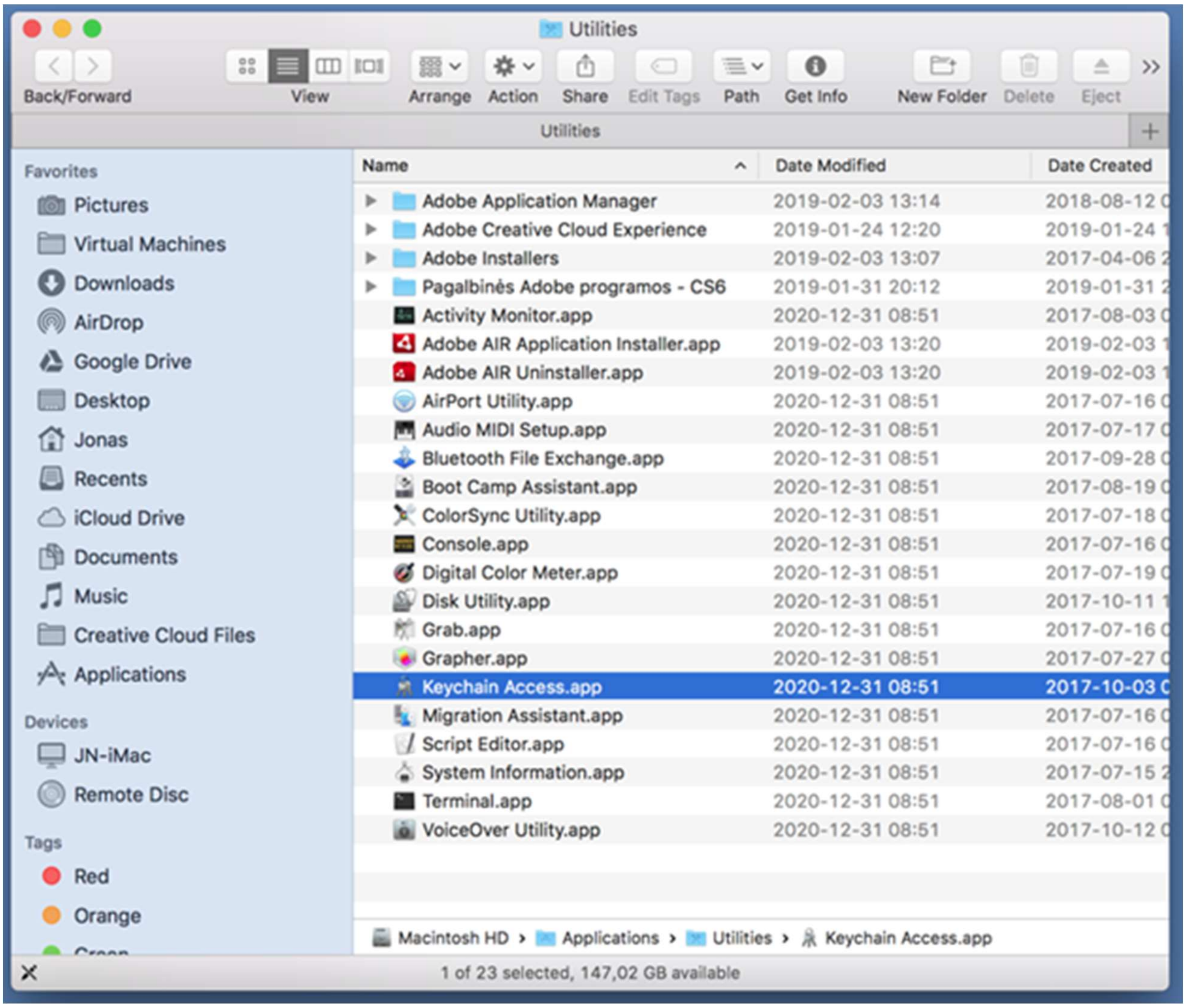
Check what files you have:

```
JN-iMac:bapcrt Jonas$ ls -l
total 12
-rw-r--r--  1 Jonas  staff  1704 Sau 29 21:29 certificate.key
-rw-r--r--  1 Jonas  staff   915 Sau 29 21:29 request.csr
-rw-r--r--  1 Jonas  staff   915 Sau 29 21:29 sertifikatas.crt
-rw-r--r--  1 Jonas  staff   915 Sau 29 21:29 sertifikatas.pfx
```

sertifikatas.pfx - file what will have your public and private key inside.

3. Certificate import in *macOS* .

Figure 57 To import a certificate from the Finder, select Go -> Utilities and start the Keychain Access application

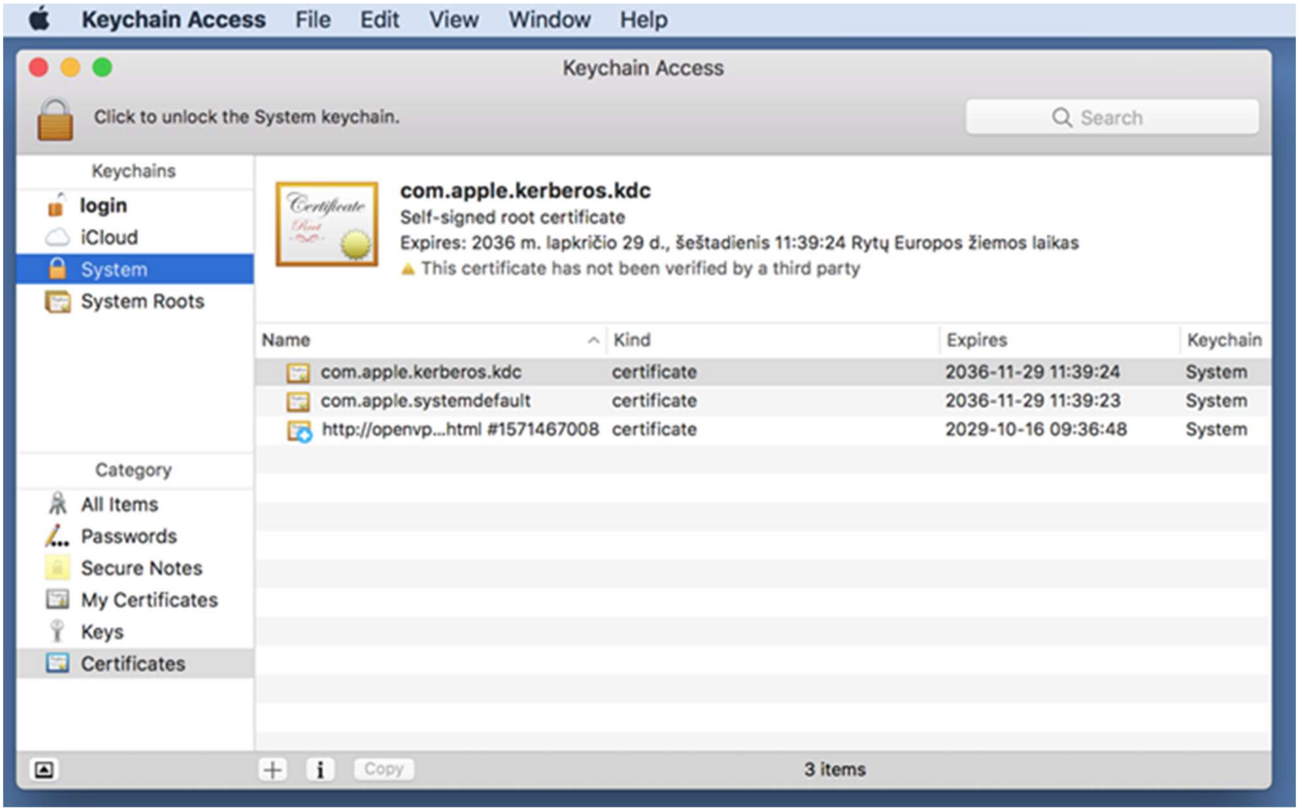


Name	Date Modified	Date Created
Adobe Application Manager	2019-02-03 13:14	2018-08-12 0
Adobe Creative Cloud Experience	2019-01-24 12:20	2019-01-24 1
Adobe Installers	2019-02-03 13:07	2017-04-06 2
Pagalbinės Adobe programos - CS6	2019-01-31 20:12	2019-01-31 2
Activity Monitor.app	2020-12-31 08:51	2017-08-03 0
Adobe AIR Application Installer.app	2019-02-03 13:20	2019-02-03 1
Adobe AIR Uninstaller.app	2019-02-03 13:20	2019-02-03 1
AirPort Utility.app	2020-12-31 08:51	2017-07-16 0
Audio MIDI Setup.app	2020-12-31 08:51	2017-07-17 0
Bluetooth File Exchange.app	2020-12-31 08:51	2017-09-28 0
Boot Camp Assistant.app	2020-12-31 08:51	2017-08-19 0
ColorSync Utility.app	2020-12-31 08:51	2017-07-18 0
Console.app	2020-12-31 08:51	2017-07-16 0
Digital Color Meter.app	2020-12-31 08:51	2017-07-19 0
Disk Utility.app	2020-12-31 08:51	2017-10-11 1
Grab.app	2020-12-31 08:51	2017-07-16 0
Grapher.app	2020-12-31 08:51	2017-07-27 0
Keychain Access.app	2020-12-31 08:51	2017-10-03 0
Migration Assistant.app	2020-12-31 08:51	2017-07-16 0
Script Editor.app	2020-12-31 08:51	2017-07-16 0
System Information.app	2020-12-31 08:51	2017-07-15 2
Terminal.app	2020-12-31 08:51	2017-08-01 0
VoiceOver Utility.app	2020-12-31 08:51	2017-10-12 0

Macintosh HD › Applications › Utilities › Keychain Access.app

1 of 23 selected, 147,02 GB available

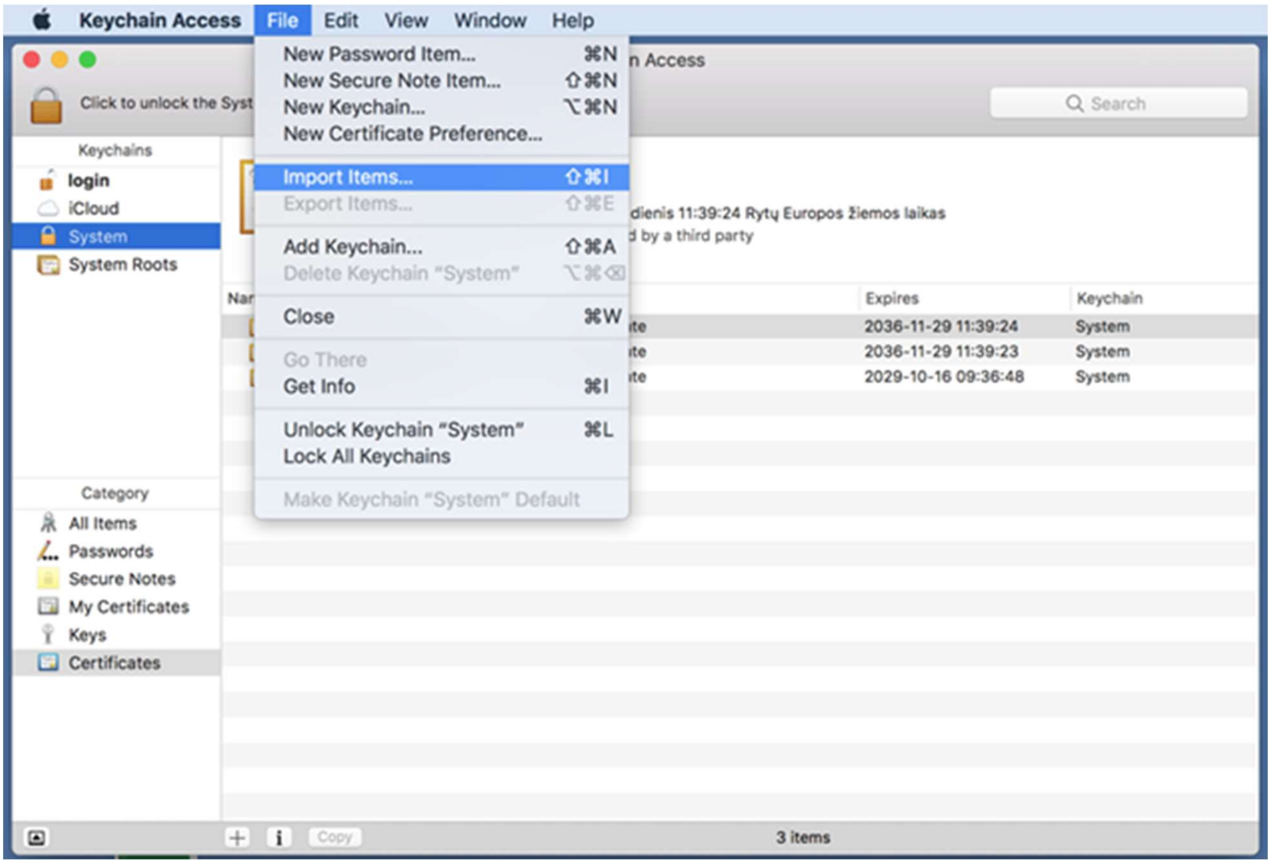
Figure 58 On the left side of the Keychain Access application, select System



com.apple.kerberos.kdc
Self-signed root certificate
Expires: 2036 m. lapkričio 29 d., šeštadienis 11:39:24 Rytų Europos žiemos laikas
⚠ This certificate has not been verified by a third party

Name	Kind	Expires	Keychain
com.apple.kerberos.kdc	certificate	2036-11-29 11:39:24	System
com.apple.systemdefault	certificate	2036-11-29 11:39:23	System
http://openvp...html #1571467008	certificate	2029-10-16 09:36:48	System

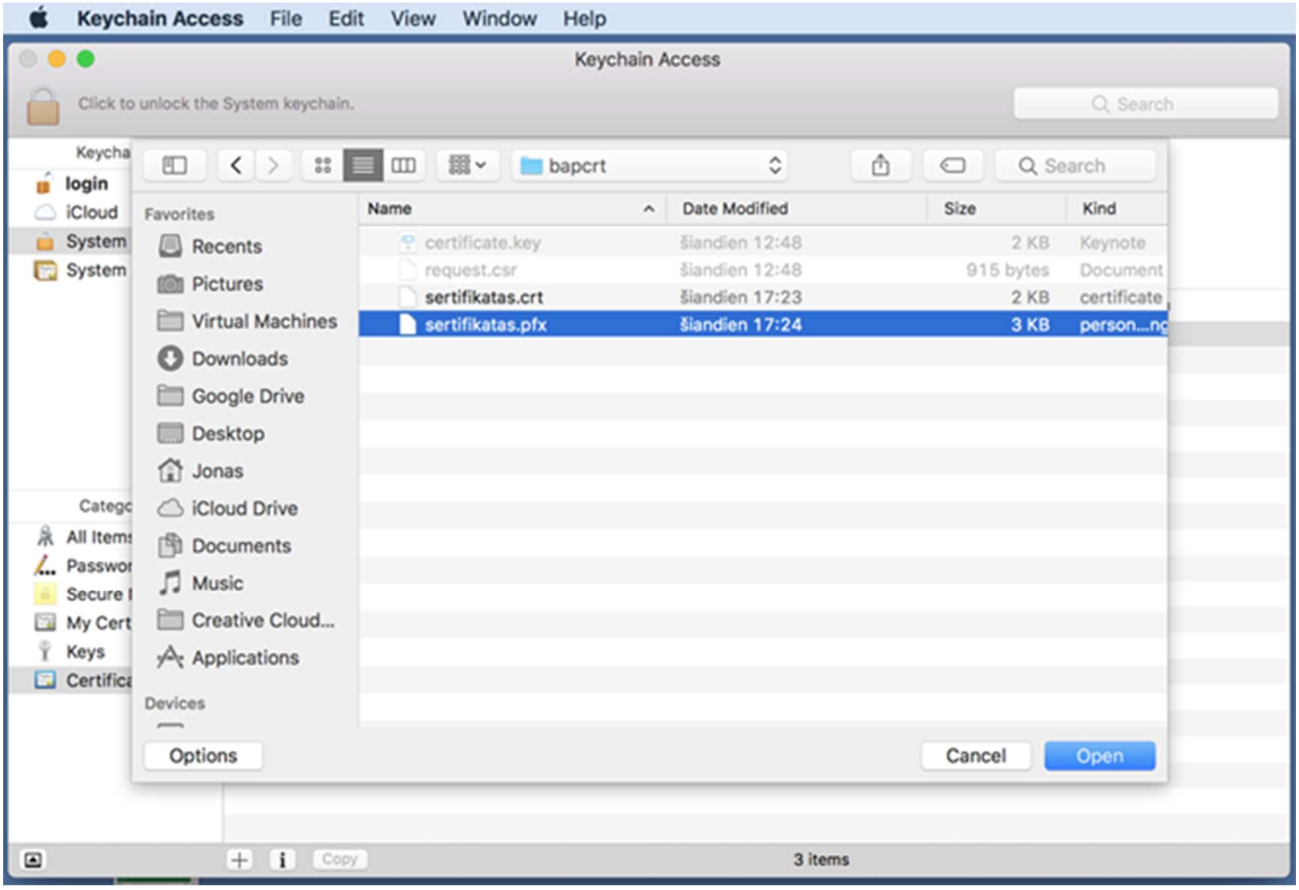
Figure 59 From the File menu, select Import Items…



dienis 11:39:24 Rytų Europos žiemos laikas
d by a third party

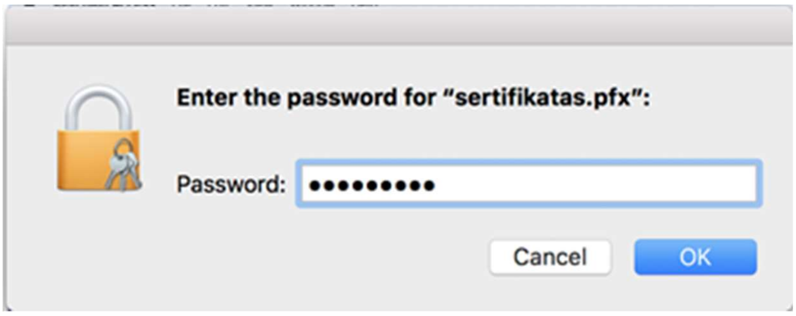
Nar		Expires	Keychain
	te	2036-11-29 11:39:24	System
	te	2036-11-29 11:39:23	System
	te	2029-10-16 09:36:48	System

Figure 60 Select the generated certificate



Name	Date Modified	Size	Kind
certificate.key	šiandien 12:48	2 KB	Keynote
request.csr	šiandien 12:48	915 bytes	Document
sertifikatas.crt	šiandien 17:23	2 KB	certificate
sertifikatas.pfx	šiandien 17:24	3 KB	person...nq

After selecting the certificate, the system will ask you to enter the administrator password, followed by the password of the generated certificate that was created in step 2.



Enter the password for "sertifikatas.pfx":

Password: •••••••••

When the certificate is imported after starting the new *Safari* browser, it will be possible to log in to bap.lrmuitine.lt after selecting the certificate. When connecting for the first time, the MacOS system will ask for the administrator name and password again. Entering them will connect to the system.

3.3 Preparing the certificate to work on another computer

To work on another computer, you need the *pfx* file that was generated in step 2 of the *Download and install the certificate.* Transfer this file to a new computer and continue with the steps in the installation instructions below.

4 CERTIFICATE MANAGEMENT IN LINUX ENVIRONMENT

4.1 Creating a certificate signing request

If you are using *Linux*, you can generate a certificate request using the "*openssl*" command via a terminal.

1. First, prepare a location on your computer where you will later save the certificate request created in the next steps of the manual, for which we recommend creating the *"bapcrt"* folder. Navigate to this folder and generate a certificate request using the "openssl" command:

```
linux@PC$ openssl req -out request.csr -utf8 -new -newkey rsa:2048 -nodes -keyout certificate.key \
  -subj "/GN=Name/SN=Surname/CN=Name Surname" \
  -reqexts SAN \
  -config <(cat /etc/ssl/openssl.cnf \
        <(printf "\n[SAN]\nsubjectAltName=email:email@example.com"))
```

"Country Name" = LT

Country Name (2 letter code) [AU]:**LT**
State or Province Name (full name) [Some-State]:**n/a**
Locality Name (eg, city) []:**n/a**
Organization Name (eg, company) [Internet Widgits Pty Ltd]:**n/a**
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:**Name Surname**

Example:

```
linux@PC$ openssl req -out request.csr -new -newkey rsa:2048 -nodes -keyout
certificate.key
Generating a 2048 bit RSA private key
...........................+++
..........................................+++
writing new private key to 'certificate.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:LT
State or Province Name (full name) [Some-State]:n/a
Locality Name (eg, city) []:n/a
Organization Name (eg, company) [Internet Widgits Pty Ltd]:n/a
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:Name Surname
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

2. Check what files you have:

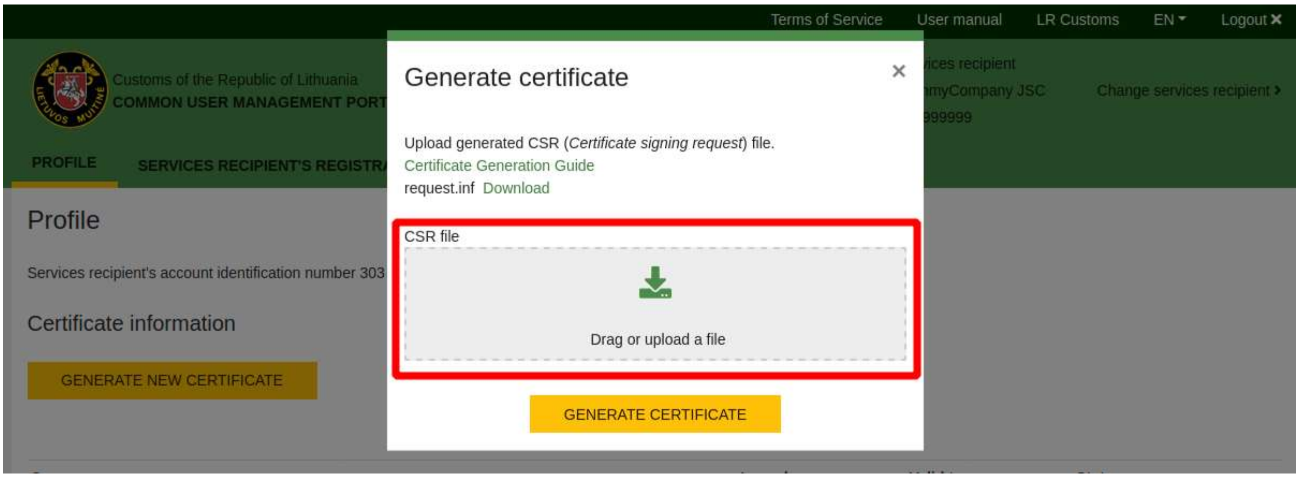
```
linux@PC$ ls -l
total 8
-rwxrwxrwx 1 root root 1704 May  7 15:37 certificate.key
-rwxrwxrwx 1 root root  980 May  7 15:37 request.csr
```

4.2 Sertifikato atsisiuntimas ir diegimas Certificate download and installation

1. If you have not used the BAP system until now and cannot log in via the Electronic Government Gateway, send the prepared *"request.csr"* file by e-mail to customs when requested. You will receive a response with *"certificate.crt"*, which we save in the *"bapcrt"* folder.

If you can log in to the BAP using the authentication service provided by the Electronic Government Gateway or you have used the BAP system before and can log in to it, attach the file *"request.csr"* in the *Profile* section by clicking the *Generate new certificate* button. Download the *"certificate.crt"* file by clicking the *Download* button in the modal window or in the certificate data table. Save the downloaded file to the *"bapcrt"* folder.

Figure 61 CSR file upload location

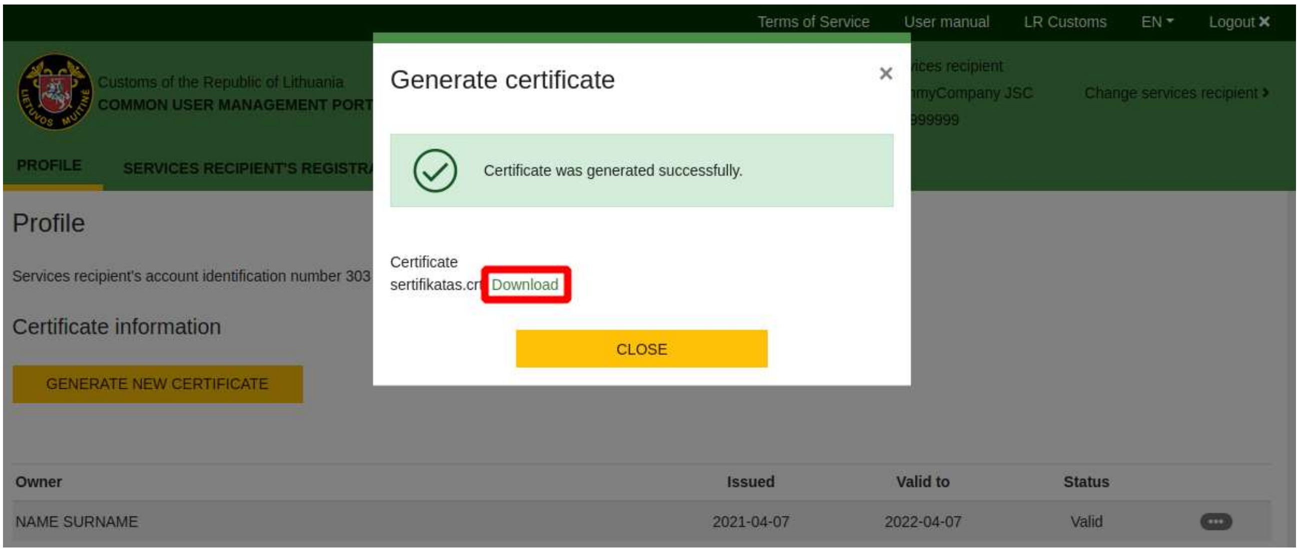


Services recipient's account identification number 303

Generate certificate

Upload generated CSR (*Certificate signing request*) file.
Certificate Generation Guide
request.inf Download

Figure 62 CRT file download



Terms of Service
User manual
LR Customs
EN
Logout
Customs of the Republic of Lithuania
COMMON USER MANAGEMENT PORT
PROFILE
SERVICES RECIPIENT'S REGISTR
Profile
Certificate information
GENERATE NEW CERTIFICATE
Change services recipient
CLOSE

Services recipient's account identification number 303

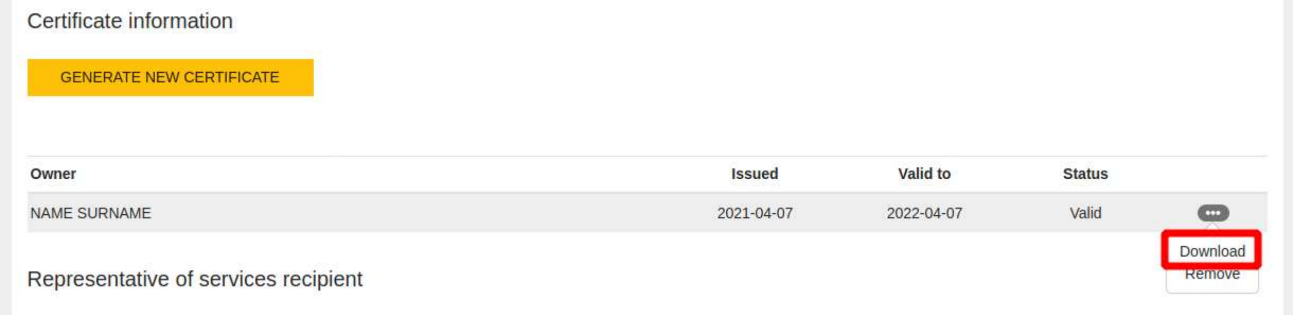
Generate certificate

Certificate was generated successfully.

Certificate
sertifikatas.crt Download

Owner	Issued	Valid to	Status
NAME SURNAME	2021-04-07	2022-04-07	Valid

Figure 63 Download of a CRT certificate from a certificate data table



Certificate information

Owner	Issued	Valid to	Status
NAME SURNAME	2021-04-07	2022-04-07	Valid

Representative of services recipient

```
linux@PC$$ ls -l
total 12
-rwxrwxrwx 1 root root 1704 May  7 15:37 certificate.key
-rwxrwxrwx 1 root root  980 May  7 15:37 request.csr
-rwxrwxrwx 1 root root 1127 May  7 15:41 sertifikatas.crt
```

2. Generate a PFX file from the certificate and key files. Create a password that will protect the private key.

```
linux@PC$:/mnt/d/bapcrt/linux$ openssl pkcs12 -export -out sertifikatas.pfx -inkey
certificate.key -in sertifikatas.crt
Enter Export Password:
Verifying - Enter Export Password:
```

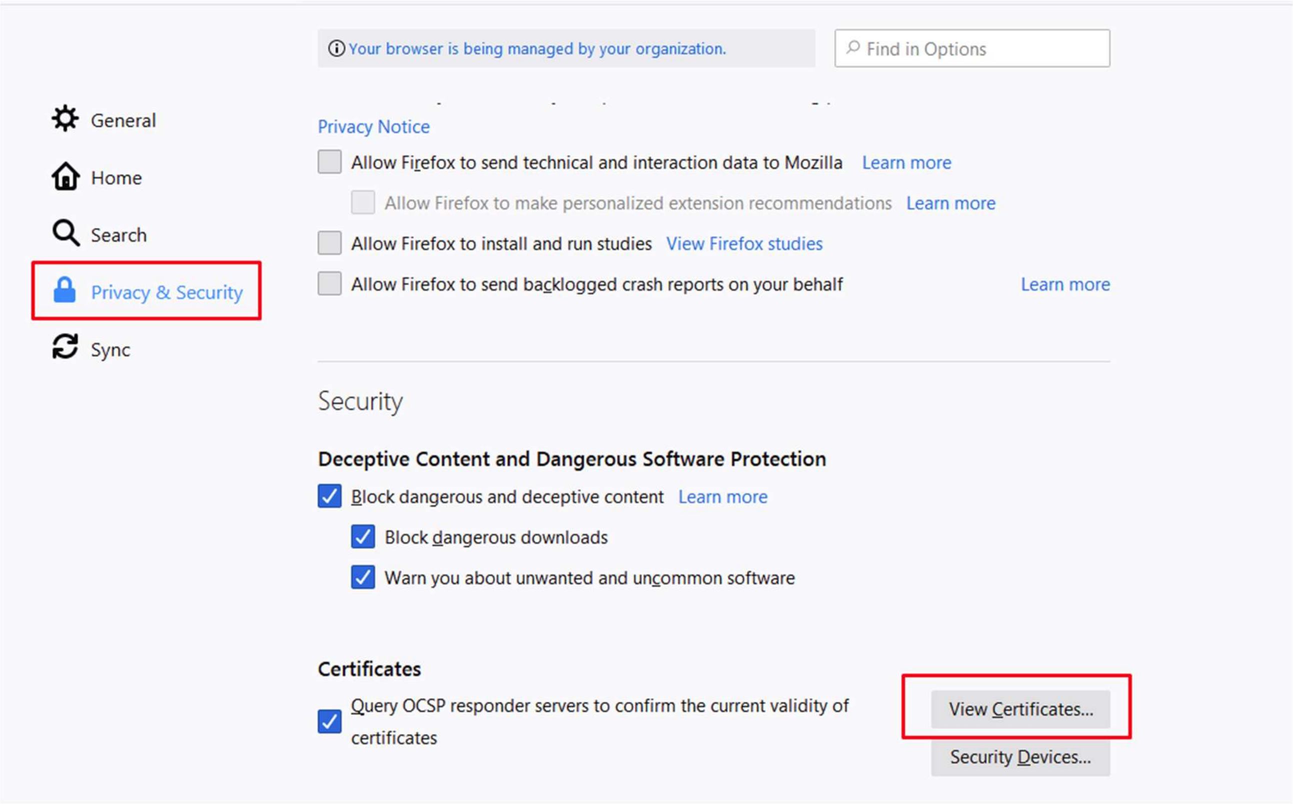
Check what files you have:

```
linux@PC$:/mnt/d/bapcrt/linux$ ls -l
total 16
-rwxrwxrwx 1 root root 1704 May  7 15:37 certificate.key
-rwxrwxrwx 1 root root  980 May  7 15:37 request.csr
-rwxrwxrwx 1 root root 1127 May  7 15:41 sertifikatas.crt
-rwxrwxrwx 1 root root 2389 May  7 15:43 sertifikatas.pfx
```

sertifikatas.pfx - file what will have your public and private key inside.

3. Importing a certificate for use on a *linux* system is configured in the browser. Open your browser settings, locate the *Privacy & Security* section, select *Certificates* option and click *View Certificates*

Figure 64 View Certificates section



Privacy Notice

□ Allow Firefox to send technical and interaction data to Mozilla Learn more

□ Allow Firefox to make personalized extension recommendations Learn more

□ Allow Firefox to install and run studies View Firefox studies

□ Allow Firefox to send backlogged crash reports on your behalf Learn more

Security

Deceptive Content and Dangerous Software Protection

☑ Block dangerous and deceptive content Learn more

☑ Block dangerous downloads

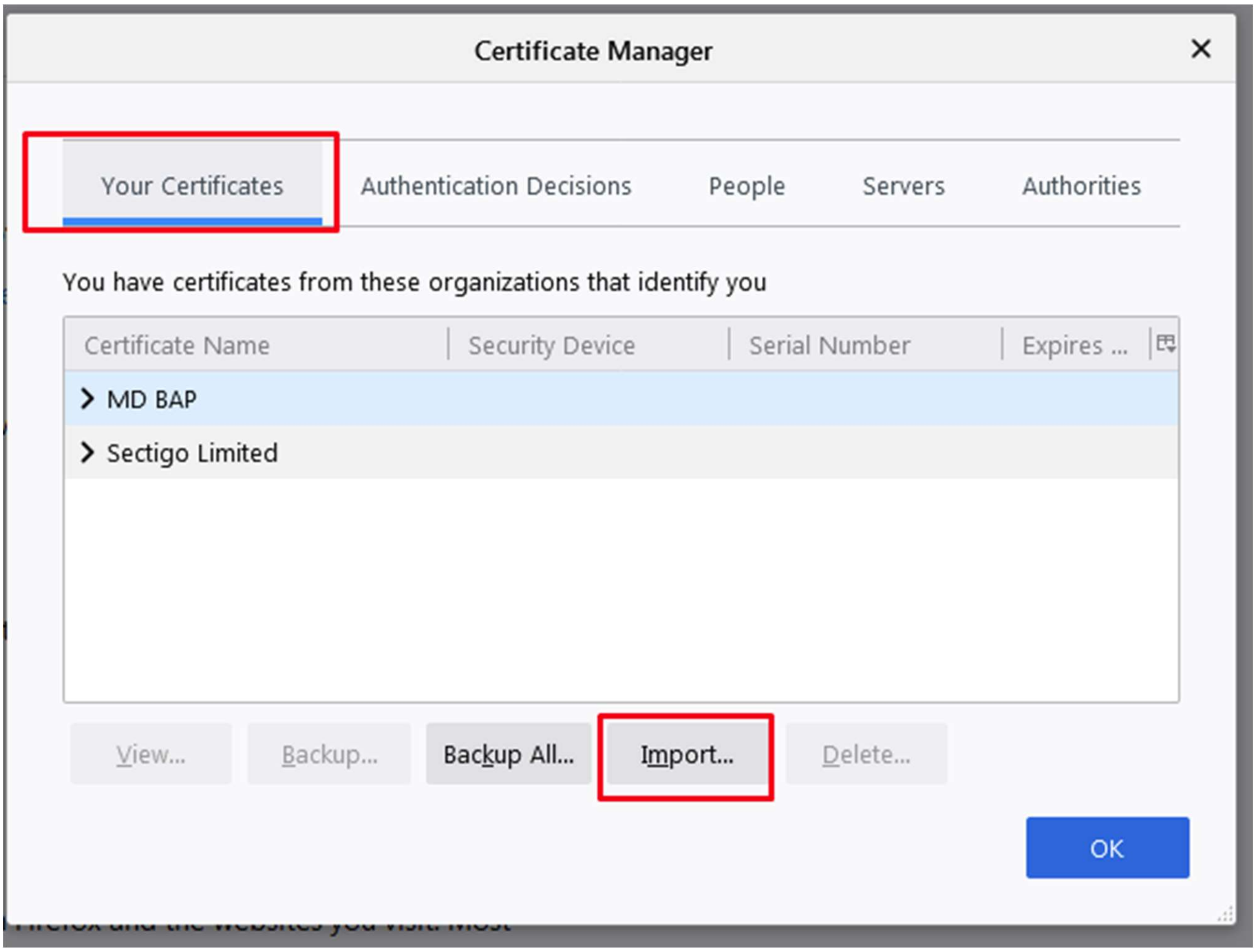
☑ Warn you about unwanted and uncommon software

Certificates

☑ Query OCSP responder servers to confirm the current validity of certificates

4. In an opened window in the *Your Certificates* section, click *Import*, specify your pfx file and the password you specified in step 3.

Figure 65 Certificate installation window



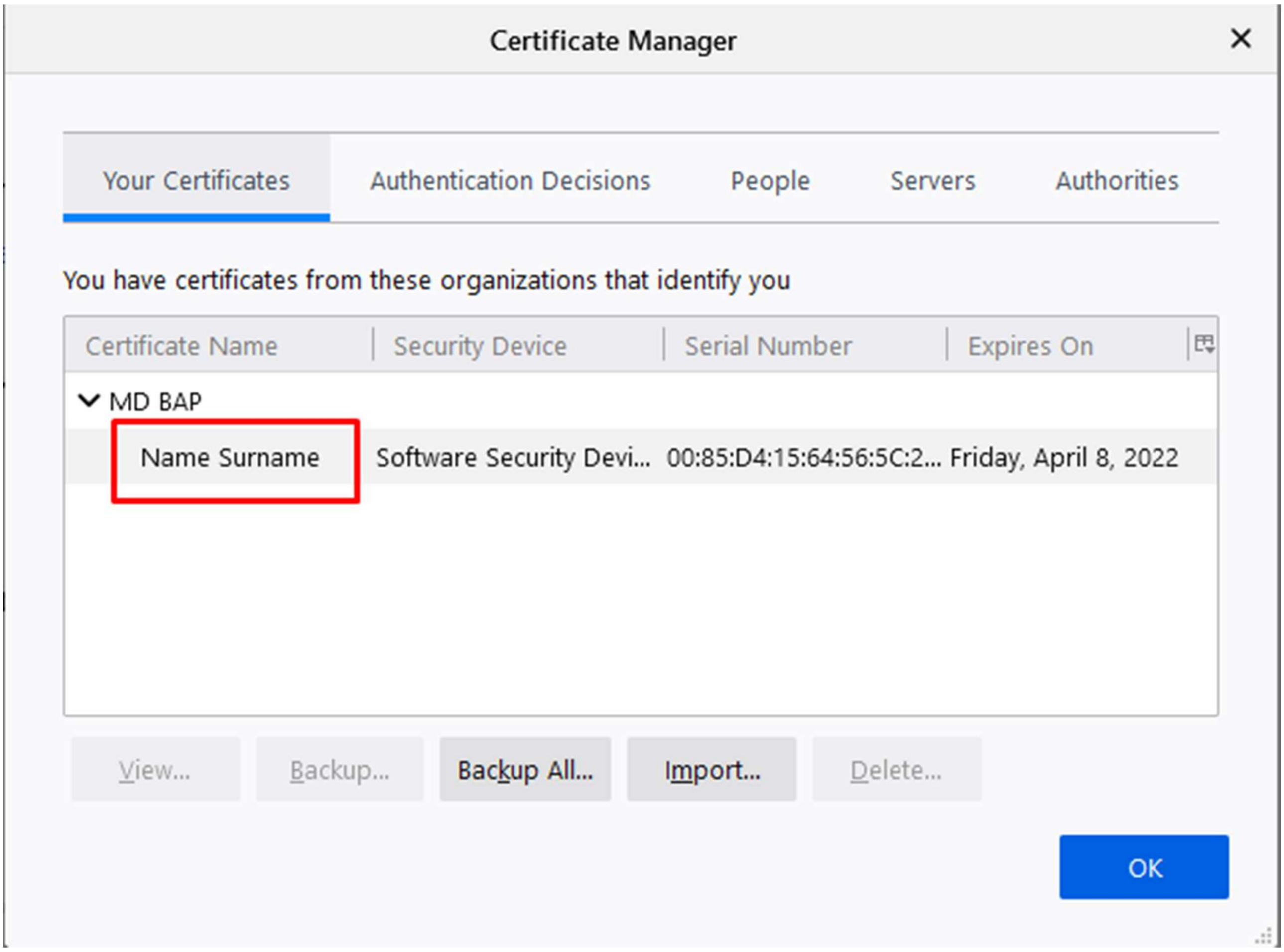
Certificate Manager

You have certificates from these organizations that identify you

Certificate Name	Security Device	Serial Number	Expires ...
> MD BAP			
> Sectigo Limited			

5. After the certificate is successfully uploaded, you will see it in the list.

Figure 66 List of certificates



You have certificates from these organizations that identify you

Certificate Name	Security Device	Serial Number	Expires On
MD BAP			
Name Surname	Software Security Devi...	00:85:D4:15:64:56:5C:2...	Friday, April 8, 2022

4.3 Preparing the certificate to work on another computer

To work on another computer, you need the *pfx* file that was generated in step 2 of the *Download and install the certificate* section. Transfer this file to a new computer and continue with the steps in the installation instructions below.