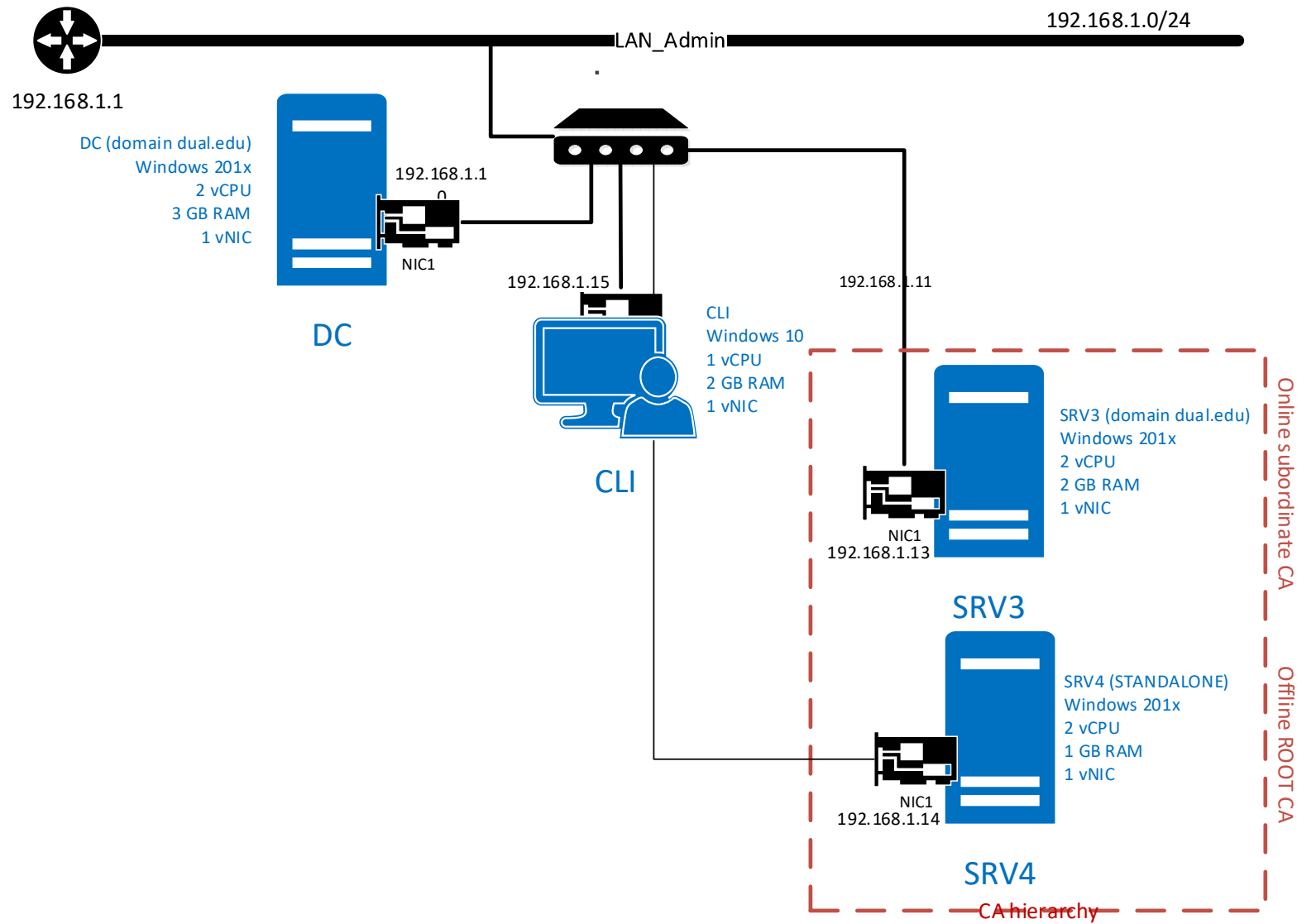


PKI inštalácia

Špecializované IKT systémy Windows

Ing. Stanislav Lukac, PhD.

LAB: CA installation



Postupnosť krokov

1. Inštalácia standalone root CA na SRV₄
2. Inštalácia enterprise subordinate CA na SRV₃
3. Deploy certificate templates
4. Enable certificate auto-enrollment
5. Set certificate revocation policies
6. Configure and verify private key archive and recovery

Root CA inštalácia

Špecializované IKT systémy Windows

Ing. Stanislav Lukac, PhD.

Krok 1

::Inštalácia role CA na SRV4

The screenshot shows the Windows Server Manager interface. The 'Local Server' tab is selected, displaying properties for 'srv4' in the 'WORKGROUP'. The 'Add Roles and Features Wizard' is open, showing the 'Select server roles' step. The 'Active Directory Certificate Services' role is selected. A list of required tools is displayed, including Remote Server Administration Tools, Role Administration Tools, and Active Directory Certificate Services Tools.

Server Manager
Server Manager ▸ Local Server

PROPERTIES
For srv4

Computer name: srv4
Workgroup: WORKGROUP
Last installed updates: Yesterday at
Windows Update: Download u

Add Roles and Features Wizard

Select server roles

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Confirmation
Results

Select one or more roles to install on the selected server.

Roles	Description
<input checked="" type="checkbox"/> Active Directory Certificate Services	Active Directory Certificate Services (AD CS) is used to create
<input type="checkbox"/> Active Directory Domain Services	
<input type="checkbox"/> Active Directory Federation Services	
<input type="checkbox"/> Active Directory Lightweight Directory Services	
<input type="checkbox"/> Active Directory Rights Management Services	
<input type="checkbox"/> Device Health	
<input type="checkbox"/> DHCP Server	
<input type="checkbox"/> DNS Server	
<input type="checkbox"/> Fax Server	
<input checked="" type="checkbox"/> File and Storage Services	
<input type="checkbox"/> Host Guardian Service	
<input type="checkbox"/> Hyper-V	

Add Roles and Features Wizard

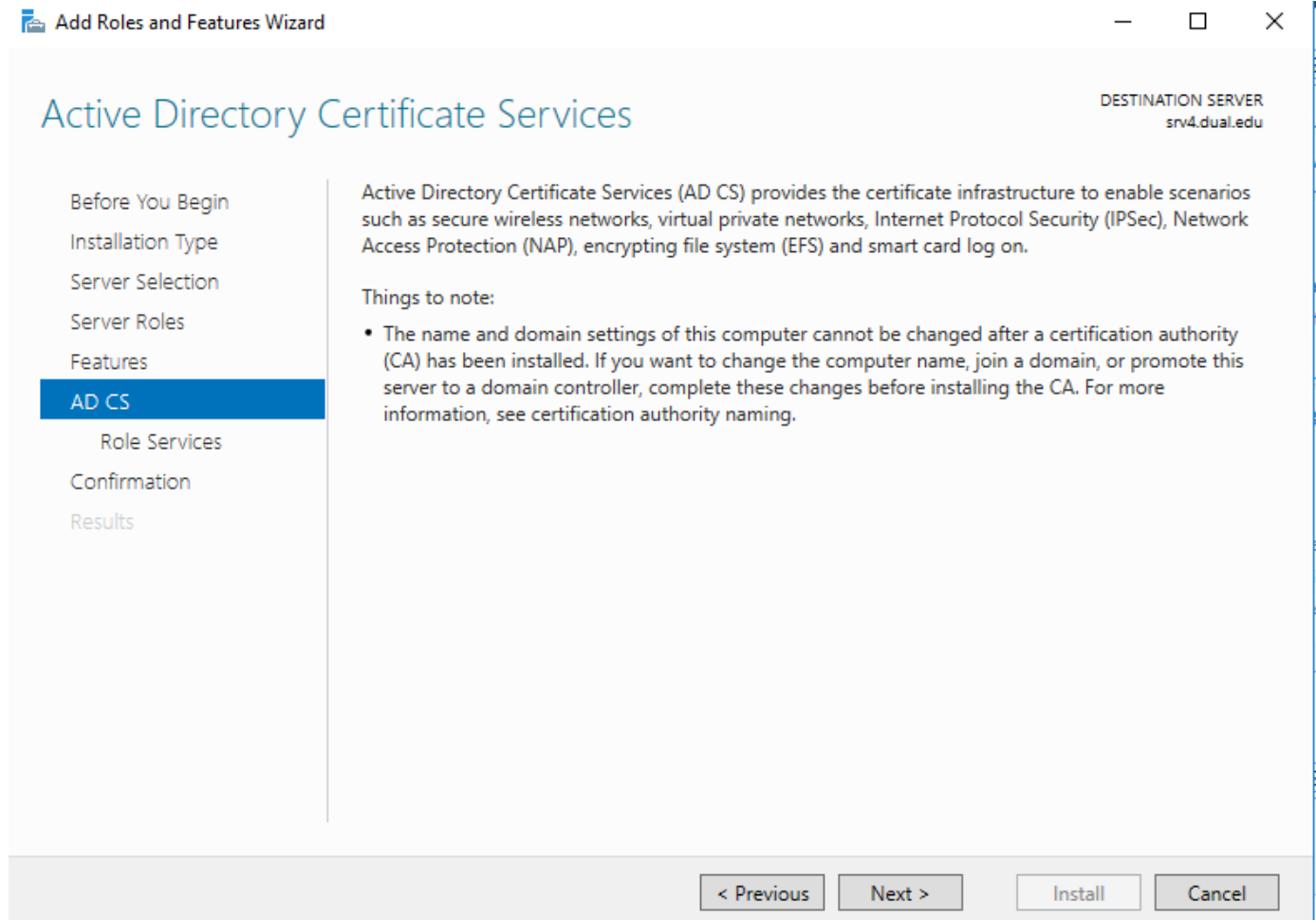
Add features that are required for Active Directory Certificate Services?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
 - Role Administration Tools
 - Active Directory Certificate Services Tools
 - [Tools] Certification Authority Management Tools

Krok 1

:: Inštalácia role CA na SRV4



Krok 1

:: Inštalácia ROOT CA na SRV4

Add Roles and Features Wizard

Select role services

DESTINATION SERVER
srv4.dual.edu

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Confirmation
Results

Select the role services to install for Active Directory Certificate Services

Role services

- ☒ **Certification Authority**
- ☐ Certificate Enrollment Policy Web Service
- ☐ Certificate Enrollment Web Service
- ☐ Certification Authority Web Enrollment
- ☐ Network Device Enrollment Service
- ☐ Online Responder

Description

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

< Previous Next > Install Cancel

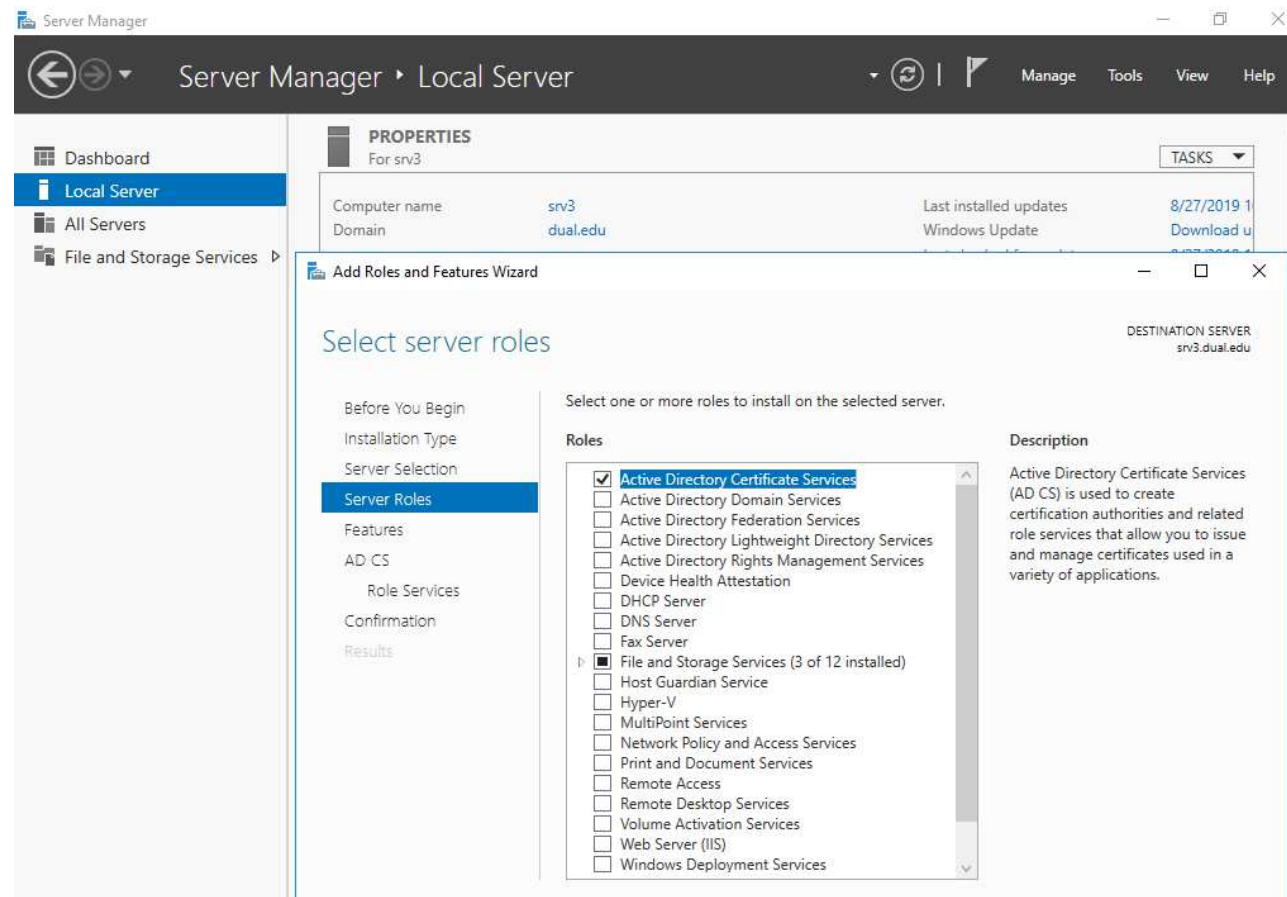
Subordinate CA inštalácia

Špecializované IKT systémy Windows

Ing. Stanislav Lukac, PhD.

Krok 2

::Inštalácia subordinate CA na SRV3



Krok 2

::Inštalácia subordinate CA na SRV3

Add Roles and Features Wizard

Select role services

DESTINATION SERVER
srv3.dual.edu

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Web Server Role (IIS)
 Role Services
Confirmation
Results

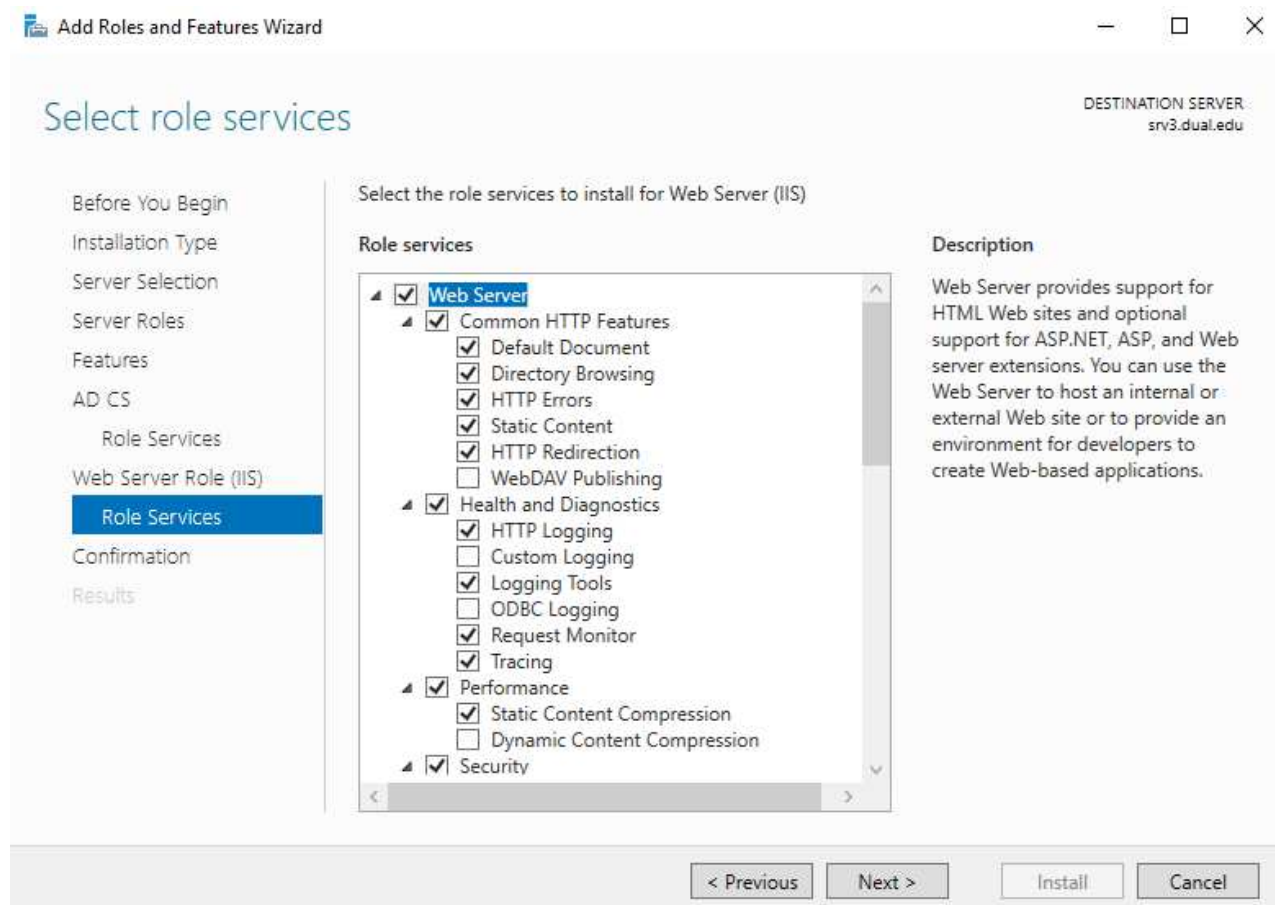
Select the role services to install for Active Directory Certificate Services

Role services	Description
<input checked="" type="checkbox"/> Certification Authority	Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.
<input type="checkbox"/> Certificate Enrollment Policy Web Service	
<input type="checkbox"/> Certificate Enrollment Web Service	
<input checked="" type="checkbox"/> Certification Authority Web Enrollment	
<input type="checkbox"/> Network Device Enrollment Service	
<input type="checkbox"/> Online Responder	

< Previous Next > Install Cancel

Krok 2

::Inštalácia subordinate CA na SRV3



Konfigurácia Root CA

Špecializované IKT systémy Windows

Ing. Stanislav Lukac, PhD.

Krok 3

::Konfigurácia RootCA

AD CS Configuration

Credentials

DESTINATION SERVER
srv4.dual.edu

Credentials

Role Services

Confirmation

Progress

Results

Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: SRV4\Administrator

Change...

[More about AD CS Server Roles](#)

< Previous

Next >

Configure

Cancel

Krok 3

::Konfigurácia RootCA

AD CS Configuration

Role Services

DESTINATION SERVER
srv4.dual.edu

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

Select Role Services to configure

- ☒ Certification Authority
- ☐ Certification Authority Web Enrollment
- ☐ Online Responder
- ☐ Network Device Enrollment Service
- ☐ Certificate Enrollment Web Service
- ☐ Certificate Enrollment Policy Web Service

[More about AD CS Server Roles](#)

< Previous

Next >

Configure

Cancel

Krok 3

::Konfigurácia RootCA

The screenshot shows the 'AD CS Configuration' console window. The 'Setup Type' step is selected in the left-hand navigation pane. The main area displays the 'Specify the setup type of the CA' section. It includes a description of Enterprise and Standalone CAs, with 'Standalone CA' selected. The 'DESTINATION SERVER' is listed as 'srv4.dual.edu'. At the bottom, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

Setup Type

DESTINATION SERVER
srv4.dual.edu

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

☐ Enterprise CA
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

☒ Standalone CA
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

[More about Setup Type](#)

< Previous Next > Configure Cancel

Krok 3

::Konfigurácia RootCA

The screenshot shows the 'AD CS Configuration' wizard window. The title bar includes the application icon, the text 'AD CS Configuration', and standard window controls (minimize, maximize, close). The main content area is titled 'CA Type' and features a left-hand navigation pane with the following items: 'Credentials', 'Role Services', 'Setup Type', 'CA Type' (highlighted with a blue bar), 'Private Key', 'Cryptography', 'CA Name', 'Validity Period', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The main pane is titled 'Specify the type of the CA' and contains explanatory text: 'When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.' Below this text are two radio button options: 'Root CA' (selected) and 'Subordinate CA'. The 'Root CA' option is accompanied by the text 'Root CAs are the first and may be the only CAs configured in a PKI hierarchy.' The 'Subordinate CA' option is accompanied by the text 'Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.' A link 'More about CA Type' is located at the bottom of the main pane. The bottom of the window features a gray bar with four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER
srv4.dual.edu

CA Type

- Credentials
- Role Services
- Setup Type
- CA Type**
- Private Key
- Cryptography
- CA Name
- Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

☒ Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

☐ Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

[More about CA Type](#)

< Previous Next > Configure Cancel

Krok 3

::Konfigurácia RootCA

The screenshot shows the 'AD CS Configuration' console window. The left-hand navigation pane lists the following steps: Credentials, Role Services, Setup Type, CA Type, **Private Key** (highlighted), Cryptography, CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main pane is titled 'Private Key' and shows the 'DESTINATION SERVER' as 'srv4.dual.edu'. Below the title, it says 'Specify the type of the private key'. A descriptive text states: 'To generate and issue certificates to clients, a certification authority (CA) must have a private key.' There are three radio button options: 1. 'Create a new private key' (selected), with the instruction 'Use this option if you do not have a private key or want to create a new private key.' 2. 'Use existing private key', with the instruction 'Use this option to ensure continuity with previously issued certificates when reinstalling a CA.' This option has two sub-radio buttons: 'Select a certificate and use its associated private key' and 'Select an existing private key on this computer'. 3. 'Select an existing private key on this computer', with the instruction 'Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.' At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER
srv4.dual.edu

Private Key

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

☒ Create a new private key
Use this option if you do not have a private key or want to create a new private key.

☐ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

☐ Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

☐ Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

[More about Private Key](#)

< Previous Next > Configure Cancel

Krok 3

::Konfigurácia RootCA

AD CS Configuration

Cryptography for CA

DESTINATION SERVER
srv4.dual.edu

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the cryptographic options

Select a cryptographic provider:
RSA#Microsoft Software Key Storage Provider

Key length:
4096

Select the hash algorithm for signing certificates issued by this CA:

SHA256
SHA384
SHA512
SHA1
MD5

☐ Allow administrator interaction when the private key is accessed by the CA.

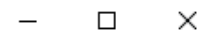
[More about Cryptography](#)

< Previous Next > Configure Cancel

Krok 3

::Konfigurácia RootCA

AD CS Configuration



CA Name

DESTINATION SERVER

srv4.dual.edu

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:

Distinguished name suffix:

Preview of distinguished name:

[More about CA Name](#)

< Previous

Next >

Configure

Cancel

Krok 3

::Konfigurácia RootCA

AD CS Configuration

Validity Period

DESTINATION SERVER
srv4.dual.edu

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):

10 Years

CA expiration Date: 8/29/2029 2:35:00 AM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

[More about Validity Period](#)

< Previous Next > Configure Cancel

Krok 3

::Konfigurácia RootCA

AD CS Configuration

CA Database

DESTINATION SERVER
srv4.dual.edu

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the database locations

Certificate database location:
C:\Windows\system32\CertLog

Certificate database log location:
C:\Windows\system32\CertLog

[More about CA Database](#)

< Previous Next > Configure Cancel

Krok 3

::Konfigurácia RootCA

AD CS Configuration

Confirmation

DESTINATION SERVER
srv4.dual.edu

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

To configure the following roles, role services, or features, click Configure.

⬆ Active Directory Certificate Services

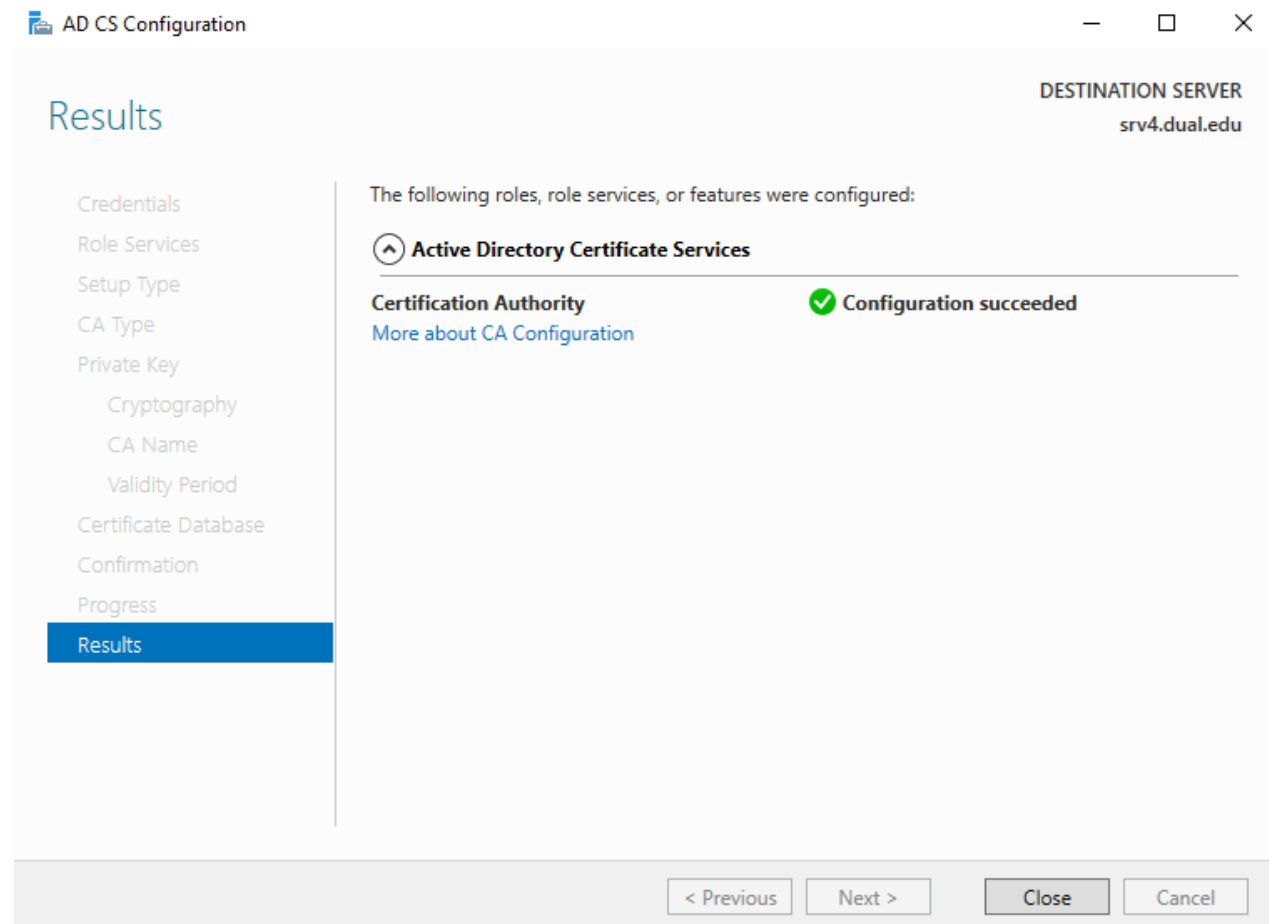
Certification Authority

CA Type:	Standalone Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA256
Key Length:	4096
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	8/29/2029 2:35:00 AM
Distinguished Name:	CN=SRV4-CA-ROOT
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

< Previous Next > Configure Cancel

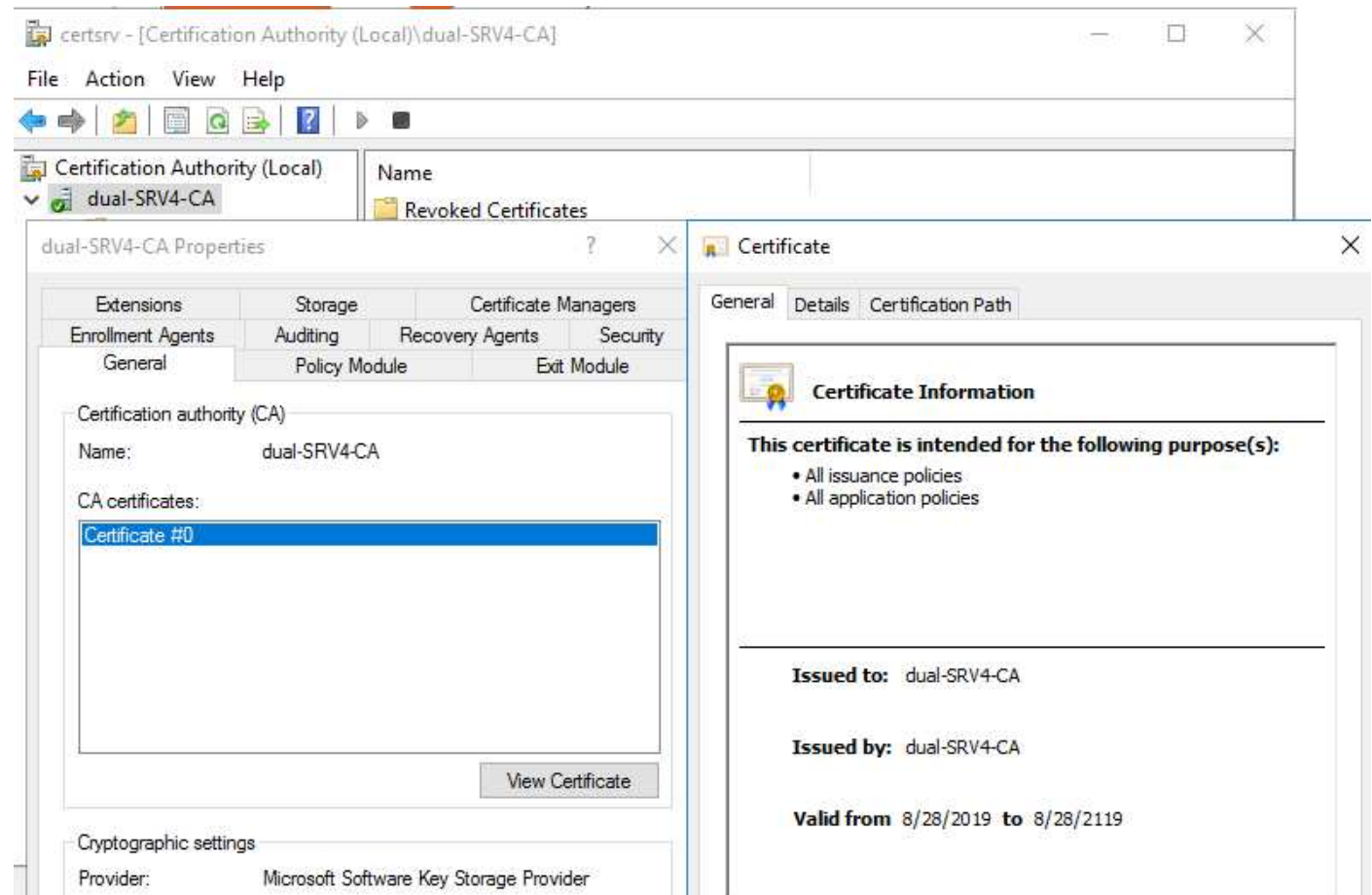
Krok 3

::Konfigurácia RootCA



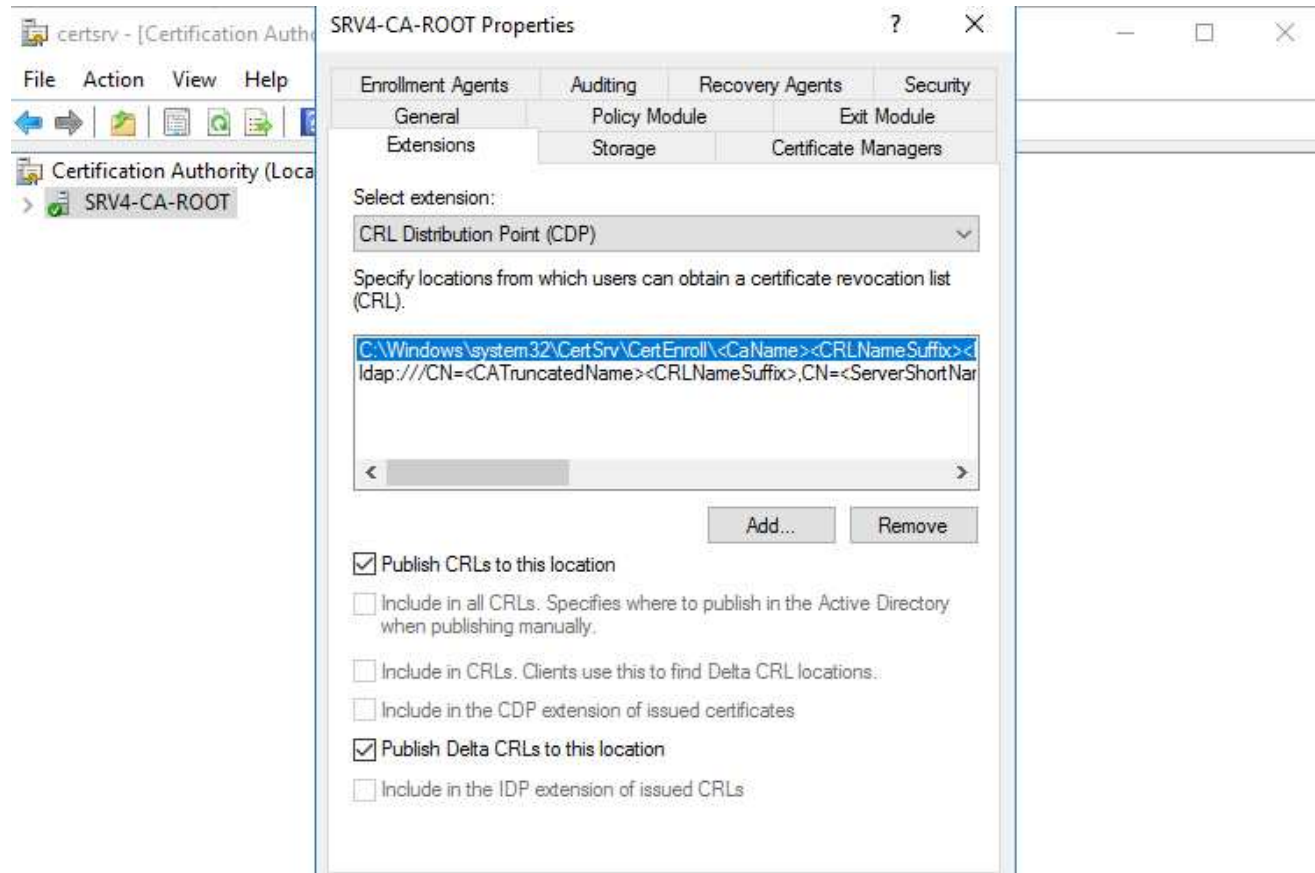
Krok 4

::Validate certificate na ROOT CA na SRV4



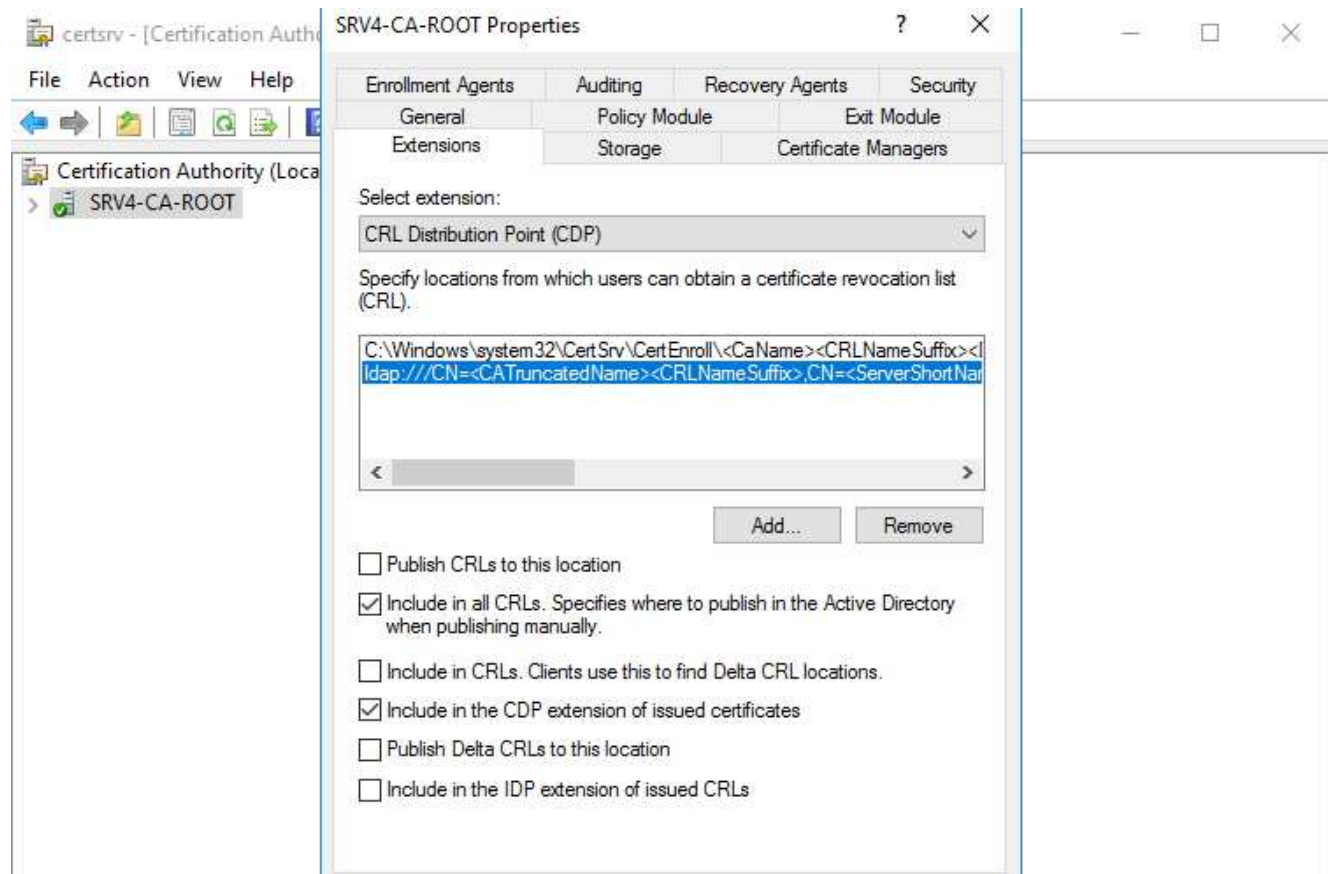
Krok 5

::Konfigurácia CDP (CRL distribution list) na RootCA



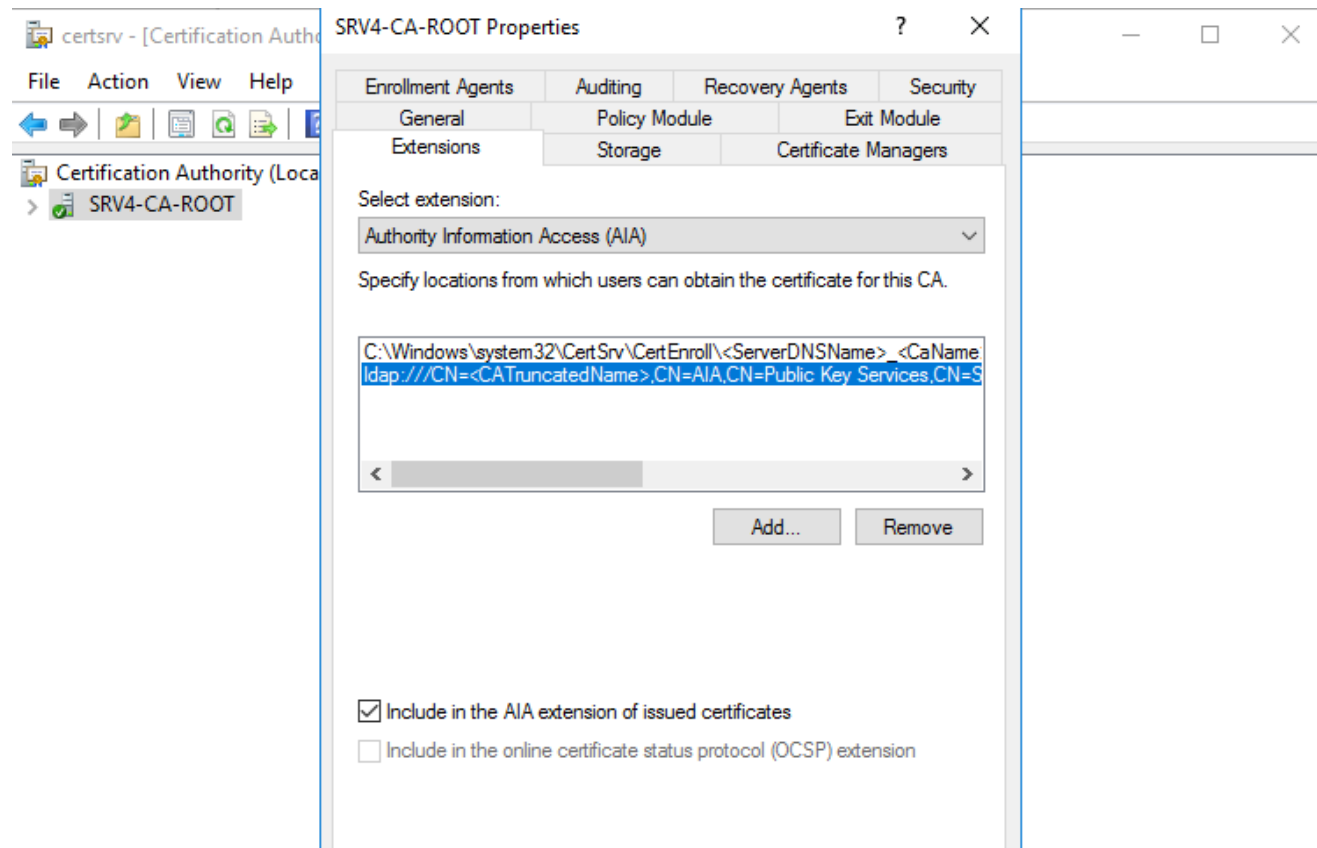
Krok 5

::Konfigurácia CDP na RootCA



Krok 5

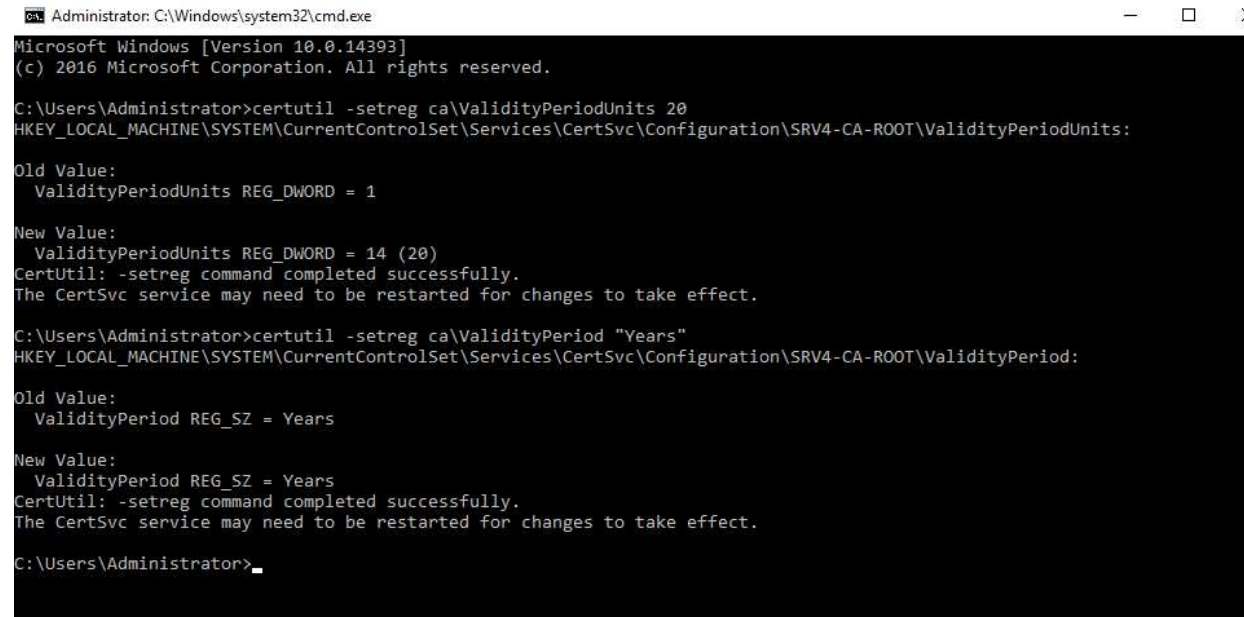
::Konfigurácia AIA (Authority information access) na RootCA



Krok 6

::Zvýšenie CRL valid periódy

```
certutil -setreg ca\ValidityPeriodUnits 20  
certutil -setreg ca\ValidityPeriod "Years"
```

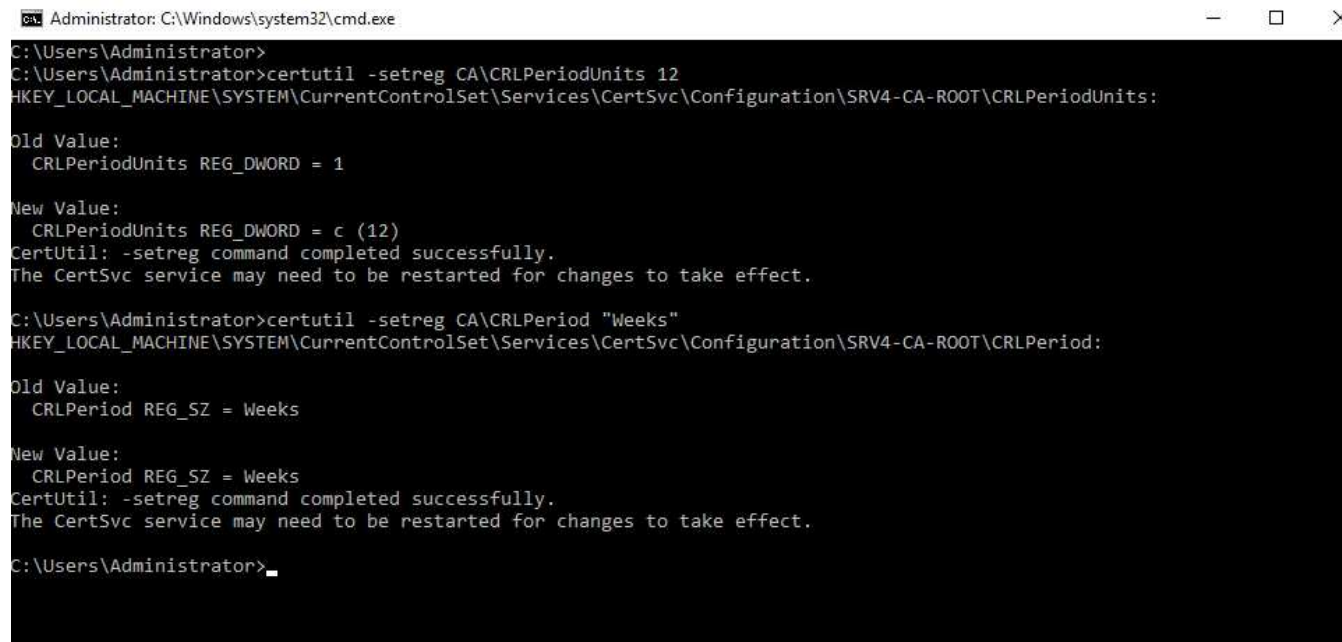


```
Administrator: C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 10.0.14393]  
(c) 2016 Microsoft Corporation. All rights reserved.  
  
C:\Users\Administrator>certutil -setreg ca\ValidityPeriodUnits 20  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\SRV4-CA-ROOT\ValidityPeriodUnits:  
  
Old Value:  
    ValidityPeriodUnits REG_DWORD = 1  
  
New Value:  
    ValidityPeriodUnits REG_DWORD = 14 (20)  
CertUtil: -setreg command completed successfully.  
The CertSvc service may need to be restarted for changes to take effect.  
  
C:\Users\Administrator>certutil -setreg ca\ValidityPeriod "Years"  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\SRV4-CA-ROOT\ValidityPeriod:  
  
Old Value:  
    ValidityPeriod REG_SZ = Years  
  
New Value:  
    ValidityPeriod REG_SZ = Years  
CertUtil: -setreg command completed successfully.  
The CertSvc service may need to be restarted for changes to take effect.  
  
C:\Users\Administrator>
```

Krok 6

::Zvýšenie CERT valid periódy

```
certutil -setreg CA\CRLPeriodUnits 12  
certutil -setreg CA\CRLPeriod "Weeks"
```



```
Administrator: C:\Windows\system32\cmd.exe  
C:\Users\Administrator>  
C:\Users\Administrator>certutil -setreg CA\CRLPeriodUnits 12  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\SRV4-CA-ROOT\CRLPeriodUnits:  
Old Value:  
    CRLPeriodUnits REG_DWORD = 1  
New Value:  
    CRLPeriodUnits REG_DWORD = c (12)  
CertUtil: -setreg command completed successfully.  
The CertSvc service may need to be restarted for changes to take effect.  
C:\Users\Administrator>certutil -setreg CA\CRLPeriod "Weeks"  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\SRV4-CA-ROOT\CRLPeriod:  
Old Value:  
    CRLPeriod REG_SZ = Weeks  
New Value:  
    CRLPeriod REG_SZ = Weeks  
CertUtil: -setreg command completed successfully.  
The CertSvc service may need to be restarted for changes to take effect.  
C:\Users\Administrator>
```

Restart service

- net stop certsvc
- net start certsvc

Krok 6

::Nastavenie premennej pre Distinguished Name na SRV4

Certutil -setreg ca\DSConfigDN "CN=Configuration,DC=dual,DC=edu"

Administrator: Command Prompt

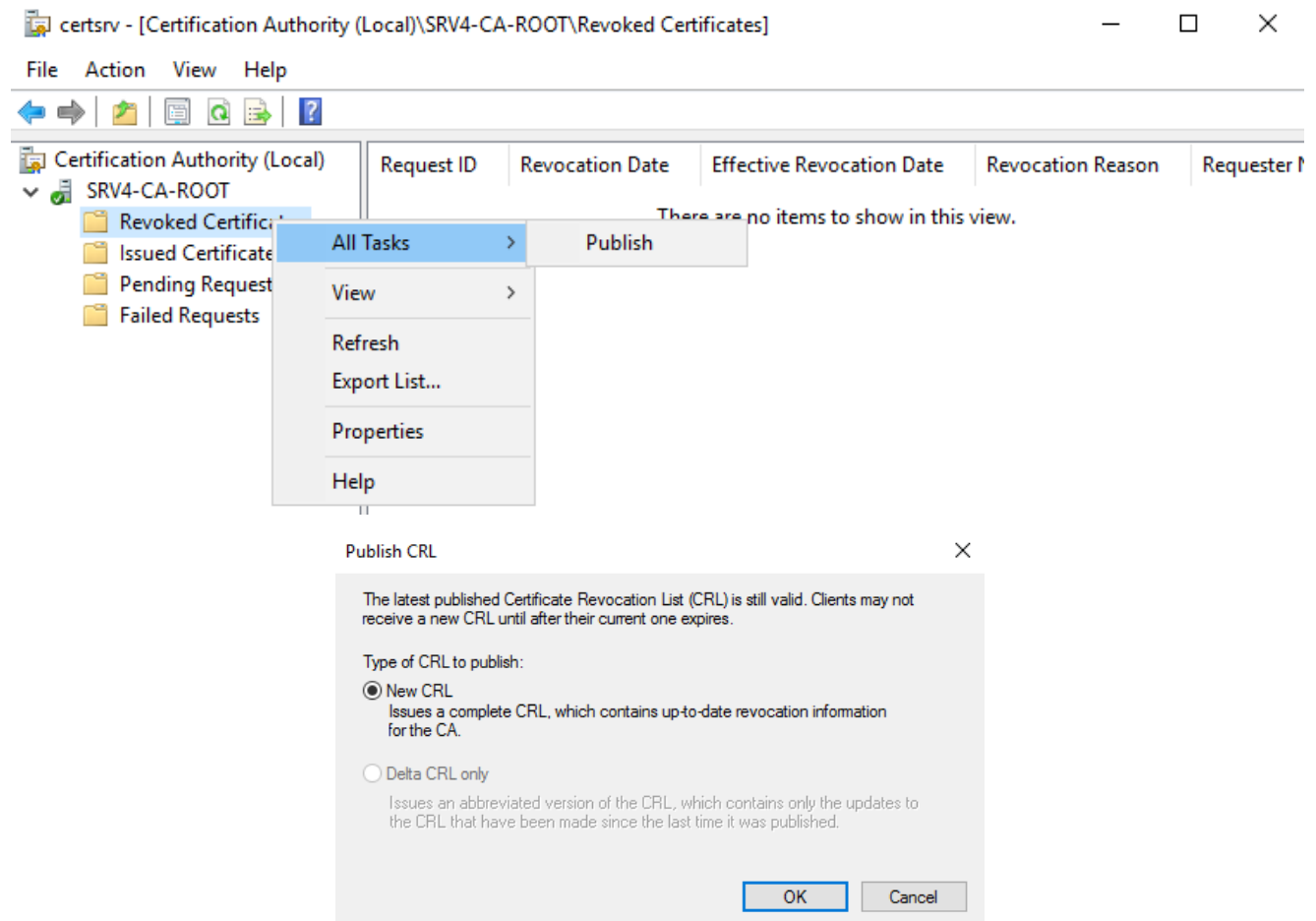
```
C:\Users\Administrator>Certutil -setreg ca\DSConfigDN "CN=Configuration,DC=dual,DC=edu"  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\SRV4-CA-ROOT\DSConfigDN:  
New Value:  
    DSConfigDN REG_SZ = CN=Configuration,DC=dual,DC=edu  
CertUtil: -setreg command completed successfully.  
The CertSvc service may need to be restarted for changes to take effect.  
C:\Users\Administrator>_
```

Restart service

- net stop certsvc
- net start certsvc

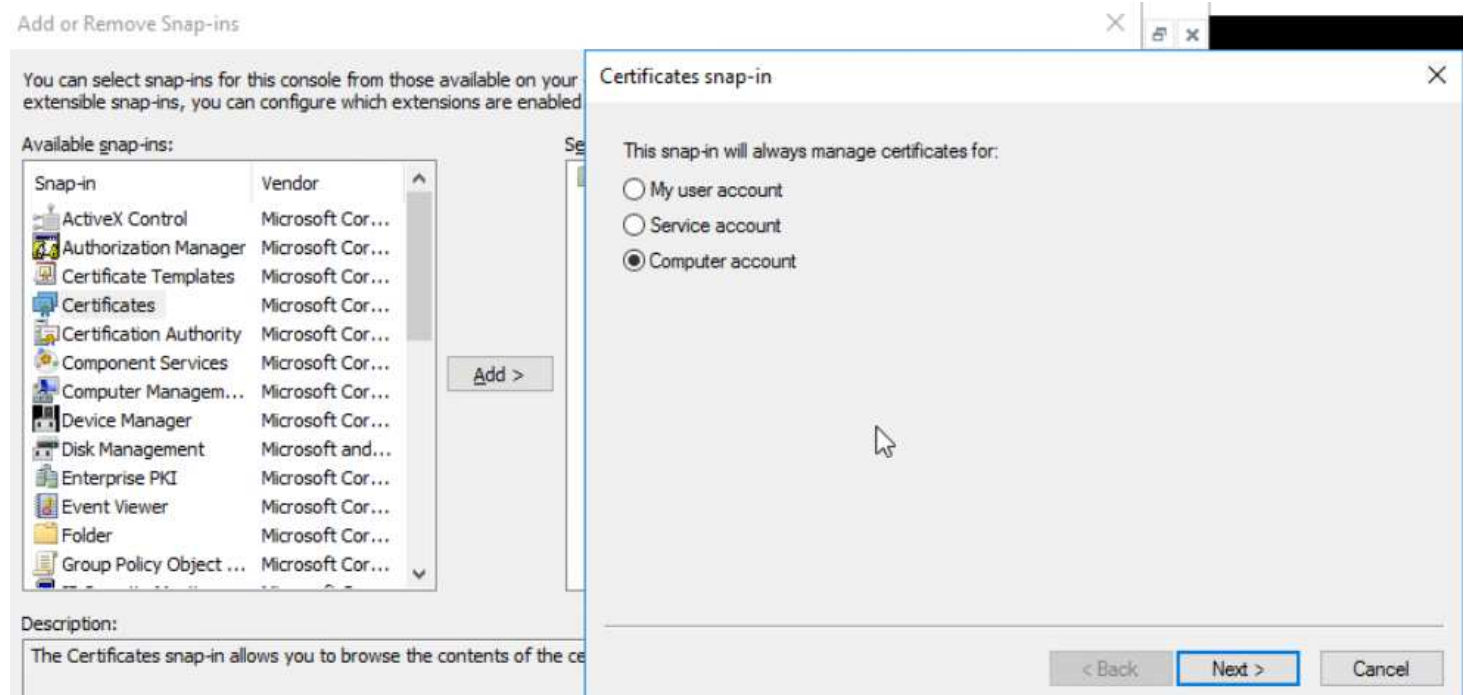
Krok 7

::Publish CRL pre import do AD



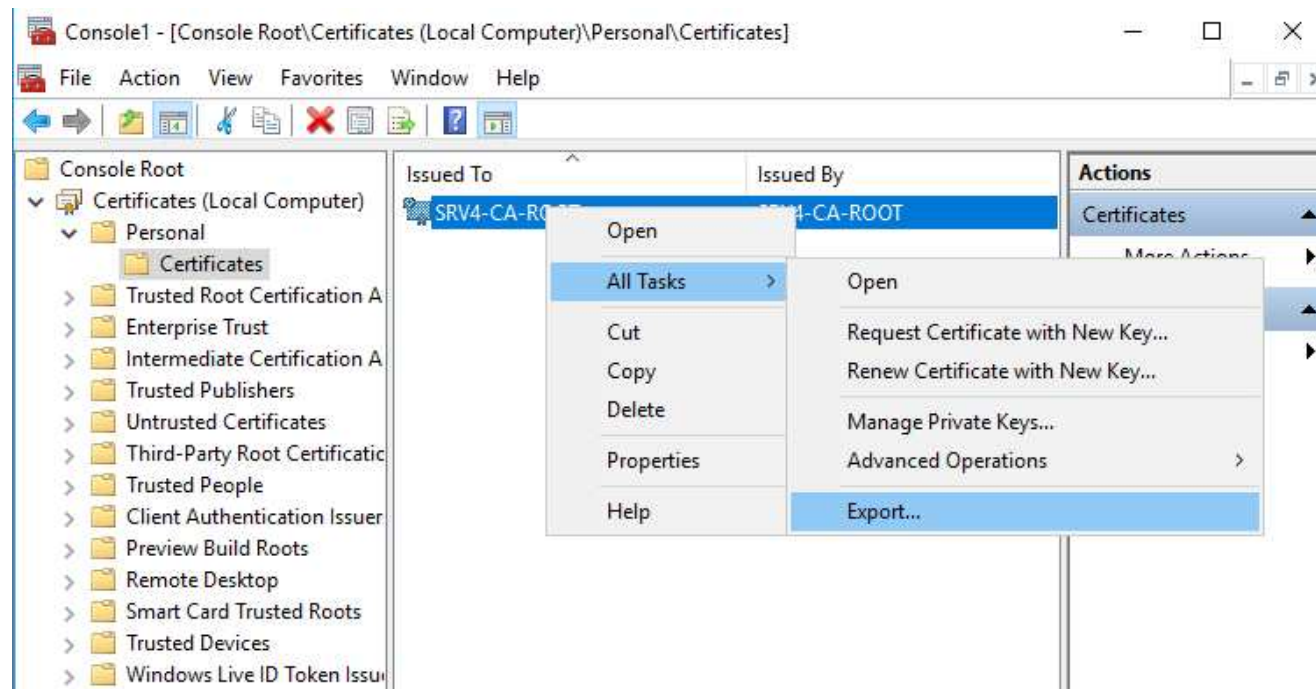
Krok 8

::Export certifikátu z rootCA pre import do AD



Krok 8

::Export certifikátu z rootCA pre import do AD



Krok 8

:: Export certifikátu z rootCA pre import do AD

← 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

NextCancel

← 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)

NextCancel

Krok 8

:: Export certifikátu z rootCA pre import do AD

 Certificate Export Wizard

 Certificate Export Wizard

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

File name:

Completing the Certificate Export Wizard

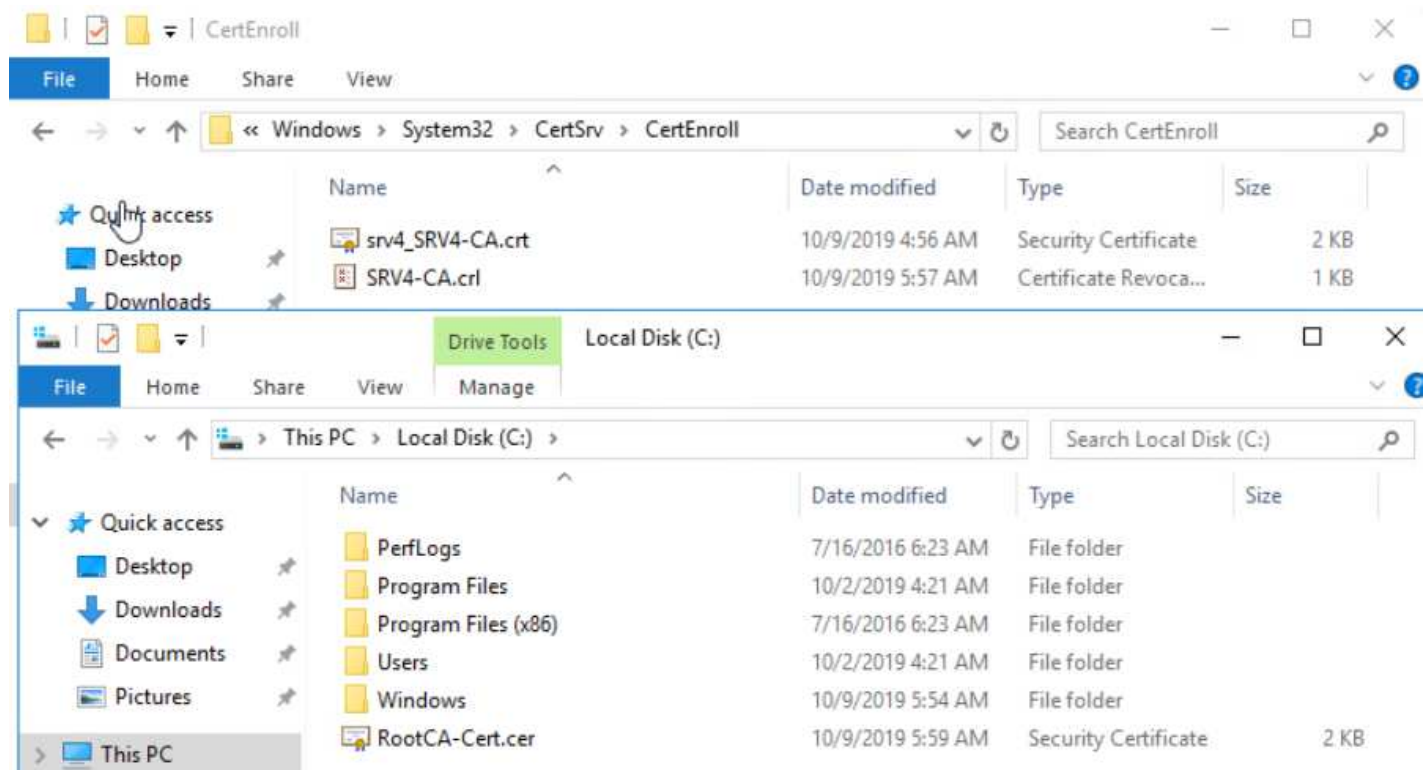
You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Cert\ExportedRootCA.cer
Export Keys	No
Include all certificates in the certification path	No
File Format	DER Encoded Binary X.509 (*.cer)

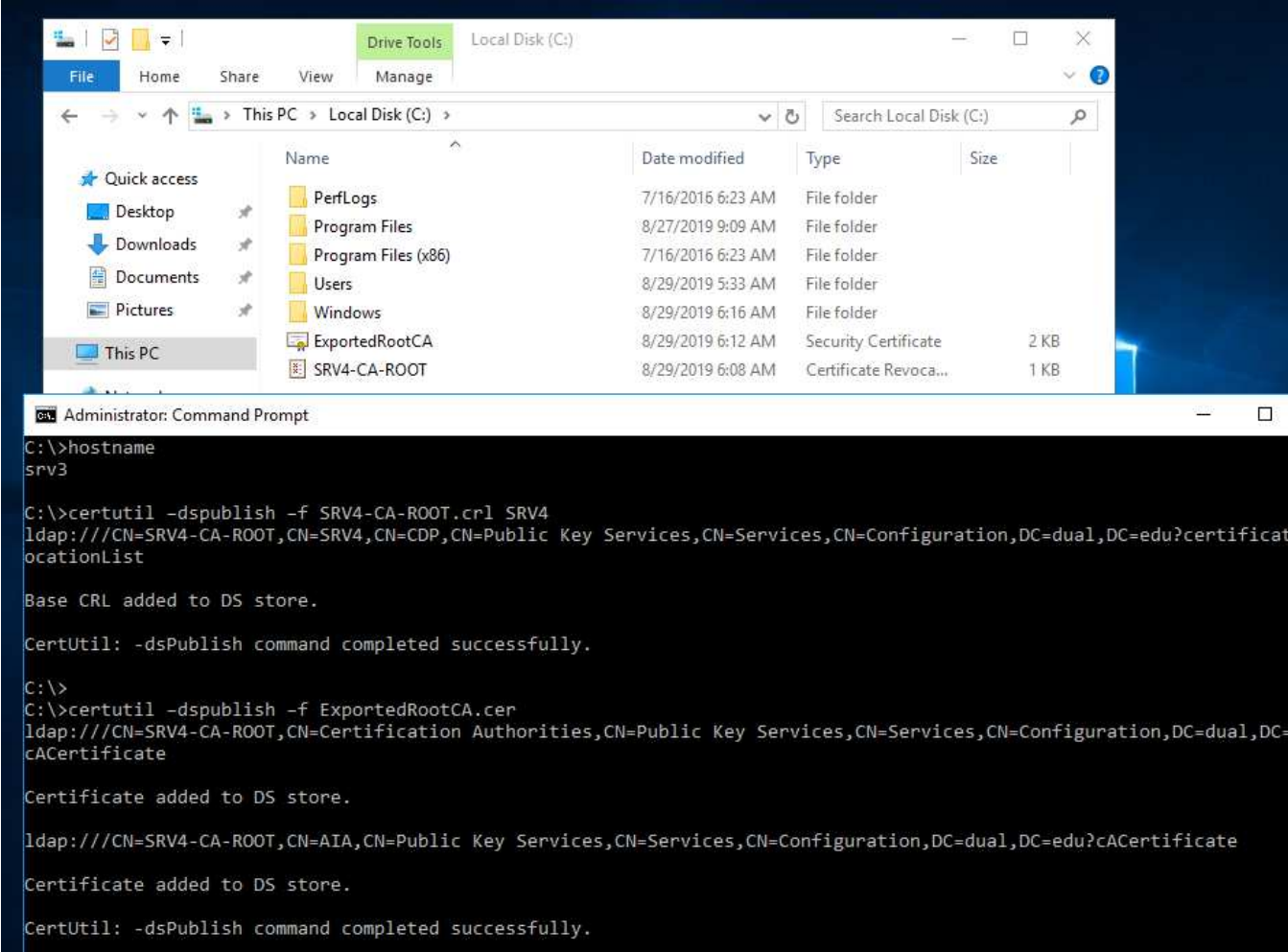
Krok 8

::Validácia certifikátov pripravených na import do AD



Krok 9

::Import exportovaných certifikátov do AD na SRV3



The screenshot displays two windows from a Windows operating system. The top window is 'File Explorer' showing the 'Local Disk (C:)' with a table of files and folders. The bottom window is an 'Administrator: Command Prompt' showing the execution of 'certutil' commands to publish certificates to an Active Directory.

Name	Date modified	Type	Size
PerfLogs	7/16/2016 6:23 AM	File folder	
Program Files	8/27/2019 9:09 AM	File folder	
Program Files (x86)	7/16/2016 6:23 AM	File folder	
Users	8/29/2019 5:33 AM	File folder	
Windows	8/29/2019 6:16 AM	File folder	
ExportedRootCA	8/29/2019 6:12 AM	Security Certificate	2 KB
SRV4-CA-ROOT	8/29/2019 6:08 AM	Certificate Revoca...	1 KB

```
C:\>hostname
srv3

C:\>certutil -dspublish -f SRV4-CA-ROOT.crl SRV4
ldap:///CN=SRV4-CA-ROOT,CN=SRV4,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=dual,DC=edu?certificateLocationList

Base CRL added to DS store.

CertUtil: -dsPublish command completed successfully.

C:\>
C:\>certutil -dspublish -f ExportedRootCA.cer
ldap:///CN=SRV4-CA-ROOT,CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=dual,DC=edu?cACertificate

Certificate added to DS store.

ldap:///CN=SRV4-CA-ROOT,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=dual,DC=edu?cACertificate

Certificate added to DS store.

CertUtil: -dsPublish command completed successfully.
```

Konfigurácia Subordinate CA

Špecializované IKT systémy Windows

Ing. Stanislav Lukac, PhD.

Krok 10

::Post konfigurácia role CA na subordinate CA (SRV3)

The screenshot shows the 'AD CS Configuration' console window. The title bar includes the application icon, the text 'AD CS Configuration', and standard window controls (minimize, maximize, close). The main content area is titled 'Role Services' and shows the 'DESTINATION SERVER' as 'srv3.dual.edu'. On the left, a navigation pane lists the steps: 'Credentials', 'Role Services' (highlighted), 'Setup Type', 'CA Type', 'Private Key', 'Cryptographyp', 'CA Name', 'Certificate Request', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The main pane is titled 'Select Role Services to configure' and contains a list of services with checkboxes: 'Certification Authority' (checked), 'Certification Authority Web Enrollment' (unchecked), 'Online Responder' (unchecked), 'Network Device Enrollment Service' (unchecked), 'Certificate Enrollment Web Service' (unchecked), and 'Certificate Enrollment Policy Web Service' (unchecked). At the bottom of the main pane is a link 'More about AD CS Server Roles'. The bottom of the window features a navigation bar with four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

Role Services

DESTINATION SERVER
srv3.dual.edu

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptographyp
CA Name
Certificate Request
Certificate Database
Confirmation
Progress
Results

Select Role Services to configure

- ☒ Certification Authority
- ☐ Certification Authority Web Enrollment
- ☐ Online Responder
- ☐ Network Device Enrollment Service
- ☐ Certificate Enrollment Web Service
- ☐ Certificate Enrollment Policy Web Service

[More about AD CS Server Roles](#)

< Previous Next > Configure Cancel

Krok 10

::Post konfigurácia role CA na subordinate CA (SRV3)

The screenshot shows the 'AD CS Configuration' console window. The title bar includes the application icon, the text 'AD CS Configuration', and standard window controls (minimize, maximize, close). The main content area is titled 'Setup Type' and shows a list of steps on the left: 'Credentials', 'Role Services', 'Setup Type' (highlighted), 'CA Type', 'Private Key', 'Cryptography', 'CA Name', 'Certificate Request', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The right pane is titled 'Specify the setup type of the CA' and contains two radio button options: 'Enterprise CA' (selected) and 'Standalone CA'. Below each option is a descriptive paragraph. The 'Enterprise CA' option states that Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies. The 'Standalone CA' option states that Standalone CAs can be members or a workgroup or domain, do not require AD DS, and can be used without a network connection (offline). A link 'More about Setup Type' is located at the bottom of the right pane. The bottom of the window features a navigation bar with four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER
srv3.dual.edu

Setup Type

- Credentials
- Role Services
- Setup Type**
- CA Type
- Private Key
- Cryptography
- CA Name
- Certificate Request
- Certificate Database
- Confirmation
- Progress
- Results

Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

☒ Enterprise CA
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

☐ Standalone CA
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

[More about Setup Type](#)

< Previous Next > Configure Cancel

Krok 10

::Post konfigurácia role CA na subordinate CA (SRV3)

The screenshot shows the 'AD CS Configuration' console window. On the left is a navigation pane with the following items: Credentials, Role Services, Setup Type, CA Type (highlighted), Private Key, Cryptography, CA Name, Certificate Request, Certificate Database, Confirmation, Progress, and Results. The main pane is titled 'CA Type' and contains the following text: 'Specify the type of the CA'. Below this is a paragraph explaining the hierarchy: 'When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.' There are two radio button options: 'Root CA' (unselected) and 'Subordinate CA' (selected). Below the 'Subordinate CA' option is a note: 'Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.' At the bottom of the main pane is a link: 'More about CA Type'. In the top right corner of the console, it says 'DESTINATION SERVER' and 'srv3.dual.edu'. At the bottom of the console are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER
srv3.dual.edu

CA Type

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Certificate Request
Certificate Database
Confirmation
Progress
Results

Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

☐ Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

☒ Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

[More about CA Type](#)

< Previous Next > Configure Cancel

Krok 10

::Post konfigurácia role CA na subordinate CA (SRV3)

The screenshot shows the 'AD CS Configuration' console window. On the left, a navigation pane lists the following steps: Credentials, Role Services, Setup Type, CA Type, **Private Key** (highlighted), Cryptography, CA Name, Certificate Request, Certificate Database, Confirmation, Progress, and Results. The main pane is titled 'Private Key' and shows the 'DESTINATION SERVER' as 'srv3.dual.edu'. Below the title, it says 'Specify the type of the private key'. A descriptive text states: 'To generate and issue certificates to clients, a certification authority (CA) must have a private key.' There are three radio button options: 1. 'Create a new private key' (selected), with a sub-note: 'Use this option if you do not have a private key or want to create a new private key.' 2. 'Use existing private key', with a sub-note: 'Use this option to ensure continuity with previously issued certificates when reinstalling a CA.' This option has two sub-options: 'Select a certificate and use its associated private key' (with a sub-note: 'Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.') and 'Select an existing private key on this computer' (with a sub-note: 'Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.'). At the bottom of the main pane is a link: 'More about Private Key'. The bottom of the window contains four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER
srv3.dual.edu

Private Key

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Certificate Request
Certificate Database
Confirmation
Progress
Results

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

☒ Create a new private key
Use this option if you do not have a private key or want to create a new private key.

☐ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

☐ Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

☐ Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

[More about Private Key](#)

< Previous Next > Configure Cancel

Krok 10

::Post konfigurácia role CA na subordinate CA (SRV3)

AD CS Configuration

Cryptography for CA

DESTINATION SERVER
srv3.dual.edu

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Certificate Request
Certificate Database
Confirmation
Progress
Results

Specify the cryptographic options

Select a cryptographic provider:
RSA#Microsoft Software Key Storage Provider

Key length:
4096

Select the hash algorithm for signing certificates issued by this CA:

SHA256
SHA384
SHA512
SHA1
MD5

☐ Allow administrator interaction when the private key is accessed by the CA.

[More about Cryptography](#)

< Previous Next > Configure Cancel

Krok 10

::Post konfigurácia role CA na subordinate CA (SRV3)

AD CS Configuration

DESTINATION SERVER
srv3.dual.edu

CA Name

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
- Cryptography
- CA Name**
- Certificate Request
- Certificate Database
- Confirmation
- Progress
- Results

Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:

Distinguished name suffix:

Preview of distinguished name:

[More about CA Name](#)

< Previous Next > Configure Cancel

Krok 10

::Post konfigurácia role CA na subordinate CA (SRV3)

AD CS Configuration

Certificate Request

DESTINATION SERVER
srv3.dual.edu

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Certificate Request
Certificate Database
Confirmation
Progress
Results

Request a certificate from parent CA

You require a certificate from a parent certification authority (CA) to allow this subordinate CA to issue certificates. You can request a certificate from an online CA or you can store your request to a file to submit to the parent CA.

☐ Send a certificate request to a parent CA:

Select:

☒ CA name
☐ Computer name

Parent CA:

☒ Save a certificate request to file on the target machine:

File name:

i You must manually get a certificate back from the parent CA to make this CA operational.

[More about Certificate Request](#)

< Previous Next > Configure Cancel

Krok 10

::Post konfigurácia role CA na subordinate CA (SRV3)

AD CS Configuration

CA Database

DESTINATION SERVER
srv3.dual.edu

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Certificate Request
Certificate Database
Confirmation
Progress
Results

Specify the database locations

Certificate database location:

Certificate database log location:

[More about CA Database](#)

< Previous Next > Configure Cancel

Krok 10

::Post konfigurácia role CA na subordinate CA (SRV3)

AD CS Configuration

DESTINATION SERVER
srv3.dual.edu

Confirmation

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
 - Cryptography
- CA Name
- Certificate Request
- Certificate Database
- Confirmation**
- Progress
- Results

To configure the following roles, role services, or features, click Configure.

⬆ **Active Directory Certificate Services**

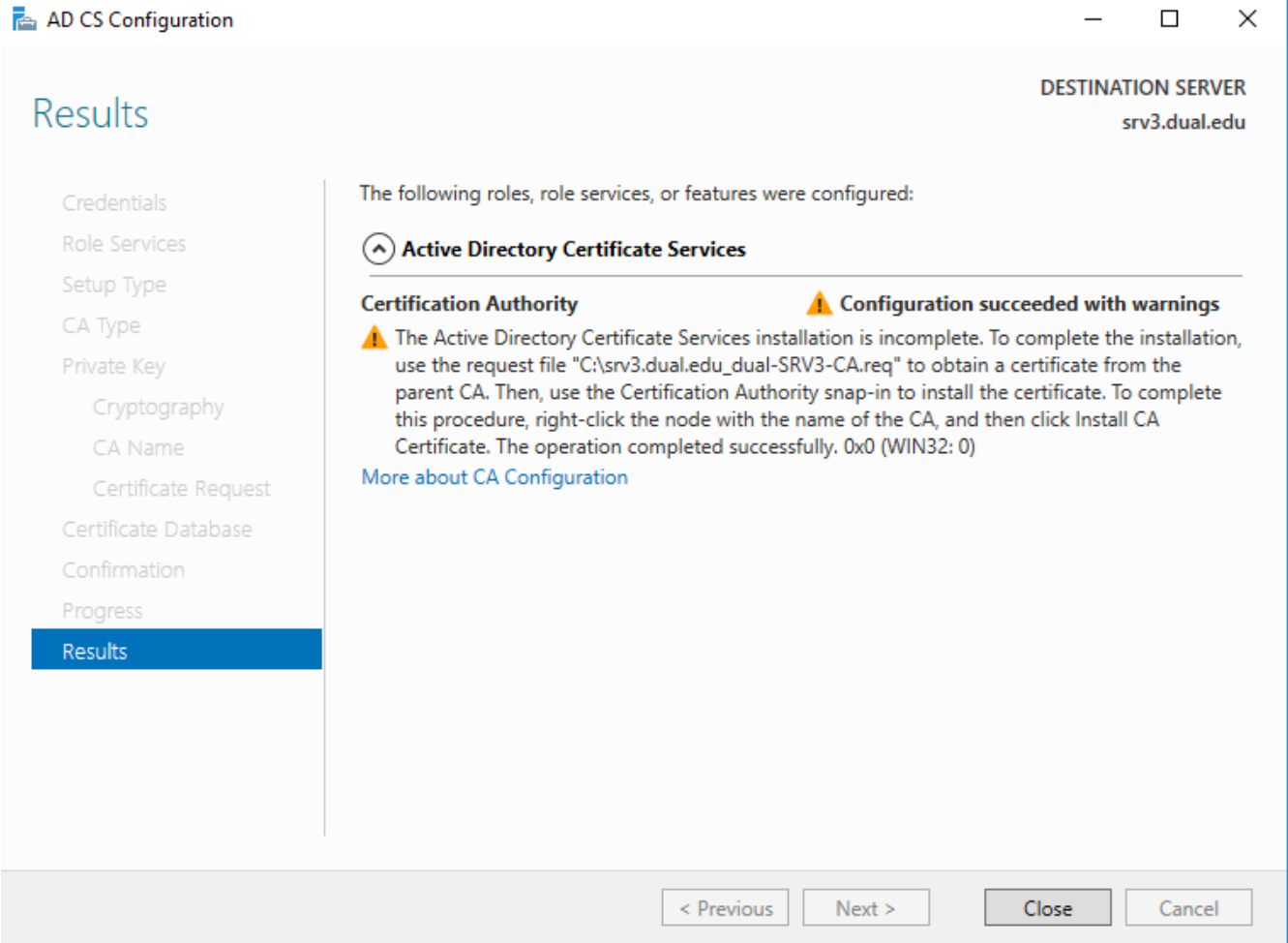
Certification Authority

CA Type:	Enterprise Subordinate
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA256
Key Length:	4096
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	Determined by the parent CA
Distinguished Name:	CN=dual-SRV3-CA,DC=dual,DC=edu
Offline Request File Location:	C:\srv3.dual.edu_dual-SRV3-CA.req
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

< Previous Next > **Configure** Cancel

Krok 10

::Post konfigurácia role CA na subordinate CA (SRV3)



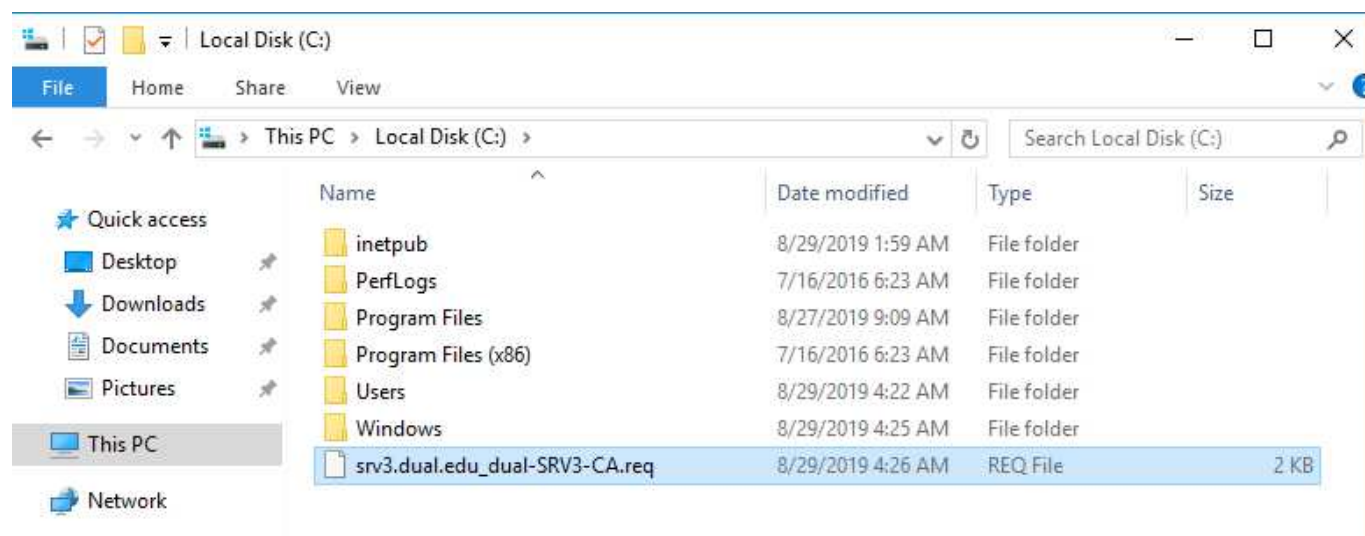
Post configuration CA

Špecializované IKT systémy Windows

Ing. Stanislav Lukac, PhD.

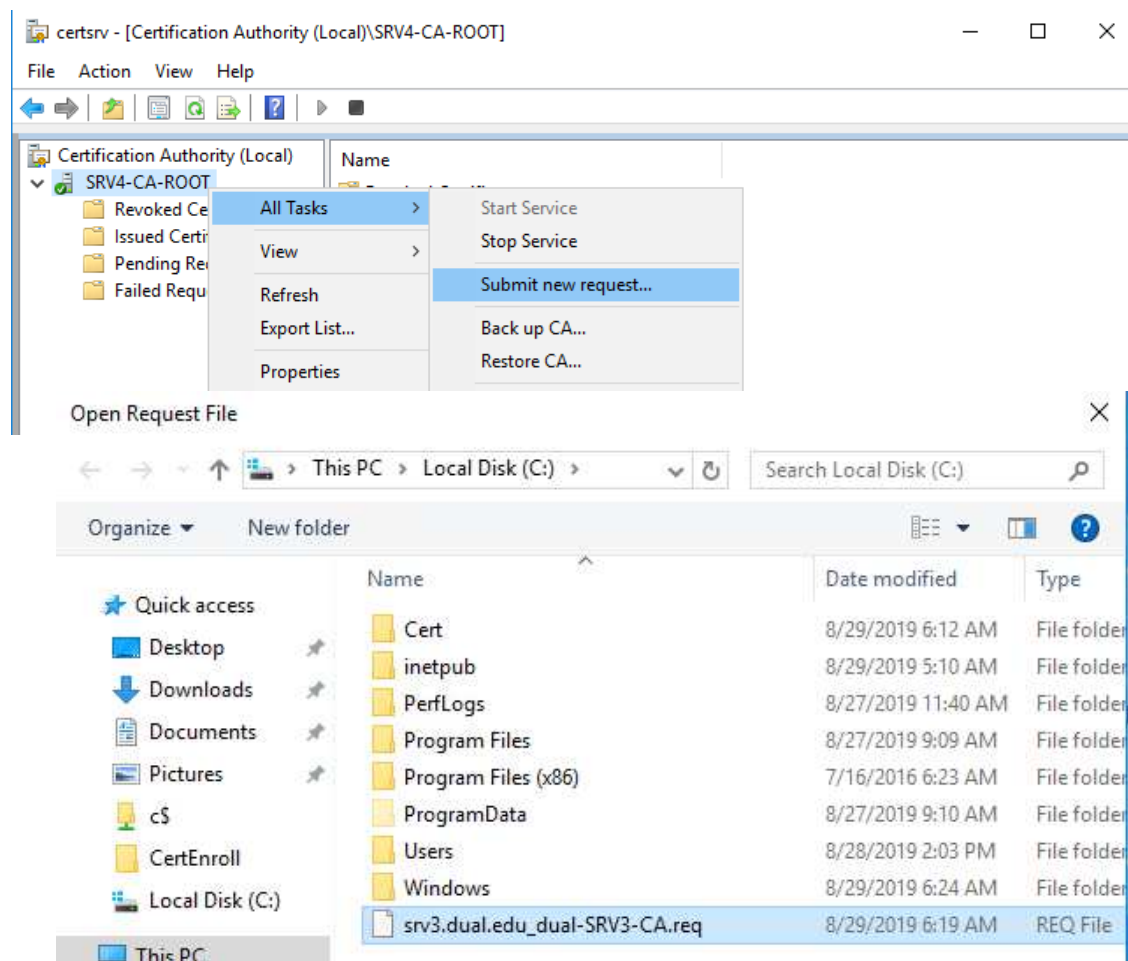
Krok 11

::Overiť certifikát request z SubordinateCA cez RootCA



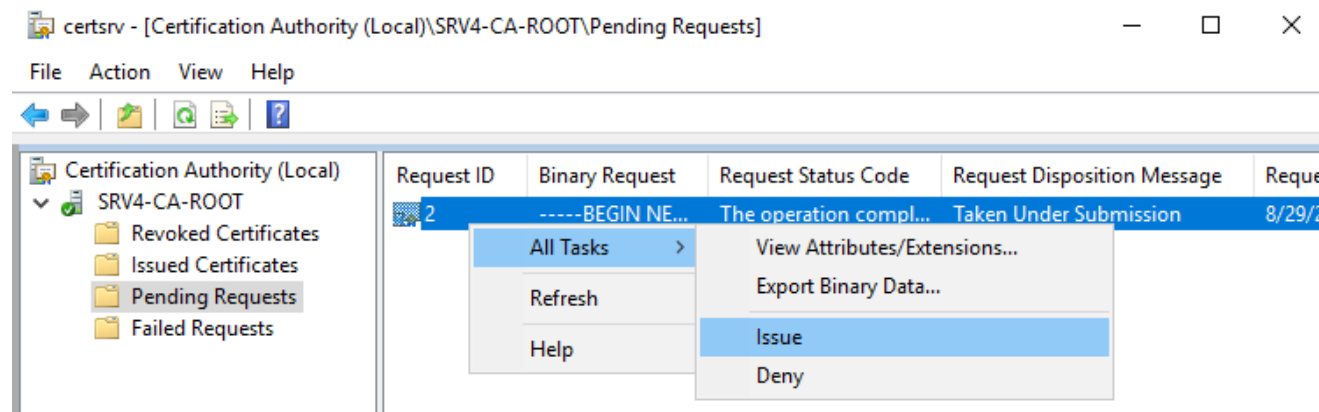
Krok 11

:: Overiť certifikát request z SubordinateCA cez RootCA



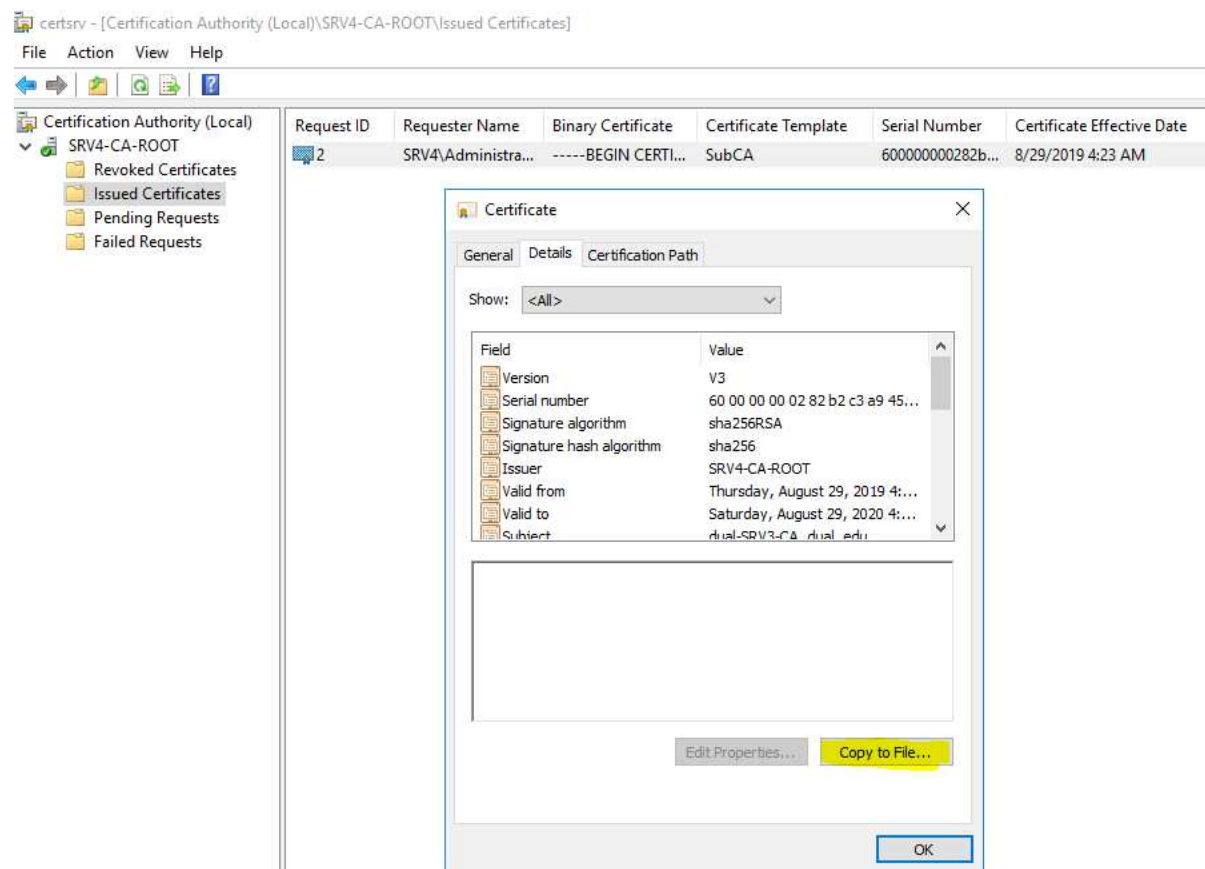
Krok 11

:: Overiť certifikát request z SubordinateCA cez RootCA



Krok 11

:: Overiť certifikát request z SubordinateCA cez RootCA



Krok 11

:: Overiť certifikát request z SubordinateCA cez RootCA

The screenshot shows the 'Certificate Export Wizard' dialog box. The left pane displays the 'Welcome to the Certificate Export Wizard' screen, which explains the wizard's purpose and provides instructions to click 'Next'. The right pane shows the 'Export File Format' step, where the user is prompted to select a format. The 'DER encoded binary X.509 (.CER)' option is selected. Below this, there are several checkboxes for additional options, all of which are currently unchecked. At the bottom of the dialog, there are 'Next' and 'Cancel' buttons.

← 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.

Next Cancel

← Certificate Export Wizard

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

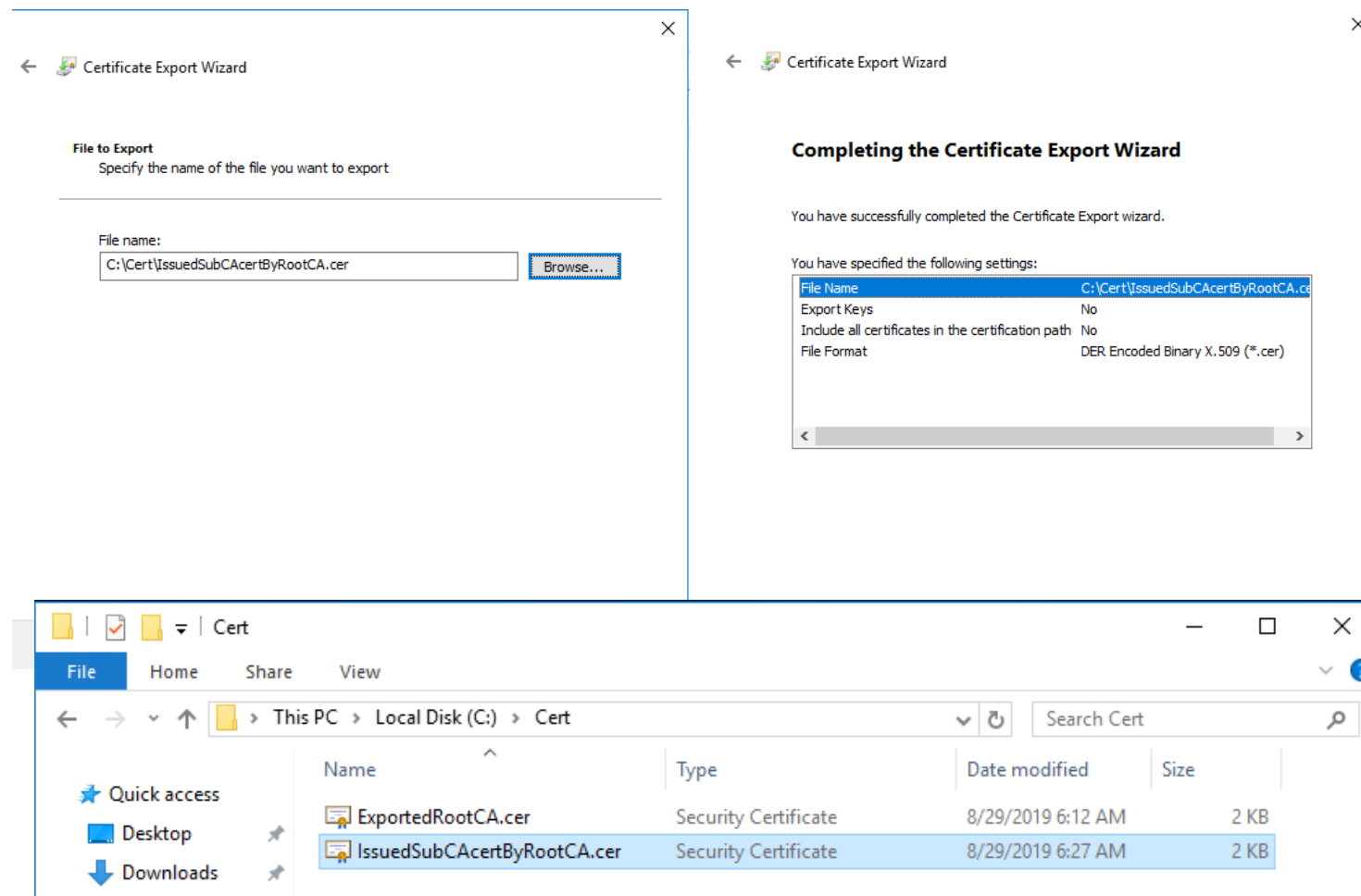
Select the format you want to use:

- ☒ 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)

Next Cancel

Krok 11

:: Overiť certifikát request z SubordinateCA cez RootCA



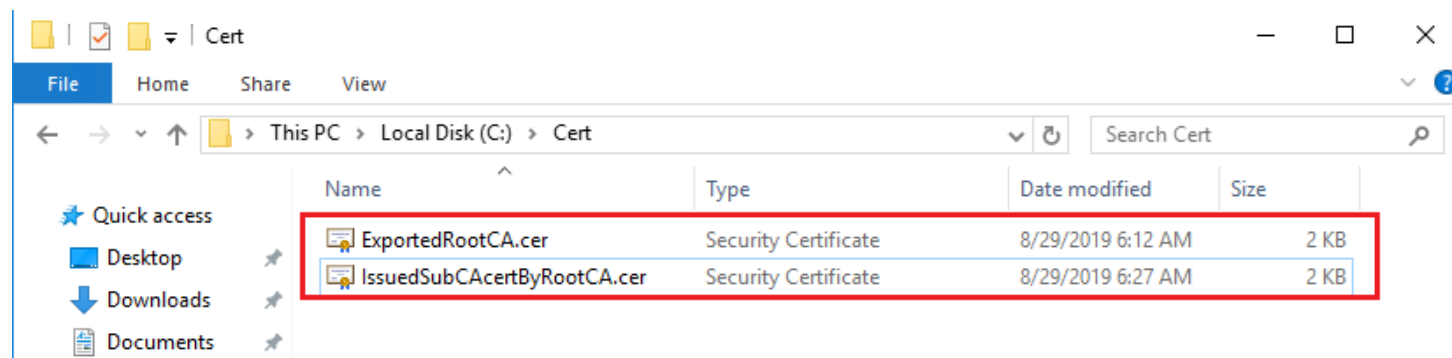
Inštalácia certifikátov

Špecializované IKT systémy Windows

Ing. Stanislav Lukac, PhD.

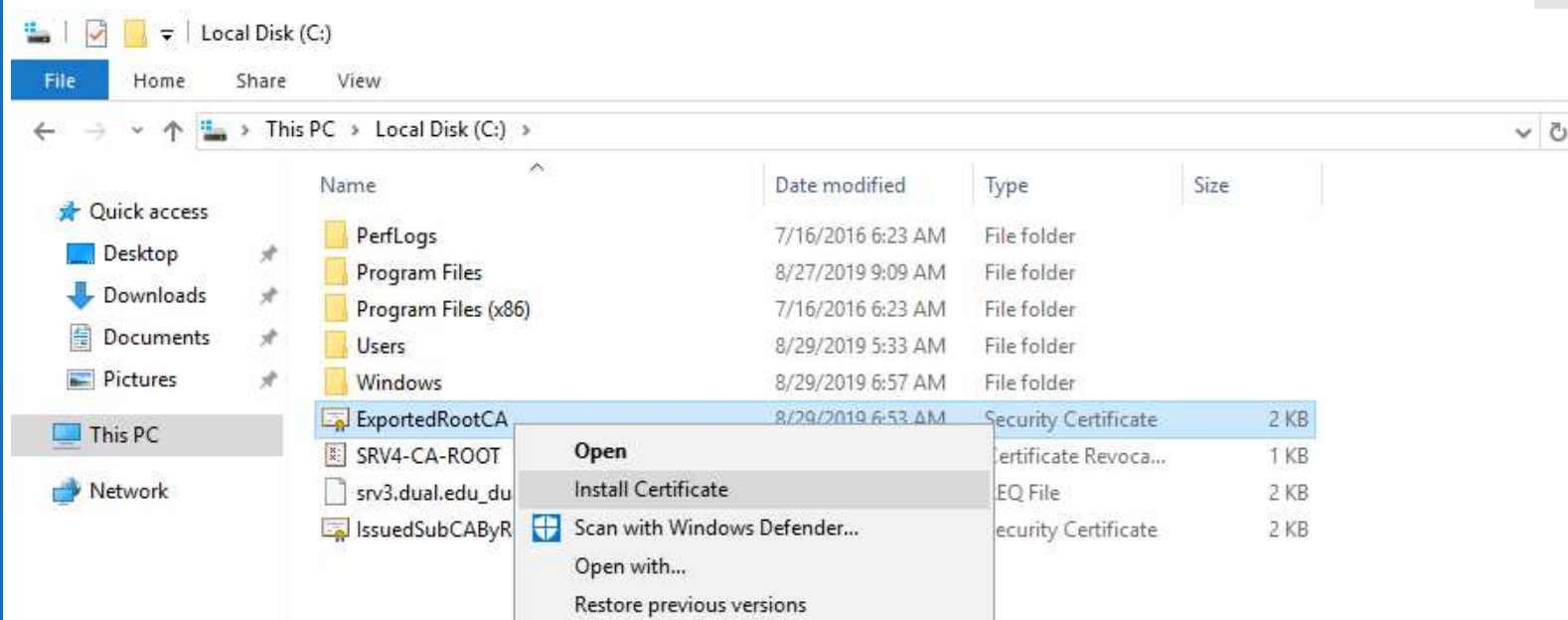
Krok 12

::Inštalácia certifikátov na Subordinate CA



Krok 12

::Inštalácia certifikátov na Subordinate CA



Krok 12

::Inštalácia certifikátov na Subordinate CA

← 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 Cancel

← 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:

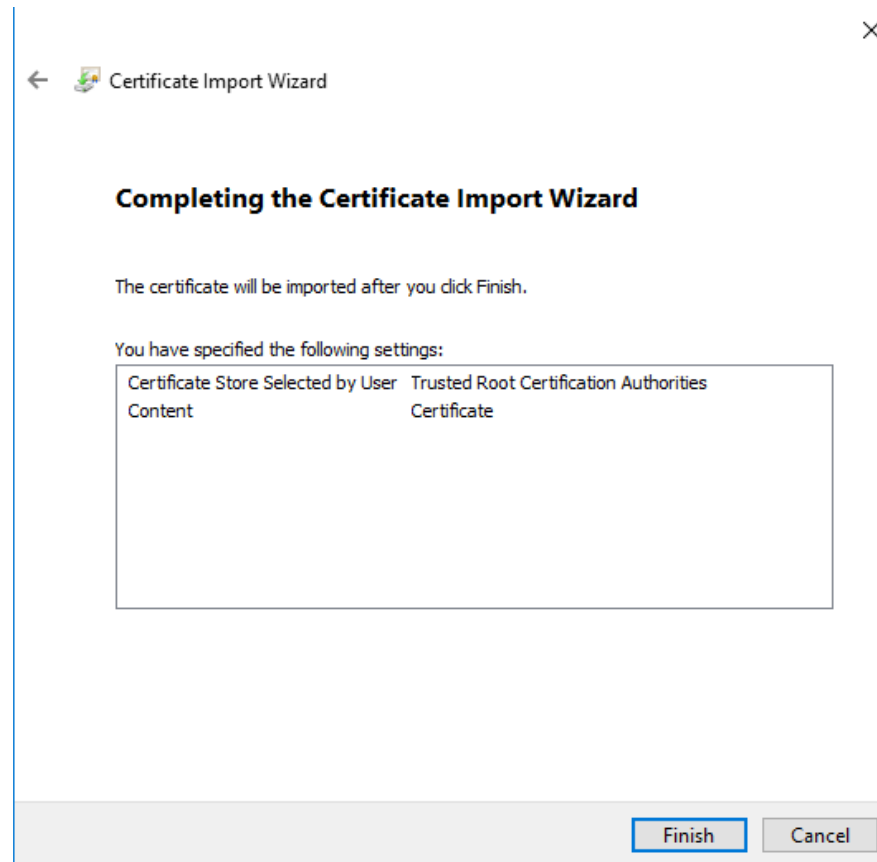
Trusted Root Certification Authorities

Browse...

Next Cancel

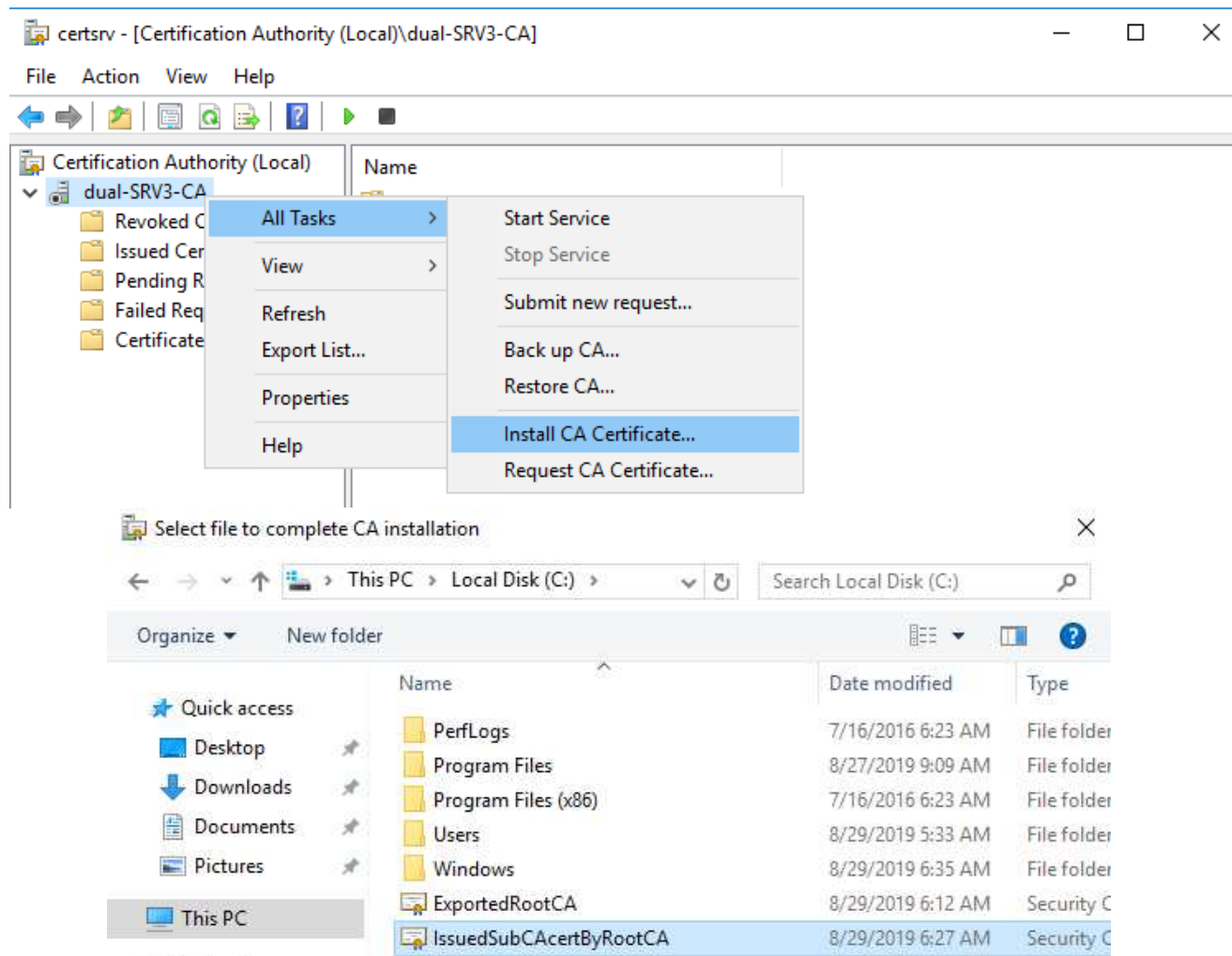
Krok 12

::Inštalácia certifikátov na Subordinate CA



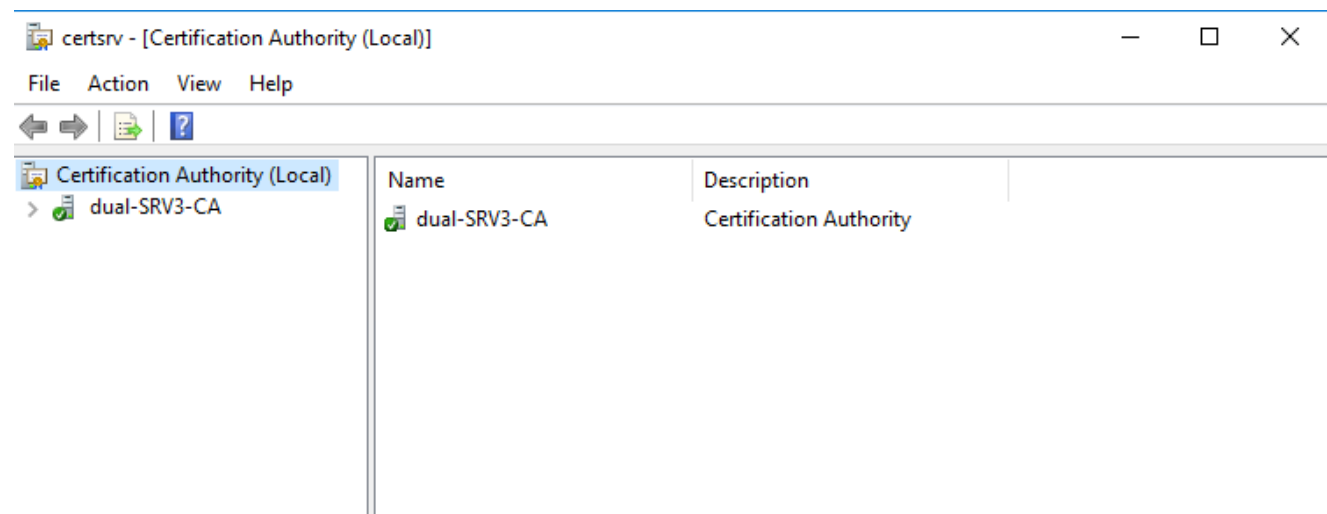
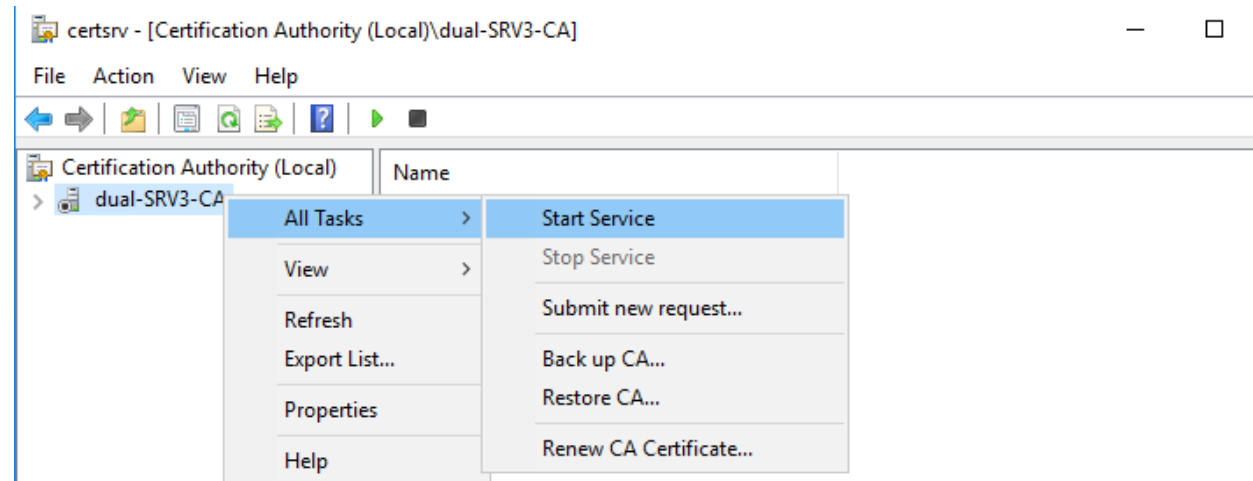
Krok 12

::Inštalácia certifikátov na Subordinate CA



Krok 13

::Start Subordinate CA service



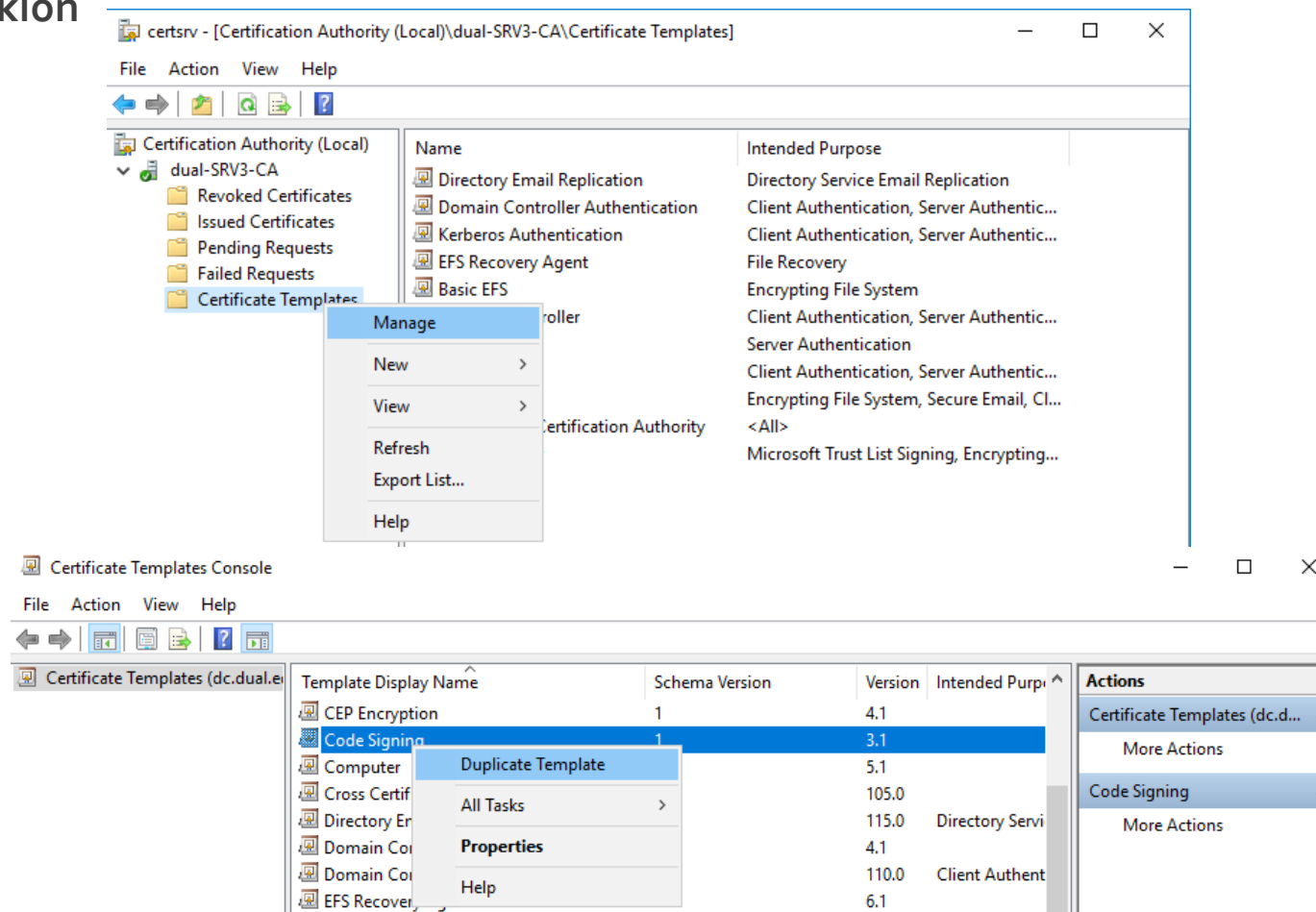
Použitie šablón

Špecializované IKT systémy Windows

Ing. Stanislav Lukac, PhD.

Krok 14

:: Na "issuing" CA vyhladáme príslušnú šablónu a vytvoríme jej klon



Krok 14

:: Na "issuing" CA pripravenie šablóny

Properties of New Template

Subject Name Server Issuance Requirements

Superseded Templates Extensions Security

Compatibility General Request Handling Cryptography Key Attestation

Template display name:
PowerShell Code Signing

Template name:
PowerShellCodeSigning

Validity period: Renewal period:
1 years 6 months

☐ Publish certificate in Active Directory
☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply Help

Properties of New Template

Subject Name Server Issuance Requirements

Superseded Templates Extensions Security

Compatibility General Request Handling Cryptography Key Attestation

Purpose: Signature

☐ Delete revoked or expired certificates (do not archive)
☐ Include symmetric algorithms allowed by the subject
☐ Archive subject's encryption private key

☐ Allow private key to be exported
☐ Renew with the same key (*)
☐ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (*)

Do the following when the subject is enrolled and when the private key associated with this certificate is used:
☒ Enroll subject without requiring any user input
☐ Prompt the user during enrollment
☐ Prompt the user during enrollment and require user input when the private key is used

* Control is disabled due to [compatibility settings](#).

OK Cancel Apply Help

Properties of New Template

Subject Name Server Issuance Requirements

Compatibility General Request Handling Cryptography Key Attestation

Superseded Templates Extensions Security

Group or user names:
Authenticated Users
Administrator
Domain Admins (DUAL\Domain Admins)
Enterprise Admins (DUAL\Enterprise Admins)

Add... Remove

Permissions for Domain Admins

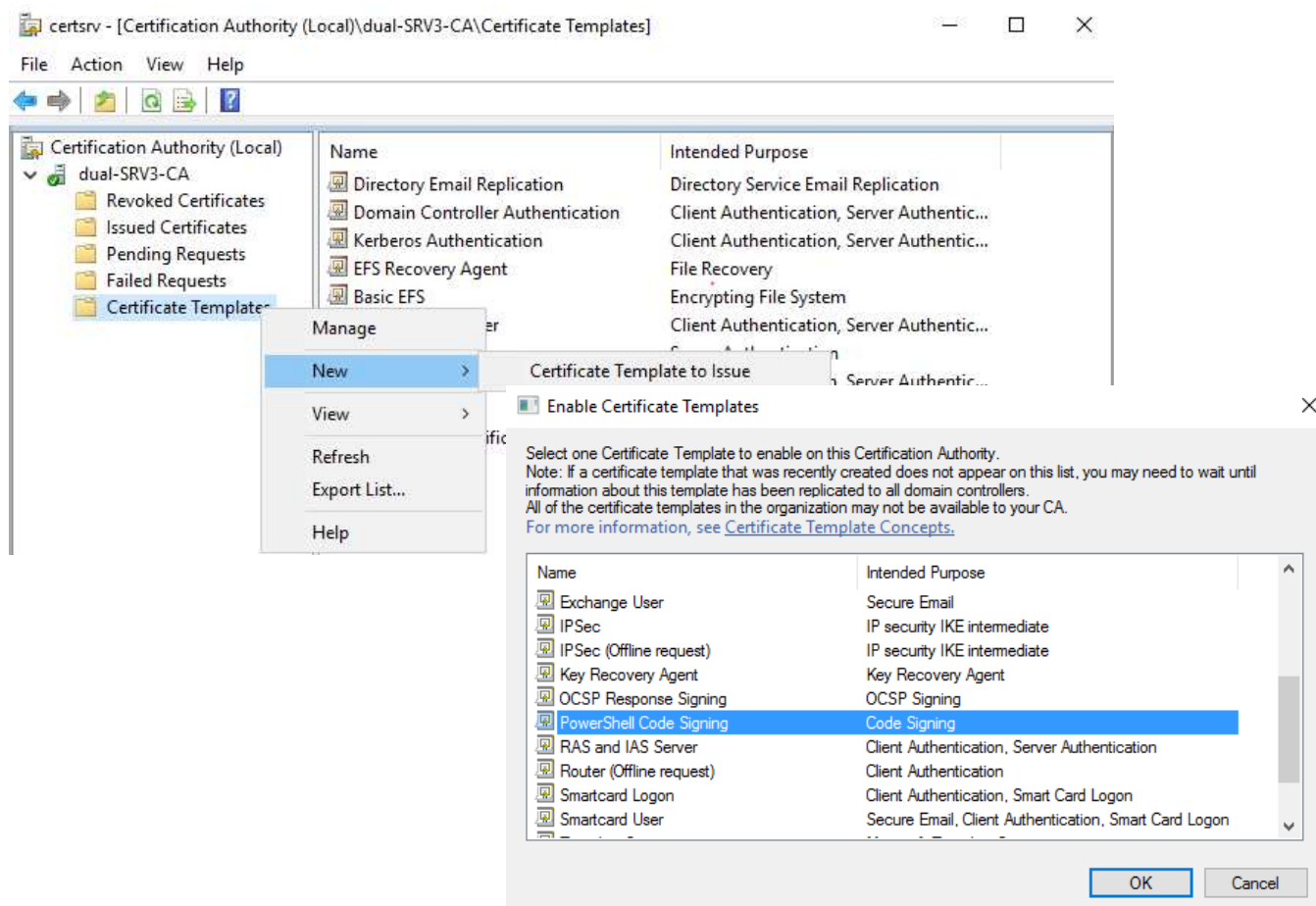
	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

OK Cancel Apply Help

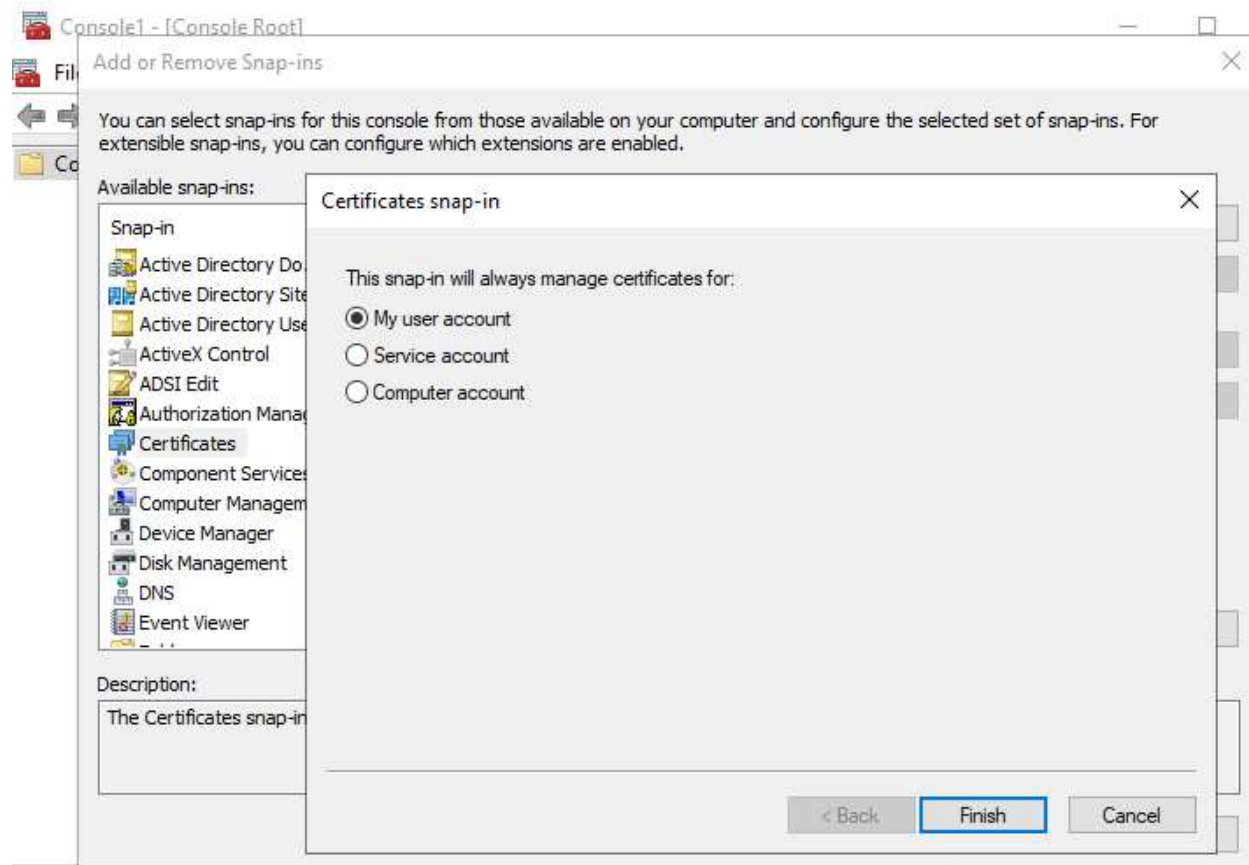
Krok 14

:: Na "issuing" CA pripravenie certifikátu pre enrollment



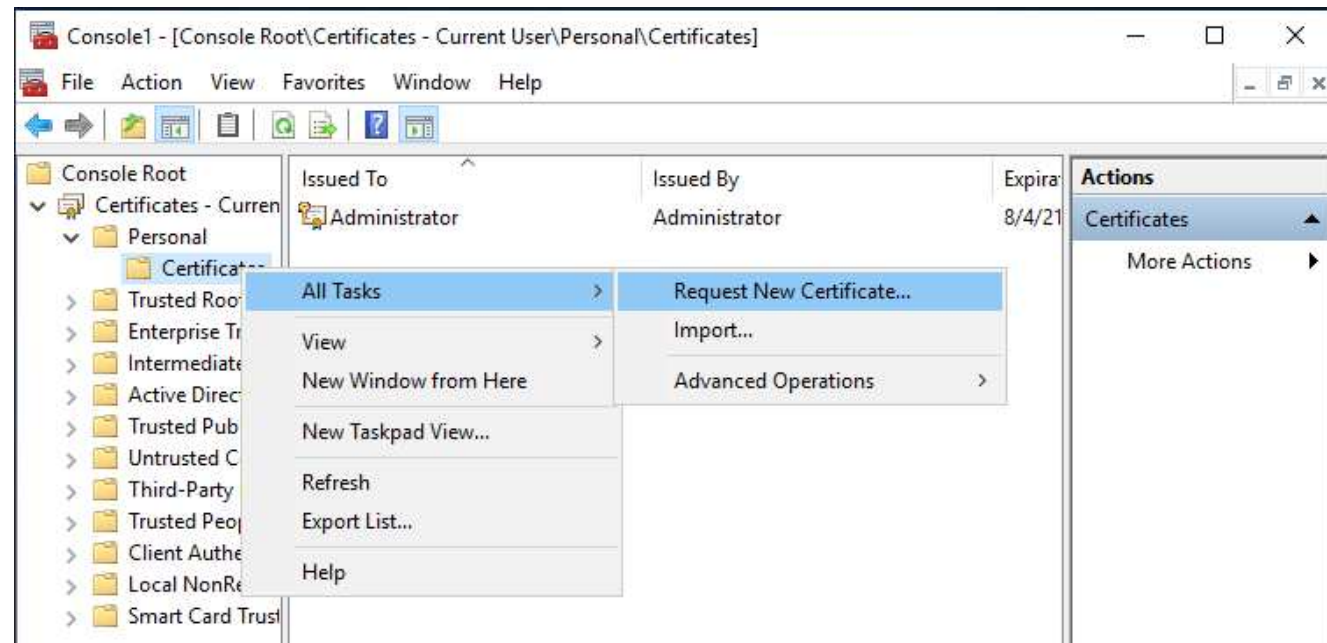
Krok 15

:: Na počítači v doméne s užívateľským účtom, ktorý je členom domain admin vyrequestujeme certifikát



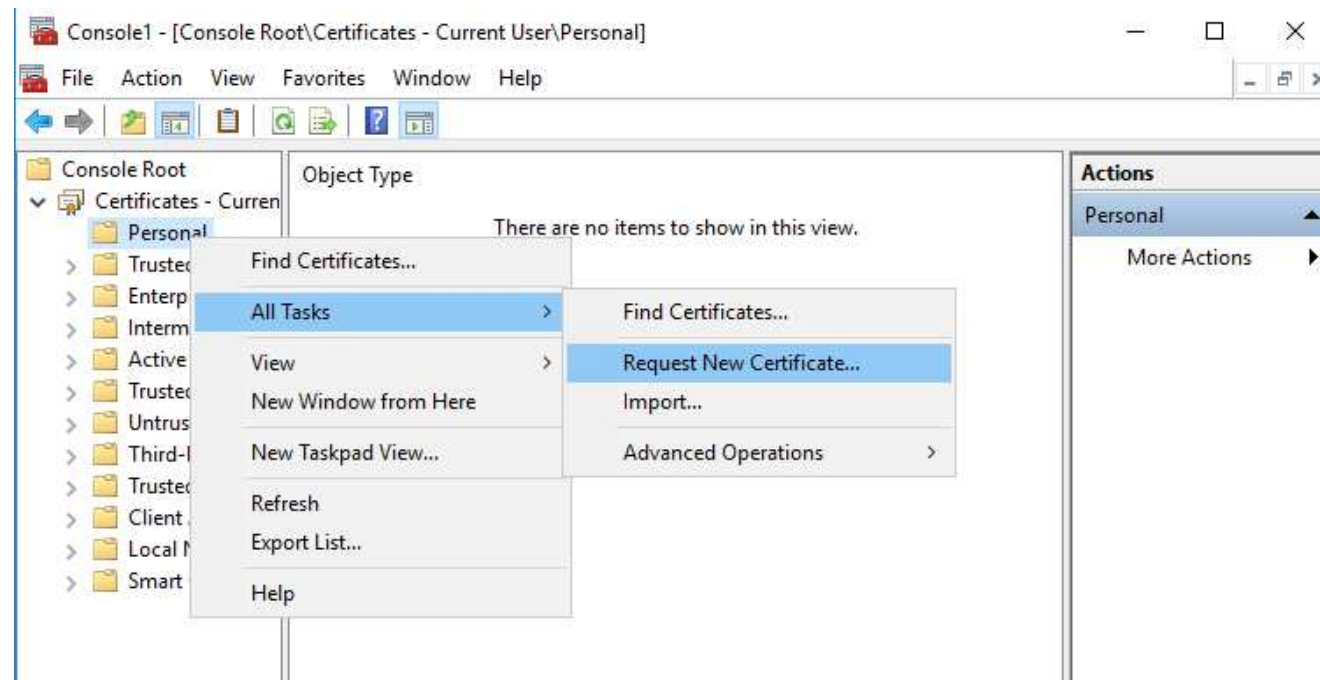
Krok 15

:: Na počítači v doméne s užívateľským účtom, ktorý je členom domain admin vyrequestujeme certifikát



Krok 15

:: Prihlásiť sa s užívateľským účtom na SRV3, ktorý je členom domain admin vyrequestujeme certifikát



Krok 15

:: Prihlásiť sa s užívateľským účtom na SRV3, ktorý je členom domain admin vyrequestujeme certifikát



Certificate Enrollment

Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

Your computer is connected to the network

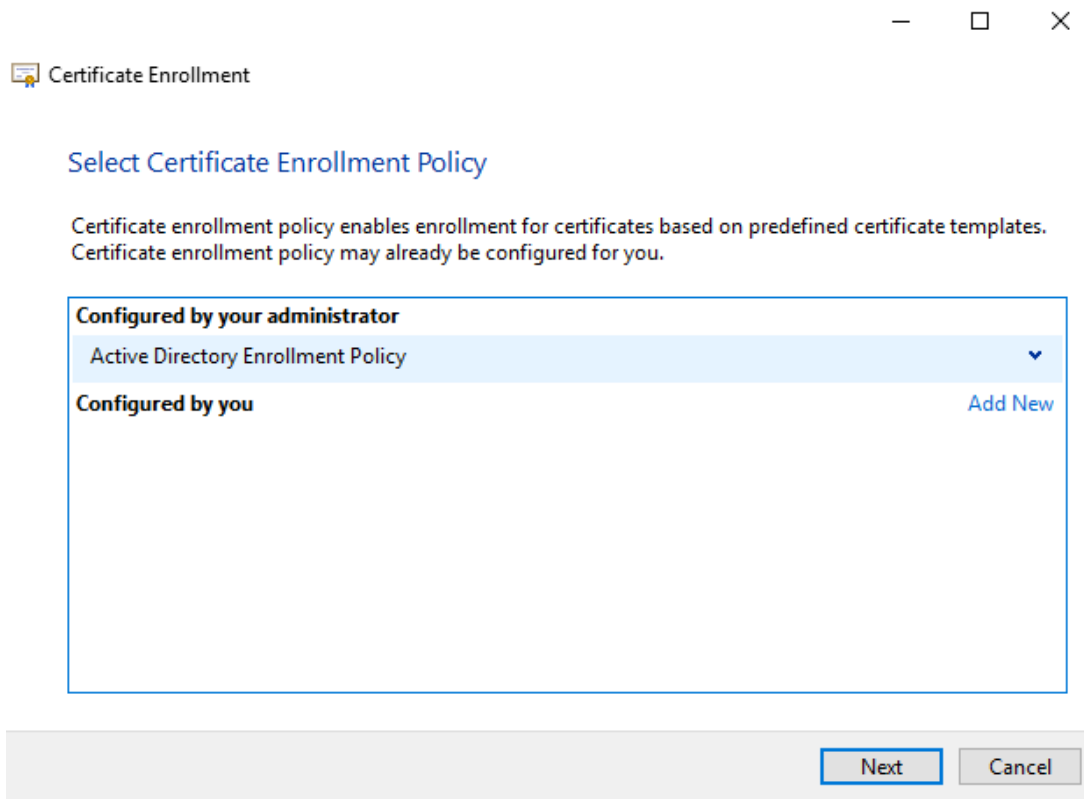
You have credentials that can be used to verify your right to obtain the certificate

Next

Cancel


Krok 15

:: Prihlásiť sa s užívateľským účtom na SRV3, ktorý je členom domain admin vyrequestujeme certifikát



The screenshot shows a Windows-style window titled "Certificate Enrollment". It has standard window controls (minimize, maximize, close) in the top right corner. The main content area is titled "Select Certificate Enrollment Policy" and includes a descriptive paragraph: "Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you." Below this, there is a list box with two sections. The first section, "Configured by your administrator", contains a single item "Active Directory Enrollment Policy" which is currently selected. The second section, "Configured by you", is currently empty. To the right of this section is a link labeled "Add New". At the bottom of the window, there are two buttons: "Next" and "Cancel".

— □ ×

 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 your administrator
Active Directory Enrollment Policy


Configured by you [Add New](#)

Next Cancel

Krok 15






:: Prihlásiť sa s užívateľským účtom na SRV3, ktorý je členom domain admin vyrequestujeme certifikát

— □ ×

 Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy		
<input type="checkbox"/> Administrator	 STATUS: Available	Details ▼
<input type="checkbox"/> Basic EFS	 STATUS: Available	Details ▼
<input type="checkbox"/> EFS Recovery Agent	 STATUS: Available	Details ▼
<input checked="" type="checkbox"/> PowerShell Code Signing	 STATUS: Available	Details ▼
<input type="checkbox"/> User	 STATUS: Available	Details ▼

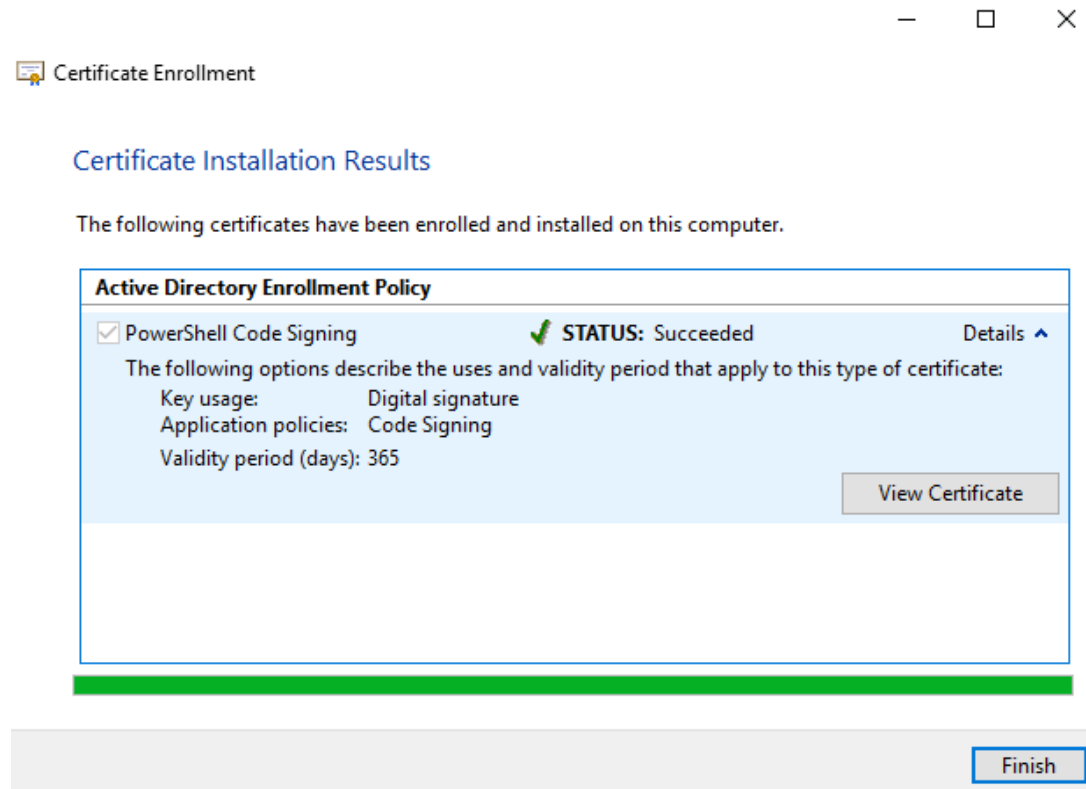
☐ Show all templates

Enroll

Cancel

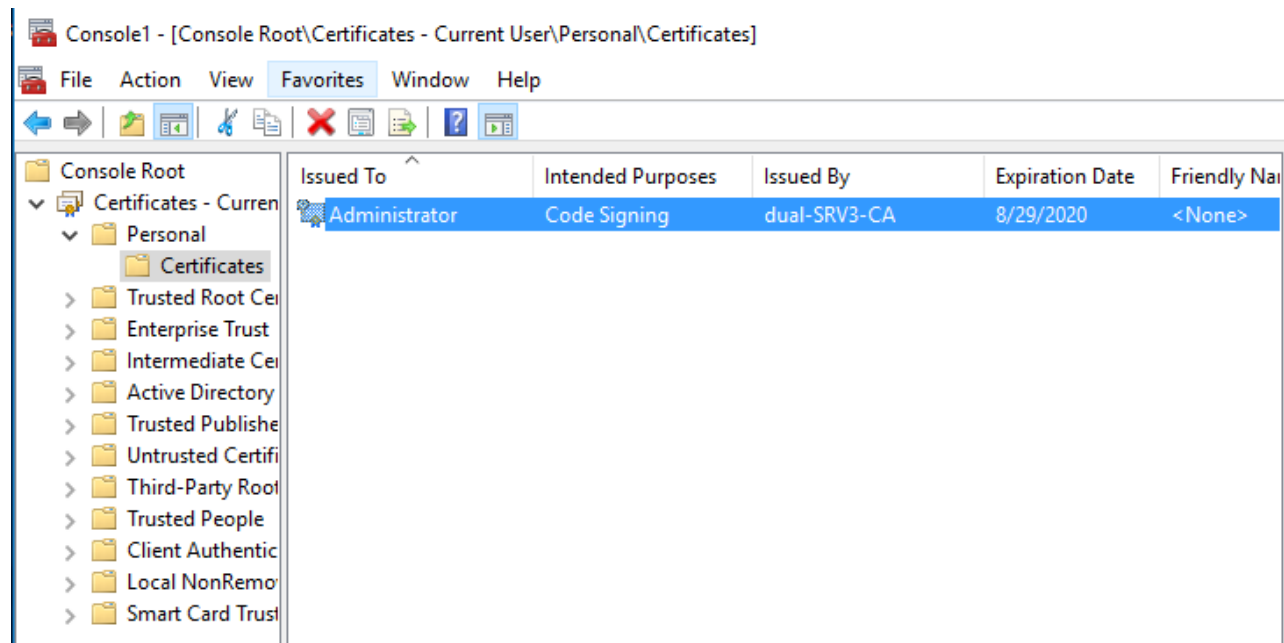
Krok 15

:: Prihlásiť sa s užívateľským účtom na SRV3, ktorý je členom domain admin vyrequestujeme certifikát



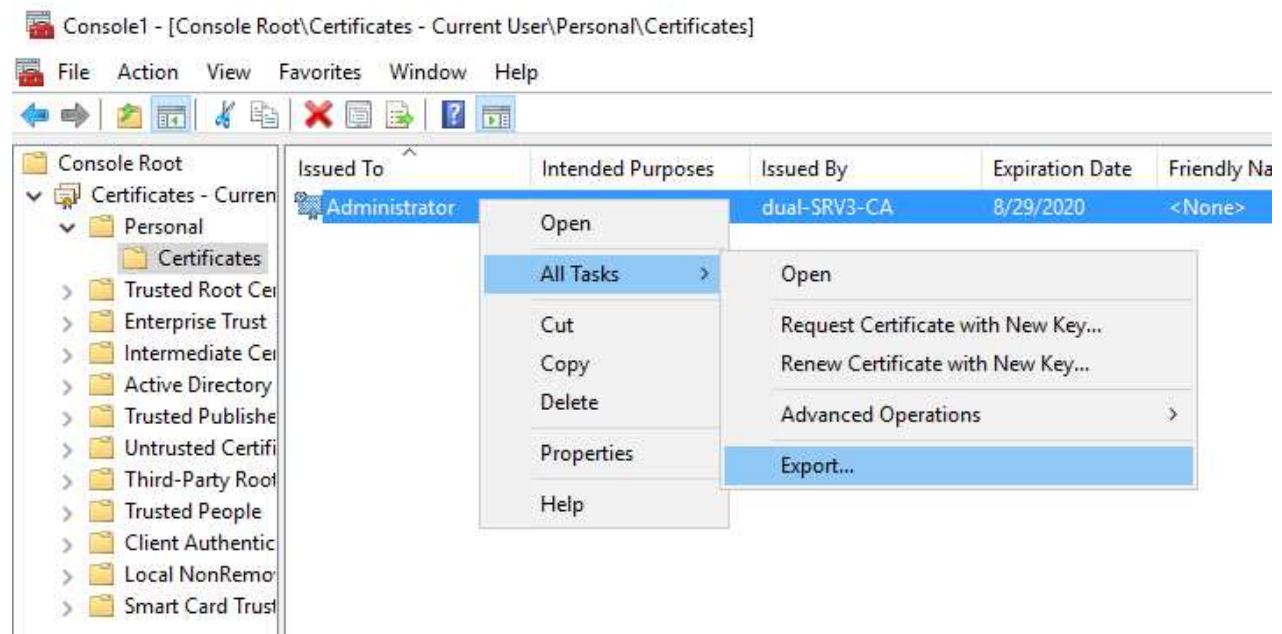
Krok 15

:: Prihlásiť sa s užívateľským účtom na SRV3, ktorý je členom domain admin vyrequestujeme certifikát



Krok 15

:: Publikovanie certifikátu pre podpisovanie PS kódov na „trusted publisher store“



Krok 15

:: Publikovanie certifikátu pre podpisovanie PS kódov na „trusted publisher store“

The image displays three sequential screenshots of the 'Certificate Export Wizard' in a Windows environment. The first screenshot, titled 'Welcome to the Certificate Export Wizard', explains the wizard's purpose and provides instructions to click 'Next'. The second screenshot, titled 'Export Private Key', asks if the user wants to export the private key with the certificate, with 'No, do not export the private key' selected. It also includes a note about non-exportable keys. The third screenshot, titled 'Export File Format', shows options for file formats, with 'Base-64 encoded X.509 (.CER)' selected. Below this, a file explorer window is open, showing the 'Personal Information Exchange - PKCS #12 (.PFX)' folder in the 'My Computer' tree, with the file 'C:\PSScriptSigning.cer' selected. The 'Next' button is highlighted in the bottom right of the wizard window.

← Certificate Export Wizard

Welcome to the Certificate Export Wizard

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

A certificate, which is issued by a certification authority and contains information used to protect data or to establish connections. A certificate store is the system area where certificates are stored.

To continue, click Next.

← 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 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

Note: The associated private key is marked as not exportable. It cannot be exported.

← 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

My Computer > Certificates > Personal Information Exchange - PKCS #12 (.PFX)

C:\PSScriptSigning.cer

Next Cancel

File to Export

Specify the name of the file you want to export

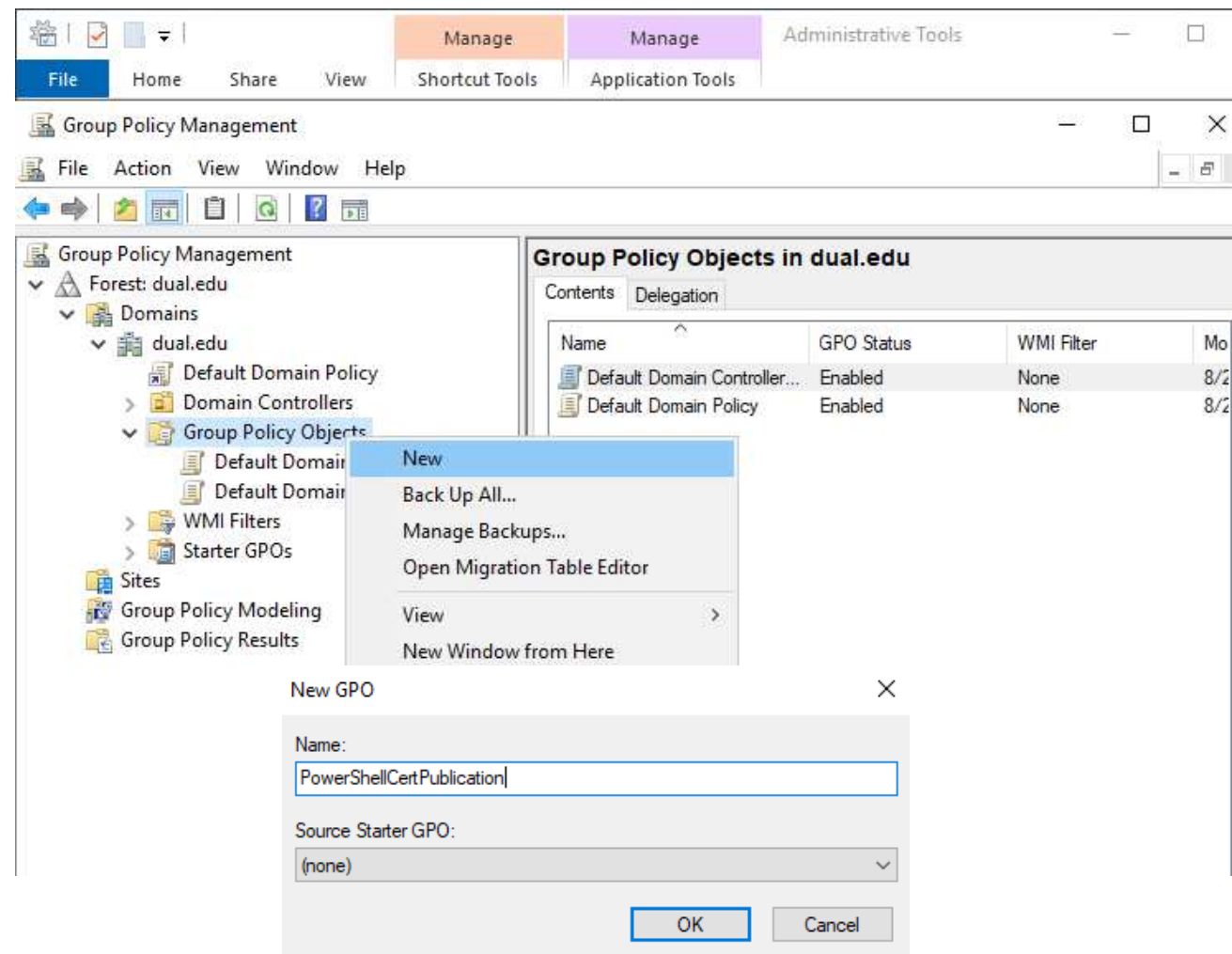
File name:

C:\PSScriptSigning.cer

Browse...

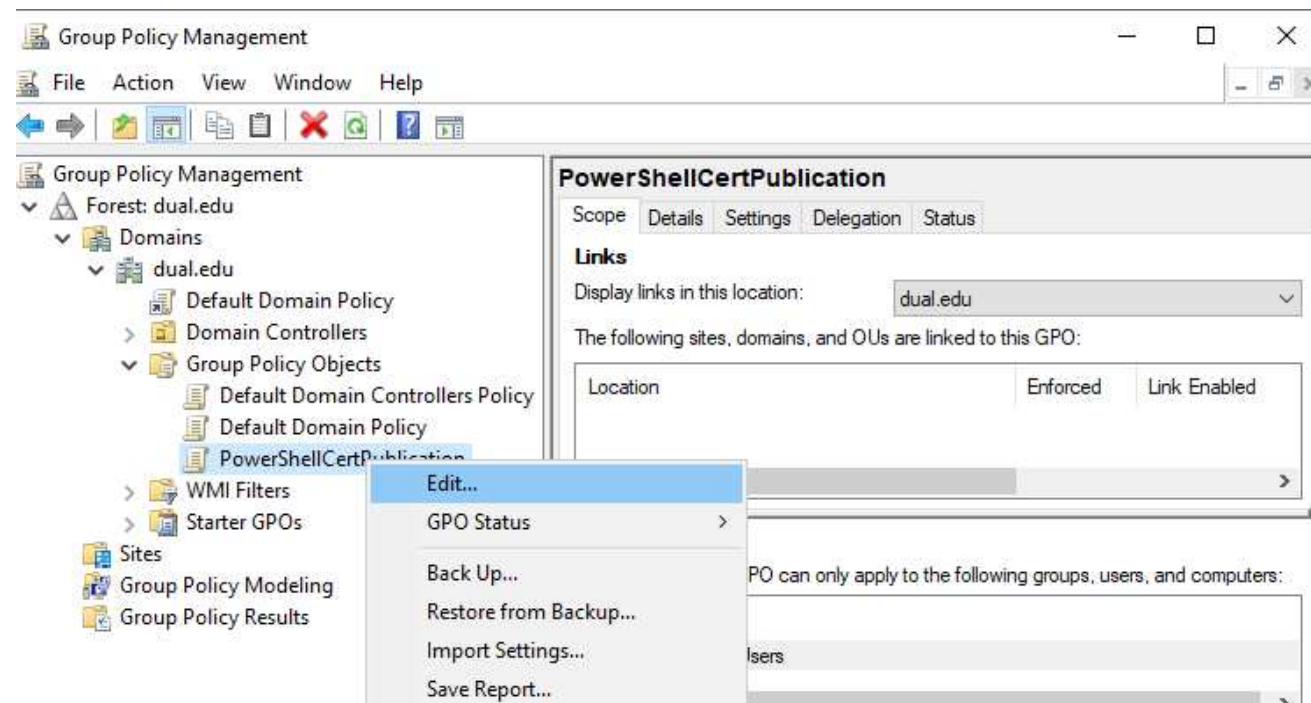
Krok 16

:: Publikovanie v rámci domény cez Group Policy



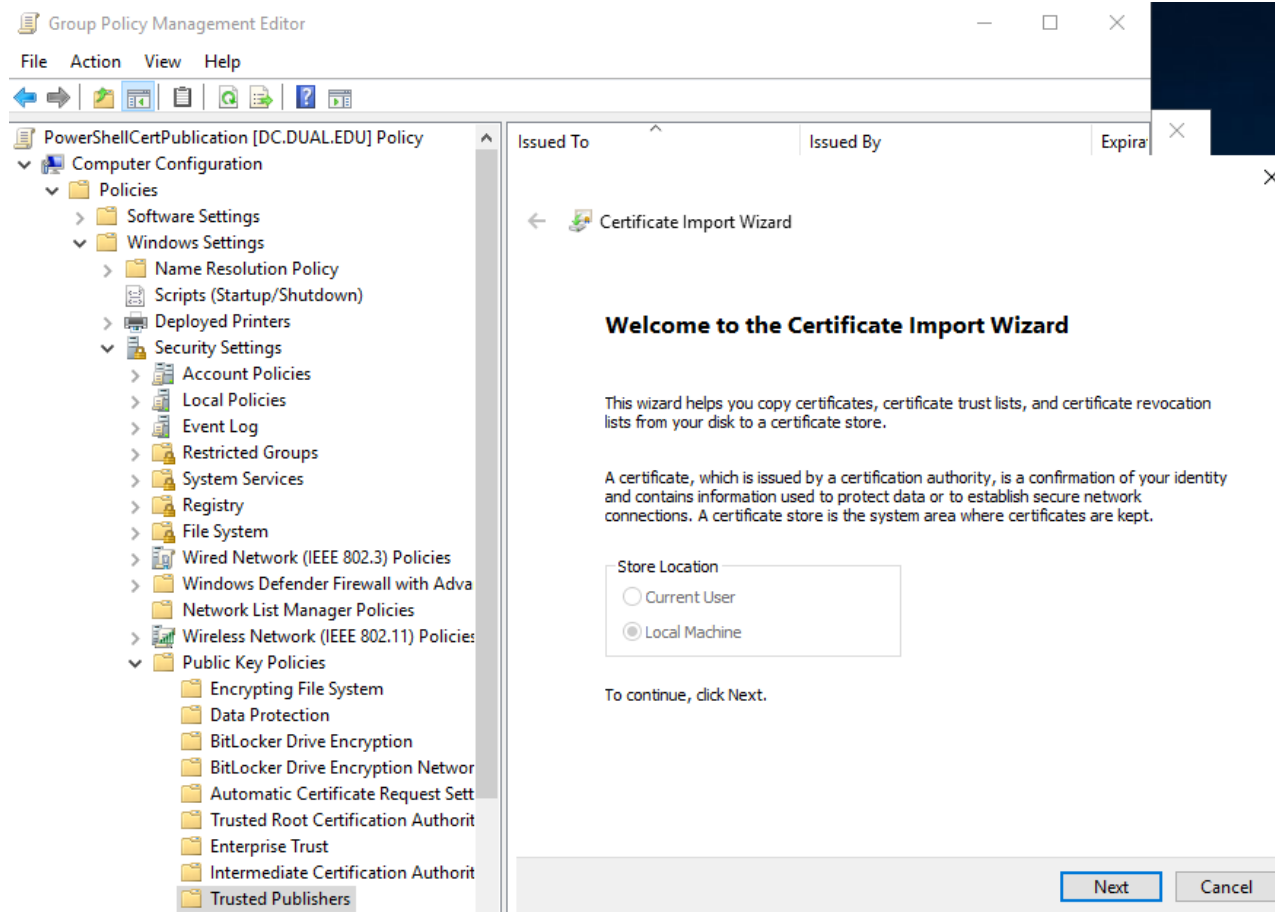
Krok 16

:: Publikovanie v rámci domény cez Group Policy



Krok 16

:: Publikovanie v rámci domény cez Group Policy



Krok 16

:: Publikovanie v rámci domény cez Group Policy

Issued To	Issued By	Expiration Date

← Certificate Import Wizard

File to Import
Specify the file you want to import.

File name:

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)

← 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.

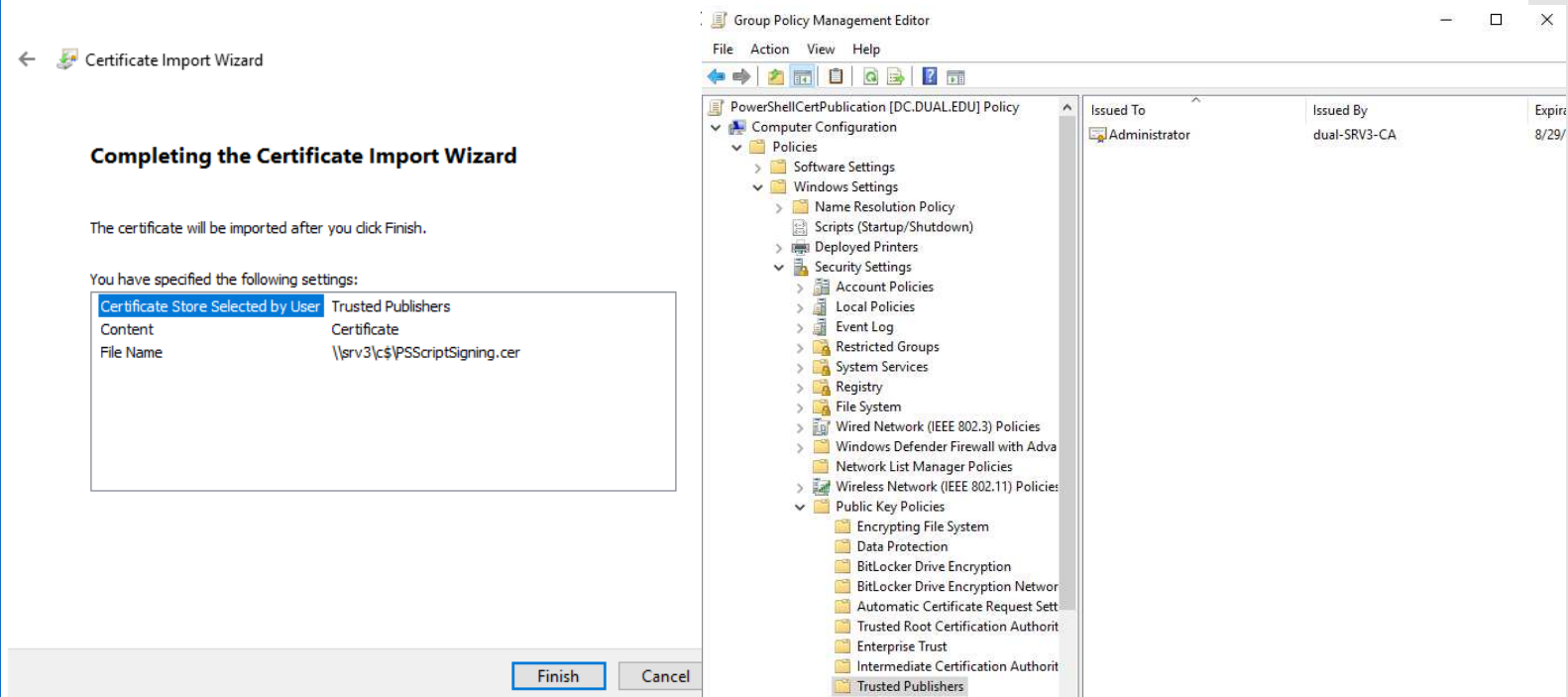
☐ Automatically select the certificate store based on the type of certificate

☒ Place all certificates in the following store

Certificate store:

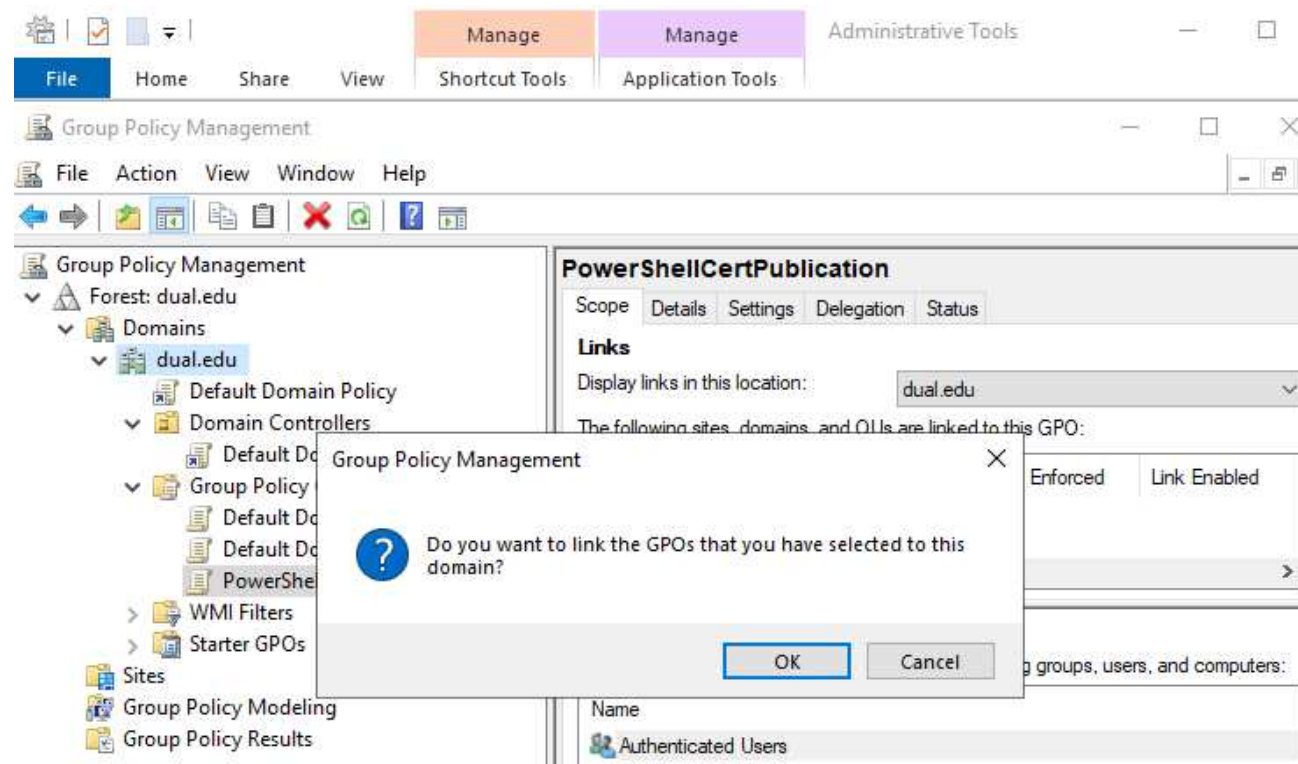
Krok 16

:: Publikovanie v rámci domény cez Group Policy



Krok 16

:: Publikovanie v rámci domény cez Group Policy



Krok 17

:: Získanie certifikátu v PS a podpísanie kódu

Console1 - [Console Root\Certificates - Current User\Trusted Publishers\Certificates]

File Action View Favorites Window Help

Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status
▼ Certificates - Current User	Administrator	dual-SRV3...	8/29/2020	Code Signing	<None>	
▼ Personal						
Certificates						
> Trusted Root Certification Authority						
> Enterprise Trust						
> Intermediate Certification Authority						
> Active Directory User Object						
▼ Trusted Publishers						
Certificates						

Select Administrator: Windows PowerShell

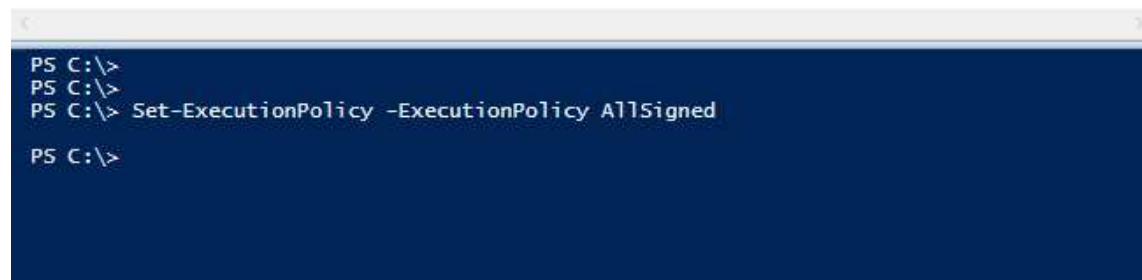
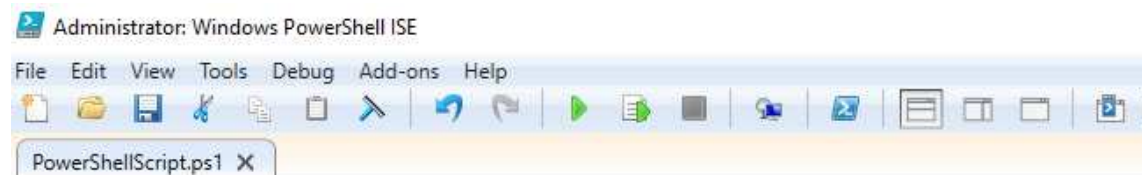
```
PS C:\Users\Administrator>
PS C:\Users\Administrator> dir Cert:\CurrentUser\TrustedPublisher\

PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\TrustedPublisher

Thumbprint                                     Subject
-----
952BCE7FA838265137C184AD347F7E6532B602F3    CN=Administrator, CN=Users, DC=dual, DC=edu
```

Krok 17

:: Získanie certifikátu v PS a podpísanie kódu



Krok 17

:: Získanie certifikátu v PS a podpísanie kódu

```
Mode                LastWriteTime         Length Name
-----
d-----          9/15/2018    9:19 AM          PerfLogs
d-r---          8/27/2019    6:28 PM        Program Files
d-----          8/27/2019    6:41 PM    Program Files (x86)
d-r---          8/27/2019    6:28 PM          Users
d-----          8/27/2019    7:42 PM        Windows
-a----          8/30/2019    5:29 PM           46 PowerShellScript.ps1
```

```
PS C:\> .\PowerShellScript.ps1
.\PowerShellScript.ps1 : File C:\PowerShellScript.ps1 cannot be loaded. The file
C:\PowerShellScript.ps1 is not digitally signed. You cannot run this script on the
current system. For more information about running scripts and setting execution
policy, see about_Execution_Policies at
https://go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\PowerShellScript.ps1
+ ~~~~~
+ CategoryInfo          : SecurityError: (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess
```

```
PS C:\> $cert = dir Cert:\CurrentUser\My\ -CodeSigningCert_
```

```
PS C:\> Set-AuthenticodeSignature -Certificate $cert -FilePath C:\PowerShellScript.ps1
```

Directory: C:\

SignerCertificate	Status	Path
-----	----	----
952BCE7FA838265137C184AD347F7E6532B602F3	Valid	PowerShellScript.ps1

Krok 17

:: Získanie certifikátu v PS a podpísanie kódu

PowerShellScript - Notepad

File Edit Format View Help

Write-Host "Test Script"

Sleep 10

Exit

SIG # Begin signature block

MIIQNgyYJKoZIhvcNAQcCoIIQJzCCECMCAQExCzAJBgUrDgMCGGUAMGkGCisGAQQB

gjcCAQSGWzBZMDQGCisGAQQBgjcCAR4wJgIDAQAABBAfzDtgWUsITrck0sYpfvNR

AgEAAgEAAgEAAgEAAgEAMCEwCQYFKw4DAhoFAAQUOh/0TsHpZu47c08UHftoywc

IEyggg2mMIIGoJCCBIqgAwIBAgITZAAAAAMZAU0shb3v3gAAAAAAzANBgkqhkiG

9w0BAQsFADBCMRMwEQYKCIImiZPyLQBGryDZWR1MRQwEgYKCIImiZPyLQBGryE

ZHVhbDEVMBMGA1UEAxMMZHVhbC1TU1YzLUNBMB4XDTE5MDgzMDE0NTIyNloXDTEw

MDgyOTE0NTIyNlowUzETMBEGCgmSJomT8ixkARkWA2VkdTEUMBIGCgmSJomT8ixk

ARkWBGR1YWwxDjAMBGNVBAMTBVZzZXJzMRywFAYDVQQDEw1BZG1pbmlzdHJhdG9y

MIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsGCYCN+1G62kYQIzsAZm

4Tcwb8H8jvQo14pmZICw1pRSzRF1jHnzcUue14aE9gcZqceitBW9FdYr930UYs

4jR+JP1e6CH6Y2AwqjH4eAwNdF++XAeyVuDzSgjF+8GyK1WoAMcHP18wlv+V3/h0

0YYAuThBAxDwJYPLCrraSjDc3zTLPTqUV8BFoH3I6BUeb/xMvm1HX10jQ4/GdfK4

zrgM01Z6L+gCM87rHI/ypqhUbcy1CzTS6o/LBRGjgcNOgB03T0nBnYYWnBrQWRMb

MZT+tmgz5H4eurBXGtugK0nEp0txPPyXMZAVYUgZ0ey+Amjxmpch3IjHgK7YNHmL

awIDAQAB04ICfjCCAnowPgYJKwYBBAGCNxUHBDEwLwYnKwYBBAGCNxUIgsD4PoS/

9EuBoYkyhNCGZ4PqhyiBbYSv3TqC5451AgFkAgEDMBMGA1UdJQQMAoGCCsGAQUF

BwMDMA4GA1UdDwEB/wQEAwIHgDABBgkrBgEEAYI3FQoEDjAMMAoGCCsGAQUFBwMD

MB0GA1UdDgQWBBSad2AbfphVyLiuiq0wRTgnhkWhhDAfBgNVHSMEGDAWgBTmrWdr

vzJ35vpoR50L3LZymoxDkjCBxAYDVR0fB1G8MIG5MIG2oIGzoIGwhoGtbGRhcDov

Ly9DTj1kdWFsLVNSVjMtQ0EsQ049c3J2MyxDTj1DRFAsQ049UHViBGljJTlW52V5

NEXT

::Install ONLINE responder

<https://www.tech-coffee.net/public-key-infrastructure-part-8-ocsp-responder/>

::Configure PS cert for script signing

<https://devblogs.microsoft.com/scripting/hey-scripting-guy-how-can-i-sign-windows-powershell-scripts-with-an-enterprise-windows-pki-part-1-of-2/>

https://sysadminplus.blogspot.com/2016/08/stop-running-unsecure-scripts-how-to_21.html

<https://redmad.com/pki/sign-powershell-scripts-enterprise-pki/#!>

<https://www.darkoperator.com/blog/2013/3/5/powershell-basics-execution-policy-part-1.html>

::Configure cert for HTTPS Web

<https://www.petri.com/enable-https-certificate-authority-web-enrollment-windows-server-2008-2012>

<https://www.petri.com/enable-https-certificate-authority-web-enrollment-windows-server-2008-2012>