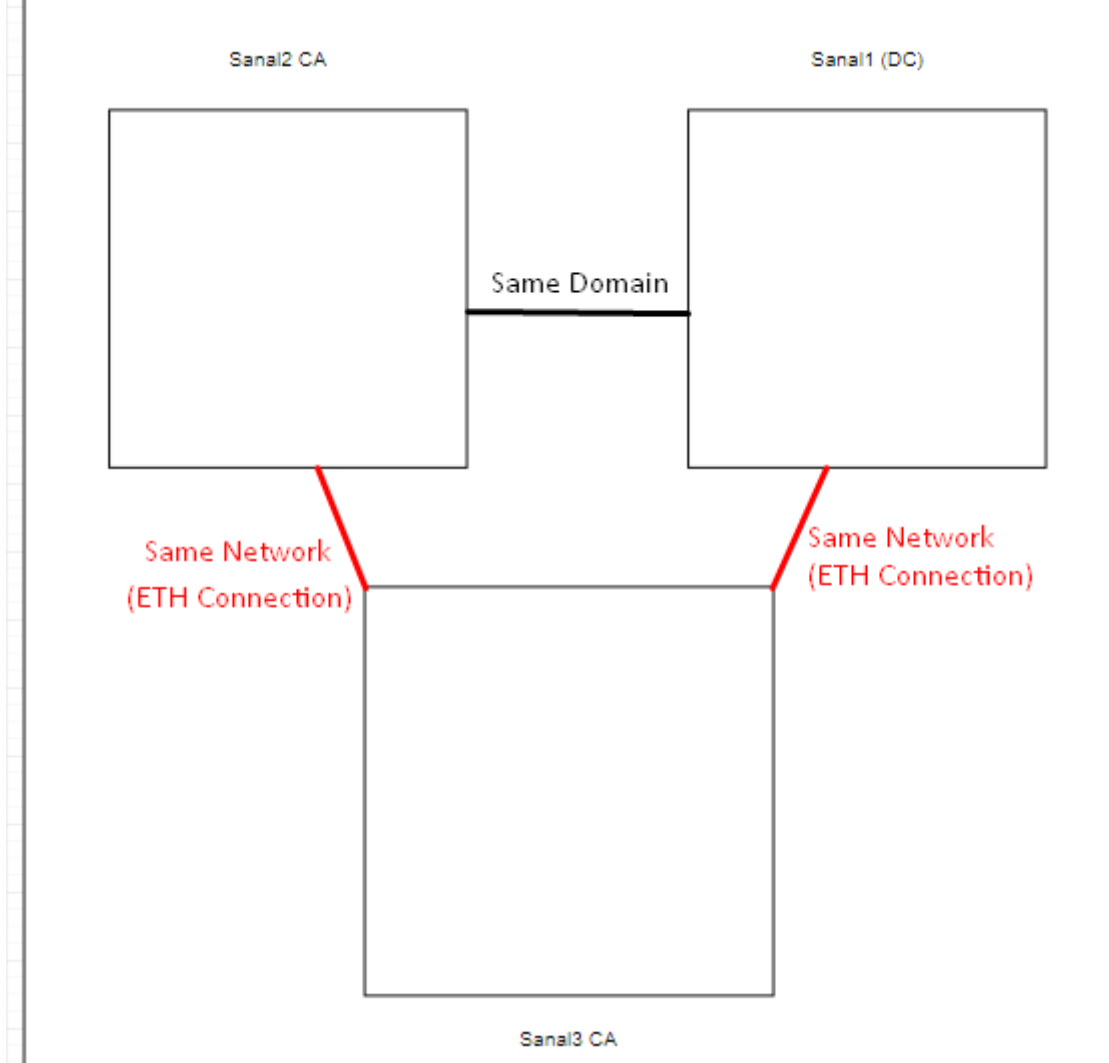


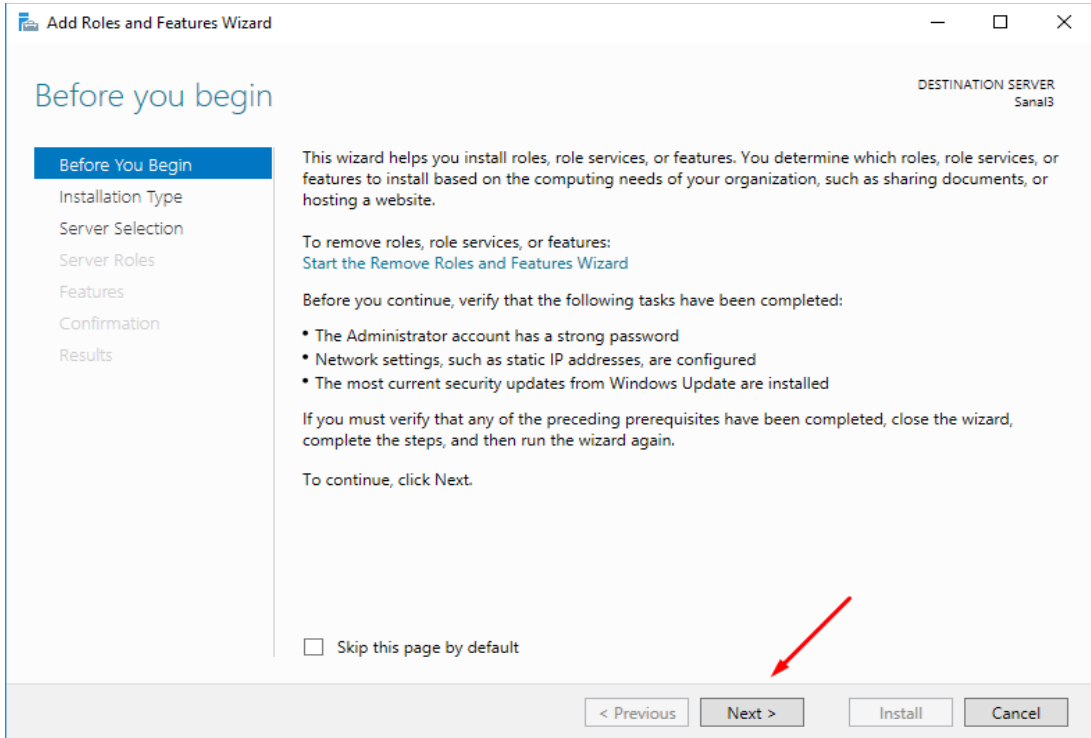
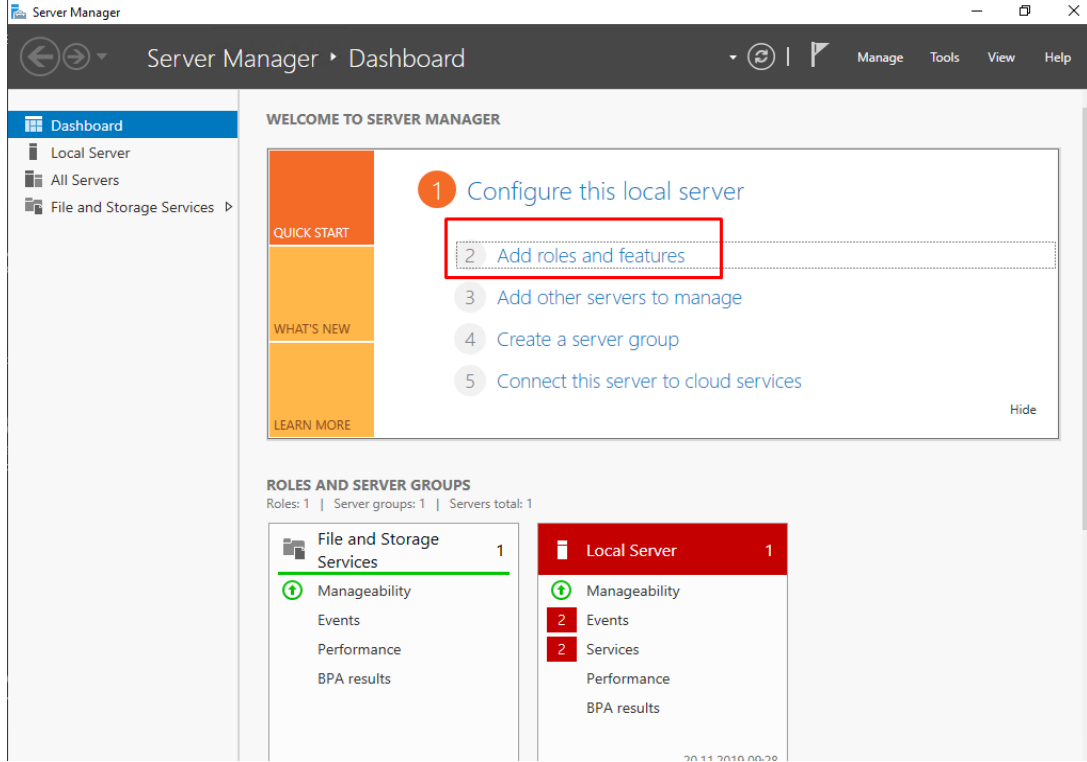
Active Directory Certificate Services

Bu proje için Windows Server 2016 ile 3 farklı cihazla birlikte Active Directory'de şirket/domain içinde ki kullanıcıların giriş yapabilmesi için sertifika vericez.

Domain içinde olmayan Sanal3 cihazı sertifikanın kurulacağı cihaz olup, aynı domain içinde olan Sanal1 adlı cihaz Domain Controller (DC) olup Sanal2 cihazı Sanal3 cihazından sertifikayı alıp DC ile kullanıcılara vermekle yükümlü olacaktır. Sanal3 cihazının domain içinde olmaması sertifikanın korunumu ve güvenliği içindir. Tüm cihazlar aynı network'tedir ve birbirleri ile haberleşebilmektedirler.



İşlem1 : İlk olarak Sanal3 cihazına (Sertifikanın kurulacağı cihaz) sertifika oluşturmak için “Active Directory Certificate Services” indirilir. Bunun için aşağıdaki adımlar takip edilir.



Add Roles and Features Wizard

Select installation type

DESTINATION SERVER
Sanal3

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

☒ **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

☐ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous

Next >

Install

Cancel

Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
Sanal3

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select a server or a virtual hard disk on which to install roles and features.

☒ Select a server from the server pool

☐ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
Sanal3	10.10.10.5	Microsoft Windows Server 2016 Datacenter Evaluation

1 Computer(s) found

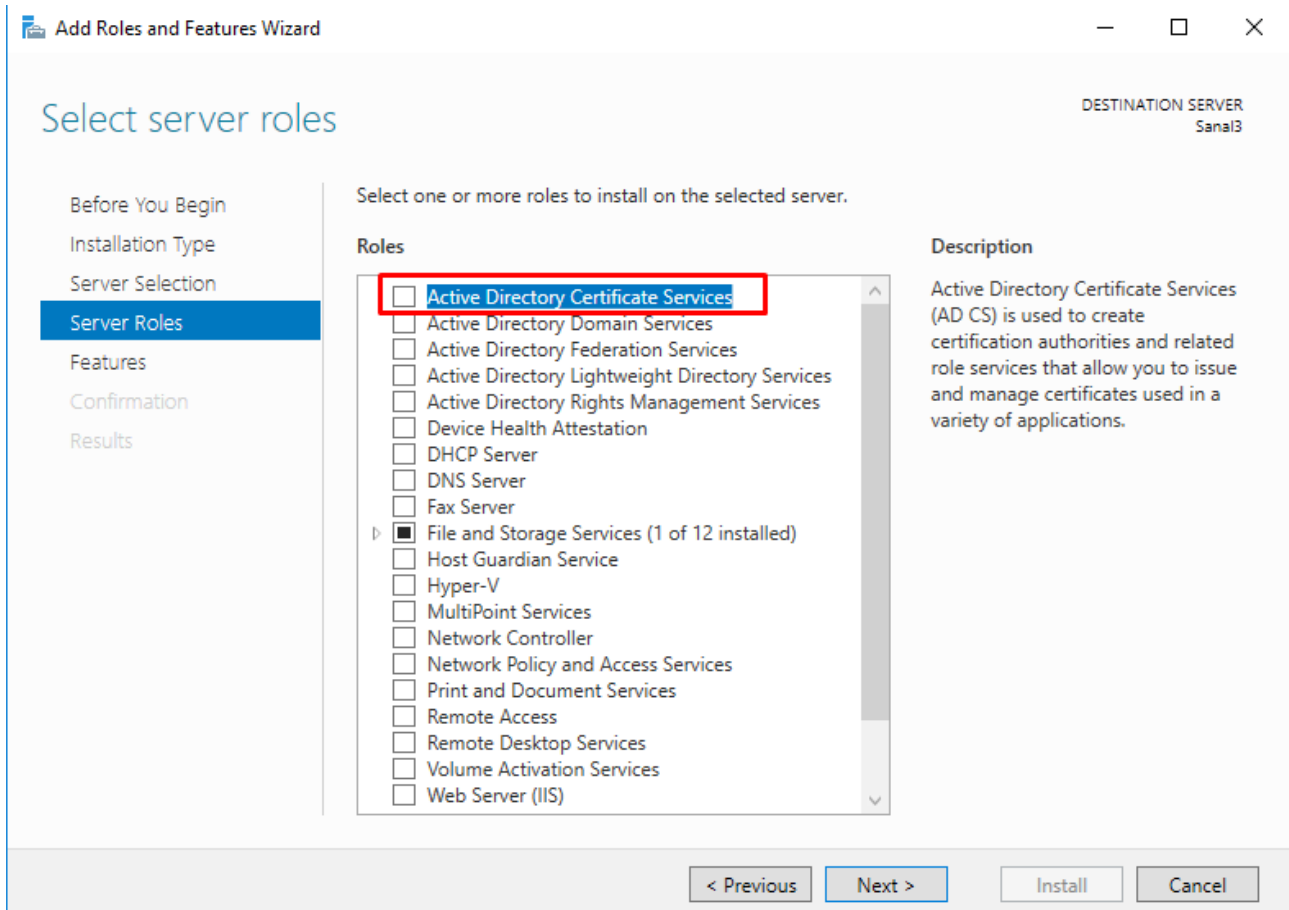
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous

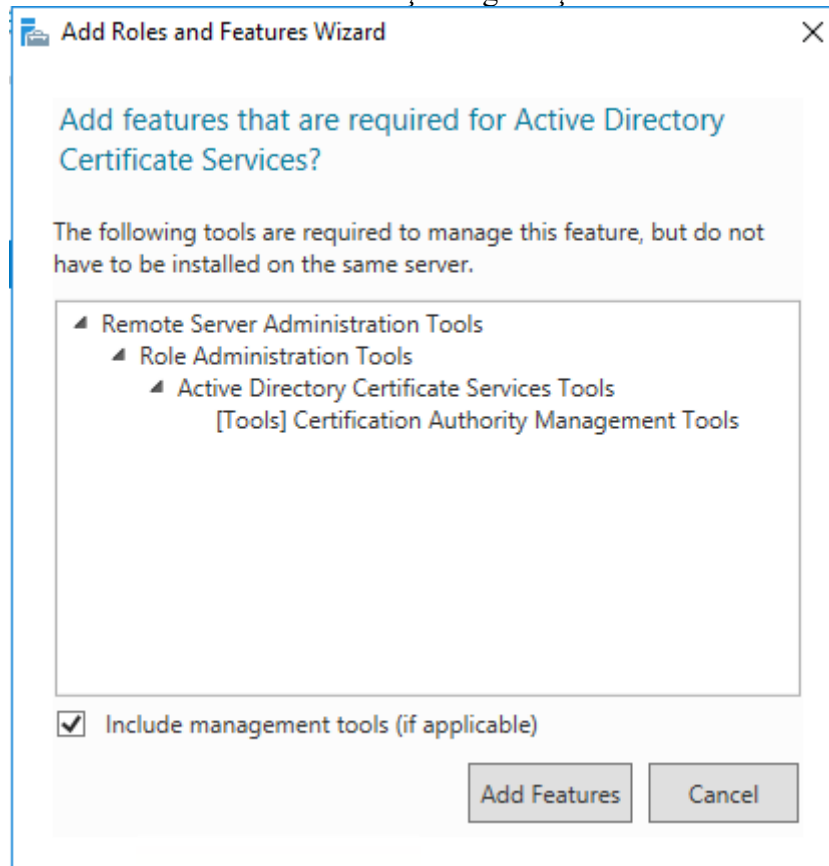
Next >

Install

Cancel



- Add Features ile Tool'lar eklenir ve tik işareti gelmiş olur.



Add Roles and Features Wizard

DESTINATION SERVER
Sanal3

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 certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
<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 Attestation	
<input type="checkbox"/> DHCP Server	
<input type="checkbox"/> DNS Server	
<input type="checkbox"/> Fax Server	
<input checked="" type="checkbox"/> File and Storage Services (1 of 12 installed)	
<input type="checkbox"/> Host Guardian Service	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> MultiPoint Services	
<input type="checkbox"/> Network Controller	
<input type="checkbox"/> Network Policy and Access Services	
<input type="checkbox"/> Print and Document Services	
<input type="checkbox"/> Remote Access	
<input type="checkbox"/> Remote Desktop Services	
<input type="checkbox"/> Volume Activation Services	
<input type="checkbox"/> Web Server (IIS)	

< Previous Next > Install Cancel

- Select Features altında herhangi bir şey işaretlenmeden devam edilir.

Add Roles and Features Wizard

DESTINATION SERVER
Sanal3

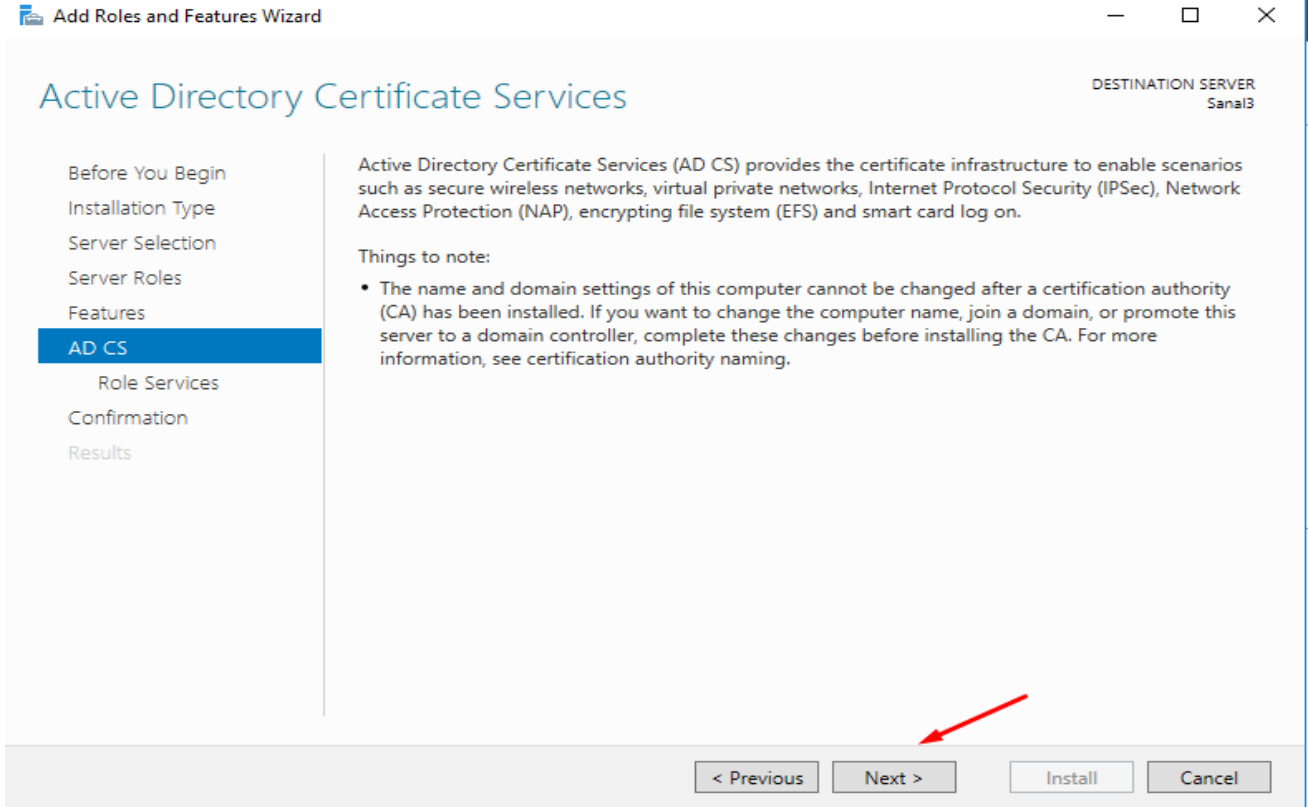
Select features

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

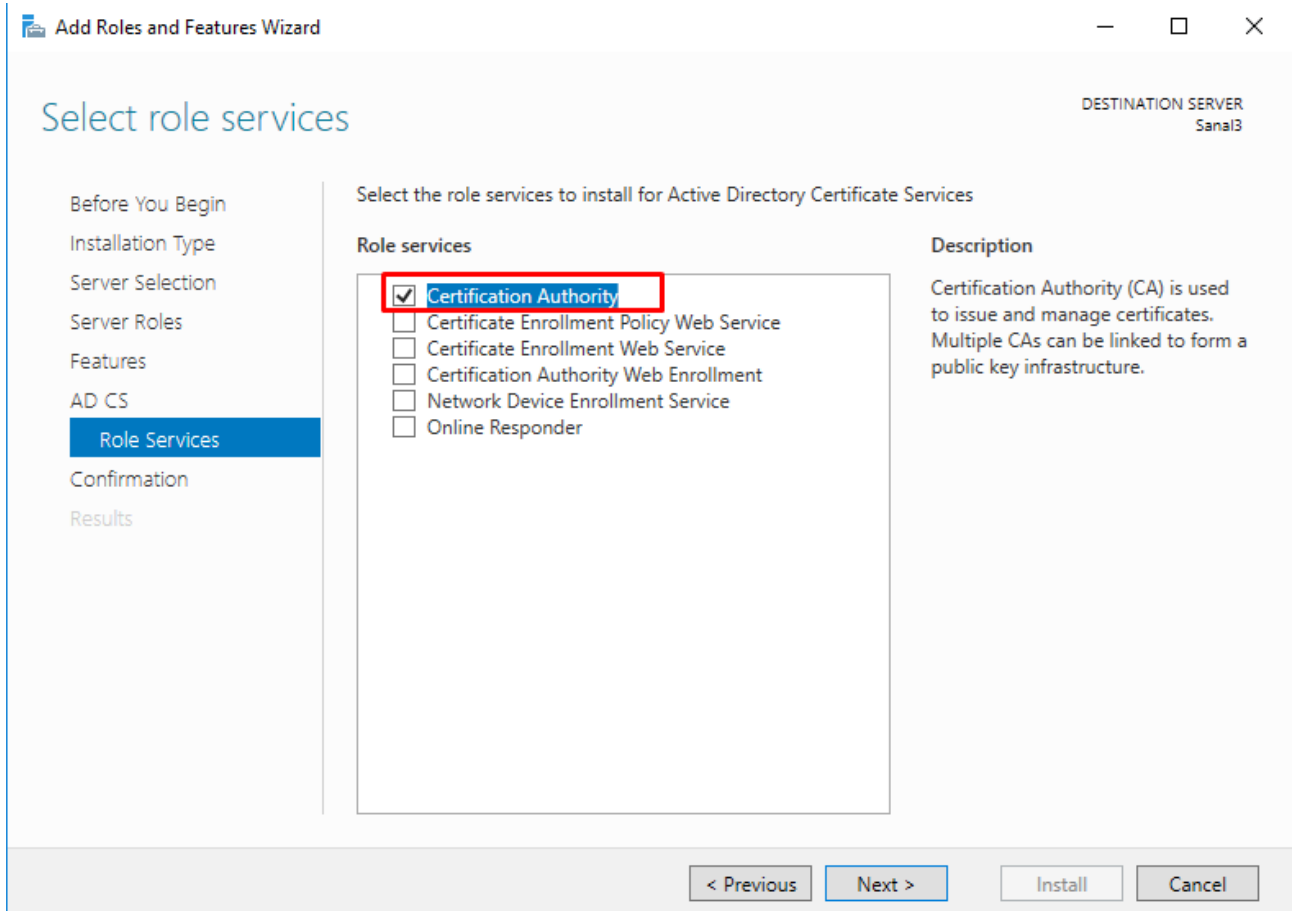
Select one or more features to install on the selected server.

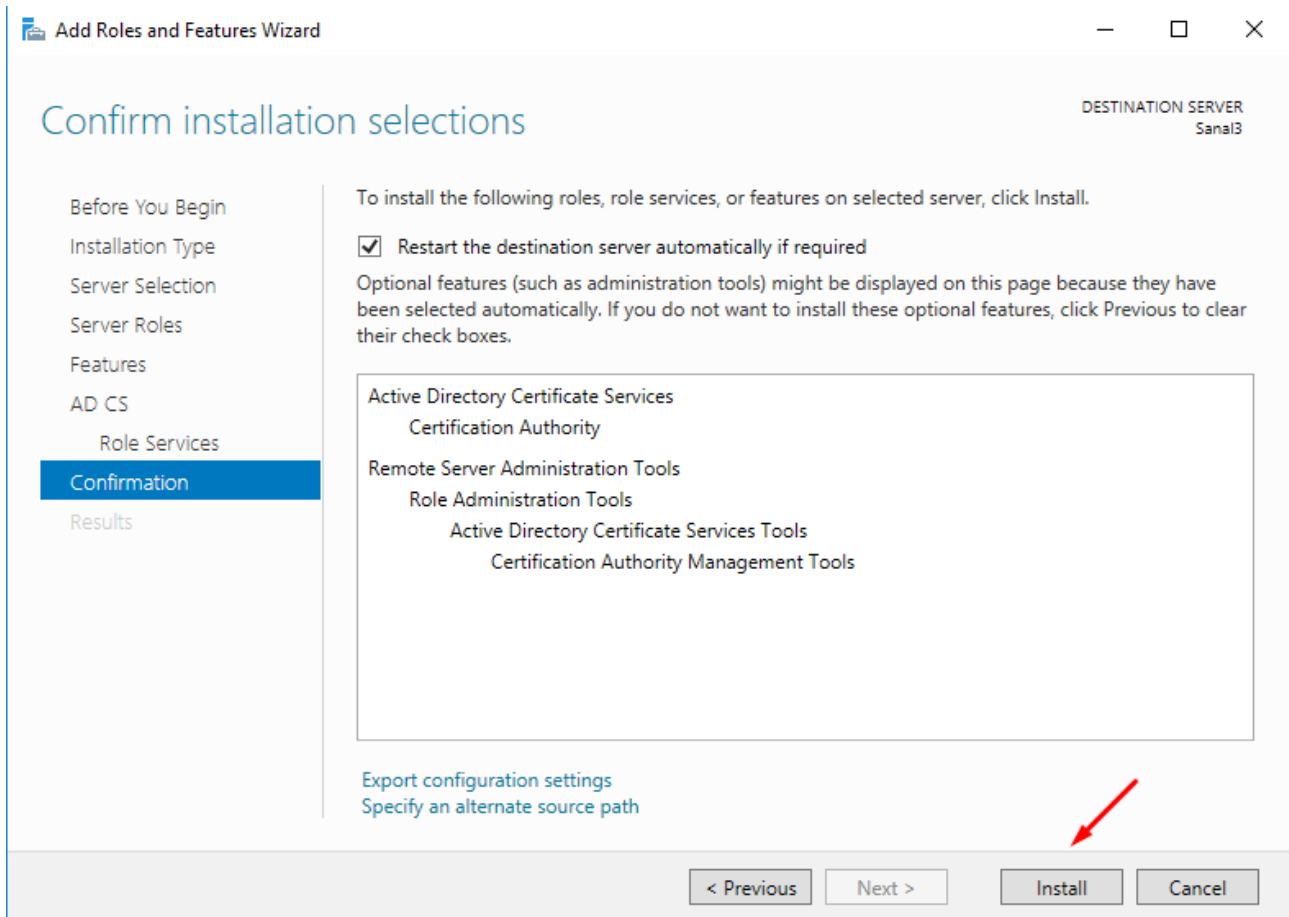
Features	Description
<input type="checkbox"/> .NET Framework 3.5 Features	.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
<input checked="" type="checkbox"/> .NET Framework 4.6 Features (2 of 7 installed)	
<input type="checkbox"/> Background Intelligent Transfer Service (BITS)	
<input type="checkbox"/> BitLocker Drive Encryption	
<input type="checkbox"/> BitLocker Network Unlock	
<input type="checkbox"/> BranchCache	
<input type="checkbox"/> Client for NFS	
<input type="checkbox"/> Containers	
<input type="checkbox"/> Data Center Bridging	
<input type="checkbox"/> Direct Play	
<input type="checkbox"/> Enhanced Storage	
<input type="checkbox"/> Failover Clustering	
<input type="checkbox"/> Group Policy Management	
<input type="checkbox"/> Host Guardian Hyper-V Support	
<input type="checkbox"/> I/O Quality of Service	
<input type="checkbox"/> IIS Hostable Web Core	
<input type="checkbox"/> Internet Printing Client	
<input type="checkbox"/> IP Address Management (IPAM) Server	
<input type="checkbox"/> iSNS Server service	

< Previous Next > Install Cancel

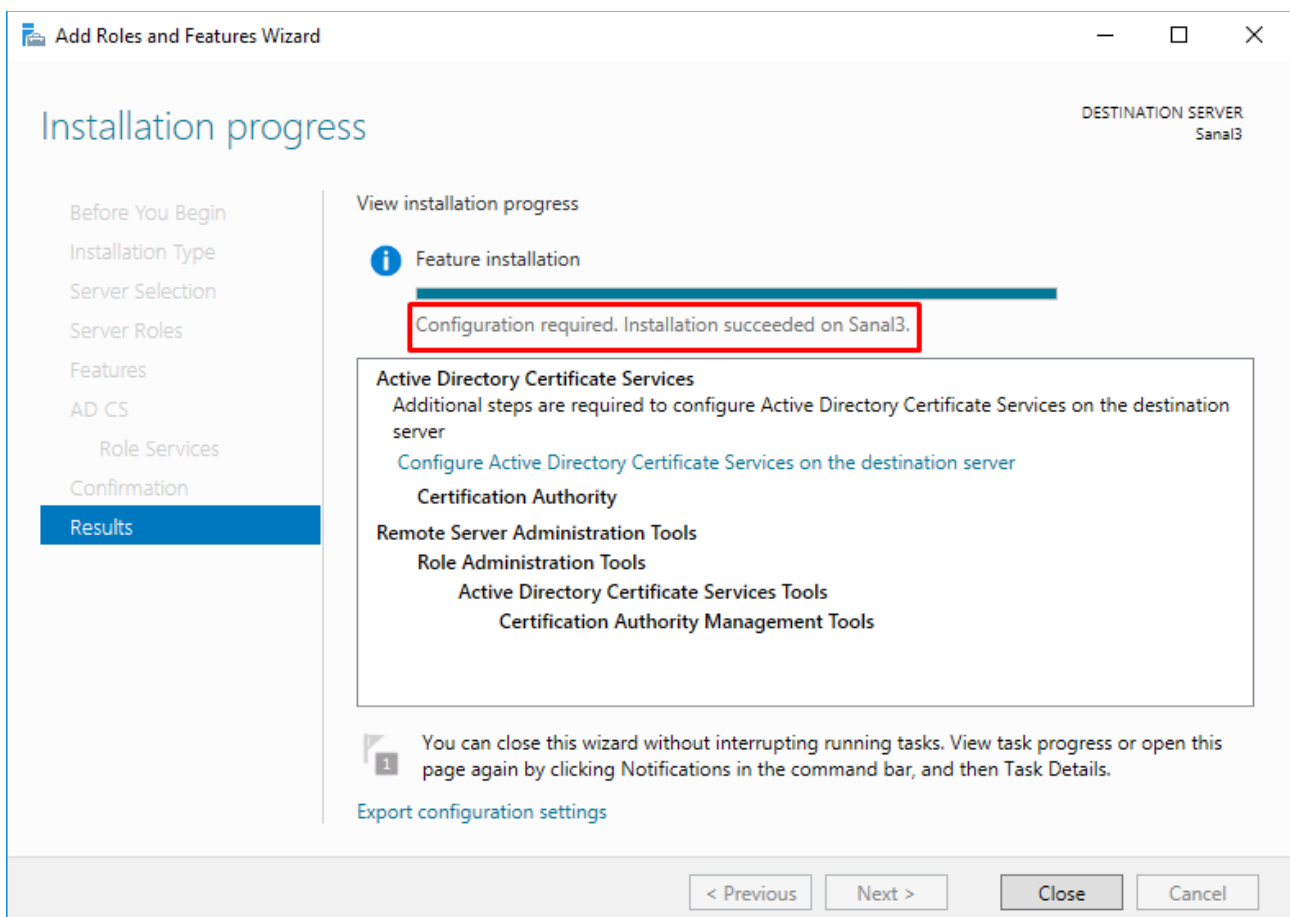


- AD CS altında Role Services kısmında “Certification Authority” işaretlenir.

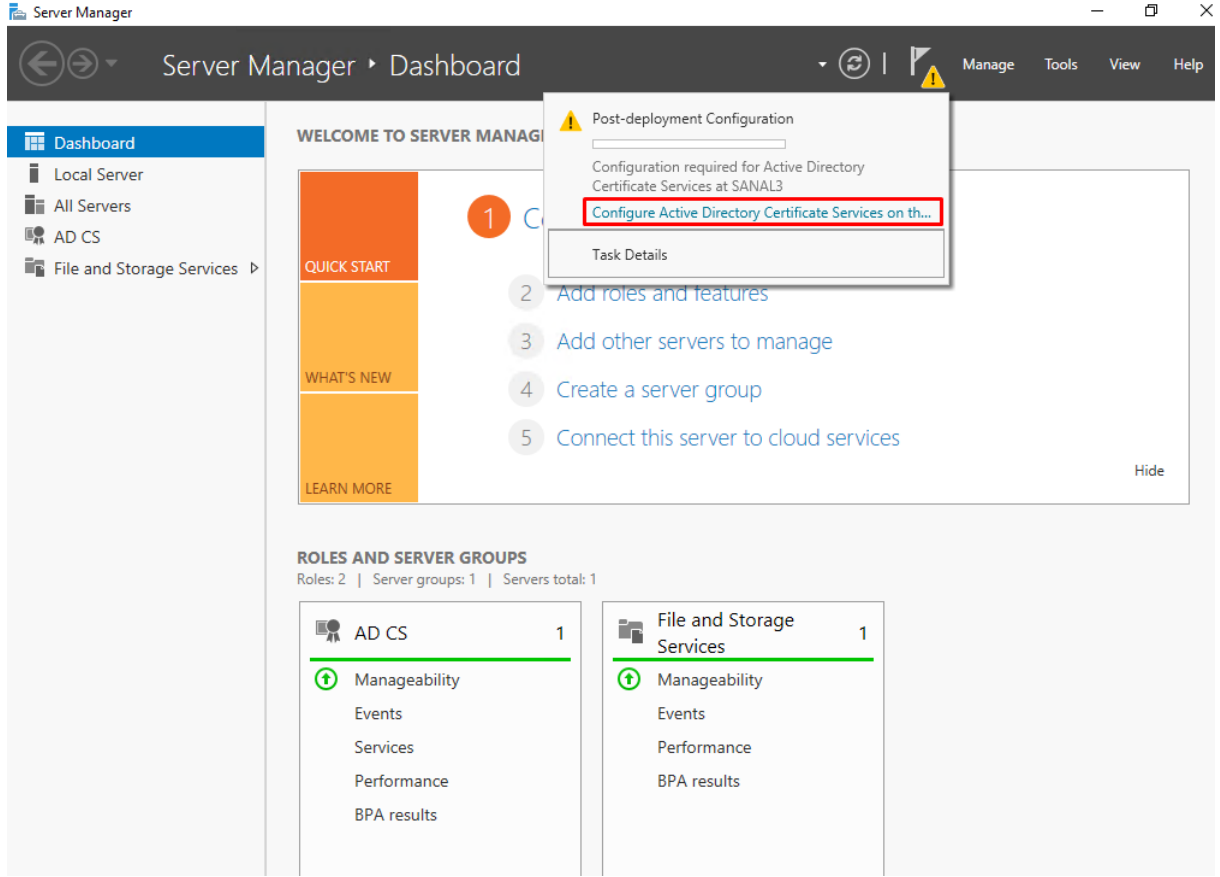




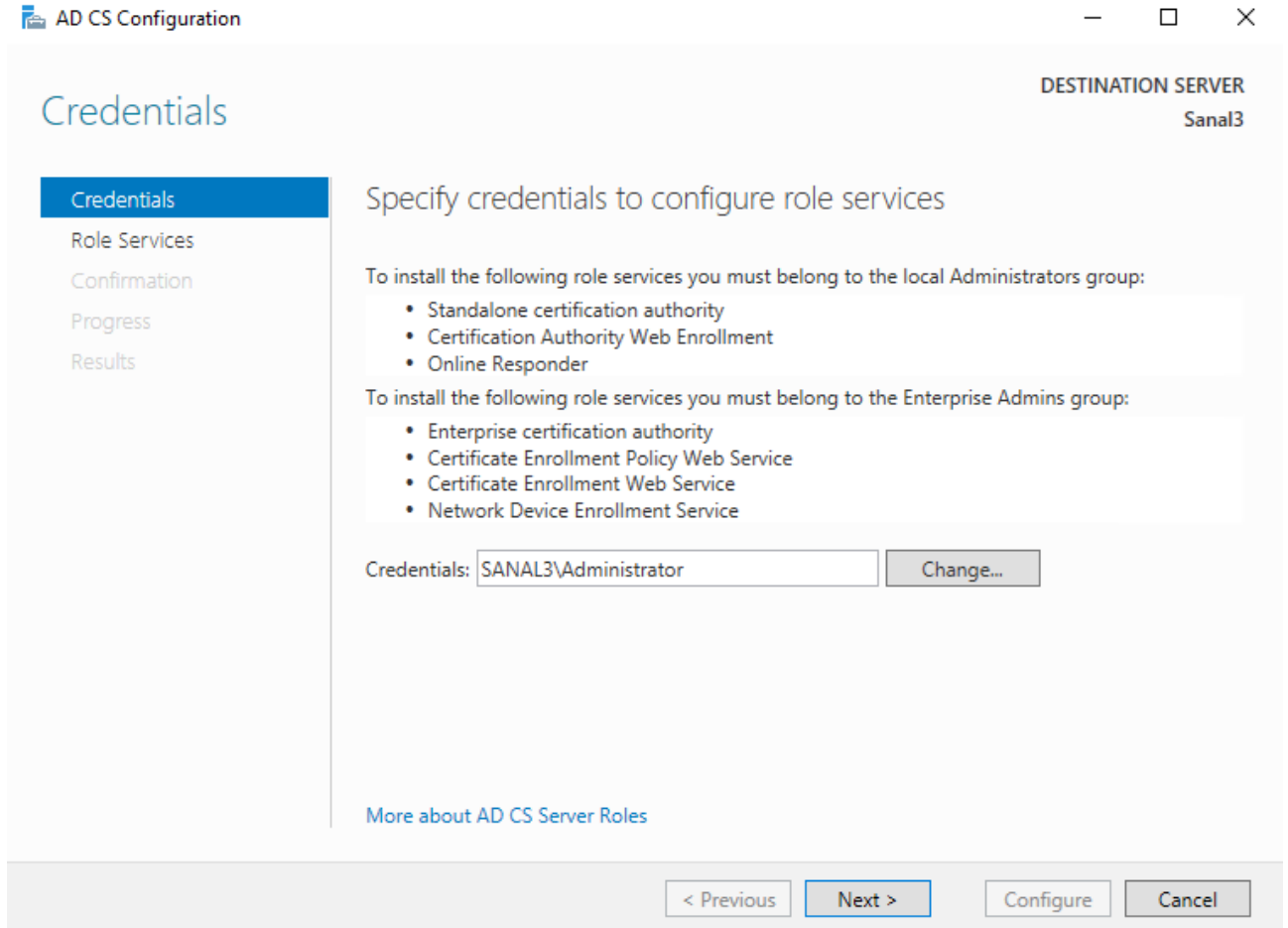
- Add Install ile kurulum biter ve yüklendikten sonra cihaz yeniden başlatılır.



İşlem2 : Cihaz yeniden başlatıldıktan sonra Server Manager üzerinde “Bayrak” simgesini tıklayıp “Configure Active Directory Certificate Services on the...” tıklanır.



- Next denir.



- Certification Authority'nin işaretli olduğu kontrol edilip Next denir.

AD CS Configuration

DESTINATION SERVER
Sanal3

Role Services

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

- Standalone CA seçilir ve Next denir.

AD CS Configuration

DESTINATION SERVER
Sanal3

Setup Type

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

- Root CA seçilir ve Next denir.

AD CS Configuration

DESTINATION SERVER
Sanal3

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

- Yeni bir sertifika oluşturduğumuzdan “Create a new private key” seçilir.

AD CS Configuration

DESTINATION SERVER
Sanal3

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

- Key'in şifreleneceği method seçilir.

The screenshot shows the 'Cryptography for CA' window in the AD CS Configuration console. The left-hand navigation pane lists various steps: Credentials, Role Services, Setup Type, CA Type, Private Key, **Cryptography** (highlighted), CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the cryptographic options'. It contains two dropdown menus: 'Select a cryptographic provider:' set to 'RSA#Microsoft Software Key Storage Provider' and 'Key length:' set to '2048'. Below these is a list box for 'Select the hash algorithm for signing certificates issued by this CA:' with options SHA256, SHA384, SHA512, SHA1, and MD5. A checkbox labeled 'Allow administrator interaction when the private key is accessed by the CA.' is currently unchecked. At the bottom right of the main area is a link 'More about Cryptography'. The bottom of the window features four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

- CA Name kısmı aynen kalır ve Next denir.

The screenshot shows the 'CA Name' window in the AD CS Configuration console. The left-hand navigation pane is the same as the previous window, but 'CA Name' is now highlighted. The main area is titled 'Specify the name of the CA'. It includes a text box for 'Common name for this CA:' containing 'SANAL3-CA'. Below it is an empty text box for 'Distinguished name suffix:'. A 'Preview of distinguished name:' section shows 'CN=SANAL3-CA'. At the bottom right of the main area is a link 'More about CA Name'. The bottom of the window features the same four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

- Key'in geçerlilik süresi belirlenir.

AD CS Configuration

DESTINATION SERVER
Sanal3

Validity Period

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):

5 Years

CA expiration Date: 20.11.2024 09:38:00

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

- Next denir.

AD CS Configuration

DESTINATION SERVER
Sanal3

CA Database

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

- Configure denir ve konfigürasyon tamamlanır.

AD CS Configuration

DESTINATION SERVER
Sanal3

Confirmation

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:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	20.11.2024 09:38:00
Distinguished Name:	CN=SANAL3-CA
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

< Previous Next > **Configure** Cancel

AD CS Configuration

DESTINATION SERVER
Sanal3

Results

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

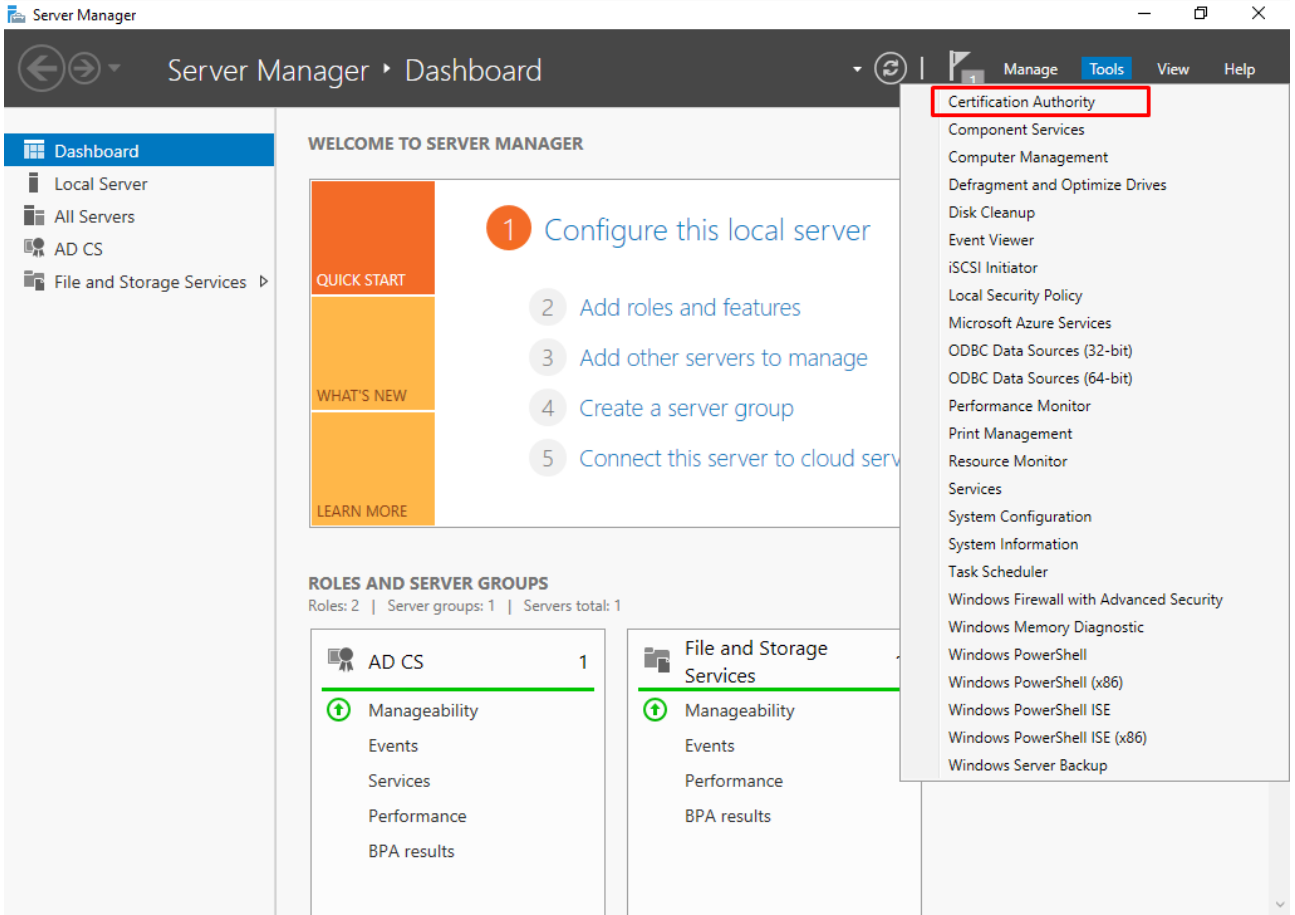
The following roles, role services, or features were configured:

Active Directory Certificate Services

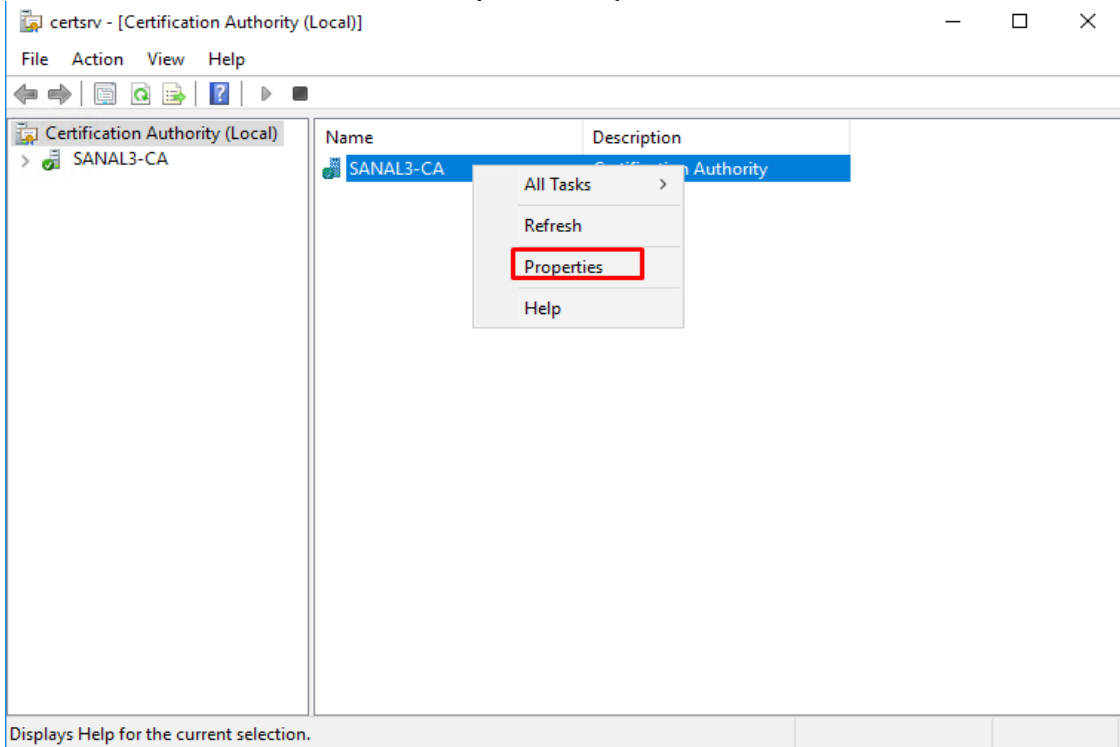
Certification Authority ✓ Configuration succeeded
[More about CA Configuration](#)

< Previous Next > **Close** Cancel

İşlem3 : Konfigürasyonun tamamlanmasının ardından Server Manager üzerinde “Tools” kısmından “Certification Authority” tıklanır.



– Sertifika cihazımız altında “Properties” seçilir.



- “Extansions” altında “CRL Distribution Point (CDP)” kısmında “http” olan kısım silinir ve yenisi için “Add”e tıklanır.

The screenshot shows the 'SANAL3-CA Properties' dialog box with the 'Extensions' tab selected. The 'Select extension:' dropdown menu is set to 'CRL Distribution Point (CDP)'. Below this, the text box contains the following URL template: `C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix>\Idap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortName>http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLNameSuffix>file:///<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLNameSuffix>`. The 'http' part of the URL is highlighted in blue. Below the text box, there are two buttons: 'Add...' and 'Remove'. The 'Remove' button is highlighted with a red box. Below these buttons, there are several checkboxes: 'Publish CRLs to this location', 'Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.', 'Include in CRLs. Clients use this to find Delta CRL locations.', 'Include in the CDP extension of issued certificates', 'Publish Delta CRLs to this location', and 'Include in the IDP extension of issued CRLs'. At the bottom of the dialog box, there are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

- `http://Sanal2.root.local/CertData/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`
kodu yazılır ve eklenir. Kalın ve italik olan kısım, sertifikayı dağıtacak olan server cihazının adıdır.
Kodun eklenmesinin ardından aşağıdaki işaretli kısımlar işaretlenir.

SANAL3-CA-1 Properties

Enrollment Agents Auditing Recovery Agents Security

General Policy Module Exit Module

Extensions Storage Certificate Managers

Select extension:

CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix>Idap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortName>file:///<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl

http://**Sanal2.root.local**/CertData/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl

Add... Remove

☐ Publish CRLs to this location

☐ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

☒ Include in CRLs. Clients use this to find Delta CRL locations.

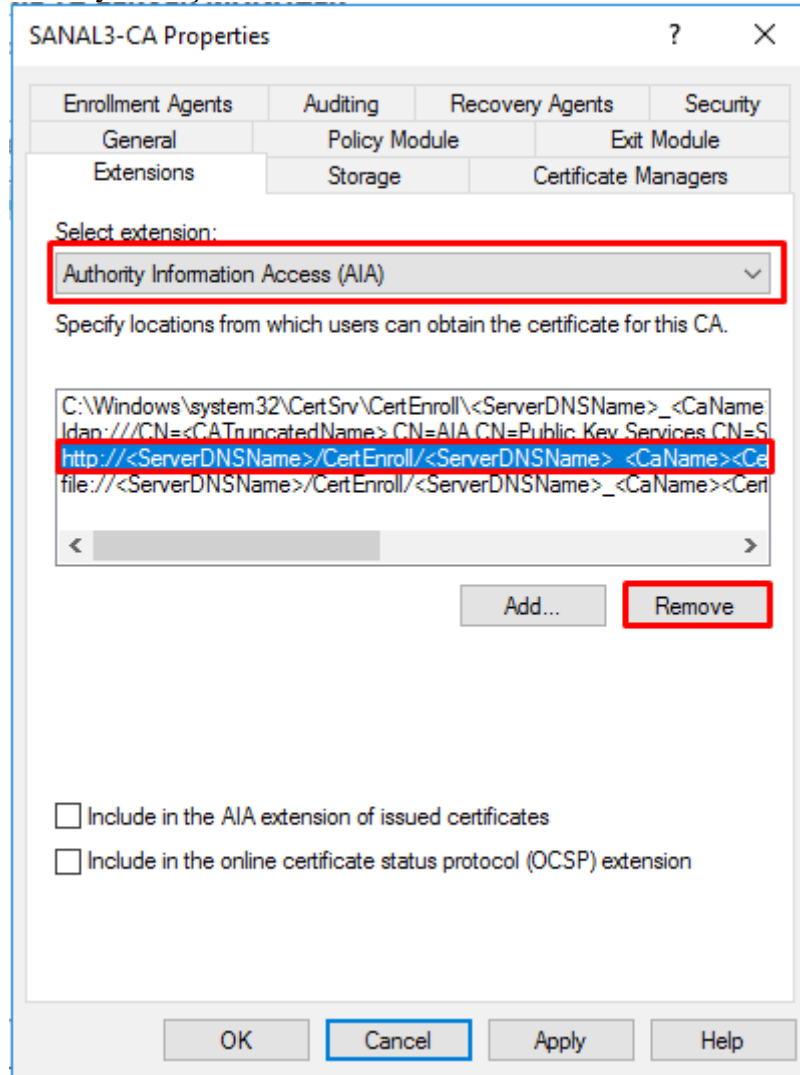
☒ Include in the CDP extension of issued certificates

☐ Publish Delta CRLs to this location

☐ Include in the IDP extension of issued CRLs

OK Cancel Apply Help

- CDP üzerindeki işlem tamamlandıktan sonra “ Authority Information Access (AIA)” altındaki “http” silinir ve yenisi için “Add”e tıklanır.

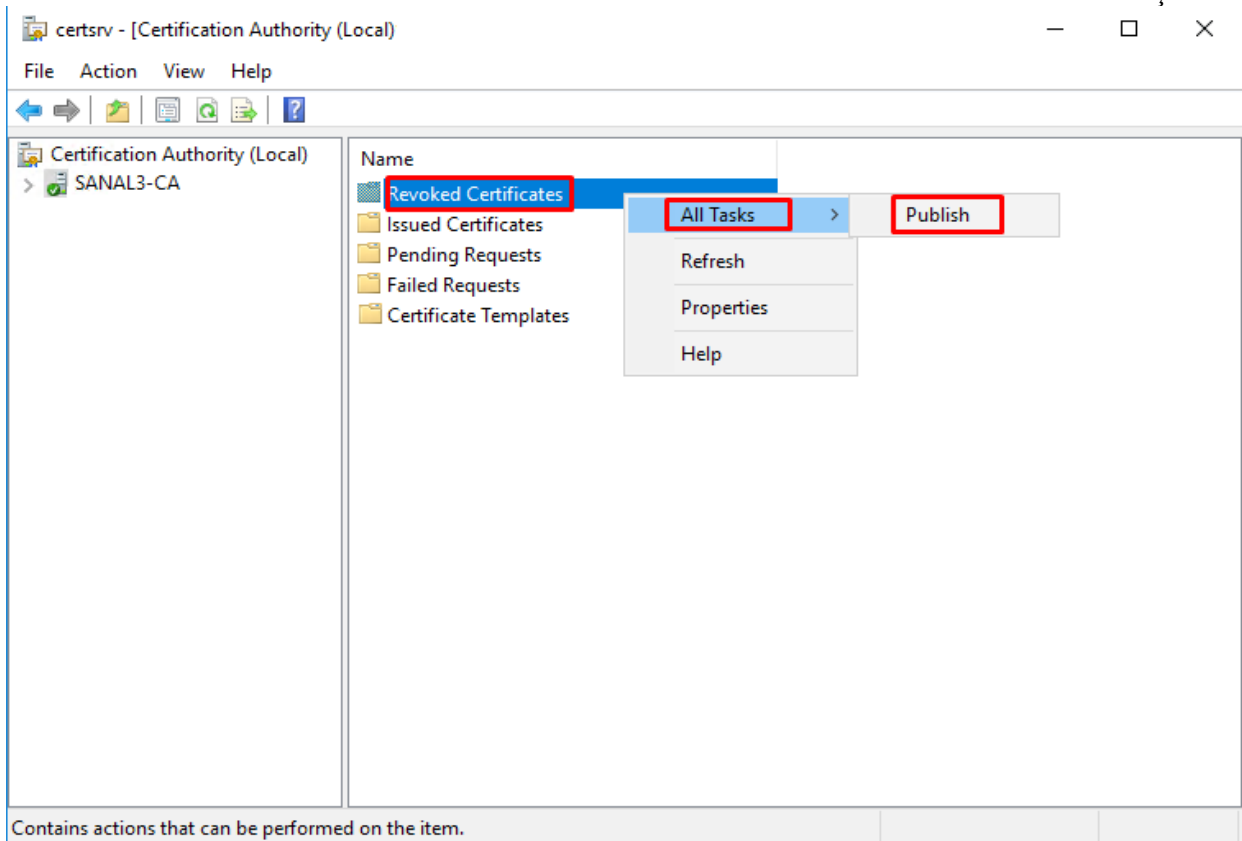


- http://**Sanal2.root.local**/CertData/<ServerDNSName> <CaName><CertificateName>.crt

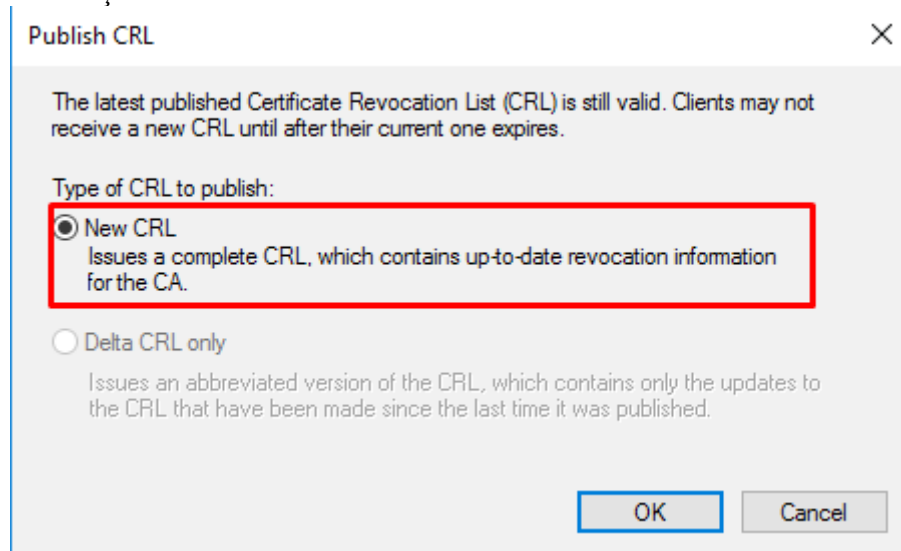
Kodu eklenir ve aşağıdaki “Include” kısmı işaretlenir. Ardından Okay denip servis yeniden başlatılır.

The screenshot shows the 'SANAL3-CA-1 Properties' dialog box with the 'Extensions' tab selected. The 'Authority Information Access (AIA)' extension is chosen from the list. The text box displays the AIA URL: `http://Sanal2.root.local/CertData/<ServerDNSName> <CaName><CertificateSerialNumber>`. The checkbox 'Include in the AIA extension of issued certificates' is checked, while 'Include in the online certificate status protocol (OCSP) extension' is unchecked. The 'Add...' button is disabled.

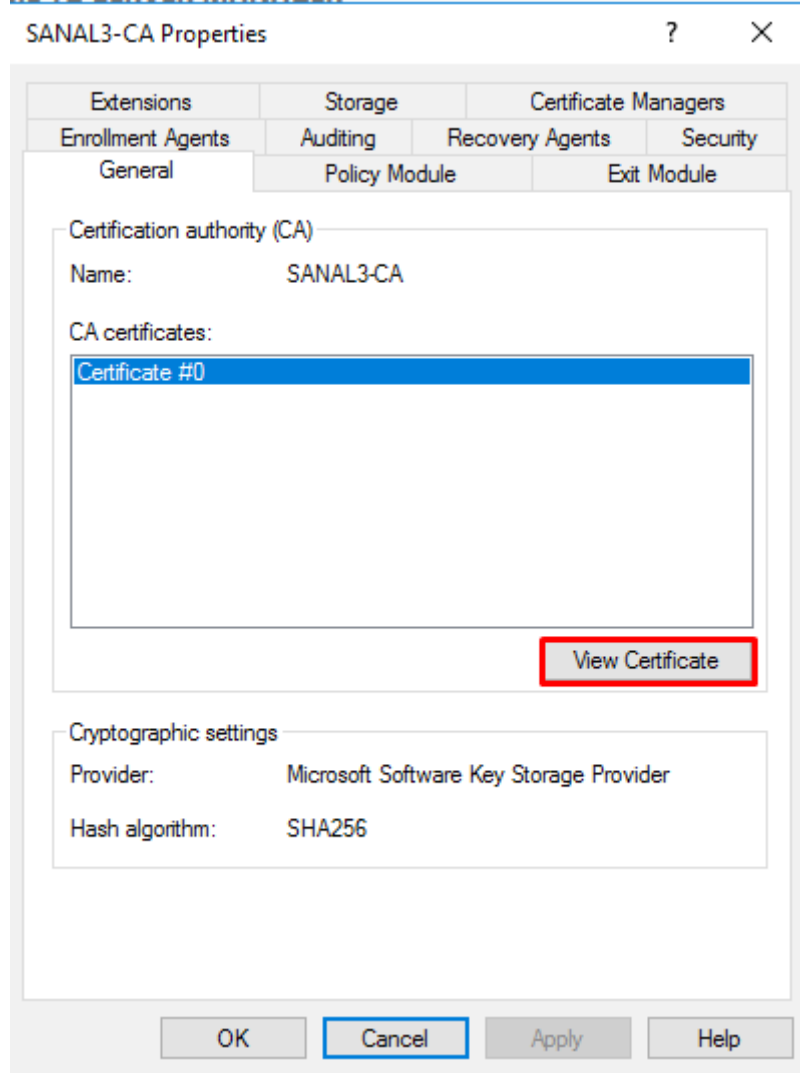
- Servis resetlendikten sonra “Revoked Certificates” altında All Tasks --> Publish seçilir.



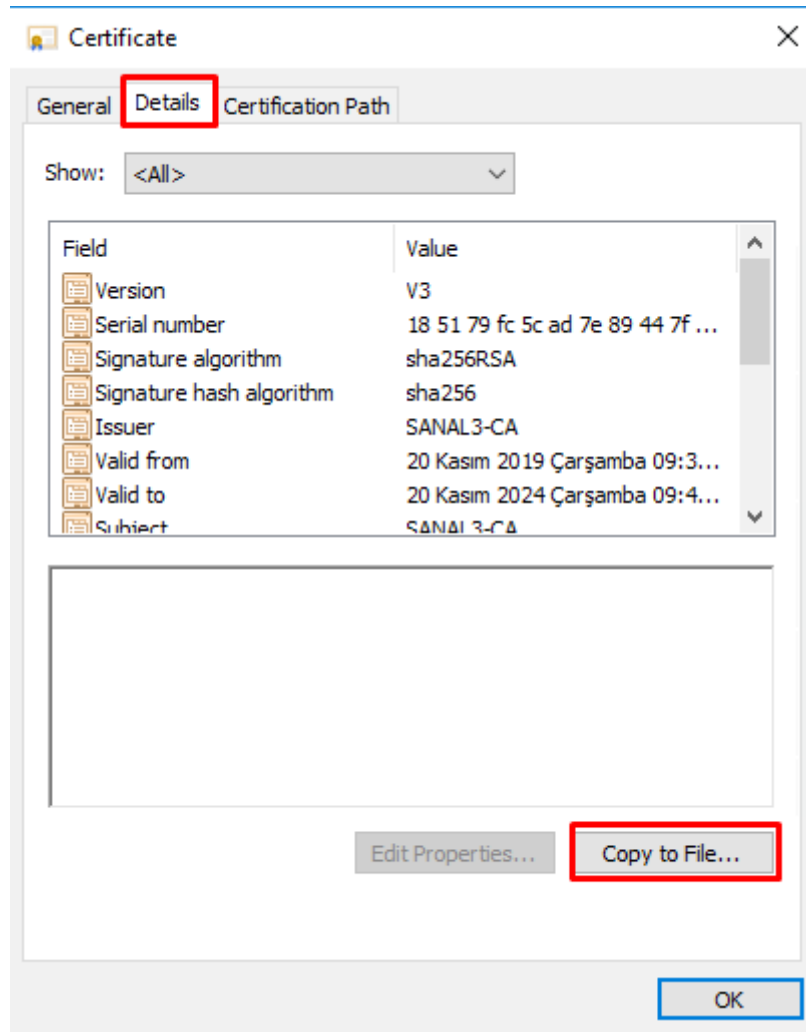
- New CRL seçilir.



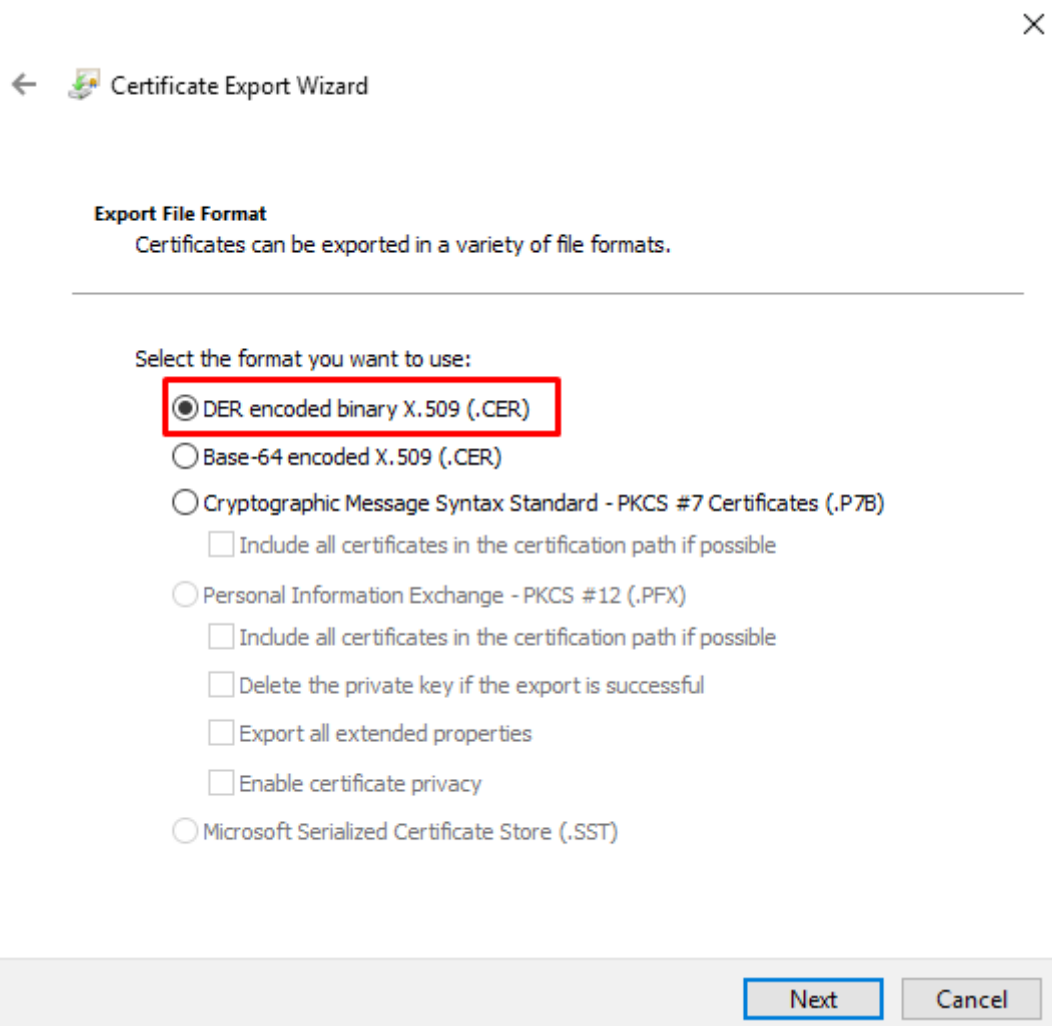
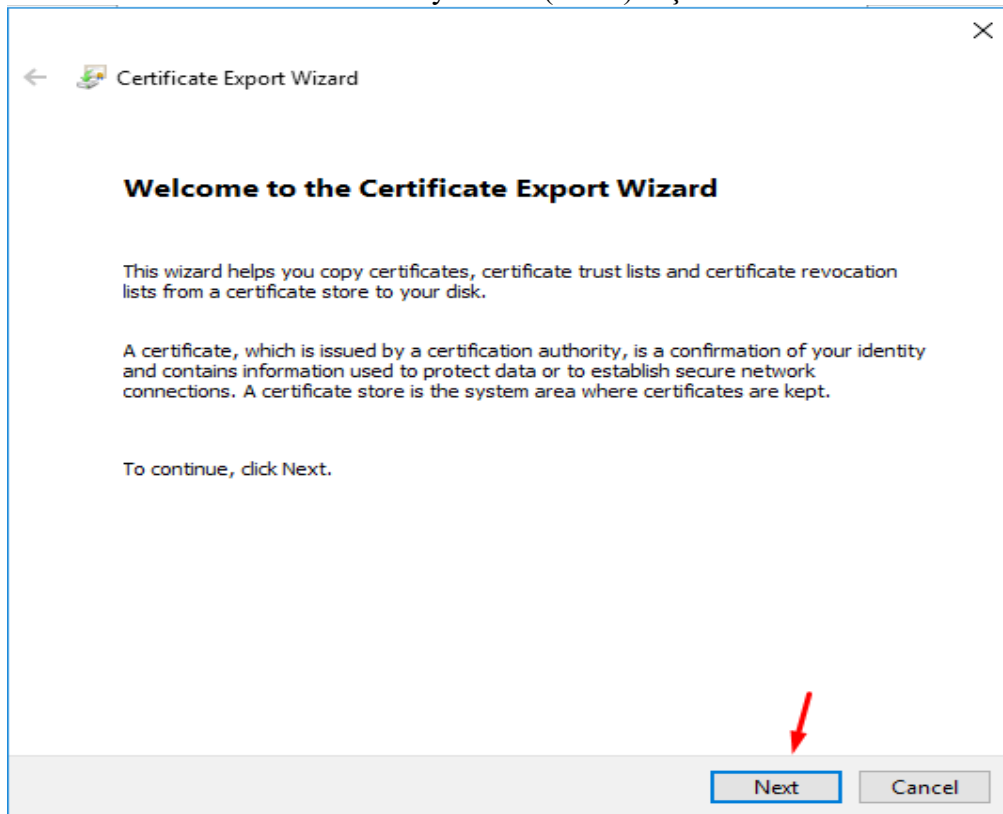
- CA cihazımız üzerinde yine “Properties” tekılanır ve “General” kısmından “View Certificate” denir.




- Details kısmına gelinir ve “Copy to File” denir.



- Next denir ve “DER encoded binary X.509 (.CER)” seçilir.



- Sertifikamızın hangi dizine oluşturulacağı seçilir ve ismi “.cer” uzantılı olarak belirlenir. Ardından sertifikamız oluşturulmuş olunur.

 Certificate Export Wizard


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

File name:
C:\Users\Administrator\Desktop\certificate.cer

Browse...

Next

Cancel

 Certificate Export Wizard

Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following:

File Name
Export Keys
Include all certificates in
File Format

Certificate Export Wizard
The export was successful.
OK

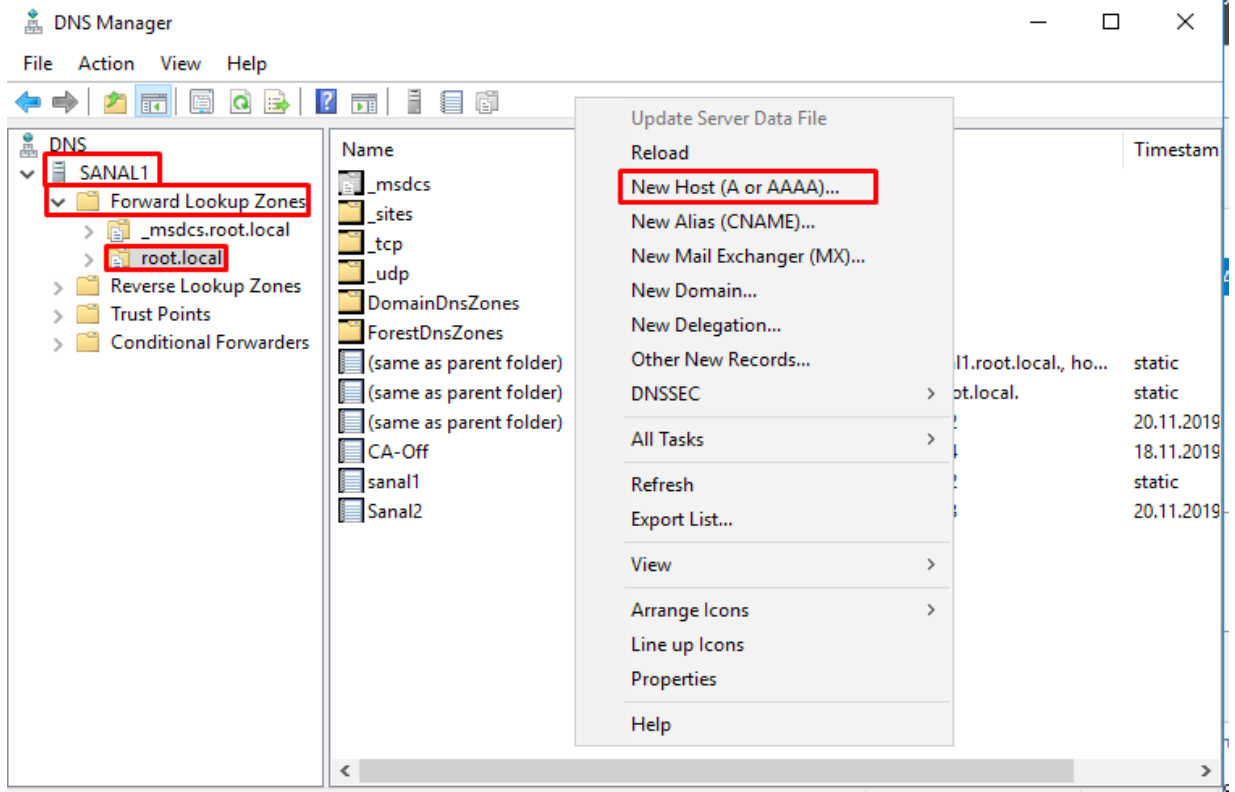
trator\Desktop\certifi
ary X.509 (*.cer)

Finish

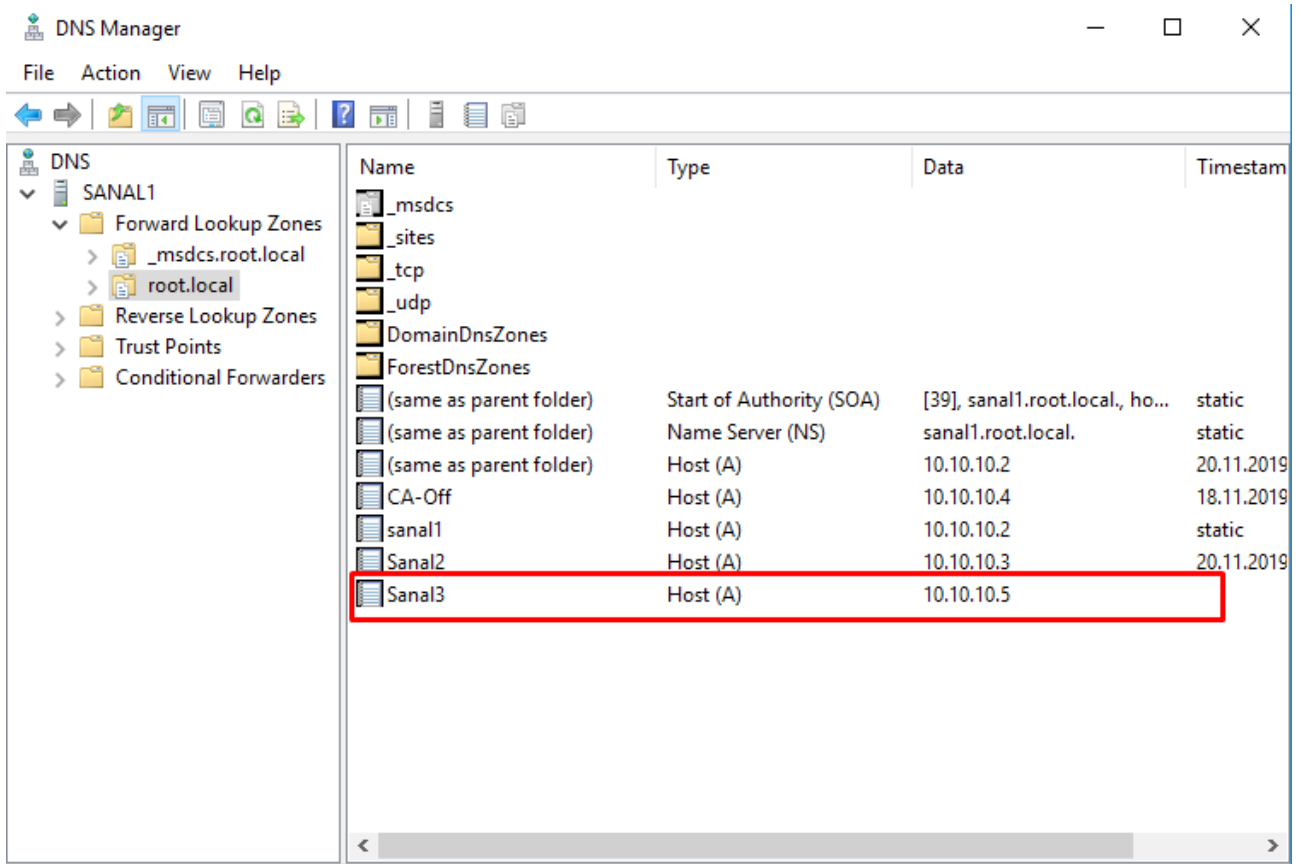
Cancel

Sertifakımız oluşturulduktan sonra Sanal3 cihazımı domain içindeki cihazlar ile konuşturmak ve bilgi alışverişi sağlamak için DC olan Sanal1 cihazımızdan DNS manager üzerinden IP adresini eklememiz gerekmektedir.

İşlem4 : Sanal1 cihazında Server Manager'da “Tools” kısmından “DNS Manager” açılır. “Forward Lookup Zones” altında domain adresine girilir ve boş alana tıklanarak “New Host” seçilir.

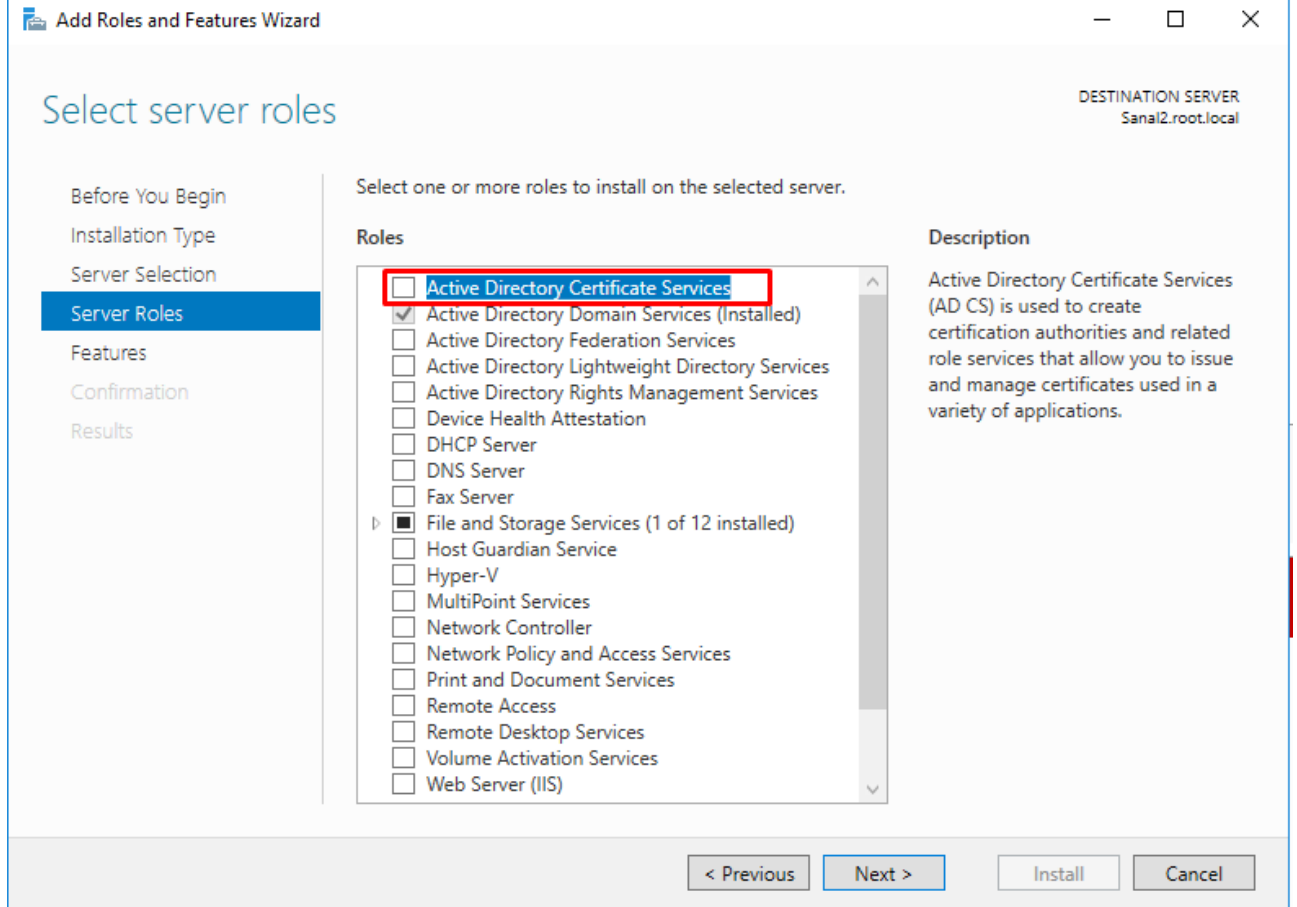


- Sanal3 cihazımızın tam adı ve IP adresi girilir, işaretli kısımlar tiklenir. PTR oluşturulamadı hatası gelirse dikkate alınmamalıdır. Sanal3 cihazımız eklenmiştir.

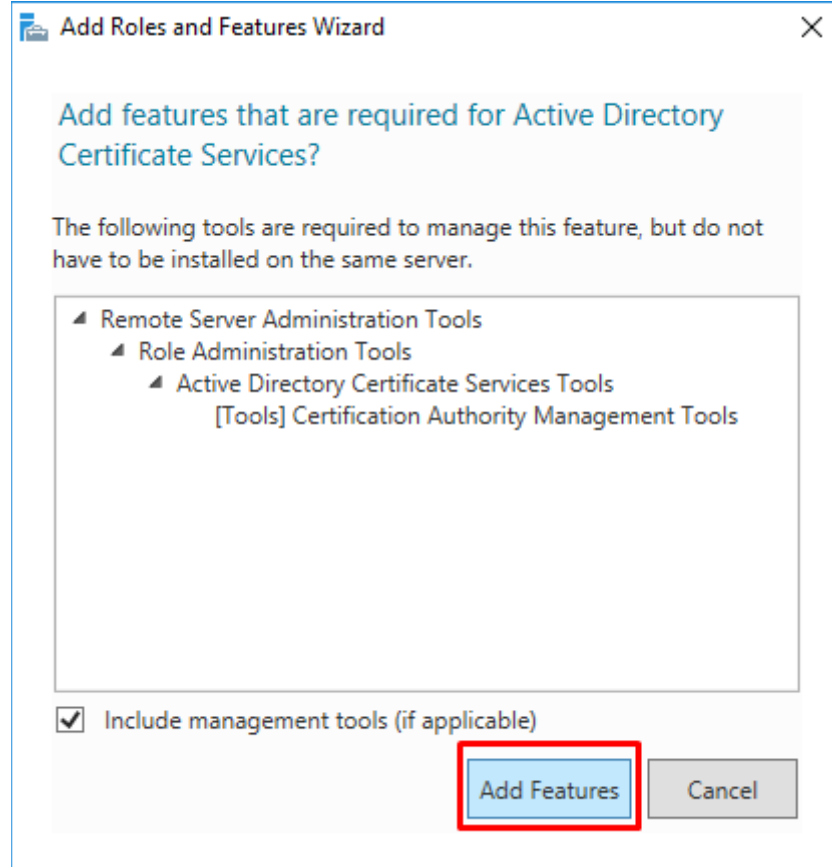


- Ardından domain içindeki Sanal2 cihazımıza Enterprise CA için kurulumlar başlanır.

İşlem5 : Server Roles kısmına kadar olan kısımlar İşlem1 adımı ile aynıdır, yeniden “Active Directory Certificate Services” seçilir.



- Add Features ile Tool'lar eklenir.



- “Certification Authority” ve “Certification Authority Web Enrollment” seçilir ve Add Features denir.

The screenshot shows the 'Add Roles and Features Wizard' window, specifically the 'Select role services' step. The left sidebar contains a list of steps: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'AD CS', 'Role Services' (highlighted), 'Confirmation', and 'Results'. The main area is titled 'Select the role services to install for Active Directory Certificate Services'. It features a table with 'Role services' and 'Description' columns. The 'Role services' column has a red box around the first four items: 'Certification Authority' (checked), 'Certificate Enrollment Policy Web Service' (unchecked), 'Certificate Enrollment Web Service' (unchecked), and 'Certification Authority Web Enrollment' (checked). The 'Description' column provides details for 'Certification Authority Web Enrollment'. At the bottom, there are buttons for '< Previous', 'Next >', 'Install', and 'Cancel'.

Role services	Description
<input checked="" type="checkbox"/> Certification Authority	
<input type="checkbox"/> Certificate Enrollment Policy Web Service	
<input type="checkbox"/> Certificate Enrollment Web Service	
<input checked="" type="checkbox"/> Certification Authority Web Enrollment	Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.
<input type="checkbox"/> Network Device Enrollment Service	
<input type="checkbox"/> Online Responder	

- Next denir.

The screenshot shows the 'Add Roles and Features Wizard' window, specifically the 'Web Server Role (IIS)' step. The left sidebar contains a list of steps: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'AD CS', 'Role Services', 'Web Server Role (IIS)' (highlighted), 'Role Services', 'Confirmation', and 'Results'. The main area is titled 'Web Server Role (IIS)'. It contains a paragraph describing web servers and a bulleted list stating that the default installation includes role services for serving static content, minor customizations, monitoring, and logging. At the bottom, there are buttons for '< Previous', 'Next >', 'Install', and 'Cancel'.

Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 10.0 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 10.0, ASP.NET, and Windows Communication Foundation.

- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

- Ayarlar aynen kalır ve Next denir.

Add Roles and Features Wizard

DESTINATION SERVER
Sanal2.root.local

Select role services

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 Web Server (IIS)

Role services

- ☒ Web Server
 - ☒ Common HTTP Features
 - ☒ Default Document
 - ☒ Directory Browsing
 - ☒ HTTP Errors
 - ☒ Static Content
 - ☒ HTTP Redirection
 - ☐ WebDAV Publishing
 - ☒ Health and Diagnostics
 - ☒ HTTP Logging
 - ☐ Custom Logging
 - ☒ Logging Tools
 - ☐ ODBC Logging
 - ☒ Request Monitor
 - ☒ Tracing
 - ☒ Performance
 - ☒ Static Content Compression
 - ☐ Dynamic Content Compression
 - ☒ Security

Description

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

< Previous Next > Install Cancel

- Kurulum başlatılır.

Add Roles and Features Wizard

DESTINATION SERVER
Sanal2.root.local

Confirm installation selections

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

To install the following roles, role services, or features on selected server, click Install.

☒ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

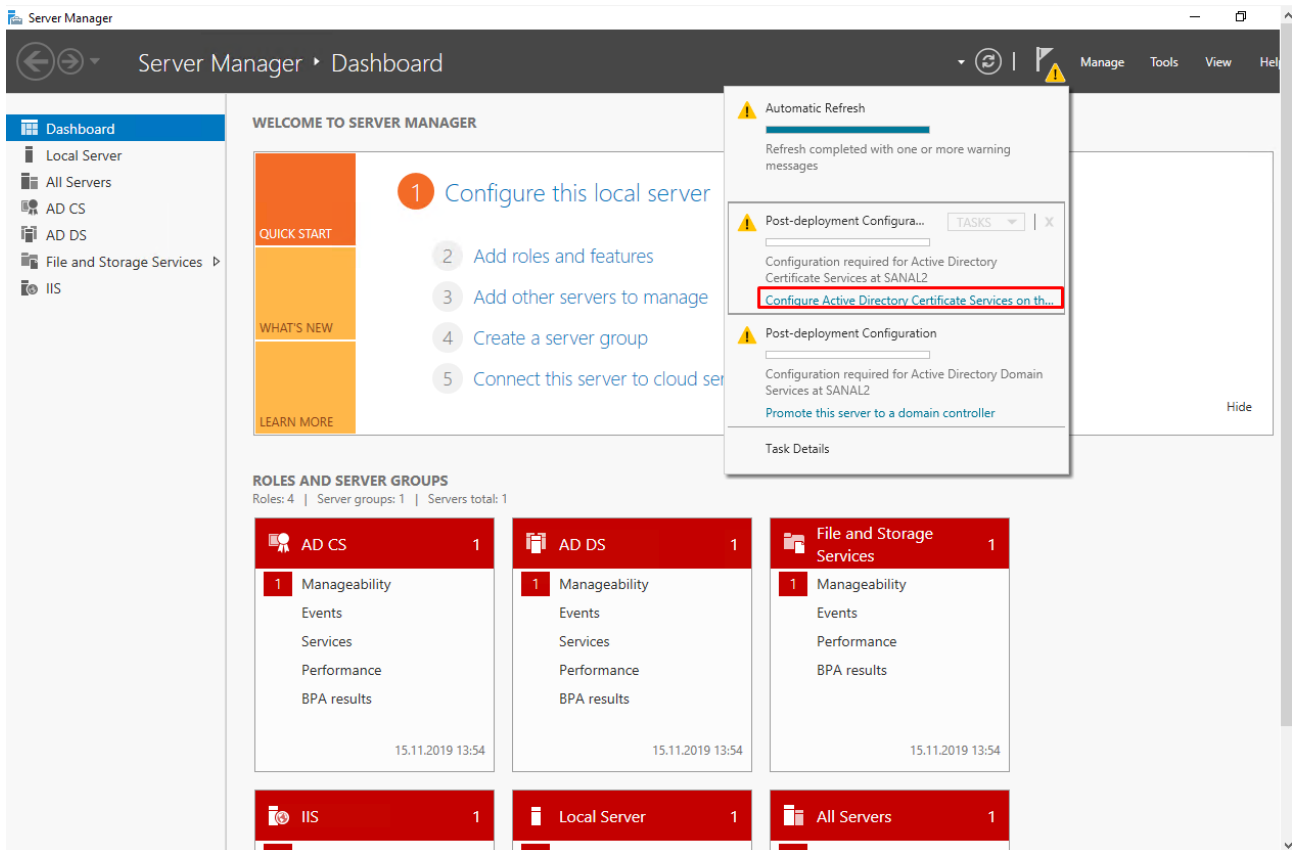
Active Directory Certificate Services

- Certification Authority
- Certification Authority Web Enrollment

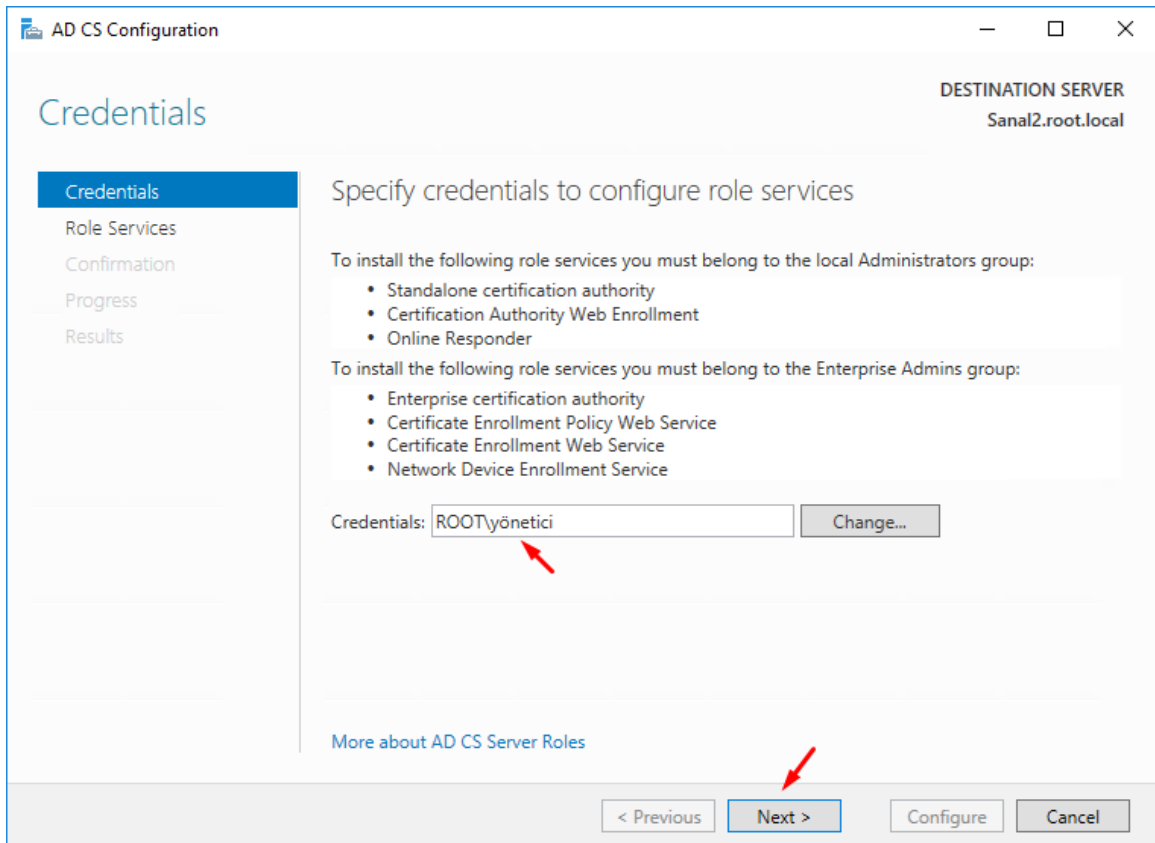
[Export configuration settings](#)
[Specify an alternate source path](#)

< Previous Next > Install Cancel

- Kurulum tamamlandıktan sonra Server Manager üzerinde “Configure Active Directory Certificate Services on the...” denir.



- Next denir.



- Certification Authority ve Certification Authority Web Enrollment kontrol edilip Next denir.

AD CS Configuration

DESTINATION SERVER
Sanal2.root.local

Role Services

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

- Enterprise CA seçilir.

AD CS Configuration

DESTINATION SERVER
Sanal2.root.local

Setup Type

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

– Subordinate CA seçilir.

The screenshot shows the 'AD CS Configuration' window with the 'CA Type' step selected in the left-hand navigation pane. The main area is titled 'Specify the type of the CA'. It contains a paragraph explaining that a root CA is at the top of the PKI hierarchy and issues its own self-signed certificate, while a subordinate CA receives a certificate from the CA above it. Two radio buttons are present: 'Root CA' and 'Subordinate CA'. The 'Subordinate CA' option is selected and highlighted with a red rectangular box. Below the options is a link that says 'More about CA Type'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER
Sanal2.root.local

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

– Create a new private key seçilir.

The screenshot shows the 'AD CS Configuration' window with the 'Private Key' step selected in the left-hand navigation pane. The main area is titled 'Specify the type of the private key'. It contains a paragraph stating that a certification authority (CA) must have a private key to generate and issue certificates to clients. Three radio buttons are present: 'Create a new private key', 'Use existing private key', and 'Select a certificate and use its associated private key'. The 'Create a new private key' option is selected and highlighted with a red rectangular box. Below it, there are two more options: 'Select an existing private key on this computer' and 'Select an existing private key from a previous installation or want to use a private key from an alternate source'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER
Sanal2.root.local

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

- Şifreleme ayarları Sanal3 cihazımızdaki ayarlar ile aynı olmak zorundadır.

The screenshot shows the 'AD CS Configuration' console window. The title bar says 'AD CS Configuration'. The main title is 'Cryptography for CA'. In the top right corner, it says 'DESTINATION SERVER Sanal2.root.local'. On the left, there is a navigation pane with the following items: Credentials, Role Services, Setup Type, CA Type, Private Key, **Cryptography** (highlighted), CA Name, Certificate Request, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the cryptographic options'. It contains two dropdown menus: 'Select a cryptographic provider:' with 'RSA#Microsoft Software Key Storage Provider' selected, and 'Key length:' with '2048' selected. Below these is a list box for 'Select the hash algorithm for signing certificates issued by this CA:' with options: SHA256, SHA384, SHA512, SHA1, and MD5. At the bottom of this section is a checkbox labeled 'Allow administrator interaction when the private key is accessed by the CA.' which is currently unchecked. A link 'More about Cryptography' is at the bottom left of the main area. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

- Next denir.

The screenshot shows the 'AD CS Configuration' console window. The title bar says 'AD CS Configuration'. The main title is 'CA Name'. In the top right corner, it says 'DESTINATION SERVER Sanal2.root.local'. On the left, there is a navigation pane with the following items: Credentials, Role Services, Setup Type, CA Type, Private Key, Cryptography, **CA Name** (highlighted), Certificate Request, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the name of the CA'. It contains a text box for 'Common name for this CA:' with the value 'root-SANAL2-CA-2'. Below it is a text box for 'Distinguished name suffix:' with the value 'DC=root,DC=local'. At the bottom of this section is a text box for 'Preview of distinguished name:' with the value 'CN=root-SANAL2-CA-2,DC=root,DC=local'. A link 'More about CA Name' is at the bottom left of the main area. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

- “Save a certificate request to file on the target machine” işaretlenir ve Next denir.

AD CS Configuration

DESTINATION SERVER
Sanal2.root.local

Certificate Request

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:

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

[More about Certificate Request](#)

- Next denir.

AD CS Configuration

DESTINATION SERVER
Sanal2.root.local

CA Database

Specify the database locations

Certificate database location:

Certificate database log location:

[More about CA Database](#)

– Configure denir.

AD CS Configuration

DESTINATION SERVER
Sanal2.root.local

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:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	Determined by the parent CA
Distinguished Name:	CN=root-SANAL2-CA-2,DC=root,DC=local
Offline Request File Location:	C:\Sanal2.root.local_root-SANAL2-CA-2.req
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

Certification Authority Web Enrollment



< Previous Next > **Configure** Cancel

– Kurulum tamamlanır ve ardından...

AD CS Configuration


DESTINATION SERVER
Sanal2.root.local


Results

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


The following roles, role services, or features were configured:

⤴ **Active Directory Certificate Services**

Certification Authority  **Configuration succeeded with warnings**

 The Active Directory Certificate Services installation is incomplete. To complete the installation, use the request file "C:\Sanal2.root.local_root-SANAL2-CA-2.req" to obtain a certificate from the parent CA. Then, use the Certification Authority snap-in to install the certificate. To complete this procedure, right-click the node with the name of the CA, and then click Install CA Certificate. The operation completed successfully. 0x0 (WIN32: 0)

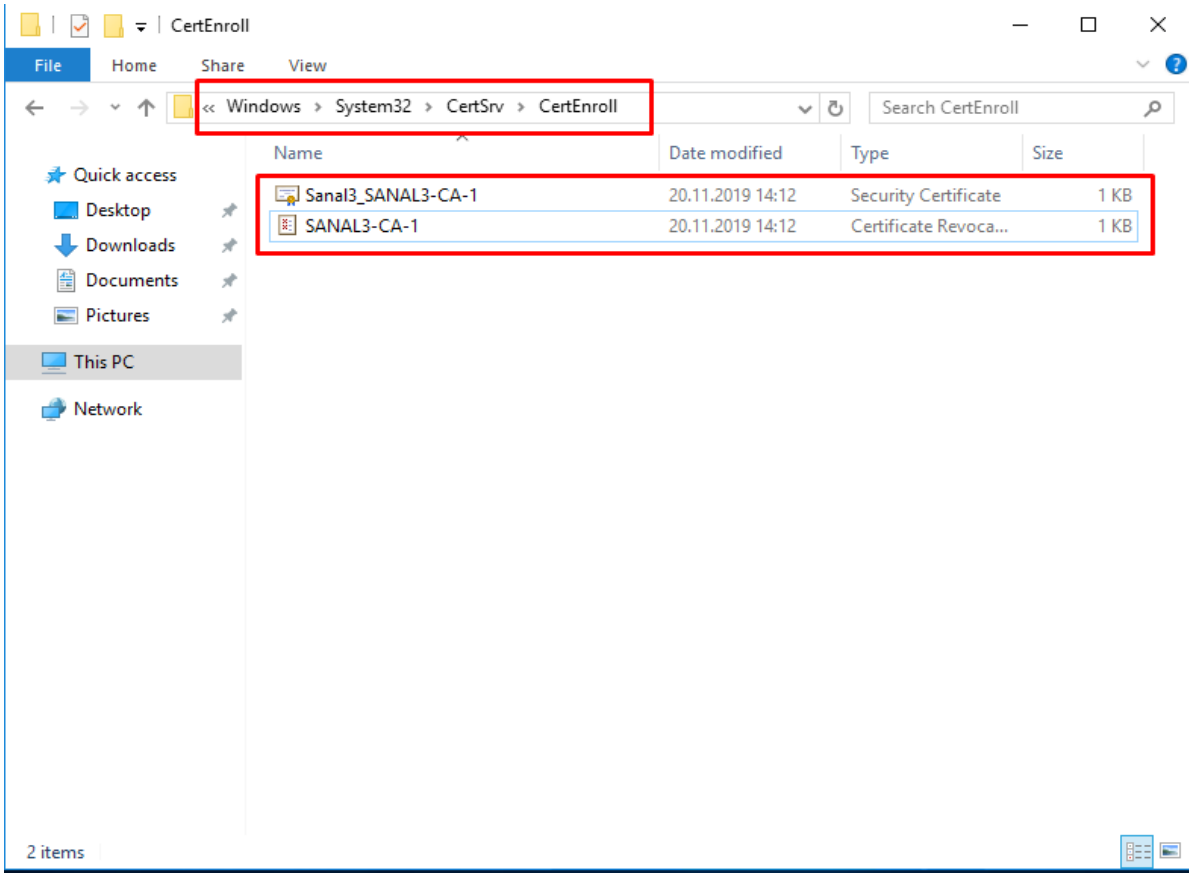
[More about CA Configuration](#)

Certification Authority Web Enrollment  **Configuration succeeded**

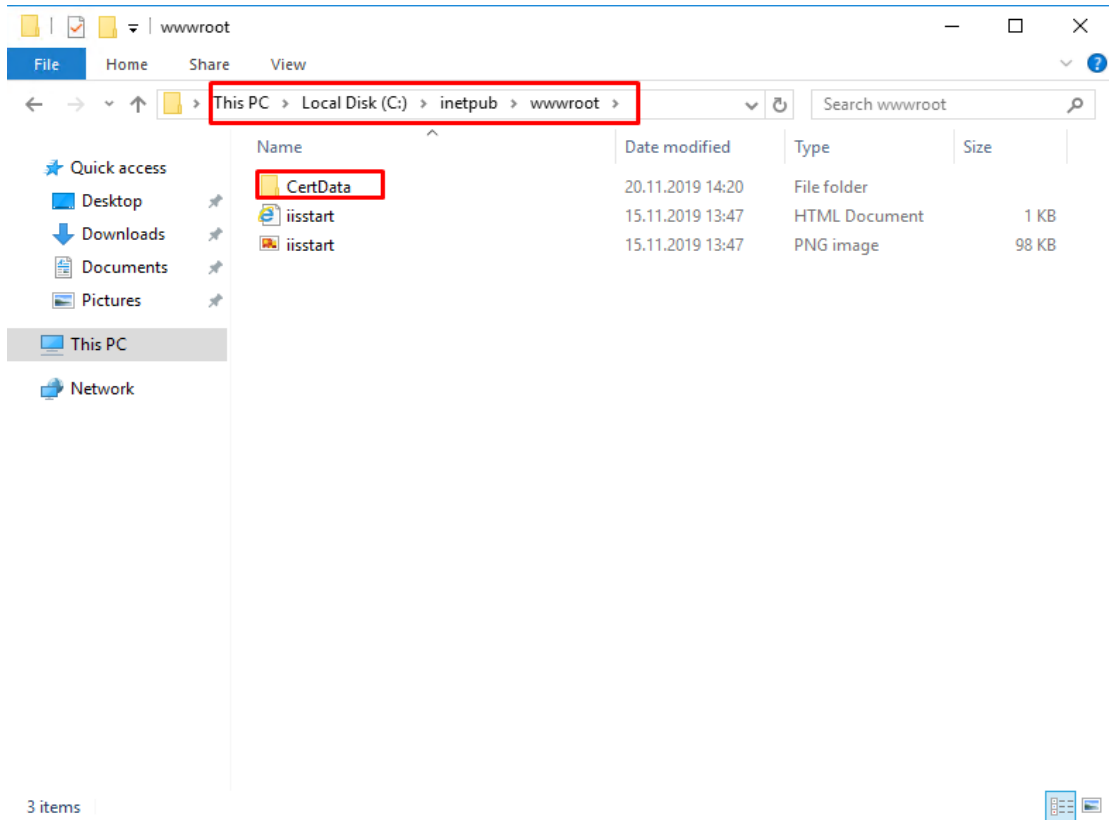
[More about Web Enrollment Configuration](#)

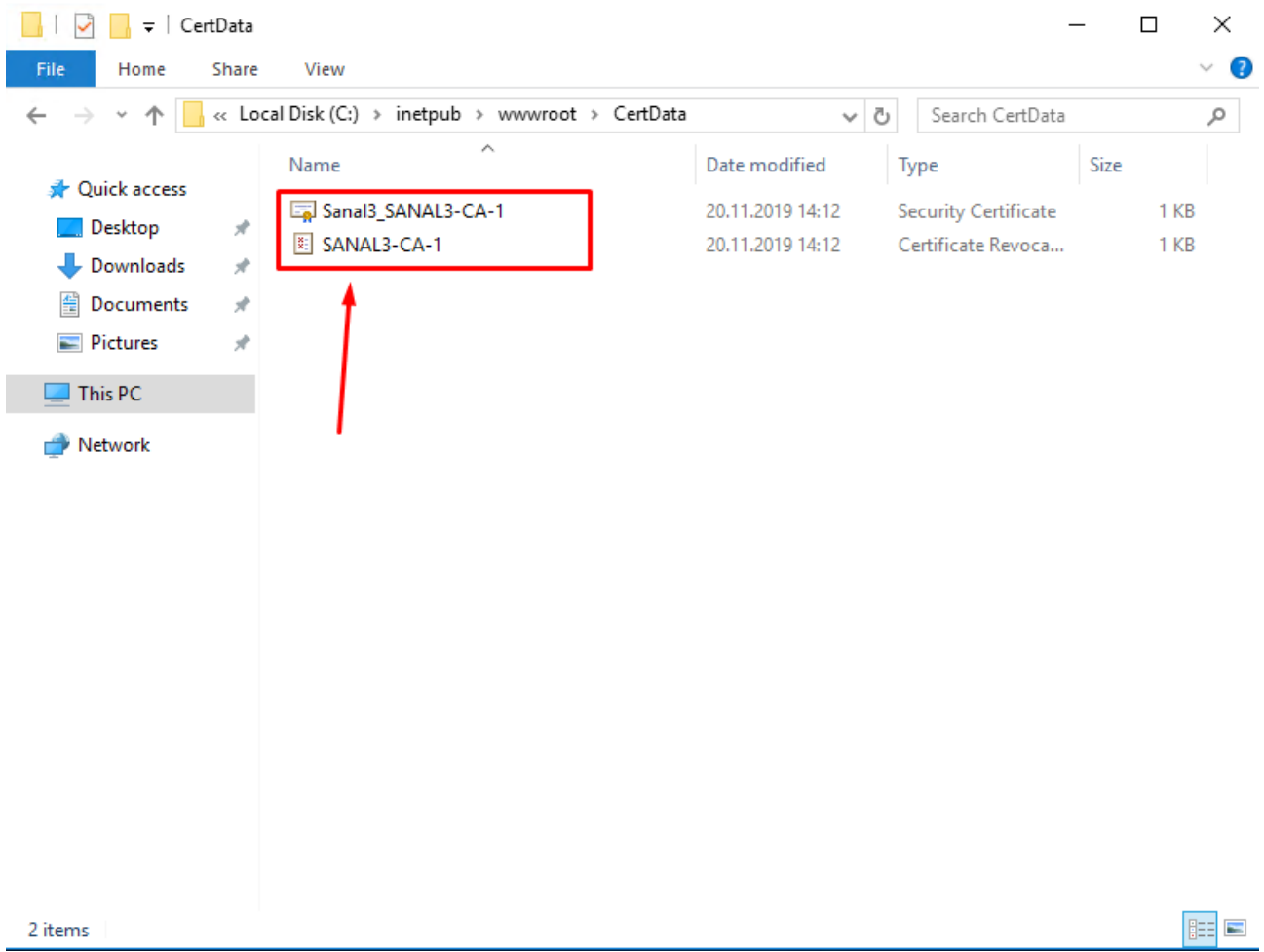
< Previous Next > **Close** Cancel

İşlem6 : Sanal3 cihazımızda oluşturduğumuz “certificate” dosyası Sanal2 cihazında masaüstüne kopyalanır. Ardından Sanal3 cihazındaki...

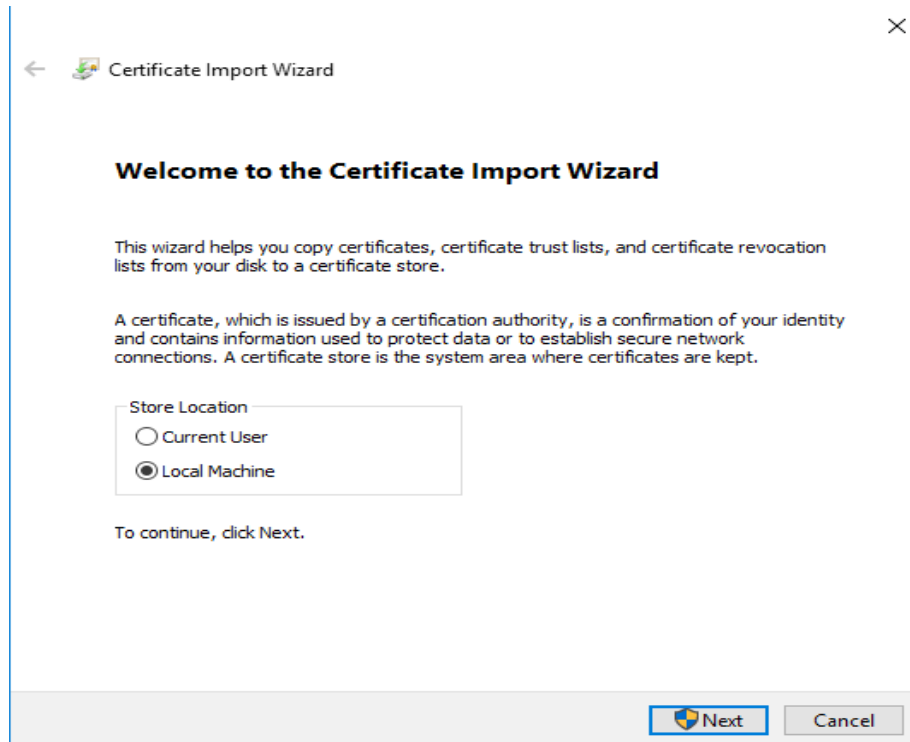


dizini altındaki dosyalar kopyalanır ve Sanal2 cihazında “C:” sürücüsü altında inetpub --> wwwroot --> “CertData” klasörü oluşturulup altına yapıştırılır. Klasörler yoksa maunal olarak oluşturulabilir.

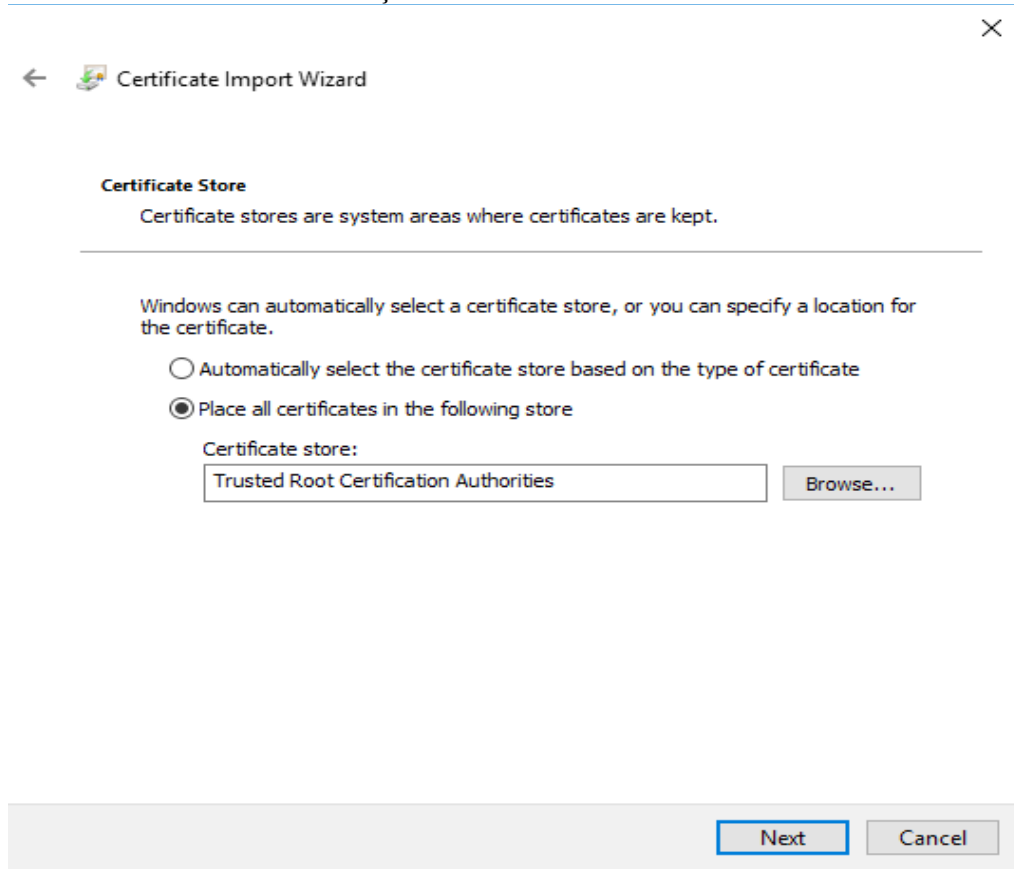




- Dosyalar kopyalandıktan sonra Sanal3 cihazımızdan kopyaladığımız “certificate” dosyasına sağ tıklanır ve “Install Certificate” denir. “Local Machine” seçilir.



- “Place all certificates in the following store” seçilir ve “Browse” denerek “Trusted Root Certification Authorities” seçilir ve Next denir.



← Certificate Import Wizard

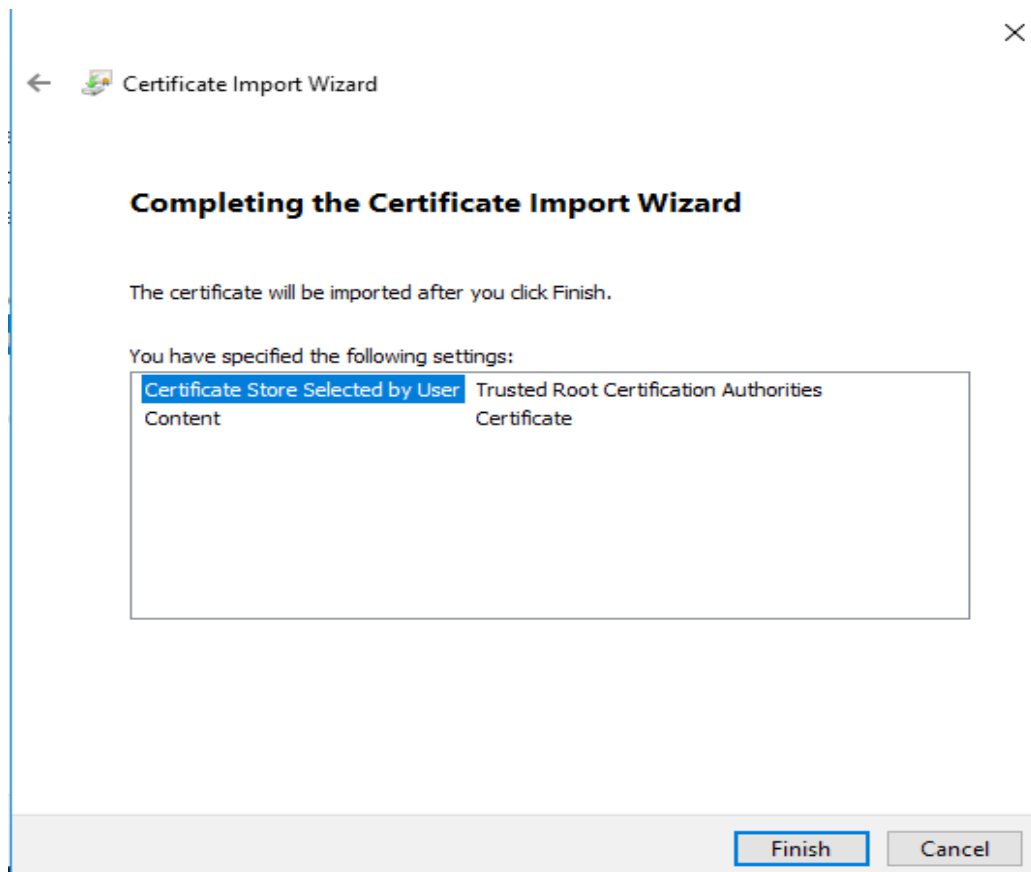
Certificate Store
Certificate stores are system areas where certificates are kept.

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:



← Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

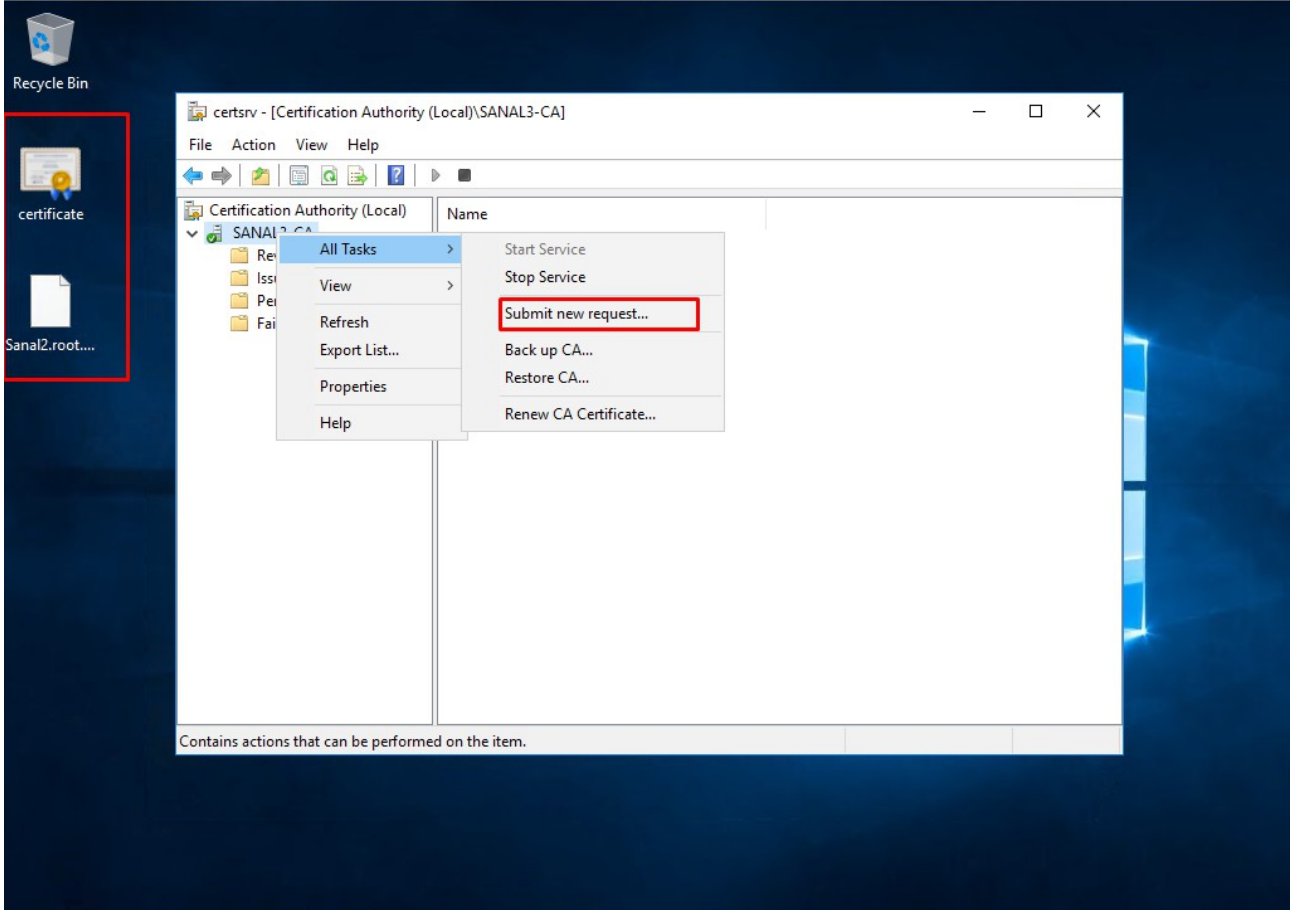
Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

- Yükleme tamamlandıktan sonra...

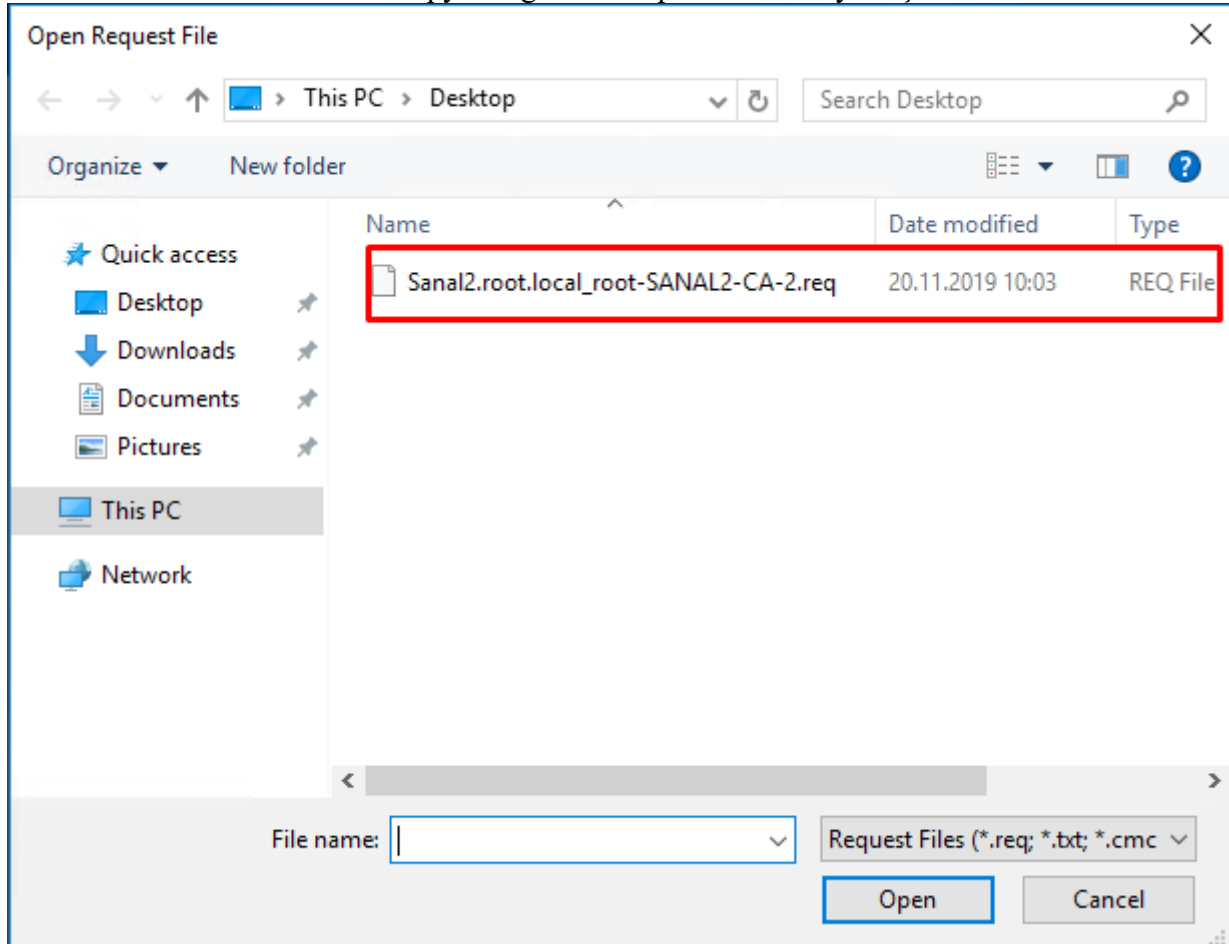
☒ Save a certificate request to file on the target machine:

File name:

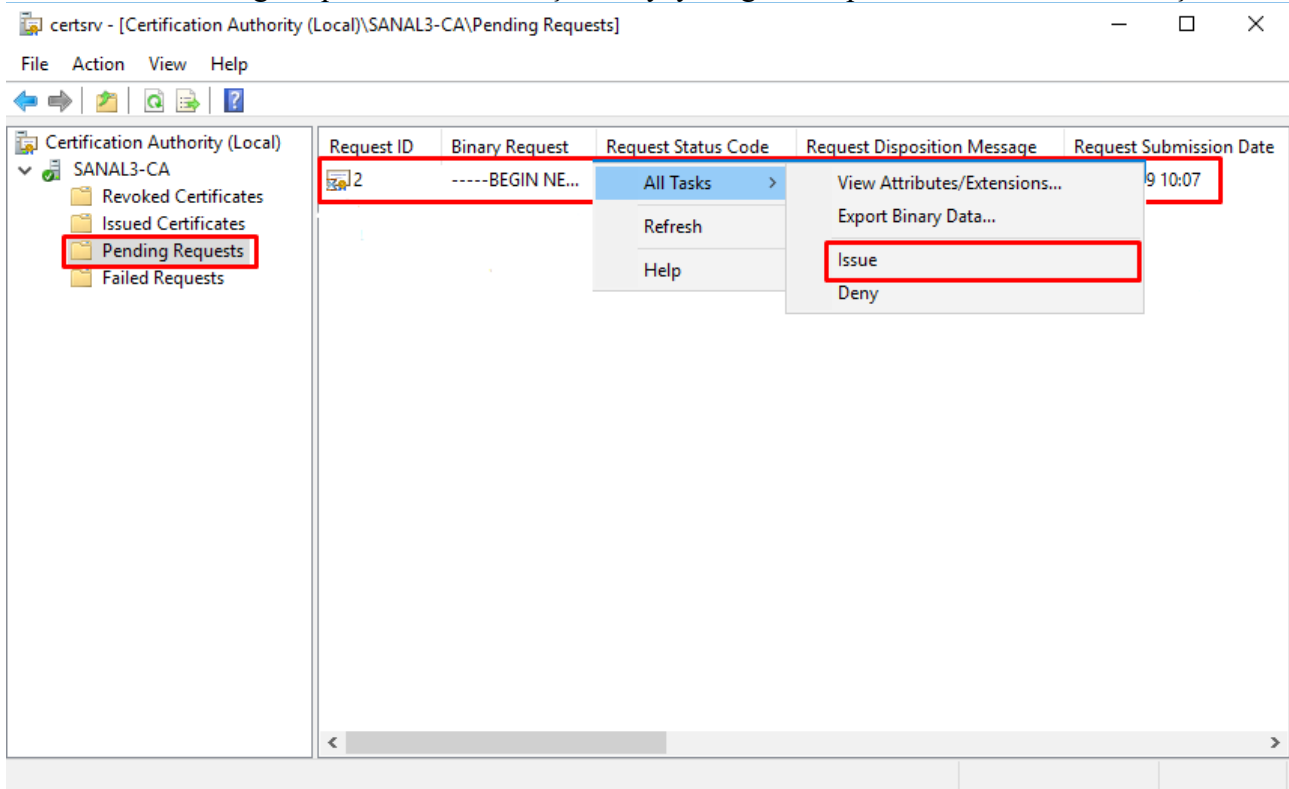
konumunda oluşturulan “.req” uzantılı dosya kopyalanır ve Sanal3 cihazına yapıştırılır. Ardından “Certificate Authority” altında cihazıma sağ tıklayıp All Tasks --> “Submit new requests” seçilir.



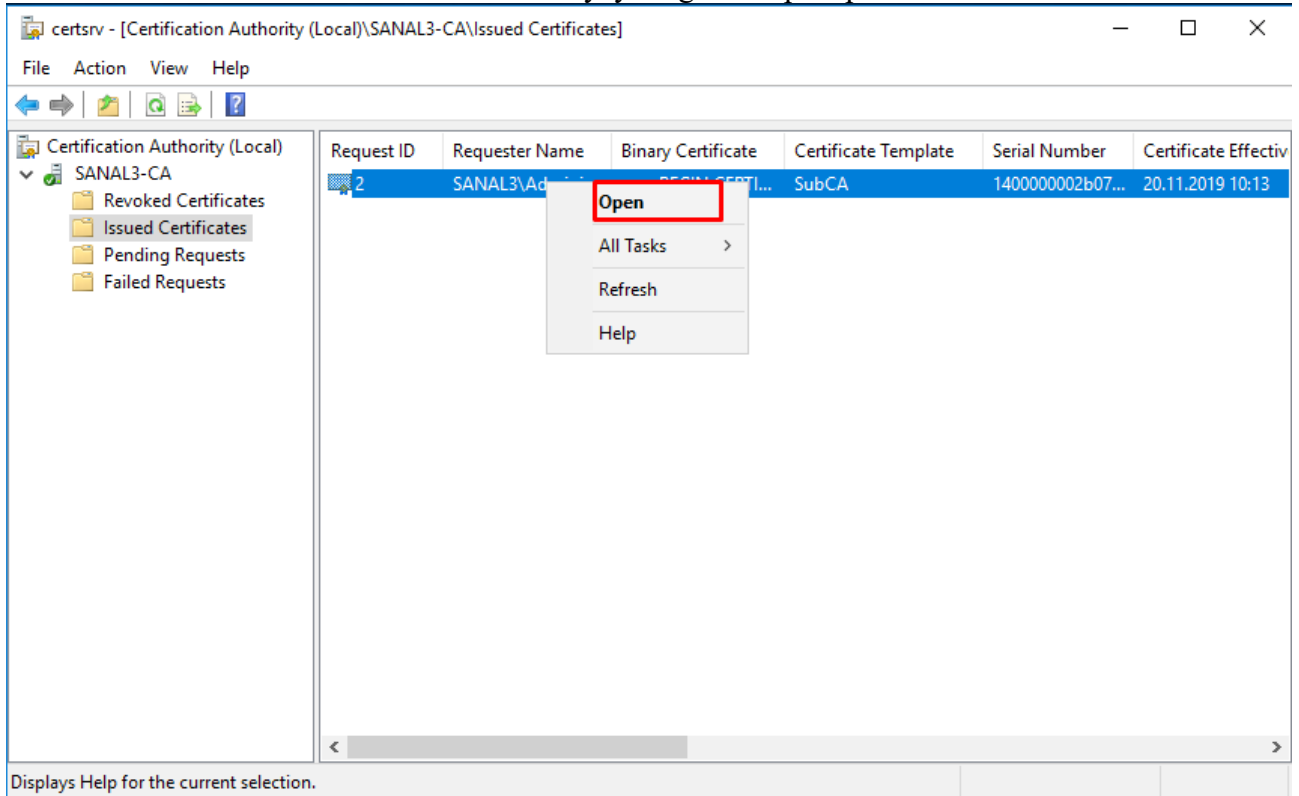
- Sanal2 cihazımızdan kopyaladığımız “.req” uzantılı dosya seçilir.



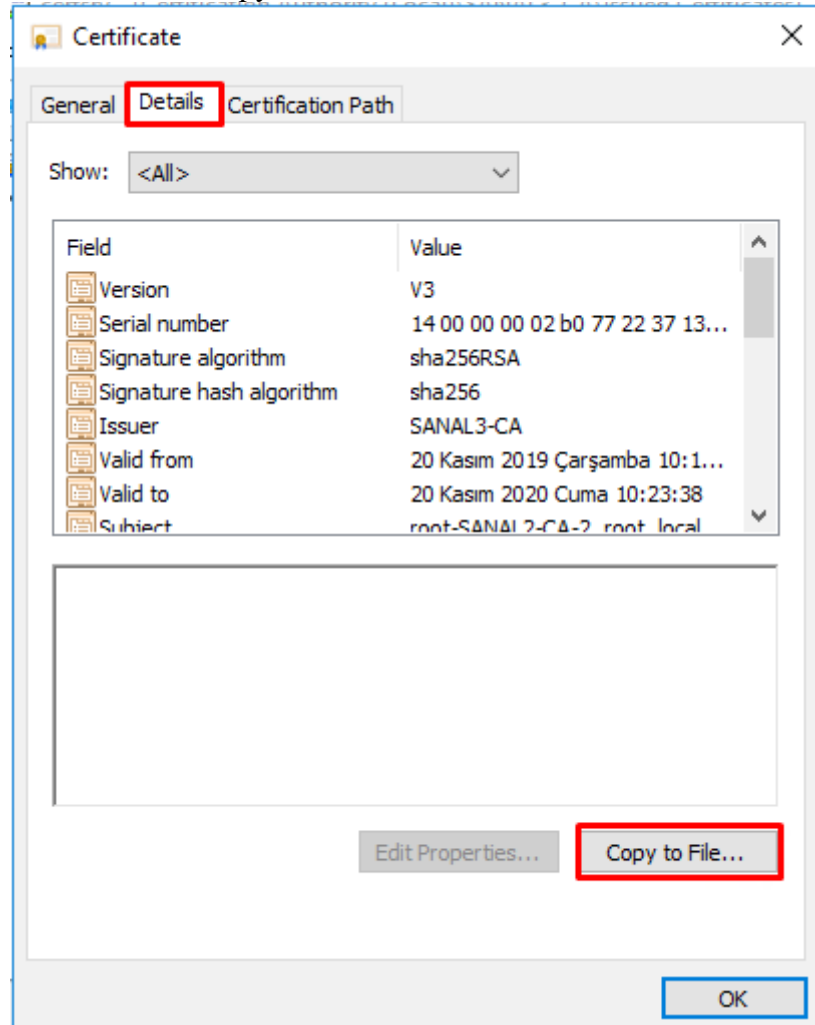
- “Pending Requests” altında oluşan dosyaya sağ tıklanıp All Tasks --> “Issue” seçilir.



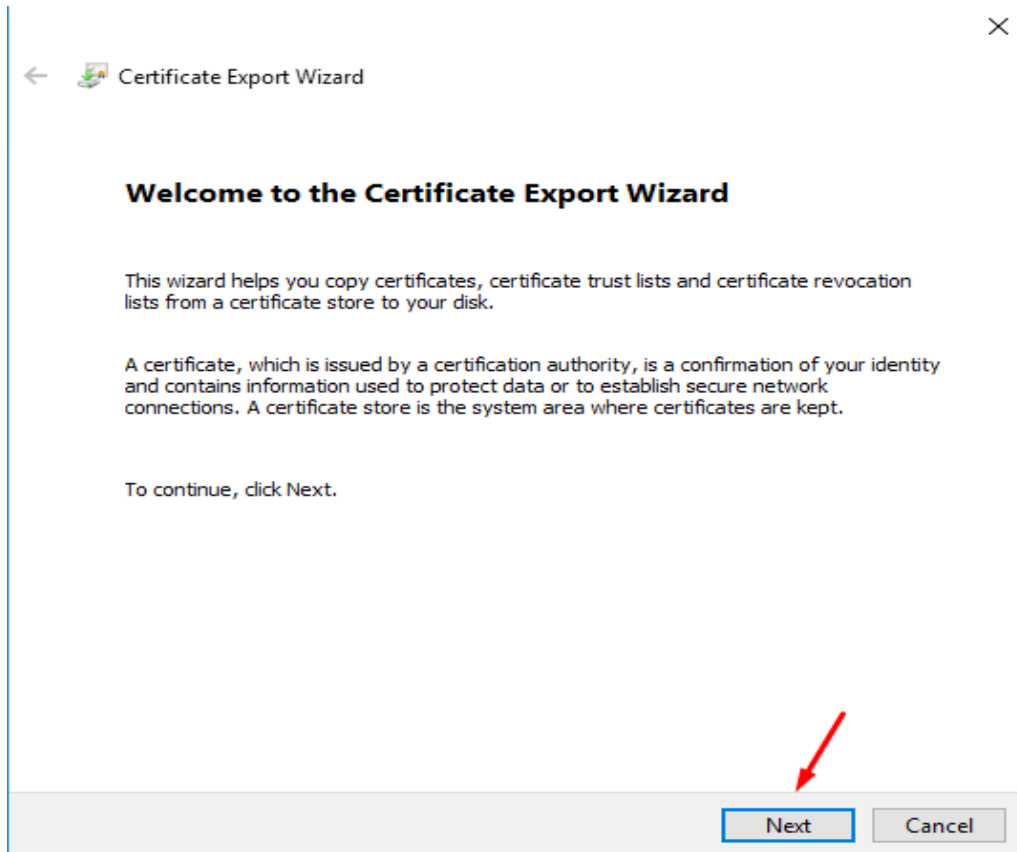
- “Issued Certificate” altında ki dosyaya sağ tıklanıp “Open” denir.



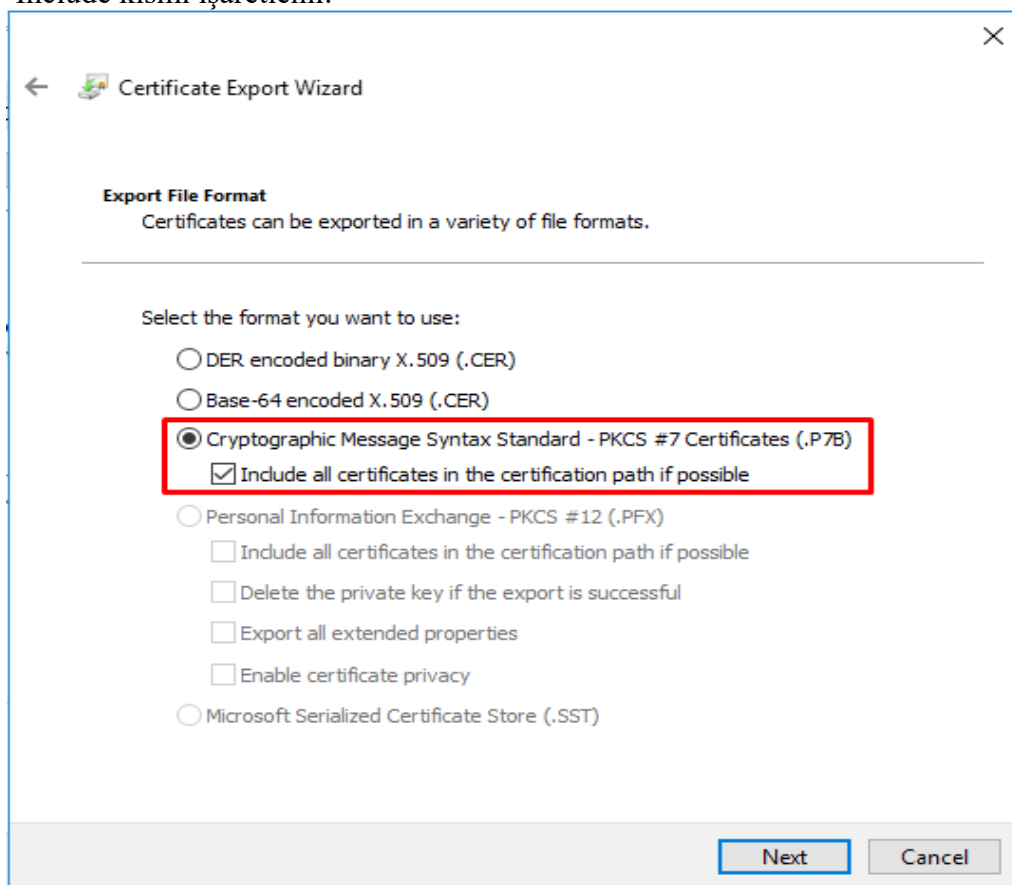
- “Details” kısmından “Copy to File” denir.



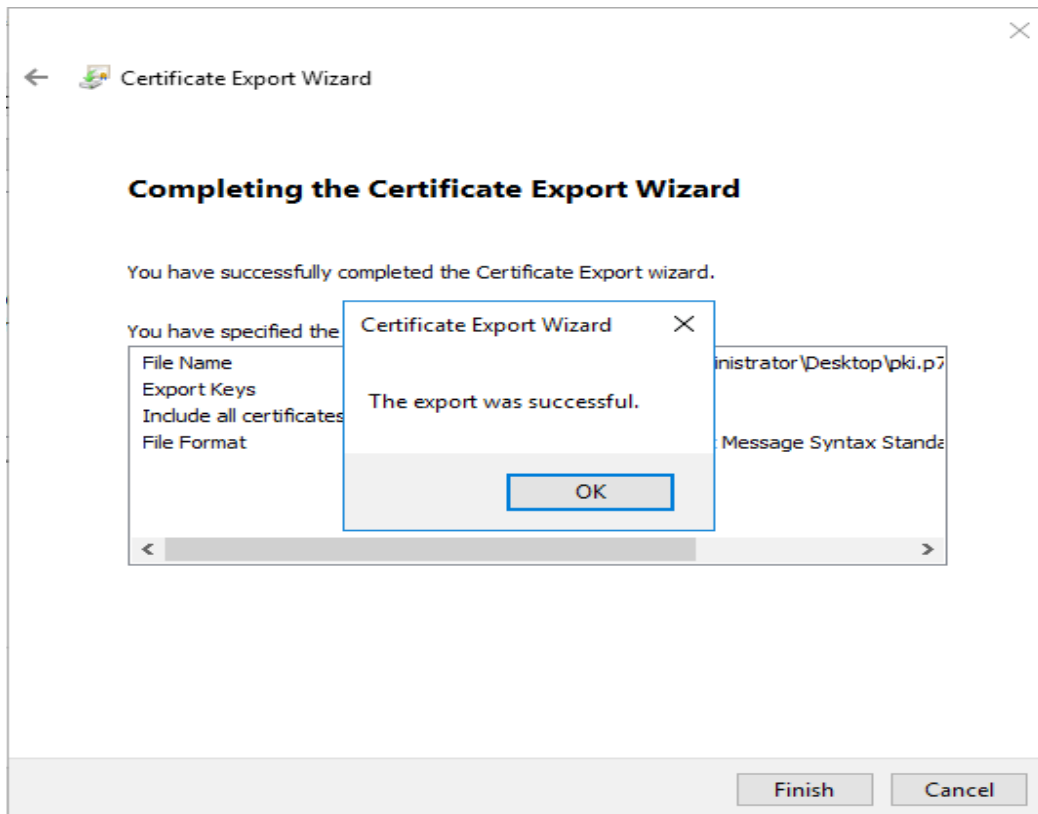
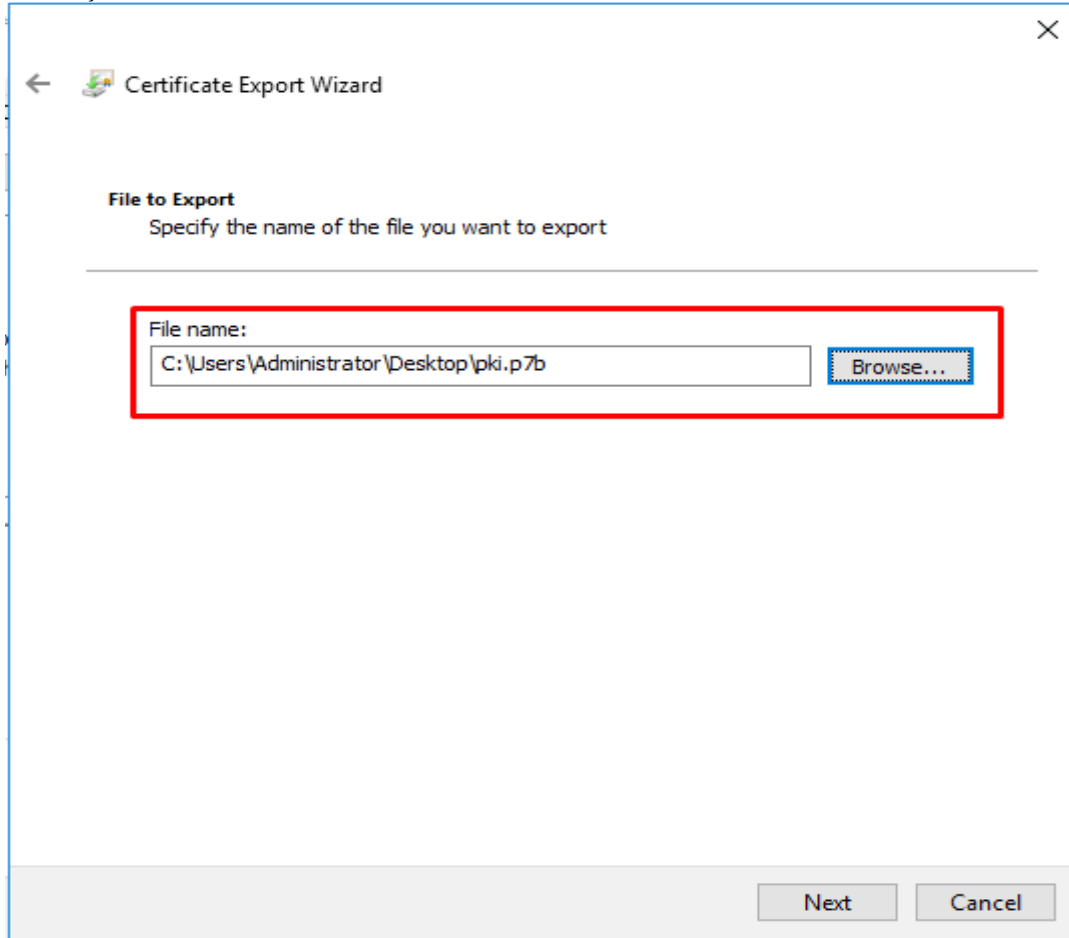
- Next denir.



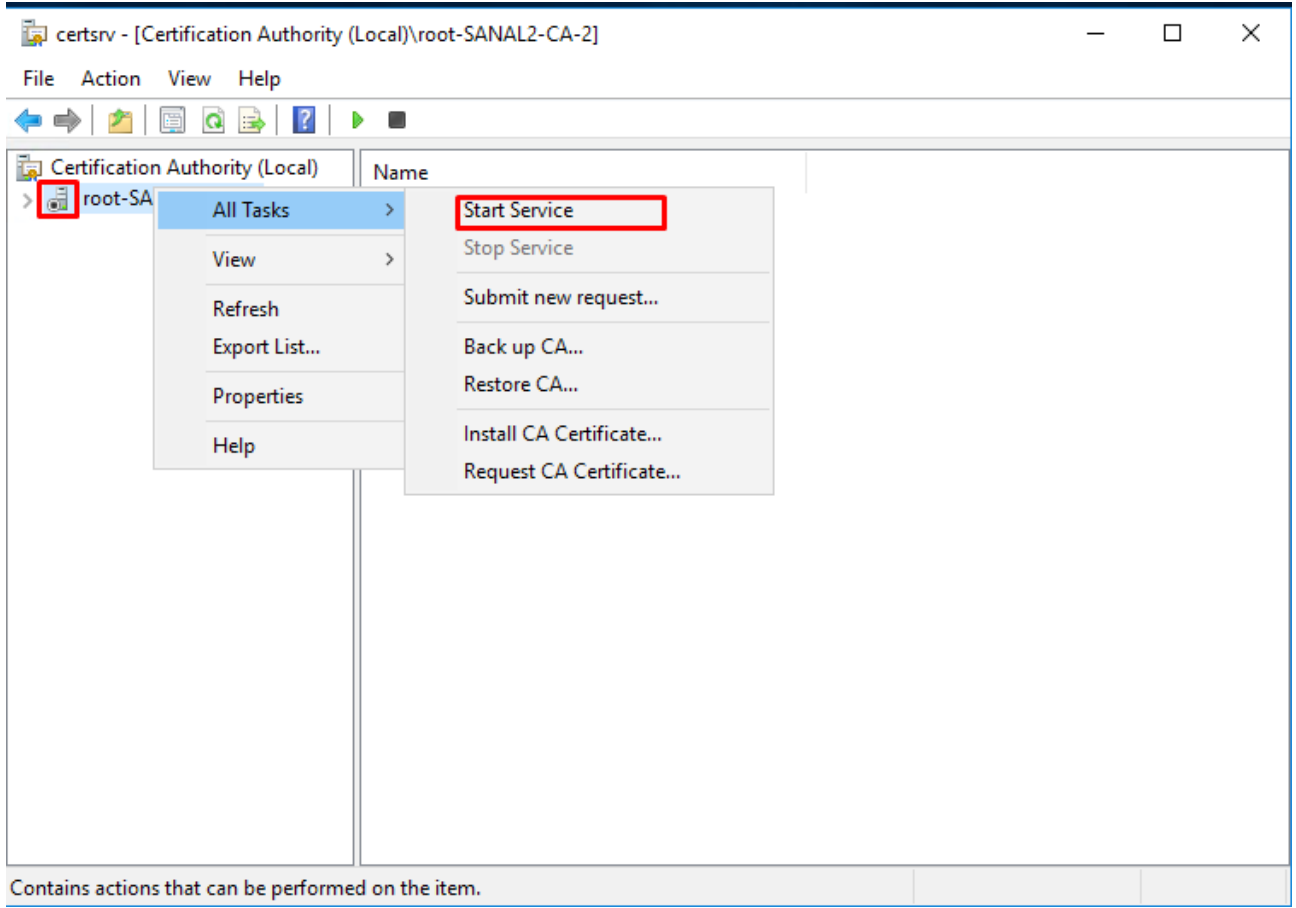
- “Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B) seçilir ve Include kısmı işaretlenir.



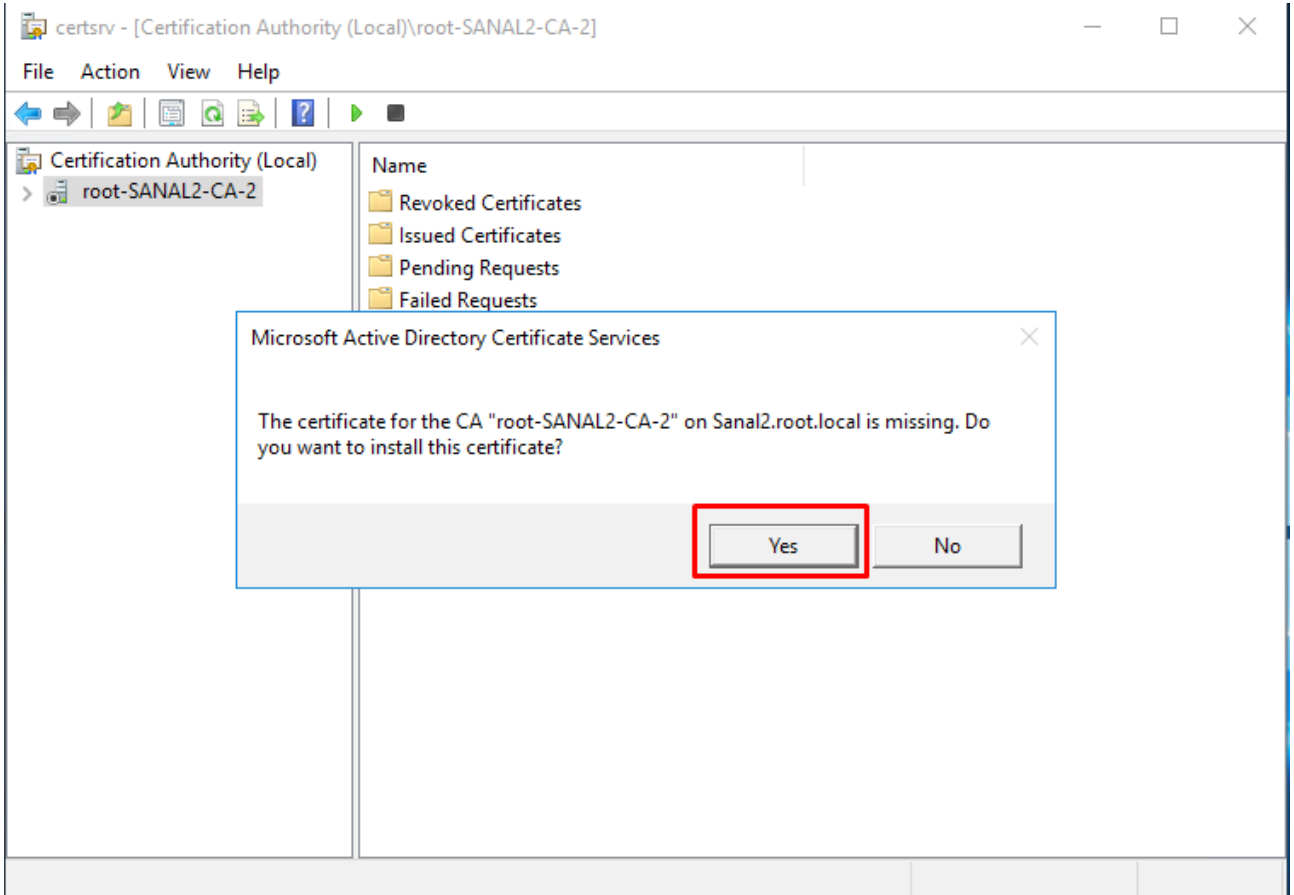
- Yeni sertifikanın oluşturulacağı dizin ve adı “.p7b” uzantılı olmak üzere belirlenir ve oluşturulur.



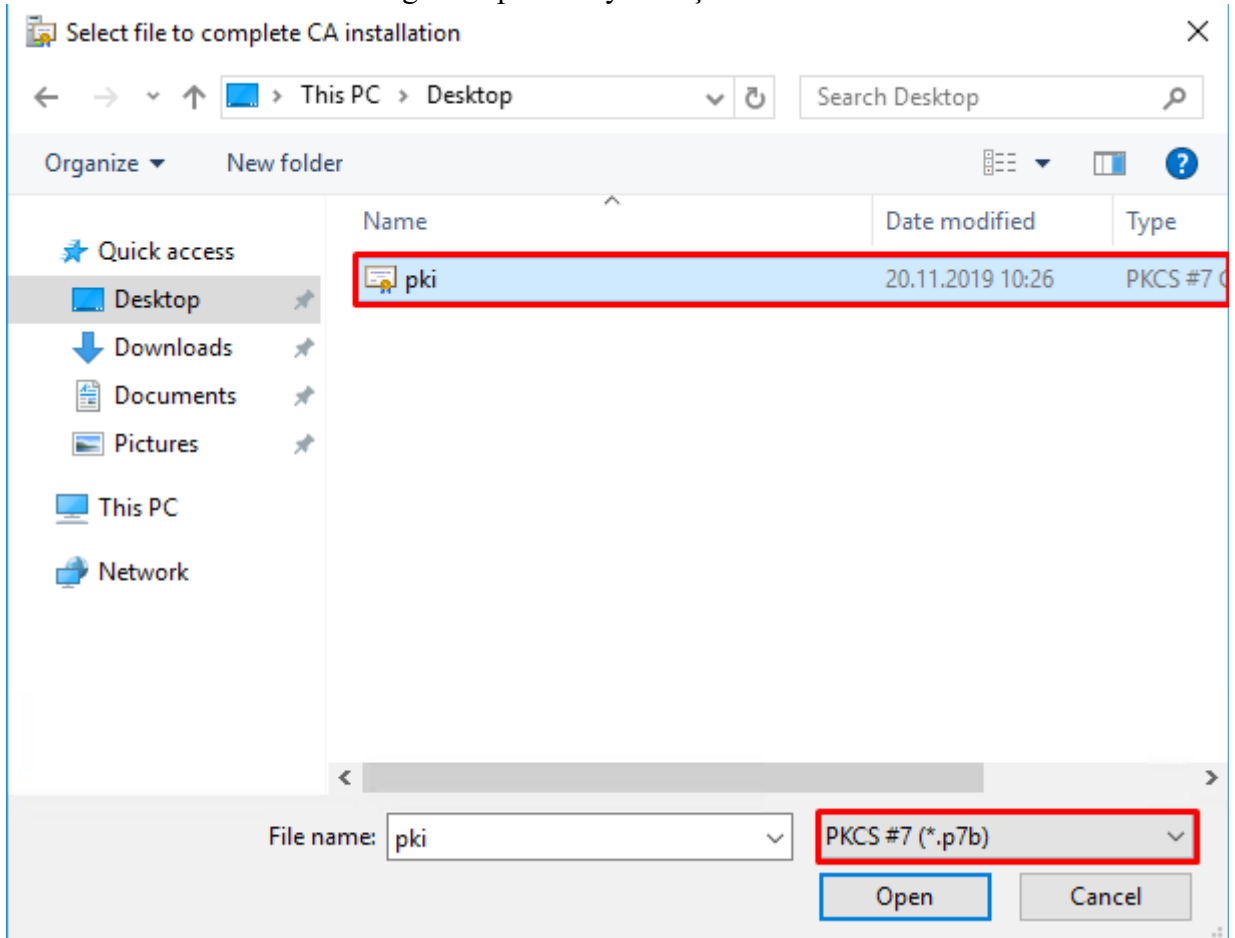
- Oluşturduğumuz “pki.p7b” dosyasını Sanal2 cihazımıza kopyalarız ve Sanal2 cihazımızda “Certificate Authority” açılır. Cihaza sağ tıklanıp All Tasks --> “Start Service” denir.



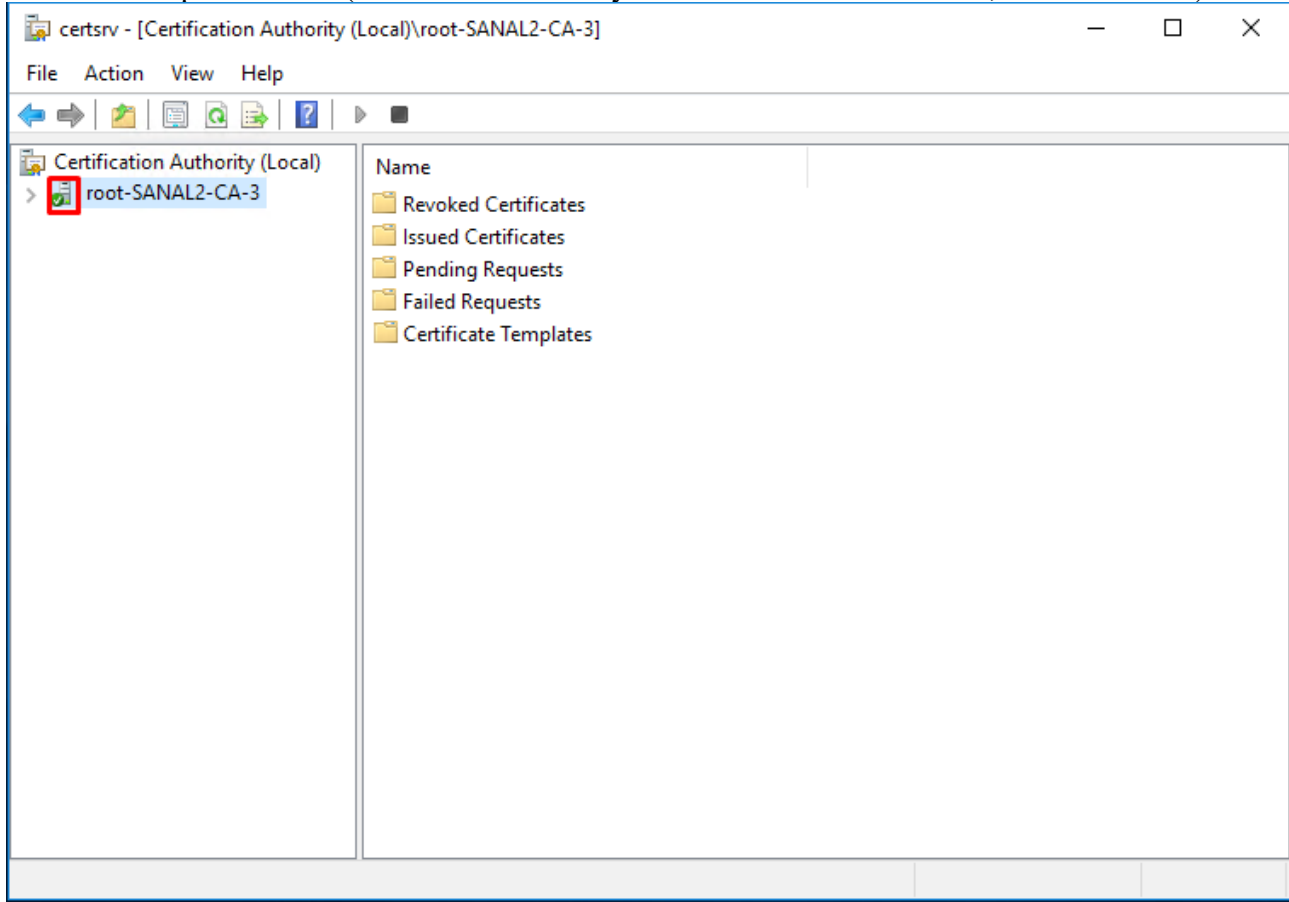
- Yes denir.



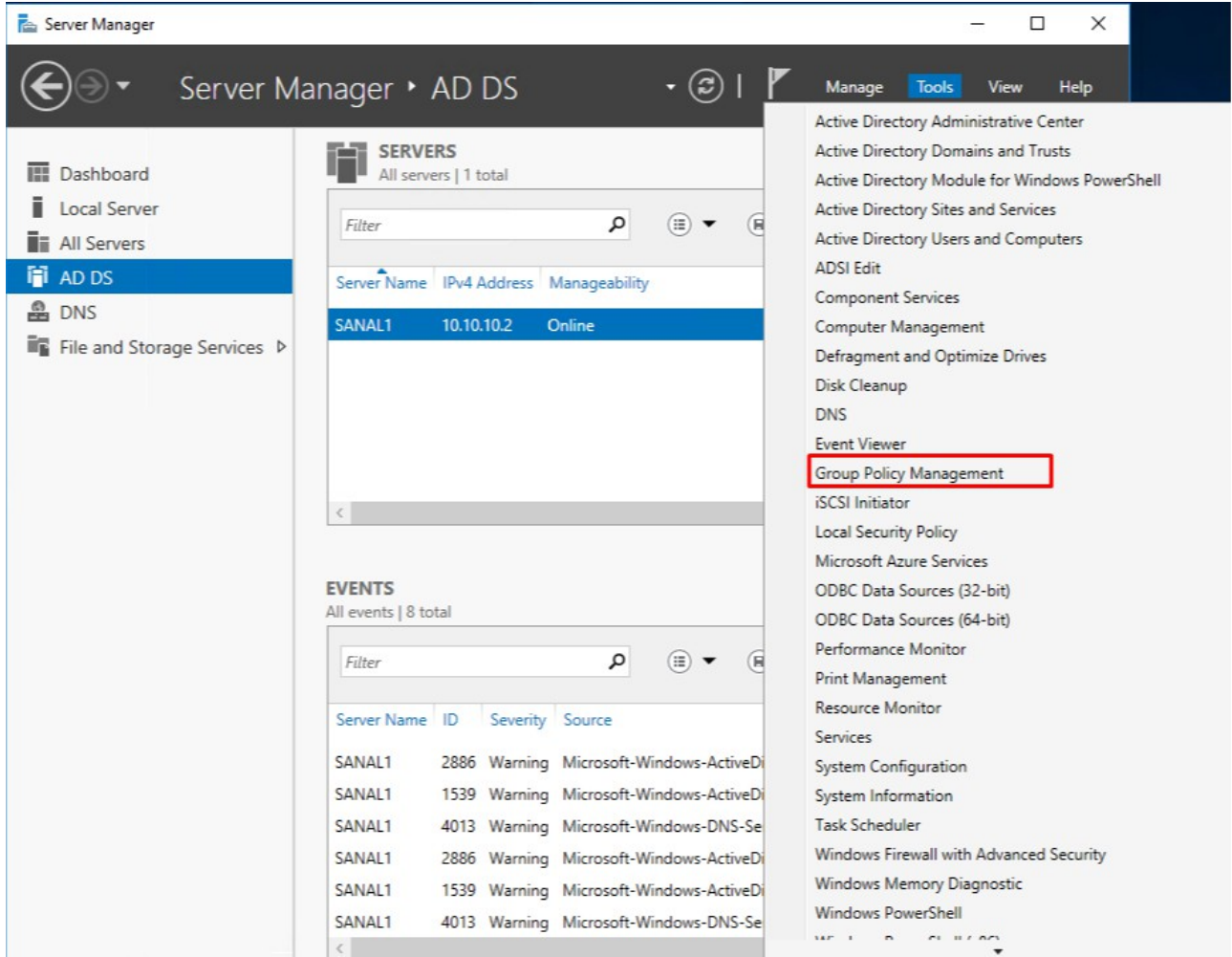
-Sanal3 cihazımızdan aldığımız “pki” dosyası seçilir.



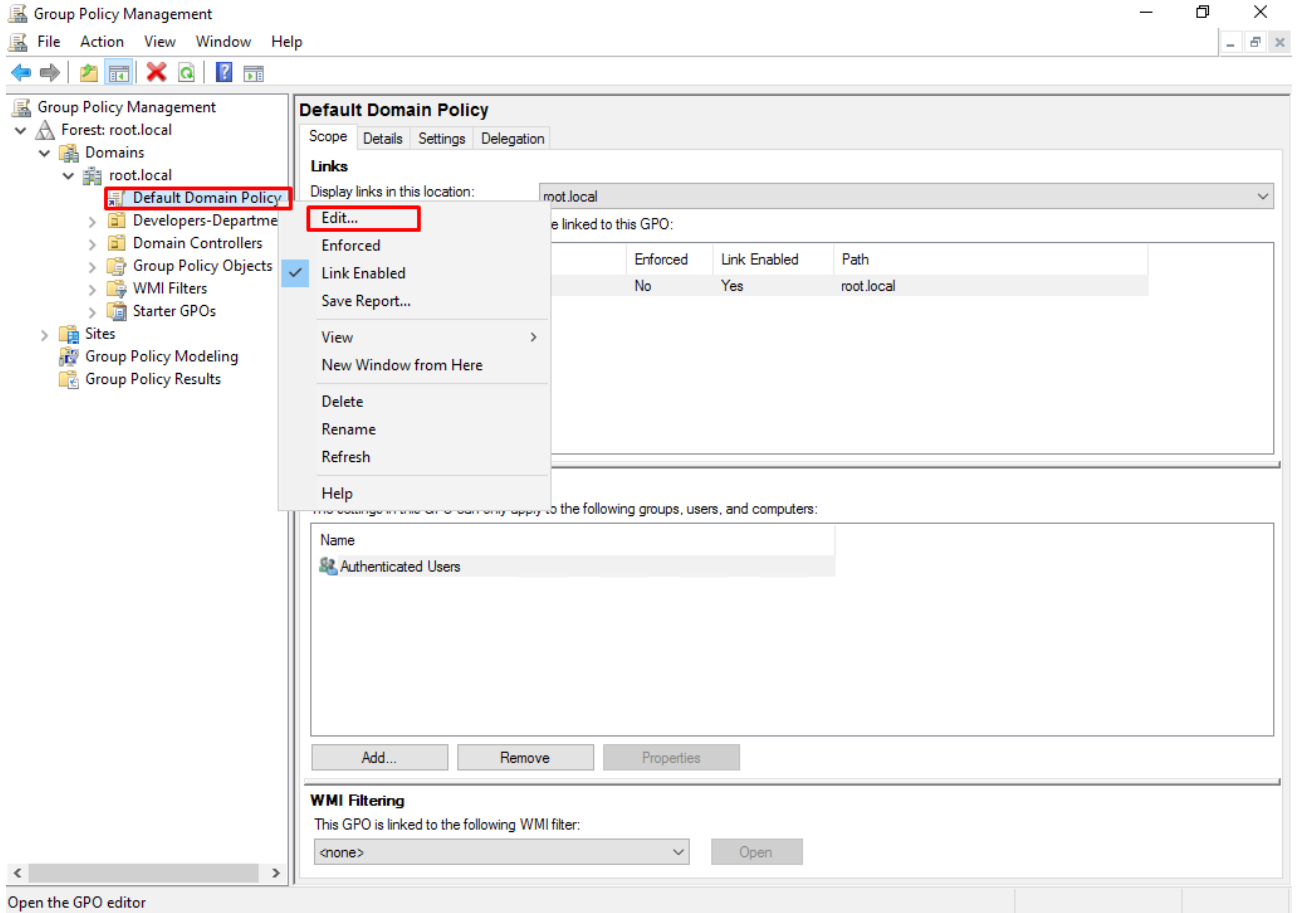
- Yönetim işlemi artık Sanal2 cihazı üzerinden yapılmaktadır bundan sonra Sanal3 cihazı kapatılabilir. (Hata alınırsa DNS ayarlarında sorun var demektir, kontrol ediniz!)



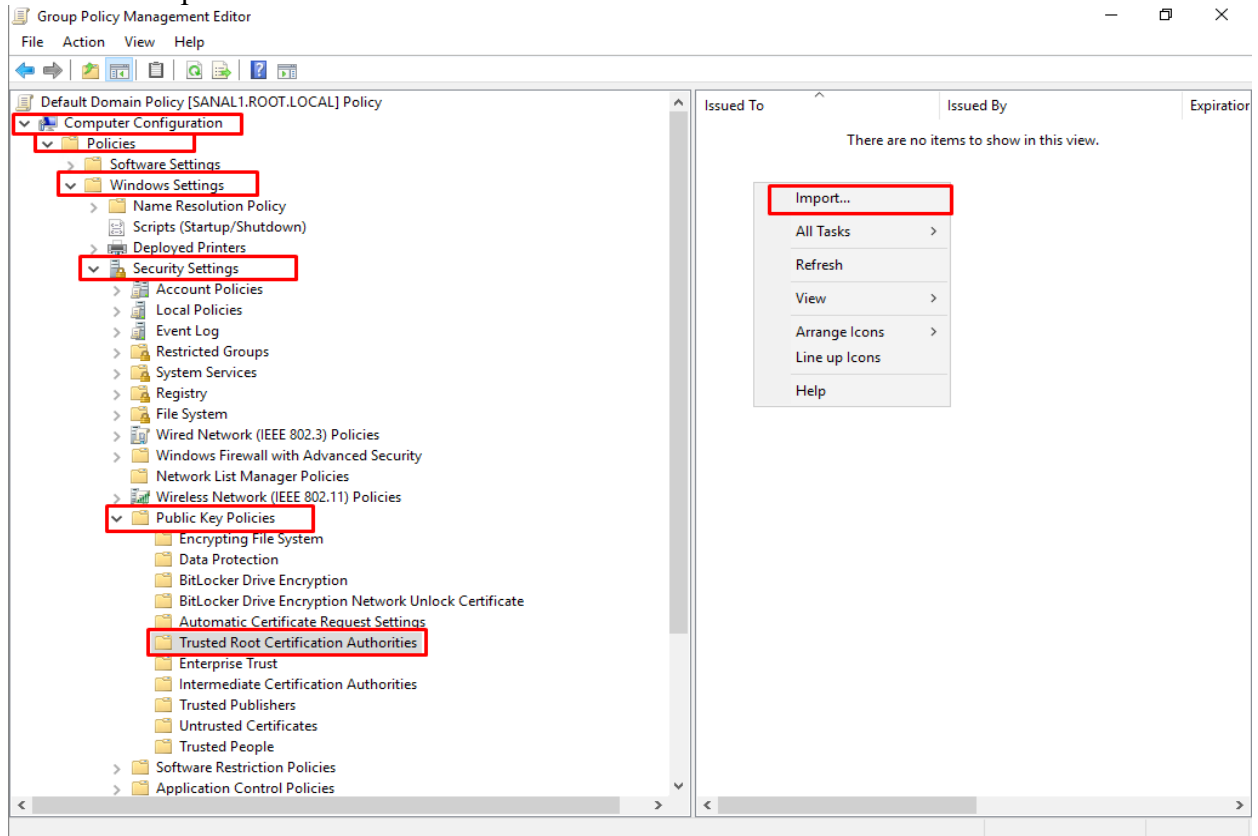
İşlem7 : Son adımlar DC olan Sanal 1 Cihazımızda yapılmakta olup, Sanal3 Cihazımızda ilk oluşturduğumuz “.crt” uzantılı dosya olan “Sanal3_SANAL3-CA-1.crt” dosyası Sanal1 cihazımıza kopyalanır. Ardından Server Manager üzerinden Tools kısmından “Group Policy Management” açılır.



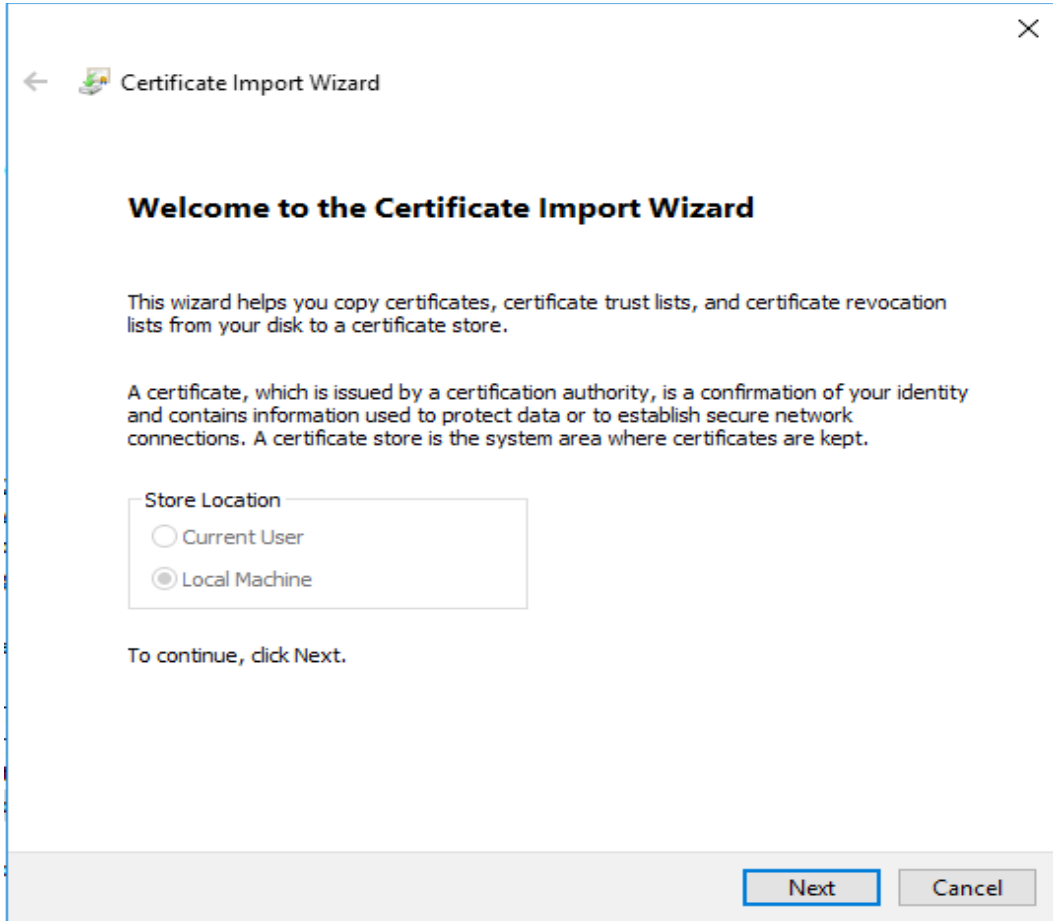
- “Default Domain Policy”e “Edit” denir.



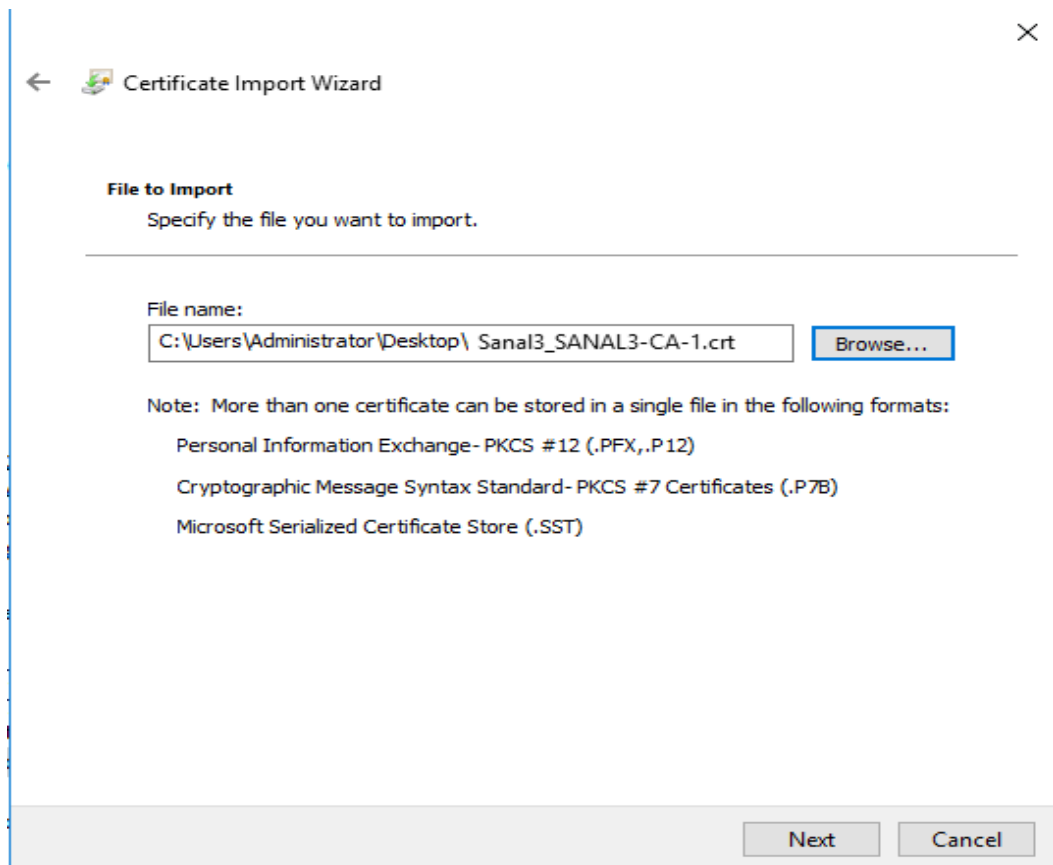
- Computer Configuration --> Policies --> Windows Settings --> Security Settings --> Public Key Policies --> Trusted Root Certification Authorities altında sağ tıklayıp “Import” deriz.



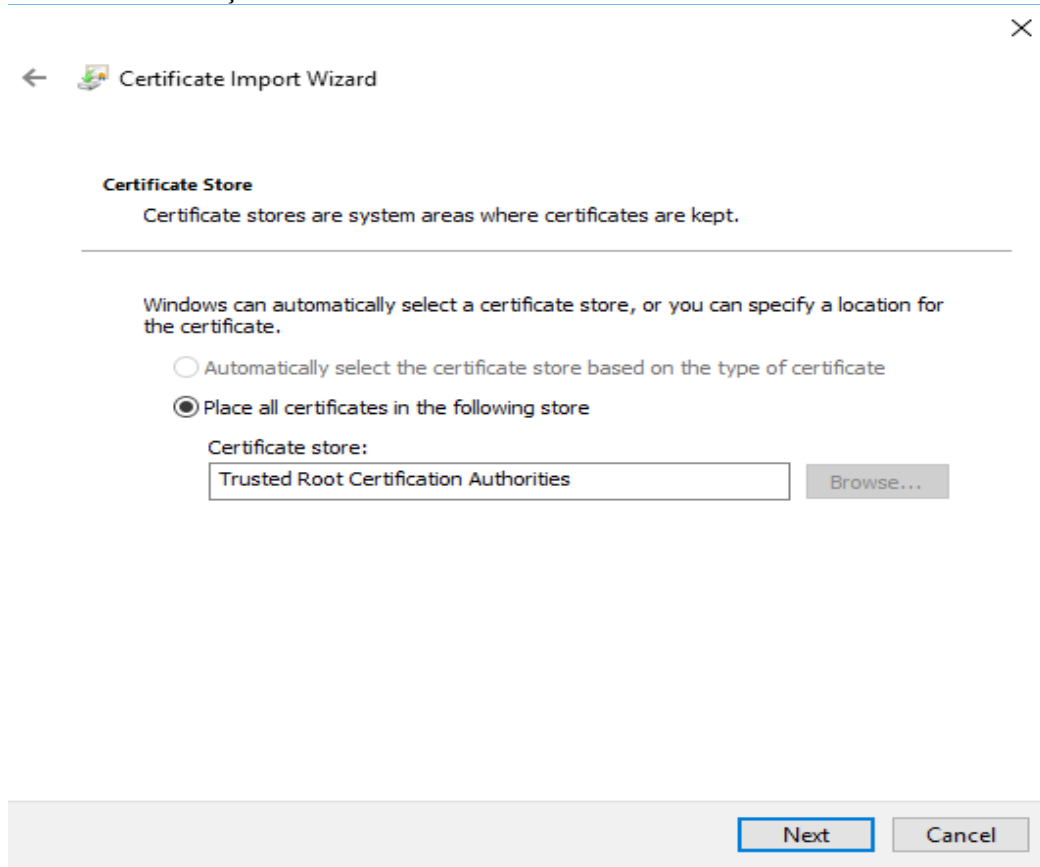
- Next denir.



- Sanal3 cihazımızdan aldığımız “.crt” uzantılı sertifika dosyası seçilir.



- “Place all certificates in the following store” seçilip “Trusted Root Certification Authorities” seçilir.



The screenshot shows the 'Certificate Import Wizard' window. The title bar says 'Certificate Import Wizard'. Below the title bar, there is a back arrow and a forward arrow. The main heading is 'Certificate Store'. Below it, a text box says 'Certificate stores are system areas where certificates are kept.' A horizontal line separates this from the next section. The next section says 'Windows can automatically select a certificate store, or you can specify a location for the certificate.' There are two radio buttons: 'Automatically select the certificate store based on the type of certificate' (unselected) and 'Place all certificates in the following store' (selected). Below the radio buttons, there is a text box labeled 'Certificate store:' containing 'Trusted Root Certification Authorities'. To the right of this text box is a 'Browse...' button. At the bottom right, there are 'Next' and 'Cancel' buttons.

← 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.

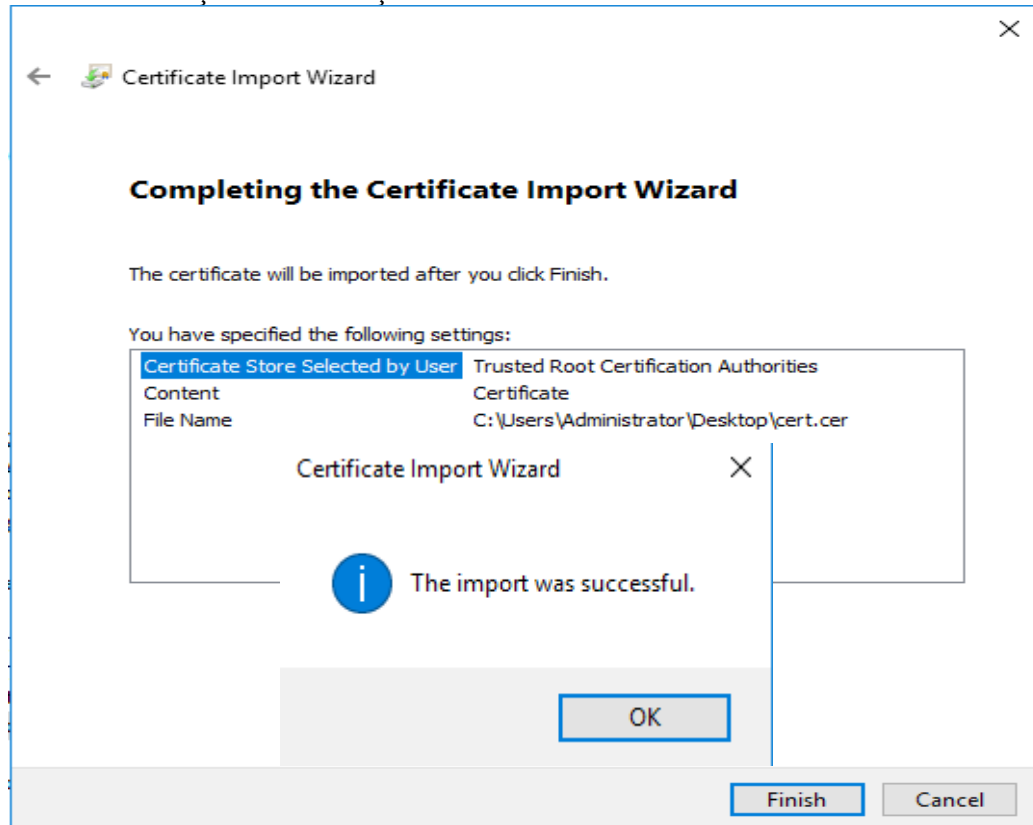
☐ Automatically select the certificate store based on the type of certificate
☒ Place all certificates in the following store

Certificate store:
Trusted Root Certification Authorities

Browse...

Next Cancel

- Ve Sertifika işlemleri bitmiş olunur.



The screenshot shows the 'Completing the Certificate Import Wizard' screen. The title bar says 'Certificate Import Wizard'. Below the title bar, there is a back arrow and a forward arrow. The main heading is 'Completing the Certificate Import Wizard'. Below it, a text box says 'The certificate will be imported after you click Finish.' Another text box says 'You have specified the following settings:'. Below this, there is a table with the following content:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate
File Name	C:\Users\Administrator\Desktop\cert.cer

Below the table, there is a 'Certificate Import Wizard' window with a close button (X). Below this, there is a blue information icon (i) and the text 'The import was successful.' At the bottom right, there are 'Finish' and 'Cancel' buttons.

← Certificate Import Wizard

Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate
File Name	C:\Users\Administrator\Desktop\cert.cer

Certificate Import Wizard

The import was successful.

OK

Finish Cancel

- Yetki ayarları ile Java grubuna sertifika yetki verilmemesi sebebiyle, üyesi olan “java2” kullanıcısı sertifika hatası almaktadır. Artık domain içinde izin verilen sertifika yetkili kullanıcılar, gruplar ve OU'lar direk giriş yapabilmektedirler.

