PKI Infrastructure

Table of Contents

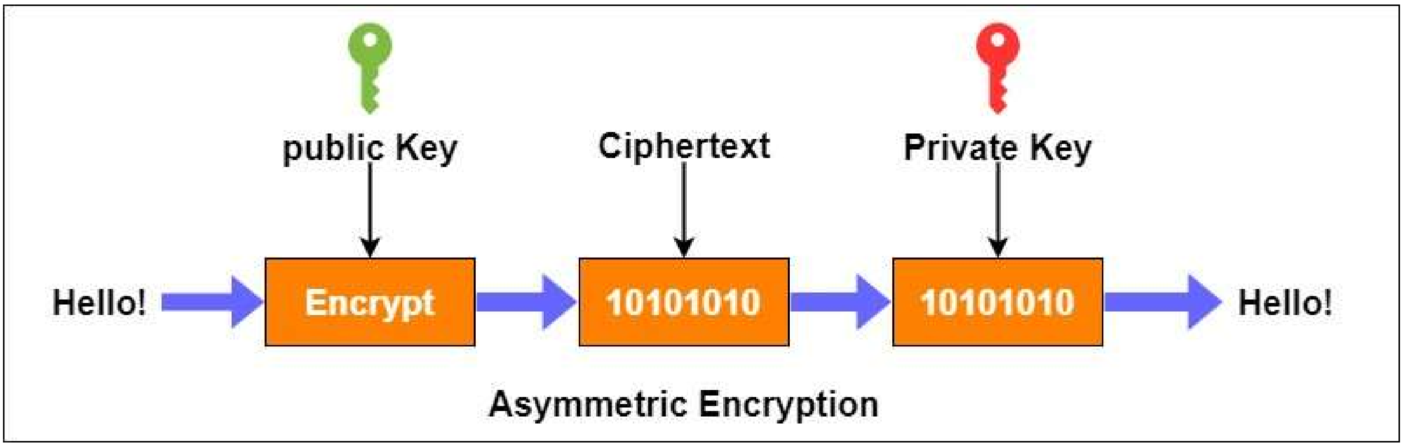
1 Executive Summary:

Secure communication can only be assured if there is a way to verify the other party's identity digitally. Otherwise, an assailant can easily capture the transmission and impersonate involved entities, by performing a MITM Attack. After the introduction of public-key cryptography, the technology becomes the game-changer in decision making to verify a partner's public key trust. in the context of the private key they hold. Means that only legitimate users or system who holds the respective private key can communicate with each other

2 Introduction:

Public Key infrastructure is defined as a framework for managing digital certificate, encryption keys and anything in between. the primary(Isirova and Potii, 2018) role of the PKI to Establish the identity and encrypt the data flowing across the network, thus protective sensitive information being access by un-authorised parties, public Key Cryptography is the system that makes it possible by issuing two key systems that make both parties to verify each other identities and then establish the encrypted connection between each other

The Authentication process relies on the Asymmetric Encryption, in which two key systems Public Key and Private Key combination used to encrypt and decrypt the data so anything encrypted with the public key can be decrypted by the private key .Figure 1.1 Graphical Presentation is the clear and concise process how Asymmetric Encryption works

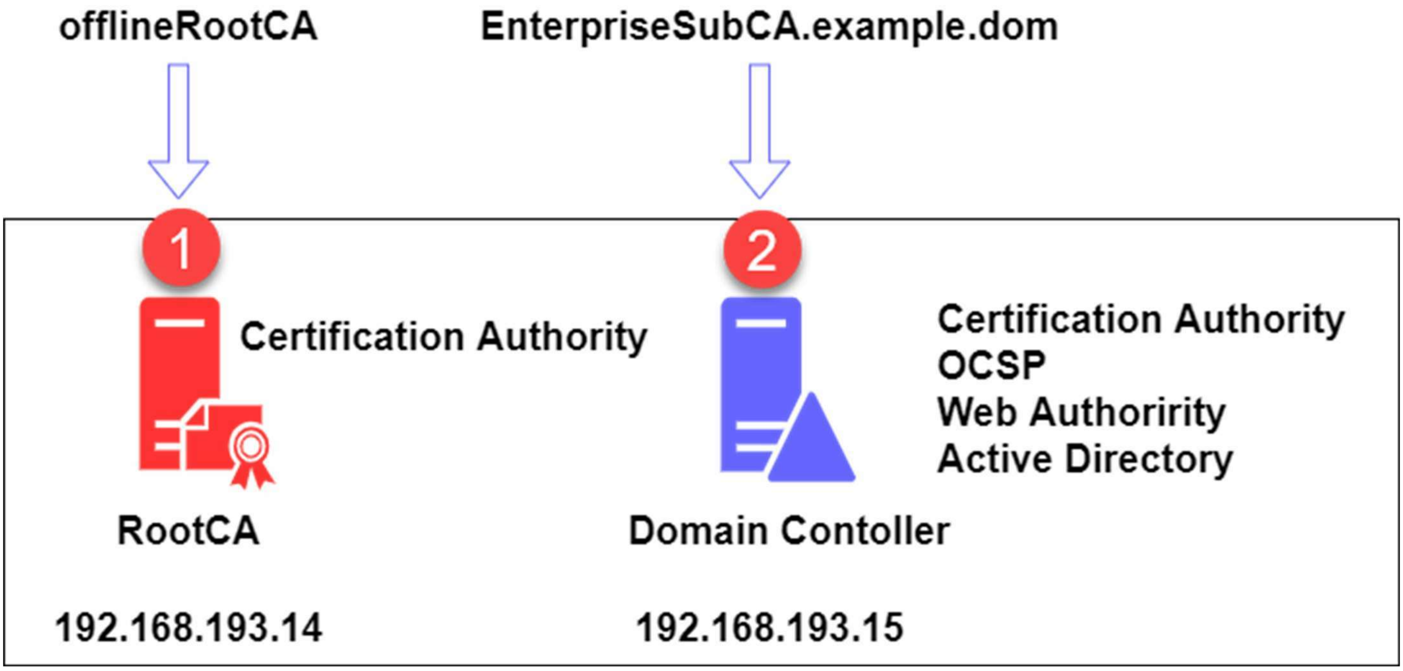


Encryption and Decryption Process is Vice-versa according to Figure 1

.

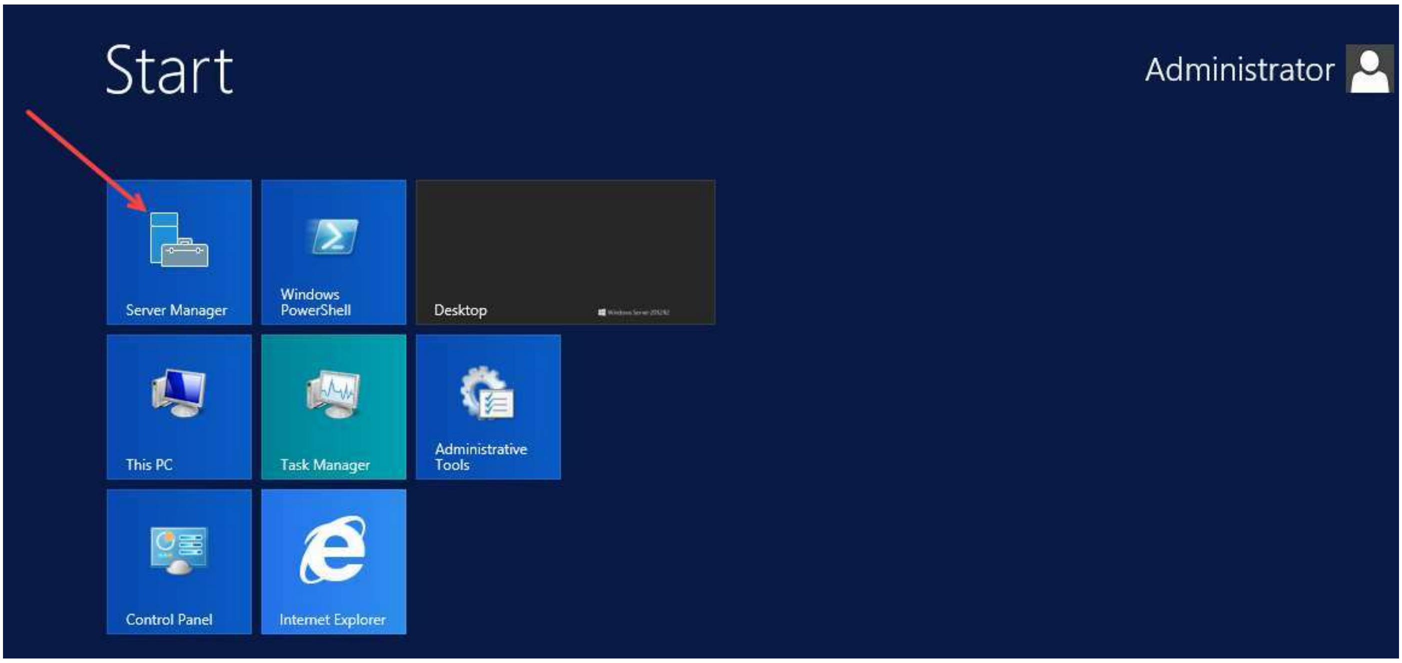
this paper demonstrates an SSL and PKI design Implementation in detailed structure overview and evaluates the security posture of if its applicability and availability in the context of the different attack vector and threat model and It also explore critical discussion and ethical issue based on previous research and current research outcome. then it will suggest the remediation steps which can be applied to protect and harden the current PKI system,

3 SSL PKI Design & Implementation:

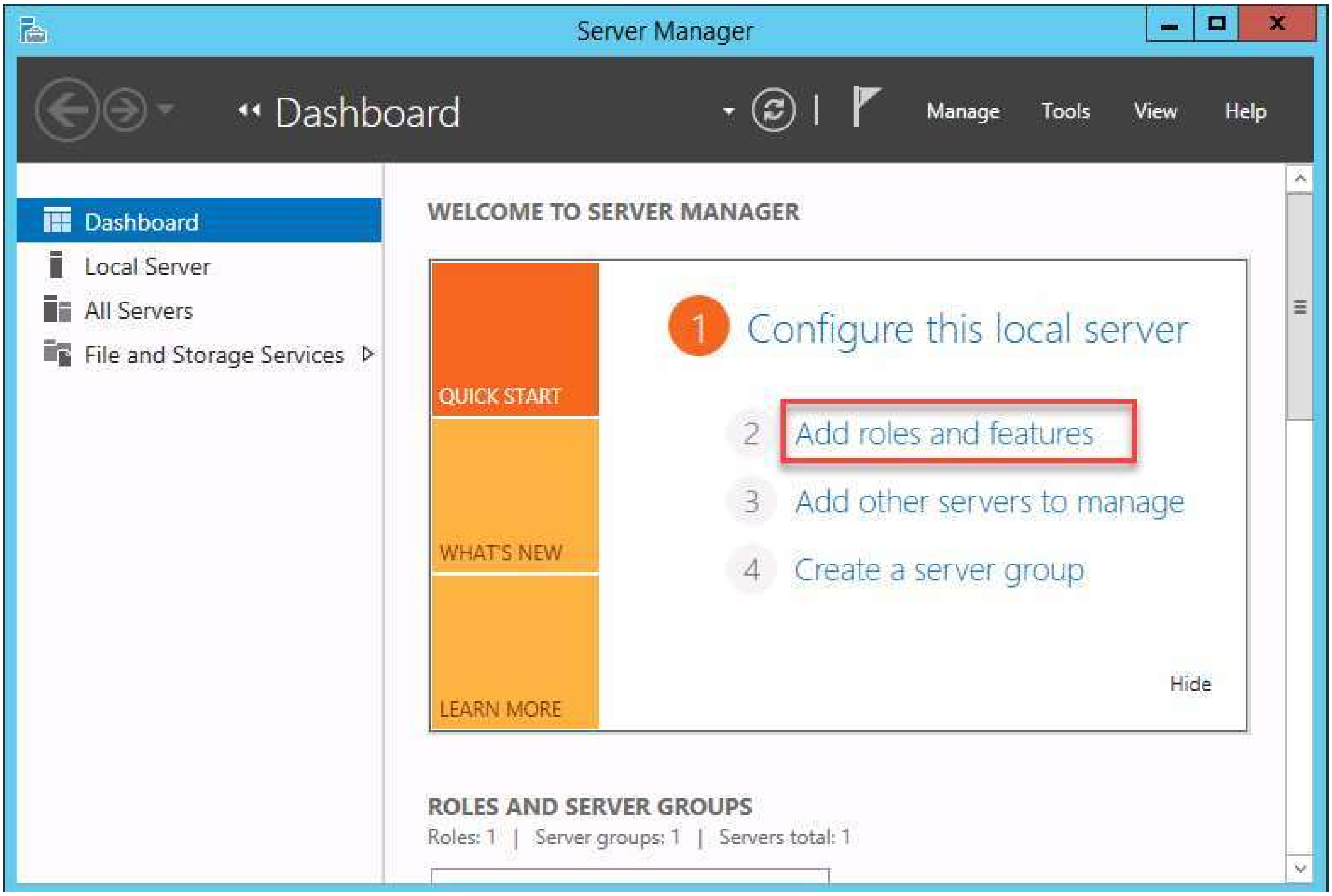


3.1 Install and configure an offline Root Certification Authority

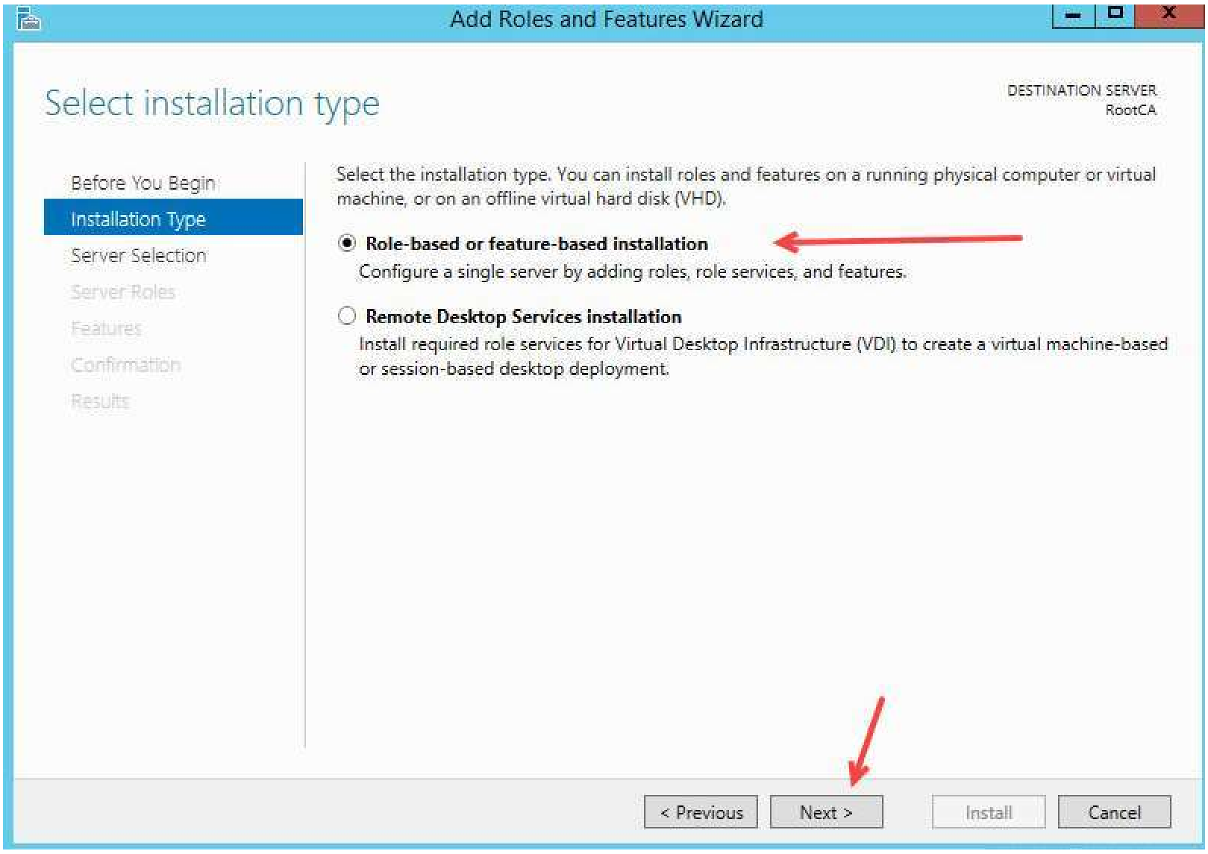
1 Click on the Server manager to install Certificate service



2 Click on the Add Role and Feature



3 Select the **Role-based** or **Feature-based** Installation and click next



Add Roles and Features Wizard

Select installation type

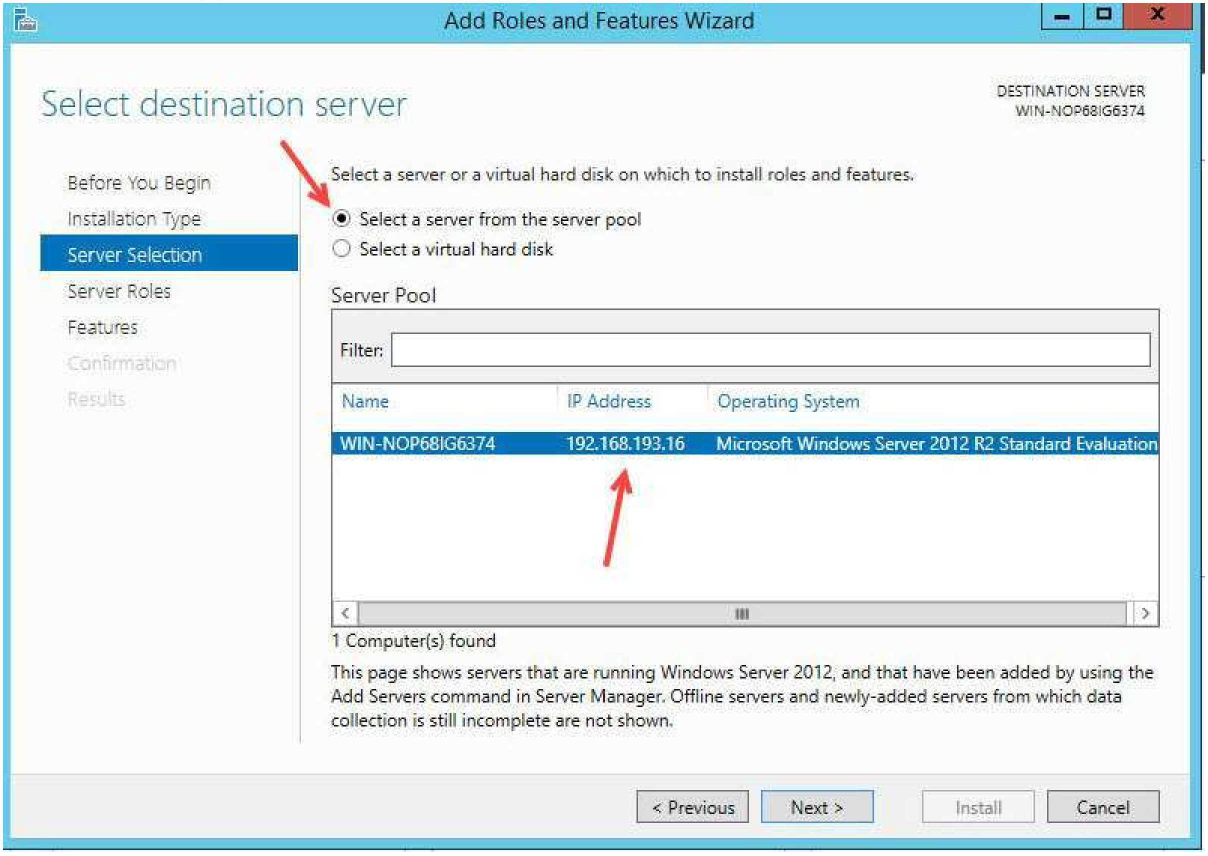
DESTINATION SERVER
RootCA

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.

4 Select the Applicable server from the List



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
WIN-NOP68IG6374

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

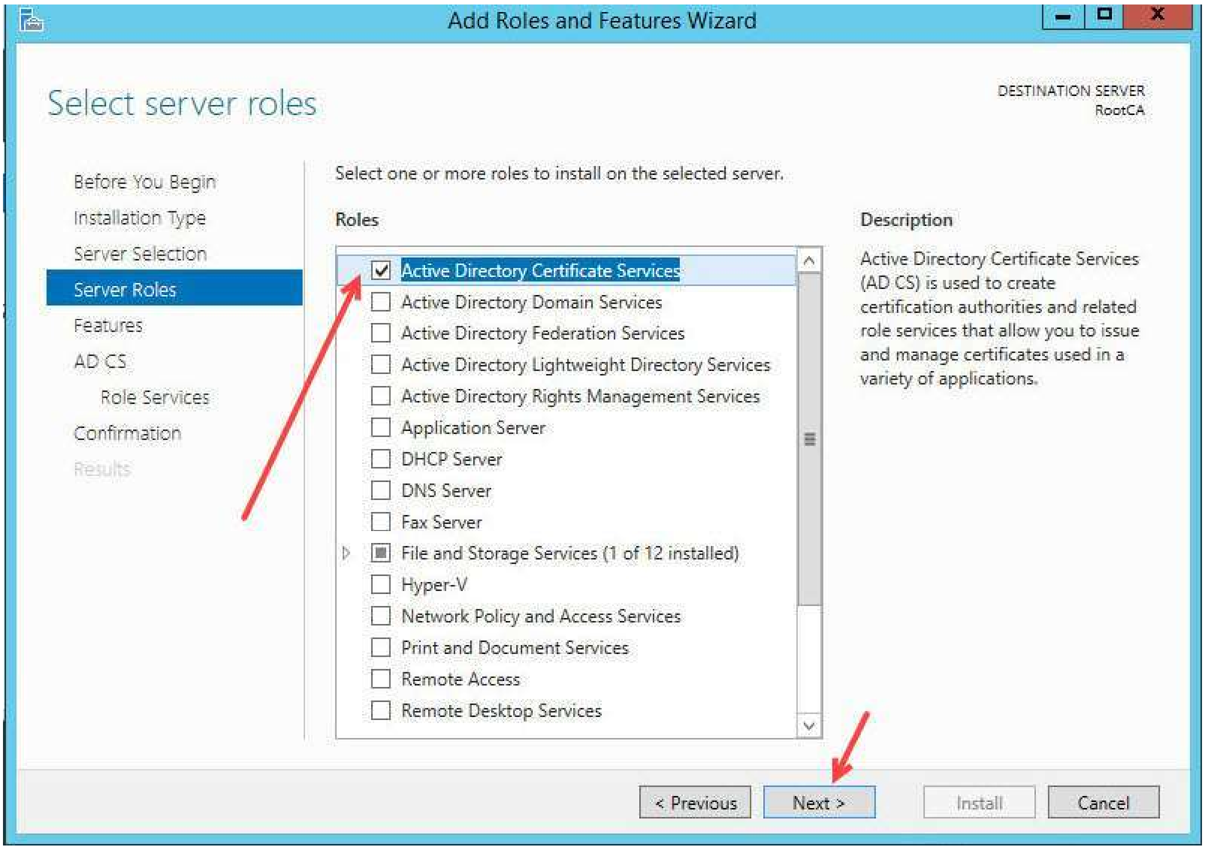
Filter:

Name	IP Address	Operating System
WIN-NOP68IG6374	192.168.193.16	Microsoft Windows Server 2012 R2 Standard Evaluation

1 Computer(s) found

This page shows servers that are running Windows Server 2012, 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.

5 Click on the ***Active Directory Certificate service*** and click on the next



Select server roles

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

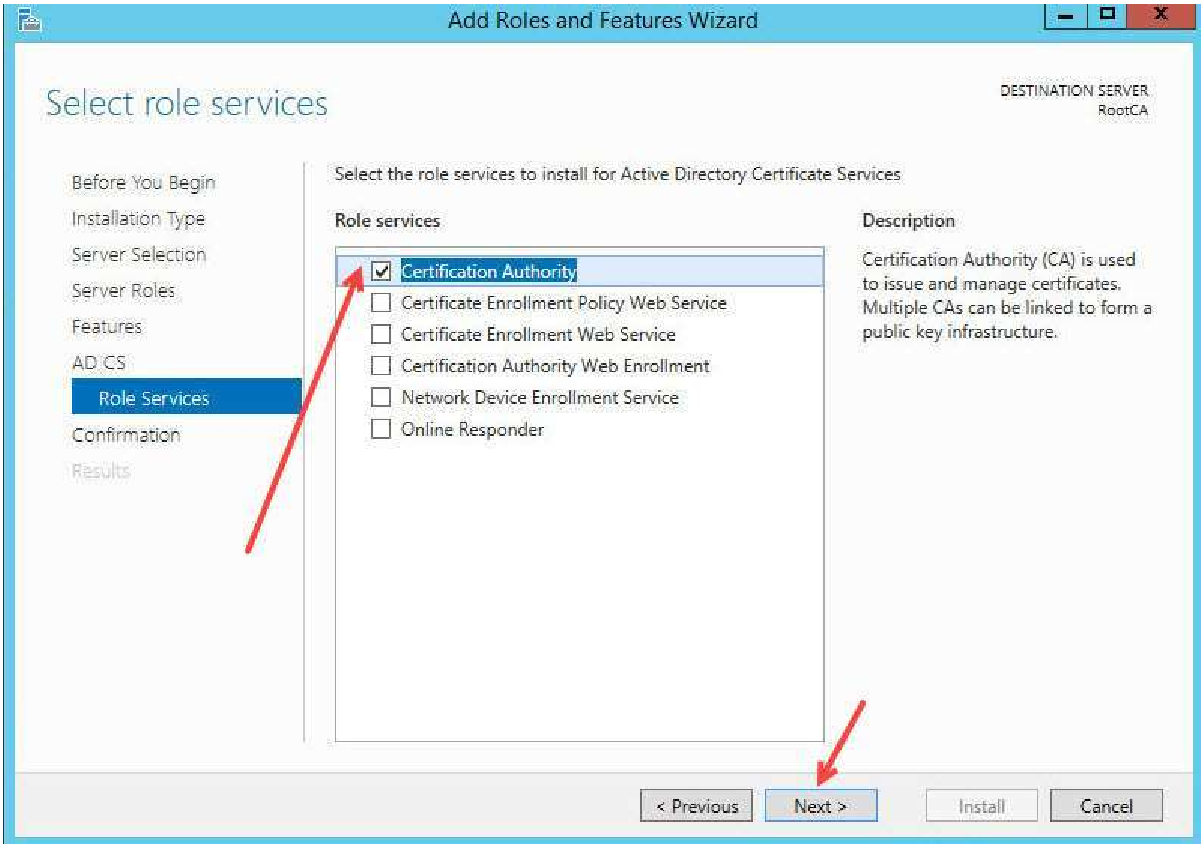
Roles

- ☑ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ▣ File and Storage Services (1 of 12 installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services

Description

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.

6 Now select the Checkbox for **Certificate Authority**



Add Roles and Features Wizard

DESTINATION SERVER
RootCA

Select role services

Select the role services to install for Active Directory Certificate Services

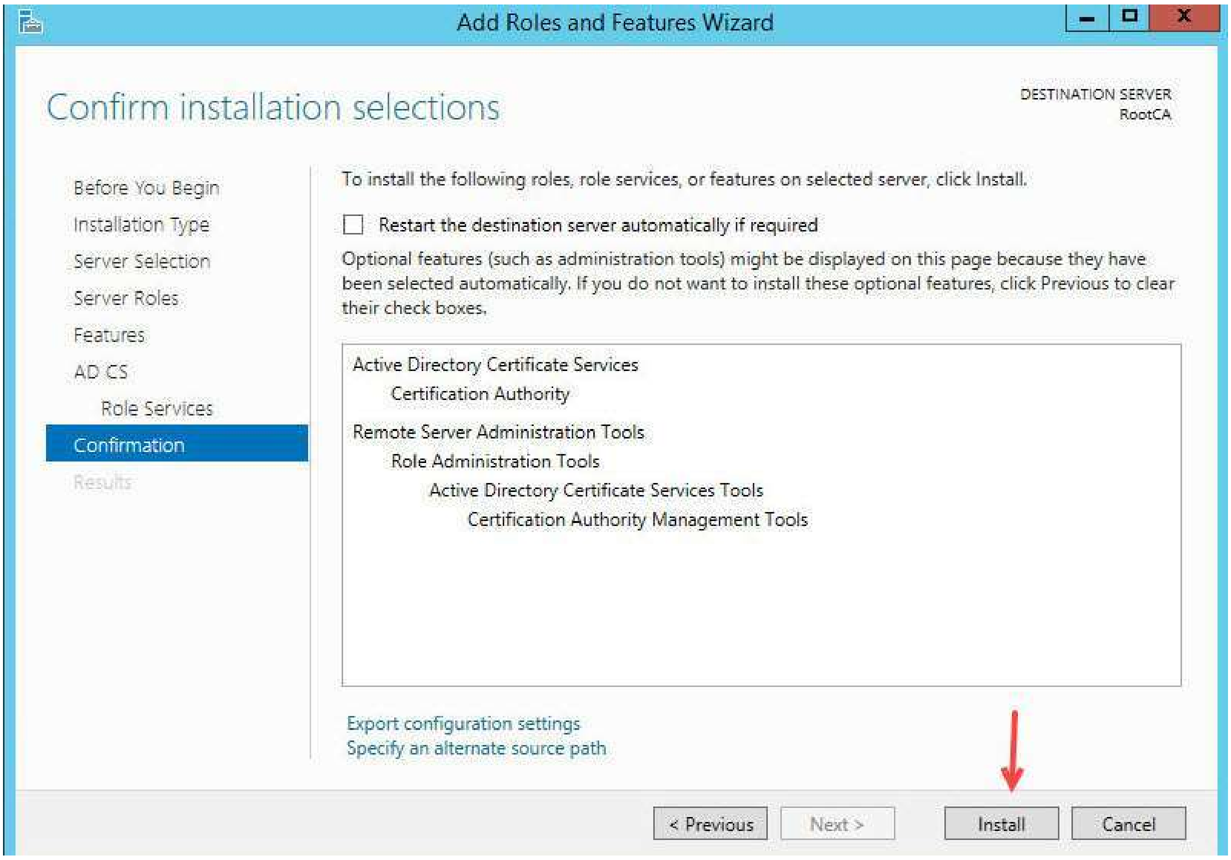
Role services

- ☑ 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.

7 Click on the **Install** button



Add Roles and Features Wizard

DESTINATION SERVER
RootCA

Confirm installation selections

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

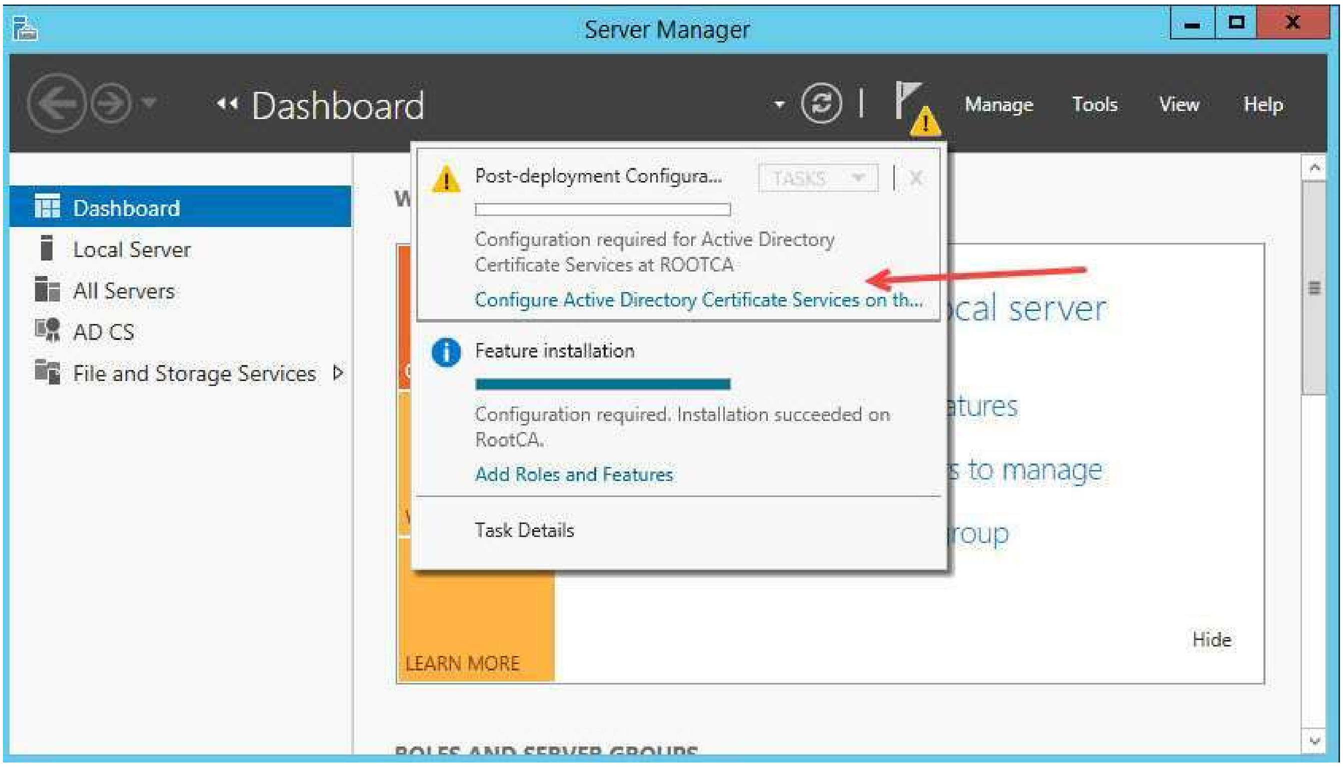
□ Restart the destination server automatically if required

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

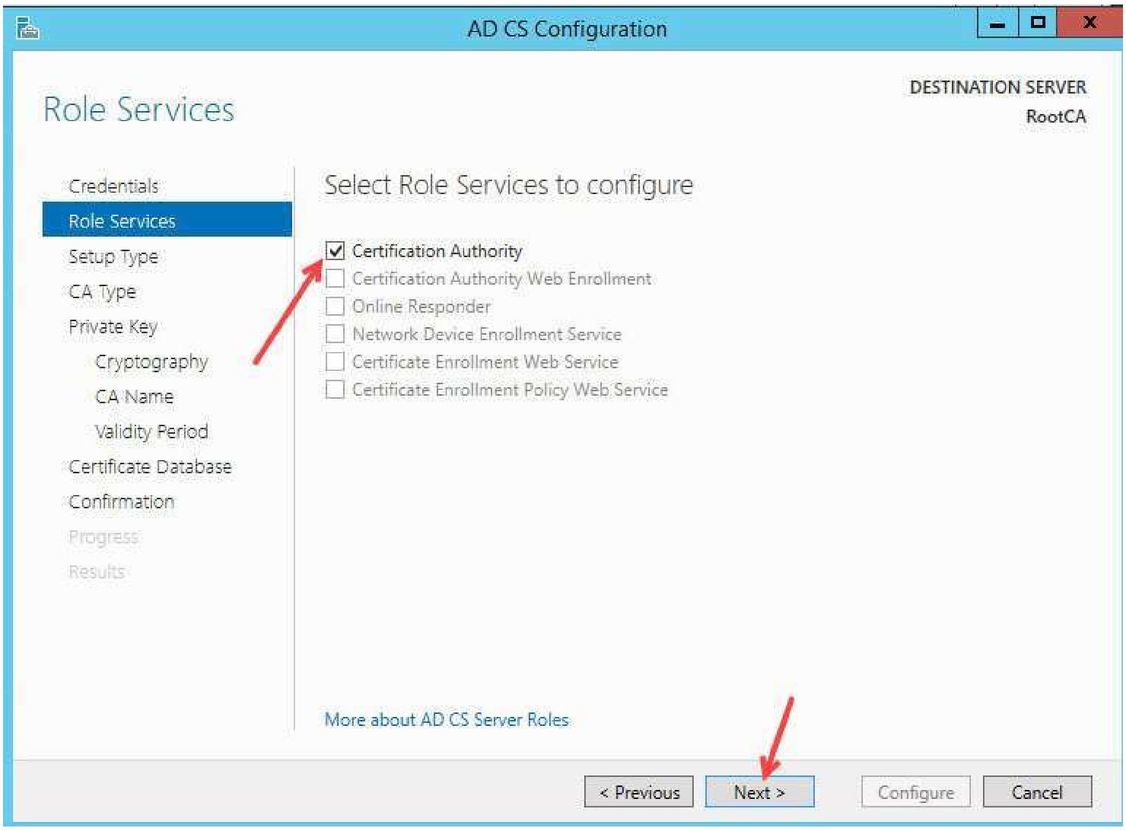
Export configuration settings
Specify an alternate source path

8 After the Installation click on Notification area and execute Active Directory Configuration service



Server Manager
Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD CS
File and Storage Services
Post-deployment Configura...
TASKS
Configuration required for Active Directory Certificate Services at ROOTCA
Configure Active Directory Certificate Services on th...
Feature installation
Configuration required. Installation succeeded on RootCA.
Add Roles and Features
Task Details
LEARN MORE
Hide

9 Select the **Certificate Authority** and Click next

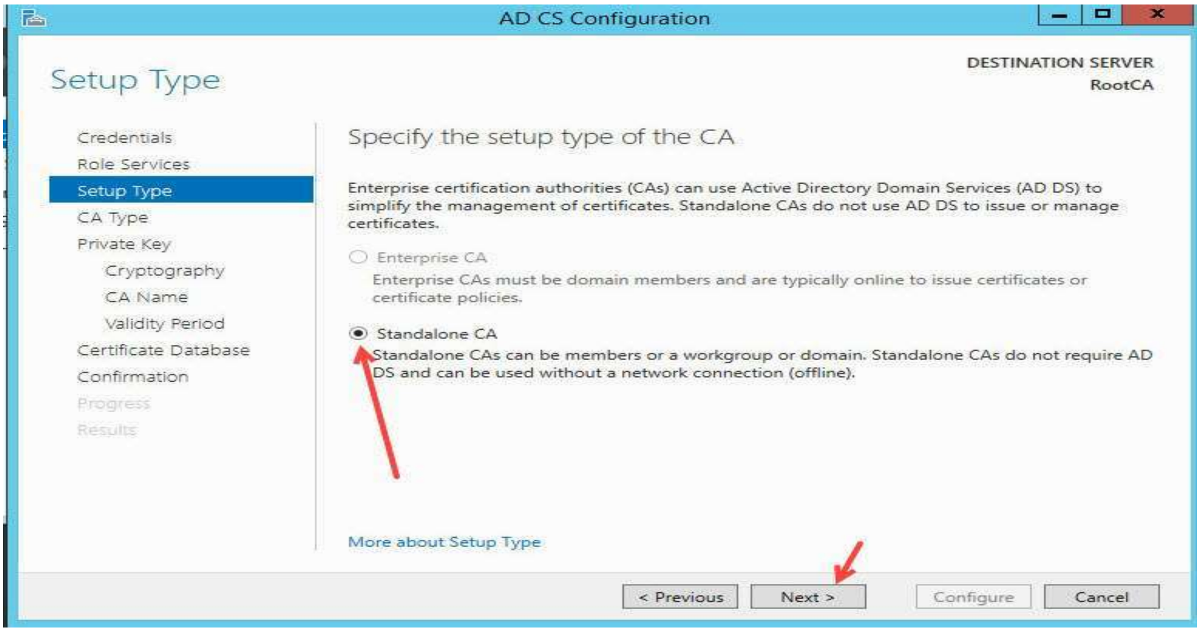


AD CS Configuration
Role Services
DESTINATION SERVER
RootCA
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Select Role Services to configure
☑ Certification Authority
☐ Certification Authority Web Enrollment
☐ 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

10 There are two option for the Root CA deployment

Enterprise CA: It can be Integrated with Active Directory (Imran Ijaz, 2012)Environment with automatic trust mechanism, but the only disadvantage of such time deployment is that server must be online

Standalone CA: Standalone server can be work in offline mode as well as it can be installed any server environment



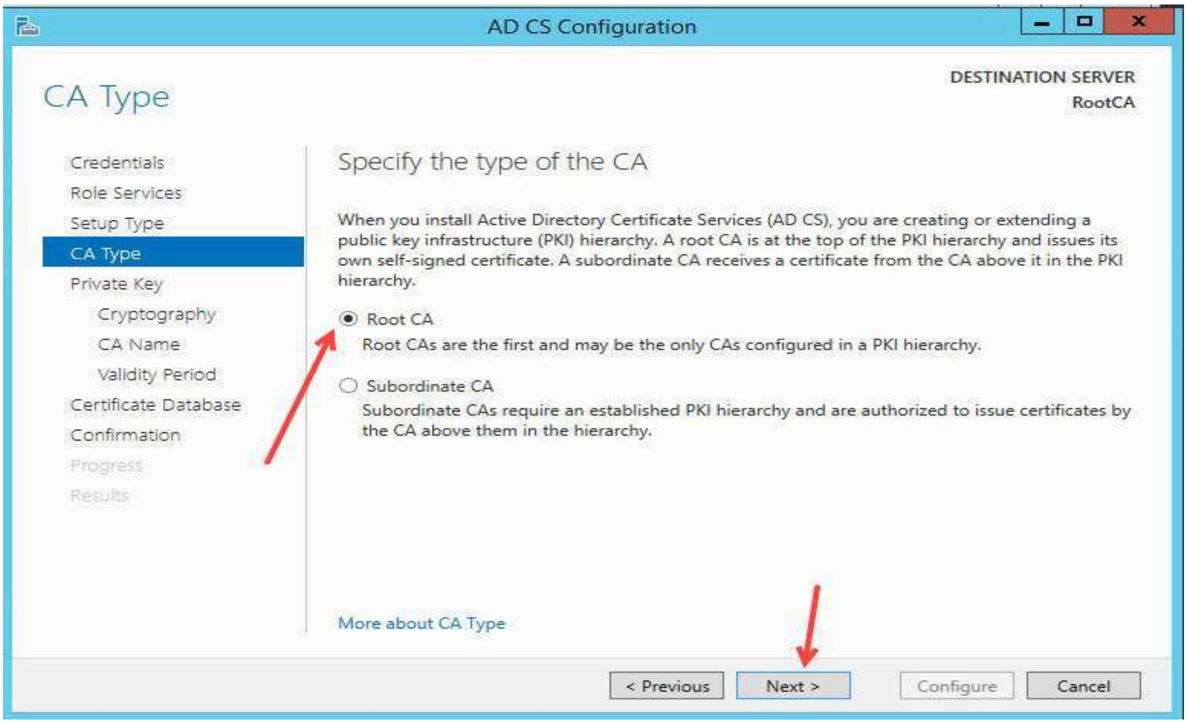
Specify the setup type of the CA

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).

11 Select the **Root CA**



Specify the type of the CA

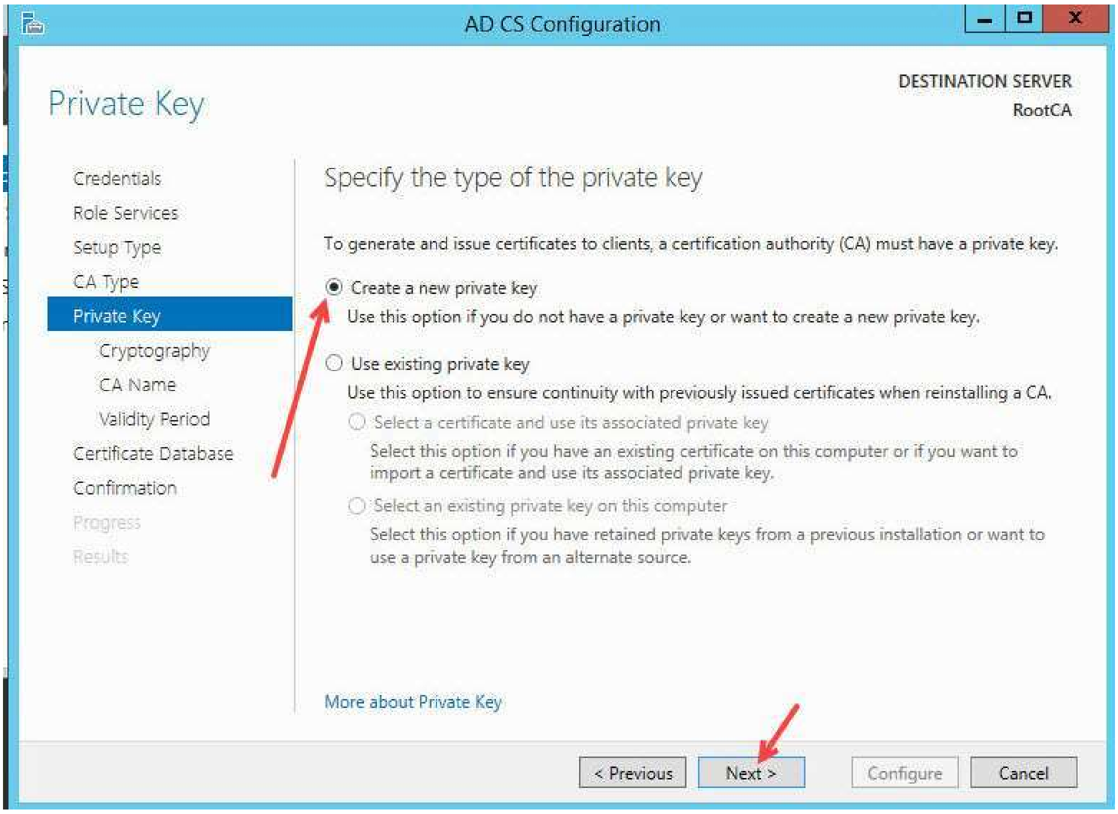
When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

● 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.

12 Select Create new Private Key

There are two forms of cryptography:(Fernando, Sison and Medina, 2019) the symmetric and asymmetric key cryptography. Symmetric Cryptography performs encryption and decryption using the single key while Asymmetric cryptography involves two key-pair which mathematically paired with each other. the public key is placed generally on the server and Private key are hold by a person or a computer who want to access the service or decrypt the data



Specify the type of the private key

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

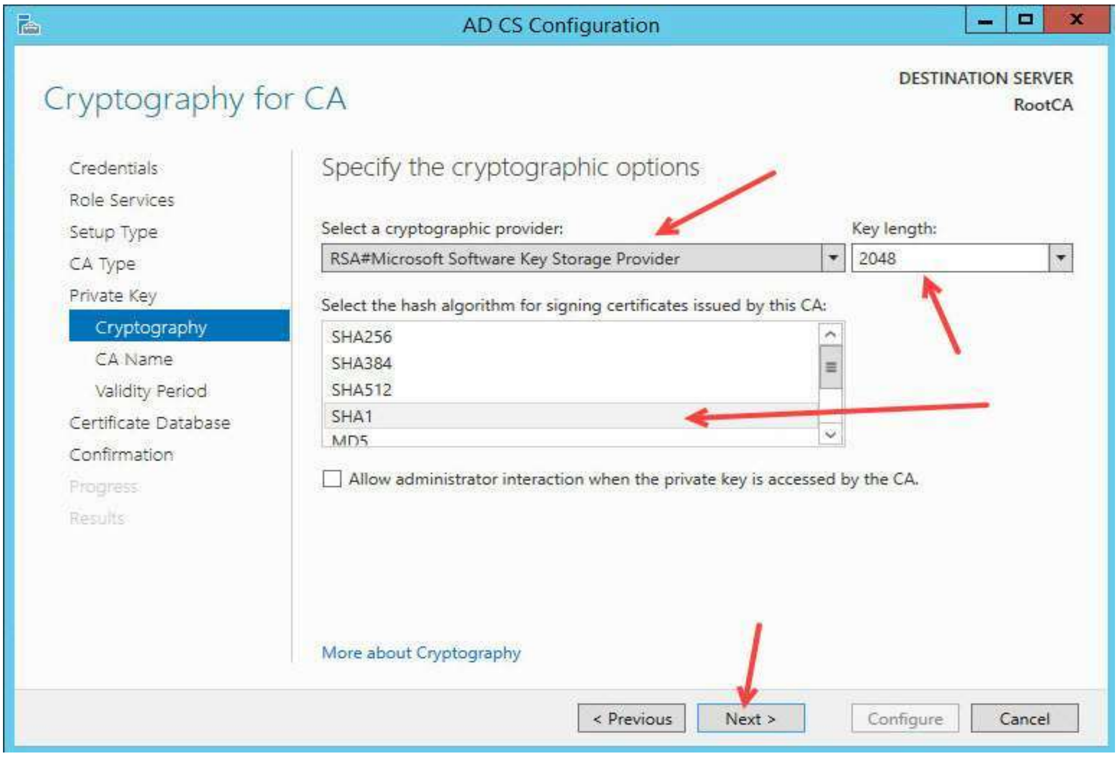
● Create a new private key
Use this option if you do not have a private key or want to create a new private key.

○ 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.

13 Select the Cryptographic Provider as **RSA** with **2048** key length and **SHA1** Hash Algorithm



Cryptography for CA

DESTINATION SERVER
RootCA

Specify the cryptographic options

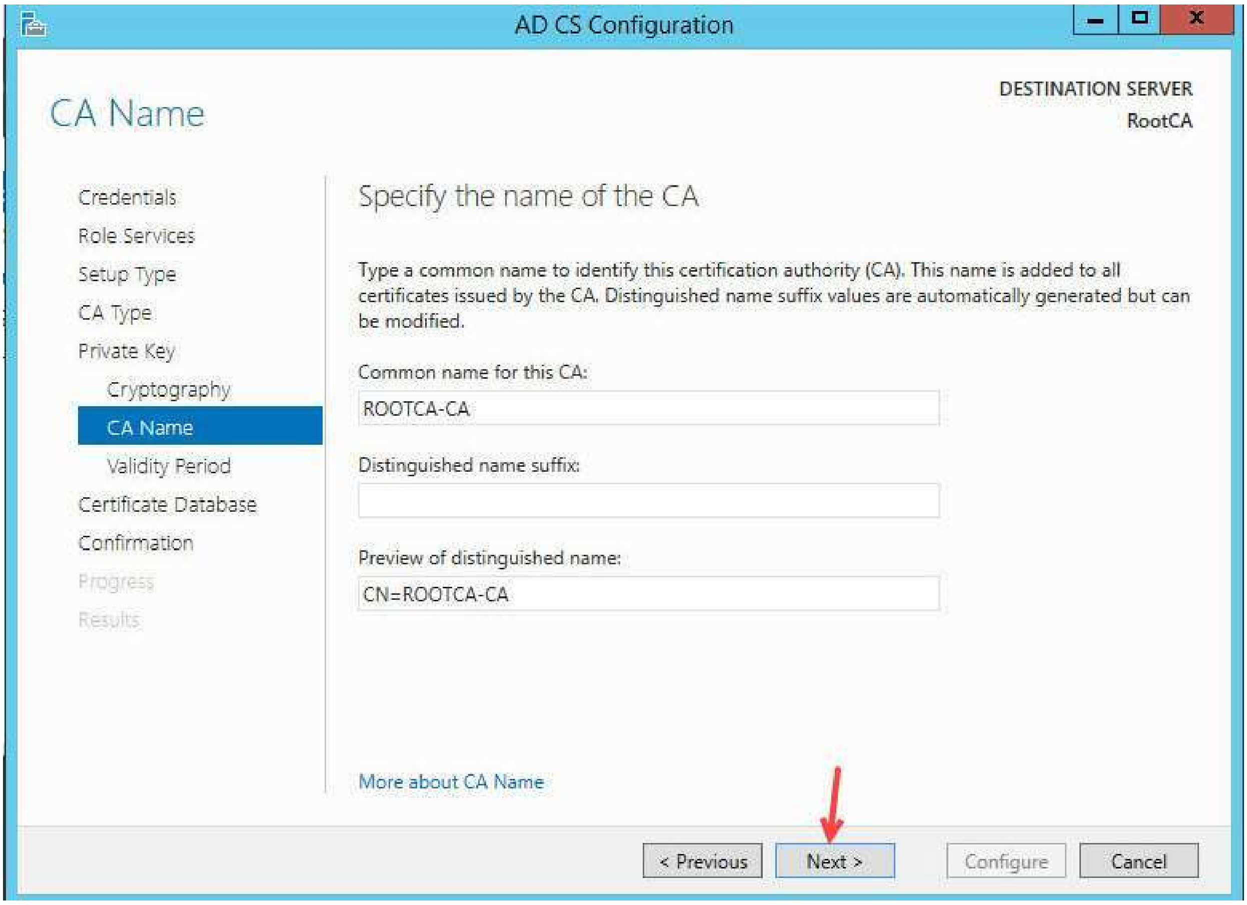
Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

Key length: 2048

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

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

14 Again, Click next Button



CA Name

DESTINATION SERVER
RootCA

Specify the name of the CA

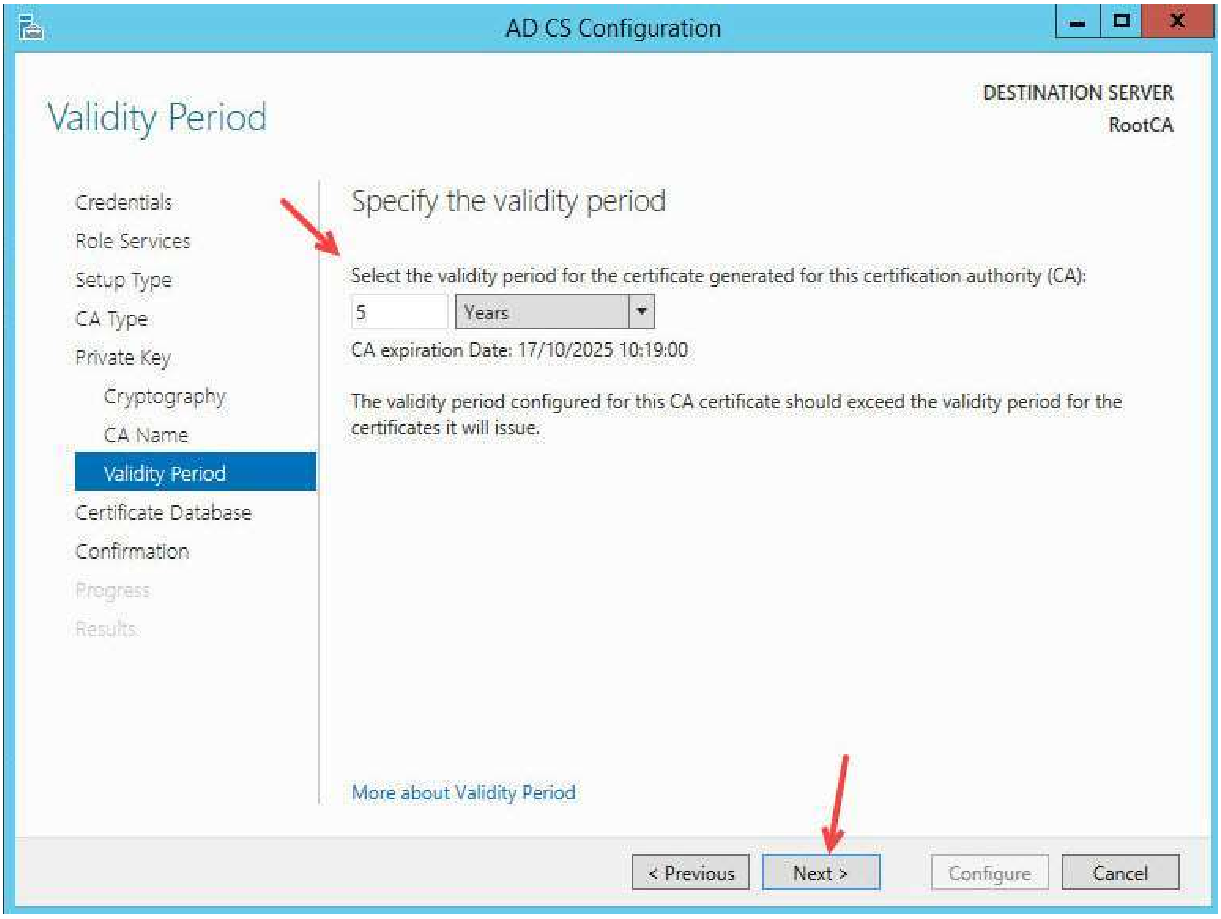
Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA: ROOTCA-CA

Distinguished name suffix:

Preview of distinguished name: CN=ROOTCA-CA

15 Validity of the Certificate will be set **5 years**



Specify the validity period

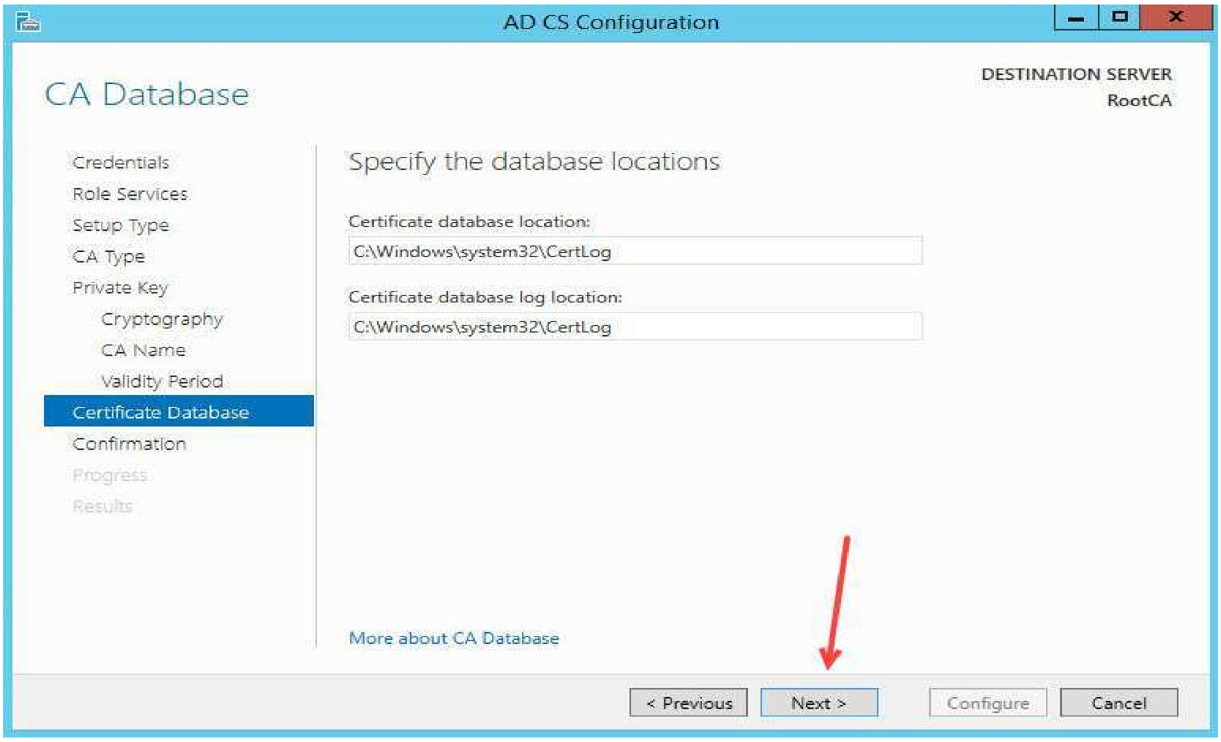
Select the validity period for the certificate generated for this certification authority (CA):

5 Years

CA expiration Date: 17/10/2025 10:19:00

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

16 Click on the Next



Specify the database locations

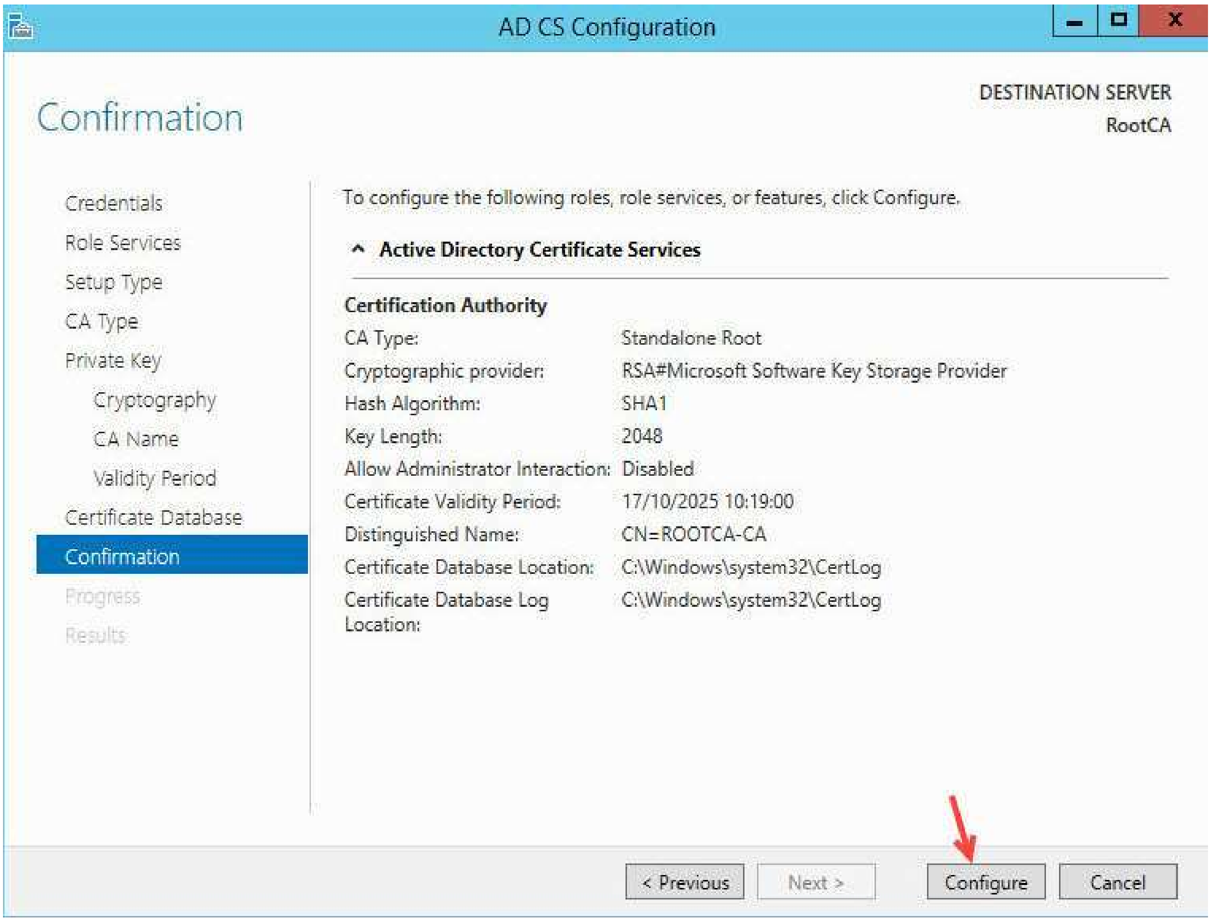
Certificate database location:

C:\Windows\system32\CertLog

Certificate database log location:

C:\Windows\system32\CertLog

17 Click on the Configure



Confirmation

DESTINATION SERVER
RootCA

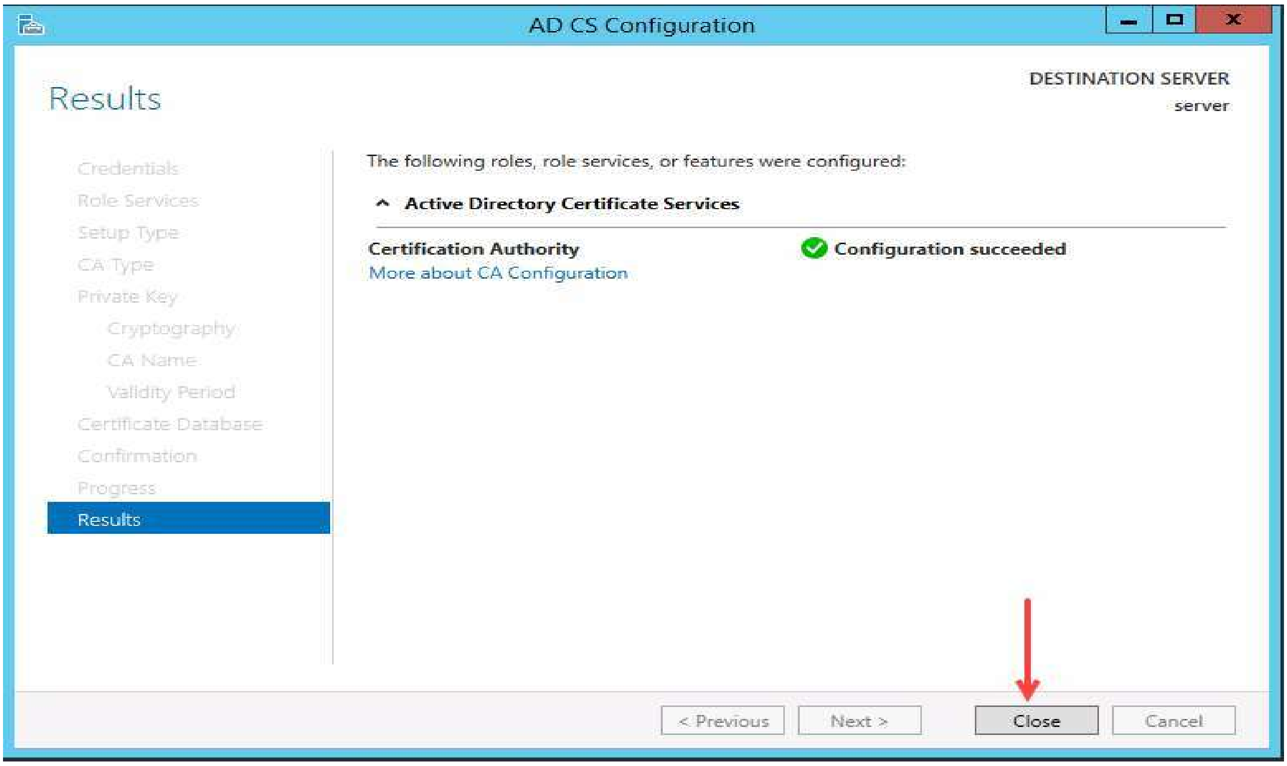
To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Certification Authority

CA Type:	Standalone Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA1
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	17/10/2025 10:19:00
Distinguished Name:	CN=ROOTCA-CA
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

18 Configuration Complete now close the Wizard



Results

DESTINATION SERVER
server

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

Active Directory Certificate Services

Certification Authority ✓ Configuration succeeded
More about CA Configuration