Microsoft DNS

Integration Guide

CryptoServer HSM

4.45.5.1

utimaco®

Imprint

Copyright 2026	Utimaco IS GmbH
	Krefelder Straße 220
	52070 Aachen
	Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226)
	EMEA +49 800-627-3081
	APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2026-05-20
Status	PUBLISHED
Document No.	IG-2026-0041

Table of Contents

1 Introduction 5
1.1 About This Guide 5
1.1.1 Target Audience for This Guide 5
1.1.2 Document Conventions 5
1.1.3 Abbreviations 6
2 Overview 9
2.1 Microsoft DNS 9
2.2 Utimaco CryptoServer HSM 9
3 Prerequisites and Requirements 10
3.1 Tested Versions 10
3.2 Software Requirements 10
3.3 Hardware Requirements 11
3.4 Prerequisites 11
4 Configuring the CSP-CNG Provider 12
4.1 Introduction and Prerequisites 12
4.2 Creating HSM Users 12
4.2.1 Creating a Key Manager User 12
4.2.2 Creating a Crypto User 13
4.3 Setting up the CSP/CNG Provider 14
4.3.1 Testing Connection 16
5 Integrating Microsoft DNS Server with Utimaco HSM 18
5.1 Install Microsoft DNS 18
5.2 Create Forward Lookup Zone in DNS Manager 23
5.3 Sign Forward Lookup Zone 31
5.4 Create Record in Forward Lookup Zone 50
5.5 Create Reverse Lookup Zone in DNS Manager 51
5.6 Sign Reverse Lookup Zone 60
5.7 Create Record in Reverse Lookup Zone 75
6 Troubleshooting 78
7 Further Information 79
8 References 80

9 Contact and Support Information 81

1 Introduction

This guide is part of the information and support provided by Utimaco. Additional documents produced to support your Utimaco SecurityServer product can be found in the document directory of the Utimaco SecurityServer product bundle. All Utimaco SecurityServer product documentation is available on Utimaco's website at https://utimaco.com/.

1.1 About This Guide

This guide describes how to enable HSM integration with Microsoft DNS. Utimaco HSM securely stores the key signing key (KSK) and zone signing key (ZSK) used by Microsoft DNS Security Extension and offloads the signing operations on the HSM.

1.1.1 Target Audience for This Guide

This guide is intended for Microsoft DNS and Utimaco HSM administrators.

1.1.2 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Select **Details** and click on **Properties** button
`Monospaced`	Code that is given for explanation or as an example, file paths	`certreq.exe -new request.inf IISCertRequest.csr`
Italic	References and important terms	Operating system listed in *Tested Versions*

Table 1: Document conventions

Table 1: Document conventions

We use special icons to highlight the most important notes and information.

Here you will find important safety information that should be followed.

Here you will find additional notes or supplementary information.

This message marks the result expected after the successful execution of an instruction.

1.1.3 Abbreviations

The following abbreviations are used in this guide:

Abbreviation	Meaning
API	Application Programming Interface
CD	Compact Disc
CNG	Cryptography API Next Generation
CSP	Cryptographic Service Provider
CSADM	CryptoServer Command-line Administration Tool
CXI	Cryptographic eXtended Services Interface
DNS	Domain Name System

Abbreviation	Meaning
DNSSEC	Domain Name System Security Extension
GUI	Graphical User Interface
HMAC	Hash-based message authentication code
HSM	Hardware Security Module
ID	Identity
IP	Internet Protocol
KSK	Key Signing Key
LAN	Local Area Network
MBK	Master Backup Key
NSEC	Next Secure
PCIe	PCI Express Interface
PIN	Personal Identification number
PTR	Pointer
TAs	Trust Anchors
TCP	Transmission Control Protocol

Abbreviation	Meaning
URL	Uniform Resource Locator
ZSK	Zone Signing Key

Table 2: List of abbreviations

2 Overview

2.1 Microsoft DNS

Domain Name System (DNS) is one of the industry-standard suites of protocols that comprise TCP/IP, and together the DNS Client and DNS Server provide computer name-to-IP address mapping name resolution services to computers and users.

Domain Name System Security Extensions (DNSSEC) is a suite of extensions that add security to the DNS protocol by enabling DNS responses to be validated. Specifically, DNSSEC provides origin authority, data integrity, and authenticated denial of existence. With DNSSEC, the DNS protocol is much less susceptible to certain types of attacks, particularly DNS spoofing attacks.

DNS zone can be secured with DNSSEC using a process called zone signing. The keys used in zone signing are stored on Utimaco HSM. Signing a zone with DNSSEC adds validation support to a zone without changing the basic mechanism of a DNS query and response.

Validation of DNS responses occurs using digital signatures that are included with DNS responses. These digital signatures are contained in new, DNSSEC-related resource records that are generated and added to the zone during zone signing.

2.2 Utimaco CryptoServer HSM

CryptoServer is a hardware security module developed by Utimaco IS GmbH. CryptoServer is a physically protected specialized computer unit designed to perform sensitive cryptographic tasks and to securely manage as well as store cryptographic keys and data. It can be used as a universal, independent security component for heterogeneous computer systems.

3 Prerequisites and Requirements

Ensure that the system environment you will be using meets the following hardware and software requirements.

This guide assumes that the user has already installed and configured the required software.

3.1 Tested Versions

The integrations that have been successfully tested with the Utimaco HSM with Microsoft DNS.

Operating Systems	Utimaco Security Server Version	Utimaco HSM
Windows Server 2019	SecurityServer 4.45.5.1	CryptoServer CSe-Series/Se-Series

Table 3: List of tested versions

3.2 Software Requirements

Product	Version
HSM Interfaces	CryptoServer CSP/CNG Provider

Table 4: List of software requirements

3.3 Hardware Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	CryptoServer CSe-Series/Se-Series LAN with firmware SecurityServer 4.45.5.1 or higher
Utimaco PCI-e HSM	CryptoServer CSe-Series/Se-Series PCI-e with firmware SecurityServer 4.45.5.1 or higher

Table 5: List of hardware requirements

3.4 Prerequisites

Please ensure that:

- The CryptoServer is set up and configured. Refer to the CryptoServer documentations to set up the HSM.
- The MBK is created and stored onto each HSM. Refer to the CryptoServer documentations to set up the MBK.
- The CryptoServer Default Admin is replaced with a new admin user. Admin user is required for installing software.
- The operating system used is listed in Tested Versions.
- The SecurityServer used is listed in Tested Version.
- There is Static IP assigned before installing DNS Server Role.
- Port 53 is allowed through Firewall.
- You familiarize yourself with the MS DNS documents and setup process.

4 Configuring the CSP-CNG Provider

4.1 Introduction and Prerequisites

A CSP (Cryptographic Service Provider) is a general-purpose cryptography standard, developed by Microsoft. On one side it defines a cryptographic interface to be used by applications (CryptoAPI). On the other side it defines an interface to be used by manufacturers to integrate their cryptographic hardware.

A CNG (Cryptography API Next Generation) is the second-generation cryptographic interface, developed by Microsoft. It offers updated cryptographic algorithms and is intended for a long-term replacement of CSP.

When installing the CryptoServer Setup make sure to select the CPS/CNG - Cryptographic Service Provider (Microsoft) interface. A Cryptographic User should be created as well as an MBK should be generated.

Generating the MBK is necessary for the HSM to become operational. Without the MBK, one cannot run any cryptographic operations.

4.2 Creating HSM Users

Start the CryptoServer Administration Tool and log in a user with the permission level of at least 02000000.

4.2.1 Creating a Key Manager User

If the Key Manager and Crypto user roles are separated, a Key Manager user might need to be created.

More users with the permission level 00000010 might be needed (Group 1) to enforce "m of n" security policy for the key management and smart card authentication might need to be used.

For this guide, only one Key Manager user will be created.

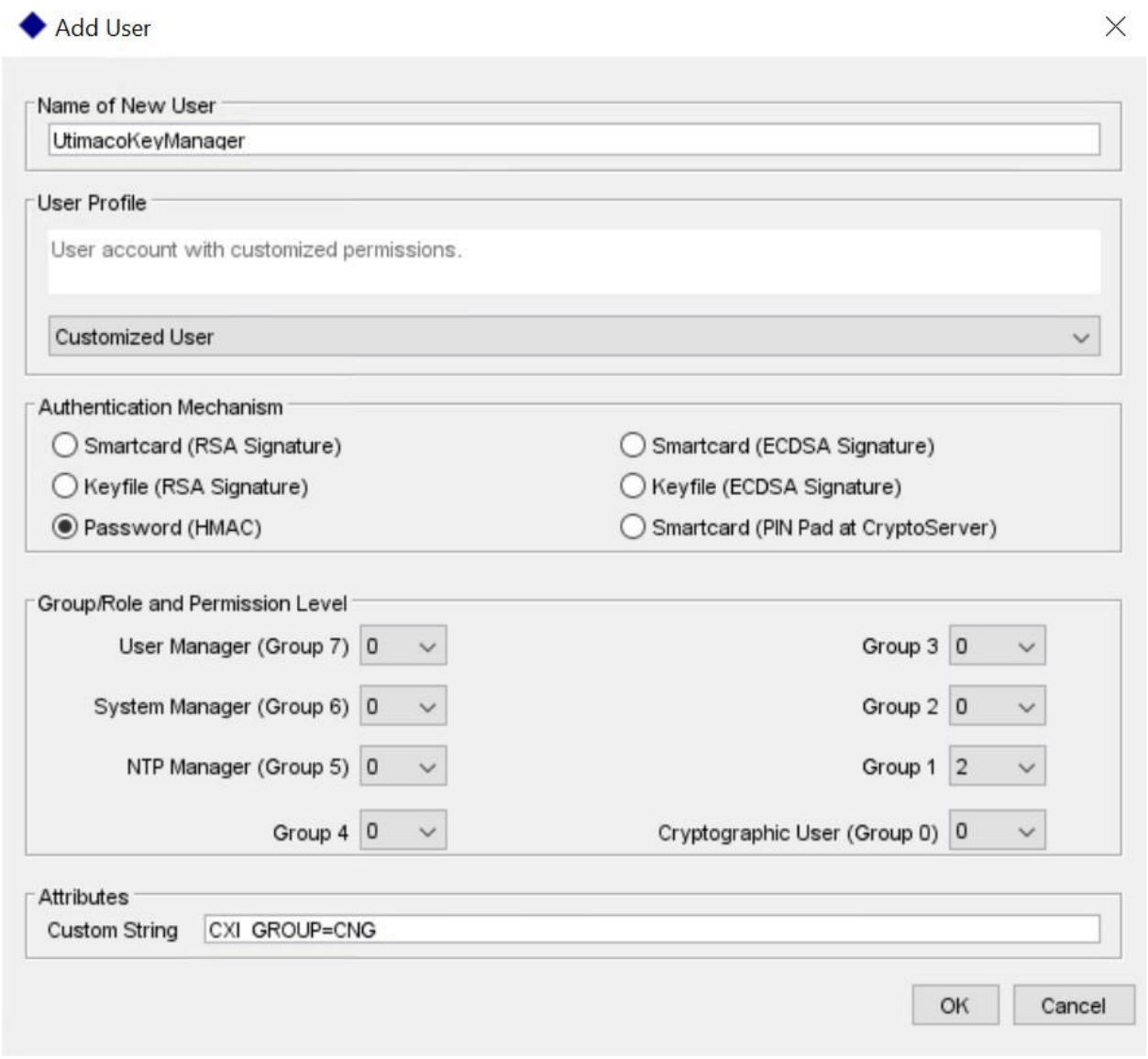

Figure 1 : Creating key manager user

4.2.2 Creating a Crypto User

Crypto Users with permission level of 00000002 will have to be created. Use encrypted passwords. For this guide, a user with permission level of 00000002, CXI Group "CNG" and HMAC password will be created.

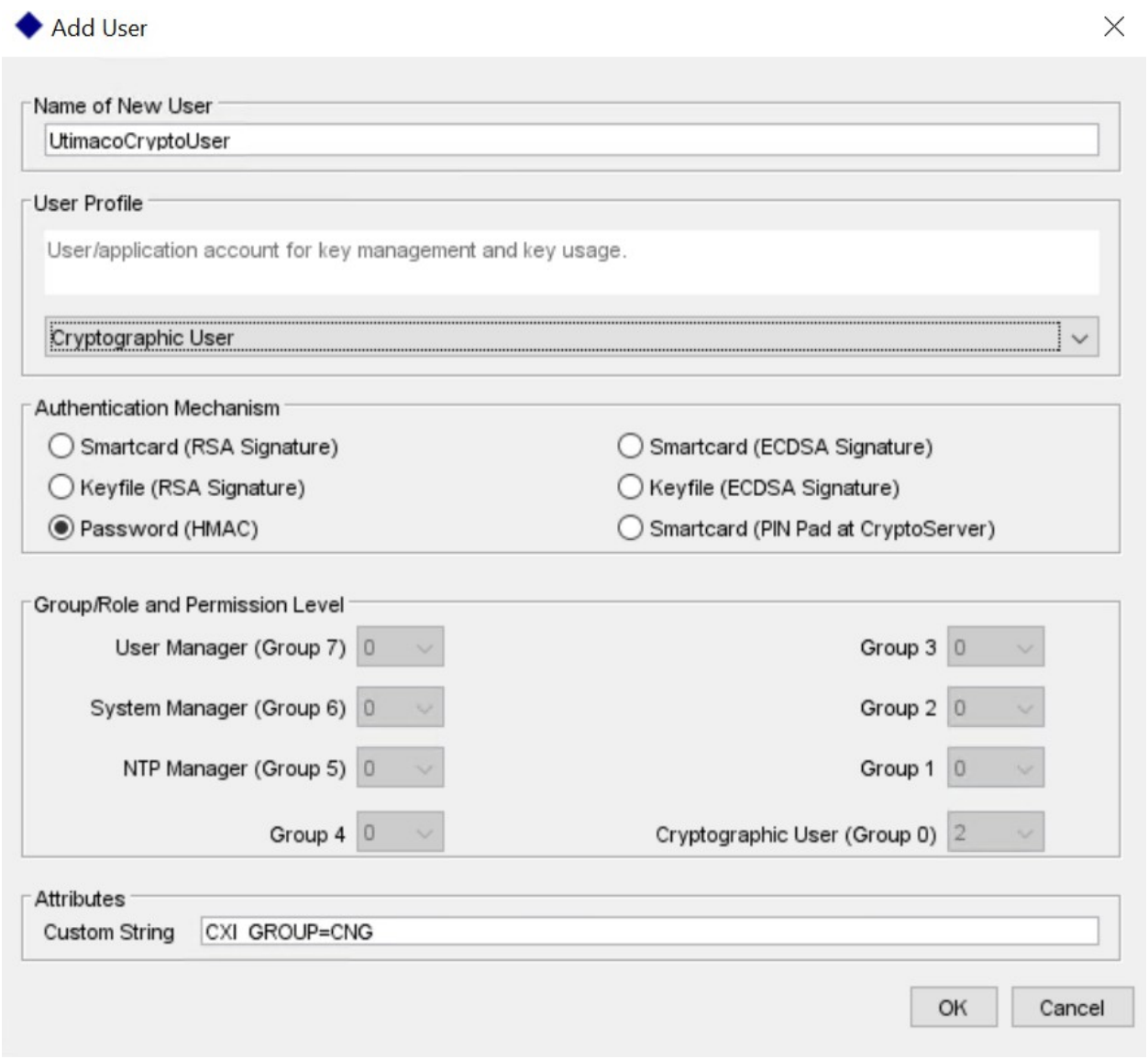

Figure 2 : Creating a crypto user

Based on your requirement, the user can use Password (HMAC), Smart Card or KeyFile protection type. If you are using Smartcard Authentication, the prompt will go on the PIN Pad device to insert Smartcard and enter the pin. Then press OK button on the PIN Pad.

4.3 Setting up the CSP/CNG Provider

The CS_CNG_CFG environment variable contains the path and name of the configuration file. By default, it is located at C:\ProgramData\Utimaco\CNG\cs_cng.cfg.

For more advanced configuration, refer to [CspCng];.

1. Open the cs_cng.cfg file with an appropriate text editor.

›_ Console

```
> notepad %CS_CNG_CFG%
```

2. For this installation set the path to the log file and set the log level to "ERROR".

›_ Console

```
# Path to the logfile (name of logfile is attached by the API)

Logpath = C:\ProgramData\Utimaco\CNG\log

# Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE)

Logging = 1
```

To make your testing easier, it would be good to enable the CNG log file. That can be enabled by editing the **Logging Loglevel**. Set the **LogPath** and **Logging Loglevel** to 1. For testing you may want to increase it to 4.

The added **LogPath** points to a writable directory, not to a file.

If you encounter problems, check the log file named `cs_cng.log` in the **LogPath** defined directory. When you are done testing, you should change **Logging** to 1 or 2. This will limit the logging to only critical and important messages.

3. Set the Login. In this case, the name of the Cryptographic User is "UtimacoCryptoUser" with an HMAC password "Utimaco19".

›_ Console

```
Login = UtimacoCryptoUser,HMACPwd=Utimaco19
```

If using Smartcard or KeyFile protection make the appropriate change in the **Login** section as shown below:

`Login = username,RSASign=filename#password`

`Login = "SmartCardUser,RSASign=:cs2:auto:USB0@<HSM-IP>"`

For additional information refer to `CryptoServer_csadm_Manual_Systemadministrators.pdf` document, found on the product CD in the Documentation directory.

4. Set the group name and IP address of the HSM.

›_ Console

```
Group = CNG
# default device and fallback devices
Device = 10.44.223.141
```

For more information regarding the commands and command parameters, please check the Utimaco documentation. The device may be a CryptoServer (PCIe or LAN) device. The device line will follow one of these patterns, based on the HSM form-factor:

`Device = 288@<HSM IP address> Hardware (LAN) HSM`

OR

`Device = /dev/cs2.0 Hardware (PCIe) HSM`

4.3.1 Testing Connection

To enumerate providers, use the following command:

›_ Console

```
> cngtool EnumProvider

Microsoft Key Protection Provider Microsoft Passport Key Storage Provider
Microsoft Platform Crypto Provider Microsoft Primitive Provider

Microsoft Smart Card Key Storage Provider Microsoft Software Key Storage
Provider Microsoft SSL Protocol Provider

Windows Client Key Protection Provider

Utimaco CryptoServer Key Storage Provider
```

To get the provider information, use the following command:

›_ Console

```
>cngtool ProviderInfo

Provider : Utimaco CryptoServer Key Storage Provider Device : 10.44.223.141

Group : CNG

Mode : Internal Key Storage

Name : Utimaco CryptoServer Key Storage Provider Name : Utimaco CryptoServer Key
Storage Provider Version : 0x02010000

Impl. -Type : 0x00000011 MaxNameLength : 0x00000104 Device : 10.44.223.141

Group : CNG

Mode : Internal Key Storage
```

5 Integrating Microsoft DNS Server with Utimaco HSM

5.1 Install Microsoft DNS

1. Log onto the machine with **Admin** privileges.
2. Open the **Server Manager**.
3. Click on **Add Roles** and **Features** and click **Next**.

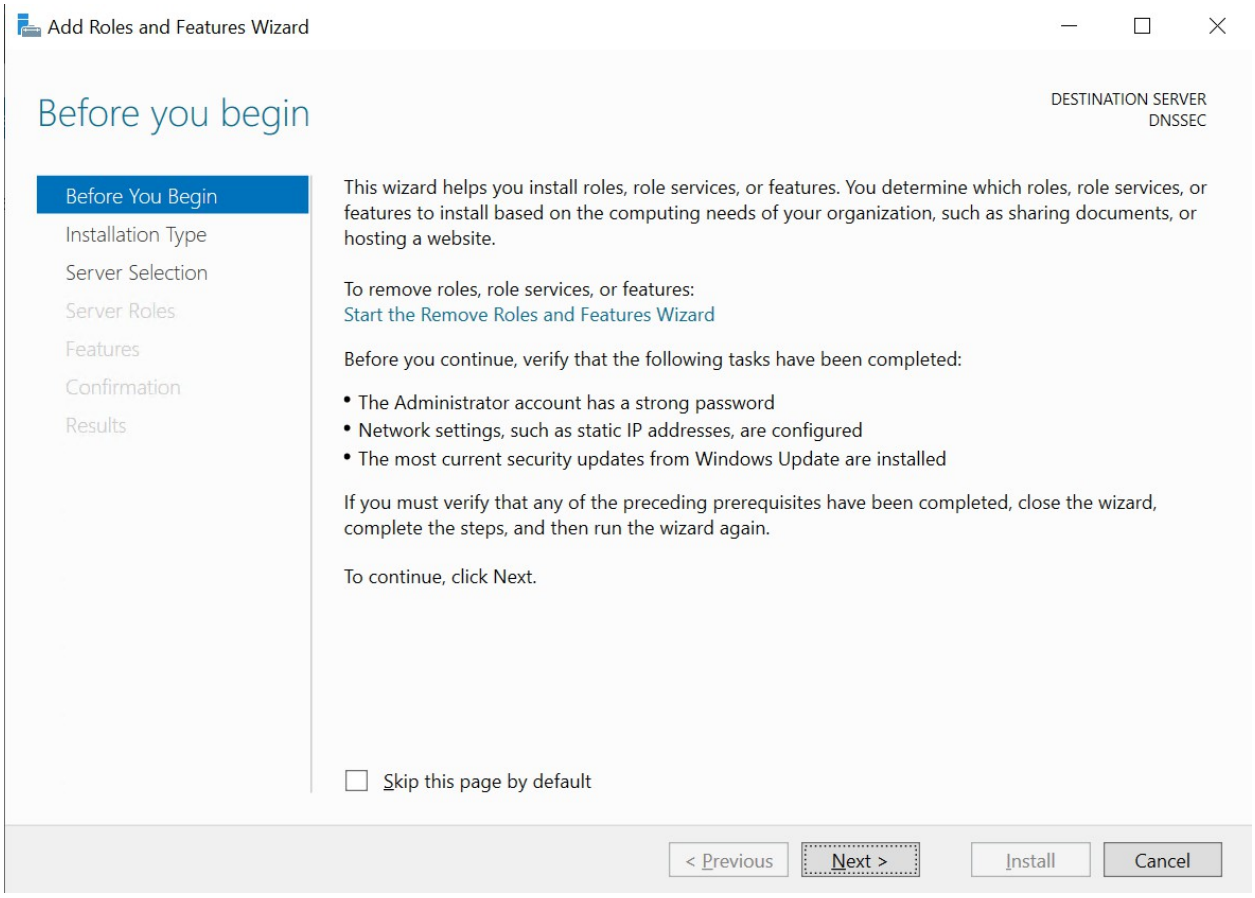

Figure 3 : Add roles and features wizard

4. Select **Installation Type** and click **Next**.

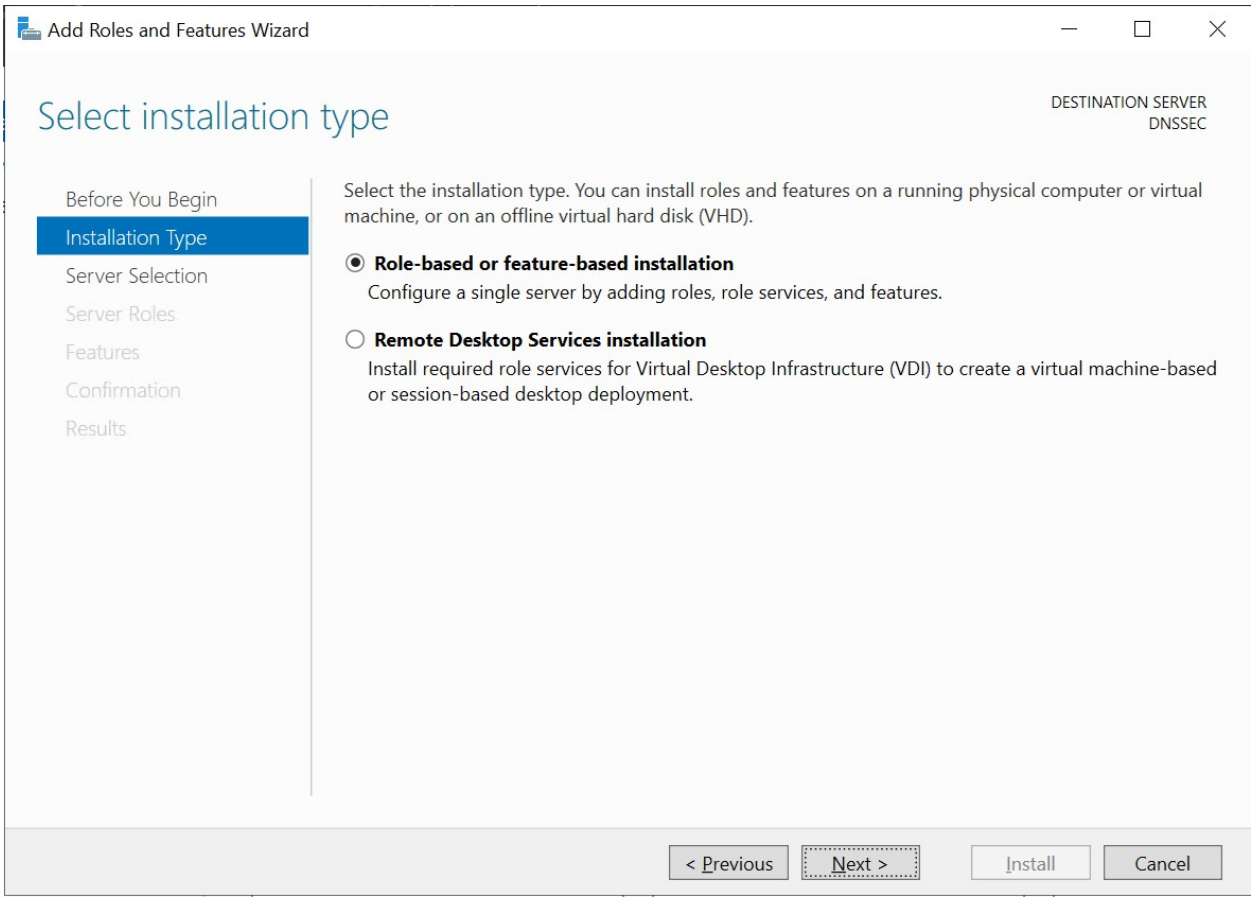

Figure 4 : Select installation type

5. Select **Destination Server** and click **Next**.

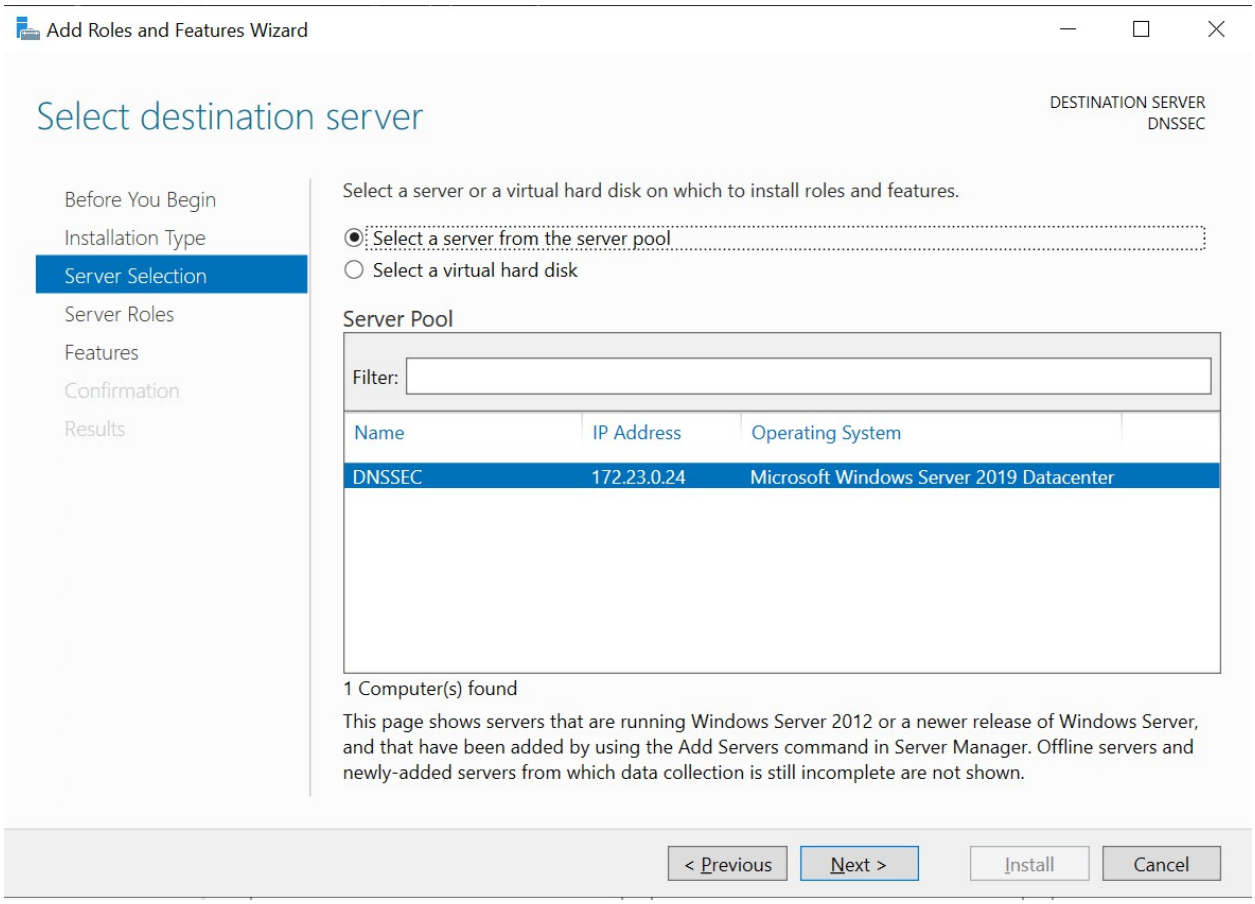

Figure 5 : Select destination server

6. In **Select Server Role** click on **DNS Server** and click **Next**. Click on **Add Features**, and click **Next**.

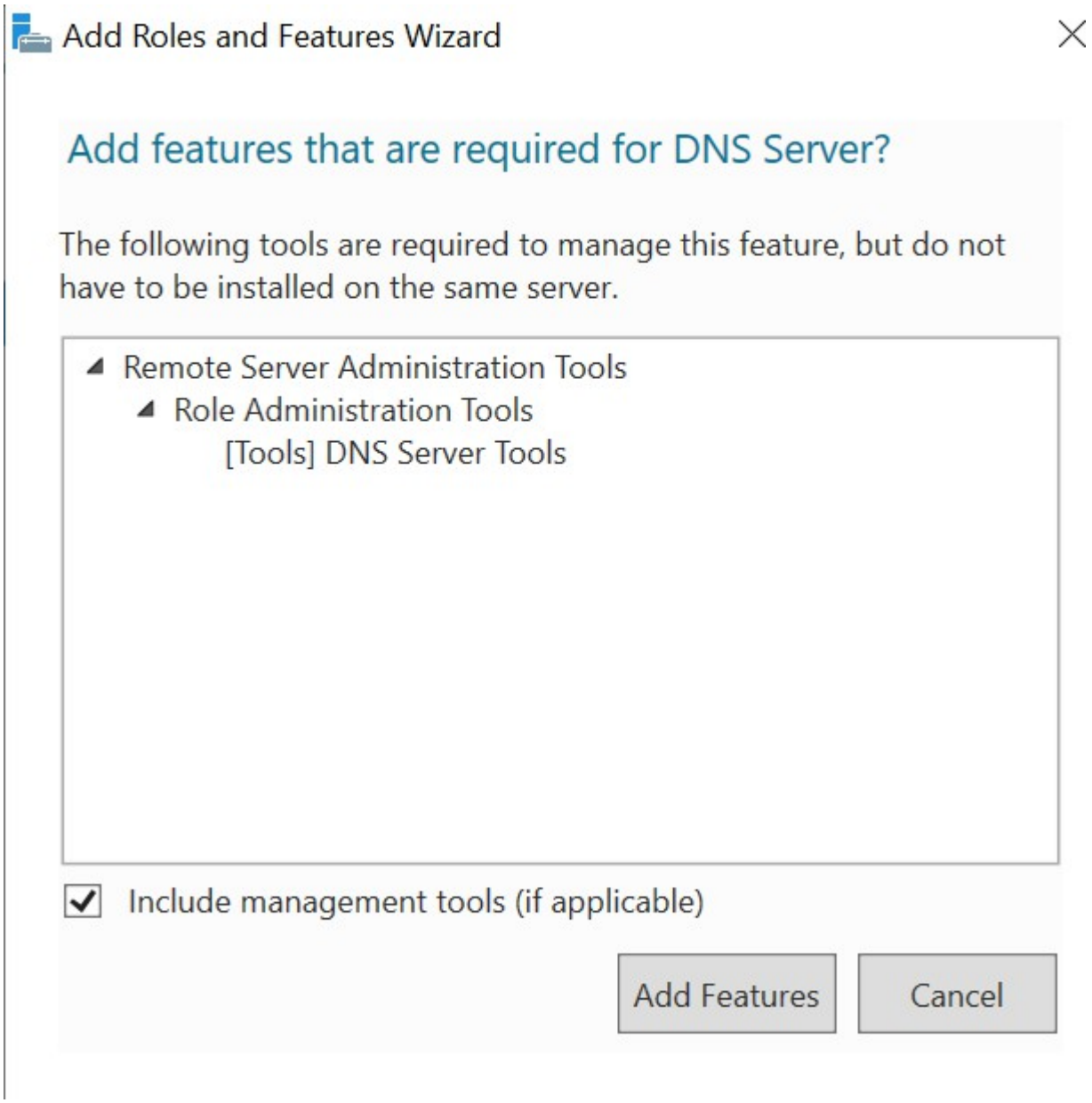

Figure 6 : Add features

7. Click **Next** on **Select Features** and click **Next** on **DNS Server**.
8. On the **Confirm installation selections** screen select **Restart the destination server automatically if required** and click on **Install**.

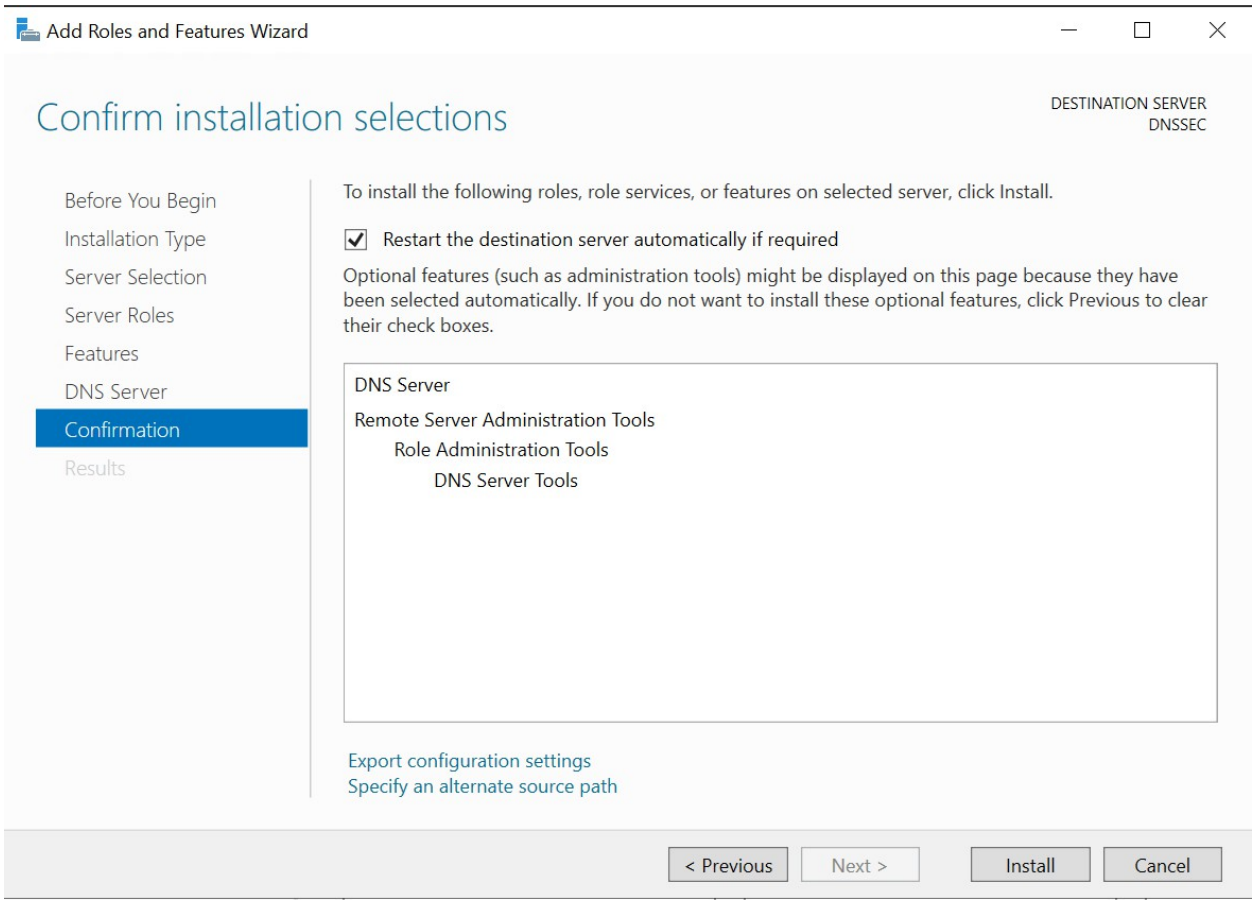

Figure 7 : Confirm installation selections

9. Check the installation progress.

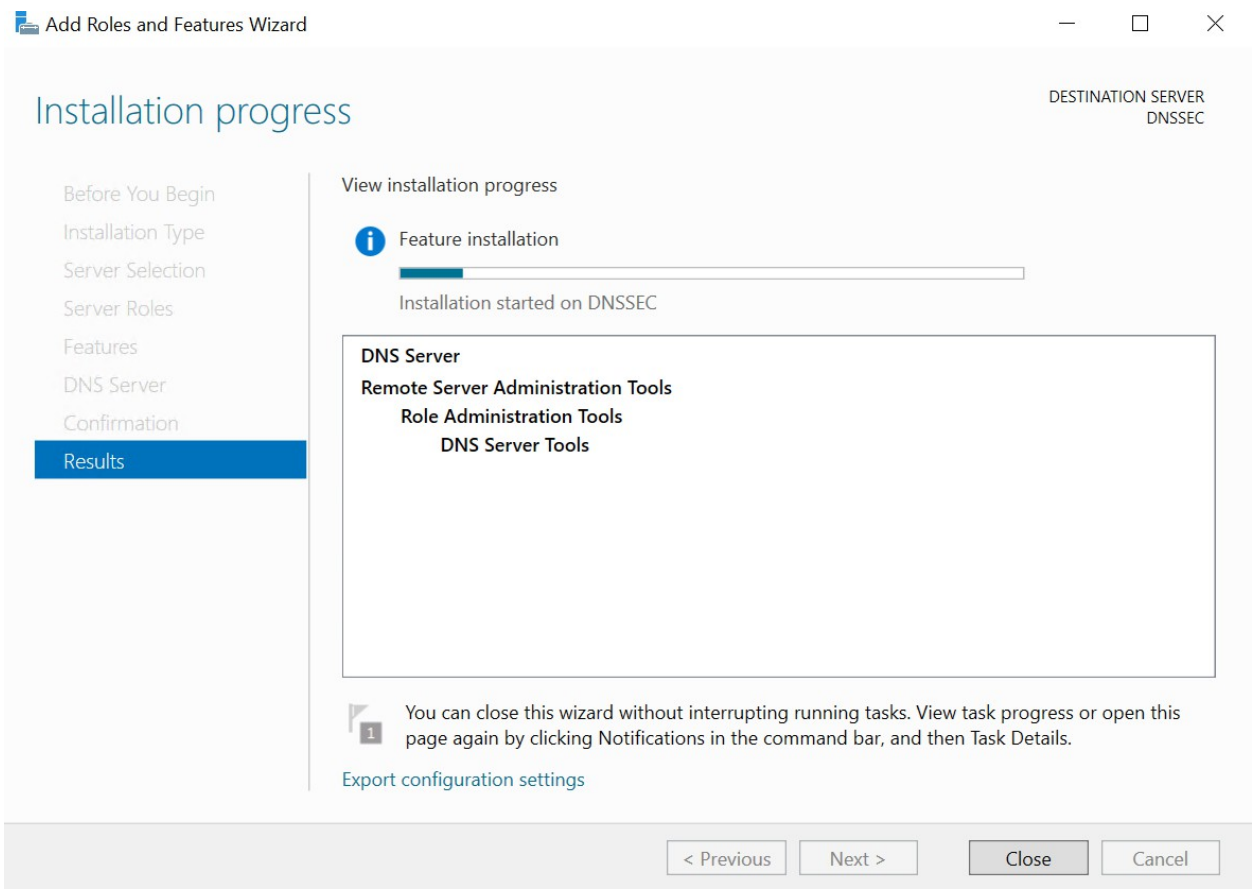

Figure 8 : Installation progress

10. Once done, close the wizard and open **DNS** from **Tools** menu of **Server Manager**.

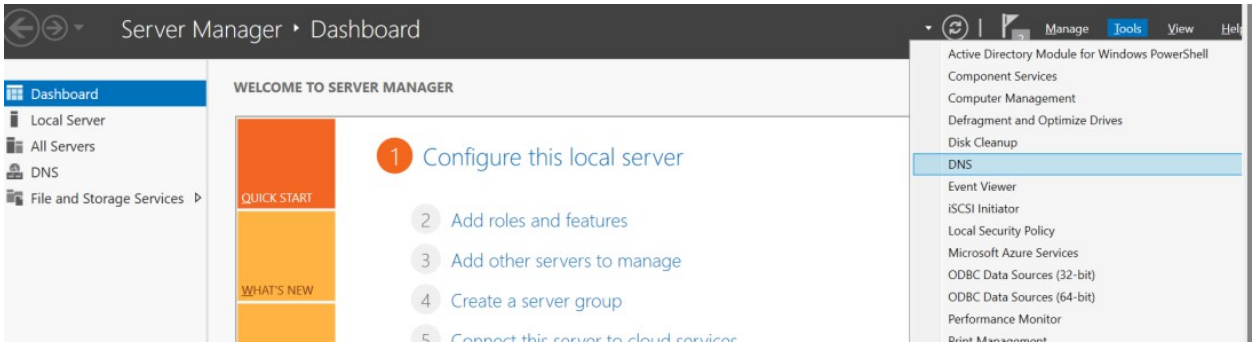

Figure 9 : Server manager

5.2 Create Forward Lookup Zone in DNS Manager

1. In DNS Manager right click on Forward Lookup Zone and click on New Zone…

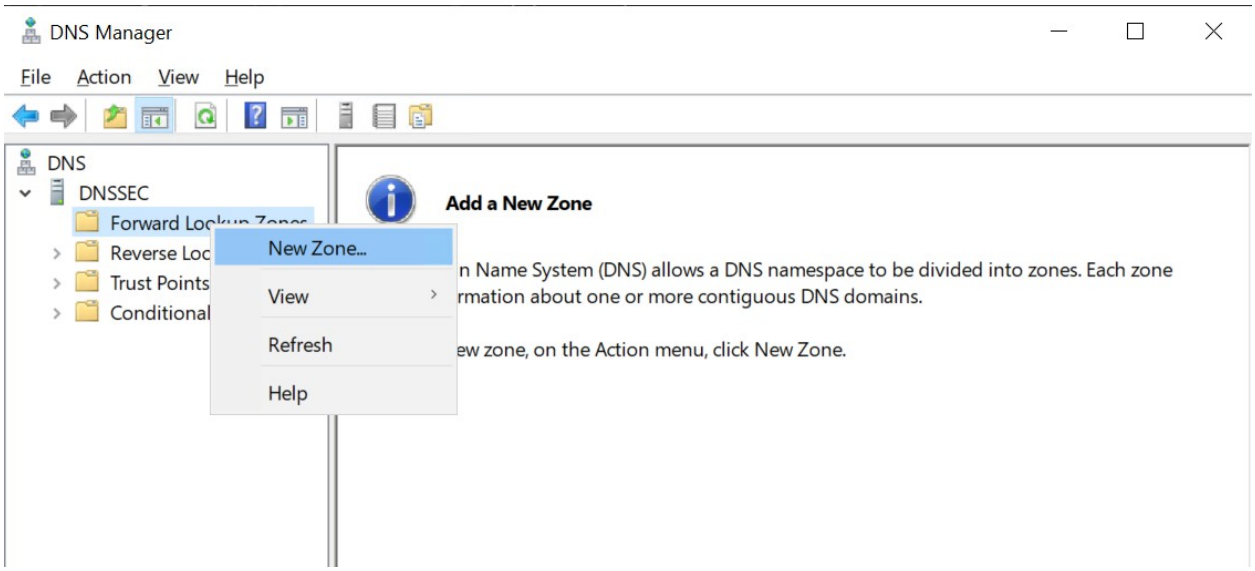

Figure 10 : DNS manager

2. In **New Zone Wizard** click **Next**.

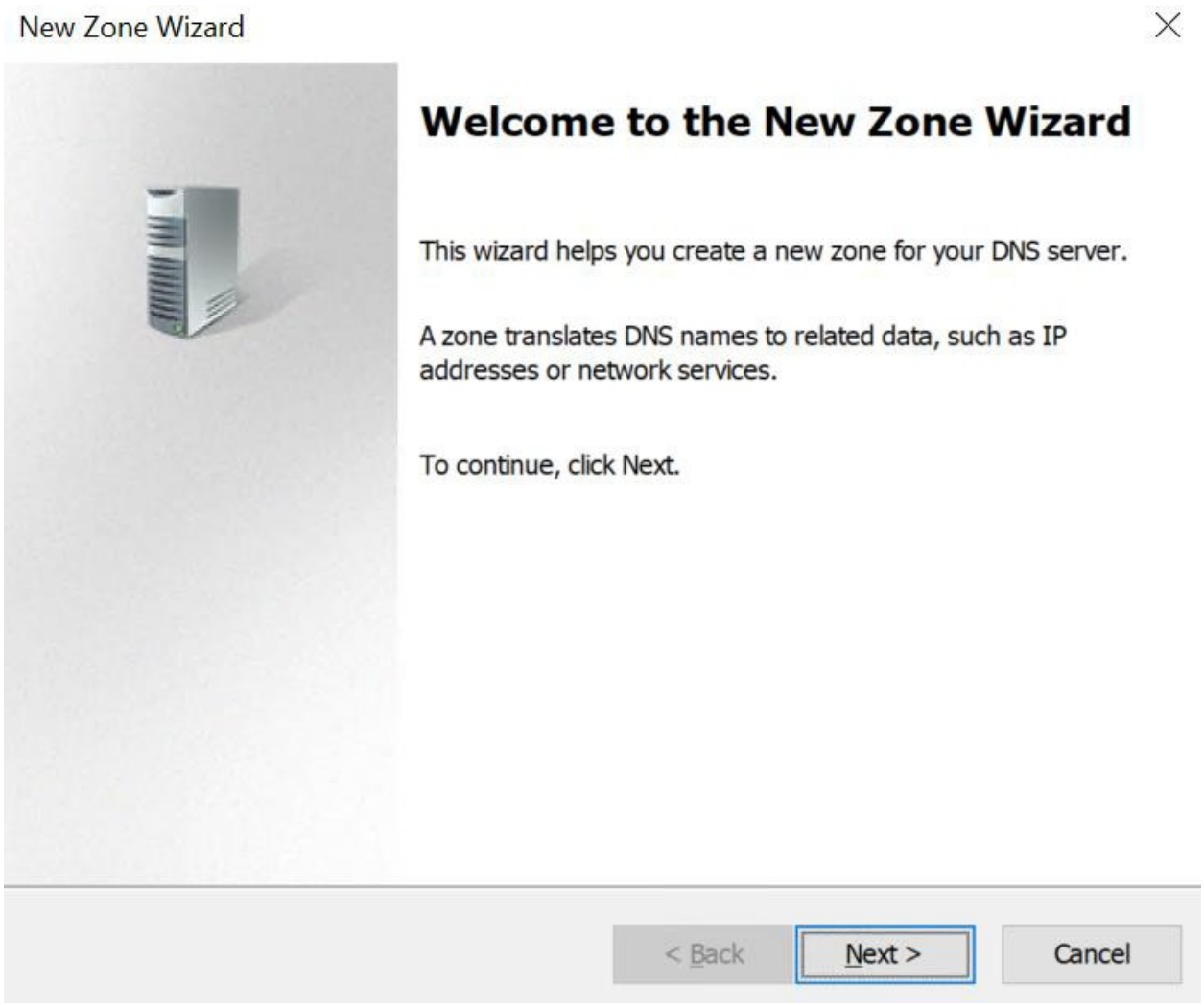

Figure 11 : Zone creation wizard

3. Select **Zone Type** and click **Next**.

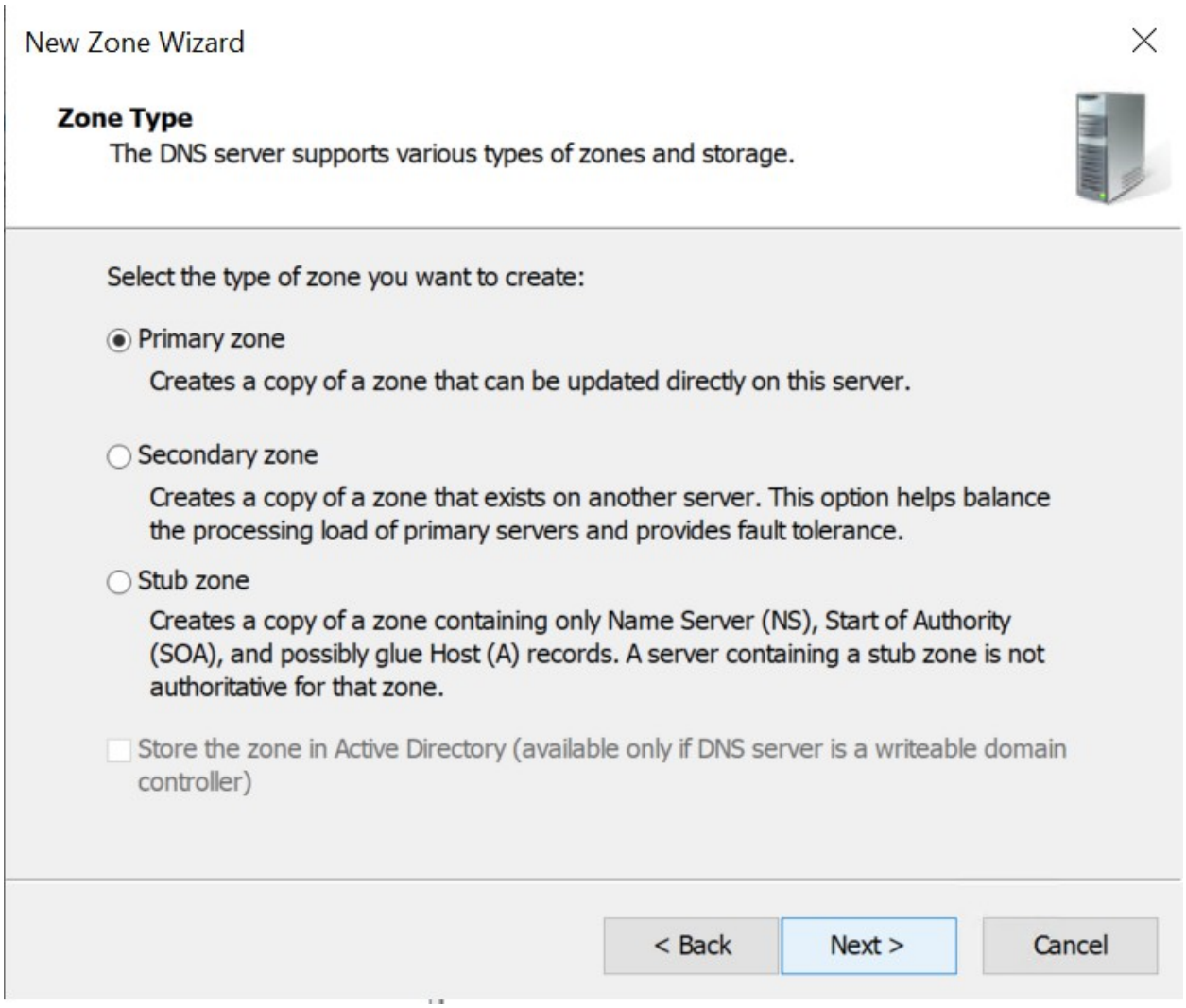

Figure 12 : New Zone Wizard

If your system is joined to domain, then you will get the option to select the **Active Directory Zone Replication Scope** as shown below.

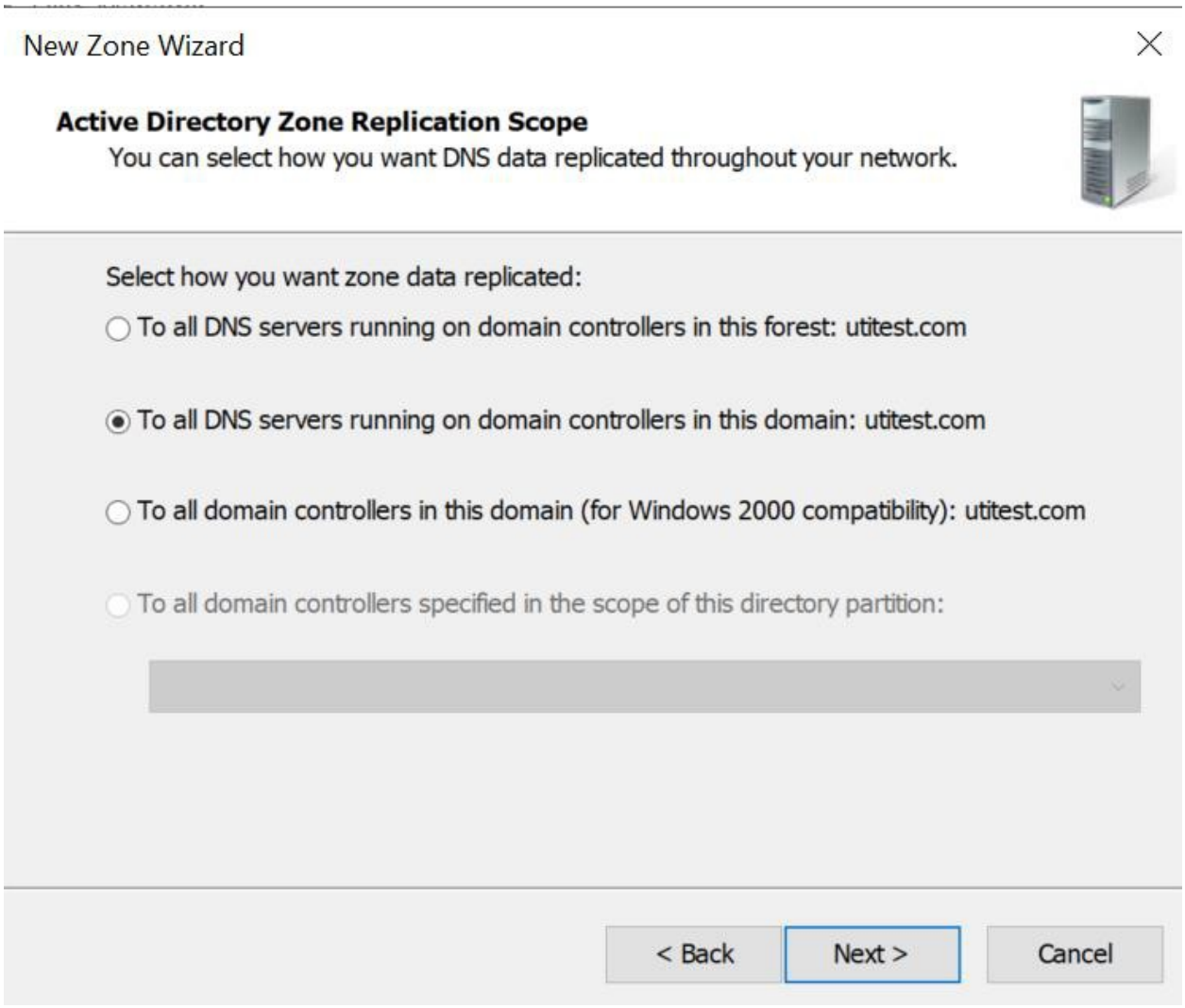

Figure 13 : Active Directory Zone Replication Scope

4. Assign the **Zone Name** and click **Next**.

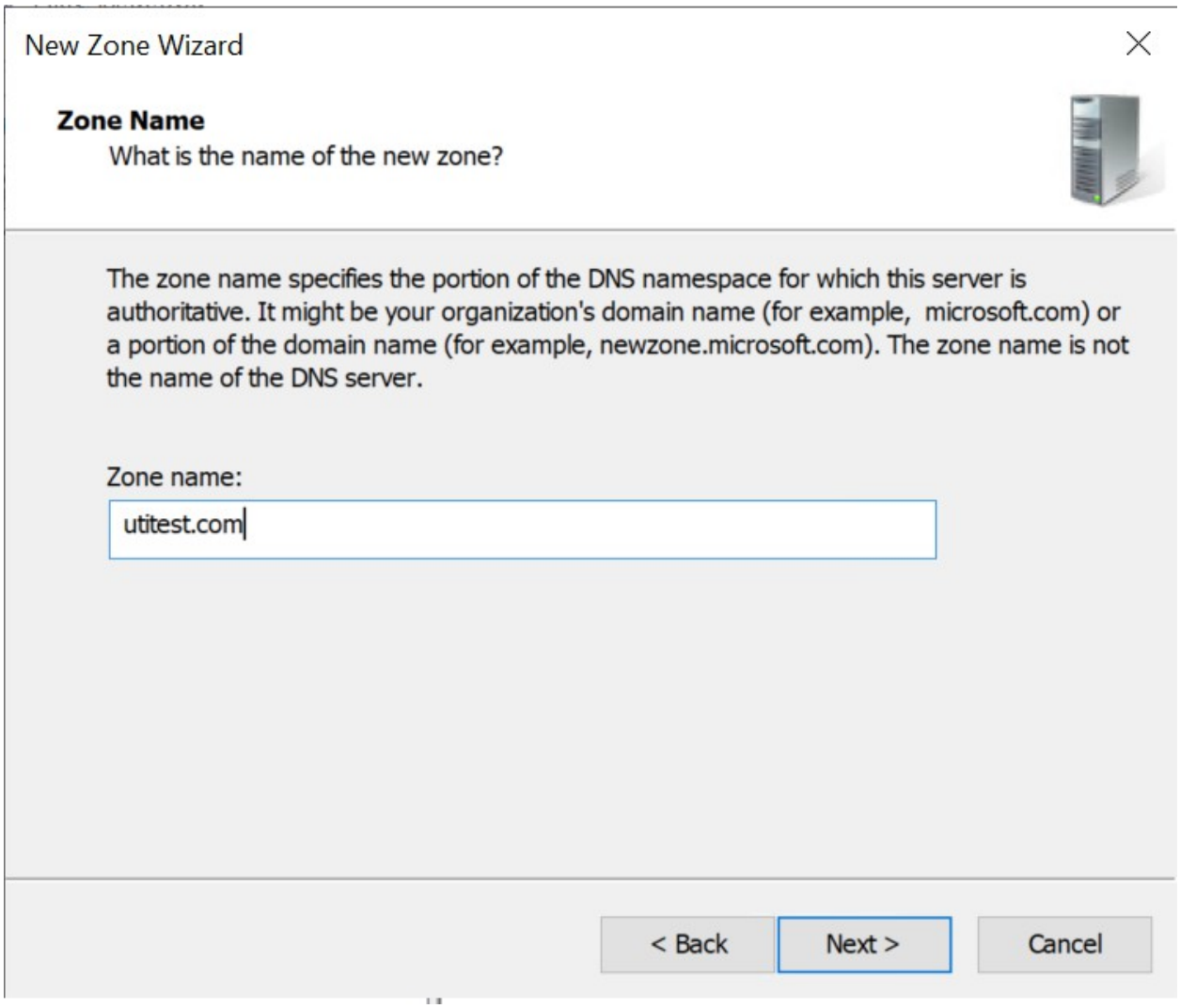

Figure 14 : Zone Name

5. Select the **Zone File** option and click **Next**.

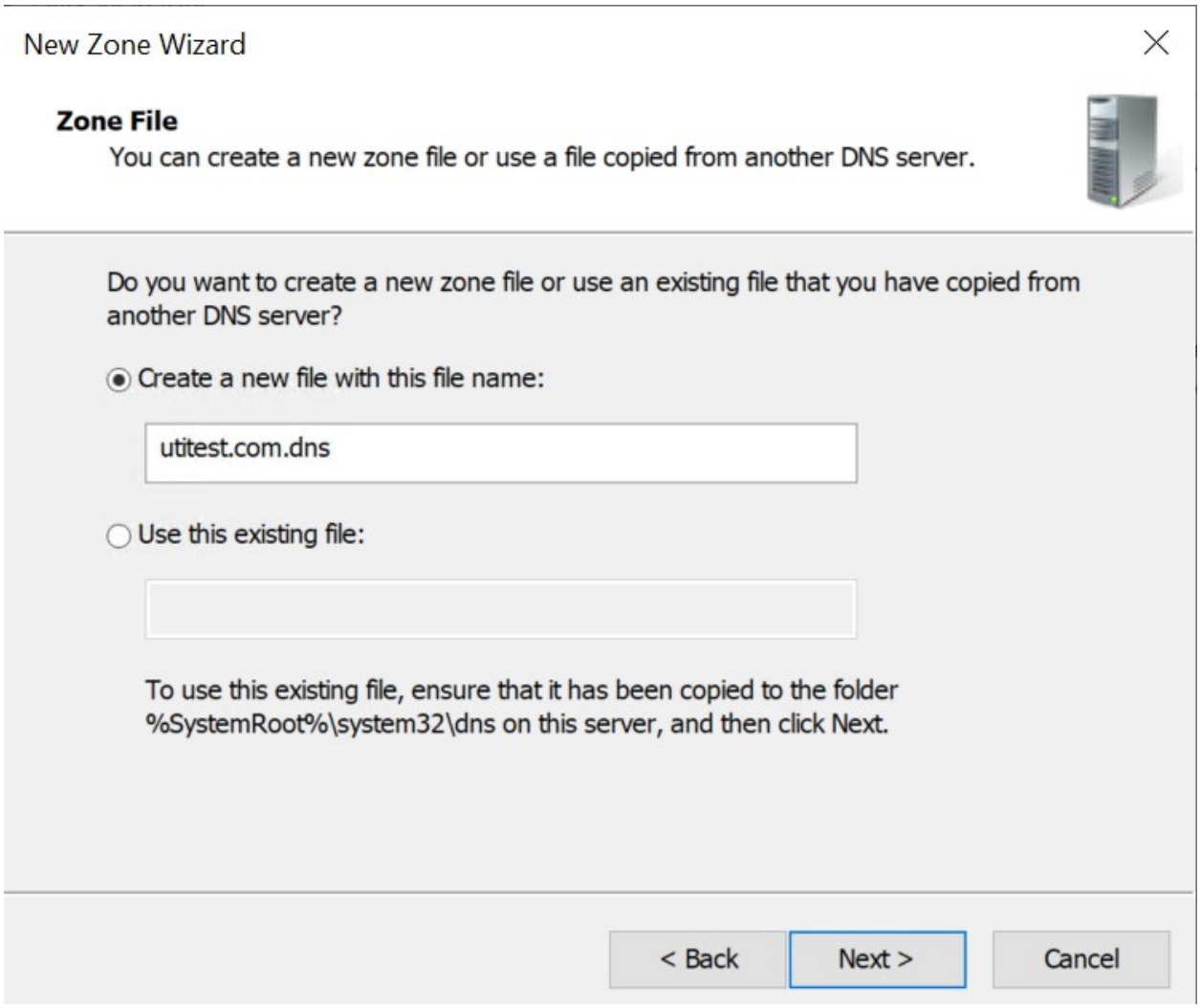

Figure 15 : Zone File name

6. Select the **Dynamic Update** option and click **Next**.

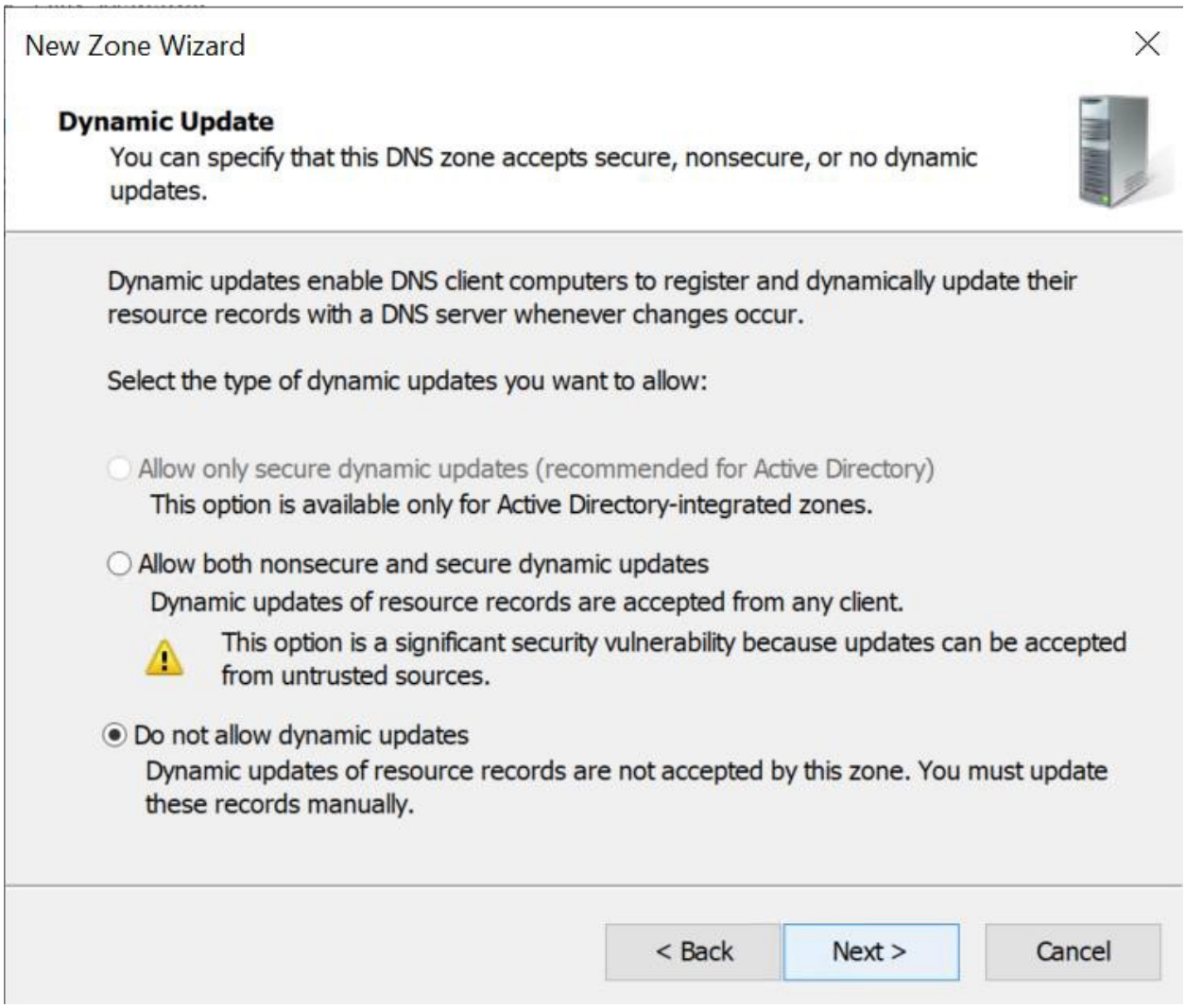

Figure 16 : Dynamic Update option

If your system is in domain, then all the options will be available.

7. Check the information and click **Finish**.

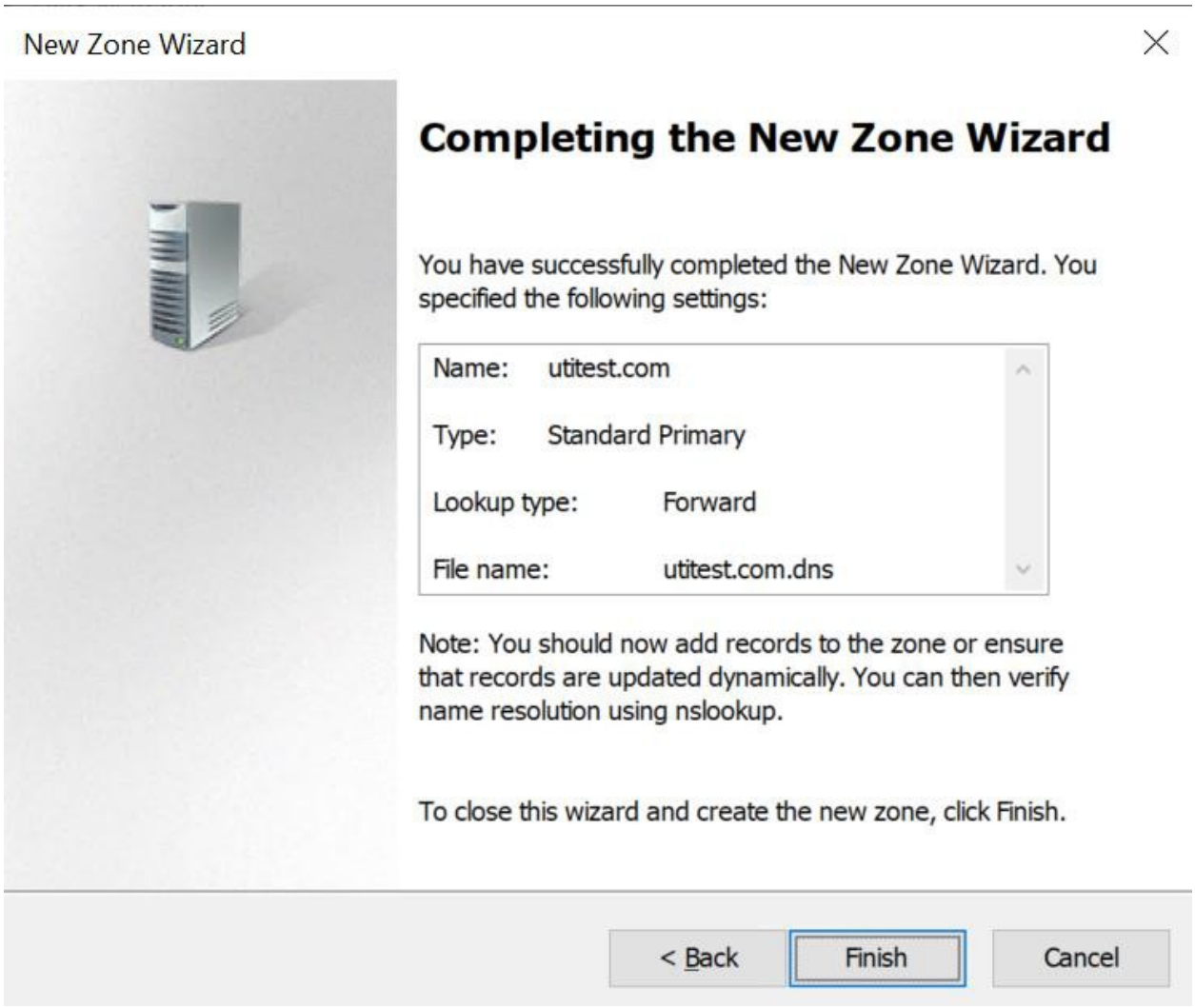

Figure 17 : Completing New Zone Wizard

5.3 Sign Forward Lookup Zone

1. Click on **Server Manager** by selecting **Start** > **Server Manager**.
2. Click **Tools** and open **DNS Manager**.

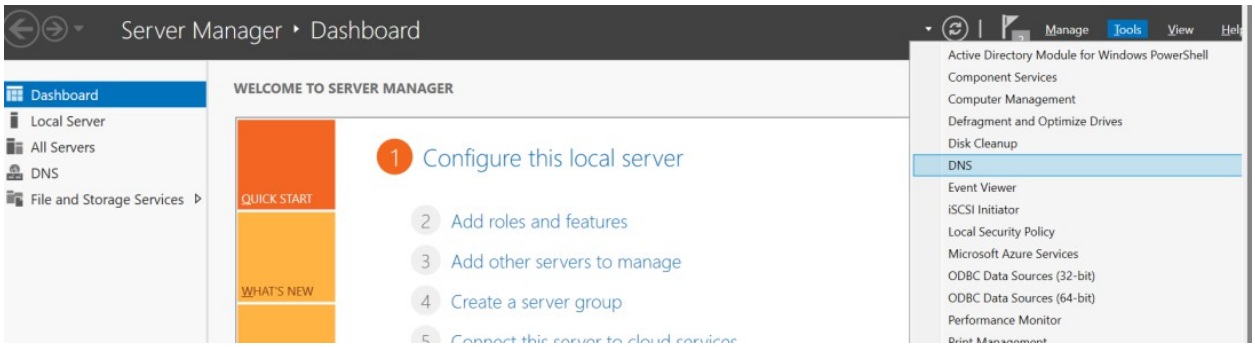

Figure 18 : Server Manager

3. In the **DNS Manager**, browse to your **Domain** name, then right click on the forward zone that you have created.
4. Click **DNSSEC** and then click **Sign the Zone**.

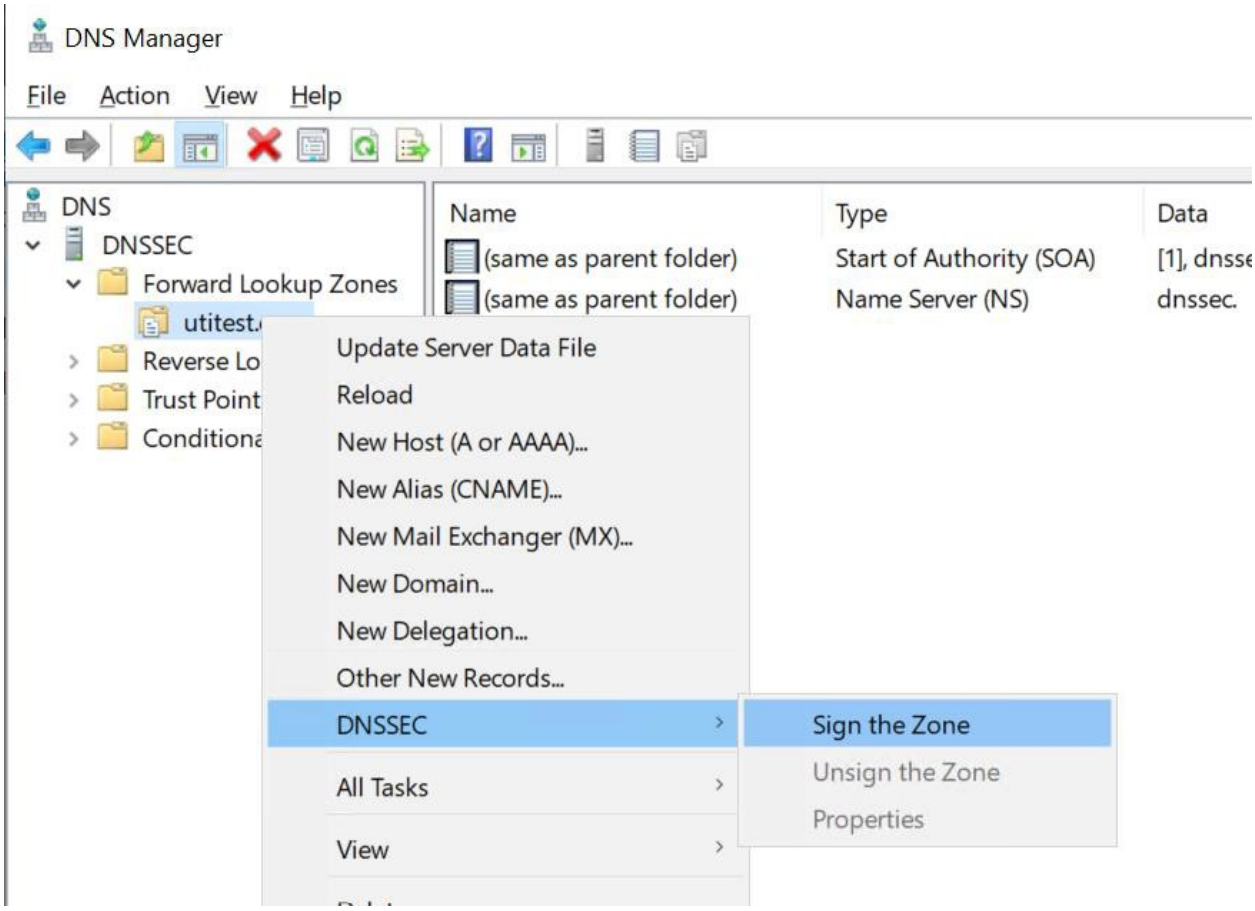

Figure 19 : Sign the Zone

5. In the **Zone Signing Wizard**, click **Next**.

Figure 20 : Zone Signing Wizard

6. In the **Zone Signing Wizard** options, click **Customize zone signing parameters**, and then click **Next**.

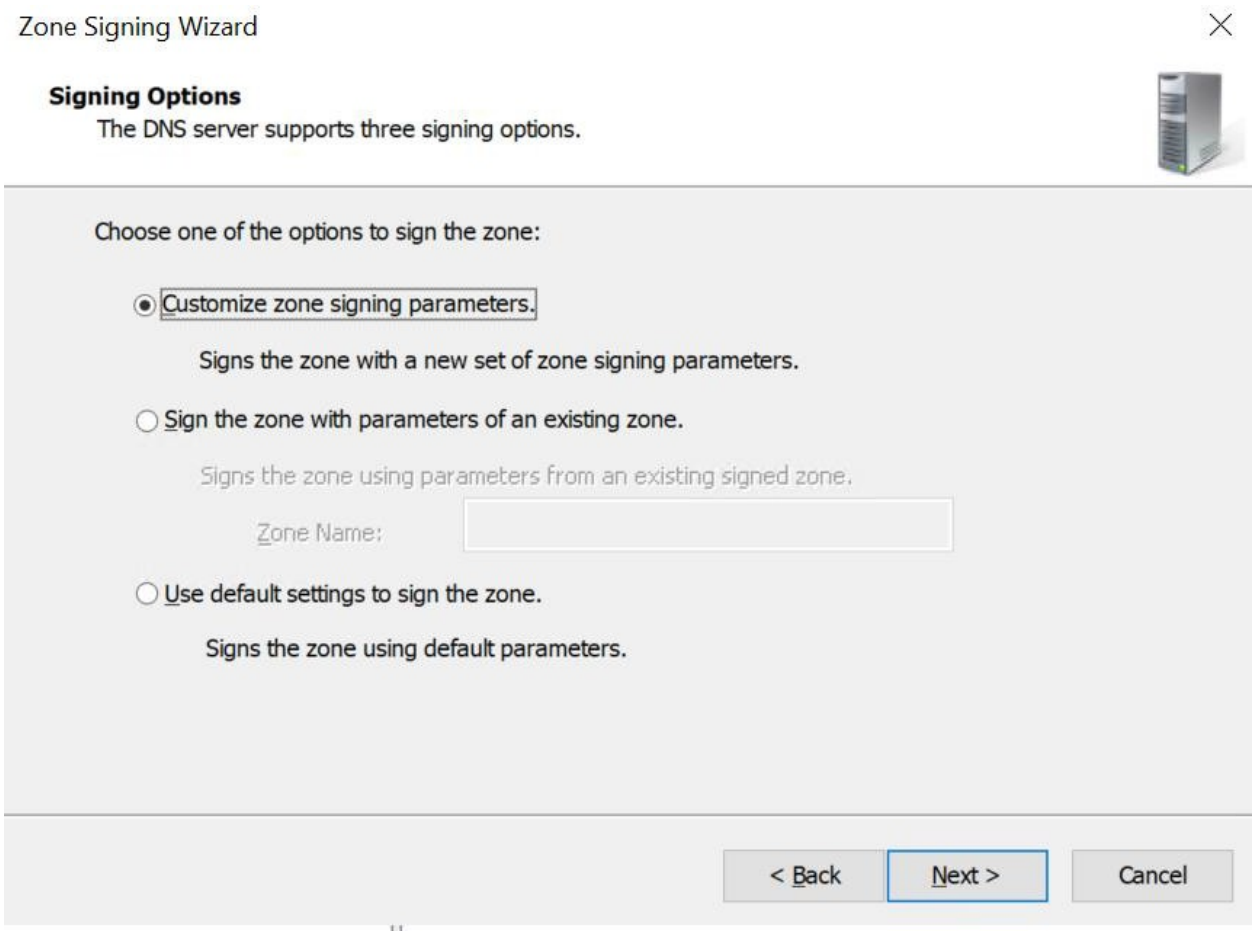

Figure 21 : Signing Options

7. On the **Key Signing Key (KSK)** Wizard, click **Next**.

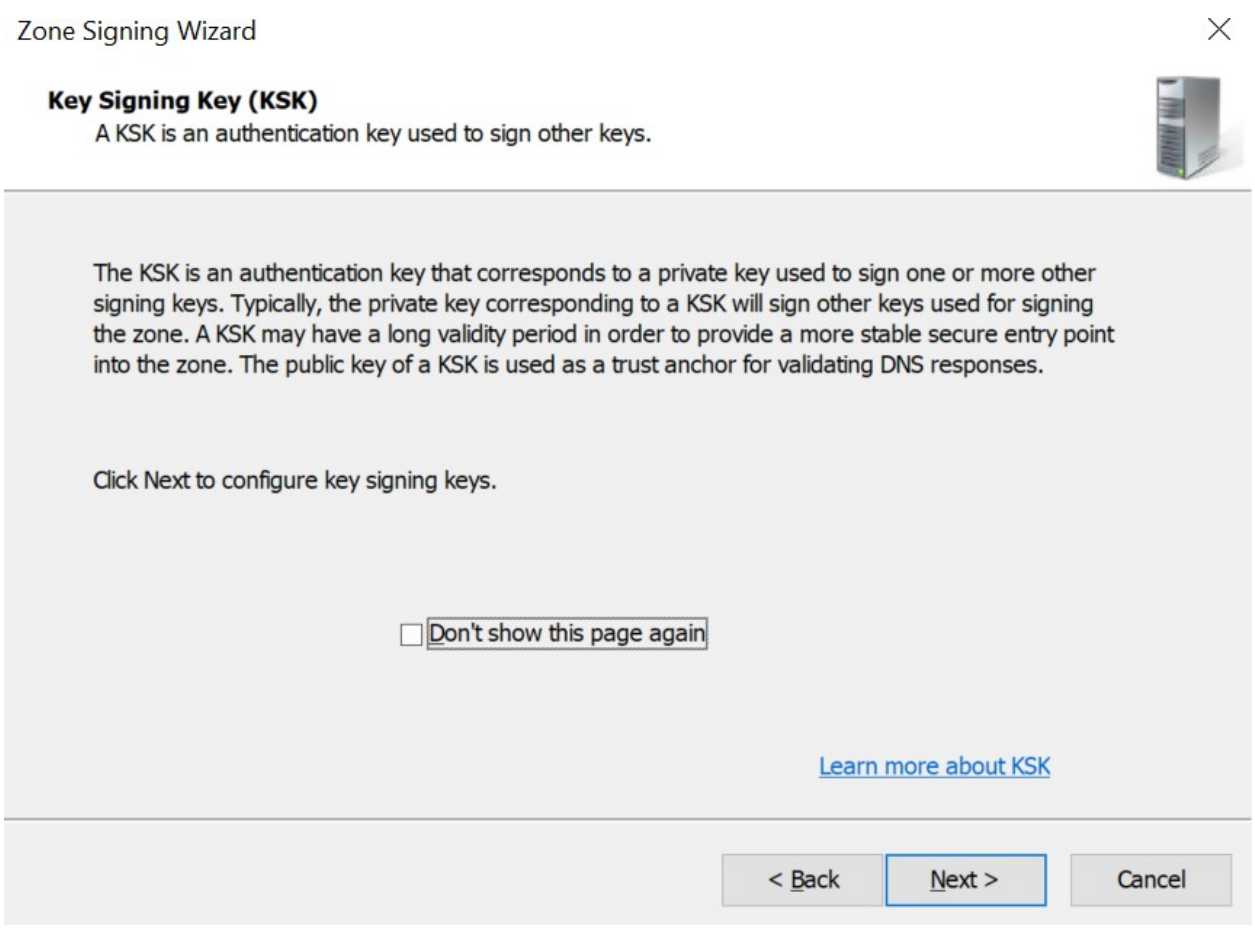

Figure 22 : Key Signing Key

8. On the **Key Signing Key (KSK)** Wizard, click **Add**.

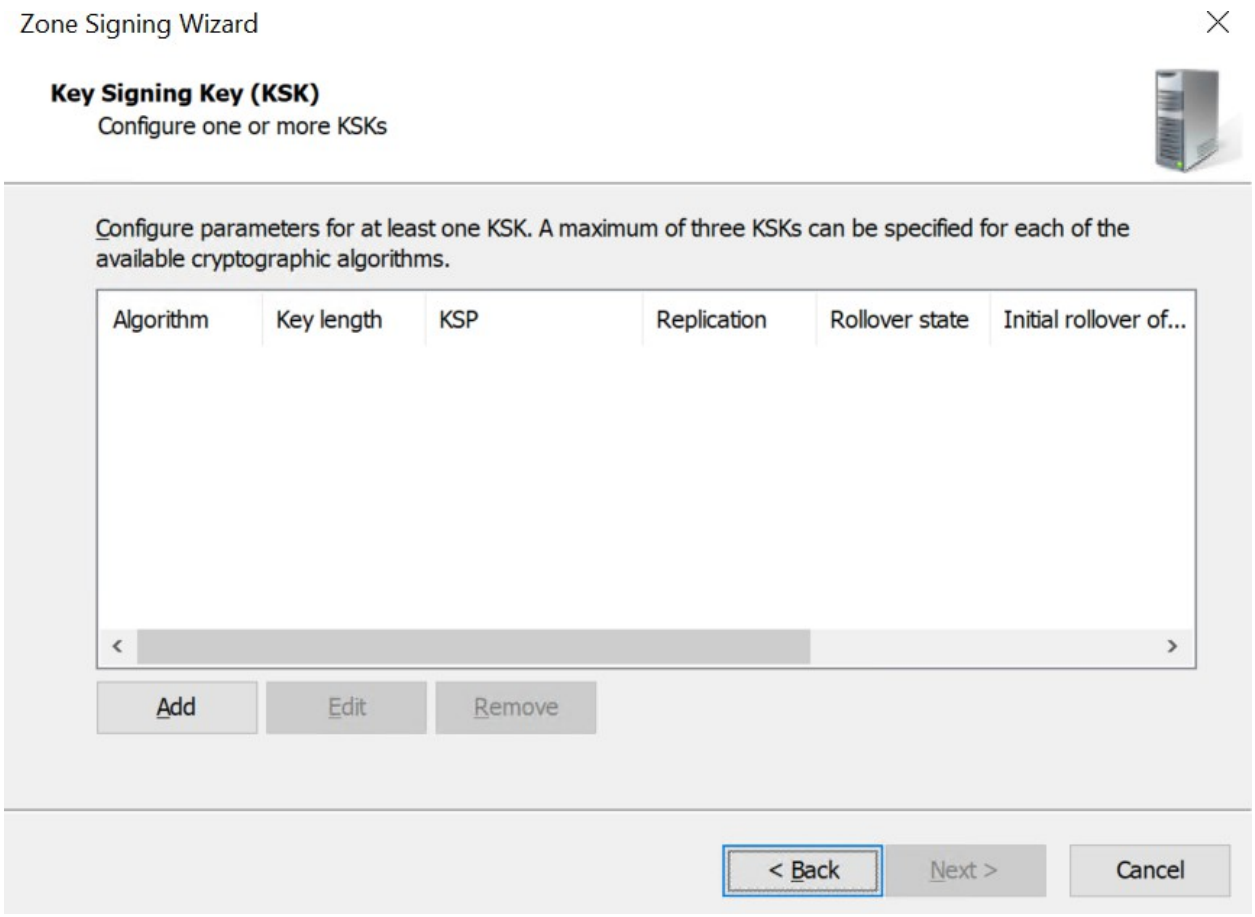

Figure 23 : Key Signing Key Wizard

9. On the **New Key Signing Key (KSK)** Wizard, from the dropdown of **Select a key storage provider to generate and store keys**, select **Utimaco CryptoServer Key Storage Provider**.
10. Provide other information such as **Cryptographic Algorithm** and **Key Length** and then click **OK**.
11. Uncheck the **rollover** option.

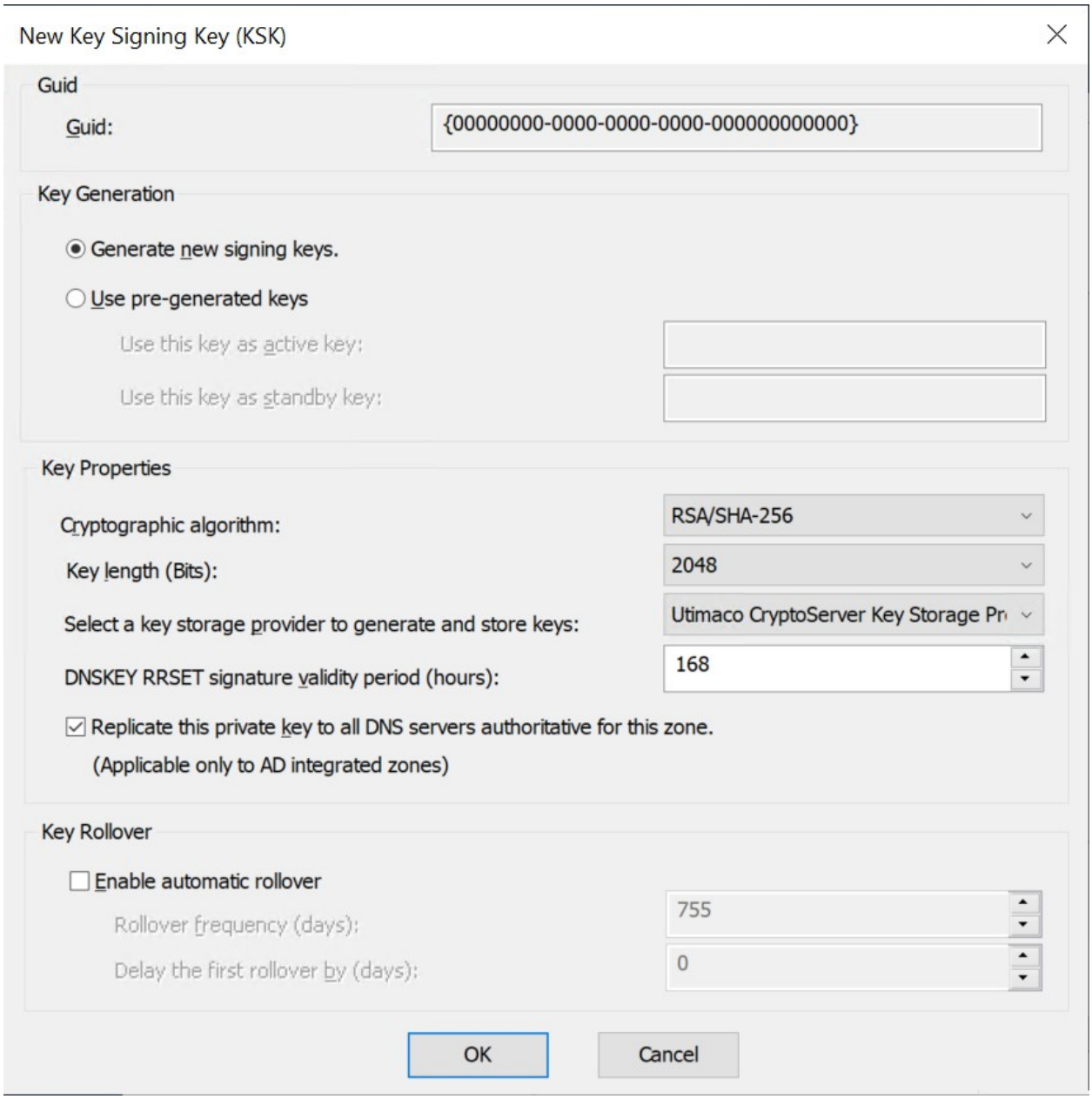

Figure 24 : New Key Signing Key

Automatic key rollover is not supported with Utimaco HSM. The user has to manually rollover the keys before their expiry.

12. On the **Key Signing Key (KSK)** interface, click **Next**.

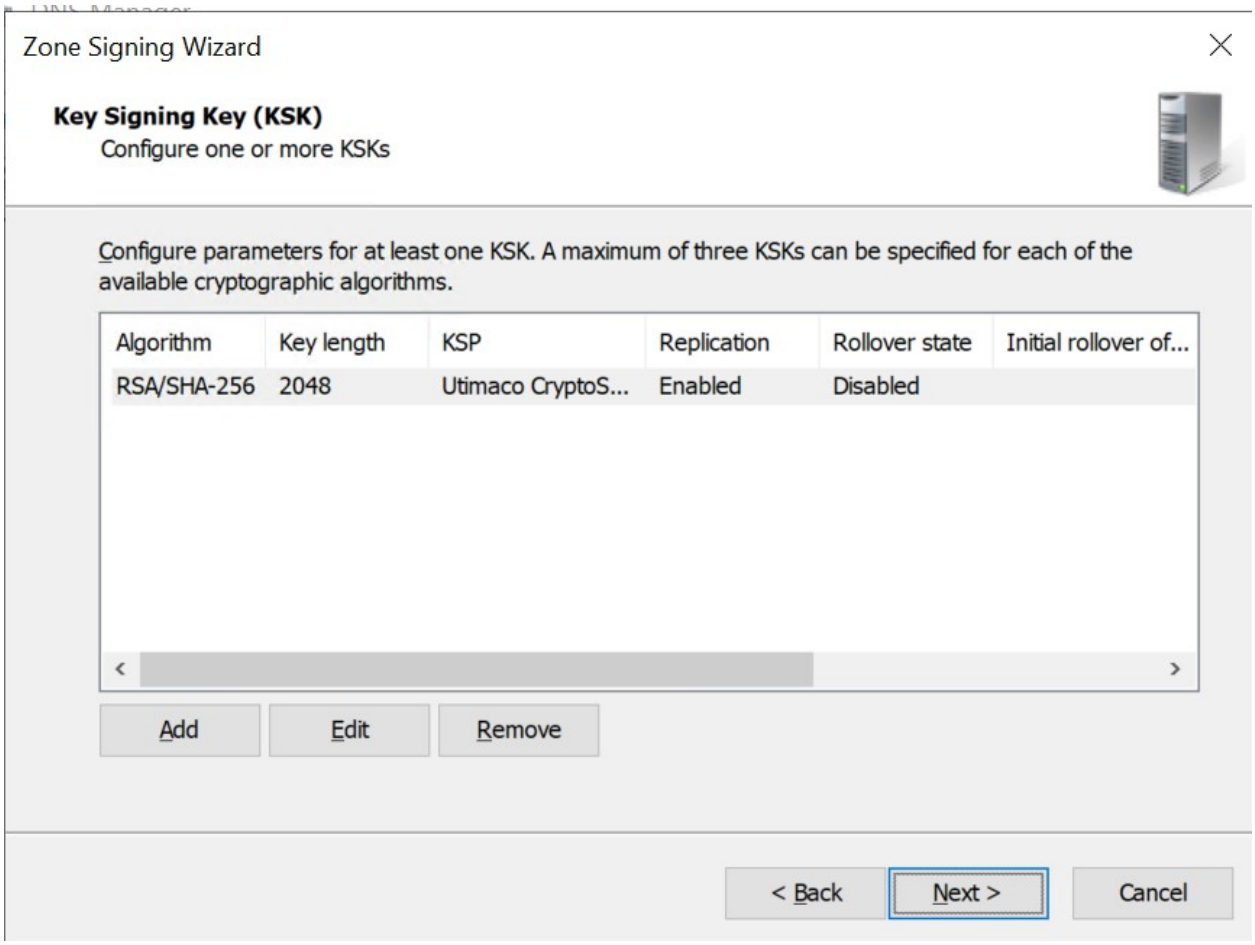

Figure 25 : New Key Signing Key

13. On the **Zone Signing Key (ZSK)** Wizard, click **Next**.

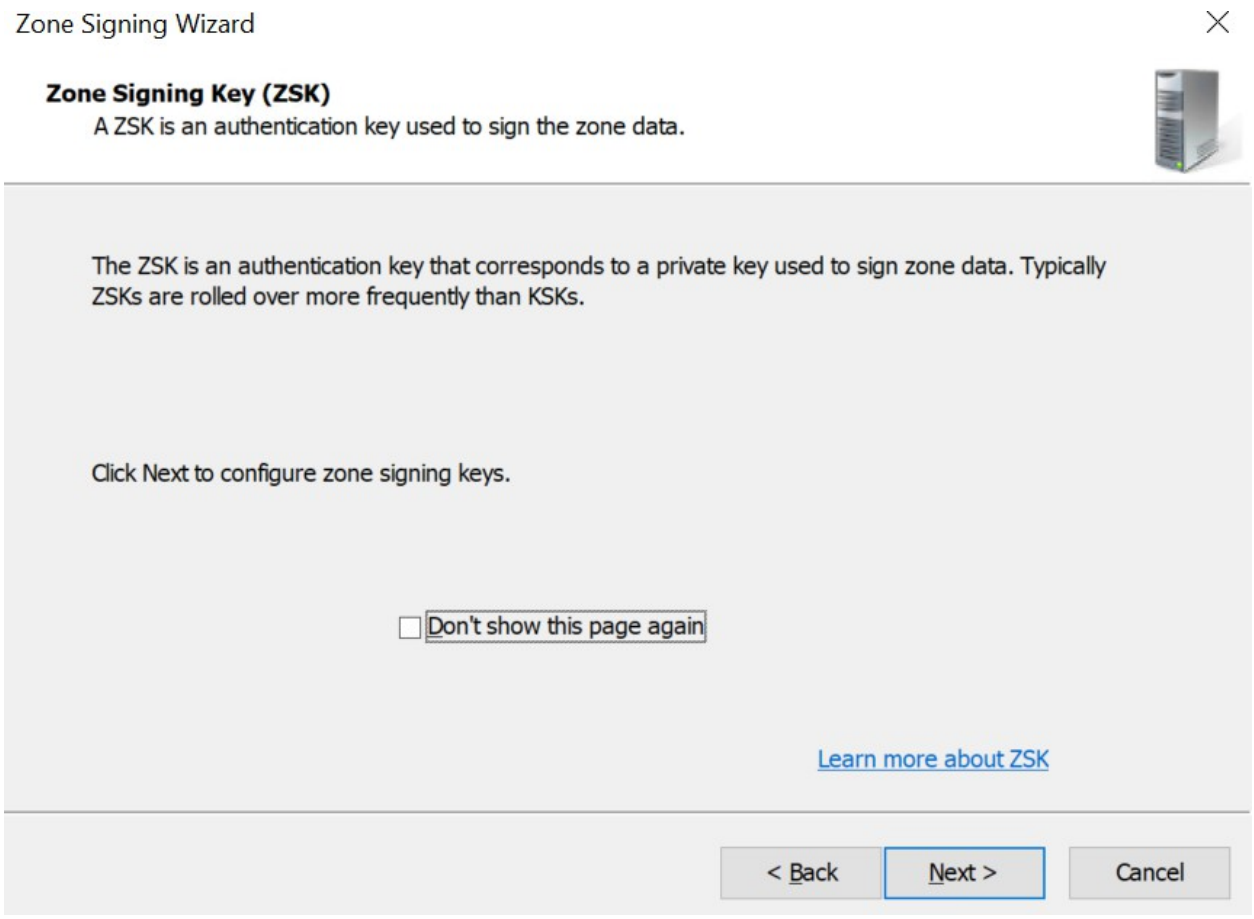

Figure 26 : Zone Signing Key Wizard

14. On the **Zone Signing Key (ZSK)** interface, click **Add**.
15. On the **New Zone Signing Key (ZSK)** interface, from the dropdown of **Select a key storage provider to generate and store keys**, select **Utimaco Key Storage Provider**.
16. Provide other information such as **Cryptographic Algorithm** and **Key Length** and click **OK**.
17. Uncheck the **rollover** option.

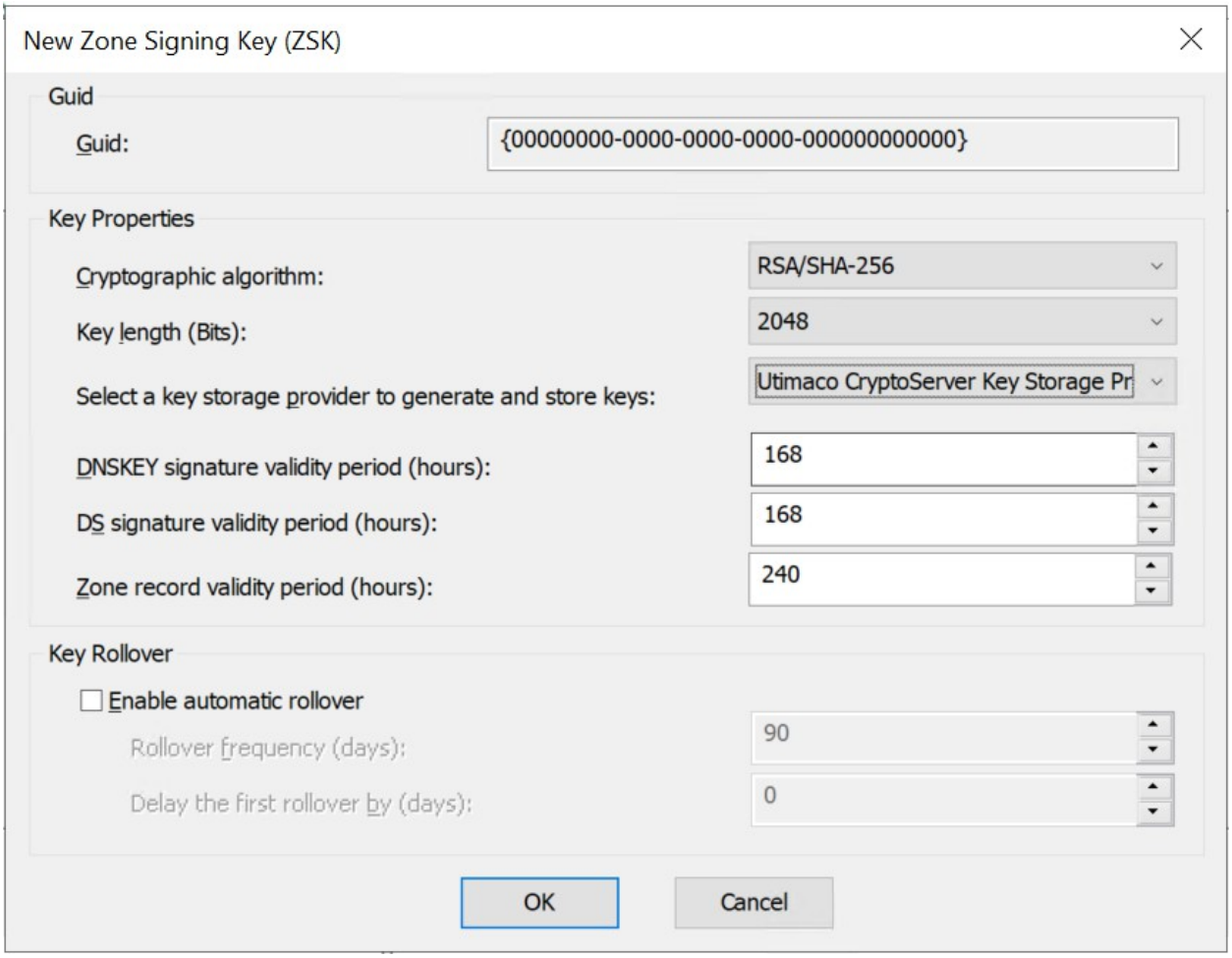

Figure 27 : New Zone Signing Key

Automatic key rollover is not supported with Utimaco HSM. The user has to manually rollover the keys before their expiry.

18. On the **Zone Signing Key (ZSK)** Wizard, click **Next**.

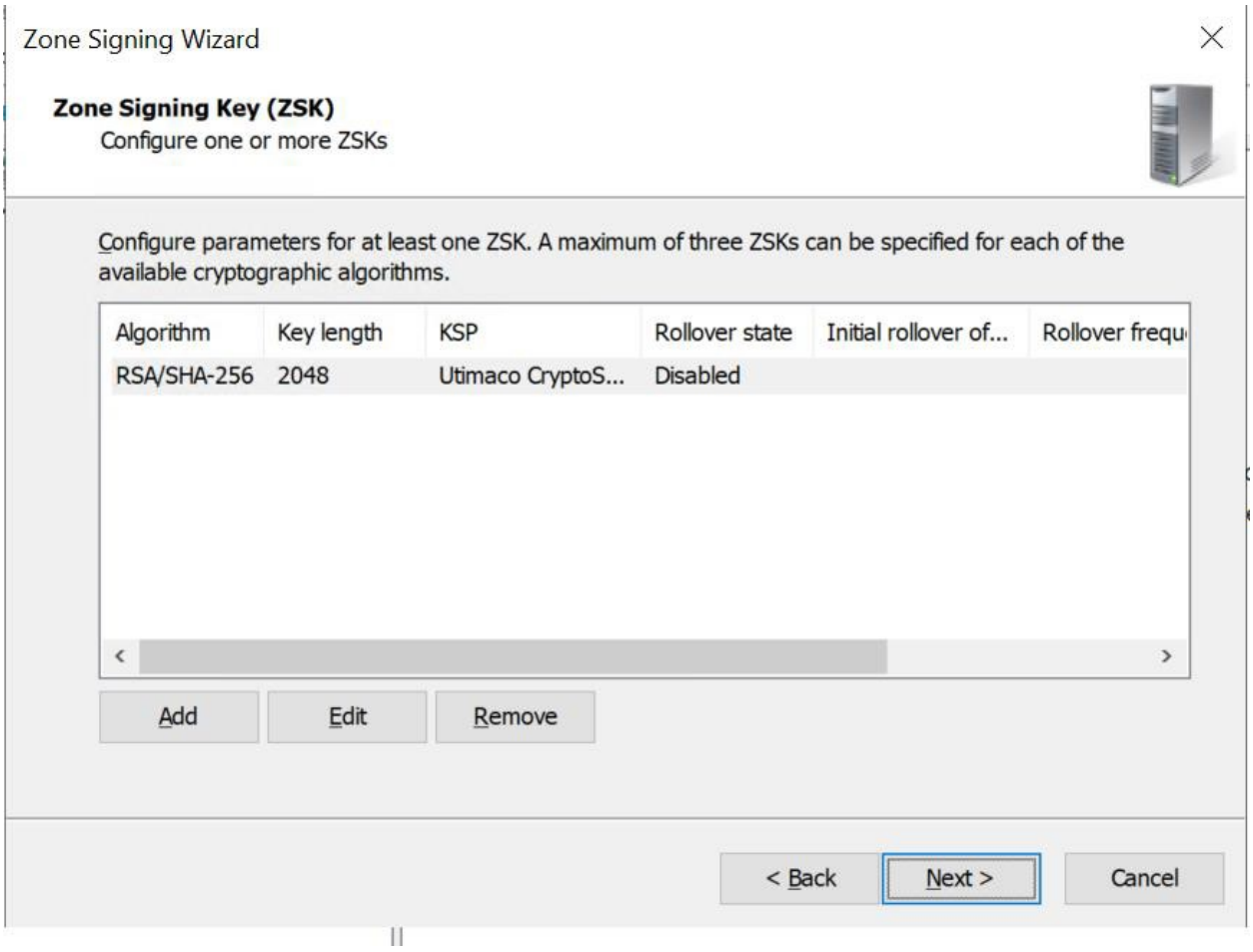

Figure 28 : Configure parameters for Zone Signing Key

19. On the **Next Secure (NSEC)** Wizard select **NSEC3**, click **Next**.

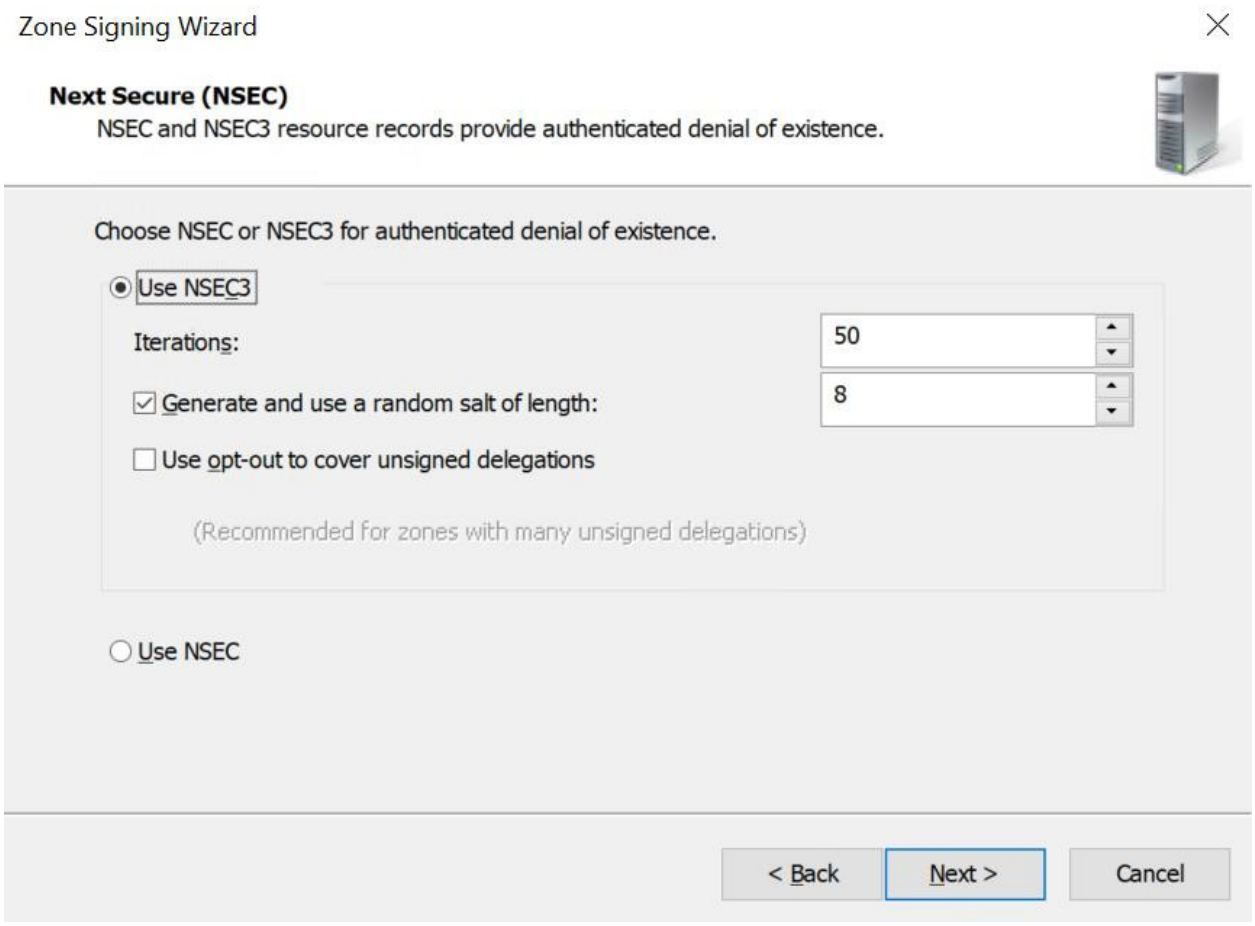

Figure 29 : Next Secure Wizard

20. On the **Trust Anchors (TAs)** interface, check the **Enable the distribution of trust anchors for this zone** box, and click **Next**.

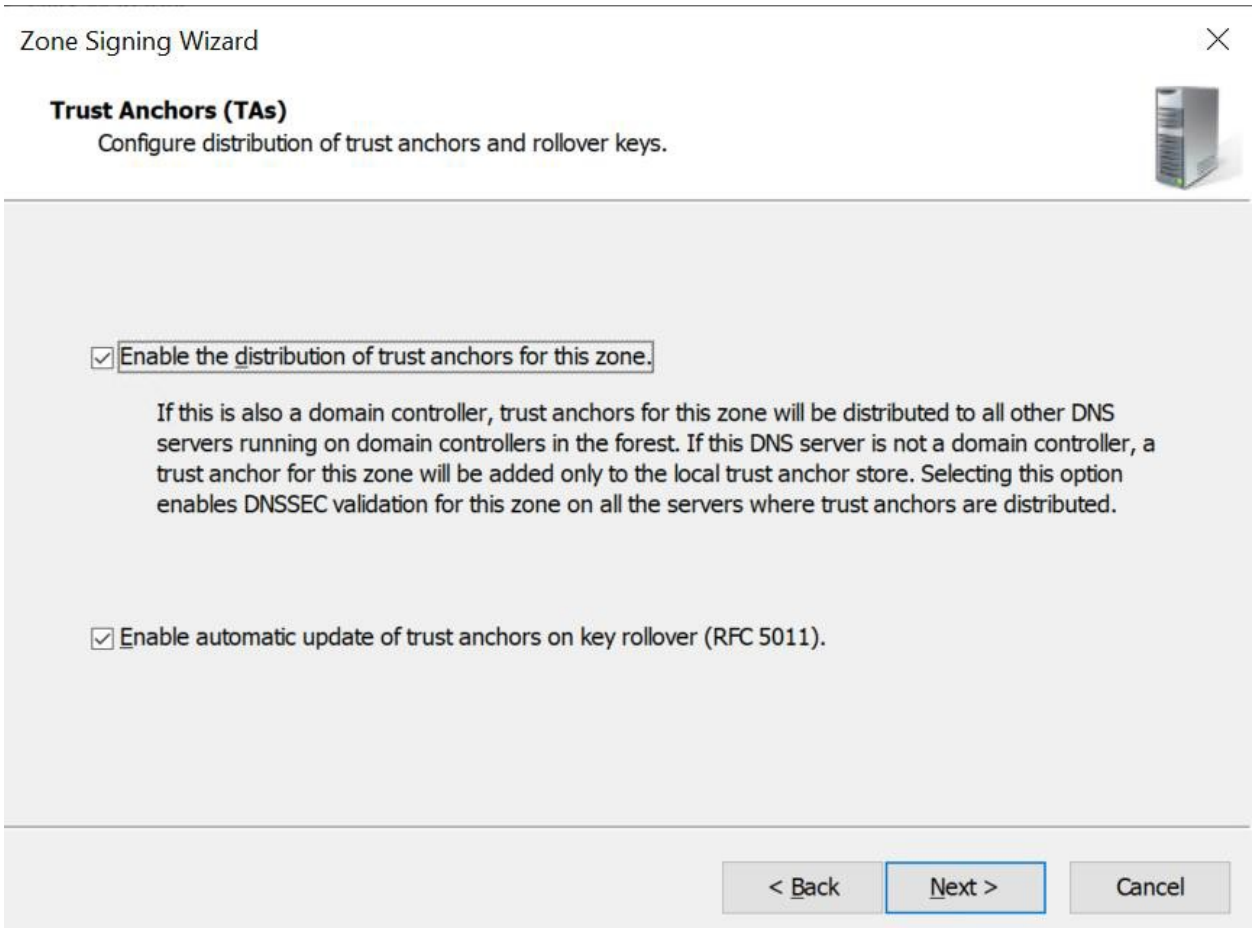

Figure 30 : Trust Anchors

21. On the **Signing and Polling Parameters** wizard, click **Next**.

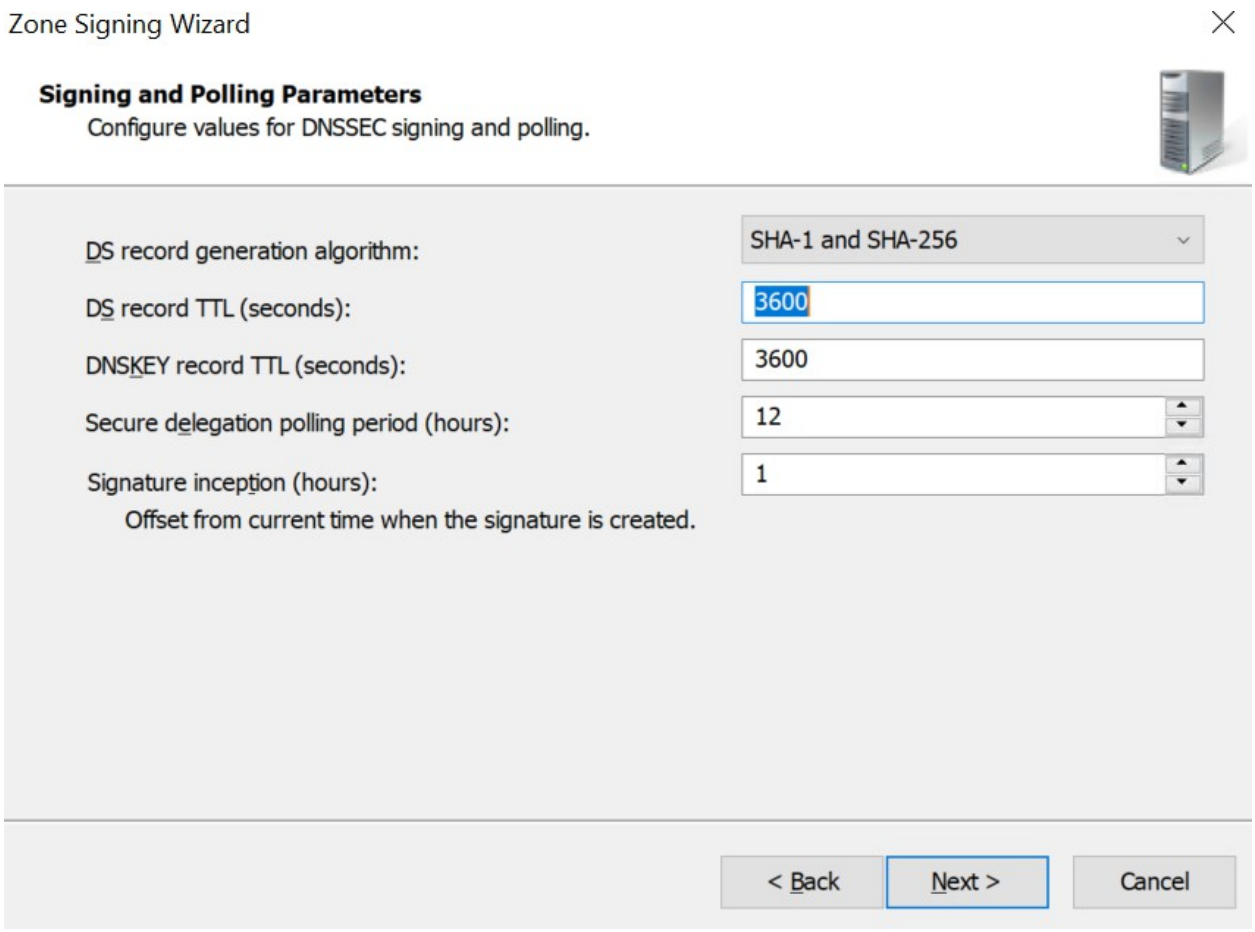

Figure 31 : Signing and Polling Parameters

22. On the **DNS Security Extensions (DNSSEC)** interface, click **Next**, and then click **Finish**.

Figure 32 : DNS Security Extensions

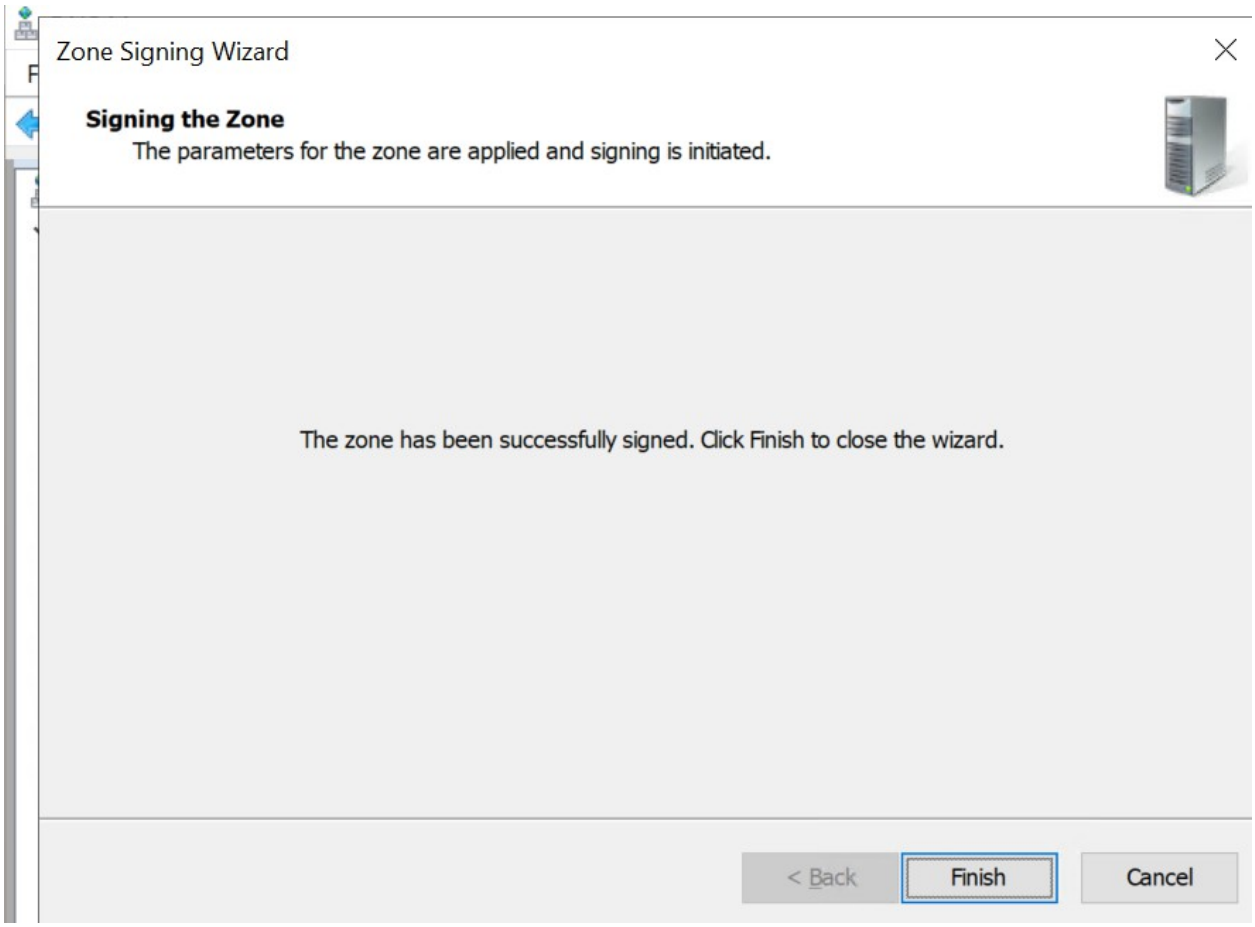

Figure 33 : Signing the Zone

23. In the DNS console, expand **Trust Points**, then select **com** and select **utitest**, and click your domain name.

24. Ensure that the DNSKEY resource records display, and that their status is valid.

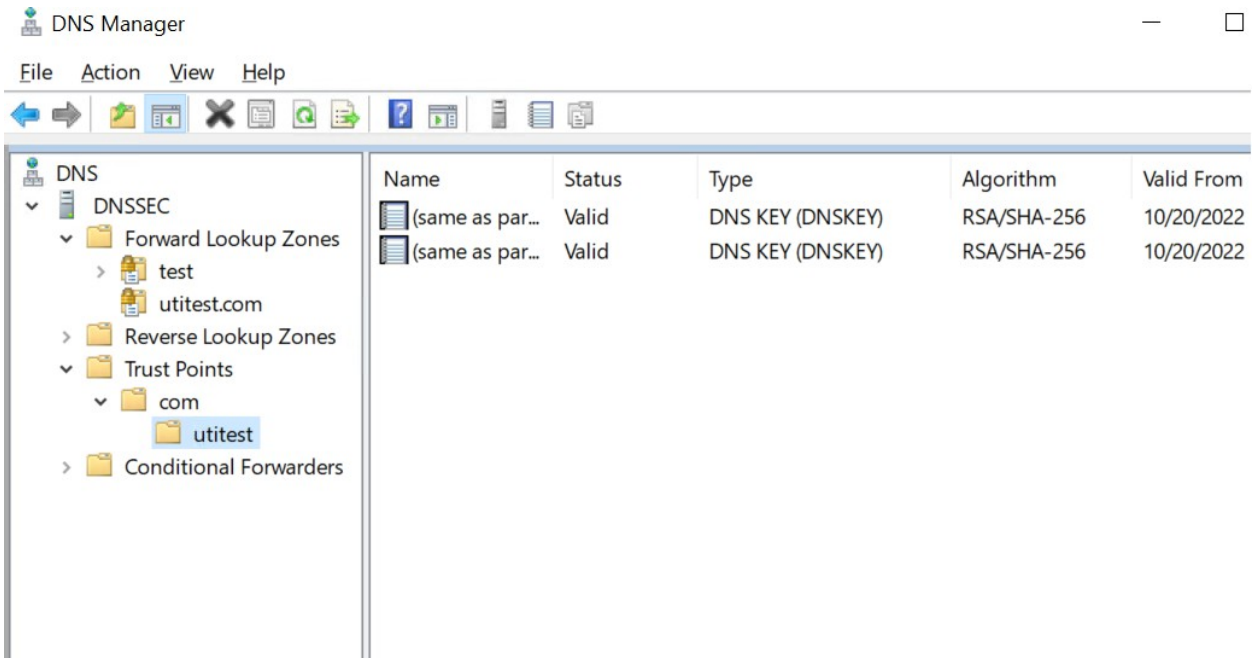

Figure 34 : DNS Manager

25. Open **Server Manager**, click **Tools** and open **Group Policy Management**.

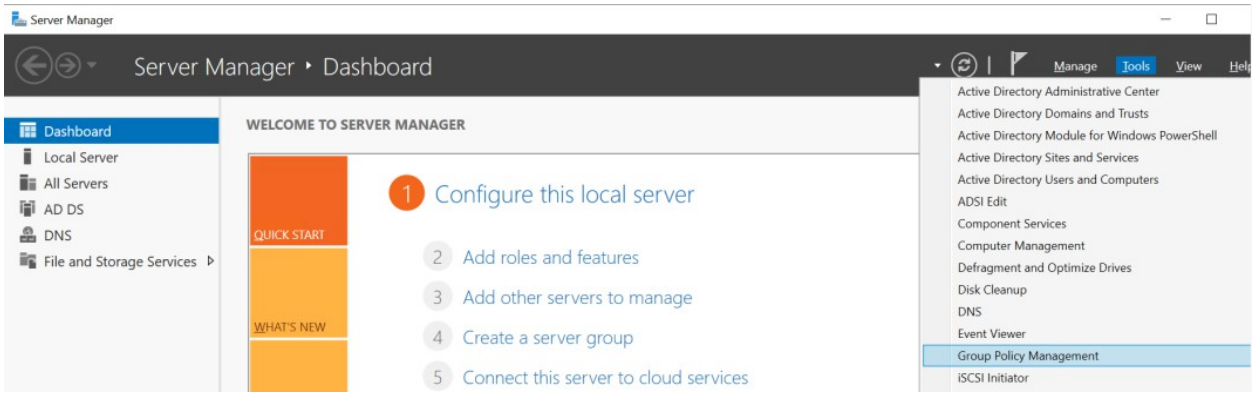

Figure 35 : Server Manager

26. Next, open **Local Computer policy** -> **Computer Configuration** -> **Windows Settings** -> **Name Resolution Policy**.

Figure 36 : Local Group Policy Editor

27. In the right pane, under **Create Rules**, in the **Suffix** box, type utitest.com to apply the rule to the suffix of the namespace.
28. Select both the **Enable DNSSEC in this rule** check box and the **Require DNS clients to check that the name and address data has been validated by the DNS server** check box, and click **Create**.
29. Restart DNS service and check its settings.

›_ Console

```
C:\> net stop dns

C:\> net start dns C:\> Get-DnsServer
```

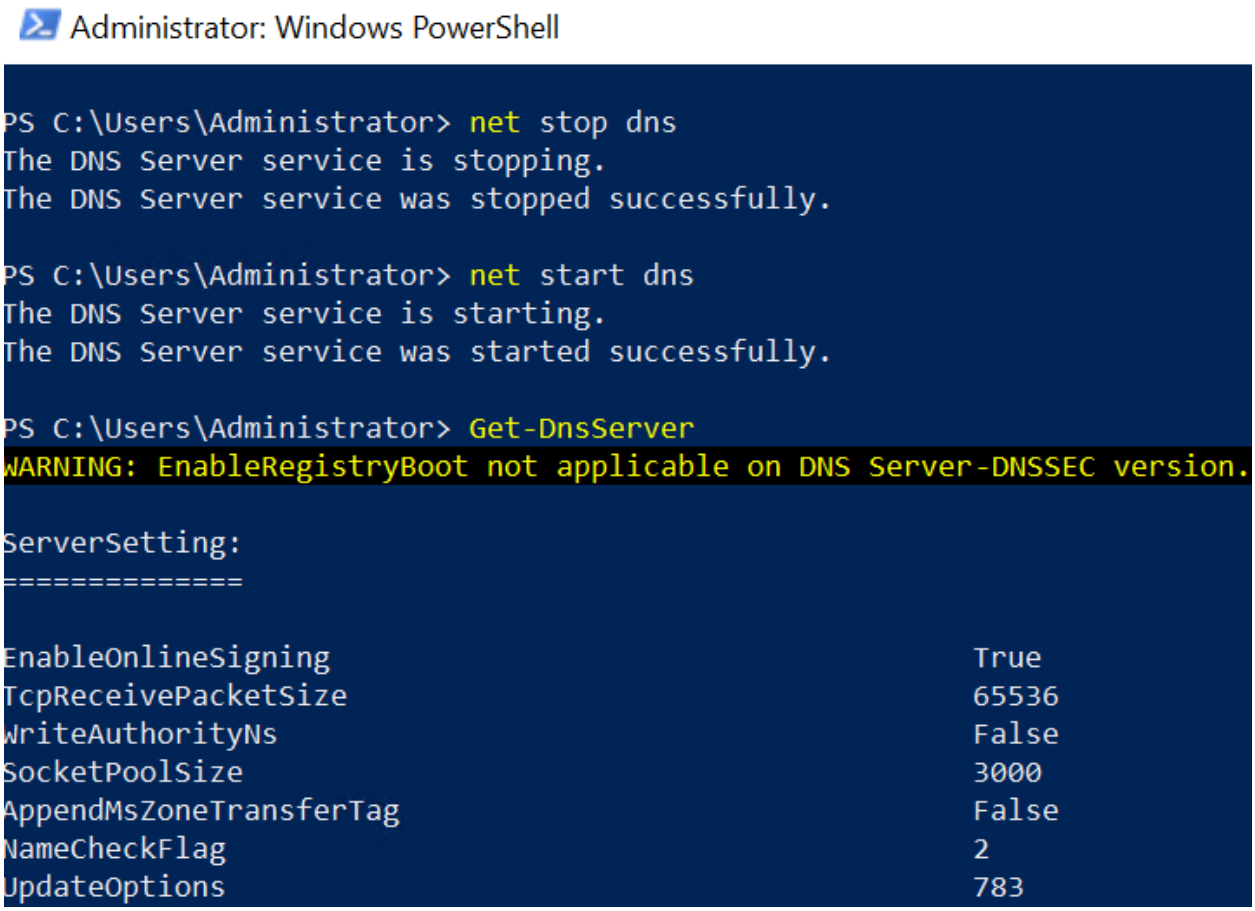

Figure 37 : DNS service stop and start

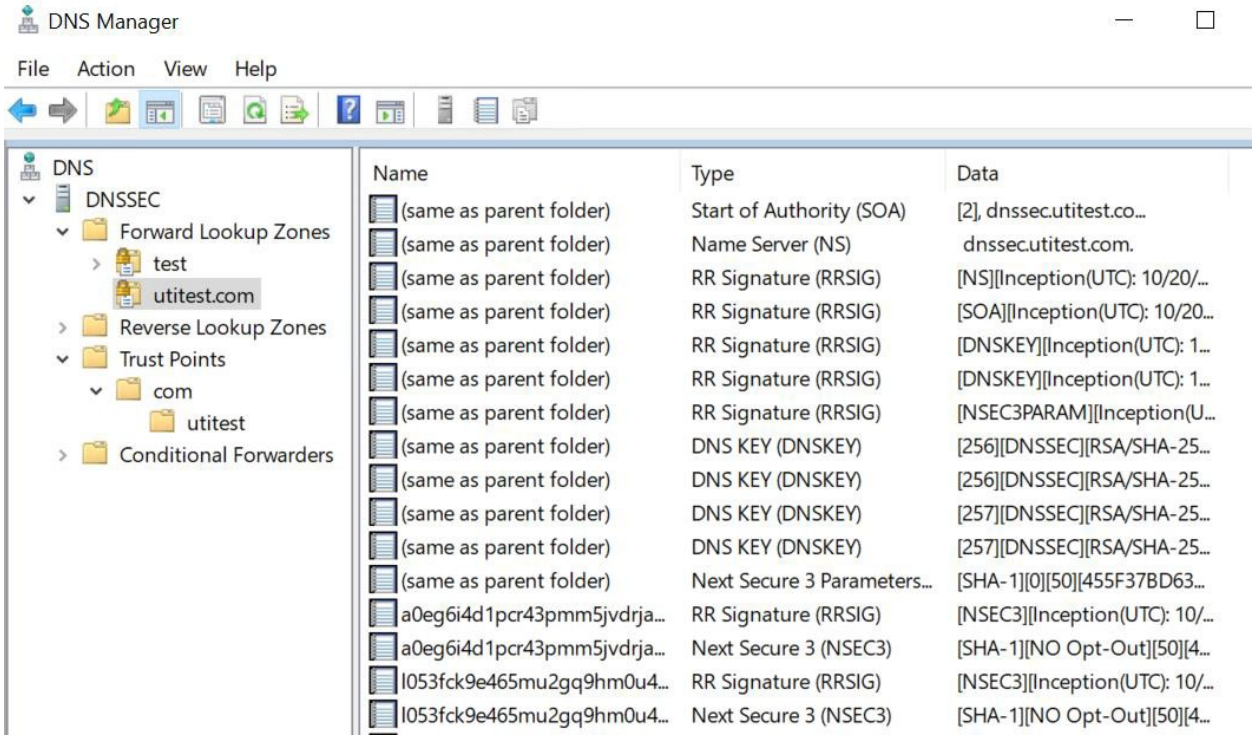

Figure 38 : DNS Manager

30. Verify that the keys are generated on the HSM.

›_ Console

```
C:\> cngtool ListKeys
```

5.4 Create Record in Forward Lookup Zone

1. In the right-side pane right-click on the forward lookup zone that you have created and click on New Host (A or AAAA) record.

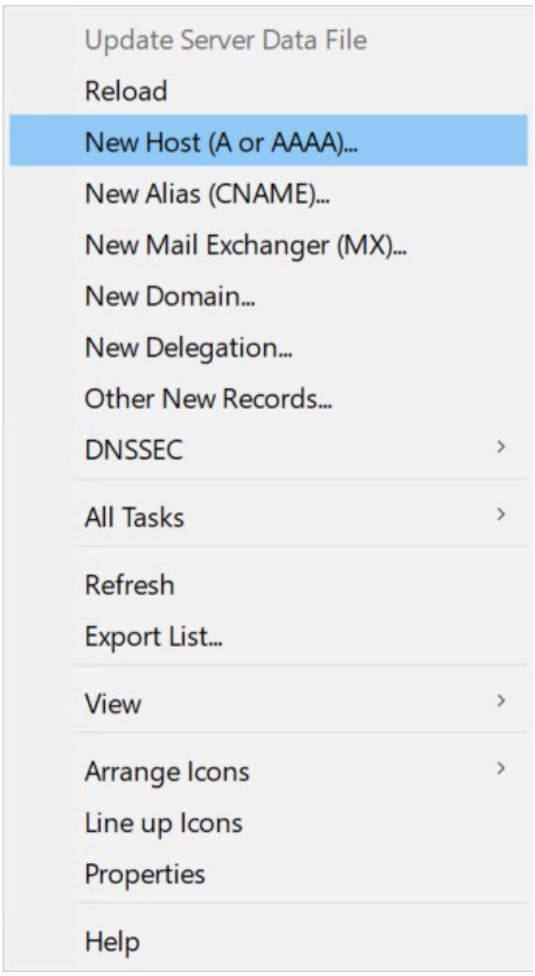

Figure 39 : Create new records

5.5 Create Reverse Lookup Zone in DNS Manager

1. Click on **Server Manager** by selecting **Start** > **Server Manager** > click **Tools** and open **DNS Manager**.

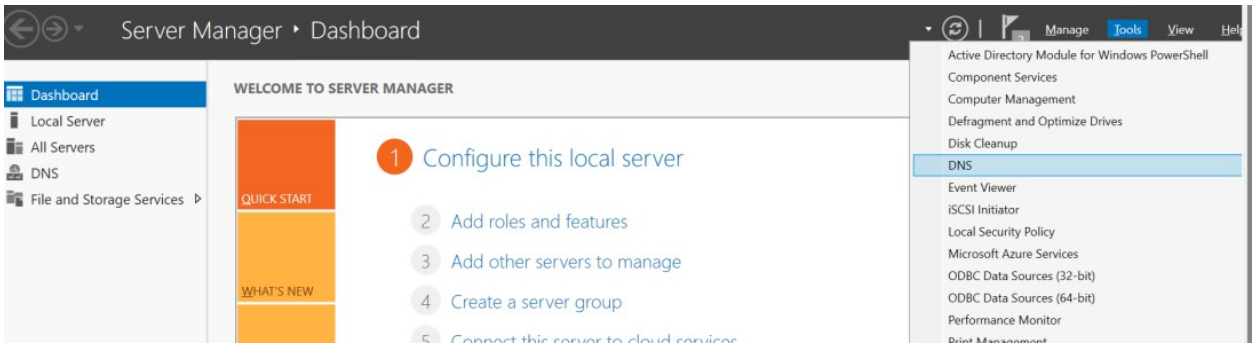

Figure 40 : Server Manager

2. In **DNS Manager** right-click on **Reverse Lookup Zone** and click on **New Zone**.

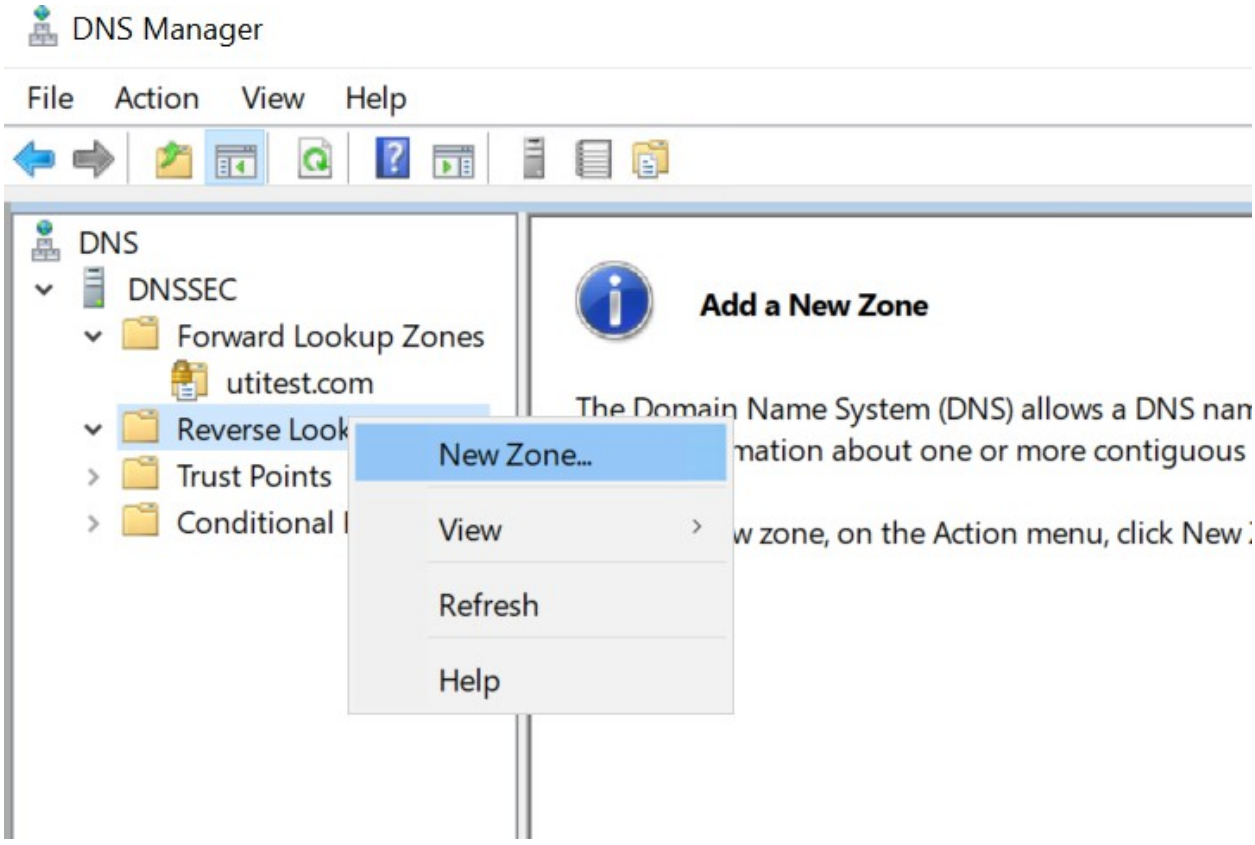

Figure 41 : DNS Manager

3. In **New Zone Wizard** click **Next**.

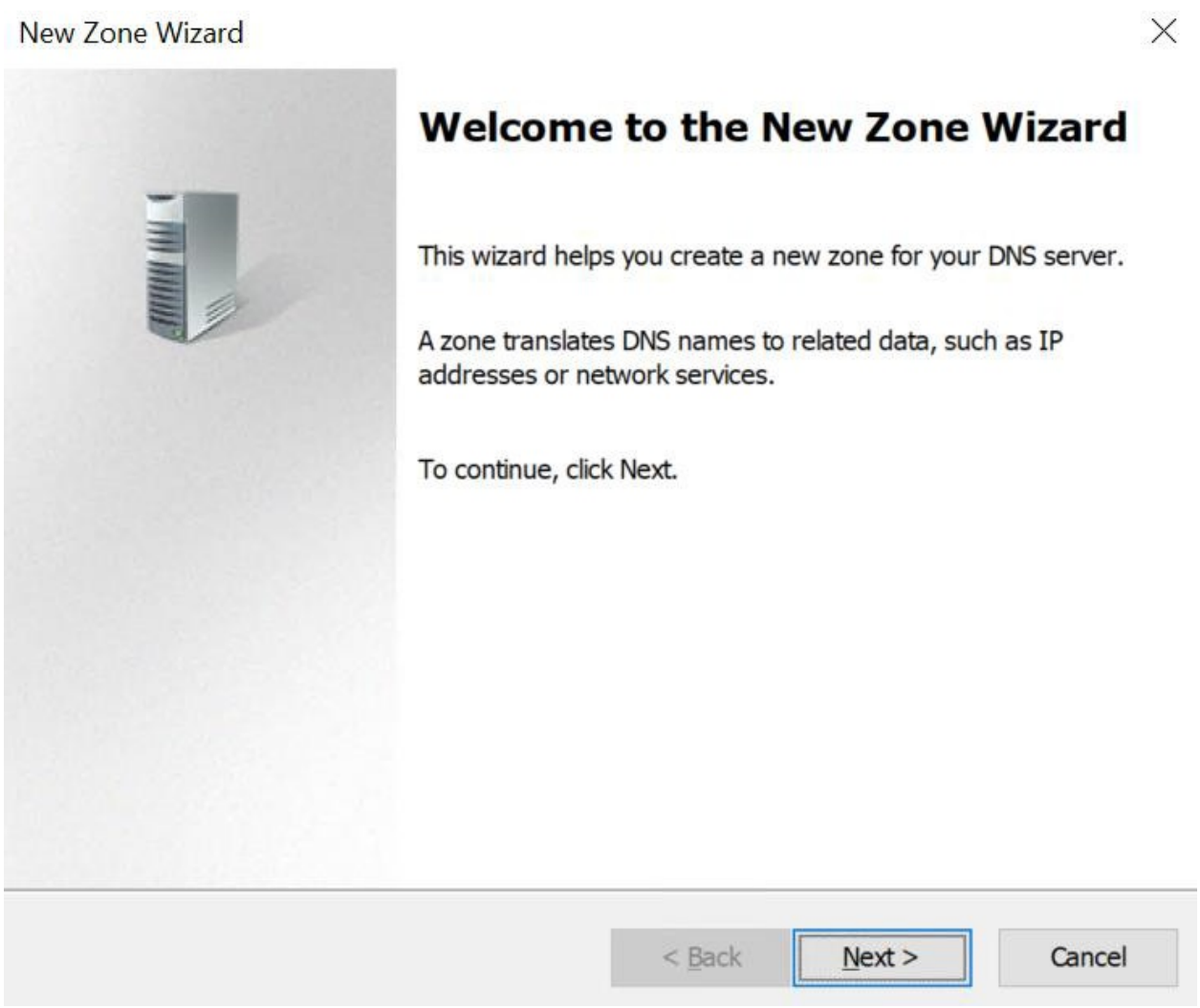

Figure 42 : New Zone Wizard

4. Select **Zone Type** and click **Next**.

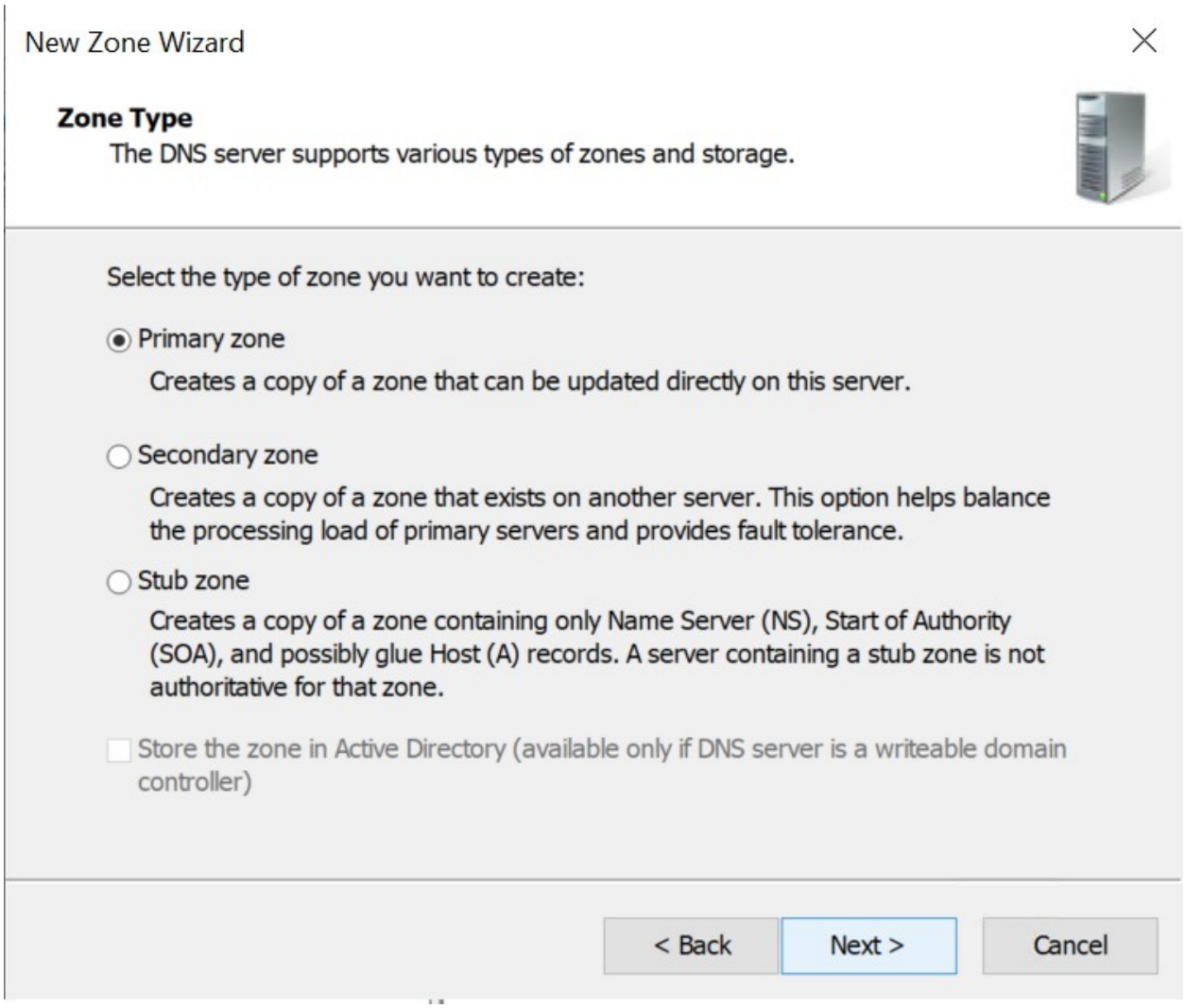

Figure 43 : Zone Type

If your system is joined to domain, then you will get the option to select the **Active Directory Zone Replication Scope**.

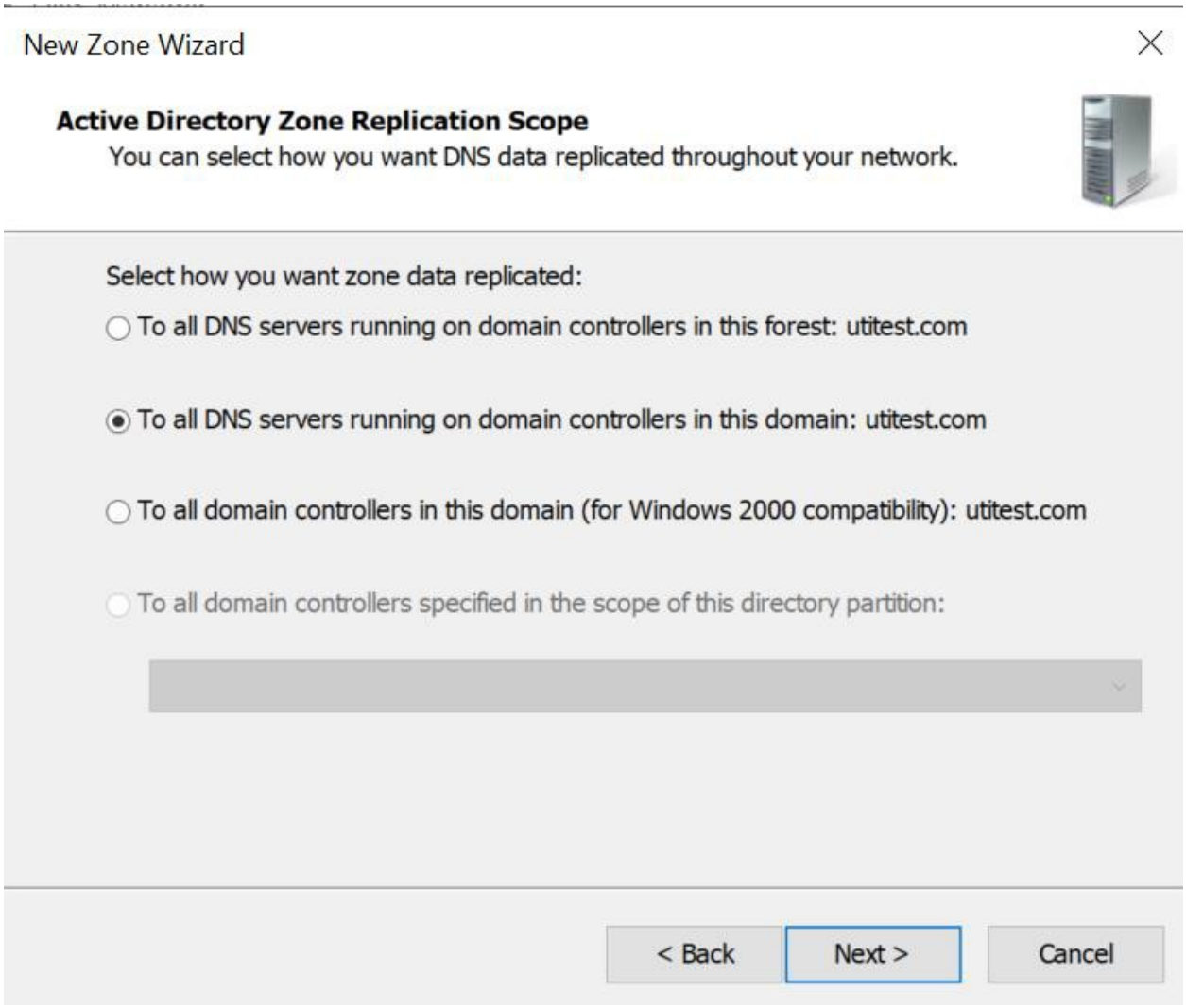

Figure 44 : Active Directory Zone Replication Scope

5. Select the **Reverse Lookup Zone Name** and click **Next**.
6. Select the **IPv4** or **IPv6 Reverse Lookup Zone**.

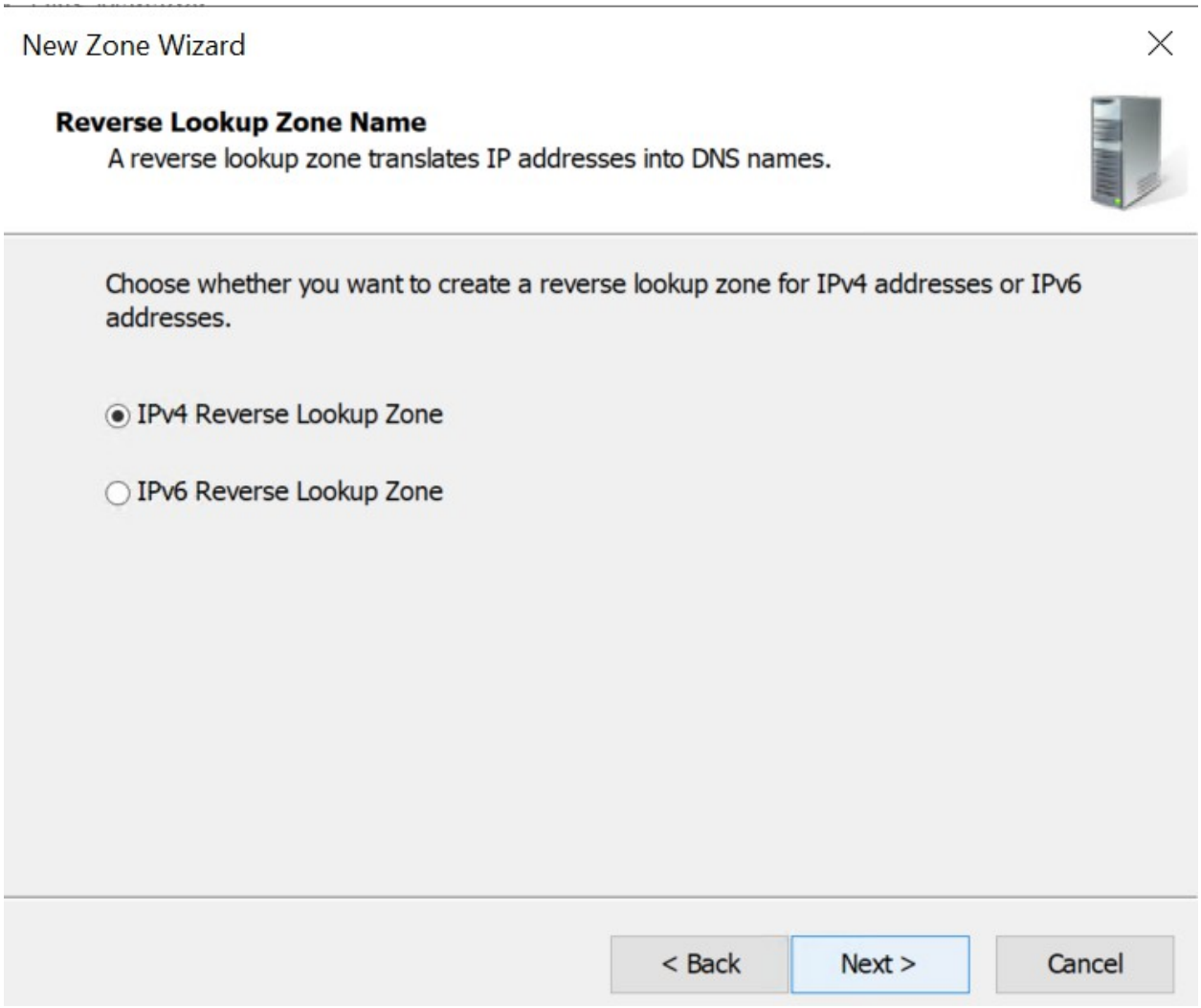

Figure 45 : Reverse Lookup Zone Name

7. Provide **Network ID** and click **Next**.

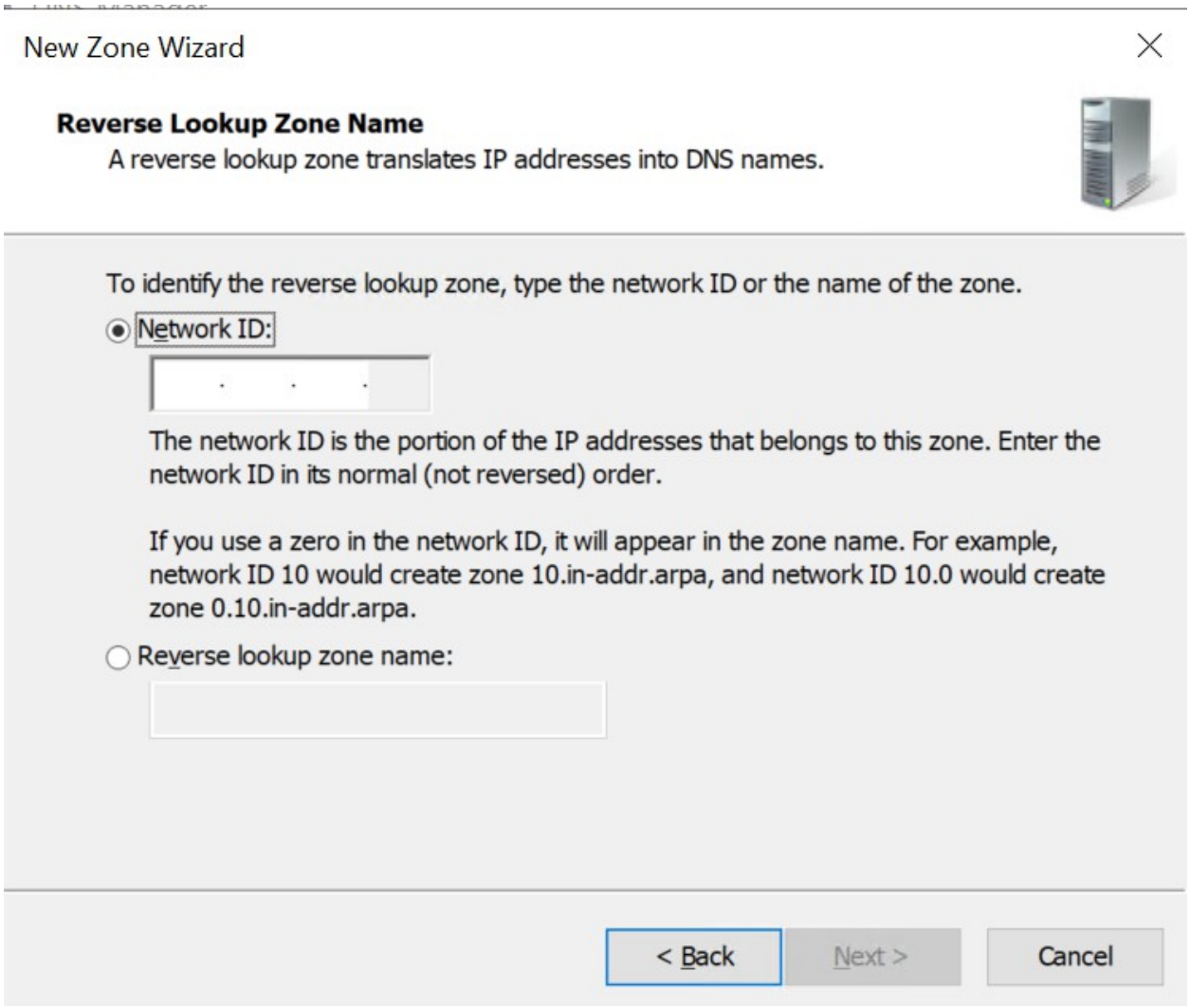

Figure 46 : Reverse Lookup Zone Name

8. Select the option to create a new file with this file name and click **Next**.

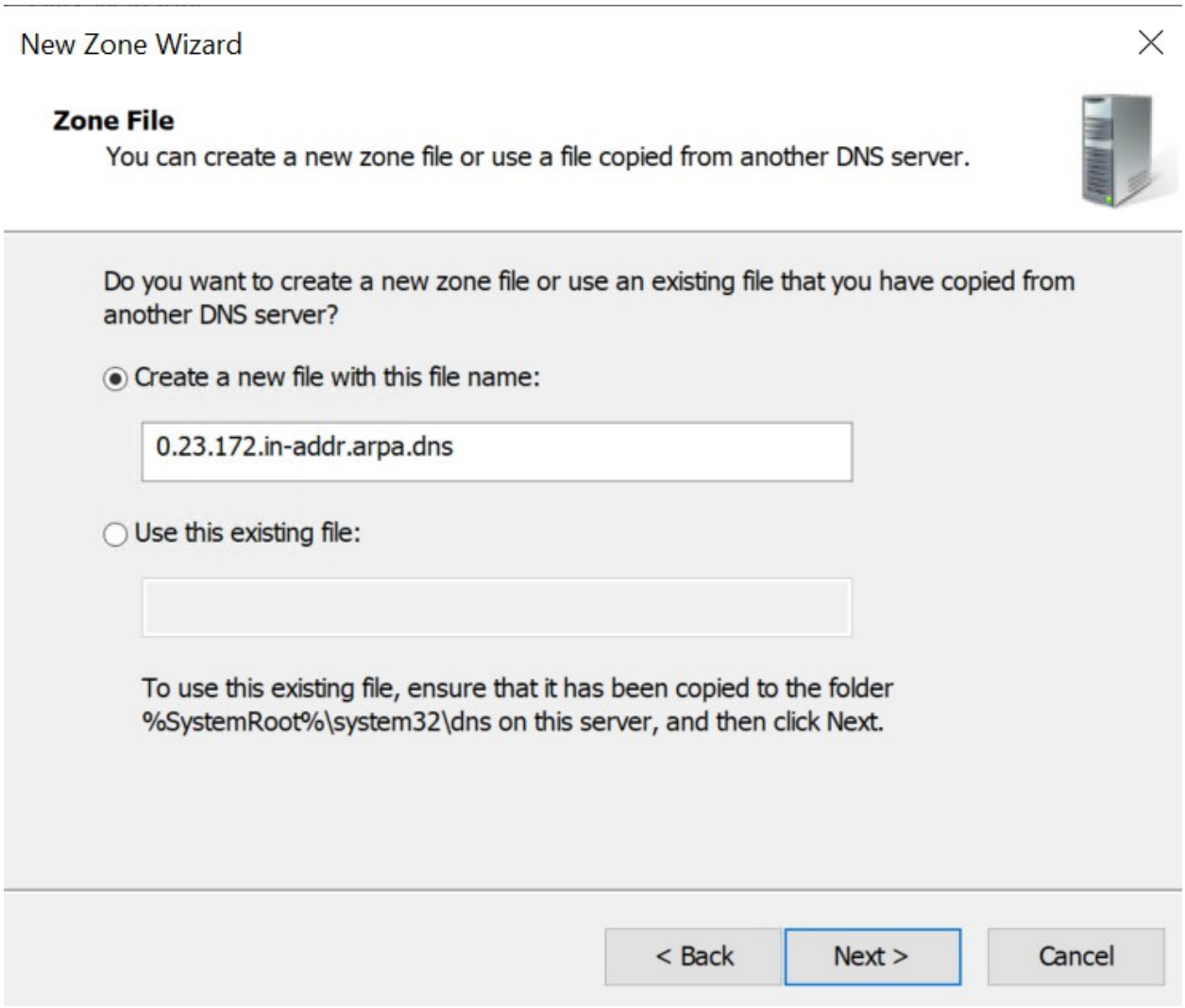

Figure 47 : Zone File

9. Select a **Dynamic Update** type and click **Next**.

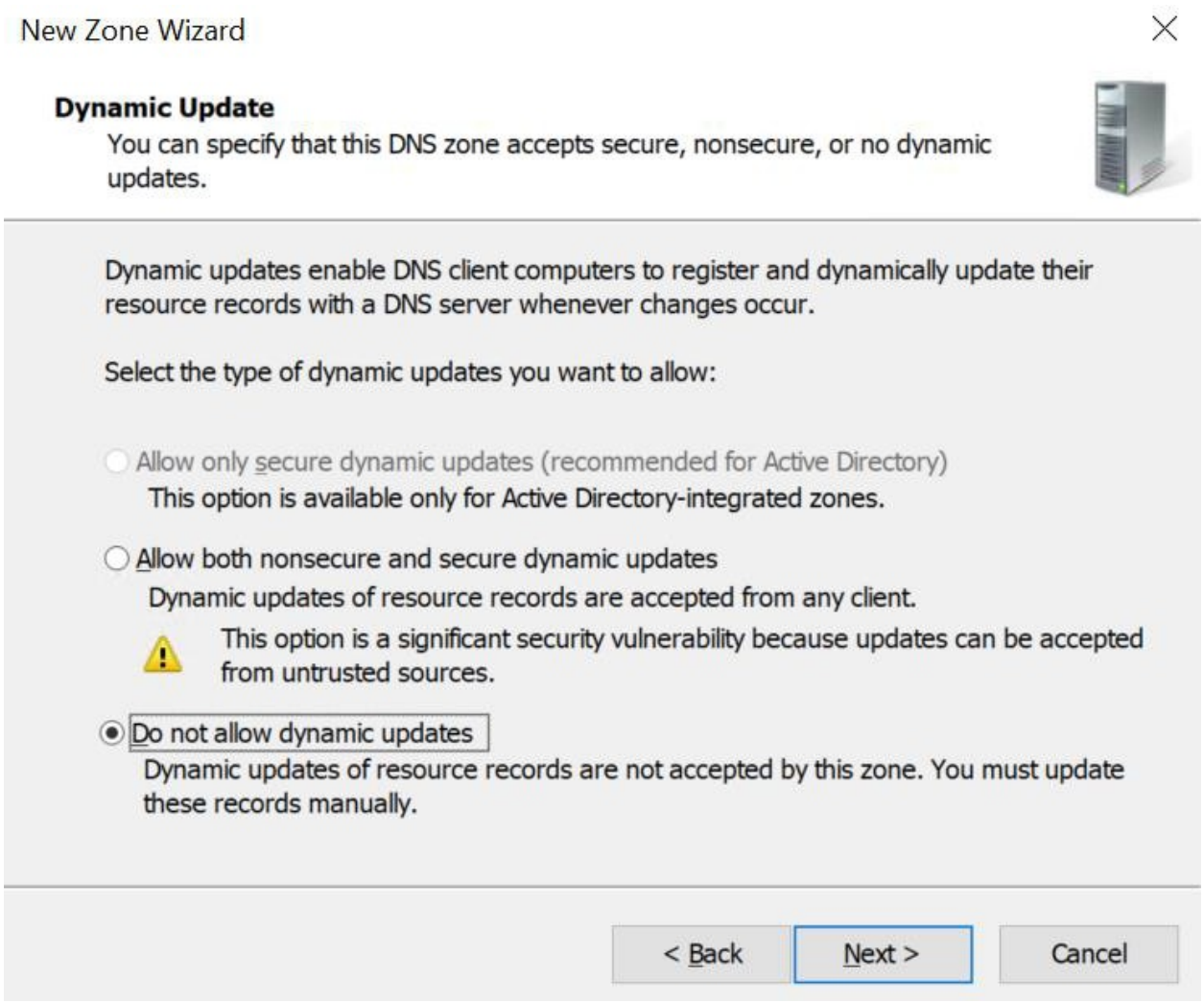

Figure 48 : Dynamic Update

If your system is in domain, all the options will be available.

10. Check the information and click **Finish**.

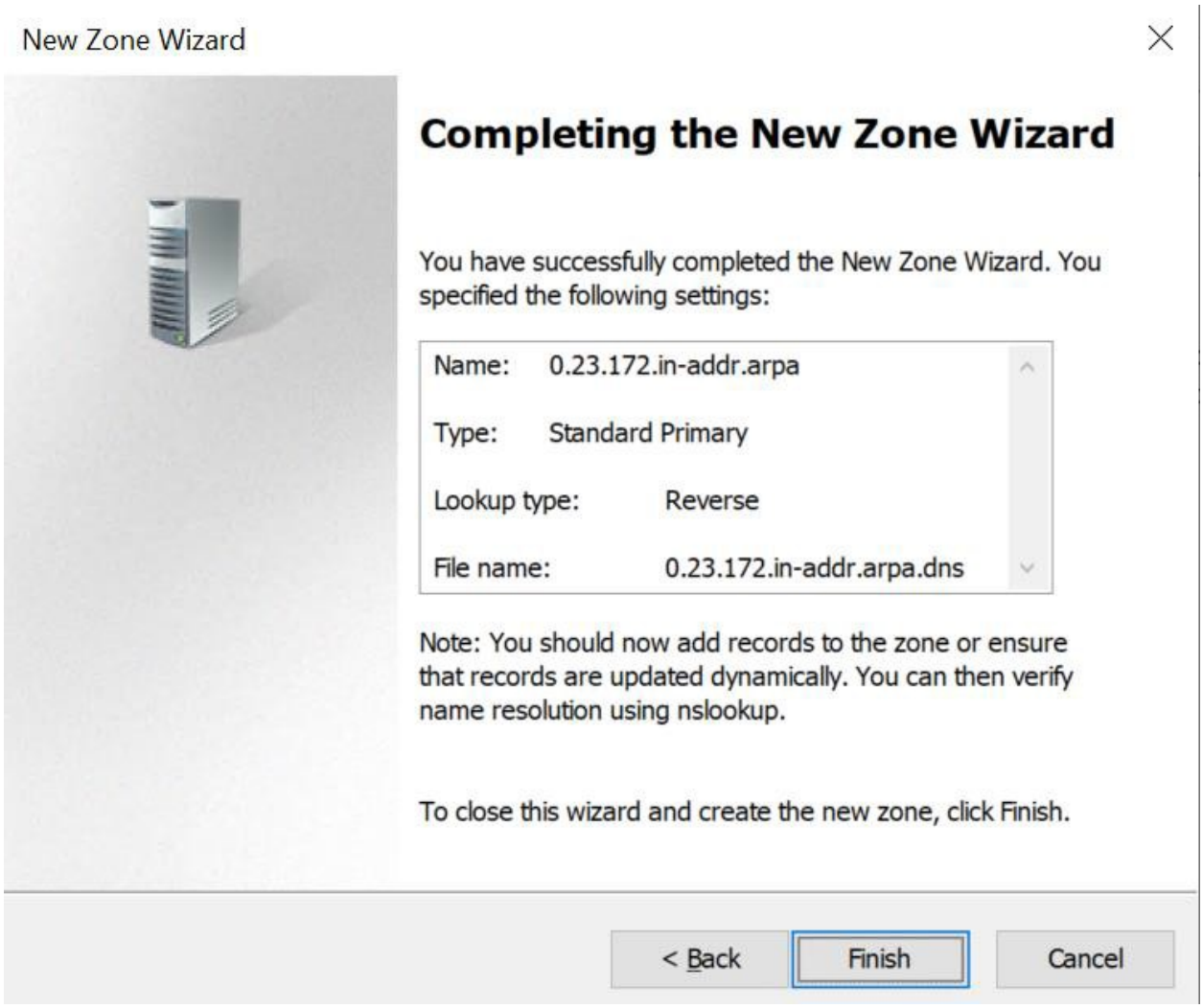

Figure 49 : Complete New Zone Wizard

5.6 Sign Reverse Lookup Zone

1. Click on **Server Manager** by selecting **Start** > **Server Manager** > click **Tools** and open **DNS Manager**.

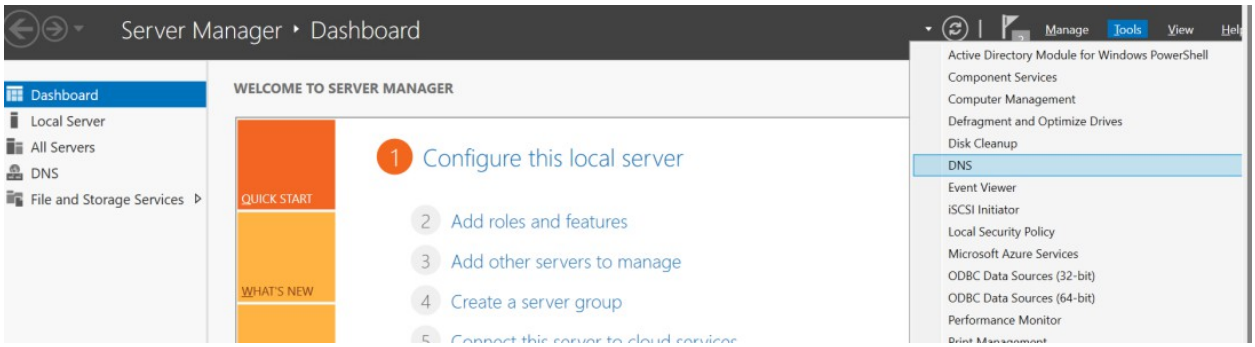

Figure 50 : Server Manager

2. In the **DNS Manager**, browse to your **Domain** name, then right click on **Reverse Lookup Zone**.
3. Click **DNSSEC** and then click **Sign the Zone**.

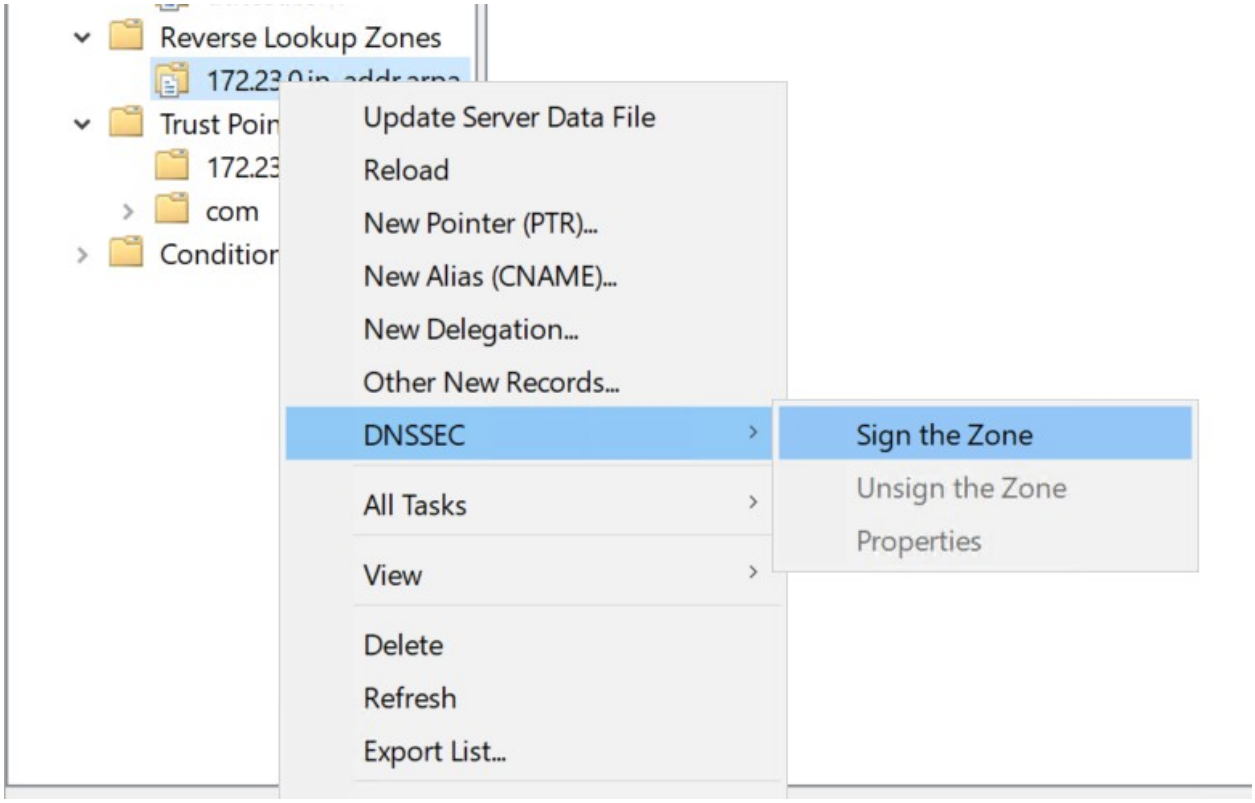

Figure 51 : Sign the Zone

4. In the **Zone Signing Wizard**, click **Next**.

Figure 52 : Zone Signing Wizard

5. On the **Signing Options** interface, click **Customize zone signing parameters**, and then click **Next**.

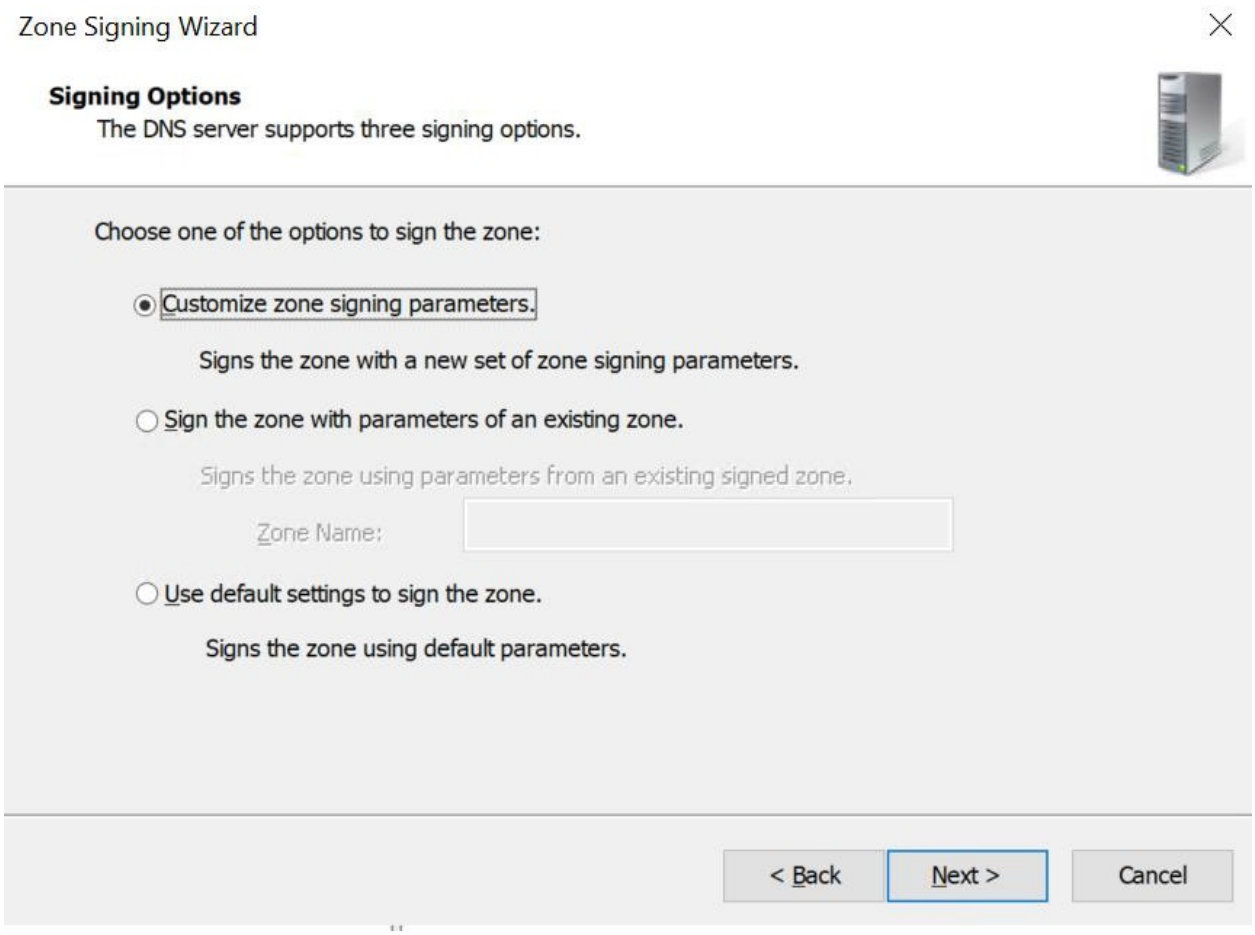

Figure 53 : Zone Signing Parameters

6. On the **Key Signing Key (KSK)** Wizard, click **Next**.

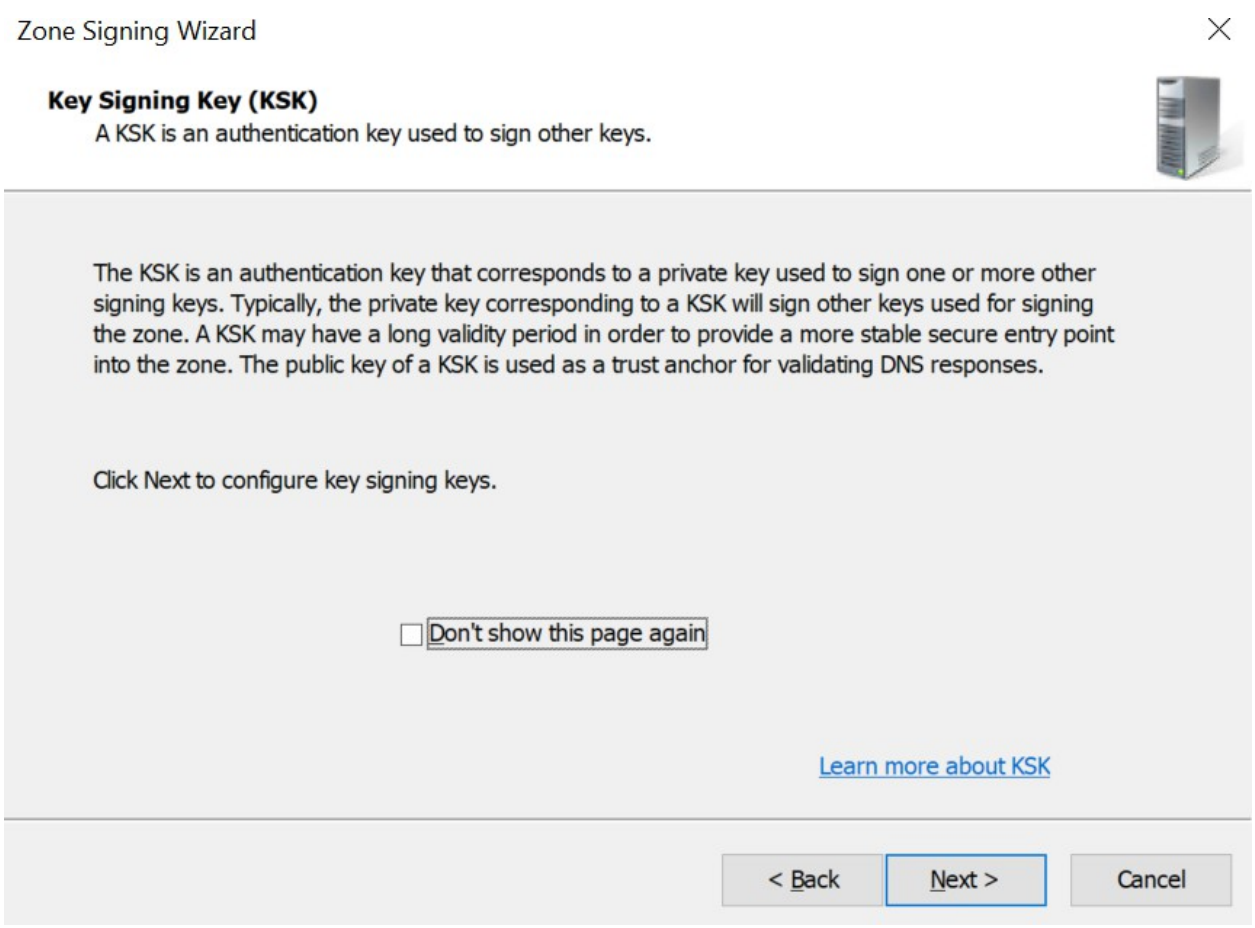

Figure 54 : Key Signing Key (KSK) Wizard

7. On the **Key Signing Key (KSK)** Wizard, click **Add**.

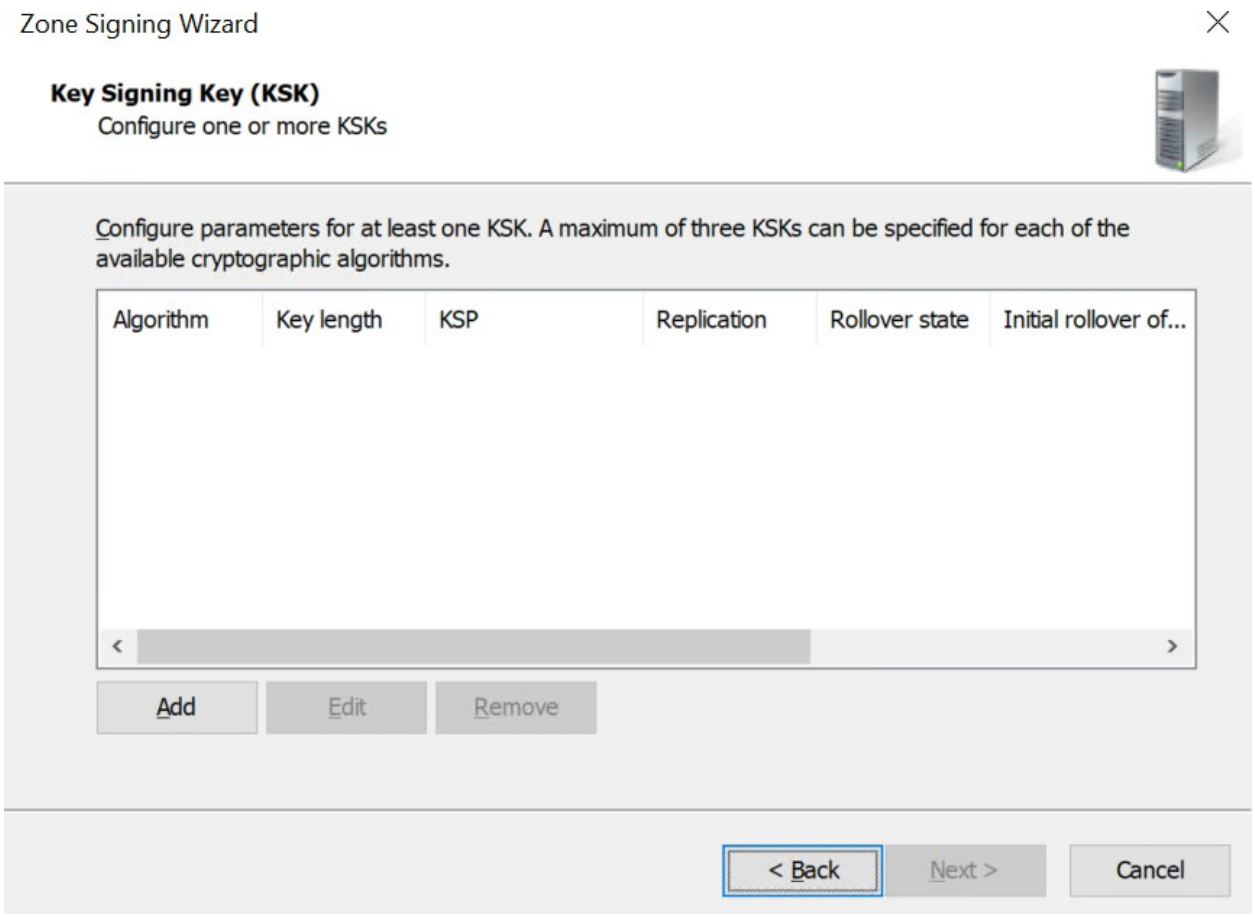

Figure 55 : Key Signing Key (KSK) Wizard

8. On the **New Key Signing Key (KSK)** Wizard, from the dropdown of **Select a key storage provider to generate and store keys**, select **Utimaco CryptoServer Key Storage Provider**.
9. Provide other information such as **Cryptographic Algorithm** and **Key Length** and then click **OK**.
10. Uncheck the **rollover** option.

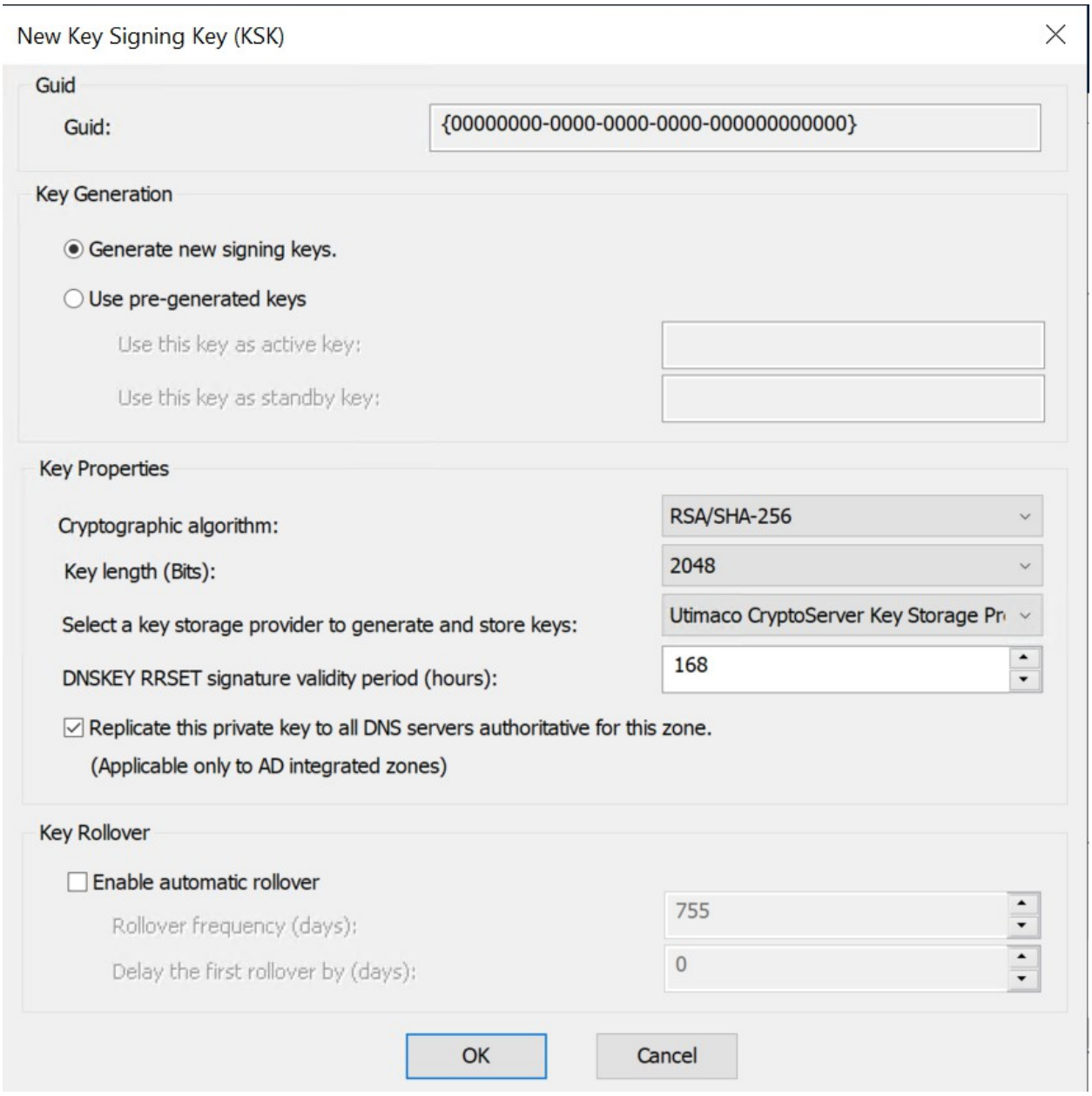

Figure 56 : New Key Signing Key (KSK) Wizard

Automatic Key Rollover is not supported with Utimaco HSM. The user has to manually rollover the keys before its expiry.

11. On the **Key Signing Key (KSK)** Wizard, click **Next**.

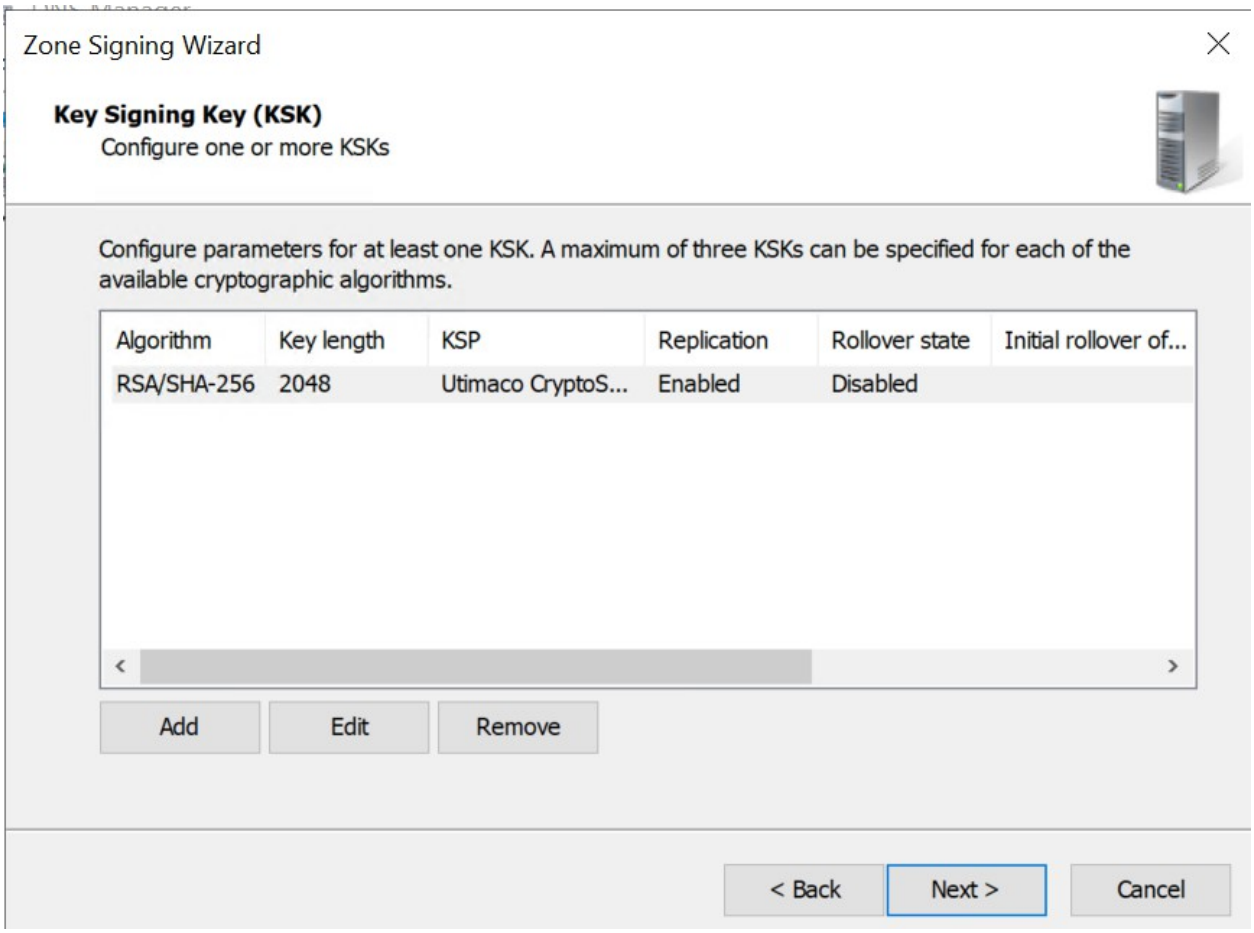

Figure 57 : Key Signing Key (KSK) Wizard

12. On the **Zone Signing Key (ZSK)** Wizard, click **Next**.

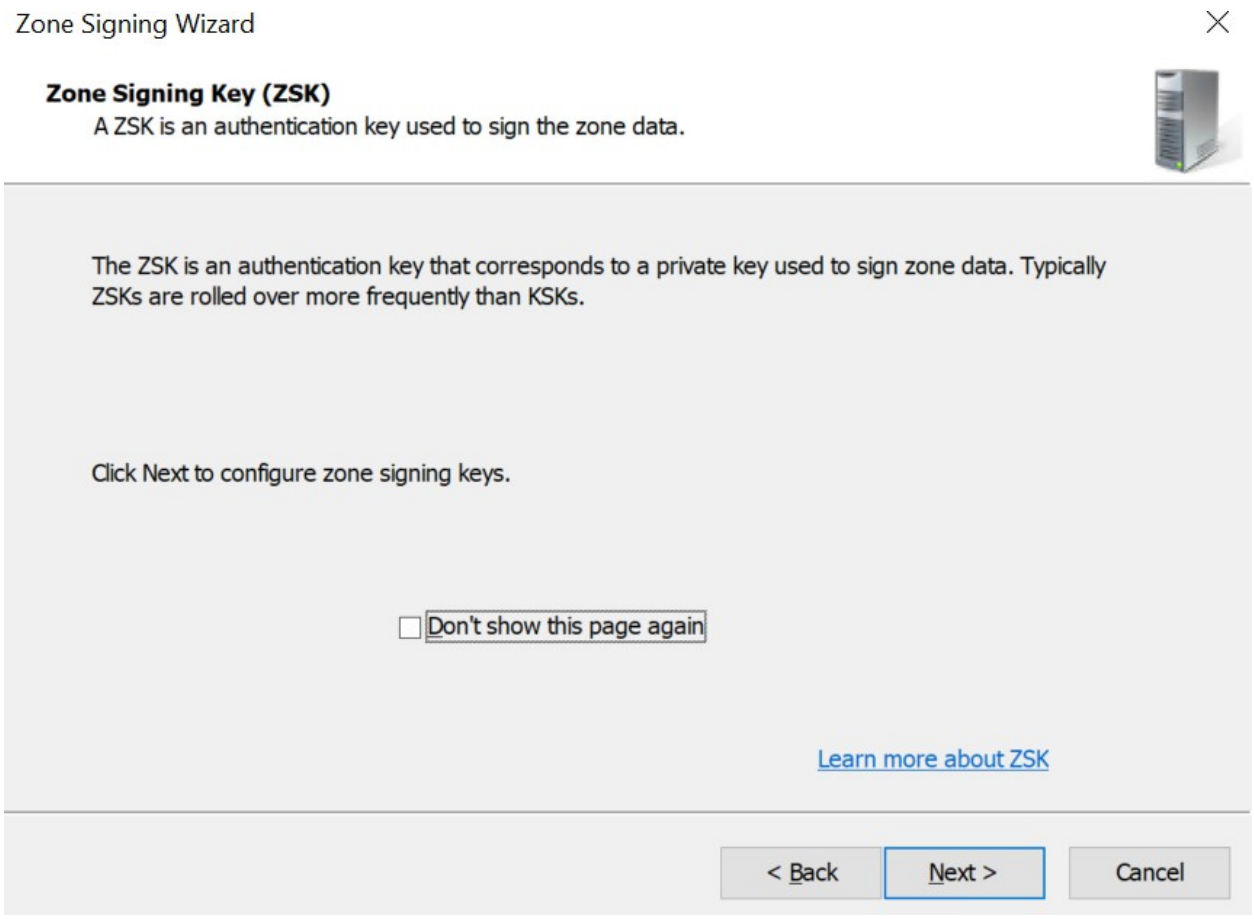

Figure 58 : Zone Signing Key Wizard

13. On the **Zone Signing Key (ZSK)** wizard, click **Add**.
14. On the **New Zone Signing Key (ZSK)** Wizard, from the dropdown of **Select a key storage provider to generate and store keys**, select **Utimaco CryptoServer Key Storage Provider**.
15. Provide other information such as **Cryptographic Algorithm** and **Key Length** and then click **OK**.
16. Uncheck the rollover option.

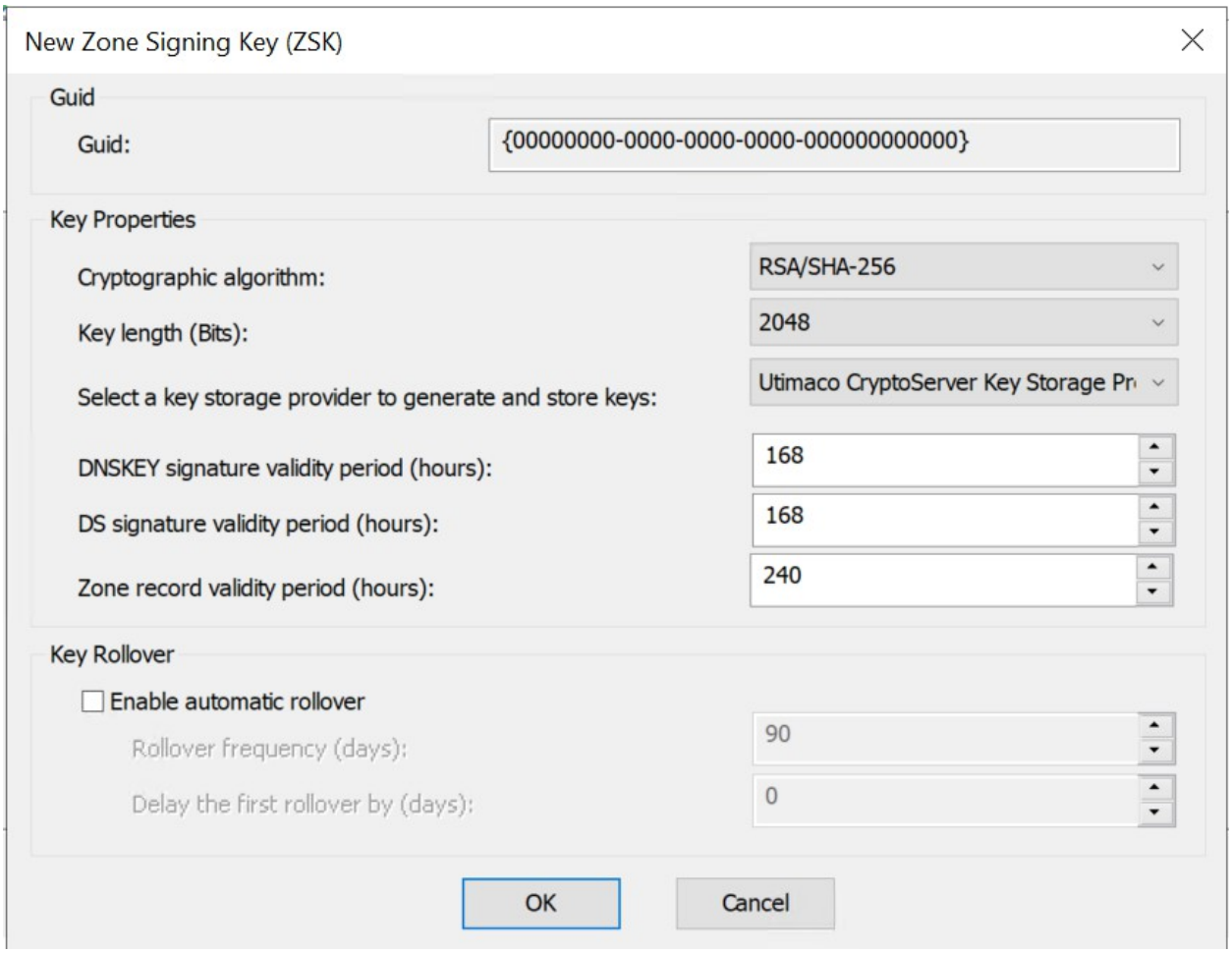

Figure 59 : Zone Signing Key (ZSK) Wizard

Automatic **Key Rollover** is not supported with Utimaco HSM. The user has to manually rollover the keys before its expiry.

17. On the **Zone Signing Key (ZSK)** Wizard, click **Next**.

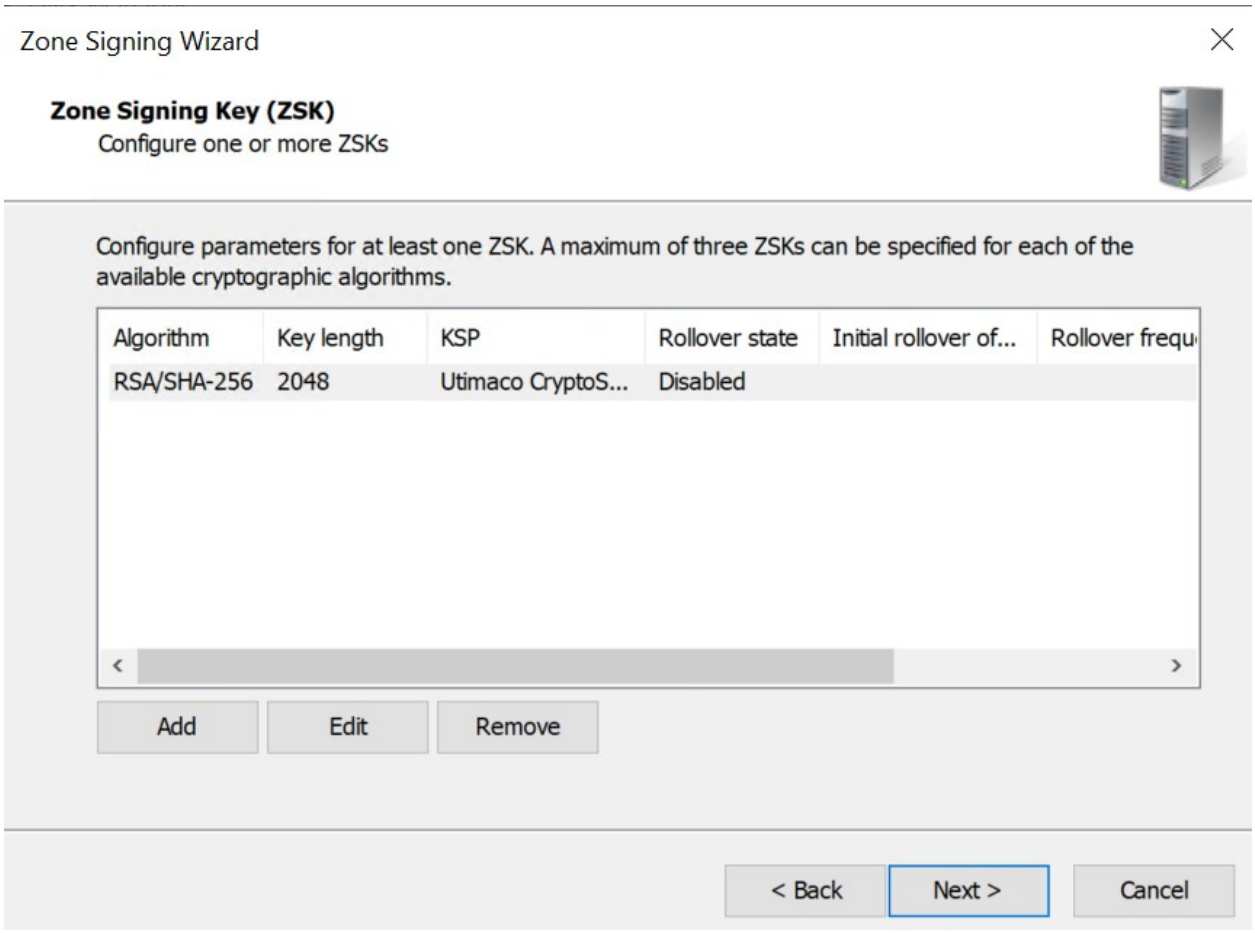

Figure 60 : Zone Signing Key (ZSK) Wizard

18. On the **Next Secure (NSEC)** Wizard select use **NSEC3**, click **Next**.

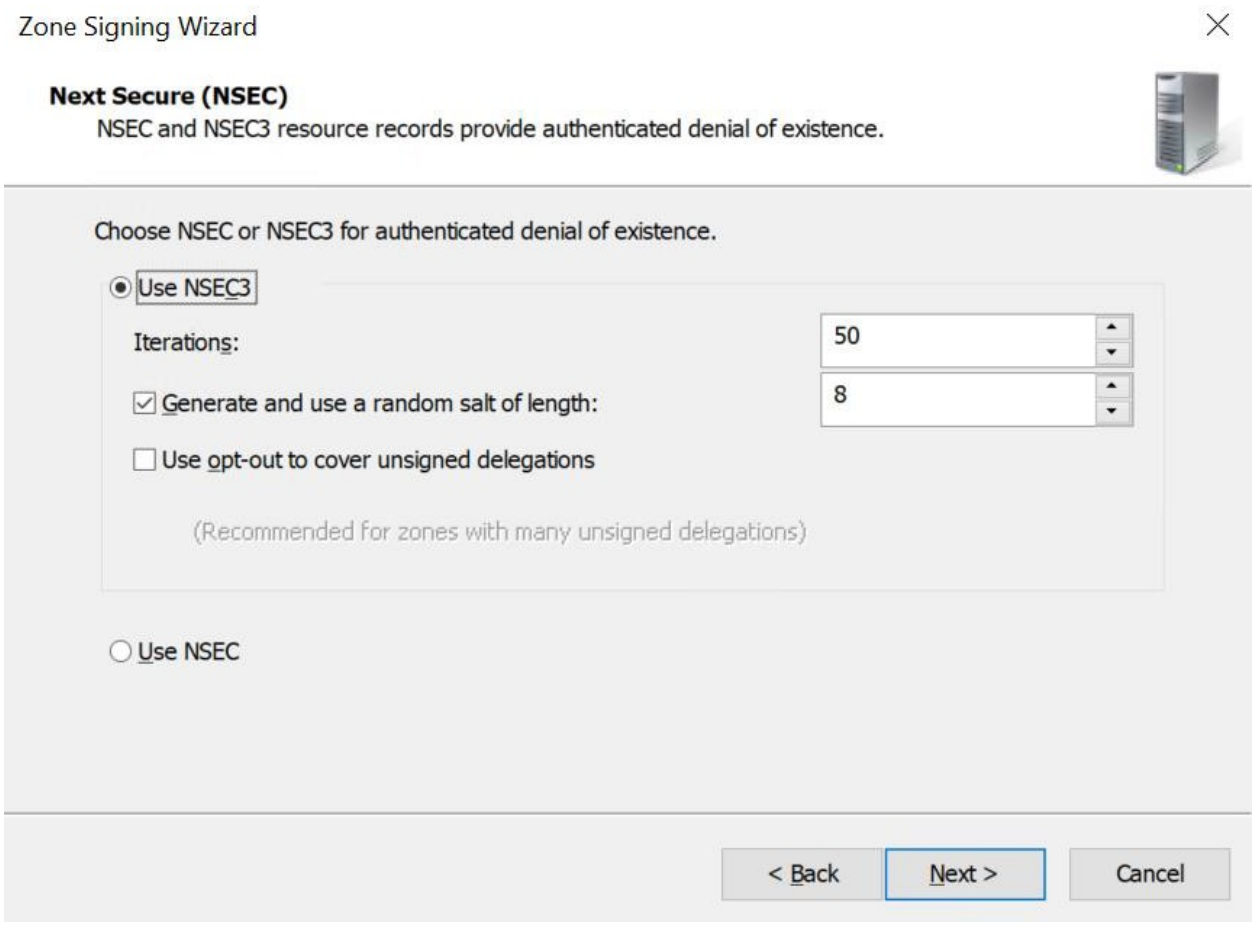

Figure 61 : Next Secure (NSEC) Wizard

19. On the **Trust Anchors (TAs)** Wizard, check the E**nable the distribution of trust anchors for this zone** check box, and then click **Next**.

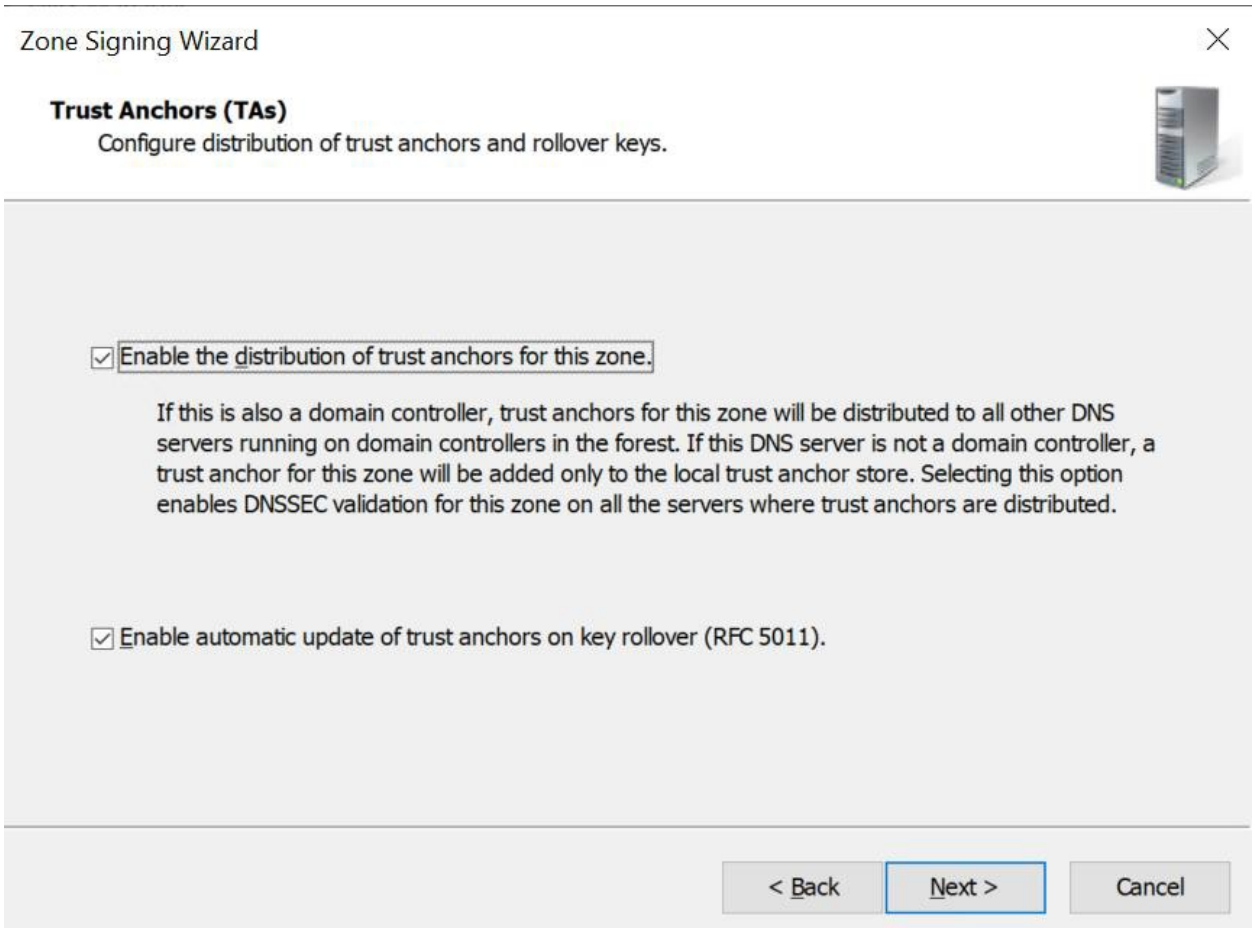

Figure 62 : Trust Anchors (TAs) Wizard

20. On the **Signing and Polling Parameters** wizard, click **Next**.

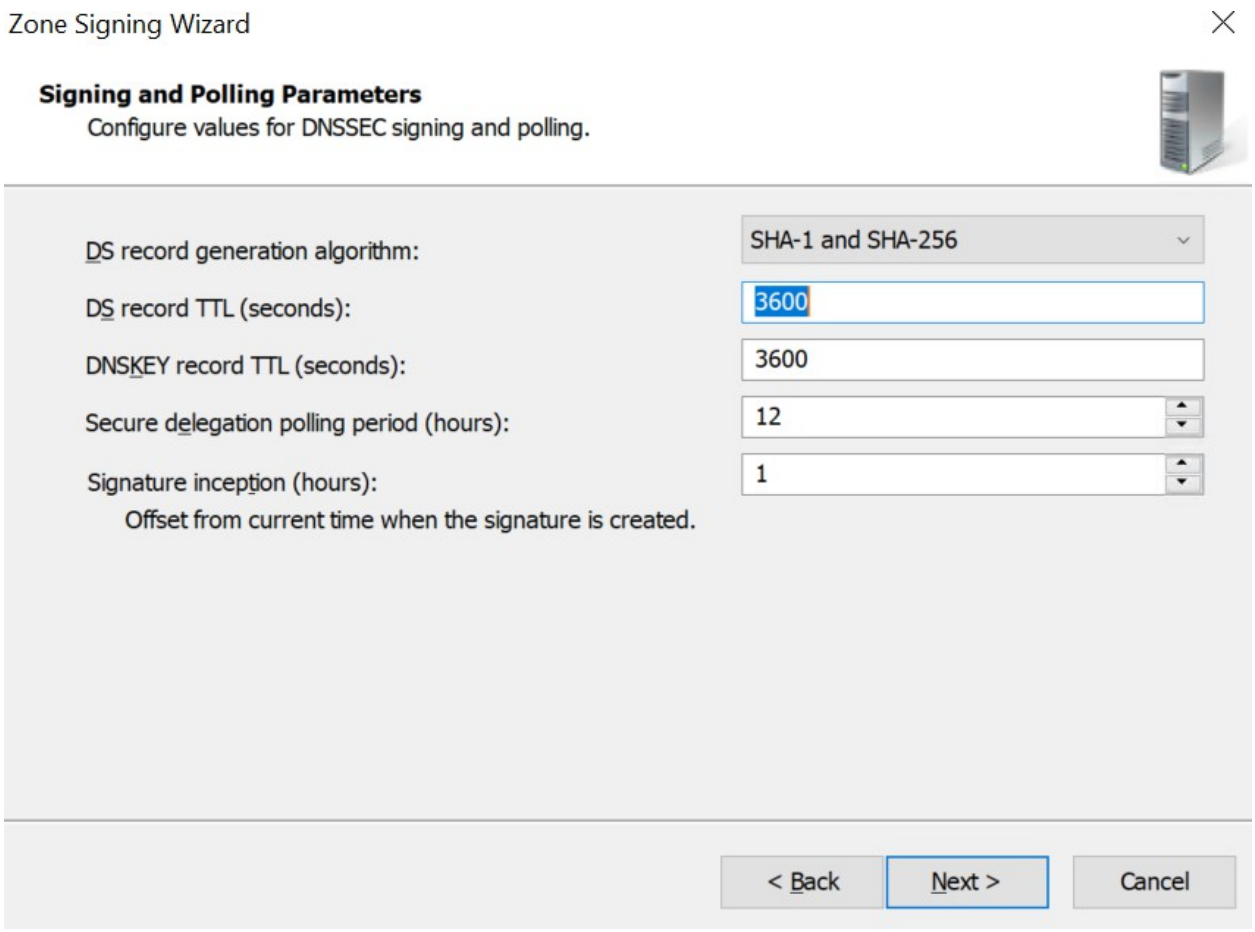

Figure 63 : Signing and Polling Parameters Wizard

21. On the **DNS Security Extensions (DNSSEC)** Wizard, click **Next**, and then click **Finish**.

Figure 64 : DNS Security Extensions (DNSSEC) Wizard

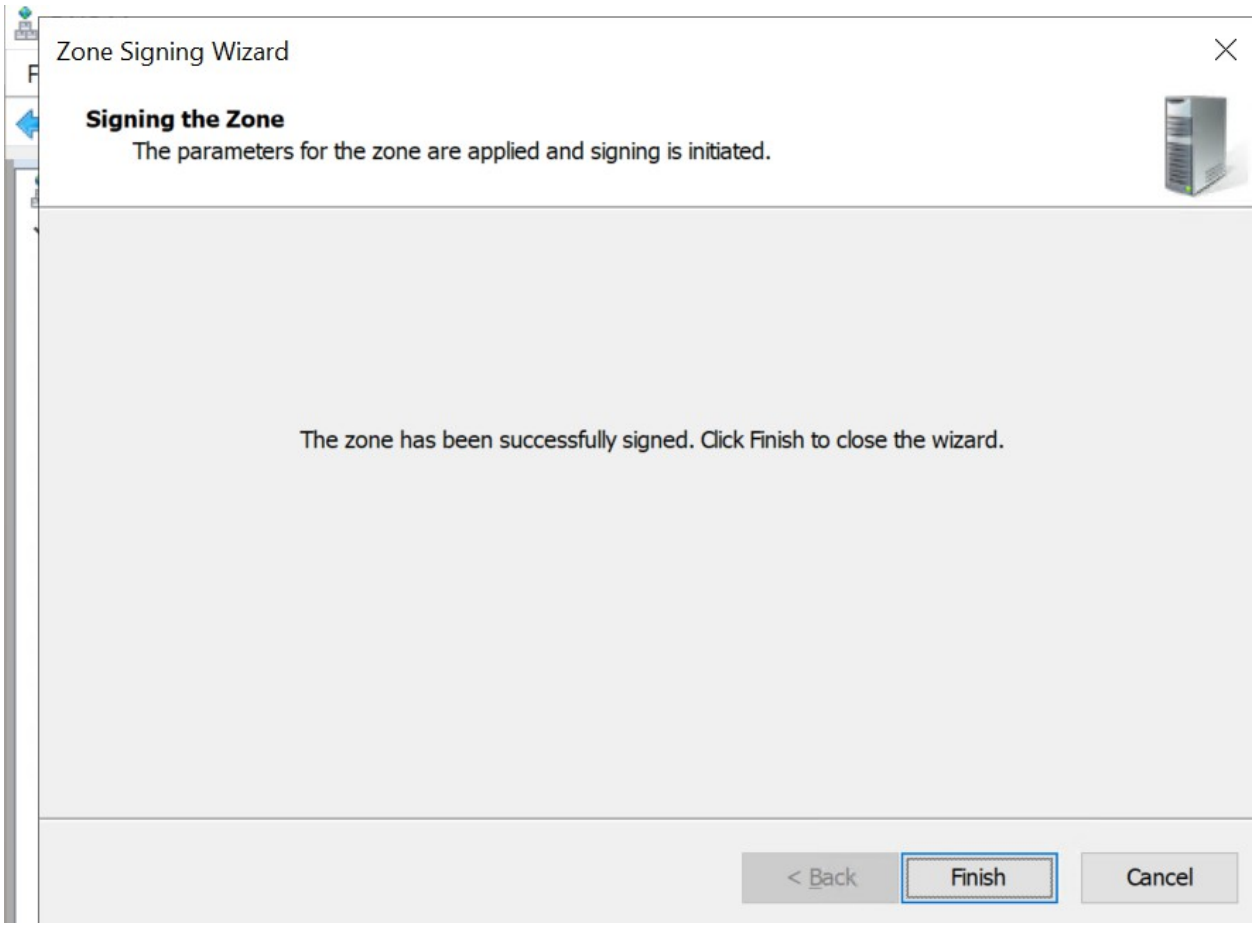

Figure 65 : Signing the Zone

5.7 Create Record in Reverse Lookup Zone

1. Open DNS using **Tools** on **Server Manager**.
2. In the right-side pane, right-click on the reverse zone that you have created and click on **New Pointer (PTR)...** record.

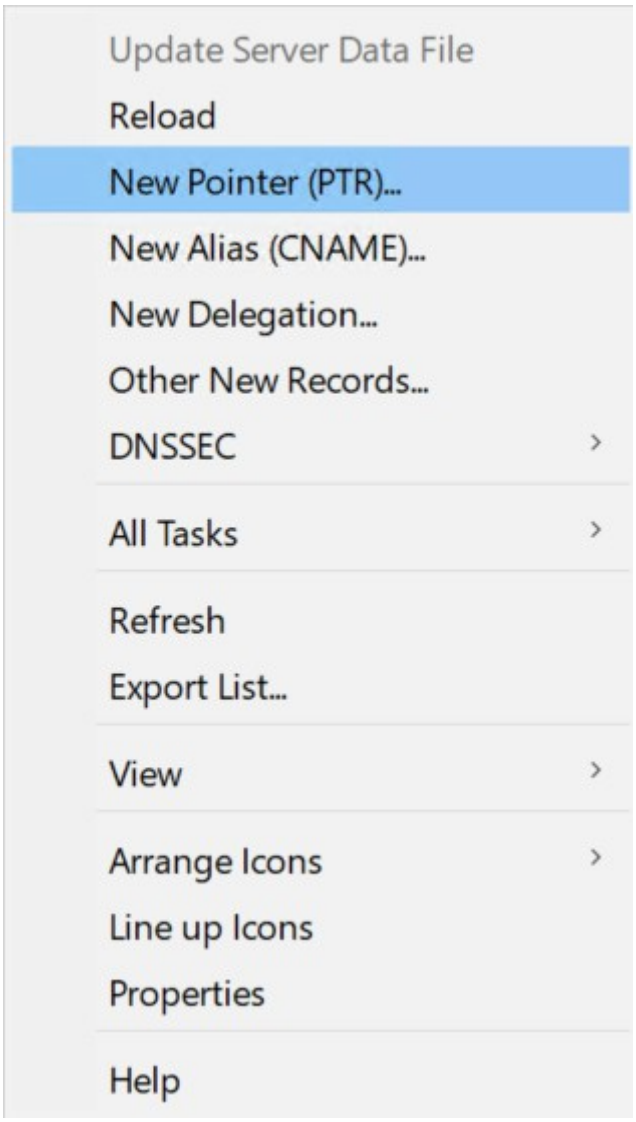

Figure 66 : New Pointer (PTR) Record

3. On **New Resource Record** add the **IP Address** and **Host name**.
4. Click on **OK**.

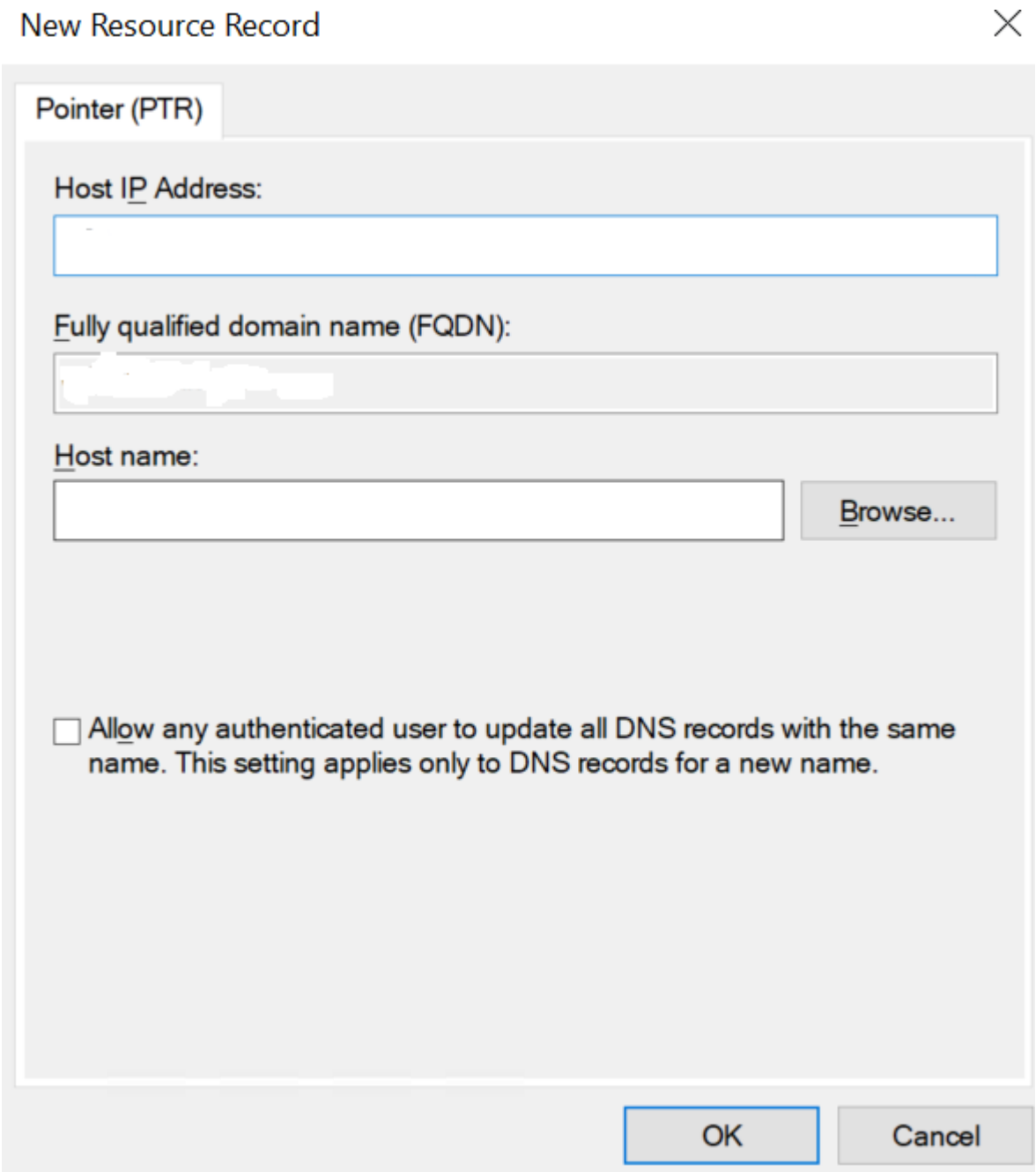

Figure 67 : New Resource Record

5. Click on **Add Host**.

6 Troubleshooting

Error	Diagnosis
cngtool ListKeys E: NCryptOpenStorageProvider [Utimaco CryptoServer Key Storage Provider] returned: Error 0x80090011 Object was not found. ListKeys returned: Error 0x80090011 Object was not found.	Ensure that the Utimaco CNG/CSP providers are correctly installed and set.
Not able to create or delete the DNS record from Forward or Reverse Lookup zone	Check the HSM is working

Table 6: List of errors and their diagnoses

7 Further Information

This document forms a part of the information and support which is provided by the Utimaco IS GmbH. Additional documentation can be found on the product CD in the `Documentation` directory.

All u.trust GP HSM product documentation is also available at the Utimaco IS GmbH website: https://utimaco.com/ .

8 References

Reference	Title/Company	Document No.
[CSADMIN]	CryptoServer – csadm Manual/Utimaco IS GmbH	2009-0003
[CSADMIN2]	CryptoServer_csadm_Manual_Systemadministrators.pdf	2009-0003
[CSLAN]	CryptoServerLAN_V5_Manual_Systemadministrators.pdf	2018-0010
[CSP-CNG]	CryptoServer_Manual_CSP_CNG.pdf	2008-0002

Table 7: References

9 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.