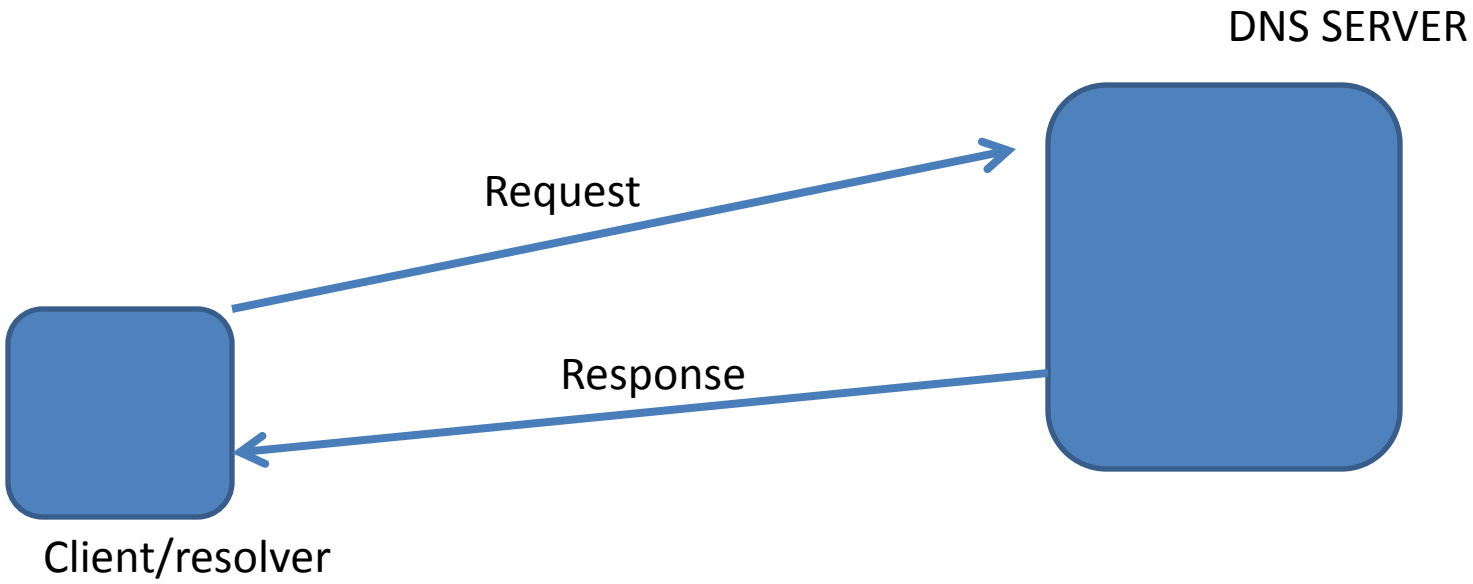
DNSSEC

DNSSEC provides security for DNS traffic



- Origin authentication of DNS data
- Data integrity
- Authenticated denial of existence

All of the above give protection against DNS attacks eg DNS spoofing

- DNSSEC was designed to protect applications (and caching resolvers serving those applications) from using forged or manipulated DNS data, such as that created by DNS cache poisoning.

- All answers from DNSSEC protected zones are digitally signed.

- By checking the digital signature, a DNS resolver is able to check if the information is identical (i.e. unmodified and complete) to the information published by the zone owner and served on an authoritative DNS server.

A recursive or forwarding DNS server knows that the zone supports DNSSEC if it has a DNSKEY (also called a trust anchor) for that zone.

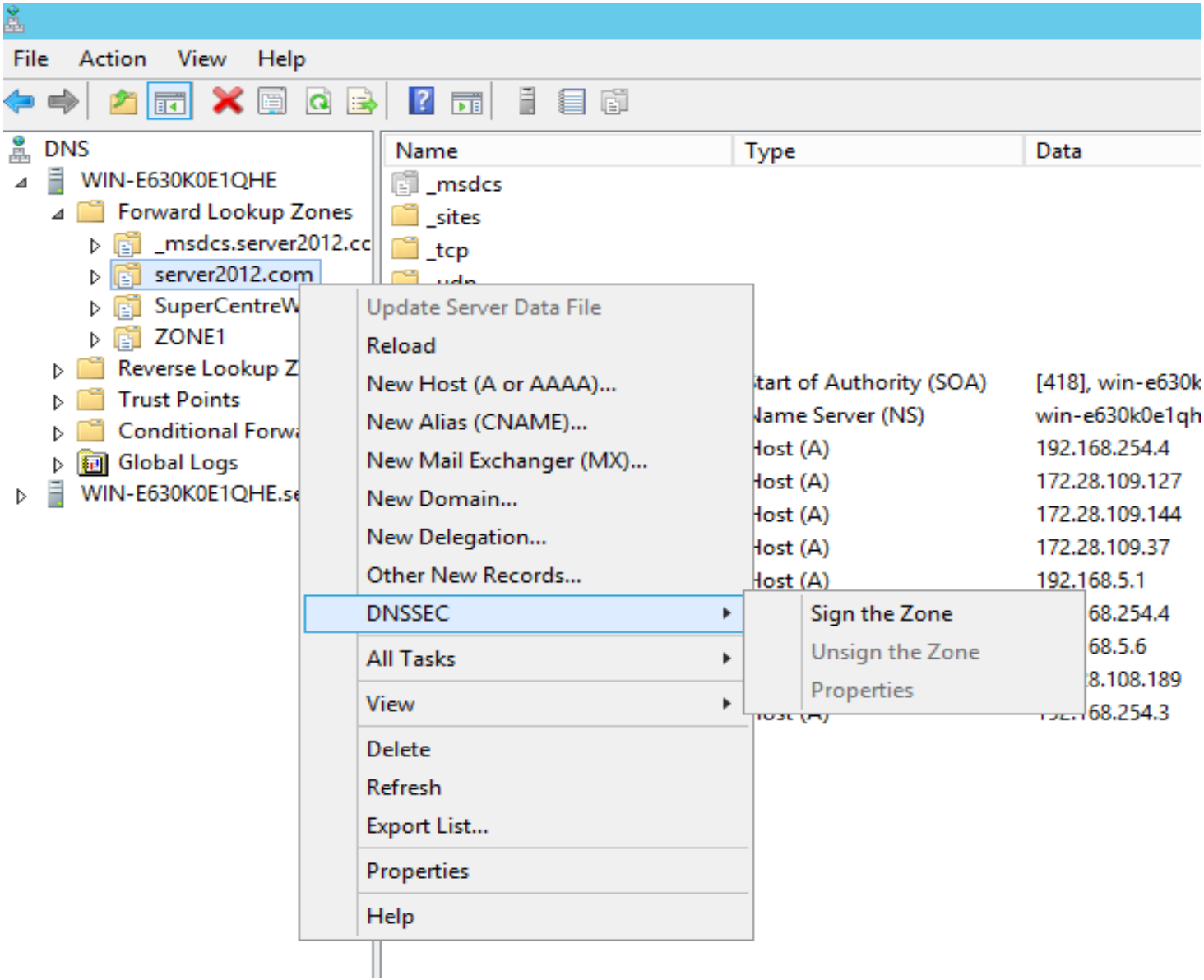
DNSSEC validation

A recursive DNS server uses the DNSKEY resource record to validate responses from the authoritative DNS server by decrypting digital signatures contained in DNSSEC-related resource records and then computing and comparing hash values. If hash values are the same, it provides a reply to the DNS client with the DNS data it requested (such as an A record).

If hash values are not the same, it replies with a SERVFAIL message

Additionally, if the DNS client is DNSSEC-aware, the recursive DNS server will indicate that DNSSEC validation was performed, which can be required by the client

SIGNING THE ZONE LAB- RIGHT CLICK ON THE ZONE IN DNS MANAGER, SELECT DNSSEC. SELECT SIGN THE ZONE



Zone Signing Wizard

DNS Security Extensions (DNSSEC)

Domain Name System Security Extensions (DNSSEC) is a suite of extensions that add security to the DNS protocol. Specifically, DNSSEC provides origin authority, data integrity, and authenticated denial of existence. DNSSEC provides the ability for DNS servers and resolvers to trust DNS responses by using digital signatures for validation.

To continue, click Next and this wizard will guide you through the zone signing process.

☐ Don't show this page again

Learn more about DNSSEC

< Back | Next > | Cancel

Zone Signing Wizard

Signing Options

The DNS server supports three signing options.

Choose one of the options to sign the zone:

- (•) Customize zone signing parameters.

  Signs the zone with a new set of zone signing parameters.

- ( ) Sign the zone with parameters of an existing zone.

  Signs the zone using parameters from an existing signed zone.

  Zone Name:

- ( ) Use default settings to sign the zone.

  Signs the zone using default parameters.

< Back | Next > | Cancel

Zone Signing Wizard

Key Master

Choose the Key Master for this zone.

The Key Master is a DNS server that generates and manages cryptographic keys for a DNSSEC protected zone. Any authoritative DNS server that hosts a primary copy of the zone can be the Key Master.

By default, the current DNS server is chosen to be the Key Master. You can also choose another DNS server as the Key Master for this zone.

- (•) The DNS server WIN-E630K0E1QHE is the Key Master.
- ( ) Select another primary server as the Key Master:

< Back | Next > | Cancel

Zone Signing Wizard

Key Signing Key (KSK)

A KSK is an authentication key used to sign other keys.

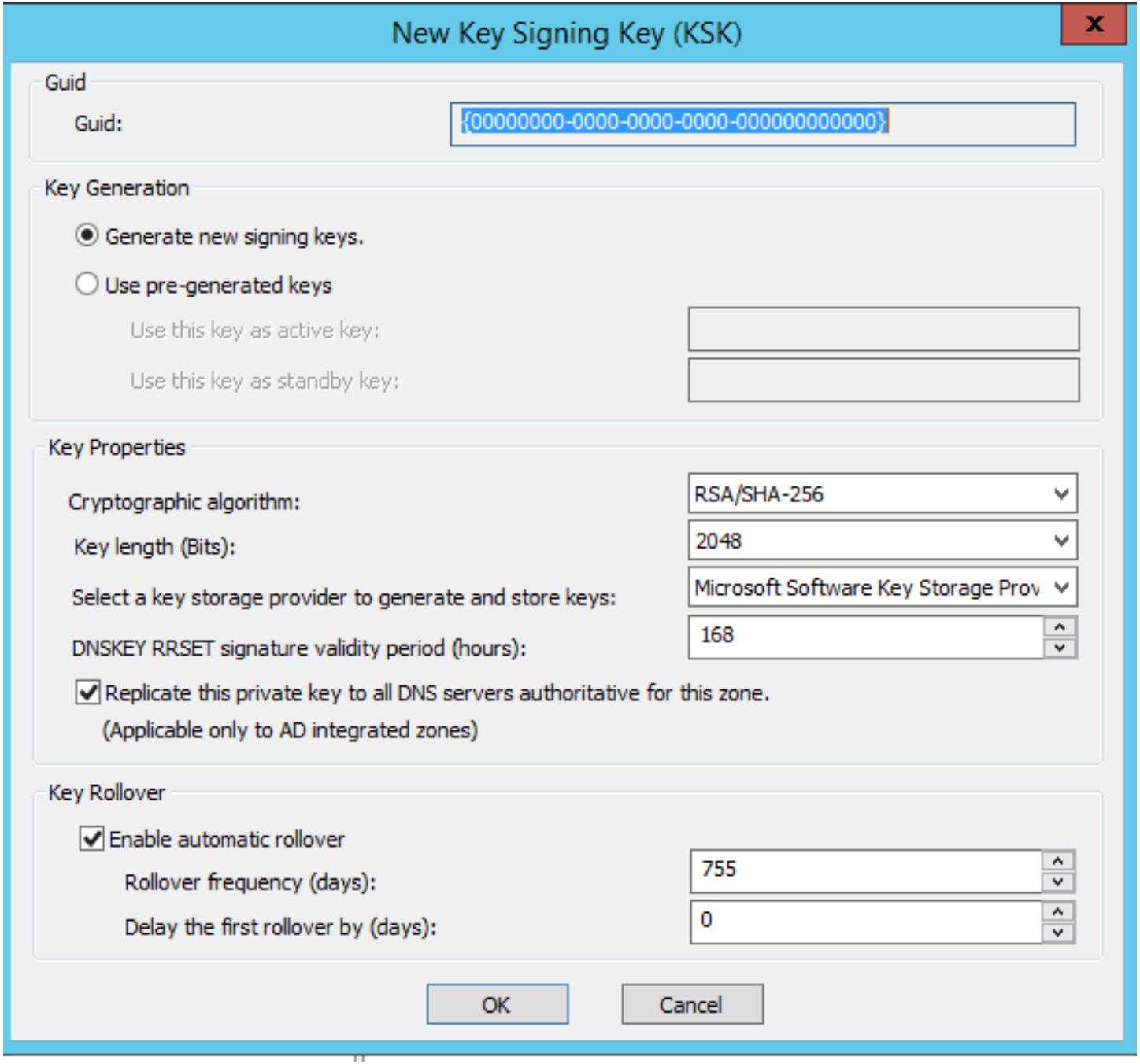
The KSK is an authentication key that corresponds to a private key used to sign one or more other signing keys. Typically, the private key corresponding to a KSK will sign other keys used for signing the zone. A KSK may have a long validity period in order to provide a more stable secure entry point into the zone. The public key of a KSK is used as a trust anchor for validating DNS responses.

Click Next to configure key signing keys.

☐ Don't show this page again

Learn more about KSK

< Back | Next > | Cancel


New Key Signing Key (KSK)
Guid
Guid:
{00000000-0000-0000-0000-000000000000}
Key Generation
Generate new signing keys.
Use pre-generated keys
Use this key as active key:
Use this key as standby key:
Key Properties
Cryptographic algorithm:
RSA/SHA-256
Key length (Bits):
2048
Select a key storage provider to generate and store keys:
Microsoft Software Key Storage Prov
DNSKEY RRSET signature validity period (hours):
168
Replicate this private key to all DNS servers authoritative for this zone.
(Applicable only to AD integrated zones)
Key Rollover
Enable automatic rollover
Rollover frequency (days):
755
Delay the first rollover by (days):
0
OK
Cancel

Zone Signing Wizard

Key Signing Key (KSK)

Configure one or more KSKs

Configure parameters for at least one KSK. A maximum of three KSKs can be specified for each of the available cryptographic algorithms.

Algorithm	Key length	KSP	Replication	Rollover state	Initial rollover o...
RSA/SHA-256	2048	Microsoft Softw...	Enabled	Enabled	0

Add | Edit | Remove

< Back | Next > | Cancel

Zone Signing Wizard

Zone Signing Key (ZSK)

A ZSK is an authentication key used to sign the zone data.

The ZSK is an authentication key that corresponds to a private key used to sign zone data. Typically ZSKs are rolled over more frequently than KSKs.

Click Next to configure zone signing keys.

☐ Don't show this page again

Learn more about ZSK

< Back | Next > | Cancel

Zone Signing Wizard

Zone Signing Key (ZSK)

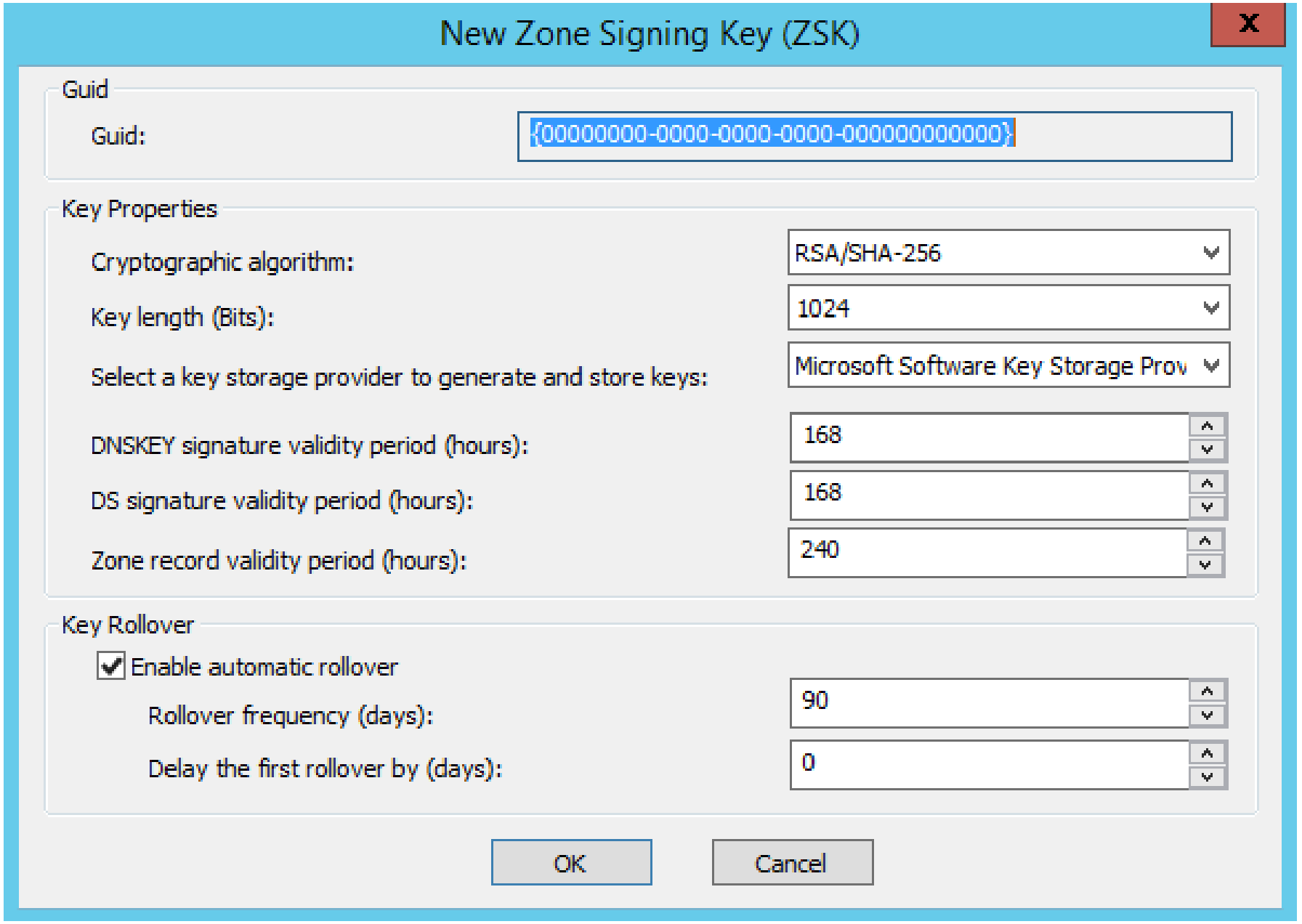
Configure one or more ZSKs

Configure parameters for at least one ZSK. A maximum of three ZSKs can be specified for each of the available cryptographic algorithms.

Algorithm	Key length	KSP	Rollover state	Initial rollover o...	Rollover frequ

Add | Edit | Remove

< Back | Next > | Cancel


New Zone Signing Key (ZSK)
Guid
Guid:
{00000000-0000-0000-0000-000000000000}
Key Properties
Cryptographic algorithm:
RSA/SHA-256
Key length (Bits):
1024
Select a key storage provider to generate and store keys:
Microsoft Software Key Storage Prov
DNSKEY signature validity period (hours):
168
DS signature validity period (hours):
168
Zone record validity period (hours):
240
Key Rollover
Enable automatic rollover
Rollover frequency (days):
90
Delay the first rollover by (days):
0
OK
Cancel

Zone Signing Wizard

Zone Signing Key (ZSK)

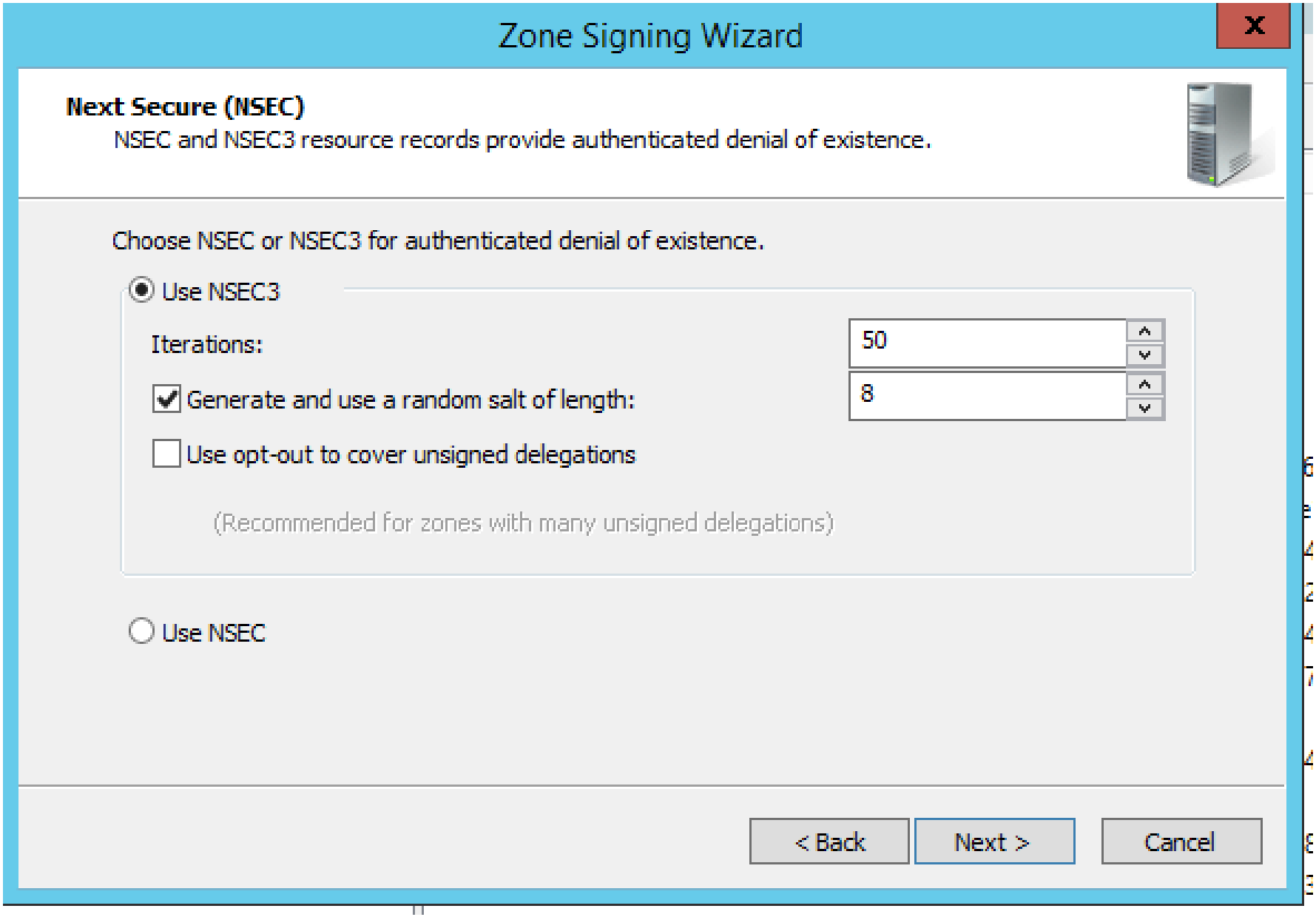
Configure one or more ZSKs

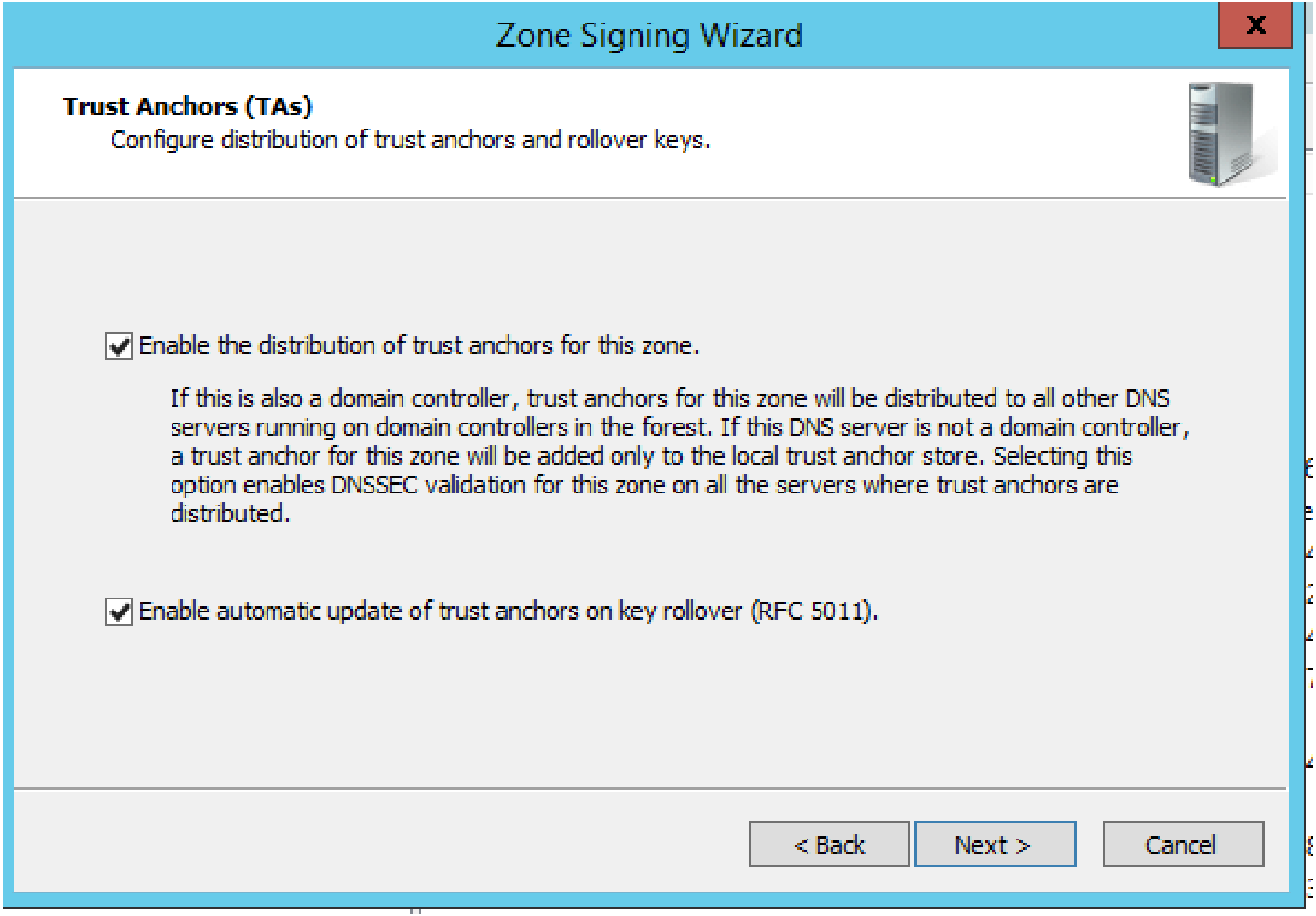
Configure parameters for at least one ZSK. A maximum of three ZSKs can be specified for each of the available cryptographic algorithms.

Algorithm	Key length	KSP	Rollover state	Initial rollover o...	Rollover frequ
RSA/SHA-256	1024	Microsoft Softw...	Enabled	0	90

Add | Edit | Remove

< Back | Next > | Cancel


Zone Signing Wizard
Next Secure (NSEC)
NSEC and NSEC3 resource records provide authenticated denial of existence.
Choose NSEC or NSEC3 for authenticated denial of existence.
Use NSEC3
Iterations:
50
Generate and use a random salt of length:
8
Use opt-out to cover unsigned delegations
(Recommended for zones with many unsigned delegations)
Use NSEC
< Back
Next >
Cancel


Zone Signing Wizard
Trust Anchors (TAs)
Configure distribution of trust anchors and rollover keys.
Enable the distribution of trust anchors for this zone.
If this is also a domain controller, trust anchors for this zone will be distributed to all other DNS servers running on domain controllers in the forest. If this DNS server is not a domain controller, a trust anchor for this zone will be added only to the local trust anchor store. Selecting this option enables DNSSEC validation for this zone on all the servers where trust anchors are distributed.
Enable automatic update of trust anchors on key rollover (RFC 5011).
< Back
Next >
Cancel

Zone Signing Wizard

Signing and Polling Parameters

Configure values for DNSSEC signing and polling.

DS record generation algorithm: SHA-1 and SHA-256

DS record TTL (seconds): 3600

DNSKEY record TTL (seconds): 3600

Secure delegation polling period (hours): 12

Signature inception (hours): 1

Offset from current time when the signature is created.

< Back | Next > | Cancel

Zone Signing Wizard

DNS Security Extensions (DNSSEC)

You have successfully configured the following parameters to sign the zone.

Zone name: server2012.com

Key Master: WIN-E630K0E1QHE

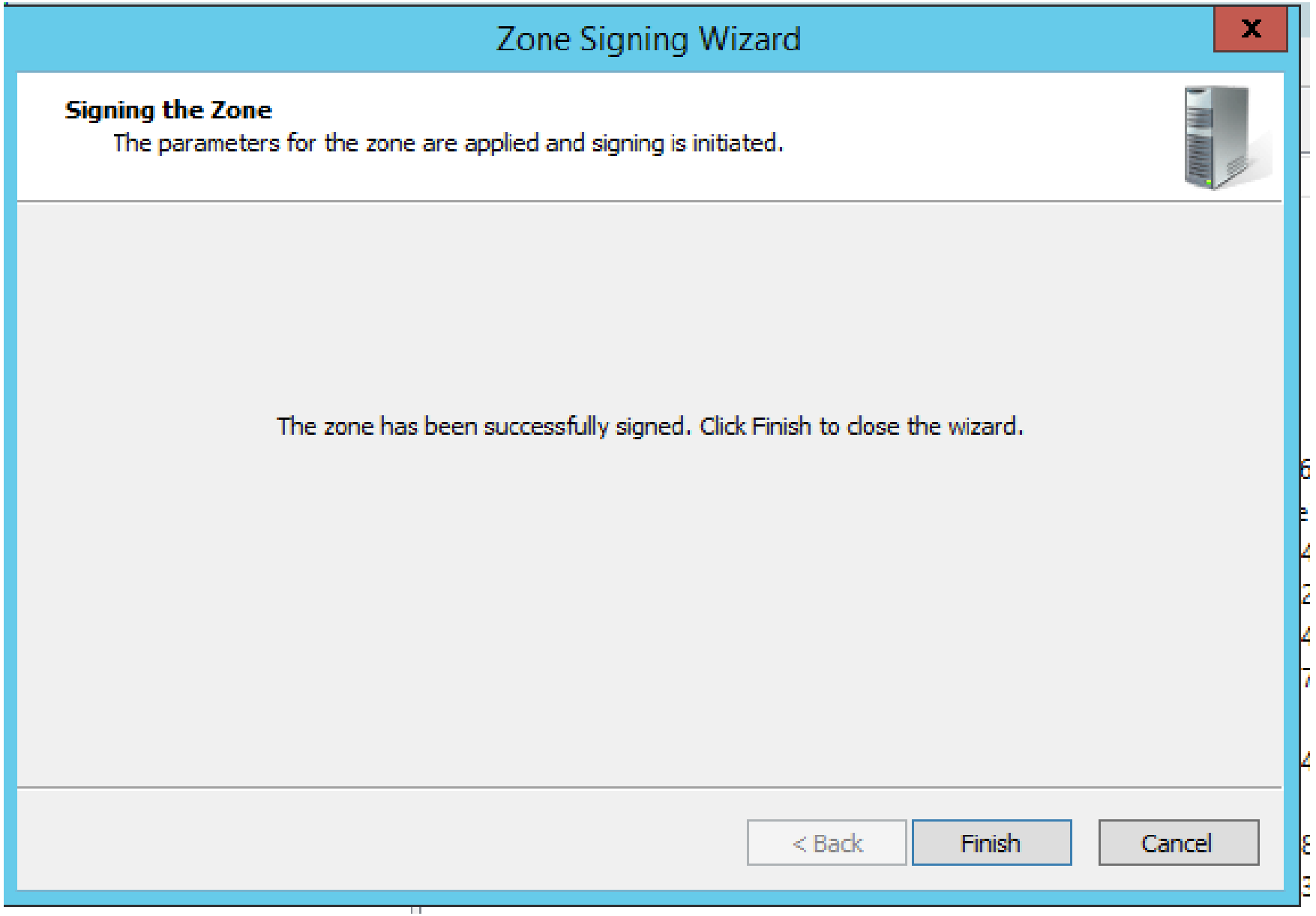
[Key signing key (KSK): 1]
Algorithm: RSA/SHA-256
Key length: 2048 bits
KSP: Microsoft Software Key Storage Provider
DNSKEY signature validity: 168 hours

To configure different parameters, click Back.

To begin signing the zone, click Next.

To close the wizard without signing the zone, click Cancel.

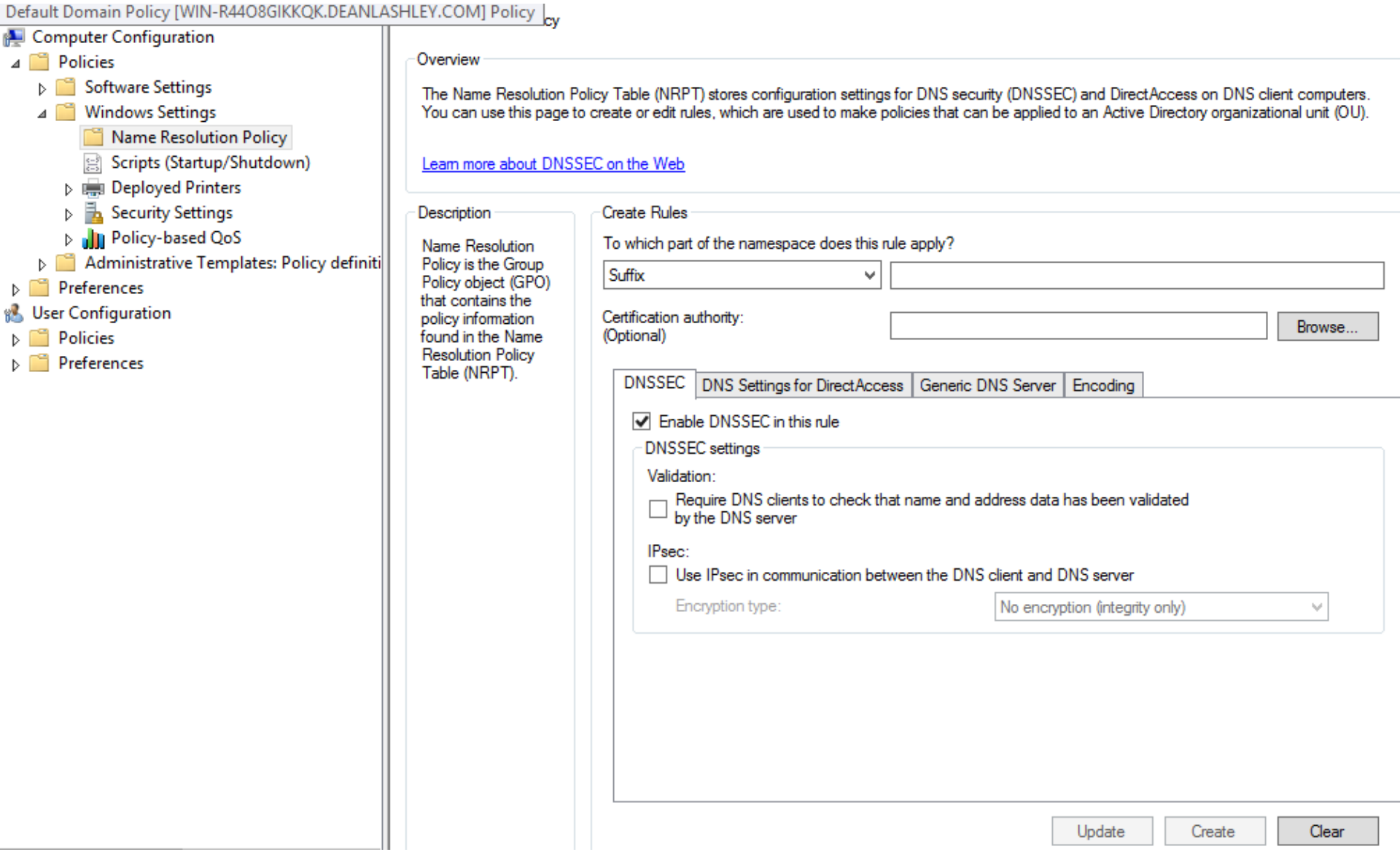
< Back | Next > | Cancel


Zone Signing Wizard
Signing the Zone
The parameters for the zone are applied and signing is initiated.
The zone has been successfully signed. Click Finish to close the wizard.
< Back
Finish
Cancel

The NRPT stores configurations and settings that are used to deploy DNS Security Extensions (DNSSEC), and also stores information related to DirectAccess, a remote access technology
.
The NRPT can be configured using Group Policy or by using the Windows Registry.

The preferred method of configuring the NRPT is with the Group Policy Management Editor.

The DNS client computer only performs DNSSEC validation on domain names where the NRPT has configured the DNS client computers to do so. A client computer that is running Windows 7 is DNSSEC-aware, but it does not perform validation. Instead, it relies on the security-aware DNS server to perform validation on its behalf


Default Domain Policy [WIN-R44O8GIKKQK.DEANLASHLEY.COM] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Policy-based QoS
Administrative Templates: Policy definiti
Preferences
User Configuration
Policies
Preferences
Overview
The Name Resolution Policy Table (NRPT) stores configuration settings for DNS security (DNSSEC) and DirectAccess on DNS client computers. You can use this page to create or edit rules, which are used to make policies that can be applied to an Active Directory organizational unit (OU).
Learn more about DNSSEC on the Web
Description
Name Resolution Policy is the Group Policy object (GPO) that contains the policy information found in the Name Resolution Policy Table (NRPT).
Create Rules
To which part of the namespace does this rule apply?
Suffix
Certification authority: (Optional)
Browse...
DNSSEC
DNS Settings for DirectAccess
Generic DNS Server
Encoding
Enable DNSSEC in this rule
DNSSEC settings
Validation:
Require DNS clients to check that name and address data has been validated by the DNS server
IPsec:
Use IPsec in communication between the DNS client and DNS server
Encryption type:
No encryption (integrity only)
Update
Create
Clear