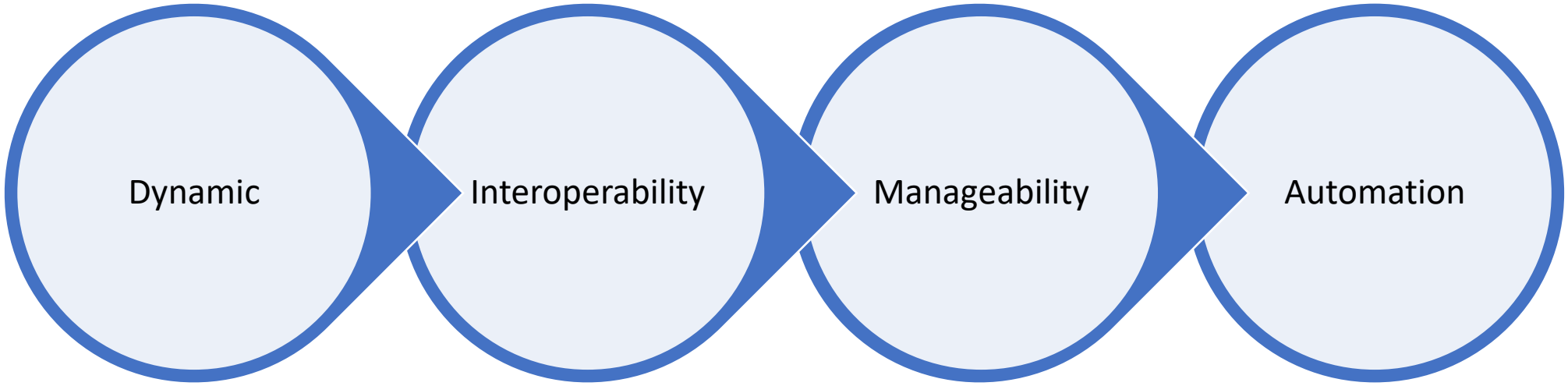
DNSSEC in Windows DNS Server

Kumar Ashutosh, Microsoft

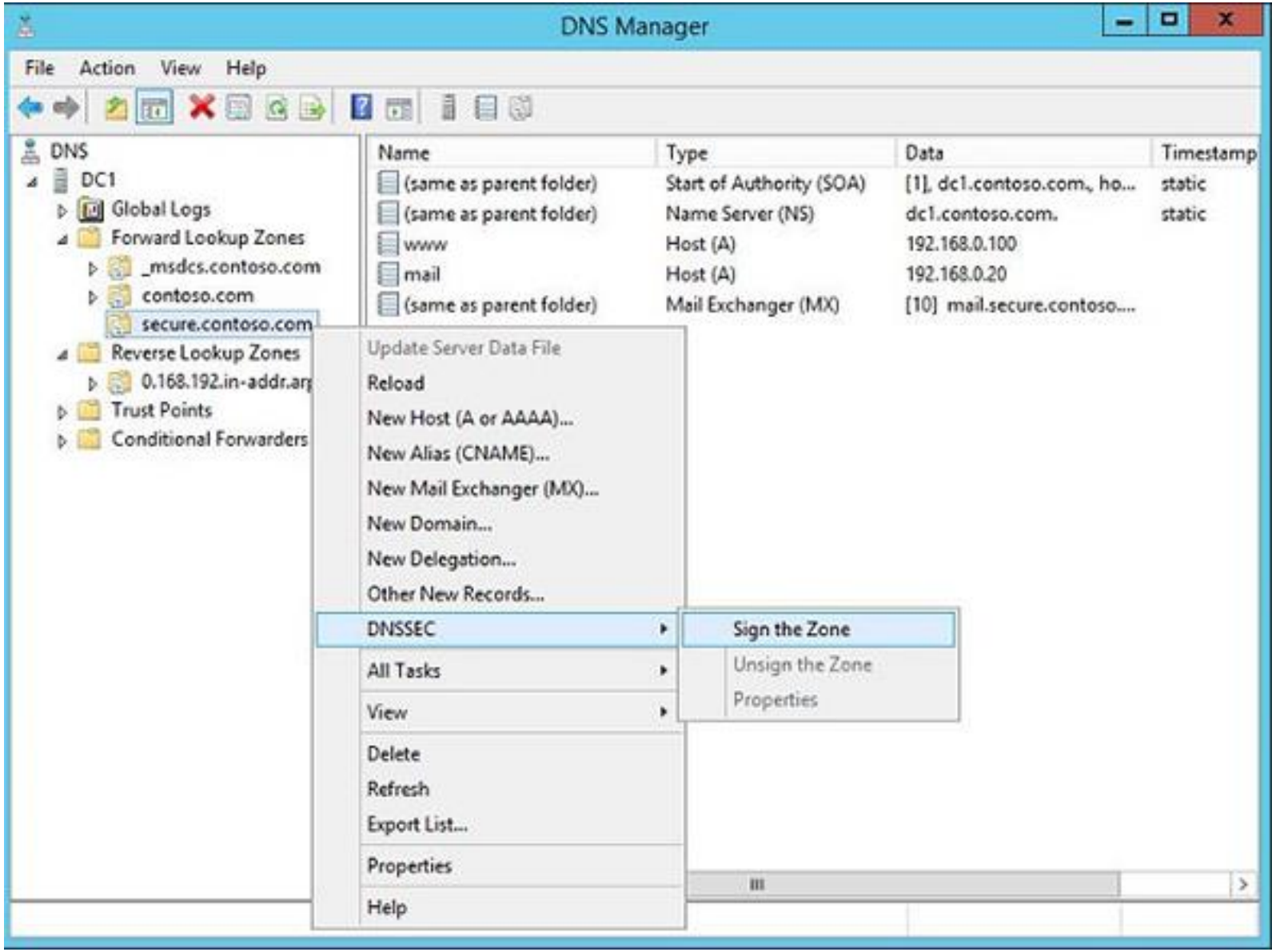
@krash0x35



Overview

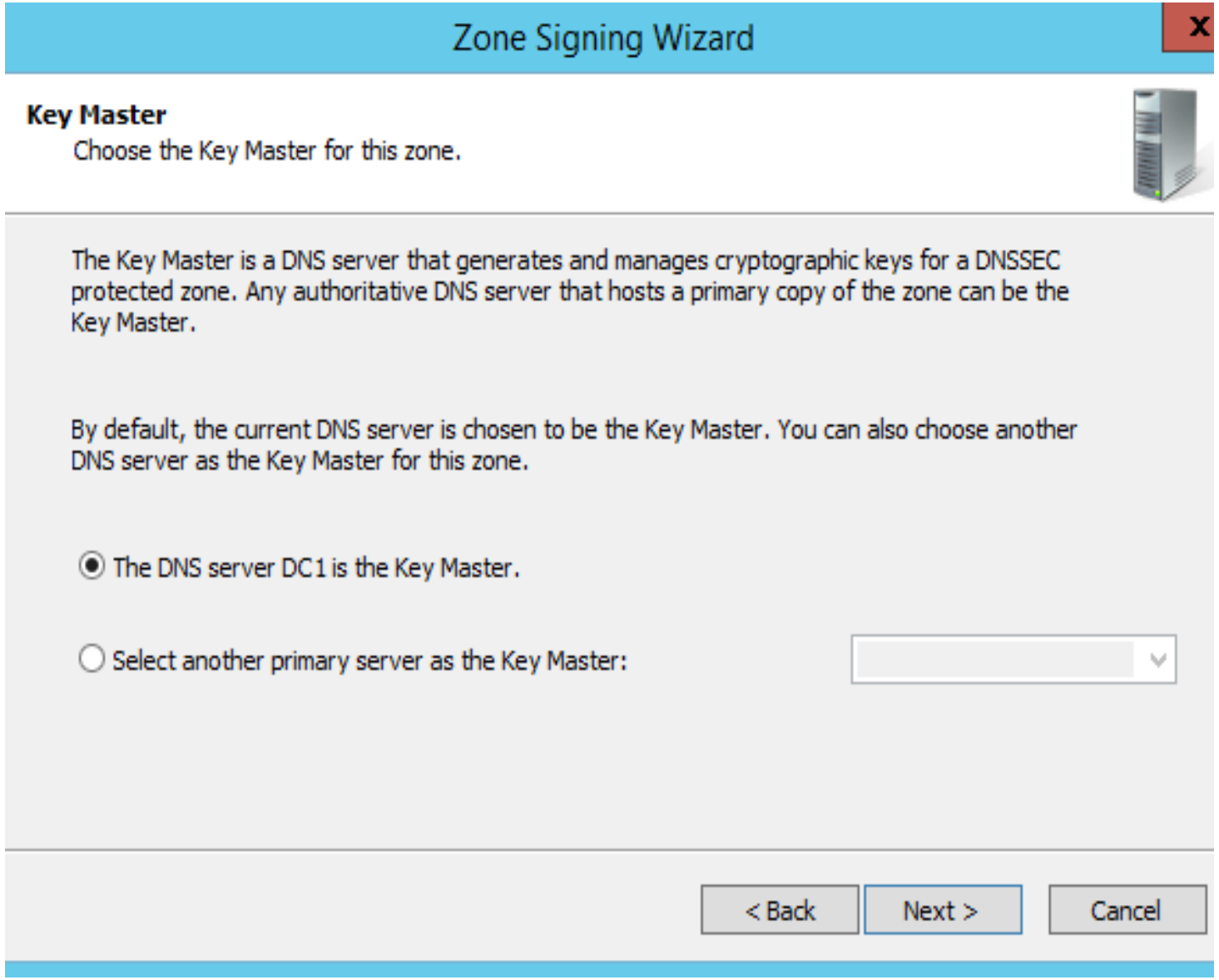
Zone Signing

- Choose the Key Master
- Signing keys
- KSK configuration
- ZSK configuration
- NSEC
- Trust anchors
- Signing and polling
- Summary



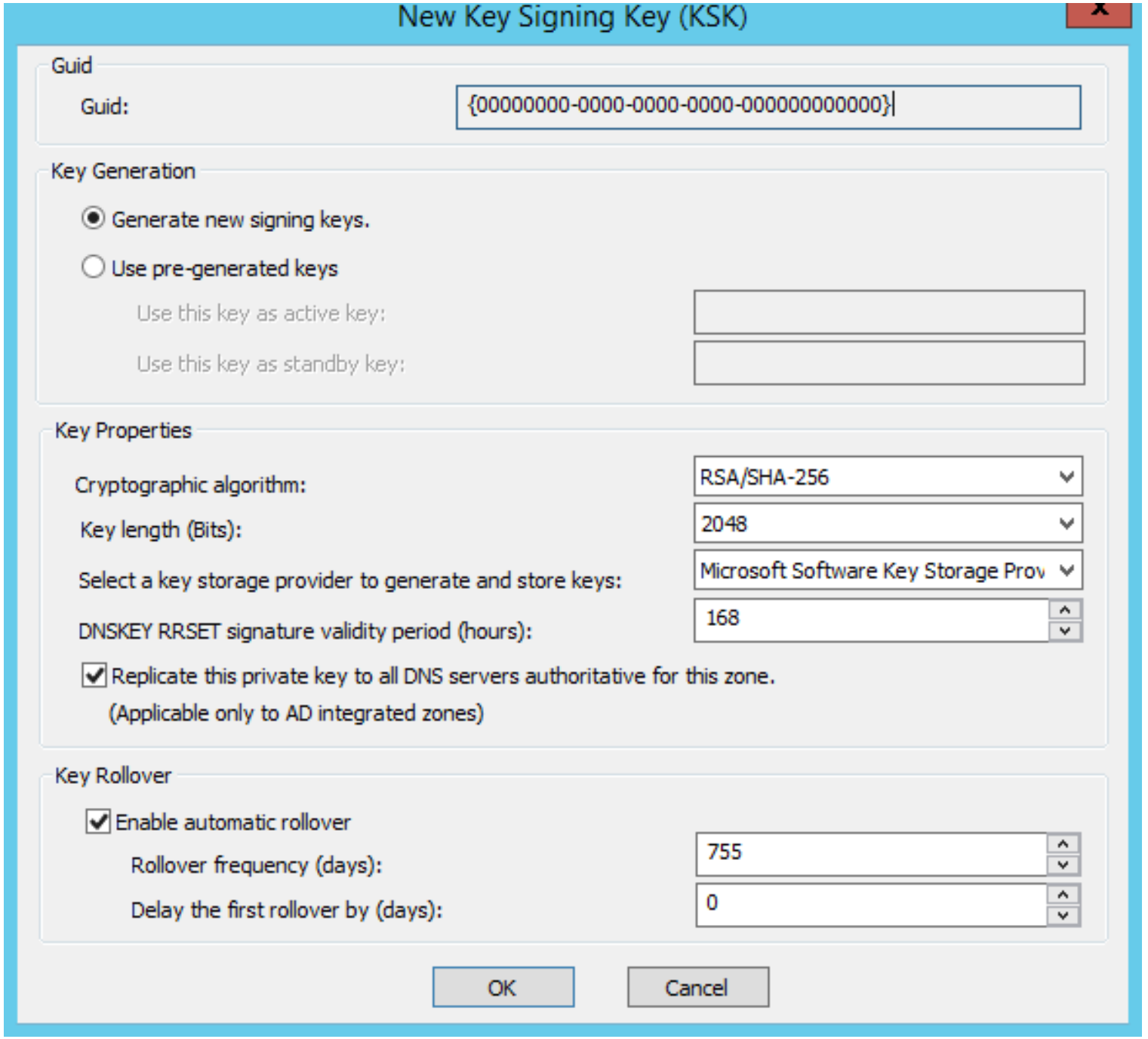
Zone Signing: Select Key Master

- Single location for all key generation and management
- Responsible for automated key rollover



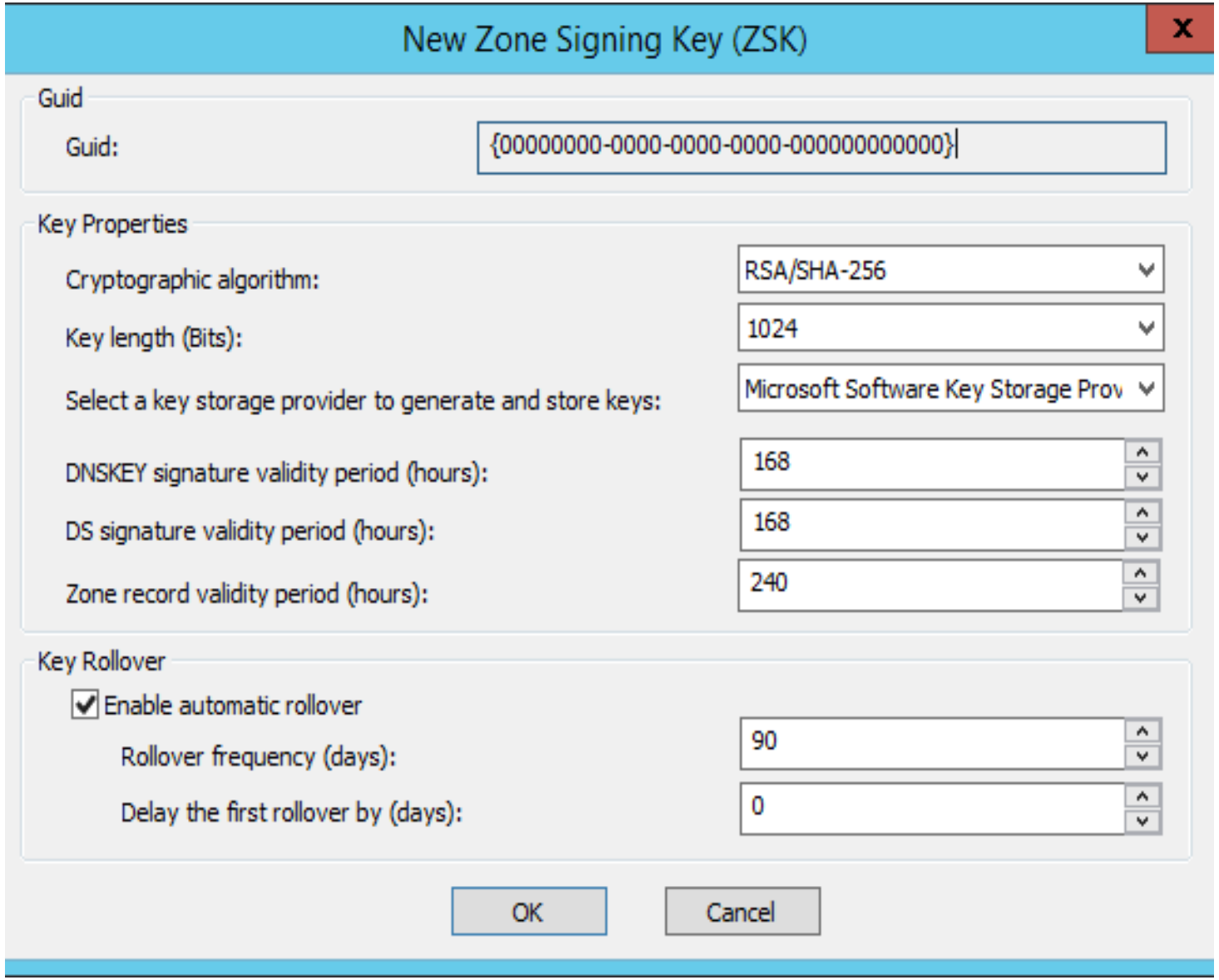
Zone Signing: Configure KSK

- Key signing keys (KSK) are used to sign other DNSKEY records



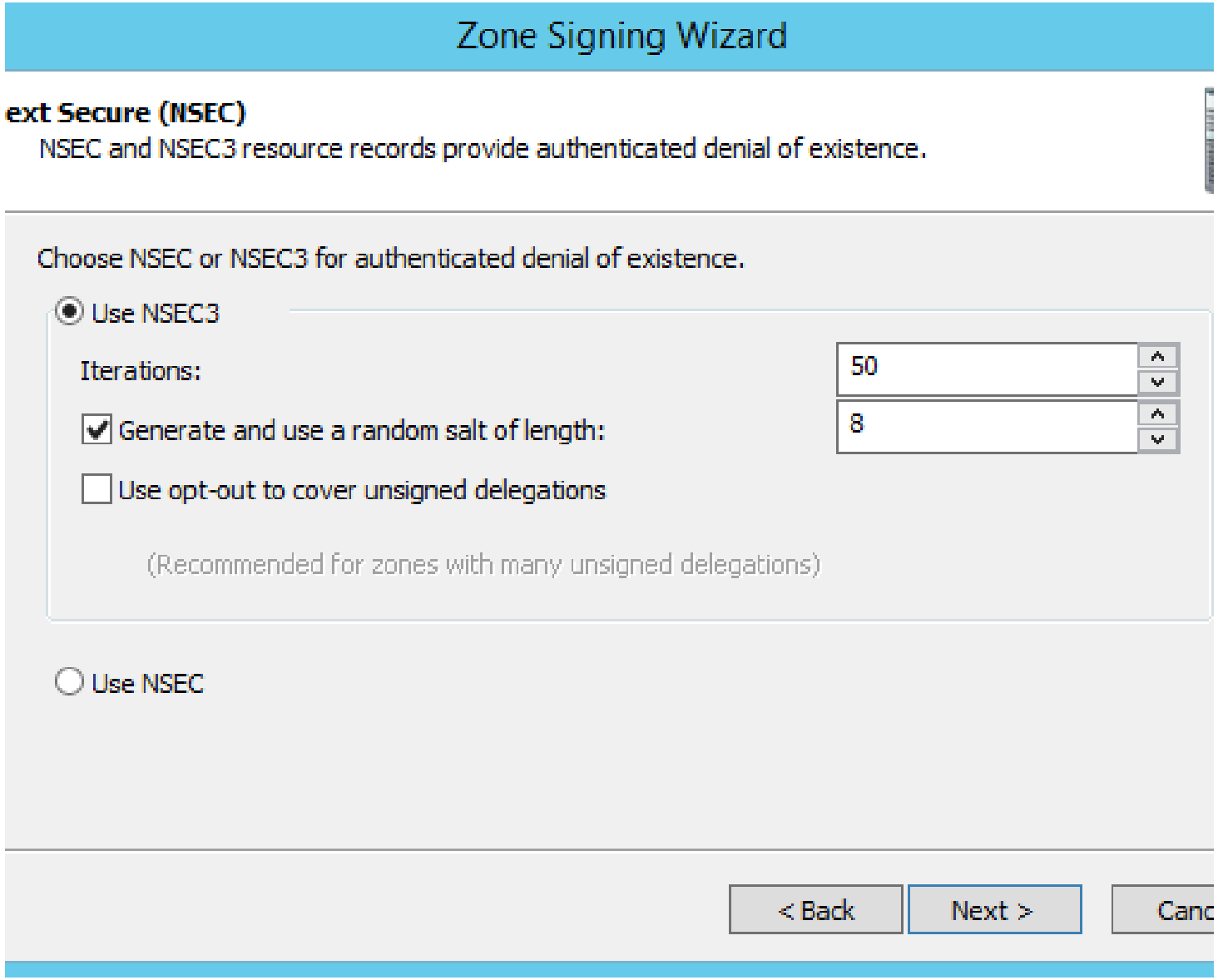
Zone Signing: Configure ZSK

- Zone signing keys (ZSK) are used to sign other records



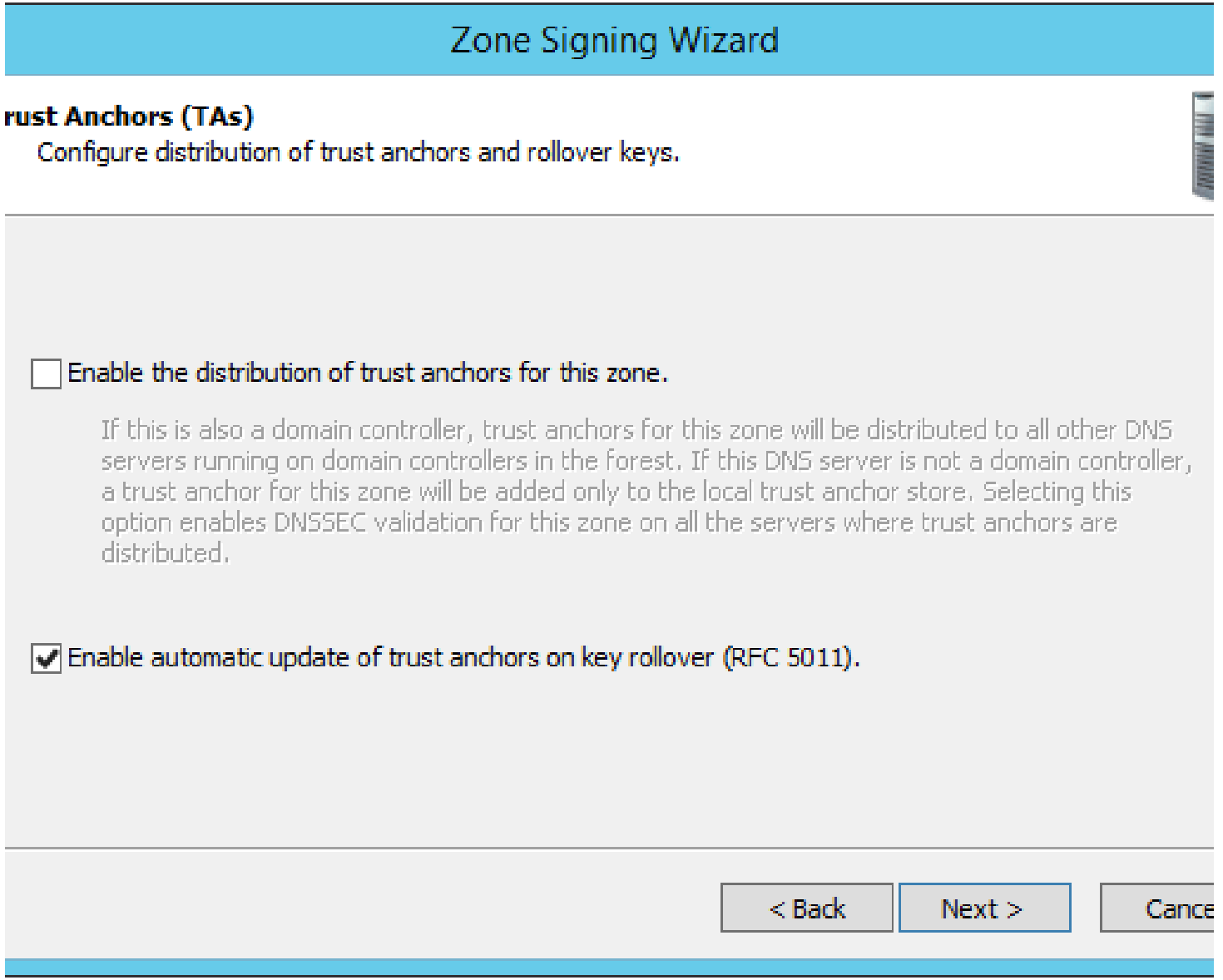
Zone Signing: Denial of Existence

- NSEC
- NSEC3

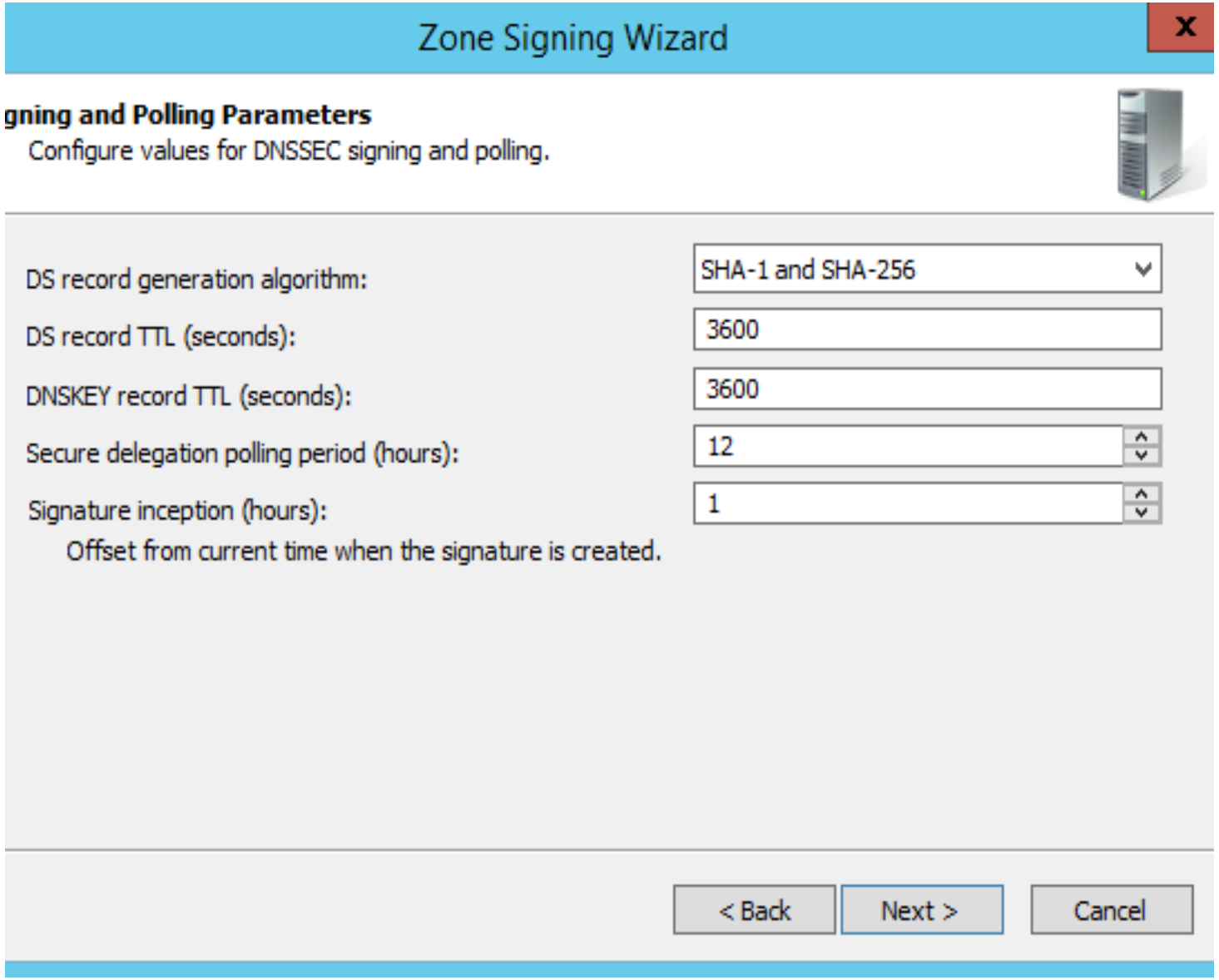


Zone Signing: Trust Anchors

- A trust anchor (or trust “point”) is a public cryptographic key for a signed zone.
- Delegation Signer (DS)
- DNSKEY



Zone Signing: Signaling And Polling



Flexibility

- Chose your Keys
- Dynamic unsign/re-sign
- Change Properties
- DDNS with DNSSEC
- AD/Non-AD
- Primary Secondary
- DNSSEC with Traffic Management
- Chose your Key Store

Powershell Automation

Sign with Default

- Invoke-DnsServerZoneSign -ZoneName secure.contoso.com –SignWithDefault -Force

Customize your parameters

- PS C:\> Reset-DnsServerZoneKeyMasterRole -ZoneName fabrikam.com -KeyMasterServer dc2.contoso.com -SeizeRole -Force
- PS C:\> Set-DnsServerDnsSecZoneSetting -ZoneName fabrikam.com -DenialOfExistence NSec
- PS C:\> Add-DnsServerSigningKey -ZoneName fabrikam.com -Type KeySigningKey -CryptoAlgorithm RsaSha1 -KeyLength 2048
- PS C:\> Add-DnsServerSigningKey -ZoneName fabrikam.com -Type ZoneSigningKey -CryptoAlgorithm RsaSha1 -KeyLength 1024
- PS C:\> Invoke-DnsServerZoneSign -ZoneName fabrikam.com -Force

Distribute Trust Anchors

Export a Trust Point

- Export-DnsServerDnsSecPublicKey -ComputerName DC2.contoso.com -ZoneName secure.contoso.com -Path \\Myshare\keys
- Export-DnsServerDnsSecPublicKey -ComputerName DC2.contoso.com -ZoneName secure.contoso.com -Path \\Myshare\keys -DigestType sha1

Import a Trust Point

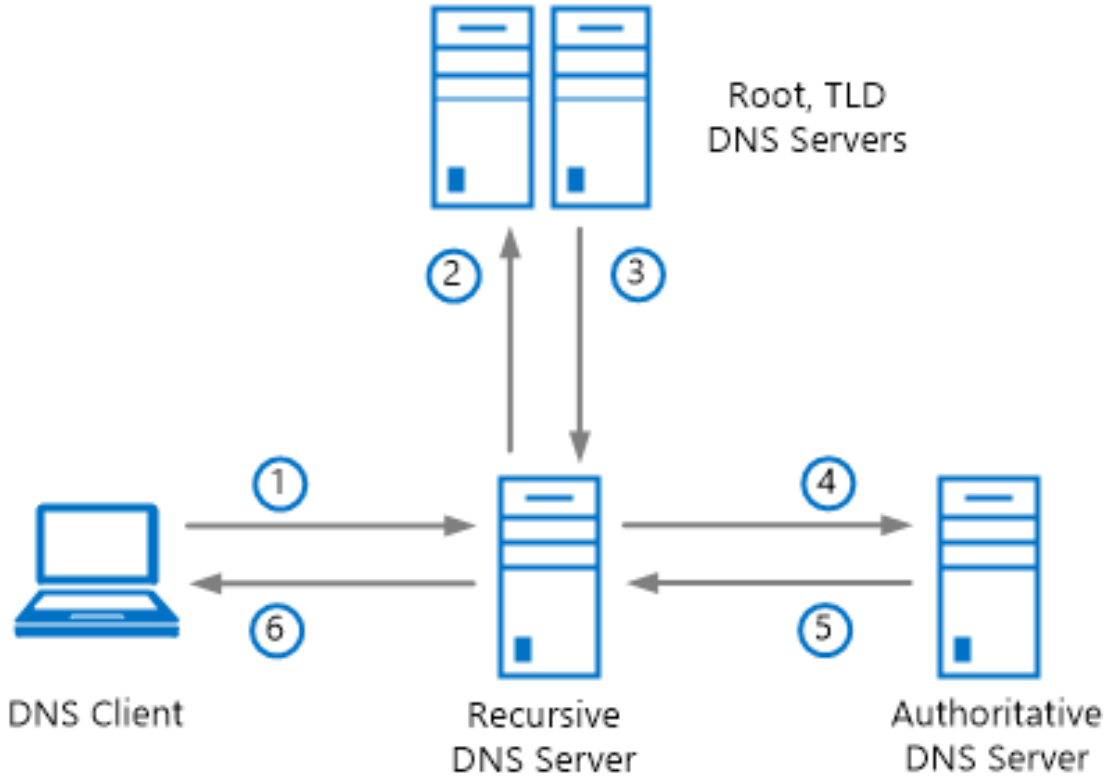
- Import-DnsServerTrustAnchor -KeySetFile "\\File1\DNSKeys\keyset-secure.contoso.com"

Add Root Trust Anchor

- Add-DnsServerTrustAnchor -Root

Verify DNSSEC: Demonstration

Step	Query-response	Optional DNSSEC data
1	A DNS client sends a DNS query to a recursive DNS server.	The DNS client can indicate that it is DNSSEC-aware (DO=1).
2	The recursive DNS server sends a DNS query to the root and top-level domain (TLD) DNS servers.	The recursive DNS server can indicate that it is DNSSEC-aware (DO=1).
3	The root and TLD servers return a DNS response to the recursive DNS server providing the IP address of the authoritative DNS server for the zone.	Authoritative servers for the parent zone can indicate that the child zone is signed using DNSSEC and include a secure delegation (DS record).
4	The recursive DNS server sends a DNS query to the authoritative DNS server for the zone.	The recursive DNS server can indicate that it is DNSSEC-aware (DO=1) and capable of validating signed resource records (CD=1) to be sent in the response.
5	The authoritative DNS server returns a DNS response to the recursive DNS server, providing the resource record data.	The authoritative DNS server can include DNSSEC signatures in the form of RRSIG records in the DNS response, for use in validation.
6	The recursive DNS server returns a DNS response to the DNS client, providing the resource record data.	The recursive DNS server can indicate whether or not the DNS response was validated (AD=1) using DNSSEC.



Thank You

For more details visit:

https://technet.microsoft.com/en-us/library/dn593694(v=ws.11).aspx