Deploying DNSSEC in Windows Server 2012

David Cates
Platform Services Group
Microsoft Corporation

Agenda

Overview

Deployment

Operations

New in DNS

The Basic Idea

- DNSSEC introduces 5 new record types:
  - Resource Record Signature (RRSIG)
  - DNS Public Key (DNSKEY)
  - Delegation Signer (DS)
  - Next Secure (NSEC)
  - Next Secure 3 (NSEC3)
- Using the new records resolvers build a chain of trust for any signed zone
- DNS Responses include signatures and can be validated

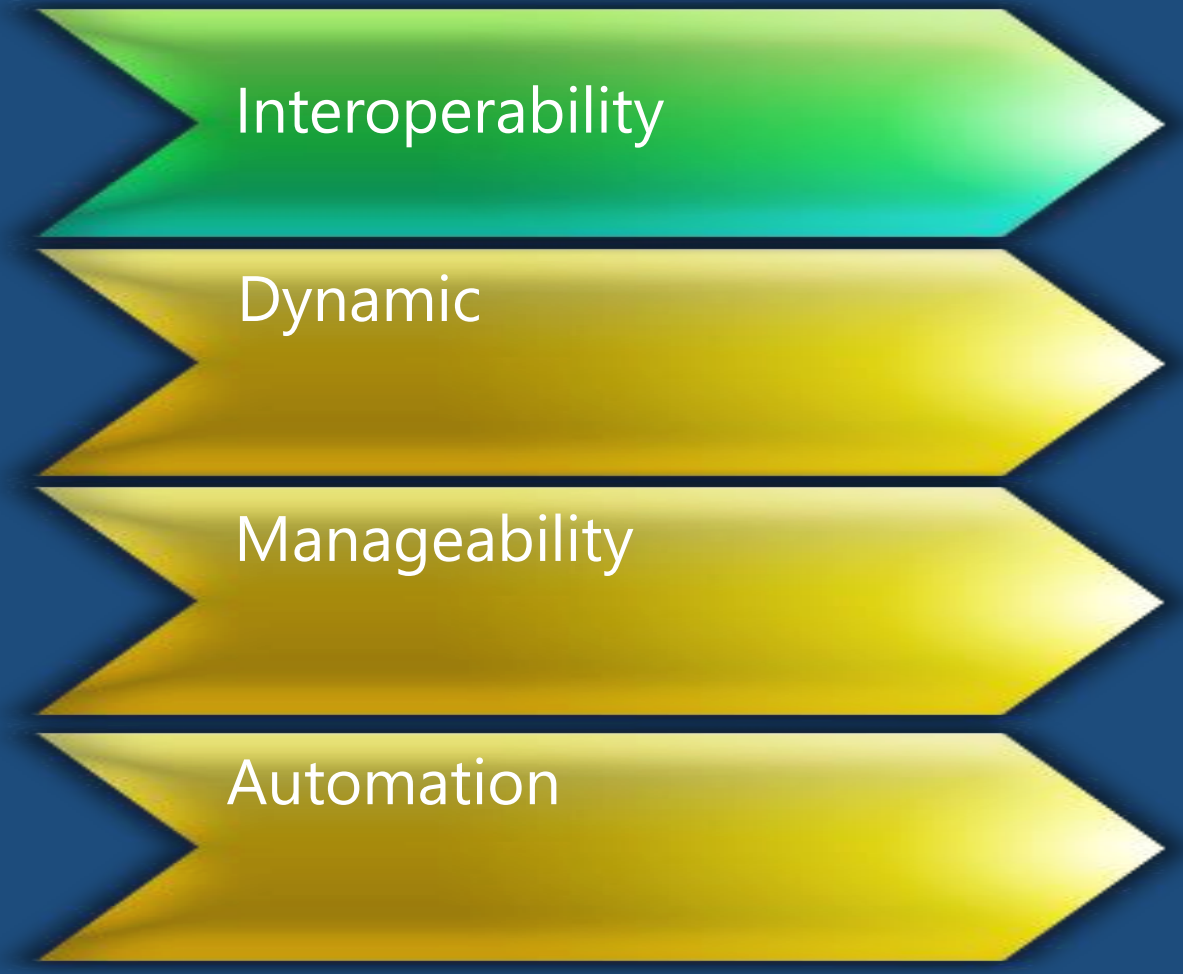
DNSSEC in Windows 2008 R2

- Microsoft introduced support for DNSSEC in Windows 2008 R2…
  - Ability to sign zones offline and host signed zones
  - Validation of signed responses
  - Support for NSEC

DNSSEC in Windows Server 2012 R2

Overview ✓ | Deployment | Operations | New in DNS

ENABLING ENTERPRISE DNSSEC ROLLOUT

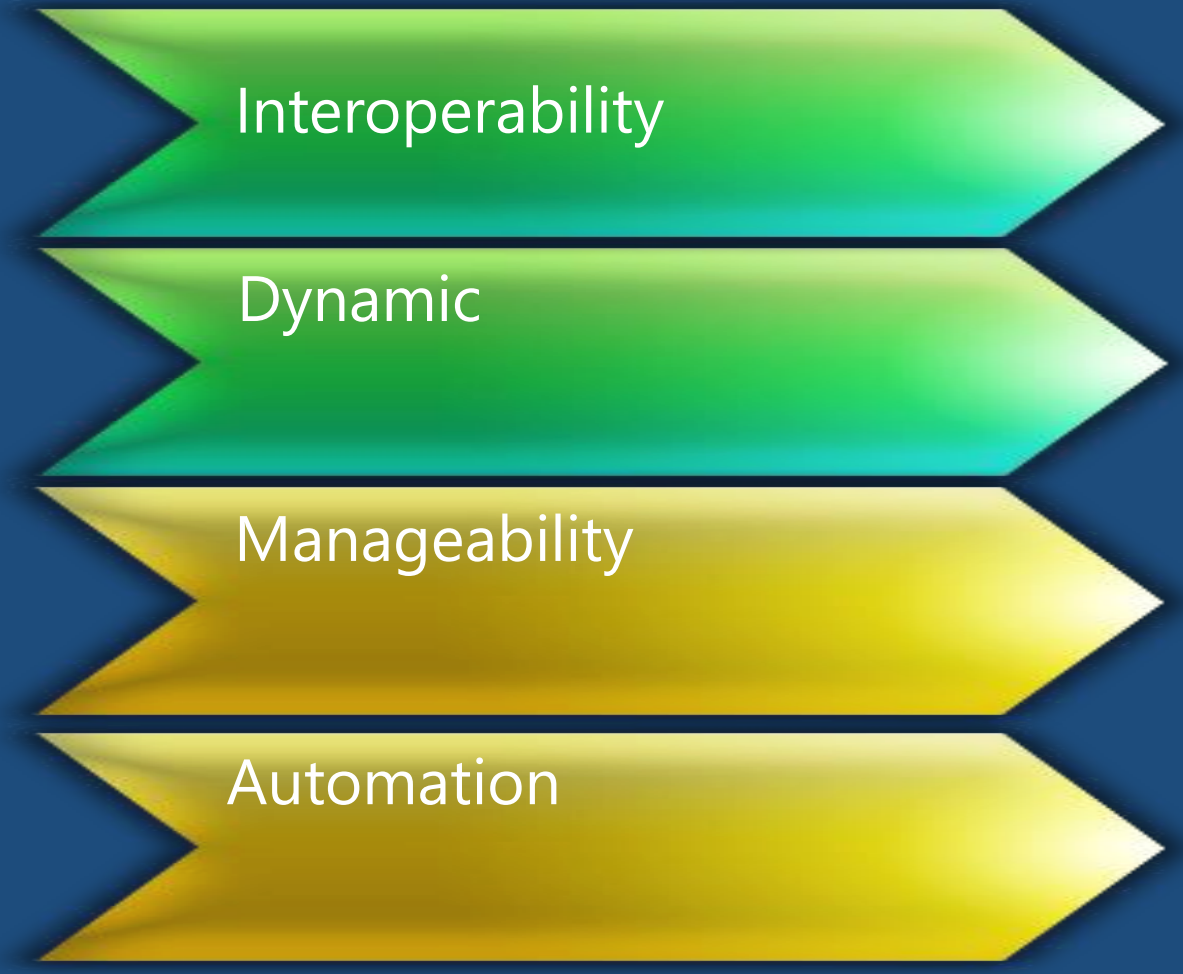


- Latest RFCs
  - NSEC3 Support
  - RSA/SHA-2, ECDSA Signing
  - Automated Trust Anchor rollover
- Support for 3rd Party Key Mgmt

DNSSEC in Windows Server 2012 R2

Overview | Deployment | Operations | New in DNS

ENABLING ENTERPRISE DNSSEC ROLLOUT



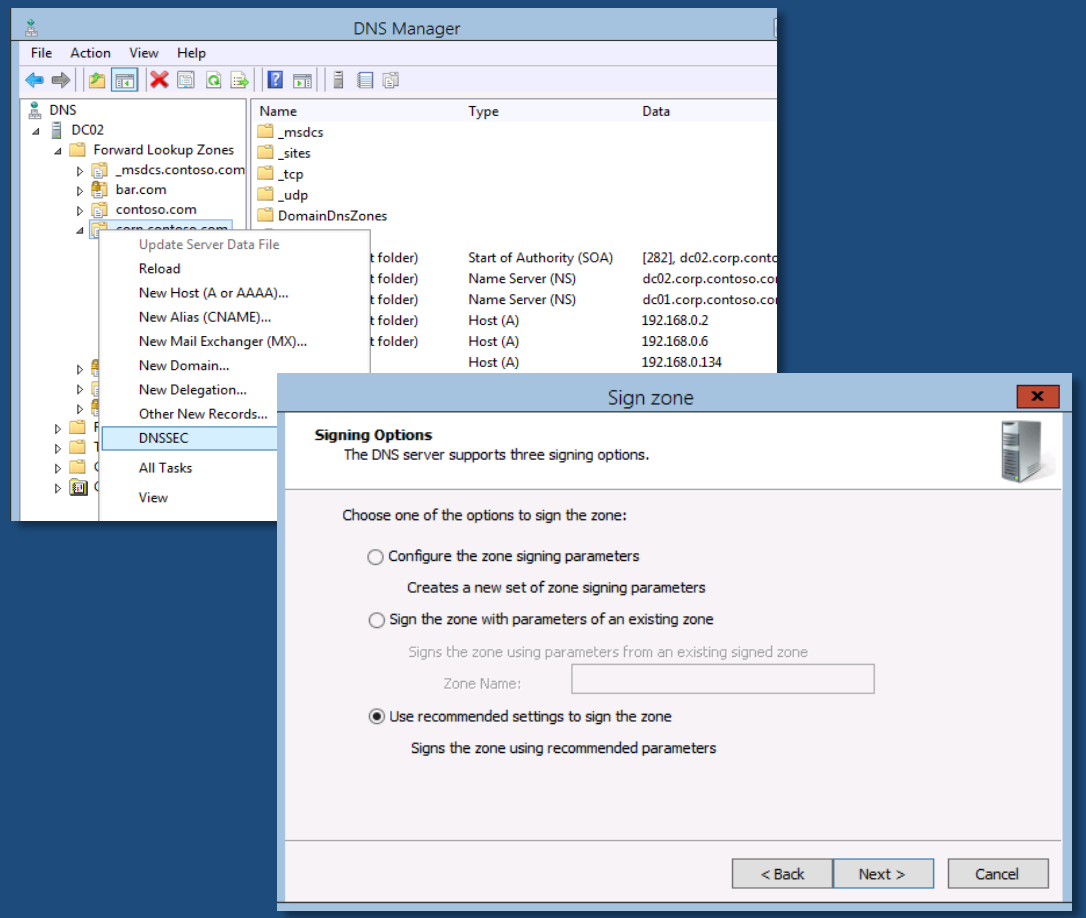
- Active Directory Integrated
  - Support for dynamic updates
  - Preserving the multi-master DNS model
  - Leverage AD for secure key distribution and Trust Anchor distribution
- Improve DNS/DNSSEC server performance

DNSSEC in Windows Server 2012 R2

Overview | Deployment | Operations | New in DNS

ENABLING ENTERPRISE DNSSEC ROLLOUT

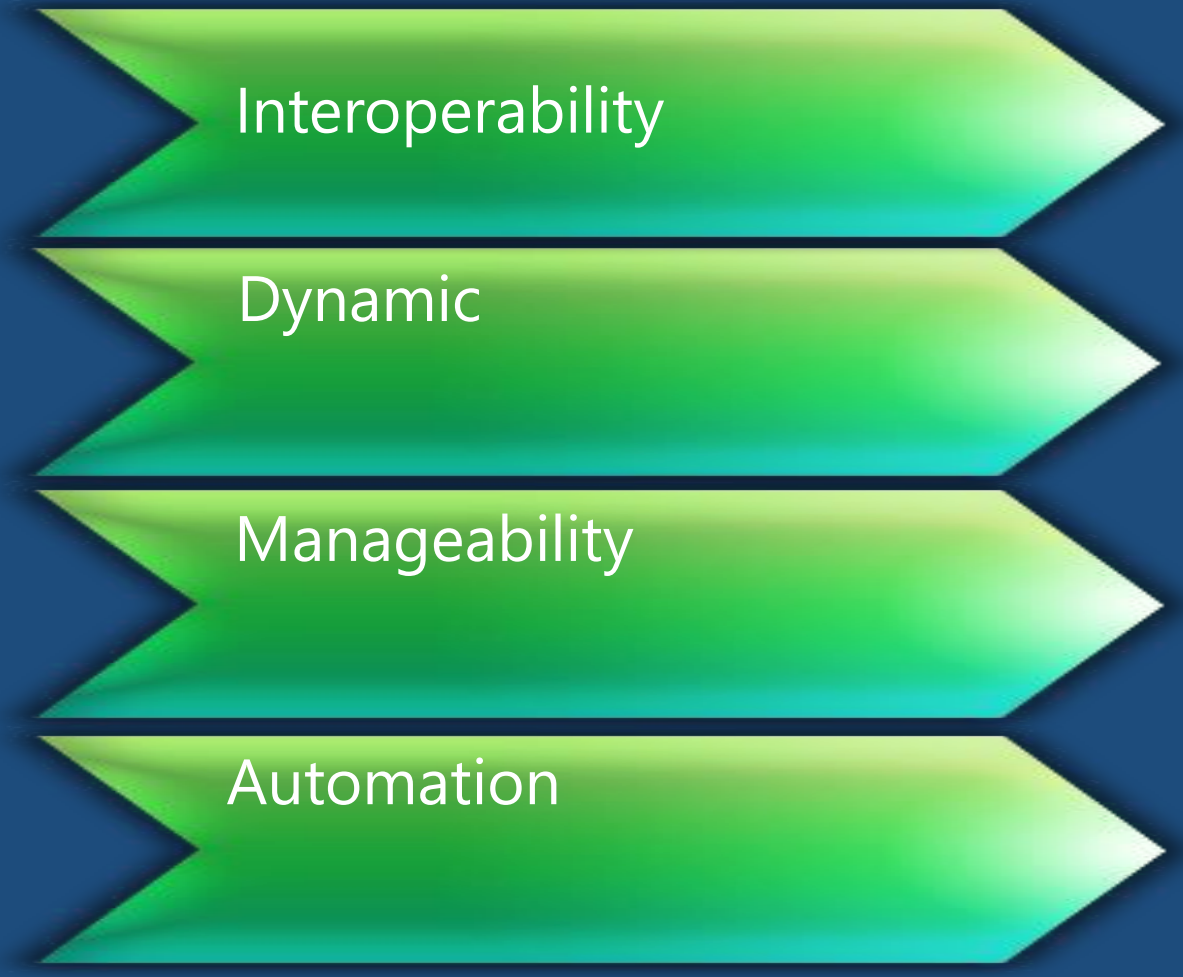
- Interoperability
- Dynamic
- Manageability
- Automation



DNSSEC in Windows Server 2012 R2

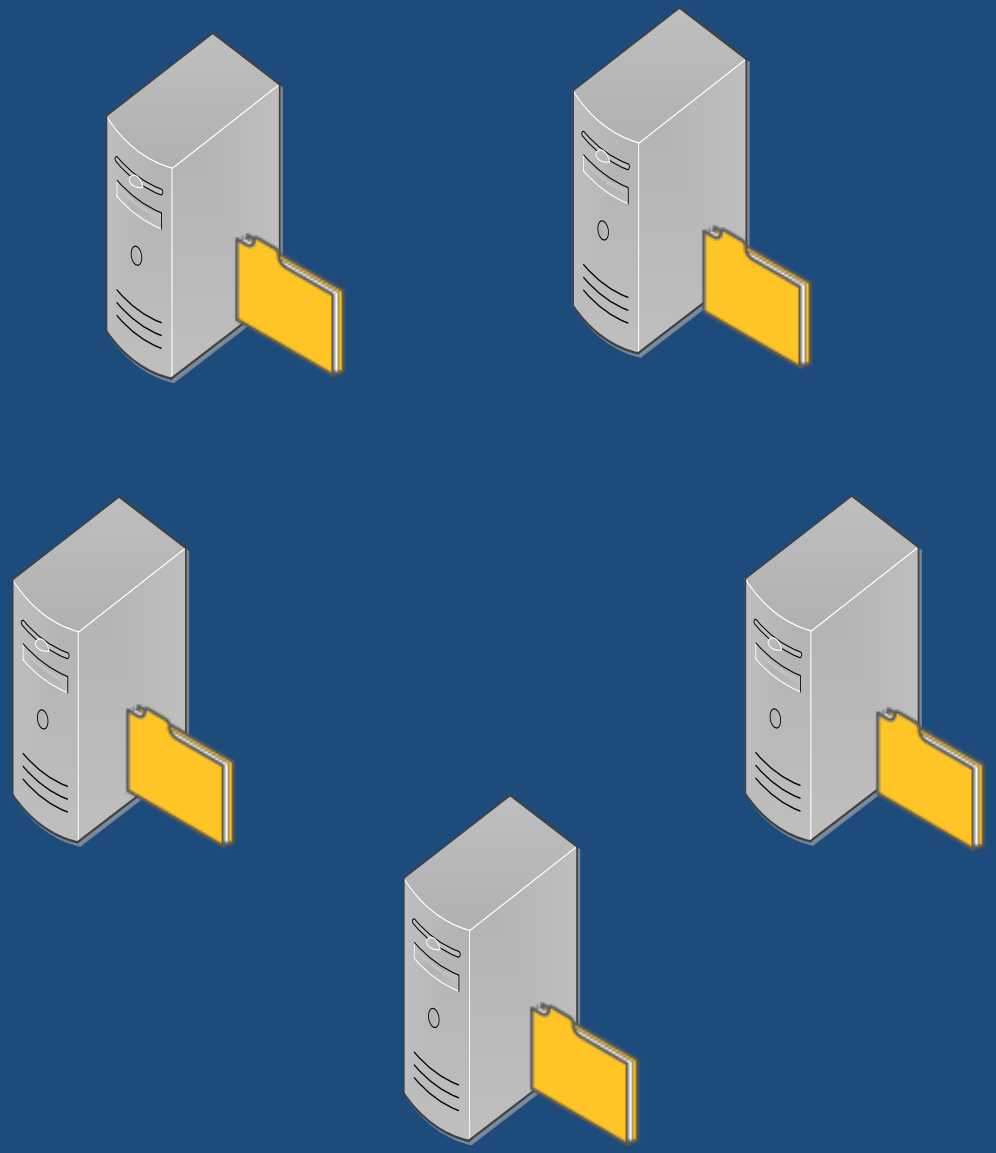
Overview | Deployment | Operations | New in DNS

ENABLING ENTERPRISE DNSSEC ROLLOUT



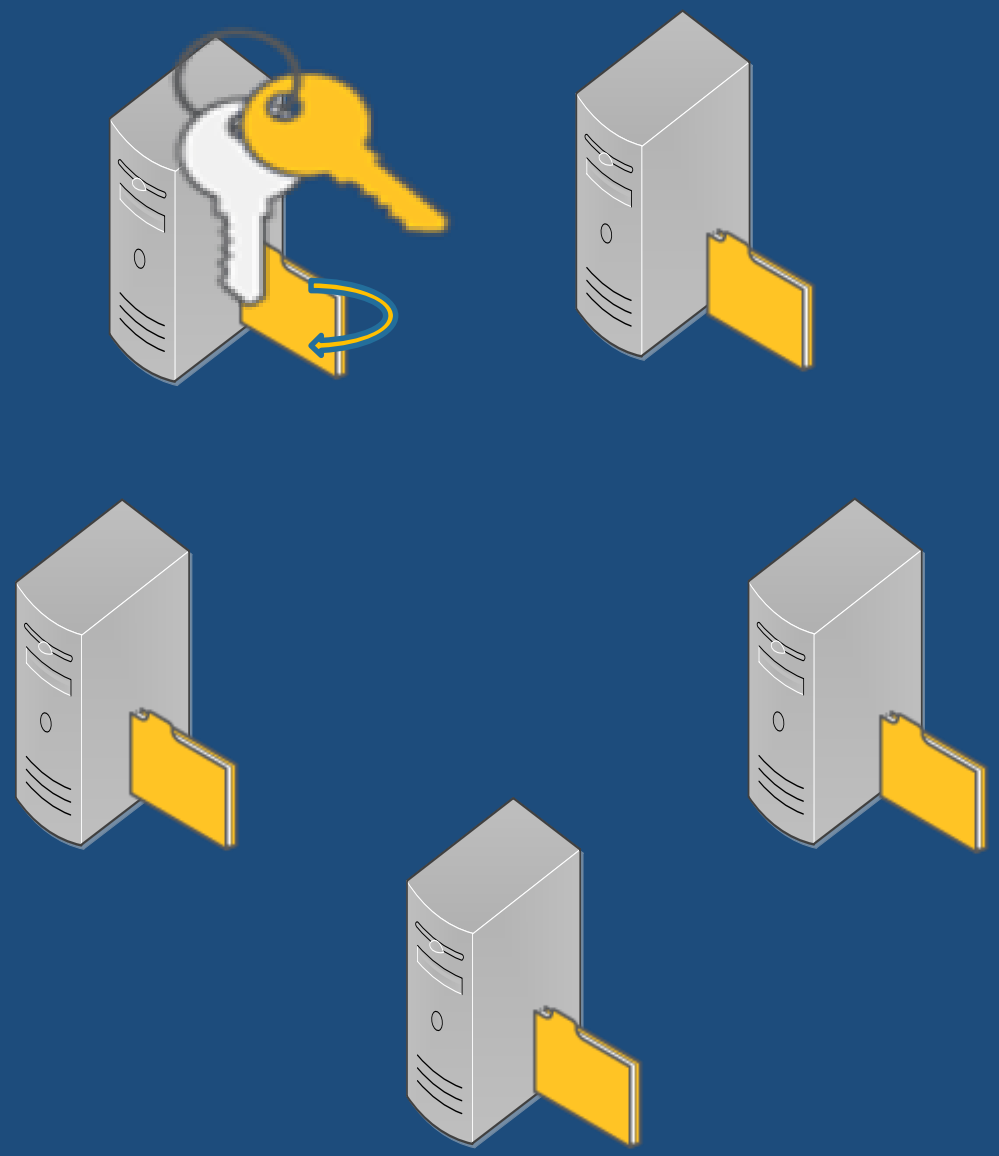
- Automated **re-signing** on static and dynamic updates
- Automated **key rollovers**
- Automated **signature refresh**
- Automated **updating of secure delegations**
- Automated **distribution and updating of Trust Anchors**

Introduce Windows Server 2012



- Active Directory integrated zone
- Classic multi-master deployment
  - Hosted on five DNS servers that are also domain controllers

Signing a zone



Overview | Deployment | Operations | New in DNS

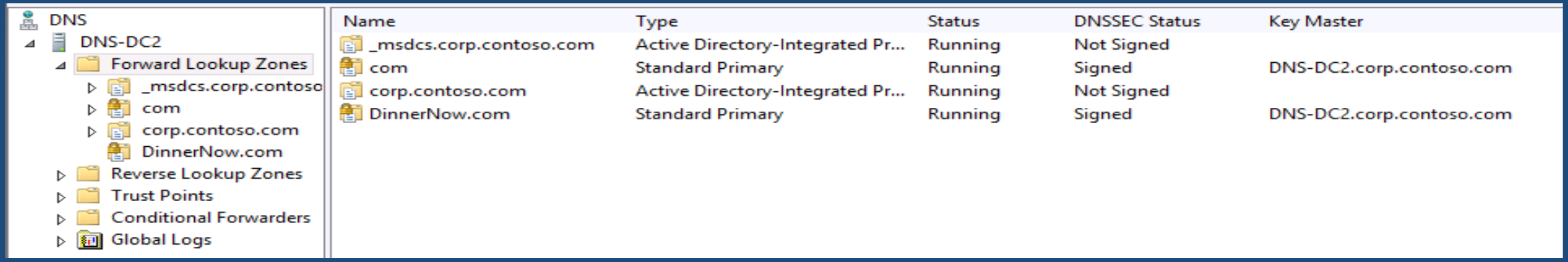
AD integrated zone

- DNS Manager wizard walks admin through signing process
- Generates Keys for signing zone on the first DC.
- Signs it's own copy of the zone

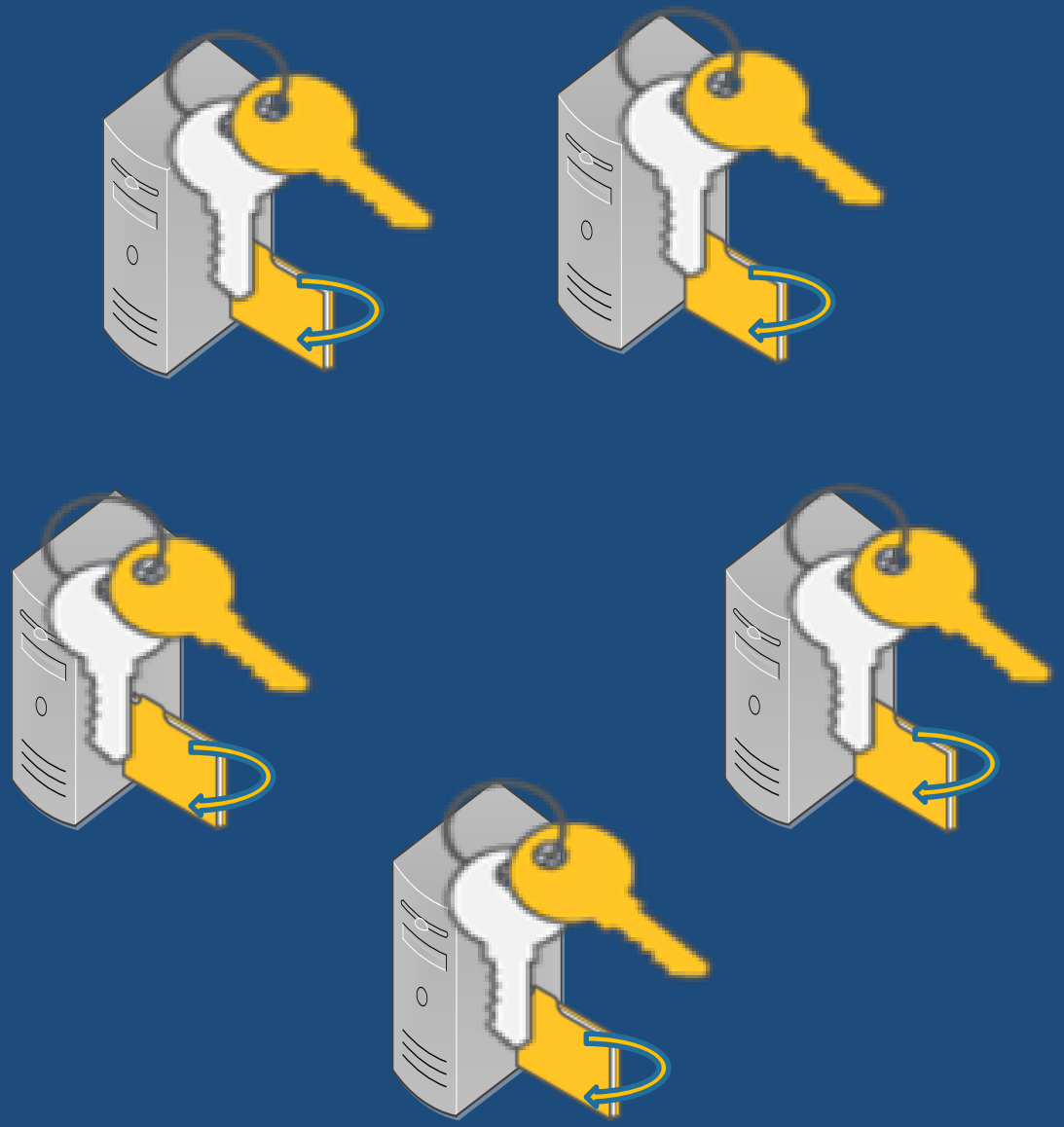
Key Master Role

Overview | Deployment | Operations | New in DNS

- Single location for all key generation and management
  - Responsible for automated key rollover
- Administrator designates one server to be the key master
  - First DNSSEC server becomes KM

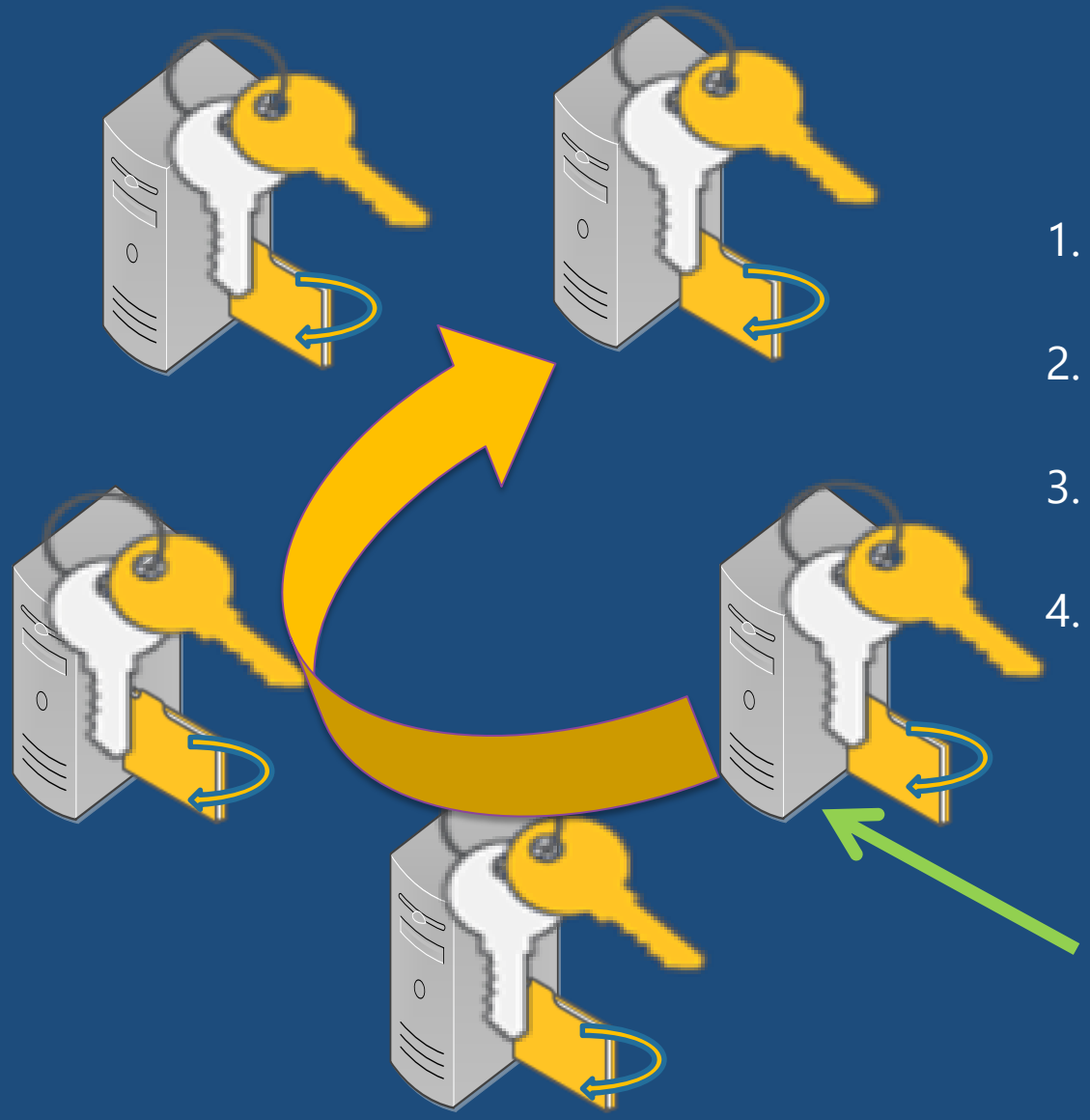


Signing entire zone

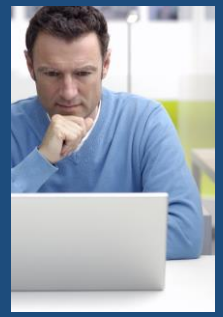


- Private zone signing keys replicate automatically to all DCs hosting the zone through AD replication
- Each zone owner signs its own copy of the zone when it receives the key
  - Only Server 2012 DCs will sign their copy of the zone

Updating zone data

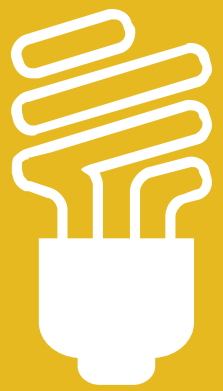


1. Client sends dynamic update to any authoritative DNS server
2. That DNS server updates its own copy of the zone and generates signatures
3. The *unsigned* update is replicated to all other authoritative servers
4. Each DNS server adds the update to its copy of the zone and generates signatures



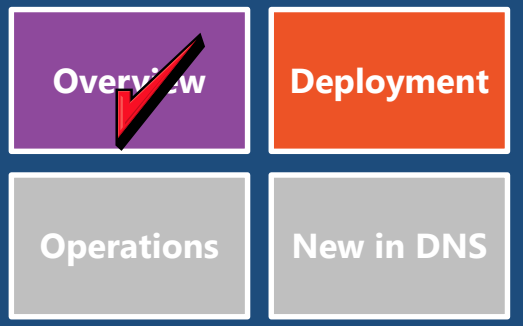
Microsoft

Signing a zone



Demo

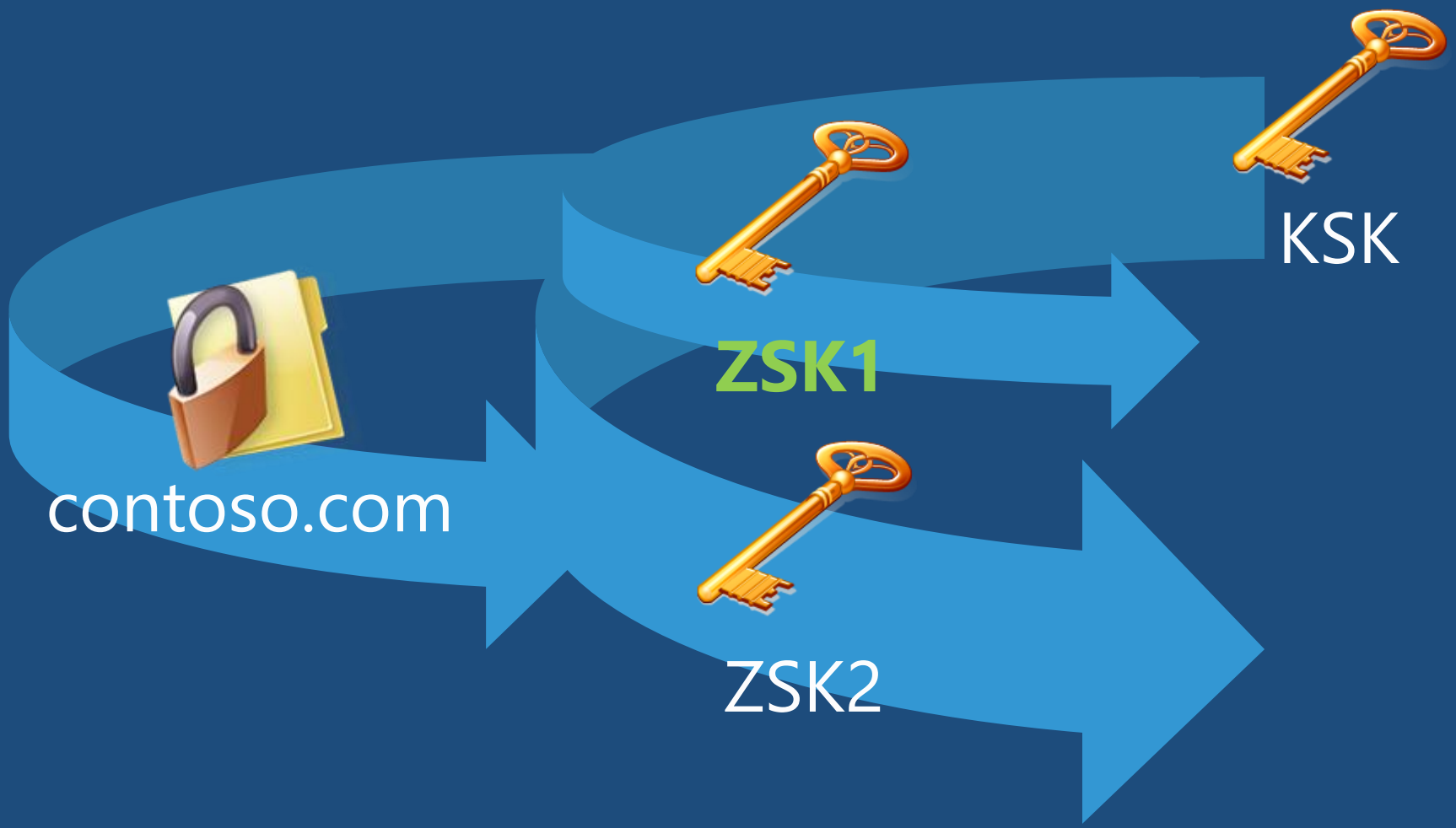
Trust Anchor Distribution & Mgmt.

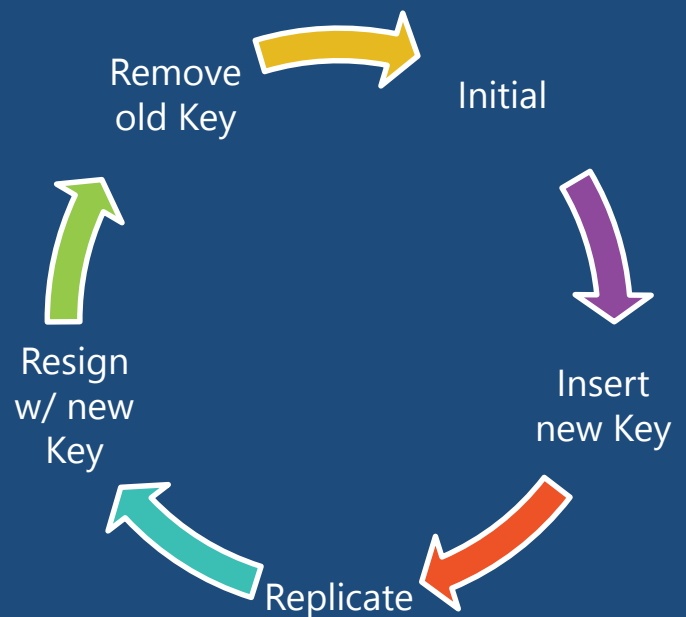


- Trust Anchor Distribution
  - Trust Anchors replicate to all DNS servers that are DCs in the forest via AD
  - Distribution of TAs to servers not a domain controller in the forest is manual via PowerShell or DNS Manager
- Trust Anchor maintenance
  - Trust Anchor updates are automatically replicated via AD to all servers in the forest
  - Automated Trust Anchor rollover is used to keep TAs up to date

Key Rollover Process

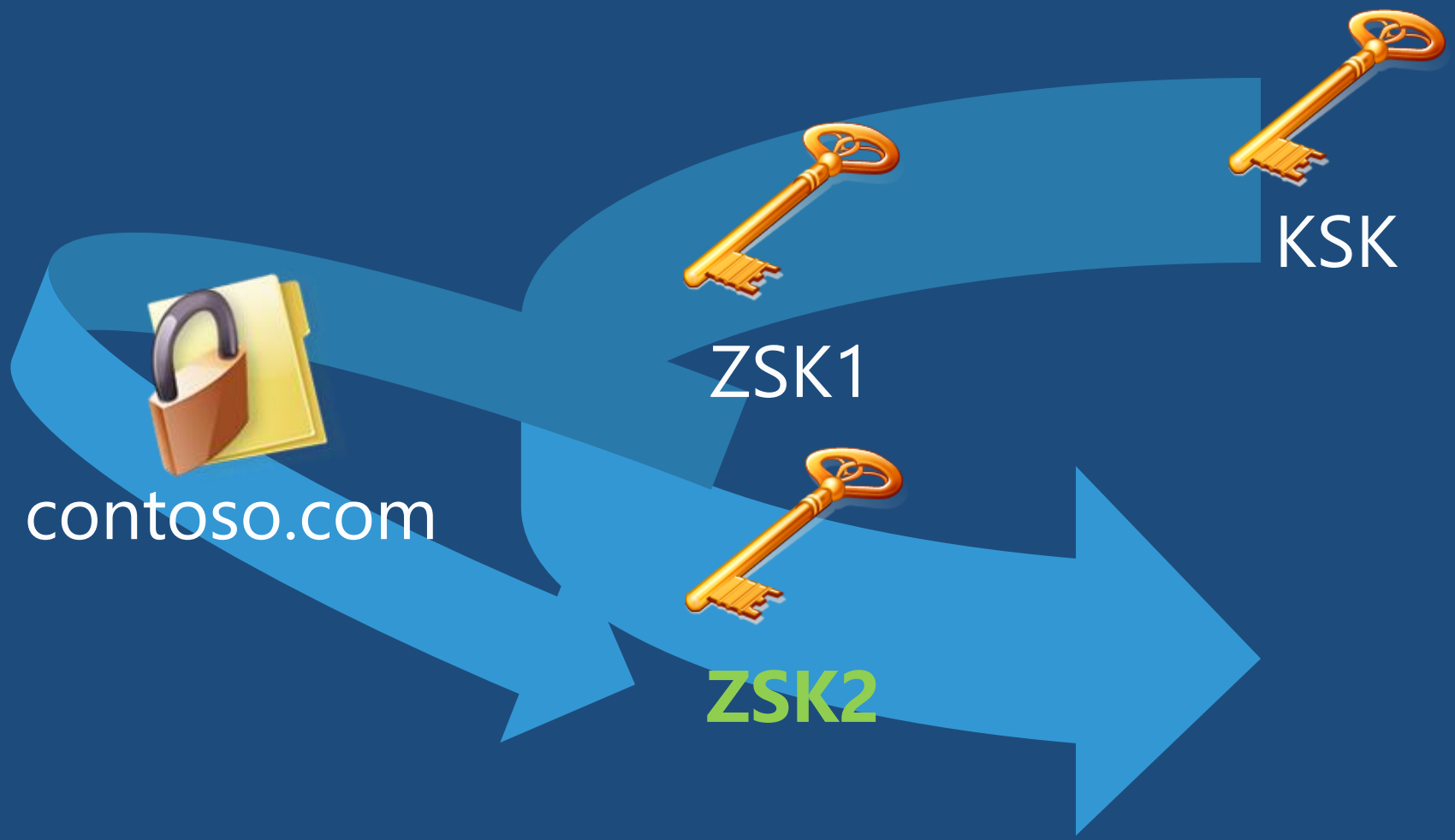
Overview ✓ | Deployment ✓ | Operations | New in DNS

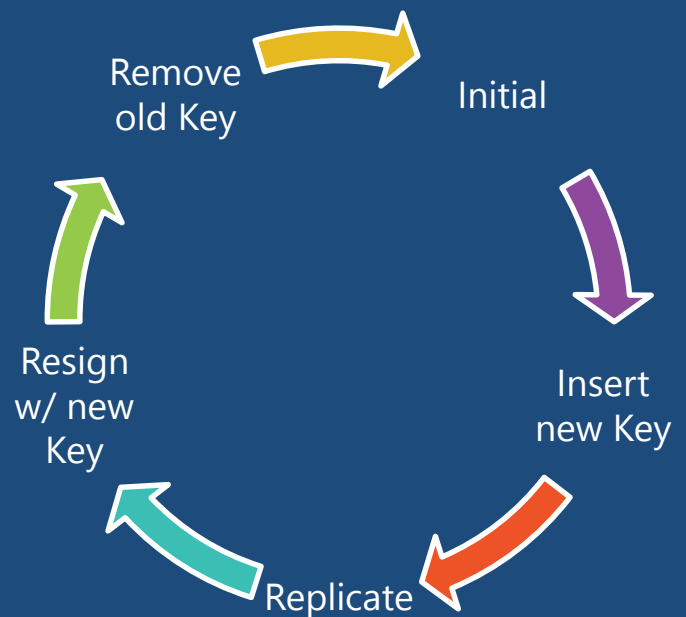




Key Rollover Process

Overview ✓ | Deployment ✓ | Operations | New in DNS



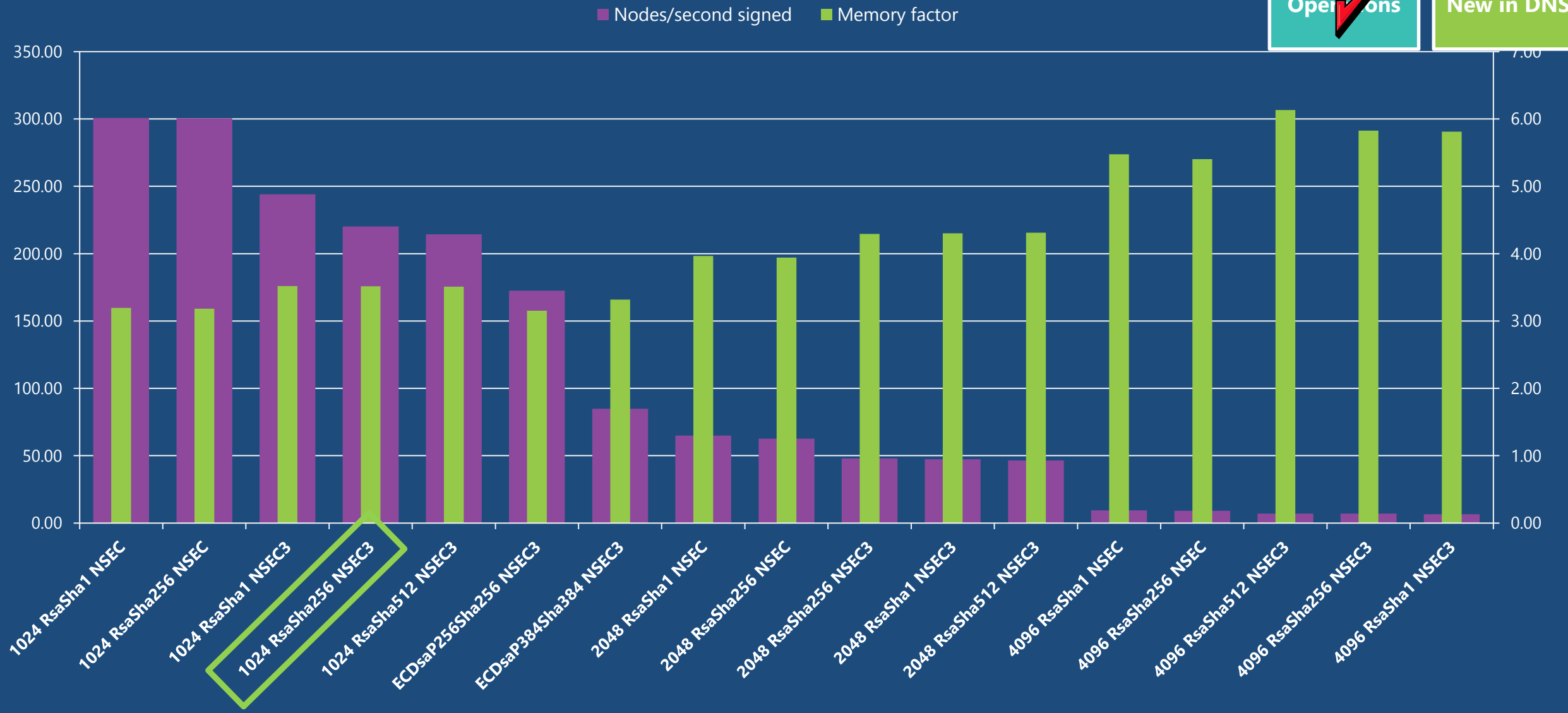


Key Management has low TCO

- Automated key rollovers
  - Key rollover frequency is configured per zone
  - Key master automatically generates new keys and replicates via AD
  - Zone owners rollover keys and re-signs the zone
  - Secure delegations from the parent are also automatically updated (within the same forest)
- Signatures stay up-to-date
  - New records are signed automatically when zone data changes
    - Static *and* dynamic updates
    - NSEC records are kept up to date

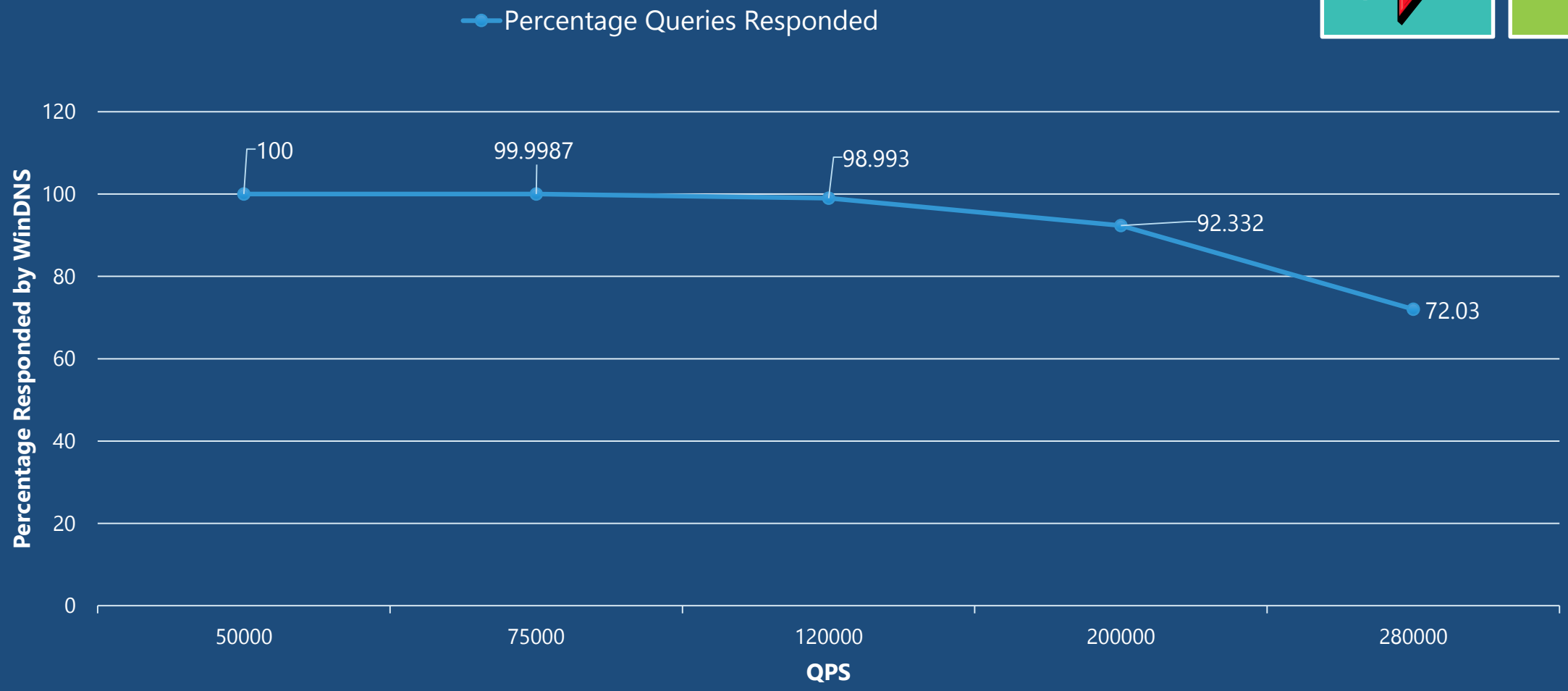
DNSSEC signing performance

Overview ✓ | Deployment ✓ | Operations ✓ | New in DNS



Windows Server 2012 R2
DNS performance

Overview ✓ | Deployment ✓ | Operations ✓ | New in DNS



New in DNS for Windows Server 2012

- IPAM
- PowerShell cmdlets
  - Near parity with dnscmd.exe
- Dynamic re-ordering of forwarders
  - Server now picks the forwarder that is responsive over the ones that are not responsive
  - Basically, unresponsive forwarders are dropped to the bottom of the list for successive queries
- WINS Support for DNSSEC

Summary

- Easy to deploy
- Smart defaults
- Automated management for day to day operations
- Standards compliant
- High Performance