

DNSSEC

Podpora v MS Windows



Miroslav Knotek, Microsoft MVP
IT Senior Consultant | KPCS CZ, s.r.o.

knotek@kpcs.cz | www.konzultant.net | www.kpcs.cz

Agenda

- DNSSEC a Windows 2003/2008
- DNSSEC a Windows 2008 R2
- DNSSEC a Windows DNS klient
- Demo: podpis zóny

DNSSEC a MS Windows 2003/2008

- Implementace dle zastaralého RFC 2535
- Nekompatibilní s Windows 2008 R2
- Neověřuje
- Chybí nástroje pro kryptografické operace
- Pouze jako sekundární DNS server

DNSSEC a MS Windows 2008 R2

- Implementace dle RFCs 4033, 4034 a 4035
- Obsahuje nástroj pro offline podpis zóny
- Provádí ověření dle RFC
- Umožňuje spravovat a konfigurovat "Trust Anchors"

DNSSEC a MS Windows 2008 R2: požadavky

- Zóna musí být statická, při každé změně znovupodepisování celé zóny
- AD integrated zónu je nutno exportovat před podpisem do souboru zóny
- Nepodporuje WINS Forwarding ani GlobalNames zónu
- Podporovaná kryptografie
 - RSA 512 – 4096 bitů
 - SHA 1

DNSSEC a Windows DNS klient

- Windows 7 / Windows Server 2008 R2
- “Non-validating security-aware stub resolver”
- Bezpečnost komunikace DNS Server <-> DNS klient pomocí IPSec
- Ověřování DNSSec vynuceno pomocí politik NRPT v GPO

DNSSEC a Name Resolution Policy Table (NRPT)

Create Rules

To which part of the namespace does this rule apply?

Suffix:

Certification authority: (Optional)

DNSSEC

☒ 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:

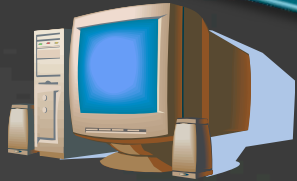
☒ Use IPsec in communication between the DNS client and DNS server

Encryption type:

Jak to funguje ?

NRPT

*.kpcs.cz IPSec DNSSEc



Chráněno IPSecem



Trust Anchors

kpcs.cz
microsoft.cz

1

www.kpcs.cz DO

www.kpcs.cz A: 200.1.1.1 AD RRSIG

IPSec

2

www.test.cz

www.test.cz A:200.1.1.10



Windows Server 2008 R2

DEMO: DNSSEC – PODPIS ZÓNY

