DNSSEC v kořenové zóně

CZ.NIC z.s.p.o.
Ondřej Surý
ondrej.sury@nic.cz
7. 6. 2010

cz nic
správce domény cz

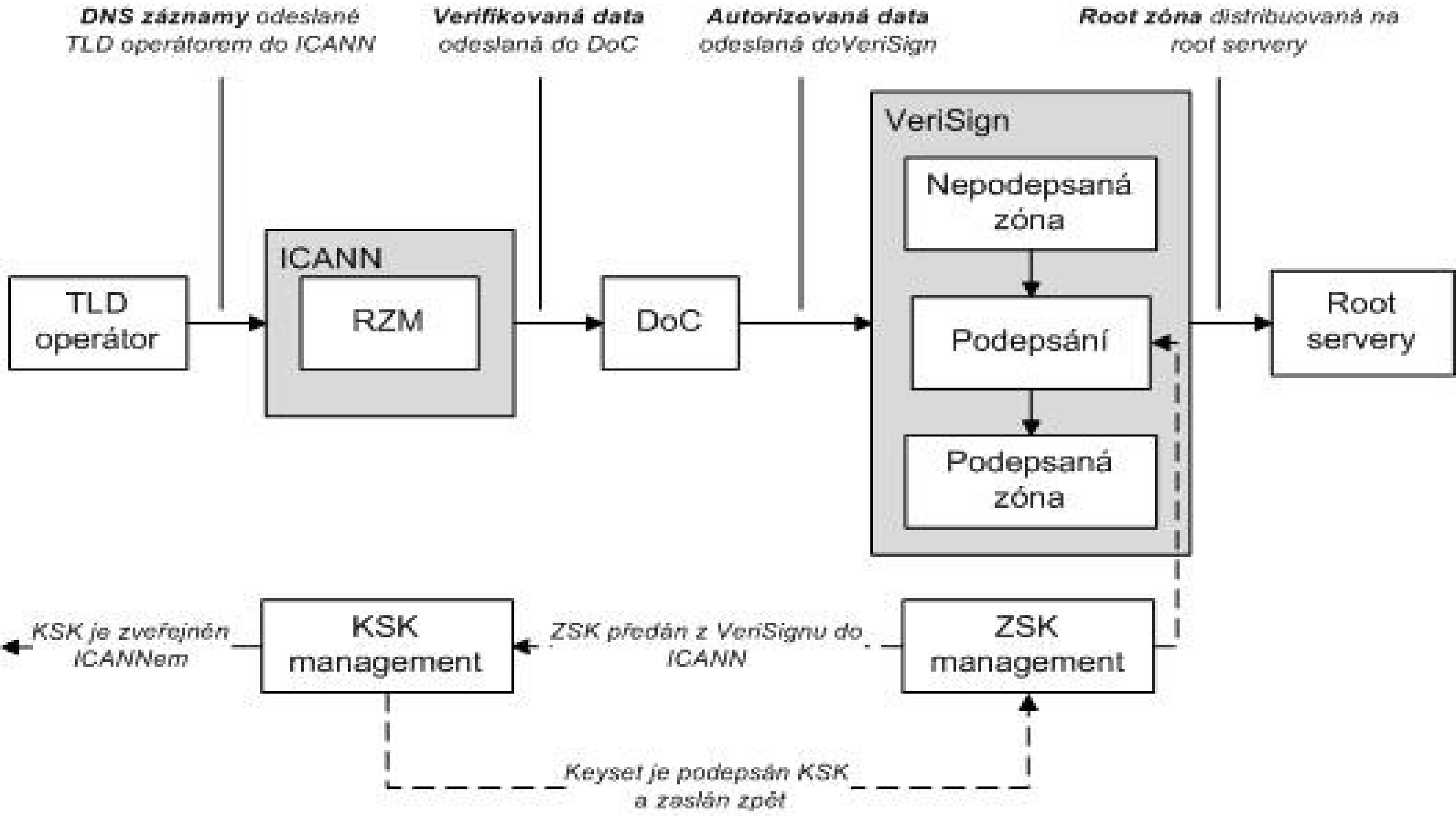
Co je to DNSSEC?

- Přidává do DNS podpisy
- Nezajišťuje soukromí
- Zajišťuje autenticitu
- Nové typy DNS záznamů
  - RRSIG, NSEC/3, DS, DNSKEY

Rychlý přehled podpisu k.z.

- Web: www.root-dnssec.org
  - Dokumenty, novinky, atd.
- Podpis kořenové zóny (DNSSEC)
  - Algoritmus RSA-SHA256
  - Délky klíčů: 2048 bitů (KSK); 1024 bitů (ZSK)
- Postupné nasazení (skoro hotovo)
- Záměrně nevalidovatelná kořeno
  - DURZ (Deliberately Unvalidateable

Rozdělení rolí



Postupné nasazení

- Postupné nasazení na všechny NS
- Všech třináct jmenných serverů má DURZ
  - 27. ledna 2010 (první – L.root-servers.net)
  - 10. února 2010 (A)
  - 3. března 2010 (M, I)
  - 24. března 2010 (D, K, E)
  - 14. dubna 2010 (B, H, C, G, F)
  - 5. května 2010 (poslední – J.root-servers.net)

Dopady nasazení

- ...

Trusted Community Representatives

- Zvýšení důvěry v proces podpisu
- 14 Crypto Officers (CO)
  - 7 východní pobřeží USA
  - 7 západní pobřeží USA
- 7 Recovery Key Share Holder (RKSH)
- Účastní se KSK ceremonie
  - Nahrávka, audit
- Generování KSK, podpis ZSK

TCR – Crypto Officers

- Mají v držení klíče
- V trezoru jsou uloženy smart card pro aktivaci HSM
- Pro aktivaci musí být přítomni 3 ze 7 CO

Recovery Key Share Holders

- Mají v držení SC kartu
  - Uložena informace o zašifrovaném KSK
- ICANN má záložní KSK
- Pro obnovu je potřeba:
  - nové HSM
  - 5 ze 7 RKSH
  - záložní KSK

Výběr TCR

- CO – musí být schopni cestovat 4 krát ročně
- RKSH – musí být schopni cestovat rychle
  - doufejme, že nebudou muset nikdy
- Nesmí být propojeni na žádnou organizaci spravující kořenovou zónu (ICANN, VeriSign, DoC)
- Geograficky distribuováni
- Respektovaní členové DNS komunity

Výběr TCR

- 61 kandidátů
  - AfriNIC – 4
  - APNIC – 12
  - ARIN – 20
  - LACNIC – 5
  - RIPE – 20
- Vybráno 21
  - Zatím neveřejný seznam

Další kroky

- 16. června 2010 – První KSK ceremonie
  - Culpeper, VA (východní pobřeží)
  - 7 CO + 7 RKSH
- 12. července 2010 – Druhá KSK ceremonie
  - El Segundo, CA (západní pobřeží)
- 15. července 2010
  - Publikace validovatelné podepsané kořenové zóny
  - Publikace pevného bodu důvěry pro k.z.
  - Publikace TLD klíčů (DS záznamů)

Questions?