.CZ in the DNSSECland

CZ.NIC
Ondrej Sury / *ondrej.sury@nic.cz*
20. 10. 2008

cz nic
cz domain registry

Peek into a rabbit hole

- What we have now?
- What troubles we had?
- What troubles we still have?
- What is still missing?

Where we are now...

- .0.2.4.e164.arpa signed in April '08
- .cz signed in September '08
- Signing still only in SW
- EPP interface launched on Sep 30
- **205** secure delegations in first **20 days**
- 5 registrars
- 177 DS from one registrar
- 14 from CZ.NIC

Problems encountered

- AXFR & IXFR
- HSM support pain
- Bugs in tools

XFR troubles

- .cz fully generated on each run
- ~500.000 domain names
- Don't even think about AXFR
- Don't even think about full resigning
- Prepare to throw some money on memory

XFR troubles – plain AXFR

- .cz regenerated every 30 minutes
- .cz zonefile size: 40MB
- .cz.signed zonefile size: 180MB
- 19 slave nodes around the world
- ~3.5GB every 30 minutes to download
- Got some calls from upstream provider ;)

XFR troubles – does IXFR help?

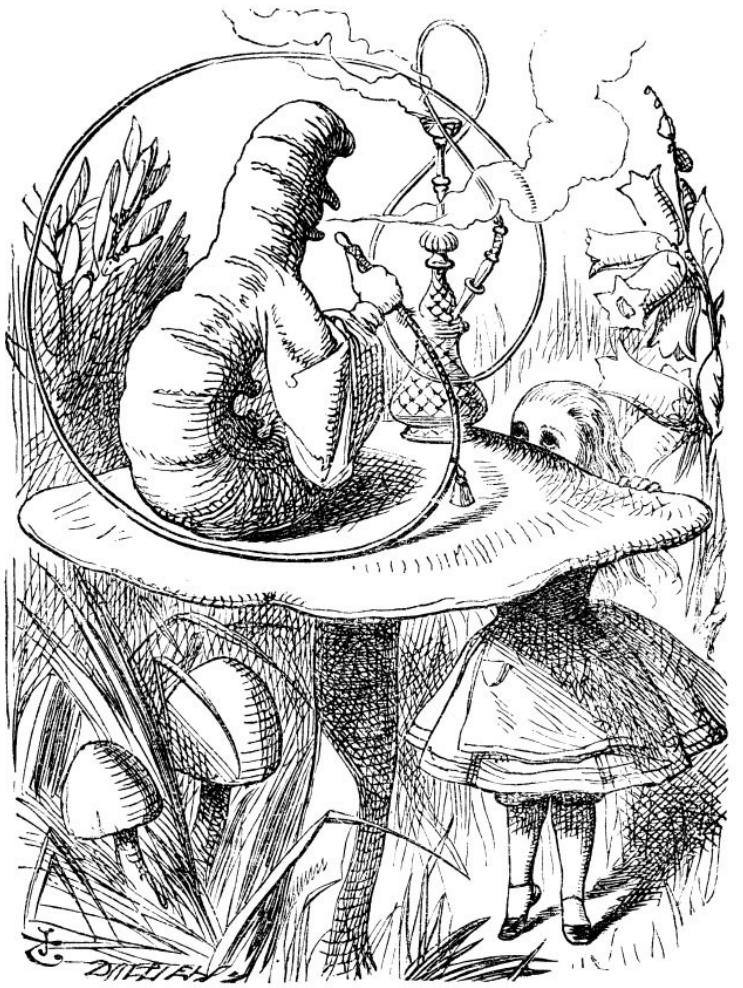
- NO
- .cz fully generated on each run
- IXFR size even bigger then AXFR
- What changes we need to send?
  - Remove all RRSIGS
  - Add all RRSIGS
- HUGE

XFR – both AXFR and IXFR

- Huge data transfers
- Huge journal sizes
- Disk space requirements grows
- Memory requirements grows

XFR troubles - solution

- Reuse old signatures!
- Merge old signatures from previous cz.signed
- Had to write tool for merging newly generated zone and old signatures
  - Based on ldns (merged into ldns-read-zone)
- Everything is ok now



HSM – SCA6000 and software

- Supported only on Solaris (and some ancient RHEL)
- Maximum RSA key size is 2048
- Bind 9.6: New and updated tools (needs patched OpenSSL)
  - dnssec-keyfromlabel – should generate key from RSA on card
  - contrib/pkcs11-keygen/ – should generate new key on HSM
  - dnssec-signzone – supports new .private key format
- nsigner5 (interfaces PKCS#11 directly)
  - Bunch of tools + patched Bind
- ldns (patched OpenSSL)
  - ldns-signzone support openssl engines (including pkcs#11)

HSM – SCA6000 and software

- Does it work?
  - No
  - Blame the Solaris ;)
  - Small user base
  - Not well tested
  - Working with ISC and others to have it fixed

Other bugs found

- LDNS
  - ldns-signzone broken (fixed in r2764)
  - library cripples DS records with space (fixed in r2748)
  - upstream very responsive (Jelte must regret he gave me his jabber ;)
  - tools are meant to be just examples
  - library and tools are slow (very slow) sometimes

Key maintainance tools

- dnssec-tools.org
  - easy to use (zonesigner -genkeys <zone> and you're ready)
  - designed for small zones (will eat all your memory, uses my $file)
  - doesn't properly check return codes of system() calls
  - maintainer unresponsive :(
- ZKT
  - looks nice, small and easy to use enough
  - maintainer responds to my emails
- DNSSEC Key Management Tools (RIPE NCC DISI)
  - needs bunch of Perl modules
  - complicated to setup

What needs to be done

- Documentation has to get better
- Tools have to get better and easier to use
  - One “click” should be enough
- One more reference implementation
  - Fast and with same CLI as Bind9 tools
- Bugs need to be fixed ;)

Questions?