.CZ in the DNSSECland

CZ.NIC
Ondrej Sury / *ondrej.sury@nic.cz*
24. 9. 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
- .cz automatically signed in September
- Signing still only in SW
- EPP interface launches on Sep 30

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?

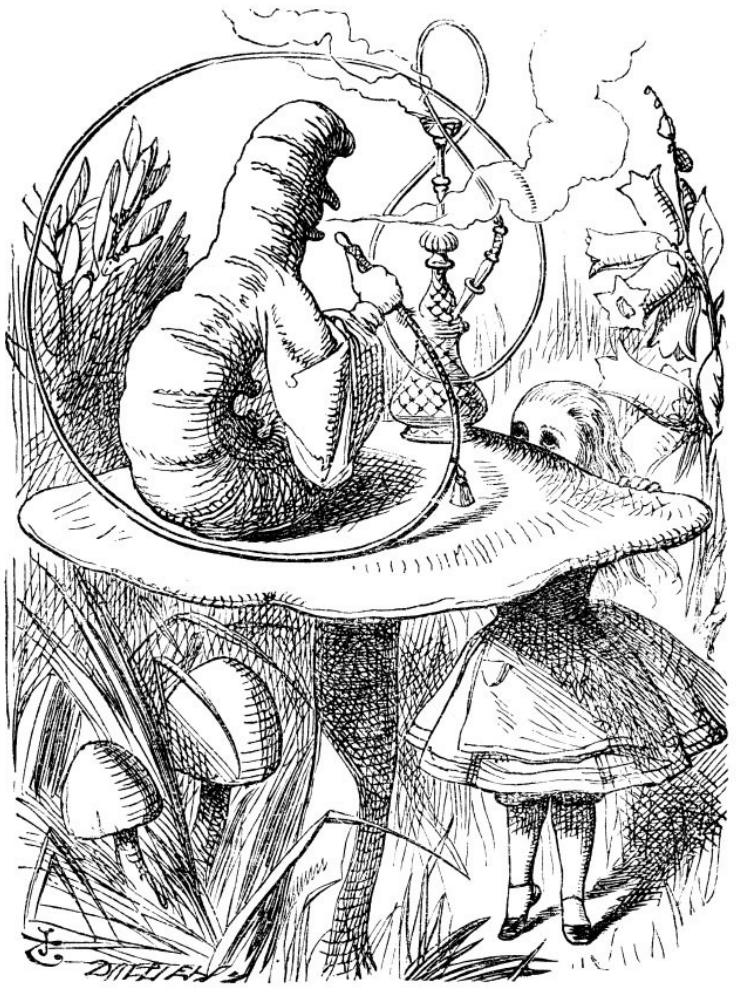
- NO
- IXFR sizes even bigger then AXFR
- What changes we need to send?
  - Remove all RRSets
  - Add all RRSets
- HUGE

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
  - ldns-merge-dnssec
  - (NLNet #212)
- Everything is ok now



HSM

- HSM's are cool
- HSM's are unsupported
- Tools available:
  - Bind 9.6 CVS
  - nsigner (from Rick Lamb)
  - LDNS
- Tools are very rough at the edges

HSM – Sun SCA6000

- Supported only on Solaris and some prehistoric RHEL
- Maximum RSA key size is 2048
- Need to patch OpenSSL
- Or use engine_pkcs11 from OpenSC project

HSM – Bind 9.6 CVS

- New tools available:
  - dnssec-keyfromlabel – should generate key from RSA
  - contrib/pkcs11-keygen/ – should generate new key on HSM
- Changed tools
  - dnssec-signzone – supports new .private key format

HSM – dnssec-keyfromlabel

- Looks good, but...

```
# dnssec-keyfromlabel -a RSASHA1 -l cz,zsk,00001 cz
dnssec-keyfromlabel: failed to generate key cz/RSASHA1: out of memory
```

HSM - pkcs11-keygen

- Looks good, but...

```
contrib/pkcs11-keygen# ./genkey.sh -z cz -x 1234 -p $PIN -b 1024 -e pkcs11 -k /tmp
Generating key
C_GenerateKeyPair: Error = 0x00000101
```

HSM - pkcs11-keygen

- Modify to use slots
- Looks good, but...

```
pkcs11-keygen-custom# ./genkey.sh -z cz -x 1235 -p $PIN -b 1024 -s 3 -e pkcs11 -k /tmp
Generating key
Exporting public key
Loading public key slot_3-id_1235
Error loading public key
20518:error:26097081:engine routines:func(151):reason(129):eng_pkey.c:162:
```

nsigner5 (last checkout)

- Looks good, but...

```
# pkcs11-find -P $PIN -S 3 > hsmtable
Using hsmconfig ./sca6000.hsmconfig
PKCS11_LIBRARY_PATH=/usr/lib/libpkcs11.so
Scanning slot 3
70 public keys:
pkcs11: error: C_GetAttributeValue returned 0x00000012
pkcs11: error: C_GetAttributeValue returned 0x00000012
[...]
# ./kgen cz
GMT:20080923081244 DN:cz Keyindex file:cz.keyindex Key bundle dir:fob Key
bundle file:fob/cz.keybundle Key log file:fob/cz.keylog Temp file:20533.tmp
Timings KSK_EFFECTIVITY_PERIOD:365 days ZSK_EFFECTIVITY_PERIOD:30
days ZSK2_EFFECTIVITY_PERIOD:14 days DEFAULT_TTL:3600 secs
MAX_TTL:15 secs MIN_CLOCK_SKEW:1800 secs
error: Could not find key in hsmtable.  Update hardware configuration.
error: KSK key generation failed for cz
```

HSM - LDNS

- Had some success with LDNS
- ldns-signzone -k <id>,<int>
- Looks good, but...
- ldns-signzone is/was buggy (fixed in SVN, bug #210)
  - signs NS records when it shouldn't

Other bugs

- LDNS
  - library cripples DS records with space (#213)
- dnssec-tools.org
  - zonesigner cannot be configured to run 'named-checkzone -i none' after signing
  - zonesigner refuse to sign already signed zone
  - some more bugs reported by users (typo in rollerd)
  - I have to report those bugs yet

What needs to be done

- Documentation has to get better
- Tools have to get better and easier to use
- Bugs need to be fixed ;)

Questions?