DNSSEC deployment in .cz & 0.2.4.e164.arpa

CZ.NIC
Ondrej Filip / ondrej.filip@nic.cz
http://www.nic.cz

5th November 2008 – ccNSO Meeting, ICANN, Cairo

About CZ.NIC

- Founded in 1998

- 57 members – growing (open membership)

- Registry-Registrar model (28 registrars)

- Liberal registration model – no restrictions

- Domains currently

  - .cz   480 000

  - 0.2.4.e164.arpa   4 700

- Fast growth – 36%

- Nameservers IPv4/IPv6, Anycasting

Situation in Czech Republic

- Usually no spam nor phishing in past – users not aware of those issues

- First phishing attacks in Czech language (or translated to Czech) appeared this year

- Largest banks under attack

- Kaminski attack

Conditions

- Available for .cz and 0.2.4.e164.arpa
- Key sharing
    - same keys for multiple domains
    - reduces overhead
- Free of charge
    - not service, but feature
    - within domain registration fee
- Using registrars – no model change
- Fully integrated into FRED http://fred.nic.cz

Conditions

- Operations and security
  - Based on RFCs
  - Keys RSA-SHA1 2048/1024bit
  - High security
- Zone walking problem
  - no personal data disclosed
  - approved by Personal Data Protection Office
  - NSEC3 later
- ISC DLV

Timeline

How it began?

Timeline

29.2.2008   Public announcement – WP issued

28.4.2008   ENUM zone signed

28.4.2008   Final version of WP issued - development started

15.8.2008   Testing for registrars

1.9.2008   .CZ zone signed

30.9.2008   End user registration start

Zones

- Every 30 minutes
- Nameservers memory upgrade
- hardware security modules
- Four Solaris servers
- KSK + ZSK
- Sun Crypto Accelerator 6000 PCI - problems

Current status

- 250 signed .cz domain

- 6 signed ENUM domains

- Supported by largest registrars - special product – "secure domain"

- Large newspaper support - http://www.lidovky.cz

- Some ISPs joined

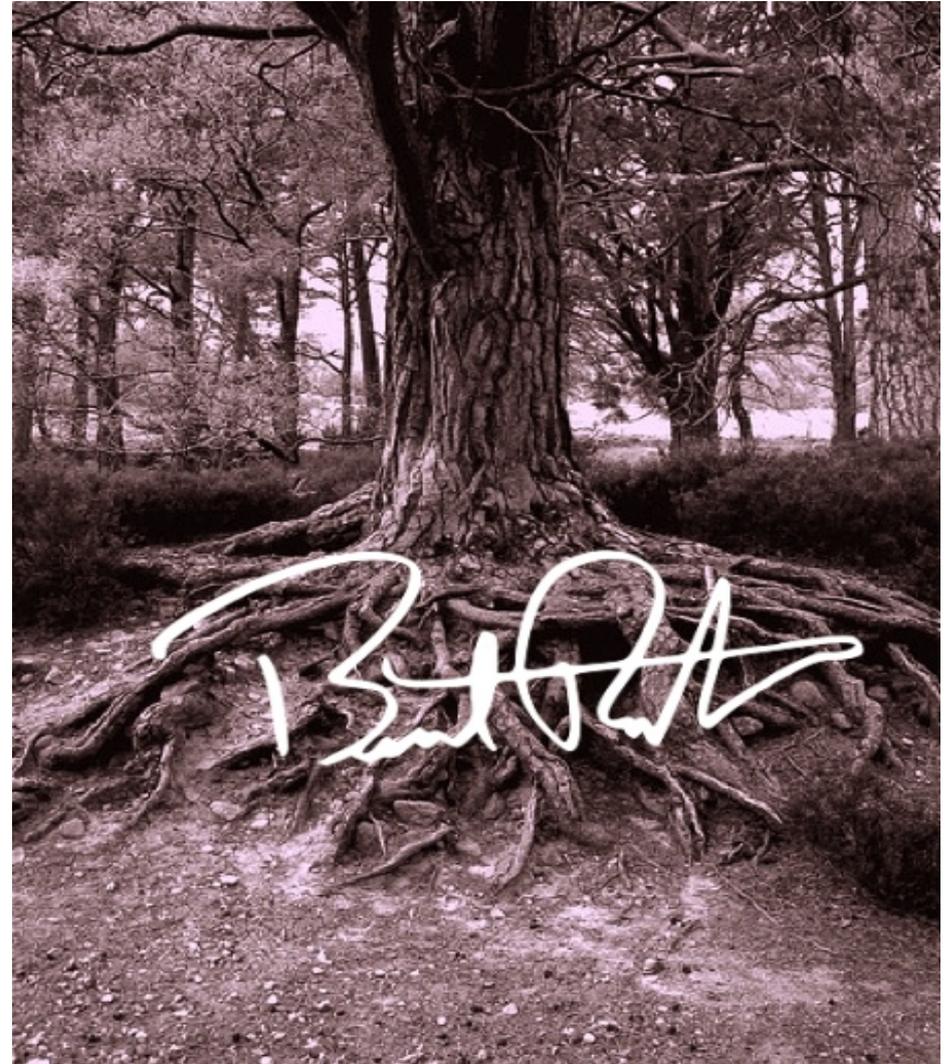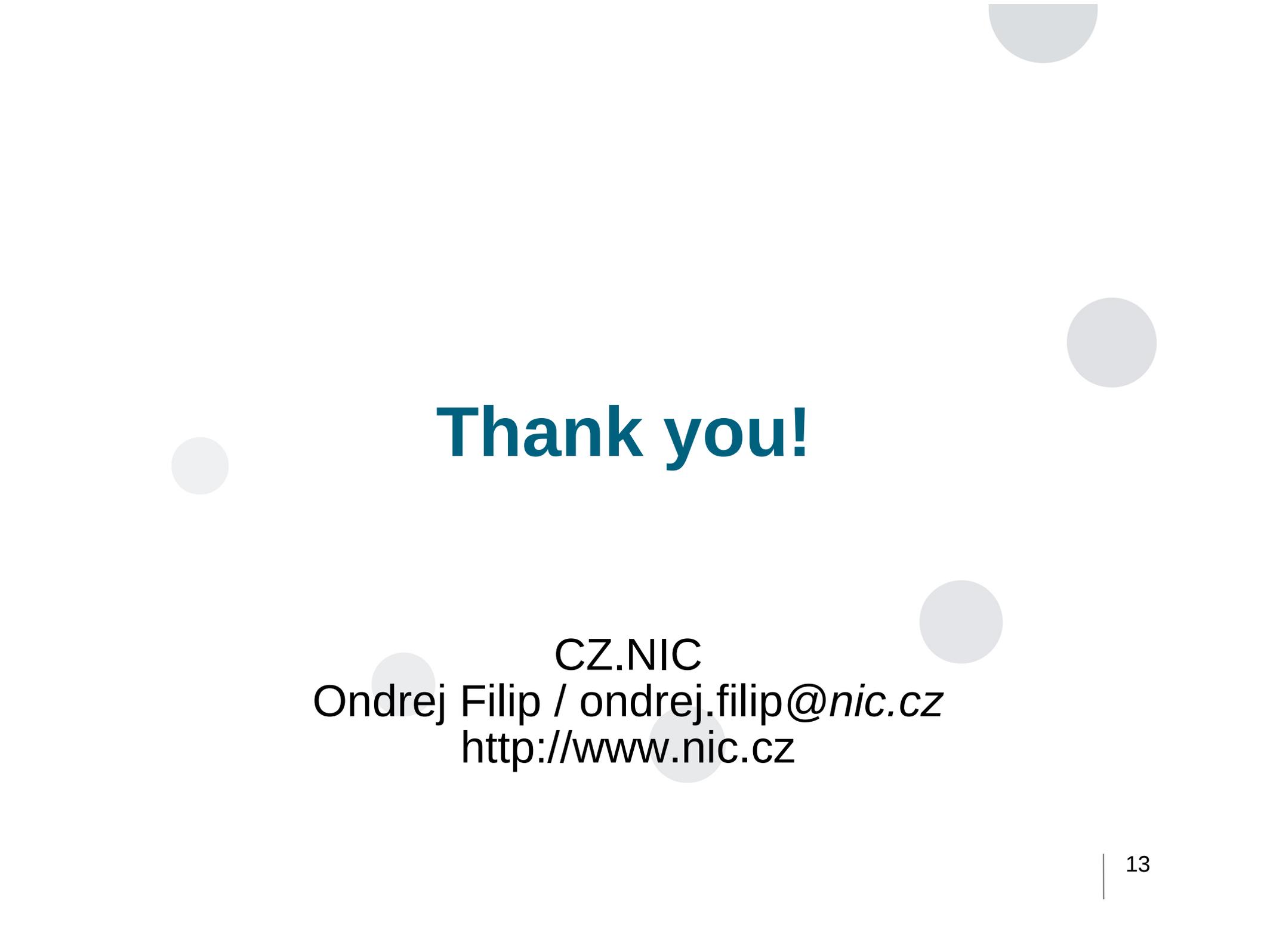- http://www.nic.cz/dnssec - information and simple test

Future work

- Communication
    - Largest ISPs
    - Portals and search engines
    - Large companies – banks, newspapers
    - Government
- Laboratory – dnssec compatibility
- Bugfixing and development
- Education
- Other registries

Sign the root!

- Currently ISC DLV
- ITAR would help

Thank you!

CZ.NIC
Ondrej Filip / ondrej.filip@*nic.cz*
http://www.nic.cz