DNSSEC.CZ

CZ.NIC - http://www.nic.cz
Ondrej Filip / ondrej.filip@*nic.cz*
Dec 8 2010, Cartagena, Colombia
DNSSEC Workshop – ICANN Meeting

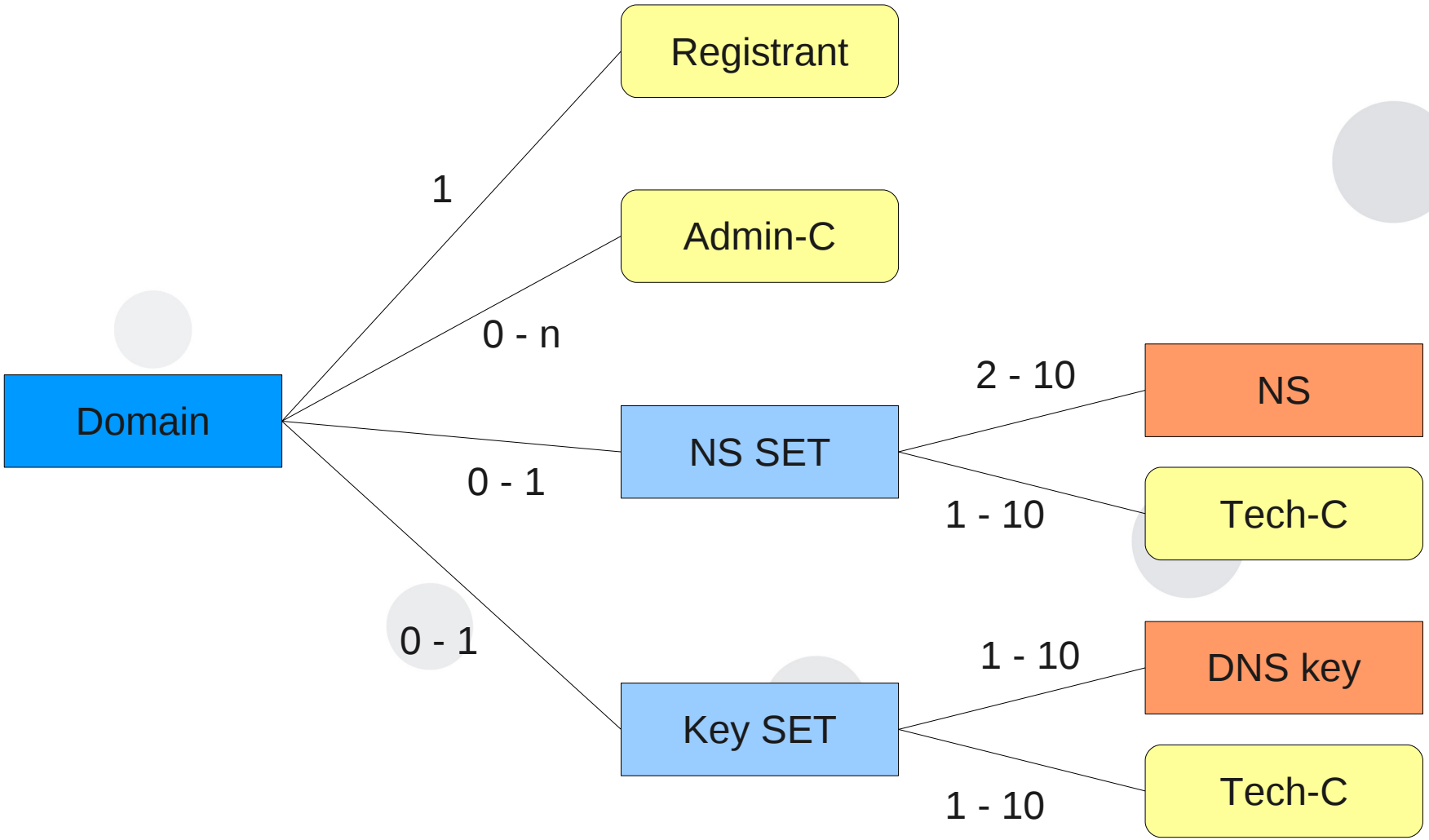
CZ DOMAIN REGISTRY

DNSSEC

High level design

- DNS
  - NSEC3 - RSASHA512
  - KSK - 2048 bits (rollover every 2 years)
  - ZSK - 1024 bits (rollover every 2 month)
  - BIND + ZKT
- Registry
  - Own opensource software Fred – http://fred.nic.cz
  - The same scheme as for domain names registration – registry -> registrar -> registrant
  - EPP protocol
  - Key sharing (next slide)

Design - data structure



Keys can be reused for multiple domains!

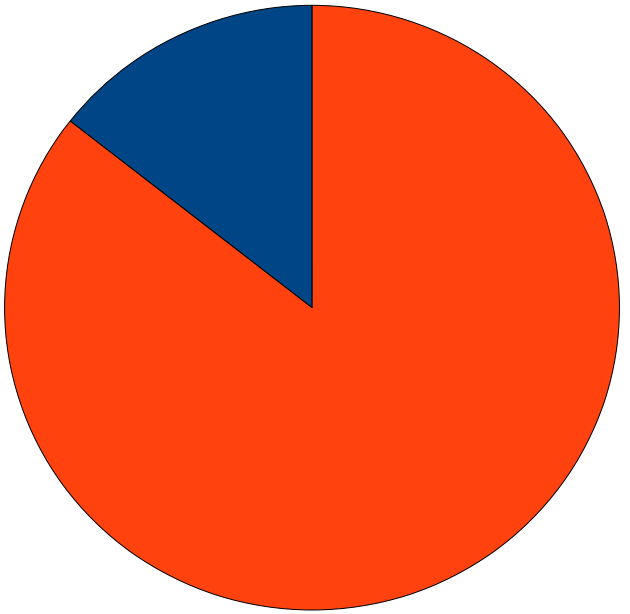
Deployment

- March 3, 2008 - project announced
- April 4, 2008 - ENUM (0.2.4.e164.arpa)

  zone signed – first signed ENUM
- September 2, 2008 – .CZ signed
- September 30, 2008 - .CZ open for end-user public key registration (DS records)
- August 24, 2010 - NSEC -> NSEC3 transition

DNSSEC penetration

- About 15% domains is signed
- That means ~ **109.000** domains! (of 742k)
- Check numbers at http://www.nic.cz
- Default by two registrars – Active24, Web4U
- More to come



Challenges

- Technical (easy)
  - Lack of sw support, bugs in implementation (2008)
  - Larger zone, IXFR, signature reusing
- Communication
  - DNSSEC “invisibility” - Firefox DNSSEC Plugin
  - Communication with end users (companies, press, government – eu2009.cz) - campaigns
  - Registrars – no additional fees, advantages registrars supporting DNSSEC – co-marketing -> DNSSEC enabled by default
  - ISPs - validation

Lessons & conclusions

- Registry responsibility
- Security is not a special service, it is a feature, natural part of domains
- Need to find allies - ISPs, registrars, content providers, endusers – communication is very important
- DNSSEC can be deployed at larger scale
- Plan your DNS infrastructure
- Test, test, test...
- Registrars with more TLDs (e.g. .cz + .eu)

Thank you

Ondrej Filip

ondrej.filip@nic.cz

http://www.dnssec.cz