

# DNSSEC – Facts or fiction?

CZ.NIC  
Pavel Tuma  
*pavel.tuma@nic.cz*  
4. 3. 2009



# No DNSSEC, because ...

- No business model?
- Useless until majority of domains is signed?
- Registrars not interested?
- End users not interested?
- Too complex to explain?
- End user complaints and confusion?
- True? ... let's find out!

# Business models

- Three experienced business models
- Cross-sell / up-sell
- System integration
- Training & education

# Business models

## Cross-sell / up-sell

- DNSSEC = complementary service to DNS hosting
- Key & signatures management
- Active24
  - .CZ market share 18 % (#2)
  - “Secure domain” service
  - DNSSEC + notifications
  - 2 EUR / year (25% of domain price)



# Business models

## Cross-sell / up-sell

- Reasons (benefits expected)
  - broad service portfolio
  - competitive advantage
  - revenues and margins increase
- Costs: **14 mandays** for internal development!
- Communication so far
  - Press release
  - Website promotion
  - Newsletter promotion
  - Dealer channels

# Business models

## Cross-sell / up-sell

- Results?
- 500+ domains w/ DNSSEC
- 80 domains per month
- Evaluation: Success!
  - Service up and running
  - Media attention gained
  - Target revenues goal reached
  - ROI 4 months

# Business models

## System integration

- DNSSEC = feature to provided as service
- Outsourcing deployment projects
- NTVAGE
  - Outsourcing web sites operation
  - DNSSEC for media group w/ 50 domains
- Reasons (benefits expected)
  - References & visibility
  - Extra revenue

# Business models

## Education & training

- DNSSEC = new topic with very few experts
- Training courses
- Training by CZ.NIC
  - One day training
  - How to deploy DNSSEC for BIND/Unbound
- Results
  - Three trainings
  - Fully booked within 48 hours



# Business models

## Other?

- DNSSEC = enabler of new products/services?
- Innovation?
- Example
  - SSL for internal service
  - Self-signed vs. CA signed SSL certificate?
- Self-signed certificates stored DNSSEC secured DNS
  - Trusted domain name (WHOIS validation)
  - Chain of trust
  - Higher security than entry-level CA signed certificates!

# Majority does not matter

- Don't worry whether there are 5 or 5 millions signed domains
- Content not worth to be attacked ... no need to be secured
  - Personal pages?
  - Blogs?
  - Life-style sites?
  - ...?
- Matter of opinion!
- **Provide the infrastructure ... do not judge**

# Registrars supporting DNSSEC

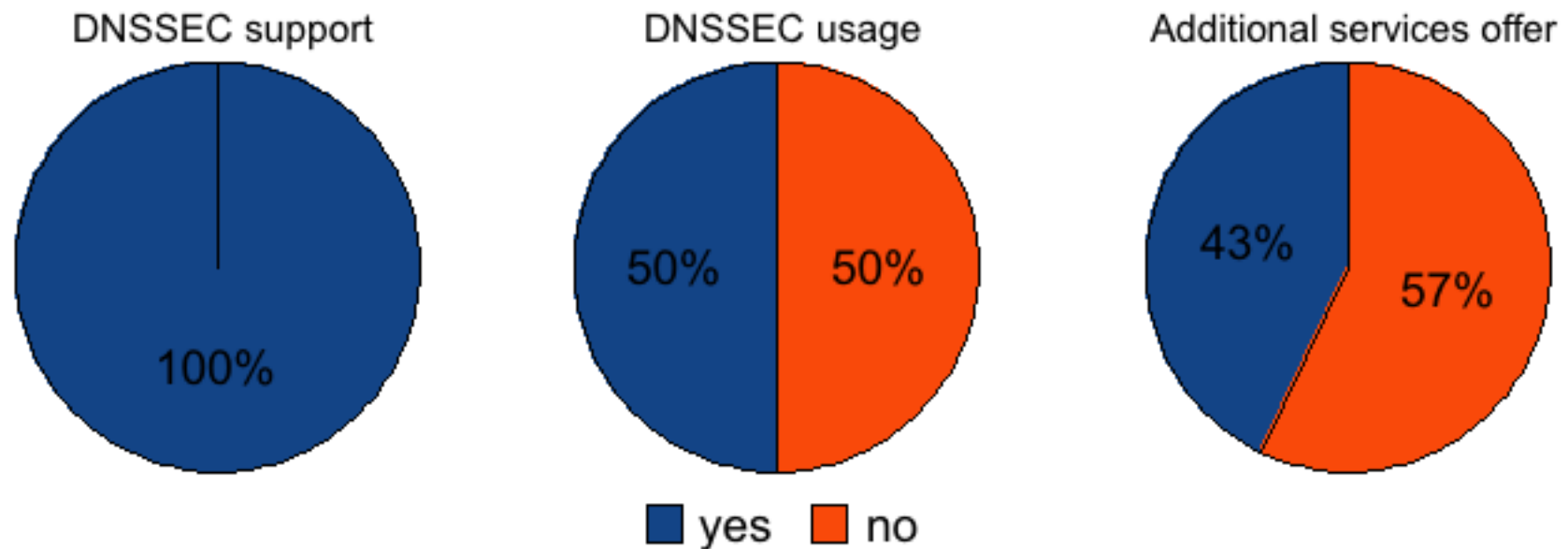
## Why? How many?

- What does it mean to “support DNSSEC” ?
- DS records manipulation ability
  - DNSKEY
  - More complex, but advantage for end user
- **One extra field in registration page!**
- Really need all of them?
  - One is enough ...
  - End users voice: we will change our registrar!

# Registrars supporting DNSSEC

## .CZ experience

- Intro: 6 months before launch
- Final milestone: full testing system 1 month before launch
- Mini research - “What do you plan?”

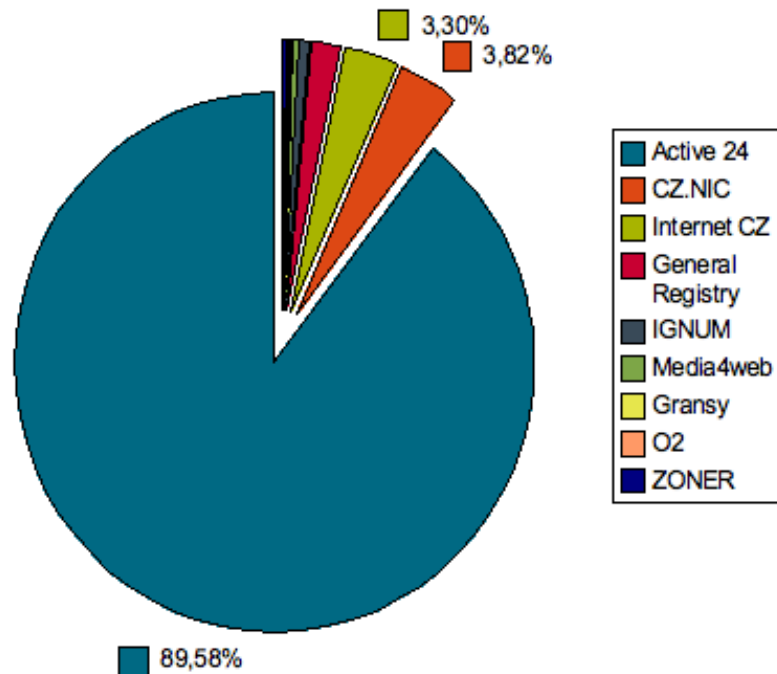


- Launch: 3 registrars (covering 40% of the market)

# Registrars supporting DNSSEC

## .CZ experience

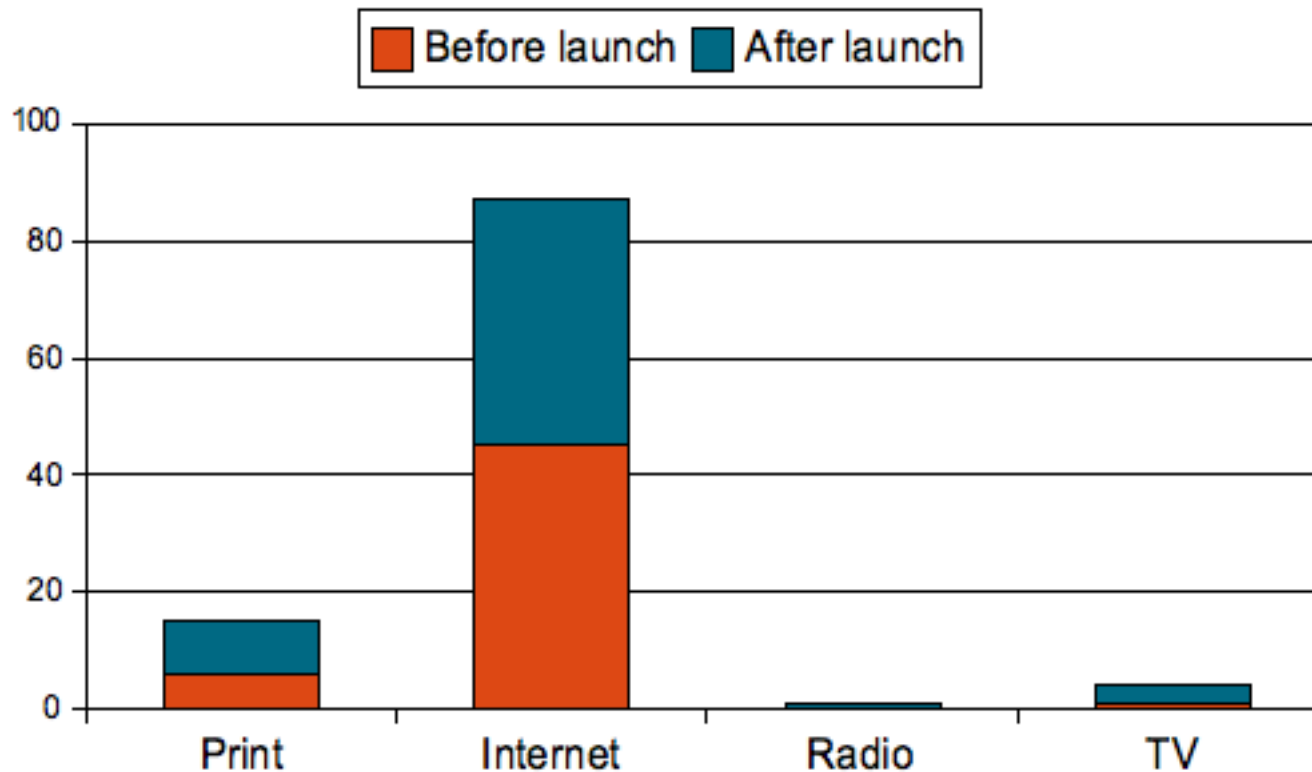
- 6 months after: 9 registrars (covering 87% of the market)



- All registrars support virtually
  - New software mandatory

# End users interest

- Depends on communication
- Media are keen to inform – security is important!
- DNSSEC coverage in czech media



# End users interest

- Prospective target groups
  - Banks? Partially
  - Media? Yes
  - Government? Partially
  - E-shops? Yes
- Recently announced support



**KB**

**economia**



internet

info

# DNSSEC communication

## How to win hearts and minds

- Hard to explain, but ...
- Show the impacts by examples
  - Real vs. forged pages





# DNSSEC communication

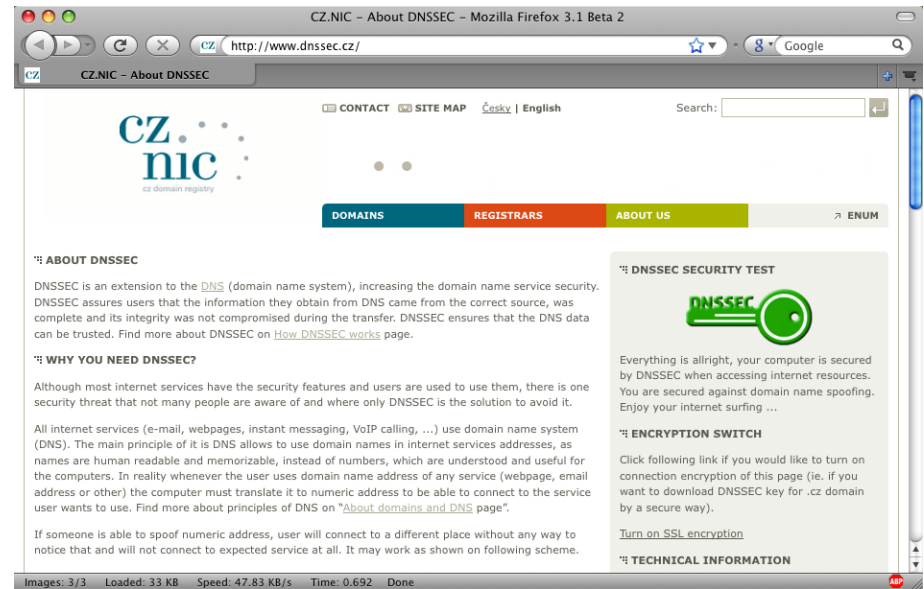
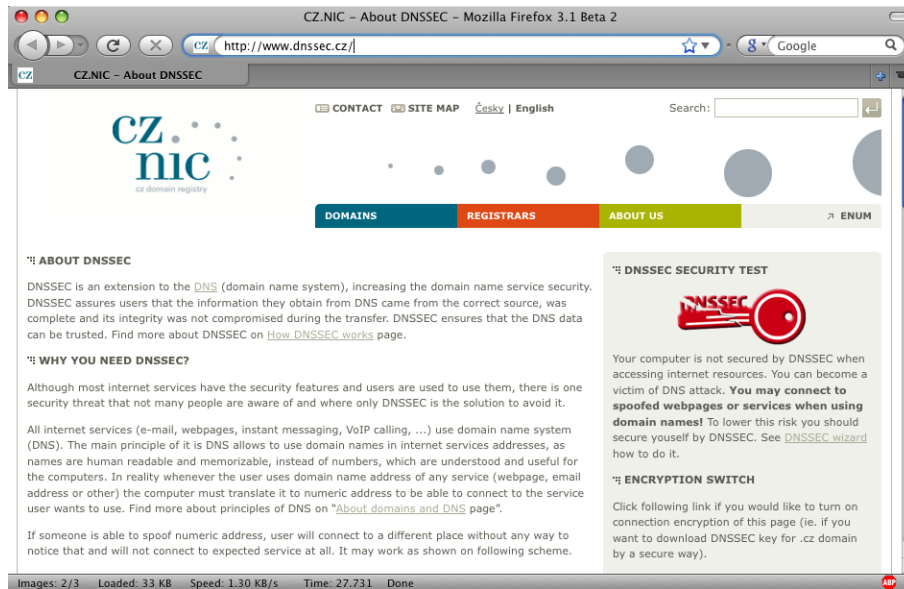
## How to win hearts and minds

- Scare a bit :)
- Attacks are too virtual ... show the numbers
- Brute force DNS attack in CZ.NIC lab
  - 3 nodes over 1 Gbps LAN
  - Minimum time 1:01, maximum time 10:40!
- Show how “difficult” is to launch the attack
- Recalculate it into time/money – everybody understands

# DNSSEC communication

## Tools used/planned for .CZ

- Deployment wizard
  - “How can I secure myself by DNSSEC” guide
- Test page – [www.dnssec.cz](http://www.dnssec.cz)



- DNSSEC brand / logo

# Confusion and complaints

## What if something does not work?

- Fear of keys mismanagement
- DNSSEC is just a tool ... as other technologies
- **Non-accessible service is actually good!**
- Trade off security / simplicity
  
- Does anybody blame these?
  - Anti-viruses
  - VPNs
  - Spam filters



# Thank you

DNSSEC – Facts or fiction?

Pavel Tůma

[pavel.tuma@nic.cz](mailto:pavel.tuma@nic.cz)