

Nové aplikace DNS

CZ.NIC z. s. p. o.

Ondřej Filip / ondrej.filip@nic.cz

4. června 2009 – IT09, Praha

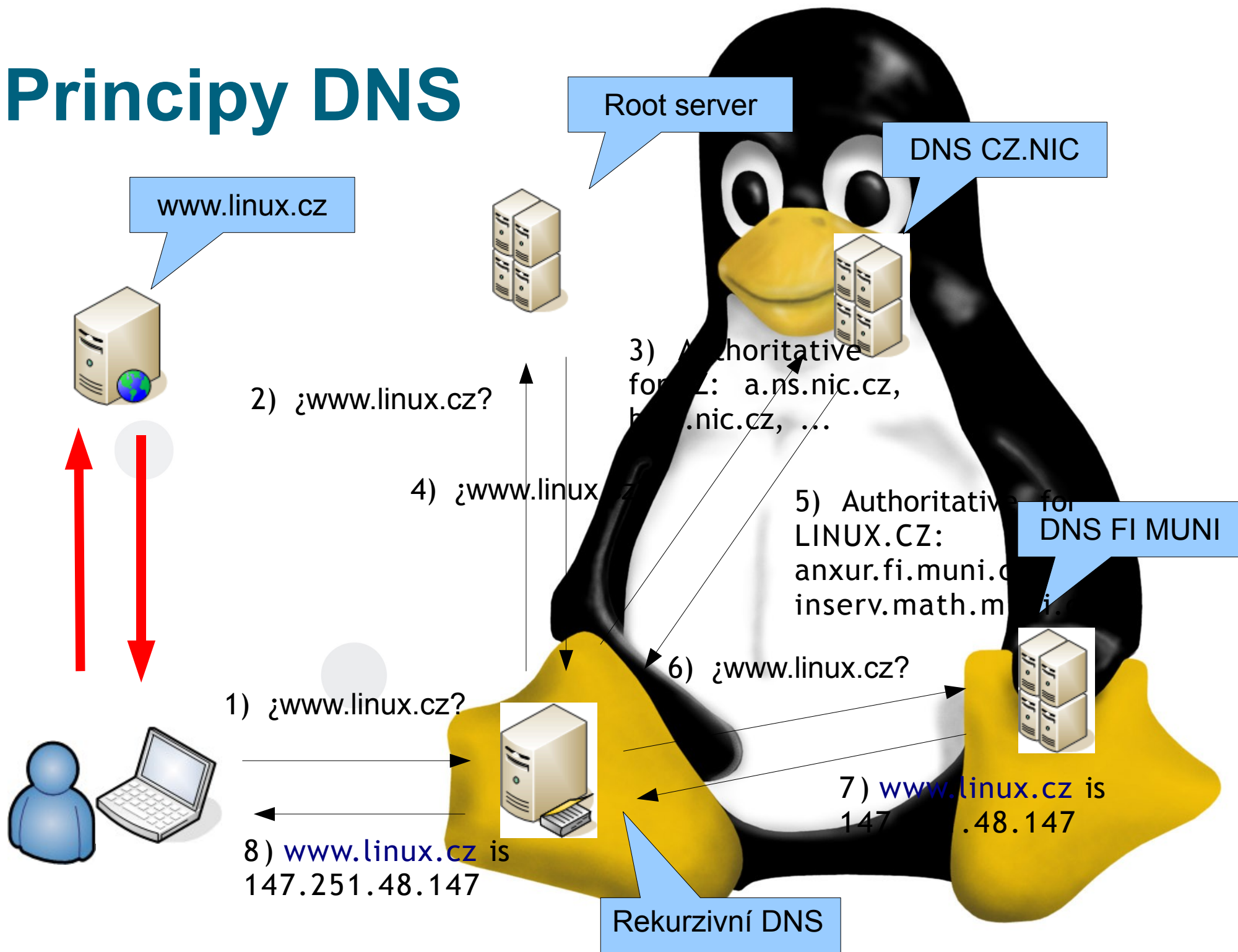


Protokol DNS

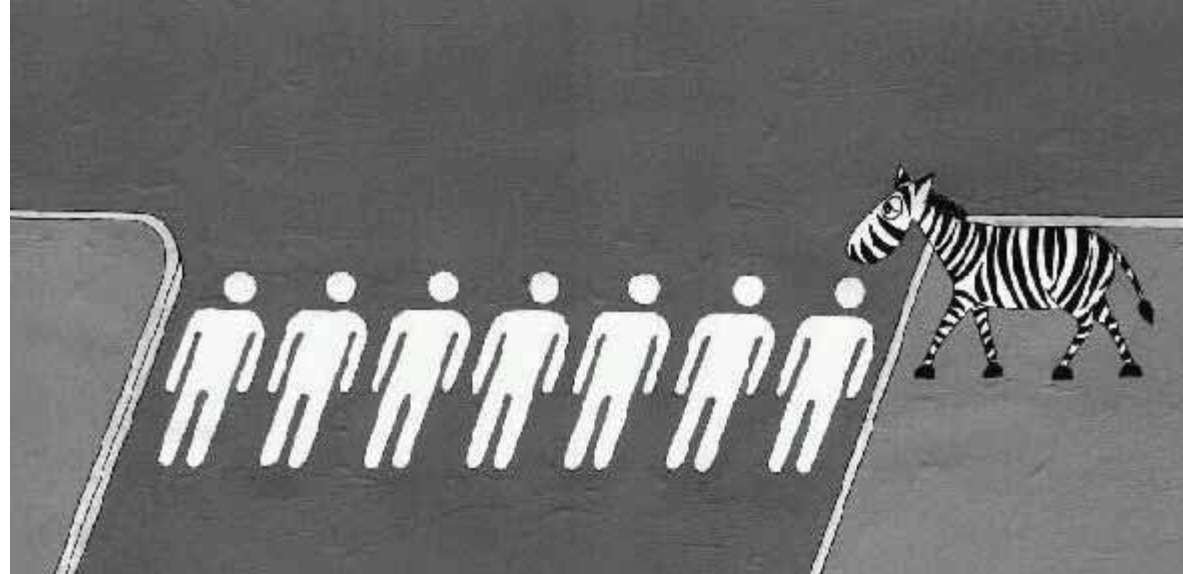


- Navržen pro rychlý překlad jmen na čísla
- Směrování služeb (MX)
- Zpočátku nezabezpečený
- Hierarchická struktura – domény
- `www.nic.cz` -> `217.31.205.50`
- `www.nic.cz` -> `2001:1488:0:3::2`
- MX `nic.cz` -> priority 10 `mail.nic.cz`

Principy DNS



Protokol DNS



- Reverzní DNS

217.31.205.50

-> 50.205.31.217.in-addr.arpa

-> www.nic.cz

- ENUM

+420222745111

-> 1.1.1.5.4.7.2.2.2.0.2.4.e164.arpa

-> "!^.*\$!sip:kontakt@nic.cz!"

e.num
WEMANAGENUMBERS

Databáze DNS

- Úložiště dat (určené strojům)
- Globální veřejná databáze
- Data uvnitř domény spravuje její držitel
- Spolehlivá
- Dříve nezabezpečená
- Nyní - DNSSEC

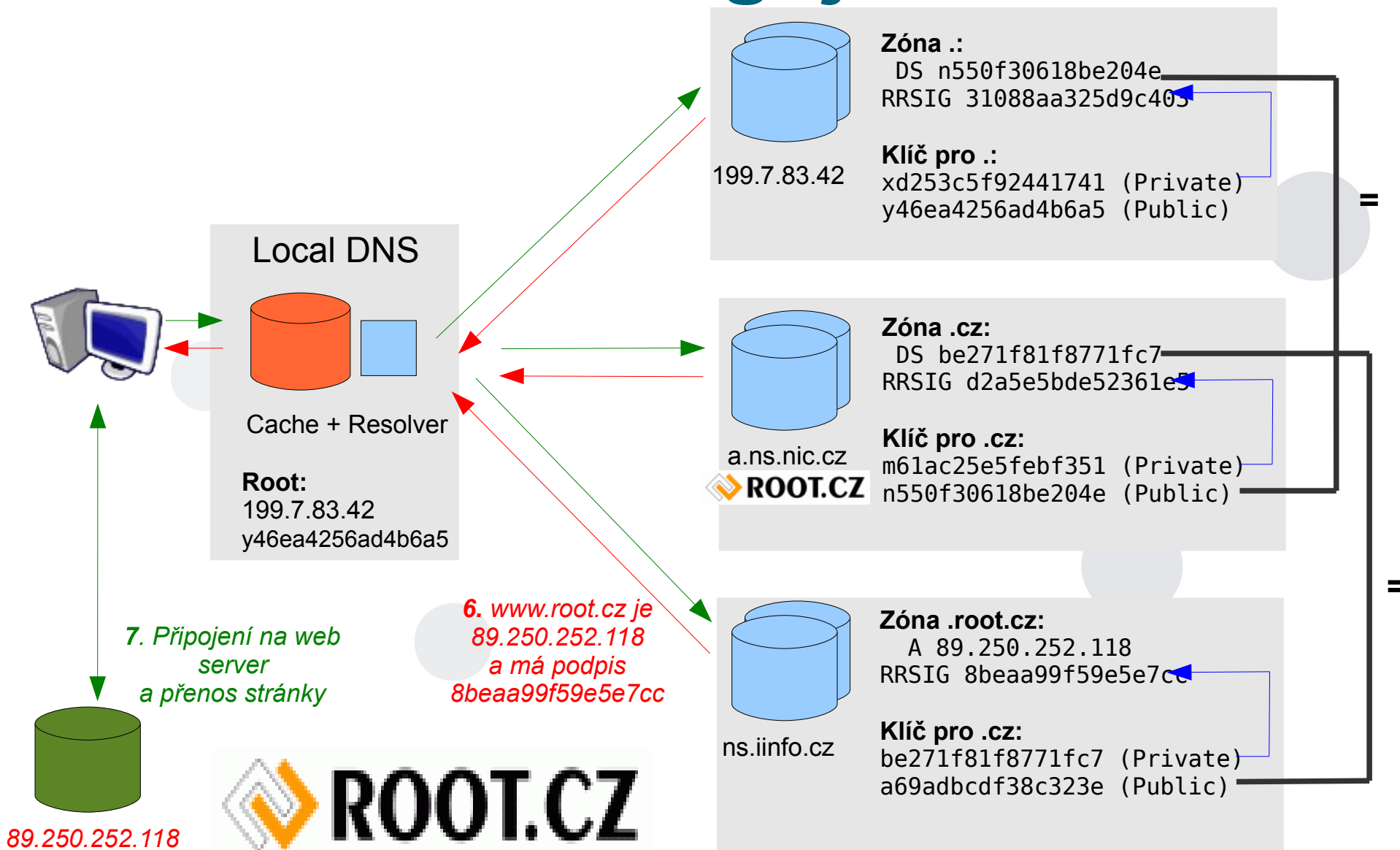


Jak DNSSEC funguje?

- Zavádí do DNS asymetrickou kryptografii
 - Soukromé + veřejné klíče
 - Pro DNSSEC pouze podpis
 - Pomocí veřejného klíče ověřím podpis učiněný privátním klíčem
- Data v DNS jsou digitálně podepsána
- Klíče jsou také uloženy v DNS
- Ověření podpisů se provádí u nadřazené autority (=doména vyšší úrovně)
- Řetěz důvěry – podobně jako u SSL



Jak DNSSEC funguje?



Stav ve světě

- Chybí podpis kořenové zóny
- Včerejší prohlášení – ICANN, NTIA, NIST, Verisign
- Plán mít podepsaný root **V ROCE 2009 (!)**
- 2 „workarouny“ - DLV, ITAR
- 6 ccTLD - .se, .br, .pr, .bg, .cz, .th
- 3 gTLD - .museum; .gov, .org (NSEC3)
- Některé další TLD plánují



Co je nového s DNSSEC

- Žádná viditelná změna pro koncové uživatele
- Žádná viditelná změna v designu DNS
- Co se tedy změnilo?
- Máme bezpečnou veřejnou federativní databázi
- Každý může ukládat záznamy
- Záznamy vkládá držitel domény



Malý příklad SSHFP

```
$ ssh server.nic.cz
```

```
The authenticity of host 'mamlas.feela.net' can't be established.
```

```
DSA key fingerprint is
```

```
14:2b:4b:18:a7:8b:99:1b:e2:2d:52:e2:3e:4d:bc:0f.
```

```
Are you sure you want to continue connecting (yes/no)?
```

Co na to říct?



Malý příklad SSHFP

- SSH login na neznámy server
- Každý ignoruje otázku a píše 'yes'
- Uložme tedy otisk (fingerprint) SSH klíče serveru do DNS
- ```
server.nic.cz. IN SSHFP 1 1
8c211d5b58e625cf61889ffe38b6d082b1c841a3
```
- A už se neptá. :-)
- Ne příliš zajímavé. Ale co dál?



# Co třeba SSL-HTTPS certifikáty?

- Dnes pouze CA ze seznamu Exploreru/Mozilly/Operry/Safari/Chrome
- Placená služba – často v základní verzi pouze verifikace na základě whois
- Proč ne fingerprint self-signed certifikátu do DNS?
- Zatím jen myšlenka, na které se pracuje
- CZ.NIC Labs



# Máme jiné služby?

- Obdobná situace je u SMTP
- Většina MTA podporuje SMTPs.
- Ale prakticky se nepoužívá
- Vložme tedy certifikáty do DNS
- Okamžité zavedení kryptování poštovního provozu
- Jiné služby? Jiné certifikáty...?



¿Dotazy?  
<http://www.nic.cz/akademie>

**CZ**

**nic**

správce domény cz