

# DNSSEC – co bylo a co bude

CZ.NIC z.s.p.o.

Ondřej Surý / [ondrej.sury@nic.cz](mailto:ondrej.sury@nic.cz)

20. 5. 2008

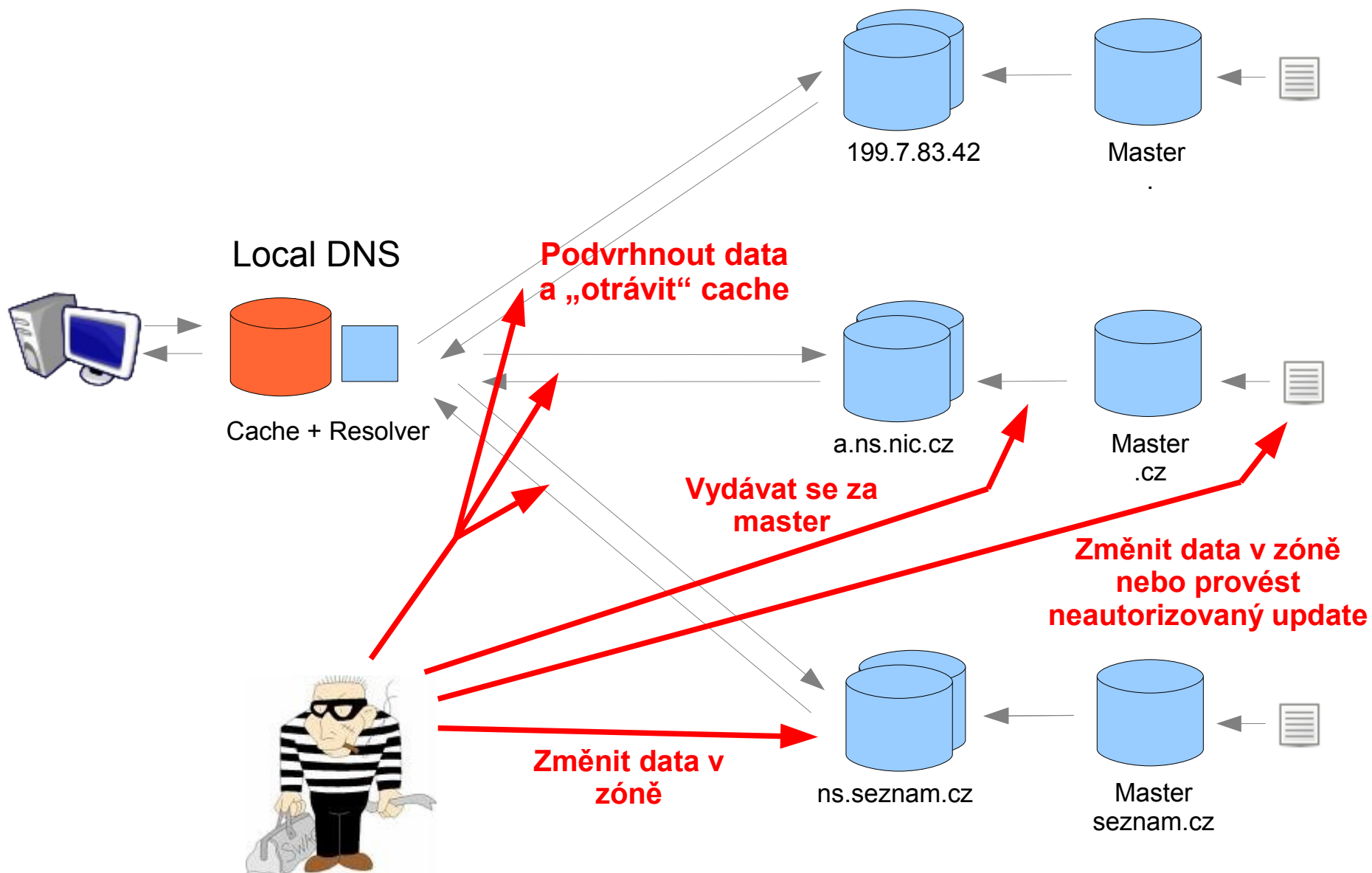
# Stručná historie DNS

- 1973-1983 – centralizovaný systém
- 1983 – John Postel a Paul Mockapetris sepisují základy DNS (RFC881,882,883), první DNS server – Jeeves
- 1986 – DNS jako IETF standard: RFC1034 a RFC1035
- 1988 – DNS se začíná prosazovat, první verze BINDu

# Stručná historie DNSSECu

- 1990 – Steven Bellovin objevuje vážnou chybu v DNS, publikování této chyby odloženo na 1995
  - Autentizace přístupů pomocí jména počítačů (rsh, rlogin)
- 1995 – Steven Bellovin publikuje svojí zprávu z roku 1990
- 1995 – IETF začíná diskutovat o zabezpečení DNS
- 1997 – publikováno RFC2065 – předchůdce RFC2535
- 1999 – publikováno RFC2535 – první verze DNSSEC

# Zranitelnost DNS



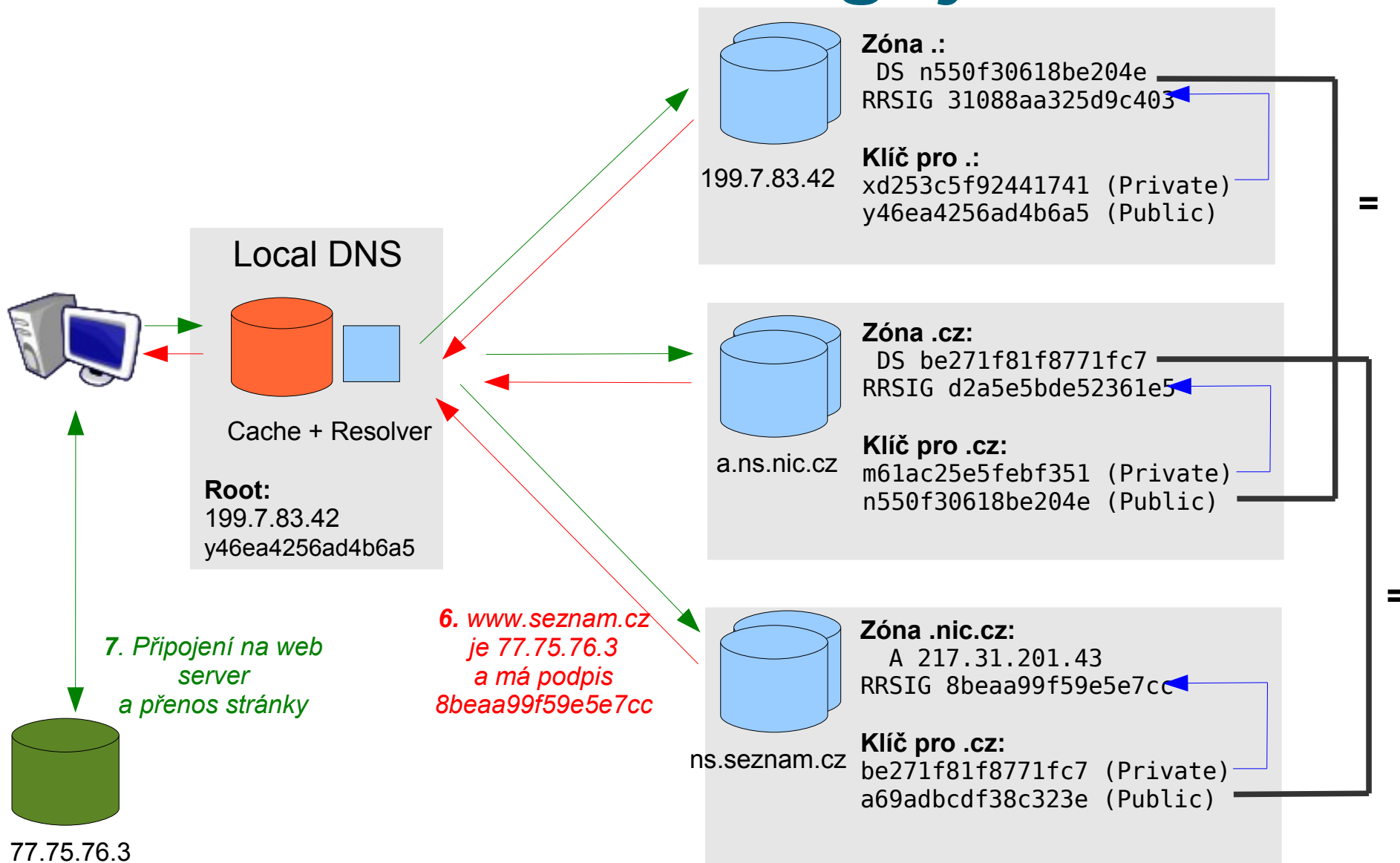
# DNSSEC – verze první

- 1999 – BIND9 implementuje DNSSEC
- 1999-2001 – nasazení DNSSECu stagnuje
- 2001 – ukazuje se, že DNSSEC je nevhodný k nasazení
  - Podepsání záznamů vyžadovalo komplexní komunikaci s nadřazeným serverem
  - Změna klíče u nadřazeného serveru vyžadovala změnu ve všech podřízených zónách

# DNSSECbis – verze druhá

- 2001 – pro vyřešení problémů byla navržena nová verze (draft), která definovala DS záznam a zjednodušila tak komunikaci.
- 2002-2003 – implementace v BIND9, první testu ukazují, že 2535bis je použitelné pro nasazení
- 2004 – podpora 2535bis v BIND 9.3 a NSD2, čeká se na standardizaci
- březen 2005 – publikováno jako RFC4033, RFC4034 a RFC4035
- říjen 2005 – .SE podepisuje jako první svojí zónu

# Jak DNSSECbis funguje?



# DNSSECbis – nové záznamy v DNS

- **DNSKEY** – klíč, kterým je zóna podepsaná

- 256 3 5

- ```
AwEAAaoFOP2o28rmVB8sE2beNr/1FQAKW1zUTOAWbADDg7Y3Unqkv  
bTwOFTRg2MdSC6uWNn4AkO1OZyv/9P01ZOR5rvsZ+Yrw7nrV0hIzT  
6JjGMGC3Xg/oTMZLpsu4HSx71a8ZeEk1EXp/SYNAFhEvAyP8EsBBF  
RatyNQ8w4fLJOjPJX
```

- **RRSIG** – podpis RR záznamu

- NS 5 5 18000 20080616154046 20080519154046 15963  
0.2.4.e164.arpa.

- ```
Qp5OYsWY47yu6MDUvQzaM4XbIer1LNfxtotkQqZDguQf9q018PrJ2  
TXU033Dri+CedEwgtac9WYbxTgG+gZ+Cg==
```

# DNSSECbis – nové záznamy v DNS

- NSEC – ukazatel na další záznam v DNS

- 1.7.4.3.9.8.1.0.2.4.e164.arpa. NS SOA RRSIG NSEC  
DNSKEY

- DS – identifikátor podpisového klíče

- 15963 5 1 1615c6b8b801b1e42791b08cc1a2ed93d6600348

# Problémy DNSSECbis – zone walk

- DNSSEC byl navržen, aby zvýšil bezpečnost
- DNSSEC jak je definován v RFC4033-4035 zveřejňuje všechny záznamy
- NSEC
  - ukazuje na další záznam (abecedně)
  - test na neexistující záznam musí být také podepsán
  - můžeme iterovat přes všechny záznamy v DNS

# NSEC3 – řešení zone walkingu

- NSEC záznam obsahuje další záznam
- NSEC3 záznam obsahuje hash místo doménového jména
- březen 2008 – publikováno jako RFC5155
- NSEC3
  - volitelně počet iterací a salt

# NSEC3 – nové záznamy v DNS

- NSEC3PARAM – určuje počet iterací, algoritmus a salt
  - 1 0 2 deadbeaf
- NSEC3 – hashovaný odkaz na další záznam
  - 1 0 2 deadbeaf chg7f1e19uij84995c92n1847va43lvk NS  
SOA MX RRSIG DNSKEY NSEC3PARAM

# Současné problémy DNSSECu

- Podepsaní root zóny
  - hierarchie důvěry
- Výměna klíčů
- Výkonnostní problémy
  - nárůst velikosti zóny
  - ověřování podpisů
- Výměna algoritmů
- Různé aplikační problémy

# Software a další

- Software
  - BIND 9.x - <http://www.isc.org/sw/bind/>
  - NSD 3.x - <http://www.nlnetlabs.nl/nsd/>
  - UNBOUND 1.0 - <http://www.unbound.net/>
  - LDNS 1.3.x - <http://www.nlnetlabs.nl/ldns/>
- Další...
  - <http://www.dnssec.net/>
  - <http://www.dnssec-deployment.org/>