Úvod do DNSSEC

Jan Kadlec • jan.kadlec@nic.cz • 13.05.2014

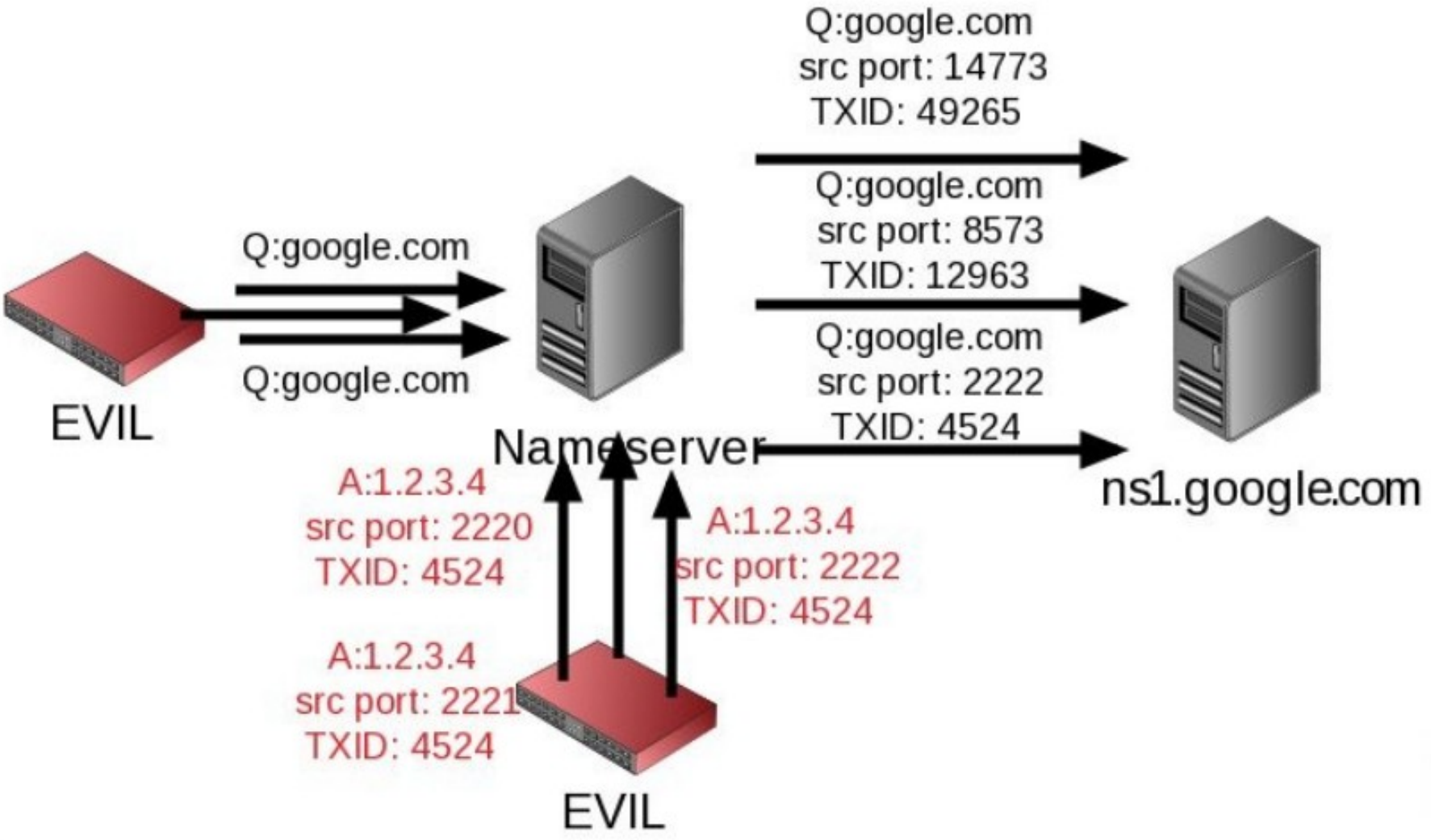
Co se dozvíte

- Proč potřebujeme DNSSEC?
- Jak DNSSEC funguje?
- Jaké jsou s DNSSEC problémy?
- Přehled SW pro práci s DNSSEC.

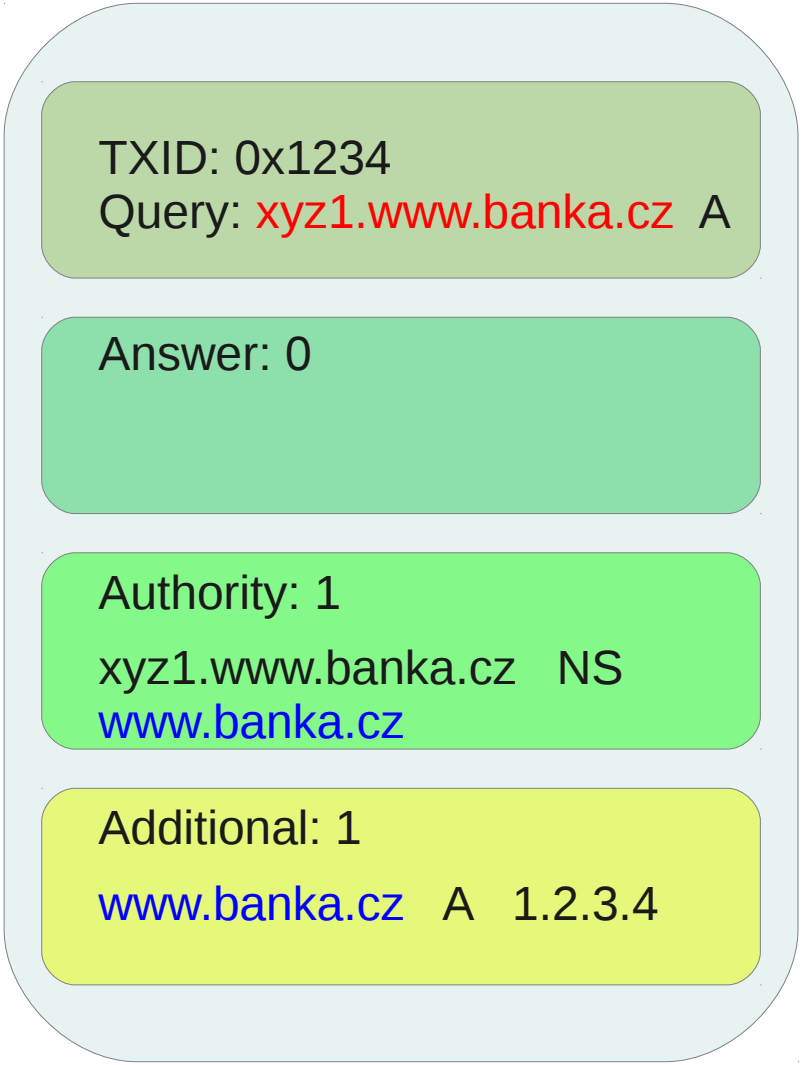
Proč DNSSEC?

- Bez DNSSEC není možné ověřit správnost DNS dat
  - Původní návrh protokolu s bezpečností nepočítá
- Na DNSSEC závisí další protokoly
  - DANE …

Cache poisoning útok



Cache poisoning - Kaminsky



- Nestihl útočník uhodnout TXID/port u dotazu na xyz1.www.banka.cz?
- Nevadí
- Zkusí okamžitě na xyz2.www.banka.cz
- .....

Hezberg & Shulman (2013)

- Útok pomocí fragmentace IP paketů
  - Protokol povoluje fragmentaci velkých paketů kvůli omezení fyzického média (ethernet)
  - Zdroje náhodnosti (UDP port, DNS-ID) zůstávají v prvním fragmentu
  - Zbývá uhodnout IP-ID (16-bit) a UDP checksum
    - Vhodně položený dotaz a zóna generují stejný kontrolní součet
    - Zbývá uhodnout IP-ID
- IP stack složí podvržený paket, pokud se

  útočník trefí do IP-ID a jeho fragment příjde dřív

Základní principy DNSSEC

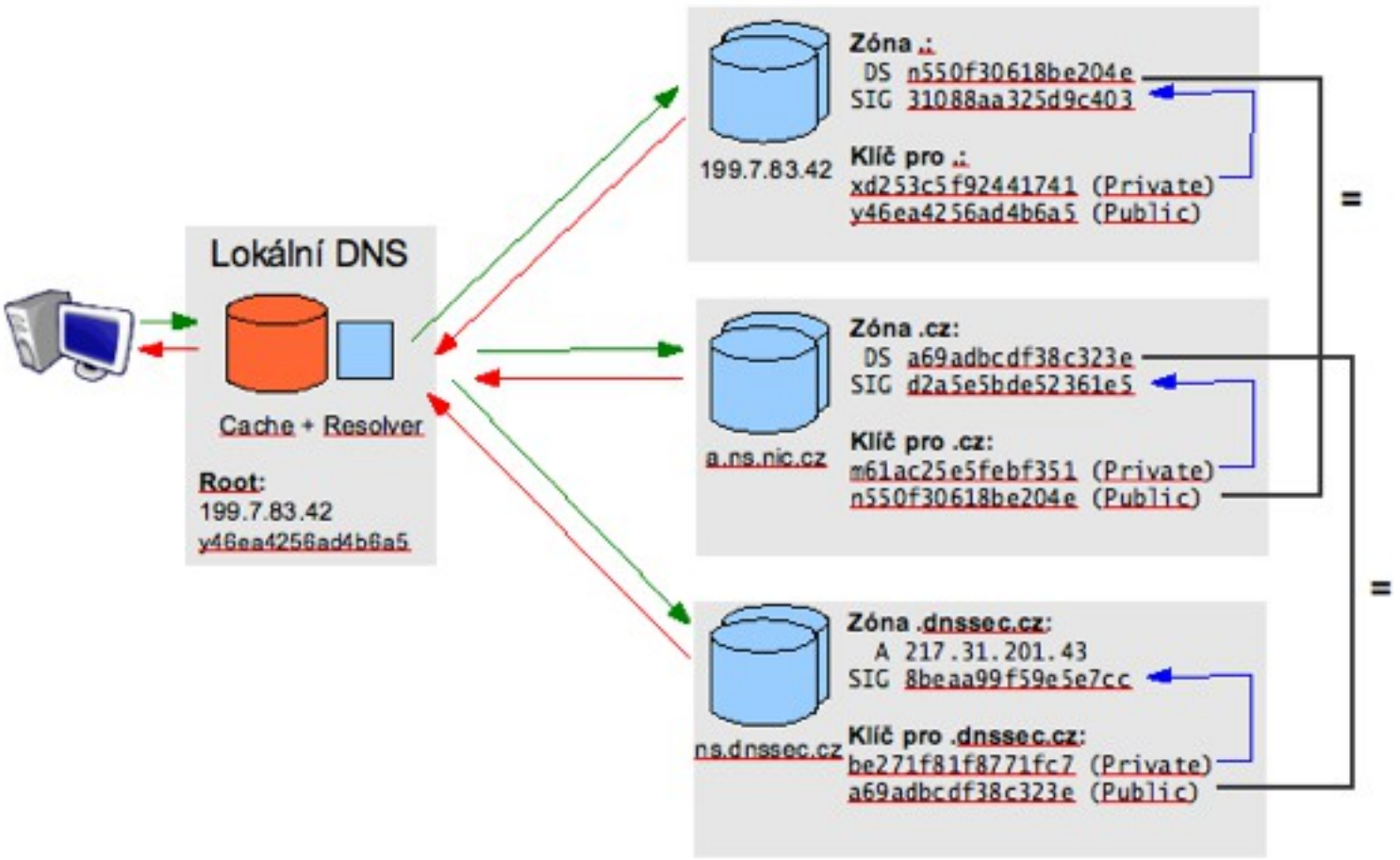
- DNSSEC umožňuje autoritativním serverům poskytovat k „standardním“ DNS datům navíc digitální podpisy RRSetů
- Resolvery ověřující DNSSEC podpisy poskytují potvrzené odpovědi
- Klienti, kteří používají validující resolvery, získávají „správná“ data
- Odpovědi, které nejsou validní, jsou klientovi vráceny z nadřazeného resolveru s chybou „SERVFAIL”

Základní principy DNSSEC

- Dotazy a odpovědi jdou stále po síti nezašifrované!
- Neochrání vás, pokud vám někdo přenastaví resolver v /etc/resolv.conf nebo na routeru!
  - Řešení je validovat lokálně, použijte forwading.


WE NEED TO GO
DEEPER

Základní principy DNSSEC

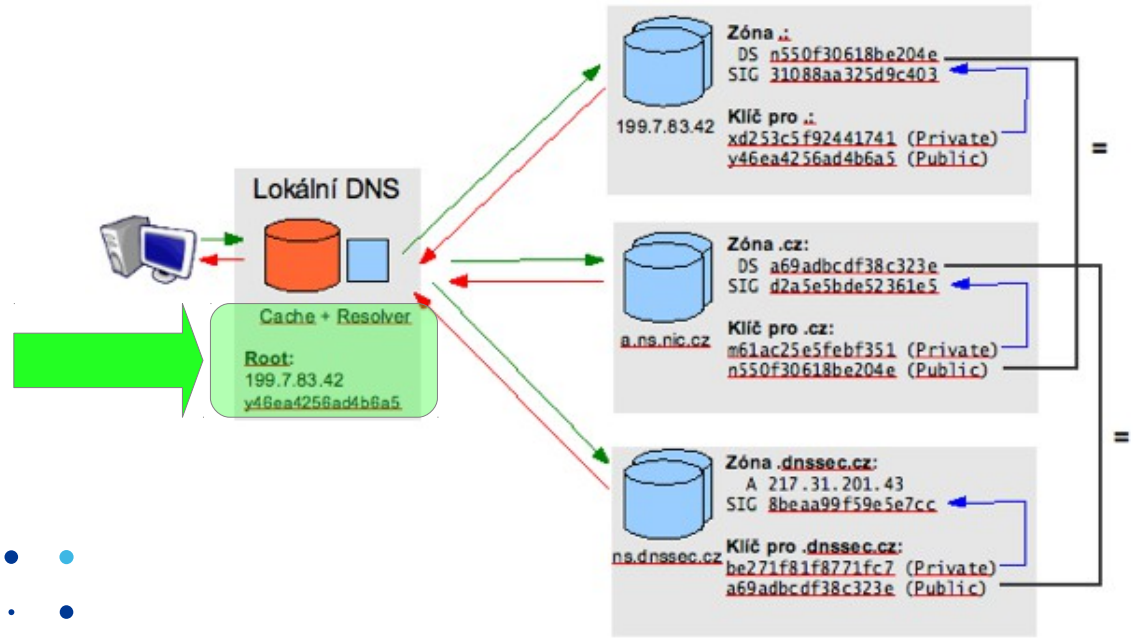


Základní pojmy DNSSEC

- Pevný bod důvěry
- Řetěz důvěry
- Důvěryhodný klíč
- Ostrov důvěry
- Validující Resolver
- Key Signing Key (KSK)
- Zone Signing Key (ZSK)

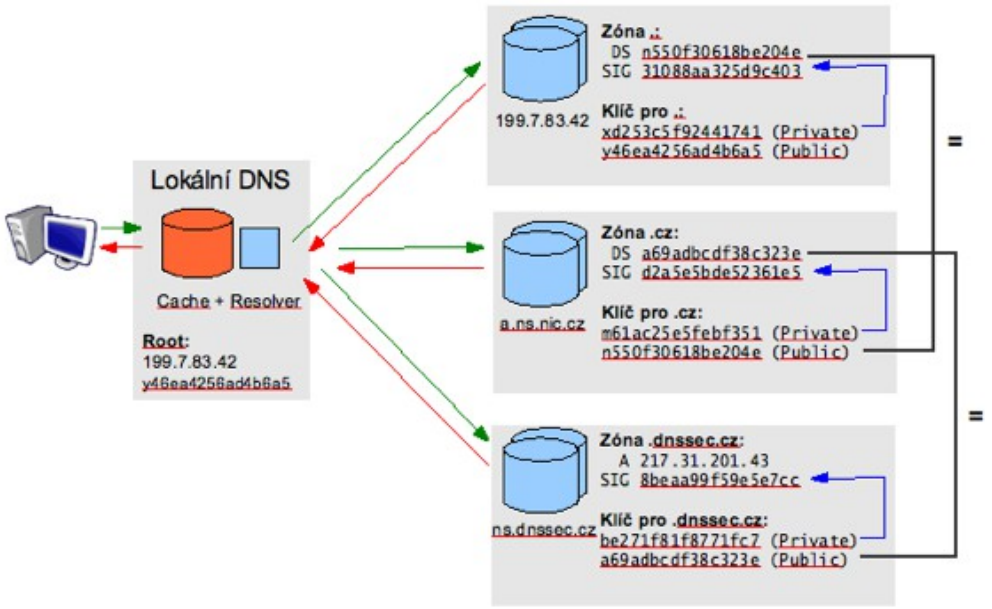
Pevný bod důvěry (Trust Anchor)

- Nakonfigurovaný klíč (nebo jeho hash), kterému důvěřujeme
- Musíme ho získat nějakou bezpečnou cestou
  - (S distribucí, přes TLS, pošta, telefon)



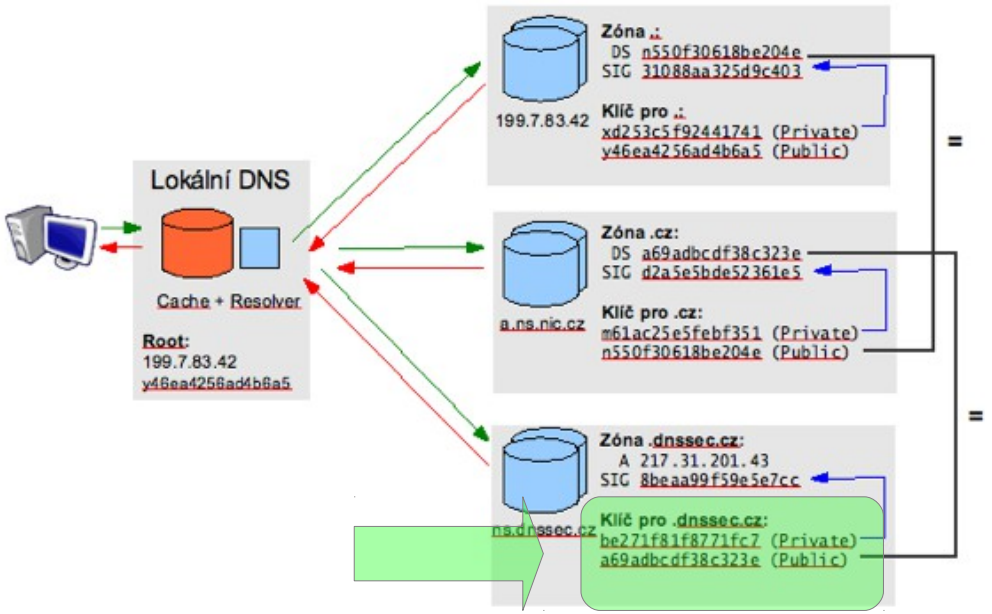
Řetěz důvěry

- Sekvence DNSSEC záznamů (DNSKEY a DS) vedoucí od Pevného bodu důvěry k uzlu v DNS stromu
- V každém uzlu/úrovni máme ověřená data



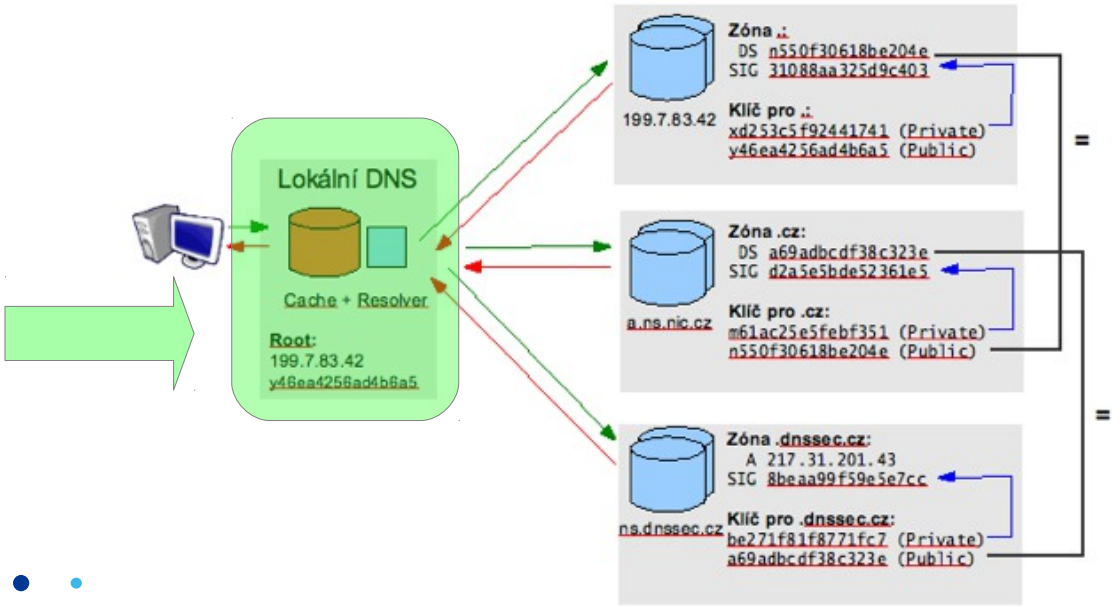
Důvěryhodný klíč

- DNSSEC klíč, který je důvěryhodný (you don't say...)
  - 1.) Pevný bod důvěry
  - 2.) Klíč získaný přes Řetěz důvěry



Validující Resolver

- Posílá DNS dotazy s DNSSEC OK
- Ověřuje validitu DNSSEC podpisů v DNS odpovědích
- Má nakonfigurovaný alespoň jeden Pevný bod důvěry



Key Signing Key

- DNSSEC klíč používaný pro podepsání dalších klíčů
- Silnější
  - Více bitů
  - Výpočetně složitější
  - Více dat
- Speciální bit (SEP) v příznacích DNSSEC klíče

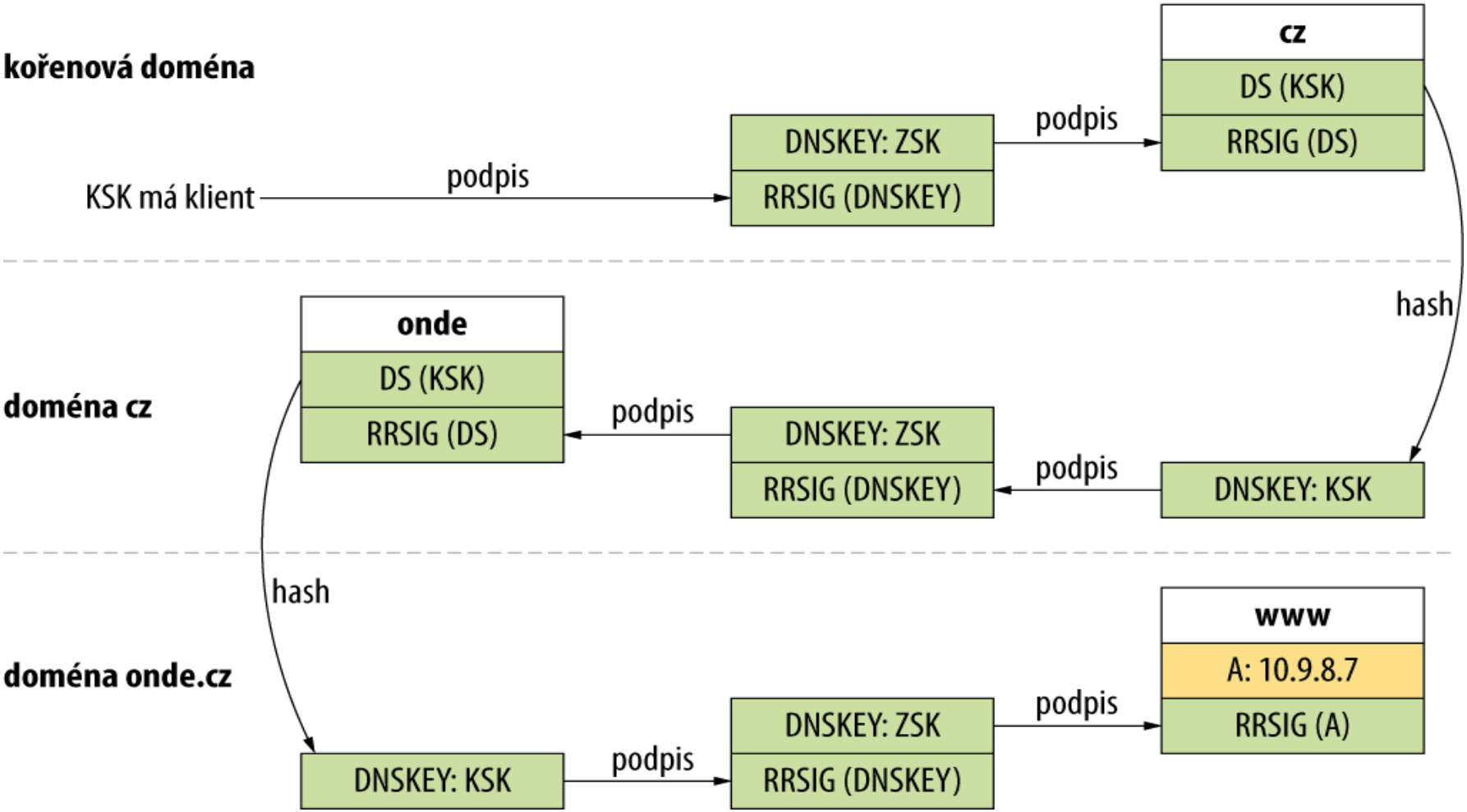
Zone Signing Key

- DNSSEC klíč používaný pro podepsání vlastního obsahu zóny
- Slabší
  - Méně bitů
  - Výpočetně jednodušší
  - Rychlejší podpis i ověřování
  - Méně dat

Stavební bloky bychom měli, dohromady to funguje takto:

http://bit.ly/1iLm1Nf

Příklad: doména onde.cz



Nové RR záznamy

DNSKEY RR záznam

- DNSSEC klíč
- RDATA obsahují
  - Příznaky (Flags)
  - Protocol (vždy 3)
  - Algoritmus (5 - RSASHA1)
  - Veřejný klíč
- `IN DNSKEY 257 3 5 AwEAAd[...]kNB8Qc=`

RRSIG RR záznam

- Digitální podpis RRSetu
- Obsahuje:
  - Podepsaný RR typ
  - Algoritmus
  - Počet labelů v podpisovaném jméně (kvůli *)
  - Původní TTL
  - Datum platnosti (začátek a konec)
  - Key Tag, Jméno zóny
  - Digitální podpis
- `IN RRSIG A 5 3 600 20081203010003 20081103010003 58773 dnssec.cz. V0JXuw[...]`

NSEC RR záznam

- Záznam vyznačující neexistenci doménového jména – pomocí vyjmenování dalšího následujícího labelu
- Zóna musí být abecedně setřízena (v každé úrovni hierarchie)
- Obsahuje:
  - Další doménové jméno
  - Bitová mapa existujících typů (pro vlastníka)
- `IN NSEC udp53.cz. NS RRSIG NSEC DS`

NSEC3 RR záznam

- Řeší zone walking problém s NSEC
- NSEC3 jména hashuje
- NSEC3 RR tvoří řetěz v hashovaném pořadí
- NSEC3 RR dokáže existenci hierarchicky „nejbližšího“ jména a neexistenci přesnější zhody
- Zvýšená zátěž jak pro nameserver, tak pro resolver
  - Možnost zahltit nameserver neexistujícími dotazy
- Možnost vypustit z řetězu nepodepsané delegace
  - NSEC3 Opt-out

NSEC3PARAM záznam

- Obsahuje kód algoritmu a NSEC3 salt
  - Salt – použit při vytváření NSEC3 záznamů
- TTL může být nulové
  - Dle RFC se nesmí použít na validaci
- Vlastníkem vždy vrchol zóny
- cz. 0 IN NSEC3PARAM 1 0 10 [Hex salt]
  - Obsahuje: algoritmus, flags (0), délku salt, salt
  - Kód algoritmu musí odpovídat tomu v NSEC3 záznamech

DS RR záznam

- Záznam o bezpečné delegaci
- V nadřazené zóne
- RDATA obsahují hash DNSKEY klíče, kterým je zóna podepsaná
- Obsahuje:
  - Key Tag
  - Algoritmus
  - Digest Type
  - Digest
- `IN DS 17398 5 1 BBDDD[...]3502D`


I HAVE NO IDEA WHAT YOU'RE
TRYING TO TELL ME RIGHT NOW

Co je potřeba?

- Aktuální SW :)
- Podepsaná doména
- DS záznamy v nadřazené doméně
- Automatizace výměny klíčů
  - Ruční výměna možná, ale pravděpodobnost chyb je značná.
- Validující resolver
- Rozumné firewally
  - Omezení UDP > 512B, zahození dotazů s EDNS0

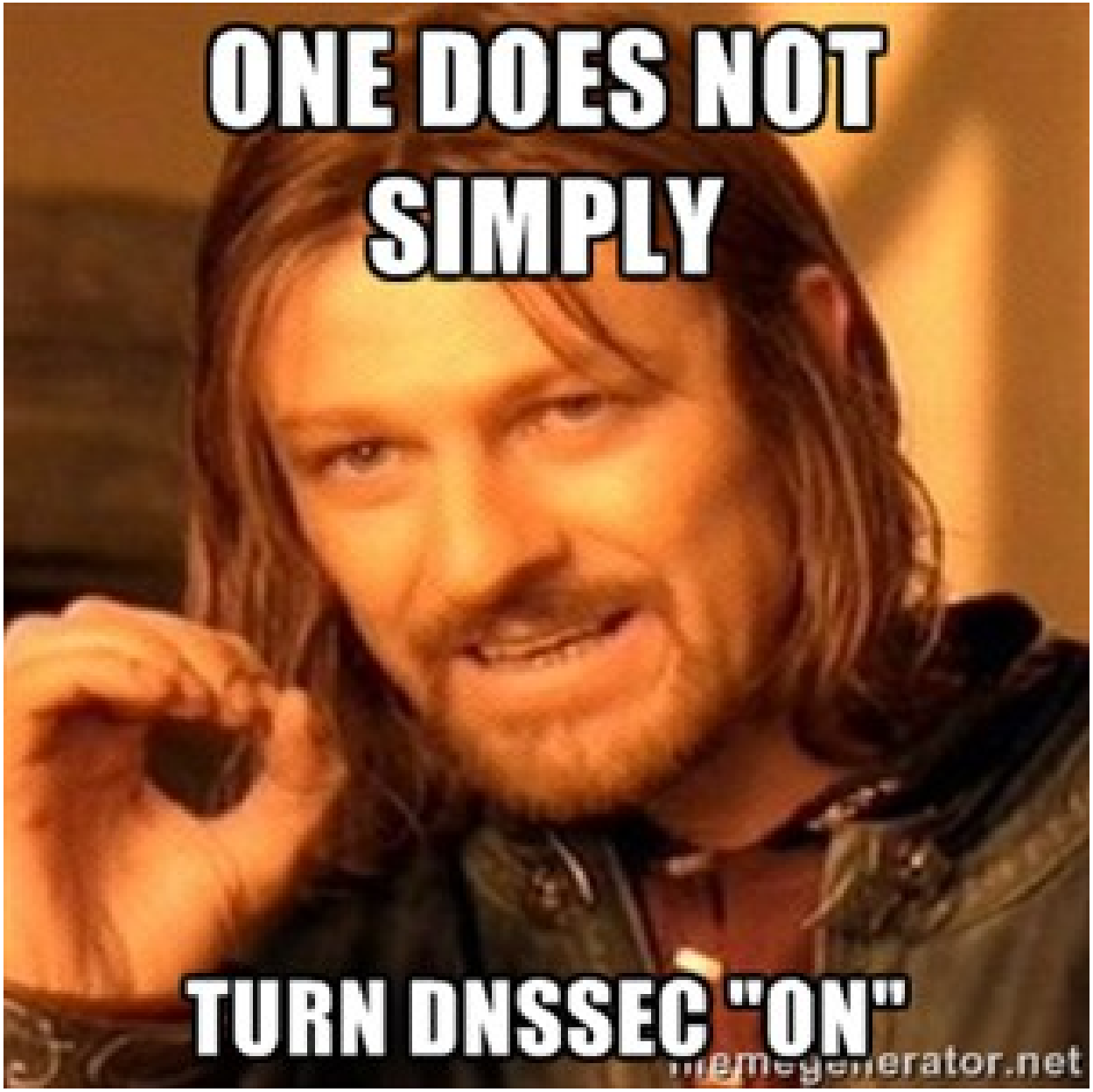
Software pro DNSSEC

- Unbound
- BIND a jeho nástroje
  - Automatické podepisování
  - Ruční podepisování: dnssec-keygen
    dnssec-signzone
- OpenDNSSEC
- Knot DNS
  - Automatické podepisování, nástroje brzy :)
- PowerDNS

DNSSEC debugging

- dig, dnssec-verify, ldns-verify-zone
- dnssec-trigger
- DNSSEC validator plugin
- Online nástroje:
  - DNSViz
  - DNSSEC analyzer

Problémy s DNSSEC


ONE DOES NOT
SIMPLY
TURN DNSSEC "ON"
memegenerator.net

Problémy s DNSSEC

- Složité nasazení, žádné „ultimate solution“
- Nelze snadno automatizovat, dokud nebude RFC pro mechanismus na výměnu DS záznamů
- Zátež pro DNS infrastrukturu
  - Jak resolvery, tak autoritativní servery
- Možný „únik“ dat (NSEC)
- Značné zvětšení DNS odpovědí
  - Zjednodušuje amplification útoky

Děkuji za pozornost

Jan Kadlec • jan.kadlec@nic.cz