DNSSEC – bezpečné DNS

CZ.NIC z.s.p.o.
Matej Dioszegi
matej.dioszegi@nic.cz
8.11.2009

cz nic
správce domény cz

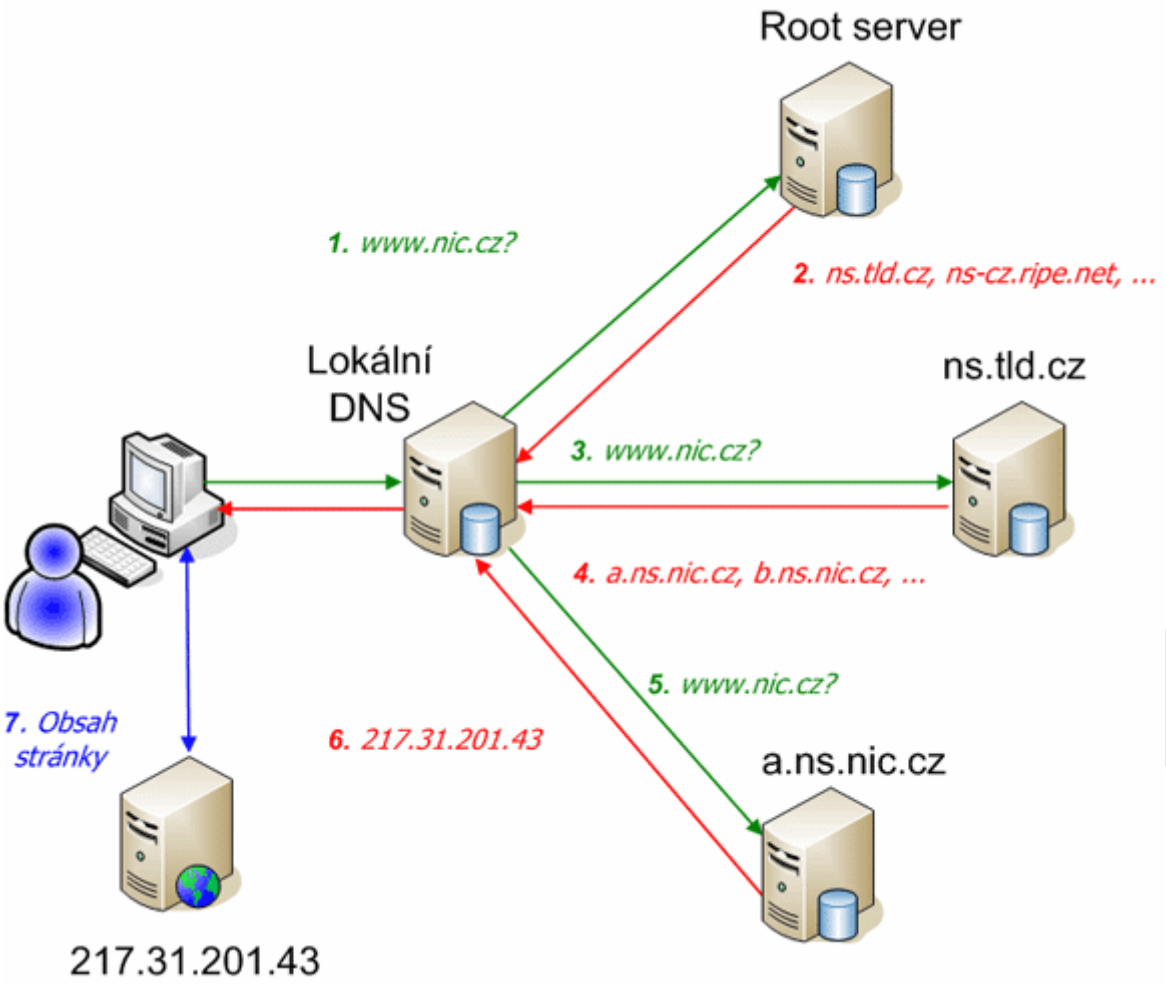
Obsah

- Motivácia DNSSEC
- Stručný popis DNSSEC
- DNSSEC pre administrátora
  - Podpis zóny
  - Zverejnenie kľúčov
  - Výmena kľúčov
- DNSSEC a „bežný užívateľ“
- Stav DNSSEC v ČR a vo svete

Útoky na DNS

- Boj na viacerých frontách
  - Útoky na autoritatívny NS
  - Útoky na komunikáciu master/slave
  - Útoky na komunikáciu auth/rec
    - Cache poisoning
- Najčastejšie práve cache poisoning
  - Vloženie falošných dat do cache resolvera
  - Všetci užívatelia, ktorí používajú tento resolver, sú v nebezpečí po dobu TTL falošných záznamov
- DNSSEC rieši práve tento prípad

DNS dotaz


Root server
1. www.nic.cz?
2. ns.tld.cz, ns-cz.ripe.net, ...
Lokální
DNS
ns.tld.cz
3. www.nic.cz?
4. a.ns.nic.cz, b.ns.nic.cz, ...
5. www.nic.cz?
6. 217.31.201.43
7. Obsah
stránky
a.ns.nic.cz
217.31.201.43

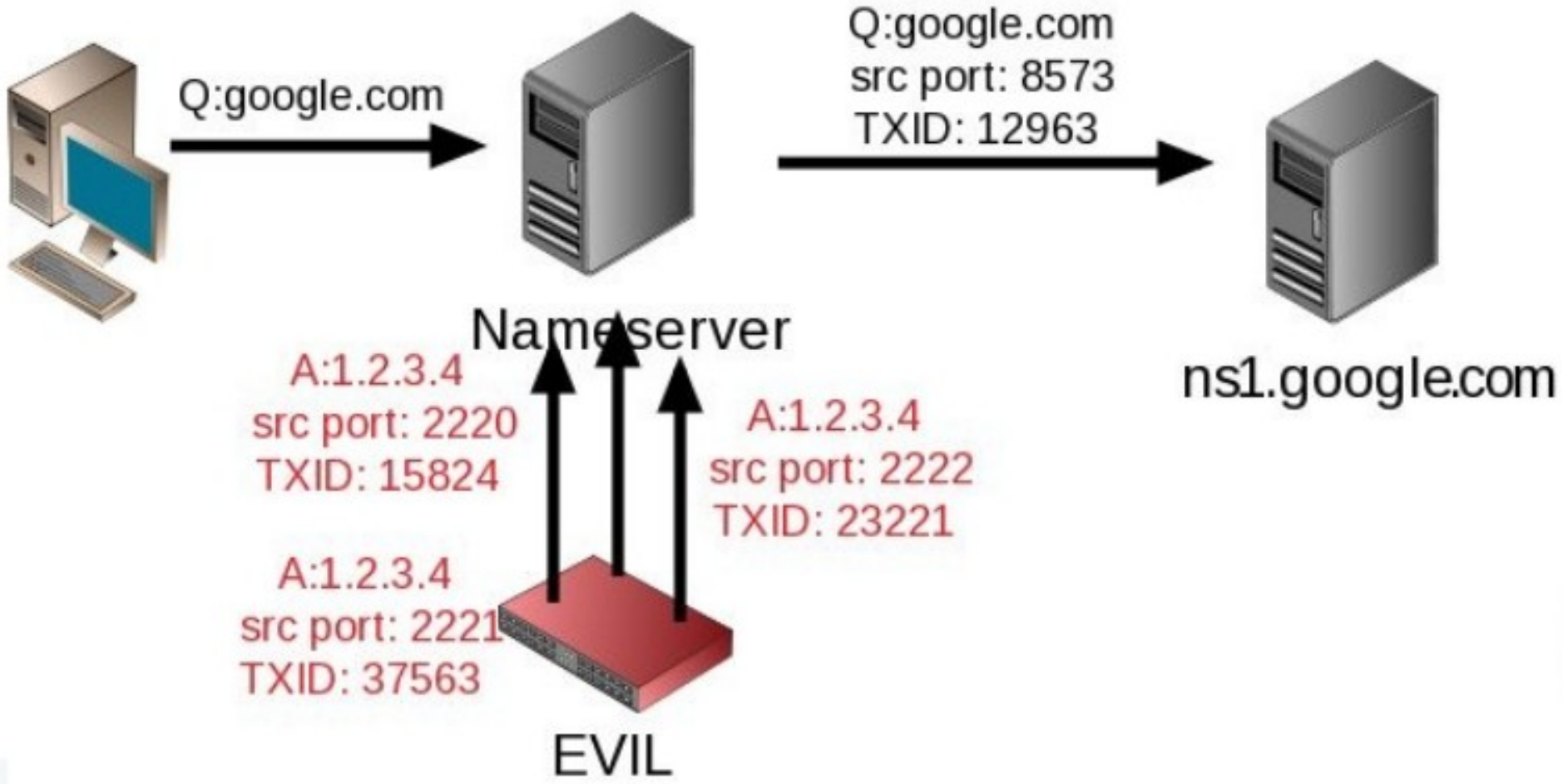
Ochrana DNS proti útokom

```
▷ User Datagram Protocol, Src Port: 58513 (58513), Dst Port: domain (53)
▽ Domain Name System (query)
    [Response In: 11196]
    Transaction ID: 0xb007
  ▷ Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▽ Queries
    ▽ www.nic.cz: type A, class IN
        Name: www.nic.cz
        Type: A (Host address)
        Class: IN (0x0001)
```

```
▷ User Datagram Protocol, Src Port: domain (53), Dst Port: 58513 (58513)
▽ Domain Name System (response)
    [Request In: 11195]
    [Time: 0.000635000 seconds]
    Transaction ID: 0xb007
  ▷ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 3
    Additional RRs: 6
  ▽ Queries
    ▽ www.nic.cz: type A, class IN
        Name: www.nic.cz
        Type: A (Host address)
        Class: IN (0x0001)
  ▽ Answers
    ▷ www.nic.cz: type A, class IN, addr 217.31.205.50
  ▽ Authoritative nameservers
    ▷ nic.cz: type NS, class IN, ns b.ns.nic.cz
    ▷ nic.cz: type NS, class IN, ns a.ns.nic.cz
    ▷ nic.cz: type NS, class IN, ns d.ns.nic.cz
  ▽ Additional records
    ▷ a.ns.nic.cz: type A, class IN, addr 217.31.205.180
    ▷ a.ns.nic.cz: type AAAA, class IN, addr 2001:1488:dada:176::180
    ▷ b.ns.nic.cz: type A, class IN, addr 217.31.205.188
    ▷ b.ns.nic.cz: type AAAA, class IN, addr 2001:1488:dada:184::188
    ▷ d.ns.nic.cz: type A, class IN, addr 193.29.206.1
    ▷ d.ns.nic.cz: type AAAA, class IN, addr 2001:678:1::1
```

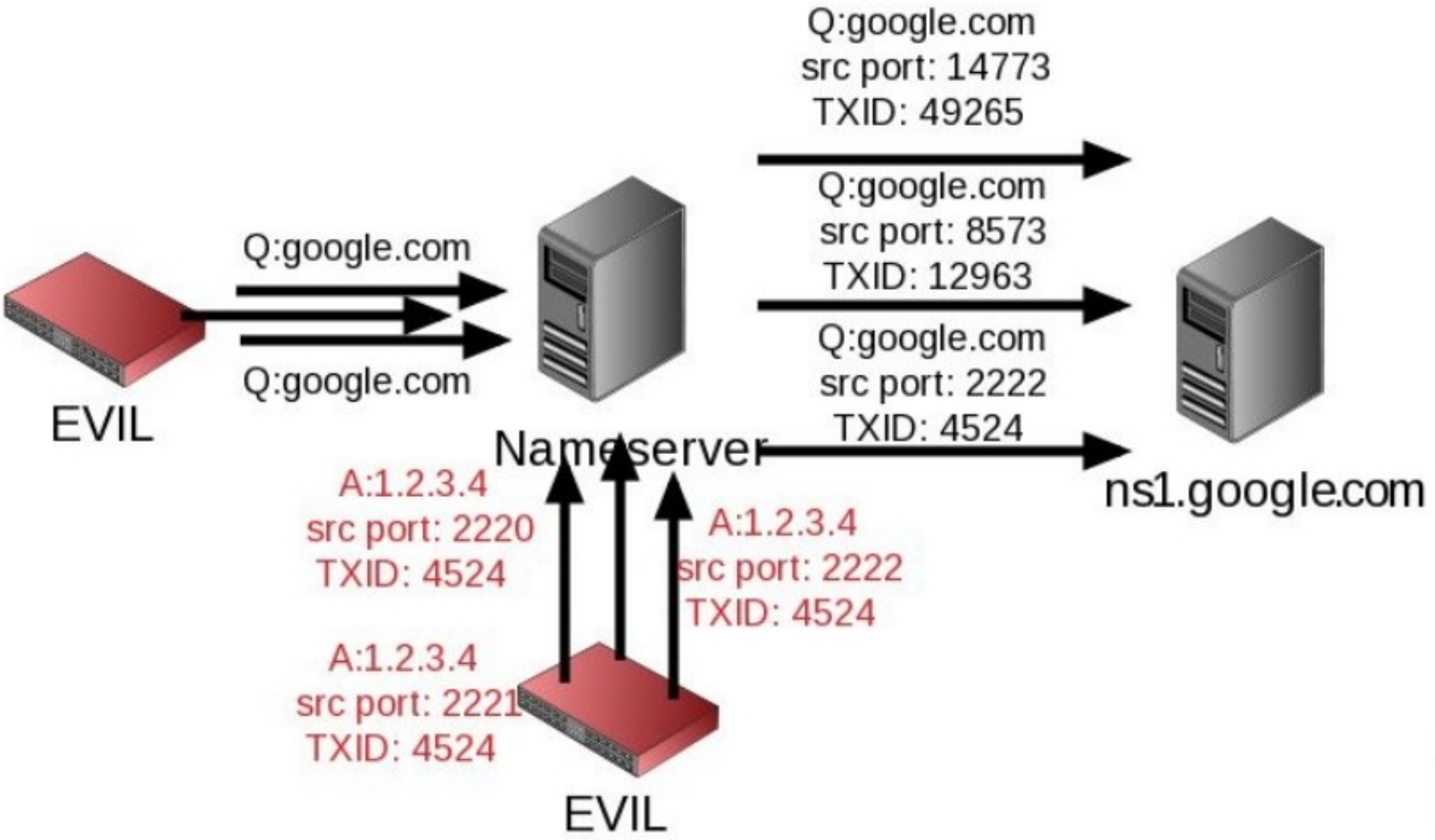
+ zhoda IP adresy na ktorú bol paket odoslaný a z ktorej bola prijatá odpoveď

Cache poisoning



zdroj: Paul Wouters, Defending your DNS in a post-Kaminsky world, Black Hat Briefings

Cache poisoning – birthday attack



zdroj: Paul Wouters, Defending your DNS in a post-Kaminsky world, Black Hat Briefings

Birthday attack

- Birthday paradox
  - V skupine 23 ľudí je pst. kolízie (2 narodeniny v 1 deň) > 50 %

$$P = 1 - (1 - \frac{1}{t})^{\frac{N \times (N-1)}{2}}$$

t = u narodenín 365, u TXID 2^16

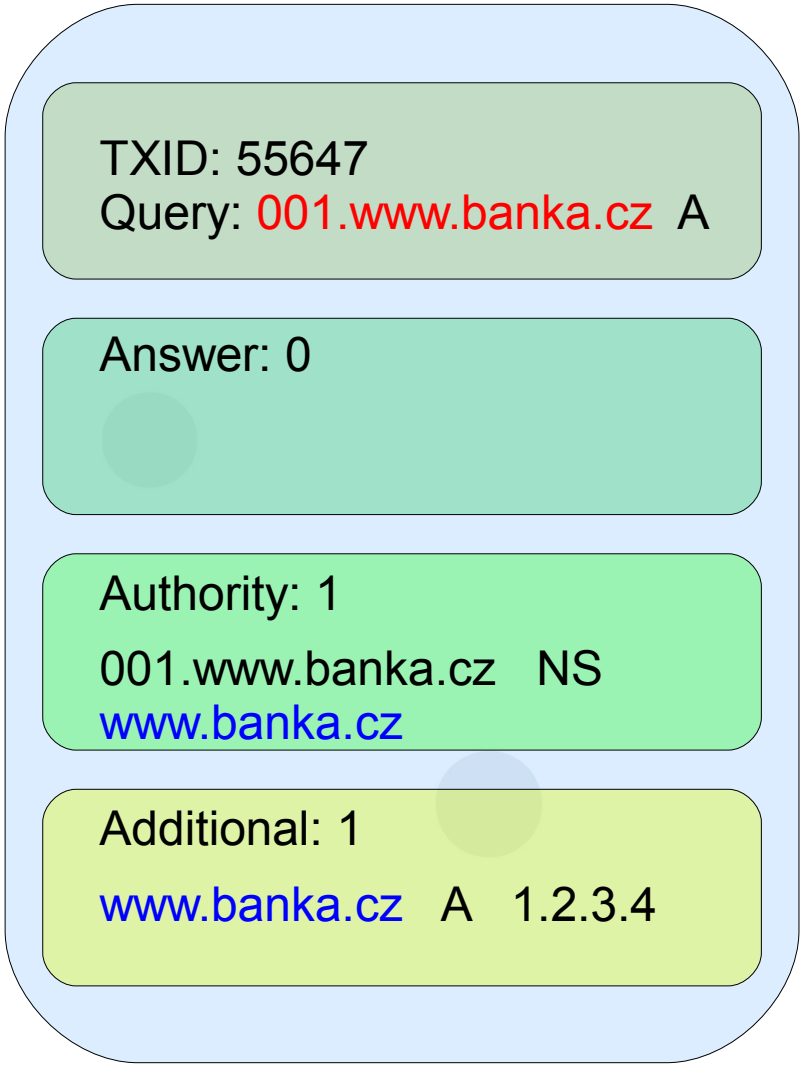
N = počet prvkov v skupine

Počet paketov	Pravdepodobnosť kolízie
10	0.0006
100	0.073
200	0.262
300	0.496
500	0.851
700	0.976

Kaminského útok

- Dan Kaminsky v 2008 prezentoval elegantný spôsob útoku
  - NS bez random ports boli prakticky „položiteľné“ v rádoch minút
  - NS s random ports odolávajú dlhšie
    - Ale nie o veľa
- Predošlé spôsoby sa snažili podvrhnúť záznam v Answer sekcii
  - DK použil glue záznamy v Additional sekcii

Kaminského útok



- Nestihol útočník uhádnuť TXID/port pri mene 001.www.banka.cz?
  - Nevadí
- Skúsi hneď na 002.www.banka.cz
- .....

Kaminského útok

- 100Mbit linka, plne patchovaný BIND
- 2 klienti
  - Implementácia E. Polyakov
- Úspech po 101 hodinách

```
root@kvm:/home/kvm/src_64bit# ./attack_client -a 172.20.20.22 -q www.google.com -n ns-poisoned.google.com -Q 1.2.3.4 -A 216.239.32.10 -s 172.20.20.22:1025:45000-64000
...
Using attack query: 1028550-e239-19450.google.com .
attack_server: dport: 45000 [45000-64000], id: 1107, packets: 4359, t: 0.0 sec, speed: 153146.2 pps.
id: e239: flags: resp: 1, opcode: 0, auth: 0, trunc: 0, RD: 1, RA: 1, rcode: 0.
        : question: 1, answer: 1, auth: 4, addon: 0.
        : question: name: '1028550-e239-19450.google.com.', type: 1, class: 1.
        : name: '1028550-e239-19450.google.com.', type: 1, class: 1, ttl: 123456, rdlen: 4, rdata: 1.2.3.4
Successfully poisoned 172.20.20.22:53 DNS server
 www.google.com IN NS  ns-poisoned.google.com
 ns-poisoned.google.com IN A     1.2.3.4
```

- V reálnom svete – Banco Bradesco 4/09, podvrhnutý záznam v cache NS providera NET Virtua

DNSSEC

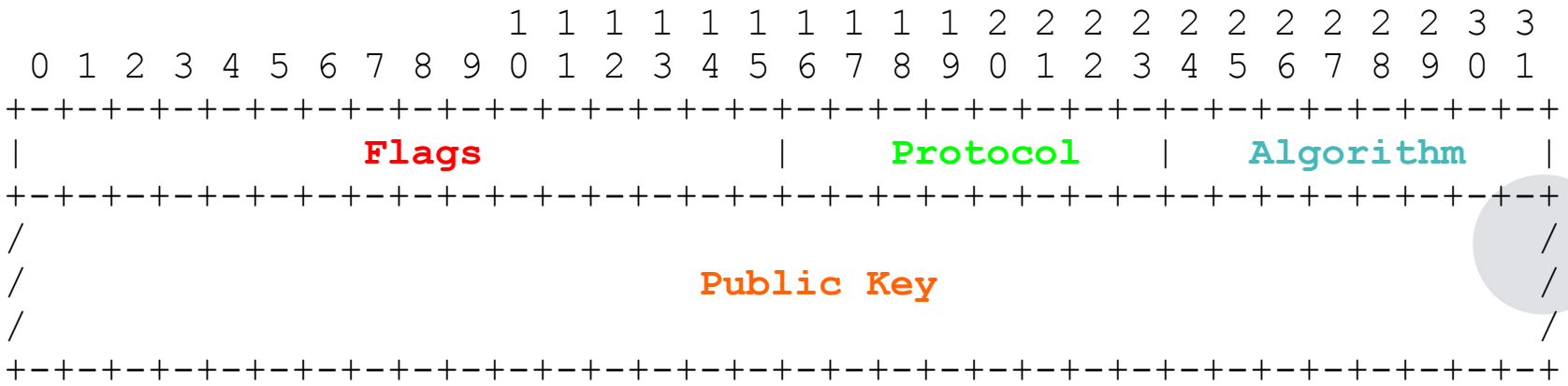
DNSSEC

- Integrita DNS dat
- Autenticita DNS dat
- Validujúci resolver je schopný skontrolovať doručené data
- Klienti využívajúci VR dostanú overené, „správne“ data
- Ak boli DNS data podvrhnuté, klient dostáva SERVFAIL
  - Podvrhnutá doména „neexistuje“

DNSSEC – nové RR

- DNSKEY
- RRSIG
- DS
- NSEC / NSEC3

DNSKEY

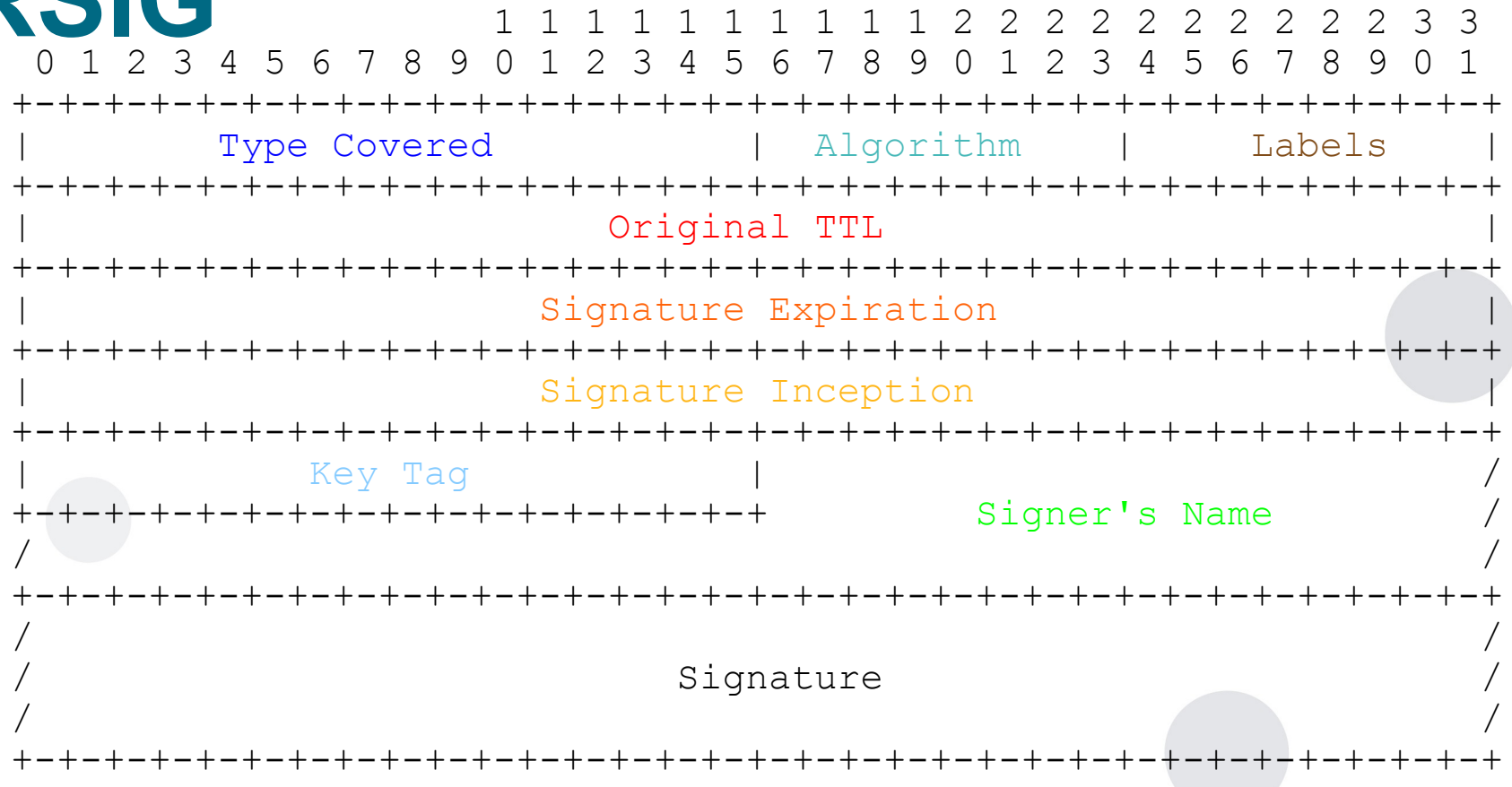


nic.cz. 3600 IN DNSKEY 256 3 5 (
BQEAAAABuG7/xcErl91ynaROnOLkCPyE2HKJGlVRR+QG
gJIqR2uxPuCrWzWOkOOJTgx+LGuaWM7N9VaJpYF91Ckk
MOnZltL29lRbsRUVQSINTjZLZEXQMoV1qUKOoxTt8NSP
TGmg5fIa6bhzgi290Hn1wOxByow+BM4WsOeaFBg+NX6G
2bk=
) ; key id = 58367

DNSKEY

- Logicky delené na
  - Zone signing key (ZSK)
    - Podpisuje všetky RRSety v zóne
  - Key signing key (Key signing key)
    - Podpisuje len DNSKEY RRset
    - Slúži ako tzv. Secure Entry Point (SEP) pri budovaní reťaze dôvery

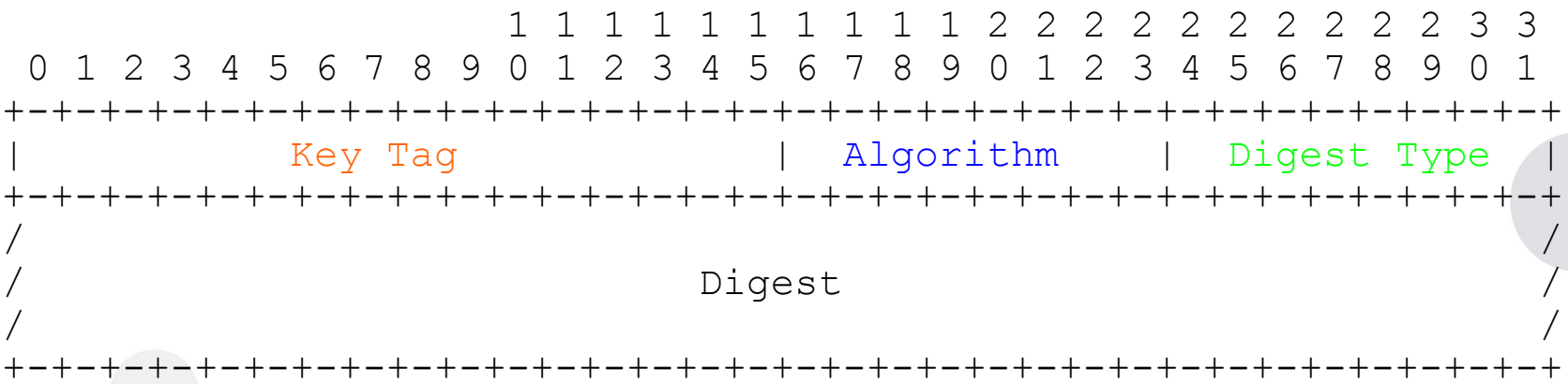
RRSIG



nic.cz. 1800 IN RRSIG SOA 5 2 1800 20091104190303 (
20091021190303 27674 nic.cz.
fBbh9o6xo9tHUv0EzaH7rfmGrAx8eI6aCsAUFJwlqFjl

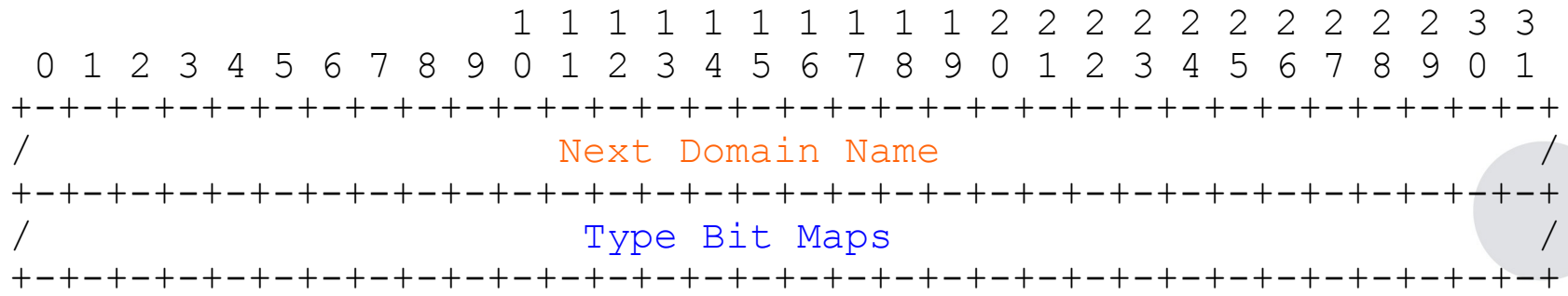
RDJ7ezqsSuzi0fB5MA+015PfkvNUUms7TQg0NqakQS8z
LIDK0b0obMq90ddPXi/j5uPtyH8uj9vTEXlTYnrEK123
vjNhqvkwbEJJ/fYNylxJTQKZAlVWBfA9/uCeZZY=)

DS



nic.cz. 18000 IN DS 27979 5 1 (
FF11E740A0254EC63C738A47E52ABF3AD91D8C43)

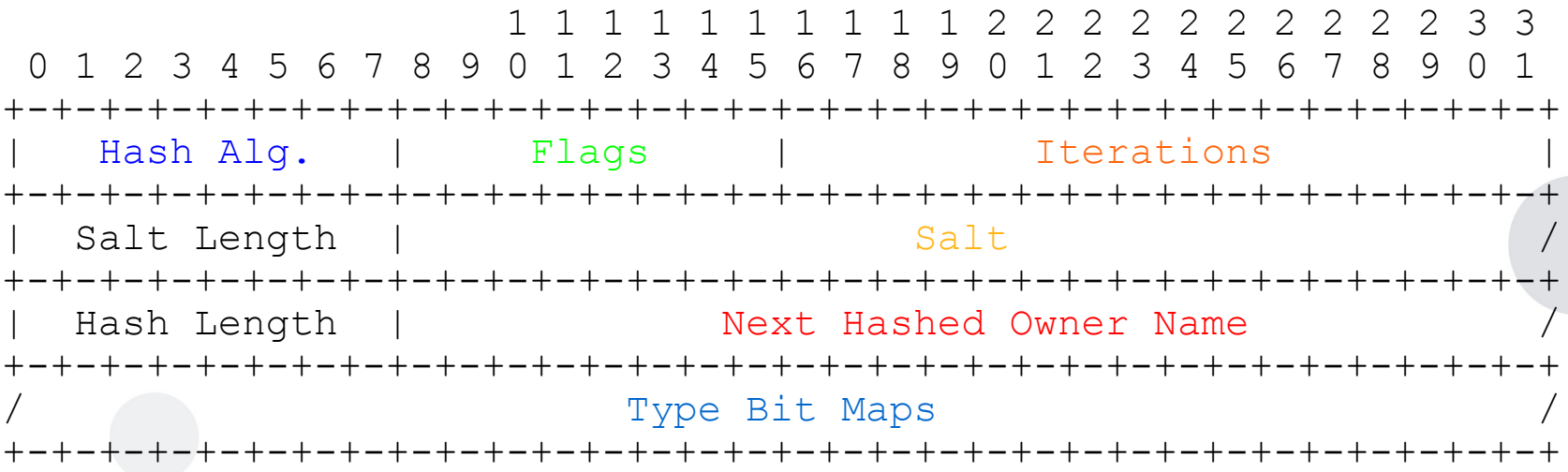
NSEC



nic.cz. 7200 IN NSEC _jabber._tcp.nic.cz. A NS SOA MX AAAA RRSIG NSEC DNSKEY

- Autentické popretie existencie
- Zone walking problem!
  - Veľa administrátorov odmieta nasadiť DNSSEC kvôli zone-walking-u

NSEC3



ITC22N1PN0941OM1Q0382RM01P9MU9HF.gov. 86400 IN NSEC3 1 0 10 56A8
ITRFNQI62NLR2HV0MHNTT53ELA9K4FGP NS SOA RRSIG DNSKEY NSEC3PARAM

- Nemožný zone walking
- NSEC3 navyše dáva možnosť vynechať v reťazi nepodpísané delegácie

NSEC3

- Zložitejšie pre nameserver aj pre resolver pri overovaní
  - Mená su hashované, iteratívne so soľou
  - Klientovi sa posiela hash „najdlhšieho predka“ (v zmysle stromovej hierarchickej štruktúry) a dôkaz, že neexistuje presnejšia zhoda z požadovaným menom
  - Klient sa dozvie len najdlhšie meno predka

NSEC3 vs. NSEC

QUERY

```
;; Question
a.c.x.w.example.          IN A
```

ZONE

```
H(example)        = 0p9mhaveqvm6t7vbl5lop2u3t2rp3tom
H(a.example)      = 35mthgpgcu1qg68fab165klnsnk3dpvl
H(ai.example)     = gjeqe526plbf1g8mklp59enfd789njgi
H(ns1.example)    = 2t7b4g4vsa5smi47k61mv5bv1a22bojr
H(ns2.example)    = q04jkcevqvmu85r014c7dkba38o0ji5r
H(w.example)      = k8udemvp1j2f7eg6jebps17vp3n8i58h
H(*.w.example)    = r53bq7cc2uvmubfu5ocmm6pers9tk9en
H(x.w.example)    = b4um86eghhds6nea196smvmlo4ors995
H(y.w.example)    = ji6neoaepv8b5o6k4ev33abha8ht9fgc
H(x.y.w.example)  = 2vptu5timamqttgl4luu9kg21e0aor3s
H(xx.example)     = t644ebqk9bibcna874givr6joj62mlhv
```

NSEC3

```
;; H(c.x.w.example) = 0va5bpr2ou0vk0lbqeeljri88laipsfh
0p9mhaveqvm6t7vbl5lop2u3t2rp3tom.example. NSEC3 1 1 12 aabbccdd (
                        2t7b4g4vsa5smi47k61mv5bv1a22bojr MX DNSKEY NS
                        SOA NSEC3PARAM RRSIG )

;; H(x.w.example) = b4um86eghhds6nea196smvmlo4ors995
b4um86eghhds6nea196smvmlo4ors995.example. NSEC3 1 1 12 aabbccdd (
                        gjeqe526plbf1g8mklp59enfd789njgi MX RRSIG )

;; H(*.x.w.example) = 92pqneegtaue7pjatc3l3qnk738c6v5m
35mthgpgcu1qg68fab165klnsnk3dpvl.example. NSEC3 1 1 12 aabbccdd (
                        b4um86eghhds6nea196smvmlo4ors995 NS DS RRSIG )
```

NSEC

```
x.w.example. NSEC y.w.example.com (
                          MX NSEC RRSIG )
```

- Najdlhší predok: x.w.example – zhoda záznamu 2
- Bližšia zhoda (c.x.w.example) neexistuje – pokrýva záznam 1
- Wildcard (*.x.w.example) neexistuje – pokrýva záznam 3
- Klient sa dozvie: v zóne existuje meno x.w.example

DNSSEC pre administrátora

DNSSEC pre administrátora

- DNS
  - Vytvoriť zónový súbor
  - Nakonfigurovať NS, aby poskytoval zónu z tohoto súboru
  - V prípade zmeny zónového súboru reload

- DNSSEC
  - Vytvoriť zónový súbor
  - Vygenerovať kľúče
  - Podpísať zónu
  - Nakonfigurovať NS aby reagoval na DO bit a poskytoval zónu z tohoto súboru
  - Predať nadradenej zóne DNSKEY/DS
  - V prípade zmeny v zóne znova podpísať a reload
  - Po vypršaní platnosti podpisu znova podpísať
  - Pravidelne obmieňať kľúče

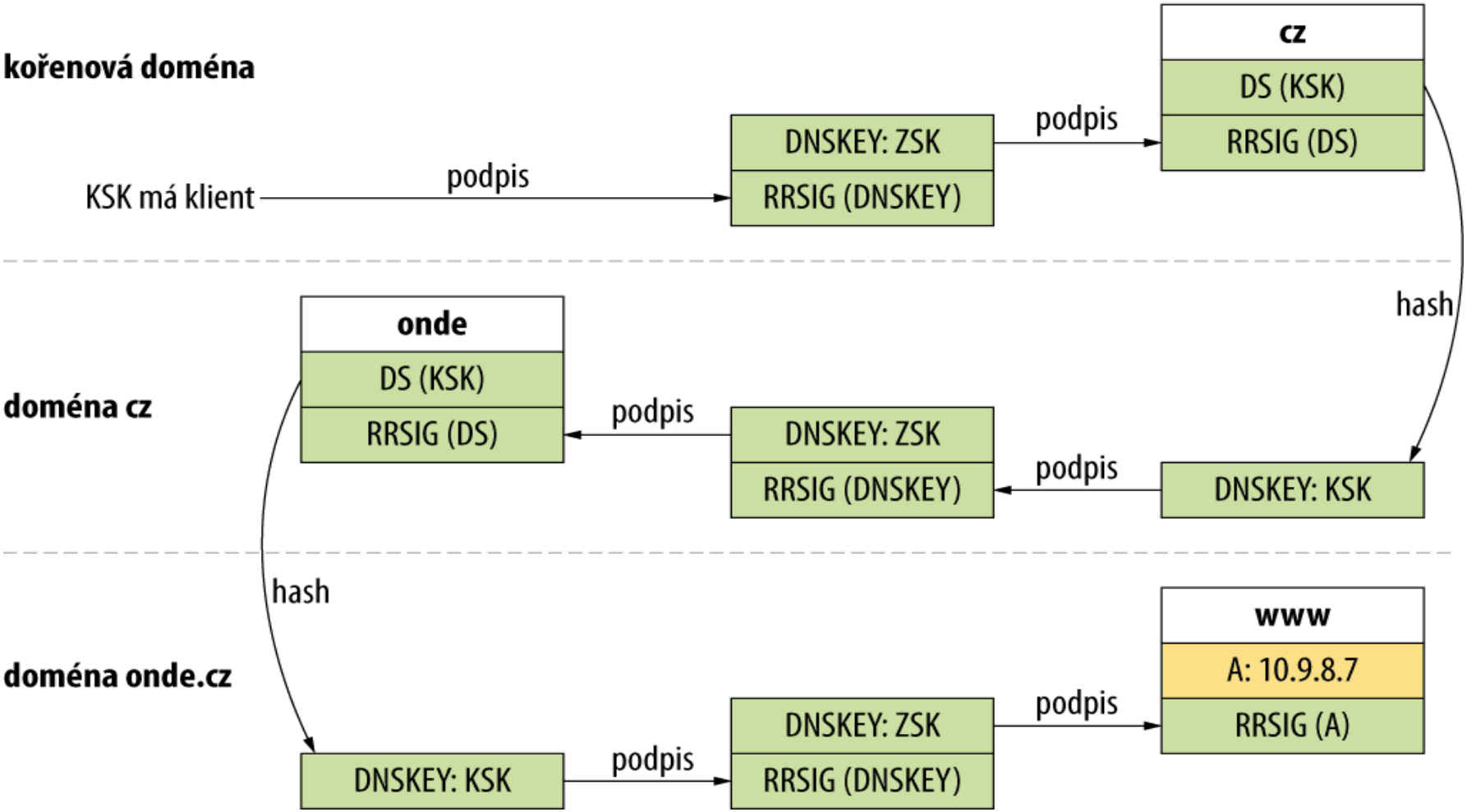
Zverejnenie kľúčov

- Dôležité pre vybudovanie reťaze dôvery
- Predať nadradenej zóne, ak podporuje DNSSEC
  - V ČR podporuje DNSSEC 3-8 registrátorov
- Špeciálny dočasný register – DLV
  - Pre operátorov TLD existuje samostatný register-ITAR

Reťaz dôvery

- Reťazec overených DS a DNSKEY záznamov
- Začína v pevnom bode dôvery (trust anchor)
- Končí pri kľúči, ktorý podpísal overovaný RRset

Reťaz dôvery



Vytvorenie reťaze dôvery

- Pri delegácii sa odosielajú okrem NS aj DS záznamy
- V potomkovi resolver skontroluje KSK DNSKEY
  - V rámci overovania buď ďalšej delegácie alebo dat
- Reťaz dôvery sa začína stavať v pevnom bode dôvery
  - Nakonfigurovaný v resolveri
  - Ak sa resolver dostane do podpísanej zóny nebezpečnou delegáciou, skúsi DLV

DLV a ITAR

- Nadradená zóna nepodporuje DNSSEC
- Zverejním svoj KSK v DLV (Domain Lookaside Validation)
  - Doména dlv.isc.org, záznamy odpovedajú menám zón
    - nic.cz.dlv.isc.org
- TLD sa zverejňujú v ITAR (do podpísania root zóny)
  - ITAR je offline, je potrebné sledovať zmeny

Výmena kľúčov

- Neexistuje revocation list
- Životnosť kľúča neobmedzená
- Doporučuje sa meniť
  - Frekencia výmen podľa dĺžky kľúča....
- Na výmenu opatrne!
  - Aktuálne kľúče a podpisy sú nacachované po svete
  - Ak zrazu prestane existovať kľúč, validujúce resolvery nebudú schopné validovať

Výmena kľúčov

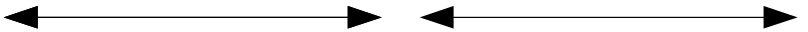
- 2 rôzne postupy
  - Predpublikovanie (pre-publish)
    - Obvykle na výmenu ZSK
  - Dvojitý podpis (double signature)
    - Obvykle na výmenu KSK

Pre - publish

- Nový kľúč sa zverejní v zóne, nepoužíva sa k podpisovaniu
- Po rozšírení po DNS strome sa zóna prepodpíše novým kľúčom, starý v nej ostane
- Po čase sa odstráni starý kľúč

Pre - publish

initial	new DNSKEY	new RRSIGs	DNSKEY removal
SOA0	SOA1	SOA2	SOA3
RRSIG10(SOA0)	RRSIG10(SOA1)	RRSIG11(SOA2)	RRSIG11(SOA3)
DNSKEY1	DNSKEY1	DNSKEY1	DNSKEY1
DNSKEY10	DNSKEY10	DNSKEY10	DNSKEY11
	DNSKEY11	DNSKEY11	
RRSIG1 (DNSKEY)	RRSIG1 (DNSKEY)	RRSIG1(DNSKEY)	RRSIG1 (DNSKEY)
RRSIG10(DNSKEY)	RRSIG10(DNSKEY)	RRSIG11(DNSKEY)	RRSIG11(DNSKEY)



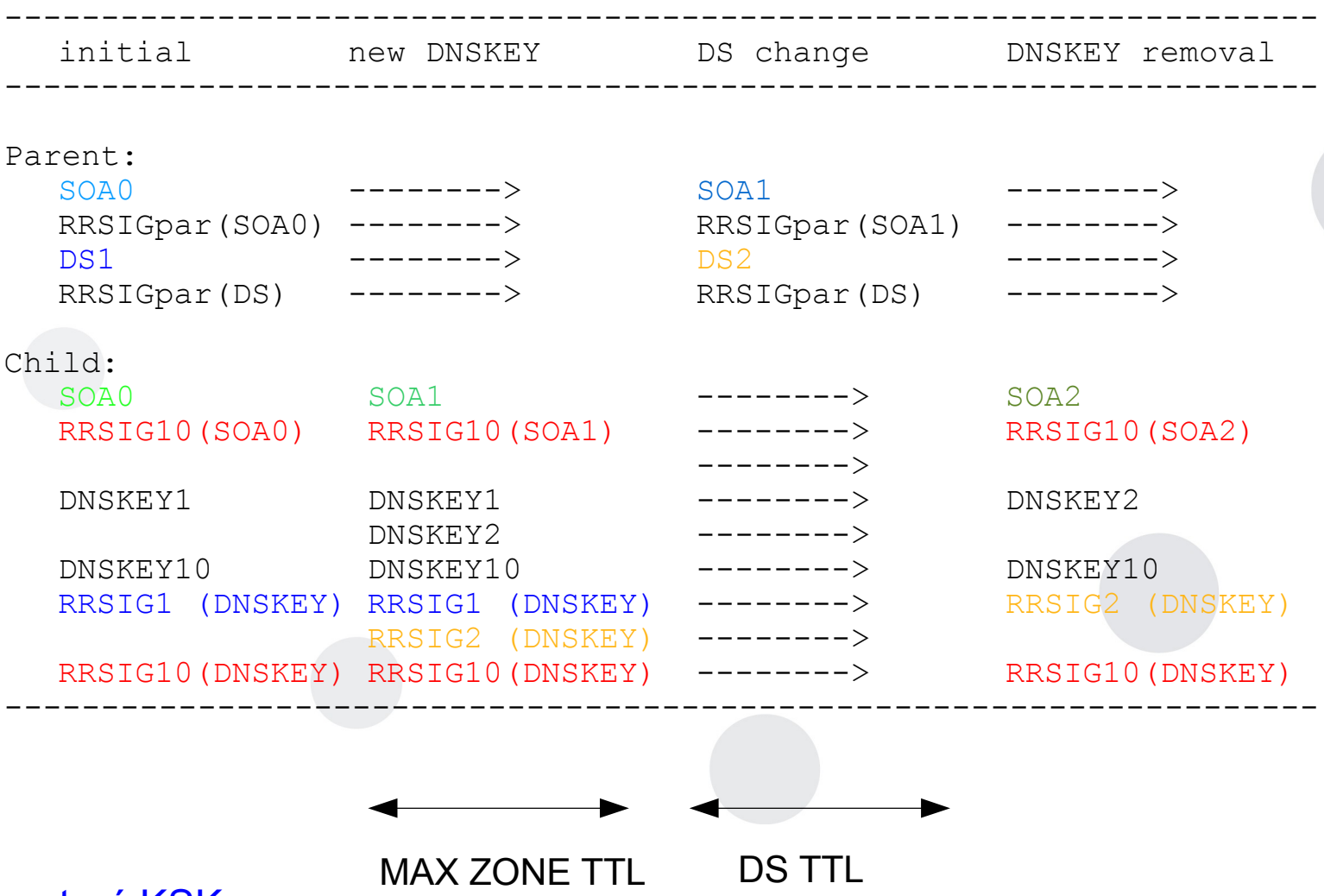
DNSKEY TTL MAX ZONE TTL

1 – KSK
10 – starý ZSK
11 – nový ZSK

Dvojitý podpis

- Do zóny sa pridá nový kľúč a sú vytvorené podpisy starým aj novým kľúčom
- Po uplynutí doby sa starý kľúč odstráni a ostanú len podpisy novým kľúčom
- Výmena KSK – nie je nutné mať 2 podpisy pre všetky RRSety, len pre DNSKEY RRset

Dvojitý podpis – výmena KSK



1 – starý KSK
10 – ZSK
2 – nový KSK

DNSEC – údržba zóny

- „Ručne“ príliš namáhavé
- Podpisovanie – existuje niekoľko nástrojov
- Sledovanie zmien pevných bodov dôvery
  - Trustman / dnssec-tools.org
- Automatizované výmeny kľúčov
  - Roller / dnssec-tools.org
- …

DNSSEC pre bežného užívateľa

DNSSEC pre bežného užívateľa

- Ak funguje, tak to užívateľ nepozná...
- .... spozná to, až to fungovať prestane
  - SERVFAIL ak zlyhá validácia
- Zatiaľ málo aplikácií, ktoré využívajú DNSSEC
  - Existuje niekoľko patchov od dnssec-tools.org
    - Firefox, Thunderbird, ssh, postfix, sendmail, wget....

DNSSEC pre bežného užívateľa

- DNSSEC Firefox plugin
  - Alfa
  - 3.0, 3.5
  - http://labs.nic.cz/page/691/dnssec-doplnek-pro-firefox/

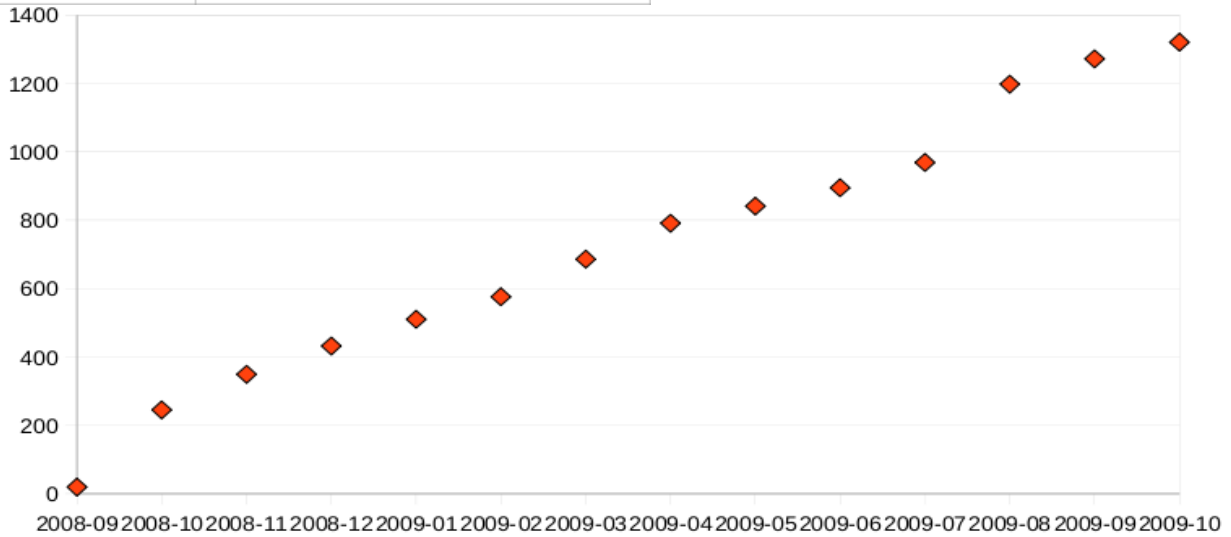
Validujúce resolvery

- U providerov minimálne
- Sputiť si vlastný validujúci resolver
  - Domáce zariadenie
    - Možnosť otestovať
    - http://www.dnssec-tester.cz/
- Použiť validujúce resolvery tretích strán
  - DNS OARC
    - 3 kusy, 149.20.64.20-22
  - CZ NIC
    - 1 kus, dočasne na 217.31.57.6

DNSSEC v „cz.“ a „.“

DNSEC v ČR

Měsíc	Domén v zóně	Zabezpečeno DNSSEC
2008-09	471748	19
2008-10	483288	245
2008-11	491900	349
2008-12	501355	432
2009-01	513132	510
2009-02	524992	576
2009-03	537567	686
2009-04	550328	791
2009-05	560070	841
2009-06	570297	895
2009-07	579294	969
2009-08	589083	1198
2009-09	599300	1272
2009-10	604535	1321



DNSSEC v ČR

- Oficiálne 3 registrátori
- Najznámejšie nedávno podpísané zóny
  - ihned.cz a poddomény
  - Exekutorská komora ČR a ich portaldrazeb.cz
- Hypoteční banka

DNSSEC vo svete

- Podpísaných niekoľko TLD domén
  - .cz, .br, .bg, .th, .pr, .se, .ch, .li, .na, .nu
  - .gov, .org, (.museum)
- Nedávno spustila testovací režim Kanada (.ca)
  - NSEC3, na samostatných NS
- Root zóna zatiaľ nepodpísaná
- Ale....

DNSSEC - root zone

- Cca v polovici 2009 ICANN oznámil, že root bude podpísaný do konca roka
- 10/2009 na konferencii RIPE 59 v Lisabone bol predvedený konkrétny plán

DNSSEC – root zone

- Začne podpisovať 1.12.2009, len interne, testovanie procesov
- 1.1.2010-1.7.2010 – podpísaná zóna dostupná verejne, ale kľúč nezverejnený
  - Resp. zverejnený vo forme:

```
. 3600 IN DNSKEY 256 3 5 (
AwEAAa++++++++++++++++++++++++++++++
++THIS/KEY/AN/INVALID/KEY/AND/SHOULD
/NOT/BE/USED/CONTACT/ROOTSIGN/AT/ICA
NN/DOT/ORG/FOR/MORE/INFORMATION+++++
++[.....]++++/=
) ; Key ID = 6477
```

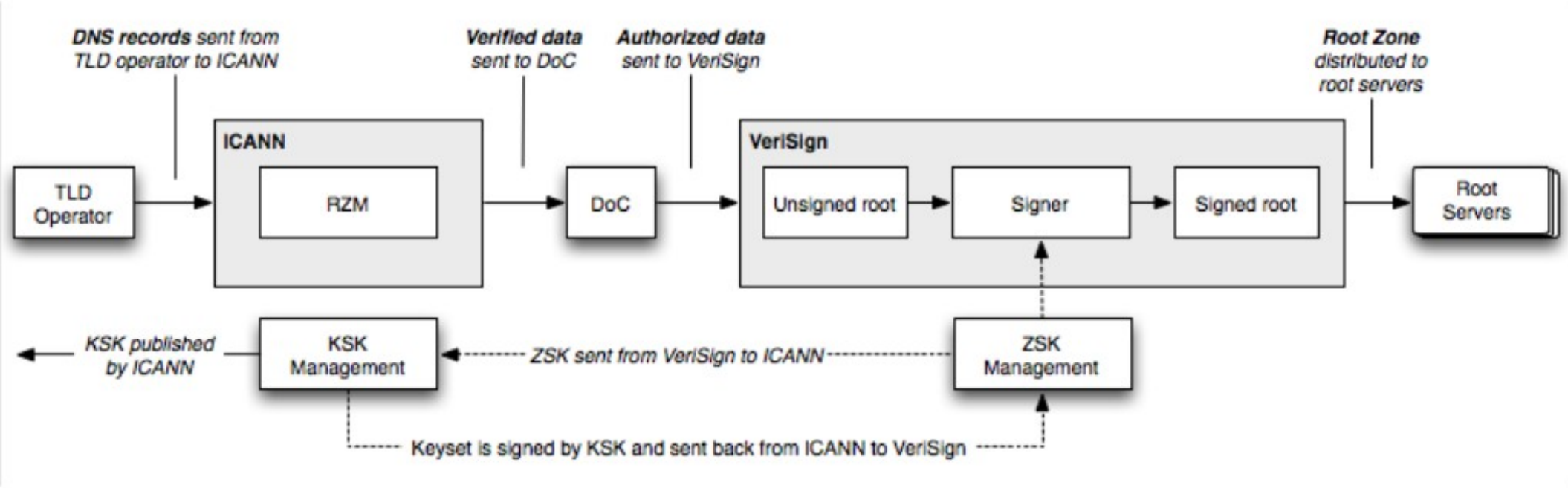
DNSSEC – root zone

- „Podpísaná“ zóna sa začne distribuovať najprv na L.root-servers.net,, postupne až k A
  - A je najviac zaťažený, pravdepodobne kvôli chybnej implementácii DNS v niektorých klientoch
- Tento proces skončí 7/2010
  - Root sa podpíše validnými kľúčmi, ktoré sa zverejnia

DNSSEC – root zone

- ICANN/IANA – bude držať KSK kľúče a príjmať zmeny v DS záznamoch
- DoC NTIA – bude schvaľovať zmeny v DS záznamoch a zmeny v kľúčoch root zóny
- VeriSign – bude spravovať ZSK a podpisovať root zónu

DNSSEC – root zone



- KSK – 2048b, RSA/SHA-256
  - Výmena 2-5 rokov
- ZSK – 1024b, RSA/SHA-256, NSEC
  - 4 výmeny ročne

Ďakujem za pozornosť

Matej Dioszegi
CZ NIC
matej.dioszegi@nic.cz

www.nic.cz