DNSSEC: implementace a přechod na algoritmus ECDSA

Konference Internet a Technologie 2017
21. 6. 2017

Martin Švec
ZONER software, a.s.
martin.svec@zoner.cz

Zoner

ZONER software, a.s.

- **Na trhu od roku 1993**
- **Divize software**
  - Zoner Photo Studio X
- **Divize internetových služeb**
  - CZECHIA.COM
  - registrátor domén, webhosting, serverhosting
  - e-commerce, cloudové služby
  - SSL certifikáty
- **Vydavatelství Zoner Press**

Zoner

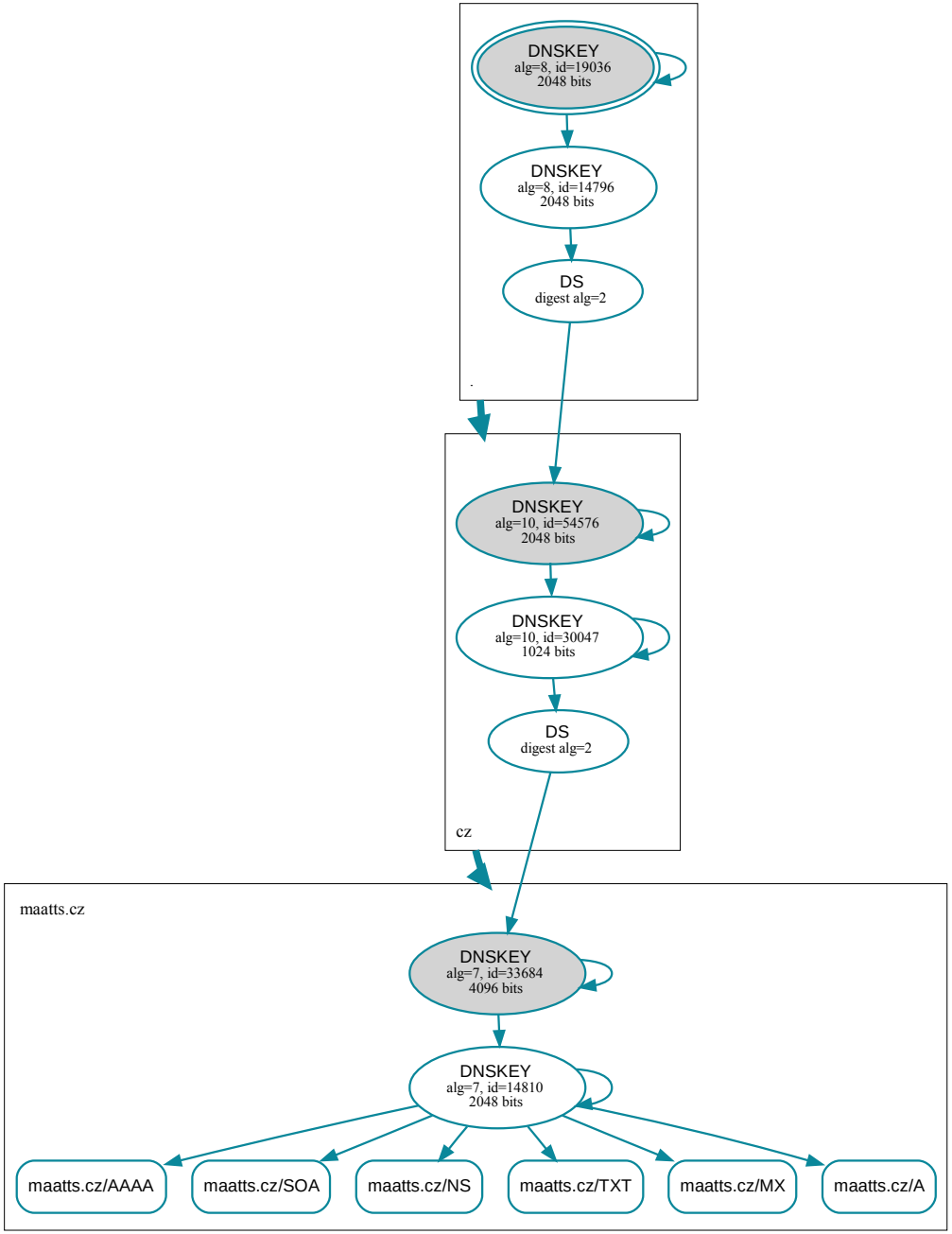
DNSSEC

- **Bezpečnostní rozšíření protokolu DNS**
- **Asymetrická kryptografie**
  - RSA
  - ECDSA
- **Řetěz důvěry od kořenové zóny k listům**
  - autenticita DNS záznamů
  - detekce změn při přenosu

Zoner

DNSSEC

- **DNSKEY**
  - veřejné klíče
  - KSK, ZSK
- **DS**
  - delegace v nadřazené zóně
- **RRSIG**
  - podpisy RRsetů
- **NSEC/NSEC3**

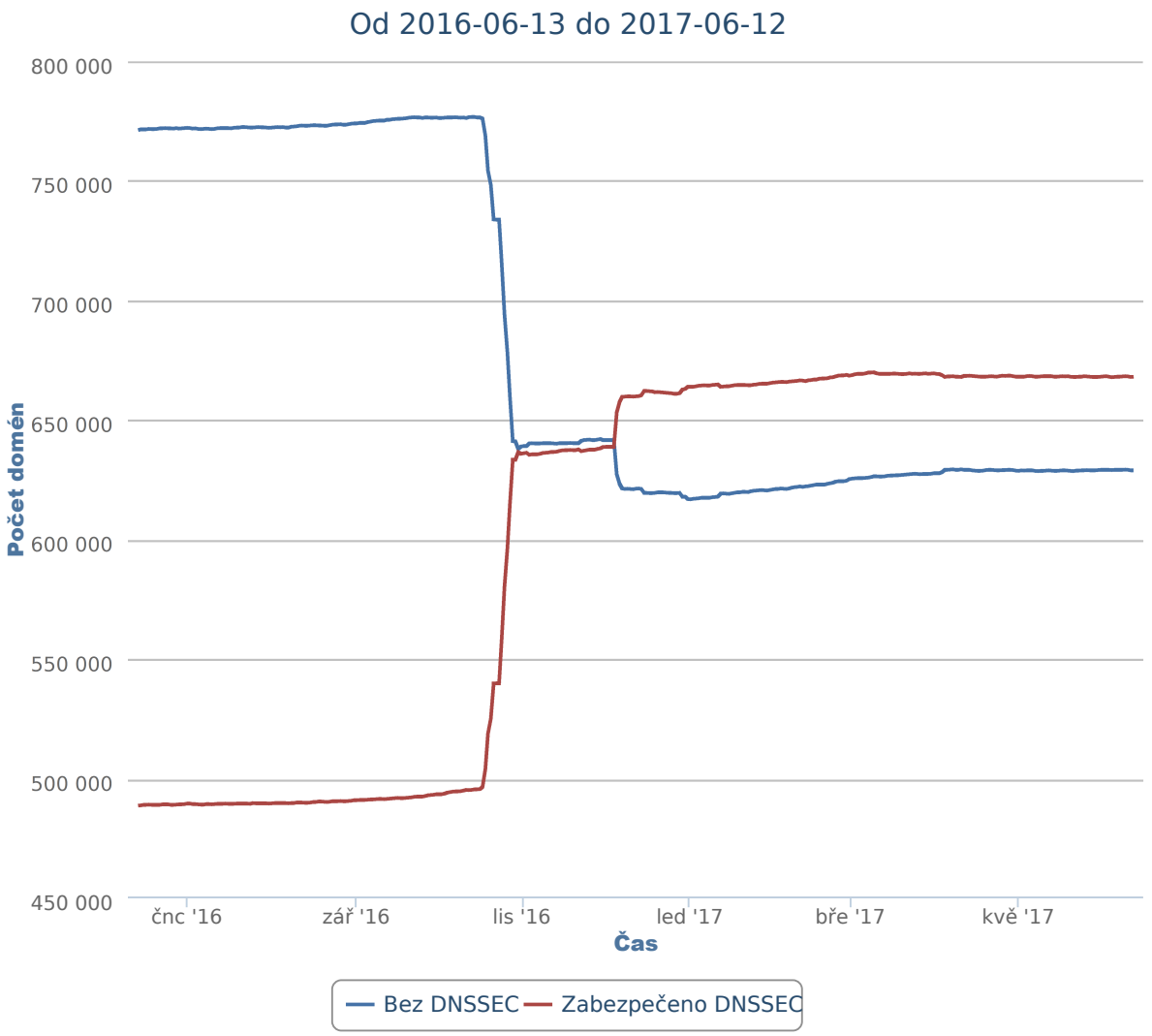


Zoner

DNSSEC v .CZ zóně

Stav k 13.6.2017:

- 668 210 zón
- 51.51%



Zoner

Eliptické křivky

- **Elliptic Curve Digital Signature Algorithm (ECDSA)**
  - založen na ECC (elliptic curve cryptography) místo RSA
- **Asymetrické šifrování**
  - princip jako RSA
  - privátní a veřejný klíč
  - hledání diskrétního logaritmu náhodného elementu eliptické křivky s ohledem na známý základní bod (Wikipedie)
  - Neal Koblitz, Victor S. Miller, 1985
- **NIST**
  - P-192, P-256, P-384, P-521 (RFC 5114)

Eliptické křivky v DNSSEC

- **RFC 6605 – duben 2012**
- **Přidány algoritmy 13 a 14**
  - ECDSAP256SHA256 (alg. 13)
  - ECDSAP384SHA384 (alg. 14)
- **Implementace**
  - podpora v autoritativních nameserverech
  - podpora v DNS resolverech
  - podpora v TLD registrech

Zoner

Přednosti ECDSA

- **Bezpečnost**
  - ECDSA P-256: síla cca jako RSA 3072
  - nejsou nutné časté rotace
  - lze použít jen jeden klíč místo KSK + ZSK
- **Velikost záznamů**
  - velikost zónových souborů
  - DNS reflection útoky
  - fragmentace paketů
- **Rychlost podepisování**
  - online podpisy

Problémy ECDSA

- **(Ne)podpora v DNS resolverech**
  - resolvery vracející „INSECURE“ = „nepodepsaná“ zóna
  - chyba v dnsmasq 2.72 – 2.74
- **Pomalejší ověřování?**
  - vyšší nároky na resolvery – nezaznamenali jsme...
- **Výměna algoritmu (algorithm rollover)**
  - komplikace při přechodu od RSA na živé sadě zón

Podpora ECDSA v resolverech

- **https://stats.labs.apnic.net/ecdsa**
- **Česká republika (k 13.6.2017)**
  - 34.66% validuje RSA
  - 30.75% validuje ECDSA
  - 27.57% validuje RSA i ECDSA
- **dnsmasq?**
  - zanedbatelné množství...

Zoner

Výměna algoritmu

- **RFC 6781, sec. 4.1.4**
  - nelze provést prostou rotaci klíčů!
- **Dvojí podpis všech zón**
  - staré verze Unboundu zóny bez dvojího podpisu označí jako „BOGUS“
  - dočasné zdvojnásobení velikosti zóny
  - pět kroků pro výměnu všech KSK a ZSK klíčů
  - prodlevy pro uvolnění starých záznamů z cachí

Vstupní podmínky

- **Nameservery Zoneru (11/2016)**
  - celkem zón: 112.000
  - podepsaných zón: 43.200
  - podepsaných .CZ zón: 30.500
  - podepsaných .EU zón: 12.700
  - NSD, velikost nsd.db: 329 MiB
- **Změna algoritmu**
  - původní: RSA 4096/2048 (alg. 7)
  - nový: ECDSAP256SHA256 (alg. 13)

Zoner

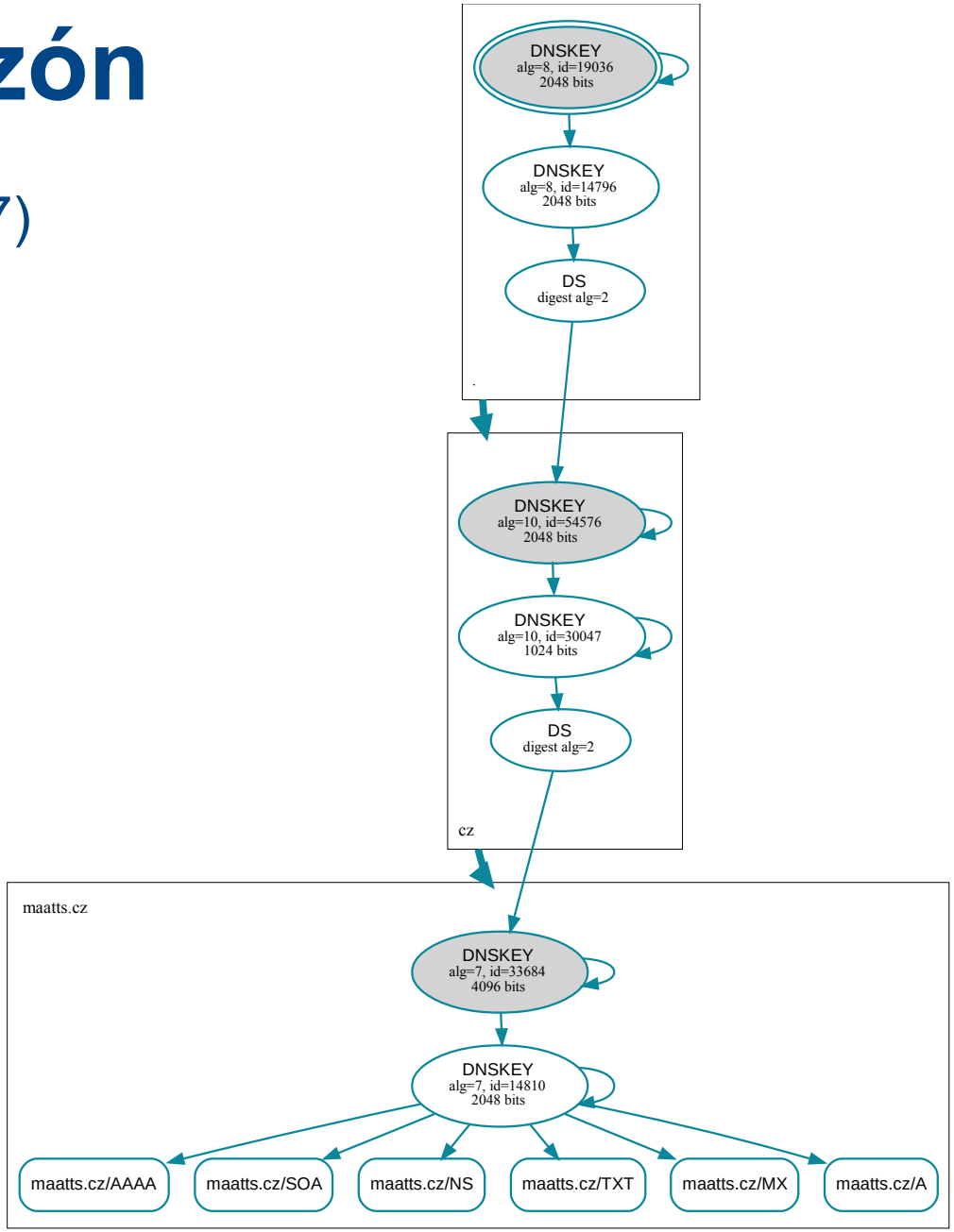
Implementace

- **Na straně Zoneru**
  - každá zóna má stavový automat rotace klíčů, řízeno z db
  - využití aktivního a pasivního ZSK z běžné rotace
  - rozšíření tabulky zón o druhý KSK
  - rozšíření stavového automatu o stavy výměny algoritmu
- **Na straně CZ.NICu**
  - objekt KEYSET
  - výměna DS záznamů pro všechny zóny naráz :-)

Zoner

Výchozí stav .CZ zón

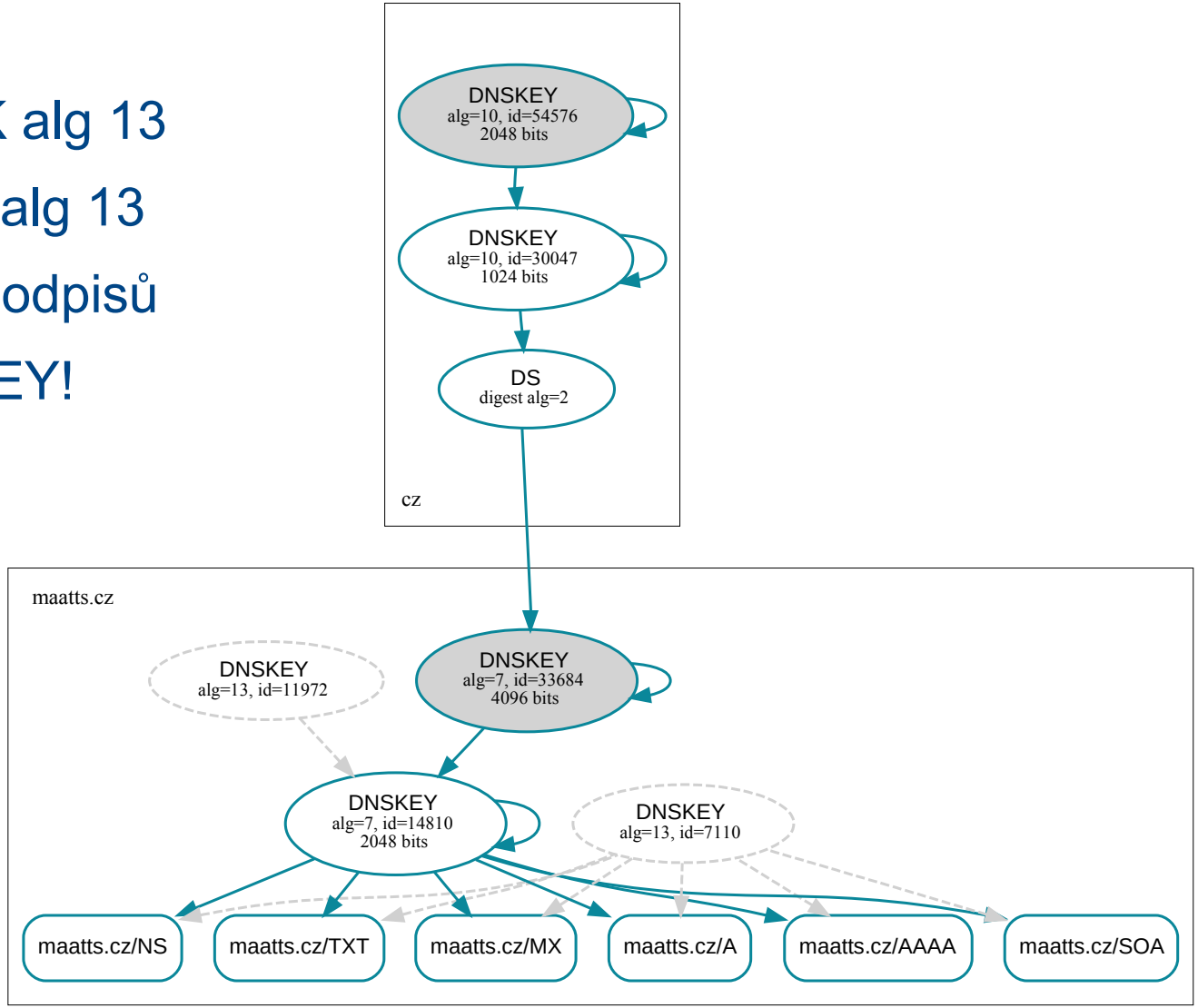
- RSASHA1-NSEC3-SHA1 (alg 7)
- KSK 4096 bitů
- ZSK 2048 bitů



Zoner

1. Nové klíče a RRSIGy

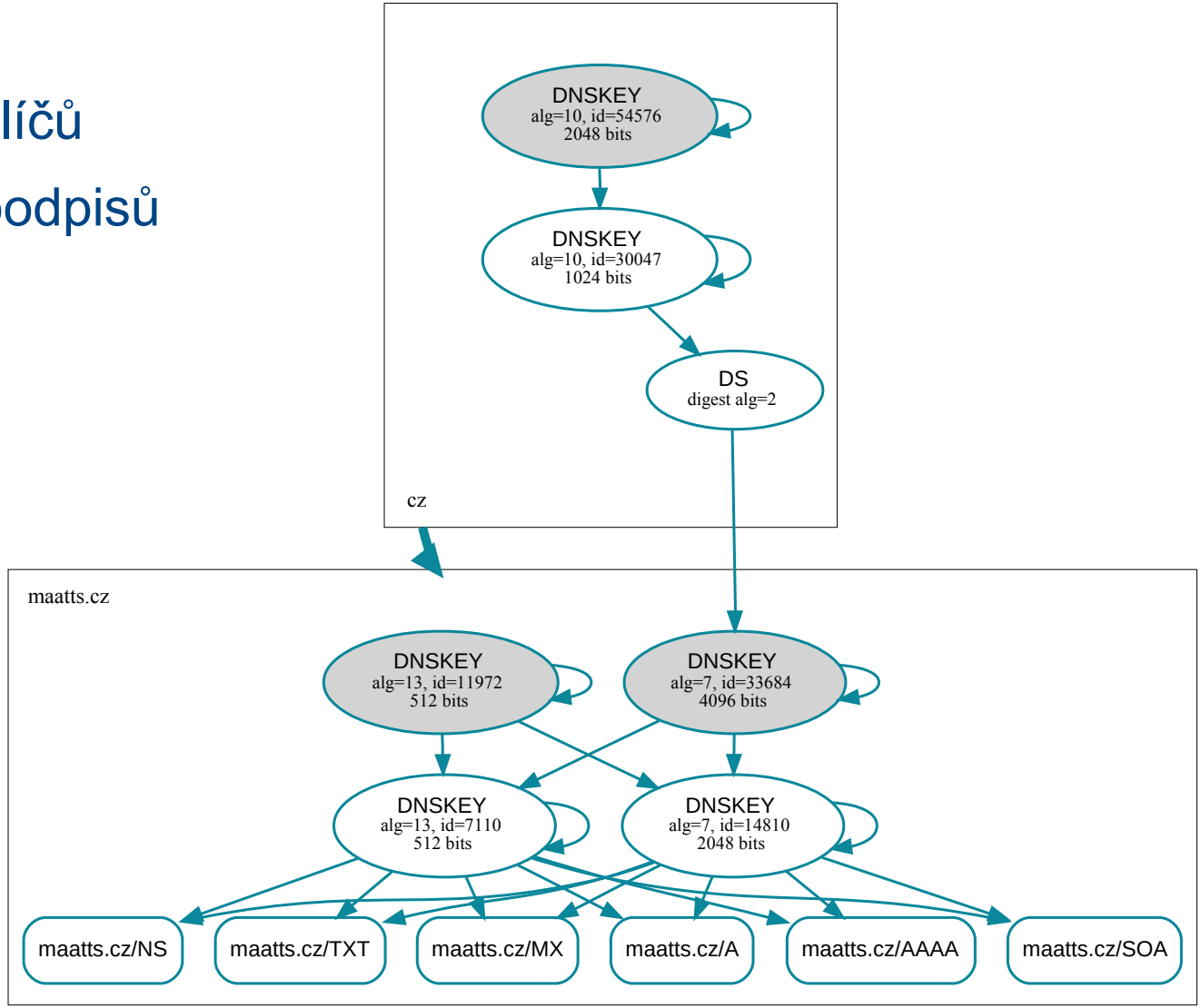
- 28.11.2016
- nový společný KSK alg 13
- vygenerování ZSK alg 13
- publikace dvojích podpisů
- pouze staré DNSKEY!



Zoner

2. Publikace nových DNSKEY

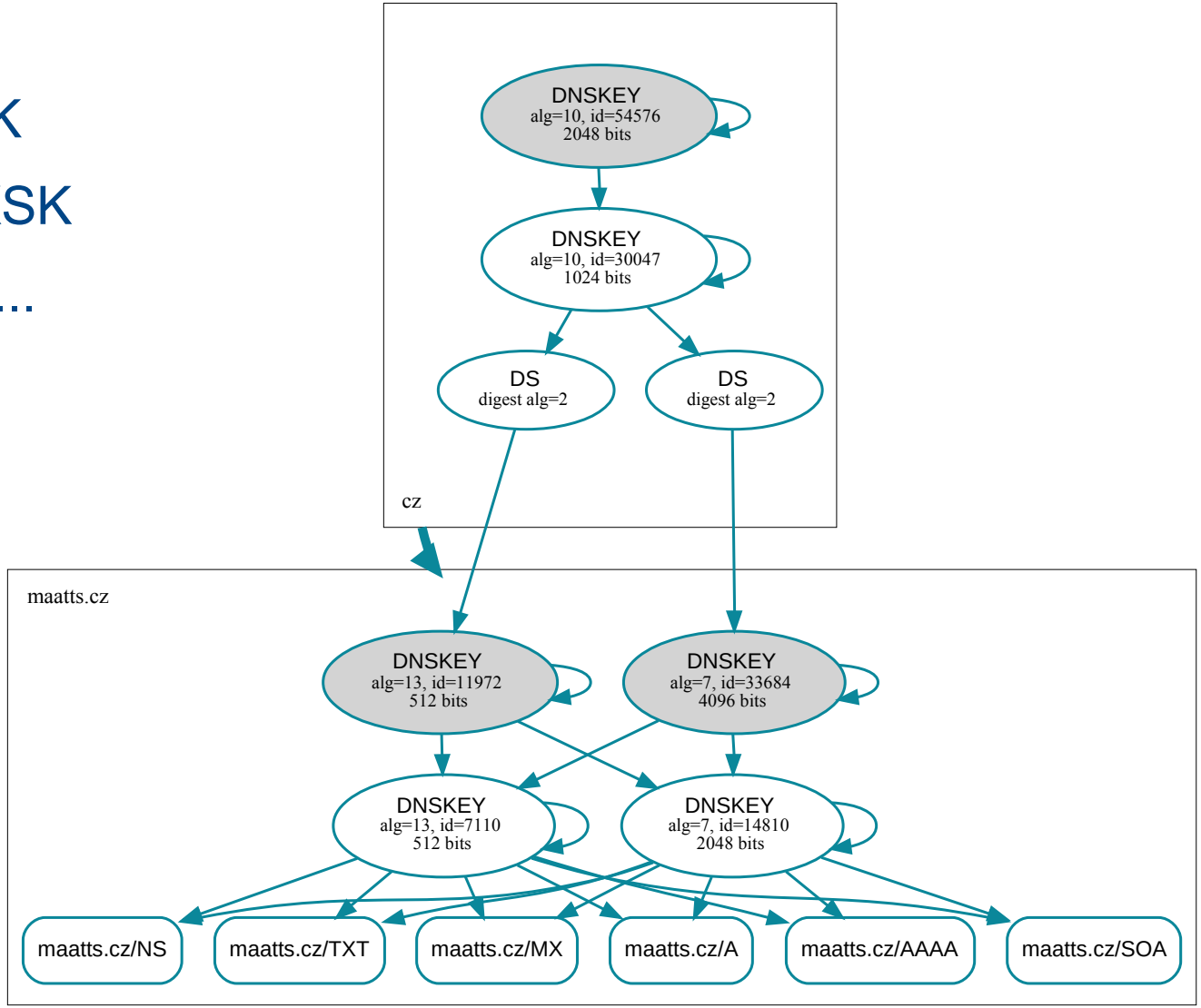
- 29.11.2016
- publikace dvojích klíčů
- publikace dvojích podpisů



Zoner

3. Výměna klíče v KEYSETu

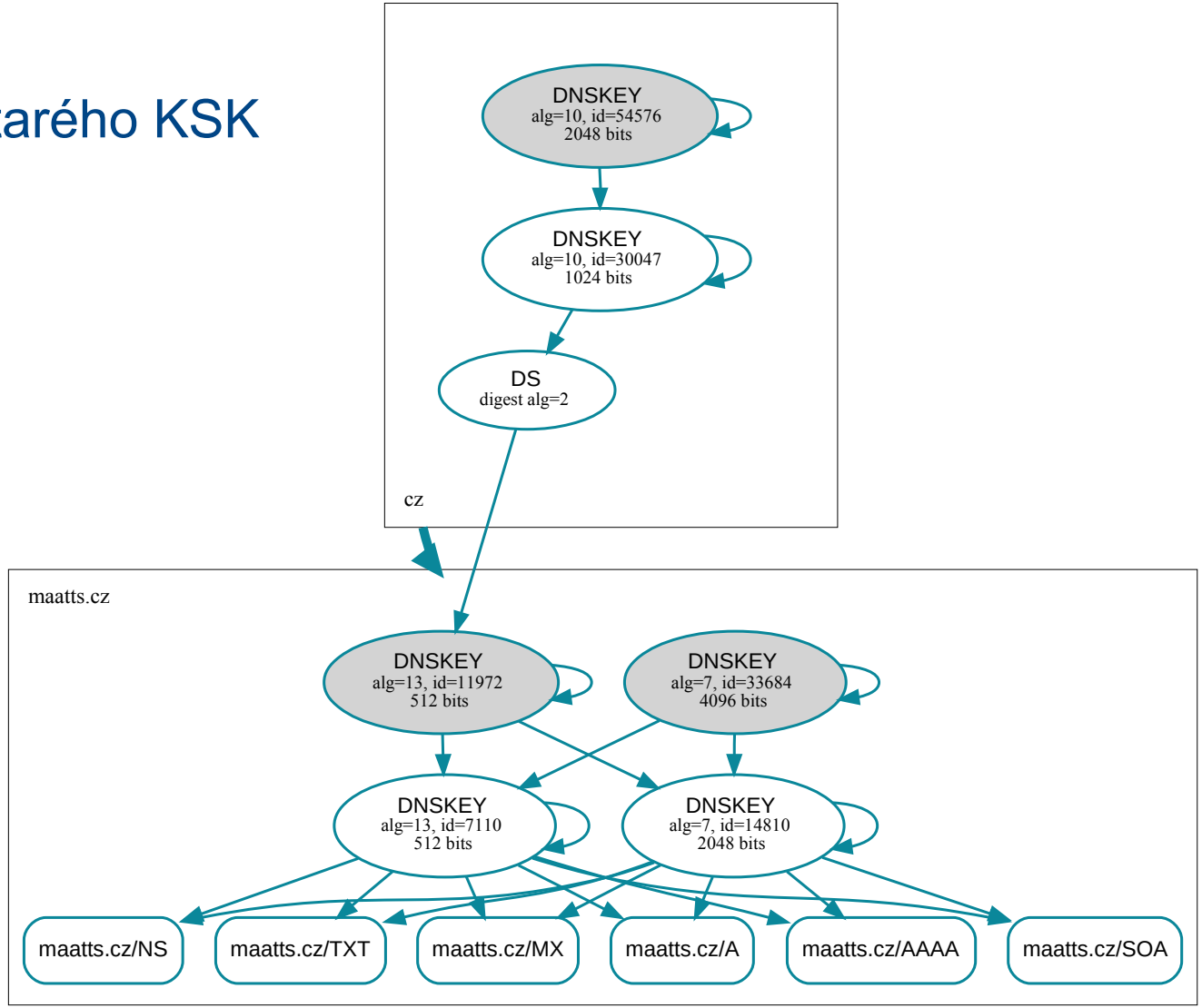
- 1.12.2016
- přidání nového KSK
- odebrání starého KSK
- lze v jednom kroku...



Zoner

3. Výměna klíče v KEYSETu

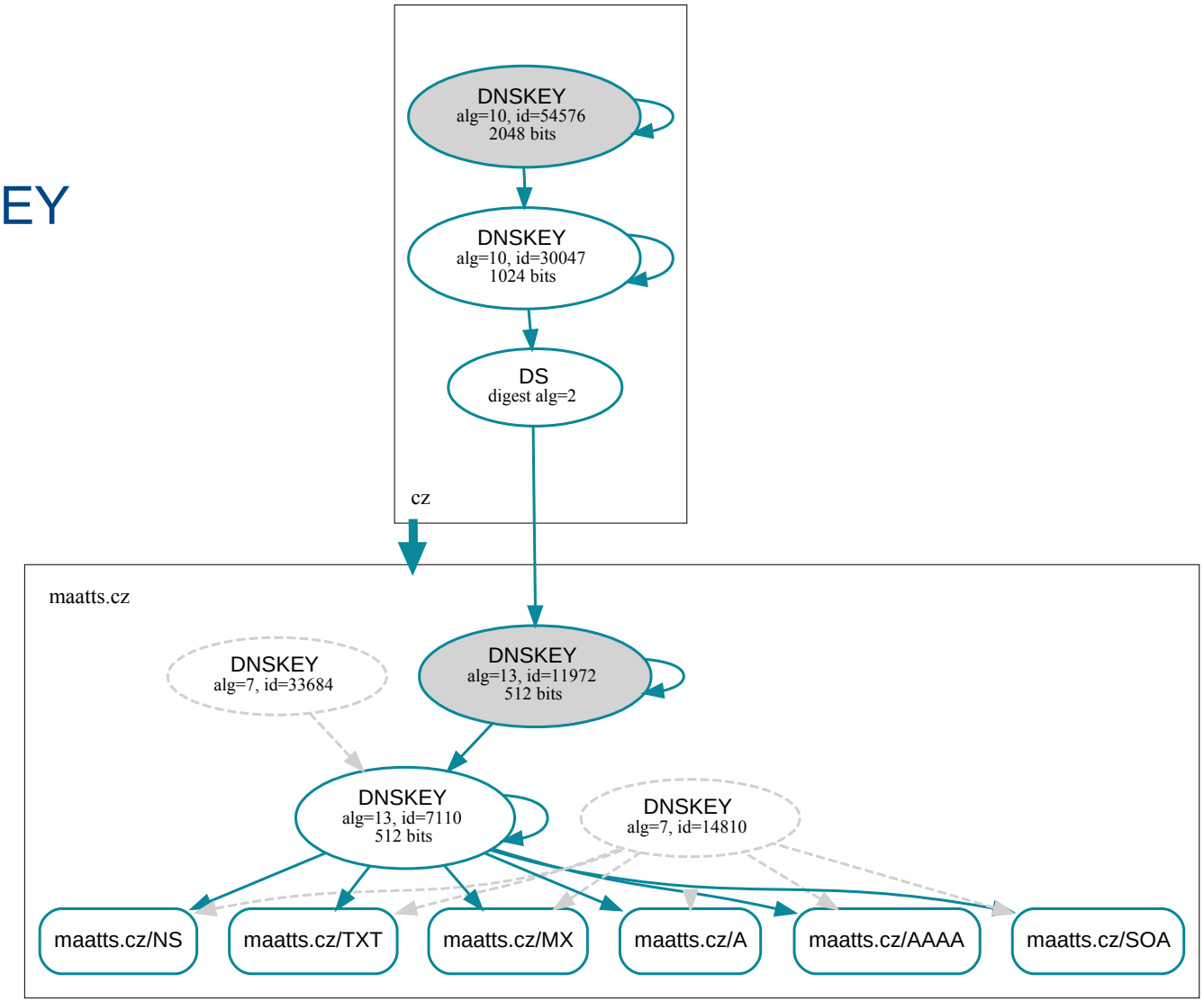
- 1.12.2016
- stav po odebrání starého KSK



Zoner

4. Odebrání starých DNSKEY

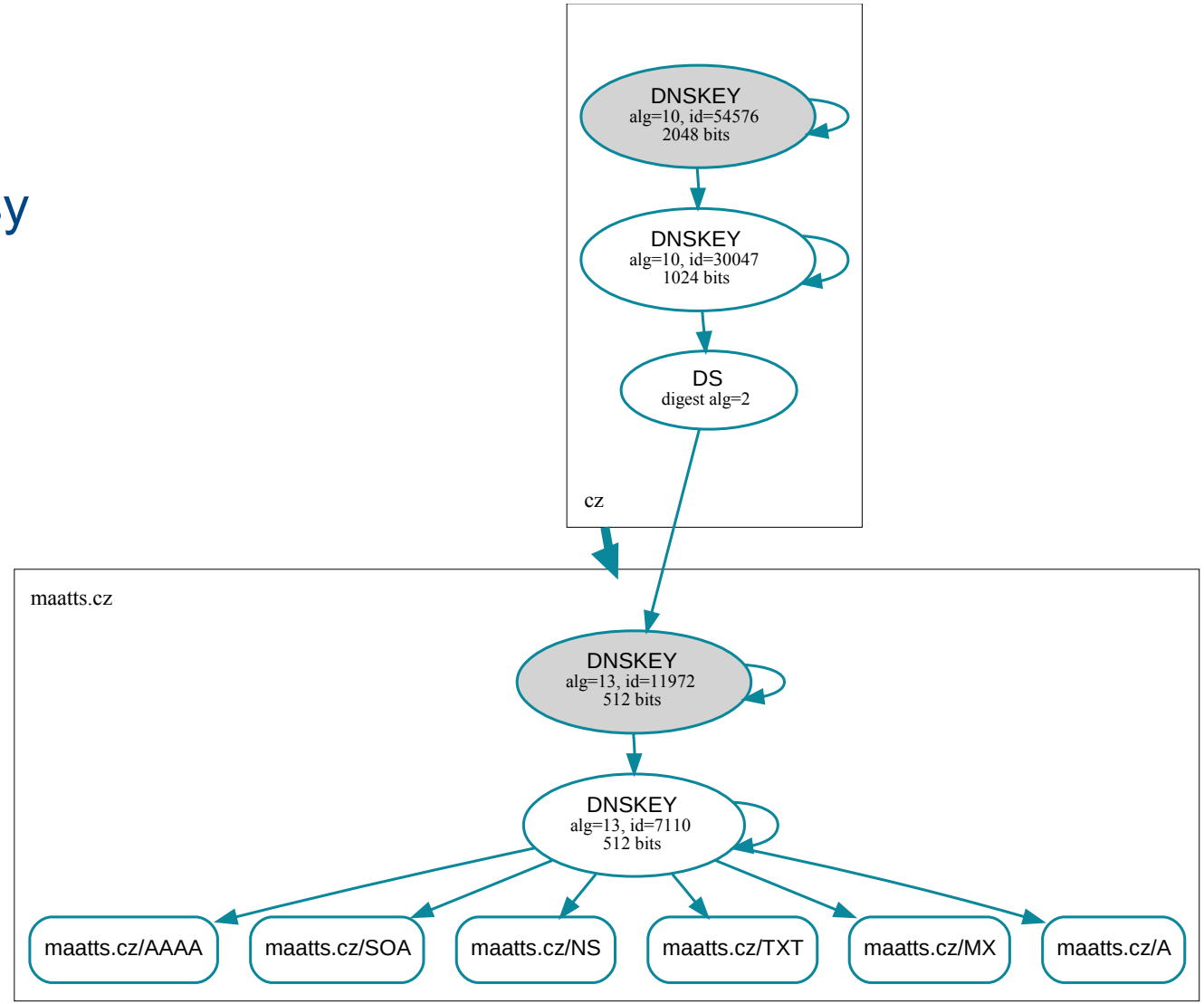
- 13.12.2016
- dvojí RRSIGy
- pouze nové DNSKEY



Zoner

5. Finální stav

- 14.12.2016
- pouze nové klíče
- pouze nové podpisy



Přechod na ECDSA u .EU

- cca 12.700 zón
- identický postup jako u .CZ
- konec prosince 2016

Zoner

Výsledky přechodu na ECDSA

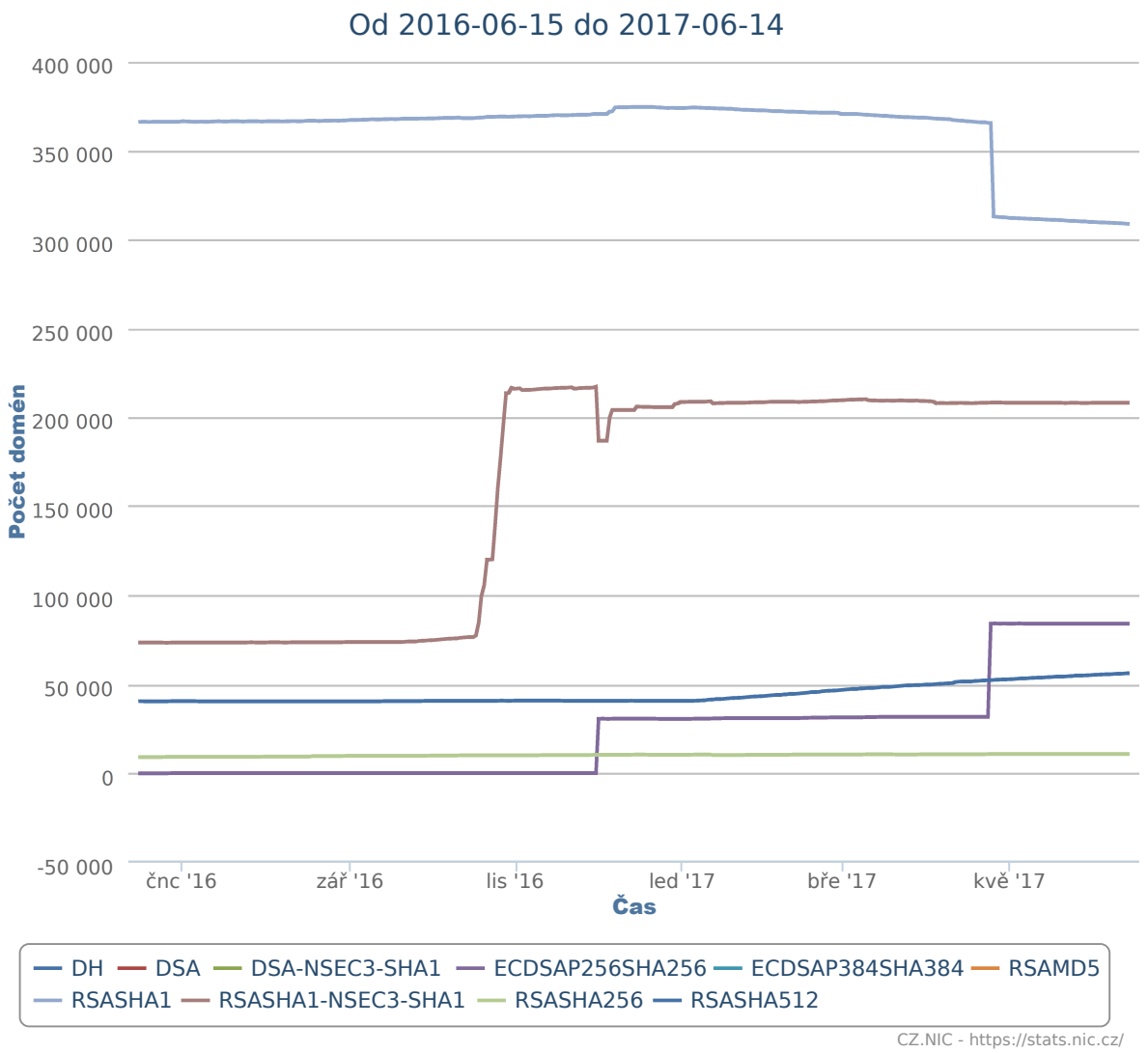
- původní velikost nsd.db: 329 MiB
- maximální velikost při rolloveru: 393 MiB
- finální velikost nsd.db: 164 MiB
- zkrácení doby kompilace zón: cca o 30%
- žádné negativní odezvy
- žádné nepředvídané komplikace

Zoner

DNSSEC algoritmy v .CZ

Stav k 13.6.2017:

- 84 107 ECDSA
- 12.59%



Zoner

Děkuji za pozornost

Zoner