Pět kroků k elipse

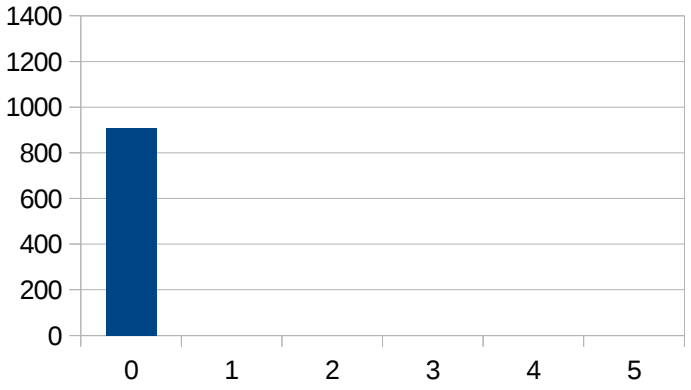
Výměna DNSSEC klíče v doméně .CZ se změnou algoritmu na ECDSA

Jaromír Talíř • jaromir.talir@nic.cz • 12. 6. 2018

Výměna KSK v .CZ

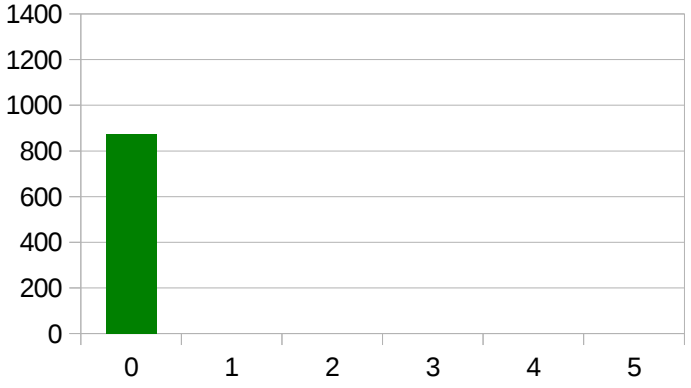
- 4. 6. – 8. 6. 2018
- **Třetí** výměna KSK v .CZ
- **Druhá** výměna KSK v .CZ se změnou algoritmu
- **První** nasazení algoritmu ECDSA založeného na eliptických křivkách v TLD na světě
- Detaily o důvodech na blogu: https://blog.nic.cz/2018/05/30/prechod-na-eliptic ke-krivky-v-domene-cz/

Začátek



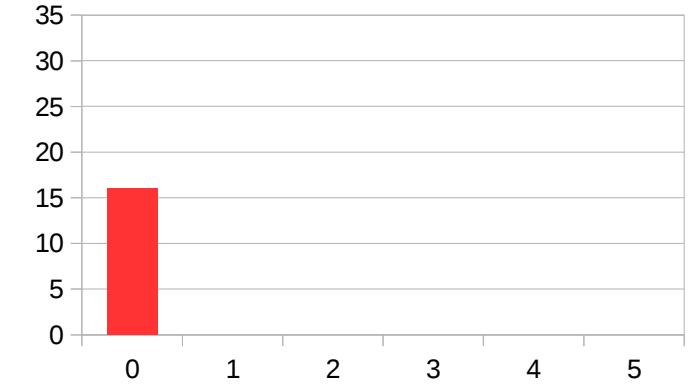
Velikost DNSKEY odpovědi

907 B



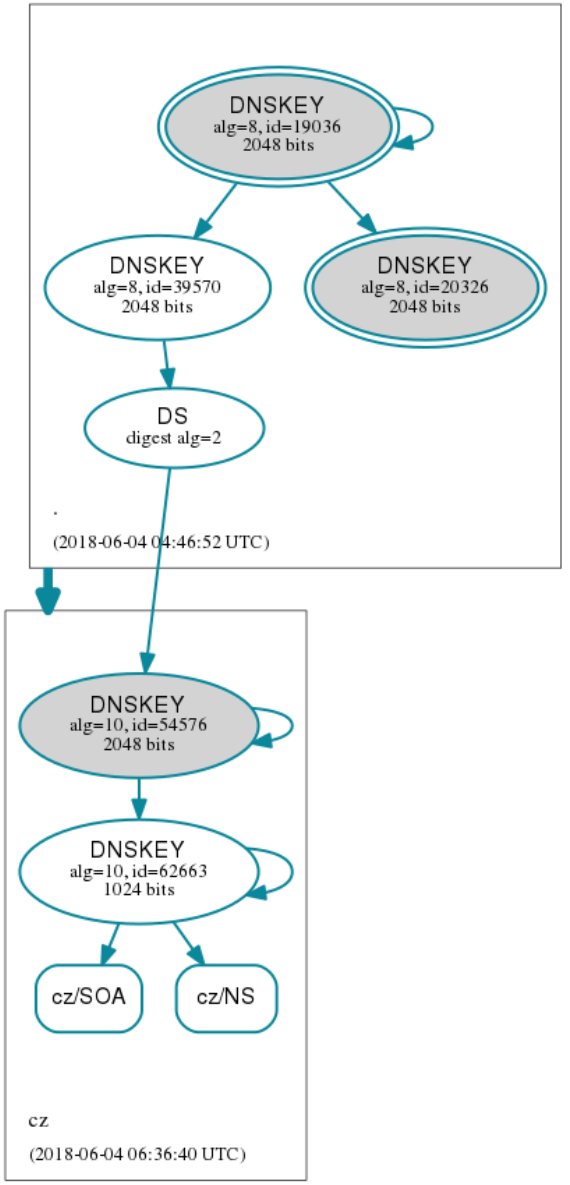
Velikost zóny s podpisy

875 MB

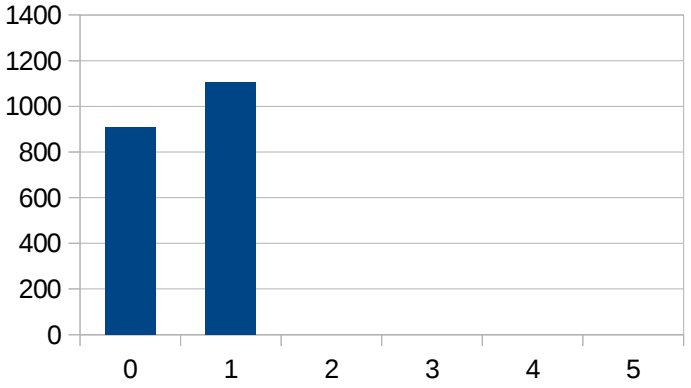


Doba publikace

15 min

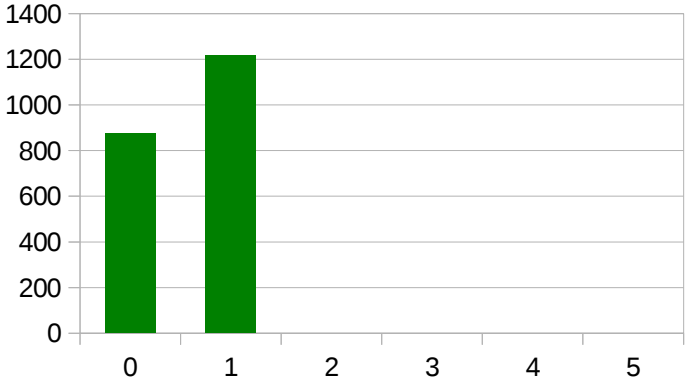


Krok 1 - publikace ECDSA podpisů



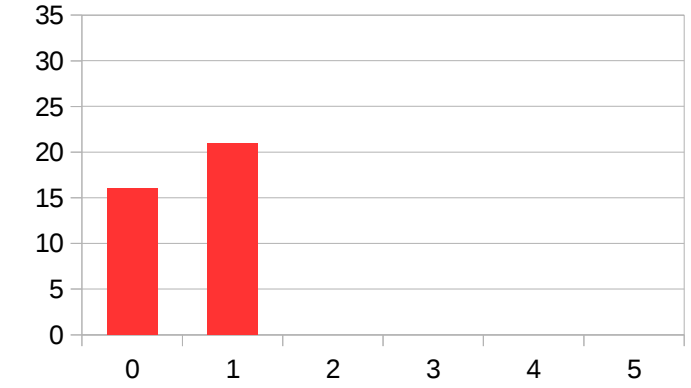
Velikost DNSKEY odpovědi

1103 B



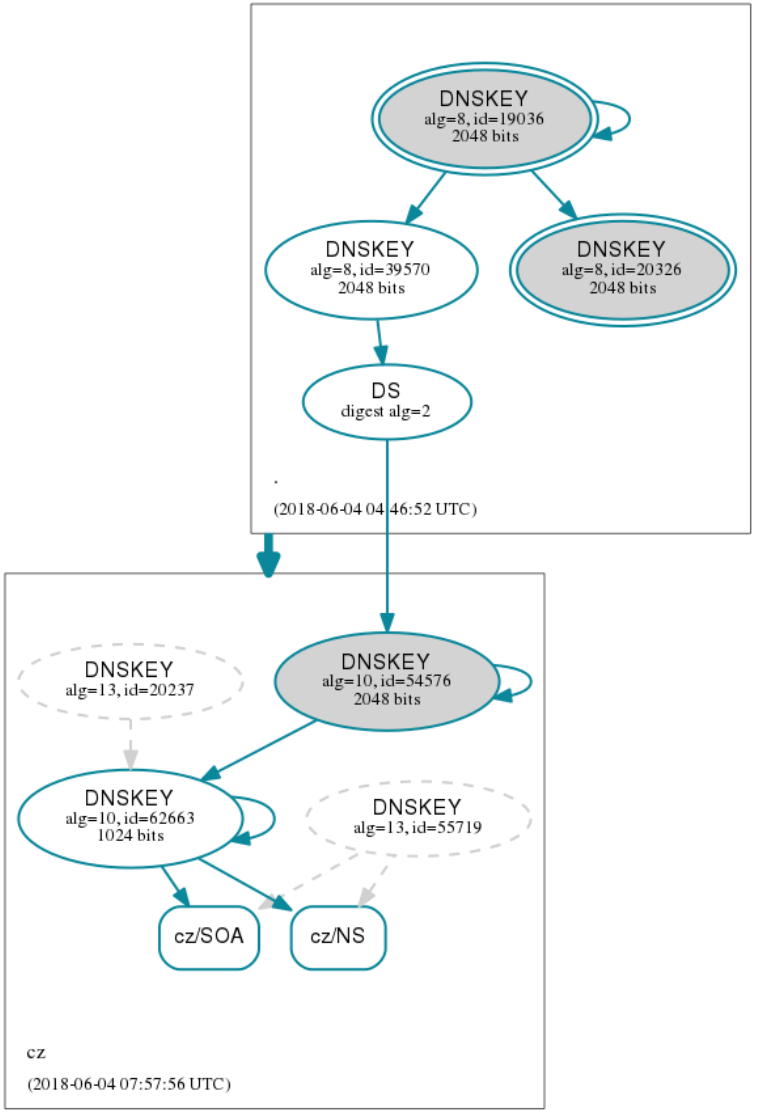
Velikost zóny s podpisy

1217 MB

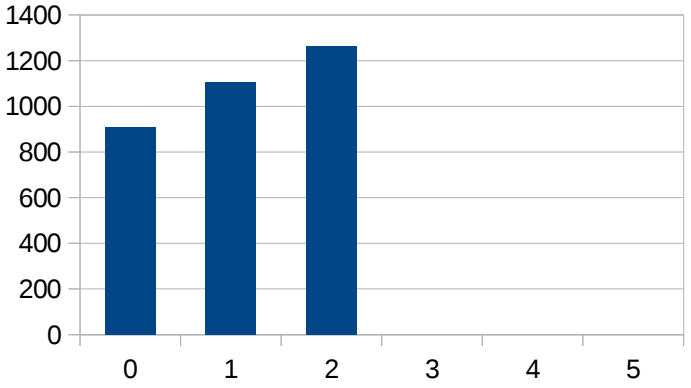


Doba publikace

21 min

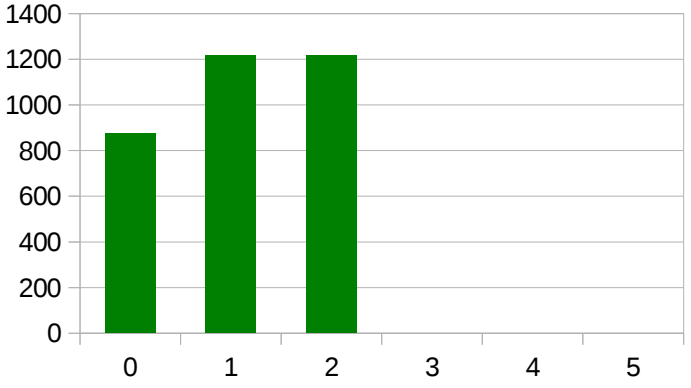


Krok 2 - publikace ECDSA klíčů



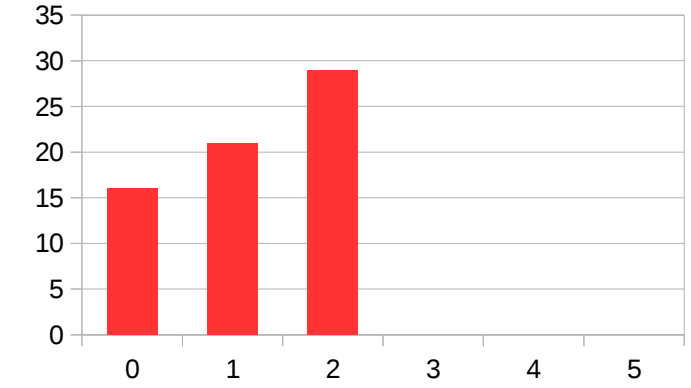
Velikost DNSKEY odpovědi

1263 B



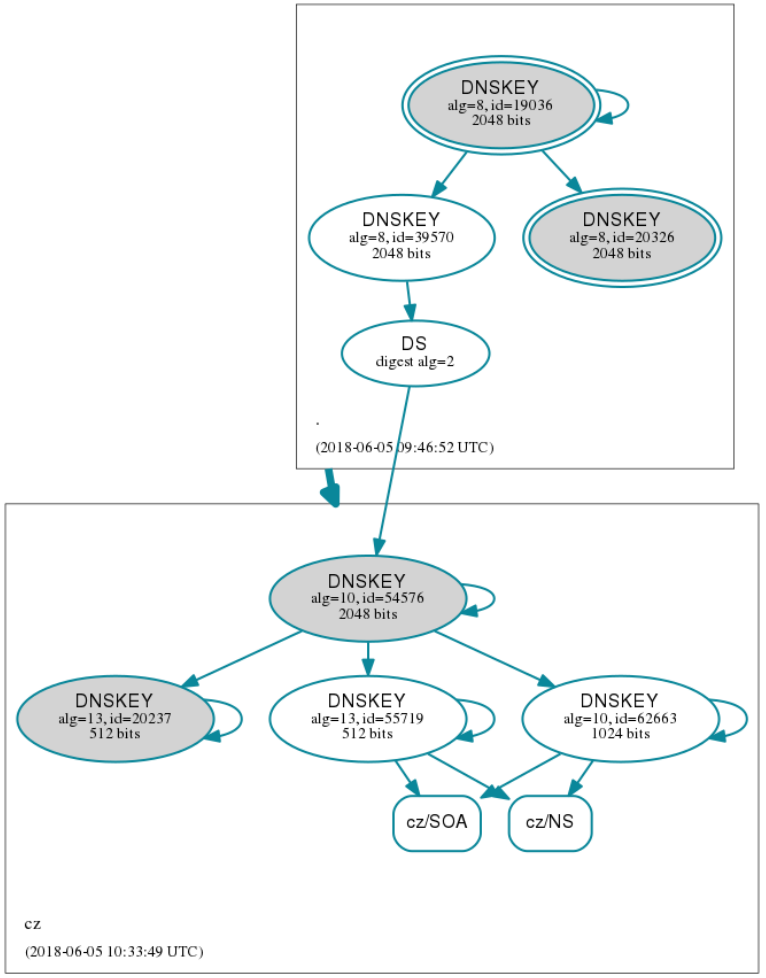
Velikost zóny s podpisy

1217 MB

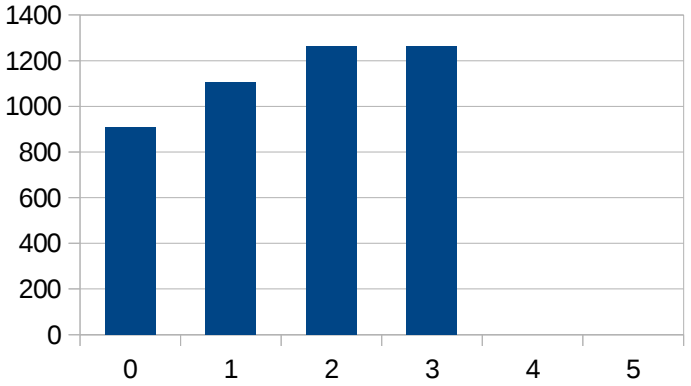


Doba publikace

29 min

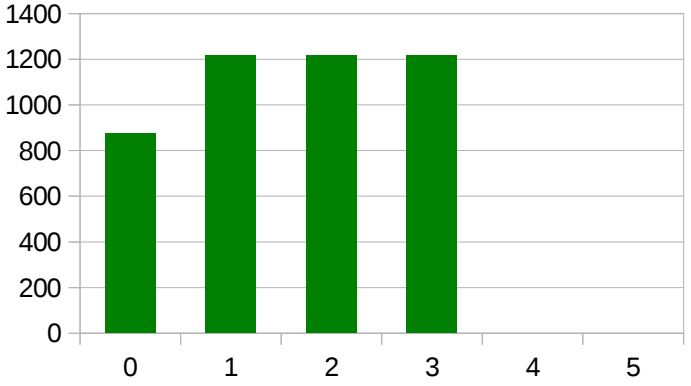


Krok 3 - změna DS záznamů v IANA



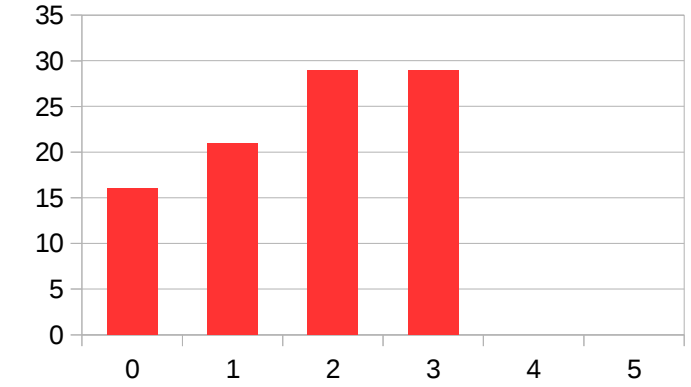
Velikost DNSKEY odpovědi

1263 B



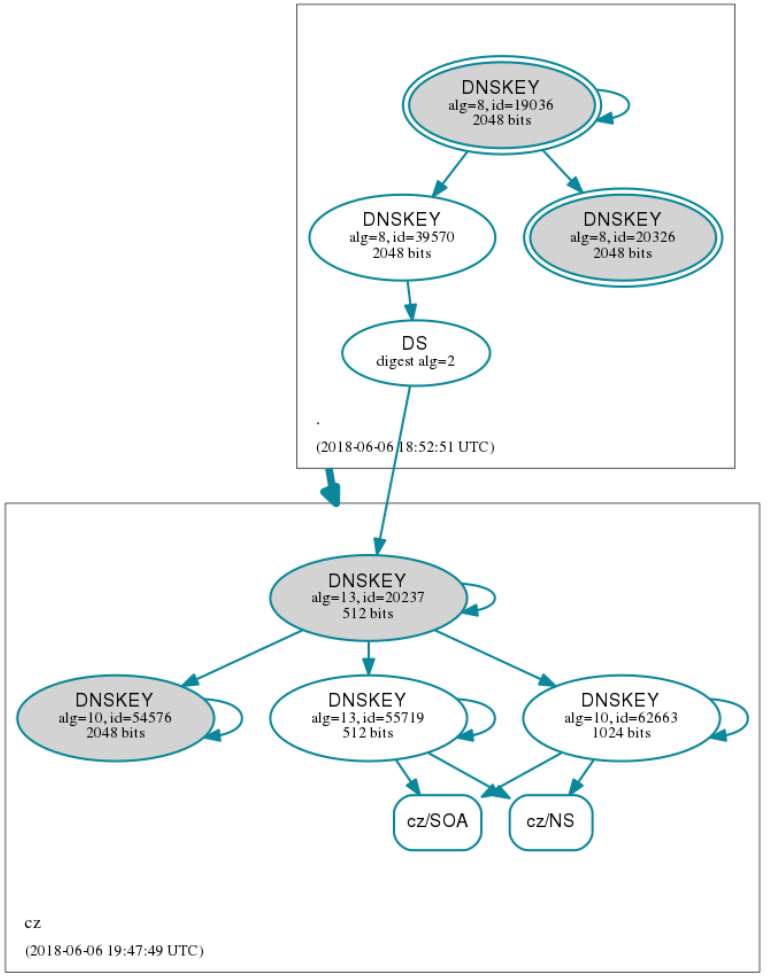
Velikost zóny s podpisy

1217 MB

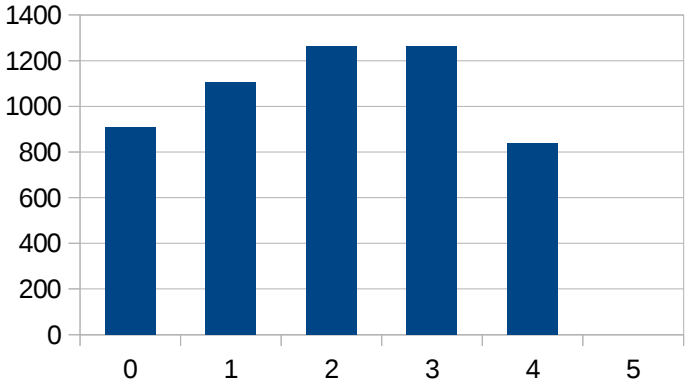


Doba publikace

29 min

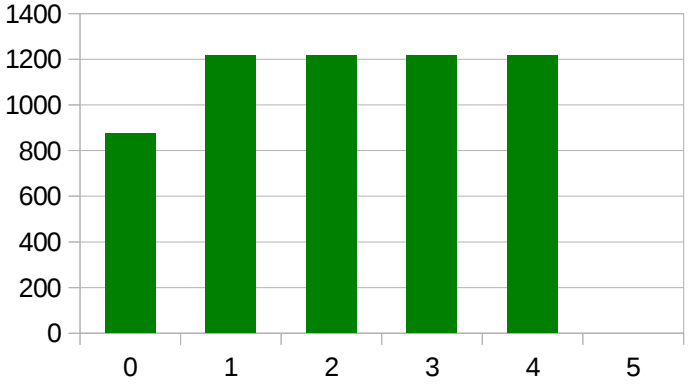


Krok 4 - odstranění RSA klíčů



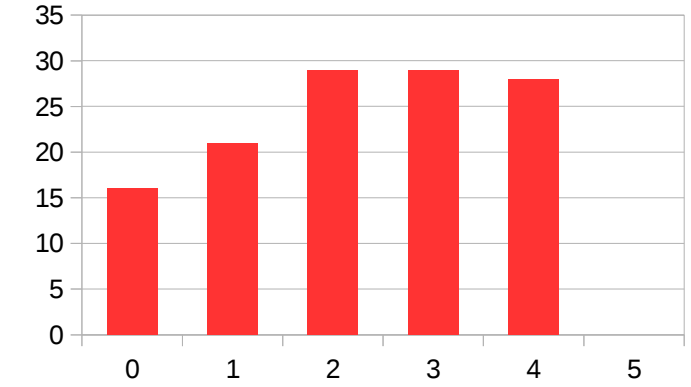
Velikost DNSKEY odpovědi

839 B



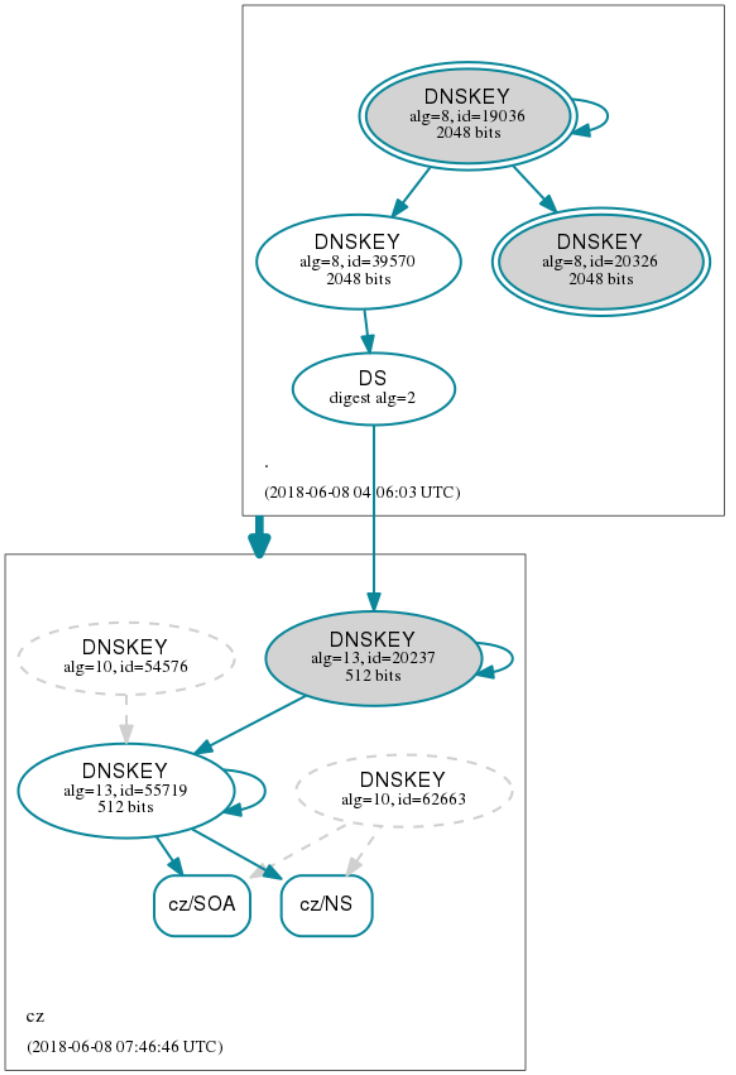
Velikost zóny s podpisy

1217 MB

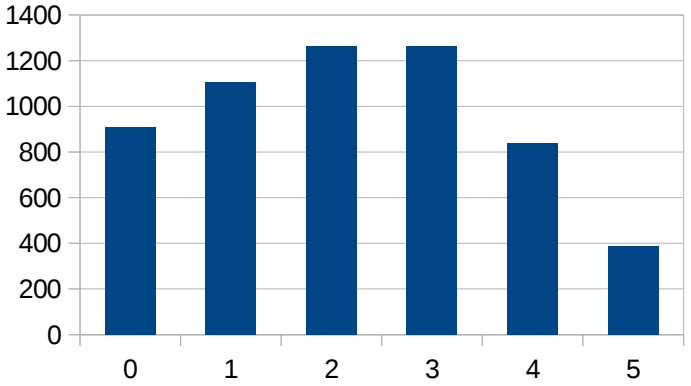


Doba publikace

28 min

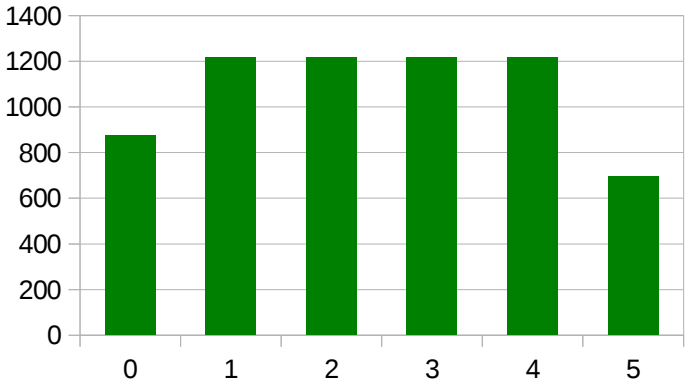


Krok 5 - odstranění RSA podpisů



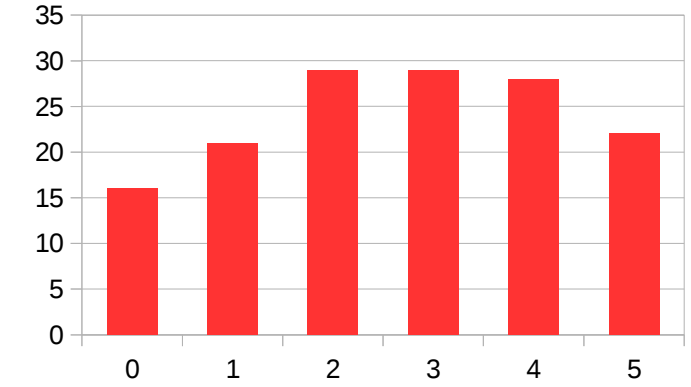
Velikost DNSKEY odpovědi

387 B



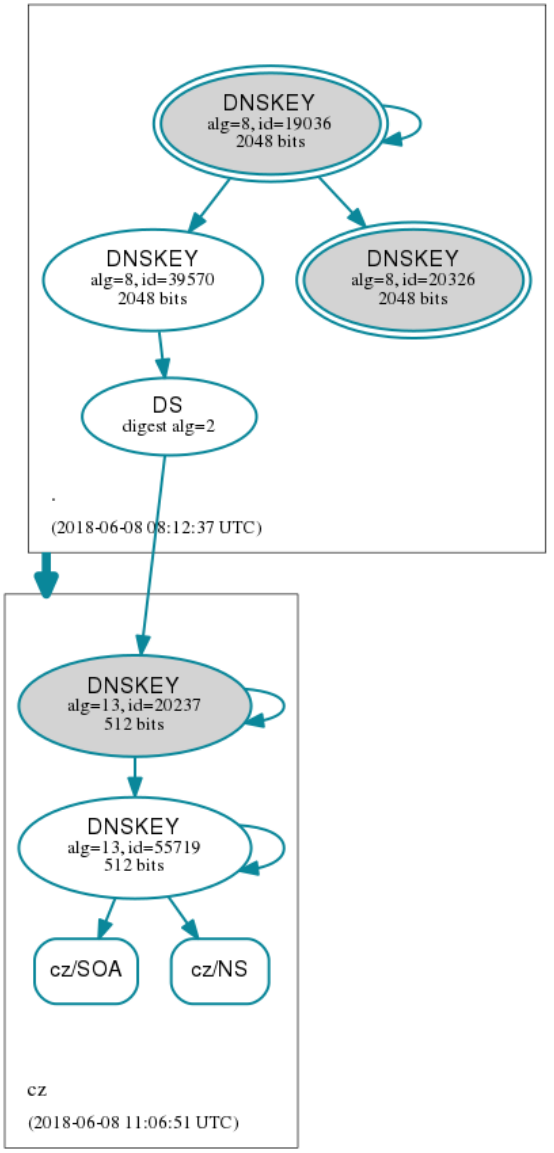
Velikost zóny s podpisy

695 MB



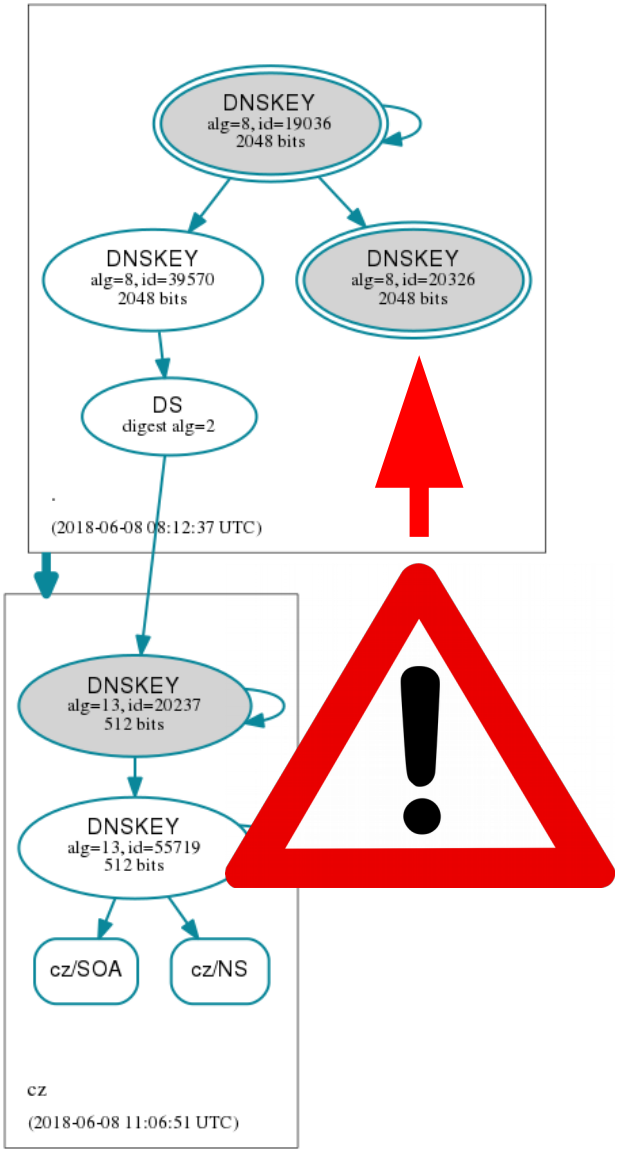
Doba publikace

22 min



Změna KSK kořenové zóny

- Původně plánováno na 11. října 2017
  - Odloženo kvůli kvůli výsledkům testů DNS resolverů
- Znovu naplánováno na **11. října 2018**
  - https://www.icann.org/resources/pages/ksk-rollover



Zhodnocení

- Bezproblémový přechod
- Pozitivní odezva z celého světa
- Dík patří kolegům z DNS týmu (Marian, Tomáš) a CSIRT týmu (Michal, Pavel)
  - U příští výměny KSK můžete být i vy https://www.nic.cz/kariera

Děkuji za pozornost

Jaromír Talíř • jaromir.talir@nic.cz