ECDSA in .CZ

Story of first usage of ECDSA in TLD space

Jaromír Talíř • jaromir.talir@nic.cz • 13. 10. 2018

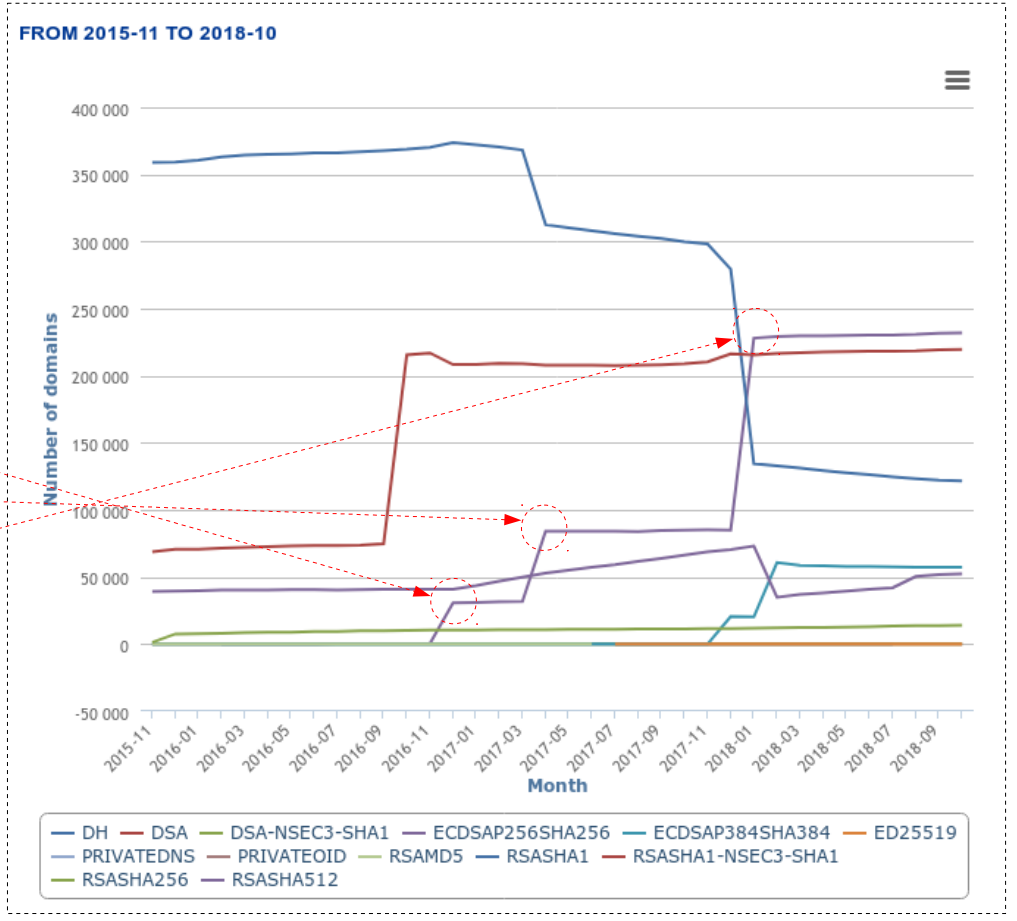
CZ DOMAIN REGISTRY

Long, long time ago ...

- **2006** - DNSSEC deployed using RSASHA1
- **2010** - First KSK rollover (switch to RSASHA512 with NSEC3)
  - First algorithm rollover in TLD space
  - Liberal approach – Unbound failed to validate .CZ
- **2013** - Second KSK rollover (no change to algorithm)
  - Split management of ZSK and KSK
- **2016** - Decision made to switch to ECDSA for third rollover
  - RZM not ready to accept ECDSA algorithm

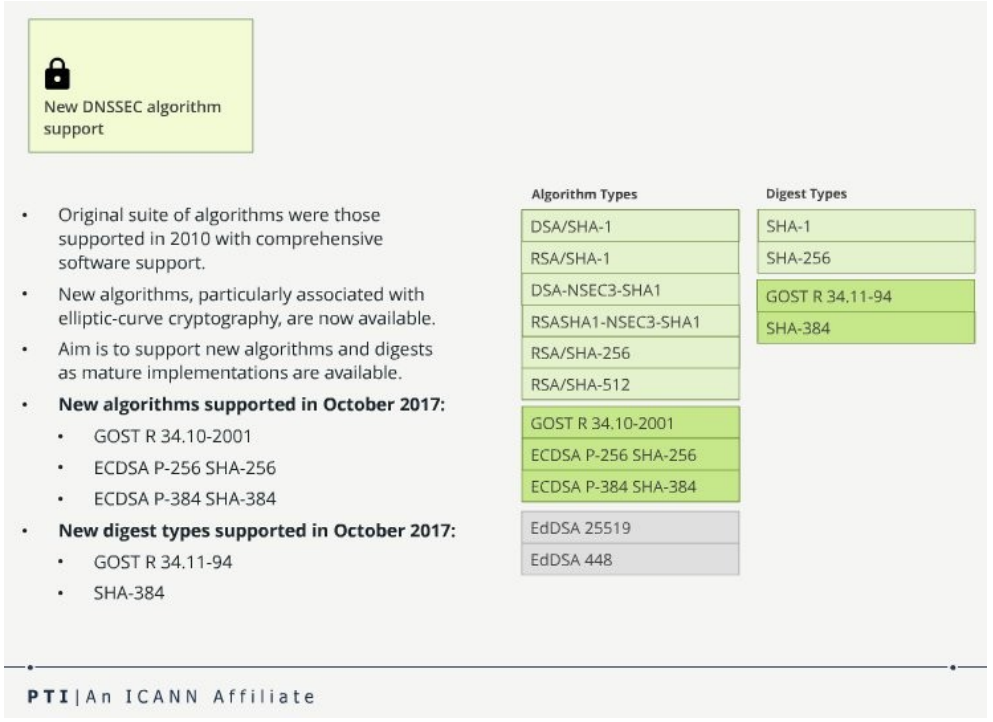
ECDSA on 2nd level

- Publications of alg. stats
- Meetings with registrars
  - regZone!cz – 30 000
  - Ignum – 50 000
  - Active24 – 150 000
- ECDSAP256SHA256 is the most used DNSSEC algorithm



Situation in RZM

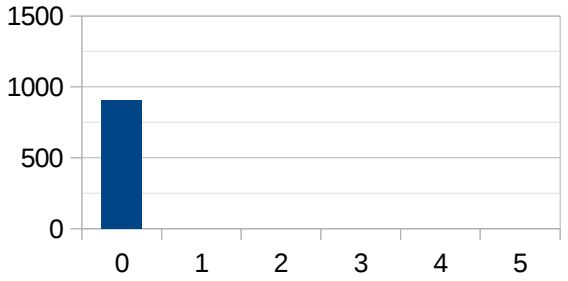
- Keep poking IANA/PTI during the year until RZM got updated at the end of 2017
- Still not all algorithms from IANA tables allowed in RZM

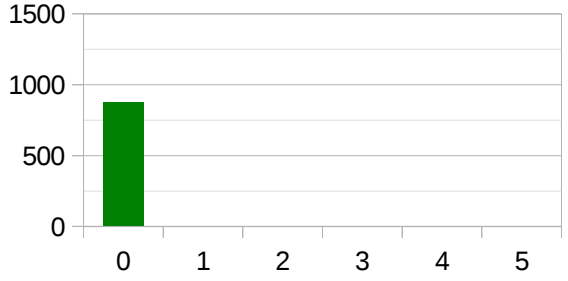


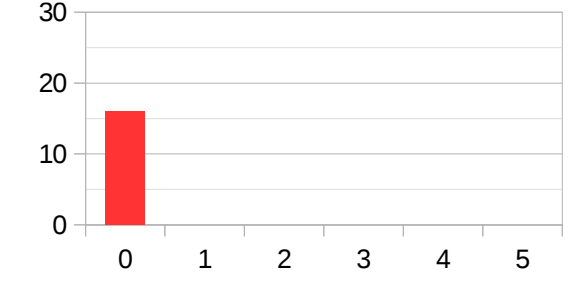
Rollover planning

- Conservative approach selected
- Carefully tested because of splitted ZSK and KSK administration
- Scheduled for week June 4th – 8th
- Operational updates
  - Zone publication changed from 30min period to 60min period
  - Max UDP response size changed from 1232B to 1300B

Beginning







DNSKEY response size with signatures

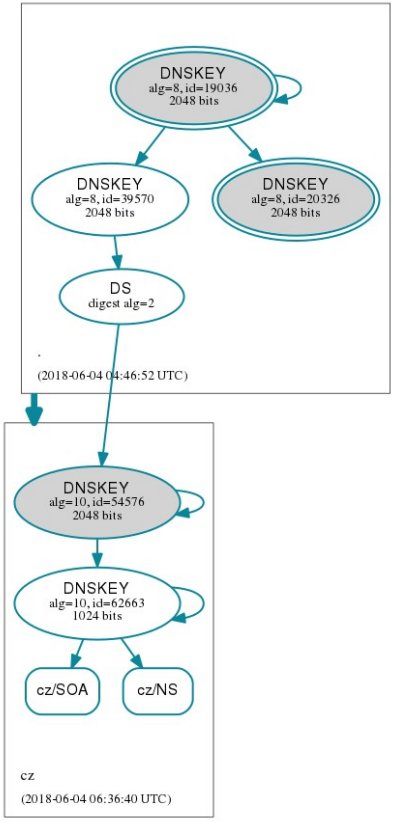
907 B

Size of the zonefile with signatures

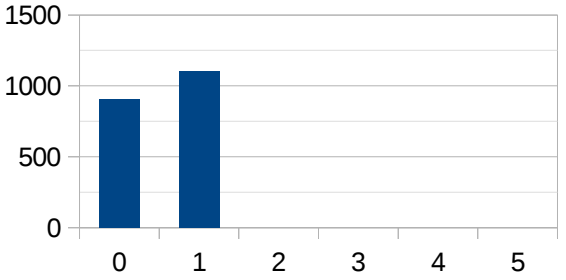
875 MB

Publication time

15 min

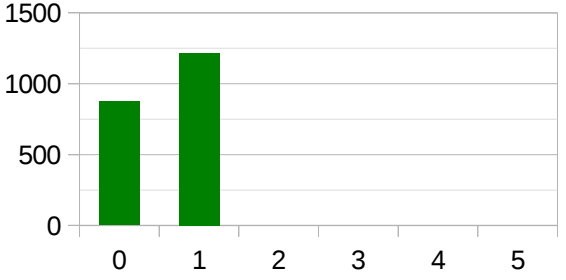


Step 1 – publication of ECDSA signatures



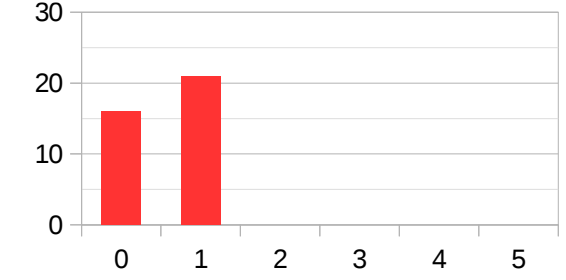
DNSKEY response size with signatures

1103 B



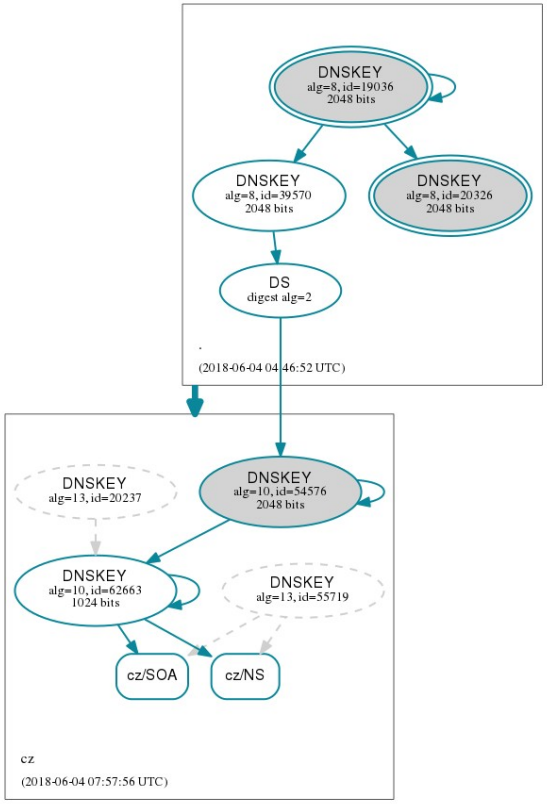
Size of the zonefile with signatures

1217 MB

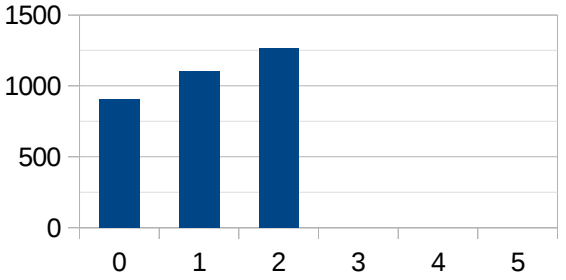


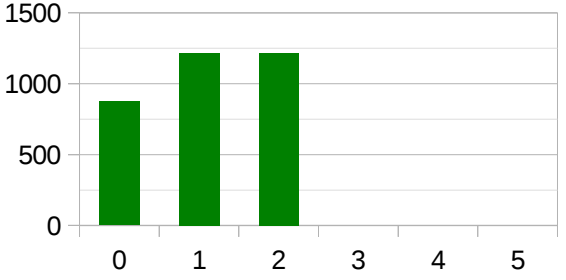
Publication time

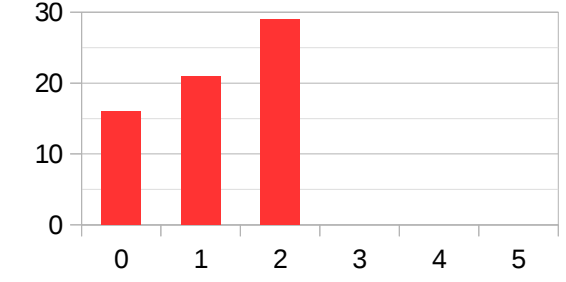
21 min



Step 2 – publication of ECDSA keys







DNSKEY response size with signatures

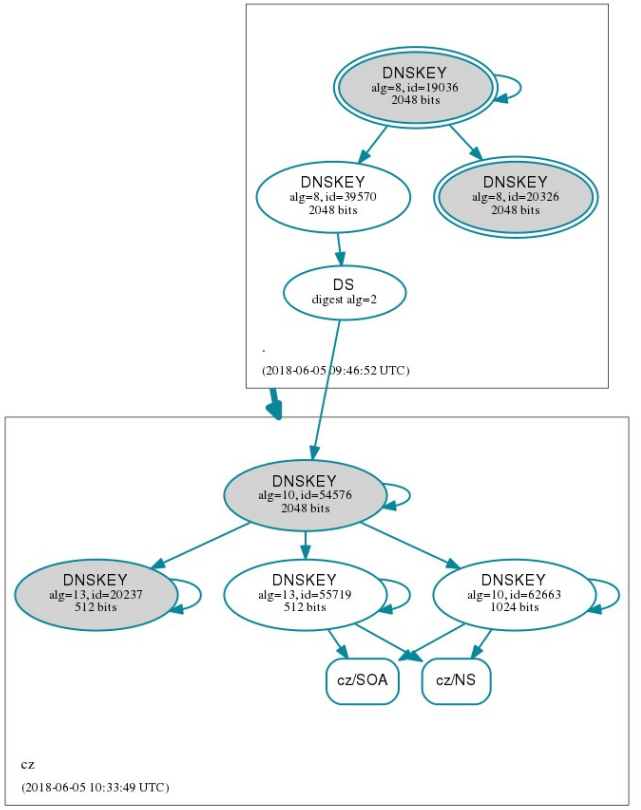
1263 B

Size of the zonefile with signatures

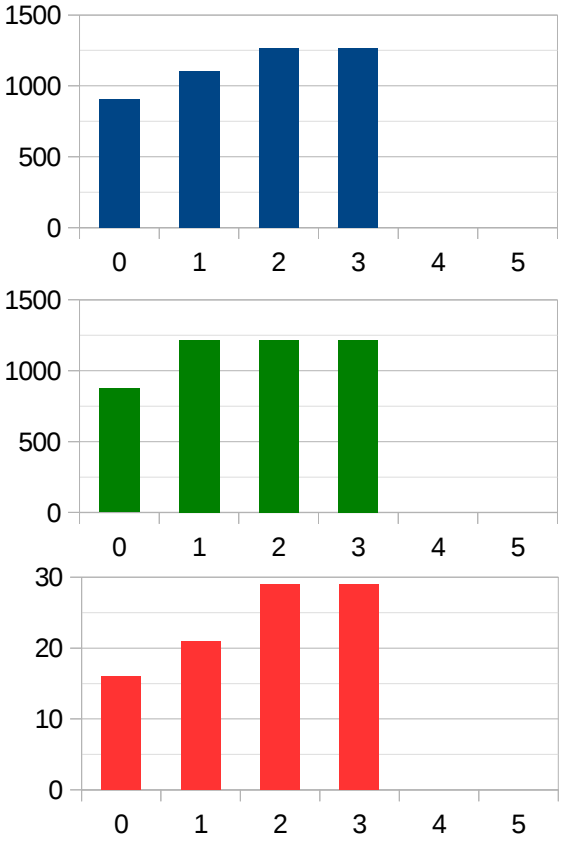
1217 MB

Publication time

29 min



Step 3 – change of DS records



DNSKEY response size with signatures

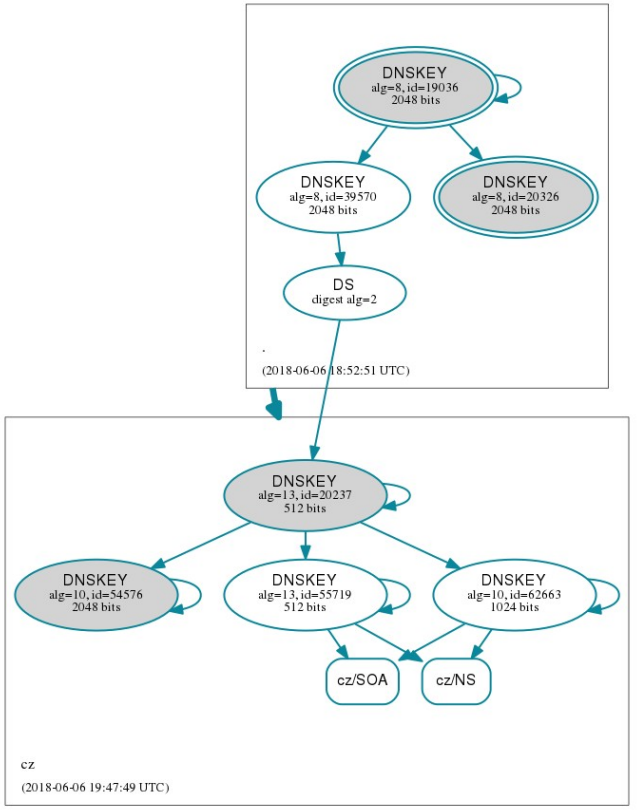
1263 B

Size of the zonefile with signatures

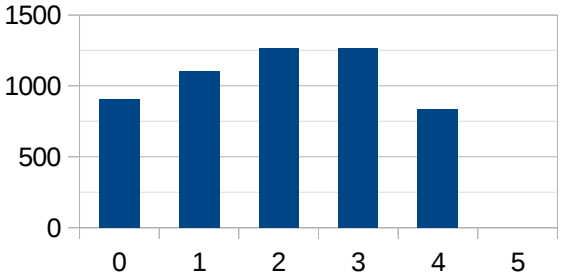
1217 MB

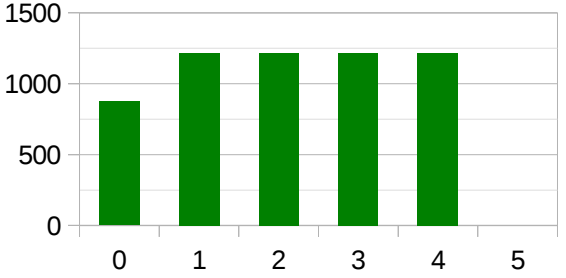
Publication time

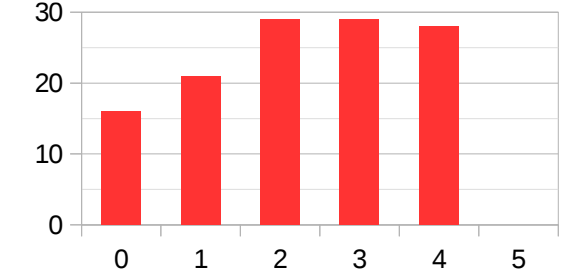
29 min



Step 4 – removal of RSA keys







DNSKEY response size with signatures

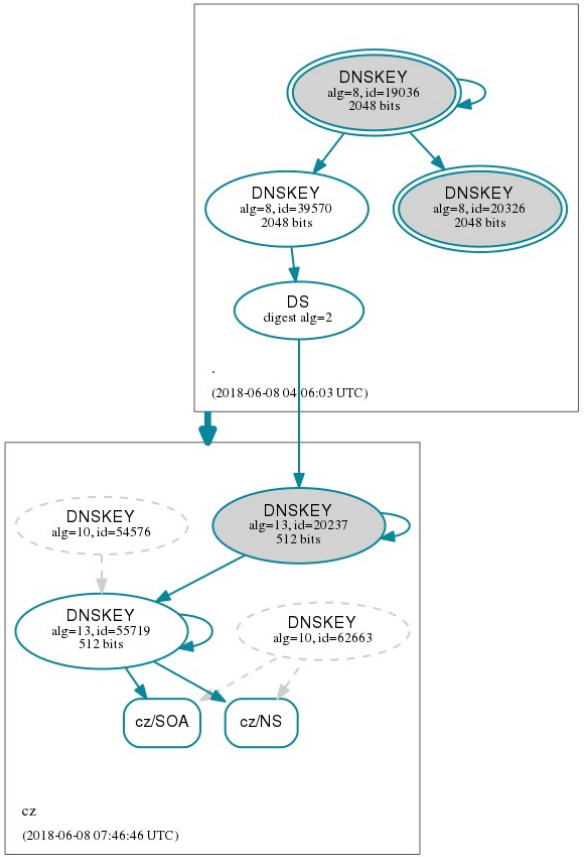
839 B

Size of the zonefile with signatures

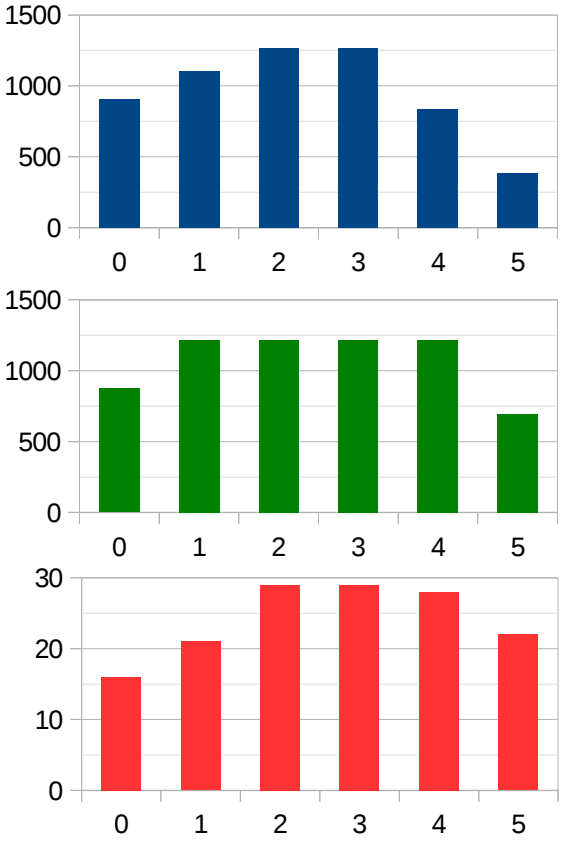
1217 MB

Publication time

28 min



Step 5 – removal of RSA signatures



DNSKEY response size with signatures

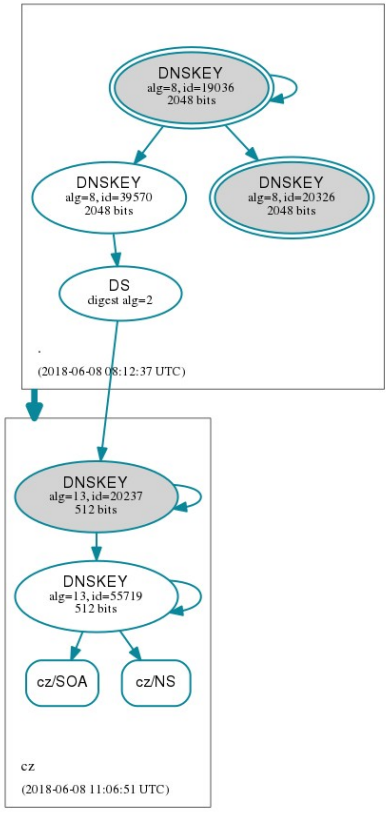
387 B

Size of the zonefile with signatures

695 MB

Publication time

22 min



Conclusion 1

- Conservative approach doesn‘t mean that nothing breaks
- OpenWRT with Unbound 1.4.5 failed to validate CZ
  - Liberal validation appeared in 1.4.7
  - ECDSA support appeared in 1.4.17
  - 8 years old, but actually reason why conservative approach was selected
- So do we need conservative approach at all?

Conclusion 2

- Speed of signing needs to be considered
- One would expected decrease of signing time
- We are using dnssec-signzone from Bind 9.11
  - Validation of generated signatures may slow down whole process
  - Received suggestion to try rewritten signer in most recent Bind

General conclusions

- It is safe to use ECDSA for a TLD
- Confirmed by .BR soon after

Thank you

Jaromír Talíř • jaromir.talir@nic.cz

CZ DOMAIN REGISTRY