

# DNSSEC automation in .CZ

APTLD 85 – Goa

# What to automate

- Signing
  - Expiration of signatures requires regular resigning
  - It is recommended to roll signing keys after some time and rollover process may not be easy especially if change of algorithm is involved
- Provisioning
  - Registry collects DS or DNSKEY from domain registrants and put it into the zone.  
Traditional approach where registrant has to manually approach registrar and fill DNSSEC information shows it's limits

# Signing



- We signed .CZ in 2008
- For many years we used a bunch of shell scripts around dnssec-signzone from Bind
  - There is an issue with maintenance of such scripts
- Since 2011 we are developing authoritative DNS server KnotDNS
  - Over the time this software got support for online DNSSEC signing
- In 2021 we switched .CZ DNSSEC signing process to fully rely on KnotDNS
  - Many organizations already switched to KnotDNS as well
    - .DE, .DK, .SE, .UA, RIPE NCC

# Provisioning

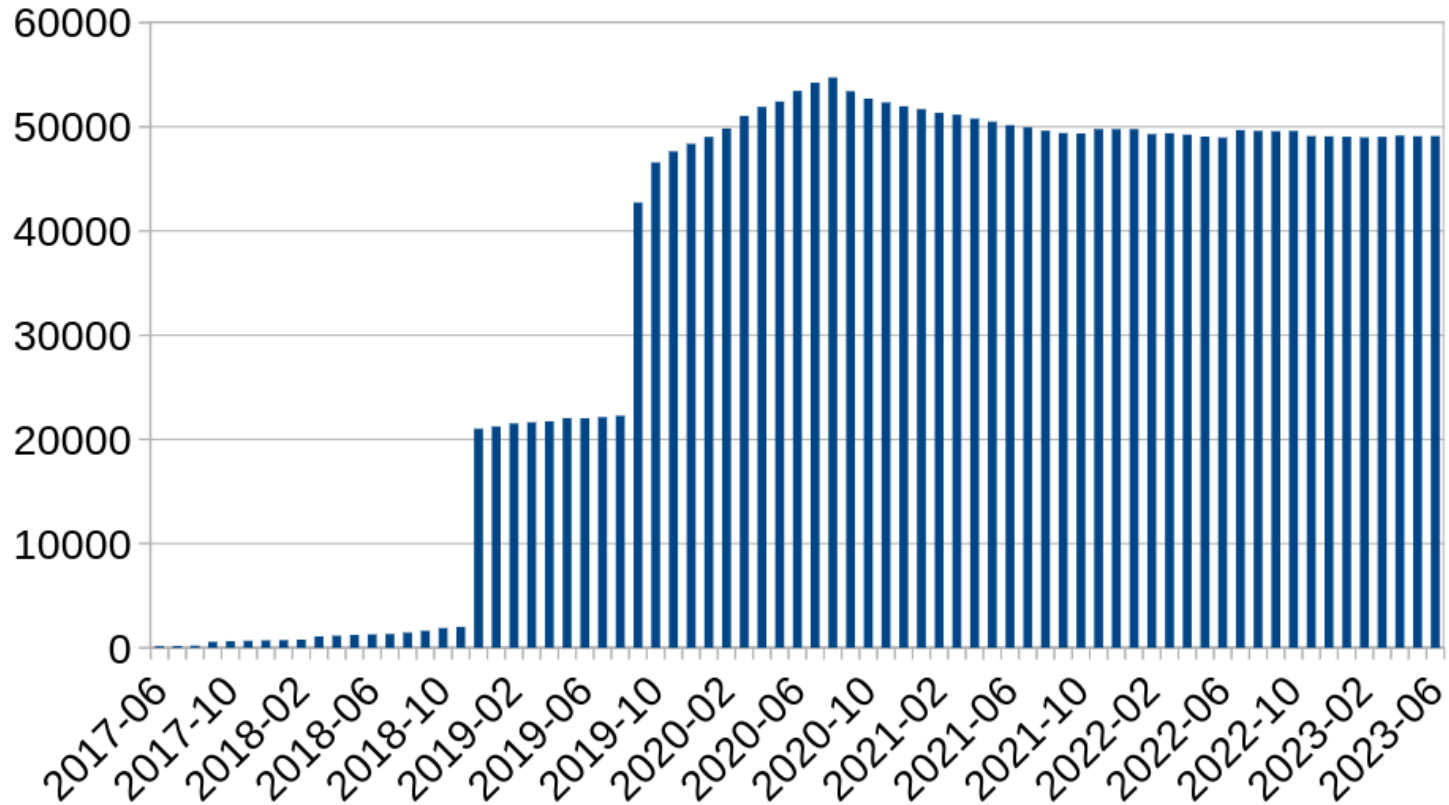
- Multiple ways how to automate DNSSEC provisioning
  - RFC 7344 from 2014 updated by RFC 8078 from 2017
  - draft-ietf-dnssec-bootstrapping
- We implemented and deployed first approach on in 2017

- We call this Automated Keyset Management
- Part of open source registry software FRED – <https://fred.nic.cz>
  - Currently running also in .CR
- Daily scans of whole zone for CDNSKEY records
  - Signed domains gets update immediately
  - Unsigned domain are scanned repeatedly next 7 days and result must be consistent for the update to take place

# Open issues

- Conflict with Registry Locks – should user be able to opt – out?
- How to inform registrants – emails, web page?
- Liberal or strict approach? Should we let invalid keys get in?
- Number of scanning locations vs. length of waiting period

# Statistics



# Future

- For signing part it would be interesting to automated KSK rollover in IANA
  - CDS/CDNSKEY scanning of root zone
  - API to RZM
- On our side we have implemented second generation of AKM
  - Multiple locations, results on the web page instead of emails
  - Now running in production in parallel with old scanner and we are evaluating results



# Thank you for watching!