

# Recent DNSSEC Automation Developments in .CZ

Jaromír Talíř • [jaromir.talir@nic.cz](mailto:jaromir.talir@nic.cz) • 27.10.2021



# Agenda

- Migration of DNSSEC signer from Bind to KnotDNS
- Development of 2nd generation CDNSKEY processing tool



# Automation of DNSSEC signing procedure for .CZ



# Original DNSSEC signing procedure

- Ubuntu LTS, Bind 9.10.x
- Internal shell scripts for zone checks and DNSSEC signing
- Offline KSK
- Driven by cron jobs



# Main motives for migration

- **„Eat our own bread“**
  - move from BIND to KNOT DNS
- **„Take it with butter“**
  - zone checker from KNOT DNS
  - automated DNSSEC signing with KNOT DNS
- **„Don't hessitate to ask for ham“**
  - easier maintenance & fewer potential mistakes
  - following development – incremental zone change



**KNOT  
DNS**



# Migration procedure

- Building and using a test infrastructure
  - setting up a new offline KSK ceremony equipment
  - „sacrificing“ of one HM servers → Debian 10, KNOT 3.0
- 6 migration phases
  - parked SLDs
  - other SLDs
  - internal SLDs on DNS anycast
  - hosted TLDs & SLDs on DNS anycast
  - ENUM on DNS anycast
  - .CZ on DNS anycast



# Offline KSK

- Ceremony stays the same
  - ZSK team: 6 ZSKs for following 6 months, KSR
  - KSK team: KSR -> SKR
  - ZSK team: check SKR, import to HM and reload the zone
- Tools have changed
  - KSK team: keymgr generate + keymgr signksr
  - ZSK team: keymgr pregenerate + generate-ksr + keymgr import-skr



# Migration results

- Much easier management of zones
- DNSSEC signing is fully automated (except offline KSK for .CZ)
- No „home-made“ scripts and cron jobs
  - 23 -> 5 minutes for ENUM and .CZ zones generating and signing
  - lower error rate propensity
  - knot-backup/knot-restore
- Changes in monitoring (timestamp in SOA)
- Possible future development





# Automated Keyset Management in open source registry FRED

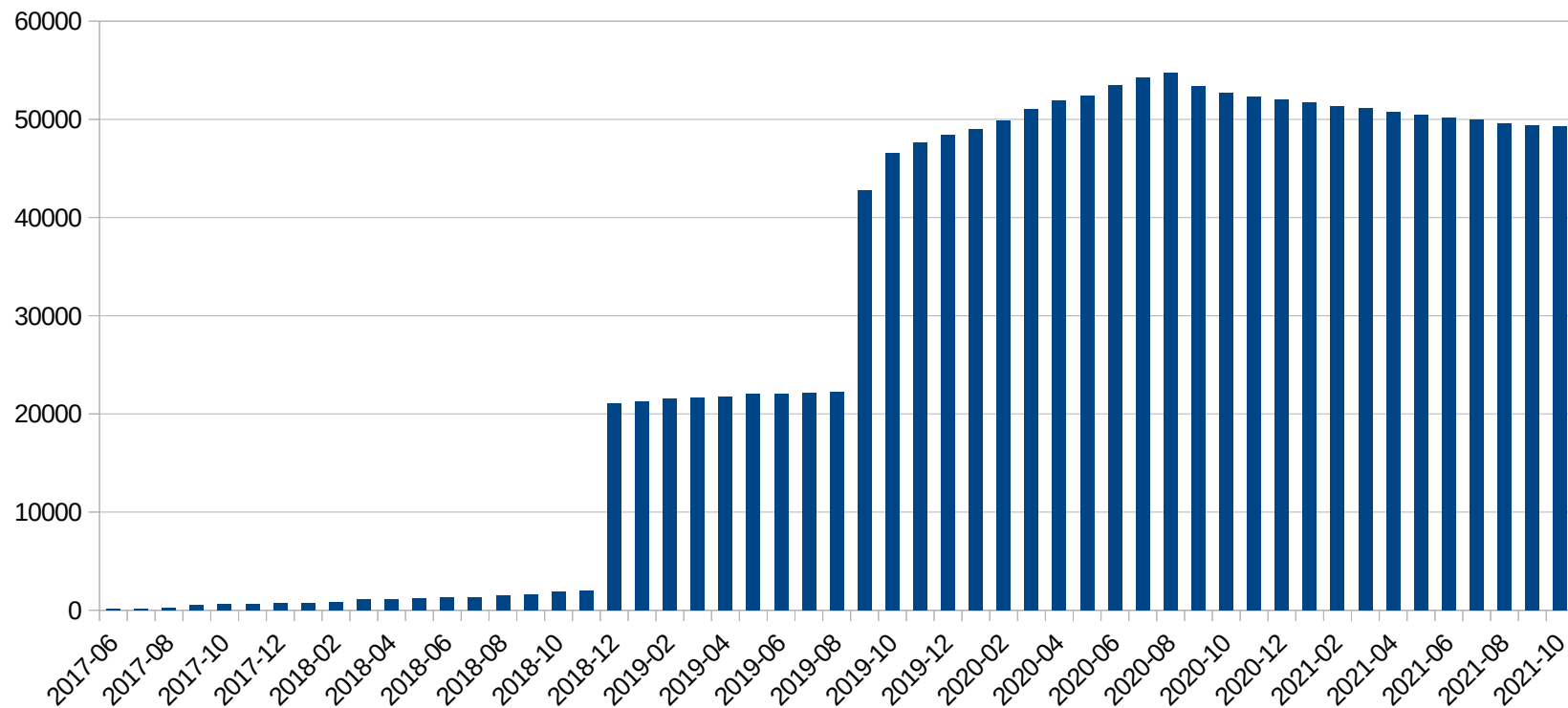


# Automated Keyset Management

- Launched in 2017
- Scanning CDNSKEY from single site
- 7 daily scans must be identical for DNSSEC bootstrapping
- Notification about changes via e-mail
- Scan results stored in SQLite database
- System linked with registry system FRED via CORBA API



# Statistics

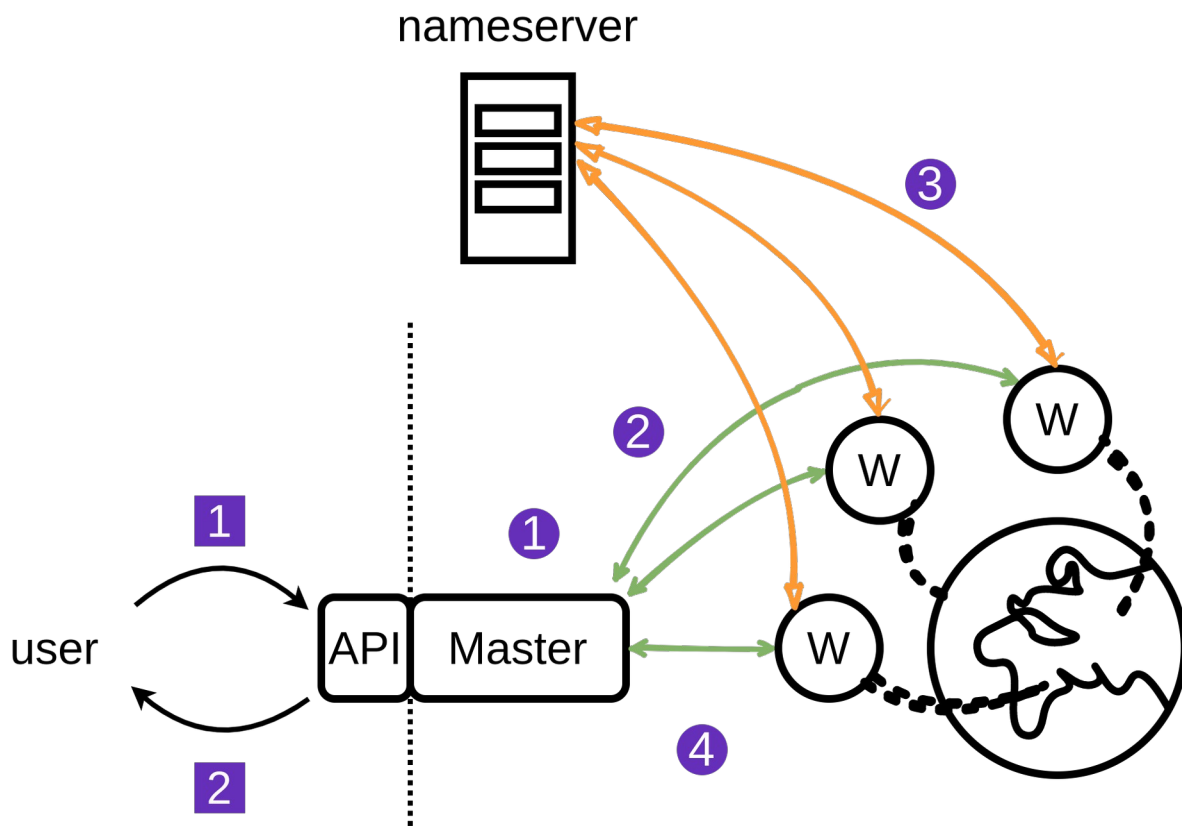


# Issues

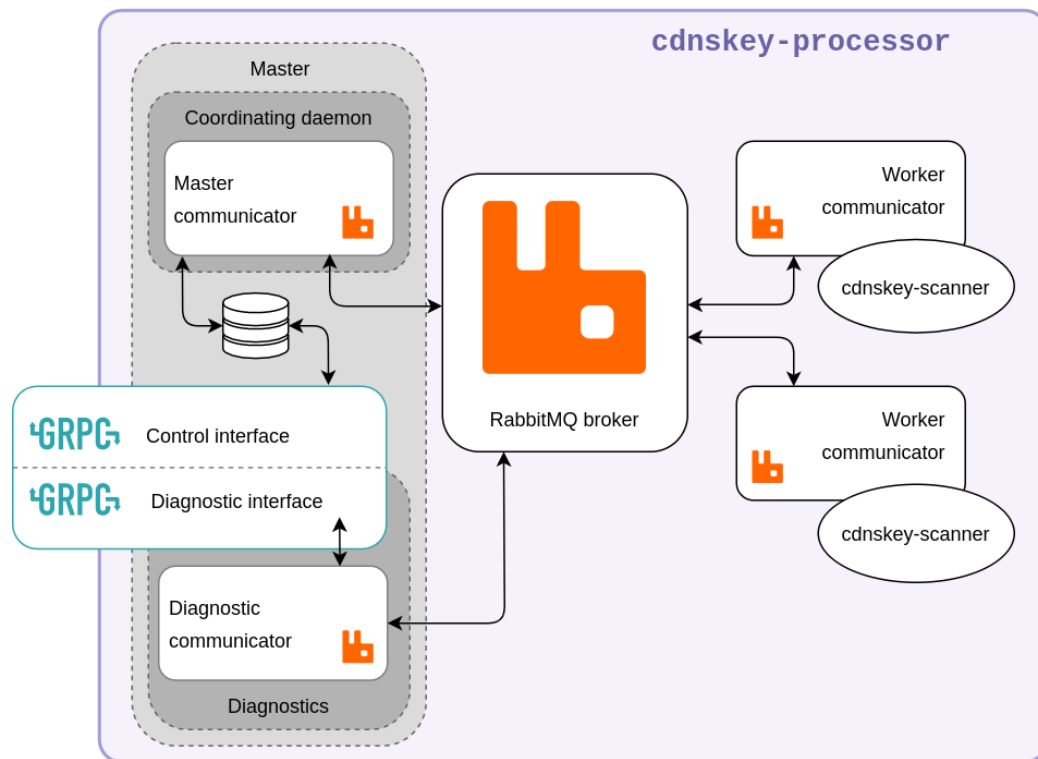
- 7 days period is quite long – scanning from multiple networks can make it shorter
- End users are confused by e-mail communication – information on the website could be enough
- Conflict with Registry Lock – should we ignore it? Yet undecided
- HA with SQLite is hard – using regular PostgreSQL used for registry is better



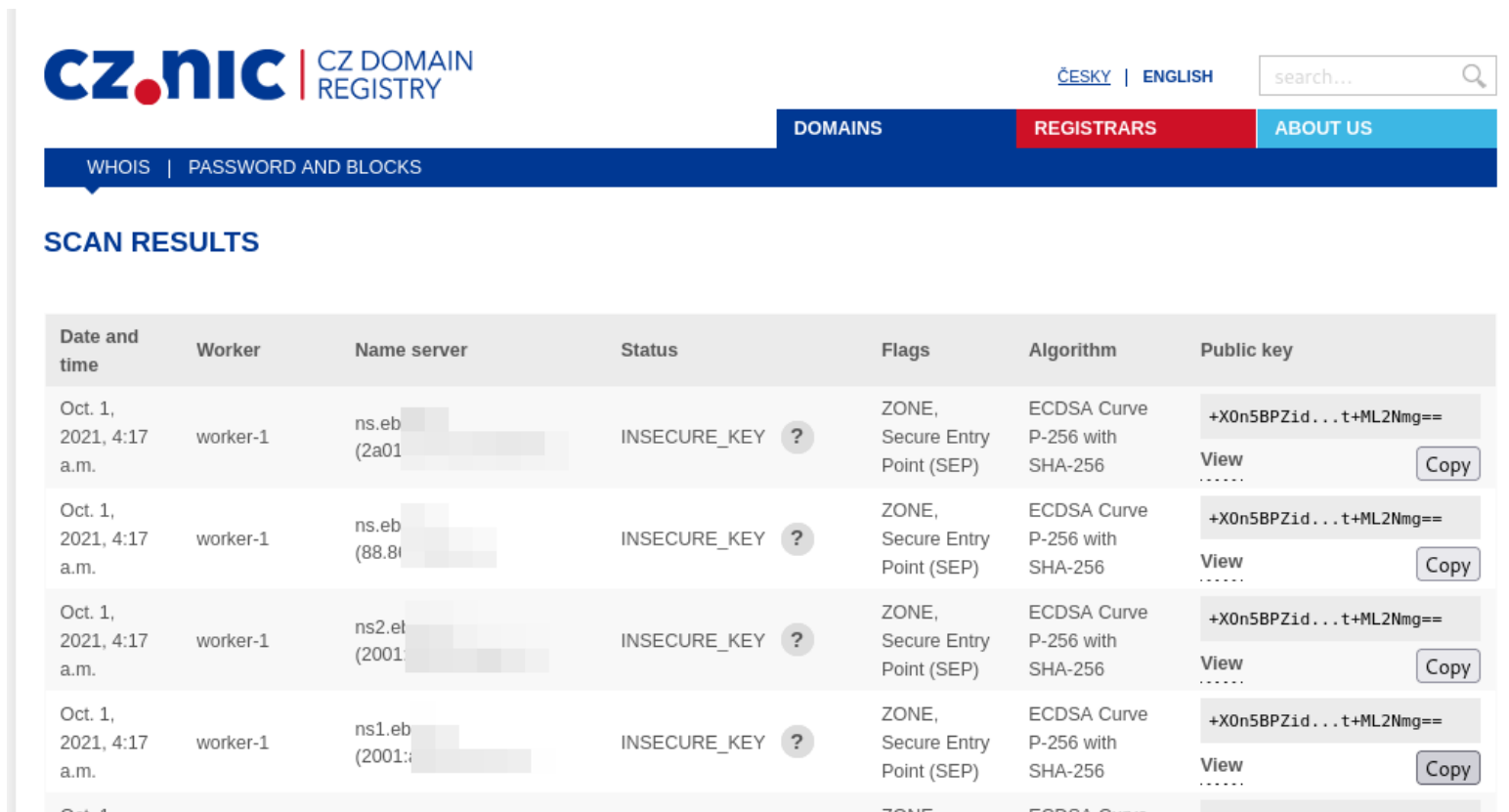
# From cdnskey-scanner to cdnskey-processor



# Detail of cdnskey-processor



# Results of scans on the web



The screenshot shows the CZ.nic website interface. At the top, there is a navigation bar with 'DOMAINS', 'REGISTRARS', and 'ABOUT US' tabs. Below this is a 'SCAN RESULTS' section with a table of scan data. The table has columns for Date and time, Worker, Name server, Status, Flags, Algorithm, and Public key. Each row represents a scan of a name server, all of which are marked as 'INSECURE\_KEY'.

Date and time	Worker	Name server	Status	Flags	Algorithm	Public key
Oct. 1, 2021, 4:17 a.m.	worker-1	ns.eb(2a01...)	INSECURE_KEY ?	ZONE, Secure Entry Point (SEP)	ECDSA Curve P-256 with SHA-256	+X0n5BPZid...t+ML2Nmg== View ..... Copy
Oct. 1, 2021, 4:17 a.m.	worker-1	ns.eb(88.8...)	INSECURE_KEY ?	ZONE, Secure Entry Point (SEP)	ECDSA Curve P-256 with SHA-256	+X0n5BPZid...t+ML2Nmg== View ..... Copy
Oct. 1, 2021, 4:17 a.m.	worker-1	ns2.el(2001...)	INSECURE_KEY ?	ZONE, Secure Entry Point (SEP)	ECDSA Curve P-256 with SHA-256	+X0n5BPZid...t+ML2Nmg== View ..... Copy
Oct. 1, 2021, 4:17 a.m.	worker-1	ns1.eb(2001...)	INSECURE_KEY ?	ZONE, Secure Entry Point (SEP)	ECDSA Curve P-256 with SHA-256	+X0n5BPZid...t+ML2Nmg== View ..... Copy

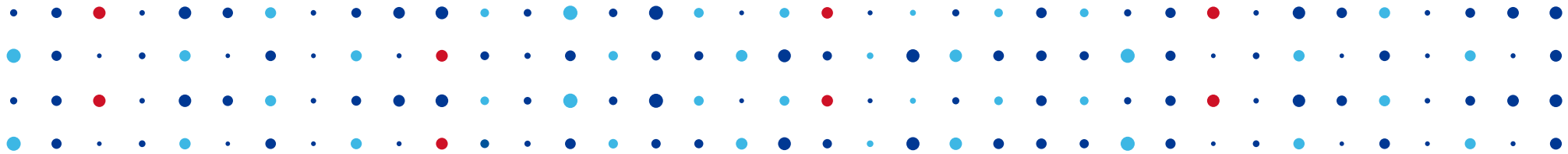


# Summary

- Improvements
  - More robust architecture with multisite scanning and batch processing
  - Better for integration with other registries
- Next steps
  - Currently running in parallel with the old version
  - Results are being compared and evaluated (13h -> 9h)
  - Estimated time to production is 2-3 months.







# Thanks

Jaromír Talíř • [jaromir.talir@nic.cz](mailto:jaromir.talir@nic.cz)

