DS automation success story at .CZ

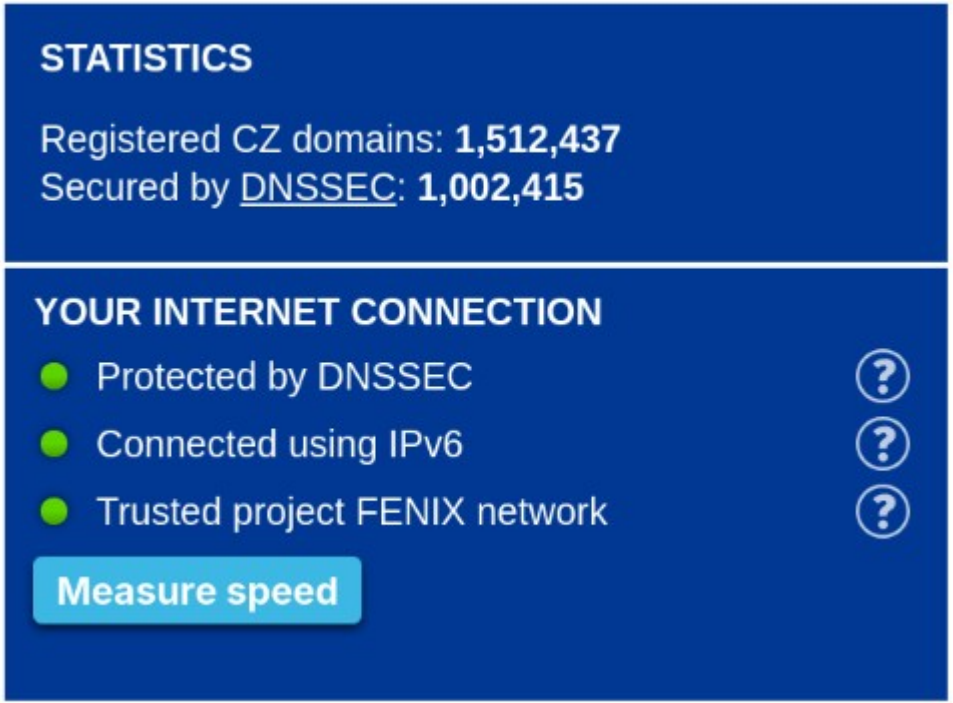
DNSSEC Workshop – ICANN 84 Dublin

Ondřej Filip • 29. 10. 2025

CZ DOMAIN REGISTRY

DNSSEC.CZ

- DNSSEC launched in 2008
- AKM - launched in 2017
- Cca 1M signed domain of 1,5M
  - 66% signed



Three main ways to - DNSSEC

- Self signing and submission of a key material via registrar portal (and then via EPP) – rarely used
- Many registrars signs all domains under their control automatically and submit key material also via EPP
- Automated Keyset Management (AKM – DS automation) – very popular in combination with Knot DNS – for DNS providers and independent entities

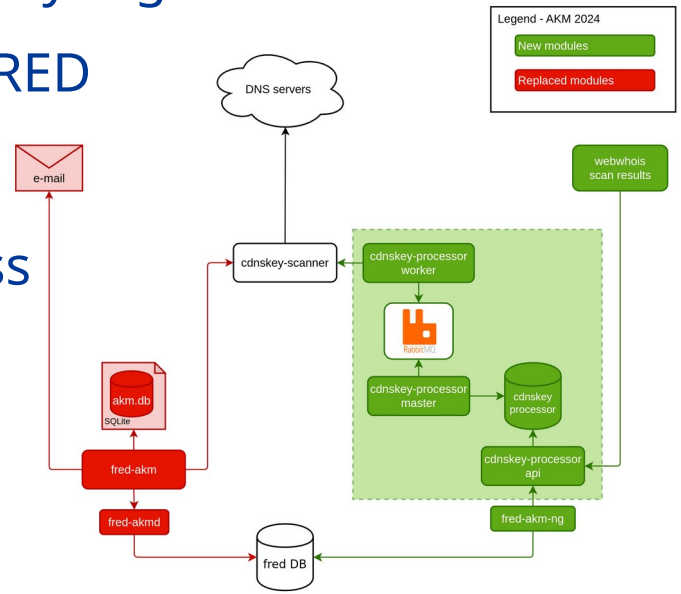
AKM@CZ

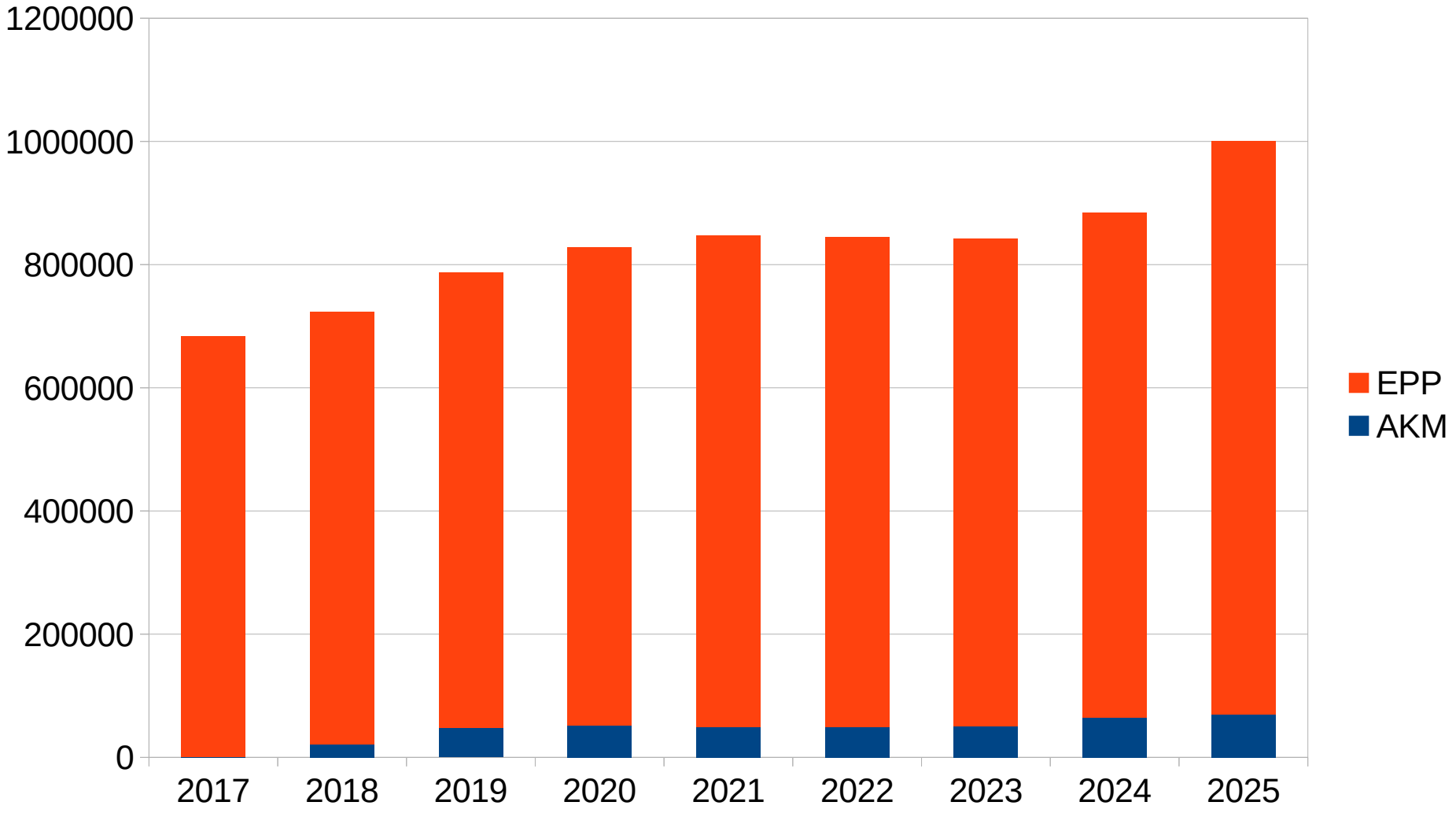
- Discussion with registrars → registry should do it

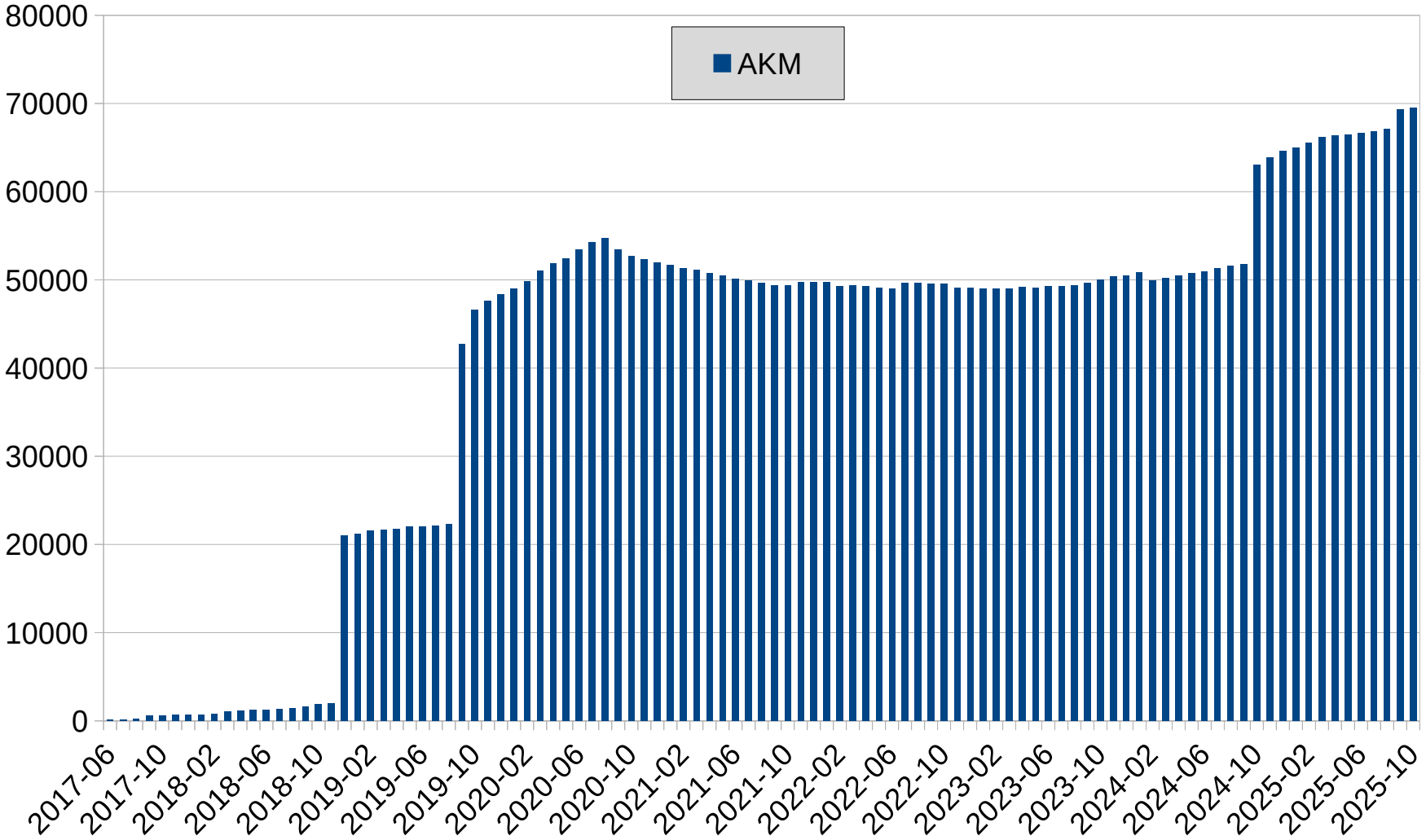
- Scanning CDNSKEY – cdnskey-scanner part of FRED
- 7 daily scans must be identical for DNSSEC bootstrapping
- KEYSET created and assigned in FRED db
- Changes of signed domains are processed immediately
- Also support CDNSKEY record with specific values (CDNSKEY 0 3 0 AA==)

AKM@CZ new version

- Scanned CDNSKEY records published in web whois
  - https://www.nic.cz/whois/domain/example.cz/scan-results
- Automatically generated KEYSETs cannot be used by registrars
- Better for integration with other registries than FRED
- Ready to run the test from multiple sites
- No more end user notifications in normal business




1200000
1000000
800000
600000
400000
200000
0
2017
2018
2019
2020
2021
2022
2023
2024
2025
EPP
AKM


AKM
80000
70000
60000
50000
40000
30000
20000
10000
0
2017-06
2017-10
2018-02
2018-06
2018-10
2019-02
2019-06
2019-10
2020-02
2020-06
2020-10
2021-02
2021-06
2021-10
2022-02
2022-06
2022-10
2023-02
2023-06
2023-10
2024-02
2024-06
2024-10
2025-02
2025-06
2025-10

Ideas for Future AKM@CZ

- RFC 9615 support - (Automatic DNSSEC Bootstrapping Using Authenticated Signals from the Zone's Operator)
  - CDNSKEY record inserted in a different zone of the DNS operator
  - CDNSKEY would be created automatically and more securely
- RFC 9859 support (Generalized DNS Notifications)
  - Possibility to signal zone changes by DNS operator
- Implementation of CSYNC
  - More general mechanism for NS records synchronization between TLD and SLD

Our ways to increase DNSSEC adoption

- DNSSEC support is a necessary condition for out certification program
- Certified registrars can enter co-marketing campaign program – CZ.NIC partially finance registrar’s marketing
- Communication with ISPs, End users (IPv6/DNSSEC Widget)
- DNSSEC training in our Academy
- Government support – all governmental web sites must support DNSSEC
- Knot DNS – fully automated singing and DNSSEC rollovers

Conclusions

- DS automation (AKM) routinely used in .cz (~70k domains) – new version of the software less dependent on FRED registry
- 66% domains signed – limited possibility to grow
- All large registrars and DNS hosting providers sign by default (providing key material either via EPP or AKM)
- We plan periodic checks based on zonemaster – change in DNSSEC policy

Thank you !

ondrej.filip@nic.cz

CZ DOMAIN REGISTRY