



# Fully automatic DNSSEC

Let the Magic Begin

Ondřej Surý • [ondrej.sury@nic.cz](mailto:ondrej.sury@nic.cz) • 16. 07. 2017

# DNSSEC Automatron

- RFC7344 - Automating DNSSEC Delegation Trust Maintenance
  - CDNSKEY/CDS Records
- RFC 8078 - Managing DS Records from the Parent via CDS/CDNSKEY
  - Enable DNSSEC
  - Rollover DNSKEY
  - Disable DNSSEC

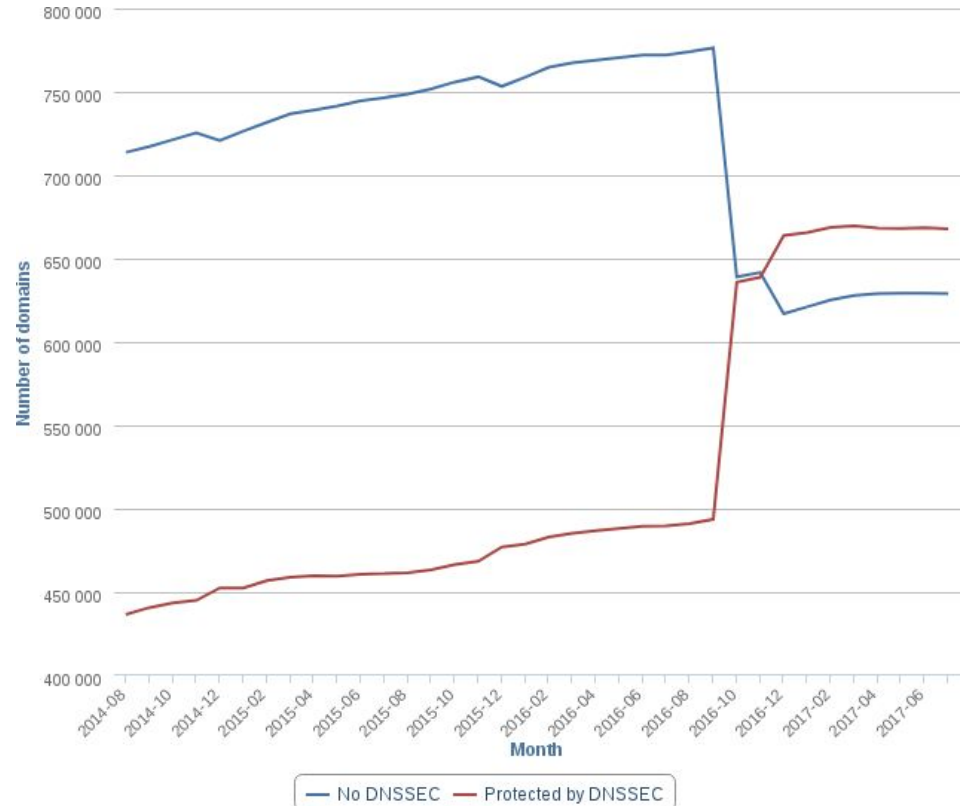


# Implementations

- TLD Registries
  - FRED – open-source registry (by CZ.NIC)
- DNS Signers
  - Knot DNS 2.5 – fully automated solution
  - BIND 9.11 – semi-manual publishing using `dnssec-keymgr` && `dnssec-settime`
  - PowerDNS – semi-manual publishing using `pdnsutil`
  - OpenDNSSEC – WIP

# Is 51.5% good enough?

- 1 296 512 registered domains
- 667 815 domains signed by DNSSEC with published DS record
- **21 156** domains signed by DNSSEC without published DS record



# FRED – the open-source registry



# FRED – Domains without assigned KEYSET

- Periodically check for CDNSKEY
  - Only via TCP
  - For all the nameservers (in the registry, not in the zone)
- If found the cycle begins:
  - Inform the NSSEC tech-c (via notify email)
  - Check the domain each day
  - If unchanged for 7 days create automatically managed KEYSET
  - Inform the domain holder (via notify email)
  - Inform the registrar (via EPP)
- Domain holder can block this via “block” operation in the registry

# FRED – Domains with automatic KEYSET

- Lookup CDNSKEY records using local DNSSEC-validating resolver
- If found, do as requested:
  - Replace DNSKEY in the automatic KEYSET
  - Remove KEYSET from domain (effectively removing DS records)
- Inform the NSSET tech-c (via notify email)
- If KEYSET was removed:
  - Inform the registrar (via EPP)
  - Inform the domain holder (via notify email)

# FRED – domains with “legacy” KEYSET (WIP)

- Lookup CDNSKEY records using local DNSSEC-validating resolver
- If found, do as requested:
  - Create new automatic KEYSET and swap it
  - Remove the KEYSET (effectively removing DS records)
- Inform the NSSET tech-c (via notify email)
- Inform the registrar (via EPP)
- Inform the domain holder (via notify email)



# Knot DNS – KSK Rollover

- Introduced in Knot DNS 2.5.0
- Double signature KSK Rollover
- Optional automatic KSK submission via CDNSKEY/CDS
- Periodic checks for configured nameservers:
  - Either all parent authoritative servers;
  - Or DNSSEC-validating resolver
- Combined Signed Key Rollover

# Knot DNS – DNSSEC made simple

## remote:

- id: local-validating-resolver  
address: [ "::1", "127.0.0.1" ]

## submission:

- **id: validating-resolver**  
**parent: local-validating-resolver**

## policy:

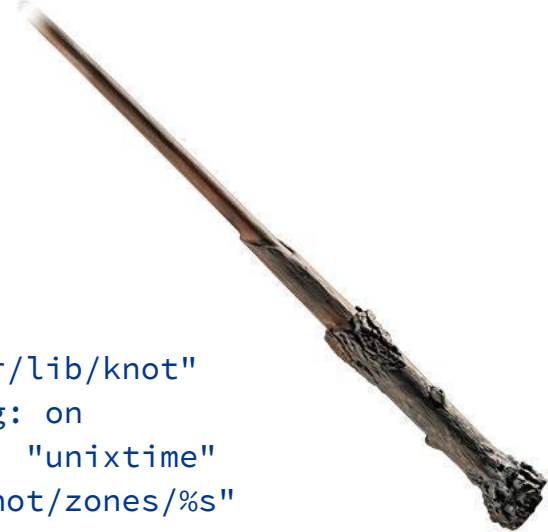
- id: default  
algorithm: ecdsap256sha256 # default  
**ksk-lifetime: 14d**  
**ksk-submission: validating-resolver**

## template:

- id: "default"  
storage: "/var/lib/knot"  
dnssec-signing: on  
serial-policy: "unixtime"  
file: "/etc/knot/zones/%s"

## zones:

- domain: dns.rocks
- domain: ed25519.cz



For full configuration syntax see: <https://www.knot-dns.cz/docs/2.5/html/reference.html>

# Knot DNS – DNSSEC roadmap

- PUSH via REST API
  - draft-ietf-regext-dnsoperator-to-rrr-protocol
- Fully Algorithm Rollover
  - Fully automated



Thank you

Ondřej Surý • [ondrej.sury@nic.cz](mailto:ondrej.sury@nic.cz) • 16. 07. 2017