Automating DNSSEC via CDNSKEY processing

RIPE75

Jaromir Talir • jaromir.talir@nic.cz • 25.10.2017

cz.nic | CZ DOMAIN REGISTRY

Agenda

- What is it about
- Motivations
- DNSSEC signer part – Knot DNS
- Registry part – FRED
- Statistics
- Plans

Whas is it about

- **RFC 7344** - Automating DNSSEC Delegation Trust Maintenance - September 2014
- **RFC 8078** - Managing DS Records from the Parent via CDS/CDNSKEY – March 2017
- **draft-ietf-regext-dnsoperator-to-rrr-protocol** - Third Party DNS operator to Registrars/Registries Protocol

Motivations

- 1 302 556 domains in CZ
  - 670 645 (51.5%) - signed with DS published
  - 21 156 (1.6%) - signed without DS published
- Breaking barriers for even wider DNSSEC adoption
- Boost DNSSEC adoption in ~10 countries where FRED registry is deployed
- New technologies need implementations to prove viability

Current implementations of RFCs

- DNSSEC signing software
  - OpenDNSSEC – planned (early 2018)
  - PowerDNS – semi-manual publishing using pdnsutil
  - Bind 9.11 – semi-manual publishing using dnssec-keymgr and dnssec-settime
  - **Knot DNS 2.6 – full support**
- Registry software
  - **FRED 2.32 – full support**

New KSK rollover in Knot DNS

- Double signature KSK rollover
- Optional KSK submission via CDS/CDNSKEY
- Periodic checks for DS existence via set of configured nameservers (all must see DS)
  - All parental authoritative nameservers
  - And/Or DNSSEC validating resolver

Configuration example

```
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: domain1.cz
  - domain: domain2.cz
```

Other supported features

- CSK (single type signing)
- Shared key
- Algorithm rollover
- DS deletion via “CDNSKEY 0 3 0 AA==” or “CDS 0 0 0 00" must be done manually

Automated Keyset Management

- Implementation of RFC7244 and RFC8078 in open source registry solution **FRED**
- Concept of KeySet
  - Collection of DNSKEY resource records
  - Can be linked to domain to generate DS in the zonefile
- Registry is taking responsibility for managing KeySet when domain publishes CDNSKEY

CDNSKEY scanning

- Daily scanning all domains in zonefile for CDNSKEY records
  - Takes roughly 3 hours for .CZ
- Three categories of domains:
  - Without KeySet
  - With automatically generated KeySet
  - With legacy KeySet created by a registrar

Domains without KeySet

- Scanning all authoritative nameservers from registry database via TCP queries
- When CDNSKEY is found, technical contact is informed via e-mail
- Keep scanning for 7 more days
- If results are always the same, new KeySet is created and linked to domain
  - Owner (via notify e-mail) and registrar (via EPP) are notified

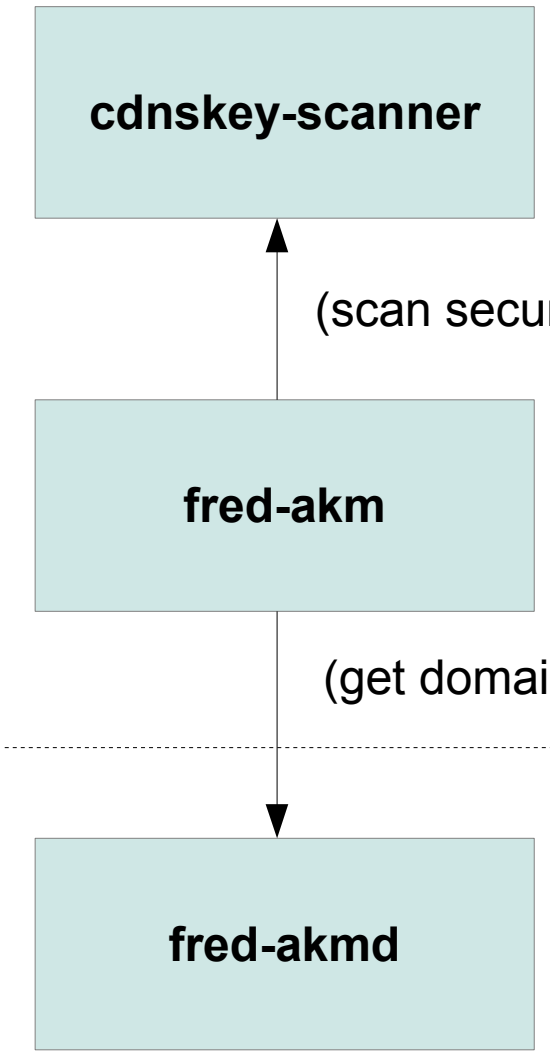
Domains with automatic KeySet

- Scan for CDNSKEY via local resolver, DNSSEC is validated inside scanner
- If CDNSKEY is found, do as requested
  - Update KeySet with new DNSKEY
  - Remove KeySet (notification of domain owner and registrar)
- Technical contact is informed via e-mail

Domains with legacy KeySet

- Scan for CDNSKEY via local resolver, DNSSEC is validated inside scanner
- If CDNSKEY is found, do as requested
  - Create new automatic KeySet and swap it in domain
  - Remove KeySet
- Technical contact is informed via e-mail
- Owner (via notify e-mail) and registrar (via EPP) are notified

Architecture



- CLI tool invoked by fred-akm
- Input: STDIN, Output: STDOUT – (remote run possible)
- Implemented with getdns + libevent
- Distribution of queries per nameserver

(scan secured/insecured domains with nameservers for CDNSKEY)

- CLI tool invoked from cron
- Implements processing logic
- SQLite database backend to store the state

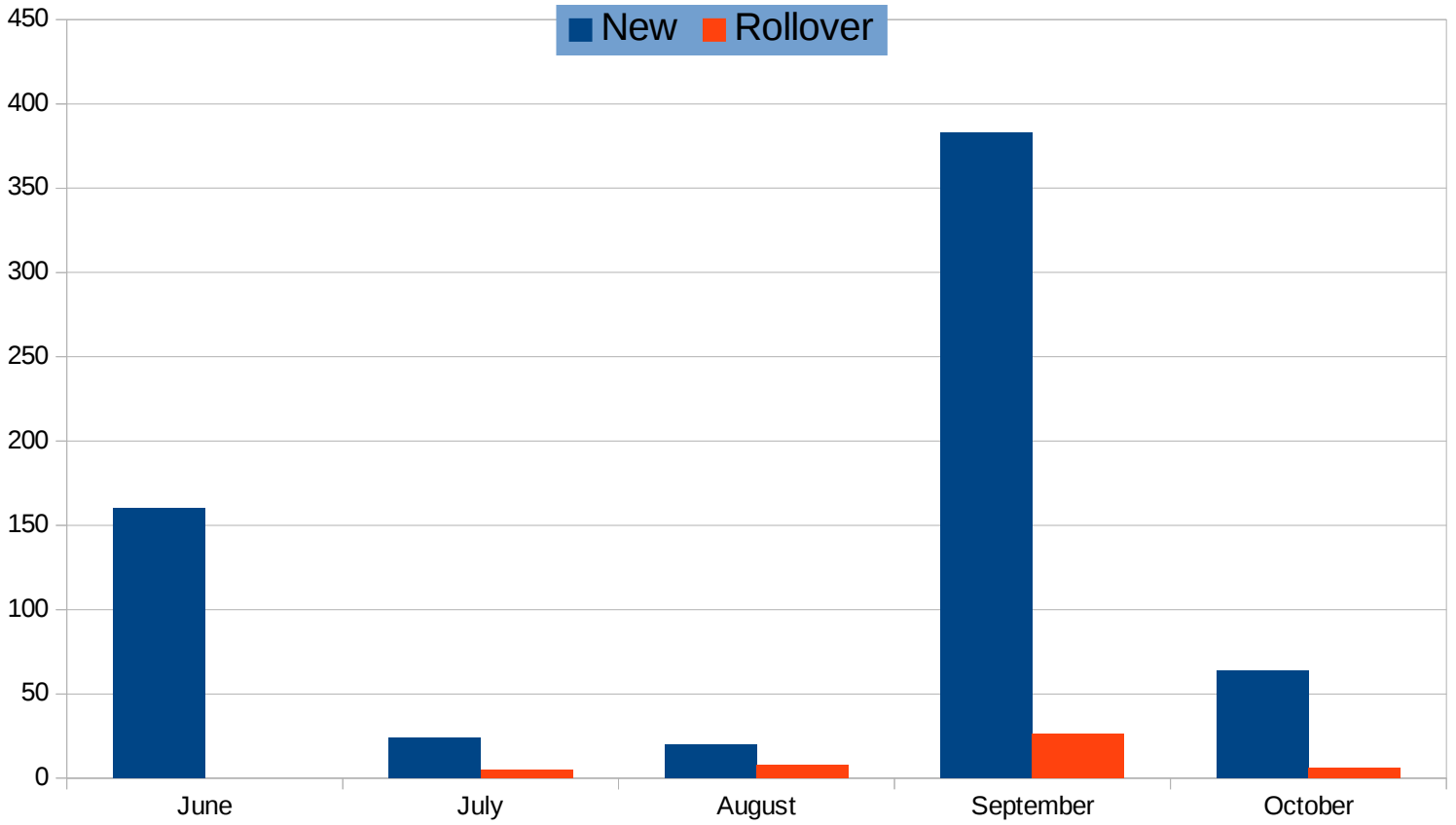
(get domains with nameservers, update DNSSEC, notify contacts)

FRED specific layer

- Server-side daemon
- Implements CORBA interface for accessing registry data
- Can be replaced with registry specific part

Statistics

- 627 domains under management



Plans

- Opt-out discussions
- Adding more scanning locations
- Updating notification of contacts
- Implementing also PUSH model according draft in both KnotDNS and FRED
- Marketing

Thank You

Jaromir Talir • jaromir.talir@nic.cz • https://fred.nic.cz
https://www.knot-dns.cz