Key & Signing Policy (KASP) in BIND 9.16

Matthijs Mekking, ISC
DNSSEC signing in 9.11 - 9.14

- Configuration:

```plaintext
options {
    auto-dnssec maintain;
};
```

- Zone must be either Dynamic, or have `inline-signing` set
- Expects keys to be created with `dnssec-keygen`
- Keys will be used for signing depending on their metadata
- Metadata can be set with `dnssec-settime`
- Manage rollovers with a Python tool `dnssec-keymgr`
- DNSSEC parameters and timings in `dnssec-policy.conf` and in `named.conf` determine metadata values
DNSSEC signing in 9.16

options {
    dnssec-policy "default";
};
DNSSEC Made Easy

- Easier for operators
  - More intuitive
  - More automated
- Easier in multi signer model
  - Easier reference
  - More vendors use KASP
- More robust
  - Don’t rely on metadata
  - Use a key timing state machine
Default Policy

- Single CSK
  - ECDSAP256SHA256. Unlimited lifetime
  - RRSIG validity 14 days, refreshes 5 days before expiration

- NSEC

- Key timings:
  - DNSKEY TTL: 3600 (1 hour), Max Zone TTL: 86400 (1 day)
  - Key publish and retire safety times: 3600 (1 hour)
  - Propagation delay: 300 (5 minutes)

- Parent timings:
  - DS TTL: 86400 (1 day)
  - Propagation delay (SLA): 3600 (1 hour)
Your own signing policy

```plaintext
zone "kitten.example" {
    dnssec-policy "cats";
};

dnssec-policy "cats" {
    keys {
        ksk lifetime 365d algorithm rsasha256 2048;
        zsk lifetime 30d algorithm rsasha256 1024;
    }
};
```
Your own signing policy

dnssec-policy "cats" {
  keys {
    ksk  lifetime 365d algorithm rsasha256 2048;
    zsk  lifetime 30d  algorithm rsasha256 1024;
  };

dnskey-ttl 600;
publish-safety PT2H;
signatures-refresh 7d;

  // to be released in 9.16.9
  nsec3param iterations 5 optout no salt "ffff";
};
Options that will be obsoleted

- auto-dnssec;
- dnskey-sig-validity;
- dnssec-dnskey-keyonly;
- dnssec-loadkeys-interval;
- dnssec-secure-to-insecure;
- dnssec-update-mode;
- inline-signing;
- max-zone-ttl;
- sig-validity-interval;
- update-check-ksk;
- ...

Death Valley, USA, 2015
The BIND key manager

- Key generation
- Publish CDS and CDNSKEY
  - Already introduced in 9.11
- Works on multiple zone types
  - Primary (dynamic or static)
  - Secondary (bump-in-the-wire)
- Algorithm rollover
  - just a reconfig
- RNDC DNSSEC commands
  - rollover, checkds, status
DEMO
What’s next?

- **Short term**
  - NSEC3 support (9.16.9)
  - Check DS RRset at parent
  - Derive TTLs from zones

- **Long(er) term**
  - RFC 5011
  - Offline KSK
  - Standby keys

RX-O Unicorn Gundam, Hakata, 2019
Thank you for your attention

Jack Parow, Liberation Festival, 2018