Automatic Key Management for BIND

Evan Hunt
ISC

BIND can roll keys (ZSKs, soon also KSKs) on a pre-determined schedule, but the scheduling has to be done by hand and is cumbersome:

```
$ ksk=`dnssec-keygen -3fk example.com`
$ zsk1=`dnssec-keygen -3 example.com`
$ dnssec-settime -I now+6mo -D now+7mo $zsk1
$ zsk2=`dnssec-keygen -S $zsk1`
$ dnssec-settime -I now+1y -D now+13mo $zsk2
$ zsk3=`dnssec-keygen -S $zsk2`
```

… and so on ...

We need fire-and-forget maintenance of DNSKEYs…

- Zone security policies (key strength, signing paramters, rollover period, coverage period) defined in a policy file, like:

```
policy default {
        algorithm rsasha256;
        coverage 1y;
        roll-period zsk 6mo;
        pre-publish zsk 6w;
        post-publish zsk 6w;
        keyttl 1h;
};
```

- Tool to be run unattended (e.g. by cron) to check the keys adherence to policy, and make changes or generate new keys when needed.

`dnssec-keymgr`

It's 90% done! Now to do the other 90%.

Python source:

https://github.com/each/bind9-collab

... in the "`dnssec-keymgr`" branch.