DNSSEC Status (operational view)

Icann 54, October 20th, 2015

Vincent Levigneron

DNSSEC's genesis at AFNIC

- ✓ DNSSEC started en 2010 (DS registration in April 2011)
  - ✓ 6 ccTLDs (.fr, .re, .tf, .pm, .wf, .yt) signed
  - ✓ 3 HSMs (Production/Sandbox/Dev) AEP Keyper in the same facility
  - ✓ NSEC3+Opt-out+Dynamic Updates
  - ✓ 1 OpenDNSSEC instance for key management, Bind used to sign the zones
  - ✓ Unique and static Salt (BA5EBA11 ☺)
  - ✓ Key ceremonies done manually (took a lot of time and sometimes failed)
  - ✓ Very few signed records in zone files

DNSSEC (re)volution at AFNIC

- ✓ Today, we still operate 6 ccTLDs but also 15 gTLDs
  - ✓ 19 HSMs distributed in 3 different locations, some dedicated for the disaster recovery plan
  - ✓ 16 independent OpenDNSSEC instances
  - ✓ Salt rolled over once a week and unique for all gTLDs and ccTLD bundle
  - ✓ 120 ZSK rollover per year (Only 6 for KSK since 2010, +6 next month)
  - ✓ Key ceremonies automatised
  - ✓ 3,1 Millions domaines names, 290 000 are signed (9,3%)
    - ✓ From 1 to 250 000 domain names signed (from 1% to 46%)

afnic

DNSSEC management at AFNIC

- ✓ AAK/SMK management can be cumbersome (it must be done physically on HSMs)
  - ✓ Same AAK is used on all productions HSMs
  - ✓ We mainly use 2 SMK, one for all gTLDs, the other for ccTLDs
- ✓ HSMs are not dedicated
  - ✓ Some host 1 TLD, others host 8 TLDs
  - ✓ Each TLD use 2 load-balanced HSMs, and another HSM for the DRP
  - ✓ We can not mix HSMs used for gTLDs with the ones used for ccTLDs
  - ✓ With only 32 sessions per HSM and the need to have more than one session for some TLDs, this ressource becomes critic (40% allocated to date)
- ✓ HSMs Batteries should be changed… We need a plan…

DNSSEC automation at AFNIC

- ✓ Tailored scripts has been written in order to support key ceremony process
- ✓ The whole ceremony now takes no more than 30 minutes
- ✓ It is done in our main facility (thanks to the load-balancer, no need to go in datacenters anymore) on a dedicated HSM used for all ceremonies
- ✓ Of course, for security reasons we still need humans to set HSM Online and backup keys on Smart Cards
- ✓ Complete rollback is possible in case of problem

DNSSEC ceremonies at AFNIC

- ✓ We need to have a key ceremony/TLD/a year
- ✓ We have scheduled that to have at least one key ceremony per month
  - ✓ 9 Operators/9 Security officers
  - ✓ 2 special operators who operate the scripts
  - ✓ 3 masters of ceremony (change every month)
- ✓ So everybody is involved, at least 2 times a year (16 ceremonies/year, one for the ccTLDs bundle, one for each gTLD)
- ✓ Backup on Smart Cards only new keys (One SC/TLD)

DNSSEC futur plans at AFNIC

- ✓ Improve our scripts
- ✓ Work on battery maintenance plan
- ✓ Add centralized control system for all OpenDNSSEC/HSMs
- ✓ Improve alert system for key exhaustion

DNSSEC (non operational view)

- ✓ 4th year of DNSSEC training program with HSC
- ✓ Live « DNSSEC Howto » sessions
- ✓ We just launched our third DNSSEC promotion plan
  - ✓ Discount for signed zones

Thank you !

www.afnic.fr
Vincent.Levigneron@afnic.fr