nominet

.uk DNSSEC Status update

02/05/2011

Brett Carr

Introduction

- .uk DNSSEC
- September 2010 Issues
- SLD DNSSEC
- DNSSEC Signing Service.

.uk DNSSEC

- .uk Signed March 2010
- Uses:
  - Opendnssec
  - Centos
  - Oracle HSM's
  - Three sets of identical hardware/software
- NSEC3 not needed but deployed.
- ZSK rolled every 6 months automatically
- KSK rolled every 3 years
- Low TTL on DNSKEYS to ensure rapid recovery from *issues*

September 2010 Issue

- HSM Hardware failure caused OS crash
- HSM Locked on reboot
- System designed with no urgency to fix so wait
- Failover to backup system
- Opendnssec key db/config file inconsistency
- 2 Day TTL on DNSKEY caused slow recovery

What did we change/learn

- Don’t lock HSM’s on reboot add’s extra security but more complexity.
- Improved checking procedures for failover
- Reduce TTL on dnskey to 1 hour so recovery is quicker

SLD DNSSEC

- Signing of:
  - me.uk
  - co.uk
  - ltd.uk
  - plc.uk
  - org.uk
  - net.uk
  - sch.uk
- Zones are very large and dynamically updated every minute.
- BIND 9.7.3 Continuous signing:
  Create the keys then add this to your configuration:
  auto-dnssec maintain;
  sig-validity-interval 35 28;
- Single Key (no KSK and ZSK) as we are the parent
- No scheduled rollover
- DS’s accepted from capable registrars 18 May

DNSSEC Signing Service

- Encourage deployment of DNSSEC further.
- Registrar gives us unsigned zone (via notify and axfr)
- Nominet signing systems create a signed zone.
- Notify sent to customer DNS system for AXFR.
- For *.uk zones Nominet signing system inserts DS record into parent.

nominet

Questions/Comments