DNSSEC at Nominet

Roy Arends
Head of Research
Nominet UK
Achievements

- Signed UK in March 2010
- NSEC3
- HSM for DNSSEC
- DNSSEC Management
- OpenDNSSEC
Signing of Second Level Domains

- Started work on Second Level Domains
- Continuous Signing in BIND 9 (2008)
- PKCS11-engine
An Unfortunate Event

- UK DNSKEY issue
- an extreme combination of events
- despite rigorous testing
- HSM failure kicked it off
- Test for 1M things does not make the system failure proof.
Redesigned SLD Architecture

- Initially, no HSMs
- No ZSK/KSK split, just one key
- Not announcing DNSKEY rollover
- Nor announcing a frequency
- Changing the DNSKEY TTL to 1H
Current state:

- Testing the entire system
- Ironing out some issues with BIND-9
- Great support from ISC’s BIND-9 team
- Don’t want to be canary in coalmine
Future of DNSSEC

- Very little validation at the moment
- Not all DNSKEY/DS queries are because of validation
- Hardly anything is signed
Despite Necessity

- Scare tactics didn’t really work
- Kaminsky: trivial attack, no evidence
- Should have been the tipping point

- Real promise are new uses, like certificates in DNS
Current Paradigm

• Create a Key
  – understand all possible variations
  – learning curve

• Sign a zone
  – a zone _FILE_ often
  – NSEC/NSEC3/OPTOUT
  – Another Learning curve

• Roll keys, Algorithms
  – Several Learning curves

• Communicate DS to parent
Paradigm Shift

- What SSH did for TELNET
- ubiquitous DNSSEC
- Server:
  - auto dnssec by default
  - simple and secure defaults
  - no manual labour
- Resolver/validator
  - ship with validation on
  - and root key hints
From the registry

- DNSSEC Signing Service
- For the registrar community
- Takes the DNSSEC headaches away
- An additional hop
- Takes unsigned, returns signed zones
Simple Signing Service
Complete Signing Service
Signing Service and OpenDNSSEC

• What about OpenDNSSEC?

• We see both having an important place in UK DNSSEC deployment
  – OpenDNSSEC:
    • anyone wanting to control their own DNSSEC deployment
  – Signing Service:
    • Getting DNSSEC up and running quickly
    • A full time service where internal resources constrained
Thank You.