nominet

Signing .uk

Ian Meikle, UKNOF15 , 21 January 2010

Agenda

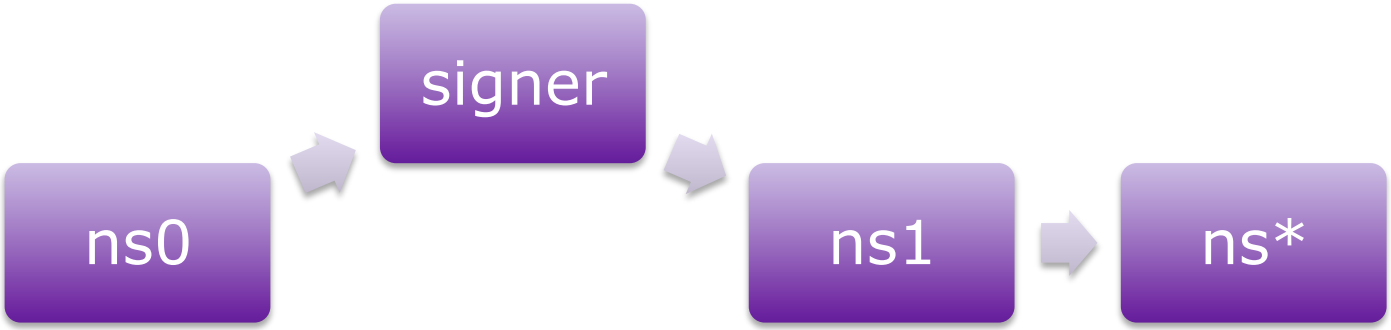
- Justification
- Signing mechanism
- Security concerns
- Timeline
- Questions

Justification

- Vision - Committed to a secure Internet
- First (and simplest) step to signing all of .uk
  - Small, static zone
  - SLDs coming next

Signing Architecture

nominet



Signing mechanism

Opendnssec

nominet

Opendnssec is a free, open-source DNSSEC tool

Intended as ‘one-stop shop’ for DNSSEC deployment

Developed by a coalition, including Nominet and other ccTLDs

Performs functions of

- Zone signer
- Auditor
- Key management
  - Scheduling key rollovers

Signing mechanism

Signing parameters

nominet

Multiple signing parameters

Non-exhaustive list:

- KSK
  - 2048 bits
  - 3 year lifetime
- ZSK
  - 1024 bits
  - 6 month lifetime
- Signatures valid for 2 weeks
- Zone signed daily

Signer

nominet

Signer consists of

- Server
  - HP DL365
  - Centos 5
- HSM
  - SCA 6000 PCI Card

Continuity

nominet

Areas of concern

Multiply redundant systems

- Signer (in Oxford)
  - With ‘leading’ HSM
- Backup signer (in Oxford)
- Offsite backup signer (at DR site)
- Exported keys

Security concerns

nominet

- External security audit commissioned
- Main recommendations
  - Encrypt USB sticks
    - Three copies
  - Lock them away
    - In different places
  - Separate access/operator roles
    - Two actors per role
  - Change management
  - Regular testing

Timeline

Major milestones

nominet

Always intended to be in early 2010

Governance issues have been primary concern

- 1 March – DNSSEC info in .uk zone
  - Using blurred keys
  - Limited to selected nameservers
- 8 March – Valid keys and signatures in .uk zone
  - On all .uk nameservers
  - But not published elsewhere
- Extended Operational Testing
- July (?) 2010 – .uk DS R in the root
  - When IANA accepts it

Signing .uk

Questions?

nominet