
DNSSEC for .nz

Report of progress

Sebastian Castro
sebastian@nzrs.net.nz

NZRS



Architecture

- “Bump on the wire”
 - Signing box receives unsigned zones and delivers signed zones
 - Implemented using
 - Sun Intel servers
 - OpenDNSSEC
 - SCA 6000 HSM
 - Redundant and fault tolerant as the SRS system is.

Policy/Procedure work

- Policy changes in progress
 - To introduce DS records as registration data
 - To encourage registrars to cooperate during signed domains nameserver change
- DNSSEC Policy and Practice Statement (DPS)
 - Almost complete
- Key Ceremony
 - Internally tested, requires refinement
 - Will use some of the elements from the Root Zone Key Ceremony

Software/Hardware

- Changes to SRS: Complete
 - But the feature is disable until deployment date
- Changes to infrastructure: almost complete
 - Signers are in place
 - Zone Generation changes are complete
- Testing system
 - Almost running automatically, should be ready in a couple of weeks

Major headaches

- SCA 6000
 - “Amusing” piece of hardware
 - We use Debian for all our system
 - Debian not supported by SCA
 - HSM drivers not stable => crashes/kernel panics
 - Switched to CentOS
 - Crashes hasn't gone away yet
- OpenDNSSEC
 - We've been heavily involved on testing, reporting bugs and providing patches
 - It's good enough, but still has rough edges

Deployment plan

- Testing should be finished by the end of February
 - ... fingers crossed
- Planning to deploy around April 2011
 - .nz will be signed first
 - Second level domain will follow, **geek.nz** likely to be the first
 - Closely afterwards we will accept DS records for it
 - Staggered activation for the rest, one SLD at a time

Questions?

- Feel free to contact us if you have
 - Suggestions
 - Comments
 - Questions
 - Interest on testing

Sebastian Castro => sebastian@nzrs.net.nz

Dave Baker => dave@nzrs.net.nz