

New Zealand Domain Name Registry Limited

# **DNSSEC** in .nz

Jay Daley 2013

 p: (+64) (4) 931 6977
 e: registry@nzrs.net.nz

 f: (+64) (4) 931 6979
 w: www.nzrs.net.nz

 P.O. Box 24361, Wellington, New Zealand

 New Zealand Domain Name Registry Limited



### **Current Position**

- Ø DNSSEC fully implemented
- Staged rollout May-Sep 2012
  - geek.nz as the first second level
  - Others including co.nz
  - Ø Moderated second levels like govt.nz
- Second send of key signing ceremonies
- ~30 signed zones from ~520,000

# Checklist

- Ø DNSSEC Practice Statement
  - « Key management policies
- Ø Signing infrastructure (using HSMs)
- Ø Software changes
- Rollout plan
- Side effects dealt with
  - Zone transfer time
  - Amplification attacks

# DNSSEC Practice Statement (DPS)

- Community acceptance
  - Agreement with regulator
  - We publish DPS and consult community
- Verifies
  - We are meeting needs of our users
  - Technical scrutiny
- BUT .... Lots of problems !
  - Ø Substantive issues follow

#### "KSK size too small"

- We chose 1152
- Some in community wanted 2048
  - "Everyone else does it"
  - "We should have the strongest possible"

- Famous cryptographer defended 1152
  - Not enough for some
- We changed to 2048

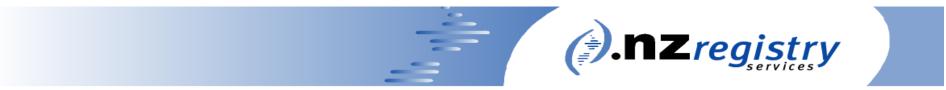
- "Must audit staff thoroughly"
  - Criminal checks
  - Financial checks
  - Ø Drug checks
- We were only planning criminal
   "We trust you but what if you leave?"
- Agreed to financial checks for new staff

- "Need Trusted Community Representatives (TCRs) like ICANN"
   "They provide independent audit"
- Our response
  - More people to security vet
  - Already have independent auditors
  - ICANN method is security theatre
- We did not include TCRs

- "Need full details of site security"
  - "Cannot trust if we do not know"
- Our concerns
  - Too much information makes them a target
- Final agreement
  - Ø Specification for site security published
  - Protocol for site access included

## Conclusion

- Community engagement on DPS is vital
- Some views will be irrational but must be accommodated
  - This is the community view after all
- Lots of very useful feedback
- Very useful process overall



New Zealand Domain Name Registry Limited

# **Any questions?**

#### jay@nzrs.net.nz

 p: (+64) (4) 931 6977
 e: registry@nzrs.net.nz

 f: (+64) (4) 931 6979
 w: www.nzrs.net.nz

 P.O. Box 24361, Wellington, New Zealand

 New Zealand Domain Name Registry Limited

