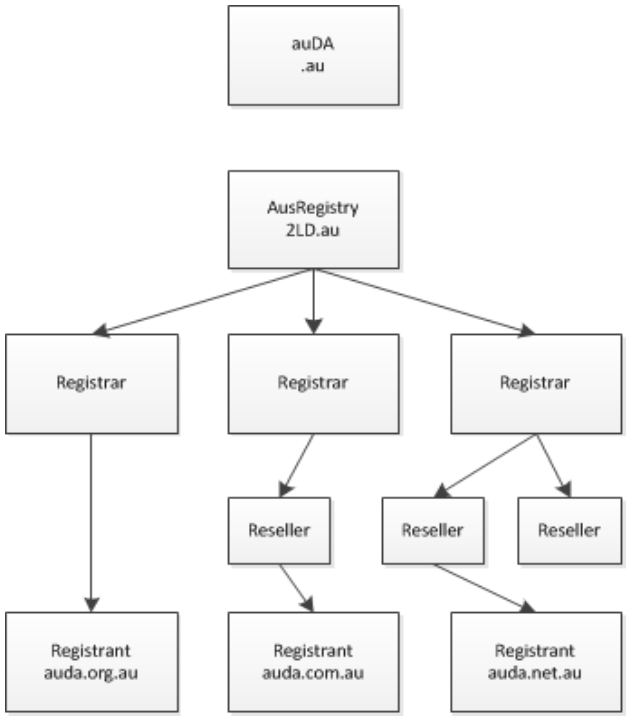
# DNSSEC deployment in .au

Adam King
.au Domain Administration Ltd (auDA)
ICANN52 DNSSEC Workshop Feb 11 2015

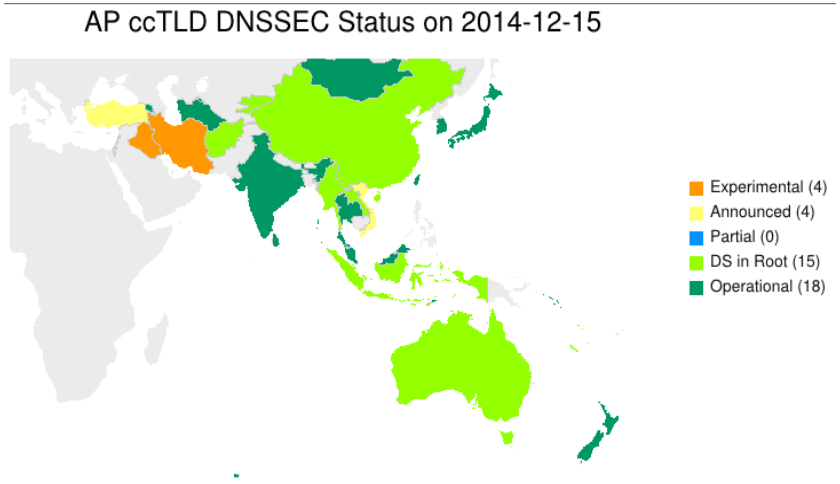
.au DOMAIN ADMINISTRATION LTD

# Background & Structure of .au




* auDA registry for .au
  * Closed space
* AusRegistry for 2LDs
  * 16 2LDs
  * 3 million registrations
* Registrars interface with AusRegistry

# Where are we now?




* Source http://www.internetsociety.org/deploy360/maps

* 20 November 2014 submitted KSK to IANA
* 25 November 2014 officially added to root
* 01 December 2014 submitted 2nd KSK to IANA
* 08 December 2014 IANA added 2nd KSK to root
* 31 January 2015 request IANA remove 1st KSK – end double sign period

# Where are we now

* 04 December 2014 added 12 2LD DS records
  * act.au, nsw.au, nt.au, qld.au, sa.au, tas.au, vic.au, wa.au, conf.au, asn.au, id.au, edu.au
* 10 December 2014 added the big 3 2LD DS records
  * com.au, net.au, org.au
* 1 February 2015 enabled registrars to add registrant DS
* Cautious approach

# How we got there

* August 2010 announced a 5 phase process
  * Experimentation, Rollout of signed zones, Trial for registrants, Production DS for registrants, Encourage validation
* 2011 tested on and off
  * Manual signing, key sizes/algorithms
  * Kept watched of those who signed (20 including .com)
    * 4 reported outages ( source http://ianix.com/pub/dnssec-outages.html)
  * Added a sub phase – working with stakeholders

# How we got there

* 2012 Inline signing & HSMs
  * Set a list of goals
    * DNSSEC as easy as DNS
      * Manual edits
    * Sign our zones with as little complication as possible using processes that are the least time consuming but are balanced with an appropriate level of security.
  * Feb Bind 9.9 released with inline signing to compliment auto-dnssec
  * Private key data on encrypted stores using LUKS on RAMDISK
    * Encrypted partition online/offline - security
    * Mount, unmount, password management etc
  * April dnssec-wg formed
    * DPS, non-registry aspects (education/awareness)
  * June/July looked at HSM providers
  * September 2012 started testing with a HSM

# How we got there

* 2013 Policy, Monitoring & Verification
  * HSM was better fit with our goals
    * Key online & protected
  * Writing policy, documentation
  * RRSIG monitoring, validated responses
  * Verification checks and scripts
    * Before pushed to slaves
    * SOA on slaves, record validation
* 2014 Finalise, Experimental, Sign
  * Processes, Ceremonies, documentation
  * April 24 added KSK & ZSK experimental
    * 1 a month for 3 months double signed
  * August moved to pre-publish 4th ZSK
  * September 5th ZSK
  * October KSK rollover

# What we learnt

* Technically not difficult
  * Time spent on policy & documentation
* It was ok to wait
  * Allowed design changes
    * Software/hardware
  * Allowed process changes
    * Double sign ZSK
    * Key validity periods
    * Interactions/personnel
  * Allowed documentation improvement
    * Rewrites, testing
  * Improved validation checks
  * Technology to improve

# What we learnt

* Manual vs automated management
  * Outages
  * Learn from other people mistakes
* Automation!!
  * Human touch
* Process & verification

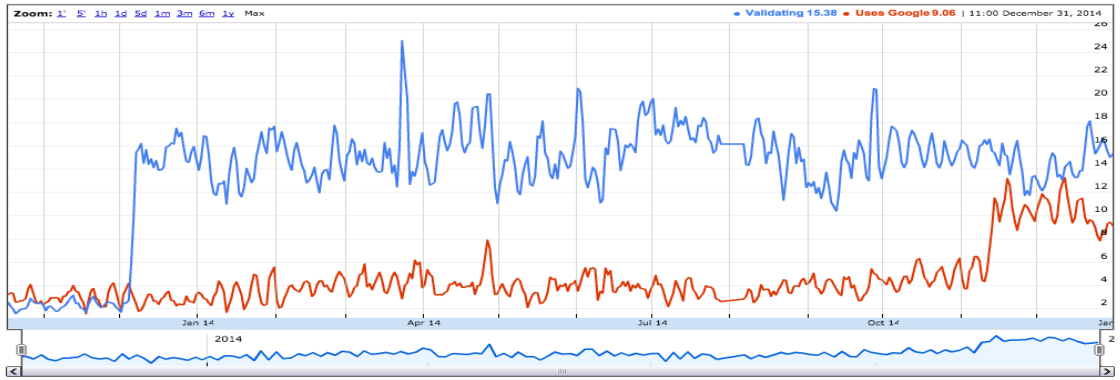
# What's next?

* 5 Phases
  * Experimental ✓
  * Rollout of signed zones ✓
  * Trial for registrants ✗
  * Production DS for registrants ✓
  * Encourage Validation
* Monitor take up
  * If needed work with Registrars
* Registrar transfer may be an issue
  * DNSSEC capable to non DNSSEC capable

# DNSSEC Validation for AU

* 2013 comment on AusNOG list
  * "2% of Australian users appear to be using DNSSEC when resolving names. Of those, 70% of them do so by virtue of their use of 8.8.8.8"
* 2014 this has increased

**Use of DNSSEC Validation for Australia (AU)**




Source http://gronggrong.rand.apnic.net/cgi-bin/ccpage?c=AU

.au DOMAIN ADMINISTRATION LTD