DNSSEC in the Reverse Tree
@LACNIC

Arturo Servín -- @the_real_r2d2
Carlos Martínez -- @carlosm3011
Why DNSSEC?

• Securing the DNS system is both necessary and, right now, doable
  – Root signed since 2010
  – No excuses!

• A signed DNS tree can also be an enabler for new applications
  – DANE WG

• DNSSEC does not solve _every_ problem in the DNS system
  – But it certainly helps a lot
DNSSEC @ LACNIC: Timeline

• 4Q 2010 – 2Q 2011
  – Training, study, tool testing

• 3Q 2011 – 1Q 2012
  – Experimental zone signing
    • <lacnic>.ip6.arpa
    • A few forward zones
  – Trial key rollovers and technical definitions

• 4Q 2012 – 1Q 2013
  – Reverse zones signed in production
DNSSEC @LACNIC: Status

- Status of DNSSEC in the reverse tree @LACNIC:
  - Reverse zones for IANA-allocated LACNIC space signed
    - ERX / Legacy depending on majority holder
  - DS records from members
    - Currently we can insert DS records manually, for testing purposes
    - Provisioning system support for DS records for 2Q 2013
Signer Architecture

- Hidden signer plus public masters
Final Remarks

• The root is signed! Make good use of it!
  – No need for static, out-of-band trust anchors
  – Making the DNS more secure is our duty as technical community

• Useful signing performance is possible even with commodity hardware
  – Unless your zones are really huge

• NSEC vs NSEC3 in the reverse space?
  – NSEC3 doesn’t seem to make a lot of sense here
THANK YOU!