Implementation of DNSSEC in .SG

Danny Chan
Technical Manager

Feb 2015
APTLD Meeting
Content

• Background
• Strategy Overview
• Software & Policy Development
• Key Ceremony
• Partial Deployment
• Full Deployment
• Further Enhancements
Background

Back in 2009…

- Working group formed to study DNSSEC
- Summary of findings:
  - Complicated and risky for DNS zone operators if not done right
  - No demand from end users or registrants
  - Software, tools, policies and best-practices are not mature
  - Once deployed at cc level, it is a irreversible commitment of resources while being subject to all the risks – technical and reputational - even if there’s no customers
Background (cont.)

2010…2011…2012…2013

• DNSSEC test-bed created
  ➢ Not successful.
  ➢ No registrar was willing to participate.

• But with the root signed, DNSSEC is likely to be a standard offering some day
  ➢ Monitor global deployment and be prepared

• Continuous effort to create the awareness
  ➢ 2 workshops for local engineers (2010 and 2014)
2014… and now in 2015

• Slightly less complicated and risky for DNS zone operators
• Still no demand (globally 0.x to 0.5%?)
• Software, tools, policies and best-practices are better
• Maybe this is about the right time to get started
Overview

- Research
  - Software
  - Policies
  - Procedures

- Development
  - Key Ceremony (KC) Rehearsal
  - Emergency Recovery Drills
  - Pilot Run
  - Actual KC

- Partial Deployment
  - DS submission to Root Zone
  - Official Launch

- Full Deployment
Research

• DNSSEC Practise Statements of pioneer registries
  ➢ Key length, algorithm, rollover, TTL, DS validation mechanism, key management…
  ➢ Root zone, .se, .nl, .nz, .cn, .com .jp, etc.

• Lessons learned from DNSSEC outages and validation failures
  ➢ KSK rollover issue
  ➢ RRSIG (Signature) validity issue
  ➢ Others (software, configuration and etc.)
Development

- Develop DNNSEC Practice Statement (completed)
- Develop key ceremony procedure (completed)
- Enhance registration & zone signing software
  - DS record validation (GIGO issue)
  - Auto dynamic signing (performance issue)
  - Automated key rollover & monitoring (unexpected issue)
- Develop transfer related policies
- Develop emergency drill plan
Key Ceremony

- Based on ICANN’s Key Ceremony procedure
- Security
  - Outsource the physical security portion (safe/vault)
  - Offline environment & controlled room
  - Two-man rule
  - Anti-tampering
- Transparency
  - Internal & External Witnesses
  - Recorded (log) and published on SGNIC website
Partial Deployment

• Pilot Run
  ➢ SGNIC zones will be signed
  ➢ DS records will not be submitted to Root Zone yet
  ➢ Allow trial in production environment w/o impact on normal DNS resolution
  ➢ Invite registrars to participate
    ▪ Sign their zone
    ▪ Submit their DS to SGNIC
    ▪ Add SGNIC’s public key to their validator
    ▪ Turn on the validation
Partial Deployment (cont.)

• Practise, practise and practise!
  ➢ Key ceremony rehearsals
  ➢ Key rollovers
  ➢ Recovery drills

• Conduct actual key ceremony
  ➢ Actual key will be used and monitored for a period of time before the Full Deployment
Full Deployment

- Submit DS to root zone
- Target: 2016/17
- Continue Practise, practise and practise!
Further Enhancements

• Key Expiration Alert
  ➢ Monitor children’s DNSKEY against DS record
  ➢ Monitor children’s key validity