.sg DNSSEC

Ryan TAN
Head (Technical and Operations)
7 Nov 2016
ICANN Hyderabad
Background

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
  - No registrar was willing to participate in SGNIC DNSSEC testbed
  - 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
  - But with the root signed, DNSSEC is likely to be a standard offering *some day*
- Monitor global deployment and be prepared
- Prepare the industry: 2 workshops for local engineers (2010 and 2014)
Background

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 the right time to rollout DNSSEC
Implementation Approach

Research
- Understand the lessons learnt from pioneer registries

Development
- Enhance registry software (to accept DS)
- Enhance zone signing software
- Develop Practise Statement
- Develop Key Ceremony procedures and systems

Partial Deployment
- Rehearse Key Ceremony (KC)
- Conduct KC
- Pilot Run
- Conduct emergency recovery drills

Full Deployment
- Submit DS to Root Zone
- Official Launch on 23 Sep 2016
Current Status

- 5 (out of 18) registrars support DNSSEC DS management
- 0 .sg domain name signed (as at 23 Oct 2016)
- The Singapore Government plans to sign gov.sg domain names by the first quarter of 2017
- Local DNS hosting providers still find it a challenge to implement DNSSEC
End