

Internet Identity For All

.my DNSSEC Deployment Plans & Experience

YawEng, Yong (myDNSSEC Project Leader)

22nd June 2011, Wednesday

DNSSEC Workshop

DOMAIN REGISTRY

Agenda

- Overview of DNSSEC Deployment in Malaysia
- Post Deployment Issues
- Some findings from the Public Trial
- Efforts in Promoting DNSSEC
- Challenges Ahead



Overview of DNSSEC Deployment in Malaysia



my DNSSEC Implementation Milestones

Public Trial

Duration: 29th Dec - 16th May 2010

Zones: All zones

Trust Anchor: IANA DNSSEC Root Test Bed



Production

Signed since 9th Oct 2010 (DS Added in root on 11th Dec 2010)

Zones: All zones

Trust Anchor: Root



Duration: 31st Mar - 31st Oct 2009

Zones: .my & .net.my

Trust Anchor: IANA DNSSEC Root Test Bed



.myDNSSEC Deployment Details

Key Algorithm: RSASHA256 with NSEC3 Opt-out

Key Signing Key (KSK)

KSK lifetime: 1 year (i.e. rollover every 12 months)

KSK bits : 2048

Zone Signing Key (ZSK)

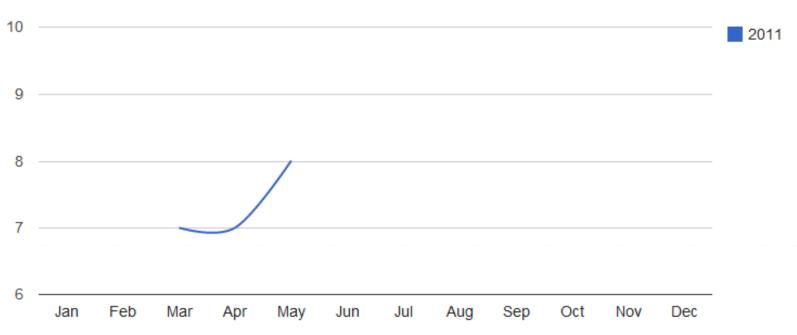
ZSK lifetime: 12 weeks (i.e. rollover every 3 months)

ZSK bits : 1024



Current Status





Number of Domain Names with DNSSEC:

** As of 24 May 2011

Month*		.my	.com.my	.net.my	.org.my	.gov.my	.edu.my	.mil.my	.name.my	Total
2011	May **	6	0	0	1	0	1	0	0	8
	Apr	5	0	0	1	0	1	0	0	7
	Mar	5	0	0	1	0	1	0	0	7

Please see: http://domainregistry.my/en/statistics.php



Post Deployment Issues

DOMAIN REGISTRY

Post Deployment Issues

2 Issues:

- Unable to get a NSEC3 response to prove that a record is without DS Record (i.e. a non-signed delegation, since NSEC3 with opt-out only sign records with DS)
 - Temporary workaround: Whenever a zone is without any DS from child, exclude the DS from .my zone.
 - E.g.: If .mil.my is without any child delegation signed, .mil.my DS will not be included in the .my zone
- 2. Timing of rollover was wrongly set (overlooked, and contain default configuration)
 - ZSK was changed before there was enough time to allow to propagate the new key (< 2x maximum TTL).
 - Fix by rectifying the configuration



Some Relevant Findings from the Public Trial



Findings from the Public Trial

- 1. General public acceptance is low because:
 - a. Lack of awareness and education on DNS technology
 - b. Not able to control own zone file (usually handled by Hosting Providers)
 - c. Reluctant as it is still perceived as not urgent
- 2. ISPs need more persuasion to support DNSSEC
- 3. The Central Bank is supportive generally. But up to banks to adopt the technology.
- 4. Does not seem to be an issue for those who are able to handle own zone file.



Efforts in Promoting DNSSEC

Efforts in Promoting DNSSEC



2006 - 2008

• .myTraining

2009

- .myTraining
- Awareness Road Show in 5 states

2010

- Meeting with Resellers
- Meeting with ISPs
- DNSSEC
 Workshop
 (APTLD 3rd
 March 2010)
- Meeting with BNM / Banks

2011

- DNSSEC
 Security Talk
 (MCMC) 3rd
 March
- ISOC
 Awareness
 Series –
 DNSSEC 12th
 May
- DNS / DNSSEC
 Training 29th
 June 1st July



Challenges Ahead

- Engaging ISPs (recursive DNS) to enable DNSSEC to do the validation
- 2. Encourage a greater adoption of DNSSEC by Authoritative DNS Administrators
- 3. Constant monitoring for any new issue with regards to DNSSEC deployment
- 4. Further improvements to the .my DNSSEC Environment (signing, key management, etc). There is a lot of room for improvements.

