.my DOMAIN REGISTRY

myDNSSEC

Technology And Innovation (TNI) Dept.

Norsuzana Harun

21st Aug 2009
myDNSSEC Implementation Plan

Phase 1
- Closed Test-bed (31st March – 31st October 2009)

Phase 2
- Public Trial (Q1 2010 – Q2 2010)

Phase 3
- Production (Q4, Oct 2010)
myDNSSEC Closed Test-bed
**myDNSSEC Closed Test-bed**

<table>
<thead>
<tr>
<th>Objective</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Raise awareness on DNSSEC technology</td>
<td></td>
</tr>
<tr>
<td>• Anticipate potential deployment issues</td>
<td></td>
</tr>
<tr>
<td>• Form “Best-Practices” Policies, especially with regards to Key Management</td>
<td></td>
</tr>
<tr>
<td>• Gather feedback from participants for improvement of .my DOMAIN REGISTRY</td>
<td></td>
</tr>
<tr>
<td>DNSSEC-enabled Registry System</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Duration</th>
<th>31st March – 31st October 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zones</td>
<td>.my</td>
</tr>
<tr>
<td></td>
<td>.net.my</td>
</tr>
<tr>
<td>IANA Test-bed</td>
<td>Joined since 23rd May 2009</td>
</tr>
</tbody>
</table>
myDNSSEC Closed Test-bed (cont...)
Zone signing process

1. Domain Registration & DNS Administration Web Interface
2. database
3. Zone Generator
   - Plain Zone
   - DS Key Generator
   - Signer
   - Signed Zone
4. DS Finger Print Retriever
   - Tester domain ‘s DNS
5. .my Key Generator
myDNSSEC Closed Test-bed (cont...)

Key’s information

- Key parameters for the zone
  - Key Usage, KSK/ZSK
  - Key Algorithm, RSA-SHA1/RSA-SHA256
  - Key Length, 2048/1024 bits

- Keys generation and signing Tool
  - dnssec-keygen to generate key
  - dnssec-signzone to sign .my and .net.my zone
myDNSSEC Closed Test-bed (cont...)

IANA DNSSEC Test Bed root server

Trust Anchor

Island of Trust

test1  test2  .net

a  b  c

.my  .com  .net  .org
myDNSSEC Closed Test-bed (cont...)

Dig your domain in Trust Anchors!

1. Dig your domain by using the Test Bed dig tool (dig for SOA).
2. You should see the “ad” flag in the result page.

```
RESULT:

dig @192.229.180.211 b.net.my soa +dnssec +multiline
; ;<>> DiG 9.3.4-P1 <<>> @192.229.180.211 b.net.my soa +dnssec +multiline
; ; (1 server found)
; ; global options: printed
; ; Got answer:
; ; =>HEADER<= opcode: QUERY, status: NOERROR, id: 53143
; ; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 7
; ; OPT PSEUDOSECTION:
; ; EDNS: version: 0, flags: do; udp: 4096
; ; QUESTION SECTION:
; ;b.net.my.
; ; ANSWER SECTION:
41 IN SOA ns1.dnshost.my. ns2.dnshost.my. (2917401847 ; serial
28800 ; refresh (8 hours)
7200 ; retry (2 hours)
604800 ; expire (1 week)
86400 ; minimum (1 day)
)

41 IN RRSIG SOA 5 3 60 20091025013130 (20090727013130 6468 b.net.my.
CIG1qulpuEUG/4vcfY3wHF73bNNc0cMKkugulTSnfd
0+fIv/7dsHglJyOdX7EyUvM277KcoCuX663Ub3k1MA
9J9dJkixe6OycKXV0mUx9xW8kKkU5KZ3nJLXb7Obtkw
1v03nKxy8ynDwR5KQqK2IN50DGJN7vFkdLs1pcE= )

; ; AUTHORITY SECTION:

b.net.my.

116438 IN NS ns2.dnshost.my.
b.net.my.

116438 IN NS ns1.dnshost.my.
b.net.my.

41 IN RRSIG NS 5 3 60 20091025013130 (20090727013130 6469 b.net.my.
WQdEMzQD7jxCwJyY99PrUMpQucYo1d65bGIdB2kXHPLM
VBw1SC5nN5X2vzsZhGYjx8bTabq1EyTVKXhe1yrFIL
6a6pTskH44az27Ibb6ECdflh43jx2pNCG0044NS/A7
K4DtW0JUqtaNp3D2INMDG9KFyfal/pCF/xdfKJt8= )
```
myDNSSEC Closed Test-bed (cont...)

Chain of trust tree from root and your domain name:

drill @192.228.180.211 -k /var/www/dnssec-html/key -S b.net.my
;; Chasing: b.net.my. A

DNSSEC Trust tree:
b.net.my. (A)
|---b.net.my. (DNSKEY keytag: 8025)
 |---b.net.my. (DNSKEY keytag: 34717)
 |---b.net.my. (DS keytag: 34717)
 |---net.my. (DNSKEY keytag: 14262)
 |---net.my. (DNSKEY keytag: 35668)
 |---net.my. (DS keytag: 35668)
 |---my. (DNSKEY keytag: 621)
 |---my. (DNSKEY keytag: 33859)
 |---my. (DS keytag: 33859)
 |---. (DNSKEY keytag: 61312)
 |---. (DNSKEY keytag: 28567)
 |---. (DNSKEY keytag: 34291)

;; Chase successful

root

my

net.my.

DNSKEY 33859 (257)
DNSKEY 621 (256)
DS 35668

DNSKEY 35668 (257)
DNSKEY 14262 (256)
DS 34717

DNSKEY 34717 (257)
DNSKEY 8025 (256)
## myDNSSEC Closed Test-bed (cont...)

<table>
<thead>
<tr>
<th>Awareness Seminar / Training</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Operators of authoritative DNS server</td>
</tr>
<tr>
<td></td>
<td>Operators of cache DNS server</td>
</tr>
</tbody>
</table>

### Activities

- Internet Banking Task Force (IBTF – 31 March 09)
- Government agencies
  - Sabah, Sarawak (27, 30 April 09)
  - Terengganu, Pahang, Johor (9, 12, 15 Jul 09)
- ISP, DNS Hosting Provider – 18 August 09
- DNS Training – Nov 09
myDNSSEC Closed Test-bed (cont...)

Steps involved  [ URL  http://www.dnssec.my ]

1. Registration
2. Add domain
3. Sign your zone
4. Upload your DS set to parent zone
5. Check your domain with Dig and Drill tool
## myDNSSEC Closed Test-bed (cont...)

<table>
<thead>
<tr>
<th>Participant Statistic (by invitation)</th>
<th>20 participants (as of 19 Aug 09)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• 7 ccTLD: Korea, Mongolia, China, Singapore, Hong Kong, Sweden, Austria</td>
</tr>
</tbody>
</table>
myDNSSEC Closed Test-bed (cont...)

Participant Statistic

- APTLD Member: 7
- Government Agency: 2
- Academia: 1
- ISP: 1
- Non-profit organization (NPO): 2
- Others: 2
- Private sector: 5

Participants by Month:
- March: 1, April: 2, May: 11, June: 11, July: 1, August: 1
<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Email</th>
<th>Company</th>
<th>Organization Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Baasansuren Burmaa</td>
<td><a href="mailto:burmaa@datacom.mn">burmaa@datacom.mn</a></td>
<td>.MN Registry, Datacom Co., Ltd</td>
<td>APTLD Member</td>
</tr>
<tr>
<td>2</td>
<td>Ben</td>
<td><a href="mailto:ben.lee@hkirc.hk">ben.lee@hkirc.hk</a></td>
<td>HKIRC</td>
<td>APTLD Member</td>
</tr>
<tr>
<td>3</td>
<td>Benjamin Choy</td>
<td><a href="mailto:ben.choy@hkirc.hk">ben.choy@hkirc.hk</a></td>
<td>Hong Kong Domain Name Registration Company Limited</td>
<td>APTLD Member</td>
</tr>
<tr>
<td>4</td>
<td>healthyao</td>
<td><a href="mailto:yaoijk@cnnic.cn">yaoijk@cnnic.cn</a></td>
<td>cnnic</td>
<td>APTLD Member</td>
</tr>
<tr>
<td>5</td>
<td>Lee Han Chuan</td>
<td><a href="mailto:hanchuan@sgnic.sg">hanchuan@sgnic.sg</a></td>
<td>SGNIC</td>
<td>APTLD Member</td>
</tr>
<tr>
<td>6</td>
<td>Marco Chan</td>
<td><a href="mailto:marco.chan@hkirc.hk">marco.chan@hkirc.hk</a></td>
<td>Hong Kong Domain Name Registration Company Limited</td>
<td>APTLD Member</td>
</tr>
<tr>
<td>7</td>
<td>YOUNGSUN LA</td>
<td><a href="mailto:rays@nida.or.kr">rays@nida.or.kr</a></td>
<td>KRNIC</td>
<td>APTLD Member</td>
</tr>
<tr>
<td>8</td>
<td>Abu Ubaidah Md Zain</td>
<td><a href="mailto:abu@ns.org.my">abu@ns.org.my</a></td>
<td>MCMC</td>
<td>Government agency</td>
</tr>
<tr>
<td>9</td>
<td>Ruzana binti Jaffar</td>
<td><a href="mailto:ruzana@johor.gov.my">ruzana@johor.gov.my</a></td>
<td>Unit Sains Teknologi dan ICT Negeri Johor</td>
<td>Government agency</td>
</tr>
<tr>
<td>10</td>
<td>Hanif Nordan</td>
<td><a href="mailto:hanif@um.edu.my">hanif@um.edu.my</a></td>
<td>Universiti Malaya</td>
<td>Academia</td>
</tr>
<tr>
<td>11</td>
<td>Paul Ooi</td>
<td><a href="mailto:paul.ooi@globaltransit.net">paul.ooi@globaltransit.net</a></td>
<td>Global Transit Communications Sdn Bhd</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>12</td>
<td>Champika</td>
<td><a href="mailto:champika@apnic.net">champika@apnic.net</a></td>
<td>Asia Pacific Network Information Centre</td>
<td>Non-profit organization (NPO)</td>
</tr>
<tr>
<td>13</td>
<td>Patrik Wallström</td>
<td><a href="mailto:patrik.wallstrom@iis.se">patrik.wallstrom@iis.se</a></td>
<td>.SE</td>
<td>Non-profit organization</td>
</tr>
<tr>
<td>14</td>
<td>Ku Geok Liong</td>
<td><a href="mailto:gl.ku@hotmail.com">gl.ku@hotmail.com</a></td>
<td>TPM</td>
<td>Others</td>
</tr>
<tr>
<td>15</td>
<td>Michael Braunoeder</td>
<td><a href="mailto:mib@nic.at">mib@nic.at</a></td>
<td>nic.at</td>
<td>Others</td>
</tr>
<tr>
<td>16</td>
<td>Chan Kelwin</td>
<td><a href="mailto:ckelwin@kompakar.com">ckelwin@kompakar.com</a></td>
<td>Kompakar eBiz Sdn Bhd</td>
<td>Private sector</td>
</tr>
<tr>
<td>17</td>
<td>Julian Vincent</td>
<td><a href="mailto:jvincent@infoweapons.com">jvincent@infoweapons.com</a></td>
<td>Infoweapons Sdn Bhd</td>
<td>Private sector</td>
</tr>
<tr>
<td>18</td>
<td>Nik Muhammad Izwan</td>
<td><a href="mailto:admin@e-hosting.com.my">admin@e-hosting.com.my</a></td>
<td>Nikhost Technology</td>
<td>Private sector</td>
</tr>
<tr>
<td>19</td>
<td>Torbjörn Eklöv</td>
<td><a href="mailto:torbjorn.eklov@interlan.se">torbjorn.eklov@interlan.se</a></td>
<td>Interlan Gefle AB</td>
<td>Private sector</td>
</tr>
<tr>
<td>20</td>
<td>Backbone Technologies</td>
<td><a href="mailto:support@backbone.com.my">support@backbone.com.my</a></td>
<td>Backbone Technologies</td>
<td>Private sector</td>
</tr>
</tbody>
</table>
myDNSSEC Public Trial (Way Forward)
### myDNSSEC Public Trial

<table>
<thead>
<tr>
<th>Objective</th>
<th>To continue:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Raise awareness on DNSSEC technology</td>
</tr>
<tr>
<td></td>
<td>• Anticipate potential deployment issues</td>
</tr>
<tr>
<td></td>
<td>• Form “Best-Practices” Policies, especially with regards to Key Management</td>
</tr>
<tr>
<td></td>
<td>• Gather feedback from participants for improvement of .my DOMAIN REGISTRY DNSSEC-enabled Registry System</td>
</tr>
<tr>
<td></td>
<td>• Create and sustain deeper cooperation with operators of authoritative DNS server and operators of cache DNS server</td>
</tr>
<tr>
<td>Duration</td>
<td>Q1 2010 – Q2 2010 (est. 6 months)</td>
</tr>
</tbody>
</table>
myDNSSEC Public Trial (cont...)

1.0 Key Generator

- KEYS.db file
- USB Key Storage
- Keys Generation
- Secure Terminal
- Secure Tunnel
- USB Key Generator
- Signer
myDNSSEC Public Trial (cont...)

2.0 Zone Generator

- .my DOMAIN REGISTRY Database
- Valid Domain Name
- Zone Generator
- Valid Plain Zone file
- Signer
myDNSSEC Public Trial (cont...)

3.0 DSSET File Generator

- Child’s Keys Retrieval
- .my DOMAIN REGISTRY Database
- DSKey.db processor
- Valid Child’s DSKey (DSKey.db file)
- Signer
myDNSSEC Public Trial (cont...)

4.0 Signing

1.0
Valid KEYS.db file
(From Key Generator)

2.0
Valid Plain Zone file
(From Zone Generator)

3.0
Valid DSKey.db file
(From Zone Generator)

Signer

Error Checking +
Sign Zone

Signed Zone
Key Management Policies

• DNSSEC Operational Practices (RFC4641 [9]), advises to replace KSK’s once a year, and ZSK’s once a month.
• However, it is up to each organization to decide how long should the key lifespan be.
• Others ccTLDs key management policies !!!
## Key Management Policies Comparison (ZSK)

<table>
<thead>
<tr>
<th>CCTLD / Organization</th>
<th>Key Size (bits)</th>
<th>Algorithm</th>
<th>Scheme</th>
<th>Period (month)</th>
<th>Rollover (time/year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIPE NCC</td>
<td>1200</td>
<td>RSA/SHA1</td>
<td>Double Signature</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>ARIN</td>
<td>1024</td>
<td>RSA/SHA1</td>
<td>Pre-publish</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>.br</td>
<td>1024</td>
<td>RSA/SHA1</td>
<td>Pre-publish</td>
<td>3++</td>
<td>4</td>
</tr>
<tr>
<td>.se</td>
<td>1024</td>
<td>RSA/SHA1</td>
<td>Pre-publish</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>.cz</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>.pr</td>
<td>NA</td>
<td>RSA/SHA1</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>.bg</td>
<td>NA</td>
<td>RSA/SHA1</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>.th</td>
<td>1024</td>
<td>RSA/SHA1</td>
<td>NA</td>
<td>2</td>
<td>6</td>
</tr>
</tbody>
</table>

NA – Not available in related web site
### Key Management Policies Comparison (KSK)

<table>
<thead>
<tr>
<th>CCTLD / Organization</th>
<th>Key Size (bits)</th>
<th>Algorithm</th>
<th>Scheme</th>
<th>Period (month)</th>
<th>Rollover (time/year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIPE NCC</td>
<td>2048</td>
<td>RSA/SHA1</td>
<td>Pre-publish</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>ARIN</td>
<td>2048</td>
<td>RSA/SHA1</td>
<td>Double Signature</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>.br</td>
<td>1280</td>
<td>RSA/SHA1</td>
<td>Double Signature</td>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td>.se</td>
<td>2048</td>
<td>RSA/SHA1</td>
<td>Double Signature</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>.cz</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>.pr</td>
<td>NA</td>
<td>RSA/SHA1</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>.bg</td>
<td>NA</td>
<td>RSA/SHA1</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>.th</td>
<td>2048</td>
<td>RSA/SHA1</td>
<td>NA</td>
<td>12</td>
<td>1</td>
</tr>
</tbody>
</table>
Proposed key policy for .my

### ZSK

<table>
<thead>
<tr>
<th>Key Size (bits)</th>
<th>Algorithm</th>
<th>Scheme</th>
<th>Period (month)</th>
<th>Rollover (time/year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1024</td>
<td>RSA/SHA1</td>
<td>Pre-publish</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

### KSK

<table>
<thead>
<tr>
<th>Key Size (bits)</th>
<th>Algorithm</th>
<th>Scheme</th>
<th>Period (month)</th>
<th>Rollover (time/year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2048</td>
<td>RSA/SHA1</td>
<td>Double Signature</td>
<td>12</td>
<td>1</td>
</tr>
</tbody>
</table>

Note: Subject to further consultation and discussions with our regulator and relevant stakeholders
myDNSSEC Public Trial (cont...)

Improvement to current .my Registry System (related modules)
Conclusion

• .my strives for the production of DNSSEC (Q4, Oct 2010) with full commitment from operators of authoritative DNS server & cache DNS server

• As DNS forms a hierarchical structure stretched from the root, it is demanded that DNSSEC be introduced into all the layers of DNS from the highest layer of root DNS to DNS at the TLD level and DNS server for each domain name

• Validation of DNS responses in DNSSEC is done by cache DNS servers administered in ISPs, universities and companies
Conclusion (cont...)

• .my will continually build deeper cooperation with domestic ISPs and develop activities such as providing information on DNSSEC operation through seminars and media.

• It is important for the users to be aware of DNSSEC and whether he/she is in the environment that supports DNSSEC or not.
You are welcome to join our myDNSSEC public trial
Thank you

Norsuzana Harun
Manager Technology and Innovation Dept.
tni@domainregistry.my
http://rnd.domainregistry.my