DOMAIN REGISTRY

Internet Identity For All

myDNSSEC Project Update

Norsuzana Harun

28th October 2009

Agenda

1. Current Status
2. What's Next?
3. Proposed Key Management
4. Result of Zone Signing (Test)
5. Looking Forward

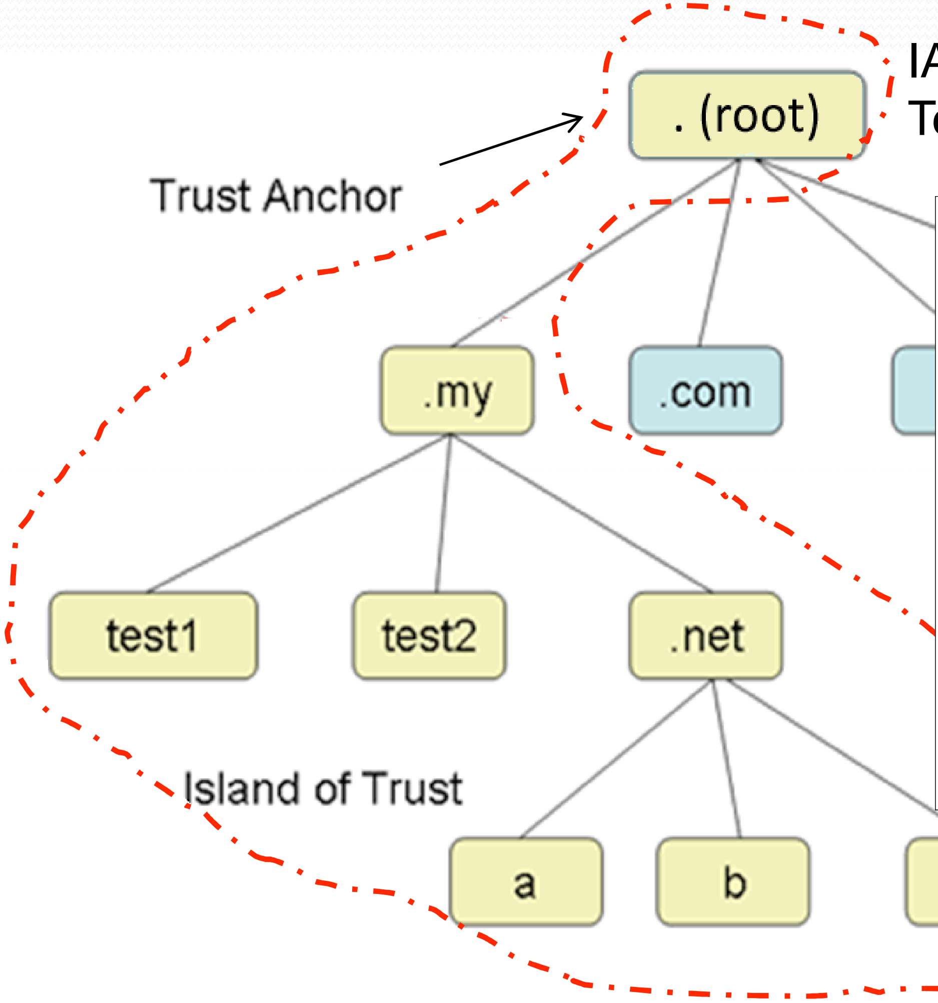
myDNSSEC Current Status

Closed Testbed (http://www.dnssec.my)	
Duration	31st March – 31st October 2009
Zones	.my .net.my
IANA DNSSEC Testbed	Joined since 23rd May 2009
Note	•First phase of implementation of myDNSSEC Project •Separated system from .my registry system •Only available for invited participants

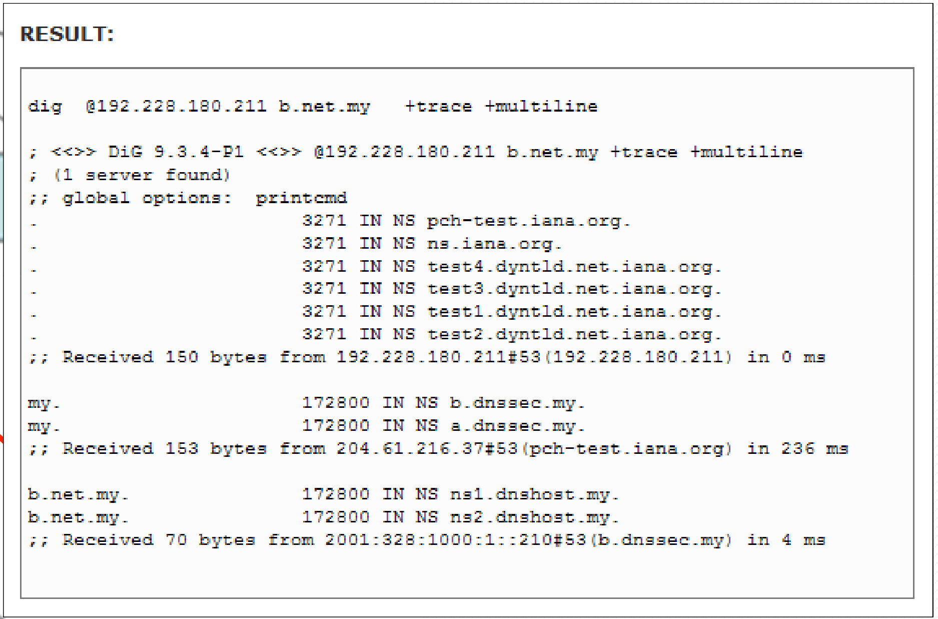
myDNSSEC Testbed Objective

- Raise awareness on DNSSEC technology
- Anticipate potential deployment issues
- Form “Best-Practices” Policies, especially with regards to Key Management
- Gather feedback from participants for improvement of .my DOMAIN REGISTRY DNSSEC-enabled Registry System
- Create and sustain deeper cooperation with operators of authoritative DNS server and cache DNS server

myDNSSEC Closed Testbed Hierarchy



IANA DNSSEC
Test Bed root server



RESULT:

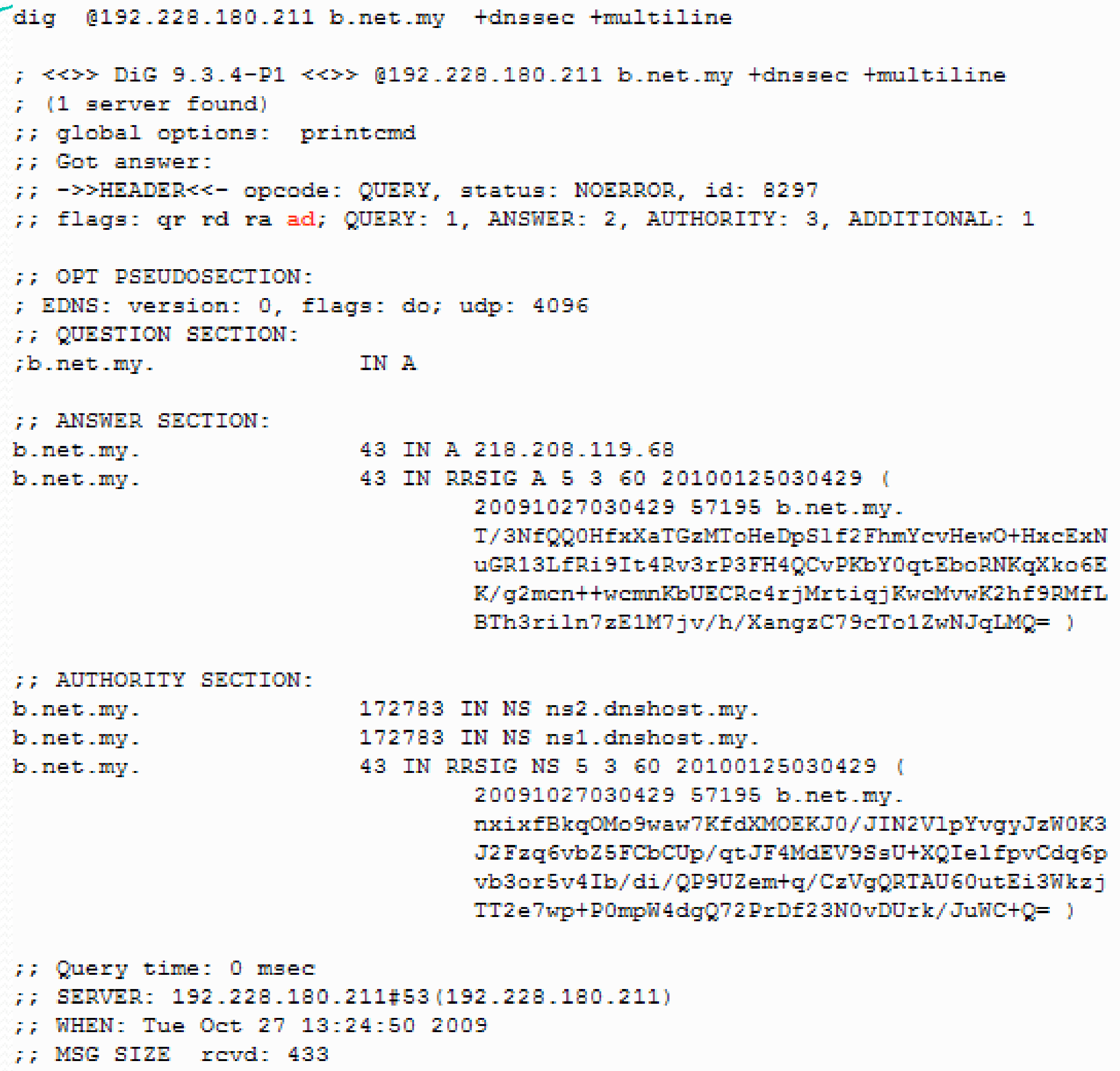
```
dig  @192.228.180.211 b.net.my   +trace +multiline

; <<>> DiG 9.3.4-P1 <<>> @192.228.180.211 b.net.my +trace +multiline
; (1 server found)
;; global options:  printcmd
.                       3271 IN NS pch-test.iana.org.
.                       3271 IN NS ns.iana.org.
.                       3271 IN NS test4.dyntld.net.iana.org.
.                       3271 IN NS test3.dyntld.net.iana.org.
.                       3271 IN NS test1.dyntld.net.iana.org.
.                       3271 IN NS test2.dyntld.net.iana.org.
;; Received 150 bytes from 192.228.180.211#53(192.228.180.211) in 0 ms

my.                     172800 IN NS b.dnssec.my.
my.                     172800 IN NS a.dnssec.my.
;; Received 153 bytes from 204.61.216.37#53(pch-test.iana.org) in 236 ms

b.net.my.               172800 IN NS ns1.dnshost.my.
b.net.my.               172800 IN NS ns2.dnshost.my.
;; Received 70 bytes from 2001:328:1000:1::210#53(b.dnssec.my) in 4 ms
```

Dig result for b.net.my



```
dig  @192.228.180.211 b.net.my  +dnssec +multiline

; <<>> DiG 9.3.4-P1 <<>> @192.228.180.211 b.net.my +dnssec +multiline
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8297
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;b.net.my.               IN A

;; ANSWER SECTION:
b.net.my.               43 IN A 218.208.119.68
b.net.my.               43 IN RRSIG A 5 3 60 20100125030429 (
                                20091027030429 57195 b.net.my.
                                T/3NfQQ0HfxXaTGzMToHeDpSlf2FhmYcvHewO+HxcExN
                                uGR13LfRi9It4Rv3rP3FH4QCvPKbY0qtEboRNKgXko6E
                                K/g2mcn++wcmnKbUECRc4rjMrtiqjKwcMvwK2hf9RMfL
                                BTh3riln7zE1M7jv/h/XangzC79cTo1ZwNJqLMQ= )

;; AUTHORITY SECTION:
b.net.my.               172783 IN NS ns2.dnshost.my.
b.net.my.               172783 IN NS ns1.dnshost.my.
b.net.my.               43 IN RRSIG NS 5 3 60 20100125030429 (
                                20091027030429 57195 b.net.my.
                                nxixfBkqOMo9waw7KfdXMOEKJ0/JIN2VlpYvgyJzW0K3
                                J2Fzq6vbZ5FCbCUp/qtJF4MdEV9SsU+XQIelfpvCdq6p
                                vb3or5v4Ib/di/QP9UZem+q/CzVgQRTAU60utEi3Wkzj
                                TT2e7wp+P0mpW4dgQ72PrDf23N0vDUrk/JuWC+Q= )

;; Query time: 0 msec
;; SERVER: 192.228.180.211#53(192.228.180.211)
;; WHEN: Tue Oct 27 13:24:50 2009
;; MSG SIZE  rcvd: 433
```

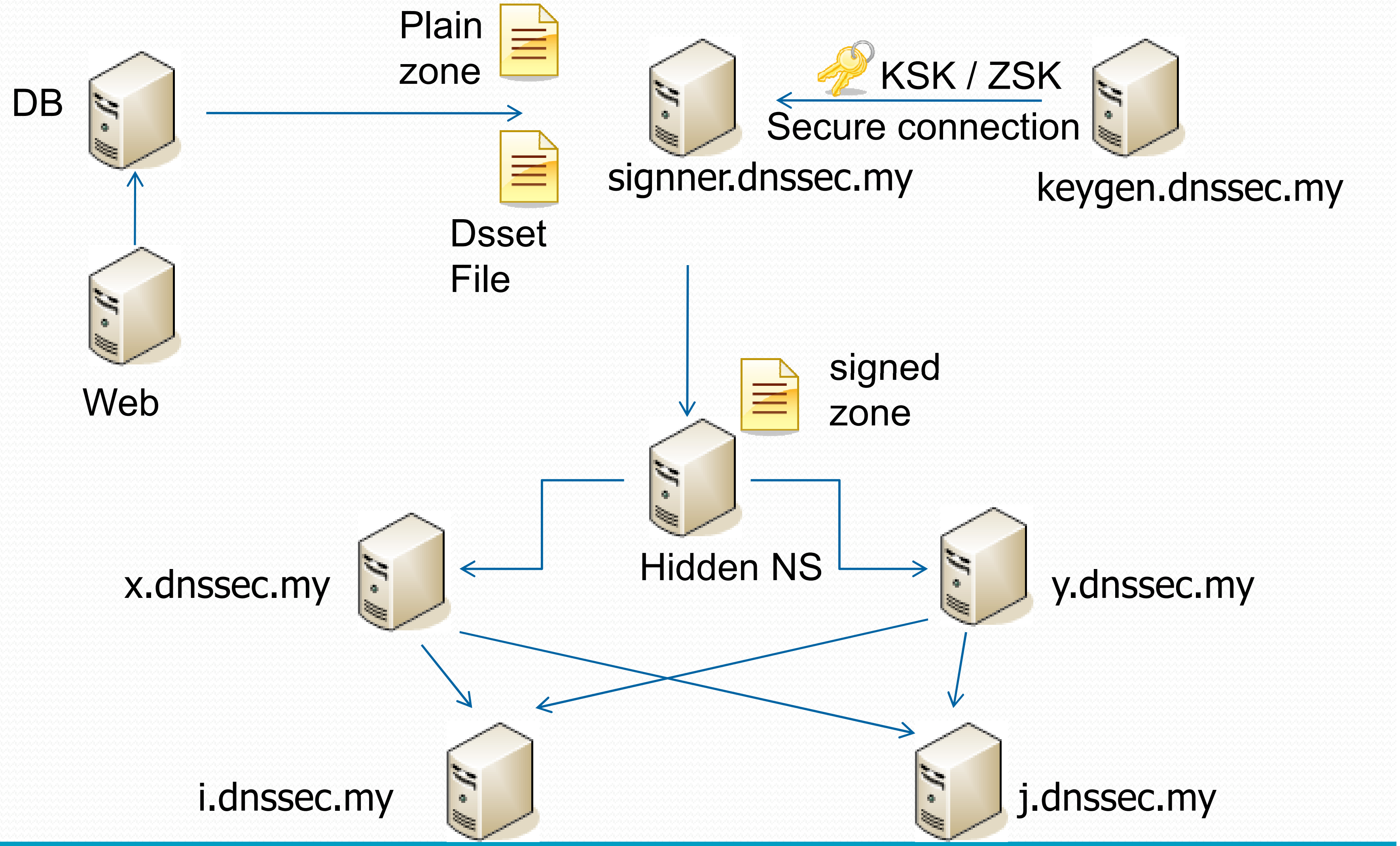
myDNSSEC Closed Testbed Report (15th Oct 09)

Participants Categories	Total Participants	Total Domain Registered
.my Resellers	1	0
Academic	1	1
APTLD Member	7 (Korea, Mongolia, China, Singapore, Hong Kong, Sweden, Austria)	4
Government agency	4	2
Internet Service Provider (ISP)	2	1
Non-profit organization (NPO)	2	0
Others	1	0
Private sector	5	5
Statutory Body	1	0
TOTAL:	**24**	**14**

What's Next?

	Closed Testbed	Public Testbed ☑
Duration	31st March – 31st October 2009	Expected launch date : December, 2009
Zones	.my .net.my	All zones
IANA Testbed	Joined since 23rd May 2009	Will continue participation
Note	•First phase of myDNSSEC implementation plan •Separated system from .my registry system •Only available for invited participants	•Second phase of myDNSSEC implementation plan •Adopt .my registry system and process flow •Open for all users or public to test

What’s Next? : Public Trial Arch.



Proposed Key Management

	Closed Testbed	Public Trial (and eventually Production)
Key Type	KSK , ZSK	KSK , ZSK
Key Algorithm	RSA-SHA1/ RSA-SHA256	RSA-SHA1/ RSA-SHA256
Key Length (KSK)	2048 bits	2048 bits
Key Length (ZSK)	1024 bits	1024 bits
Key Generation Tools	Bind Command	ZKT
Signing Tools	Bind Command	ZKT
Zones	.my and .net.my	All zones

Proposed Key Management (cont…)

ZSK

Key Size (bits)	Algorithm	Scheme	Period (month)	Rollover (time/year)
1024	RSA/SHA1	Pre-publish	3	4

KSK

Key Size (bits)	Algorithm	Scheme	Period (month)	Rollover (time/year)
2048	RSA/SHA1	Double Signature	12	1

Note: Subject to further consultation and discussions with our regulator and relevant stakeholders

Result of Zone Signing (Test)

	NSEC, RSASHA1					
	Size Before(Bytes)	Size After(Bytes)	Different (Kb)	Time Taken	No of Domain	Domain Signed
.my	1030900	6852120	**5684.79**	45s	16957	5
.com.my	3942355	26525365	**22053.72**	2m36s	63582	5
.net.my	125355	842001	**699.85**	5s	1990	5
.org.my	124926	848674	**706.79**	5s	2037	5
.gov.my	87451	532056	**434.18**	3s	1206	5
.edu.my	96101	606213	**498.16**	3s	1401	5
.mil.my	967	6313	**5.22**	< 1s	5	5
.name.my	51736	227021	**171.18**	2s	450	5

Note: Zone File size increase around 6 times

Result of Zone Signing (Test)

	NSEC3,RSASHA1					
	Size Before(Bytes)	**Size After(Bytes)**	**Different (Kb)**	**Time Taken**	**No of Domain**	**Domain Signed**
.my	1030900	6852210	**5684.87**	43s	16957	5
.com.my	3942355	26525482	**22053.83**	2m34s	63582	5
.net.my	125355	842088	**699.93**	5s	1990	5
.org.my	124926	848796	**706.90**	5s	2037	5
.gov.my	87451	532118	**434.25**	3s	1206	5
.edu.my	96101	606234	**498.18**	4s	1401	5
.mil.my	967	6328	**5.24**	< 1s	5	5
.name.my	51736	227073	**171.23**	2s	450	5

Note: Zone File size increase around 6 times

Looking Forward

More focus on:

1) Size of signed zone file (further analysis)
2) Automated child's key retrieval process
3) Key management (i.e. key size, validity period and rollover) analysis
4) Zone Time To Live (TTL)
5) Larger response size (> 512 bytes) and firewall limitation
6) Current bandwidth consumption and enhancement require if any
7) Impact of signed root zone to .my's ccTLD and downwards in the DNS hierarchy
8) Awareness and participation of authoritative and cache DNS server administrators
9) **myDNSSEC production: expected Q4 2010**

Thank You!

tni@domainregistry.my
http://rnd.domainregistry.my