



**.my DOMAIN REGISTRY**

**myDNSSEC**

**Technology And Innovation (TNI) Dept.**

**Norsuzana Harun**

**21<sup>st</sup> Aug 2009**

# myDNSSEC Implementation Plan

## Phase 1

- Closed Test-bed (31<sup>st</sup> March – 31<sup>st</sup> October 2009)

## Phase 2

- Public Trial (Q1 2010 – Q2 2010)

## Phase 3

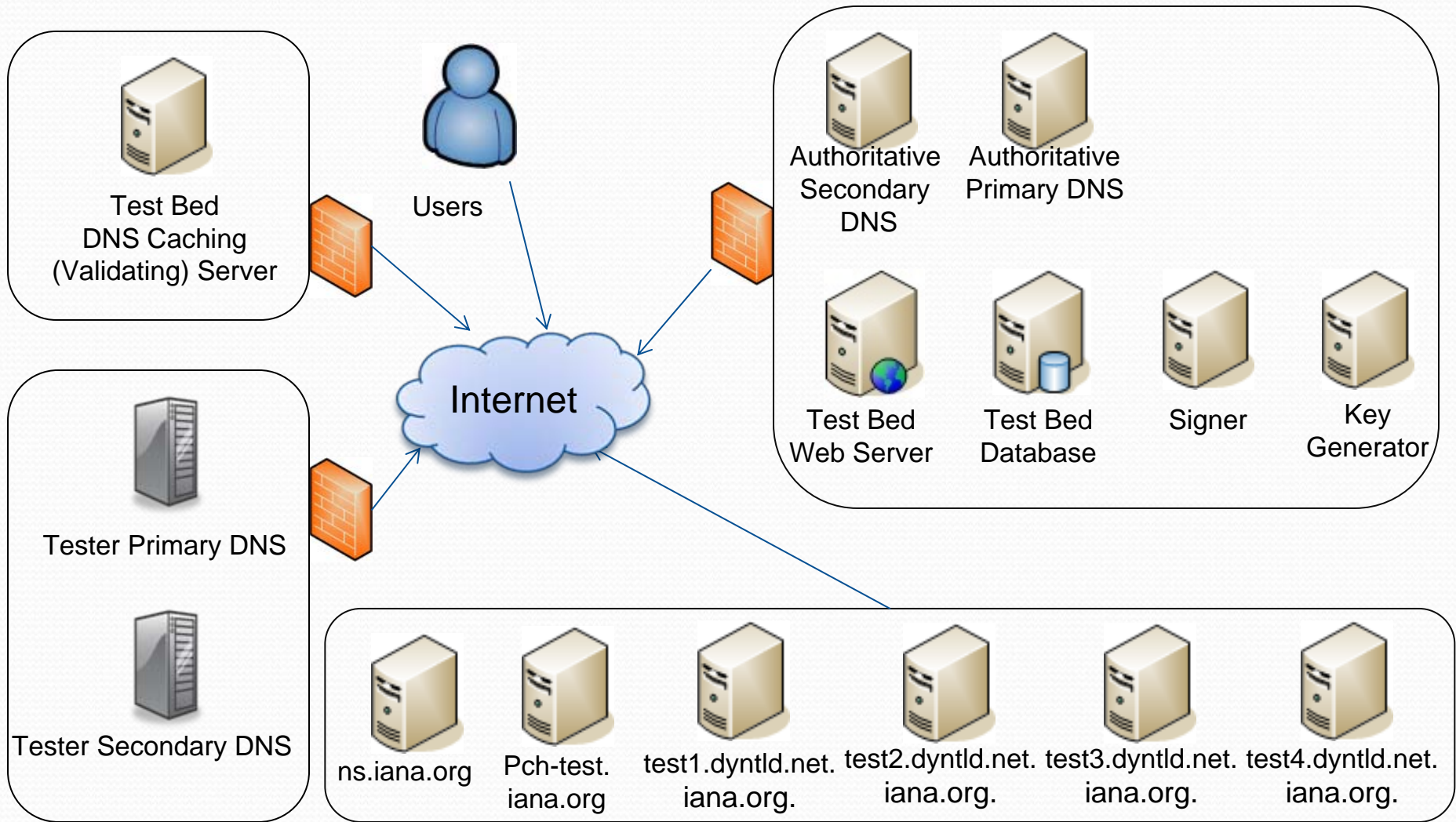
- Production (Q4, Oct 2010)

# myDNSSEC Closed Test-bed

# myDNSSEC Closed Test-bed

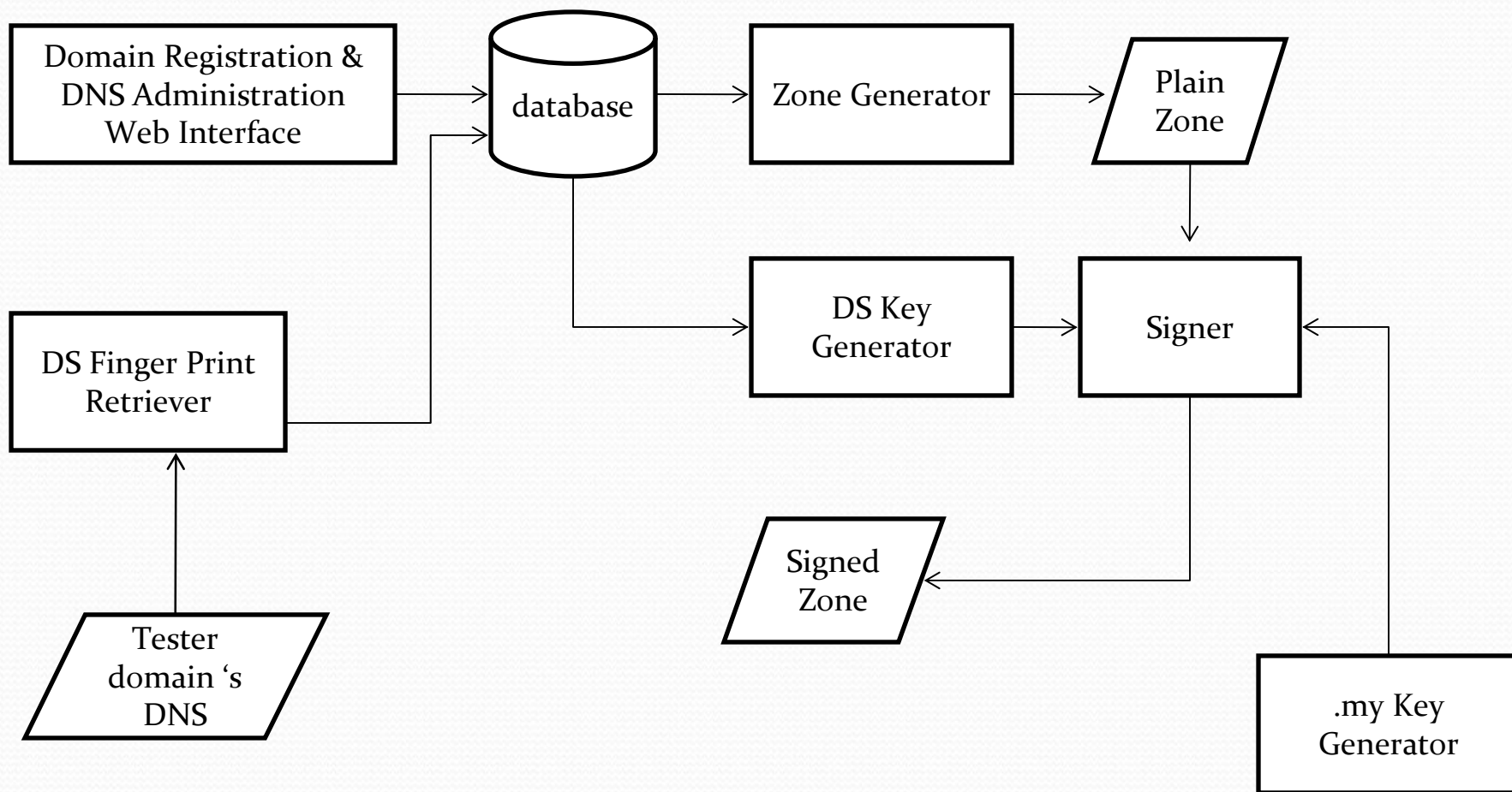
Objective	<ul style="list-style-type: none"> <li>• Raise awareness on DNSSEC technology</li> <li>• Anticipate potential deployment issues</li> <li>• Form “Best-Practices” Policies, especially with regards to Key Management</li> <li>• Gather feedback from participants for improvement of .my DOMAIN REGISTRY DNSSEC-enabled Registry System</li> </ul>
Duration	31 <sup>st</sup> March – 31 <sup>st</sup> October 2009
Zones	.my .net.my
IANA Test-bed	Joined since 23 <sup>rd</sup> May 2009

# myDNSSEC Closed Test-bed (cont...)



# myDNSSEC Closed Test-bed (cont...)

## Zone signing process

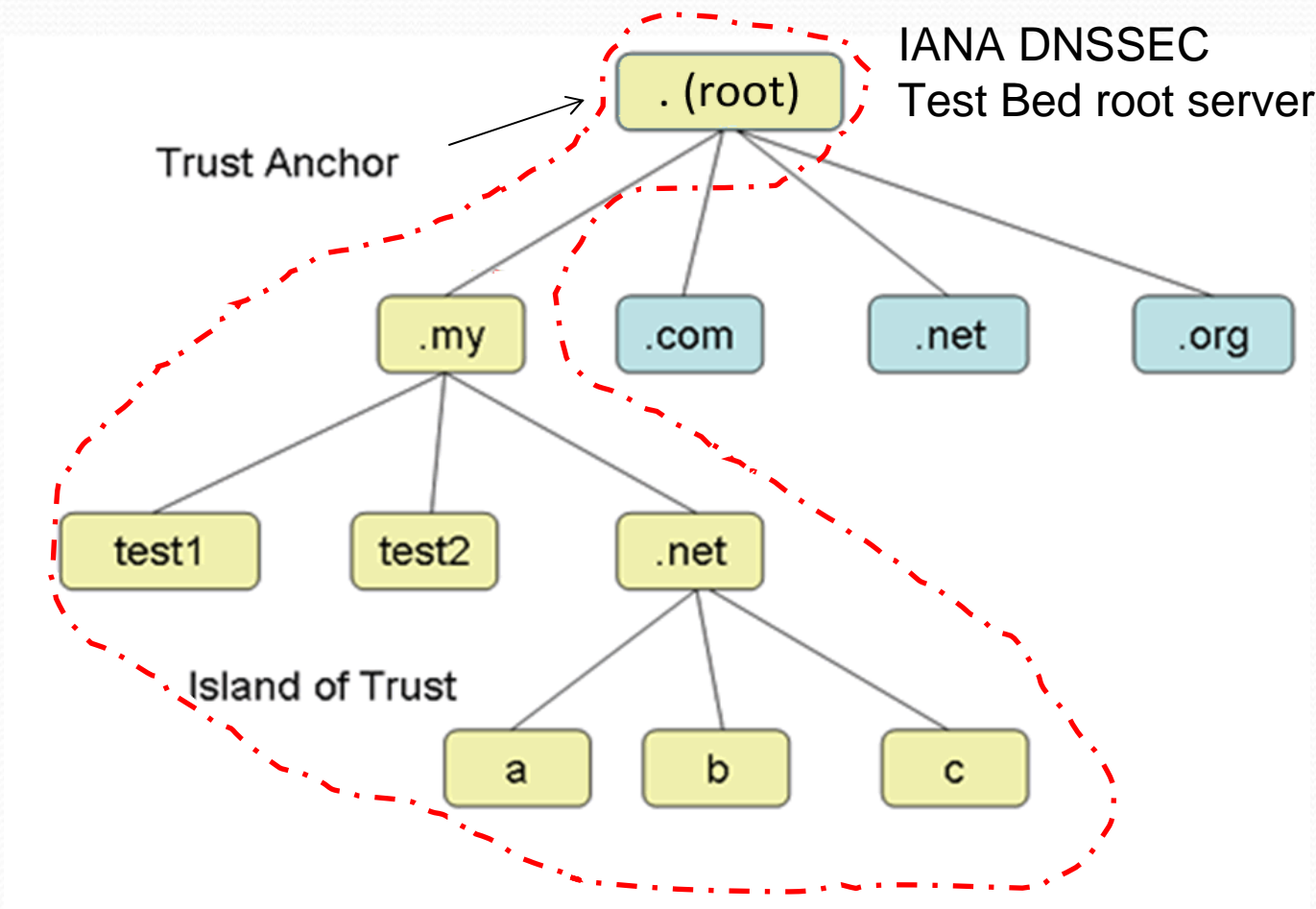


# myDNSSEC Closed Test-bed (cont...)

## 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...)



# 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 @192.228.180.211 b.net.my soa +dnssec +multiline

; <<>> DiG 9.3.4-P1 <<>> @192.228.180.211 b.net.my soa +dnssec +multiline
; (1 server found)
;; global options:      printcmd
;; 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.                IN SOA

;; ANSWER SECTION:
b.net.my.                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)
                        )
b.net.my.                41 IN RRSIG SOA 5 3 60 20091025013130 (
                        20090727013130 6468 b.net.my.
                        OIG2+ulpuEUQ/4vcFy3wHfSF3bNNodoMkKukgu1T6nfP
                        O+Lw7csFhgAJyWeH7fYgUvnZj7KGcpuX665UBh2kgIMA
                        gJ9dJJiex6OCYkKV0nQUxVWEakkUzKEknJLXzTObtpkw
                        1v03nKy8ynDwRRXQqk2IWS0DSJN7vFkdLA8ipoE= )

;; AUTHORITY SECTION:
b.net.my.                115438 IN NS ns2.dnshost.my.
b.net.my.                115438 IN NS ns1.dnshost.my.
b.net.my.                41 IN RRSIG NS 5 3 60 20091025013130 (
                        20090727013130 6468 b.net.my.
                        WQdeMzQDtjzCcWoJY99PtUMpQyo0d65bG1qDDb0XHPLM
                        VBwfSC9nNSfXzvezZhGYjaabFabg1ByTVKNzhe1YrFIL
                        6a6psTsmH43w27Ibbk6CRdqhj3jzx2pNCGO004AN8/A7
                        E4PtWoJUqtxacED2nMPG9KvfjaI/pCf/rdHXj8Y= )
```

# myDNSSEC Closed Test-bed (cont...)

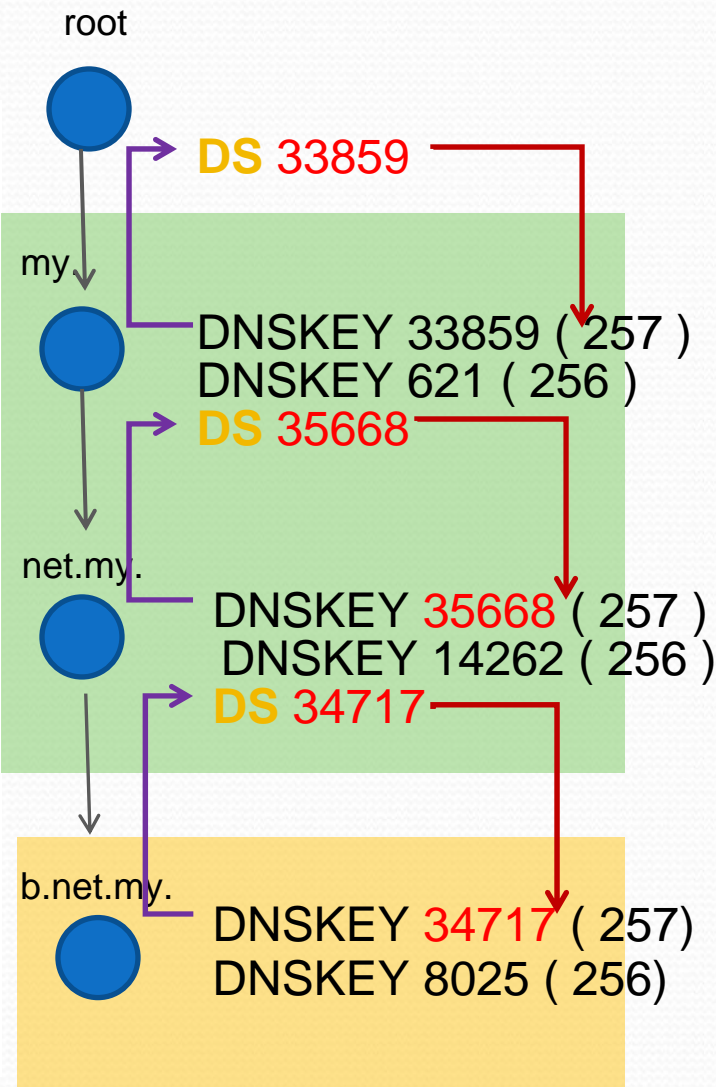
Chain of trust tree from root and your domain name:

```
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
```



# myDNSSEC Closed Test-bed (cont...)

Awareness  
Seminar /  
Training

## Target

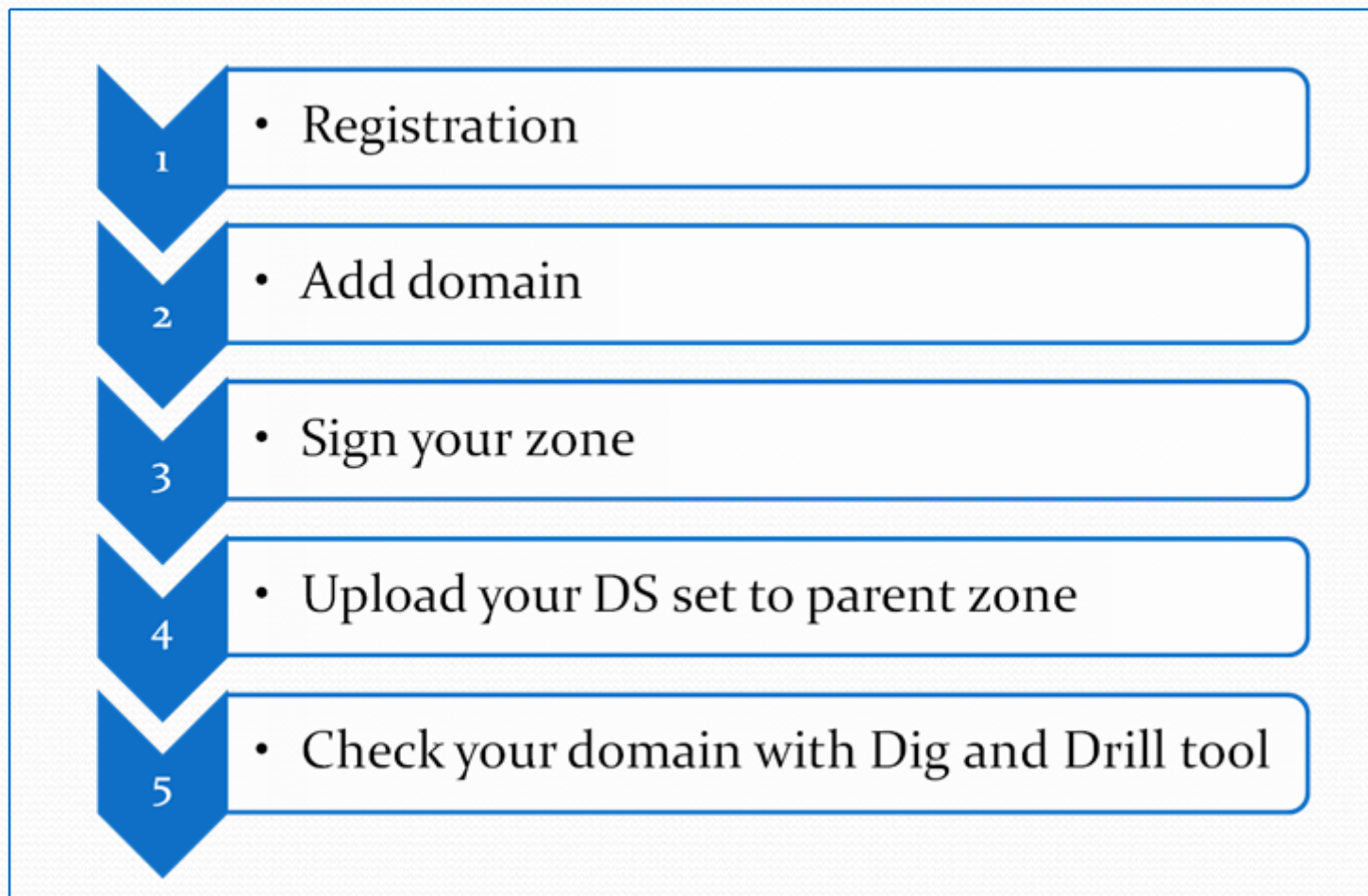
Operators of authoritative DNS server  
Operators of cache DNS server

## 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> ]

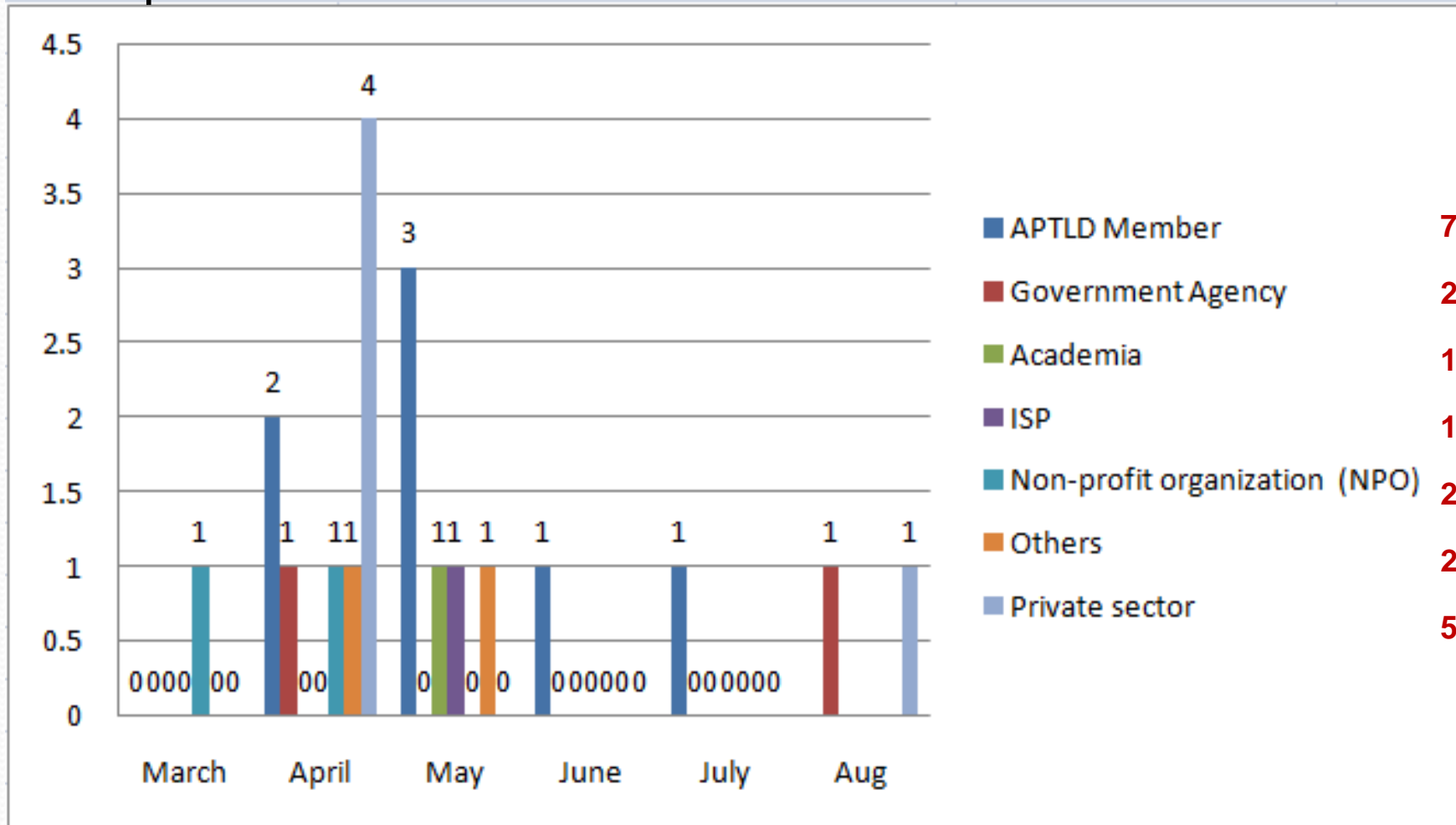


## myDNSSEC Closed Test-bed (cont...)

Participant Statistic (by invitation)	20 participants (as of 19 Aug 09) <ul style="list-style-type: none"><li>• 7 ccTLD : Korea, Mongolia, China, Singapore, Hong Kong, Sweden, Austria</li></ul>
---------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------

# myDNSSEC Closed Test-bed (cont...)

## Participant Statistic



# myDNSSEC Closed Test-bed (cont...)

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

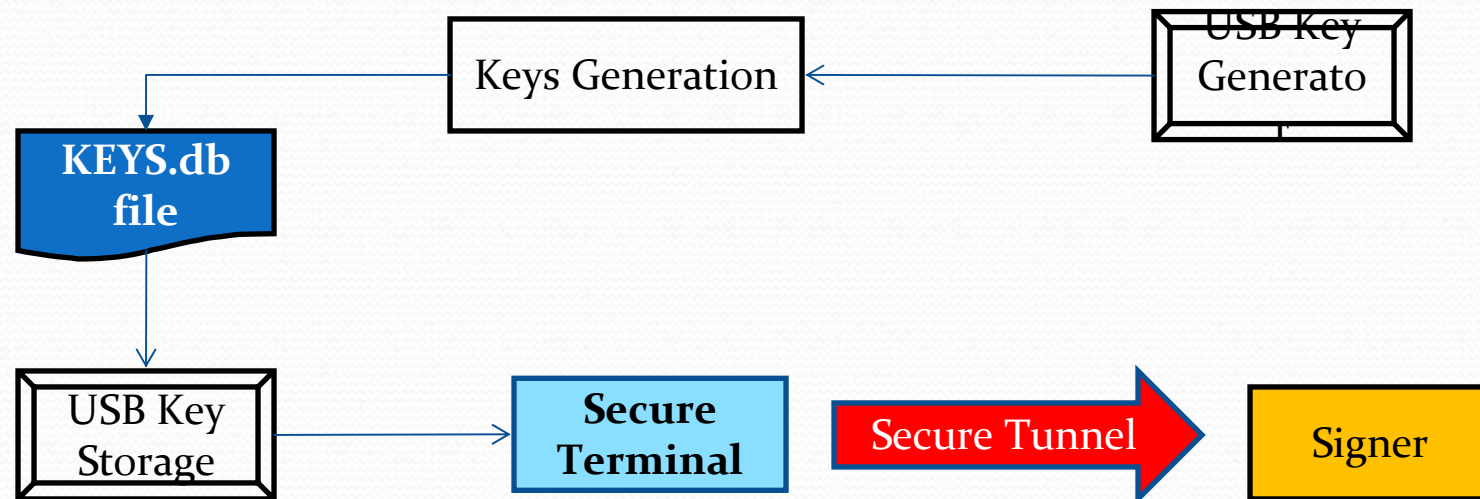
# myDNSSEC Public Trial (Way Forward)

# myDNSSEC Public Trial

Objective	<p>To continue:</p> <ul style="list-style-type: none"> <li>• Raise awareness on DNSSEC technology</li> <li>• Anticipate potential deployment issues</li> <li>• Form “Best-Practices” Policies, especially with regards to Key Management</li> <li>• Gather feedback from participants for improvement of .my DOMAIN REGISTRY DNSSEC-enabled Registry System</li> <li>• <b>Create and sustain deeper cooperation with operators of authoritative DNS server and operators of cache DNS server</b></li> </ul>
Duration	Q1 2010 – Q2 2010 (est. 6 months)
Zones	<p>.my          .net.my .com.my .gov.my .edu.my .org.my .mil.my .name.m          y</p>

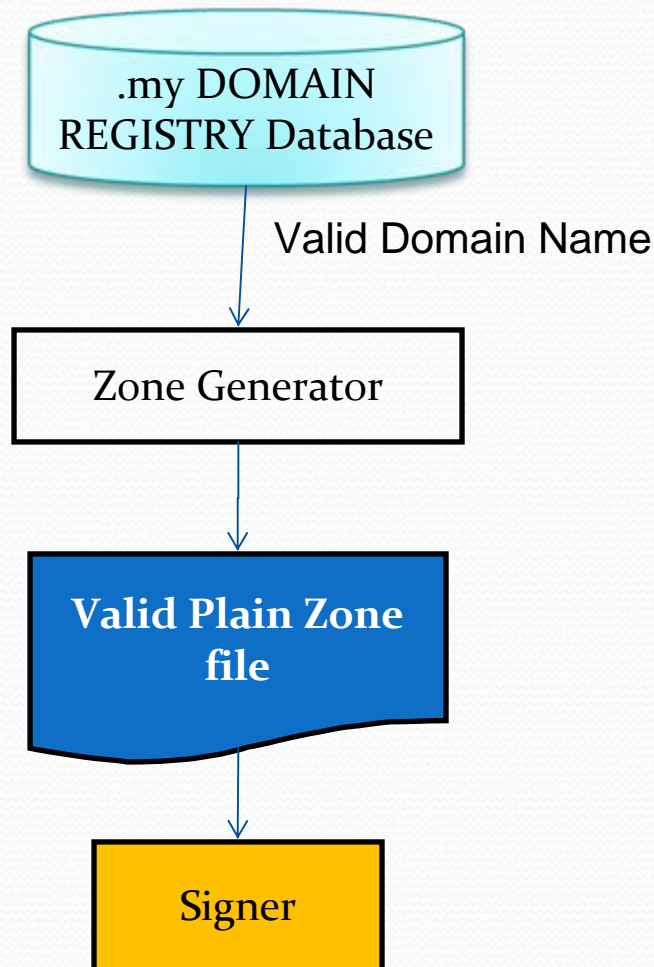
# myDNSSEC Public Trial (cont...)

## 1.0 Key Generator



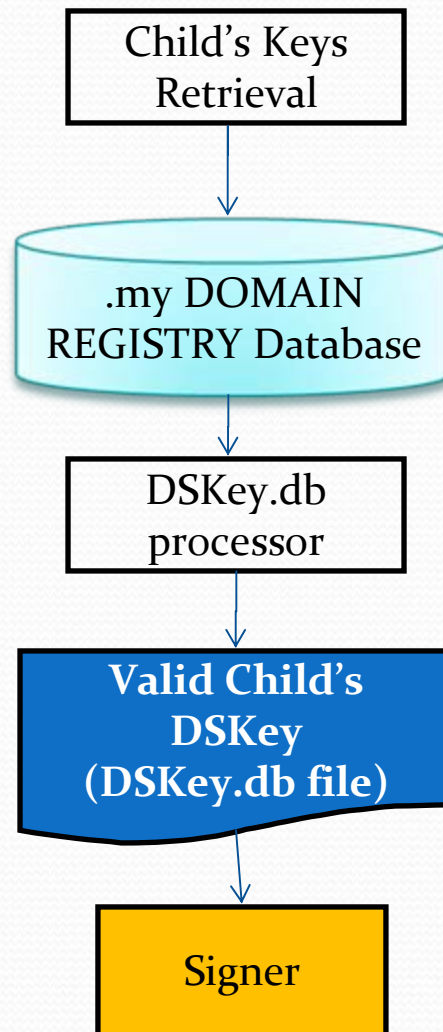
# myDNSSEC Public Trial (cont...)

## 2.0 Zone Generator



# myDNSSEC Public Trial (cont...)

## 3.0 DSSET File Generator



# myDNSSEC Public Trial (cont...)

## 4.0 Signing

1.0

2.0

3.0

Valid KEYS.db file  
(From Key Generator)

Valid Plain Zone file  
(From Zone Generator)

Valid DSKey.db file  
(From Zone Generator)

Signer

Error Checking +  
Sign Zone

Signed  
Zone

# myDNSSEC Public Trial (cont...)

## 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 !!!

# myDNSSEC Public Trial (cont...)

## Key Management Policies Comparison (ZSK)

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

NA – Not available in related web site

# myDNSSEC Public Trial (cont...)

## Key Management Policies Comparison (KSK)

CCTLD / Organization	Key Size (bits)	Algorithm	Scheme	Period (month)	Rollover (time/year)
RIPE NCC	2048	RSA/SHA1	Pre-publish	12	1
ARIN	2048	RSA/SHA1	Double Signature	12	1
.br	1280	RSA/SHA1	Double Signature	14	1
.se	2048	RSA/SHA1	Double Signature	12	1
.cz	NA	NA	NA	NA	NA
.pr	NA	RSA/SHA1	NA	NA	NA
.bg	NA	RSA/SHA1	NA	NA	NA
.th	2048	RSA/SHA1	NA	12	1

# Proposed key policy for .my

## ZSK

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

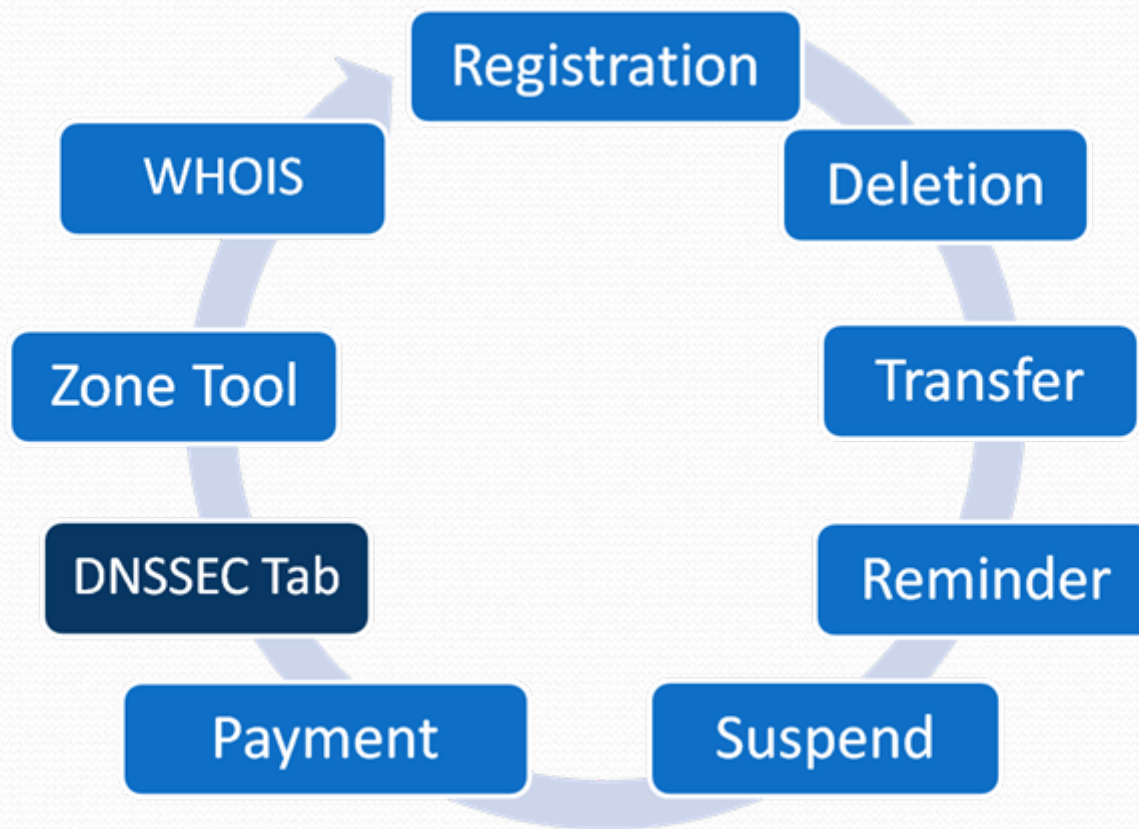
## KSK

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

# 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](mailto:tni@domainregistry.my)  
<http://rnd.domainregistry.my>