DNSSEC Plan in GO.KR

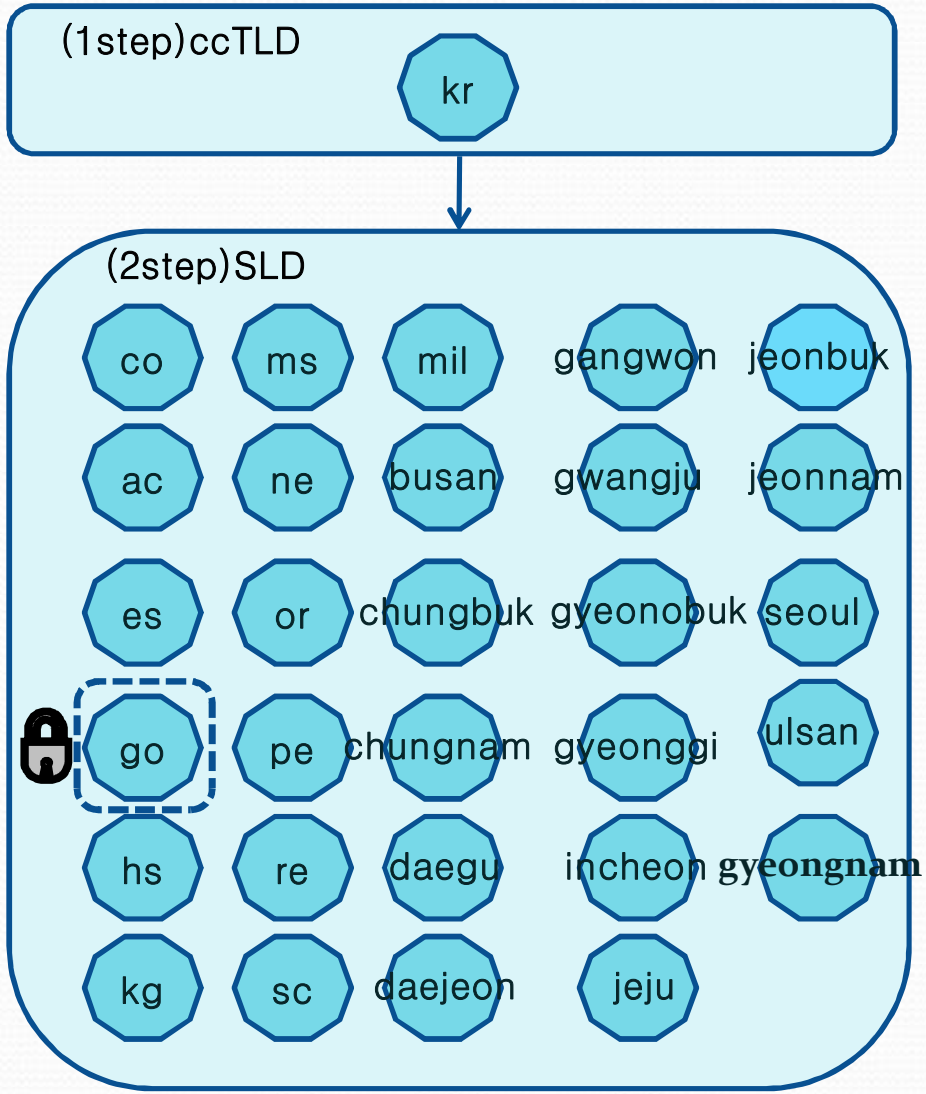
Myung Hee Choi
KISA/KRNIC
choimh@kisa.or.kr

Contests

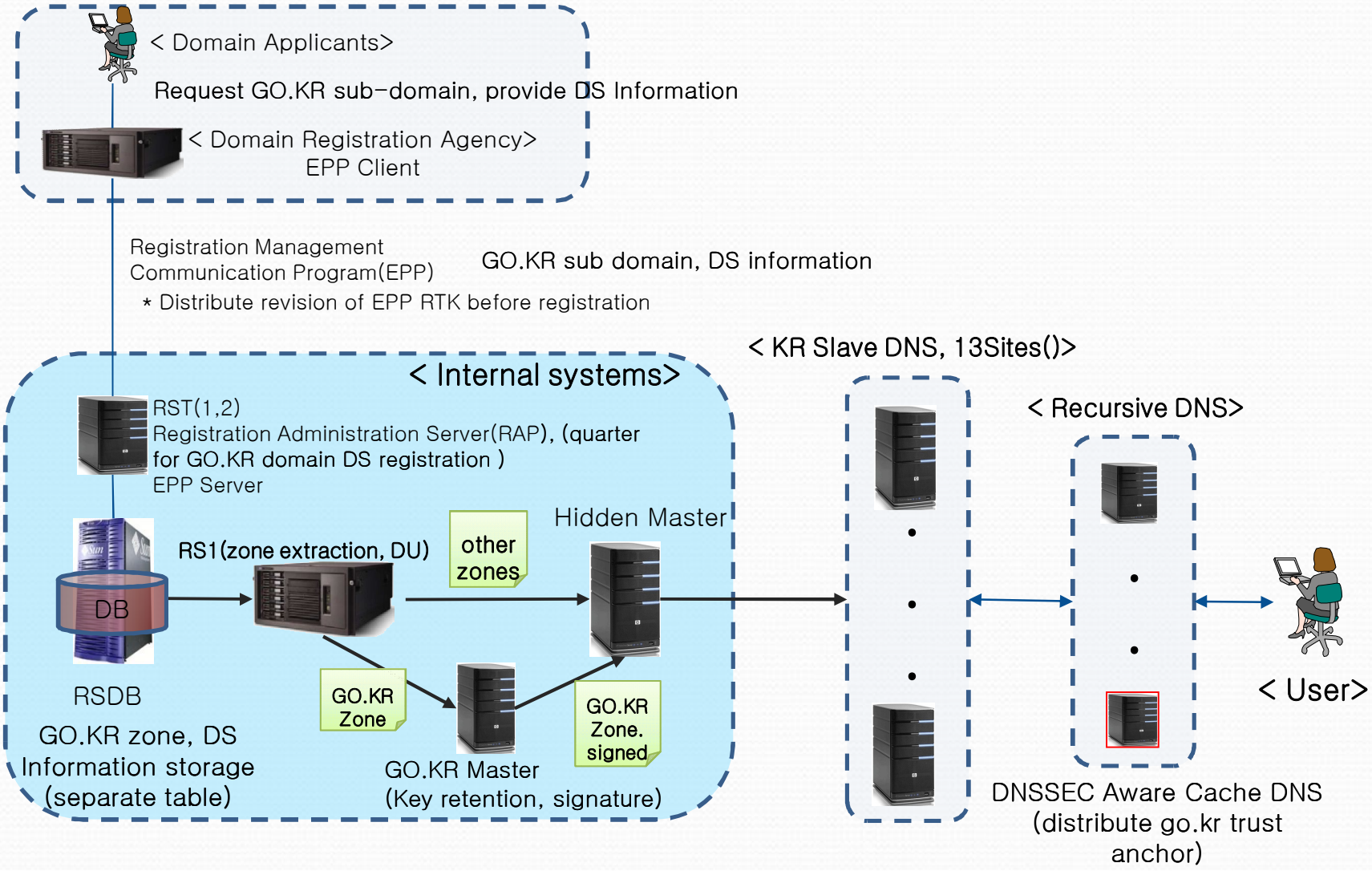
- DNSSEC Plan in GO.KR
- DNSSEC Test & Analysis
- Failure Preparation

Plan(.kr)

- Government agencies domain(go.kr) singing in 2010
- ".kr" signing in 2011 or later
- Side by side with new kr DNS deployment/ update



“go.kr” DNSSEC Plan(Overview)



“go.kr” DNSSEC Plan

- Equipment introduction : to invest go.kr DNSSEC servers
- Extract zone, signing, transfer(extract first zone)
  - DB -> RS1 -> GO.KR Master(signing) ->HM(Slave) -> KR DNS Slaves(13sites)
  - AXFR : except GO.KR zone, conducted in other zones existing
  - (GO.KR) Dynamic Update : 100 seconds, 200 per treatment
    - DB(change date) , RS1(ns-update), go.kr Master(reflected Dynamic Update)
    - Single record signing, after inserting the chain remodeling castle provided with BIND
    - Strengthening Monitoring of Dynamic Update

Key/Signature Policy(KASP)

- Algorithm : NSEX3RSASHA1
- NSEC3, OPT-OUT
- KSK(size : 2048bit, lifetime : 1year)
- ZSK(size : 1024bit, lifetime : 3month)
- Signature Validity : 1 month(resigning cycle)
- Cycle resigning support in BIND

Result of DNSSEC Test & Analysis

- Pre-analysis increased load depending on DNSSEC
- Increase server load and traffic load but, it's small size of go.kr zone and improvement H/W performance (No problem test result)
  - increase load(zone file size, zone transfer time and query/respond packet size etc)
  - Slightly increase load of sever resources(CPU, memory)
  - GO.KR vs. CO.KR

	GO.KR	CO.KR
Domain number	2203	582,316
Zone size	149KB	45MB(300times)

Test Environments

- Test target S/W : BIND-9.6.1
- Test system environments
  - Operation System : GNU/Linux
  - Processor : x.86_64
  - Hardware-Platform : x86_64
  - CPU : 2.93GHz * 16
  - Memory : 16GB

System Load Test Result

Item	Subsection	Numerical changes
Zone signature treat load	Zone file size	40MB → 206MB
	Signing time	4Min. 33sec.
	CPU utilization	6%
	Memory utilization	2.8%
AXFR	AXFR time	3sec. → 12sec
	CPU utilization	2% → 2%
	Memory utilization	0.9% → 2.5%
Operating system load (20,000 Query)	Query/Respond Time	0.899sec→ 1.5sec
	QPS	22,228 → 13,177
	CPU utilization	5% → 5%
	Memory utilization	2.5% → 2.5%
Dynamic update load(standard 500unit)	Time	14sec. → 15sec.
	CPU utilization	6% → 6%
	Memory utilization	0.9% → 2.5%

Server Load Test Result

Object	DS application rate	DS application number	Time	Processing scale
co.kr	Default Zone(DS RR X)		11 sec	
	10%	53984	1min 14sec	7 times
	20%	107968	2min 19sec	13 times
	30%	161952	3min 17sec	18 times
	40%	215936	4min 22sec	24 times
	50%	269920	5min 28sec	30 times
	60%	323903	6min40sec	36 times
	70%	377887	7min 46sec	42 times
	80%	431871	8min 34sec	47 times
	90%	485855	9min46sec	53 times
	100%	539839	10min 43sec	58 times
go .kr	Default Zone(DS RR X)		4sec	
	100%	2123	7sec	1.75 times

Traffic Load Analysis

- Traffic load test result
  - Root
    - Query 84byte→227byte
    - Response 118byte→1331byte
  - KR
    - Query 84byte →223byte
    - Response 118byte →1353byte
  - CO.KR
    - Query 84byte →244byte
    - Response 118byte →1376byte
  - Recursive server
    - Query 443byte→1525byte
    - Response 561byte →4797byte

Response Size(Byte)	Acceptability Size(Byte)	Handing
510	512 1024 2048 4096	(Only)answer Answer + Additional Answ. + Addi. + (some) Answ. + Addi. + RRSIG
1023	512 1024 2048 4096	Answ. + Addi. + RRSIG(TCP) (Only)Answer Answ. + Addi. + (some)RRSIG Answ. + Addi. + (some)RRSIG
2046	512 1024 2048 4096	Answ. + Addi. + RRSIG(TCP) Answ. + Addi. + RRSIG(TCP) (Only)Answer Answ. + Addi. + (some)RRSIG
4087	512 1024 2048 4096	Answ. + Addi. + RRSIG(TCP) Answ. + Addi. + RRSIG(TCP) Answ. + Addi. + RRSIG(TCP) (Only)Answer

Expected failures & Measures

- Failure of GO.KR Master : operating standby server(GO-SLV)
- Failure of Dynamic Update : inspection/action monitoring
- Compromise /Expired Key : checking rollover, perform an emergency rollover
- Maintenance emergency contact(system personnel)

Q & A

rays@kisa.or.kr

Thank you!!