DNSSEC Development in CNNIC

Prof. Xiaodong Lee

CEO, CNNIC

February 2015

中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

1、Review

2、What have we done in 2014?

3、Future

1、Review

CN

2013.11

DS in root

2013.10

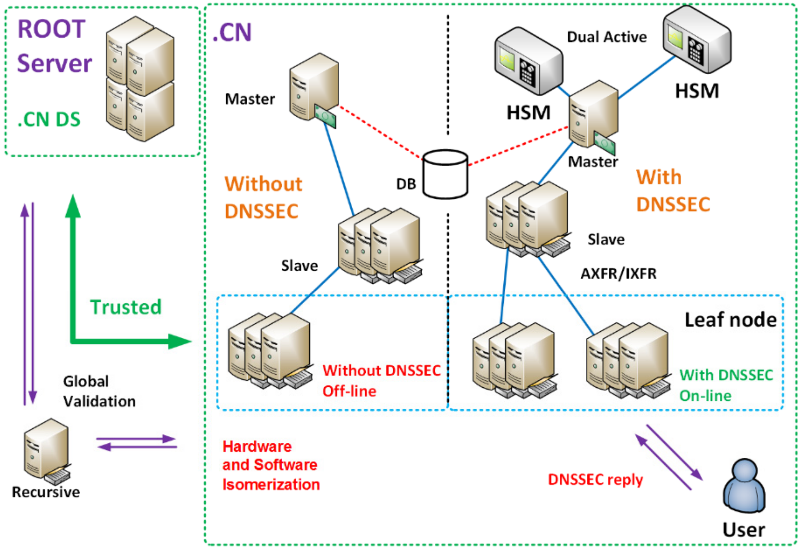
DNSSEC online

2013.06

Zone signed

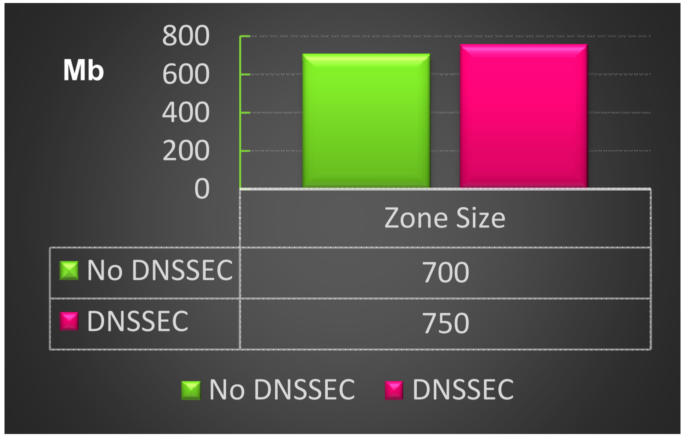
2013.05

Begin

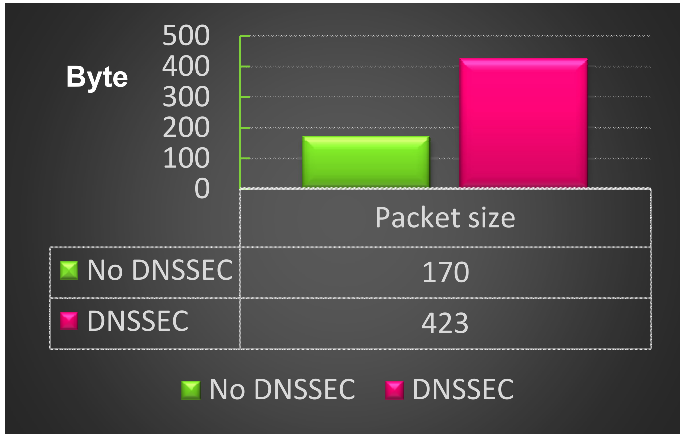


Observations

- **Zone Size**
  - Opt-out
  - **Increased a little (7%)**
- **Packet Size**
  - RRSIG
  - **2.5** times larger in average



	Zone Size
🟩 No DNSSEC	700
🟥 DNSSEC	750



	Packet size
🟩 No DNSSEC	170
🟥 DNSSEC	423

1、Review

CN

2013.11

DS in root

2013.10

DNSSEC online

2013.06

Zone signed

2013.05

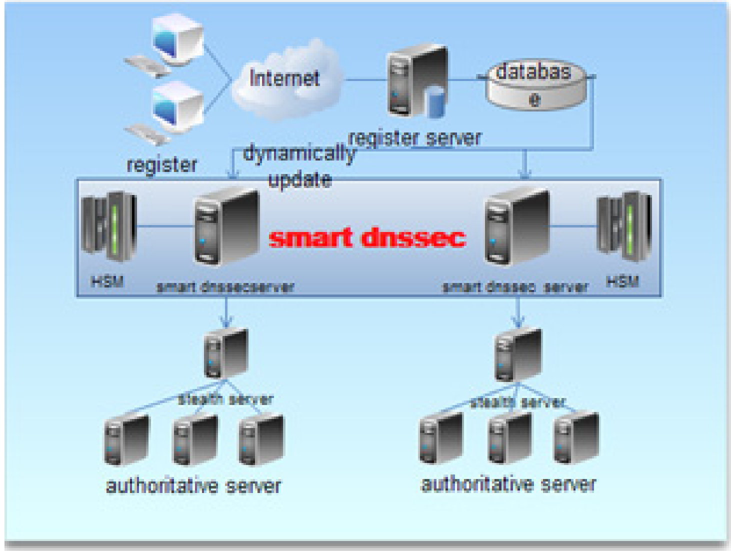
Begin

Purpose:

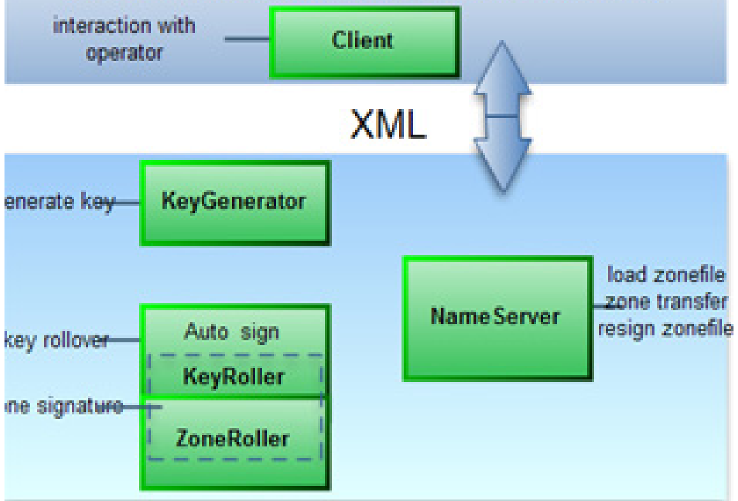
- Automated deployment of DNSSEC

Core Value:

- Control key generation through HSM API
- Normal and emergency key rollover
- Support HSM signature
- Zone management, load/transfer/resign
- Emergency Management and Disaster Recovery



smart dnssec software architecture

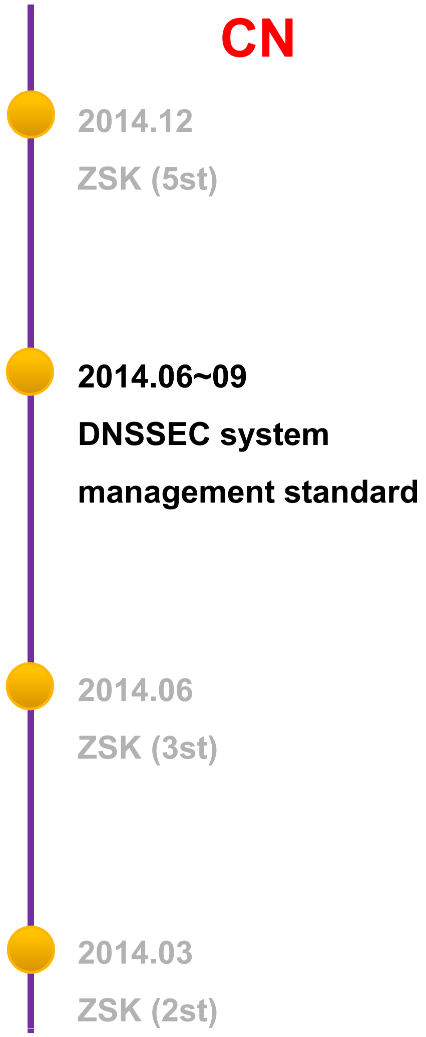


1、Review

2、What have we done in 2014?

3、Future

2、What have we done in 2014? - CN


CN

2014.12

ZSK (5st)

2014.06~09

DNSSEC system

management standard

2014.06

ZSK (3st)

2014.03

ZSK (2st)

◆ *DNSSEC system security management policies and standard*

- Management hierarchical division
- Staff responsibilities and obligations
- Routine and emergency incident plans
- Key management security policy
- Information systems management policy

Management perspective

◆ *DNSSEC system key management and maintenance manual*

- Software and hardware architecture description
- DNSKEY synchronization strategy
- DNSKEY rollover strategy
- Function card repair mechanism
- Software and hardware emergency response strategy

Technical perspective

2、What have we done in 2014? - CN

CN

2014.12
ZSK (5st)

2014.09
ZSK (4st)

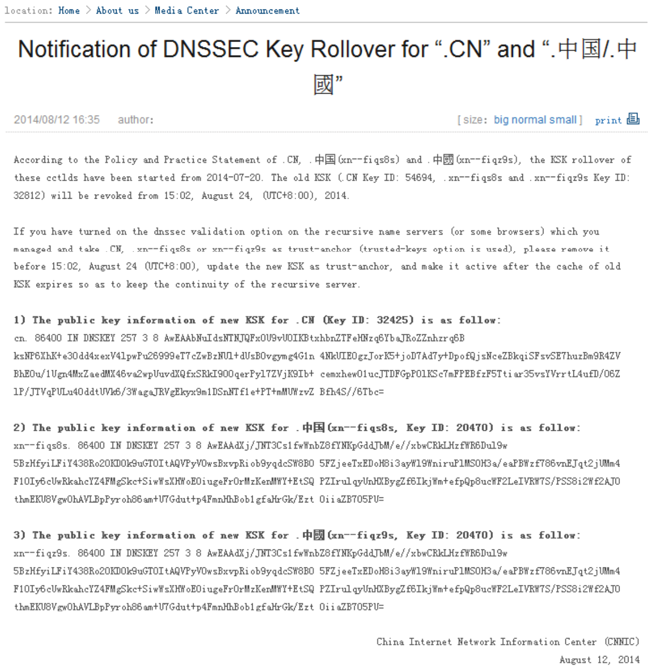
2014.08
KSK (1st)

2014.06
ZSK (3st)

2014.03
ZSK (2st)

◆ According to DNSSEC system management standard, we finished routine ZSK & KSK Rollover

- Finished ZSK rollover 4 times (Pre-publish)
- Finished KSK rollover for the **first time** (Double-signature)
  - **According to RFC 5011 style**, “Automated Updates of DNSSEC Trust Anchors”



location: Home > About us > Media Center > Announcement

Notification of DNSSEC Key Rollover for “.CN” and “.中国/.中國”

2014/08/12 16:35 author: [size: big normal small] print

According to the Policy and Practice Statement of .CN, .中国(xn--fiqs8s) and .中國(xn--fiqz9s), the KSK rollover of these cctlds have been started from 2014-07-20. The old KSK (.CN Key ID: 54694, .xn--fiqs8s and .xn--fiqz9s Key ID: 32812) will be revoked from 15:02, August 24, (UTC+8:00), 2014.

If you have turned on the dnssec validation option on the recursive name servers (or some browsers) which you managed and take .CN, .xn--fiqs8s or xn--fiqz9s as trust-anchor (trusted-keys option is used), please remove it before 15:02, August 24 (UTC+8:00), update the new KSK as trust-anchor, and make it active after the cache of old KSK expires so as to keep the continuity of the recursive server.

1) The public key information of new KSK for .CN (Key ID: 32425) is as follow:

```
cn. 86400 IN DNSKEY 257 3 8 AwEAAbNuIdsNTNJQFxOU9vUOIKBtxhbnZTFeHNzq6YbaJRoZZnhzrq6B
ksNP6XhK+e30dd4xexV4lpwPu26999eT7cZwBzNUl+dUsBOvgymg4G1n 4NkUIEOgzJorK5+joD7Ad7y+DpofQjsNceZBkqiSFsvSE7huzBm9R4ZV
BhEOu/1Ugn4MxZaedMX46va2wpUuvdXQfxSRkI900qerPyl7ZVjK9Ib+ cemxhew01ucJTDFGpP0lKSc7mFPEBfzF5Ttiar35vsYVrrtL4ufD/06Z
lP/JTVqPULu40ddtUVk6/3WagaJRVgEkyx9m1DSnNTf1e+PT+mMUWzvZ Bfh4S//6Tbc=
```

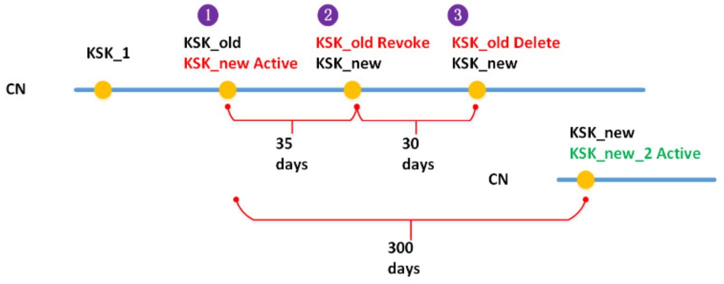
2) The public key information of new KSK for .中国(xn--fiqs8s, Key ID: 20470) is as follow:

```
xn--fiqs8s. 86400 IN DNSKEY 257 3 8 AwEAAdXj/JNT3Cs1fwWnbZ8fYNKpGddJbM/e//xbwCRkLHzfWR6Dul9w
5BzHfyiLFiY438Ro20KD0k9uGTOItAQVPyVOwsBxvpRiob9yqdcSW8BO 5FZjeeTxEDoH8i3ayWl9WniruPlMSOH3a/eaPBWzf786vnEJqt2jUMm4
F10Iy6cUwRkahcYZ4FMgSkc+SiwWsXHWoEOiugeFrOrMzKenMWY+EtSQ PZIrulqyUnHXBygZf6IkjWm+efpQp8ucWF2LeIVRW7S/PSS8i2Wf2AJO
thmEKU8VgwOhAVLBpPyroh86am+U7Gdut+p4FmnHhBob1gfaHrGk/Ezt OiiaZB705PU=
```

3) The public key information of new KSK for .中國(xn--fiqz9s, Key ID: 20470) is as follow:

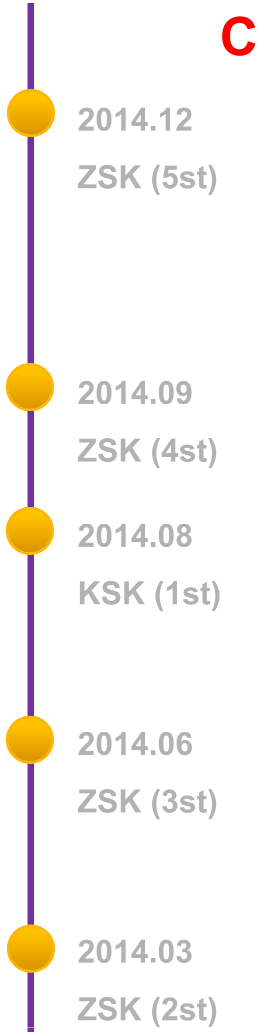
```
xn--fiqz9s. 86400 IN DNSKEY 257 3 8 AwEAAdXj/JNT3Cs1fwWnbZ8fYNKpGddJbM/e//xbwCRkLHzfWR6Dul9w
5BzHfyiLFiY438Ro20KD0k9uGTOItAQVPyVOwsBxvpRiob9yqdcSW8BO 5FZjeeTxEDoH8i3ayWl9WniruPlMSOH3a/eaPBWzf786vnEJqt2jUMm4
F10Iy6cUwRkahcYZ4FMgSkc+SiwWsXHWoEOiugeFrOrMzKenMWY+EtSQ PZIrulqyUnHXBygZf6IkjWm+efpQp8ucWF2LeIVRW7S/PSS8i2Wf2AJO
thmEKU8VgwOhAVLBpPyroh86am+U7Gdut+p4FmnHhBob1gfaHrGk/Ezt OiiaZB705PU=
```

China Internet Network Information Center (CNNIC)
August 12, 2014



2、What have we done in 2014? - CN

CN


2014.12

ZSK (5st)

2014.09

ZSK (4st)

2014.08

KSK (1st)

2014.06

ZSK (3st)

2014.03

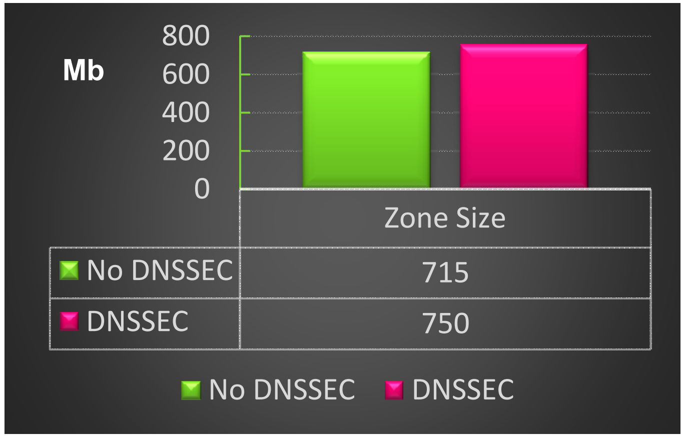
ZSK (2st)

Observations

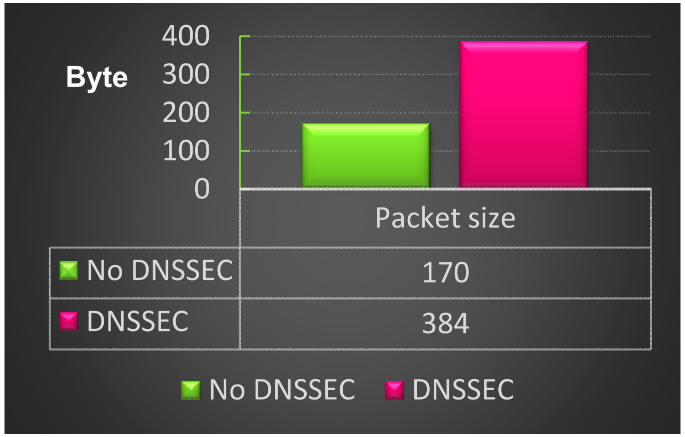
- **Zone Size (10 million+)**
  - Opt-out
  - **Increased a little (5%)** ↓
- **Packet Size**
  - RRSIG
  - **2.3** times larger in average ↓

Reasons

- **Zone Size**
  - Opt-out
  - **Played a good effect**
- **Packet Size**
  - **We upgrade BIND**
  - **Recursive upgrade software**
  - **Make query and response much "sensible"**



	Zone Size
🟩 No DNSSEC	715
🟥 DNSSEC	750



	Packet size
🟩 No DNSSEC	170
🟥 DNSSEC	384

2、What have we done in 2014? - NewG

NewG

2014.08

xn--xhq521b

（.广东）

xn--1qqw23a

（.佛山）

Onboarding

2014.01

xn--55qx5d

（.公司）

xn--io0a7i

（.网络）

Onboarding

◆ **We put 4 NewGtlds onboarding**

- 2 were applying by CNNIC
  - “xn--55qx5d” (.公司) and “xn--io0a7i” (.网络)
- 2 were hosting by CNNIC
  - “xn--xhq521b” (.广东) and “xn--1qqw23a” (.佛山)

◆ **We use similar strategies with .CN**

- Algorithm and Key Length
- SmartDNSSEC
- CookDNS

Key Type	Function	Algorithm	Length	NSEC/NSEC3
ZSK	Sign RRSET	RSA-SHA256	1024	NSEC3
KSK	Sign DNSKEY		2048	

◆ **We also become DataEscrow Agent and EBERO**

- xn--zfr164b (.政务), xn--55qw42g (.公益)
- top

2、What have we done in 2014? - R & D

SDNS-D

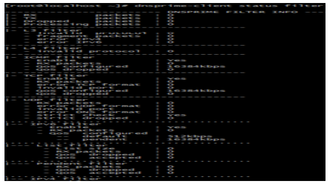
CNNIC *Anti-attack device*

Using FPGA to improve the performance

- □ Monitor the DNS query
- □ Block the DDOS attack query
- □ Emergency Cache
- □ Gigabit wire-speed one port

DNS-prime

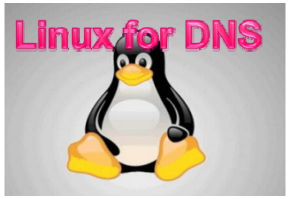
Using 10G ethernet

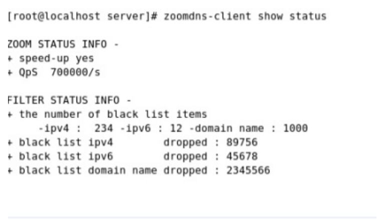


10G wire-speed one port

- □ 10 Gigabit wire-speed one port
- □ Using Zone-transfer protocol to build domain white list
- □ Traffic control for every IP and Domain
- □ Deep packet inspection

ZoomDNS





```
[root@localhost server]# zoomdns-client show status

ZOOM STATUS INFO -
+ speed-up yes
+ QpS  700000/s

FILTER STATUS INFO -
+ the number of black list items
     -ipv4 :  234 -ipv6 : 12 -domain name : 1000
+ black list ipv4        dropped : 89756
+ black list ipv6        dropped : 45678
+ black list domain name dropped : 2345566
```

- □ Lightweight solution
- □ Deep packet inspection
- □ Blacklist of domain suffixes
- □ Gigabit wire-speed
- □ Speed up the DNS performance

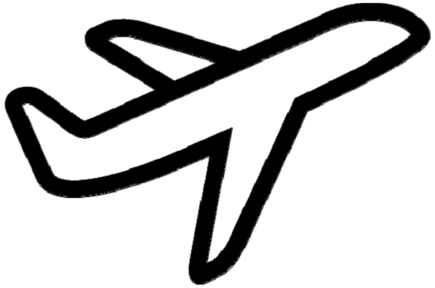
1、Review

2、What have we done in 2014?

3、Future

3、Future

DANE



IPv6

Recursive

SLD

••••••

中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

中国信息社会重要的基础设施建设者、运行者和管理者

CNNIC, No.4 South 4th Street, Zhongguancun, Haidian Dstrict, Beijing 100190,China
www.cnnic.cn