DNSSEC Deployment in .CN

DNS-OARC's 2014 Spring Workshop

Qi Zhao, CNNIC

May 10, 2014

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

1、Overview

2、Preparations

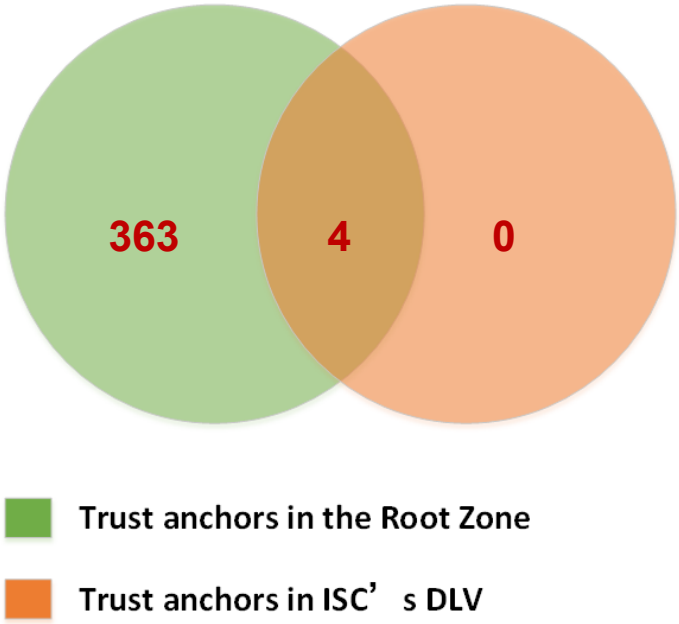
3、Deployment

4、Monitoring & Observations

Introduction

u Popular protocol in DNS

- 563 TLDs in the root zone in total
- 378 TLDs are signed
- 367 TLDs have trust anchors published as DS records in Root
- 4 TLDs have trust anchors published in ISC's DLV Repository



Ø .CN is one of the signed zones from the beginning of August, 2013.

1、Overview

2、Preparations

3、Deployment

4、Monitoring & Observations

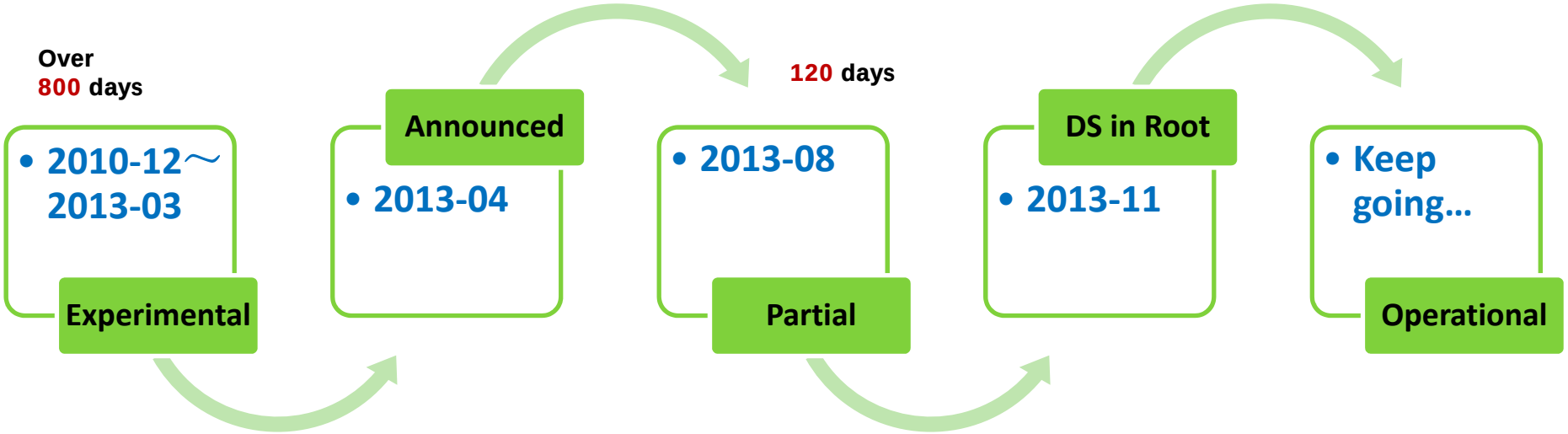
1、Overview

Announced：

- ü Hardware & software deployment
- ü Training and drills

DS in Root：

- ü Generation & submission
- ü Observations & verification



Experimental：

- ü Risk analysis
- ü Software development

Partial：

- ü Signing & roller
- ü Observations & verification

Operational：

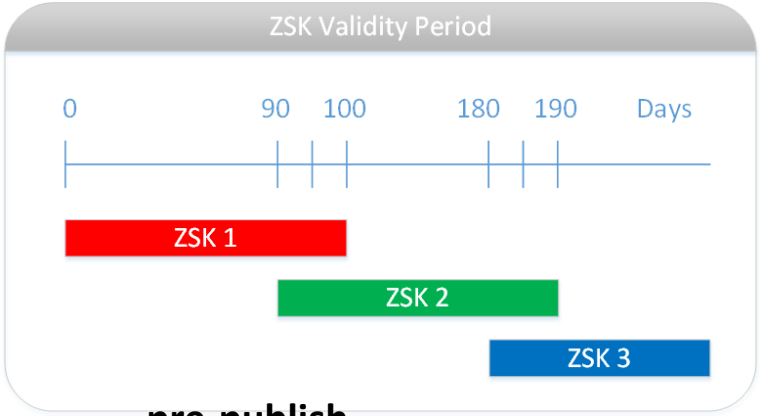
- ü Upgrades and improvements
- ü Debugging

1、Overview

Key Information

- **Algorithm and Key Length**

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

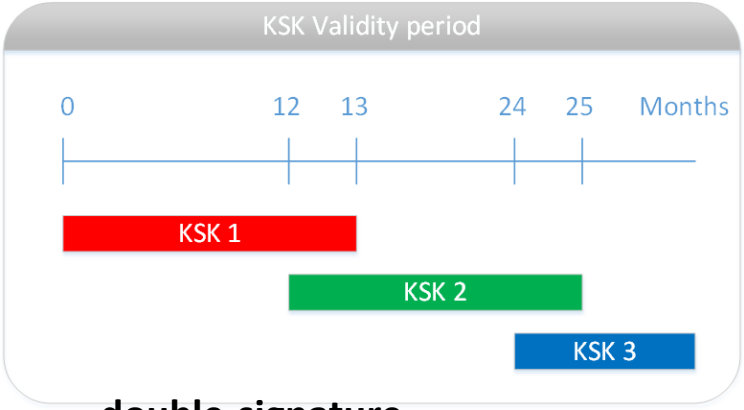


pre-publish

RFC 4641
RFC 6781

- **Key rolling cycle and RRSIG period**

Key Type	Period	Roll	Overlap	RRSIG Period
ZSK	100 day	90 day	10 day	30 day
KSK	13 month	12 month	30 day	

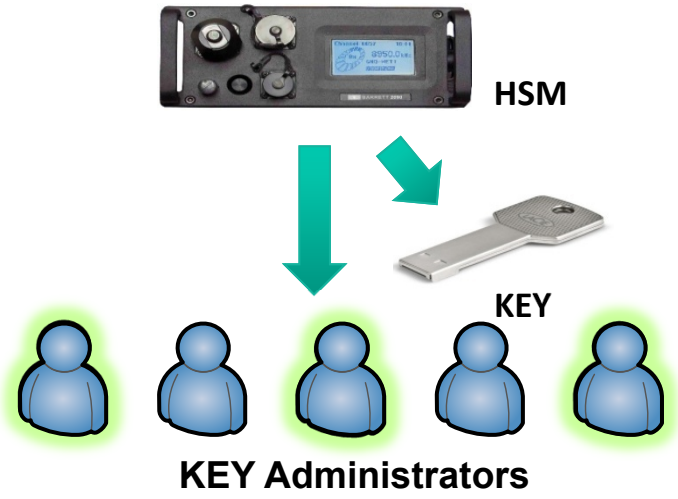


double-signature

1、Overview

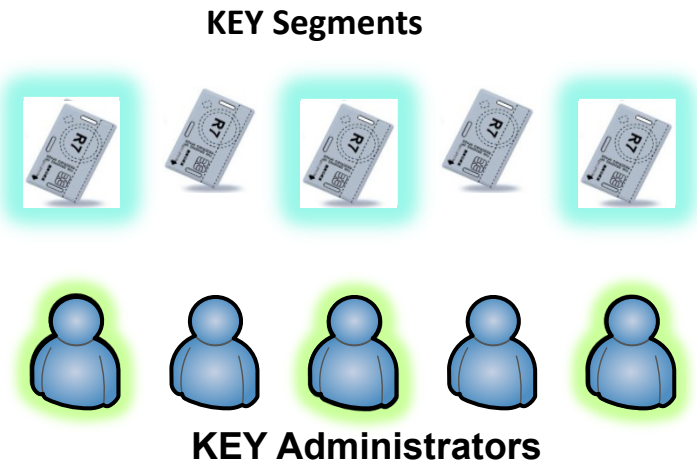
Key Pair management

- All pairs of keys are generated in HSM
- **5** key administrator accounts are generated during the HSM initialization process
- **More than half of them (>=3)** are needed for access



Private Key protection

- An encrypted key is divided into **5 segments** and stored in independent smart cards, each kept by a key administrator
- In emergency case, the key can be restored by any **3 segments**



1、Overview

Physical Security

- An electromagnetic shielding datacenter (following GJBz20219-94 “C” level of PRC) is being used, and only authorized persons may access
- HSMs and hidden master servers are kept in the electro-magnetic shielding datacenter
- A backup system is established in disaster datacenter in Chengdu, with the same security insurance level as that of Beijing

1、Overview

2、Preparations

3、Deployment

4、Monitoring & Observations

2、Preparation

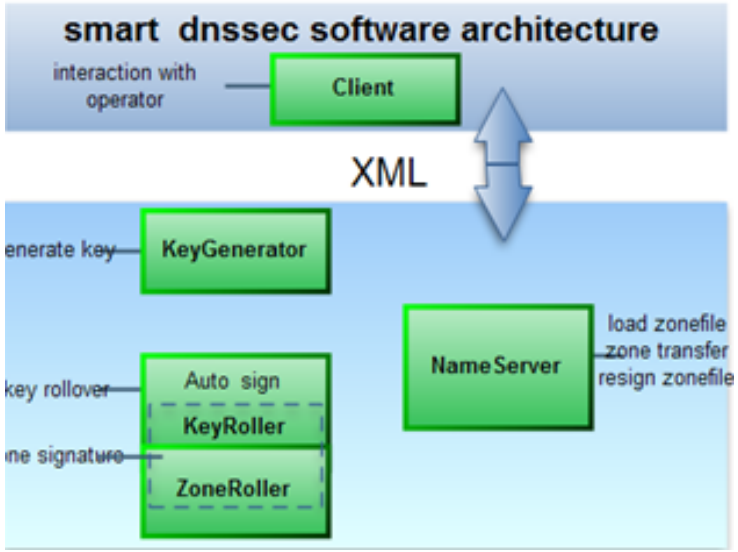
1. SmartDNSSEC - Independent R & D Software (2010.1-2012.6)

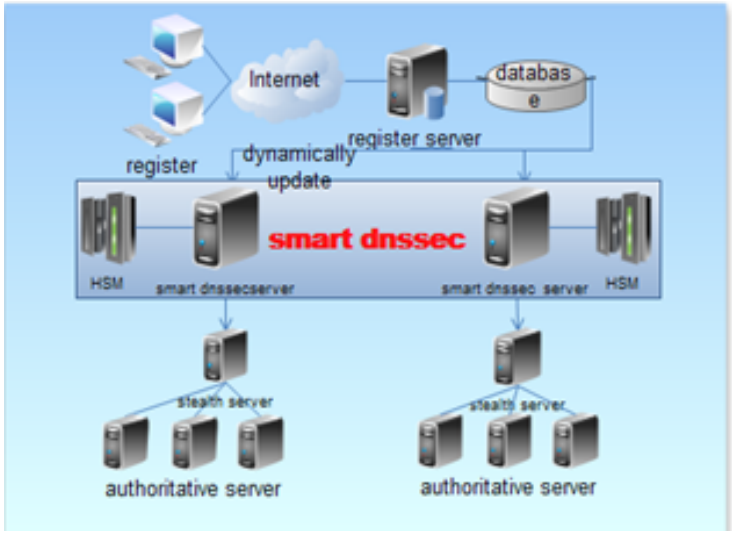
Purpose:

- 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

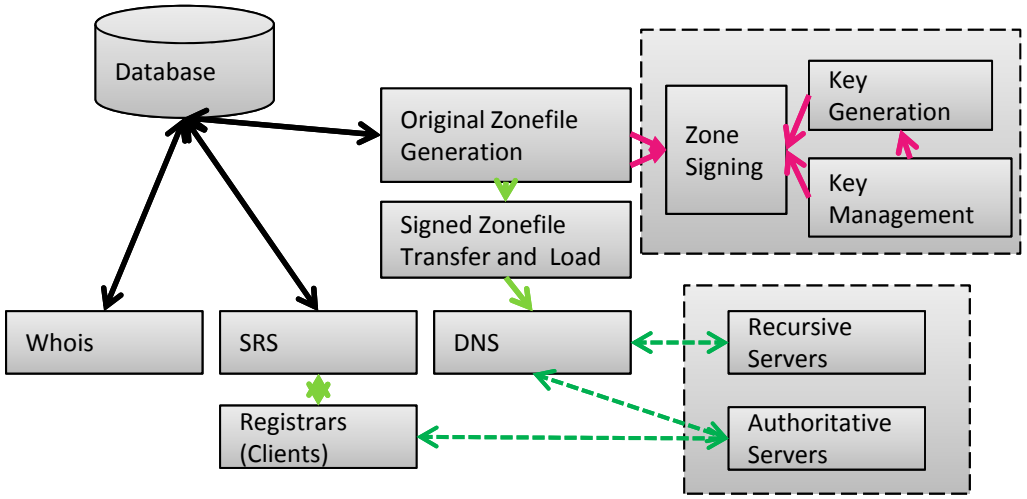


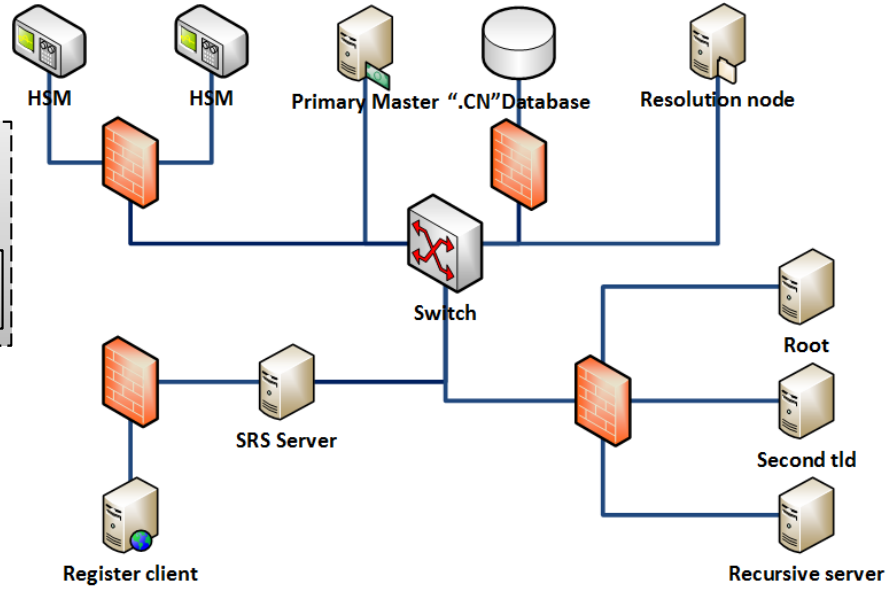


2、Preparation

2. Internal simulation test (2010.12-2013.5)

- A close-loop simulating environment with root, TLD, SLD, recursive, SRS, whois, etc
- 5,600,000 names in .CN zone , 6,900,000 times of SRS update, 170,000 DS records submission by SLD
- Key rotation: ZSK 102 times, KSK 51 times
- 20+ bugs were fixed

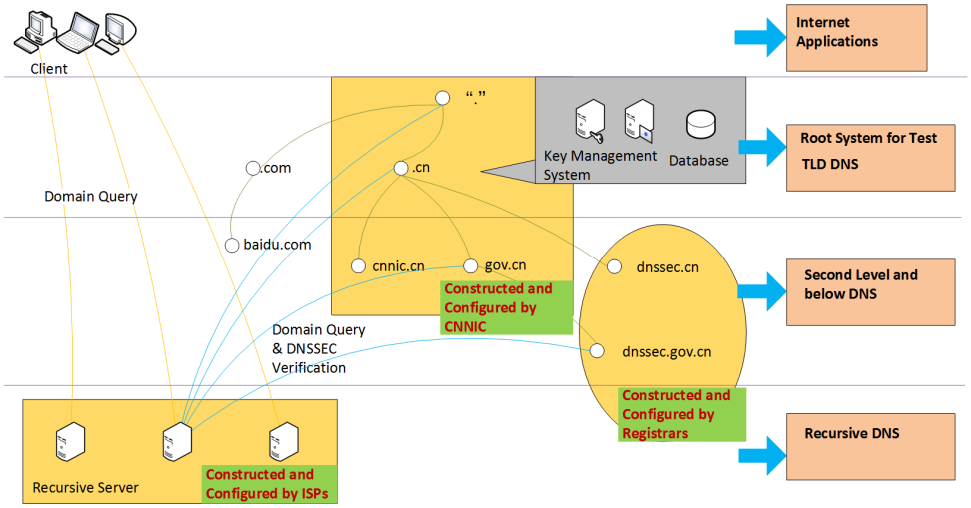


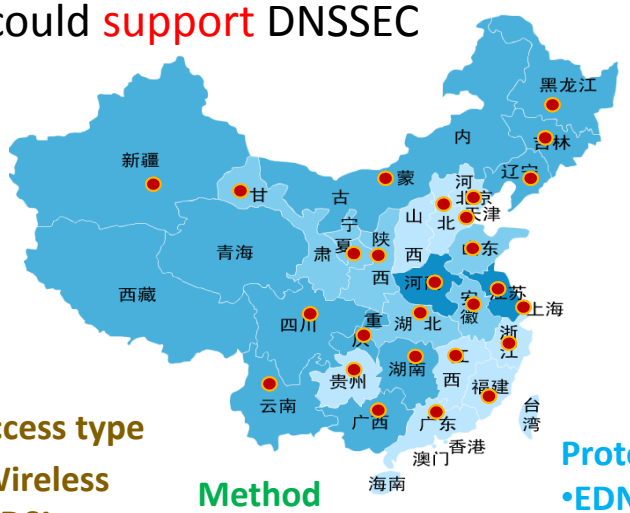


2、Preparation

3. Open test with ISPs in China (2012.1-2012.11)

- Main ISPs in China (China Telecom, China Unicom, China Mobile, CSTNET, CERNET) were covered
- Backbone: About 0.28% can't support UDP packet larger than 512 bytes, 3.41% with UDP packet size limitation policy. All these could be fixed by TCP.
- User side(Wireless, ADSL, LAN, etc.): 0.057% DNSSEC query failure. All the failures were caused by network packet loss or latency, not by DNSSEC
- Conclusion: the Internet environment in China could support DNSSEC





Access type
- Wireless
- ADSL
- LAN

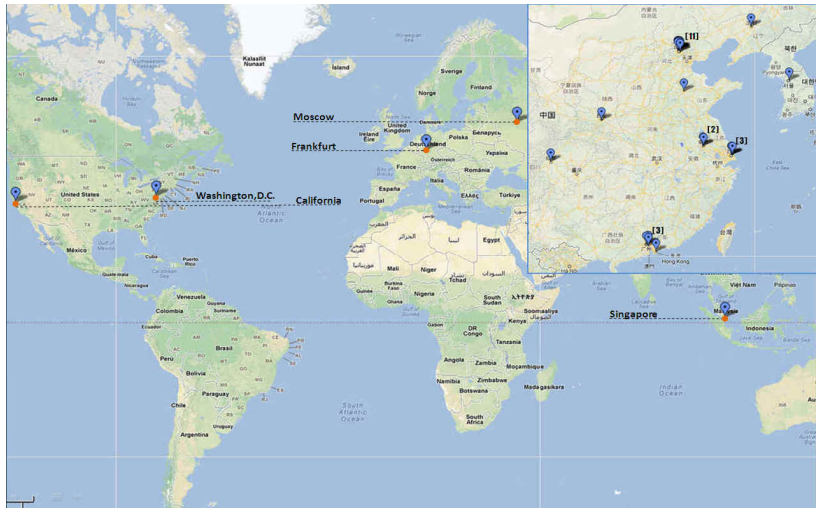
Method
- trusted-keys
- dig +dnssec

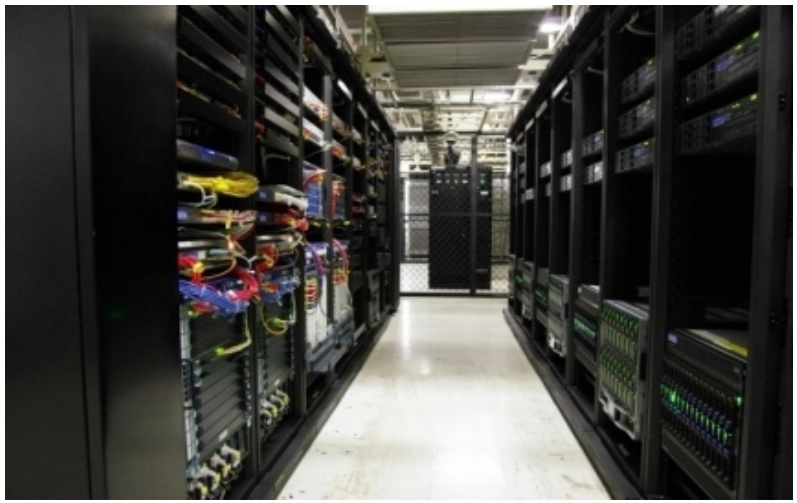
Protocol
- EDNS0
- TCP
- etc

2、Preparation

4. Platform Upgrading (2012.1-2012.10)

- HSM: produced by an industrially certified vendor
- Server: memory upgrading, 16G → 32G
- Router: support EDNS0
- Bandwidth: more for the increased length of data packet (2.5 times)





1、Overview

2、Preparations

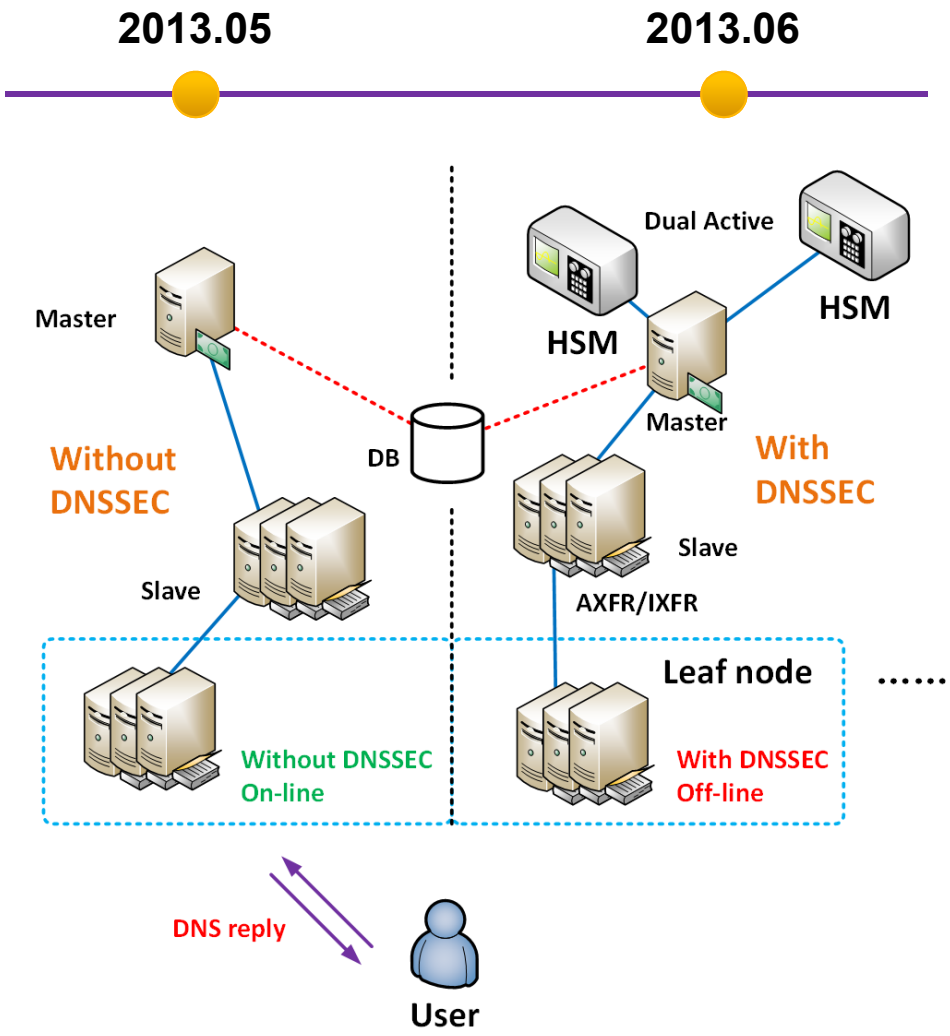
3、Deployment

4、Monitoring & Observations

3、Deployment

Zone Signing

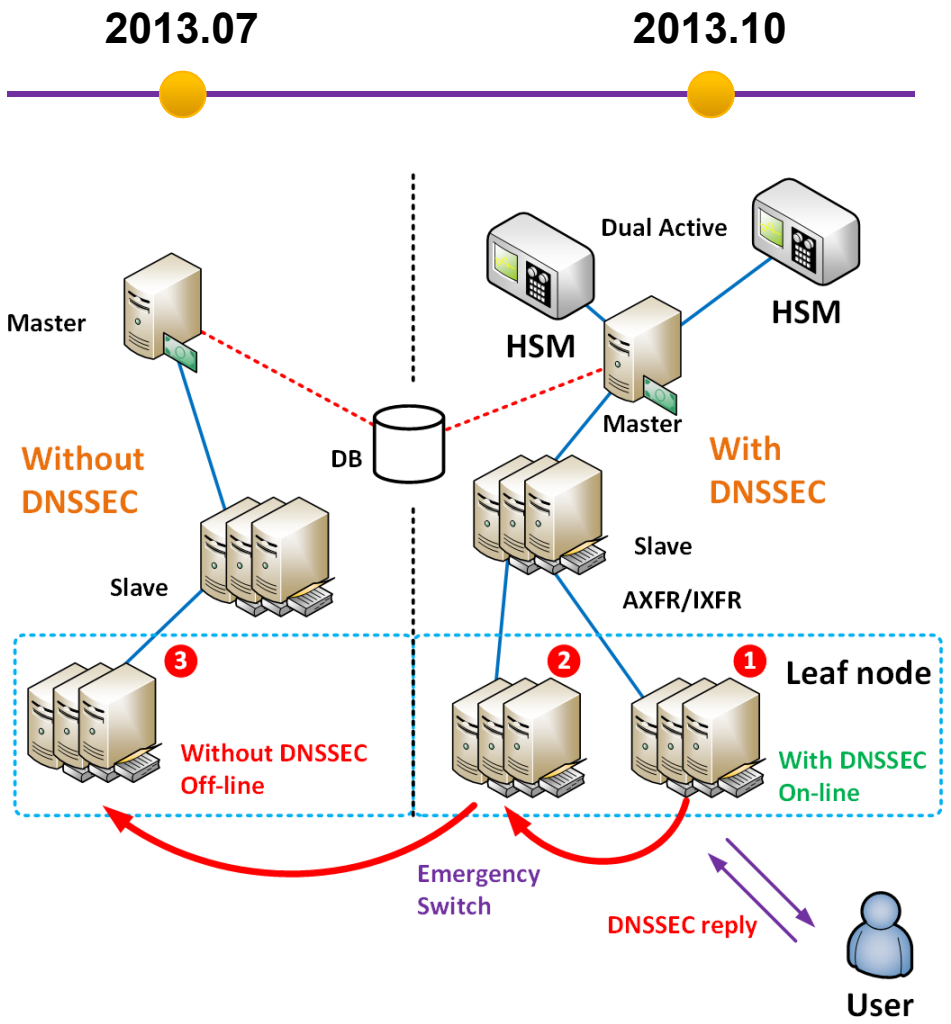
- An **independent** hidden master system for DNSSEC was established
- **.CN**, **.中国/中國** and **43 sub-domain** under .CN are signed by HSM clusters (Dual Active)
- Signing **1000w** names less than **20** minutes
- DNS services (without DNSSEC) is **on-line** for resolving, DNSSEC services is **off-line** for trial operation



3、Deployment

DNSSEC Services On-line

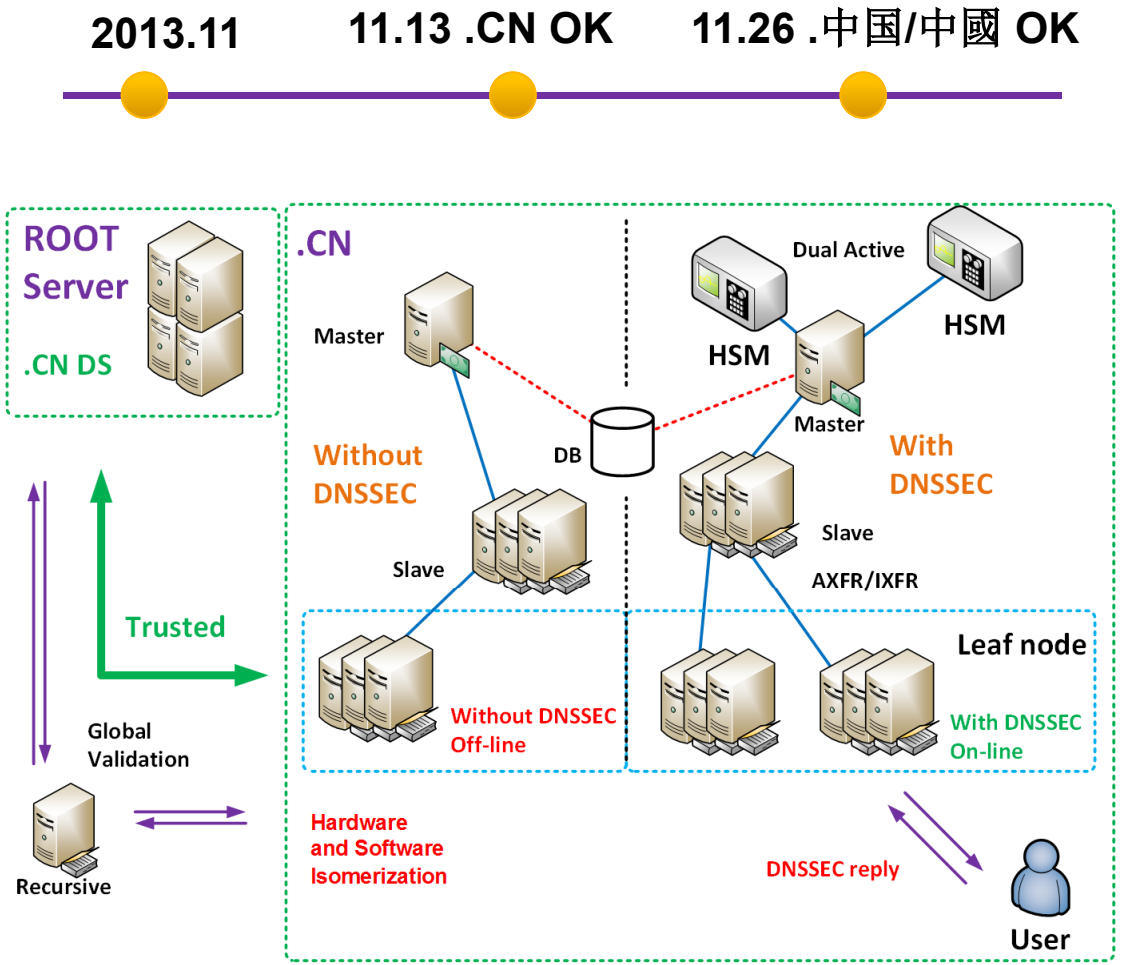
- DNSSEC servers are proceeding on-line **node by node**, **step by step** (Switching, Validation, Analysis, then next Node)
- **2 Backup system** (DNSSEC AXFR system and Non-DNSSEC IXFR system) to ensure the continuity of resolving services
- Fast switching mechanism through **centralized** management (within **5 minutes**, **on authoritative server side**)



3、Deployment

DS Submitting

- Passed IANA's **validation** for DS Record of .CN and .中国/.中國
- DS becomes effective in **Nov. 26** in the root zone
- Validation through DNSSEC enabled recursive server
- The first **ZSK Rotation** has been finished in December, 2013 and the second rotation is in March, 2014 Smoothly
- The **first KSK Rotation** is coming in this year…



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

1、Overview

2、Preparations

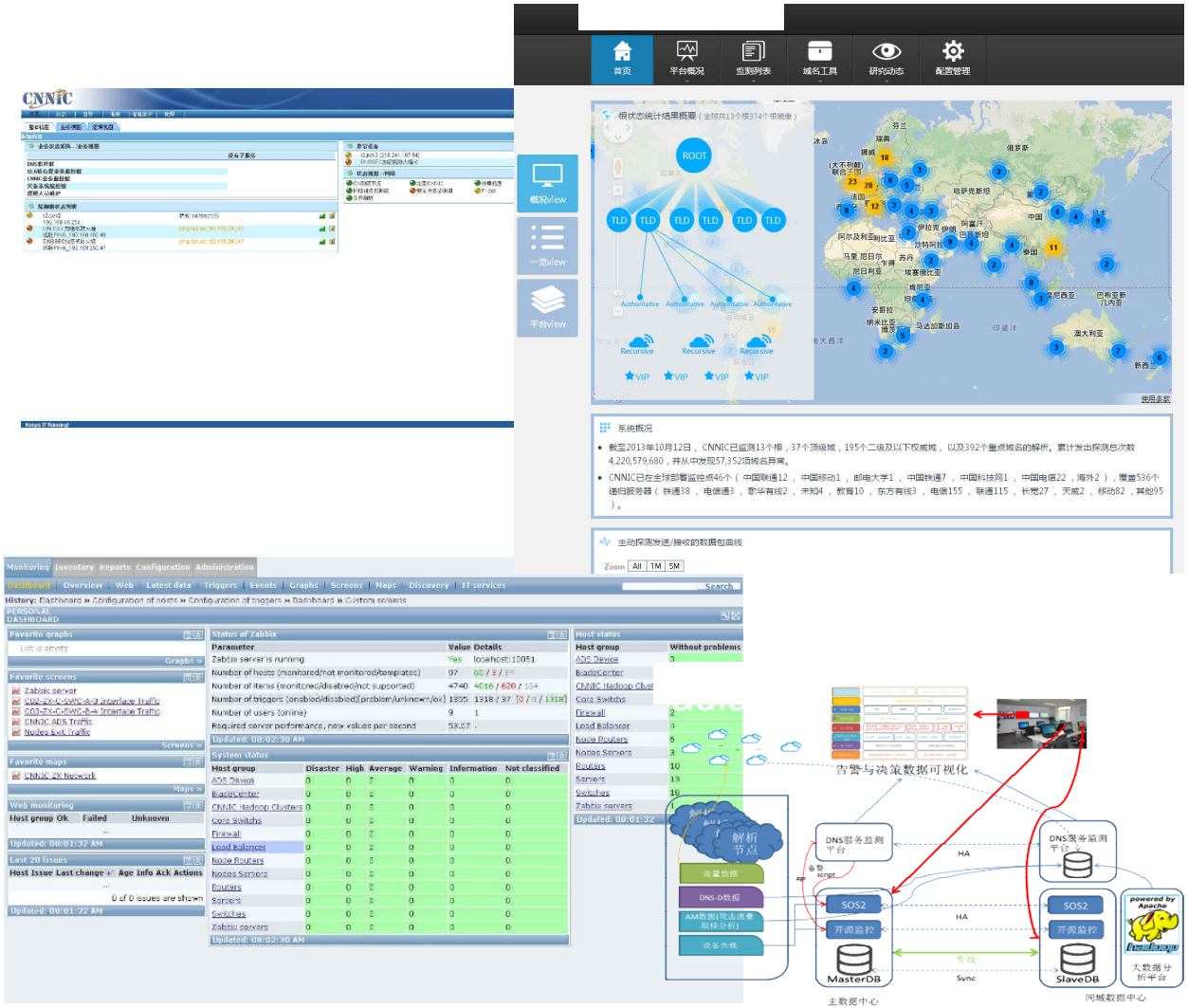
3、Deployment

4、Monitoring & Observations

4、Monitoring and Observations

Monitoring

- **Alarm**
  - WAN DNSSEC validation
  - KEY synchronization
  - SOA comparison
  - Log checking
  - VIP domain checking
  - etc
- **Warning**
  - KEY rolling event
  - DS event
  - KEY re-generation
  - etc

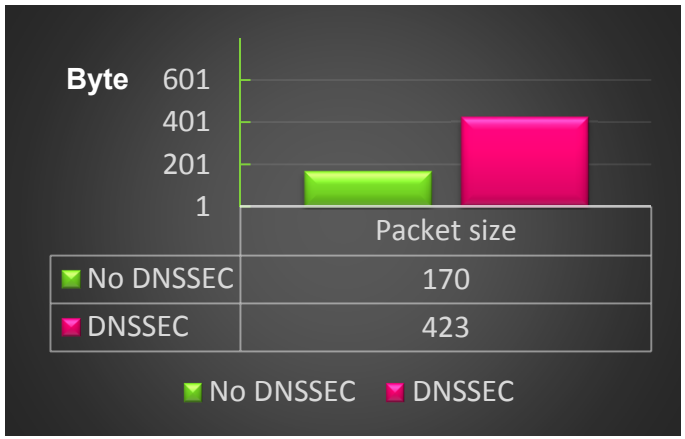


4、Monitoring and Observations

Observations

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

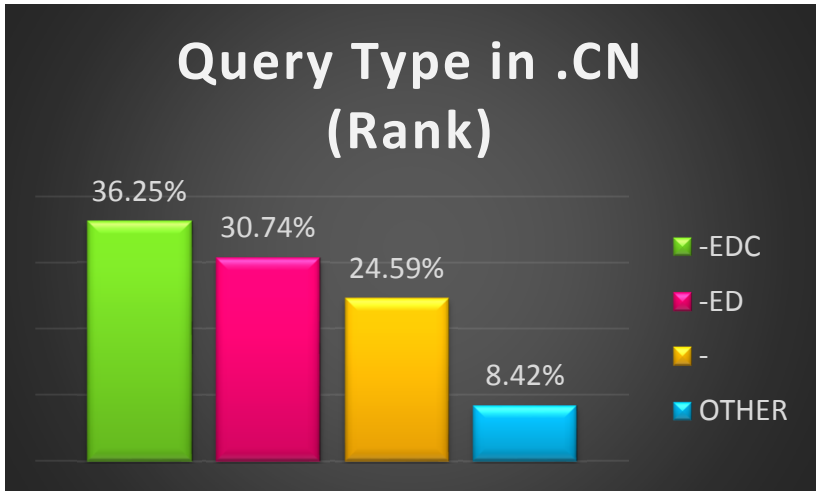
- **68%** DNSSEC query in usual
- After sub-domain and recursive nameservers having been implemented DNSSEC, bandwidth costs will be **much larger**



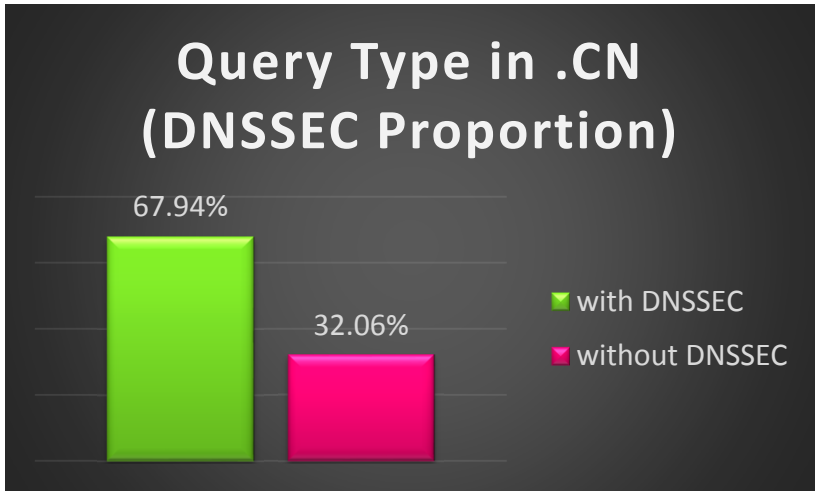
4、Monitoring and Observations

Observations

- **Query Type in .CN (Rank)**
  1. “-EDC” 36.25%
  2. “-ED” 30.74%
  3. “-” 24.59%
  4. SUM: **96.13%**



- **Query Type in .CN (DNSSEC Proportion)**
  - With DNSSEC **67.94%**
  - Without DNSSEC 32.06%



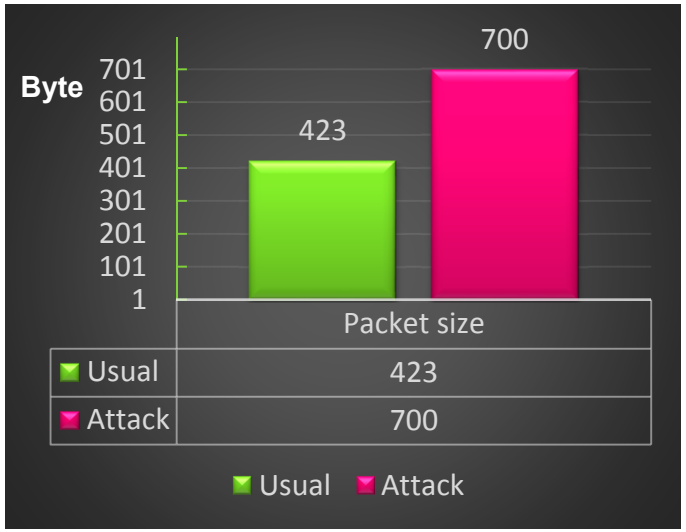
- **The same as in China and Abroad**
- Packet Size maybe increased to **542B**

4、Monitoring and Observations

Observations

2014.02.27 – a small size DDoS Attack

- QpS increased to **2.4** times larger
- Packet size increased to **700** Byte average (**1.65** times)
- Bandwidth reach **4** (2.4*1.65) times larger than usual



- *1) How to push **Second-tld** open DNSSEC?*
- *2) How to push **Recursive** open DNSSEC?*
- *How to **face the pressure** after 1) and 2)?*

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

Thank you for your time!

中国信息社会重要的基础设施建设者、运行者和管理者

www.cnnic.cn