DNSSEC Deployment in .CN

Xiaodong Lee

CEO, CNNIC

March 26, 2014

1、Overview

2、Preparations

3、Deployment

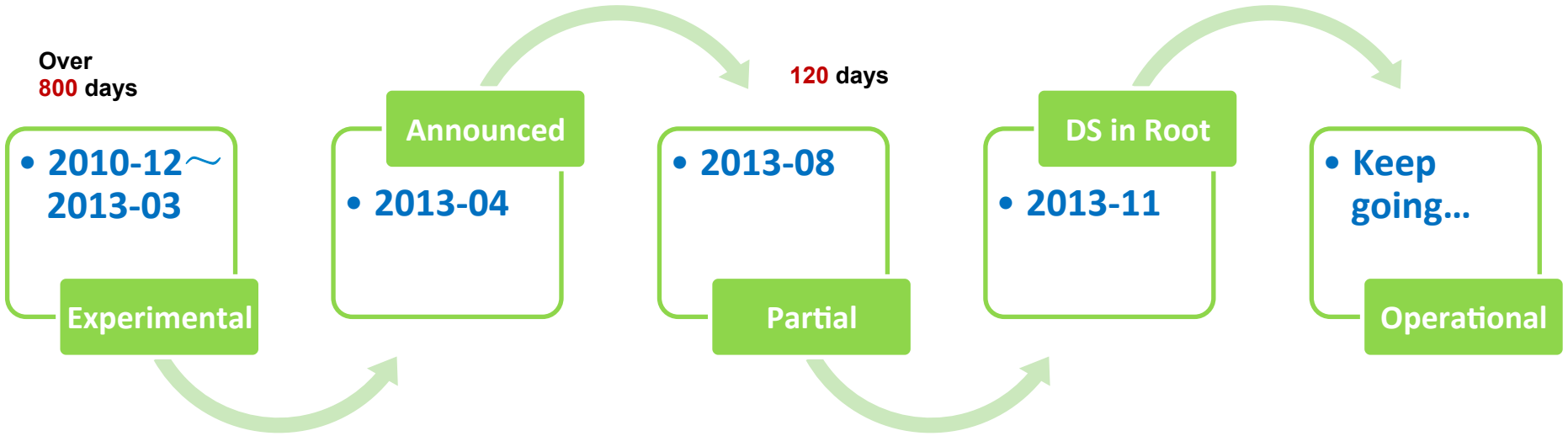
4、Monitoring & Observations

1、Overview

Announced:
- ✓ Hardware & software deployment
- ✓ Training and drills

DS in Root:
- ✓ Generation & submission
- ✓ Observations & verification

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



Experimental:
- ✓ Risk analysis
- ✓ Software development

Partial:
- ✓ Signing & roller
- ✓ Observations & verification

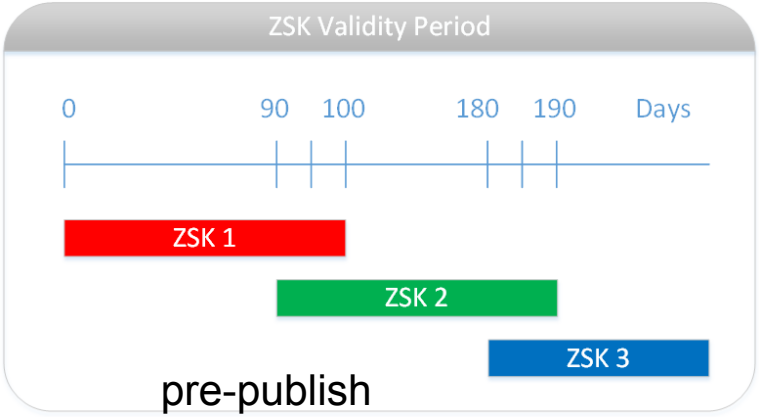
Operational:
- ✓ Upgrades and improvements
- ✓ Debugging

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	

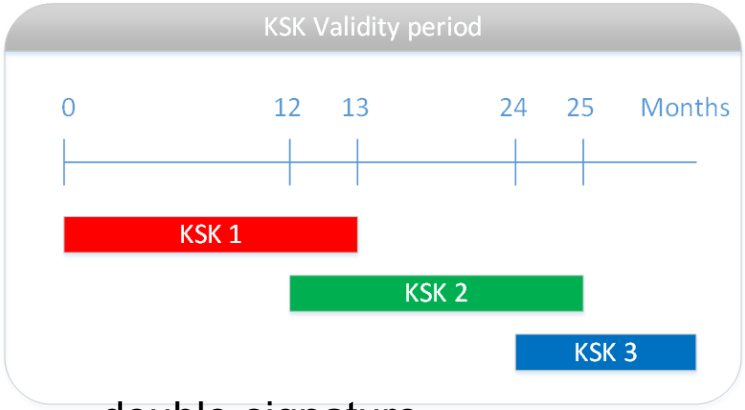


pre-publish

RFC4641

- 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	

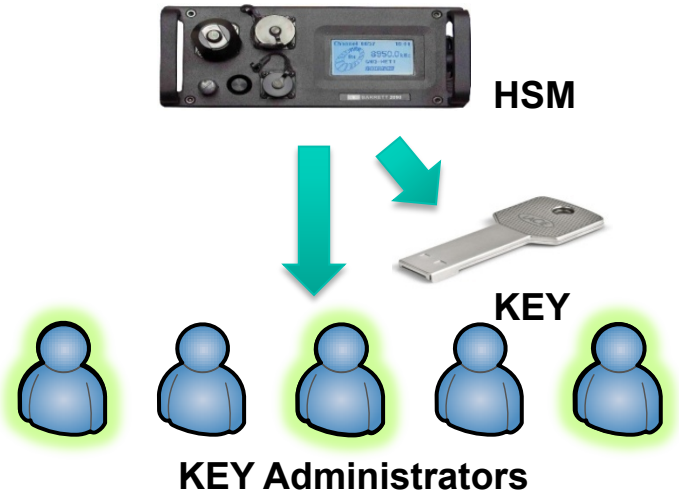


double-signature

1、Overview

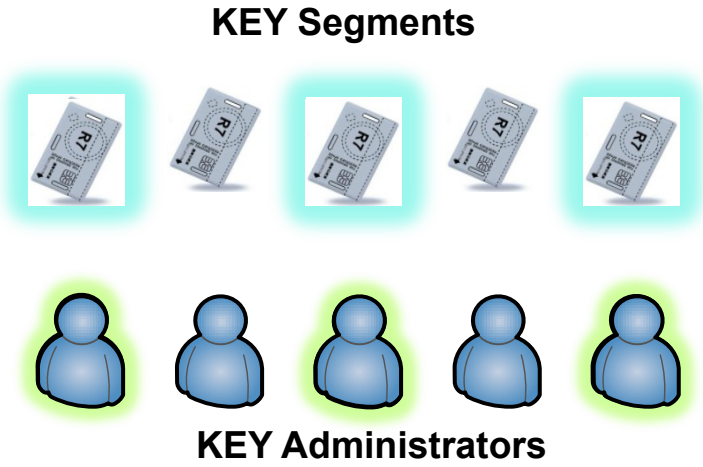
Key Pair management

- 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
- ZSK for RRset, KSK for DNSKEY RRset



Private Key protection

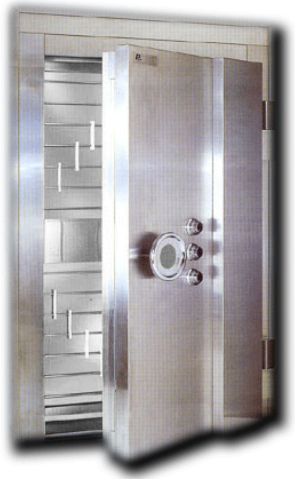
- An encrypted key is divided into **5 segments** and stored in independent smart cards, each kept by a key administrator
- In emergency case, the key can be restored by any **3 segments**



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

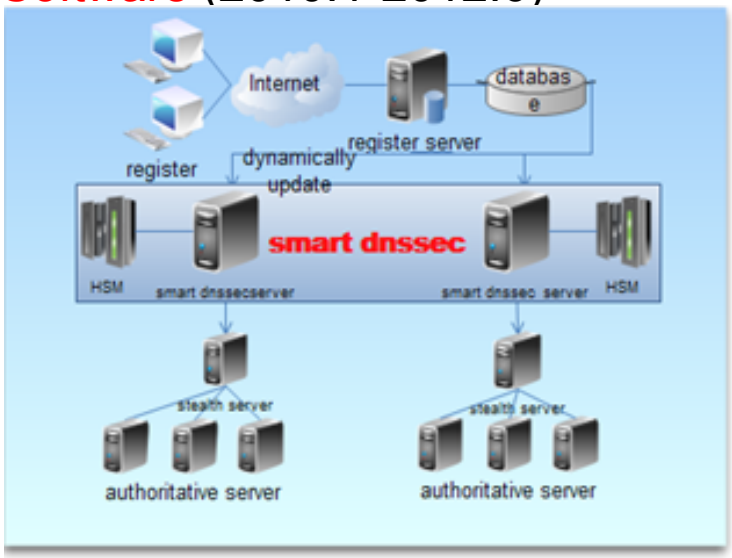
1. SmartDNSSEC - Independent R & D Software (2010.1-2012.6)

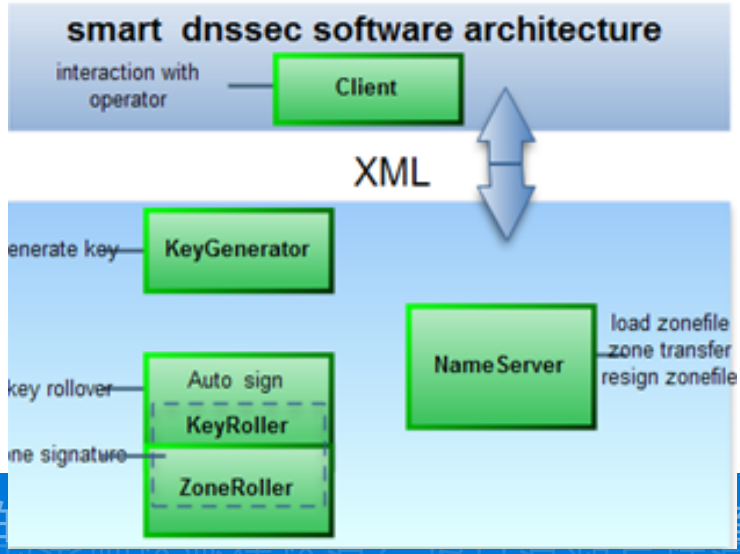
Purpose:

- 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

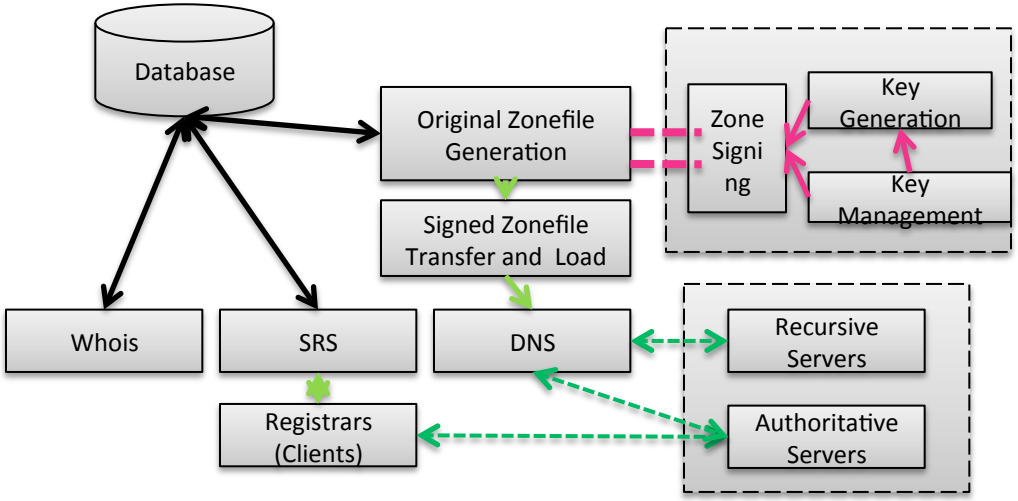


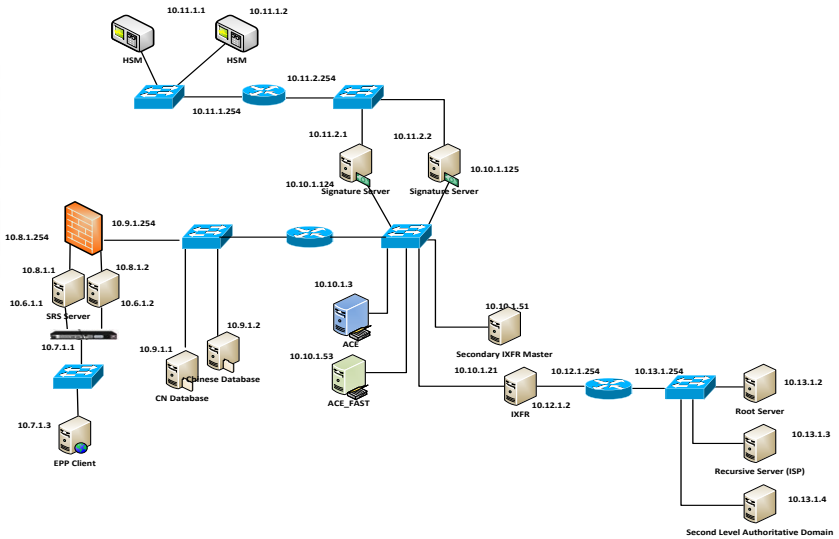


2、Preparation

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

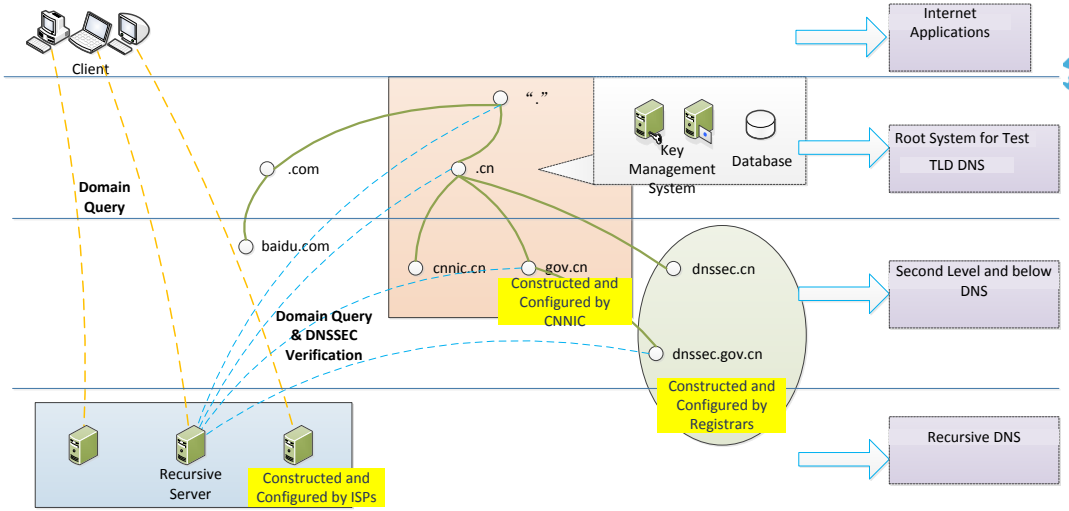


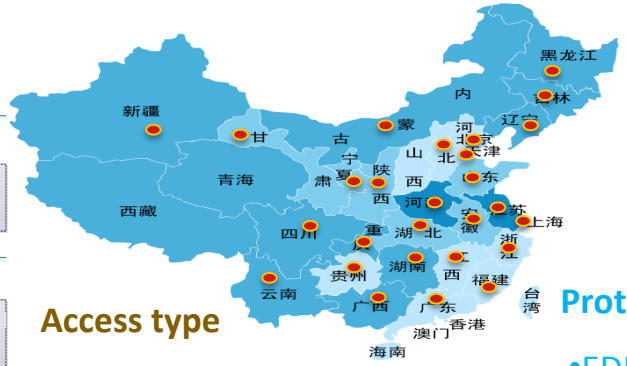


2、Preparation

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

- Main ISPs in China(China Telecom, China Unicom, China Mobile, CSTNET, CERNET) were covered.
- Backbone: About 0.28% didn't support UDP 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

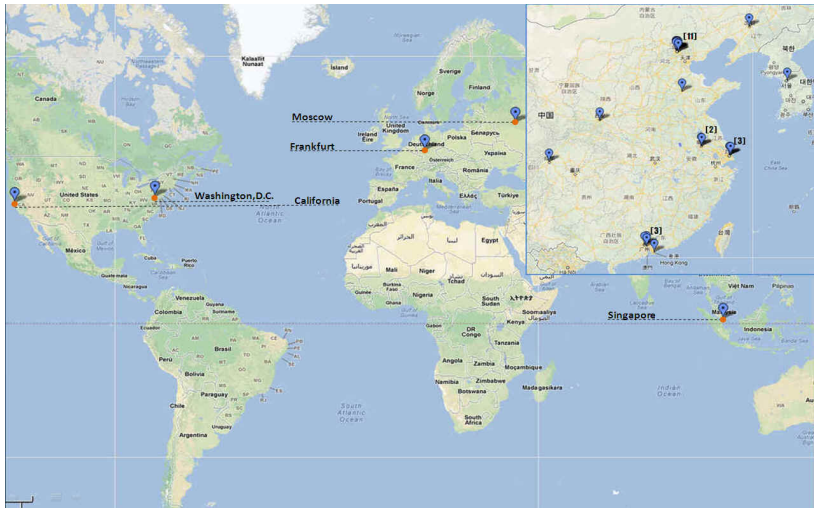
- trusted-keys
- dig +dnssec

Protocol

- EDNS0
- TCP
- etc

4. Platform Upgrading (2012.1-2012.10)

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



1、Overview

2、Preparations

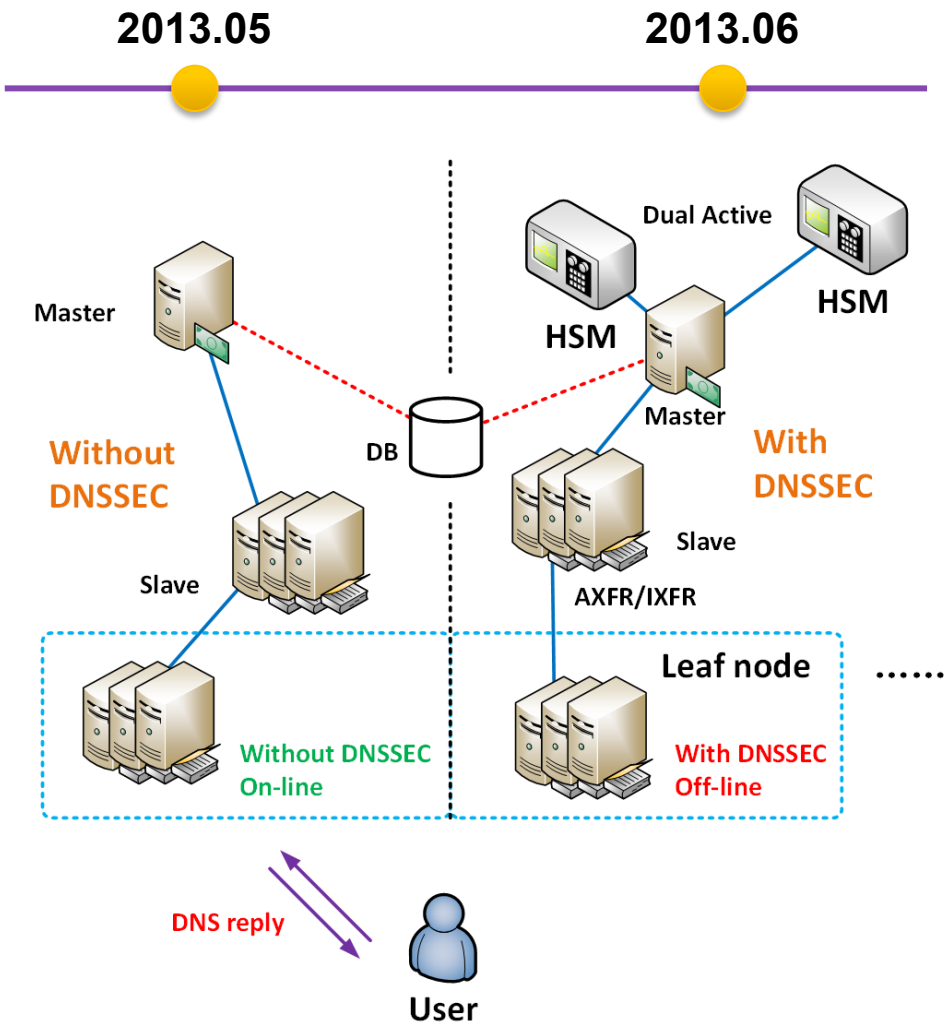
3、Deployment

4、Monitoring & Observations

3、Deployment

Zone Signing

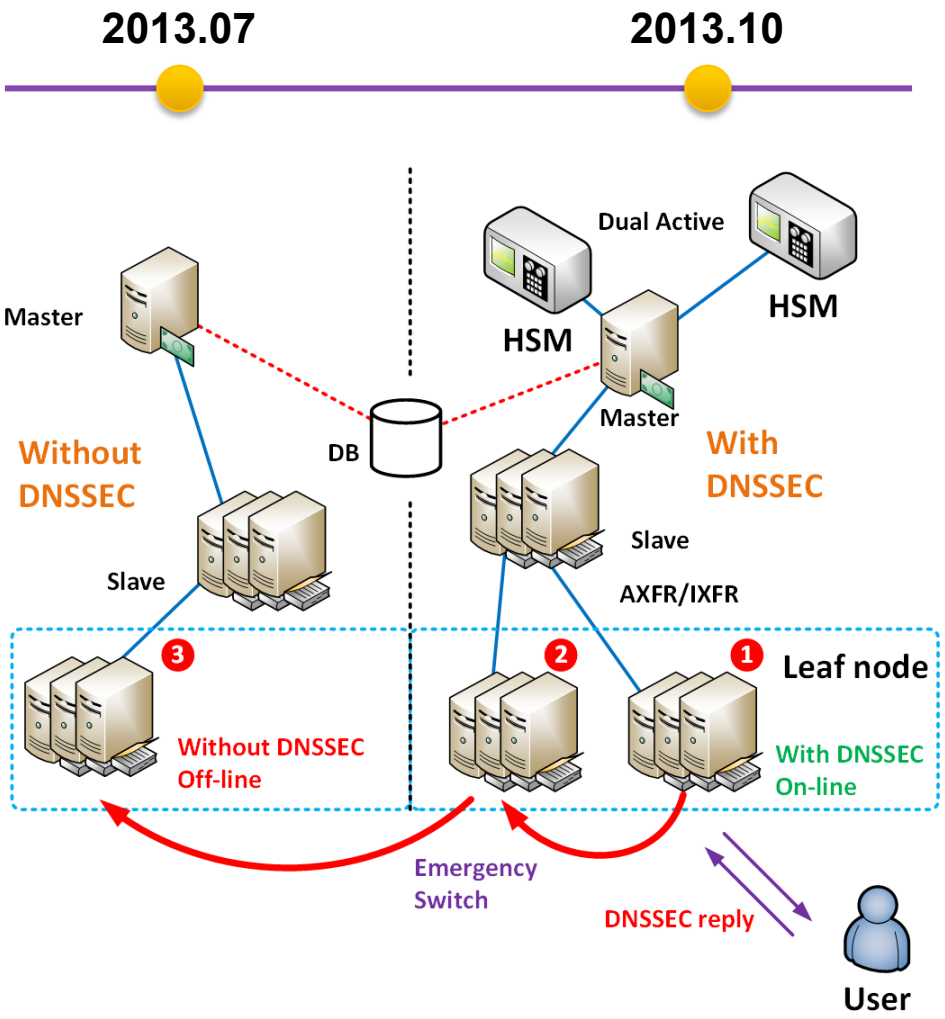
- An **independent** hidden master system for DNSSEC was established
- **.CN**, **.中国/中國** and **43 sub-domain** under .CN are signed by HSM clusters (Dual Active)
- DNS services (without DNSSEC) **on-line** for resolving, DNSSEC services **off-line** for trial operation



3、Deployment

DNSSEC Services On-line

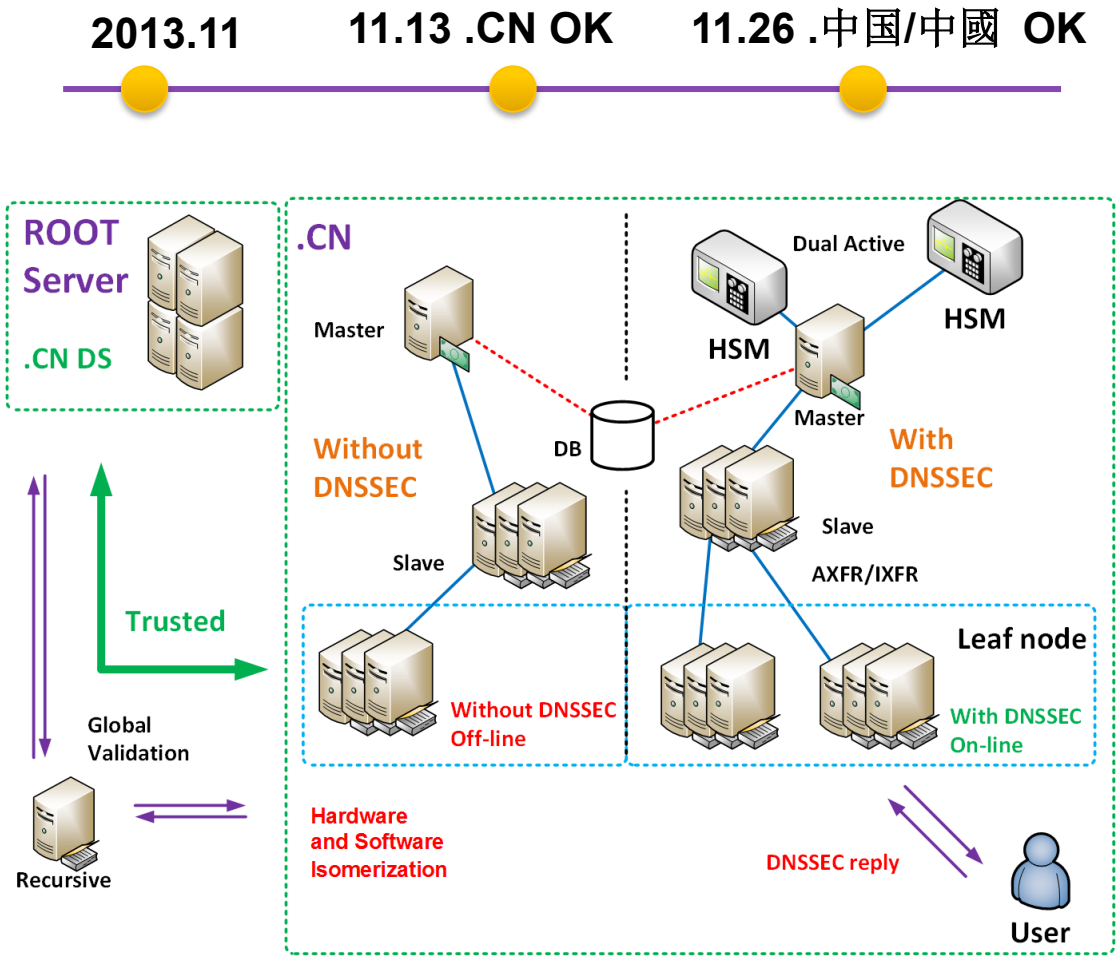
- DNSSEC server is proceeding on-line **node by node**, **step by step** (Switching, Validation, Analysis, then next Node)
- **2 Backup system** (DNSSEC AXFR system and Non-DNSSEC IXFR system) to ensure the continuity of resolving services
- Fast switching mechanism through **centralized** management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



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 Smoothly



1、Overview

2、Preparations

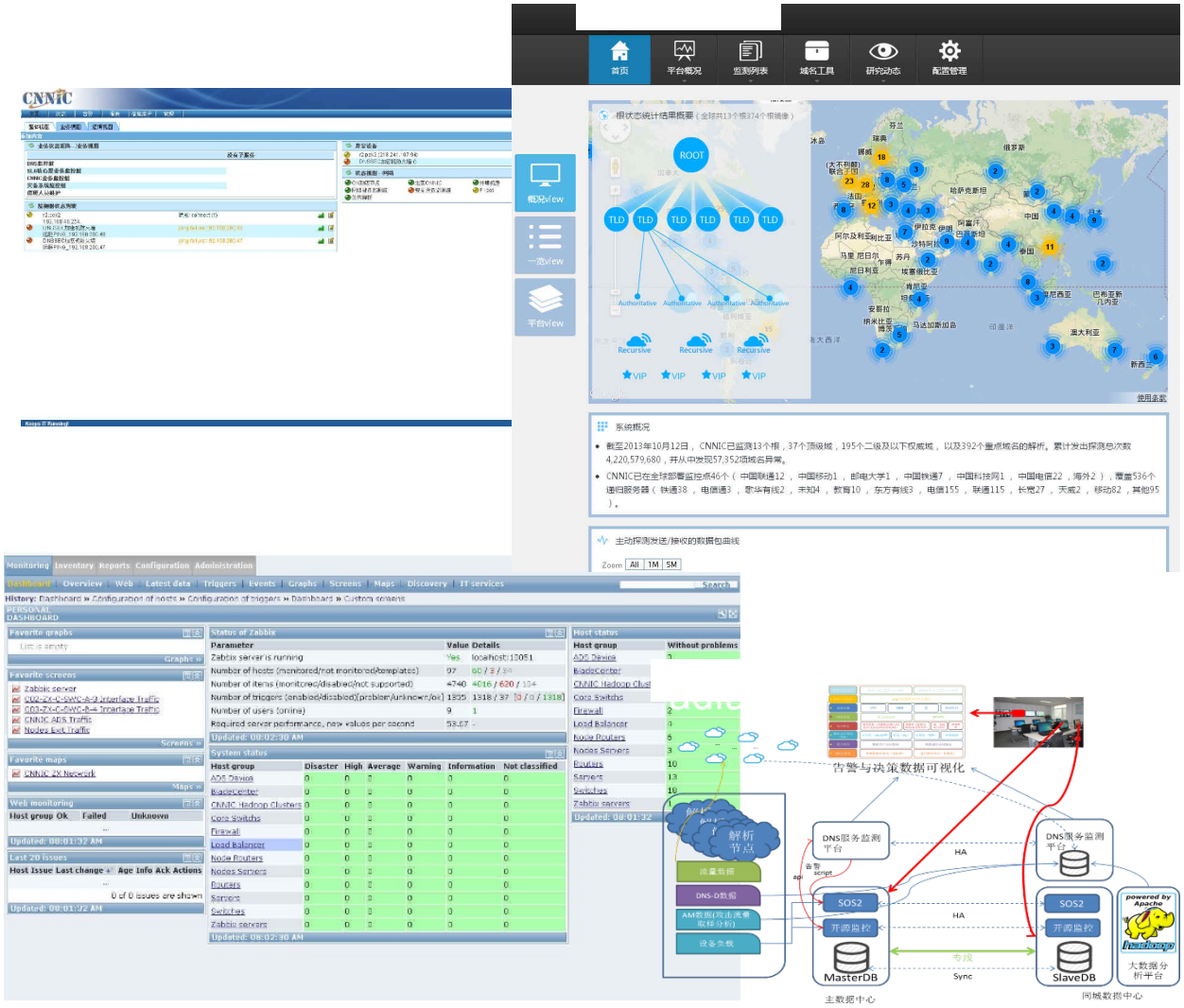
3、Deployment

4、Monitoring & Observations

Monitoring and Observations

Monitoring

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

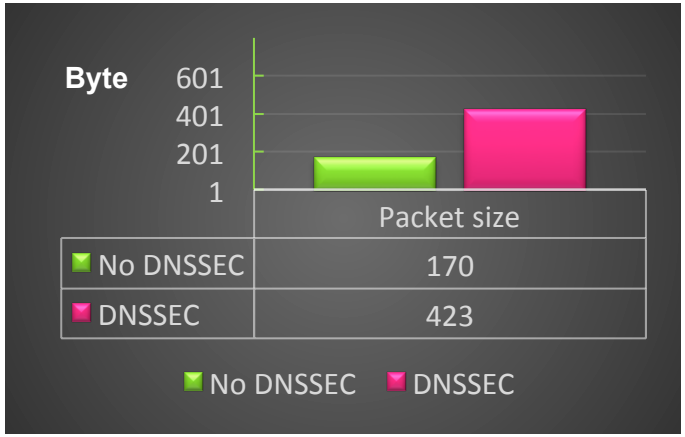


Monitoring and Observations

Observations

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

- **70%** DNSSEC query in usual
- After sub-domain and recursive nameservers having been implemented DNSSEC, bandwidth costs will be **much larger**

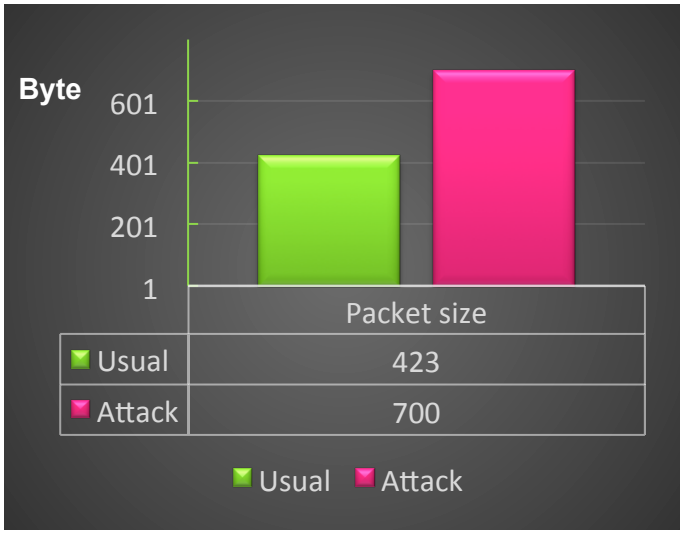


Monitoring and Observations

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)?*

中国信息社会重要的基础设施建设者、运行者和管理者

北京市海淀区中关村南四街四号中科院软件园 邮编: 100190

www.cnnic.cn