MINISTRY OF INFORMATION AND COMUNICATIONS
VIETNAM INTERNET NETWORK INFORMATION CENTER

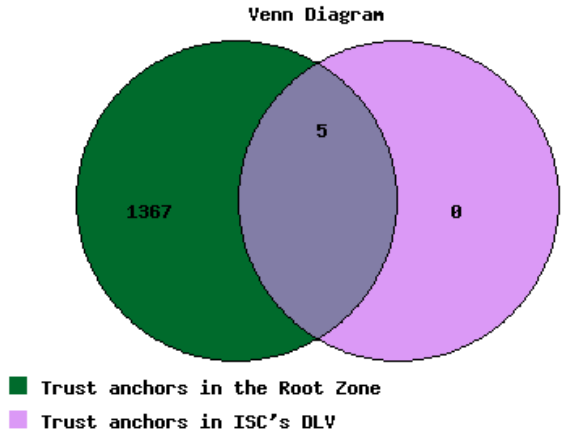
DNSSEC Deployment for .VN

Nguyen Trung Kien | Ho Chi Minh City | Feb 2017

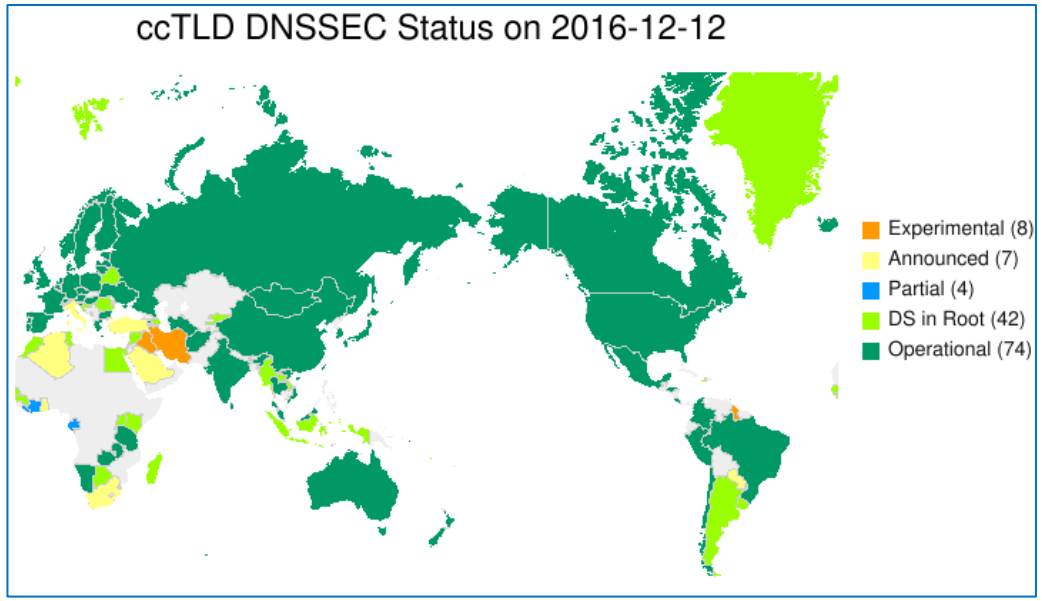
- Overview
- Preparations
- Deployment
- Next Plan

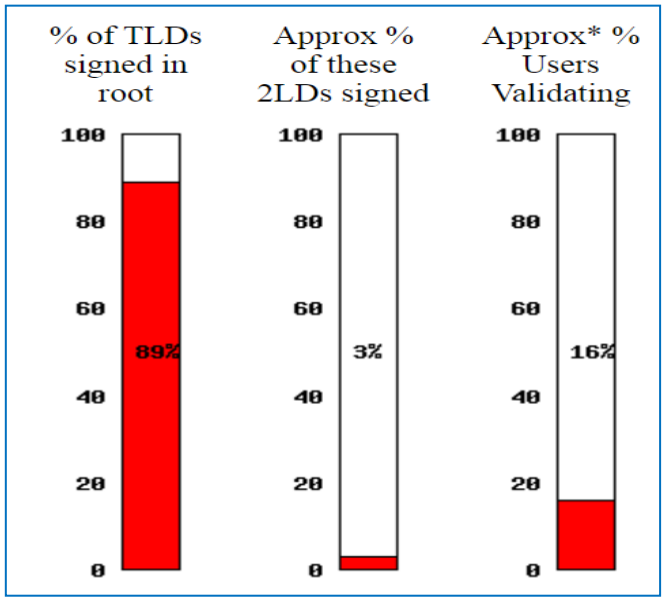
Current Status for DNSSEC Deployment

- For TLDs (24 Jan 2017):
  - 1528 TLDs in the root zone in total
  - 1383 TLDs are signed (~ 90%)

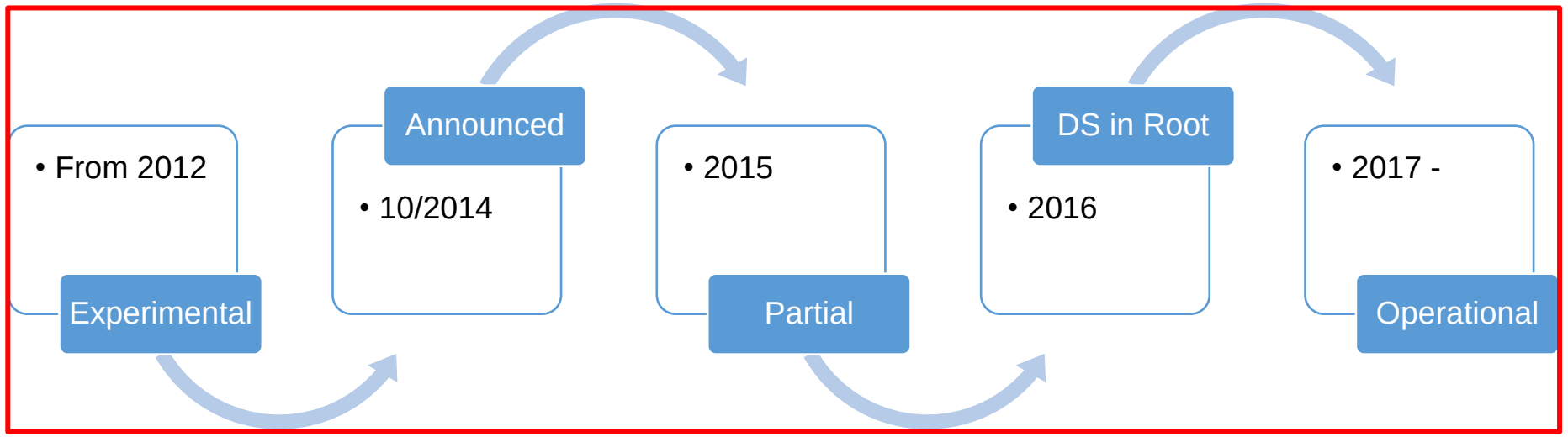


- For ccTLDs:





DNSSEC in Vietnam



1. Experimental:
- ❑ Attended the forum, conference
- ❑ Research for DNSSEC

2. Announced:
- ❑ DNSSEC OT&E
- ❑ Training

3. Partial
- ❑ Signing & Roller Key
- ❑ Tools & software development

4. DS in Root:
- ❑ Generation & submission
- ❑ Monitoring

5. Operational:
- ❑ Support to deploy DNSSEC
- ❑ Upgrades and improvements
- ❑ Debugging


Preparations

DNSSEC Plan

2015

- **Preparation**
  - Planning
  - Preparing human and technical resources
  - Promote co-operate activities, training
  - Policy, procedure, process

2016

- **Implementation**
  - Key generation & zone signing for .VN
  - .VN zone is signed & DS has been published to DNS ROOT
  - Continue promotion activities, training

2017

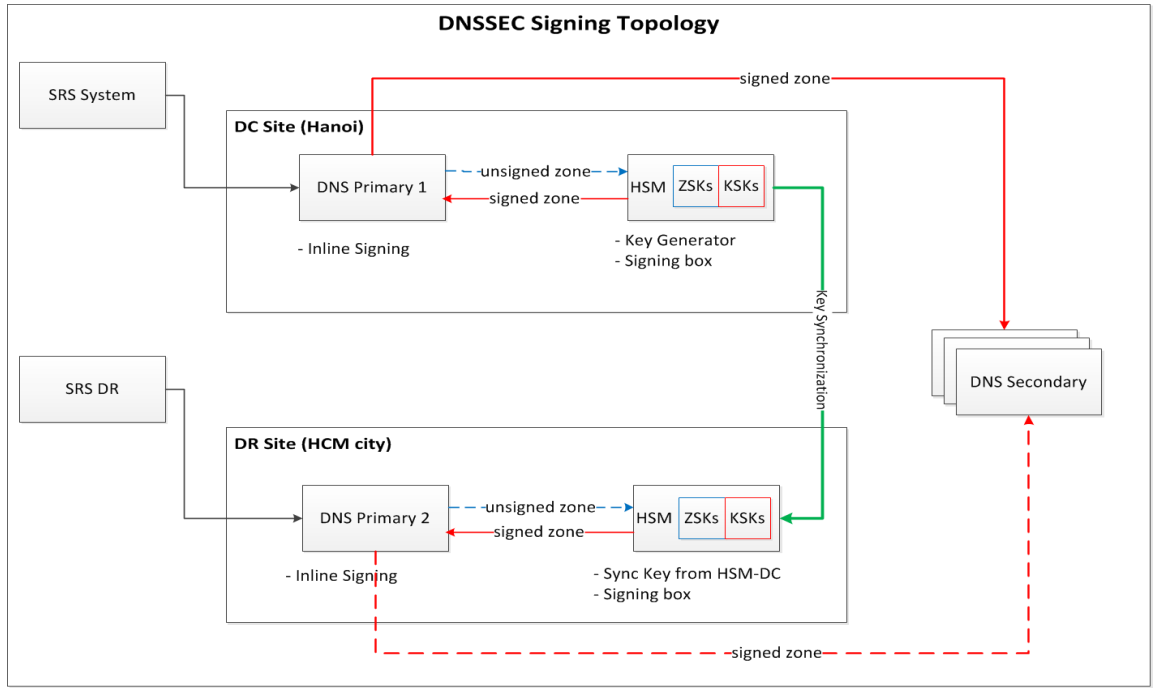
- **Accomplishment**
  - Upgrade SRS to support EPP
  - ISP, Registrar, DNS Owner in Vietnam

DNSSEC in 2016

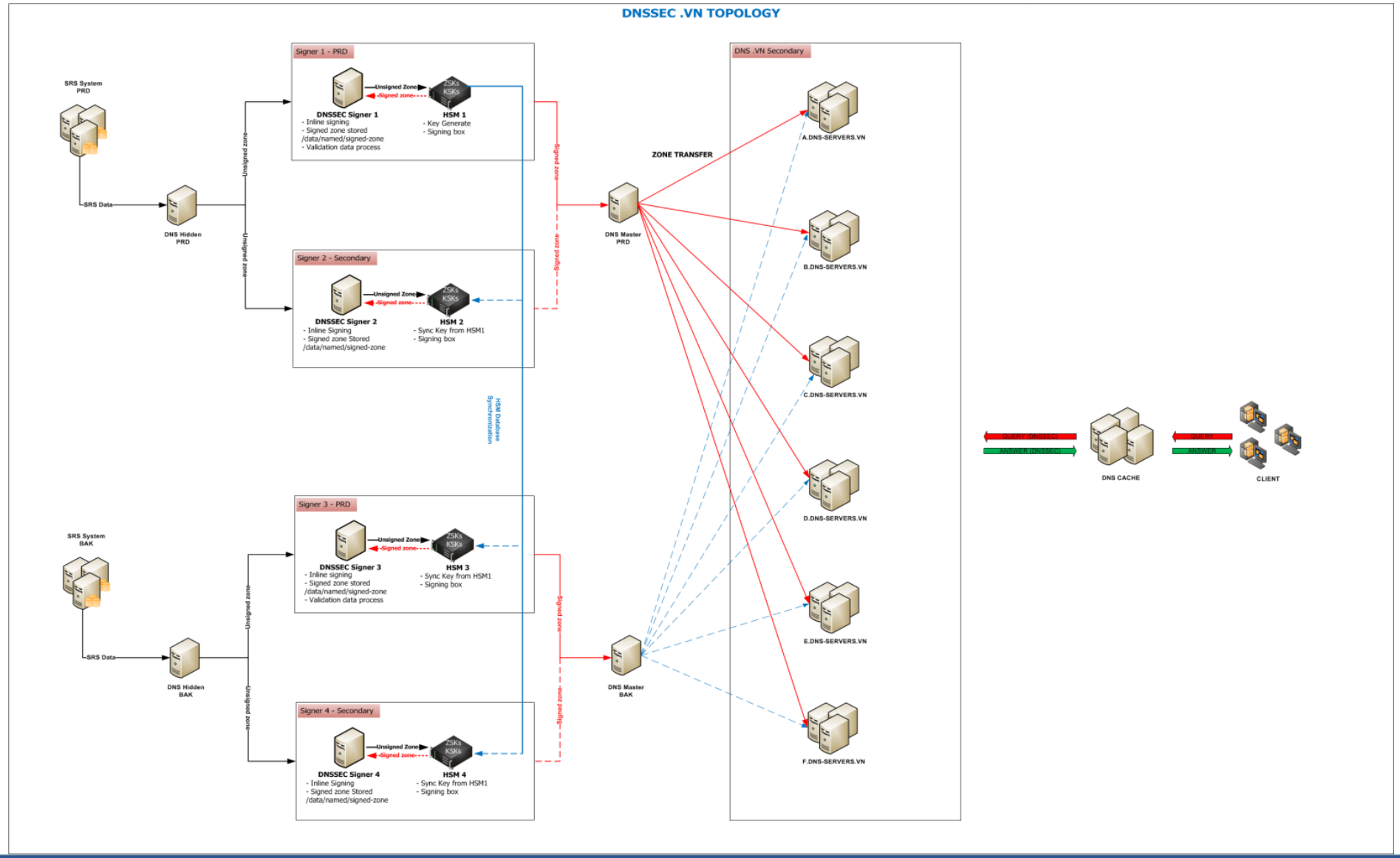
No.	Tasks
1	DNSSEC Plan for .VN domain name
2	Established DNSSEC team & Training skills
3	Infrastructure for DNSSEC: - Topology: DC/DR - DNSSEC System: DNS/DNSSEC server & HSM
4	DNSSEC documents & DPS
5	DNSSEC Production for VN zone: - DNS & HSM Integrated - Inline-signing bump in the wire - DNSSEC Monitoring
6	SRS-EPP OTE support DNSSEC
7	Key signing ceremony scripts
8	Signing VN zone & update DS to root

Topology

- Resilient: built with DC and DR (HN & HCM city)
  - Active – stanby, each site serve as a backup to the other.
  - Each site contains two independent instances of equipment which is able to sign the .VN zone
- Policy:
  - Private keys are stored in HSM
  - Public keys are stored in zone data (DNSKEY record), publish to the community
- Roles for signing key operator:
  - KGA (Key Generation Administrator)
  - SA (System Administrator)
  - SO (Security Officer)
  - WI (Witness)
- Activities:
  - Key generation (KSK, ZSK)
  - Key rollover (KSK, ZSK)
  - Key revocation (KSK, ZSK)



Topology (cont.)



Security Area

1. Security Area 3

- Network Operations Center (NOC)
- Authentication: Fingerprint, SmartCard

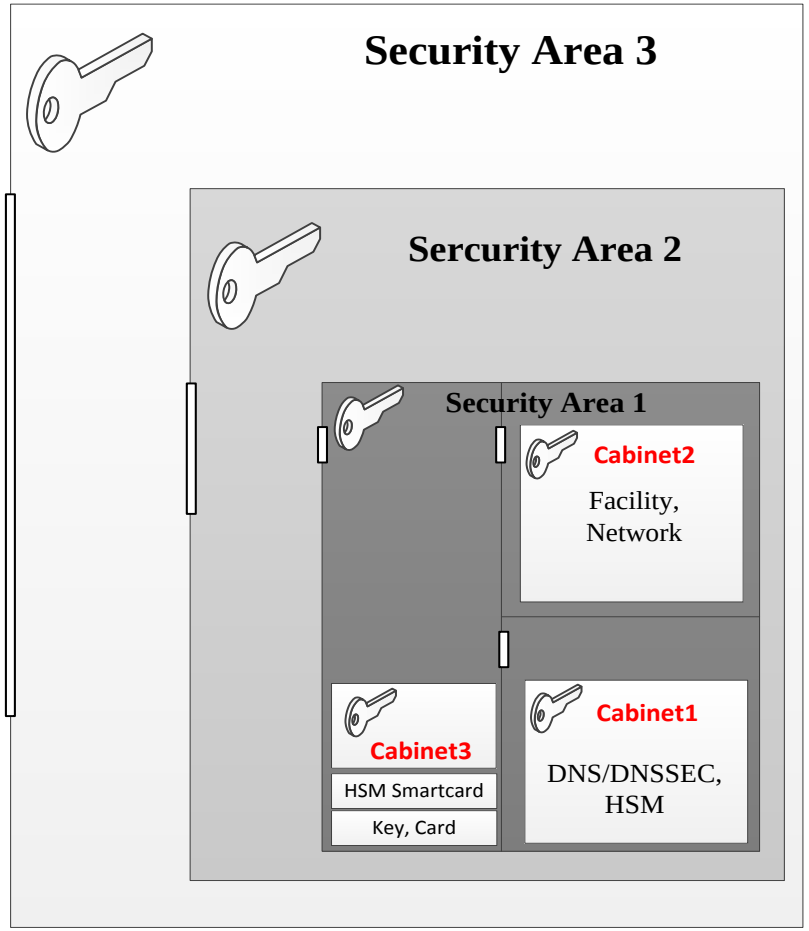
2. Security Area 2

- Server Room
- Authentication: SmartCard

3. Security Area 1

- DNSSEC Cage:
  - Cabinet 3: KGA, SA, SO access
  - Cabinet 2: SA (Facility, Network) access
  - Cabinet 1: SA (DNS, HSM), SO access

- Authentication: Fingerprint, Password



Key Parameters

KSK:

- Private/Public Key pair
- Key Algorithm: RSA/SHA-256
- Key size: 2048
- Manual rollover

ZSK:

- Private/Public Key pair
- Key Algorithm: RSA/SHA 256
- Key size: 1024
- Automatic rollover

Key Type	Funcition	Algorithm	Key length	NSEC/NSEC3
KSK	Sign DNSKEY	RSA-SHA256	2048 bits	NSEC3
ZSK	Sign RRSET		1024 bits	

Key Type	Key Rollover	Signing Validity	Refresh Time
KSK	12 months		
ZSK	90 days	30 days	7.5 days

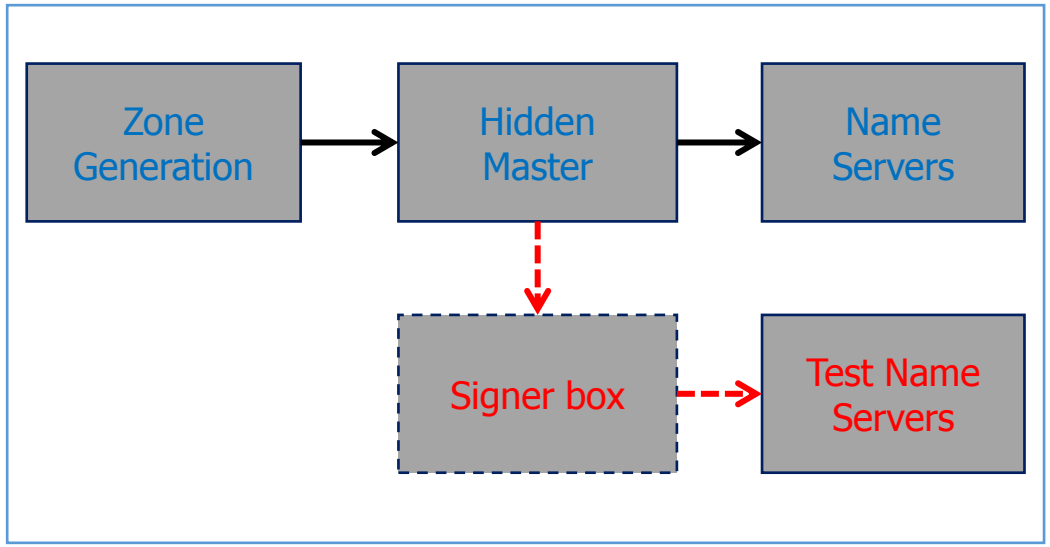
Key Generation & Rollover

- Key Generation:
  - HSM Master gererate and store new KSK, ZSK
  - HSM Master synchonize the key to other HSM (Manual synchonize)
  - DNSSEC Signer loads key label from HSM (only private key)
  - DNSSEC Signer config the DNSSEC keys, HSM will use private key to sign data.
  - Update DS to the parent zone (only with KSK generation)
  - Require a KGA, SA, SO, WI
- Key Rollover:
  - ZSK Rollover: Pre-Publish; KSK Rollover: Double Signing
  - Time to rollover:
    - KSK: 30 days before key expires.
    - ZSK: 2 days before key expires.
  - Procedure:
    - ZSK: Automatic rollover – by script.
    - KSK: Manual rollover – key signing ceremony + update DS to parent zone.


Deployment

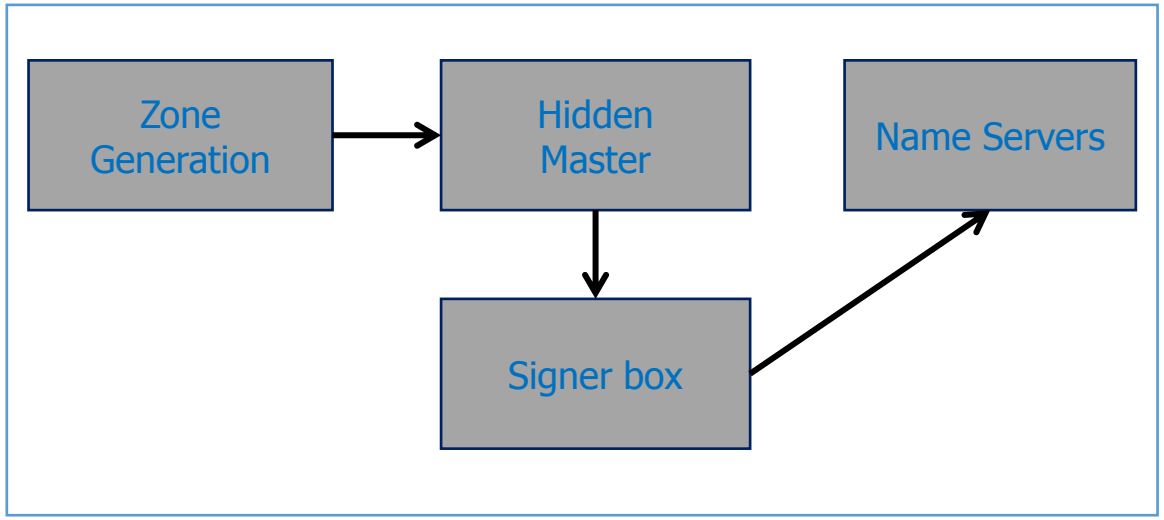
Zone Signing

- We deployed a new DNSSEC Production system:
  - New DNSSEC Hidden/Master
  - Zone transfer from DNS Hidden/Master to DNSSEC Hidden/Master
- Zone signing VN zone on DNSSEC production:
  - DC-DR model.
  - Signing with HSM Cluster (4 DNSSEC Signer/HSM)
- DNS services (without DNSSEC) on-line for resolving, DNSSEC services off-line for trial operation



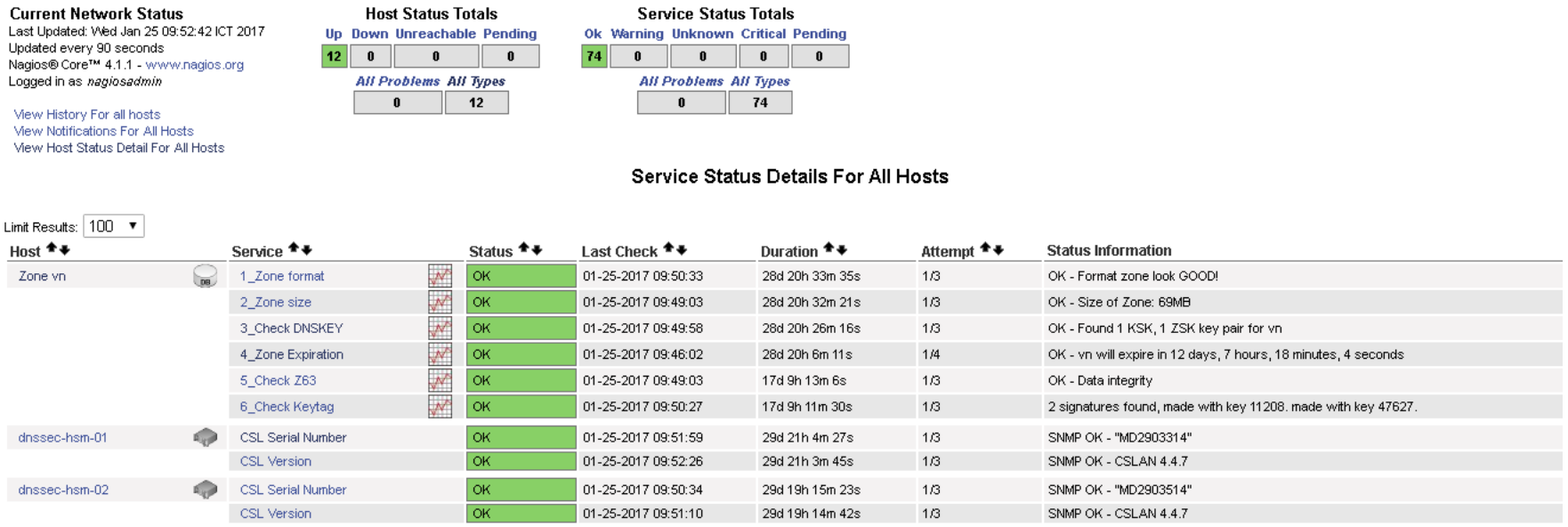
DNSSEC Online

- Key Signing Ceremony for VN zone (20 Dec 2016):
  - Internal Ceremony in VNNIC
  - Key Generation for VN zone (KSKs, ZSKs)
- Change DNS Master to DNSSEC master to publish vn signed zone.
- Check DNS Secondary after zone transfer vn signed zone (only for 5 minutes)
- Passed IANA's validation for DS Record of .VN
- DS for .VN becomes effective in 31 Dec 2016 in the root zone



DNSSEC Monitoring

- Use Nagios for monitor DNSSEC system
- Monitoring:
  - Zone size
  - Signature Expiry
  - Zone signing process
  - KSK, ZSK parameters



Current Network Status
Last Updated: Wed Jan 25 09:52:42 ICT 2017
Updated every 90 seconds
Nagios® Core™ 4.1.1 - www.nagios.org
Logged in as *nagiosadmin*

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
12	0	0	0

All Problems	All Types
0	12

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
74	0	0	0	0

All Problems	All Types
0	74

Service Status Details For All Hosts

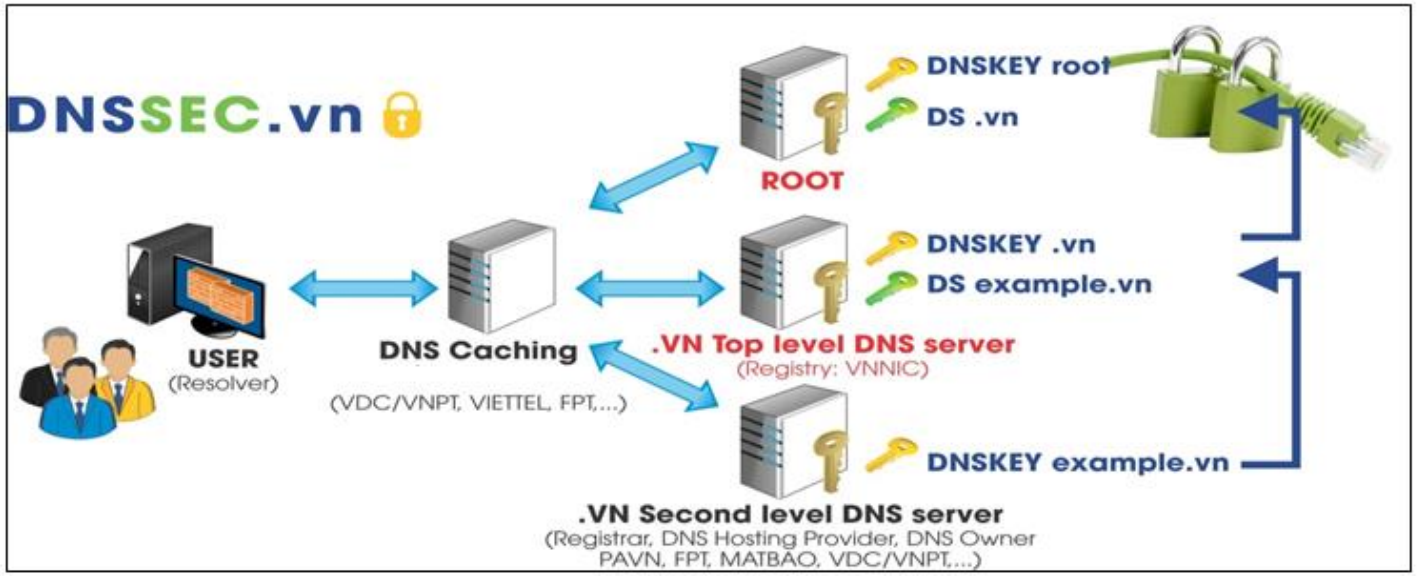
Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Zone vn	1_Zone format	OK	01-25-2017 09:50:33	28d 20h 33m 35s	1/3	OK - Format zone look GOOD!
	2_Zone size	OK	01-25-2017 09:49:03	28d 20h 32m 21s	1/3	OK - Size of Zone: 69MB
	3_Check DNSKEY	OK	01-25-2017 09:49:58	28d 20h 26m 16s	1/3	OK - Found 1 KSK, 1 ZSK key pair for vn
	4_Zone Expiration	OK	01-25-2017 09:46:02	28d 20h 6m 11s	1/4	OK - vn will expire in 12 days, 7 hours, 18 minutes, 4 seconds
	5_Check Z63	OK	01-25-2017 09:49:03	17d 9h 13m 6s	1/3	OK - Data integrity
	6_Check Keytag	OK	01-25-2017 09:50:27	17d 9h 11m 30s	1/3	2 signatures found, made with key 11208. made with key 47627.
dnssec-hsm-01	CSL Serial Number	OK	01-25-2017 09:51:59	29d 21h 4m 27s	1/3	SNMP OK - "MD2903314"
	CSL Version	OK	01-25-2017 09:52:26	29d 21h 3m 45s	1/3	SNMP OK - CSLAN 4.4.7
dnssec-hsm-02	CSL Serial Number	OK	01-25-2017 09:50:34	29d 19h 15m 23s	1/3	SNMP OK - "MD2903514"
	CSL Version	OK	01-25-2017 09:51:10	29d 19h 14m 42s	1/3	SNMP OK - CSLAN 4.4.7


Next Plan

DNSSEC in 2017

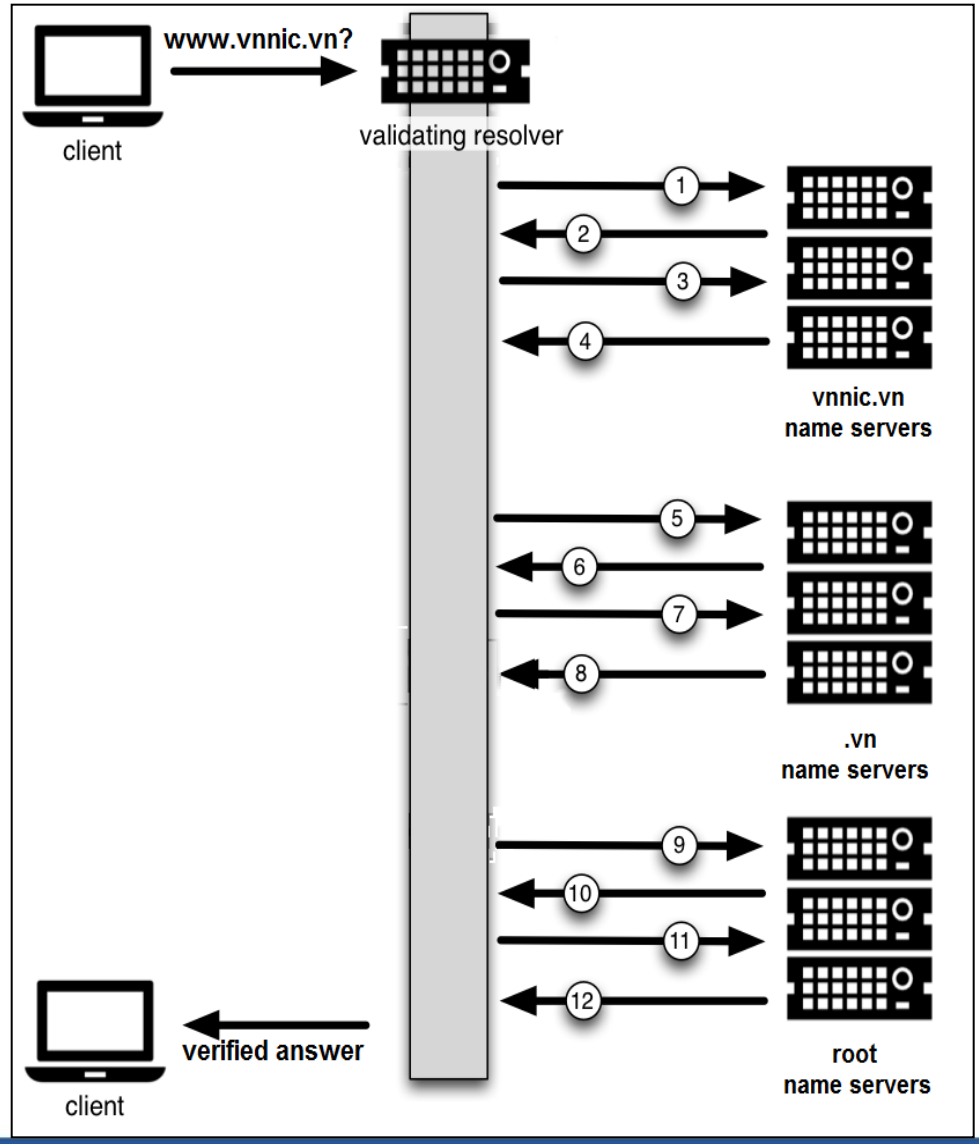
No.	Tasks
1	Sign DNSSEC for: • Sub-domain SLD, example: com.vn, net.vn, provinces domain… • Reserve domain • VNNIC's domain
2	Open testbed for Registrar to update DS
3	Support, training ISP, DNS Hosting Provider, DNS Owner to deploy DNSSEC



DNSSEC for ISPs

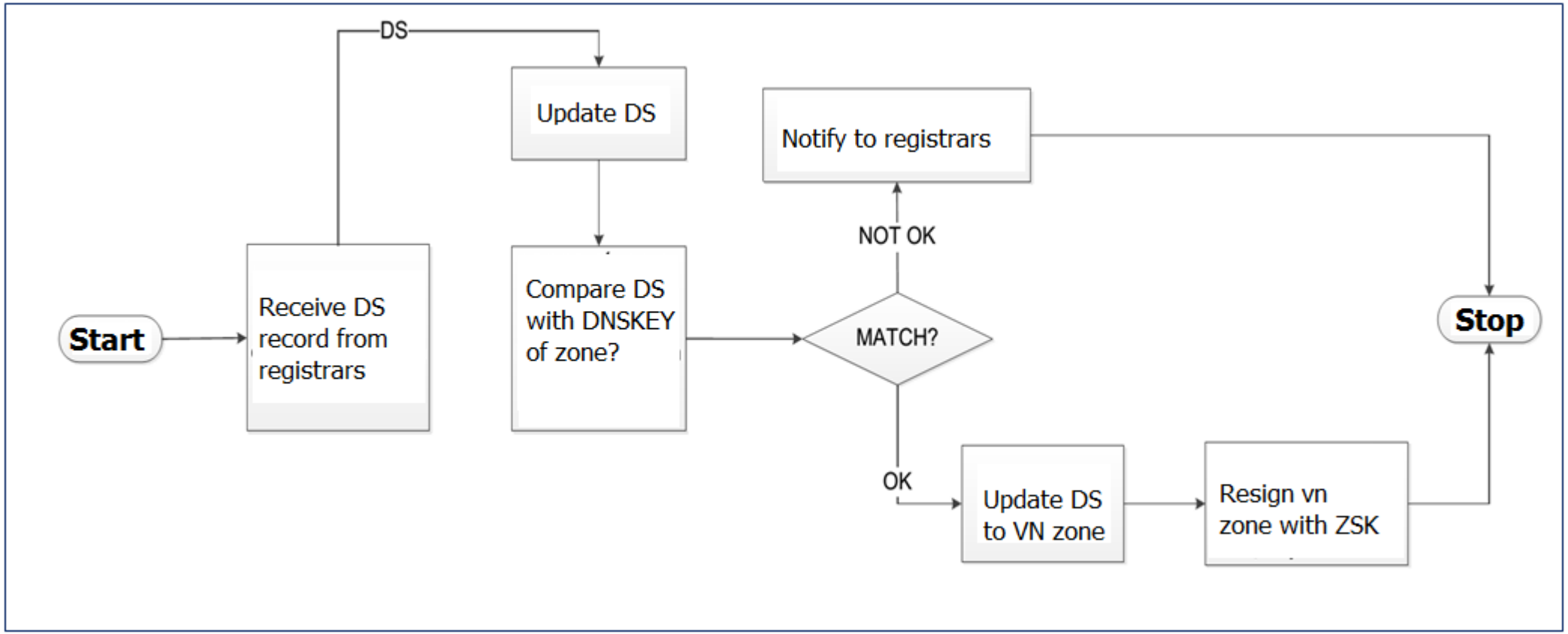
- **Network:**
  - DNSSEC adds digital signatures to DNS response packets, which often exceed 1,500 bytes → Increase Bandwidth.
  - Allow DNS query over TCP
  - Handle large UDP packets (>512 bytes, ≤4,000 bytes).

- **Pre-Deployment:**
  - Software supports DNSSEC: BIND version 9.7+, Unbound version 1.4+, Microsoft Windows Server 2012, Knot DNS 1.4.0, PowerDNS 3.0+
  - Server systems are sufficiently modern
  - Large UDP DNS packets are allowed through firewall
  - UDP fragments are not blocked by firewall



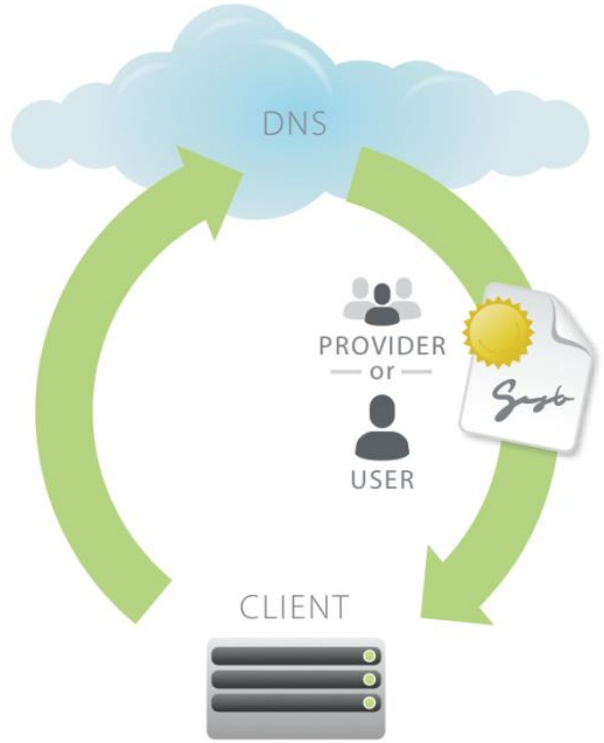
DNSSEC for Registrars

- Upgrade secdns-1.1 for EPP system for support DNSSEC.
- Connect to VNNIC's EPP system.



DNSSEC for DNS Hosting Providers

- Upgrade DNS to support DNSSEC.
- Implement Signing box
- Connect to registrar to update DS records.
- Recommendation:
  - Signing box:
    - ❑ Open Source (BIND, NSD, opendnssec, softhsm…)
    - ❑ Hardware (HSM)
  - Operation:
    - ❑ Follow policies, procedures
    - ❑ Key management (KSK, ZSK)
    - ❑ Key parameters (Algorithm, key size, NSEC/NSEC3)



Conclusion

- How to push ISP, DNS Hosting to support DNSSEC?
- Automated DS change with RFC 7344 "Automating DNSSEC Delegation Trust Maintenance"

https://tools.ietf.org/html/rfc7344

DNSSEC.vn

Thank you!