MINISTRY OF INFORMATION AND COMMUNICATIONS
VIETNAM INTERNET NETWORK INFORMATION CENTER

Lessons learned from the 2nd DNSSEC Key Rollover in .VN

DNS OARC 41
6–7, Sept 2023

Content

- DNSSEC Implementation for .VN In Brief
- 2nd DNSSEC Key Rollover in .vn
- Lessons Learned
- Some Issues
- Q&A

DNSSEC Implementation for .VN In Brief

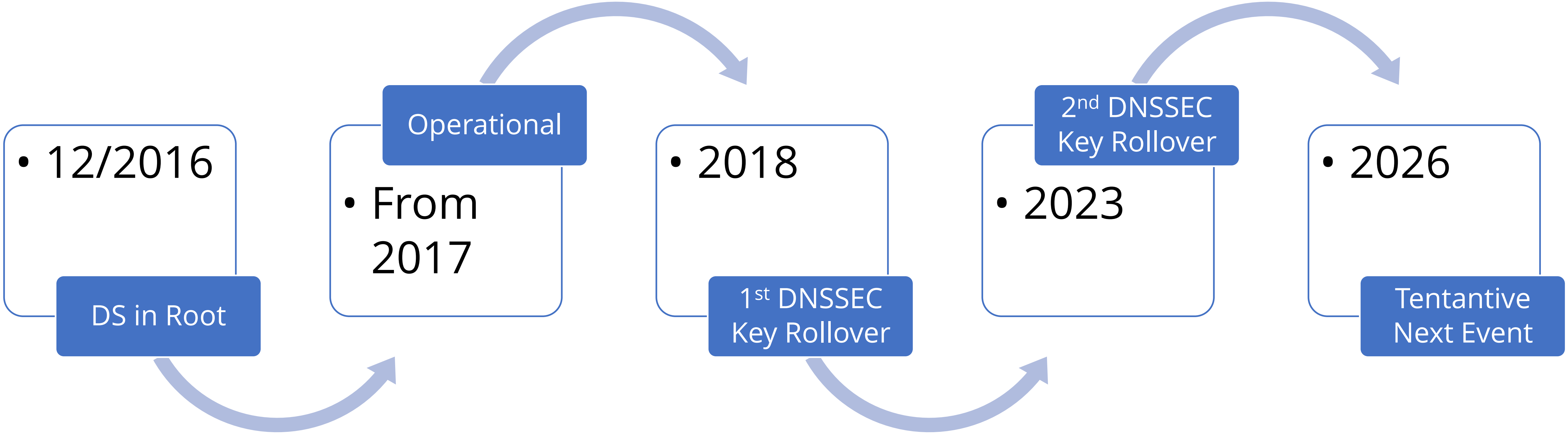
Brief Recap

- **DNSSEC Planning**
  - **23Oct, 2014:** The Minister of Information and Communication approved the project of DNSSEC deployment for .VN domain name

2015
2016
2017

- Phase 1: Preparation (2015)
  - Planning
  - Preparing human and technical resources
  - Promote co-operate activities, training
  - Policy, procedure, process
- Phase 2: Implementation (2016)
  - Key generation & zone signing for .VN
  - .VN zone is signed & DS has been published to DNS ROOT
  - Continue promotion activities, training
- Phase 3: Accomplishment (2017)
  - Upgrade SRS to support EPP
  - ISP, Registrar, DNS Owner in Vietnam

DNSSEC deployment schedule



- 12/2016

DS in Root

- From 2017

Operational

- 2018

1st DNSSEC Key Rollover

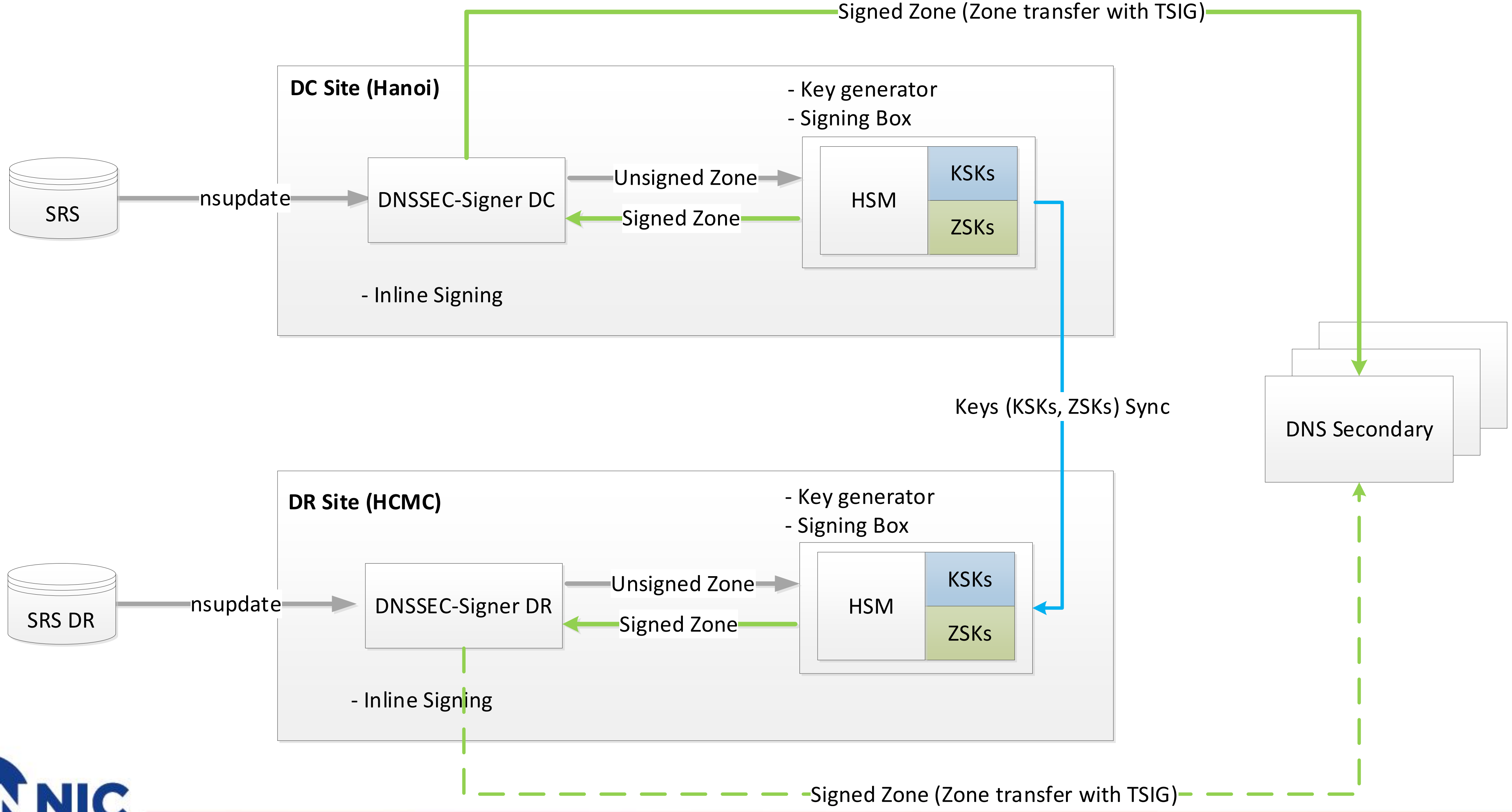
- 2023

2nd DNSSEC Key Rollover

- 2026

Tentantive Next Event

DNSSEC Architecture



vn geographical names

1st DNSSEC Key Rollover Recap

- All key pairs are generated & stored private key in HSM
  - Resilient: built with DC and DR (HN & HCM city)
  - Inline Signing: Bump in the wire (use BIND & HSM)
  - Separations of roles:
    - System Administrator (SA)
    - Security Officer (SO)
    - Witness (WI)

- 03/2018: DNSSKEC Key Rollover for zone .VN (signed in 2016)
- The first signing DNSSEC for
  - 13 generic second-level domain under .vn (com.vn, net.vn, gov.vn,…)
  - and 63 zones SLD geographical domain name under .vn (hanoi.vn, nghean.vn,…)

KSKs & ZSKs

- Key Algorithm & Key length

Key Type	Alg	Key length	NSEC/NSEC3
KSK	RSA-SHA256	2048 bits	NSEC3 opt-out
ZSK	RSA-SHA256	1024 bits	NSEC3 opt-out

- Key Timing
  - ZSK:
    - Pre-publish
    - ZSK Key Rollover: every 3 months
  - KSK
    - Double-signing
    - KSK Key Rollover: N/A

2nd DNSSEC Key Rollover in .vn

2nd DNSSEC Key Rollover Overview

- DNSSEC procedures
- Key Management
- Key Rollover
- Signing software

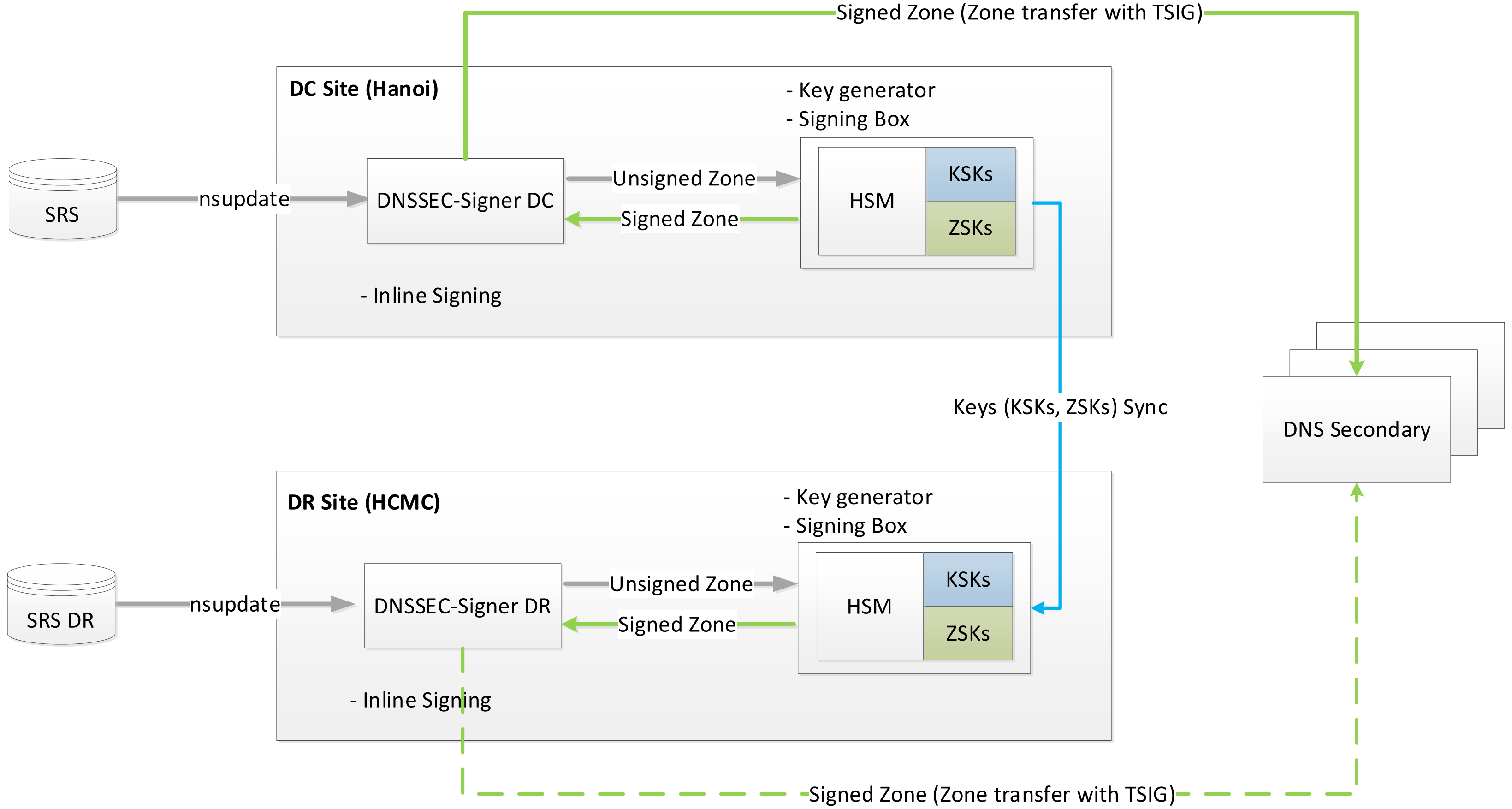
DNSSEC procedures

- Signer switch
- HSM Initialization/ upgraded
- DNSSEC Signer Initialization/ upgraded

- New Key Generation
- SLD ZSK rollover
- SLD KSK rollover
- .vn ZSK rollover
- .vn KSK rollover
- Key Backup
- Key Restore
- Monitoring

Signer switch

- Two signers, one active, one in standby
- Preparing for the uprading of HSM & DNSSEC Signer at DC site



Initialization/ upgraded

- **DNSSEC Signer**
  - Documented procedure
  - Upgrading DNSSEC Signer (OS, BIND9)
  - Ensure DNSSEC Signer can connect to HSM with Native PKCS#11
- **HSM**
  - Documented procedure
  - Upgrading HSM to latest firmware version
  - Ensure HSM can load old keys

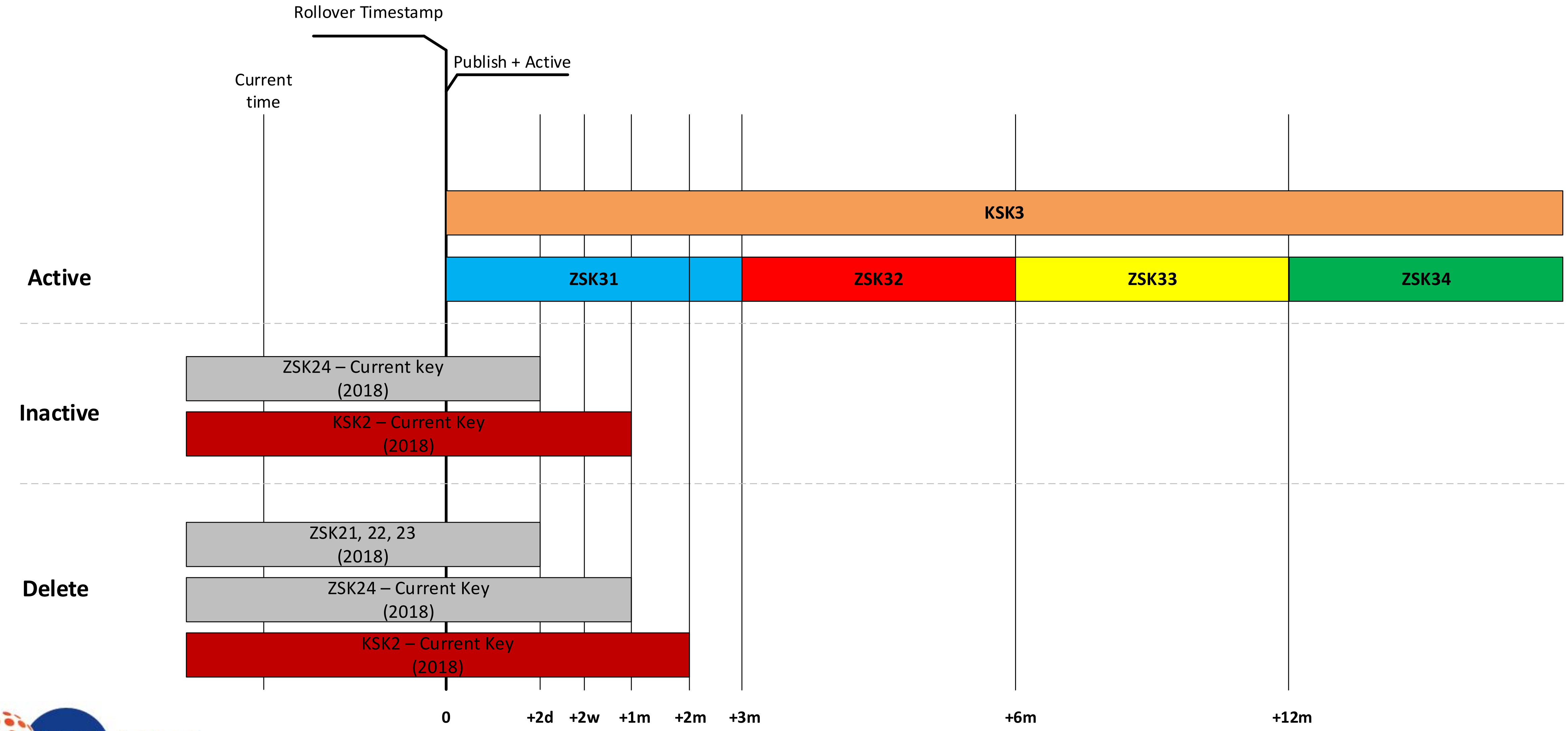
New Key Generation

- Generate all needed keys for 12 months: KSK, ZSK, .vn, SLD (using script run automatically)
- Multi-person control
  - *5-of-7 SmartCard required to generate, backup, and restore keys*
- Ensure private keys use the correct exponent
- Ensure keys are the size according to policy
  - *KSK: RSA 2048-bits*
  - *ZSK: RSA 1024-bits*
- Ensure the number of each key pair is generated
  - *4 Key pairs ZSK/zone*
  - *1 Key pairs KSK/zone*

SLD & .vn ZSK & KSK rollover

- New key is introduced automatically by BIND9 (signing with HSM via Native PKCS#11)
- ZSK & KSK Rollover Methods for SLD & .vn domains
  - ZSK:
    - Double Signature: for the first new key
    - Pre-publication:
  - KSK:
    - Double-KSK
- Timeline

Timeline

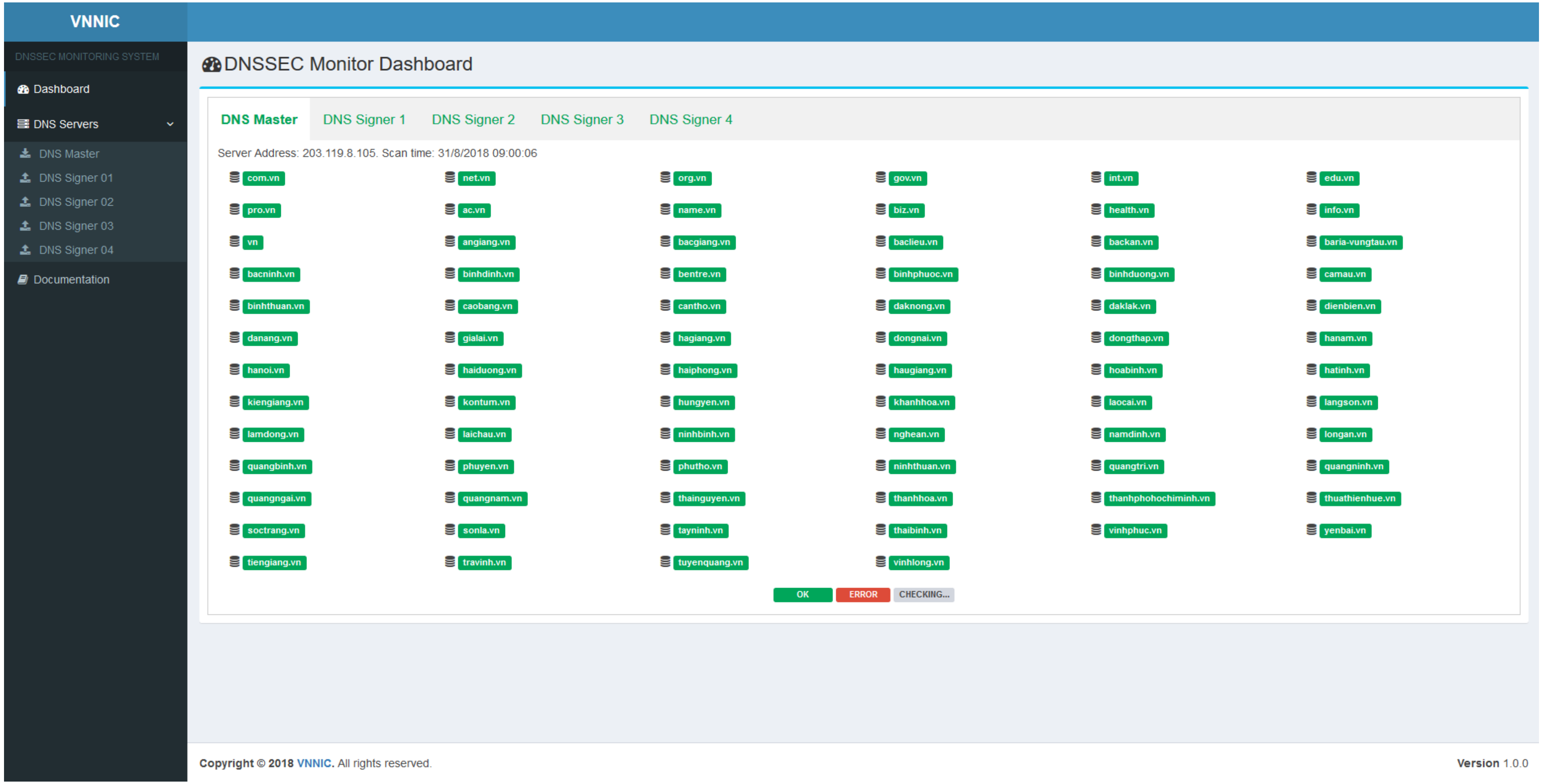

Rollover Timestamp
Publish + Active
Current time
Active
KSK3
ZSK31
ZSK32
ZSK33
ZSK34
Inactive
ZSK24 – Current key (2018)
KSK2 – Current Key (2018)
Delete
ZSK21, 22, 23 (2018)
ZSK24 – Current Key (2018)
KSK2 – Current Key (2018)
0
+2d
+2w
+1m
+2m
+3m
+6m
+12m

Key Backup & Restore

- Generate an encrypted version of the Keystore for DC/DR
- Use the backup to transfer keys to the standby signer
- Generate multiple copies for different physical sites for DR purposes
- Generate and record cryptographic hash to verify integrity
- Custody of the device preserved
- Initialize keystore using Key Backup
  - *Method to synchronize keys Ensures all signers have the duplicate keys and roles*

Monitoring

- Zones status



DNSSEC Monitor Dashboard

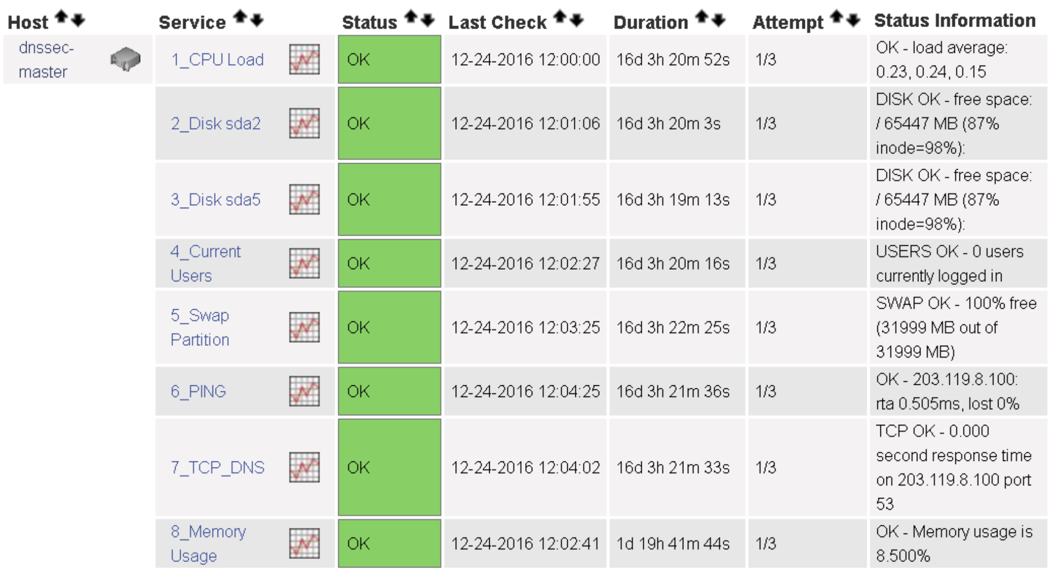
Server Address: 203.119.8.105. Scan time: 31/8/2018 09:00:06

com.vn	net.vn	org.vn	gov.vn	int.vn	edu.vn
pro.vn	ac.vn	name.vn	biz.vn	health.vn	info.vn
vn	angiang.vn	bacgiang.vn	baclieu.vn	backan.vn	baria-vungtau.vn
bacninh.vn	binhdinh.vn	bentre.vn	binhphuoc.vn	binhduong.vn	camau.vn
binhthuan.vn	caobang.vn	cantho.vn	daknong.vn	daklak.vn	dienbien.vn
danang.vn	gialai.vn	hagiang.vn	dongnai.vn	dongthap.vn	hanam.vn
hanoi.vn	haiduong.vn	haiphong.vn	haugiang.vn	hoabinh.vn	hatinh.vn
kiengiang.vn	kontum.vn	hungyen.vn	khanhhoa.vn	laocai.vn	langson.vn
lamdong.vn	laichau.vn	ninhbinh.vn	nghean.vn	namdinh.vn	longan.vn
quangbinh.vn	phuyen.vn	phutho.vn	ninhthuan.vn	quangtri.vn	quangninh.vn
quangngai.vn	quangnam.vn	thainguyen.vn	thanhhoa.vn	thanhphohochiminh.vn	thuathienhue.vn
soctrang.vn	sonla.vn	tayninh.vn	thaibinh.vn	vinhphuc.vn	yenbai.vn
tiengiang.vn	travinh.vn	tuyenquang.vn	vinhlong.vn		

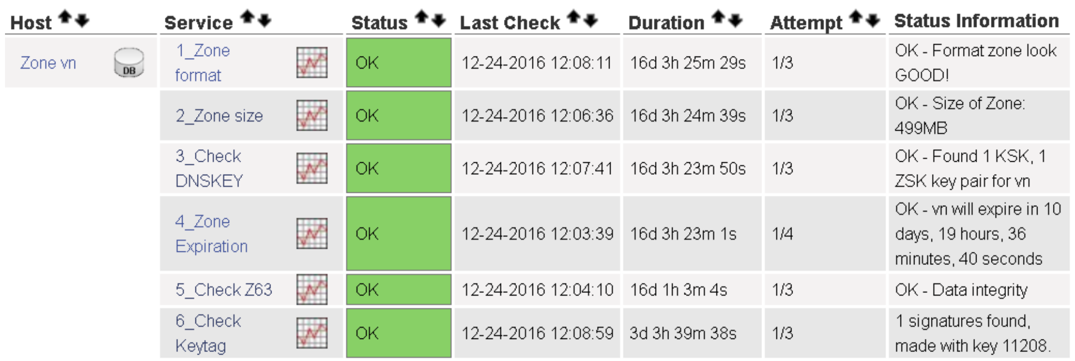
Copyright © 2018 VNNIC. All rights reserved.

Version 1.0.0

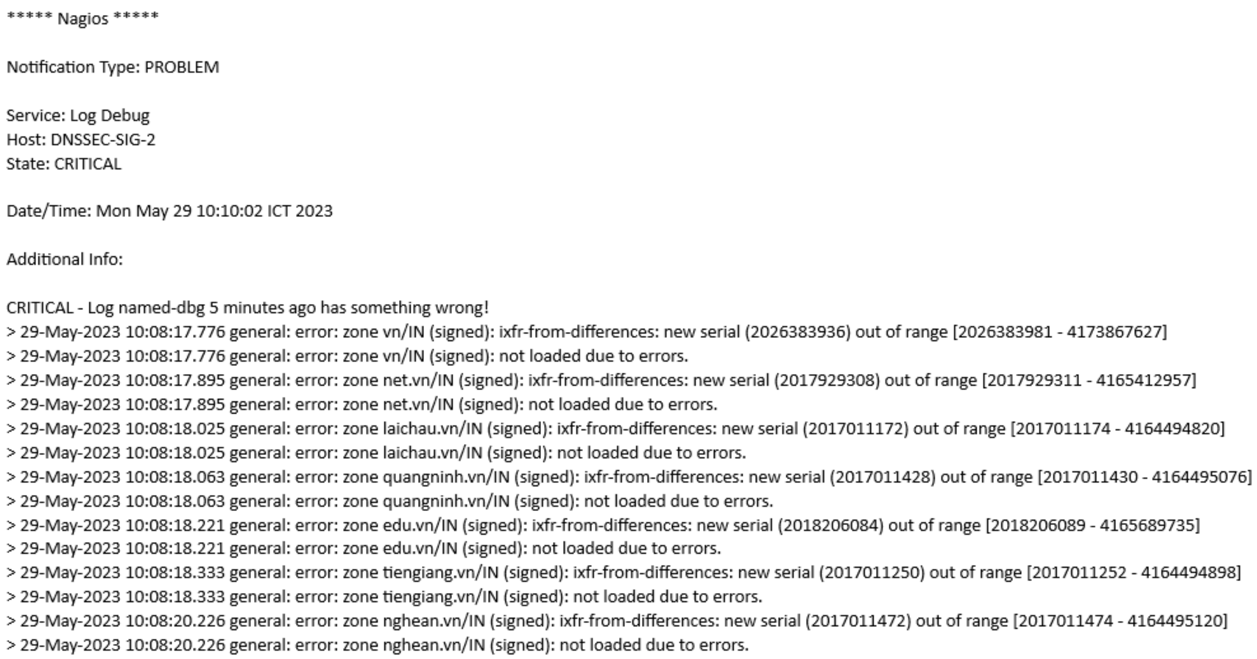
Monitoring



Host	Service	Status	Last Check	Duration	Attempt	Status Information
dnssec-master	1_CPU Load	OK	12-24-2016 12:00:00	16d 3h 20m 52s	1/3	OK - load average: 0.23, 0.24, 0.15
	2_Disk sda2	OK	12-24-2016 12:01:06	16d 3h 20m 3s	1/3	DISK OK - free space: / 65447 MB (87% inode=98%):
	3_Disk sda5	OK	12-24-2016 12:01:55	16d 3h 19m 13s	1/3	DISK OK - free space: / 65447 MB (87% inode=98%):
	4_Current Users	OK	12-24-2016 12:02:27	16d 3h 20m 16s	1/3	USERS OK - 0 users currently logged in
	5_Swap Partition	OK	12-24-2016 12:03:25	16d 3h 22m 25s	1/3	SWAP OK - 100% free (31999 MB out of 31999 MB)
	6_PING	OK	12-24-2016 12:04:25	16d 3h 21m 36s	1/3	OK - 203.119.8.100: rta 0.505ms, lost 0%
	7_TCP_DNS	OK	12-24-2016 12:04:02	16d 3h 21m 33s	1/3	TCP OK - 0.000 second response time on 203.119.8.100 port 53
	8_Memory Usage	OK	12-24-2016 12:02:41	1d 19h 41m 44s	1/3	OK - Memory usage is 8.500%



Host	Service	Status	Last Check	Duration	Attempt	Status Information
Zone vn	1_Zone format	OK	12-24-2016 12:08:11	16d 3h 25m 29s	1/3	OK - Format zone look GOOD!
	2_Zone size	OK	12-24-2016 12:06:36	16d 3h 24m 39s	1/3	OK - Size of Zone: 499MB
	3_Check DNSKEY	OK	12-24-2016 12:07:41	16d 3h 23m 50s	1/3	OK - Found 1 KSK, 1 ZSK key pair for vn
	4_Zone Expiration	OK	12-24-2016 12:03:39	16d 3h 23m 1s	1/4	OK - vn will expire in 10 days, 19 hours, 36 minutes, 40 seconds
	5_Check Z63	OK	12-24-2016 12:04:10	16d 1h 3m 4s	1/3	OK - Data integrity
	6_Check Keytag	OK	12-24-2016 12:08:59	3d 3h 39m 38s	1/3	1 signatures found, made with key 11208.

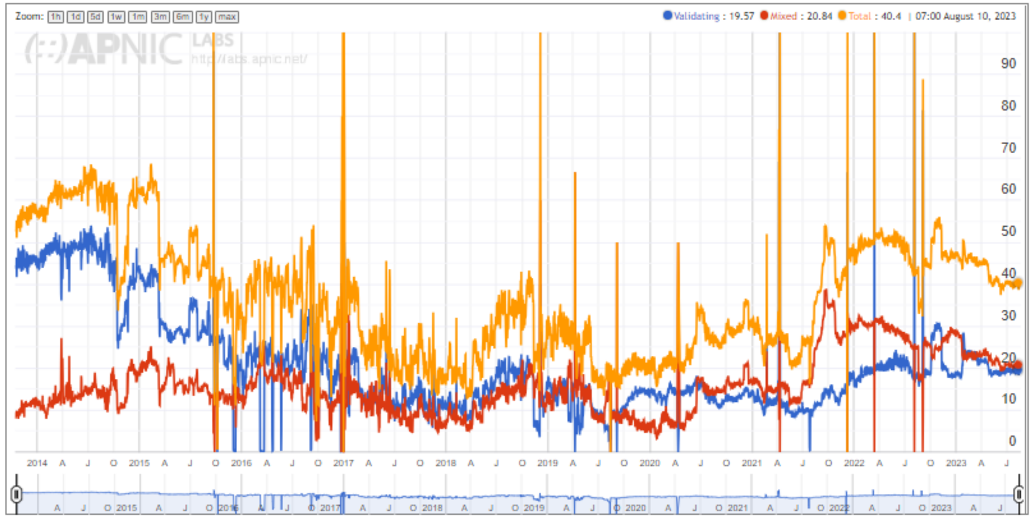


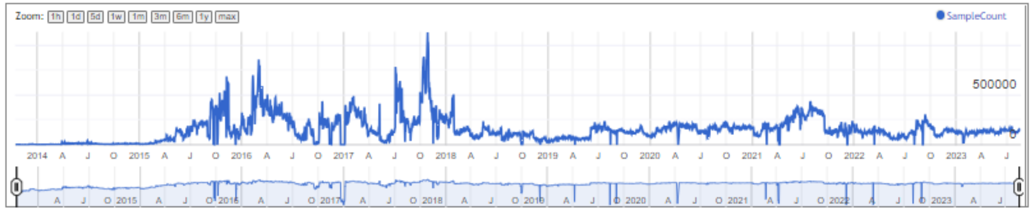
```
***** Nagios *****

Notification Type: PROBLEM

Service: Log Debug
Host: DNSSEC-SIG-2
State: CRITICAL

Date/Time: Mon May 29 10:10:02 ICT 2023

Additional Info:

CRITICAL - Log named-dbg 5 minutes ago has something wrong!
> 29-May-2023 10:08:17.776 general: error: zone vn/IN (signed): ixfr-from-differences: new serial (2026383936) out of range [2026383981 - 4173867627]
> 29-May-2023 10:08:17.776 general: error: zone vn/IN (signed): not loaded due to errors.
> 29-May-2023 10:08:17.895 general: error: zone net.vn/IN (signed): ixfr-from-differences: new serial (2017929308) out of range [2017929311 - 4165412957]
> 29-May-2023 10:08:17.895 general: error: zone net.vn/IN (signed): not loaded due to errors.
> 29-May-2023 10:08:18.025 general: error: zone laichau.vn/IN (signed): ixfr-from-differences: new serial (2017011172) out of range [2017011174 - 4164494820]
> 29-May-2023 10:08:18.025 general: error: zone laichau.vn/IN (signed): not loaded due to errors.
> 29-May-2023 10:08:18.063 general: error: zone quangninh.vn/IN (signed): ixfr-from-differences: new serial (2017011428) out of range [2017011430 - 4164495076]
> 29-May-2023 10:08:18.063 general: error: zone quangninh.vn/IN (signed): not loaded due to errors.
> 29-May-2023 10:08:18.221 general: error: zone edu.vn/IN (signed): ixfr-from-differences: new serial (2018206084) out of range [2018206089 - 4165689735]
> 29-May-2023 10:08:18.221 general: error: zone edu.vn/IN (signed): not loaded due to errors.
> 29-May-2023 10:08:18.333 general: error: zone tiengiang.vn/IN (signed): ixfr-from-differences: new serial (2017011250) out of range [2017011252 - 4164494898]
> 29-May-2023 10:08:18.333 general: error: zone tiengiang.vn/IN (signed): not loaded due to errors.
> 29-May-2023 10:08:20.226 general: error: zone nghean.vn/IN (signed): ixfr-from-differences: new serial (2017011472) out of range [2017011474 - 4164495120]
> 29-May-2023 10:08:20.226 general: error: zone nghean.vn/IN (signed): not loaded due to errors.
```

Signed domains

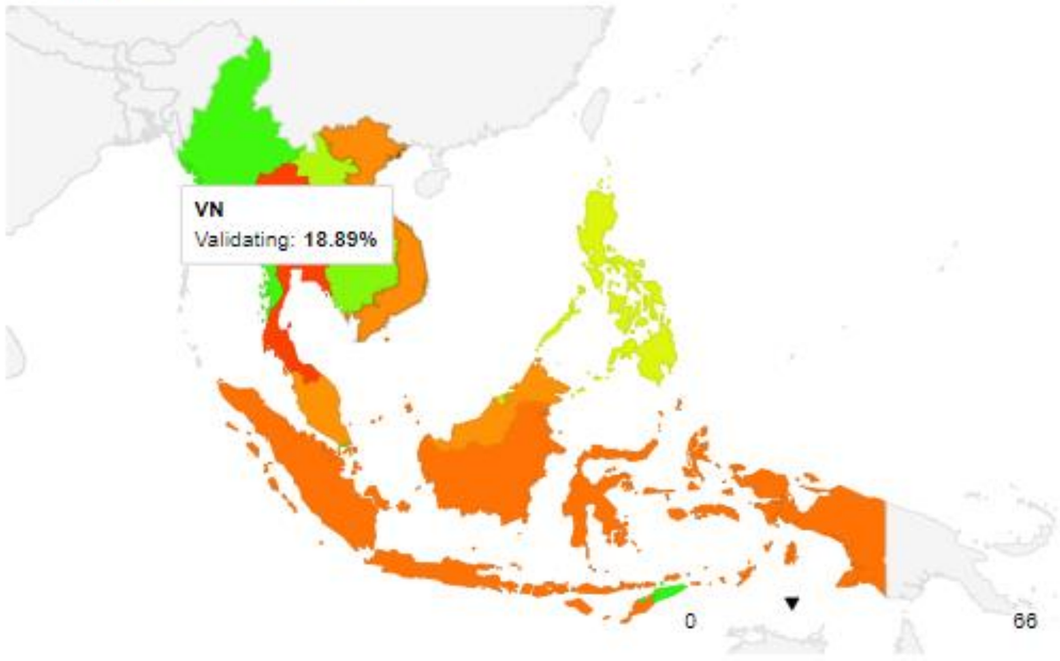
- > 7000 of .vn names are now DNSSEC signed
- DNSSEC validation

Use of DNSSEC Validation for Vietnam (VN)





Region Map for South-Eastern Asia (035)



Challenges Faced

- Double Signature: for the first new key of ZSK (fully DNSSEC signing)
  - *The DNSSEC signing process takes a considerable amount of time: it takes about 6 hours for a zone (600.000 domains)*
  - *The zone file size is significantly larger (about 5-6 times) than the original file.*

- Why Double Signature for ZSK?
  - *We generated a new key and performed the rollover simultaneously (without a dedicated prepublication phase).*

  → Do you think this is a wrong choice?

Lessons Learned

Testing and Coordination

- Is a software upgrade required?
- Can the servers handle incremental CPU load?
- Set up a monitoring regime to report errors.
- Ensure each organization provides (Registry, Registrars, ISPs,…) up-to-date POC for zone and/or security operations.
    - Who to contact when things go wrong.

Timing & DNSSEC Key Rollover methods

- Key Rollover methods
  - KSK: Double KSK ?
  - ZSK: Pre-publish ?

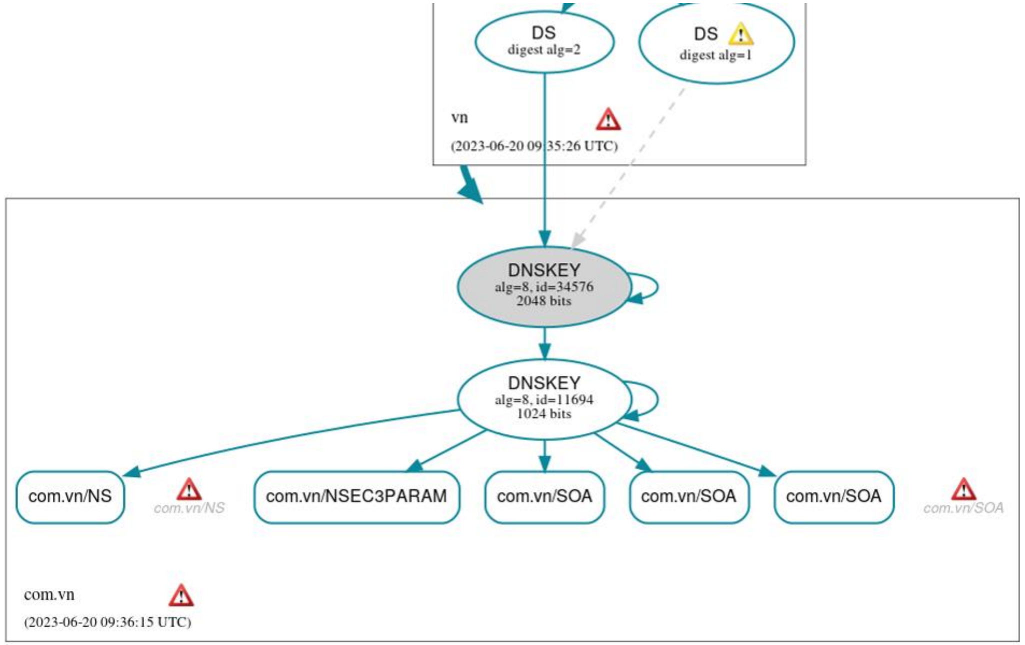
➔ *This is crucial, as even a small mistake could impact the entire DNSSEC validation process of the ccTLD.*

DNSSEC with HSM

- NTP synchronization
- Ensure the network connection between HSM & DNSSEC Signer is “stable” all the time.

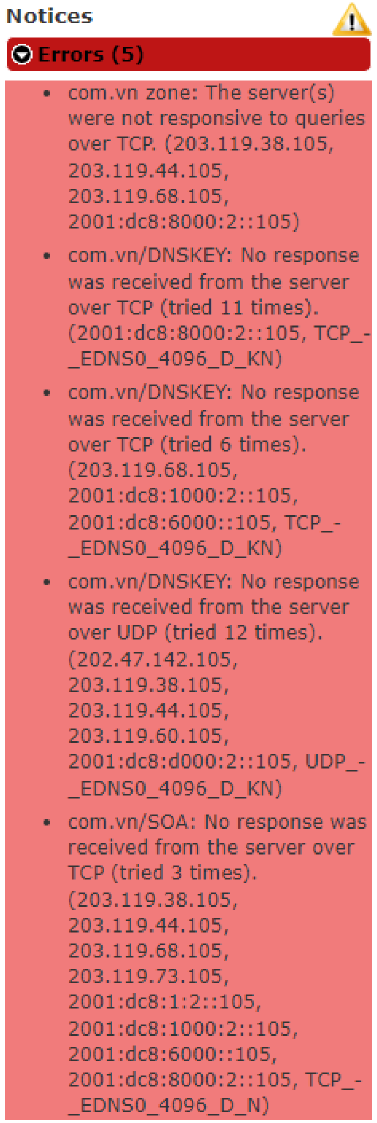
Network environment

- Ensure the network environment (Firewall,…): EDNS0 packets can pass through the firewall.
- Network equipment may need to be updated
  - Will they permit both UDP and TCP traffic on port 53?
  - Can they properly handle larger DNS responses? (with EDNS0, the response may go from 512 bytes to 4,000 bytes)
  - Can they handle fragmentation?



Issues & Problems

- The DNSSEC signing process takes a considerable amount of time when we Rollover ZSK using Double Signature method & NSEC3 opt-out
- EDNS0
- Networks environment



Notices

Errors (5)

- com.vn zone: The server(s) were not responsive to queries over TCP. (203.119.38.105, 203.119.44.105, 203.119.68.105, 2001:dc8:8000:2::105)
- com.vn/DNSKEY: No response was received from the server over TCP (tried 11 times). (2001:dc8:8000:2::105, TCP_-_EDNS0_4096_D_KN)
- com.vn/DNSKEY: No response was received from the server over TCP (tried 6 times). (203.119.68.105, 2001:dc8:1000:2::105, 2001:dc8:6000::105, TCP_-_EDNS0_4096_D_KN)
- com.vn/DNSKEY: No response was received from the server over UDP (tried 12 times). (202.47.142.105, 203.119.38.105, 203.119.44.105, 203.119.60.105, 2001:dc8:d000:2::105, UDP_-_EDNS0_4096_D_KN)
- com.vn/SOA: No response was received from the server over TCP (tried 3 times). (203.119.38.105, 203.119.44.105, 203.119.68.105, 203.119.73.105, 2001:dc8:1:2::105, 2001:dc8:1000:2::105, 2001:dc8:6000::105, 2001:dc8:8000:2::105, TCP_-_EDNS0_4096_D_N)

Questions

- Should we use NSEC3 opt-out for DNSSEC signing or not?
  - *If yes, what are the recommended DNSSEC key rollover methods for KSK and ZSK?*
- In the event of any errors during the DNSSEC Key rollover process of a ccTLD zone, what is the best rollback solution?
  - *Should we immediately request the removal of the DS record from the DNS Root?*
- Currently, many ISPs have concerns about performance issues related to their DNS systems when enabling DNSSEC validation.
  - *Does DNSSEC really impact the performance of the DNS system?*
  - *If yes, to what extent does it affect performance?*

Q&A

VNNIC
Internet for all

.vn VIET NAM'S NATIONAL DOMAIN NAME

VNIX Viet Nam National Internet eXchange

DNS National .VN Domain Name System

ASN Your Net ID

INTERNET SPEED by VNNIC

IP v4 v6 Internet Address

VNIXNOG VietNam National Internet eXchange Network Operators Group

VNNIC INTERNET CONFERENCE

VNNIC INTERNET ACADEMY

VNNIC INTERNET ATLAS

MINISTRY OF INFORMATION AND COMMUNICATIONS
VIETNAM INTERNET NETWORK INFORMATION CENTER

Headquarters: Floor 24th, VNTA Building, Duong Dinh Nghe st., Yen Hoa Ward, Cau Giay Dist., Hanoi
Da Nang Branch: Lot 21, 7th st., An Don Industry Zone, Son Tra Dist., Da Nang City
HCMC Branch: 20th St., Tan Thuan Manufacturing area, 7 Dist., Ho Chi Minh City

☎ +84 24 3556 4944 facebook.com/myVNNIC/
✉ webmaster@vnnic.vn https://vnnic.vn/

Thank you !