DNSSEC Deployment for .VN

Nguyen Trung Kien | Ho Chi Minh City | Feb 2017
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:

![Venn Diagram showing trust anchors in the root zone and IEC's BLV](image)

![ccTLD DNSSEC Status map on 2016-12-12](image)

![Graph showing % of TLDs signed in root, % of these 2LDs signed, and % Users Validating](image)
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

www.vnnic.vn
## DNSSEC in 2016

<table>
<thead>
<tr>
<th>No.</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DNSSEC Plan for .VN domain name</td>
</tr>
<tr>
<td>2</td>
<td>Established DNSSEC team &amp; Training skills</td>
</tr>
</tbody>
</table>
| 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 |
- 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)
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

<table>
<thead>
<tr>
<th>Key Type</th>
<th>Function</th>
<th>Algorithm</th>
<th>Key length</th>
<th>NSEC/NSEC3</th>
</tr>
</thead>
<tbody>
<tr>
<td>KSK</td>
<td>Sign DNSKEY</td>
<td>RSA-SHA256</td>
<td>2048 bits</td>
<td>NSEC3</td>
</tr>
<tr>
<td>ZSK</td>
<td>Sign RRSET</td>
<td></td>
<td>1024 bits</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key Type</th>
<th>Key Rollover</th>
<th>Signing Validity</th>
<th>Refresh Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>KSK</td>
<td>12 months</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ZSK</td>
<td>90 days</td>
<td>30 days</td>
<td>7.5 days</td>
</tr>
</tbody>
</table>
Key Generation & Rollover

- **Key Generation:**
  - HSM Master generate and store new KSK, ZSK
  - HSM Master synchronize the key to other HSM (Manual synchronize)
  - 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.
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
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
- Use Nagios for monitor DNSSEC system
- Monitoring:
  - Zone size
  - Signature Expiry
  - Zone signing process
  - KSK, ZSK parameters

DNSSEC Monitoring
Next Plan
## DNSSEC in 2017

<table>
<thead>
<tr>
<th>No.</th>
<th>Tasks</th>
</tr>
</thead>
</table>
| 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 |

![Diagram of DNSSEC in 2017](www.vnnic.vn)
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:
  o Signing box:
    □ Open Source (BIND, NSD,.opendnssec, softhsm...)
    □ Hardware (HSM)
  o 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”

Thank you!