DNSSEC Status & Plan in KR

Chang-Min Park
microai@kisa.or.kr
Status

- Trial: safedns.kr
- Researches: Key and Signature Policy
- Test
  - DNSSEC Tools: dnssec-tools, opendnssec, zkt
  ...
  - DNS S/W performance: NSD
Trial with “safedns.kr”

- 2006: Trial system implementation for technical verification
- 2007: Trial service(safedns.kr) with NSEC
- 2008: - (KASP researches)
- 2009: Trial service improvement
  - KR DNSSEC KASP adoption
  - NSEC-> NSEC3 transform
  - DLV adoption (ISC DLV Registry Service)
DLV Configuration

DNSSEC Look-aside Validation Registry

<table>
<thead>
<tr>
<th>Name</th>
<th>safedns.kr (delete)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>✔️ No problems were detected.</td>
</tr>
<tr>
<td>DNSKEY Records</td>
<td>2 (add)</td>
</tr>
<tr>
<td>Created</td>
<td>2009-02-26 08:58:01 UTC</td>
</tr>
<tr>
<td>Last Update</td>
<td>2009-02-26 08:58:01 UTC</td>
</tr>
</tbody>
</table>

```bash
options {
  version "unknown";
  directory "/var/named";
  dump-file "/var/named-log/cache_dump.db";
  statistics-file "/var/named-log/named_stats.txt";
  edns-udp-size 1460;
  allow-query { any; };
  dnssec-enable yes;
  dnssec-validation yes;
  dnssec-lookaside "." trust-anchor dlv.isc.org.;
  listen-on-v6 { any; };
};
```
Researches on KASP

- 2008 : research for proper values on Key and Signature information & parameters
- 2009 : KR DNSSEC KASP standard establishment (Base on RFCs)
  - 2 KSK, 3 ZSK
  - lifetime, size, rollover
  - NSEC3, opt-out
More about test

- Test with tools
  - dnssec-zkt, dnssec-tools, opendnssec
  - linux, solaris
- DNS S/W test
  - QPS, CPU, MEMORY
  - NSD Test Environment and Method
### NSD Test Result

#### NSD(Not-signed)

<table>
<thead>
<tr>
<th>Domain</th>
<th>Amount</th>
<th>Zone size</th>
<th>Signed zone size</th>
<th>nsd.db</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1M</td>
<td>32 MB</td>
<td>631 MB</td>
<td>455 MB</td>
</tr>
<tr>
<td></td>
<td>2M</td>
<td>70 MB</td>
<td>1.2 GB</td>
<td>923 MB</td>
</tr>
<tr>
<td></td>
<td>3M</td>
<td>109 MB</td>
<td>1.9 GB</td>
<td>1.4 GB</td>
</tr>
</tbody>
</table>

#### NSD(signed)

#### CPU Possession rate

#### MEMORY Use

- 100%
- 75%
- 50%

- 100% (not-signed)
- 75% (not-signed)
- 50% (not-signed)
- 100% (signed)
- 75% (signed)
- 50% (signed)
Plan

- “go.kr” signing in 2010
- “.kr” signing in 2011 or later
- should go side by side with new kr DNS deployment /upgrade

** Since traffic burdens and limitation of budget, complete deployment won’t be done in a short time.
More about plan

- Education/Publicity campaign
- Cooperation with ISP and KR Registrar(*)
- Keep testing with tools, Administration(*)
  - opendnssec, dnssec-tools, zkt, etc.
  - Performance test with various S/W
  - Independent tool development for KR if it needed
- Zone Signing effect analysis
  - traffic increase(*)

* : Concerns
Deployment Schedule

- **Key**
  - Key and Signing Policy Decision
  - Key Repository Implementation
  - Key/Signing Control Program Implementation

- **Zone (signing)**
  - Zone extraction Programming
  - Safedns.kr NSEC3 signing, BIND batch
  - Auto-Resigning Program Activation
  - Dynamic Update Implementation/validation, stress test

- **Cache server (validation)**
  - DLV Adoption
  - Trusted Anchor Implementation
  - Auto Update
  - Cache server extension

- **Admin (web)**
  - Trial system web modification/upgread
  - Key/Signing Admin web Development
  - Trusted Anchor Distribution web Development

- **User (etc.)**
  - S/W Tool, Client Application Test (ZKT, firefox, thunderbird, IE etc.)
  - Public relations, H/W Infra extension

- **2009**
  - Go.kr T.A. distribution
  - Safedns.kr T.A. distributions
  - First Key Generating for KR

- **2010**
  - Go.kr signing testbed
  - Go.kr Signing
  - KR signing(all zones)

- **2011**
  - Go.kr Zone Trusted Key Registration
  - KR zone Trusted Key Registration

- **Korea Information and Security Agency**
THANKS

“Benefit all mankind”
홍익인간(弘益人間)
(National ideal envisioned on the founding of Korea)