DNSSEC for .nl

Background, development, lessons learned
- .nl and SIDN
- .nl and DNSSEC
- Adoption strategy
- Results
- Lessons learned
- Next steps
.nl and SIDN
About SIDN

- An independent, private organisation
- Responsible for the .nl name space since 1996
- More than 60 FTE
- Roughly 1800 registrars
- Turnover in 2011: 17.9 million euros
- With over 5 mio domainnames ranked 3rd in ccTLD’s
- Growth slightly declining since 2011
- We hold a 72% market share with .NL in The Netherlands
.nl and DNSSEC
The history of DNSSEC within .nl

- 2001 - 2004: DNSSEC Testbed
- 2005: DNSSEC part of nameserver policy
- 2009: Resource support for OpenDNSSEC
- 2009: DNSSEC.nl platform founded
- 2010: Friends and Fans Program
- 2010: Tier 1 for .nl
- 2012: DNSSEC Course online and Tier2 for .nl
Technical implementation: EPP

- Our implementation follows RFC 5910.
- Key data interface (secDNS:keyData), no DS Records.
- Keydata is not deleted upon transfer unless registrar selects otherwise.
Adoption Strategy
Why should a registry support DNSSEC?

- Abuse through DNS in a zone is likely to reflect negatively on the reputation of the registry.
- It is in the registries’ interest for DNSSEC to be deployed before this abuse occurs.
- But: where does the role of the registry end?
DNSSEC adoption = bootstrapping issue

DNSSEC only functions if ISP’s validate keys

ISP’s will only do this if a significant part of the zone is signed.

But: why sign your domain name if nobody validates?
Two questions to answer:

What is your principal target group?
- Registrars?
- ISP’s?
- Registrants?

What is your solution to the bootstrapping issue?
1. Subsidize
2. Create showcases (e.g. signing of big banking sites)
3. Legislation (e.g. government makes DNSSEC mandatory)

In a way we got it all..
But are the Registrars ready?

<table>
<thead>
<tr>
<th>Question</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>How important do you consider DNSSEC for the safety of DNS? (1=unimportant, 10=very important)</td>
<td>7.2</td>
</tr>
<tr>
<td>How do you rate your teams’ knowledge of DNSSEC? (1= no knowledge, 10=expert)</td>
<td>4.9</td>
</tr>
<tr>
<td>If DNSSEC was available for .nl, how well prepared would you be to implement it? (1=not, 10=well prepared)</td>
<td>4.9</td>
</tr>
<tr>
<td>What’s the main impediment? (multiple answers)</td>
<td></td>
</tr>
<tr>
<td>Knowledge (registrar /supplier)</td>
<td></td>
</tr>
<tr>
<td>What should SIDN’s role be? (multiple answers)</td>
<td></td>
</tr>
<tr>
<td>Provide knowledge</td>
<td></td>
</tr>
</tbody>
</table>
Our initial strategy

- Focus on knowledge enhancement.
- Setup contacts with suppliers (Parallels, PowerDNS).
- Focus on limited number of high profile registrations (max. 10,000).
- Cooperate with medium-sized, b2b-oriented registrars.
- Acquisition of 5 to 10 registrars willing to offer DNSSEC at delivery of Tier 2.
Strategy revised

- New insights at beginning of 2011
- Knowledge barrier relatively easy to bridge.
- Initial investment for registrars biggest impediment.
- .SE reported good results with incentive for registrars

New strategy: promote mass signing, develop incentive
Incentive

- Approx. 8% discount.
- Two years, starting the 1st of July 2012.
- Price set just right, high enough to cover investment, not high enough to give registrants a significant discount.
- Payment per quarter, so swift ROI.
- Very little rules or constraints, one general rule in terms and conditions.
Prognosis

Large registrars start signing

Technical difficulties large registrar

Announcement

0 100,000 200,000 300,000 400,000 500,000 600,000 700,000 800,000 900,000 1,000,000

0 100,000 200,000 300,000 400,000 500,000 600,000 700,000 800,000 900,000 1,000,000

466 448,387 456,910 402 419 418 413 428 432 332 336 342 347 419 418 413 428 432 332 336 342 347

433 454 428 448,387 456,910 402 419 418 413 428 432 332 336 342 347 419 418 413 428 432 332 336 342 347

5,156 289,544 392,693 448,387 466,370 494,475 533,821 601,273 685,588 787,343 937,373 1,000,000
Timing and success factors

1. Flawless release of Tier 2 in May.
2. Fierce competition between large registrars.
3. Government placed DNSSEC on the comply-or-explain list.
4. DNSSEC had matured: tools were becoming available.
5. Close support prevented technical problems.
6. Active PR and publicity for DNSSEC
7. Availability of tools and information in Dutch.
Key accountmanagement is key

- You can’t plan this rationally: you need to be aware of how your largest customers think.

- Timing is essential: what is on their mind now and how can we make DNSSEC their priority.

- Three aspects are important:
  - Create a personal sense of urgency
  - Be aware that large registrars look at each other and use that
  - Work with them to prevent technical issues.
Results
‘Soft’ results

- Registrars actively communicated the security benefits of DNSSEC to motivate their decision to sign.

- Strengthening of our relationship with the government.
“Hard” results
Lessons learned

- An incentive can be very effective if the timing and market conditions create fertile ground for it.
- The level at which you set the incentive is important: enough to cover the investment, not too high or it will not reflect positively on the DNSSEC standard.
- It only works if you’re able and prepared to put a lot of effort in assisting your registrars and cooperating with suppliers.
- It’s only the first step: you still need to tackle the ISP’s.
Next steps

- Approach those registrars who’re not DNS Operators
- Develop and deploy an ISP adoption program
- Deployment of registrant communication program
  - General public (.cz example)
  - Owners of high profile sites
  - Government officials (comply-or-explain)
About .NL (1)
About .nl (3): registrars

![Graph showing the number of .nl registrars over time. The graph indicates a steady increase in the number of registrars from 2001 to 2004, followed by a decrease in the next few years.](image-url)
About .nl (4): Size of registrars

- Top 100 manage 70% of all domains
- Top 200 manage 80% of all domains
- Top 500 manage 90% of all domains

Number of domains as % of total domains
About .NL (5): safe and reliable
Comply-or-explain-list

- The Dutch Government has a standardisation board whose purpose it is to establish standards for electronic exchange that its parts should comply with.
  - [http://www.forumstaardisatie.nl/english/](http://www.forumstaardisatie.nl/english/)
- The list of these standards is published and government agencies who do not comply need to explain why not.
- Thanks to some lobbying on our part DNSSEC was included in June.
- We’ve cooperated with the standardisation board in organizing a successful webinar for government agencies last month.
**Incentive (2): managing the incentive**

- Multiple segments in top-100:
  - Warm (max. 80% signed exp.)
  - Lukewarm (est. 30% signed exp.)
  - Cold (est. 10% signed exp.)

- A small (approx. 5 - 10) number of large ‘warm’ parties suffice to make a difference.

- Very intensive accountmanagement for this group (25 contacts per registrar per year).
Technical implementation (3): available tooling

- [http://dnssectest.sidn.nl/](http://dnssectest.sidn.nl/) validation tool
- [http://check.sidnlabs.nl:8080/form](http://check.sidnlabs.nl:8080/form) DNSSEC portfolio checker
- [http://www.sidnlabs.nl](http://www.sidnlabs.nl) various publications on DNSSEC
- [http://www.dnssec.nl](http://www.dnssec.nl) technical guidelines and checklists in Dutch
SIDN has opted for the following implementation:

- OpenDNSSEC (signing and key management).
- BIND9 (Hidden Master), BIND9 and NSD3 (secondary).
- NSEC3 with optout.
- Online 'DNSSEC Policy & Practice' statement.
- Procedures for key-rollovers (4 eyes).