DNSSEC for .nl

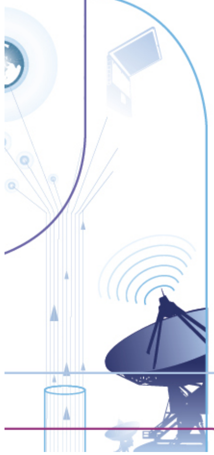
Background, development, lessons learned

Datum

SIDN

- .nl and SIDN
- .nl and DNSSEC
- Adoption strategy
- Results
- Lessons learned
- Next steps

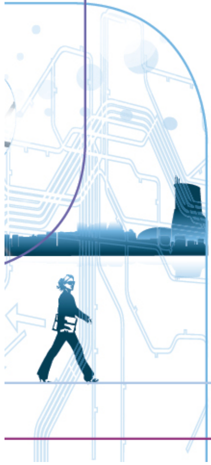
.nl and SIDN



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

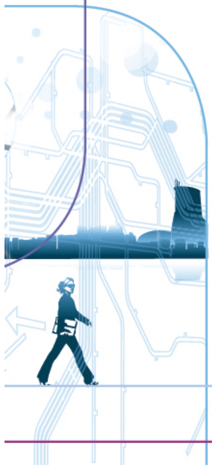
.nl and DNSSEC



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

SIDN



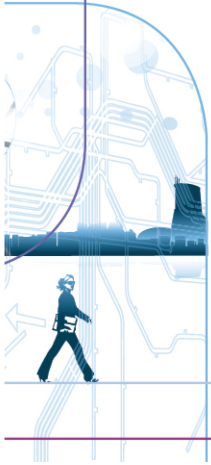
Technical implementation: EPP

- Our implementation follows RFC 5910.
- Key data interface (<secDNS:keyData>), no DS Records.
- Keydata is not deleted upon transfer unless registrar selects otherwise.

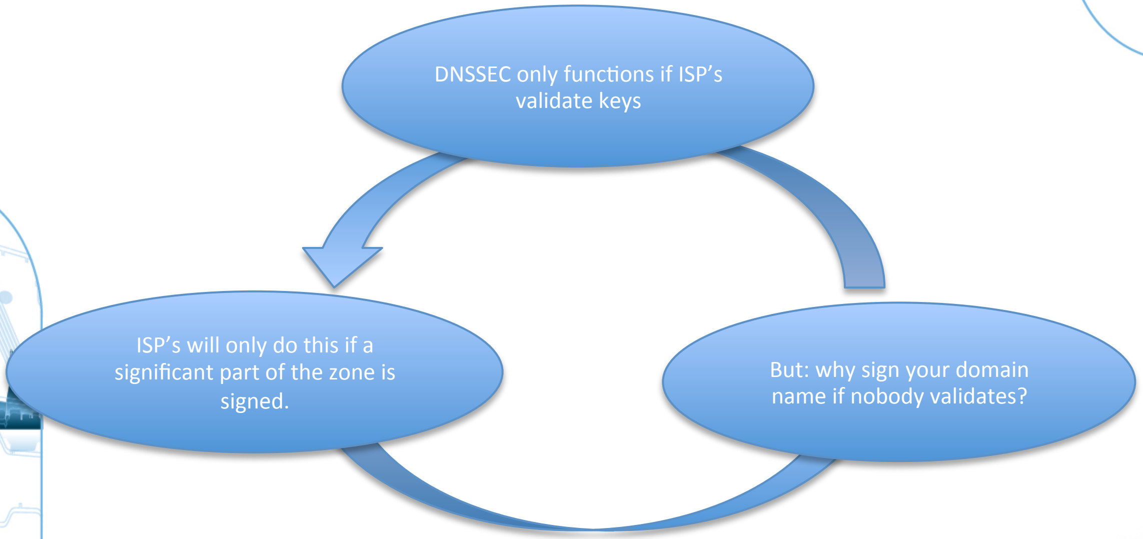
Adoption Strategy

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?



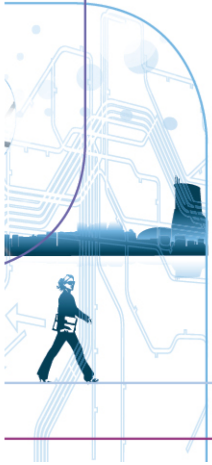
DNSSEC adoption = bootstrapping issue



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:

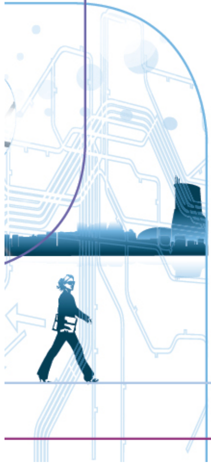
What is your principal target group?

- Registrars?
- ISP’s?
- Registrants?

What is your solution to the bootstrapping issue?

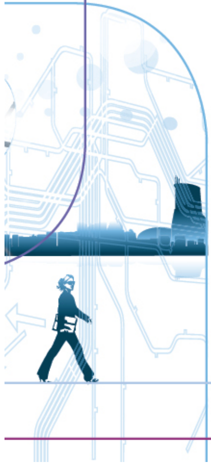
1. Subsidize
2. Create showcases (e.g. signing of big banking sites)
3. Legislation (e.g. government makes DNSSEC mandatory)

In a way we got it all..



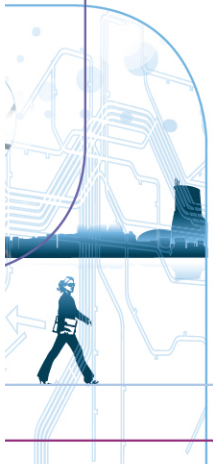
But are the Registrars ready?

	Rating
How important do you consider DNSSEC for the safety of DNS? (1=unimportant, 10=very important)	7,2
How do you rate your teams’ knowledge of DNSSEC? (1= no knowledge, 10=expert)	4,9
If DNSSEC was available for .nl, how well prepared would you be to implement it? (1=not, 10=well prepared)	4,9
What’s the main impediment? (multiple answers)	Knowledge (registrar /supplier)
What should SIDN’s role be? (multiple answers)	Provide knowledge



Our initial strategy

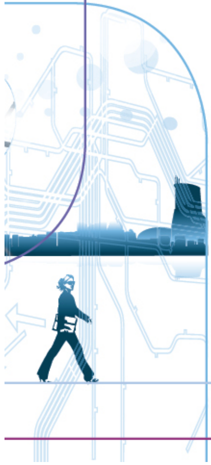
- Focus on knowledge enhancement.
- Setup contacts with suppliers (Parallells, PowerDNS).
- Focus on limited number of high profile registrations (max. 10.000).
- Cooperate with medium-sized, b2b-oriented registrars.
- Acquisition of 5 to 10 registrars willing to offer DNSSEC at delivery of Tier 2.



Strategy revised

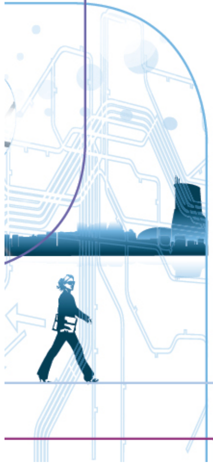
- New insights at beginning of 2011
- Knowledge barrier relatively easy to bridge.
- **Initial investment for registrars biggest impediment.**
- .SE reported good results with incentive for registrars

New strategy: promote mass signing, develop incentive

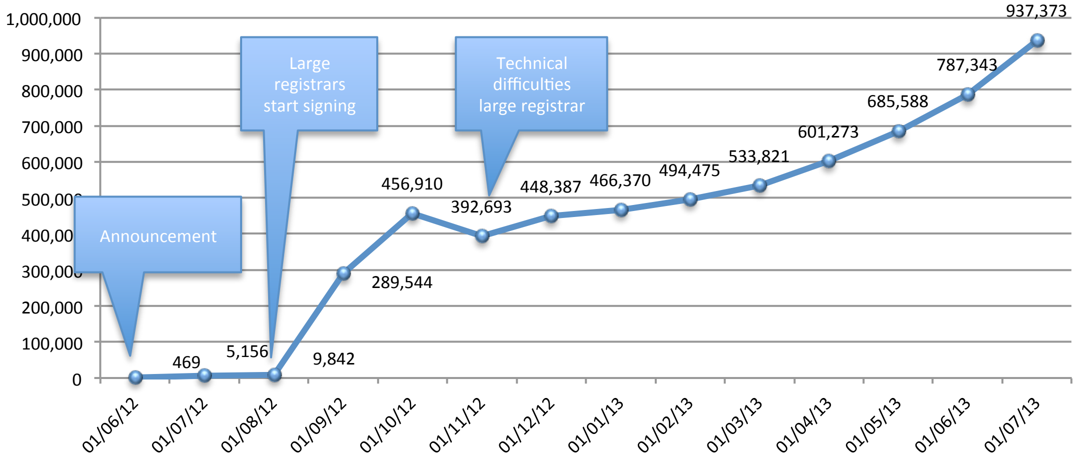


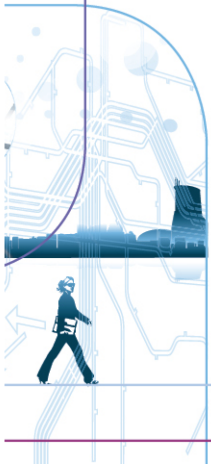
Incentive

- 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.



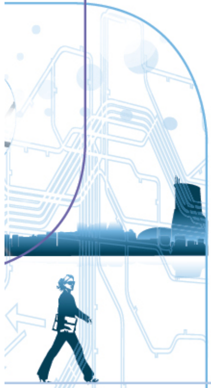
Prognosis


1,000,000
900,000
800,000
700,000
600,000
500,000
400,000
300,000
200,000
100,000
0
Announcement
Large registrars start signing
Technical difficulties large registrar
469
5,156
9,842
289,544
456,910
392,693
448,387
466,370
494,475
533,821
601,273
685,588
787,343
937,373
01/06/12
01/07/12
01/08/12
01/09/12
01/10/12
01/11/12
01/12/12
01/01/13
01/02/13
01/03/13
01/04/13
01/05/13
01/06/13
01/07/13



Timing and succes 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

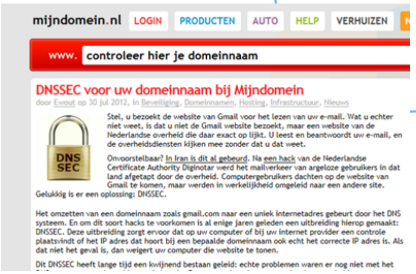
- You can’t plan this rationally: you need to be aware of how your largest customers think.
- Timing is essential: what is on their mind <u>now</u> and how can we make DNSSEC thier priority.
- Three aspects are important:
  - Create a personal sense of urgency
  - Be aware that large registrars look at each other and use that
  - Work with them tot 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.



mijndomein.nl LOGIN PRODUCTEN AUTO HELP VERHUIZEN

www. controleer hier je domeinnaam

DNSSEC voor uw domeinnaam bij Mijndomein

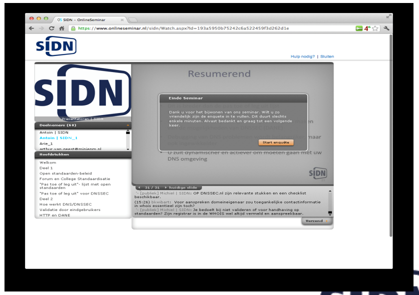
door Ewout op 30 jul 2012, in Beveiliging, Domeinnamen, Hosting, Infrastructuur, Nieuws

Stel, u bezoekt de website van Gmail voor het lezen van uw e-mail. Wat u echter niet weet, is dat u niet de Gmail website bezoekt, maar een website van de Nederlandse overheid die daar exact op lijkt. U leest en beantwoordt uw e-mail, en de overheidsdiensten kijken mee zonder dat u dat weet.

Onvoorstelbaar? In Iran is dit al gebeurd. Na een hack van de Nederlandse Certificate Authority Diginotar werd het mailverkeer van argeloze gebruikers in dat land afgetapt door de overheid. Computergebruikers dachten op de website van Gmail te komen, maar werden in werkelijkheid omgeleid naar een andere site. Gelukkig is er een oplossing: DNSSEC.

Het omzetten van een domeinnaam zoals gmail.com naar een uniek internetadres gebeurt door het DNS systeem. En om dit soort hacks te voorkomen is al enige jaren geleden een uitbreiding hierop gemaakt: DNSSEC. Deze uitbreiding zorgt ervoor dat op uw computer of bij uw internet provider een controle plaatsvindt of het IP adres dat hoort bij een bepaalde domeinnaam ook echt het correcte IP adres is. Als dat niet het geval is, dan weigert uw computer die website te tonen.

Dit DNSSEC heeft lange tijd een kwijnend bestaan geleid: echte problemen waren er nog niet met het



SIDN – OnlineSeminar

https://www.onlineseminar.nl/sidn/Watch.aspx?Id=193a5950b75242c6a522459f3d262d1e

Hulp nodig? | Sluiten

Resumerend

Einde Seminar

Dank u voor het bijwonen van ons seminar. Wilt u zo vriendelijk zijn de enquete in te vullen. Dit duurt slechts enkele minuten. Alvast bedankt en graag tot een volgende keer.

Start enquête

- Dit is breder dan de pas toe of leg uit lijst
- U zult dynamischer en actiever om moeten gaan met uw DNS omgeving

Presentatoren | SIDN

Deelnemers (68)

Antoin | SIDN
Antoin | SIDN_1
Arie_1
arthur.van.geest@minienm.nl

Hoofdstukken

Welkom
Deel 1
Open standaarden-beleid
Forum en College Standaardisatie
"Pas toe of leg uit"- lijst met open standaarden
"Pas toe of leg uit" voor DNSSEC
Deel 2
Hoe werkt DNS/DNSSEC
Validatie door eindgebruikers
HTTP en DANE

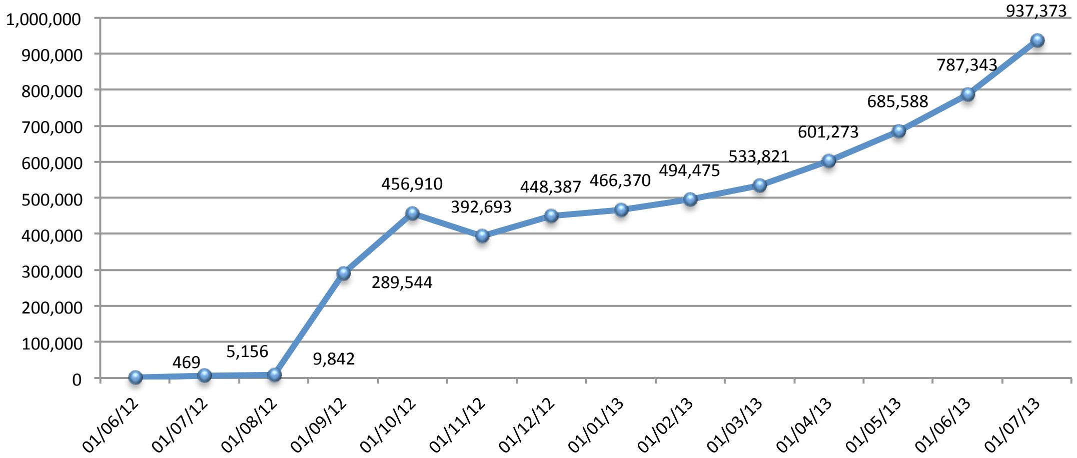
31 / 31 huidige slide

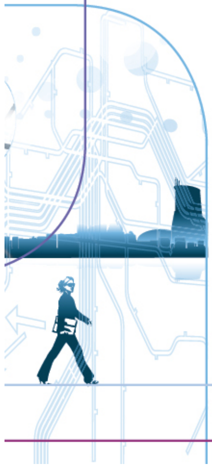
'- [publiek] Michiel | SIDN: OP DNSSEC.nl zijn relevante stukken en een checklist beschikbaar.

(15:26) bkwibart: Voor aanspreken domeineigenaar zou toegankelijke contactinformatie in whois essentieel zijn toch?

'- [publiek] Michiel | SIDN: Je bedoelt bij niet valideren of voor handhaving op standaarden? Zijn registrar is in de WHOIS wel altijd vermeld en aanspreekbaar.

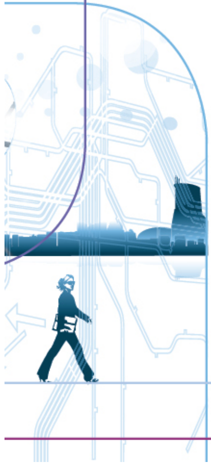
“Hard” results





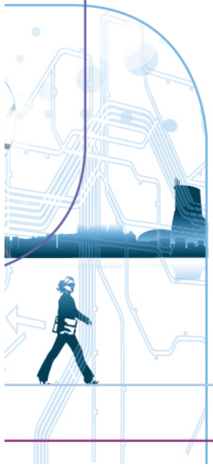
Lessons learned

- 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.

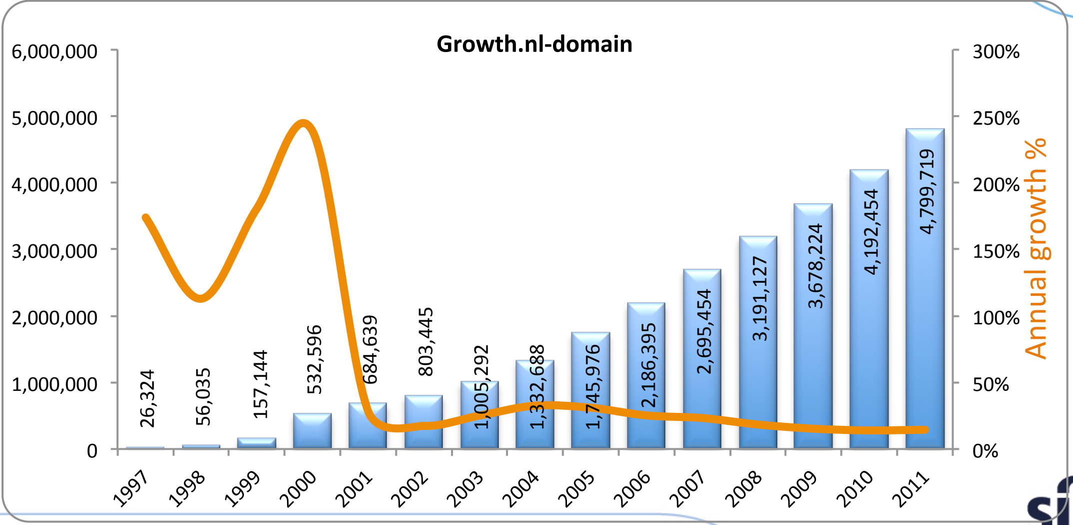


Next steps

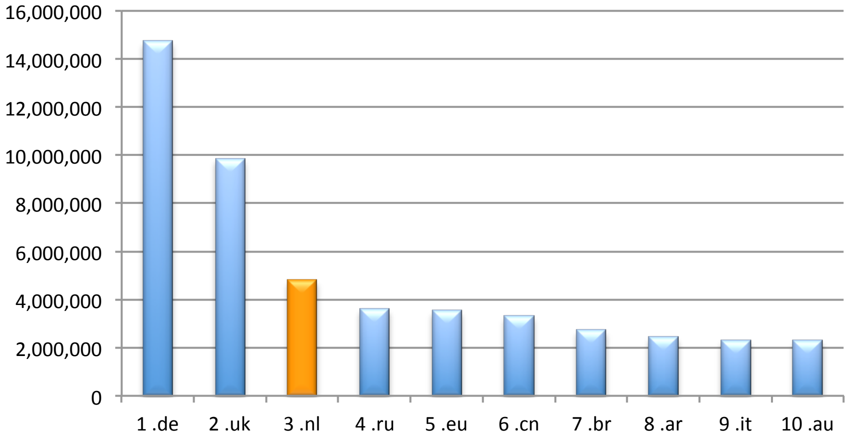
- Approach those registrars who’re not DNS Operators
- Develop and deploy an ISP adoption program
- Deployment of registrant communication program
  - General public (.cz example)
  - Owners of high profile sites
  - Government officials (comply-or-explain)

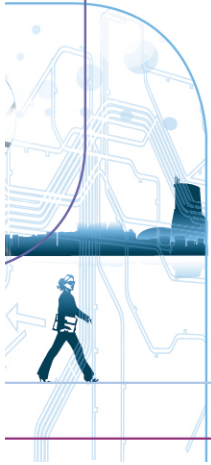


About .NL (1)

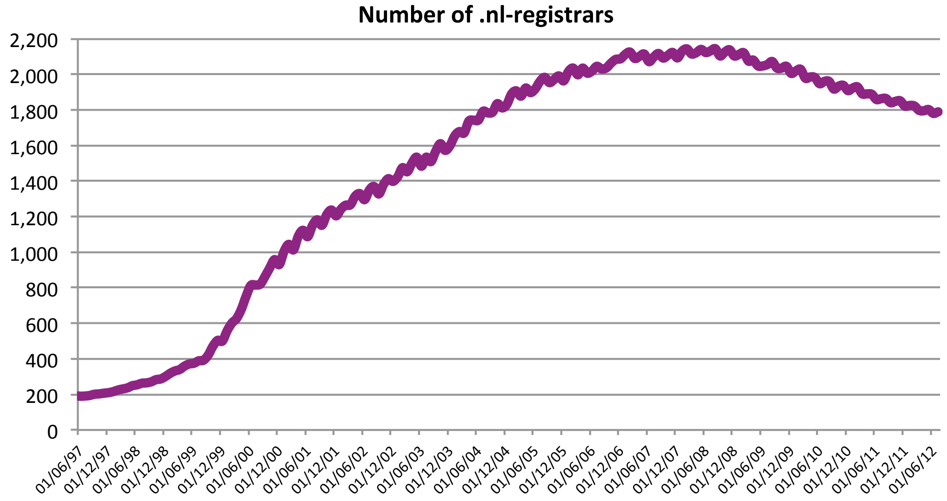

Growth.nl-domain
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
0
300%
250%
200%
150%
100%
50%
0%
Annual growth %
26,324
56,035
157,144
532,596
684,639
803,445
1,005,292
1,332,688
1,745,976
2,186,395
2,695,454
3,191,127
3,678,224
4,192,454
4,799,719
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011

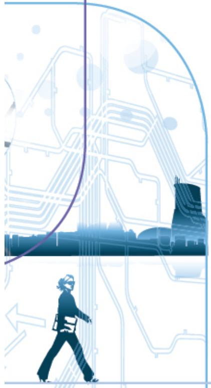
About .nl (2)


16,000,000
14,000,000
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
1 .de
2 .uk
3 .nl
4 .ru
5 .eu
6 .cn
7 .br
8 .ar
9 .it
10 .au

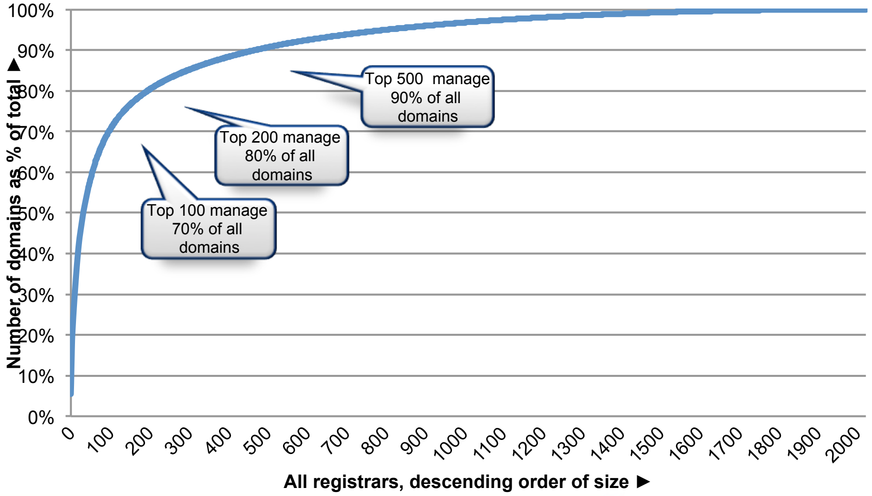


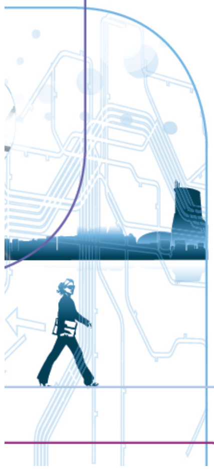
About .nl (3): registrars



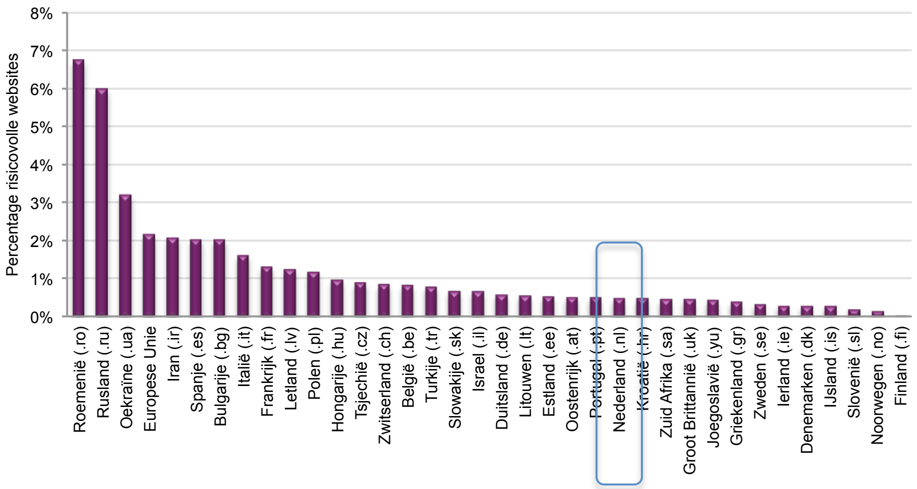


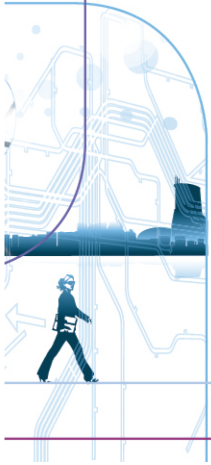
About .nl (4): Size of registrars





About .NL (5): safe and reliable

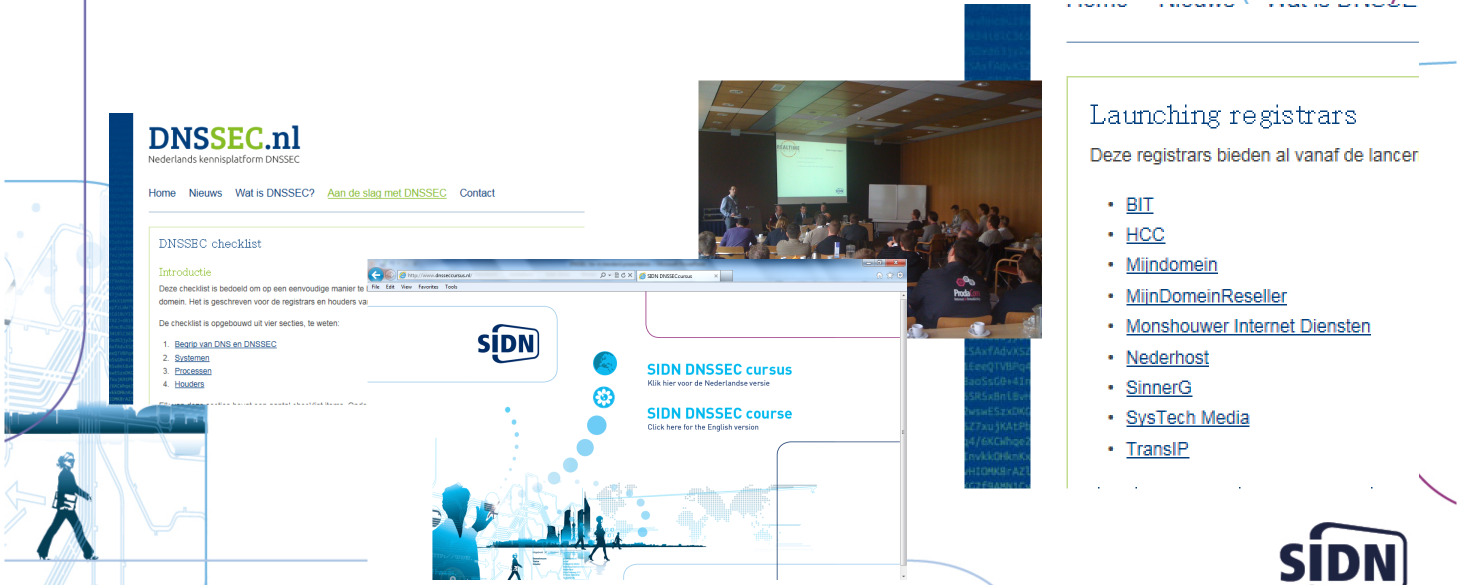




Comply-or-explain-list

- 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.forumstandaardisatie.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 succesful webinar for government agencies last month.

Deliverables



DNSSEC.nl

Nederlands kennisplatform DNSSEC

DNSSEC checklist

Introductie

Deze checklist is bedoeld om op een eenvoudige manier te

domein. Het is geschreven voor de registrars en houders va

De checklist is opgebouwd uit vier secties, te weten:

1. Begrip van DNS en DNSSEC
2. Systemen
3. Processen
4. Houders

SIDN DNSSEC cursus

Klik hier voor de Nederlandse versie

SIDN DNSSEC course

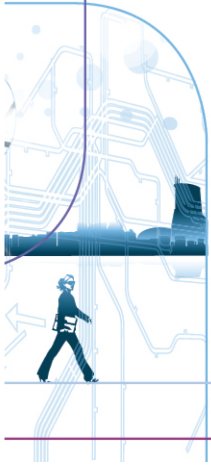
Click here for the English version

Launching registrars

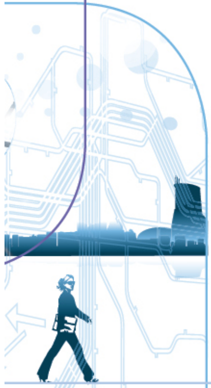
Deze registrars bieden al vanaf de lancer

- BIT
- HCC
- Mijndomein
- MijnDomeinReseller
- Monshouwer Internet Diensten
- Nederhost
- SinnerG
- SysTech Media
- TransIP

Incentive (2): managing the incentive

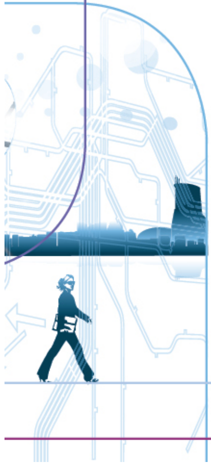


- Multiple segments in top-100:
  - Warm (max. 80% signed exp.)
  - Lukewarm (est. 30% signed exp.)
  - Cold (est. 10% signed exp.)
- A small (approx. 5 - 10) number of large ‘warm’ parties suffice to make a difference.
- Very intensive accountmanagement for this group (25 contacts per registrar per year).



Technical implementation (3): available tooling

- http://dnssectest.sidn.nl/ validation tool
- http://check.sidnlabs.nl:8080/form DNSSEC portfolio checker
- http://www.sidnlabs.nl various publications on DNSSEC
- http://www.dnssec.nl technical guidelines and checklists in Dutch



Technical implementation (1)

SIDN has opted for the following implementation:

- OpenDNSSEC (signing and key management).
- BIND9 (Hidden Master), BIND9 andNSD3 (secondary).
- NSEC3 with optout.
- Online 'DNSSEC Policy & Practice' statement.
- Procedures for key-rollovers (4 eyes).