DNSSEC College

Arjen Zonneveld

Jelte Jansen

DHPA Techday, 21 mei 2015

SIDN labs
Internet Research & Innovation
SIDN

DNS

Security / Report Claims DNS Cache Poisoning Attack Against Brazilian Bank and ISP

Report Claims DNS Cache Poisoning Attack Against Brazilian Bank and ISP

By Larry Seltzer | Posted 2009-04-22 Email Print

OPINION: Attack shows the potential for serious spoofing attacks that could leave end users helpless. The only real solution is DNSSEC, which will take years to implement under the best of circumstances.

DNS cache poisoning attac exploited in the wild

HOME « NEWS « TOP SECURITY STORIES « GOOGLE'S MALAYSIAN DOMAINS HIT WITH DNS CACHE POISONING...

GOOGLE'S MALAYSIAN DOMAINS HIT WITH DNS CACHE POISONING ATTACK

PREVIOUS CONTRIBUTORS

OCT 11, 2013

Google's Malaysian domains google.com.my and google.my were hijacked, redirecting users to a webpage that announced the attack was perpetrated by a Pakistani group called Madleets. MYNIC, the sole administrator for web addresses in Malaysia confirmed the attack in a statement.

"We can confirm there was unauthorised redirection of www.google.com.my and www.google.my to another IP address by a group which called themselves TeaM MADLEETS," the MYNIC statement says.

we provided more details in thei
HD Moore's statement on DNS c
ces are starting to see evidence o
ppears to be an attempt to take

nillions

s of surfers adrift.

DN in ISP

By Jo

DNSSEC in vogelvlucht: Signeren

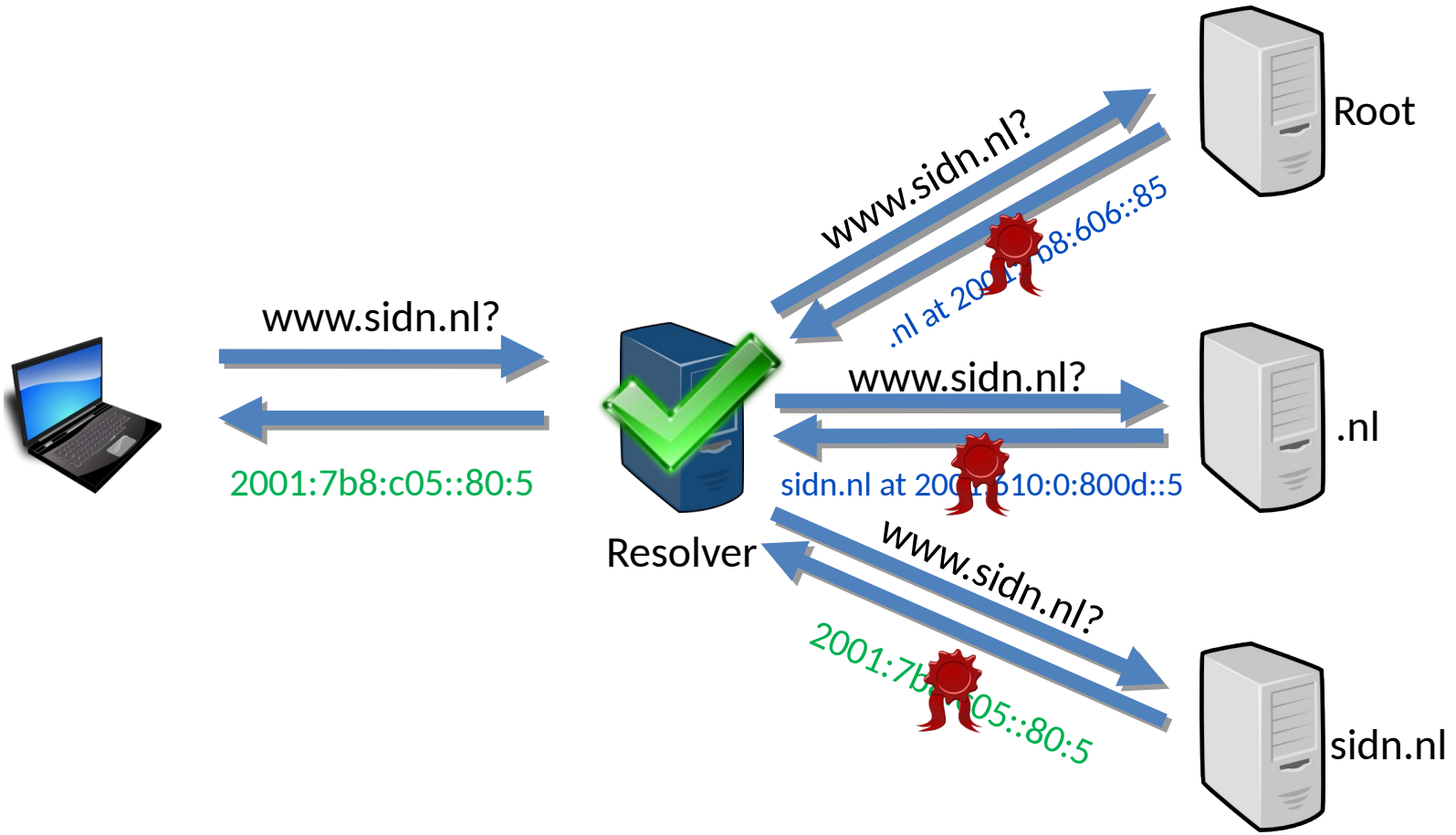
RRSIG

```
example.dom. 7200  RRSIG   SOA 5 3 7200
20131113113016 (
        20131014113016 57798 example.dom.
        TWLzBuUgXWMA9cj+xe6YMjXy2/VdauWnONk7
        uAP8JcdzsemcfWov4cFzXowS2YX291+5jBMp
        m5AlwpM7ijbSBgAGz22ywlKN8JoOg3KtCM2Y
        UX/c8/ATbYEBPKRjBs+YQKmY1NppwSjFi9Y0
        1fVEBbrCnI0EP33c/VK97s8oNG8= )
```

DNSSEC in vogelvlucht: signen

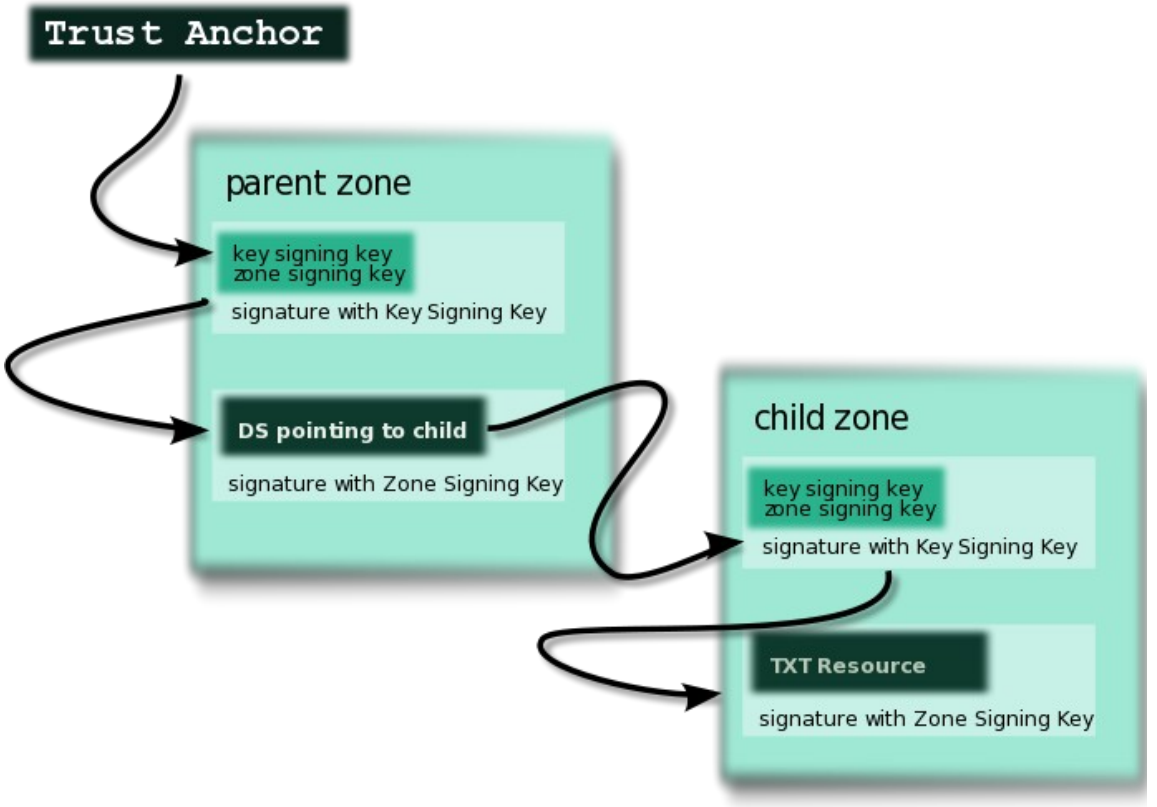
- Maak een keypair aan
- Sign je zone(s)
  - BIND, NSD+ldns, PowerDNS, Secure64, Infoblox, etc.
- Publiceer gesignde zones
- Stuur public key naar parent

DNSSEC in vogelvlucht

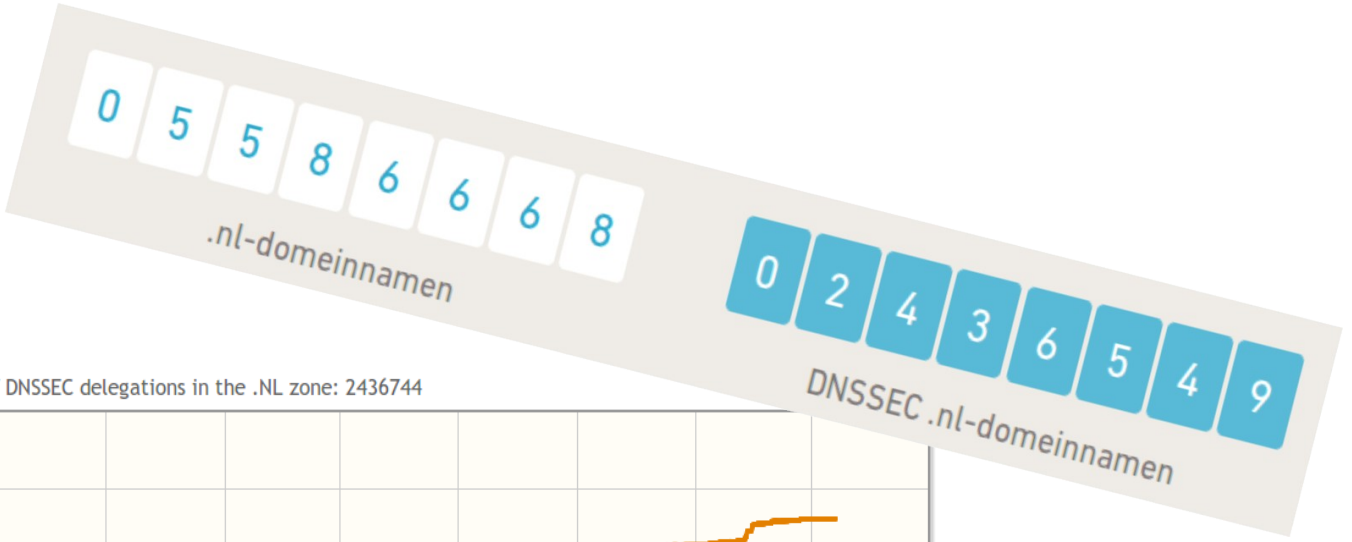


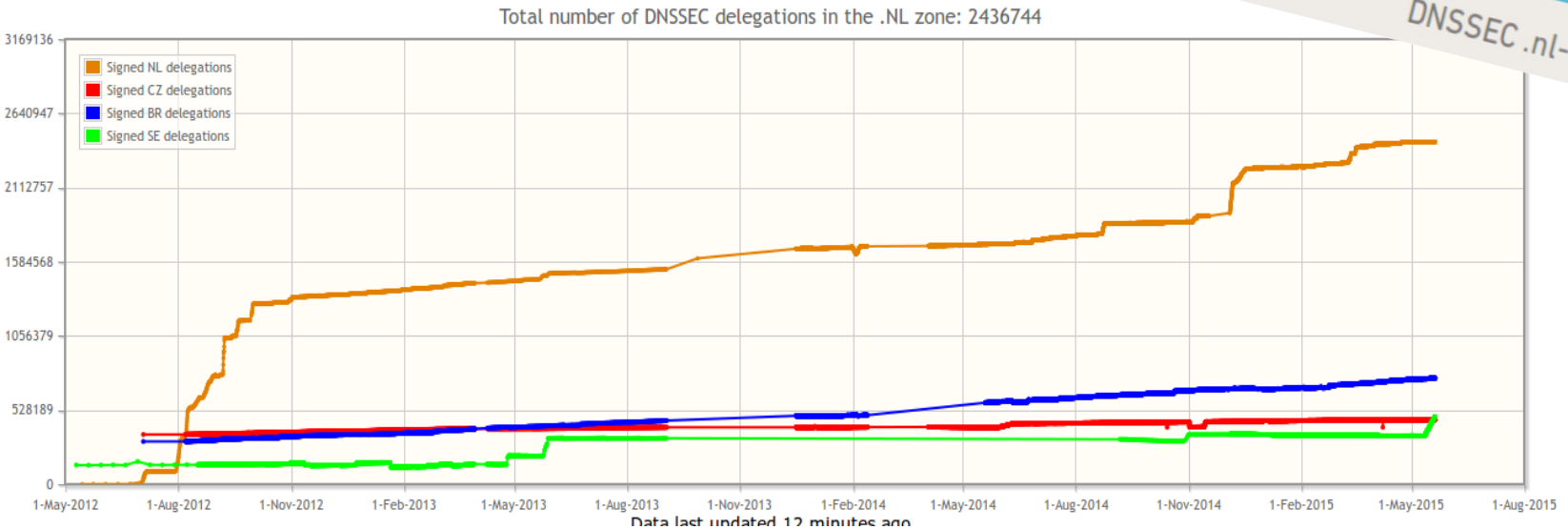
DNSSEC in vogelvlucht: chain of trust

- Chain of trust:
  - Vanaf een Trust Anchor (de root)
  - Via delegaties (.nl, sidn.nl)
  - Naar het antwoord (www.sidn.nl)



DNSSEC in .nl: zones





SIDN labs
Internet Research & Innovation

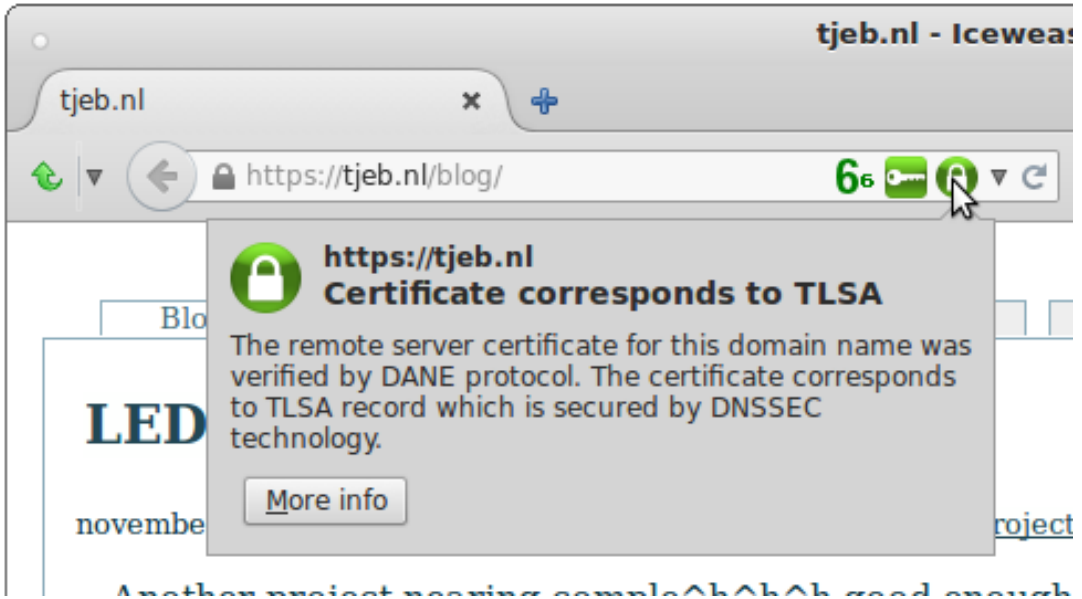
SIDN

DNSSEC als basis

- DANE: verbindt X.509 (bekend van https) met DNS(SEC)
  - Aanvullend op CA
  - Maakt werkende self-signed certificates mogelijk

- In browser (met plugin; geen native support)

- Mail Transfer Agents
  - native support in Postfix (2.11)
  - Experimental support in Exim (4.85)



DANE voor SMTP

- Nu vaak opportunistic encryption
  - Want geen interactie met gebruiker
  - Biedt weinig bescherming boven geen encryption

- Met DANE geef je certificaatkenmerken aan via DNSSEC
  - Verzender weet dat er encryption gebruikt kan worden
  - Niet meer opportunistic

- DNS Record:
  - `_25._tcp.<mailserver>.  3600 TLSA  3 0 1 <fingerprint of cert>`

DANE voor SMTP

Zonder DNSSEC/TLSA:

```
Mar 16 19:11:03 m3 postfix/smtp[25929]:
Untrusted TLS connection established to
mail1.example.de[2001:db8:100::25]:25:
TLSv1 with cipher ECDHE-RSA-AES256-SHA
(256/256 bits)
```

Met DNSSEC/TLSA:

```
Mar 16 19:20:01 m3 postfix/smtp[26131]:
Verified TLS connection established to
mail.example.de[2001:db8:100::25]:25:
TLSv1 with cipher ECDHE-RSA-AES256-SHA
(256/256 bits)
```

SSHFP

DNS:

```
<hostname> 3600  IN  SSHFP  1 1 9CF43AD8D319F3854F84B841594101A82EF8227C
```

SSH client config:

```
VerifyHostKeyDNS yes
```

SSHFP

Zonder SSHFP:

```
debug1: Server host key: RSA
a1:72:a5:45:ac:f7:8e:a5:c7:50:e8:aa:b5:d9:7f:30
The authenticity of host 'tjeb.nl (2a02:348:55:5250::80)'
can't be established.
Are you sure you want to continue connecting (yes/no)?
```

Met SSHFP:

```
debug1: Server host key: RSA
a1:72:a5:45:ac:f7:8e:a5:c7:50:e8:aa:b5:d9:7f:30
debug1: found 1 secure fingerprints in DNS
debug1: matching host key fingerprint found in DNS
debug1: ssh_rsa_verify: signature correct
```

Signing methodes

- Offline signing
  - BIND
  - OpenDNSSEC
  - ldns
- Online signing
  - BIND
  - Powerdns
  - Knot
- Automatic key rolling
  - BIND
  - OpenDNSSEC
- Plesk plugin 'Admin-ahead DNSSEC'

PowerDNS voorbeeld

Sign zone:

```
pdnssec secure-zone powerdnssec.org
pdnssec rectify-zone powerdnssec.org
```

Vraag DNSKEY (of DS) om naar parent te sturen:

```
pdnssec show-zone powerdnssec.org
```

BIND voorbeeld

Live demo

Valkuilen

- Verhuizingen
- Minder vergevingsgezind dan DNS
  - Alle delegaties moeten expliciet zijn
  - Let op met wildcards en empty-nonterminals
- Wel DS, geen DNSKEY
- Verlopen RRSIGs
- Antwoorden worden groter
  - Gebruik RRL if supported
- Controleer!

Monitoring / Debugging

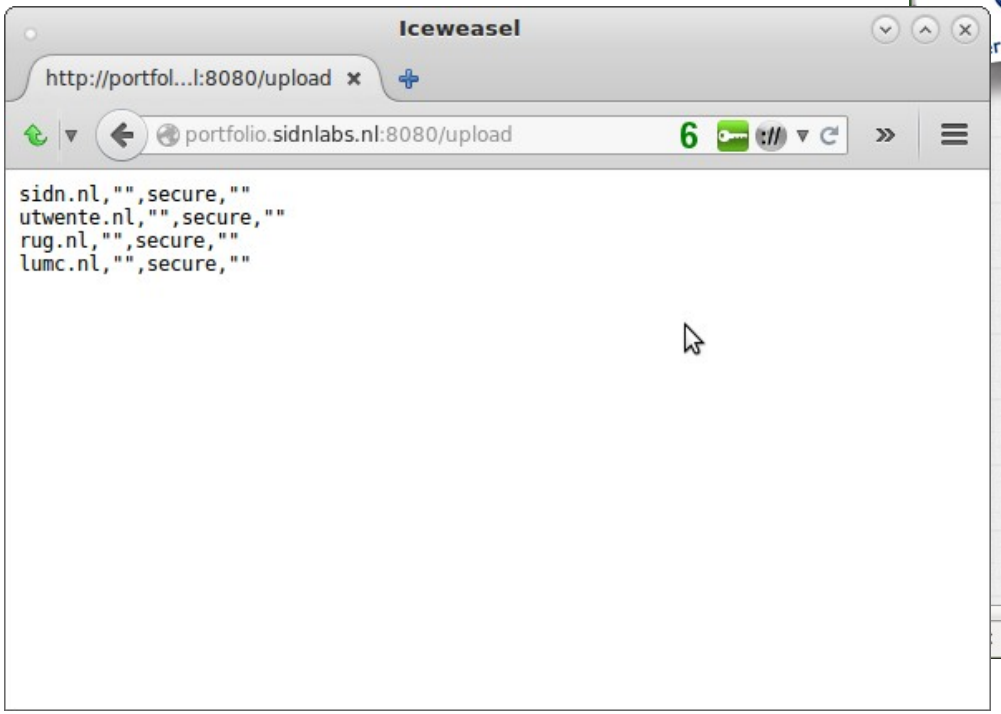
- Plugins
  - Nagios
  - Zabbix

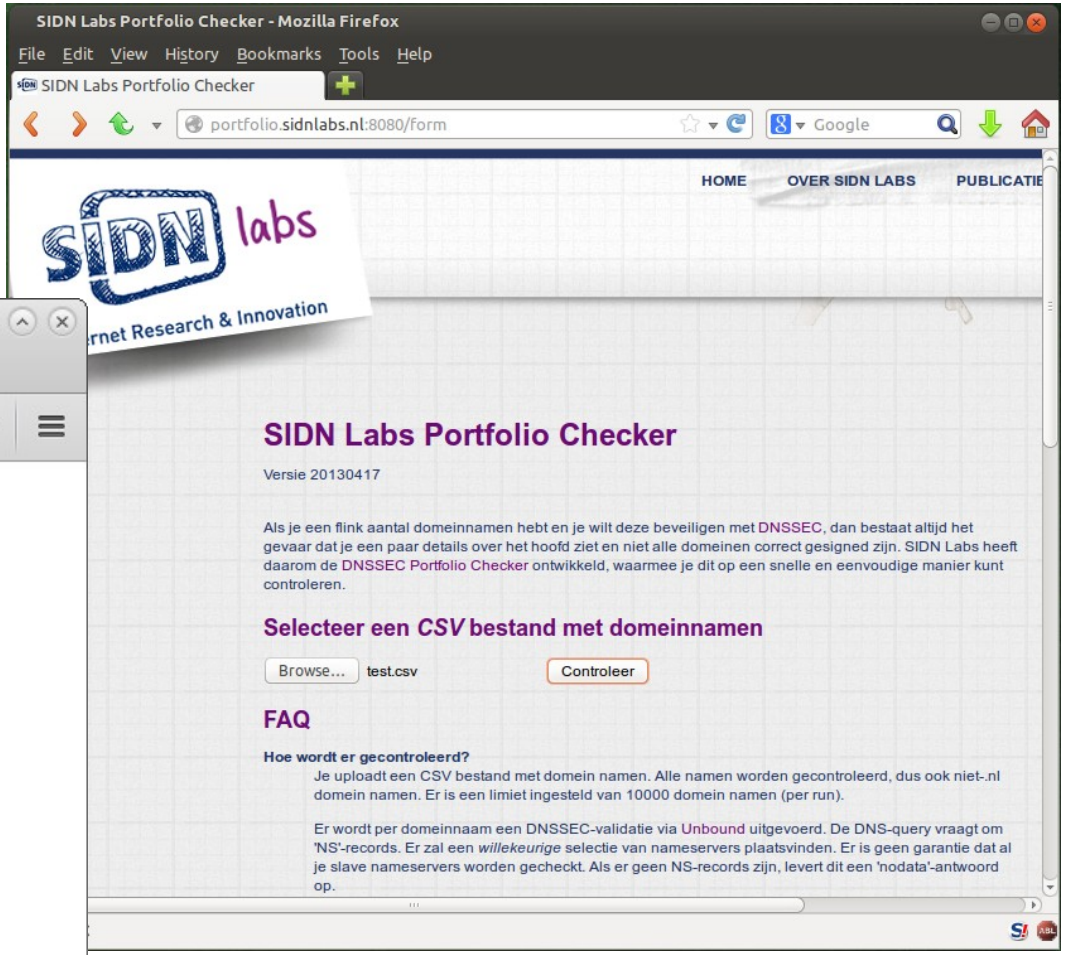
- Online tools
  - DNSViz
  - SIDN DNSSEC portfolio checker
  - DNSCheck
  - internet.nl

- CLI debugging
  - dig (BIND)
  - drill (ldns)
  - logging

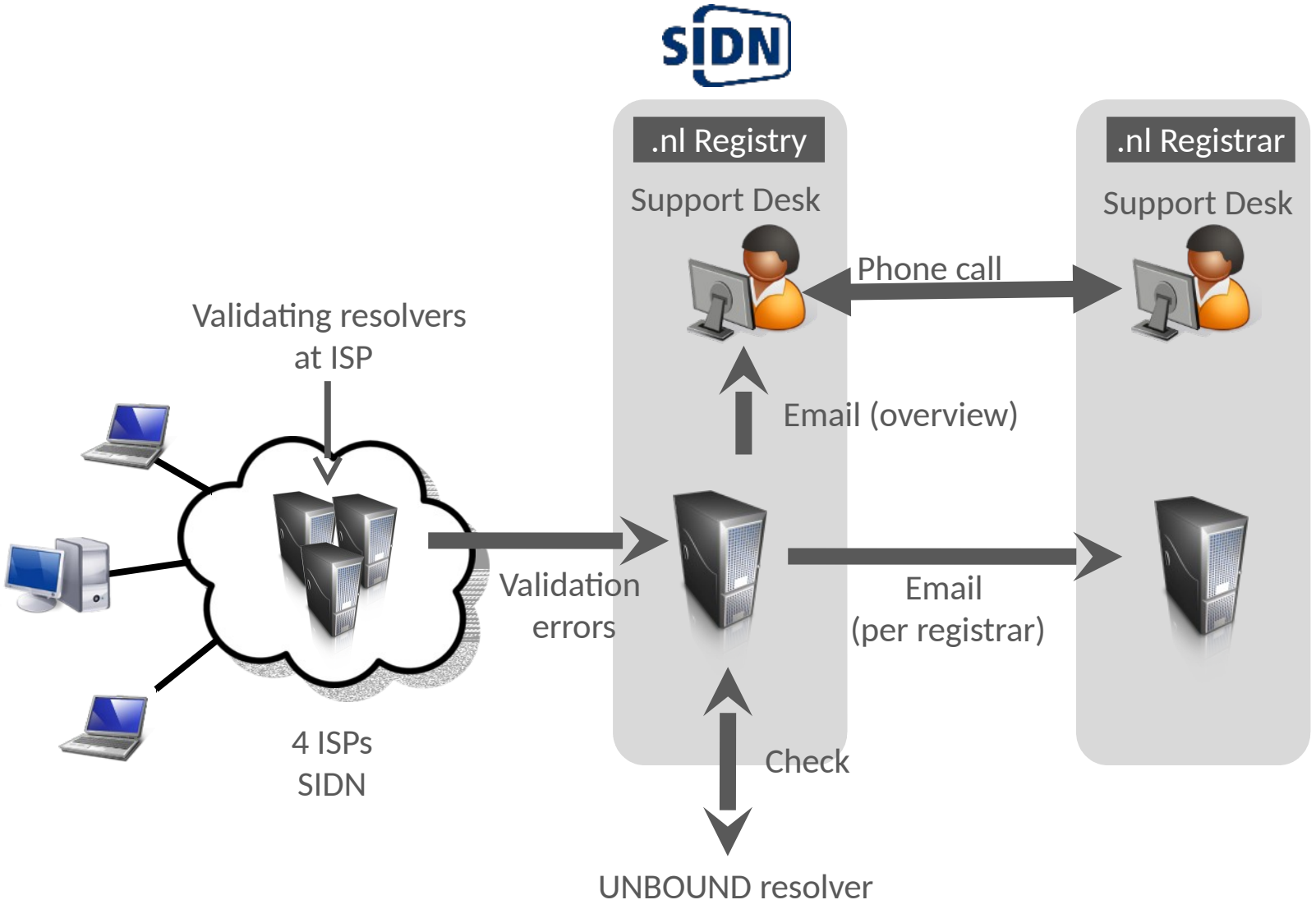
DNSSEC Test sites

- Signeren:
  - http://portfolio.sidnlabs.nl:8080/form

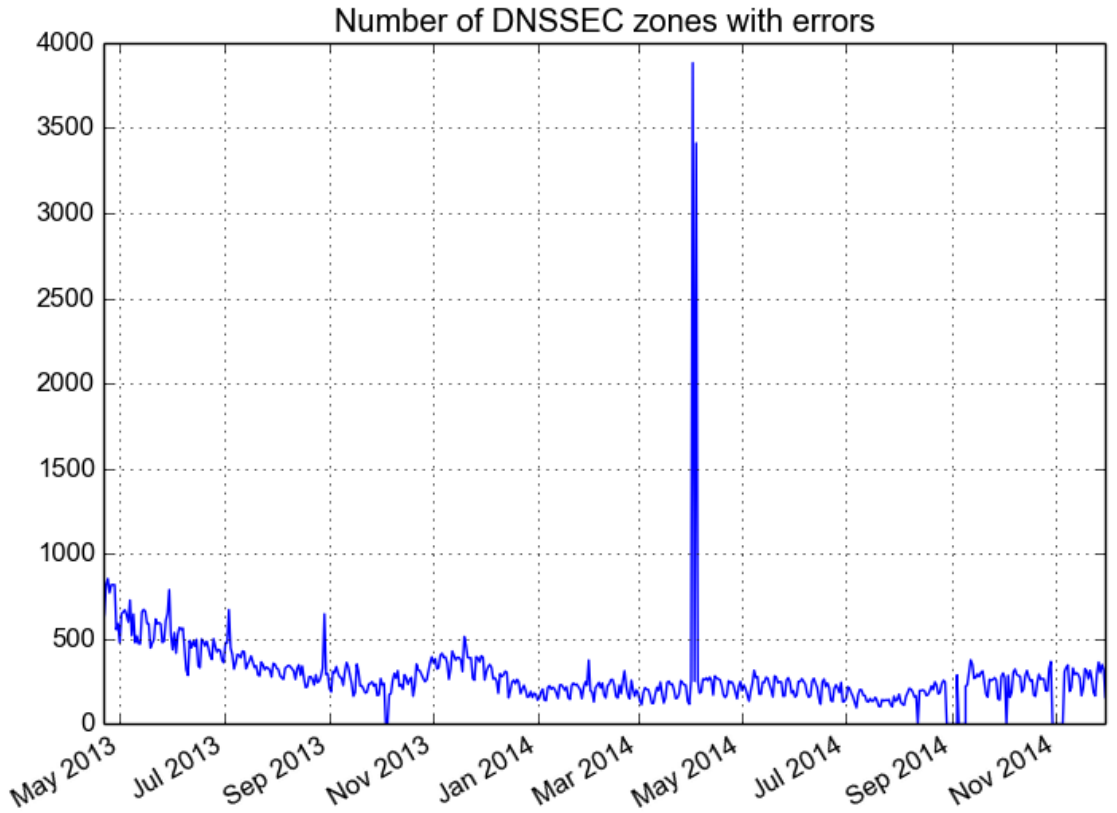




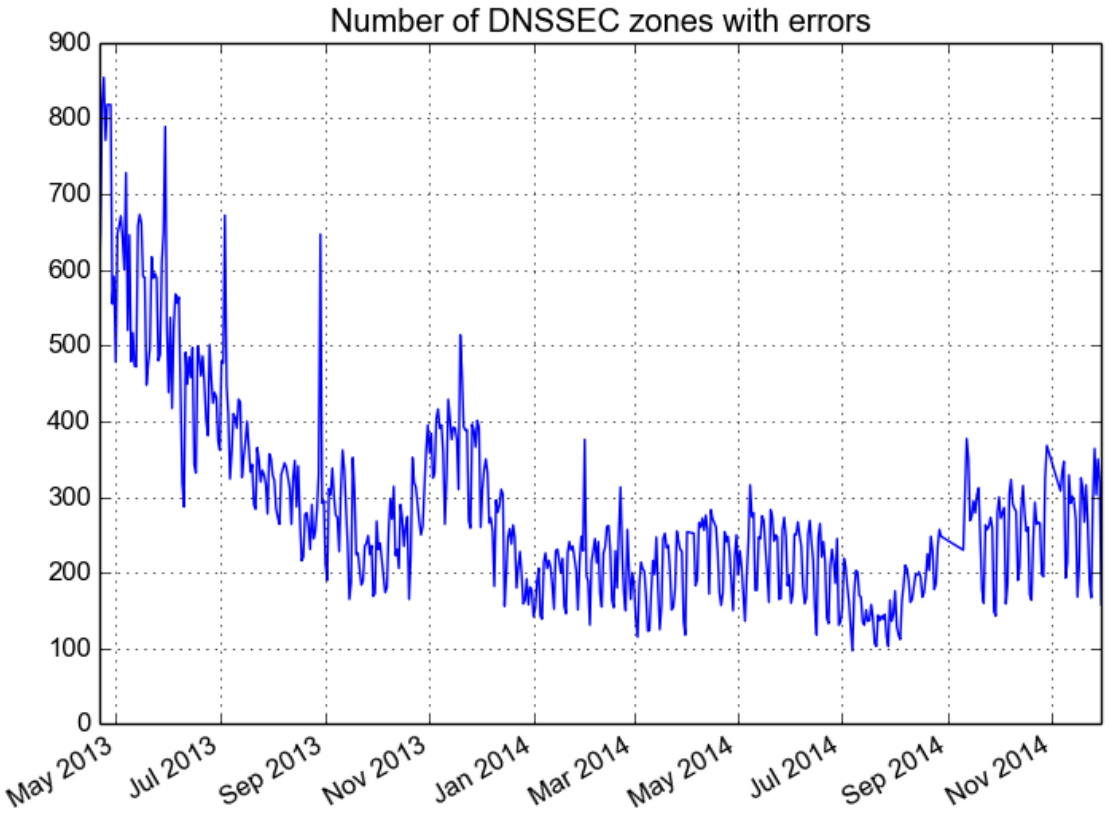
DNSSEC validatie monitor



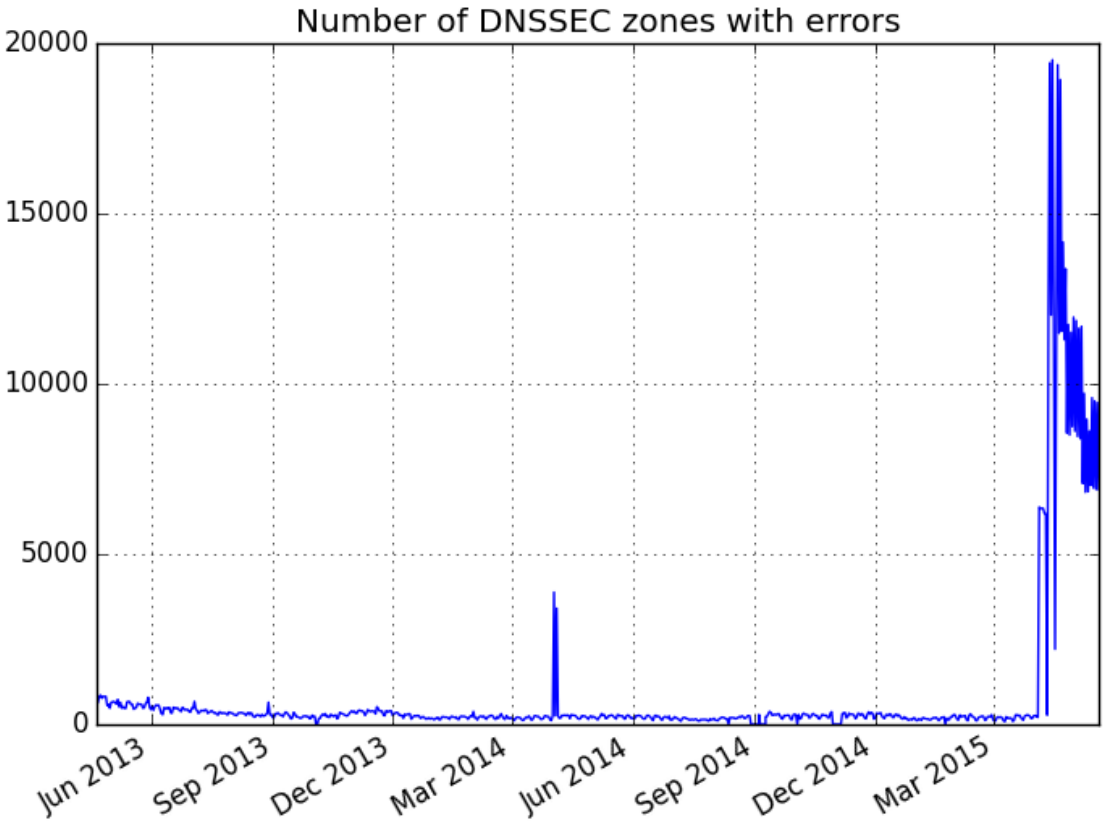
Validatie errors



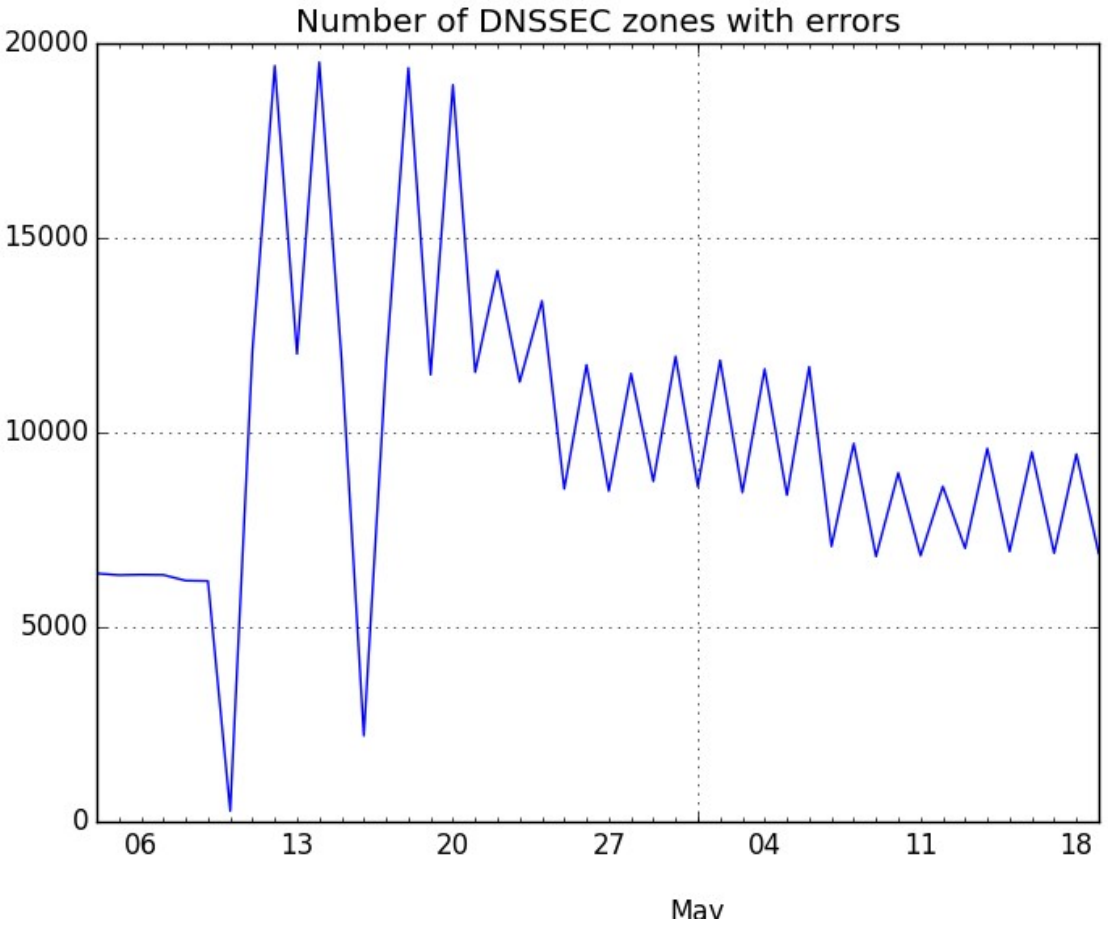
Validatie errors



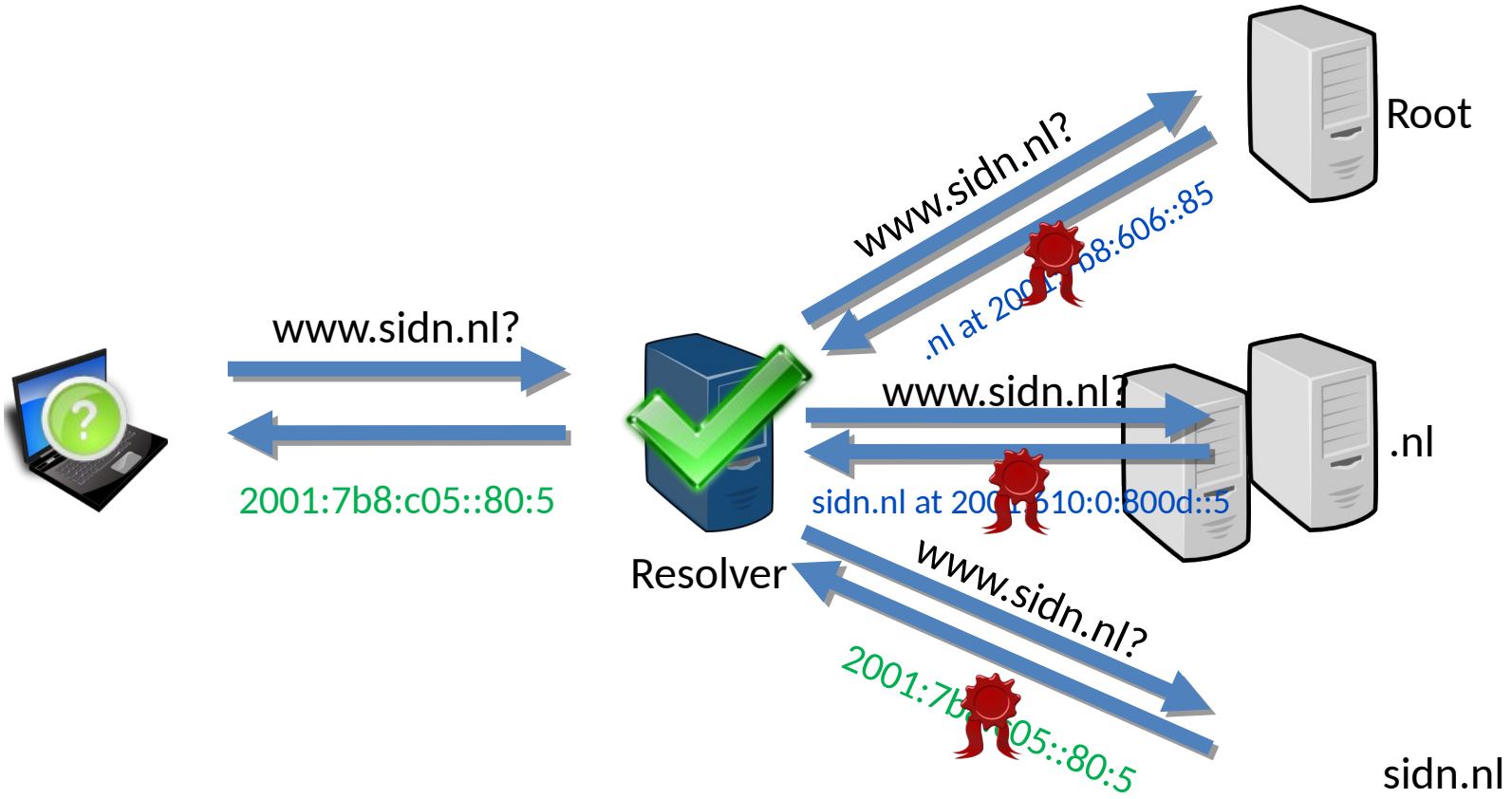
Validatie errors



Validatie errors

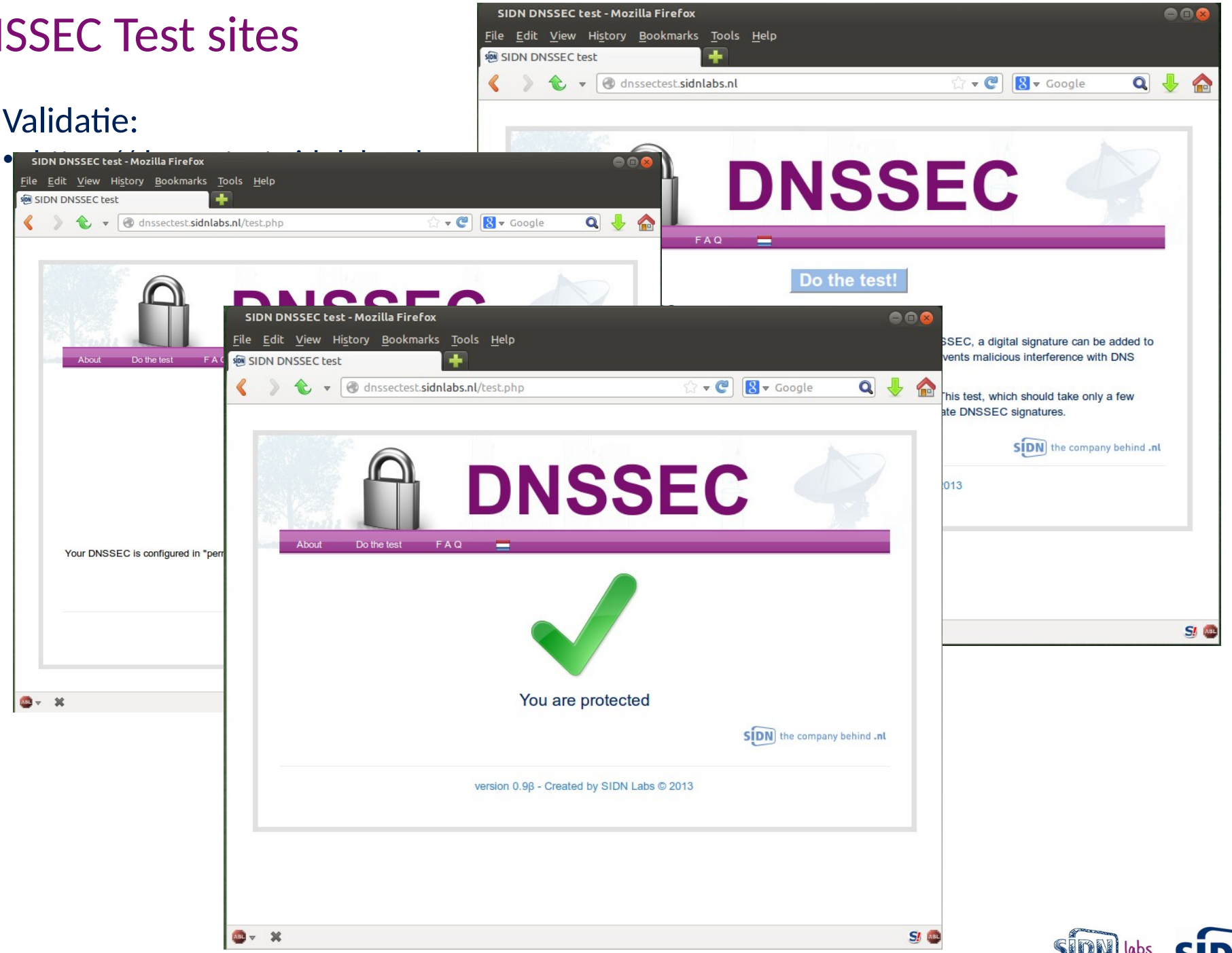


DNSSEC in vogelvlucht



DNSSEC Test sites

- Validatie:
  -



SIDN labs
Internet Research & Innovation

SIDN

DNSSEC Informatiesites

- http://www.dnssec.nl
- http://www.dnsseccursus.nl

SIDN labs
Internet Research & Innovation

SIDN

Prijsvraag!

Beantwoord de vraag:

“Hoe denk jij dat de internetsector het gebruik van DNSSEC(-validatie) zou kunnen versnellen?

en maak kans op een GL-iNet device!

DNSSEC Informatiesites

- http://www.dnssec.nl
- http://www.dnsseccursus.nl

SIDN labs
Internet Research & Innovation

SIDN