

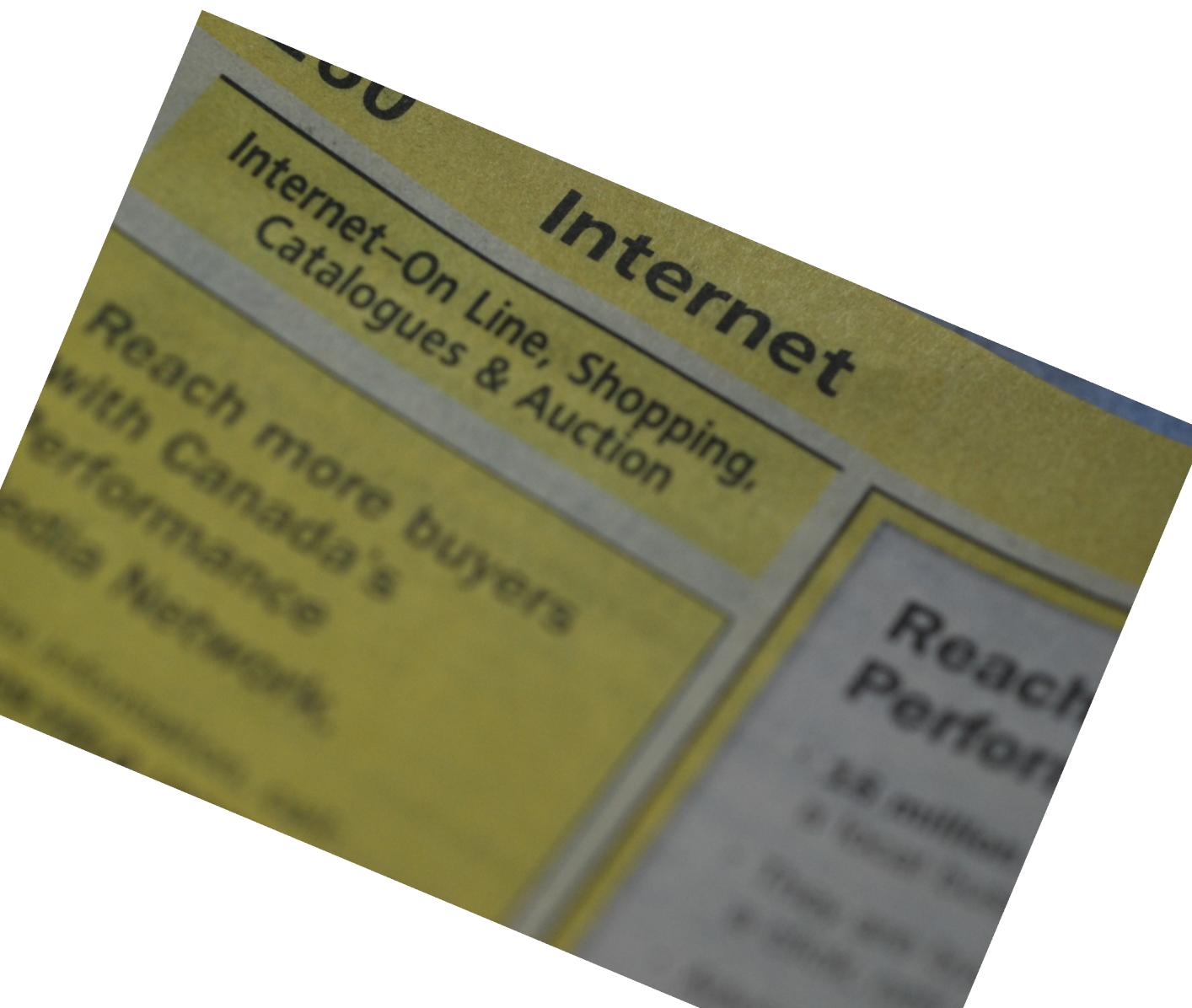
# DNSSEC College

Arjen Zonneveld

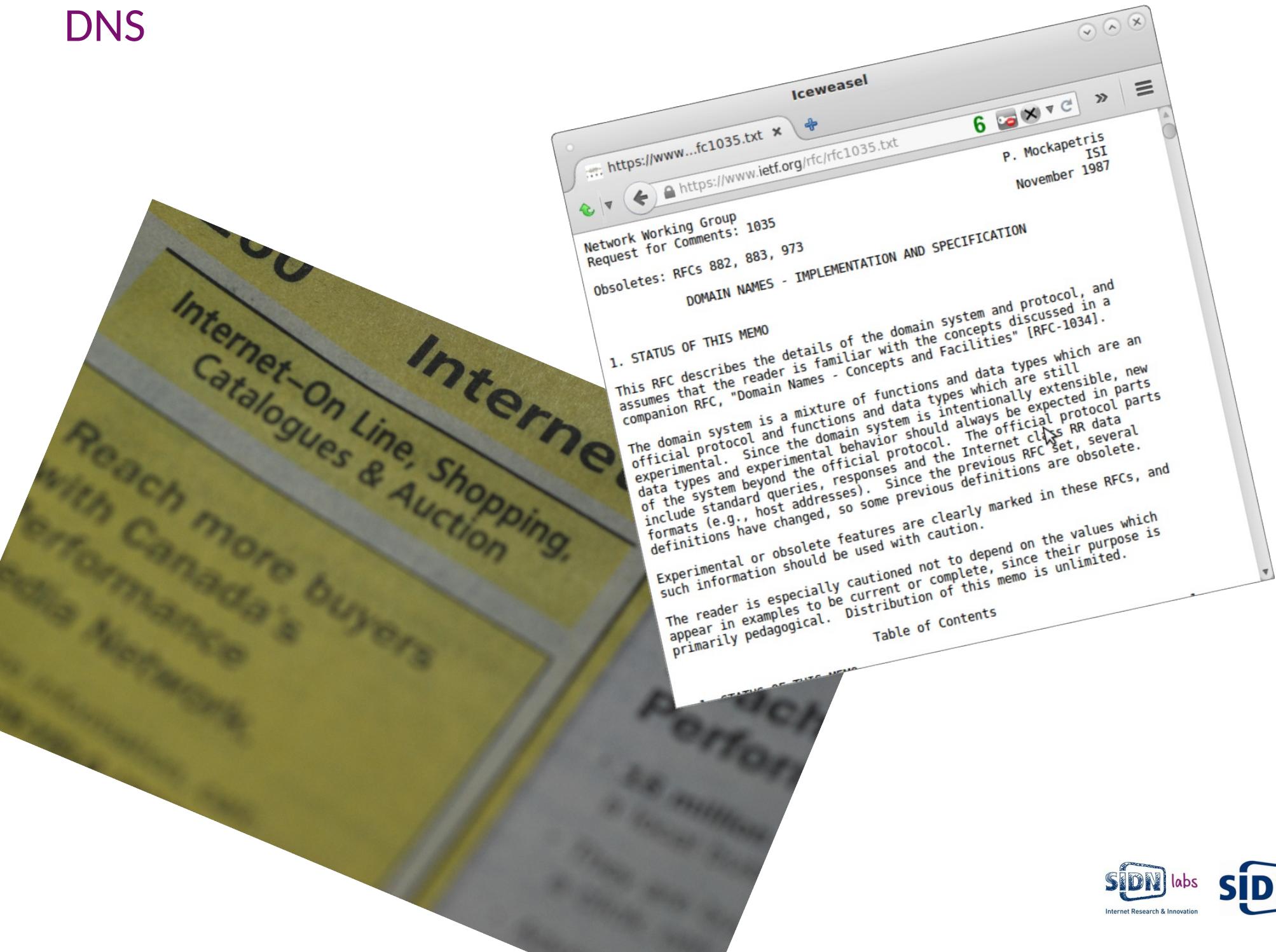
Jelte Jansen

DHPA Techday, 21 mei 2015

DNS



# DNS





Iceweasel

## The Flaw at the Heart of the Internet

DAN KAMINSKY DISCOVERED A FUNDAMENTAL SECURITY PROBLEM IN THE INTERNET AND GOT PEOPLE TO CARE IN TIME TO FIX IT. IT'S A DRAMATIC STORY WITH A HAPPY ENDING ... BUT WE WERE LUCKY THIS TIME.

By ERICA NAONE

of attacks, Kaminsky wrote a little code to make sure the situation was as bad as he thought it was. "Once I saw it work, my stomach dropped," he says. "I thought, 'What the heck am I going to do about this? This affects everything.'"

Kaminsky's technique could be used to direct Web surfers to any Web page an attacker chose. The most obvious use is to send people to phishing sites (websites designed to trick people into entering banking passwords and other personal information, allowing an attacker to steal their identities) or other fake versions of Web pages. But the danger is even worse: protocols such as those used to deliver e-mail or for secure communications over the Internet ultimately rely on DNS. A creative attacker could use Kaminsky's technique to intercept sensitive e-mail, or to create forged versions of the certificates that ensure secure transactions between users and banking websites. "Every day I find another domino," Kaminsky says. "Another thing falls over if DNS is bad ... I mean, literally, you look around and see anything that's using a network—anything that's using a network—and it's probably using DNS."

Normally, DNS is reliable but not nimble. When a computer—say, a server that helps direct traffic across Comcast's network—requests the numerical address associated with a given URL, it stores the answer for a period of time known as "time to live," which can be anywhere from seconds to days. This helps to reduce the number of requests the server makes. Kaminsky's idea was to bypass the time to live, allowing the server to get a fresh answer every time it wanted to know a site's address. Consequently, traffic on Comcast's network would be sent to the optimal address at every moment, rather than to whatever address had already been stored. Kaminsky was sure that the strategy could significantly speed up content distribution.

It was only later, after talking casually about the idea with a friend, that Kaminsky realized his "trick" could completely break the security of the domain name system and, therefore, of the Internet itself. The time to live, it turns out, was at the core of DNS security; being able to bypass it allowed for a wide variety

Kaminsky called Paul Vixie, president of the Internet Systems Consortium, a nonprofit corporation that supports several aspects of Internet infrastructure, including the software most commonly used in the domain name system. "Usually, if somebody wants to report a problem, you expect that it's going to take a fair amount of time for them to explain it—maybe a whiteboard, maybe a Word document or two," Vixie says. "In this case, it took 20 seconds for him to explain the problem, and another 20 seconds for him to answer my objections. After that, I said, 'Dan, I am speaking to you over an unsecure cell phone. Please do not ever say to anyone what you just said to me over an unsecure cell phone again.'"

Perhaps most frightening was that because the vulnerability was not located in any particular hardware or software but in the design of the DNS protocol itself, it wasn't clear how to fix it. In secret, Kaminsky and Vixie gathered together some of the top DNS experts in the world: people from the U.S. government and

Photograph by JOHN KEATLEY

FEATURE STORY 63



## 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.**



By ERICA NAONE

Dan Kaminsky, uncharacteristically, was not looking for bugs earlier this year when he happened upon a flaw at the core of the Internet. The security researcher was using his knowledge of Internet infrastructure to come up with a better way to stream videos to users. Kaminsky's expertise is in the Internet's domain name system (DNS), the protocol responsible for matching websites' URLs with the numeric addresses of the servers that host them. The same content can be hosted by multiple servers with several addresses, and Kaminsky thought he had a great trick for directing users to the servers best able to handle their requests at any given moment.

Normally, DNS is reliable but not nimble. When a computer—say, a server that helps direct traffic across Comcast's network—requests the numerical address associated with a given URL, it stores the answer for a period of time known as "time to live," which can be anywhere from seconds to days. This helps to reduce the number of requests the server makes. Kaminsky's idea was to bypass the time to live, allowing the server to get a fresh answer every time it wanted to know a site's address. Consequently, traffic on Comcast's network would be sent to the optimal address at every moment, rather than to whatever address had already been stored. Kaminsky was sure that the strategy could significantly speed up content distribution.

It was only later, after talking casually about the idea with a friend, that Kaminsky realized his "trick" could completely break the security of the domain name system and, therefore, of the Internet itself. The time to live, it turns out, was at the core of DNS security; being able to bypass it allowed for a wide variety

of attacks. Kaminsky wrote a little code to make sure the situation was as bad as he thought it was. "Once I saw it work, my stomach dropped," he says. "I thought, 'What the heck am I going to do about this? This affects everything.'"

Kaminsky's technique could be used to direct Web surfers to any Web page an attacker chose. The most obvious use is to send people to phishing sites (websites designed to trick people into entering banking passwords and other personal information, allowing an attacker to steal their identities) or other fake versions of Web pages. But the danger is even worse: protocols such as those used to deliver e-mail or for secure communications over the Internet ultimately rely on DNS. A creative attacker could use Kaminsky's technique to intercept sensitive e-mail, or to create forged versions of the certificates that ensure secure transactions between users and banking websites. "Every day I find another domino," Kaminsky says. "Another thing falls over if DNS is bad.... I mean, literally, you look around and see anything that's using a network—anything that's using a network—and it's probably using DNS."

Kaminsky called Paul Vixie, president of the Internet Systems Consortium, a nonprofit corporation that supports several aspects of Internet infrastructure, including the software most commonly used in the domain name system. "Usually, if somebody wants to report a problem, you expect that it's going to take a fair amount of time for them to explain it—maybe a whiteboard, maybe a Word document or two," Vixie says. "In this case, it took 20 seconds for him to explain the problem, and another 20 seconds for him to answer my objections. After that, I said, 'Dan, I am speaking to you over an unsecure cell phone. Please do not ever say to anyone what you just said to me over an unsecure cell phone again.'

Perhaps most frightening was that because the vulnerability was not located in any particular hardware or software but in the design of the DNS protocol itself, it wasn't clear how to fix it. In secret, Kaminsky and Vixie gathered together some of the top DNS experts in the world: people from the U.S. government and

Photograph by JOHN KEATLEY

FEATURE STORY 63



## 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 attack exploited in the wild

**Summary:** UPDATE: Arbor Networks have provided more details in their "30 Days of DNS analysis," SANS confirmed HD Moore's statement on DNS cache poisoning AT&T independent sources are starting to see evidence of attempts on their local networks, in what appears to be an attempt to take advantage of the "recent" DNS cache poisoning vulnerability :"client 143.



By Dancho Danchev for Zero Day | July 29, 2008 -- 03:24 GMT (04:24 ET)

[Get the ZDNet Security newsletter now](#)

**UPDATE:** Arbor Networks have provided more details in their "30 Days of DNS analysis," SANS confirmed HD Moore's statement on DNS cache poisoned AT&T independent sources are starting to see evidence of DNS cache poisoning attempts on their local networks, in what appears to be an attempt to take advantage of the "recent" DNS server at AT&T is NOT overtly vulnerable, however, it may be subtly vulnerable if POOR or FAIR.

Test Rating Notes Scatterplot



## 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 attack exploited in the wild

**Summary:** UPDATE: Arbor Networks have provided more details in their "DNS Cache Poisoning and Denial of Service in the Wild" analysis, SANS confirmed HD Moore's statement on DNS cache poisoning attacks. Numerous independent sources are starting to see evidence of DNS cache poisoning attempts on their local networks, in what appears to be an attempt to take down websites.

## DNS poisoning slams web traffic from millions in China into the wrong hole

**ISP blames unspecified attack for morning outage**

By John Leyden, 21 Jan 2014

# DNS



## 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.



[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

**ISP**

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.

## DNS cache poisoning attack exploited in the wild

*we provided more details in their HD Moore's statement on DNS c...  
es are starting to see evidence of...  
appears to be an attempt to take o...  
" " "*

**millions**

**s of surfers adrift.**

# DNSSEC in vogelvlucht: Signeren



# DNSSEC in vogelvlucht: Signeren



## RRSIG

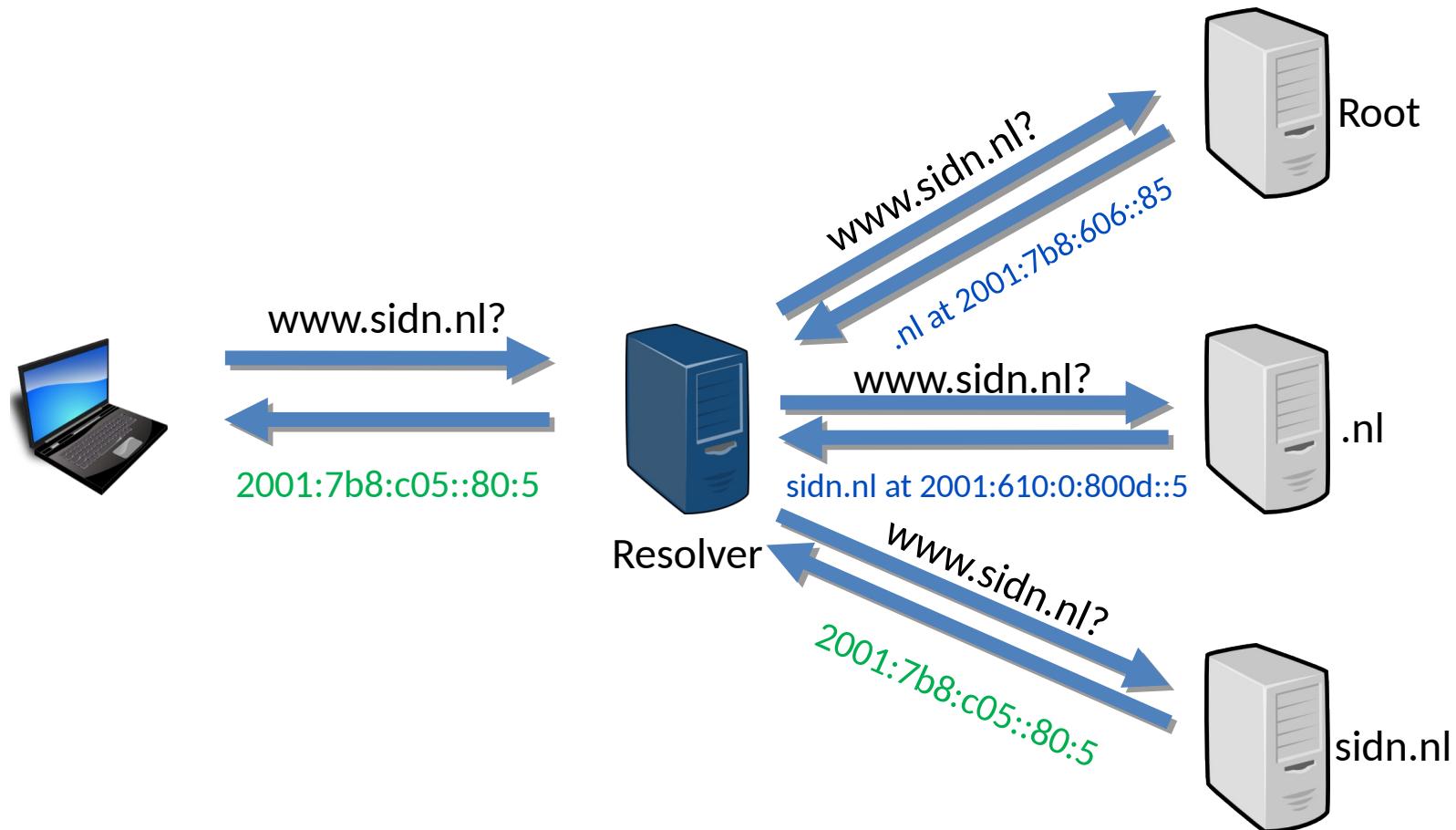
```
example.dom. 7200 RRSIG SOA 5 3 7200
20131113113016 (
    20131014113016 57798 example.dom.
    TWLzBuUgXWMA9cj+xe6YMjXy2/VdauWnONk7
    uAP8JcdzsemcfWov4cFzXowS2YX291+5jBMp
    m5AlwpM7ijjbSBgAGz22yw1KN8JoOg3KtCM2Y
    UX/c8/ATbYEWPKRjBs+YQKmY1NppwSjFi9Y0
    1fVEBbrCnI0EP33c/VK97s8oNG8= )
```

# DNSSEC in vogelvlucht: signen

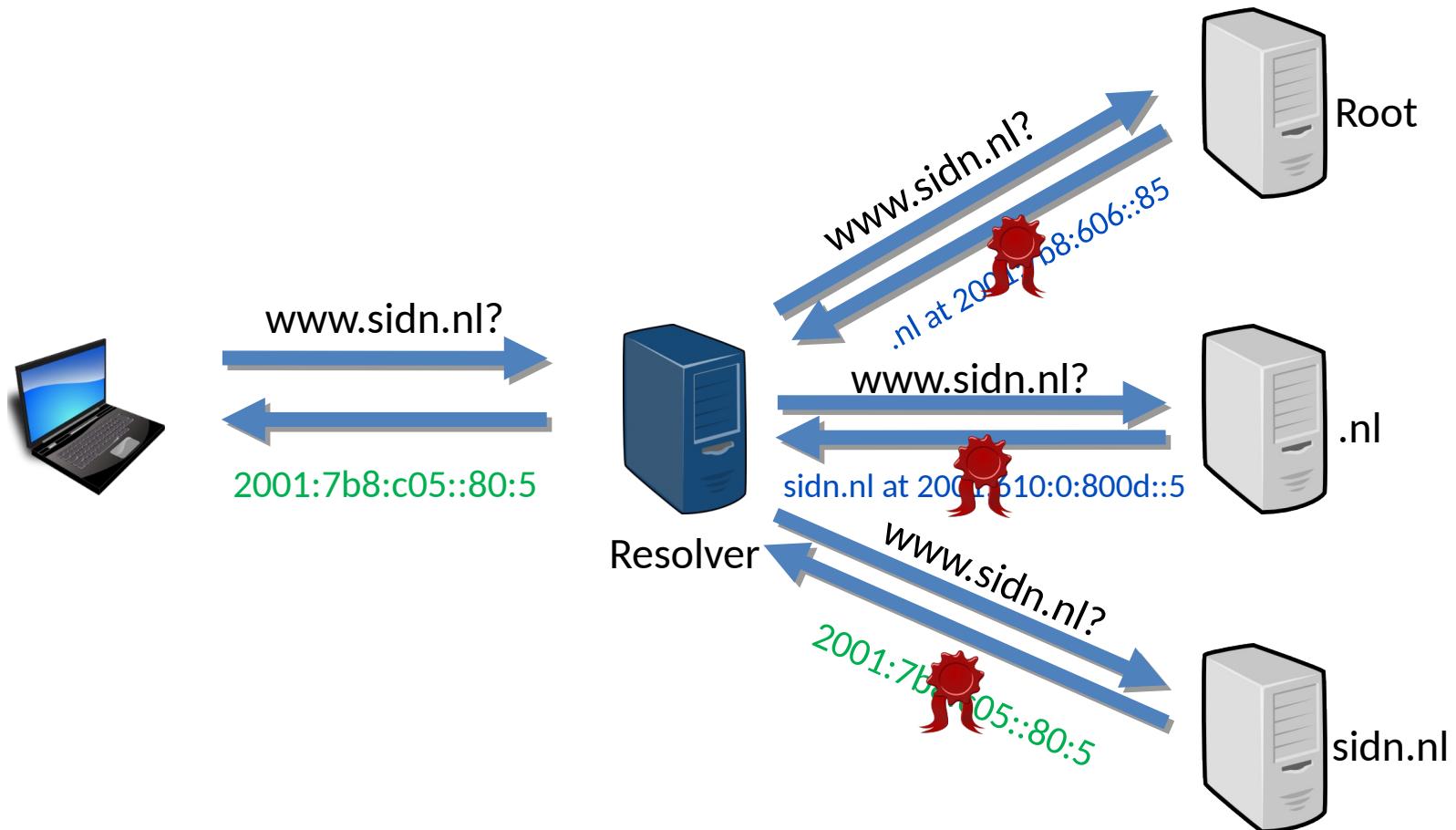
- Maak een keypair aan
- Sign je zone(s)
  - BIND, NSD+ldns, PowerDNS, Secure64, Infoblox, etc.
- Publiceer gesigneerde zones
- Stuur public key naar parent



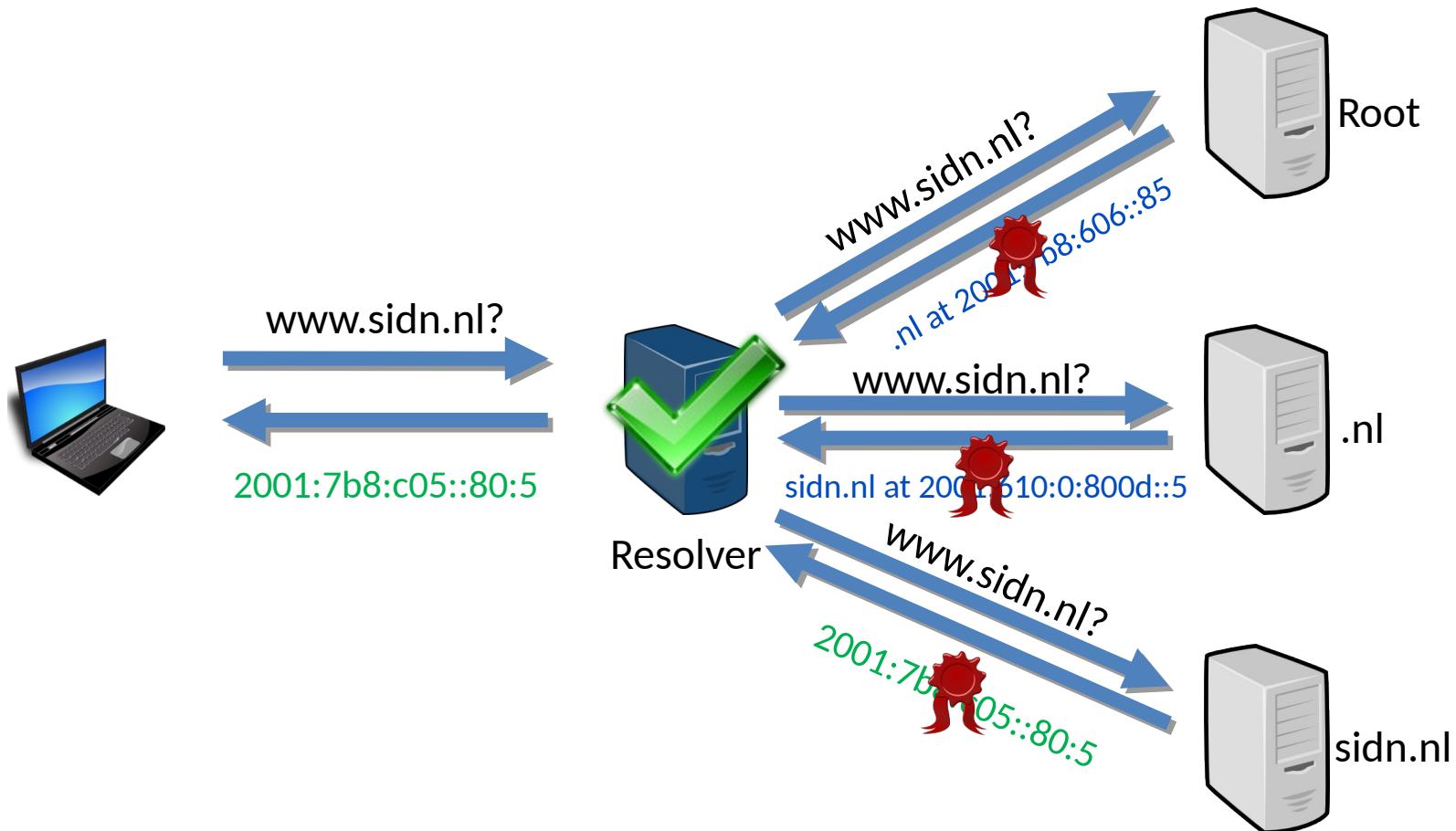
# DNSSEC in vogelvlucht



# DNSSEC in vogelvlucht



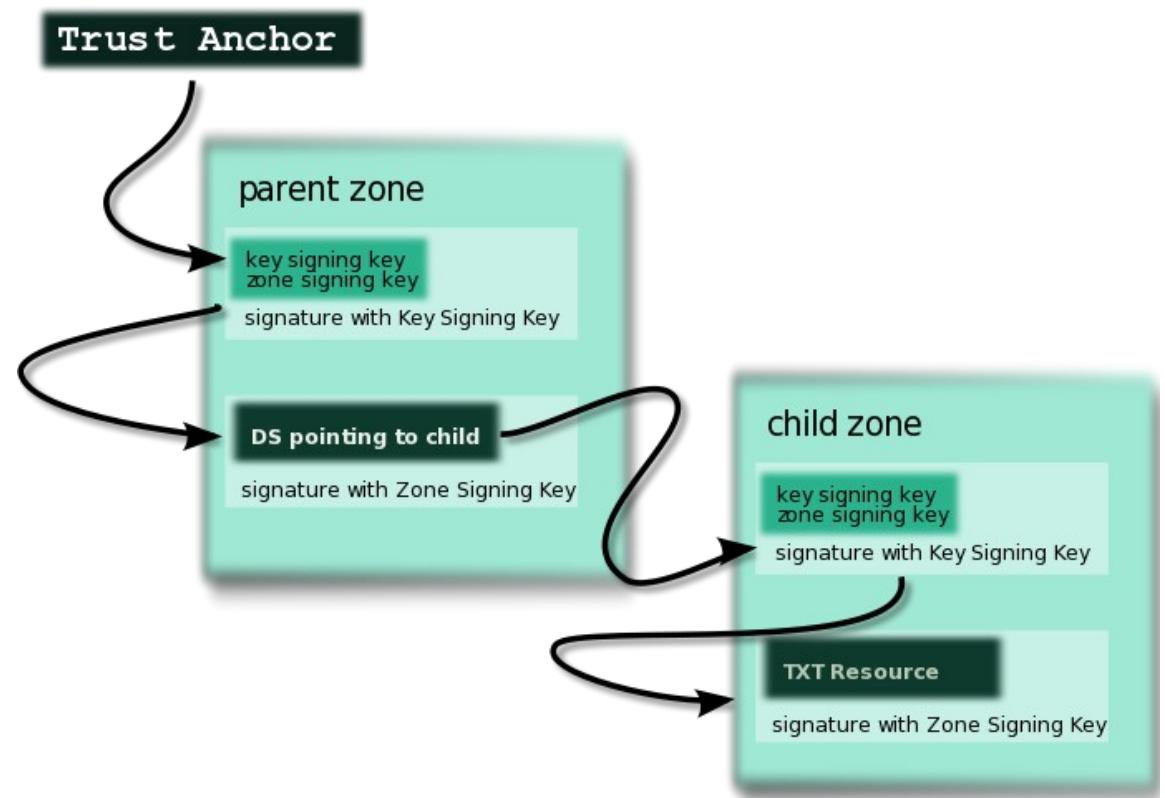
# DNSSEC in vogelvlucht



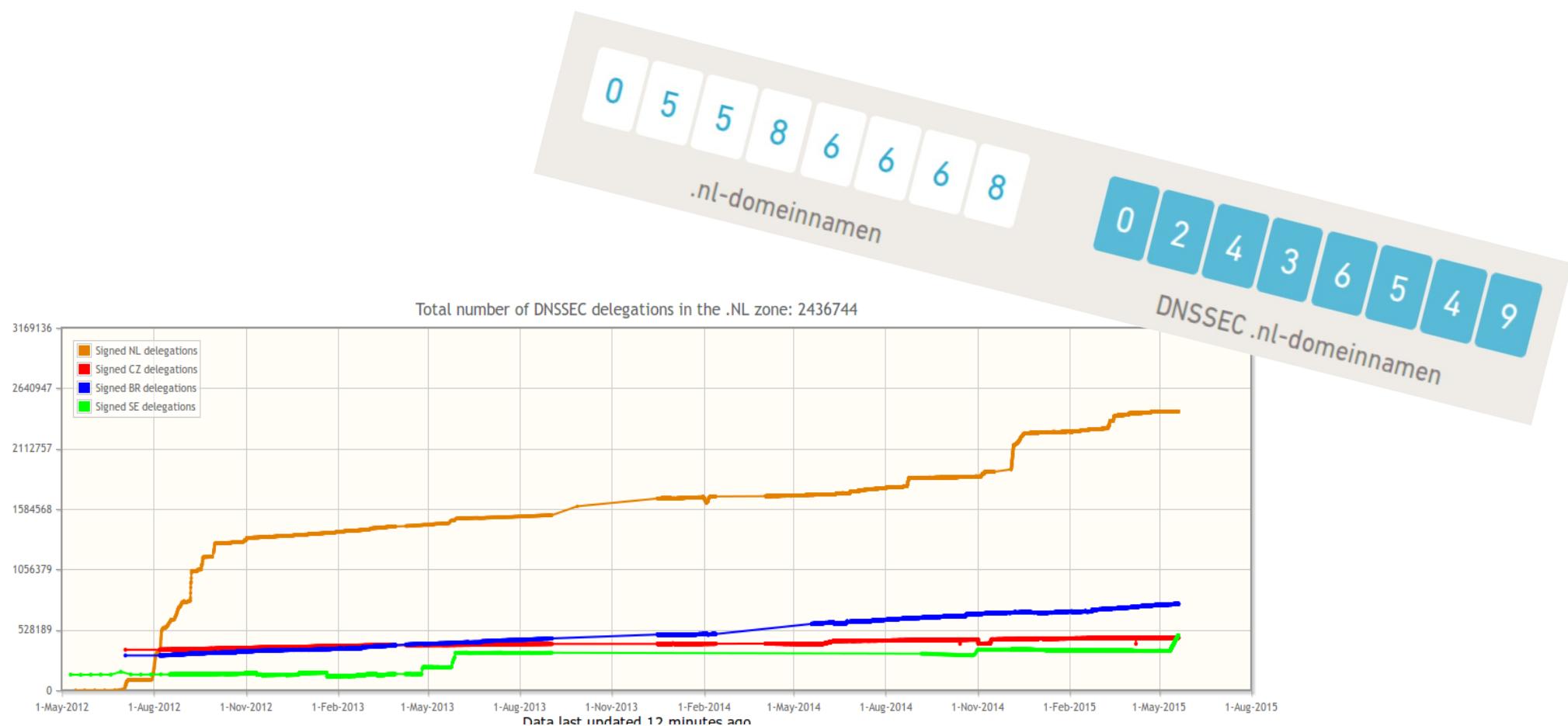
# DNSSEC in vogelvlucht: chain of trust

- Chain of trust:

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

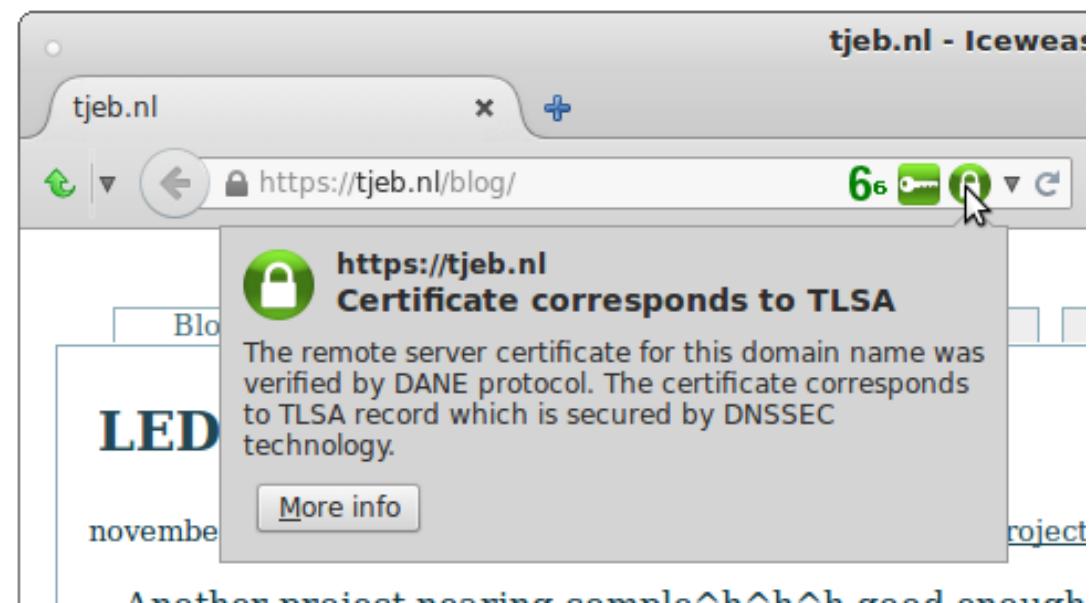


# DNSSEC in .nl: zones



# 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
  - Idns
- 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 explicet 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

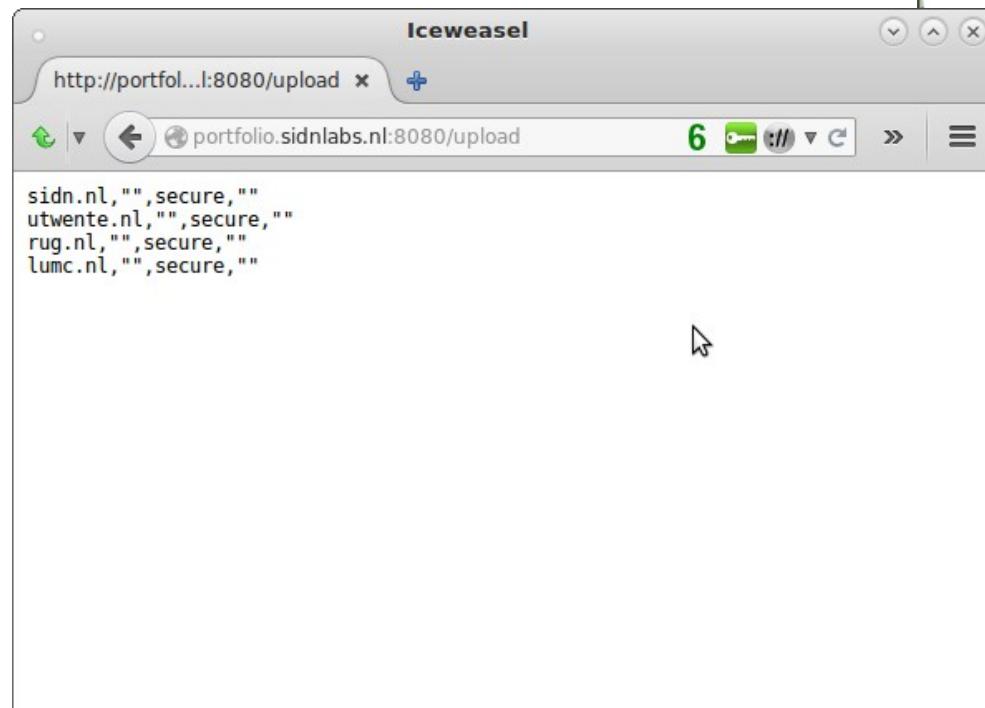
# DNSSEC Test sites

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

The screenshot shows a Mozilla Firefox browser window with the title "SIDN Labs Portfolio Checker - Mozilla Firefox". The address bar displays "portfolio.sidnlabs.nl:8080/form". The page itself is titled "SIDN Labs Portfolio Checker" and indicates "Versie 20130417". It features a large "SIDN labs" logo with the tagline "Internet Research & Innovation". Below the logo, there's a section titled "Selecteer een CSV bestand met domeinnamen" with a "Browse..." button and a file named "test.csv". To the right of this is a "Controleer" button. Further down, there's a "FAQ" section and a "Hoe wordt er gecontroleerd?" section. The "Hoe wordt er gecontroleerd?" section contains text explaining the DNSSEC validation process using Unbound and NS-records, noting a limit of 10000 domain names per run. The overall design has a light blue and white color scheme with a grid pattern in the background.

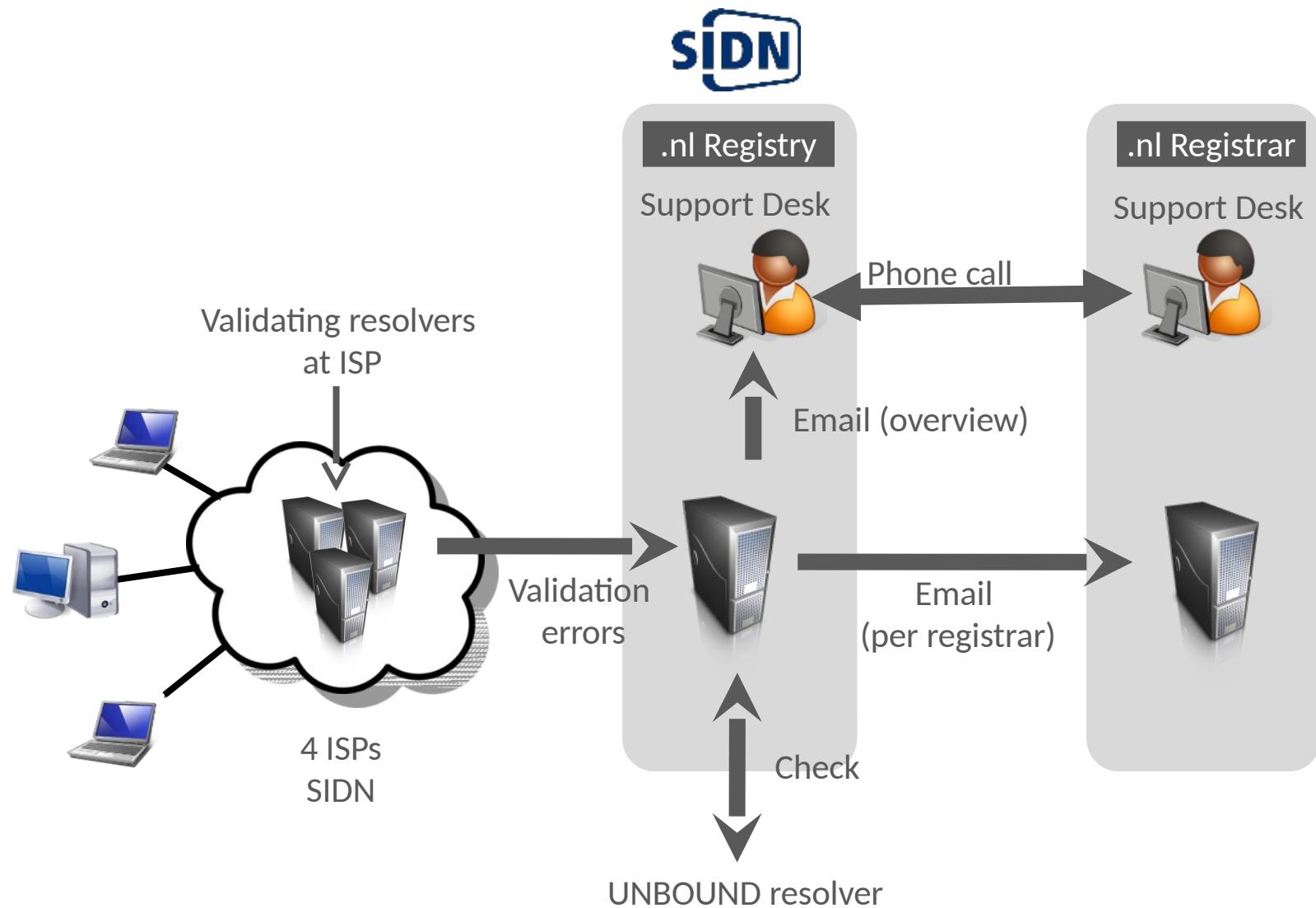
# DNSSEC Test sites

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

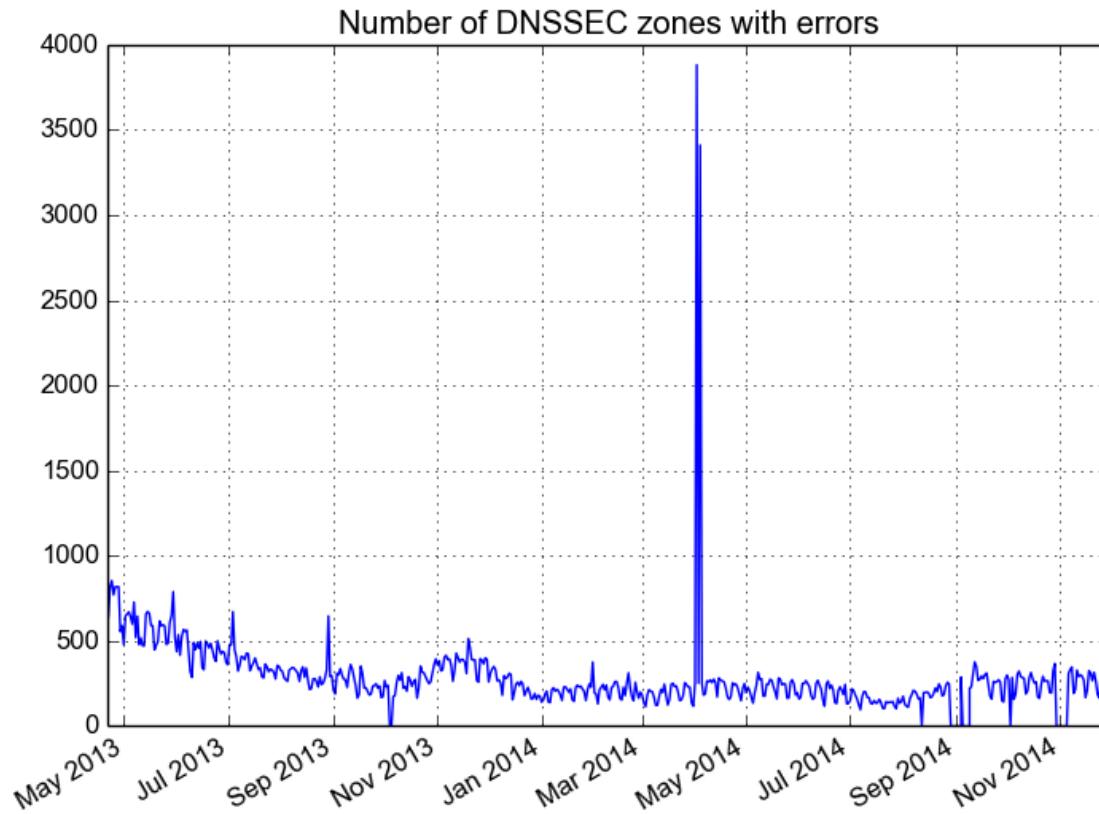


A screenshot of the SIDN Labs Portfolio Checker website in Mozilla Firefox. The page title is 'SIDN Labs Portfolio Checker - Mozilla Firefox'. The main header features the SIDN logo and the text 'Internet Research &amp; Innovation'. Below the header, the page title is 'SIDN Labs Portfolio Checker' and the subtext 'Versie 20130417'. A descriptive paragraph explains the tool's purpose: 'Als je een flink aantal domeinnamen hebt en je wilt deze beveiligen met DNSSEC, dan bestaat altijd het gevaar dat je een paar details over het hoofd ziet en niet alle domeinen correct gesigned zijn. SIDN Labs heeft daarom de DNSSEC Portfolio Checker ontwikkeld, waarmee je dit op een snelle en eenvoudige manier kunt controleren.' A section titled 'Selecteer een CSV bestand met domeinnamen' contains a 'Browse...' button set to 'test.csv' and a 'Controleer' button. Another section titled 'FAQ' includes a question 'Hoe wordt er gecontroleerd?' with an explanatory answer. The bottom right corner of the browser window shows the SIDN logo.

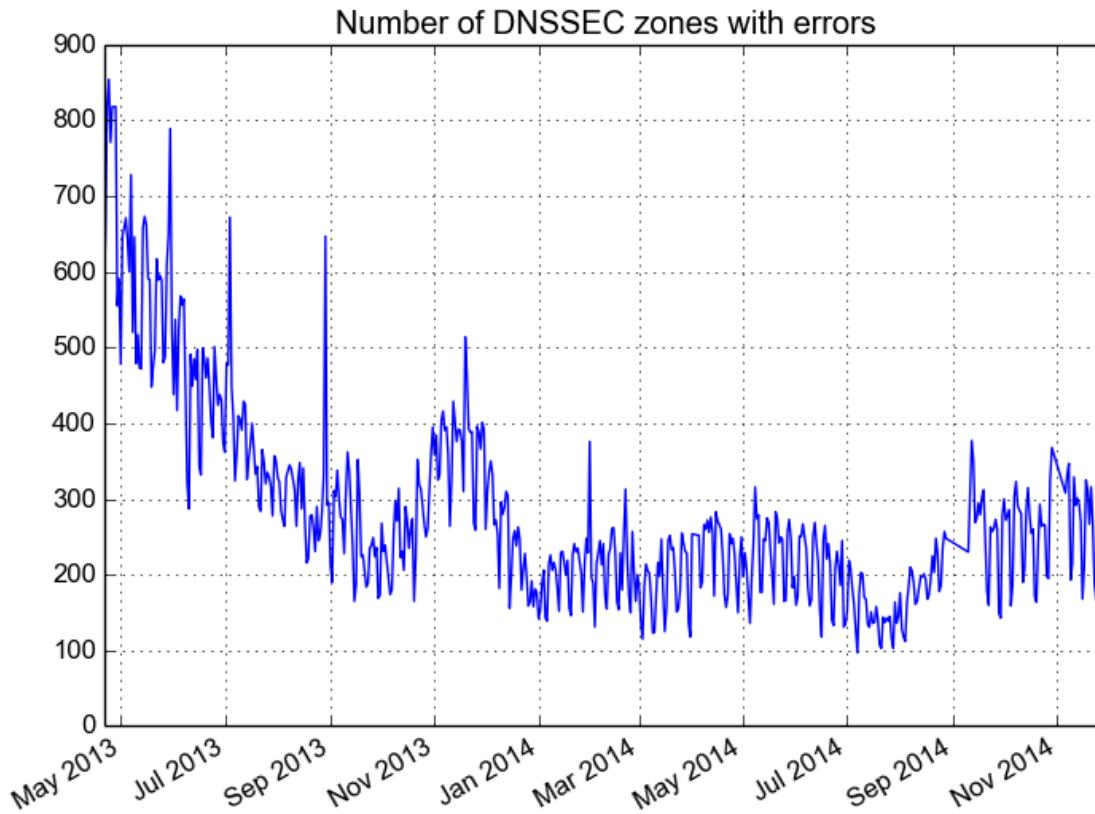
# DNSSEC validatie monitor



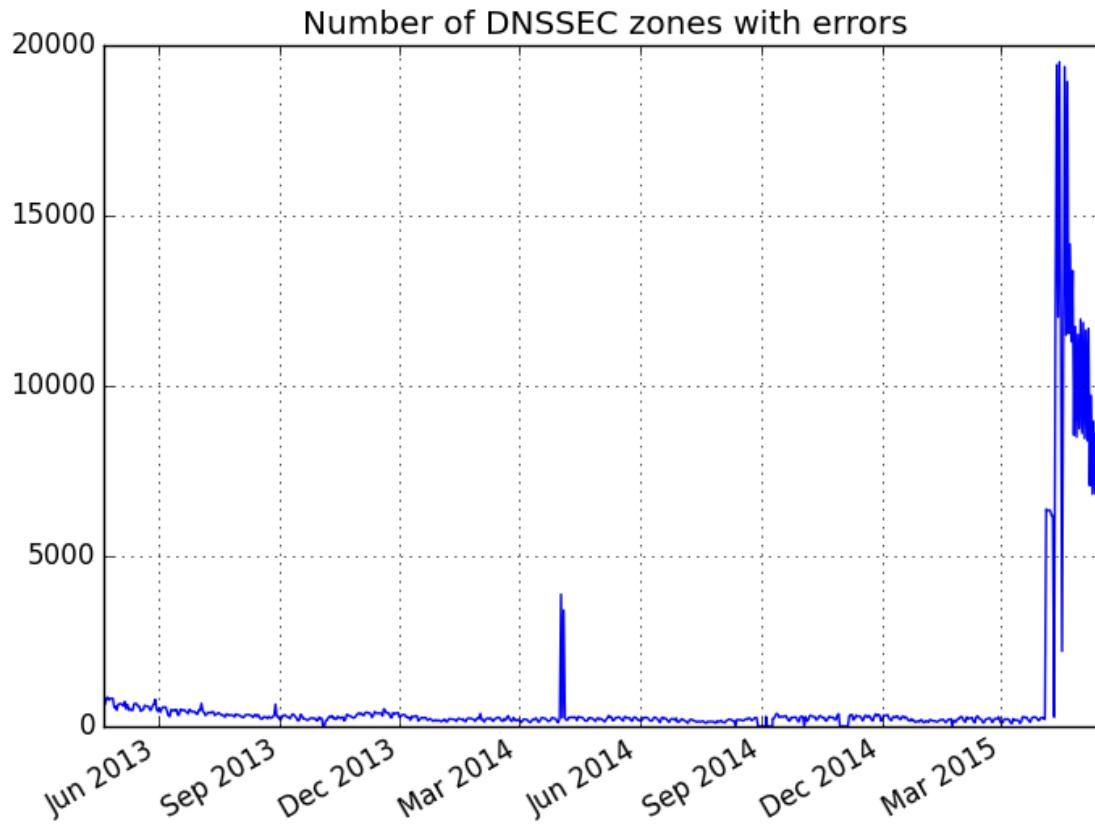
# Validatie errors



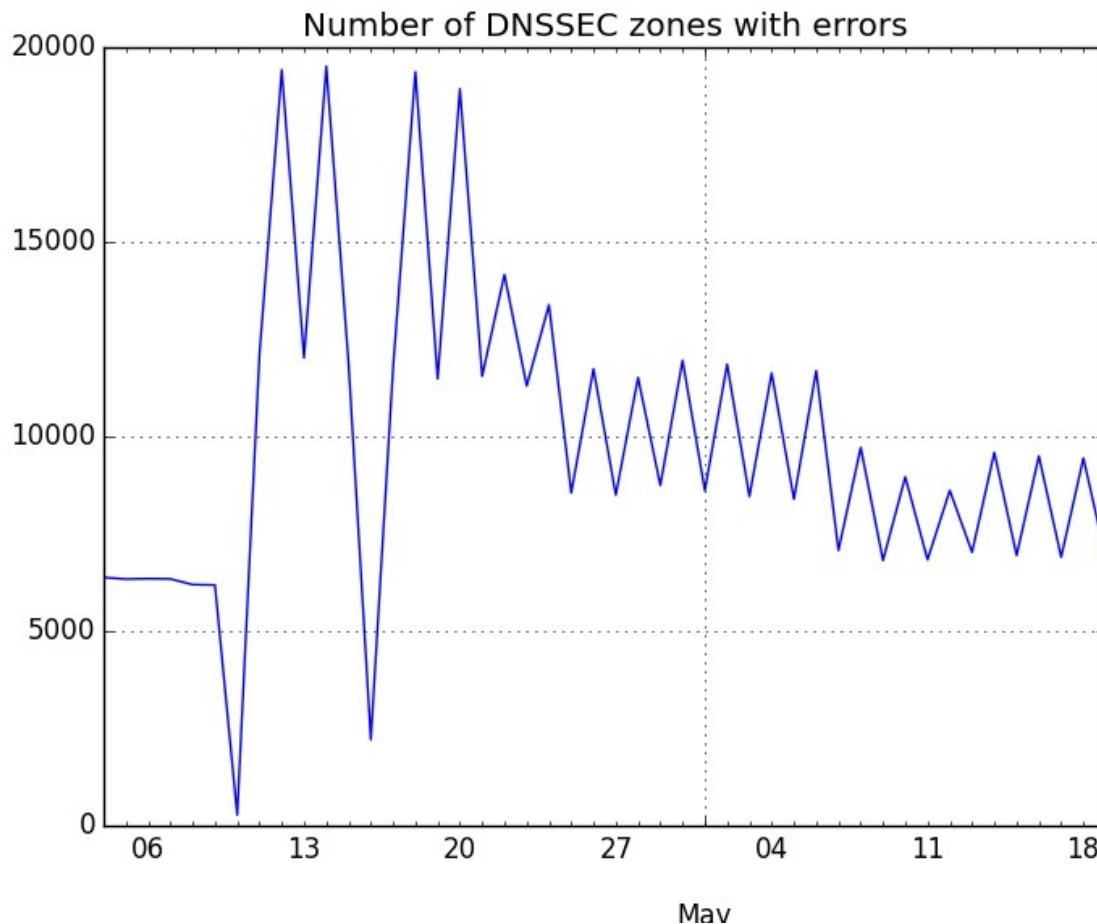
# Validatie errors



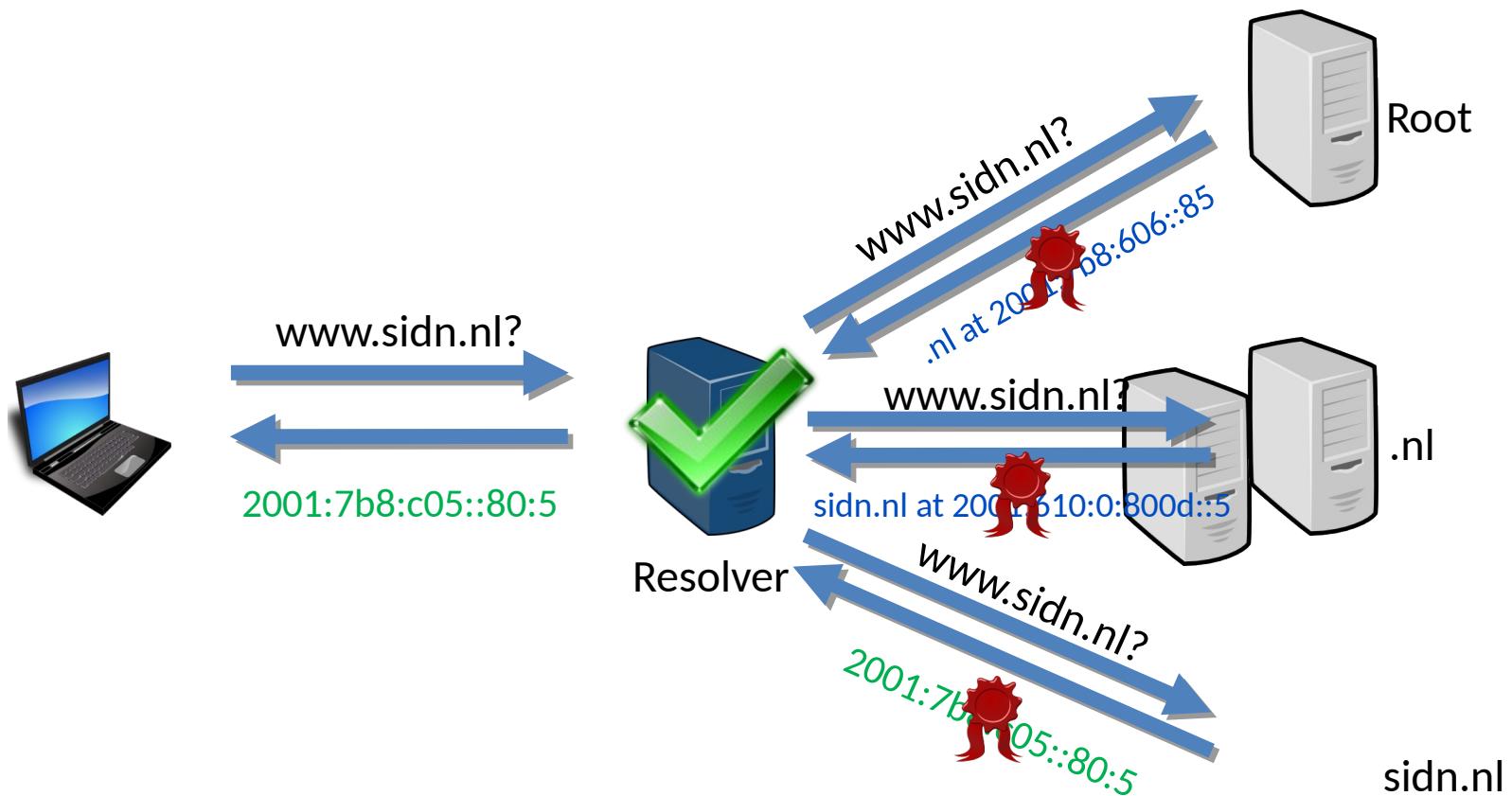
# Validatie errors



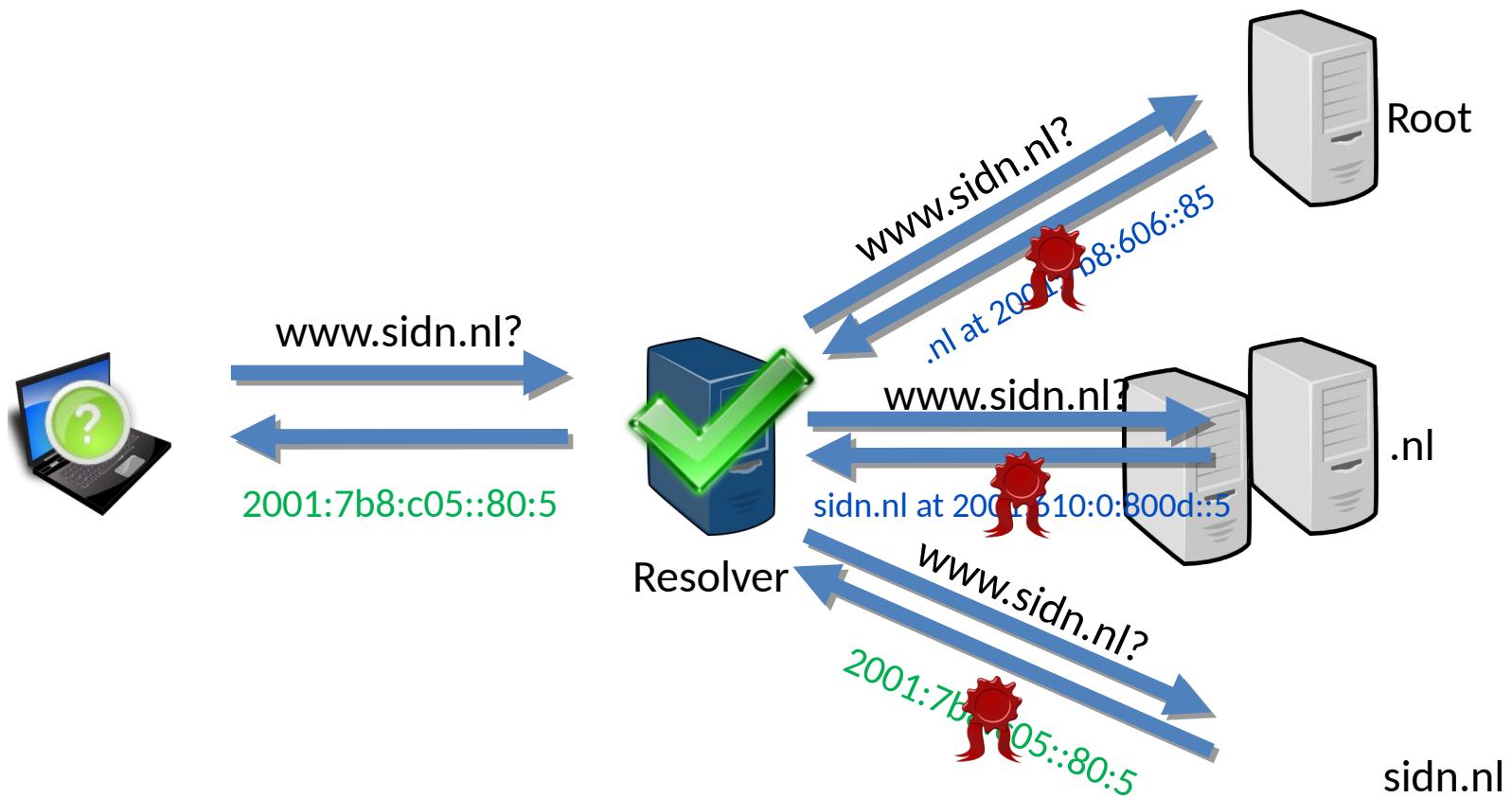
# Validatie errors



# DNSSEC in vogelvlucht



# DNSSEC in vogelvlucht



# DNSSEC Test sites

- Validatie:
  - <https://dnssectest.sidnlabs.nl>



# DNSSEC Test sites

- Validatie:

- [dnssectest.sidnlabs.nl/](http://dnssectest.sidnlabs.nl/)

The screenshot shows two Mozilla Firefox browser windows side-by-side, both displaying the SIDN DNSSEC test page at [dnssectest.sidnlabs.nl/](http://dnssectest.sidnlabs.nl/).

**Left Window (Test Result):**

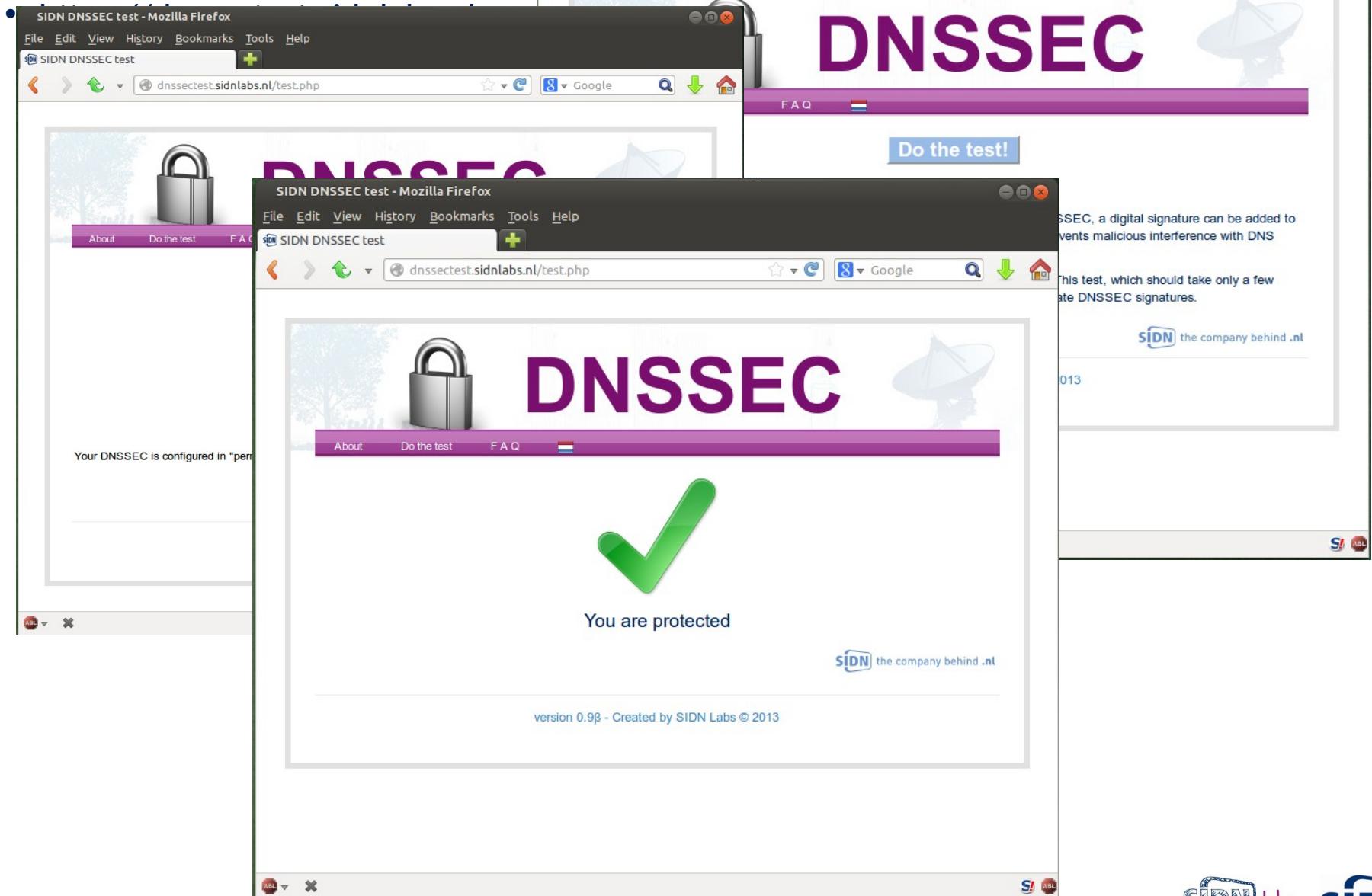
- Header:** SIDN DNSSEC test - Mozilla Firefox
- Title Bar:** dnssectest.sidnlabs.nl
- Content:**
  - Header:** DNSSEC
  - Image:** A large red 'X' icon.
  - Text:** You are not protected
  - Text:** Permissive mode detected:  
Your DNSSEC is configured in "permissive mode" (or you use a combination of validating- and non-validating resolvers) and as such you are not protected.
  - Footer:** version 0.9β - Created by SIDN Labs © 2013

**Right Window (FAQ Page):**

- Header:** SIDN DNSSEC test - Mozilla Firefox
- Title Bar:** dnssectest.sidnlabs.nl
- Content:**
  - Header:** DNSSEC
  - Image:** A satellite dish icon.
  - Section:** FAQ
  - Text:** Do the test!
  - Text:** What is DNSSEC? It is a recently deployed extension to the DNS Protocol. With DNSSEC, a digital signature can be added to the DNS data, and the recipient can validate the signature. This prevents malicious interference with DNS data.
  - Text:** Both the server and the client understand and support it. This test, which should take only a few seconds, will tell you whether the client computer you are using is able to validate DNSSEC signatures.
  - Footer:** SIDN the company behind .nl

# DNSSEC Test sites

- Validatie:



# DNSSEC Informatiesites

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



# 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>

