

# Commencing countdown: DNSSEC on!

USENIX LISA '10, San Jose, CA

Roland van Rijswijk  
roland.vanrijswijk [at] surfnet.nl

November 10<sup>th</sup>, 2010

# About SURFnet

 SURF  
NET

National Research and Education Network (NREN)

Founded in 1986

10628 km ( $\pm 6604$  mi.) of fibre-optic cables for an ultra high-bandwidth network

‘Shared ICT innovation centre’

$\geq 160$  connected institutions  
 $\pm 1$  million end-users



# International co-operation

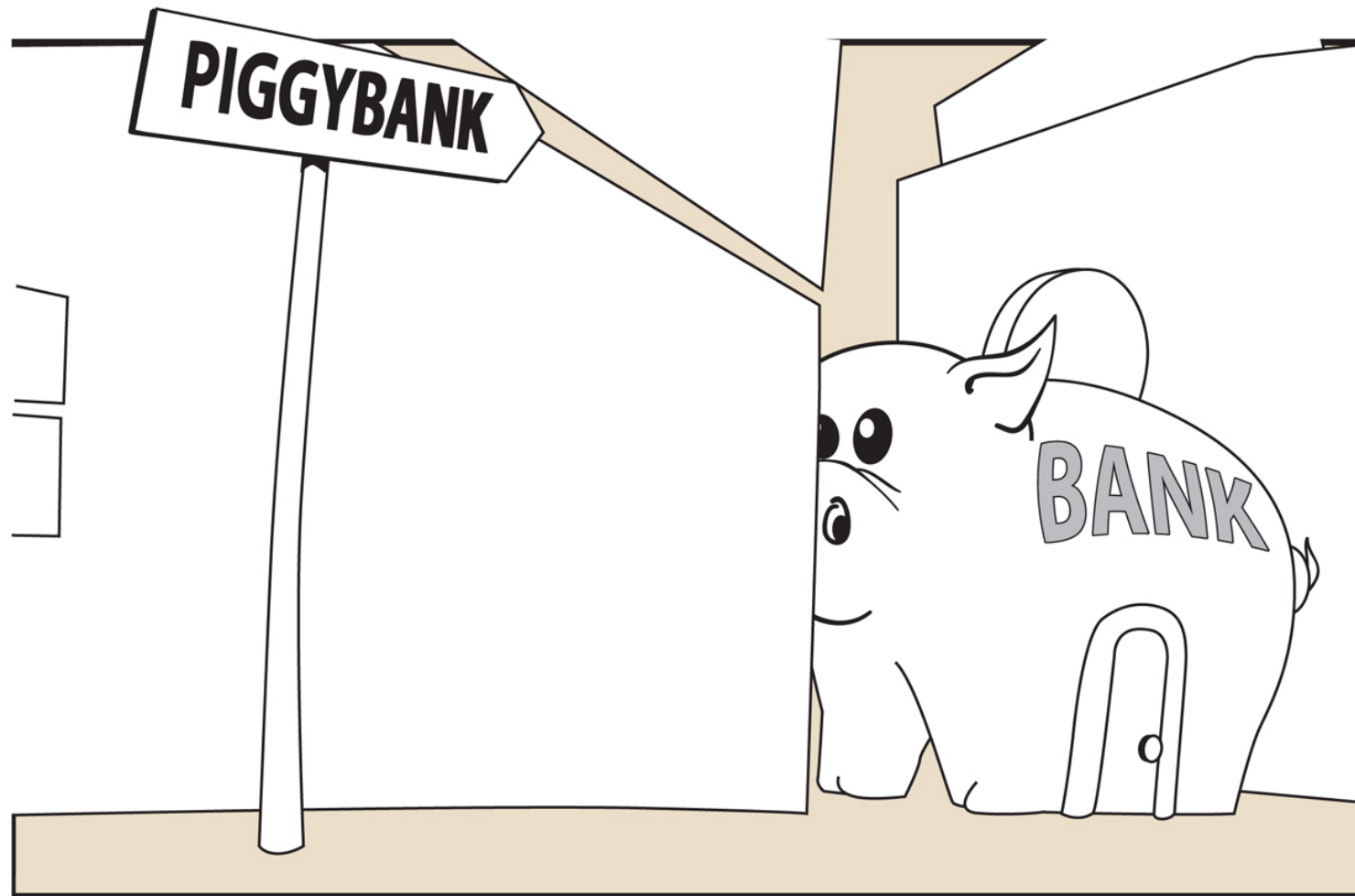


# Overview

- Intro & short recap: DNSSEC, why & what?
- Resolving
- Operating signed zones
- Lessons learned
- Monitoring
- Conclusion & questions

SURFnet. We make innovation work

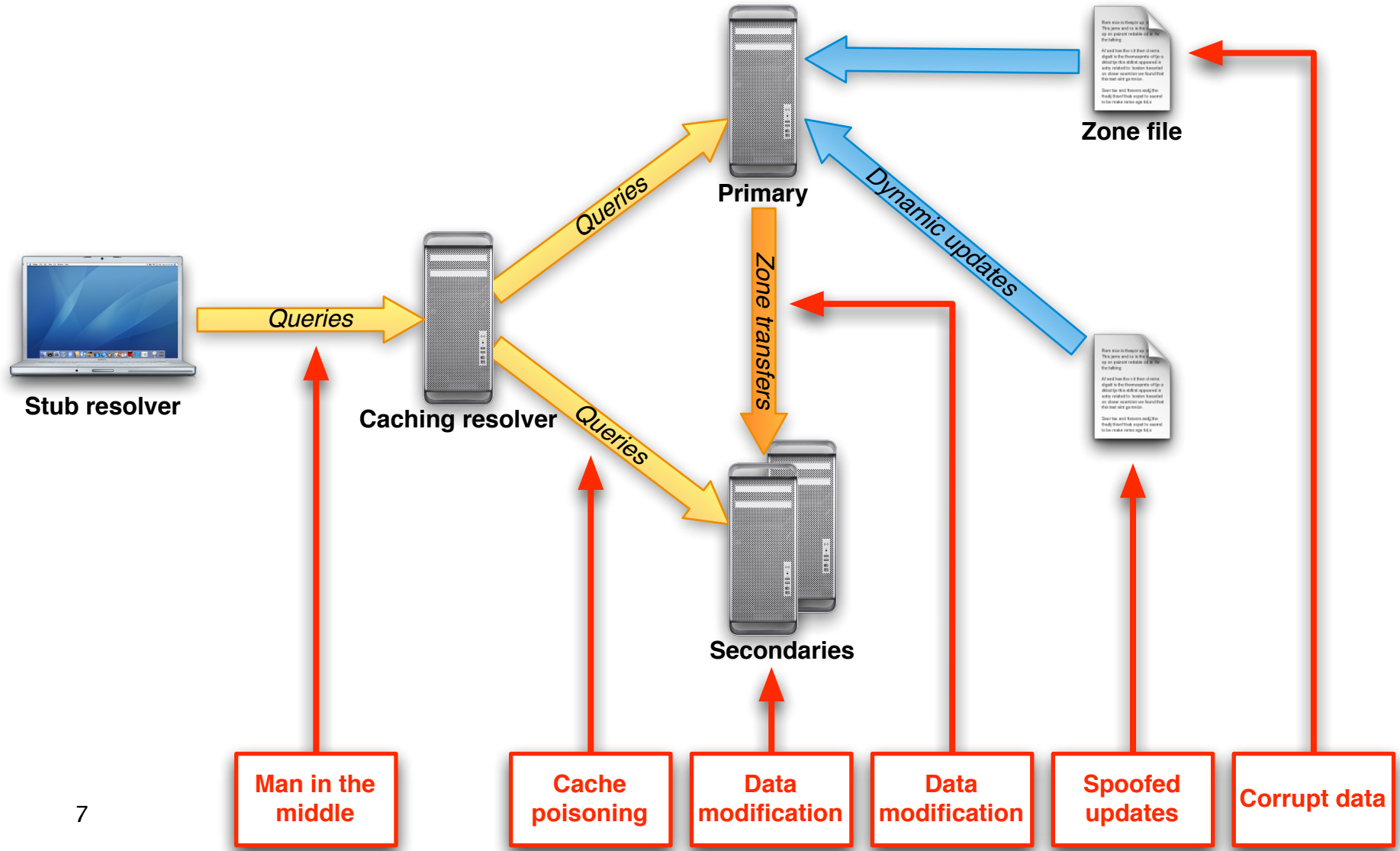
# DNS: TomTom™ for the Internet



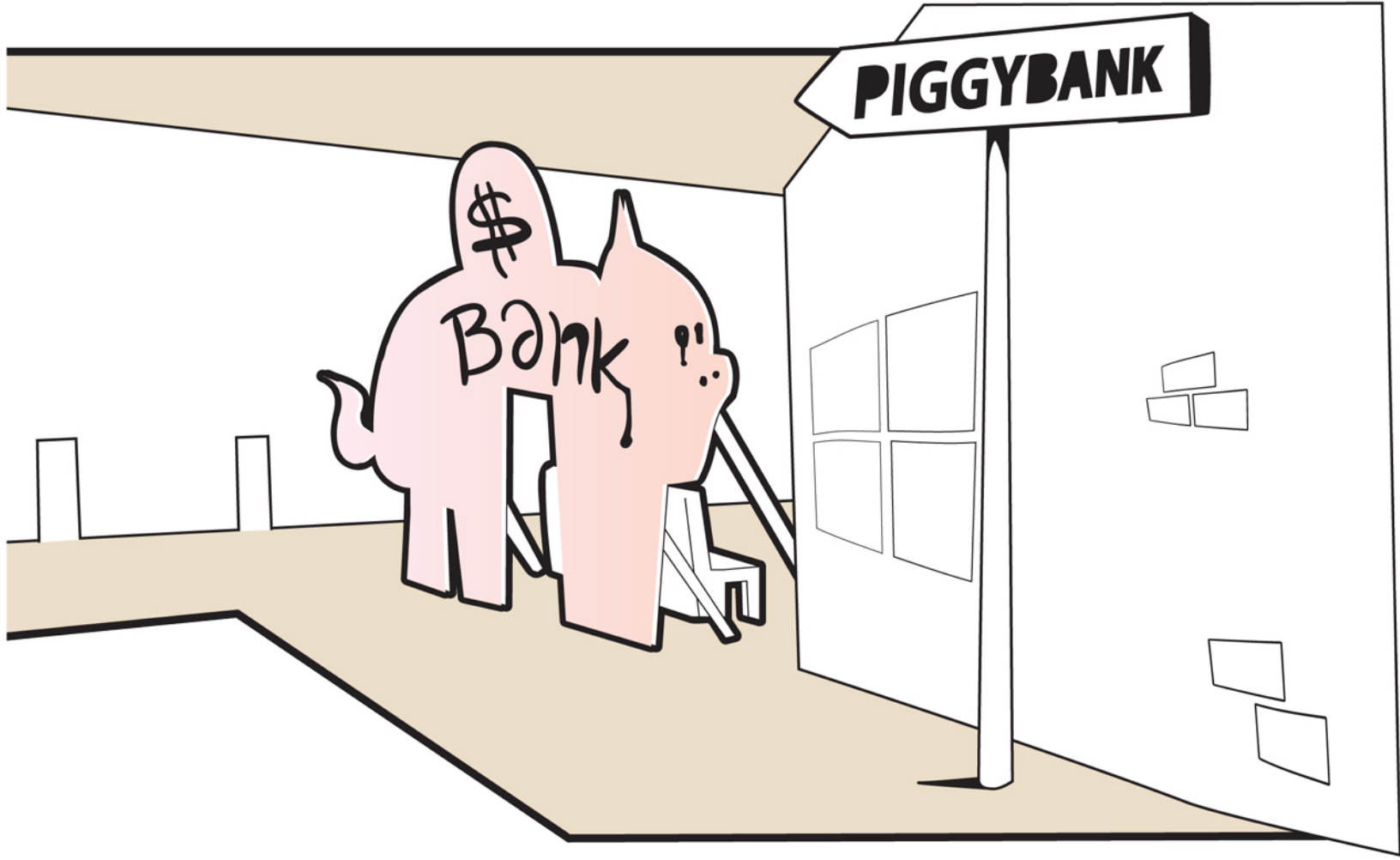
# Why attack DNS?

- DNS is **everywhere**:
  - In your phone, in your laptop, in your PC...
  - But also in your car, in an ATM, in your elevator, ...
- It is very hard to protect plain DNS against attacks
- It is very easy to attack a lot of users

# DNS attack vectors



# Cache poisoning





# Bad news...

Breaking  
Bad  
News  
with  
Baby  
Animals



Amanda  
McCall  
&  
Ben  
Schwartz



## Grandma's Dead

<http://lambicpeach.files.wordpress.com/2008/10/badnewspup.jpg>



**Good news :-)**

# DNSSEC

# What is DNSSEC?

- DNSSEC was first devised in 1997
- We are at the third generation of the protocol
  - DNSSEC (ca. 2000)
  - DNSSECbis (2005)
  - NSEC3 (2008)
- Some 20 (!) active RFCs
  - That's excluding the 'normal' DNS RFCs
- Protocol is mature
  - Changes are mainly new algorithms





# What is DNSSEC?

- Digital Signatures guarantee authenticity of DNS records
  - Like a wax seal
- Resolvers validate the signatures and discard records with bogus signatures
- DNSSEC **only** provides authenticity
  - So no confidentiality
  - nor protection against DDoS
  - or typosquatting, phishing, etc.

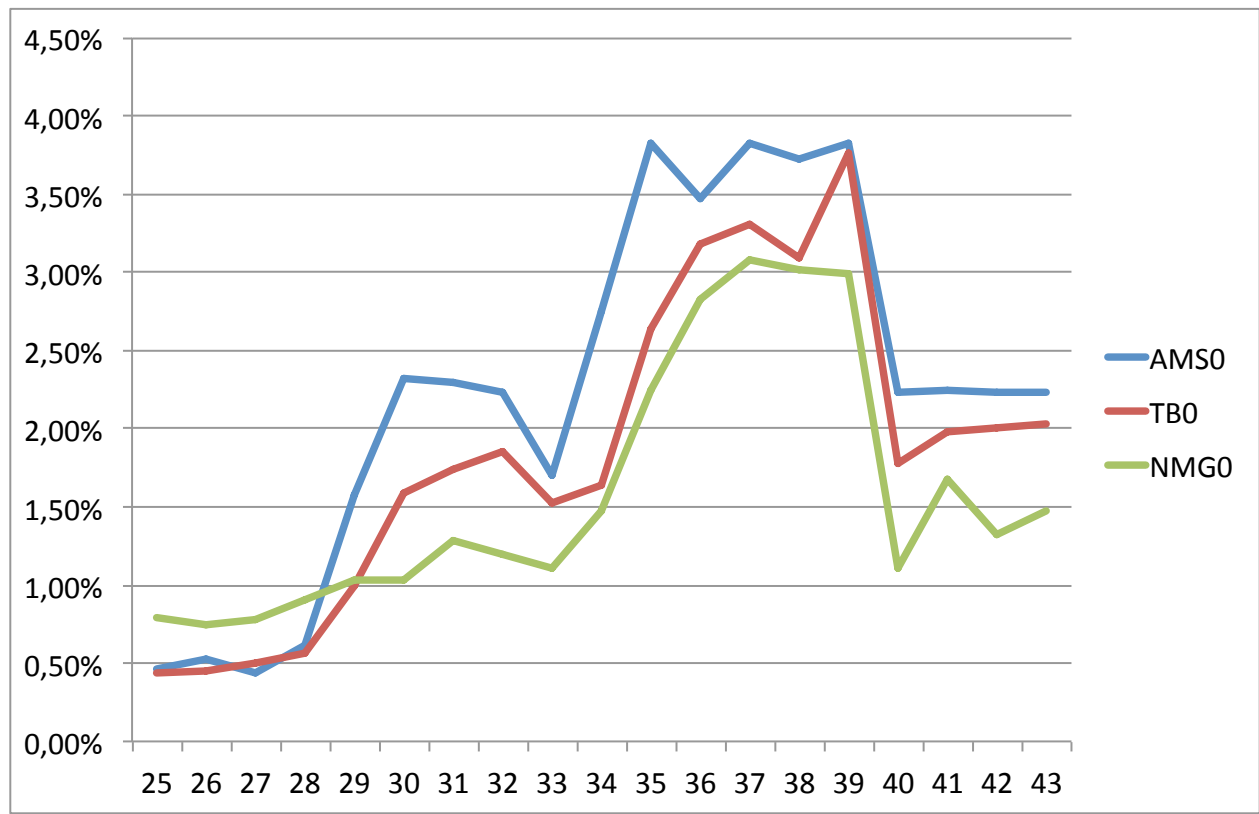


# Deployment status

- Root was signed on July 15<sup>th</sup>
  - Signed generic TLDs:  
.asia, .biz, .cat, .edu, .gov, .info, .museum, .org, .net (end of 2010), .com (March 2011)
  - Signed ccTLDs: 37 countries & counting
- 
- 
- Registrars are starting to support DNSSEC  
(28 .org registrars -- source: PIR)

# Validation rate

- The validation rates has risen significantly since the root got signed:



# Operating a validating resolver



# Software

- The majority of DNS resolvers support DNSSEC out-of-the box:

Product	DNSSEC	RFC 5011
ISC BIND	Yes	Yes
Unbound	Yes	Yes
djbdns	No	n/a
MaraDNS	No	n/a
Microsoft DNS	Yes	No*
Simple DNS Plus	Yes	No**
Nominum Vantio	Yes	No**

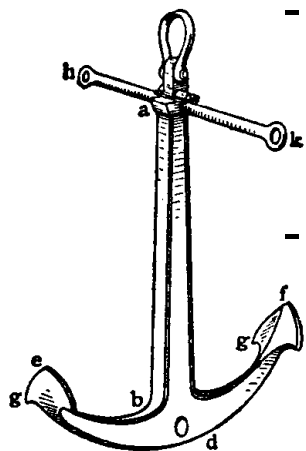
\* Confirmed

\*\* Not specified in product documentation



# Trust anchor configuration

- You should seriously consider using a resolver that supports RFC 5011
- Check the validity of your trust anchor(s) at regular intervals
- **Validate** a trust anchor before using it!



. IN DS 19036 8 2



49AAC11D7B6F6446702E54A160737160  
 7A1A41855200FD2CE1CDDE32F24E8FB5  
 xidep-pybec-tyvak-zonag-kesud-  
 vohip-cumul-fysuk-bivac-pubam-  
 hugeb-buzud-symes-tylaf-dosog-  
 vufor-huxax

# Setting up a validating resolver

- HOWTO instructions for BIND:  
<https://dnssec.surfnet.nl/?p=402>
- HOWTO instructions for Unbound:  
<https://dnssec.surfnet.nl/?p=212>
- Shameless advert: use (or try) Unbound!

<http://unbound.net>

Unbound

NLnet  
10001110001  
111010110001  
100110101000  
011000011000  
00111000100  
000101101001  
000101101011  
Labs

# Checking your setup (1)

- Perform a lookup of a record known to be signed, for instance: www.iis.se:

```
$ dig +dnssec +noauth www.iis.se @myresolver
...
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51109
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, ...

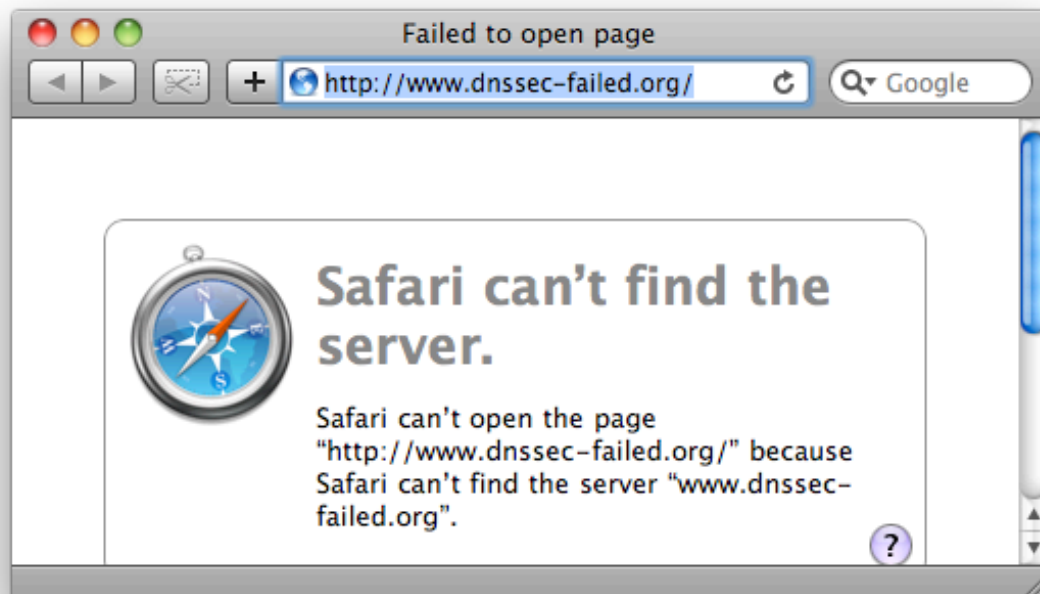
;; ANSWER SECTION:
www.iis.se. 50 IN A      212.247.7.221
www.iis.se. 50 IN RRSIG  A 5 3 60 20101111213001
                20101101213001 23384 iis.se.
                BiKEZgxBf4KASooHPwYJ7Dld/
...
...
```

# Checking your setup (2)

- Visit one of the DNSSEC test sites such as:  
<http://www.nic.cz/dnssec>  
<http://www.dnssec-failed.org>  
<http://test.dnssec-or-not.org/> <-- funny
- And verify the result:

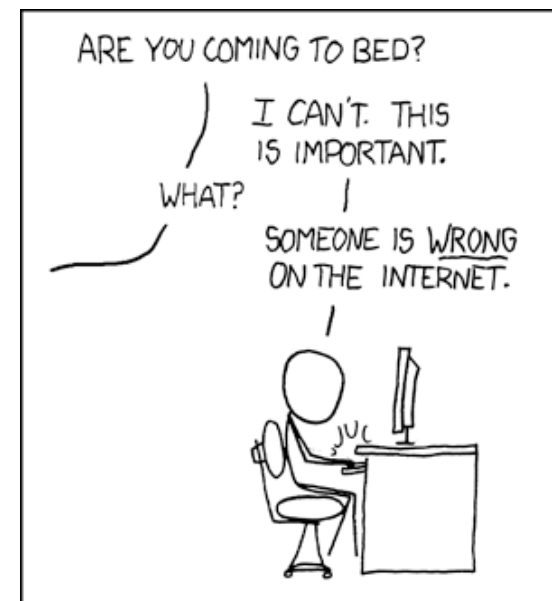


source: nic.cz



# Dealing with validation failures

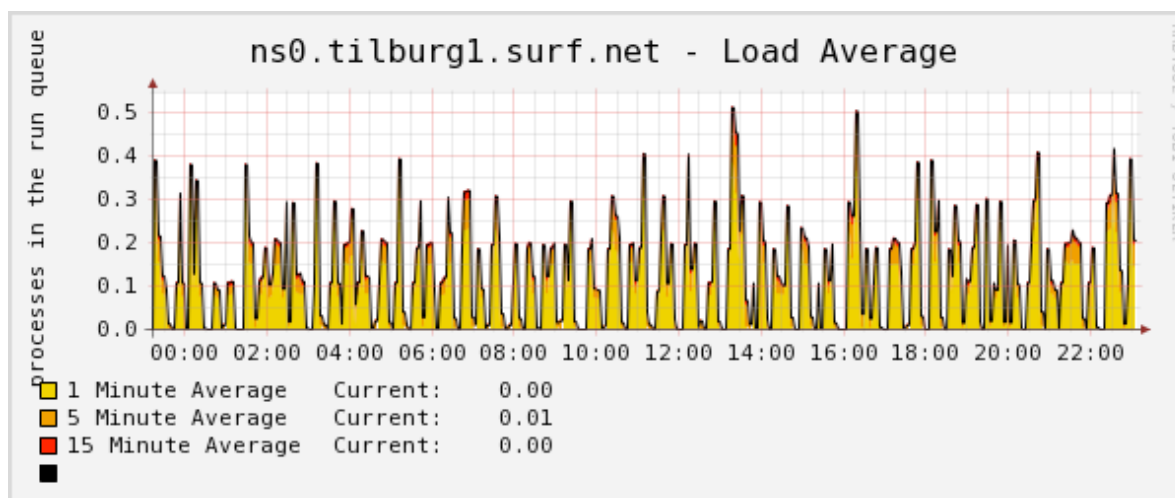
- Validation failures will lead to the resolver returning **SERVFAIL**
- Clients will try **all configured resolvers**
  - If one of them doesn't validate, the query will succeed and the user probably only notices a slight delay
- In our experience, users don't call the helpdesk
  - So no: "The Internet is broken"
- Nevertheless: if you see validation failures then try to alert the zone owner



<http://xkcd.com/386/>

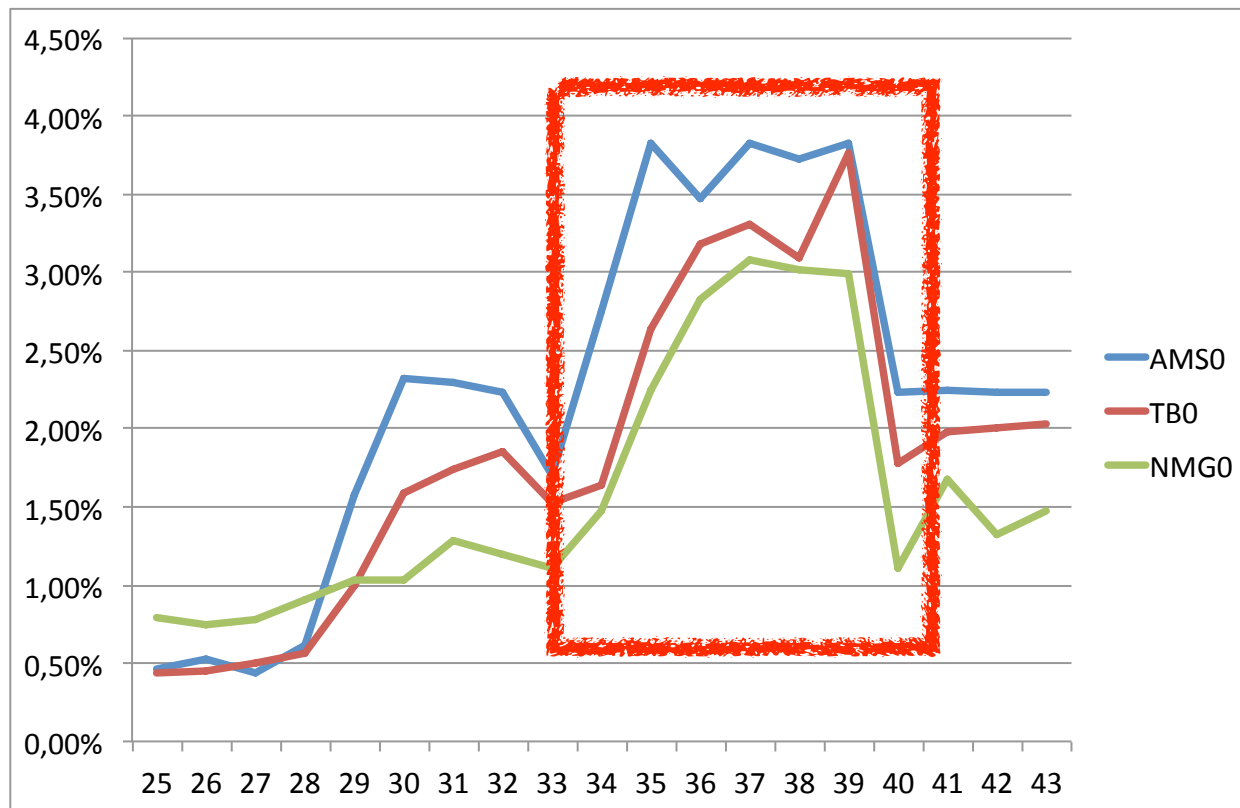
# Impact on resource use

- DNSSEC relies on public key cryptography
  - Crypto eats CPU cycles, right?
- We've been running with full validation enabled since the start of last year
- The impact on CPU load is negligible
  - Measuring doesn't show a significant difference
  - Remember: DNS resolving is all about **caching results**



# Validation rate

- Remember that odd spike in the validation rate?



# I asked blogreaders:

The screenshot shows a browser window with the address bar displaying 'DNSSEC » Puzzle of the week, win a pie :-)'. The page header features the SURFnet logo and a banner image of a yellow padlock with a network cable. The main content area is titled 'Puzzle of the week, win a pie :-)' and includes a date 'OCT 29' and author 'Roland van Rijswijk'. The text describes a new validation rate graph for DNSSEC resolvers. The graph plots validation rates for AMSO (blue line) and TBO (red line) from week 38 to week 43. The y-axis ranges from 2.00% to 4.50%. Both lines show a significant spike in week 43, with AMSO reaching approximately 3.8% and TBO reaching approximately 3.8%.

Week	AMSO (%)	TBO (%)
38	2.20	2.00
39	2.30	2.00
40	2.20	2.00
41	3.80	2.50
42	3.50	3.20
43	3.80	3.80
44	2.20	2.00
45	2.20	2.00
46	2.20	2.00
47	2.20	2.00
48	2.20	2.00
49	2.20	2.00
50	2.20	2.00
51	2.20	2.00
52	2.20	2.00

Navigation and sidebar elements include a search bar, a 'Management' section with links for 'Log in', 'Messages RSS', and 'Comments RSS', and a 'Category' section listing: Architecture (8), Crypto (6), General (9), Policy (2), Procedures (11), Resilience (10), and Security (13). An RSS icon is also present in the top right of the banner area.



# Puzzle solved



Hugo Salgado (@huguei) showing my ASCII art pie

# Troubleshooting

- DNSSEC relies on the EDNS0 extension (RFC 2671)
  - For larger messages (signatures)
  - For the DO-bit (DNSSEC OK)
- Some network hardware has problems with DNSSEC traffic
- Firewalls are notorious for blocking:
  - UDP packets over 512 bytes in size
  - Fragmented UDP packets
  - TCP on port 53
- CPE/SOHO routers also cause trouble
  - Buggy DNS implementations that interfere with your traffic -- Nominet report: <http://bit.ly/cfQBMu>



# Operating a signed zone



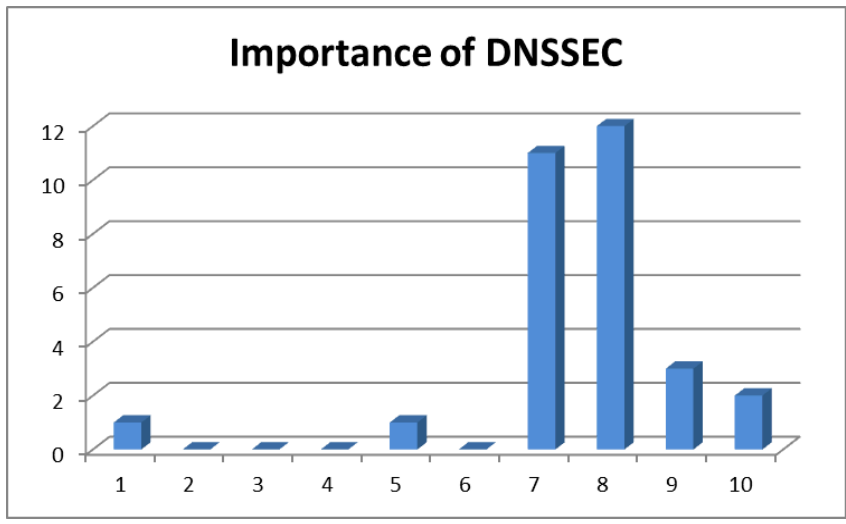
# Why sign your zone?

- Because your website represents a valuable asset for your organisation
- To prevent redirection of Internet traffic to your domain (think: VoIP, e-mail, etc.)
- To protect your users
- To leverage the trust that DNSSEC can establish
  - DNSSEC is a PKI
  - store SSH fingerprints in DNS (SSHFP record)
  - store X.509 certificates in DNS (CERT record)
- Because your competitor does it too :-)

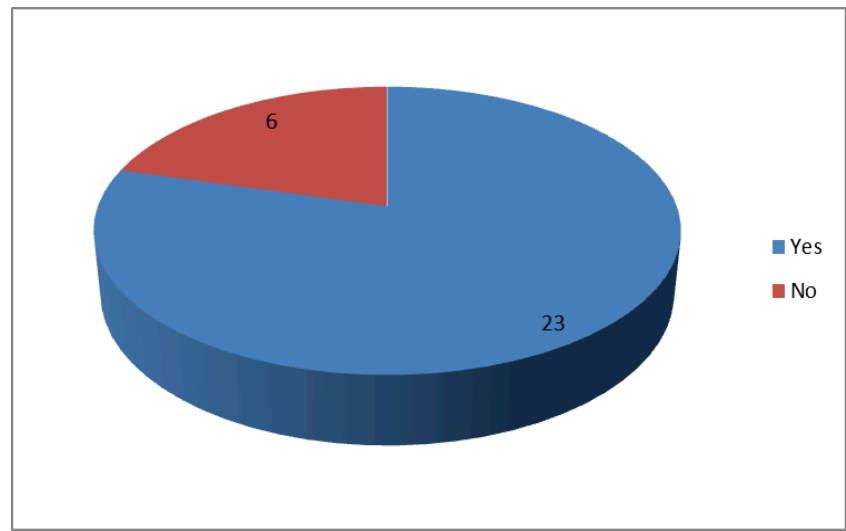
# User study

- We did a user study among our constituency
  - 169 persons asked to participate
  - 38 responded representing 37 organisations (academia, research institutions, teaching hospitals)

- Two-thirds of users feel DNSSEC is important:




- > 75% plan to sign their domain:



# When to sign your zone?

- Your infrastructure should be ready
  - Remember the firewall trouble mentioned when resolving was discussed
- You should have a clear mandate
  - DNS affects everything on your network so DNSSEC does too
- Think before you act :-)
- The way back is harder than the way forward



# How to sign your zone: case study SURFnet



- SURFnet operates a managed DNS environment called ‘SURFdomeinen’
- We ran a project this year from Q1 to Q3 to implement DNSSEC in SURFdomeinen
- Our goals:
  - To make it easy for our connected institutions to operate signed zones
  - To make it easy for **ourselves** to operate signed zones
- We enabled DNSSEC for surfnet.nl at the end of September





# Requirements

- DNSSEC should be a 'box to tick'
  - DNS is already considered to be complex by many users, something that doesn't improve if you add DNSSEC
- The integrity of zones should be guaranteed
  - SURFdomeinen should not be the 'weakest link' in the attack chain
  - Monitoring is of great importance (more on that later)
- Turning DNSSEC on or off should not take too long
  - Ideally less than 1 hour
- Once DNSSEC is turned on, customers should not notice any difference

# Design decision: using HSMs

- HSM = Hardware Security Module
- Secure and robust way to store DNSSEC key material
- We can **never** access the raw key material
- Role separation
- Standard API (PKCS #11)
- Disadvantage: expensive



# Design decision: OpenDNSSEC



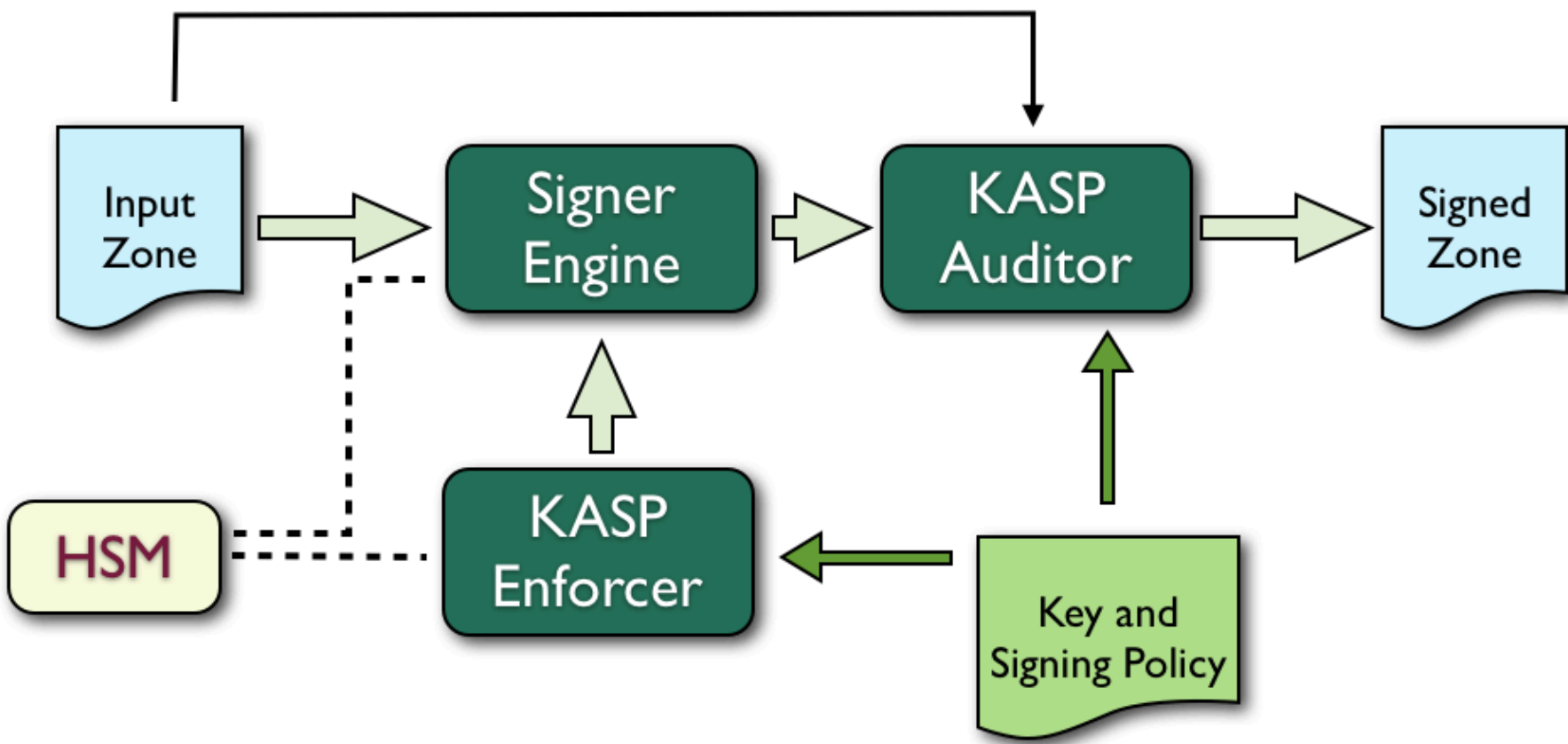
- SURFnet participates in the project
  - Other partners are: IIS (.se), Nominet (.uk), Kirei, SIDN (.nl), NLnet Labs en Sinodun
- Goal: push-the-button signing
- Functions like a ‘bump-in-the-wire’
- Possibility to have different policies for different customers
- Possibility to share keys (e.g. one set of keys per customer rather than per zone)

# Design decision: OpenDNSSEC

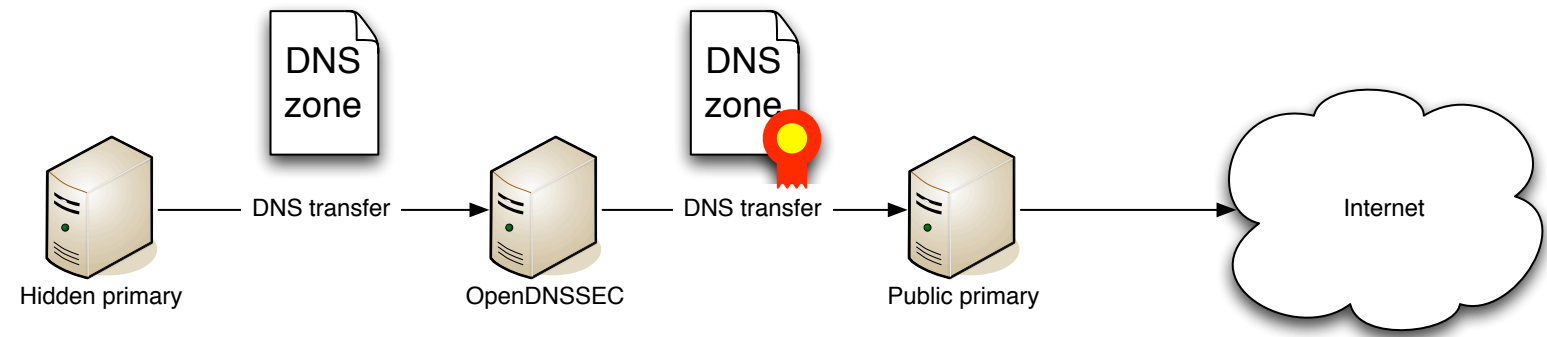
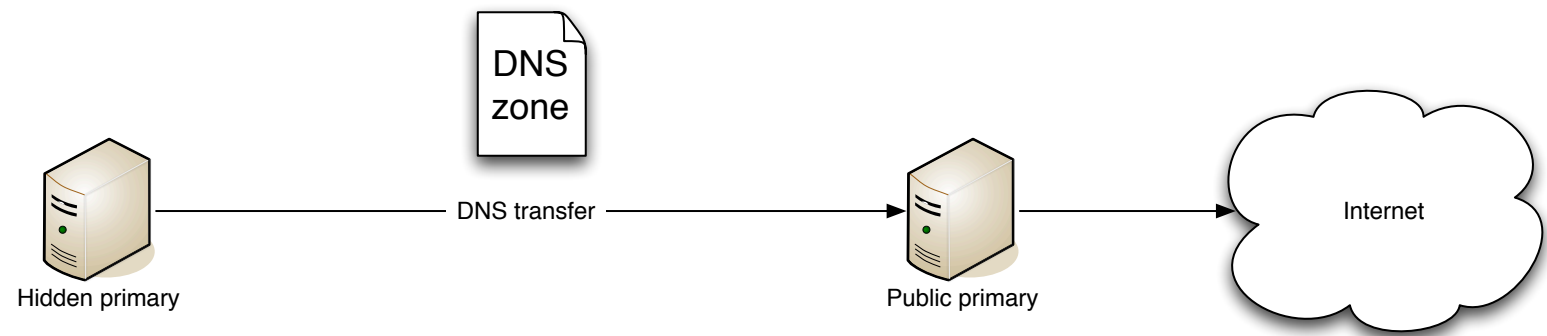


- OpenDNSSEC 1.1
  - Current version; used in production by a number of top-level domains and also for our deployment
  - Used - for instance - by .uk, .fr, .se and .nl
- OpenDNSSEC 1.2 (end of Q4 2010)
  - First beta version has been released
  - Faster signer engine in C
  - Better support for 'key-sharing'
- OpenDNSSEC 1.3 ( $\pm$ Q2 2011)
  - Design is underway
  - Performance improvements for larger setups (50000+ zones)
  - Multi-threaded signer for better performance
  - SURFnet and IIS (.se) investing in extra development effort

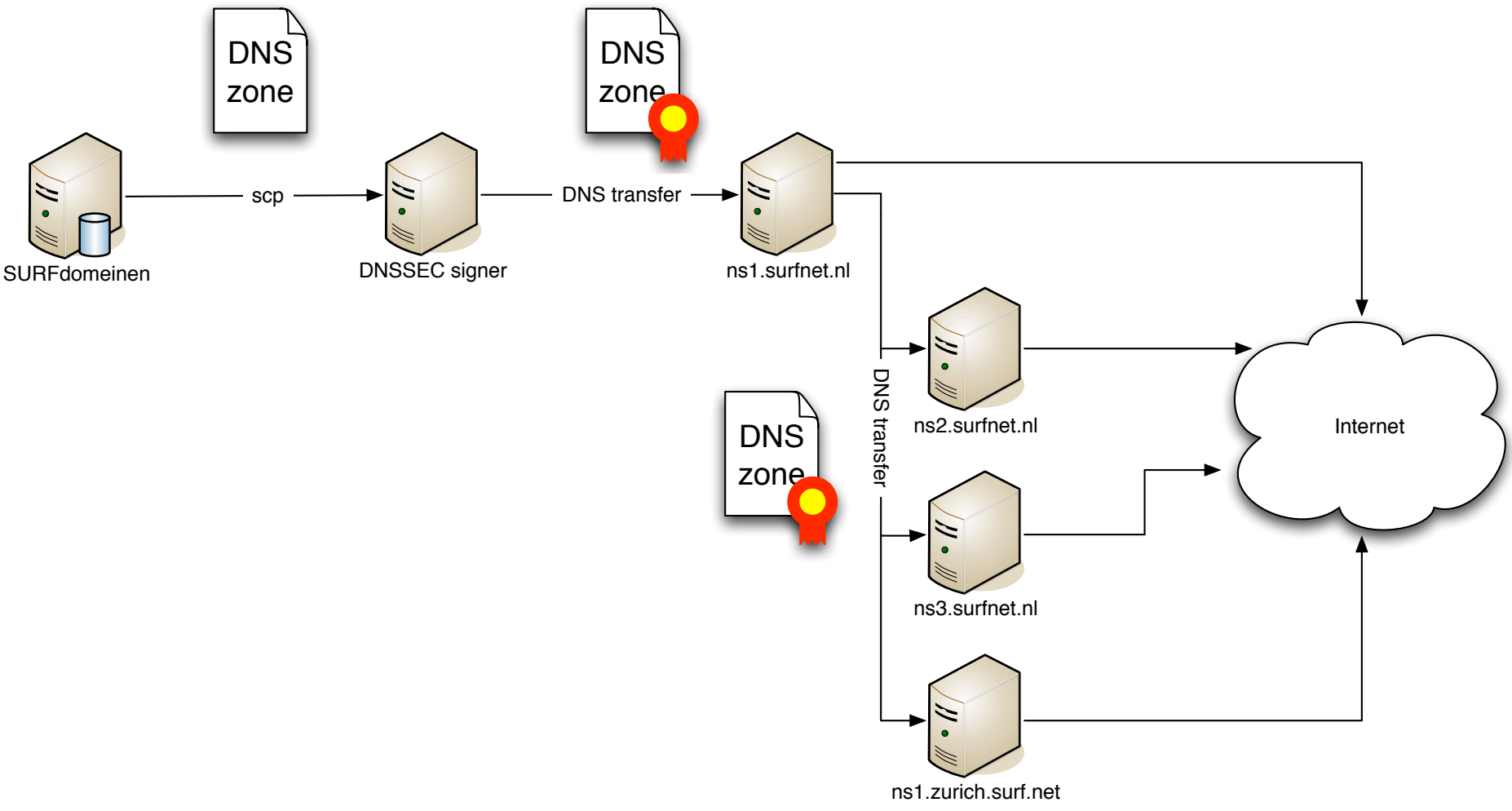
# OpenDNSSEC architecture



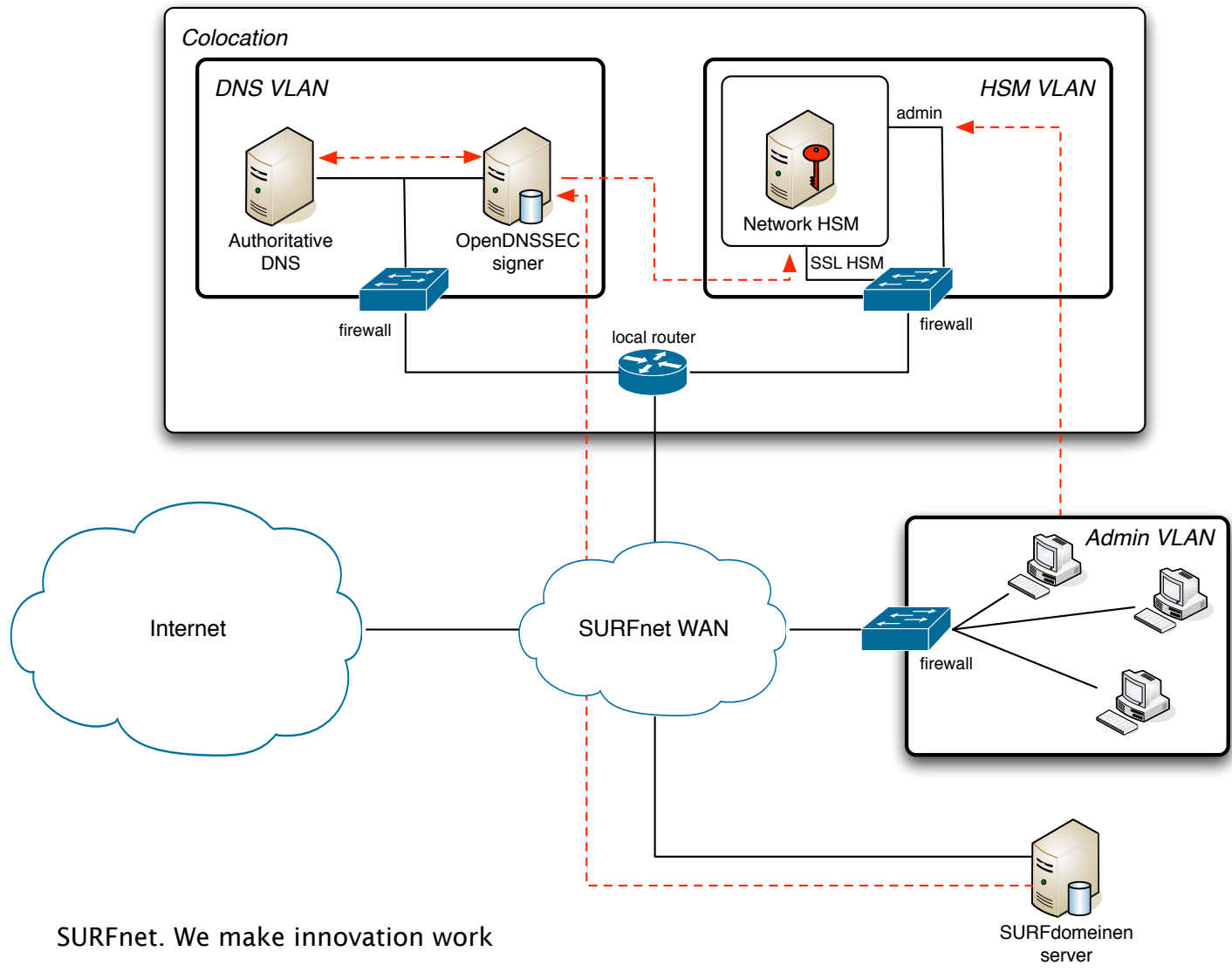
# Design: bump-in-the-wire



# Design: data flow



# Design: network security





# Design: redundancy

## Signer:

- Warm standby system in a different co-location
- MySQL master-slave replication
- Failover is a manual process (not time critical)

## HSM:

- Two HSMs in two different locations
- High-availability mode
- Offline secure backup on a third location
- Keys will only be used after a backup

# Enabling DNSSEC: user perspective

- Push-the-button signing:



- Unsigned to signed in 15 minutes

# Monitoring

- Monitoring helps to detect problems early-on
- When monitoring a signed zone, look for:
  - Signature expiry
  - MTU problems (firewalls!)
  - Continuous validation
- Also monitor from outside your own network
- Many tools are available, for example:  
<http://www.dnssecmonitor.org>  
<http://www.dnsviz.net>

# Advice for getting started

- Make use of available tooling
  - OSS: OpenDNSSEC, BIND
  - Commercial signer solutions
- Make sure you have good monitoring
- Write down policies and procedures
- Carefully think about your design
- Make your users' life easy!
- **Check with your secondaries for DNSSEC support**

# Signer software (1)

- Of course there's not just OpenDNSSEC; there are lots of open source solutions:
- BIND 9.x
  - Key storage in the clear on disk
  - HSM support only through **patched** OpenSSL
  - No automated key rollover (scriptable though)
- BIND 10
  - Still heavily under development (5 year project)
  - Alpha versions have been released
- PowerDNSSEC
  - Alpha release available
- ZKT (Zone Key Tool)
  - No longer seems to be maintained

# Signer software (2)

- Secure64 DNS signer  
<http://www.secure64.com>
- Xelerance DNS-X signer  
<http://www.xelerance.com>
- IPAM vendors
  - Men & Mice
  - Infoblox
  - BlueCat networks
  - ...
- Microsoft Windows Server 2008R2



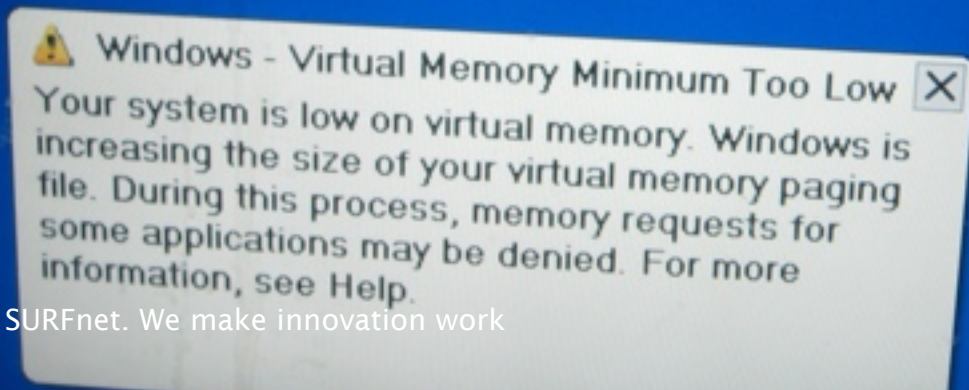
SECURE 64



# When things go wrong...

LAST TRANSACTION CANCELLED

PLEASE TAKE YOUR CARD

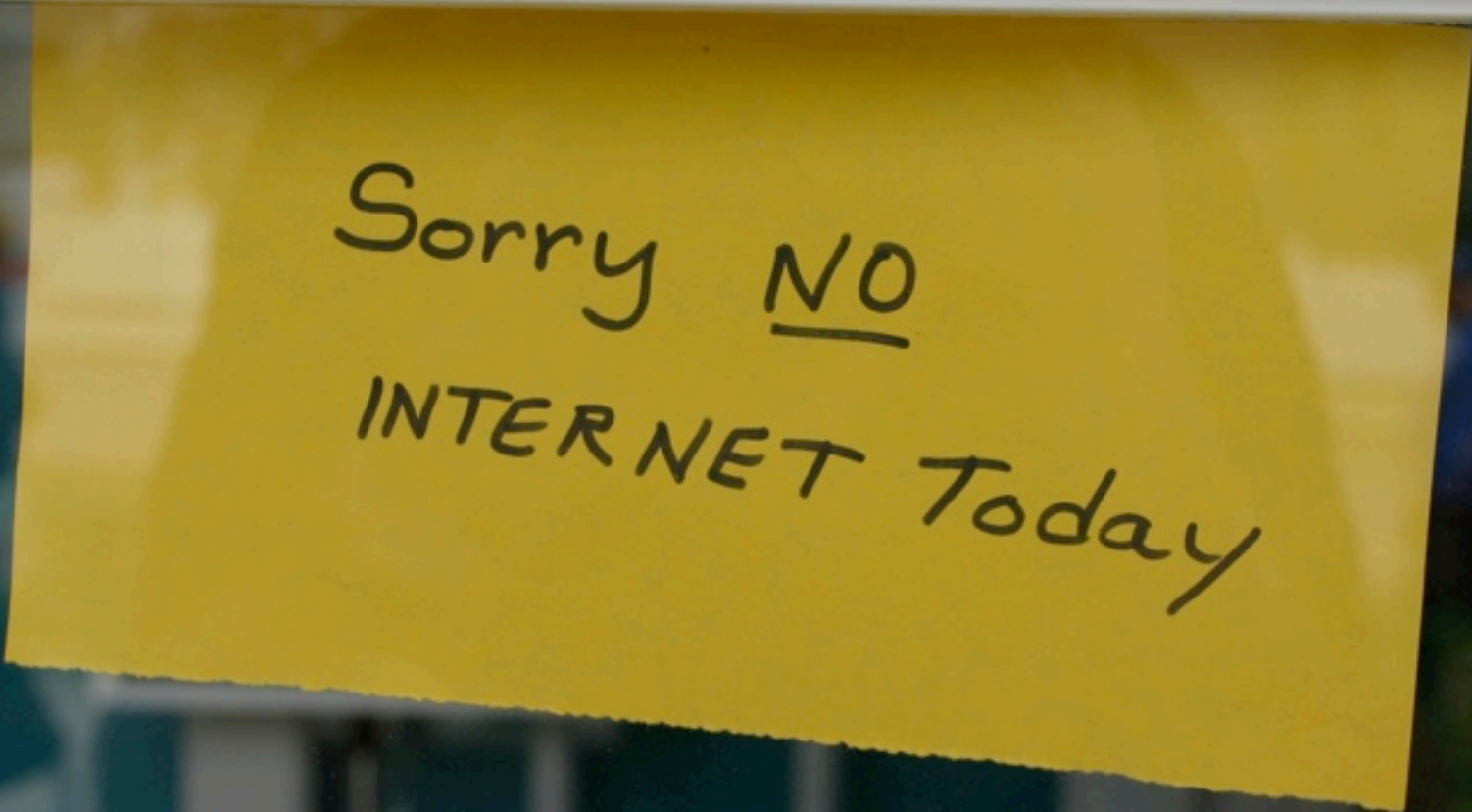


**Windows - Virtual Memory Minimum Too Low** [X]

Your system is low on virtual memory. Windows is increasing the size of your virtual memory paging file. During this process, memory requests for some applications may be denied. For more information, see Help.

A black and white photograph showing the skeletal structure of a globe, with several people visible on the surface, likely working on its construction.

# Admitting mistakes

A bright yellow rectangular sticky note with slightly irregular edges, placed on a dark, blurred background. The text is handwritten in black ink.

Sorry NO  
INTERNET Today



# AXFR bug in OpenDNSSEC

- surfnet.nl was signed for the first time in September (on a Monday)
- everything went smoothly until Thursday
- then suddenly...  
**no more mail**  
**no more website**  
**no more VoIP**
- D'oh!!!
- Garbage In --> Garbage Out
- AXFR bug in OpenDNSSEC has been fixed

**FOKKE & SUKKE**  
*Quickly diagnose  
the problem*



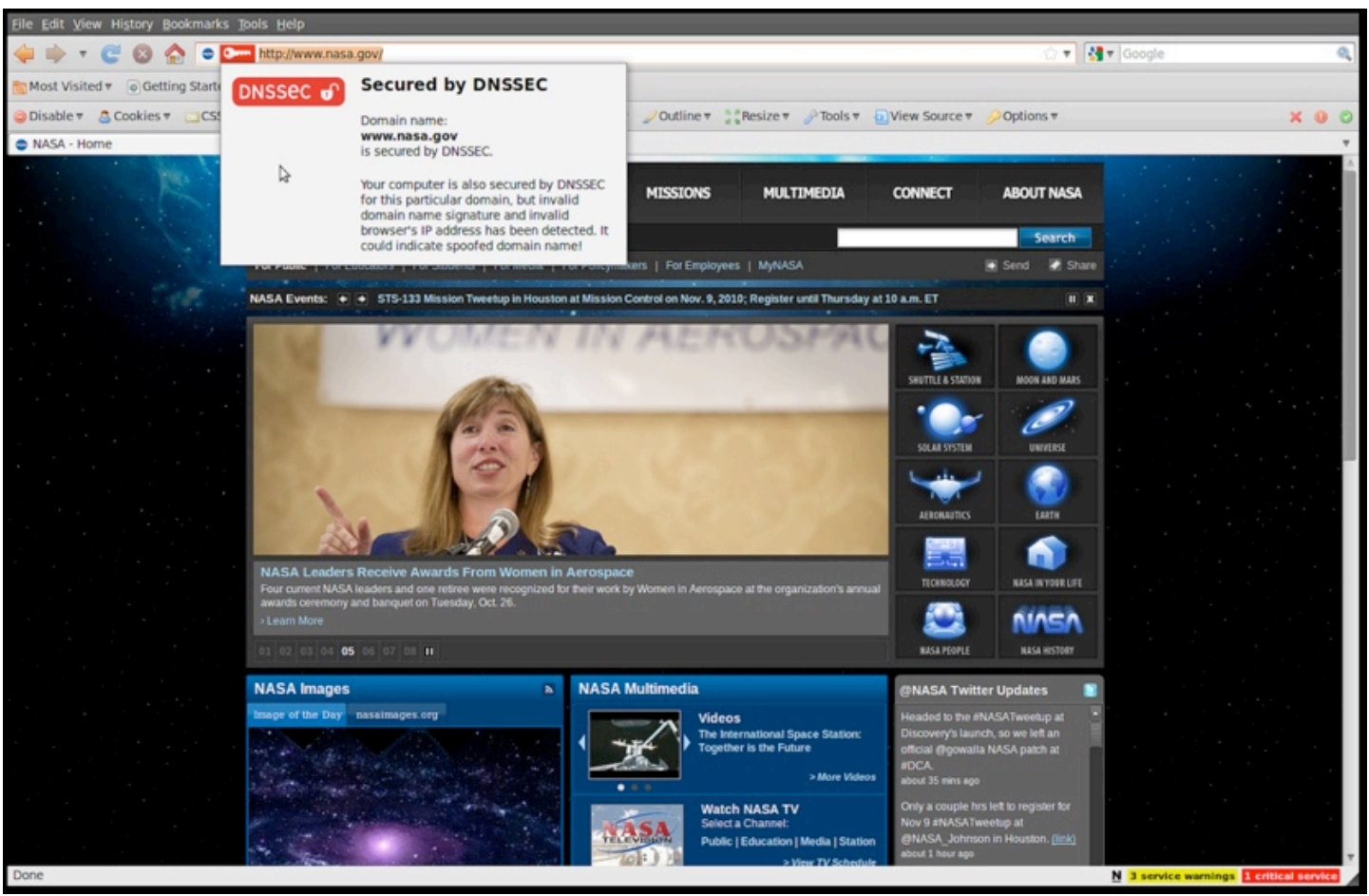
# Stories from the trenches...



- .cz and .us became ‘bogus’ because of a mistake during an algorithm rollover
- ISOC & .org nearly had a PR disaster at ICANN 38 in Brussels
- .uk became ‘bogus’ because of a glitch during a signer failover
- .be forgot to update critical signatures
- mozilla.org and nasa.gov published a DS while their zone wasn’t signed yet

# If you're lucky...

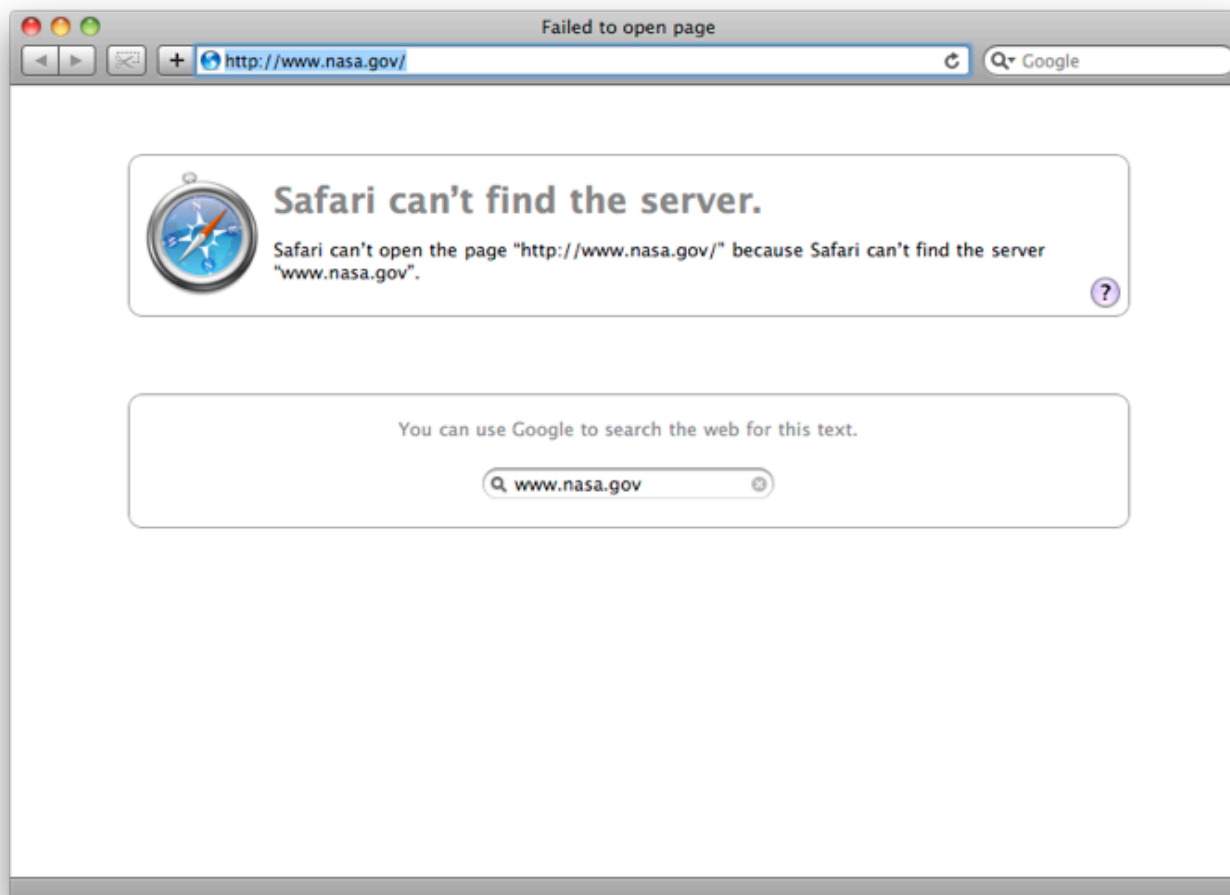
- this is what users will see:



many thanks to Marco Davids of SIDN for the screenshot

# But in most cases...

- this is what users will see:



- (and this is better IMHO!)

# Contacting domain owners is hard



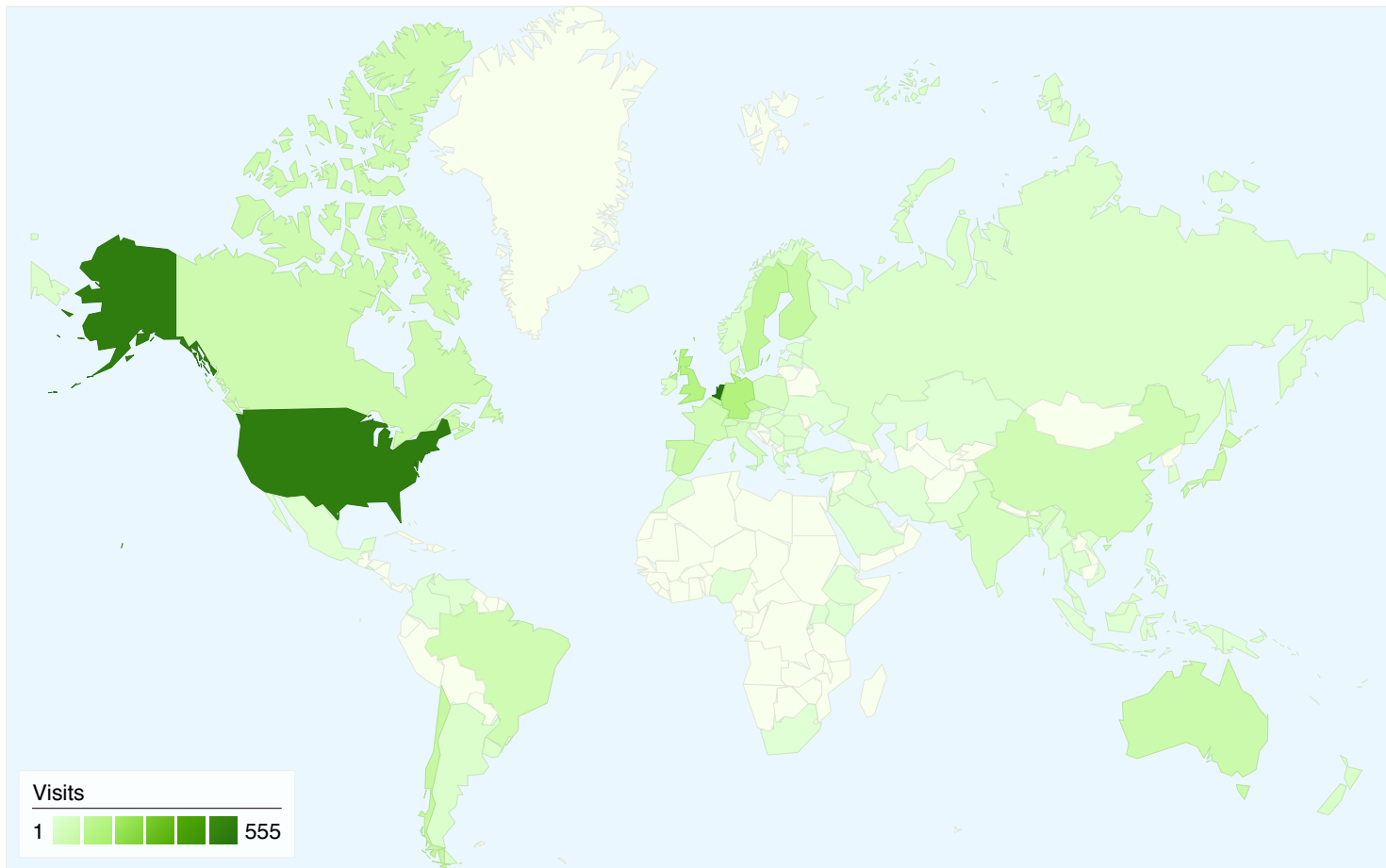
# So what have we learned?





# DNSSEC blog

- <https://dnssec.surfnet.nl>



55

**2,724 visits came from 81 countries/territories**

# Other resources

- <http://dnssec.net>
  - Comprehensive and up-to-date links to information on DNSSEC
- SURFnet white-paper (<http://www.dnssec.nu>)
  - In fairness: not 100% up-to-date but useful nevertheless
- <http://www.dnssec-deployment.org>
  - Tracks DNSSEC deployment across the net
- <http://www.practicesafedns.org>
  - PIR (.org) initiative with user stories



# Conclusions

- DNSSEC deployment has taken off
- The ball is now in your court!
- Seriously consider enabling validation on your resolver
- Think about signing
- Don't be afraid to admit mistakes
  - A lot can be learned from them!
- Once it works, you don't notice it's there

# That's all folks! Questions?

Thank you for your attention!



Roland van Rijswijk



**roland.vanrijswijk [at] surfnet.nl**



**@reseauxsansfil**

Presentation release under the Creative Commons "Attribution" license:  
(<http://creativecommons.org/licenses/by/3.0/>)

