

DNSSEC Musings

Diginotar, DANE,
and Deployment

Olaf M. Kolkmann

Acknowledgements:
Jakob Schlyter
Geoff Huston
Dan Kaminsky

I HAVE AN AGENDA



Resilient


Open

Secure

Privacy

Sustainable

Trust



101

All the basics you need to
know

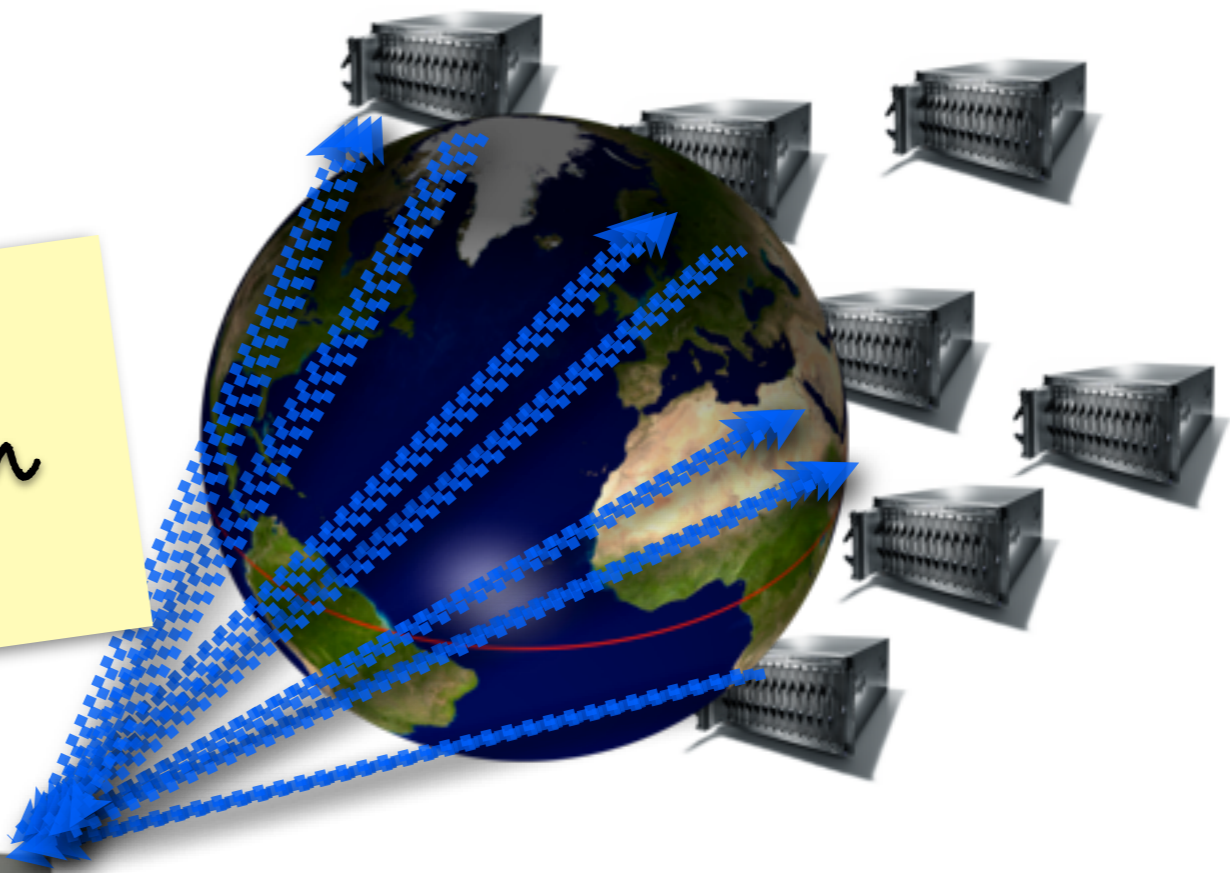


DNS

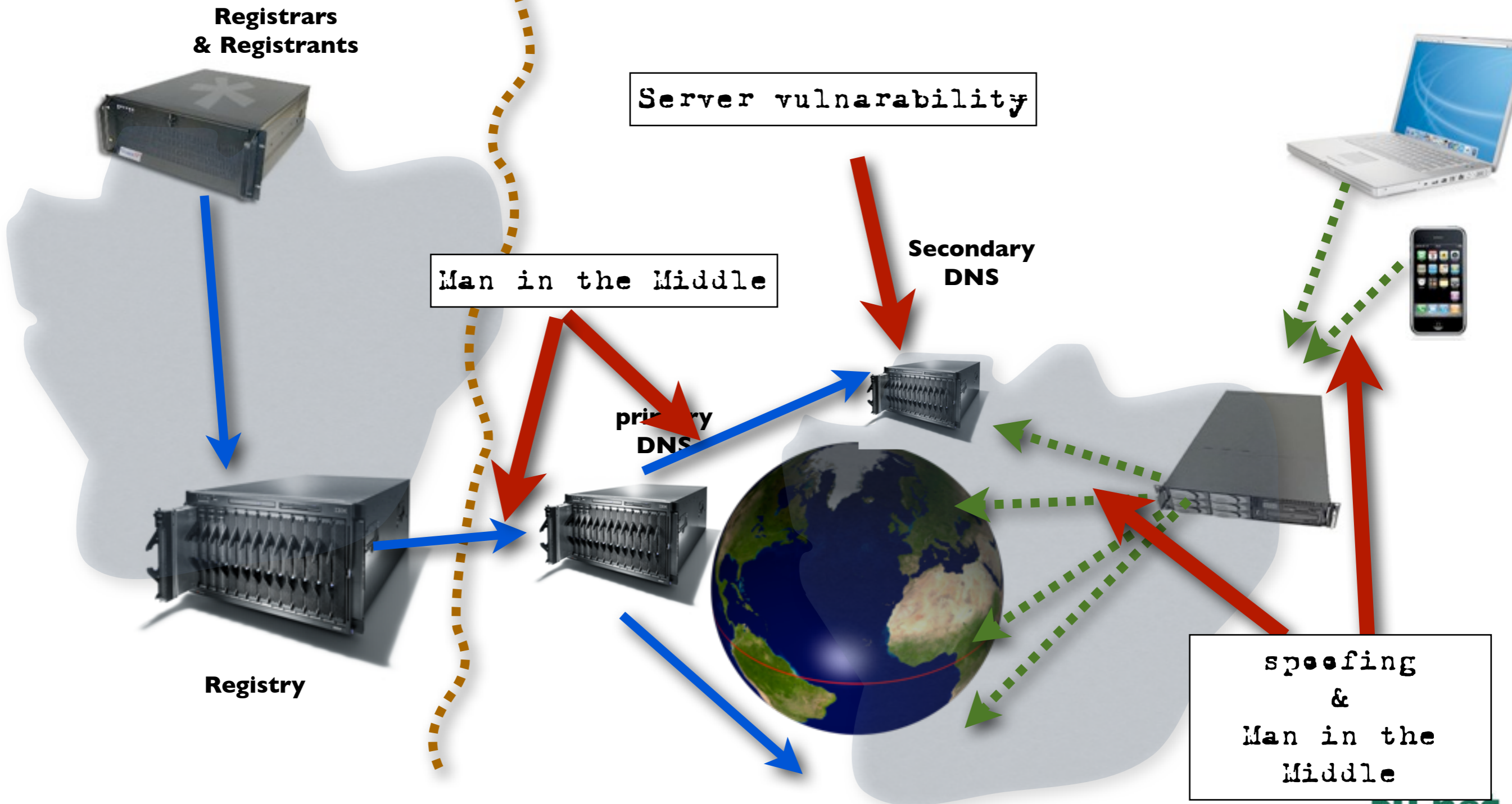
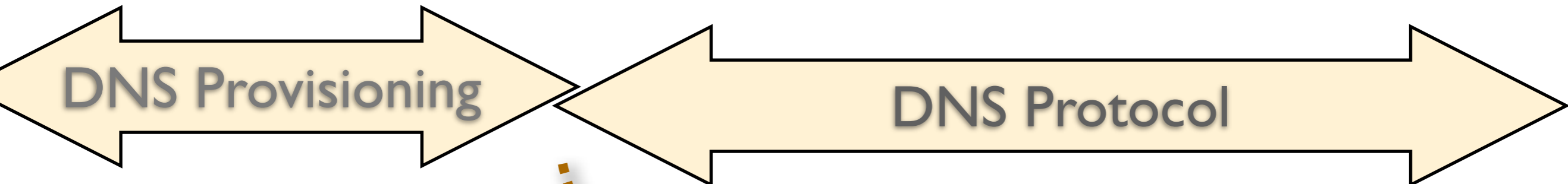
Basics: The Domain Name System

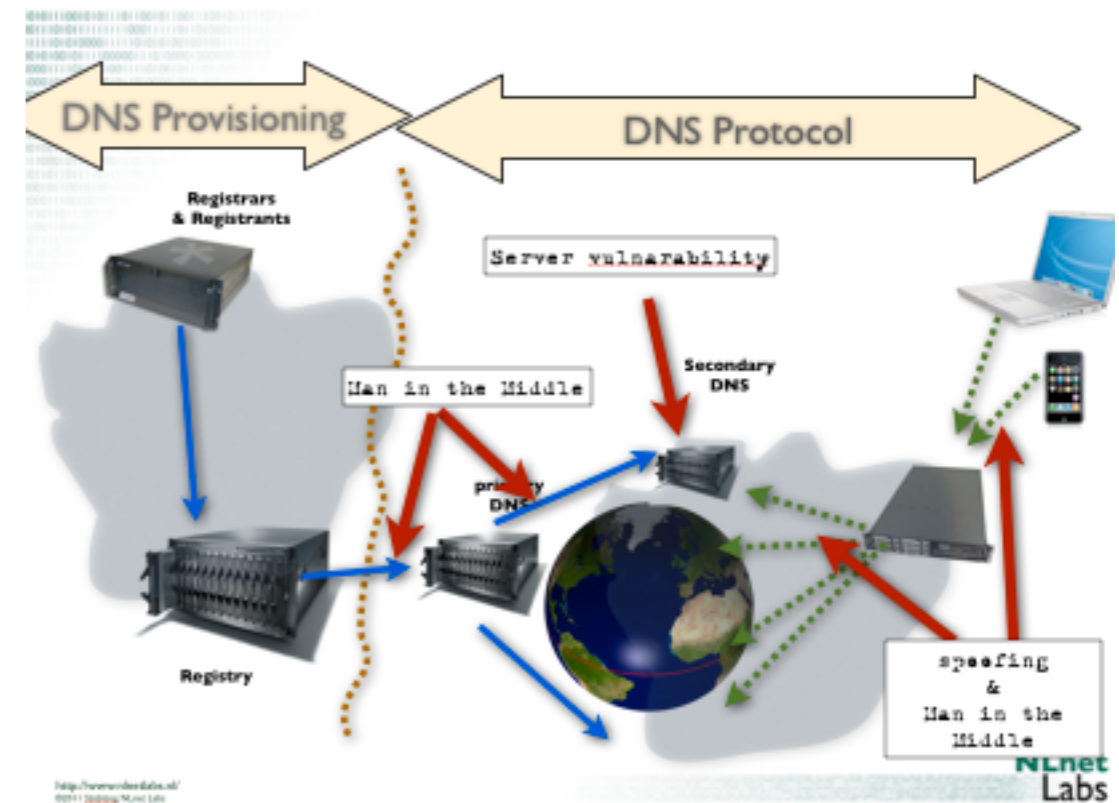
Telephone book of the Internet

The thing that translates www.NLnetLabs.nl into an service location



Highly resilient, global, scalable.



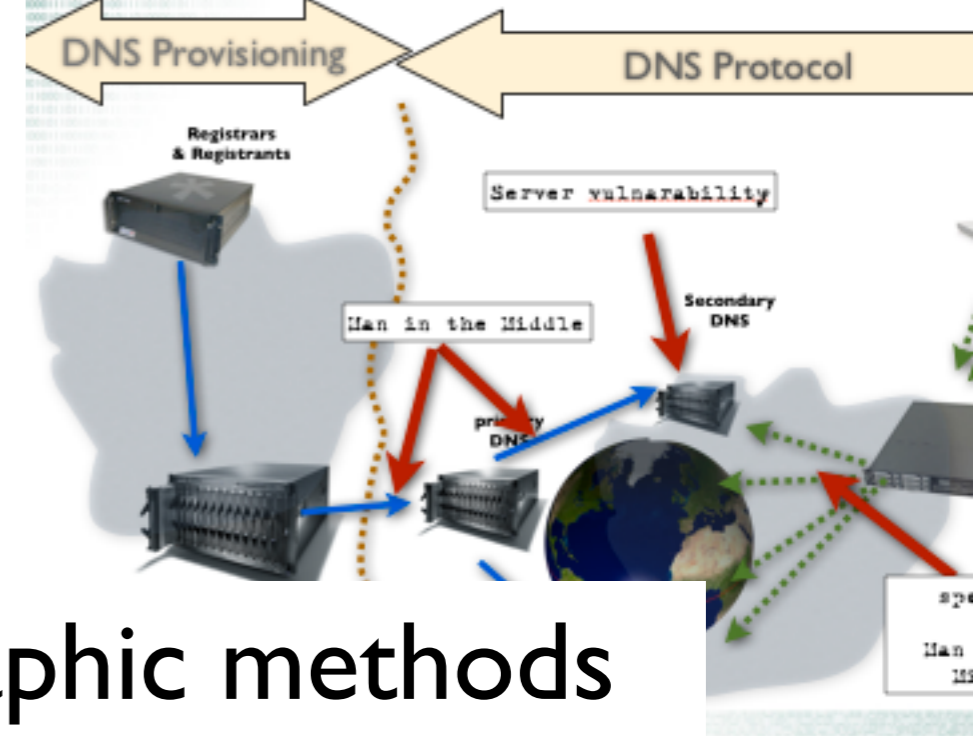


- Summary:
 - Vulnerabilities in the provisioning side
 - Vulnerabilities in the delivery (DNS protocol and infrastructure)

DNSSEC

without the details

DNSSEC



- DNSSEC provides cryptographic methods to validate the integrity and authenticity of messages send by the DNS protocol.
- Integrity is the property that a message has not been altered, or tampered with.
- Authenticity knows that you can validate the publisher of the message is the ‘zone owner’.

Internet

PKI

In this context
technology to assert
authenticity.

Provides a basis for
integrity and
confidentiality of
connections

Depends on trust in
specific 3rd parties:
Registration and
Certificate Authorities

TRANSITIVE TRUST



*Ali and his magic Browser
how failure in technology and compliance
almost brought misery and doom*

In this chapter of the presentation we talk about “Ali” and how his browser settings disclosed a major problem and caused a scandal.

1010111001010111011001011001110010111101100111
0011101011111110001111011010001111110111
111110101000011110101010010010011111011011
0010100101110000011101000010000001000001
00001110111010011101001011101100001111
100010110111001010100001000110010001
000111010011011011000111111010101
00101011101000110011100011110101
01011100100100100010110110110111
10010100110000111000001001100
0010010100011111100101010101
1110001011110011101001101
1011011011110111101101
000101100101001010101
100011100100100101
1110110111001101
1100110000011100
1011111000011100
1011010101
1010110101
111101
1011

September 2011





HOME ACTUEEL PROD

KLANTENSERVICE OVER DIGINOTAR

A Bankrupt
Certificate
Authority

zoek  

documenten online uitwisselen
Hoe toont u aan dat uw document de originele en
geautoriseerde versie is en dat het bij de juiste persoon komt?
Meer >>

Certificaten Contact FAQ

Ga direct naar ...

- Digitale Polis
- Elektronische handtekening WABO
- Overgang certificaten
- SHA256 certificaten en sleutellengte 2048
- Tarieven certificaten

Lopende projecten

Belastingdienst

DigiNotar®, Internet Trust Provider

Dé onafhankelijke partij voor het identificeren van personen en organisaties op internet en veilig digitaal documenten uitwisselen, ondertekenen en bewaren.

Expertise in o.a. online identiteiten, veilig documenten uitwisselen, privacy services, elektronisch factureren, mobiele pki, (EV)SSL, pseudonimisatie, digitale kluis, authenticatie, elektronische handtekening

[Meer info >>](#)

eHerkenning



Actueel

> **Faillissement DigiNotar**

De Rechtbank Haarlem heeft op dinsdag 20 september 2011 het faillissement uitgesproken van Diginotar B.V. onder aanstelling van mr. R. Mulder tot cura...

> **DigiNotar failliet. Overheid blijft betrokken bij operationeel beheer**

Lees hier het persbericht

> **Besluit OPTA om de registratie van DigiNotar als certificatie dienstverlener in te trekken**

De OPTA heeft op 13 september jl. besloten om de registratie van DigiNotar als leverancier van gekwalificeerde elektronische handtekeningen (certifica...

[Meer nieuws...](#)

Société Générale
Crédit Agricole, are consid
actors in the French economy,

Iranian activists feel the chill as hacker taps into e-mails

BY SOMINI SENGUPTA

He claims to be 21 years old, a student of software engineering in Tehran who reveres Ayatollah Ali Khamenei and despises dissidents in his country.

He sneaked into the computer systems of a security firm on the outskirts of Amsterdam. He created fake credentials that could allow someone to spy on Internet connections that appeared to be secure. He then declines to identify his labor as 300,000

Front-Page
News

online security mechanism that is trust-
at users all over the world.
he calls himself, in-
n and is un-
that his work
spy on anti-

govern
"I'm totally
an e-mail exchange with The New York
Times. "I just share my findings with
some people in Iran. They are free to do
anything they want with my findings
and things I share with them, but I'm
not responsible."
In the annals of Internet attacks, this
is most likely to go down as a moment of
reckoning. For activists, it shows the
HACKER, PAGE 17

The quote in the Tribune reads: "He (Ali Borhani) claims to be a 21 years old, a student of software engineering in Tehran who reveres Ayatolla ALi Khamanei and despises dissidents in his country."

International Herald Tribune
Sep 13, 2011 Front Page



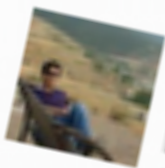


Events
chain of trust

something fishy

[Help forum](#) > [Gmail](#) > [Coffee Shop \(off-topic\)](#) > Is This MITM Attack to Gmail's SSL ?

☆ Is This MITM Attack to Gmail's SSL ?

 [alibo](#)
Level 1
8/28/11

Hi,
Today, when I trid to login to my Gmail account I saw a certificate warning in Chrome .
I took a screenshot and I saved certificate to a file .

this is the certificate file with screenshot in a zip file:
<http://www.mediafire.com/?rrklb17slctityb>

and this is text of decoded fake certificate:
<http://pastebin.com/ff7Yg663>

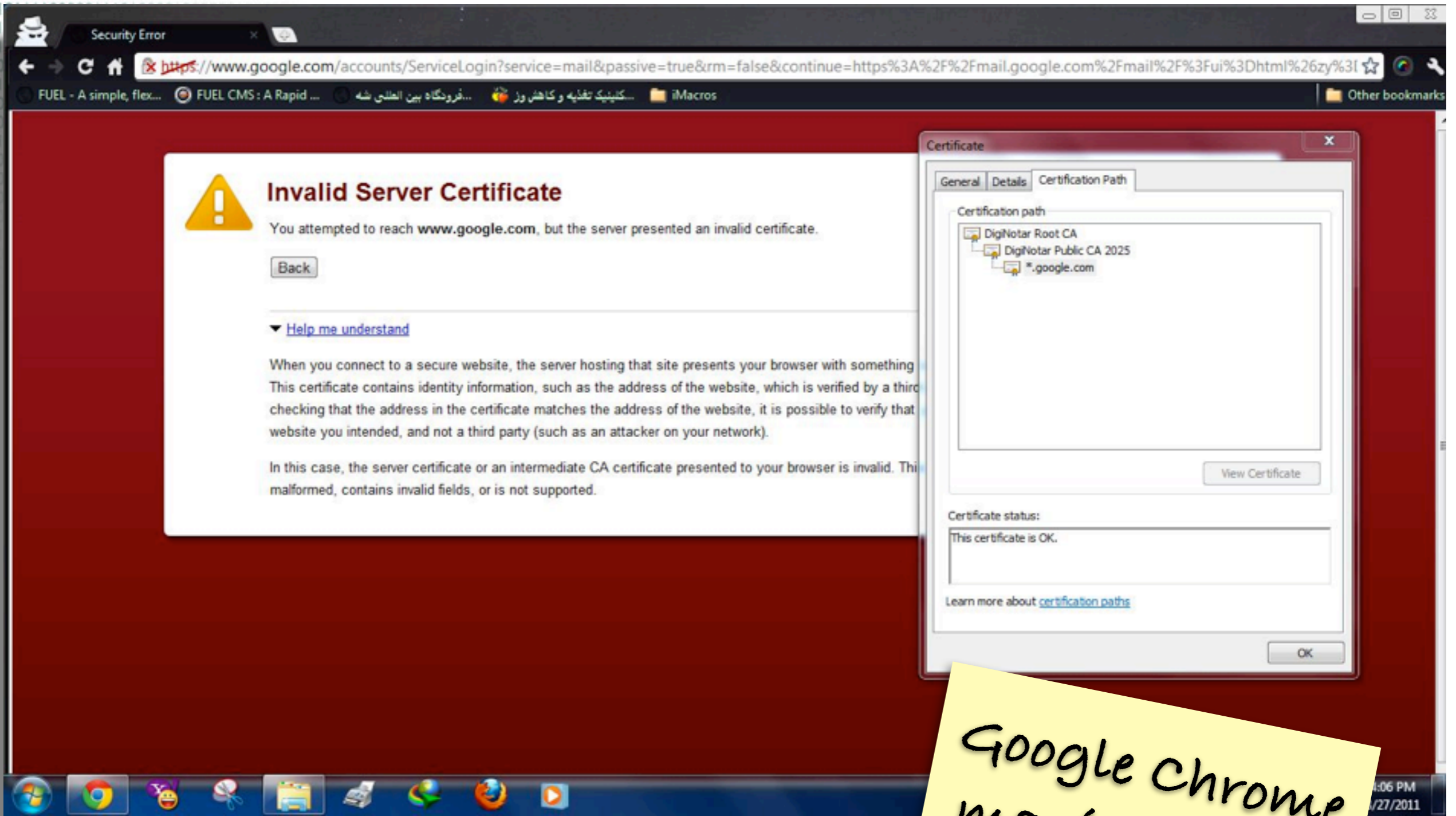
when I used a vpn I didn't see any warning ! I think my ISP or my government did this attack (because I live in Iran and you may hear something about the story of Comodo hacker!)

[Report abuse](#)

28 Aug 2011

<http://productforums.google.com/forum/#!category-topic/gmail/share-and-discuss-with-others/3j3r2jqFNTw>

link last verified 5 oct 2012 (avatar had changed from the snapshot above)



Invalid Server Certificate

You attempted to reach www.google.com, but the server presented an invalid certificate.

[Back](#)

▼ [Help me understand](#)

When you connect to a secure website, the server hosting that site presents your browser with something. This certificate contains identity information, such as the address of the website, which is verified by a third party. Checking that the address in the certificate matches the address of the website, it is possible to verify that website you intended, and not a third party (such as an attacker on your network).

In this case, the server certificate or an intermediate CA certificate presented to your browser is invalid. This certificate is malformed, contains invalid fields, or is not supported.

Certificate

General Details Certification Path

Certification path

- DigNotar Root CA
 - DigNotar Public CA 2025
 - *.google.com

[View Certificate](#)

Certificate status:

This certificate is OK.

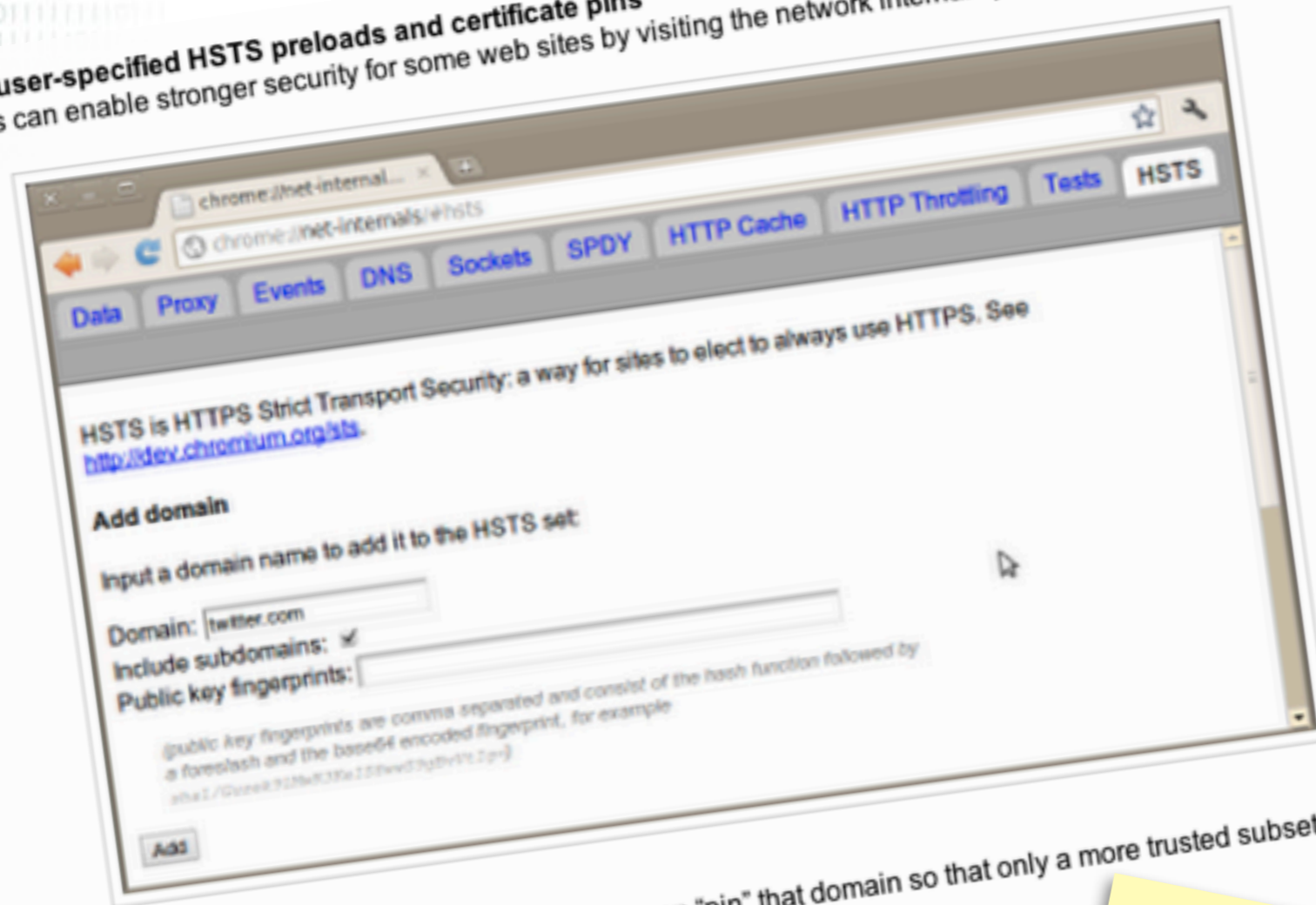
[Learn more about certification paths](#)

[OK](#)

Google Chrome magic caught this!

Chromium 12: user-specified HSTS preloads and certificate pins

Advanced users can enable stronger security for some web sites by visiting the network internals page: <chrome://net-internals/>



You can now force HTTPS for any domain you want, and even "pin" that domain so that only a more trusted subset of CAs are permitted to identify that domain.

It's an exciting feature but we'd like to warn that it's easy to break things! We recommend that you only use it in [internals settings](#).

Before June 2011 the problem would not have shown

<http://blog.chromium.org/2011/06/new-chromium-security-features-june.html>

<http://dev.chromium.org/sts> shows the list of preloaded keys 'today'. I am not 100% sure what was preloaded at the time.



What went wrong?

<http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html>
link verified oct 5, 2012

<http://www.nlnetlabs.nl/>
©2013 Stichting NLnet Labs



Compromised
certificate issued
by:



Fox-IT hired to
investigate

Earlier report (Jul
27): compromise of
External web servers

Incomplete
audit trails

Advanced and
Amateur

Fingerprint
Similarity to
Comodo Hacker

Multiple hacker
tools on the
servers

And a claim
by the hacker

Hi again! I strike back again, huh?

I told all that I can do it again, I told all in interviews that I still have accesses in Comodo resellers, I told all I have access to most of CAs, you see that words now?

You know, I have access to 4 more so HIGH profile CAs, which I can issue certs from them too which I will, I won't name them, I also had access to StartCom CA, I hacked their server too with so sophisticated methods, he was lucky by being sitted in front of HSM for signing, I will name just one more which I still have access: GlobalSign, let me use these accesses and CAs, later I'll talk about them too..

I won't talk so many detail for now, just I wanted to let the world know that ANYTHING you do will have consequences, ANYTHING your country did in past, you have to pay for it...

I was sure if I issue those certificates for myself from a company, company will be closed and will not be able to issue certs anymore, Comodo was really really lucky!

I thought if I issue certs from Dutch Gov. CA, they'll lose a lot of money:

http://www.nasdaq.com/asp/dynamic_charting.aspx?selected=VDSI&timeframe=6m&charttype=line

But I remembered something and I hacked DigiNotar without more thinking in anniversary of that mistake:

<http://www.tepav.org.tr/en/kose-yazisi-tepav/s/2551>

When Dutch government, exchanged 8000 Muslim for 30 Dutch soldiers and Animal Serbian soldiers killed 8000 Muslims in same day, Dutch government have to pay for it, nothing is changed,

The hacker made a statement that demonstrate political motives and gave some details about the attack such as the Pr0d@dm1n as adminstrator password, VNC/remote desktops etc.

By the way, ask DigiNotar about this username/password combination:

Username: PRODUCTION\Administrator (domain administrator of certificate network)

Password: Pr0d@dm1n

It's not all about passwords or cracking them,

- 1) you can't have remote desktop connection in a really closed and protected network by firewalls which doesn't allow Reverse VNC, VNC, remote desktop, etc. by packet detection.
- 2) you can't even dump hashes of domain if you don't have admin privilege to crack them
- 3) you can't access 6th layer network which have no ANY connection to internet from internet

Yeah!

Bye for now



The movie shows the geo-location of IP addresses that called the DigiNotar revocation service to test whether *.google.com had been revoked.

<http://www.youtube.com/watch?v=wZsWoSxxwVY&hd=1>

<http://www.nlnetlabs.nl/>
©2013 Stichting NLnet Labs

NLnet
Labs

My takeaway

This was a
determined
adversary

With direct access
to Nationwide
Infrastructure

My conclusion is that the Diginotar hacker is associated with an entity that has access to Nationwide infrastructure.

One wonders: hack on request, part of the dayjob, or actioned on an underground market.

As a result

The Diginotar CA got pulled from the browser

(Inconvenient)

Iranian activists potentially saw their communication tapped

(Life Threatening?)

- Pulling the CA from the browser was a major costs throughout the Dutch governmental web infrastructure. That aspect got a lot of media attention.
- The fact that Iranian activists potentially got their communication tapped by incompetence of a Dutch company did not make the news.
- Problems caused by CA compromise may not be of only economic nature

TAKEAWAY

Compliance
failure

Technology
weakness

Technology
Defenses

- There is an inherent security weakness (I will go deeper into that weakness in the next section of the presentation) and there are compliance failures (DigiNotar not performing a competent job).
- On the other hand, Chrome's technology came to the defense.. so there is hope.

The Browser and its Trust

Trust issues in today's browser.
The underlying system and assumptions.

Who to trust?

Ah, oh.... those smart girls
and boys from ... eh..



eh microfox?
must have figured
that out...

Trust decisions by regular end-users are not made consciously, they trust 'us' the specialists.



Browser trusts
~60 CAs

And therefore
~1500 subordinate CAs
(~651 organizations)

See the EFF SSL observatory
<http://www.eff.org/files/DefconSSLiverse.pdf>

Browser trusts about 60 root certificates: Hierarchical PKI structure:

- 1500 subordinate CAs
- maintained by approx 650 other organizations.

Think of those Subordinates as resellers or imprints.

Let's have a look at how a Certificate Authority functions.

What we usually call a CA consist of two functions:

- a registration authority (RA) that does all the paper work and
- the certificate authority (CA) that automates signature generation.

After following a procedure the RA instructs the CA to sign a certificate.

The role of a CA

3rd party trust broker

Subject Requests

RA performs checks

RA tells CA to sign

Browser trusts CA signed certificates

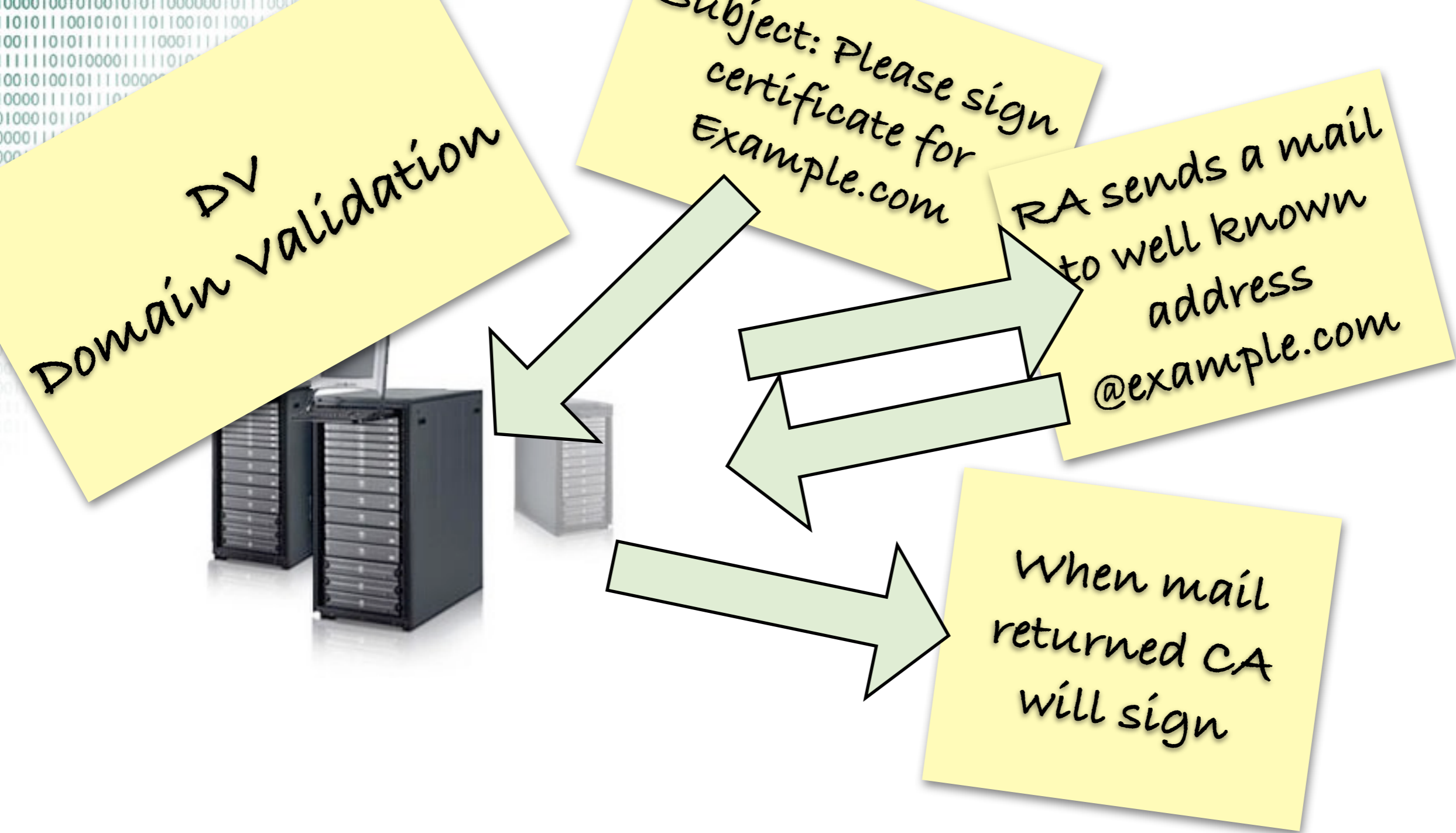


AUTOMATE THE LOT

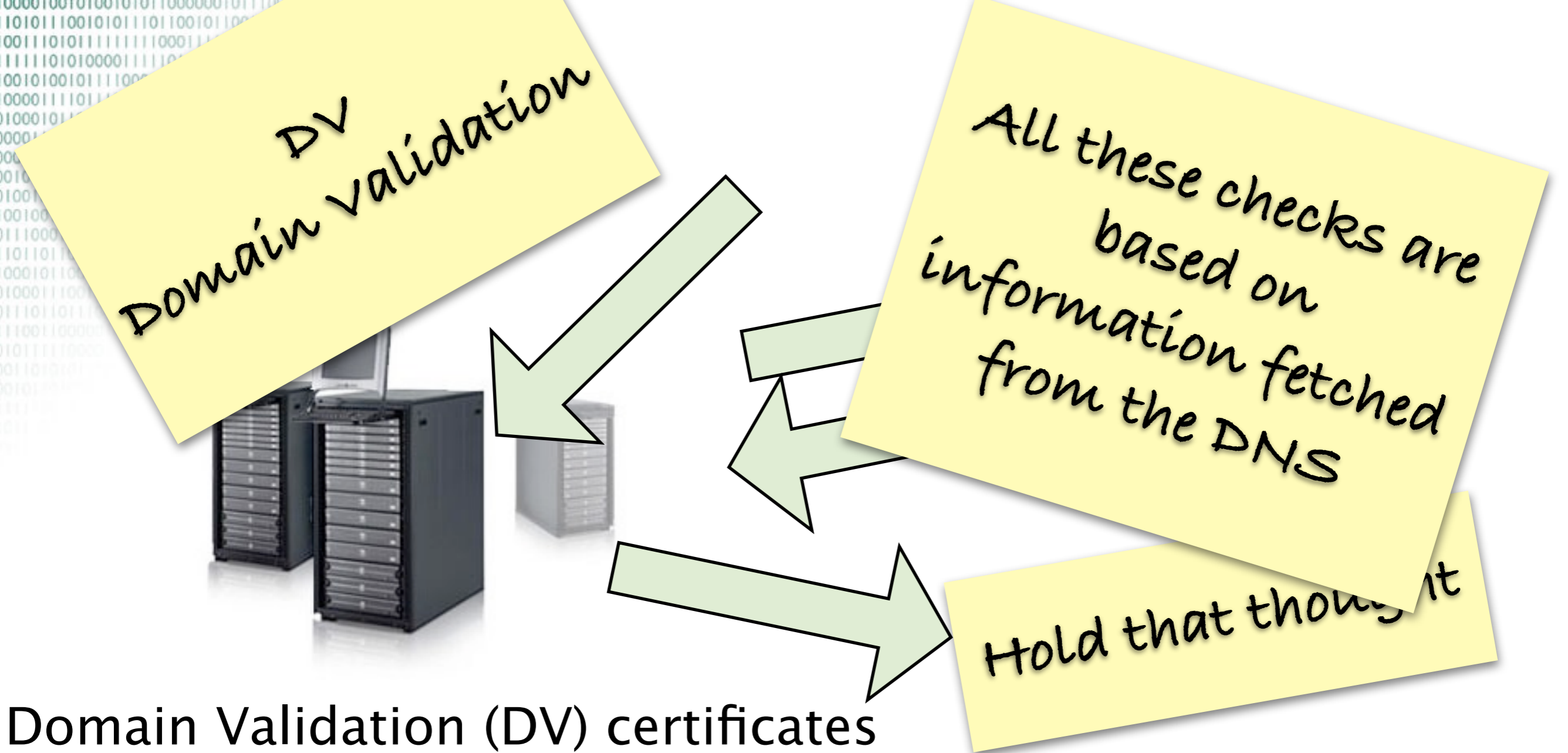
However all these
little men are a wee
bit expensive



you can automate the procedures and let those machine contact the persons that claim to be holder of a specific domain using off-band mechanisms



We end up with a system that is fully automated and does a bunch of checks based on automated e-mail exchange with well know addresses and other automatically accessible information.



Domain Validation (DV) certificates

This how the industry evolved over the first years of PKI use:
An economic raise to the bottom, causing DV certificates to cost cents or even been given away for free.

Note: the CA accessing all sorts of DNS information in order to validate the domain holdership by the subject.

10101110010101110110010110011000101011101111
001110101111111000111101101000111111111111
1111101010000111101010100100100111111111111
0010100101110000011101000010000001000000
0000111011101001110100101101100001
100010110111001011000010001100100001
00011101001101101110001111110101
0010101110
0101110010
1001010011
0010010100
1110001011
1011011011
0001011001
000111001
1110110111
1100110000
10111110000
011010101
101010101
111111111
011
111111111

In 2007 the CA/Browser forum came up with Guidelines For The Issuance And Management Of Extended Validation Certificates.

Domain validity



Extended validity

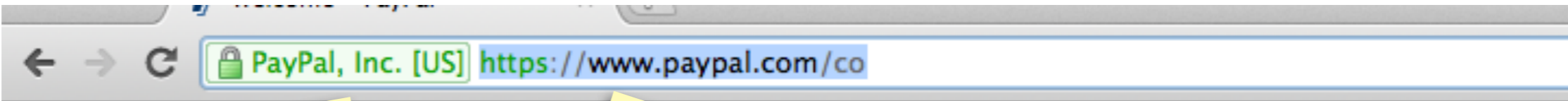
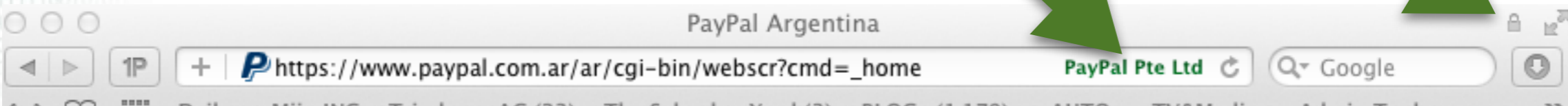
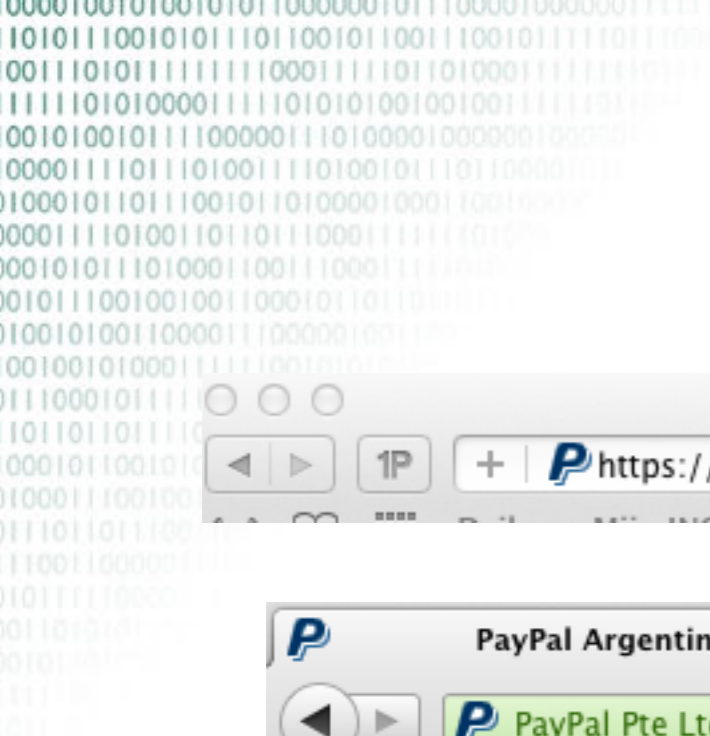


DV/EV

Would you notice the difference?

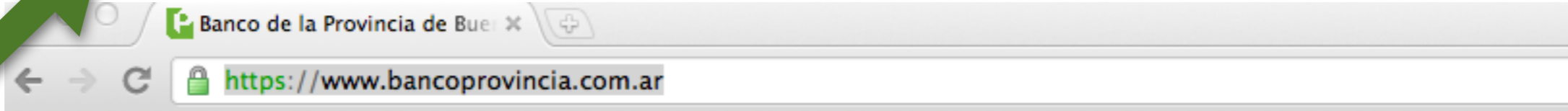
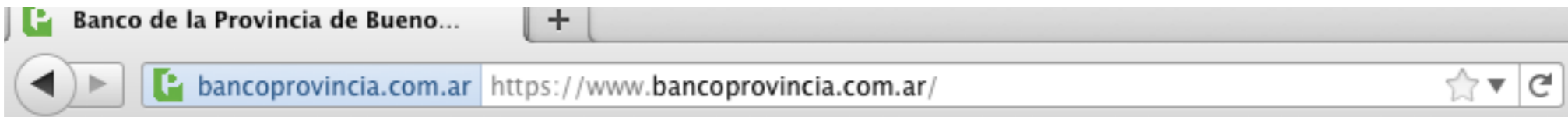
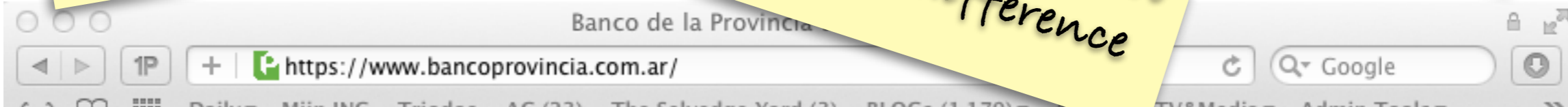


Easy!!!
Click on the pad-lock,
validate the CA, the
certificate chain and the
appropriate fields.



Fortunately

The trained eye can spot the difference



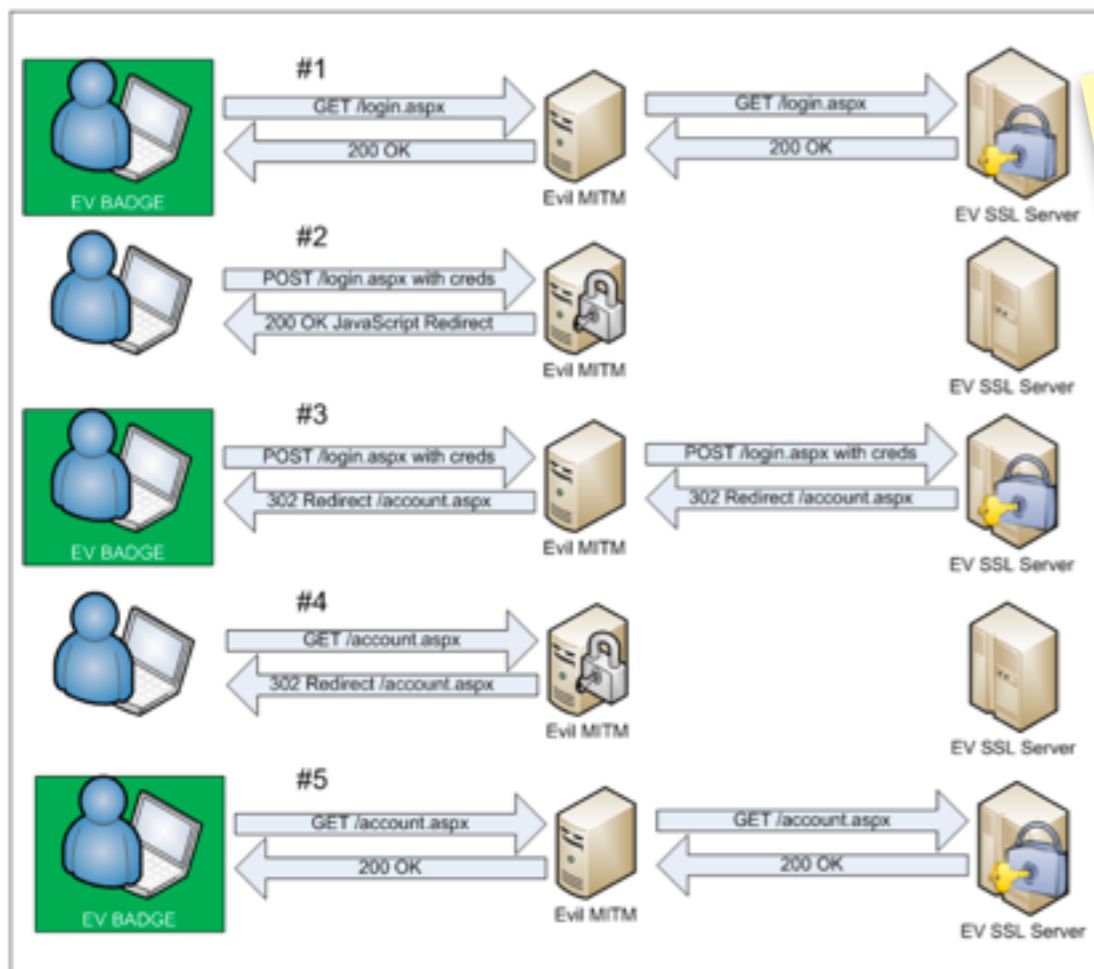


Figure: The request and response flow of an SSL Rebinding attack

Zusman & Sotirov 2009: <http://www.blackhat.com/presentations/bh-usa-09/SOTIROV/BHUSA09-Sotirov-AttackExtSSL-PAPER.pdf>

In Practice the DV-EV distinction can not be trusted

Zusman and Sotirov demonstrated rebinding attacks

UI arms-race

There have been exploits in terms of downgrading the trust relation while EV certificate badges were presented.

The underlying point is that there is an arms-race in implementation of security technology and improvement in the User Interface

651 organizations

So now and then one
of those organizations
will make a mistake or
be compromised



‘When you make an omelet you’ll break eggs’
‘When you chop there will be wood chips’

- The most recent example of operational mistakes causing wrong certificates to be leaked is TurkTrust.

Most recent case

TURKTRUST

- No malice but an operational mistake after an audit that caused this.

Operational mistake

- It is not to bash on this industry, but in any organization where people work there will be mistakes. And in the global infrastructure those sort of mistakes can cause damages.

No known exploits

No malice

<https://groups.google.com/forum/#!msg/mozilla.dev.security.policy/aqn0Zm-KxQ0/xIhfTMGwE2AJ>

And then there
are the
economics



This security world is highly competitive.

- There is a Race to the bottom: Minimal effort to live up to the compliance.
- The general mindset seems to be how can we make most money instead of how can we do the best job

Light at the end of the tunnel?

No Magic Bullets and Global Perspective

Counter Measures

Whitelisting

Blacklisting

When making a taxonomy of solutions

- We can use blacklists: test if certificate is rogue, or
- We can use whitelists: test if certificate is in vogue.

Counter Measures

Blacklisting

CRL

OCSP

Doesn't scale well
Only reliable when compromise is
known to have happened

The blacklist technologies

- Certificate Revocation lists
- Online certificate status protocol.

Problems

- Scaling properties
- Reliance on the party that made the mistake to revoke

Economic Incentive is to not be transparent.

Counter Measures

Whitelisting is proactive

- Pre-populating all browsers with all public keys doesn't scale well:
- fall back to caching systems with material you already visited.

Alternatively you could use alternative infrastructure:

- Specific services that offer certificates from different vantage points in order to single out the man in the middle attacks.
- 3rd Party trust broker (e.g Trusteer)
- DNS based solutions

Whitelisting

HTSP

Leap of Faith

And/or use alternative infrastructure

Domain Name
System

Independent Hierarchical
Registration

One root

Scalable and
Global

Namespace maps 1:1 to PKI
use

The certificates used within PKIX map to the DNS namespace.

The availability of the (correct) DNS data is directly related with the availability of the service in the first place.

Therefore storing fingerprints, public keys, or certificates in the DNS is not a bad idea.

Fate sharing

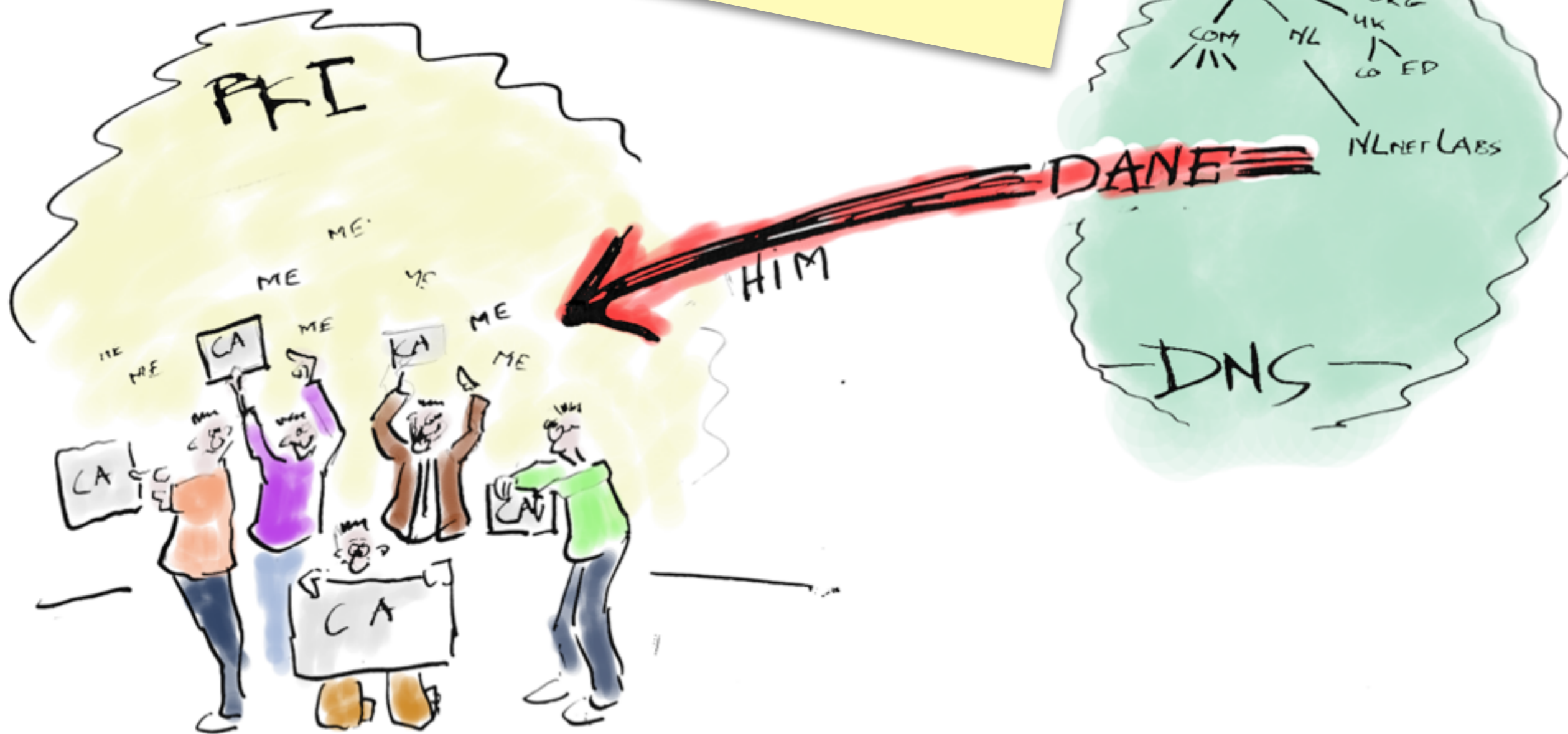
DANE

Using Secure DNS to Associate Certificates with Domain Names for TLS

<http://tools.ietf.org/wg/dane>

RFC 6698

Use the independent
DNS infrastructure to
vouch for the CA



TLSA RR

2.3. TLSA RR Examples

An example of a hashed (SHA-256) association of a certificate:

```
_443._tcp.www.example.com. IN TLSA (  
 0 0 1 d2abde240d7cd3ee6b4b28c54df034b9  
 7983ald16e8a410e4561cb106618e971 )
```

An example of a hashed (SHA-512) subject public key association of a PKIX end entity certificate:

```
_443._tcp.www.example.com. IN TLSA  
 1 1 2 92003ba34942dc74152e2f2c408d29ec  
 a5a520e7f2e06bb944f4dca346baf63c  
 1b177615d466f6c4b71c216a50292bd5  
 8c9ebdd2f74e38fe51ffd48c43326cbc )
```

An example of a full certificate association of a PKIX trust anchor:

```
_443._tcp.www.example.com. IN TLSA  
 2 0 0 30820307308201efa003020102020... )
```

- Store a public key of the CA that is supposed to sign a entity's certificate in the DNS
- Store a public key of the entities certificate in the DNS
- Store the certificate of the CA in the DNS
- Store the certificate of the entity in the DNS

Dane can also be used by the CA's to test if certificates offered to them are not intended to be signed by others.

Prevents DigiNotar CA vouching for google because google can signal they use Thawte

valid CERTs and/or CAs are stored in the the DNS: allow only those for your connection

assumption of compliance: CA will look up DANE RR before signing certificates

BEST OF BOTH WORLDS

DANE offers the protection that you are looking at a valid EV certificate

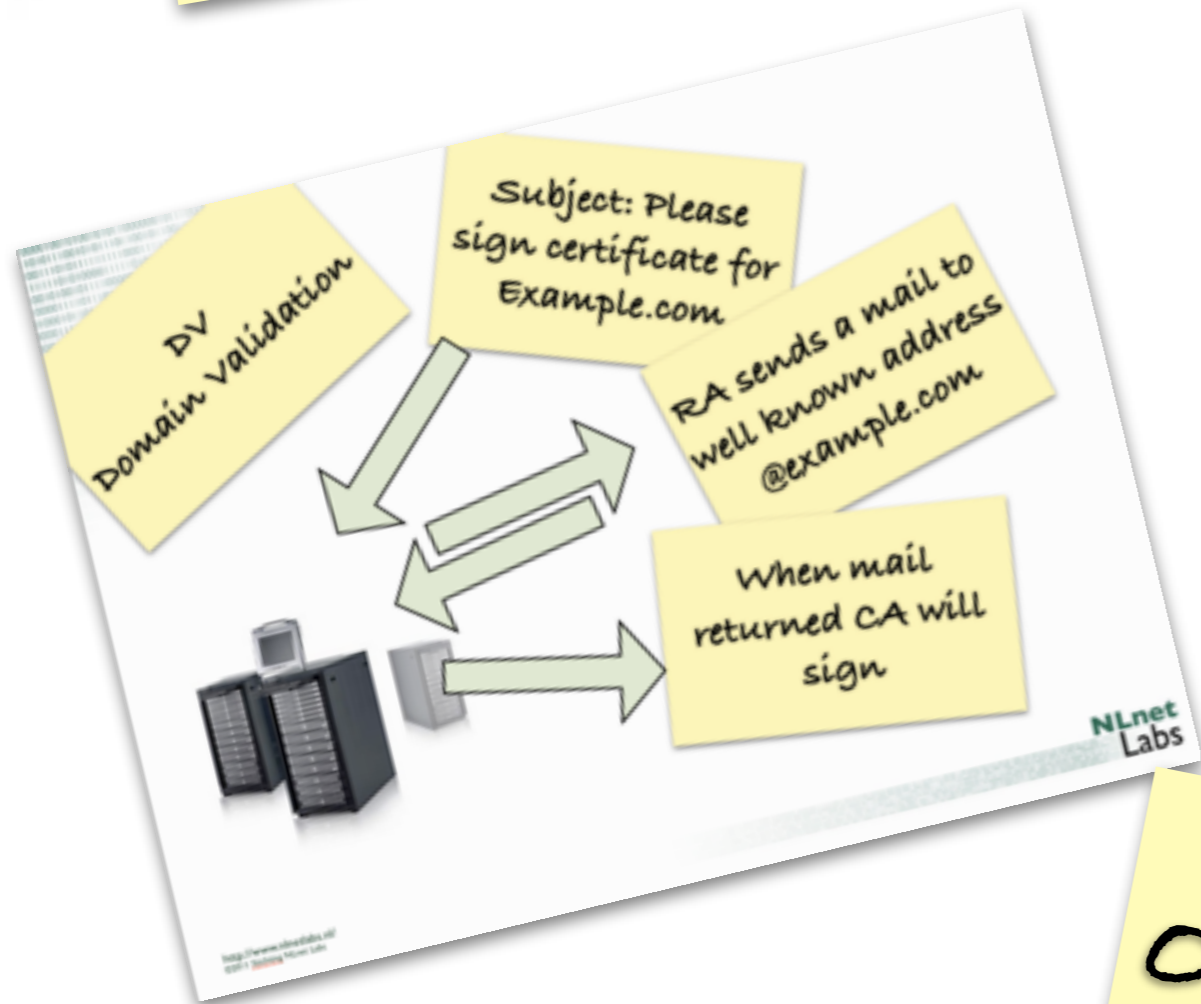
The EV certificate offers you the legal paper trail that you are doing business with a real company

How about DV certificates,
are they useless?

CAs checking the
DNS are not
needed

The CERT can be
stored in the DNS at
once

One of DANE's use cases



How does
DNSSEC get
into the picture



DANE depends on the
authenticity and integrity

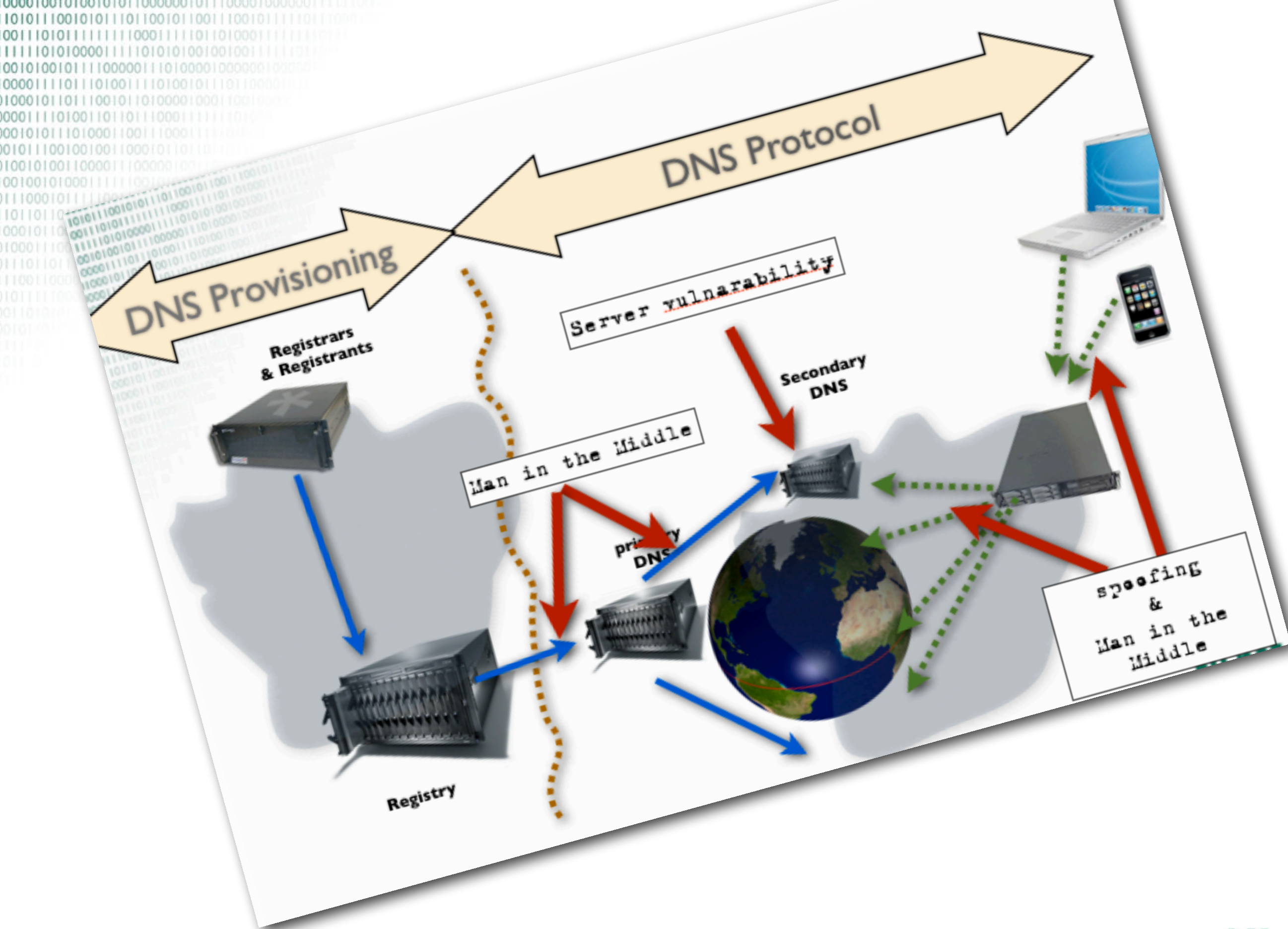
**PREVENTS A CLASS OF
MAN IN THE MIDDLE
ATTACKS THAT MAKE
CERTIFICATE EXPLOITS
POSSIBLE**

And it offers a building
for further security
innovation

10101110010101110110010110011100101111011001111
0011101011111110001111011010001111110111
11111010100011110101010010010011111011011
001010010111000011101000100000100001
0000111011101001110100101101100001111
10001011011100101010001000110010001
00011110101101101100111111010111
001010110100110011000111110111
010111001001001000101101101111
100101001100011100001001100
001001010011111001010101
111000101111001101001111
101101101110111101111
00010110010100101001
1000111001001001
1110110111001111
110011000011111
10111110001111
101101011111
111111111111
101111111111
111111111111
101111111111
111111111111

Hold it

*you only talked DNSSEC
technology*



Note though that w.r.t. provisioning DNS has similar weaknesses. Registries and Registrars sometimes make mistakes

technology.ie/google-ie-hijacked/

NEWS / VIEWS / REVIEWS

TECHNOLOGY

WEEKLY PODCAST AND UPDATES FROM THE TECH SCENE

Home General Podcasts Video

Google.ie Hijacked?

by Michele on October 9, 2012 in security

Tweet Like +1 Share

It looks like Google.ie has been hijacked

The current whois record shows:



Image via CrunchBase

“ *whois google.ie*

*% Rights restricted by copyright;
http://iedr.ie/index.php/mnudomregs/mnudnssearch/96
% Do not remove this notice*

domain: google.ie
descr: Google, Inc
descr: Body Corporate (Ltd,PLC,Company)
descr: Registered Trade Mark Name
admin-c: KR59-IEDR

Search...

POPULAR LATEST COMMENTS TAGS

- Google.ie Hijacked? OCTOBER 9, 2012
- Breaking: Portugal Says Peer to Peer Sharing Is Legal SEPTEMBER 26, 2012
- Technology.ie Podcast #1 SEPTEMBER 28, 2011
- Some Ulster Bank Memes JULY 6, 2012
- Croatian Startup To Power US Presidential Debate Twitter Interaction OCTOBER 3, 2012

- In the DNS registration space similar problems to PKI
- For DV reduction in attack surface:
 - Instead of offering two potential points of compromise in the registration chain you only offer one.
- But for Extended Validity certificates compromising the DNS doesn't trivially result in the possibility to obtain a EV certificate.
- Fate sharing in the DNS: If the DNS is compromised it is trivial to not offer an HTTPS service and use a fallback attack towards a service.
- Trust in correct functioning of the DNS is already critically



Wrap-up

DANE has the potential to solve important aspects PKI/TLS problems

Not a magic bullet

Not the only approach

'convergence'

DNSSEC is needed infrastructure: securing and enabling at the same time

Not a magic bullet either

The Internet PKI has a trust issue.

A global trust issue

Scalability problems:
compliance and
technology

Internet Trust is Global
Trust

Local action global
effect

misaligned
incentives



How to increase
global trust in
the internet?

Without a race to
the bottom of
minimal
compliance?

With meaningful
incremental steps
in improving
technology?

NLnet Labs is a not-for-profit R&D lab that develops Open Source and Open Standards for the good of the Internet.

Our contributions include the NSD and Unbound name servers, a number of RFCs and technical publications. With competent technical input about Internet Technology we have impact in standardisation and Internet Governance.

We welcome your support.

That's it folk

**Questions, comments,
ideas:
olaf@nlnetlabs.nl**

