DNSSEC Musings

Diginotar, DANE, and Deployment

Olaf M. Kolkman

Acknowledgements:
Jakob Schlyter
Geoff Huston
Dan Kaminsky

http://www.nlnetlabs.nl/

NLnet Labs

Olaf Kolkman
NLnet Labs

- I have an agenda; I want an Internet that is:
  - resilient
  - secure
  - open
  - sustainable
  - trustworthy

101

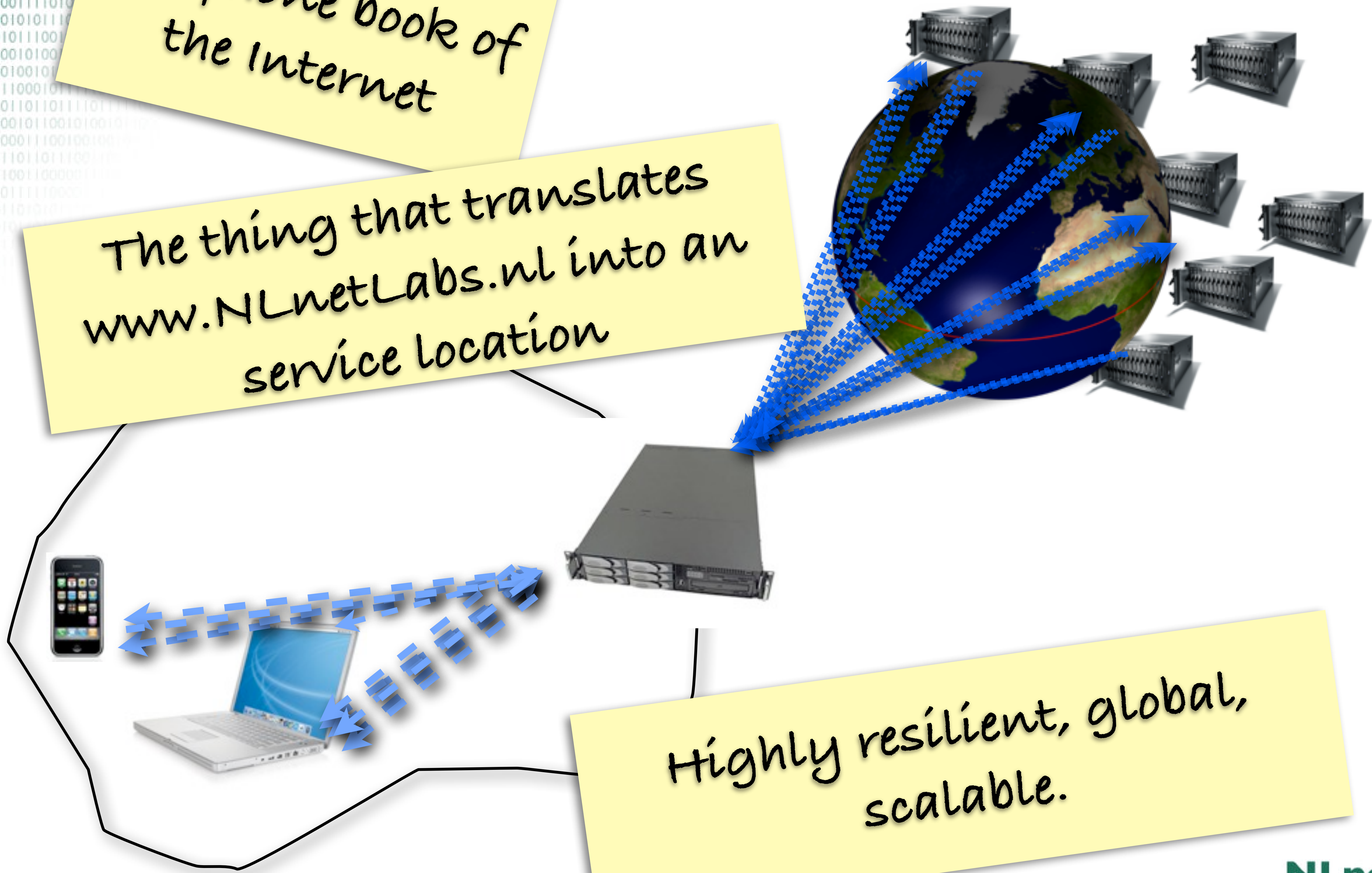
All the basics you need to know

DNS

Basics: The Domain Name System

Telephone book of the Internet

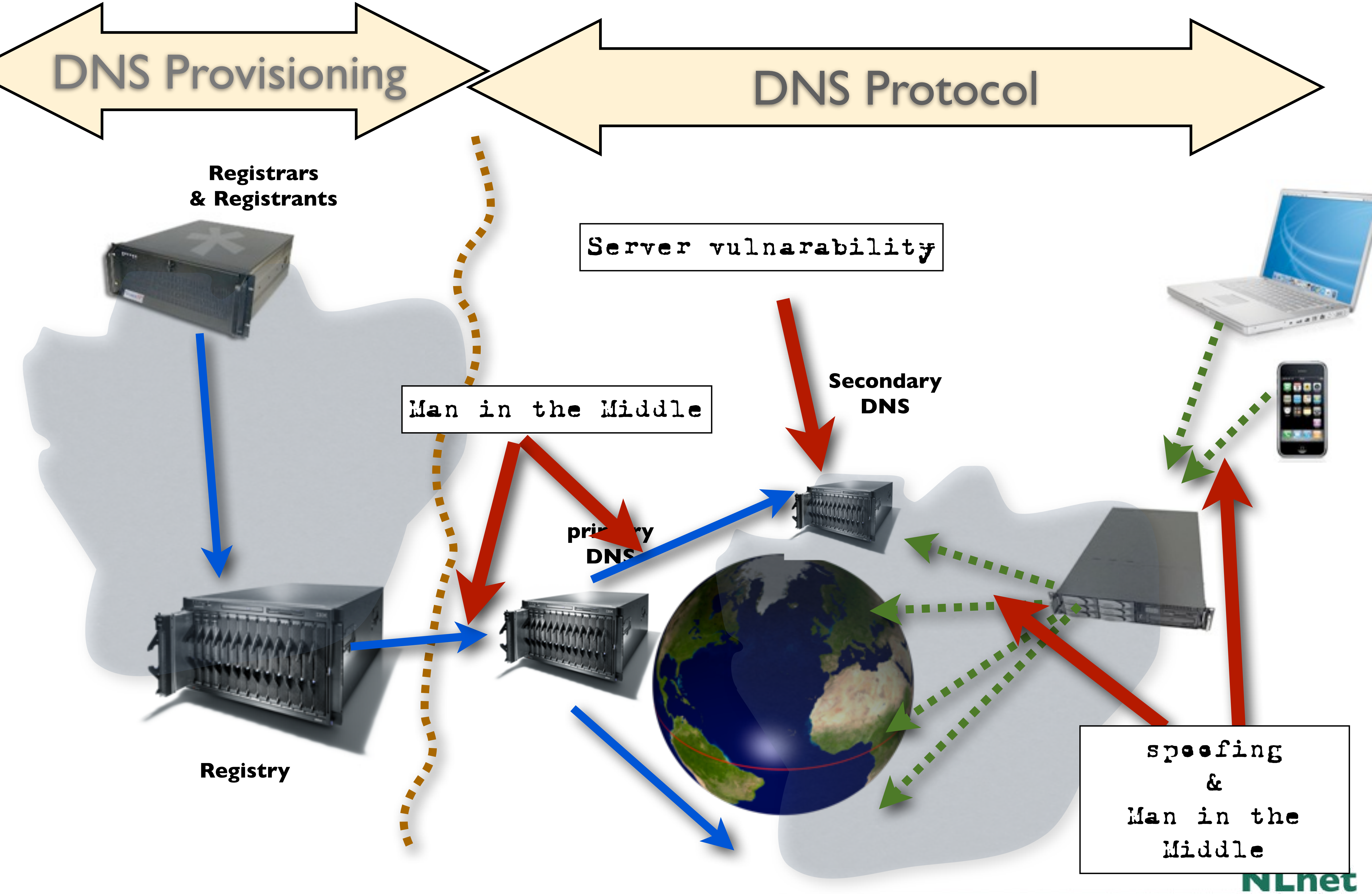
The thing that translates www.NLnetLabs.nl into an service location



Highly resilient, global, scalable.

http://www.nlnetlabs.nl/

NLnet Labs



DNS Provisioning

DNS Protocol

Registrars
& Registrants

Server vulnarability

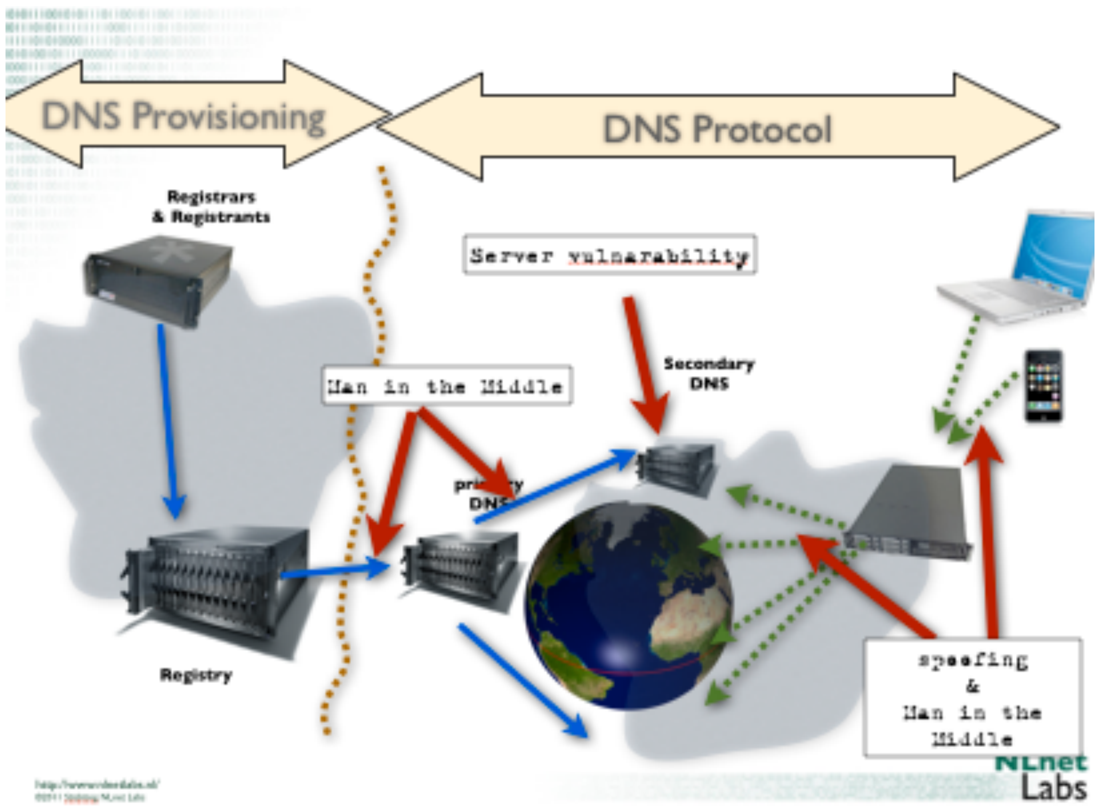
Man in the Middle

Secondary
DNS

primary
DNS

Registry

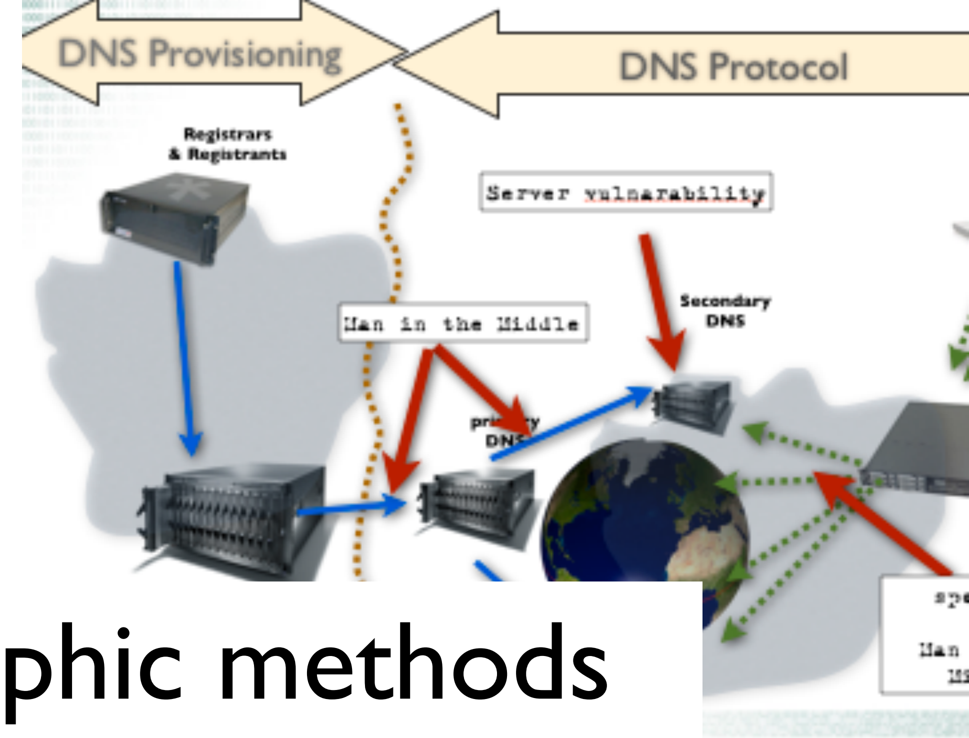
spoofing
&
Man in the
Middle



- 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

- Certification assert authenticity of public key material.
- Authenticity of Certificate forms the basis for integrity and confidentiality of SSL and TLS
- only widely deployed security technology on the Internet and depends to a great extend on trust in a set of specific 3rd parties: The registration authorities.
- We will talk about the role of these registration authorities later in this presentation.

In this context technology to assert authenticity.

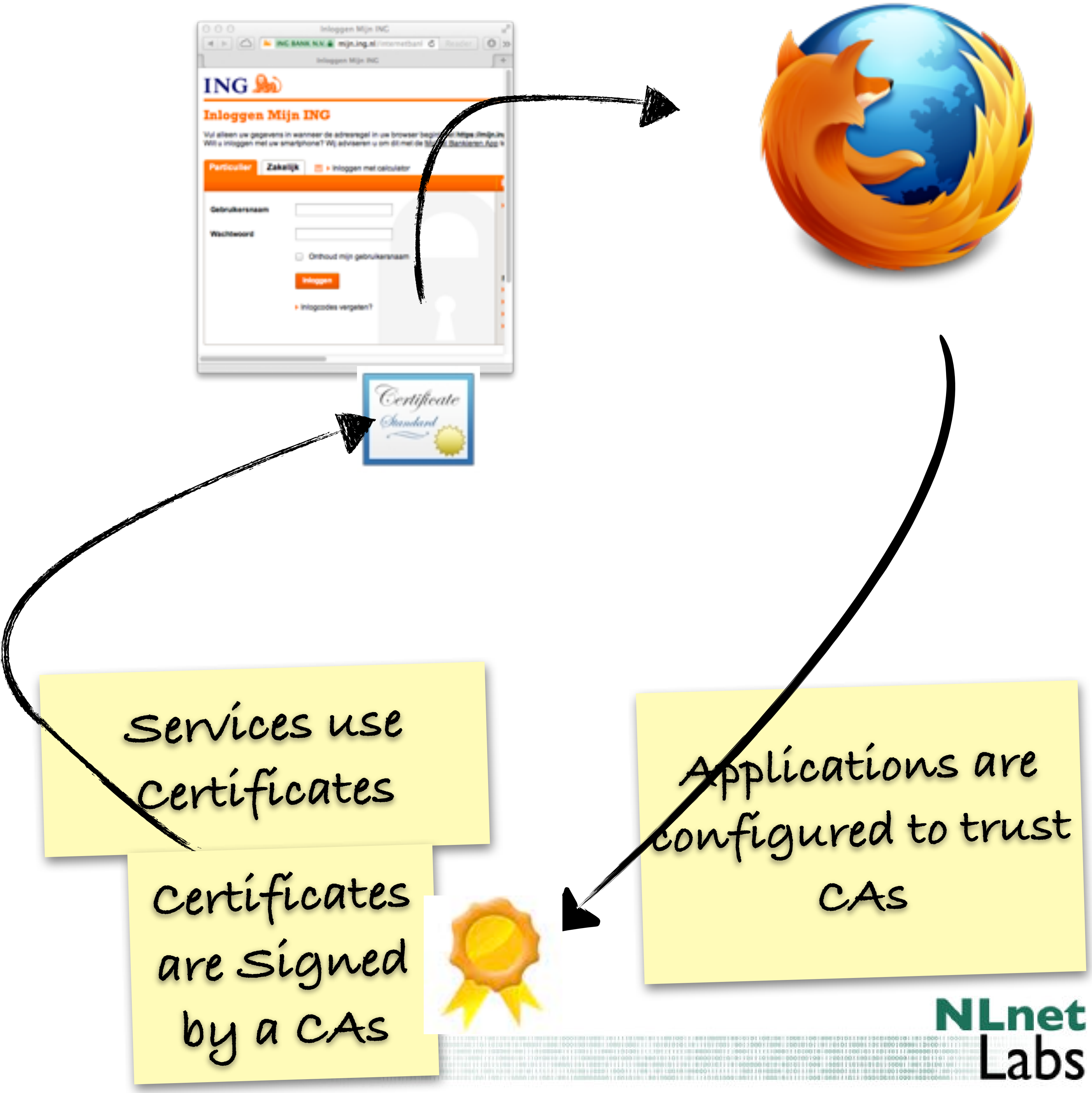
Provides a basis for integrity and confidentiality of connections

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

TRANSITIVE TRUST

- Trust a certain browser vendor (OS vendor) results in
- Trust in Certification Authorities
- Signatures over service names provided by CAs result in browsers trusting those services.

If one of the entities in this chain breaks trust then the trust breaks down.



Services use certificates

Certificates are signed by a CAs

Applications are configured to trust CAs

Ali and his magic Browser

how failure in technology and compliance almost brought misery and doom

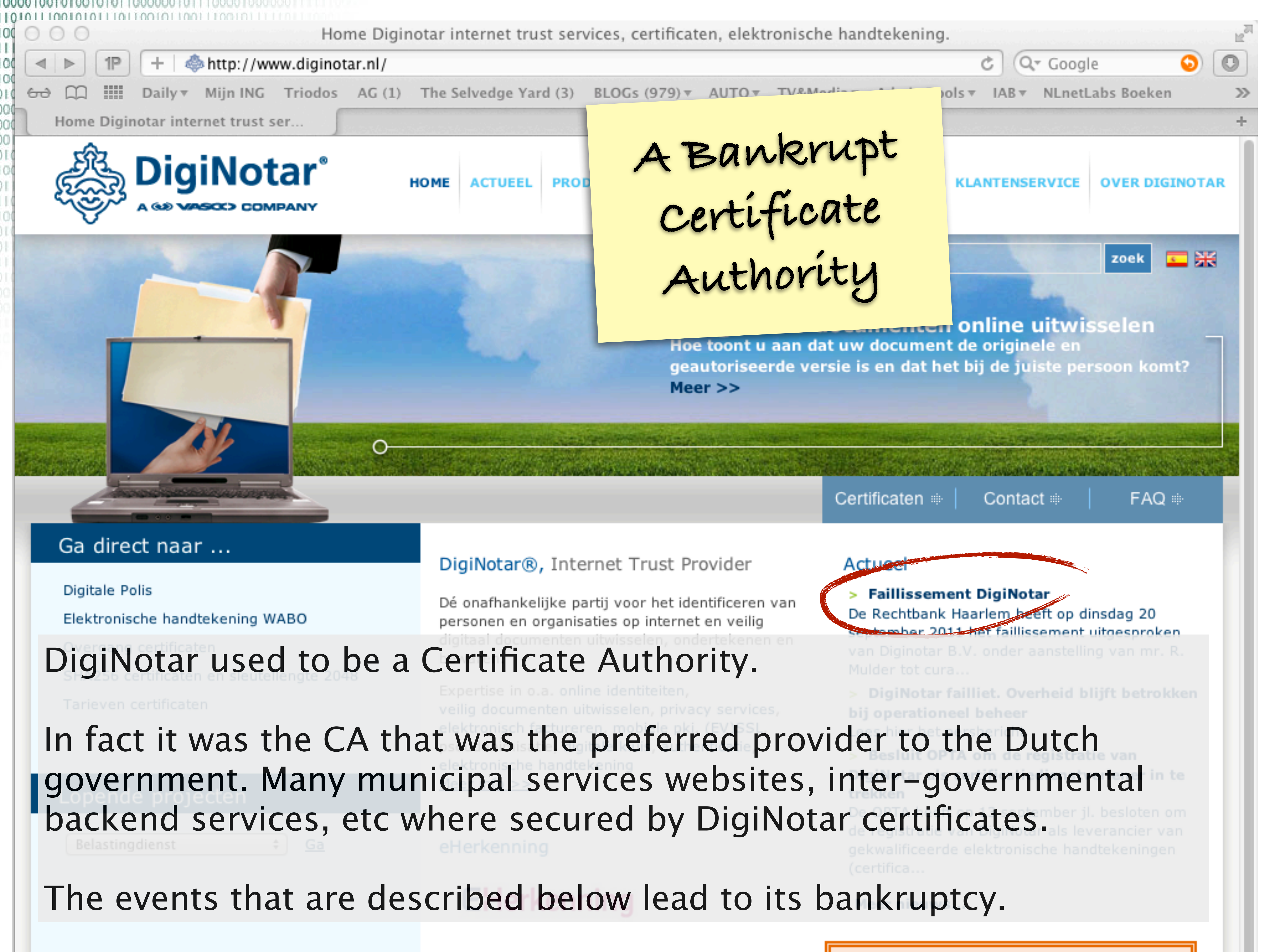
In this chapter of the presentation we talk about “Ali” and how his browser settings disclosed a major problem and caused a scandal.

September 2011

DigiNotar®
A VASCO COMPANY

This is the story of DigiNotar: A Dutch X509 Certificate Authority

A Bankrupt Certificate Authority



Home Diginotar internet trust services, certificaten, elektronische handtekening.

http://www.diginotar.nl/

Google

Daily Mijn ING Triodos AG (1) The Selvedge Yard (3) BLOGs (979) AUTO TV&Media ools IAB NLnetLabs Boeken

Home Diginotar internet trust ser...

DigiNotar® A VASCO COMPANY

HOME ACTUEEL PROD KLANTENSERVICE OVER DIGINOTAR

zoek

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

Overzicht certificaten

SHA256 certificaten en sleutellengte 2048

Tarieven certificaten

Lopende projecten

Belastingdienst Ga

DigiNotar®, Internet Trust Provider

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

Expertise in o.a. online identiteiten, veilig documenten uitwisselen, privacy services, elektronisch factureren, mobiele pki, (EV)SSL

elektronische handtekening

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

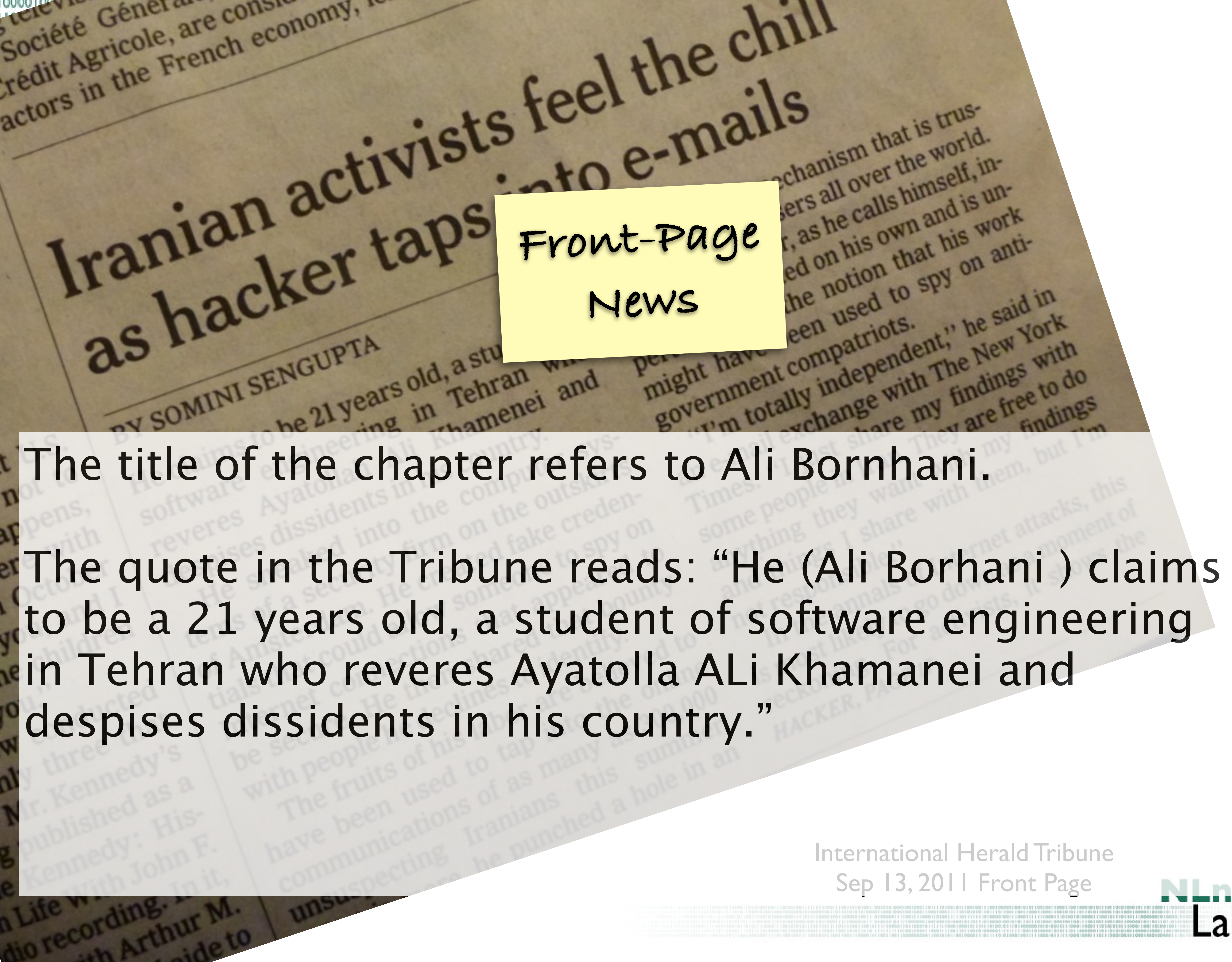
> Besluit OPTA om de registratie van DigiNotar in te trekken

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

DigiNotar used to be a Certificate Authority.

In fact it was the CA that was the preferred provider to the Dutch government. Many municipal services websites, inter-governmental backend services, etc where secured by DigiNotar certificates.

The events that are described below lead to its bankruptcy.



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

BY SOMINI SENGUPTA

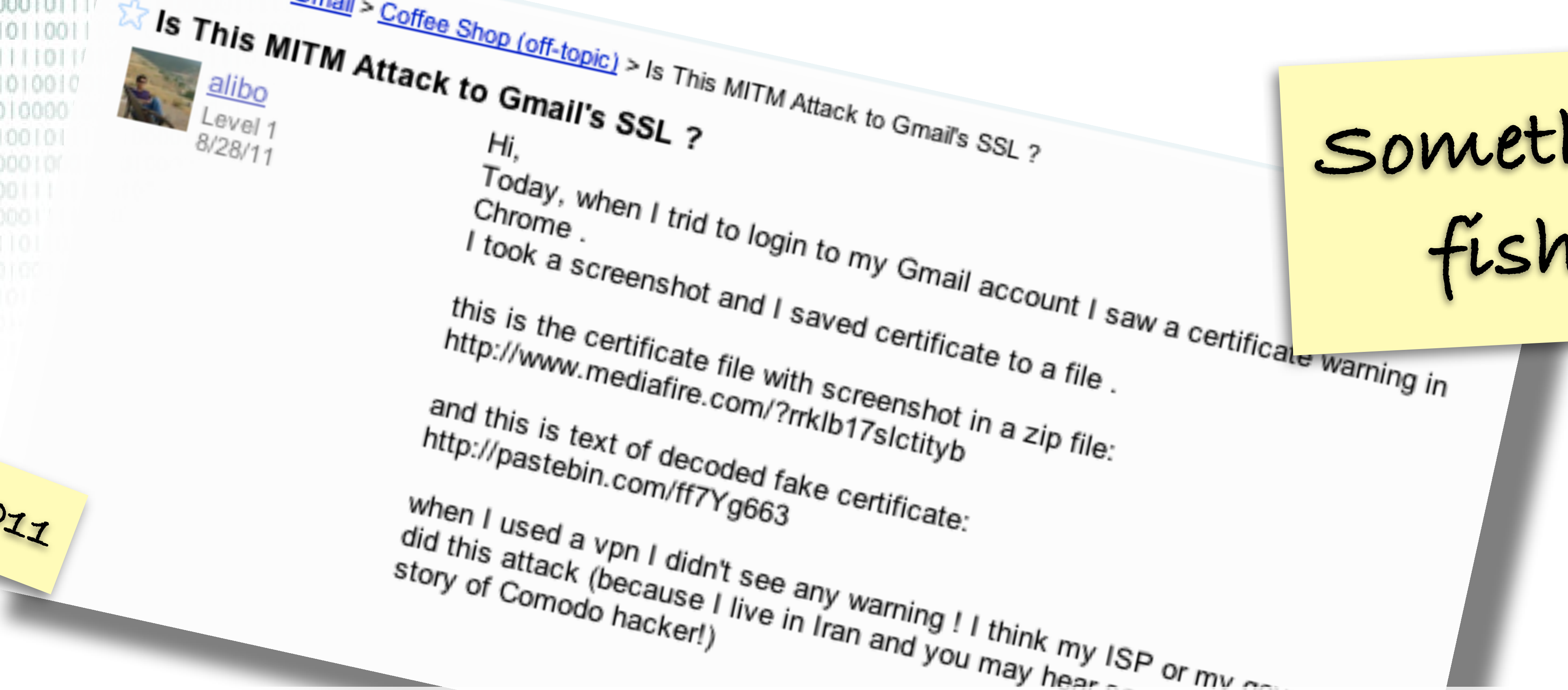
Front-Page News

The title of the chapter refers to Ali Bornhani.

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

Chain of ~~trust~~ Events



mail > 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 story of Comodo hacker!)

Something fishy

28 Aug 2011

August 28 Iranian blogger Ali Borhani (Alibo) astutely noticed fake certificate. He posted the warning message that his Chrome browser showed to a Gmail forum.

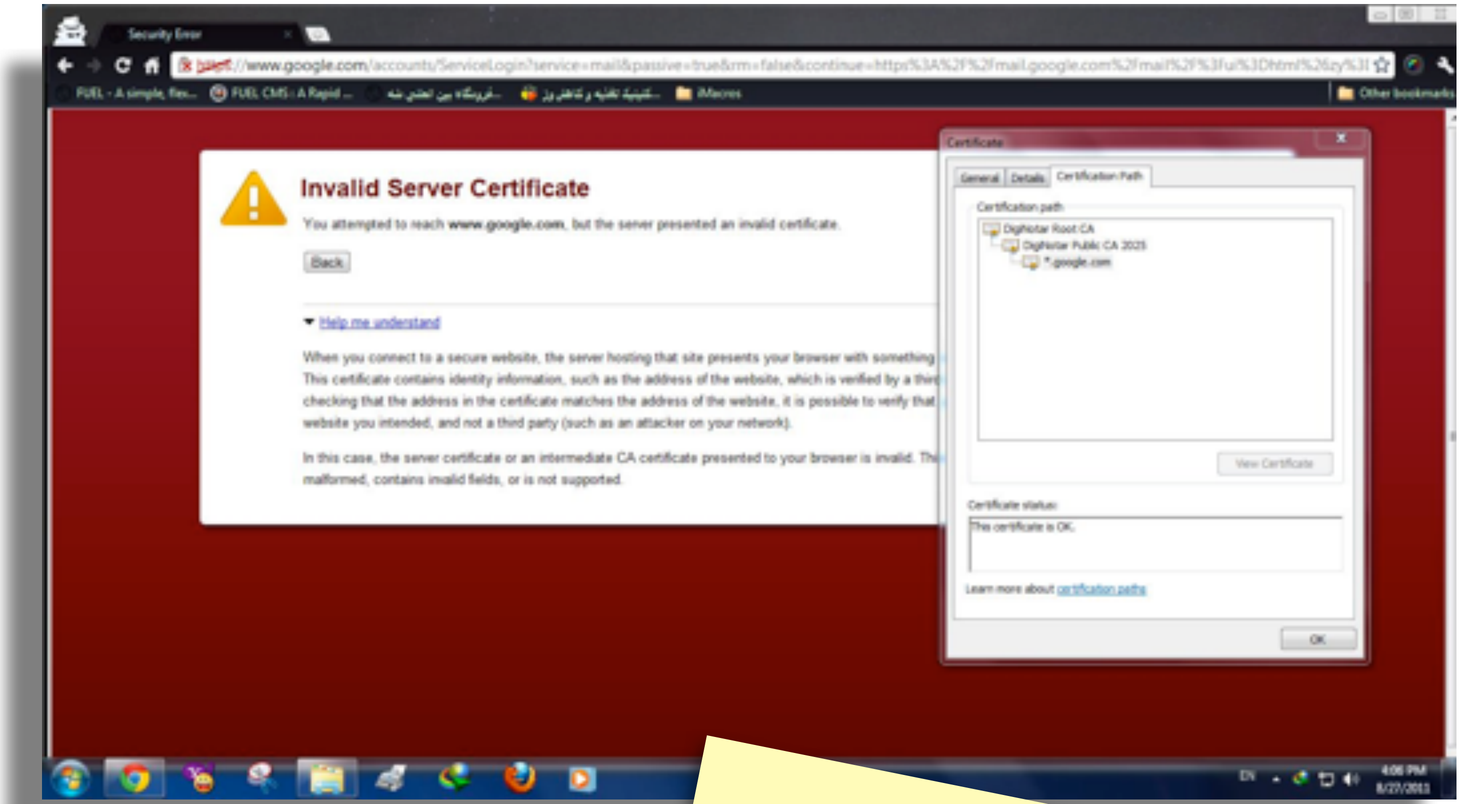
He knew about previous incidents with Certificate infrastructure and did an experiment using a VPN where he did not notice problems: His thesis was “Man in the Middle attack by Government or ISP”.

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)

This is the screen shot Ali posted.

It is the Chrome browser showing that there is a signed google wildcard certificate that is validated by DIGInotar. However Chrome still flagged this as invalid.


Security Error
https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=https%3A%2F%2Fmail.google.com%2Fmail%2F%3Fui%3Dhtml%26zy%3I
Other bookmarks

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 thir
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. Th
malformed, contains invalid fields, or is not supported.

Certificate

General | Details | Certification Path

Certification path

DigiNotar Root CA
DigiNotar Public CA 2025
*.google.com

View Certificate

Certificate status:

This certificate is OK.

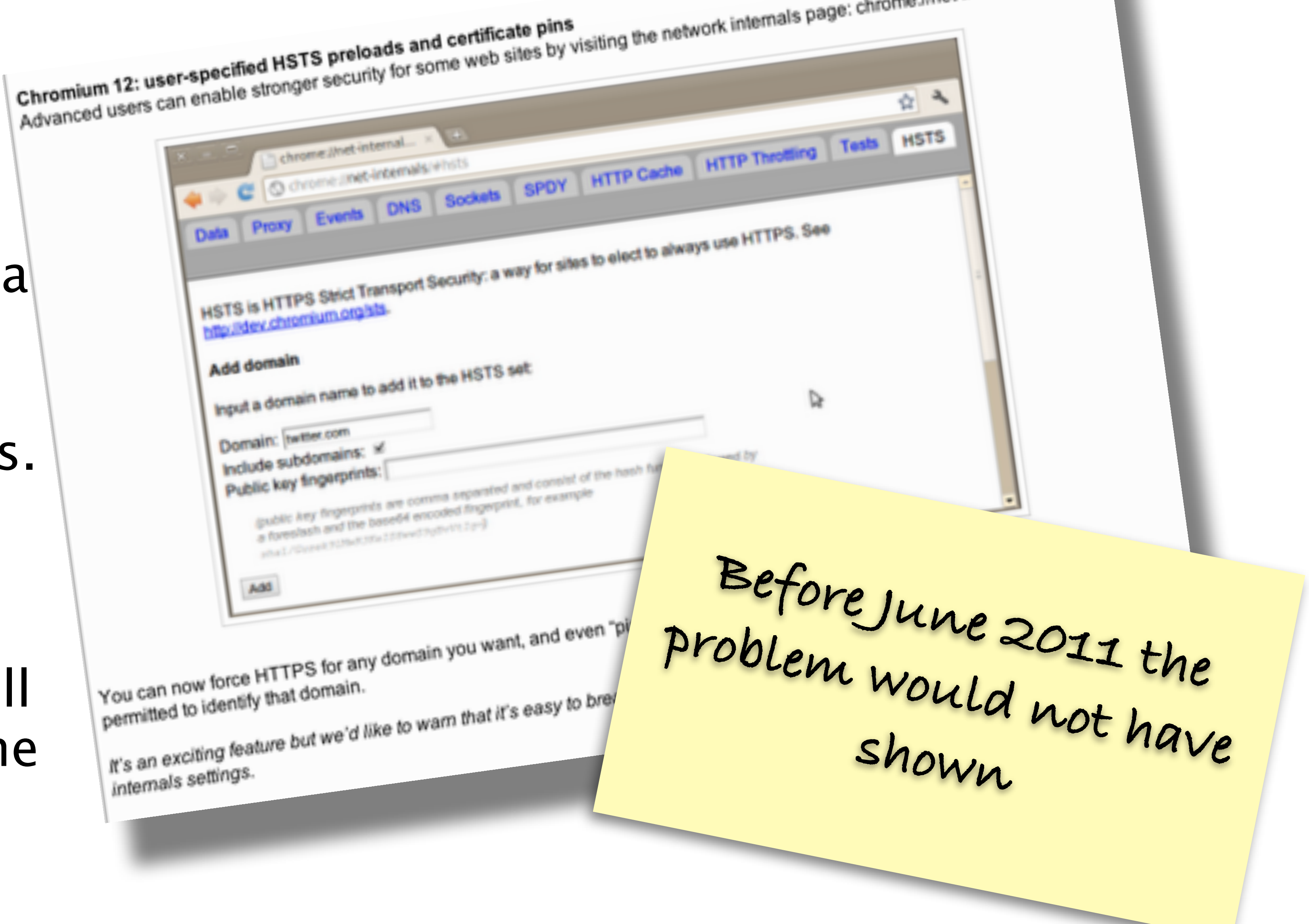
Learn more about certification paths

OK

Google Chrome magic caught this!

In June Chrome had introduced a technique called HTTPS Strict Transport Security (HSTS) in combination with certificate pins.

Fingerprint of certificates used for specific connections are being cached and exceptions will be flagged. The fingerprint of the google certificates come preconfigured.



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://ne

HSTS is HTTPS Strict Transport Security: a way for sites to elect to always use HTTPS. See http://dev.chromium.org/sts.

Add domain

Input a domain name to add it to the HSTS set:

Domain: twitter.com
Include subdomains: ✓
Public key fingerprints:

(public key fingerprints are comma separated and consist of the hash fu[illegible]ed by a foreslash and the base64 encoded fingerprint, for example [illegible])

You can now force HTTPS for any domain you want, and even "pi
permitted to identify that domain.

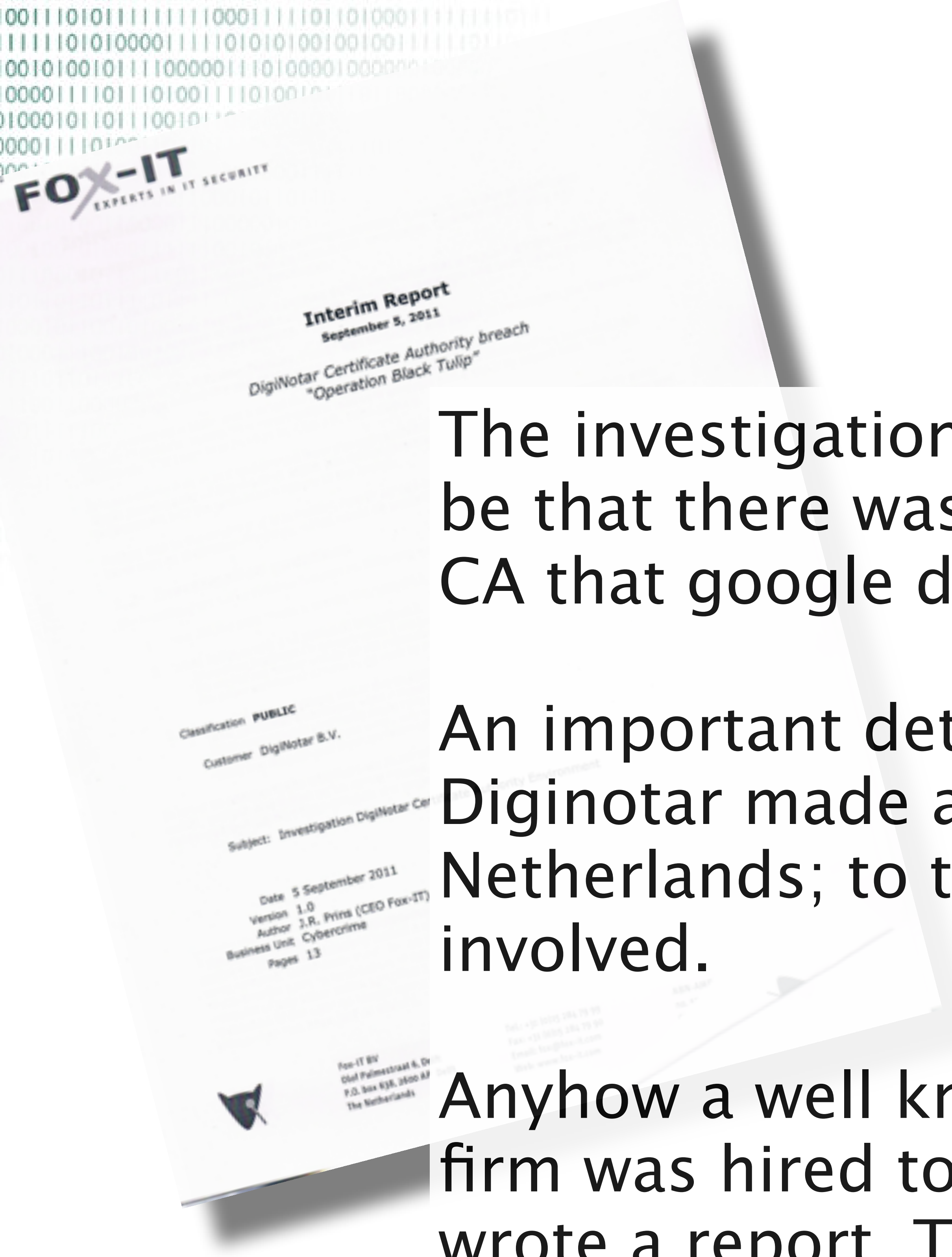
*It's an exciting feature but we'd like to warn that it's easy to bre
internals settings.*

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?



FOX-IT
EXPERTS IN IT SECURITY

Interim Report
September 5, 2011

DigiNotar Certificate Authority breach
"Operation Black Tulip"

Classification **PUBLIC**

Customer DigiNotar B.V.

Subject: Investigation DigiNotar Ce

Date 5 September 2011
Version 1.0
Author J.R. Prins (CEO Fox-IT)
Business Unit Cybercrime
Pages 13

Fox-IT BV
Olof Palmestraat 6, De
P.O. Box 638, 2600 AP
The Netherlands

The investigation zoomed into Diginotar: How could it be that there was a signed google certificate from a CA that google doesn't o business with?

An important detail is that a perceived problem with Diginotar made all kinds of alarm bells go off in the Netherlands; to the point the responsible minister got involved.

Anyhow a well known and respected Dutch security firm was hired to investigate what went on and they wrote a report. That report is a good read.

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

Compromised certificate issued by: DigiNotar

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

Incomplete audit trails

Fox-IT hired t investigate

Multiple hacker tools on the servers

Specialized PKI scripts

Fingerprint Similarity to Comodo Hacker

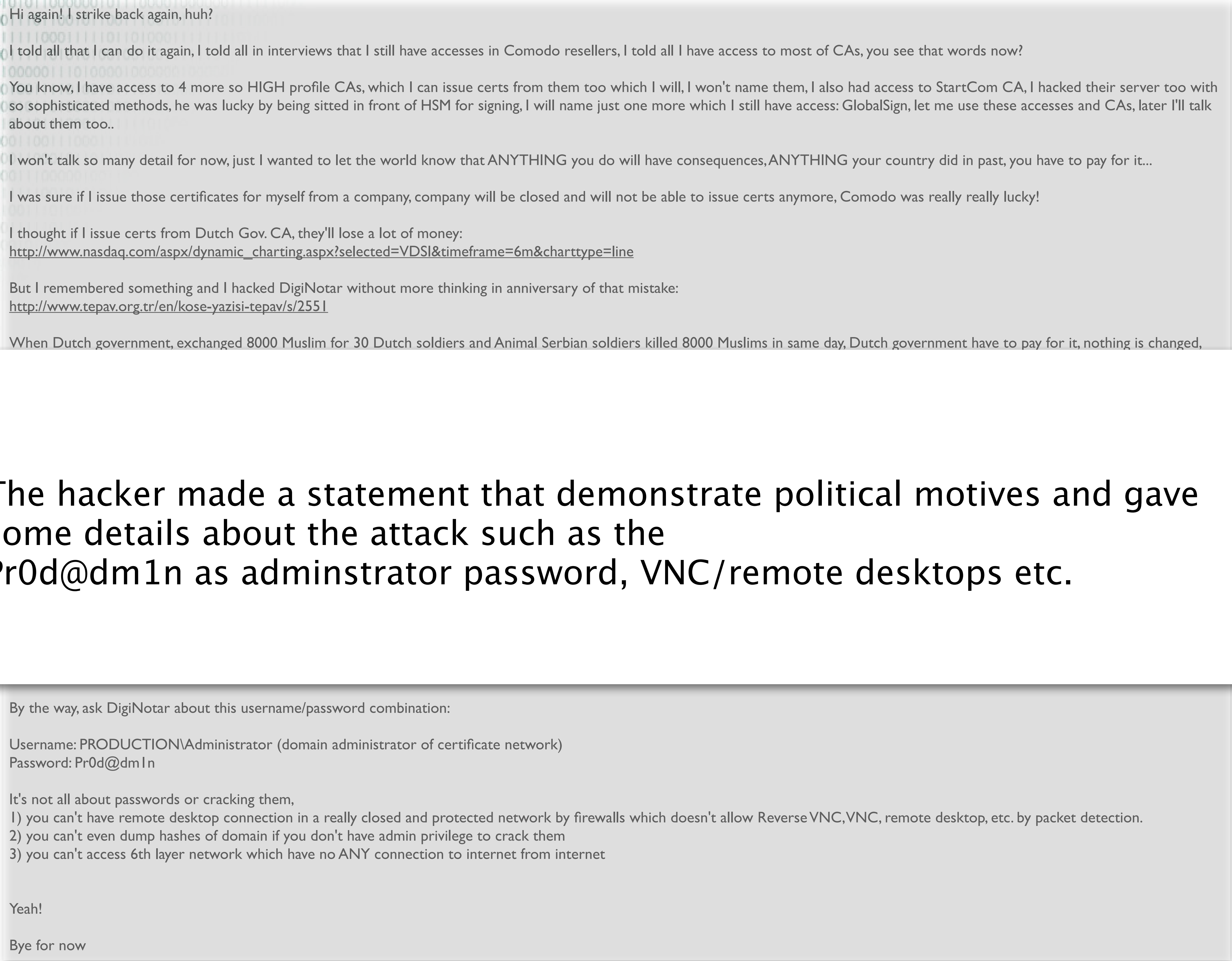
Advanced and Amateur

And a claim by the hacker

My summary of the report: A bloody scandal. Exploits were noticed and not made public. Commercial Interests got in the way of transparency.

The details: Fox-IT traced back how hackers found their way into the Diginotar systems. They discovered dedicated and highly specialized scripts for PKI management, but also some script-kiddy material.

The Diginotar people had incomplete audit trails, knew about earlier compromise, and had remained silent about it.



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/aspx/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,

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 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.

http://pastebin.com/1AxH30em

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

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

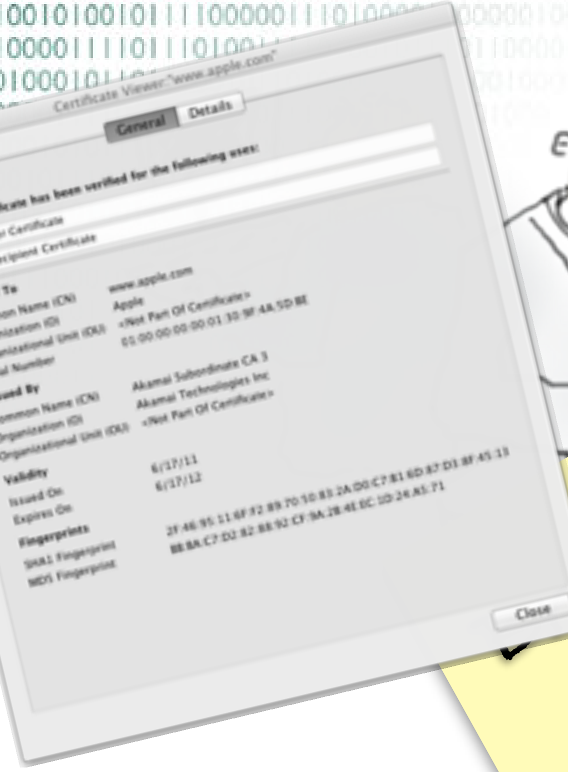
Trust issues in todays browser.
The underlying system and assumptions.

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.

This grandma was borrowed from http://farm3.staticflickr.com/2145/1713612630_2ddcec1d2a_z.jpg



Certificate Viewer:"www.apple.com"

General | Details

icate has been verified for the following uses:

r Certificate

ipient Certificate

To	
on Name (CN)	www.apple.com
ization (O)	Apple
anizational Unit (OU)	<Not Part Of Certificate>
al Number	01:00:00:00:00:01:30:9F:4A:5D:8E
ued By	
ommon Name (CN)	Akamai Subordinate CA 3
rganization (O)	Akamai Technologies Inc
Organizational Unit (OU)	<Not Part Of Certificate>
Validity	
Issued On	6/17/11
Expires On	6/17/12
Fingerprints	
SHA1 Fingerprint	2F:46:95:11:6F:F2:89:70:10:83:2A:D0:C7:81:6D:87:D1:8F:45:13
MD5 Fingerprint	88:8A:C7:D2:82:88:92:CF:9A:28:4E:DC:1D:24:A5:71

owser 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 aprox 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

CA
RA
SUBJECT

Subject Requests

RA performs checks

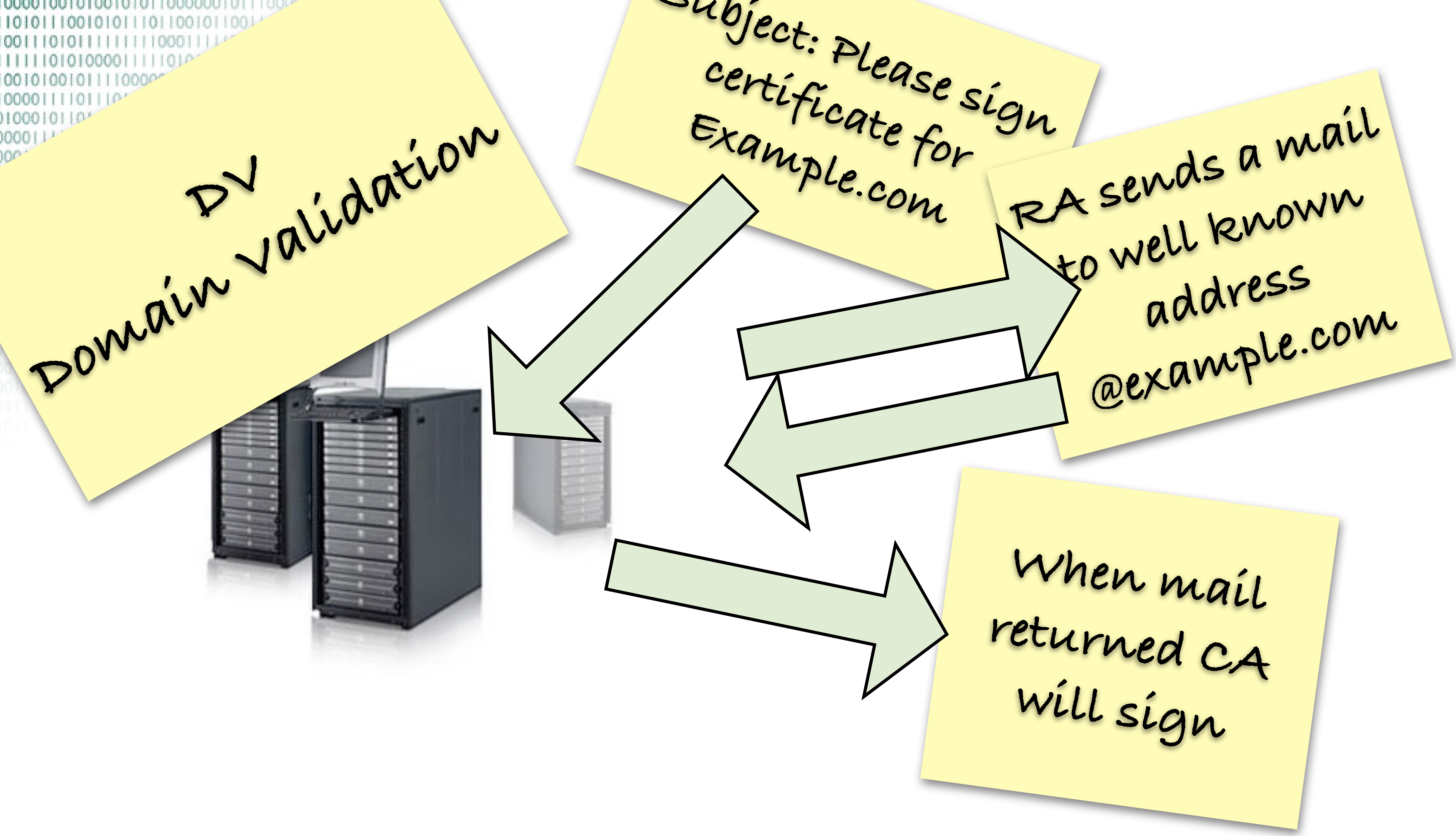
RA tells CA to sign

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



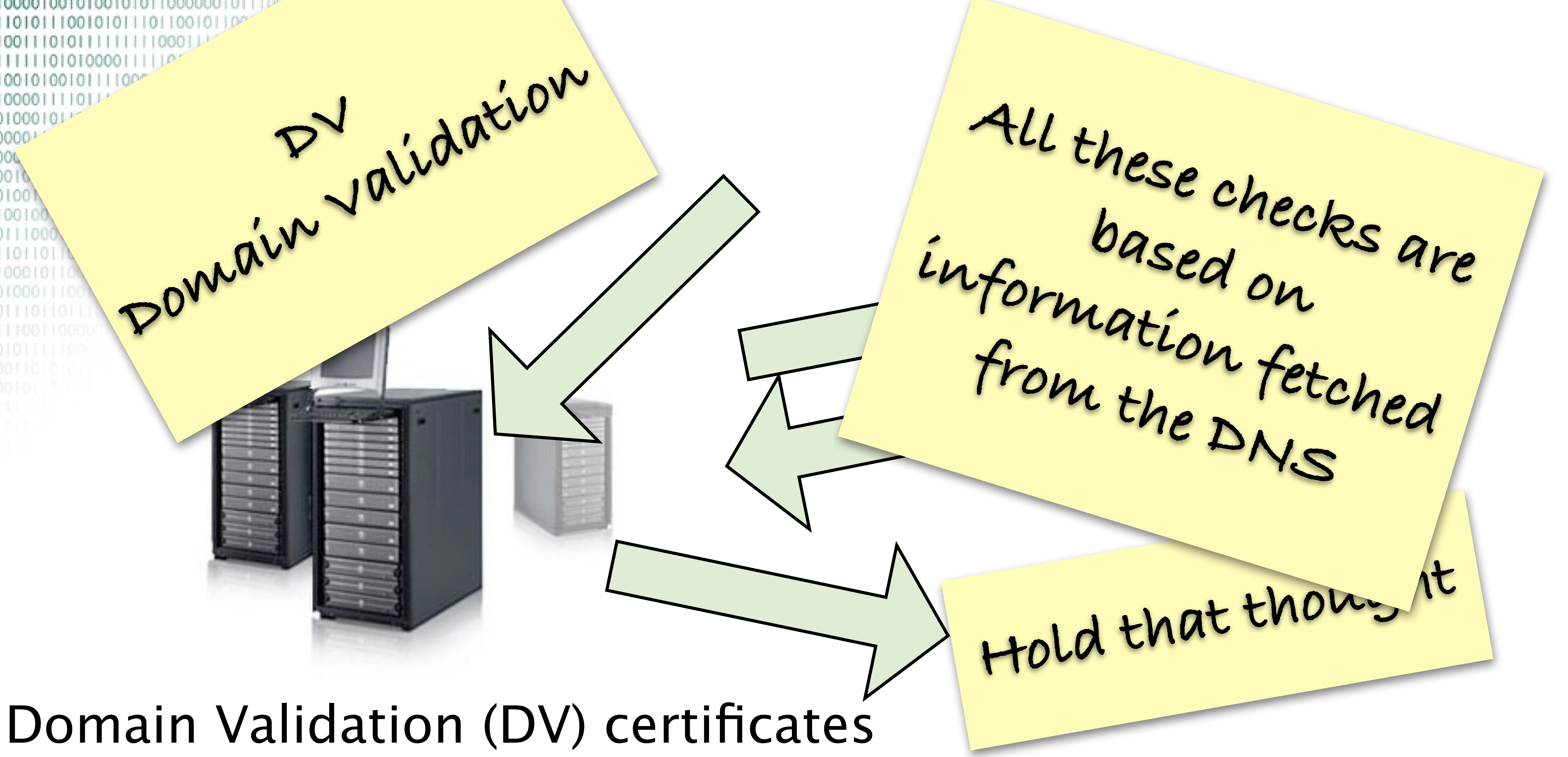
DV
Domain Validation

Subject: Please sign certificate for Example.com

RA sends a mail to well known address @example.com

When mail returned CA will sign

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



DV
Domain Validation

All these checks are based on information fetched from the DNS

Hold that thought

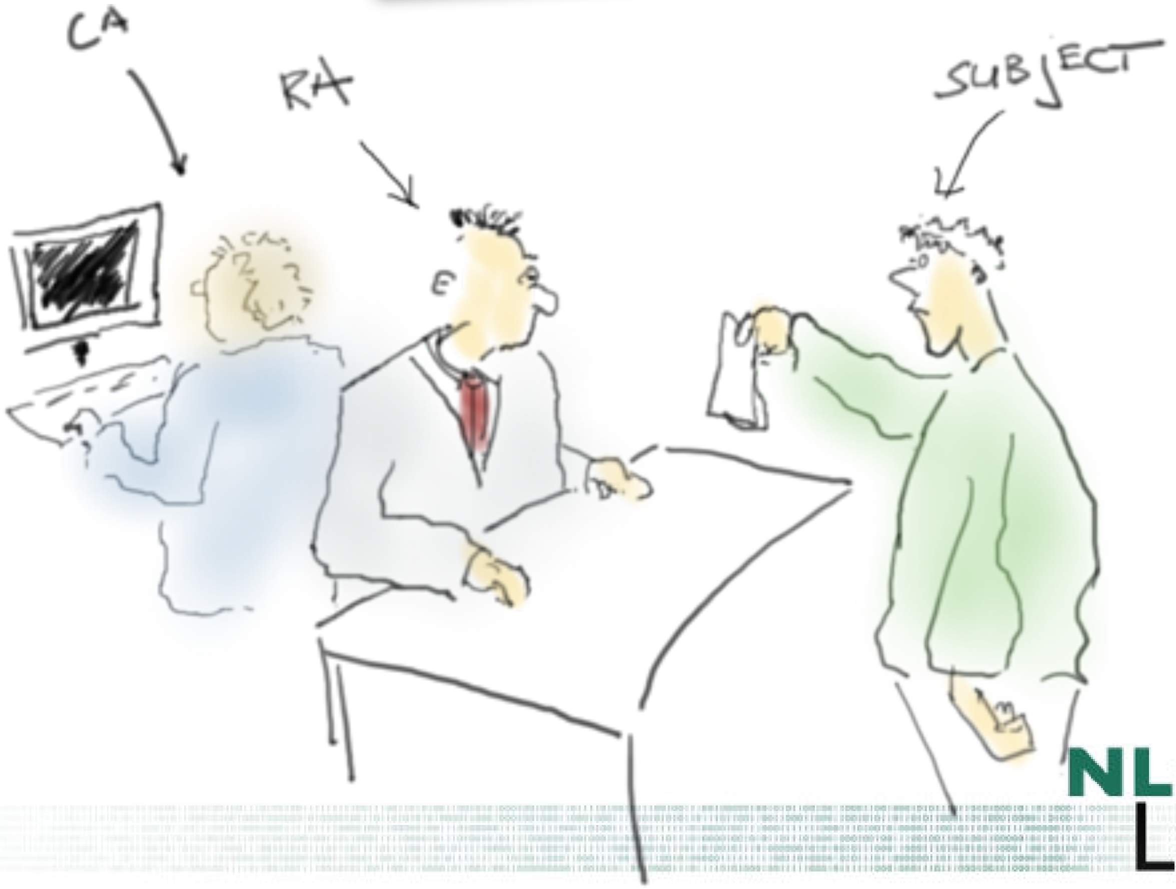
Domain Validation (DV) certificates
This how the industry evolved over the first years of PKI use:
An economic raise to the bottom, causing DV certificates to cost cents or even been given away for free.

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

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

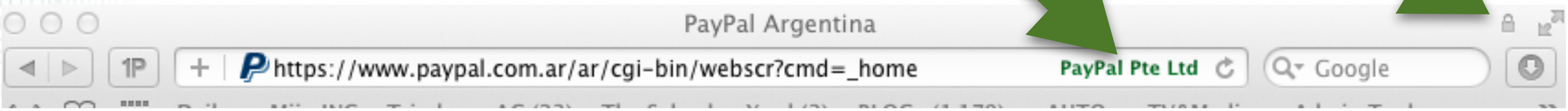
Domain validity

Extended validity



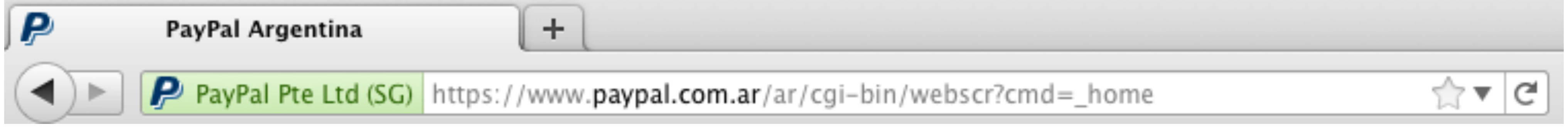
DV/EV
Would you notice the difference?

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



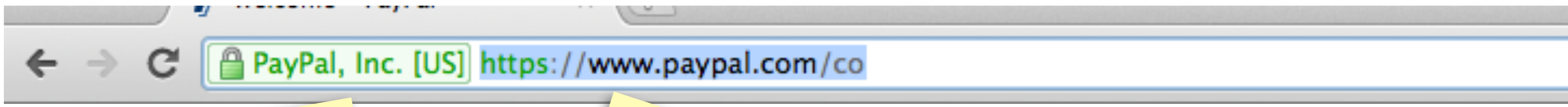
PayPal Argentina

https://www.paypal.com.ar/ar/cgi-bin/webscr?cmd=_home PayPal Pte Ltd



PayPal Argentina

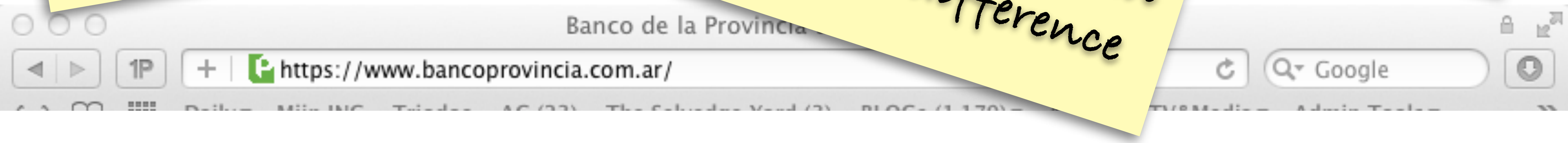
PayPal Pte Ltd (SG) https://www.paypal.com.ar/ar/cgi-bin/webscr?cmd=_home



PayPal, Inc. [US] https://www.paypal.com/co

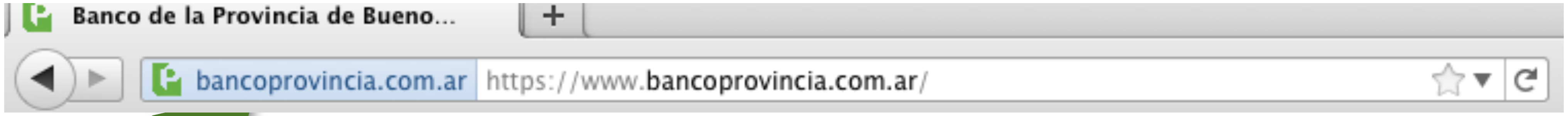
Fortunately

The trained eye can spot the difference



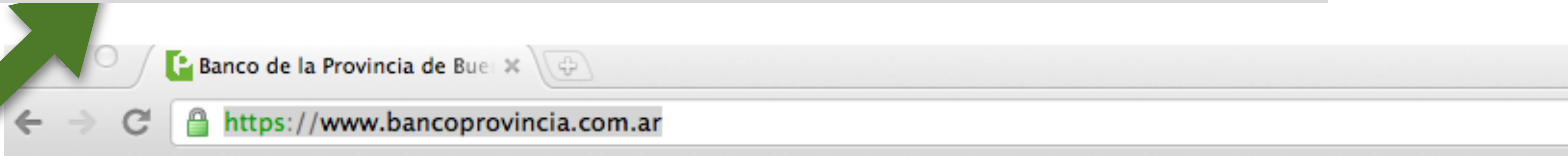
Banco de la Provincia

https://www.bancoprovincia.com.ar/



Banco de la Provincia de Bueno...

bancoprovincia.com.ar https://www.bancoprovincia.com.ar/



Banco de la Provincia de Bue

https://www.bancoprovincia.com.ar

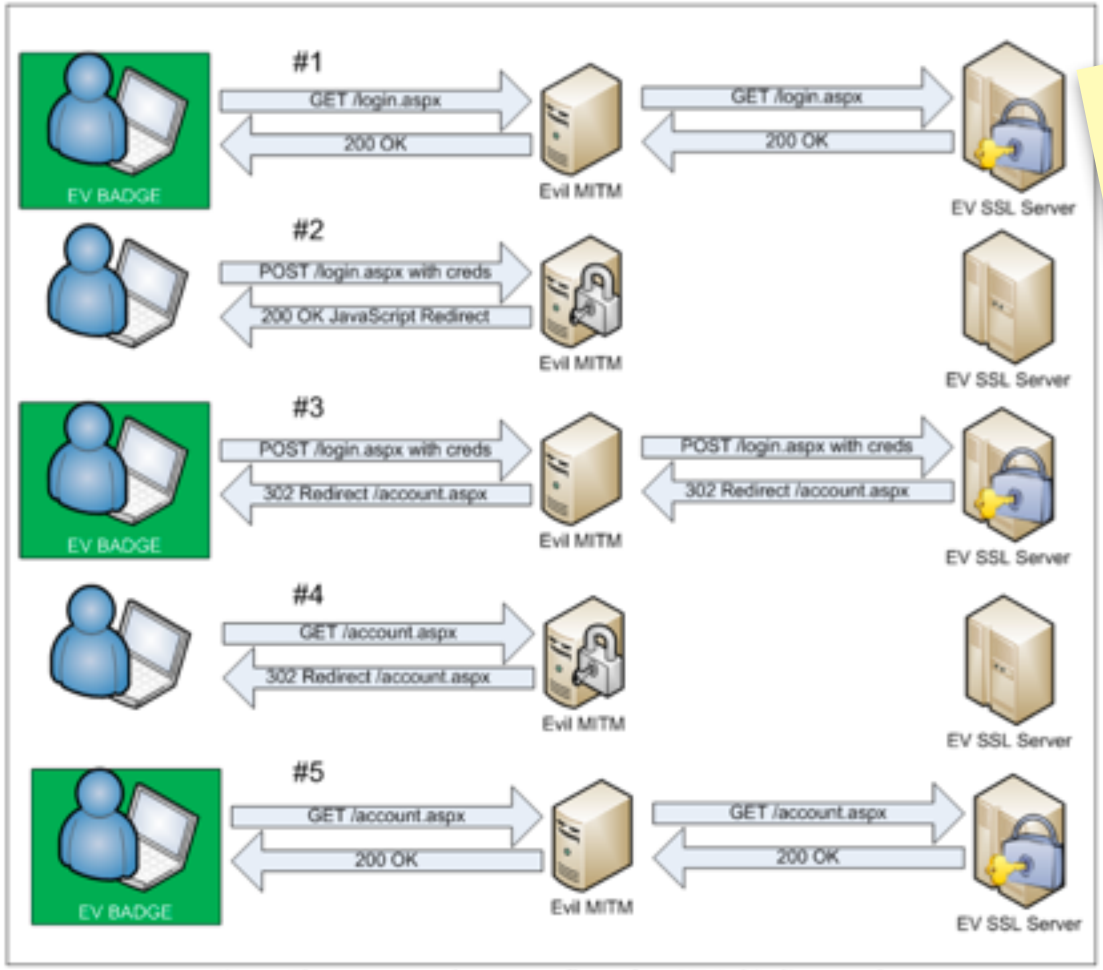


Figure: The request and response flow of an SSL Rebinding attack

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

Waar Gehakt Wordt
Vallen Spaanders

‘When you make an omelet you’l 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.
- No malice but an operational mistake after an audit that caused this.
- 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.

Most recent case

TURKTRUST

Operational mistake

No known exploits

No malice

https://groups.google.com/forum/#!msg/mozilla.dev.security.policy/aqn0Zm-KxQ0/x1hfTMGwE2AJ

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

picture from http://e-devotion.blogspot.nl/2012/03/light-at-end-of-tunnel.html

Light at the end of the tunnel?

No Magic Bullets and Global Perpective

Counter Measures

Blacklisting

Whitelisting

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

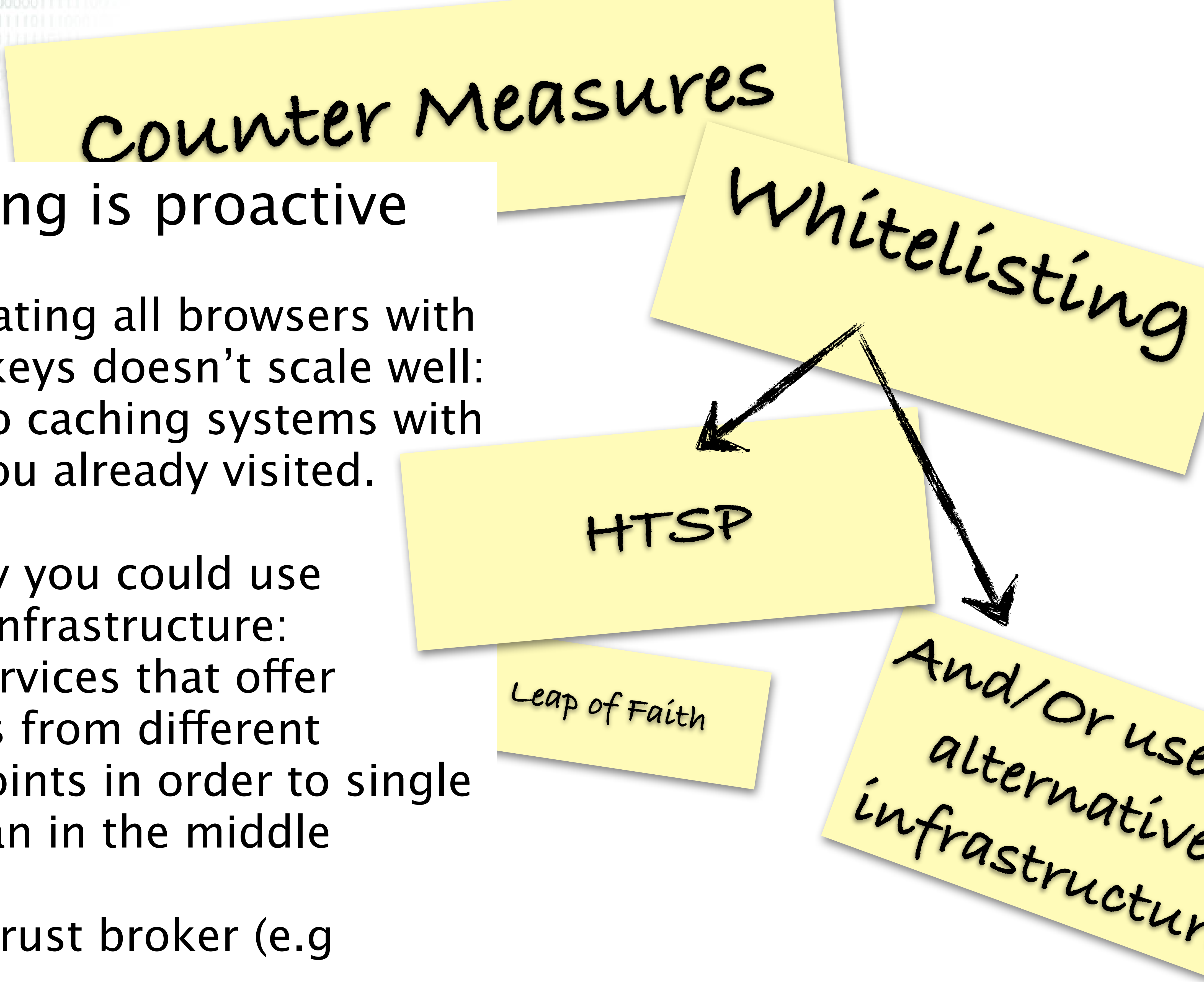
Economic Incentive is to not be transparent.

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



NLnet Labs

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

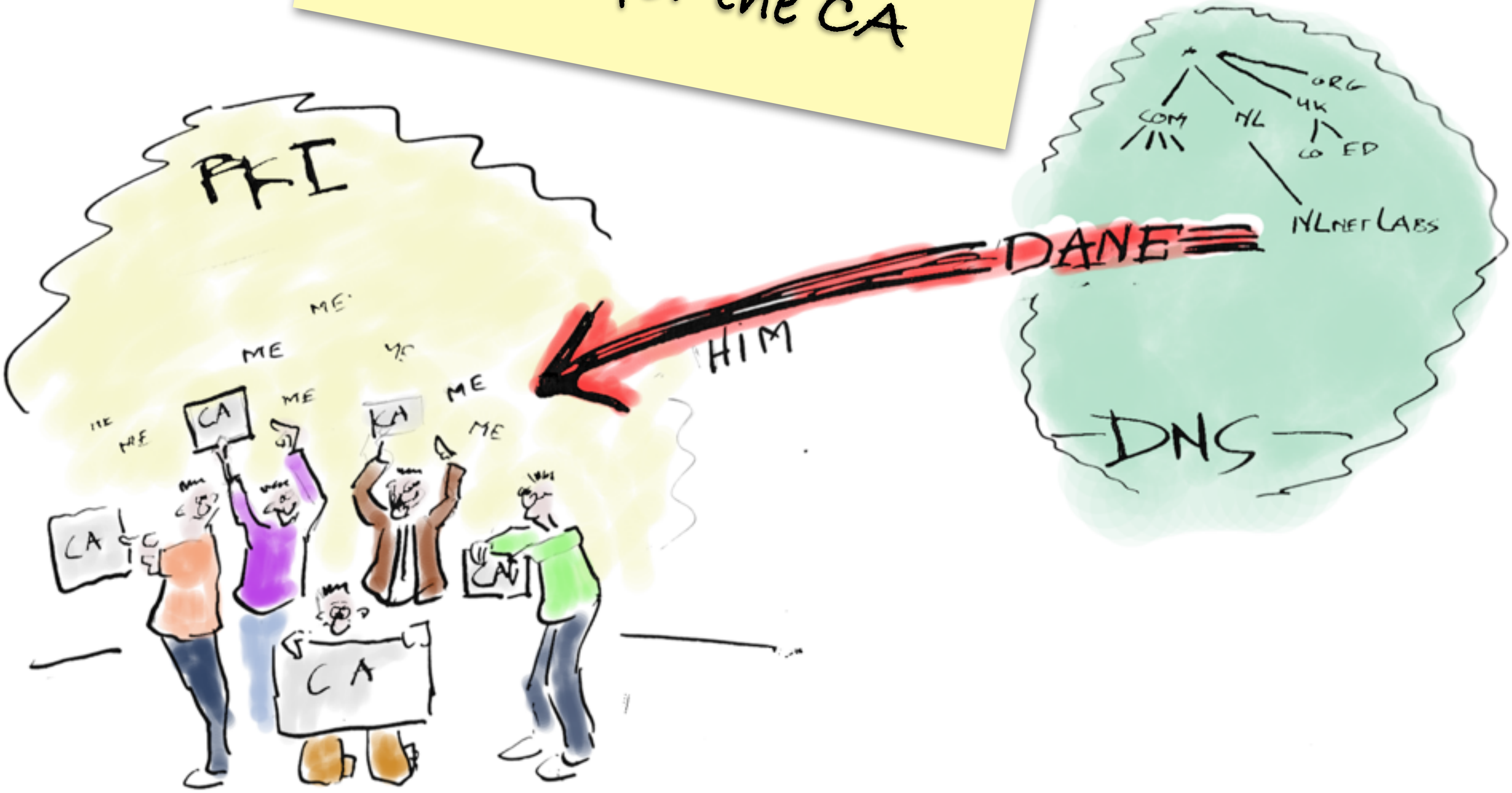
DANE

Using Secure DNS to Associate Certificates with Domain Names for TLS

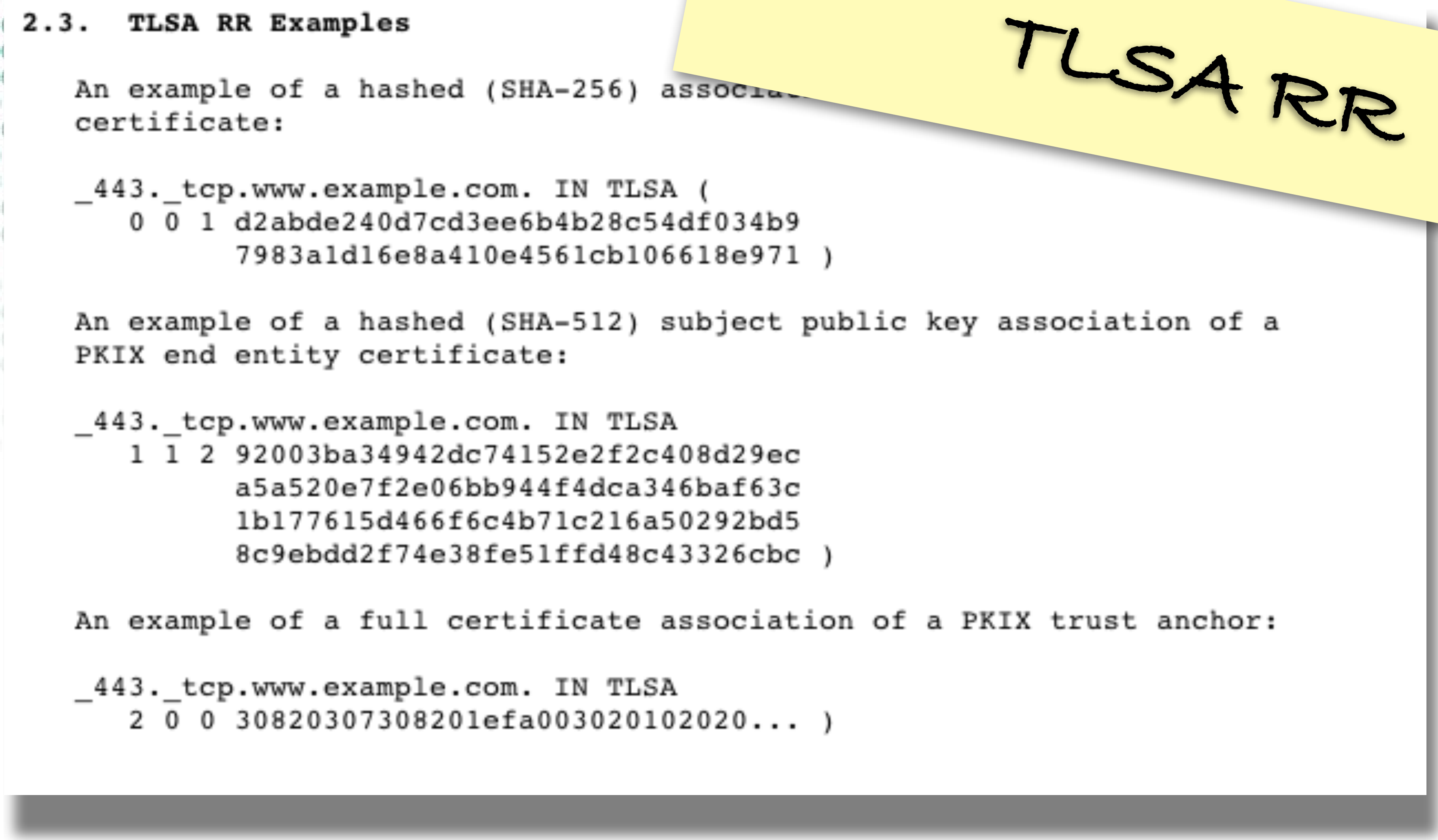
http://tools.ietf.org/wg/dane

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) associa
   certificate:

   _443._tcp.www.example.com. IN TLSA (
      0 0 1 d2abde240d7cd3ee6b4b28c54df034b9
            7983a1d16e8a410e4561cb106618e971 )

   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.

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

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

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

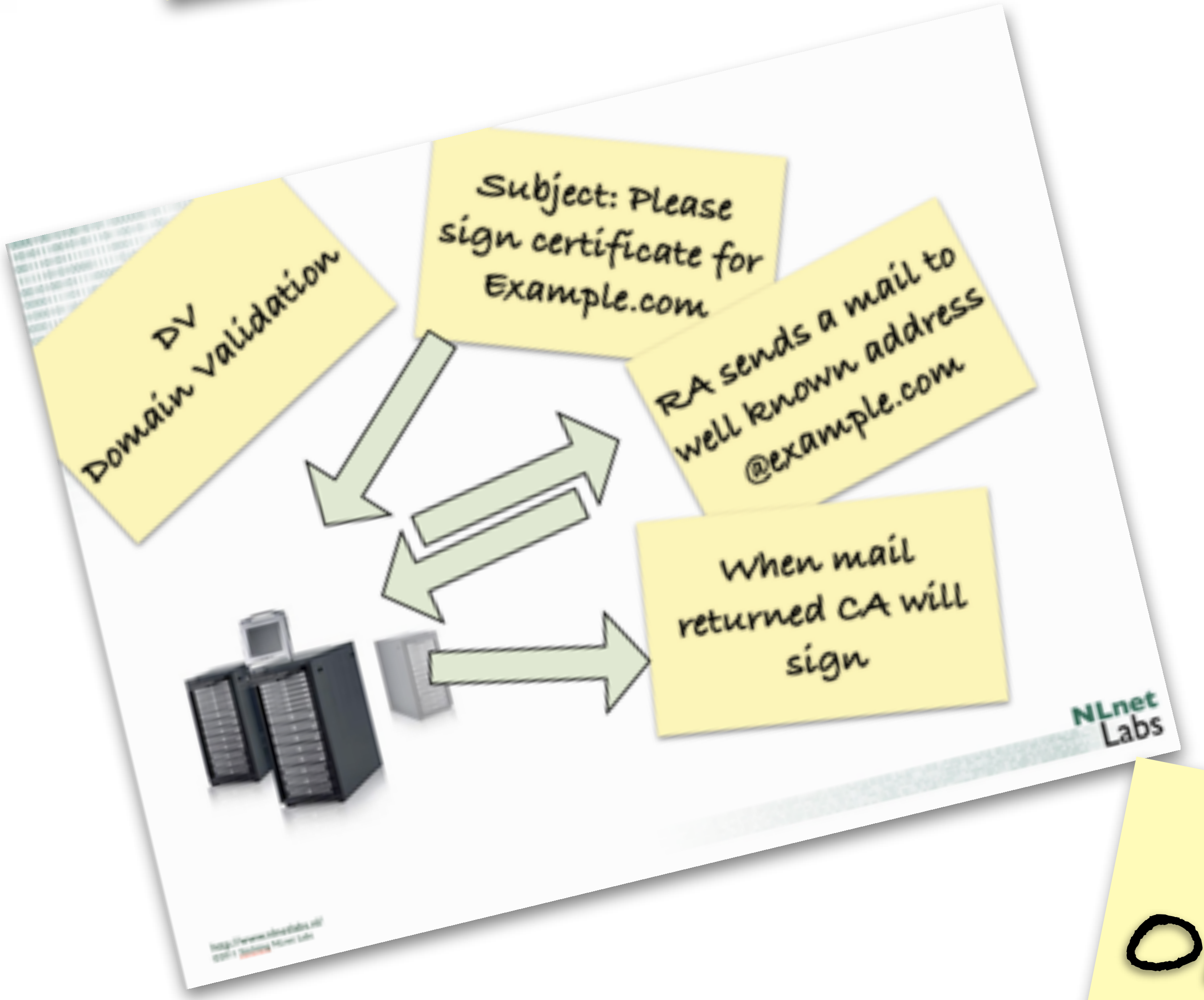
BEST OF BOTH WORLDS

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



DV
Domain Validation

Subject: Please sign certificate for Example.com

RA sends a mail to well known address @example.com

When mail returned CA will sign

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

- Dane critically depends on the authenticity and integrity of the DNS information.
- DNSSEC offers those properties
- (For the ‘protocol side’ of the DNS, the provisioning side is another aspect).

Even if we do not have DANE it is useful to deploy DNSSEC

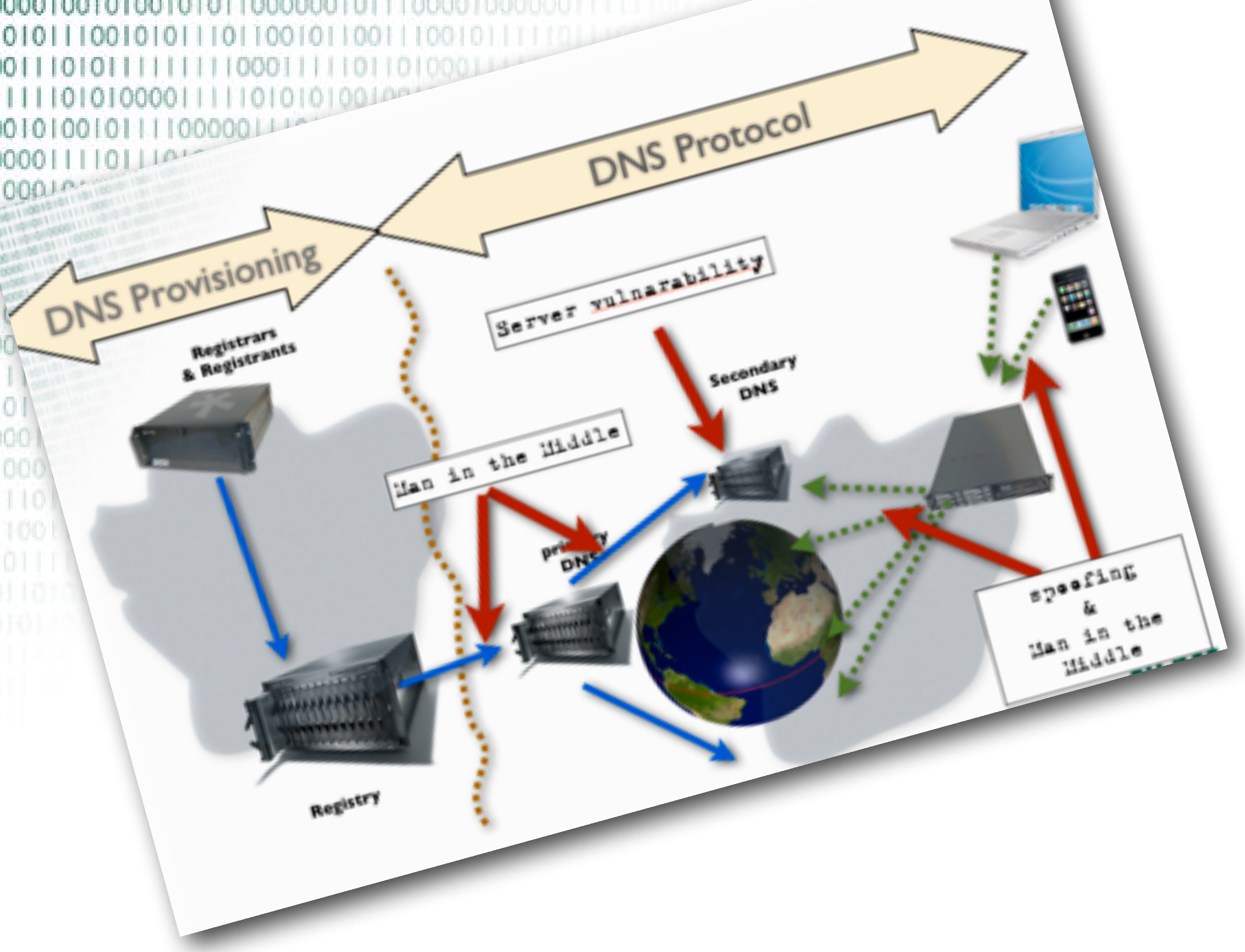
PREVENTS A CLASS OF MAN IN THE MIDDLE ATTACKS THAT MAKE CERTIFICATE EXPLOITS POSSBLE

And it offers a building for further security innovation

Hold it

you only talked DNSSEC technology

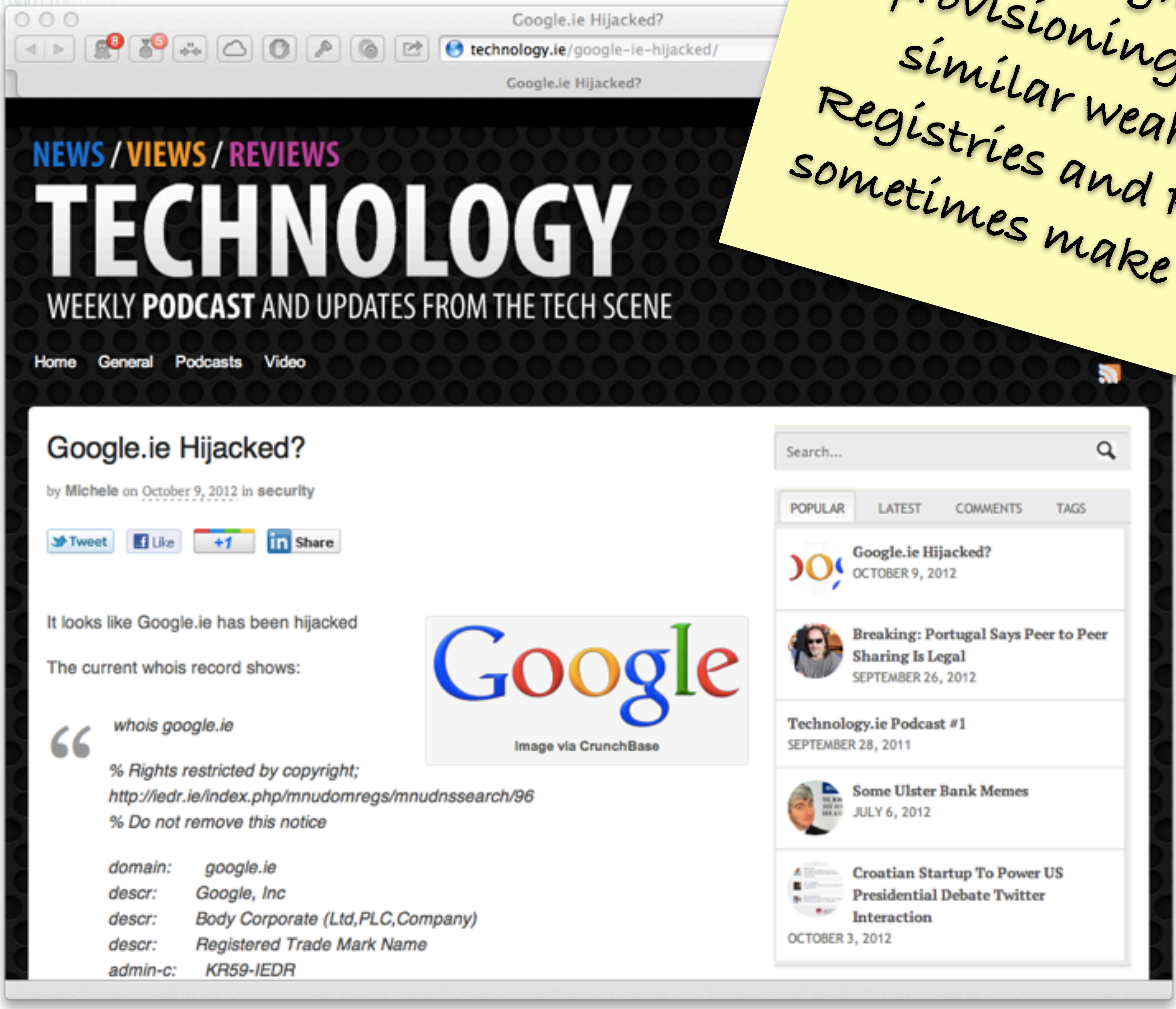
- We talked about DNSSEC as a solution to Certificate Authority compromises.
- But DNSSEC applies to technology to transport DNS data. The problems with PKI are in the policies and procedures, and have to do with user interface issues.
- Aren't there similar issues in DNS?



Yes:

- The DNSSEC only applies to the protocol
- The assumption is that registration at the left hand side is done correctly

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



Google.ie Hijacked?

by Michele on October 9, 2012 in security

It looks like Google.ie has been hijacked

The current whois record shows:

> 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

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

EV Certs Trust But Verify! DNSSEC/DANE

- 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 important.

Wrap-up

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

Not a magic bullet

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

Not the only approach

'convergence'

Not a magic bullet either

The Internet PKI has a trust issue.

A global trust issue

Scalability problems: compliance and technology

Local action global effect

Internet Trust is Global Trust

misaligned incentives

Global Trust:

- I trust different institutions than you.
- Local action can have global effects.
  - But Local Choice remains a fundamental principle (User choice in trust-anchors etc).
- Be aware of misaligned incentives during deployment: they increase the hurdles of getting solutions out there (e.g. DNSSEC).

How to increase global trust in the Internet?

Without a race to the bottom of minimal compliance?

With meaningful incremental steps in improving technology?

- Technology is only part of the answer
- Open Solutions, please!
- Small meaningful steps may be more effective in approaching a solution than when we try to work for paradigm shift

That's it folk

Questions, comments, ideas: olaf@nlnetlabs.nl