The Business Case for DNSSEC

ICANN Meeting
Singapore
18 March 2014
richard.lamb@icann.org

DNS Basics

- DNS converts names (www.dbs.com.sg) to numbers (23.41.187.241, 184.26.219.241)
- ..to identify services such as www and e-mail
- ..that identify and link customers to business and visa versa

+1-202-709-5262
VoIP

DNS is a part of all IT ecosystems

US-NSTIC effort

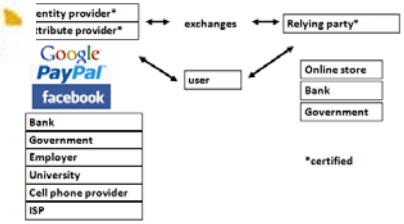
Google

OpenID

facebook

ebay

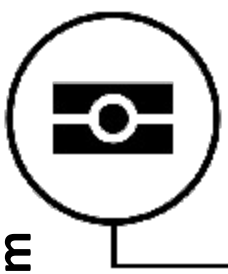
AADHAAR



PayPal

OECS ID effort

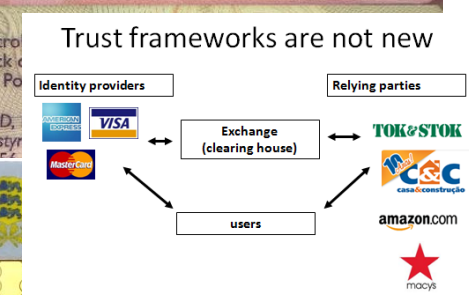
amazon Prime



ICP Brasil
O Brasil na era da certificação digital

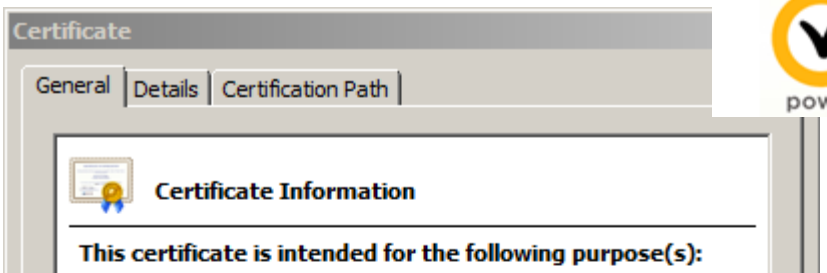
DigiNotar
A VASCO COMPANY

COMODO
Creating Trust Online



Smart Electrical Grid

Norton SECURED
powered by VeriSign



lamb@xtcn.com

mydomainname.com

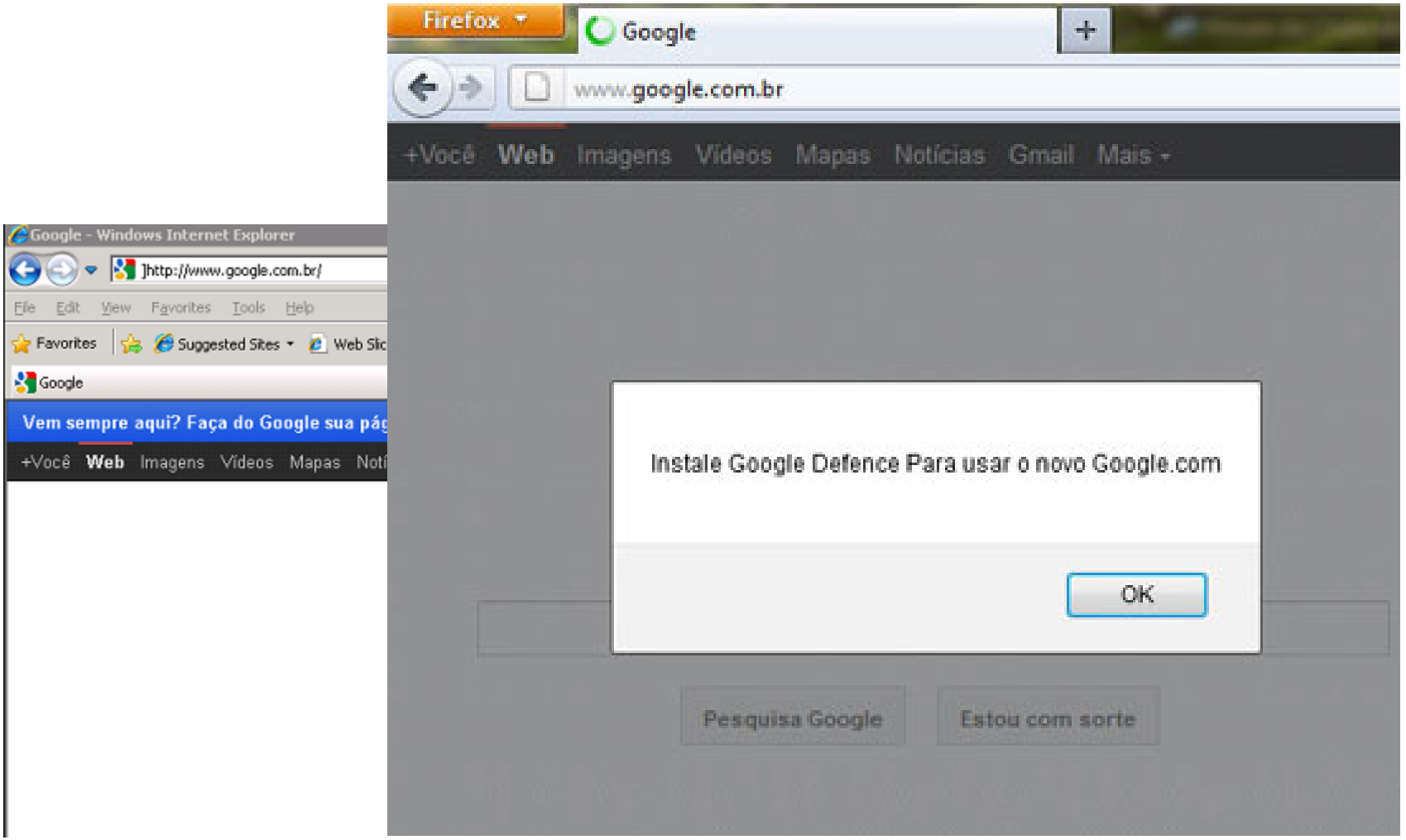
Where DNSSEC fits in

- ..but CPU and bandwidth advances make legacy DNS vulnerable to MITM attacks
- DNS Security Extensions (DNSSEC) introduces digital signatures into DNS to cryptographically protect contents
- With DNSSEC fully deployed a business can be sure a customer gets un-modified data (and visa versa)

The Bad: DNSChanger - 'Biggest Cybercriminal Takedown in History' – 4M machines, 100 countries, $14M

Nov 2011 http://krebsonsecurity.com/2011/11/malware-click-fraud-kingpins-arrested-in-estonia/
End-2-end DNSSEC validation would have avoided the problems

The Bad: Brazilian ISP fall victim to a series of DNS attacks



7 Nov 2011 http://www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil

End-2-end DNSSEC validation would have avoided the problems

The Bad: Other DNS hijacks*

- 25 Dec 2010 - Russian e-Payment Giant ChronoPay Hacked
- 18 Dec 2009 – Twitter – “Iranian cyber army”
- 13 Aug 2010 - Chinese gmail phishing attack
- 25 Dec 2010 Tunisia DNS Hijack
- 2009-2012 google.*
  - April 28 2009 Google Puerto Rico sites redirected in DNS attack
  - May 9 2009 Morocco temporarily seize Google domain name
- 9 Sep 2011 - Diginotar certificate compromise for Iranian users
- 7 Jan 2013 – Turktrust / EGO
- SSL / TLS doesn't tell you if you've been sent to the correct site, it only tells you if the DNS matches the name in the certificate. Unfortunately, majority of Web site certificates rely on DNS to validate identity.
- DNS is relied on for unexpected things though insecure.

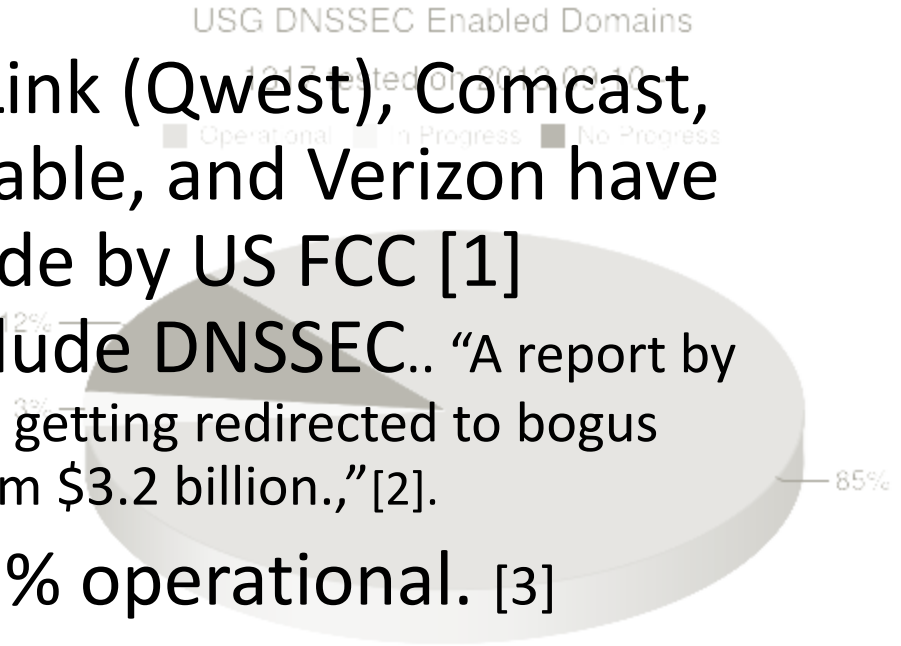
*A Brief History of DNS Hijacking - Google
http://costarica43.icann.org/meetings/sanjose2012/presentation-dns-hijackings-marquis-boire-12mar12-en.pdf

The Business Case for DNSSEC

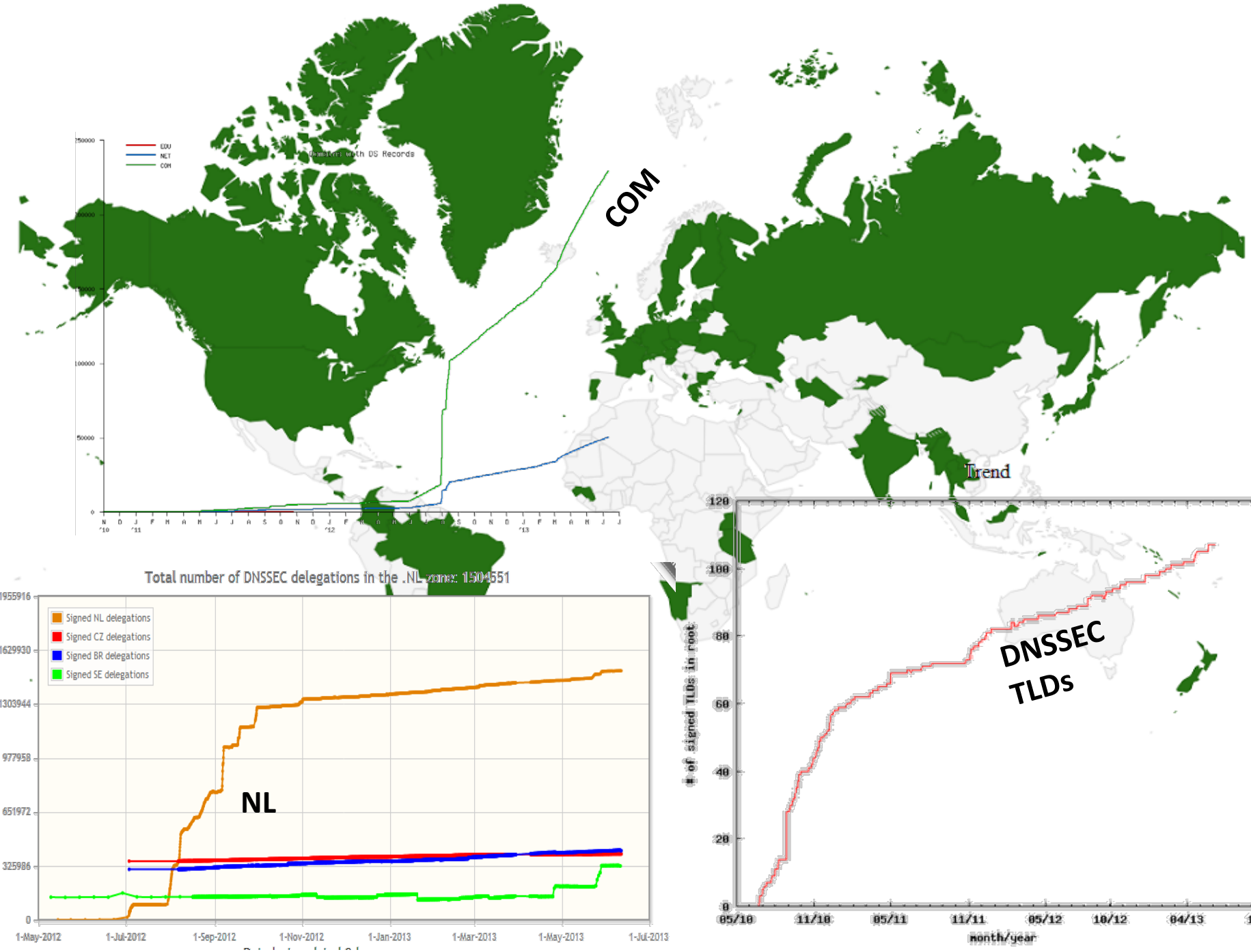
- Cyber security is becoming a greater concern to enterprises, government, and end users. DNSSEC is a key tool and differentiator.
- DNSSEC is the biggest security upgrade to Internet infrastructure in over 20 years. It is a platform for new security applications (for those that see the opportunity).
- DNSSEC infrastructure deployment has been brisk but requires expertise. Getting ahead of the curve is a competitive advantage.

DNSSEC interest from governments

- Sweden, Brazil, Netherlands, Czech Republic and others encourage DNSSEC deployment to varying degrees
- Mar 2012 - AT&T, CenturyLink (Qwest), Comcast, Cox, Sprint, TimeWarner Cable, and Verizon have pledged to comply and abide by US FCC [1] recommendations that include DNSSEC.. "A report by Gartner found 3.6 million Americans getting redirected to bogus websites in a single year, costing them $3.2 billion.,"[2].
- 2008 US .gov mandate. 85% operational. [3]



[1] FCC=Federal Communications Commission=US communications Ministry
[2] http://securitywatch.pcmag.com/security/295722-isps-agree-to-fcc-rules-on-anti-botnet-dnssec-internet-routing
[3] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-23.pdf
http://fedv6-deployment.antd.nist.gov/snap-all.html


COM
Trend
Total number of DNSSEC delegations in the .NL zone: 1504551
Signed NL delegations
Signed CZ delegations
Signed BR delegations
Signed SE delegations
NL
DNSSEC
TLDs
# of signed TLDs in root
month/year

DNSSEC - Where we are

- Deployed on 285/483 TLDs (13 Mar 2014 ~60% .com .uk .de .jp .cn .ru .pф .my ملیسیا .asia .tw 台灣, .kr 한국 .net, .post, +gtlds)
- Root signed** and audited
- > 86% of domain names could have DNSSEC
- Required in new gTLDs. Basic support by ICANN registrars
- Growing ISP support*
- 3rd party signing solutions***
- Growing S/W H/W support: NLNetLabs, ISC, Microsoft, PowerDNS, Secure64…? openssl, mozilla: early DANE support
- IETF standard on DNSSEC SSL certificates (RFC6698)
- Growing support from major players…(Apple iPhone/iPad, Google 8.8.8.8,…)

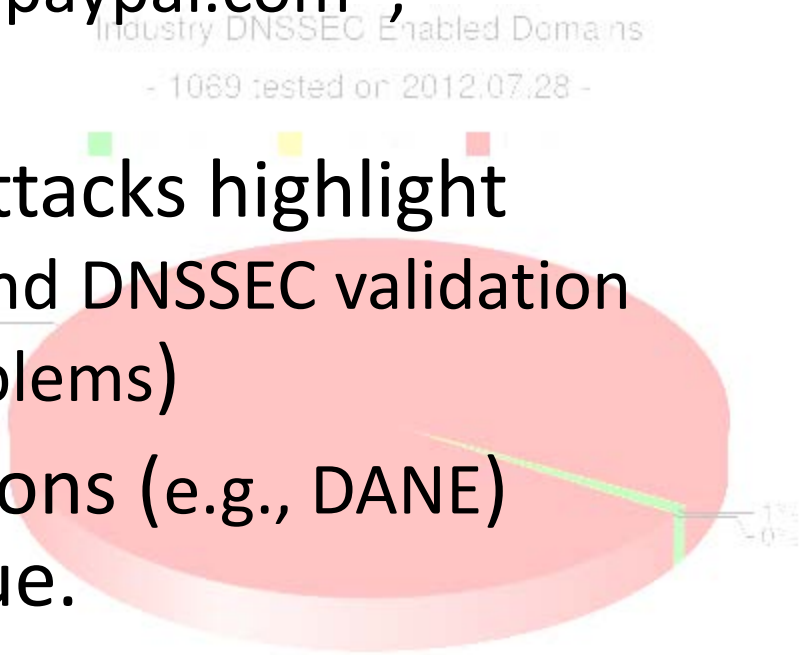
***COMCAST Internet (18M), TeliaSonera SE, Sprint,Vodafone CZ,Telefonica CZ, T-mobile NL, SurfNet NL, SANYO Information Technology Solutions JP, others..**

****Int'l bottom-up trust model /w 21 TCRs from: TT, BF, RU, CN, US, SE, NL, UG, BR, Benin, PT, NP, Mauritius, CZ, CA, JP, UK, NZ…**

***** Partial list of registrars: https://www.icann.org/en/news/in-focus/dnssec/deployment**

But…

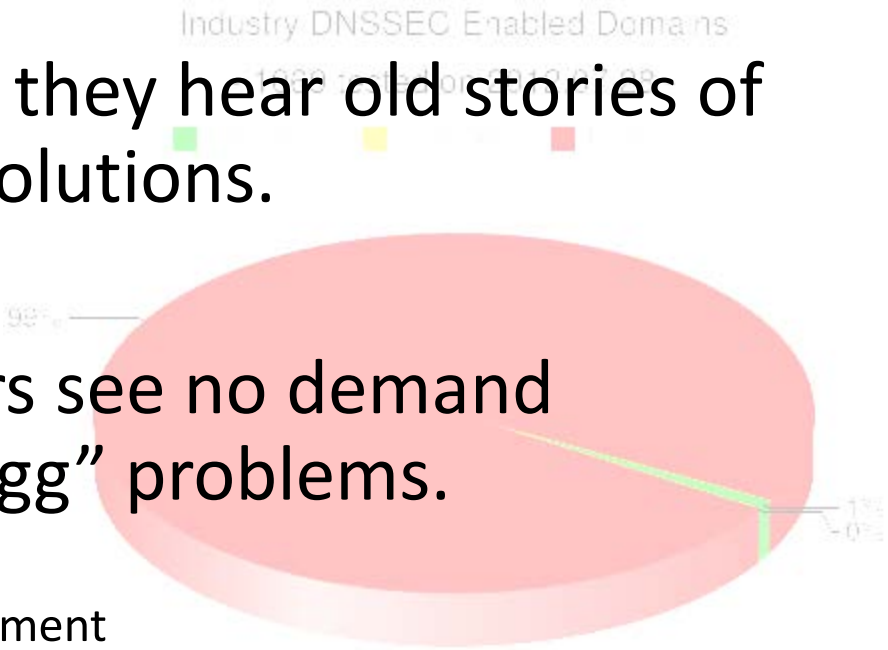
- But deployed on ~1% (~2M) of 2nd level domains. Many have plans. Few have taken the step (e.g., yandex.com, paypal.com*, comcast.com).
- DNSChanger and other attacks highlight today's need. (e.g end-2-end DNSSEC validation would have avoided the problems)
- Innovative security solutions (e.g., DANE) highlight tomorrow's value.



*** http://fedv6-deployment.antd.nist.gov/cgi-bin/generate-com**
http://www.thesecuritypractice.com/the_security_practice/2011/12/all-paypal-domains-are-now-using-dnssec.html
http://www.nacion.com/2012-03-15/Tecnologia/Sitios-web-de-bancos-ticos-podran-ser-mas-seguros.aspx

DNSSEC: So what's the problem?

- Not enough IT departments know about it or are too busy putting out other fires.
- When they do look into it they hear old stories of FUD and lack of turnkey solutions.
- Registrars*/DNS providers see no demand leading to "chicken-and-egg" problems.



*but required by new ICANN registrar agreement

What you can do

- ***For Companies:***
  - Sign your corporate domain names
  - Just turn on validation on corporate DNS resolvers
- ***For Users:***
  - Ask ISP to turn on validation on their DNS resolvers
- ***For All:***
  - Take advantage of ICANN, ISOC and other organizations offering DNSSEC education and training

I smell opportunity !

Game changing Internet Core Infrastructure Upgrade

- “More has happened here today than meets the eye. An infrastructure has been created for a hierarchical security system, which can be purposed and re-purposed in a number of different ways. ..” – Vint Cerf (June 2010)

The Bad: SSL Dilution of Trust
The Good: DNSSEC = Global "free" PKI

CA Certificate roots ~1482

DNSSEC root - 1

Content security
Commercial SSL
Certificates for
Web and e-mail

Content security
"Free SSL"
certificates for Web
and e-mail and "trust
agility"

Cross-
organizational and
trans-national
identity and
authentication

DANE and other yet to be
discovered security
innovations, enhancements,
and synergies

Network security
IPSECKEY RFC4025

Securing VoIP

Domain Names

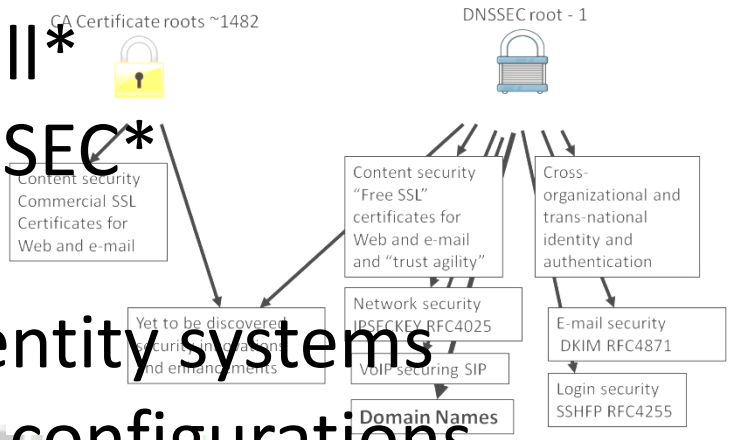
E-mail security
DKIM RFC4871

Login security
SSHFP RFC4255

https://www.eff.org/observatory
http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/

Opportunity: New Security Products

- Improved Web SSL and certificates for all*
- Secured e-mail (S/MIME) for all*
- Validated remote login SSH, IPSEC*
- Securing VoIP
- Cross organizational digital identity systems
- Secured content delivery (e.g. configurations, updates, keys)
- Securing Smart Grid efforts
- A global PKI
- Increasing trust in e-commerce



A good ref http://www.internetsociety.org/deploy360/dnssec/

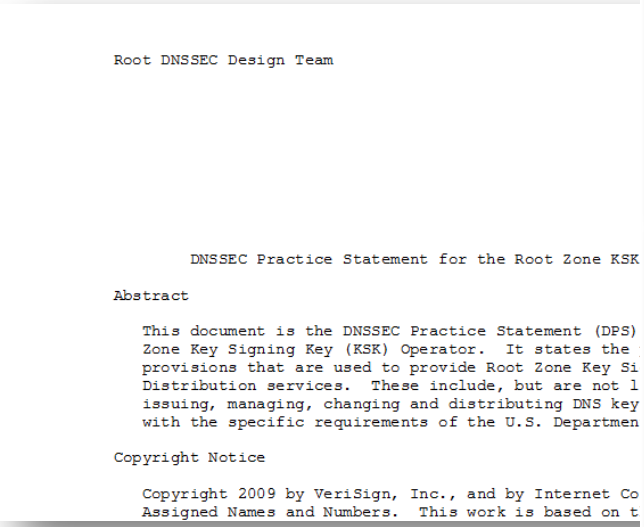
***IETF standards complete or currently being developed**

DNSSEC: Internet infrastructure upgrade to help address today’s needs and create tomorrow’s opportunity.

Hmm…how do I trust it?

ICANN DNSSEC Deployment @Root

- **Multi-stakeholder, bottom-up trust model* /w 21 crypto officers from around the world**
- **Broadcast Key Ceremonies and public docs**
- **SysTrust audited**
- **FIPS 140-2 level 4 HSMs**



Root DNSSEC Design Team

DNSSEC Practice Statement for the Root Zone KSK

Abstract

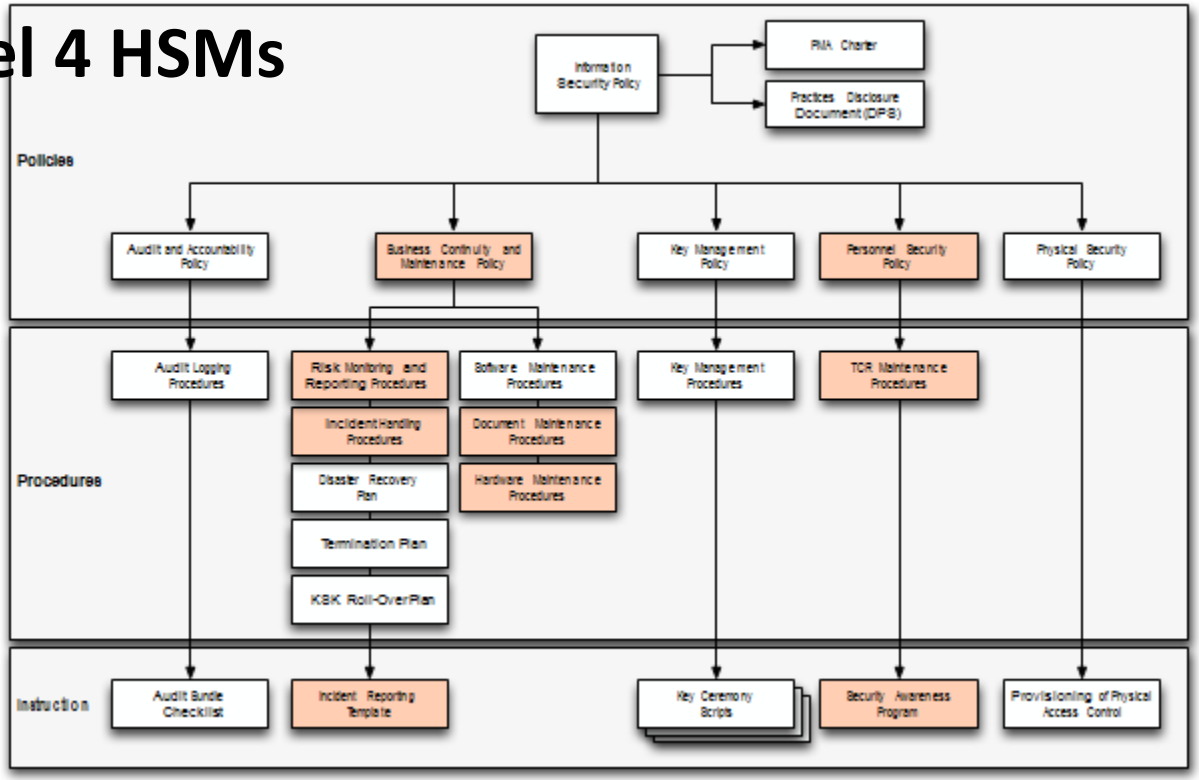
This document is the DNSSEC Practice Statement (DPS) Zone Key Signing Key (KSK) Operator. It states the provisions that are used to provide Root Zone Key Si Distribution services. These include, but are not l issuing, managing, changing and distributing DNS key with the specific requirements of the U.S. Departmen

Copyright Notice

Copyright 2009 by VeriSign, Inc., and by Internet Co Assigned Names and Numbers. This work is based on t

Root DPS

DNSSEC Practice Statement



ICANN DNSSEC Deployment @Root (and elsewhere)

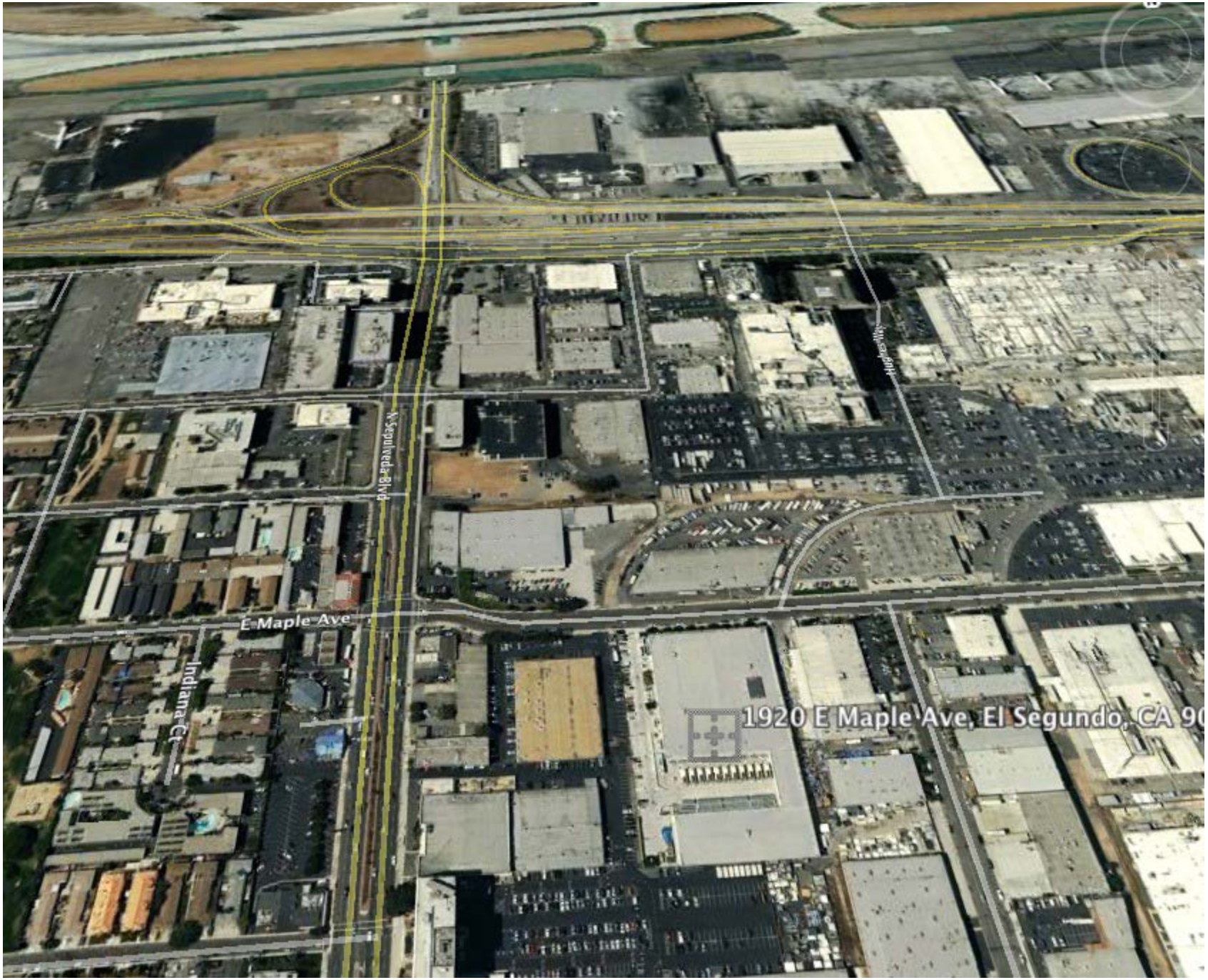
FIPS 140-2 level 4

SysTrust

DCID 6/9

http://www.flickr.com/photos/kjd/sets/72157624302045698/

Photos: Kim Davies


E Maple Ave
N Sepulveda Blvd
Indiana Ct
1920 E Maple Ave, El Segundo, CA 90

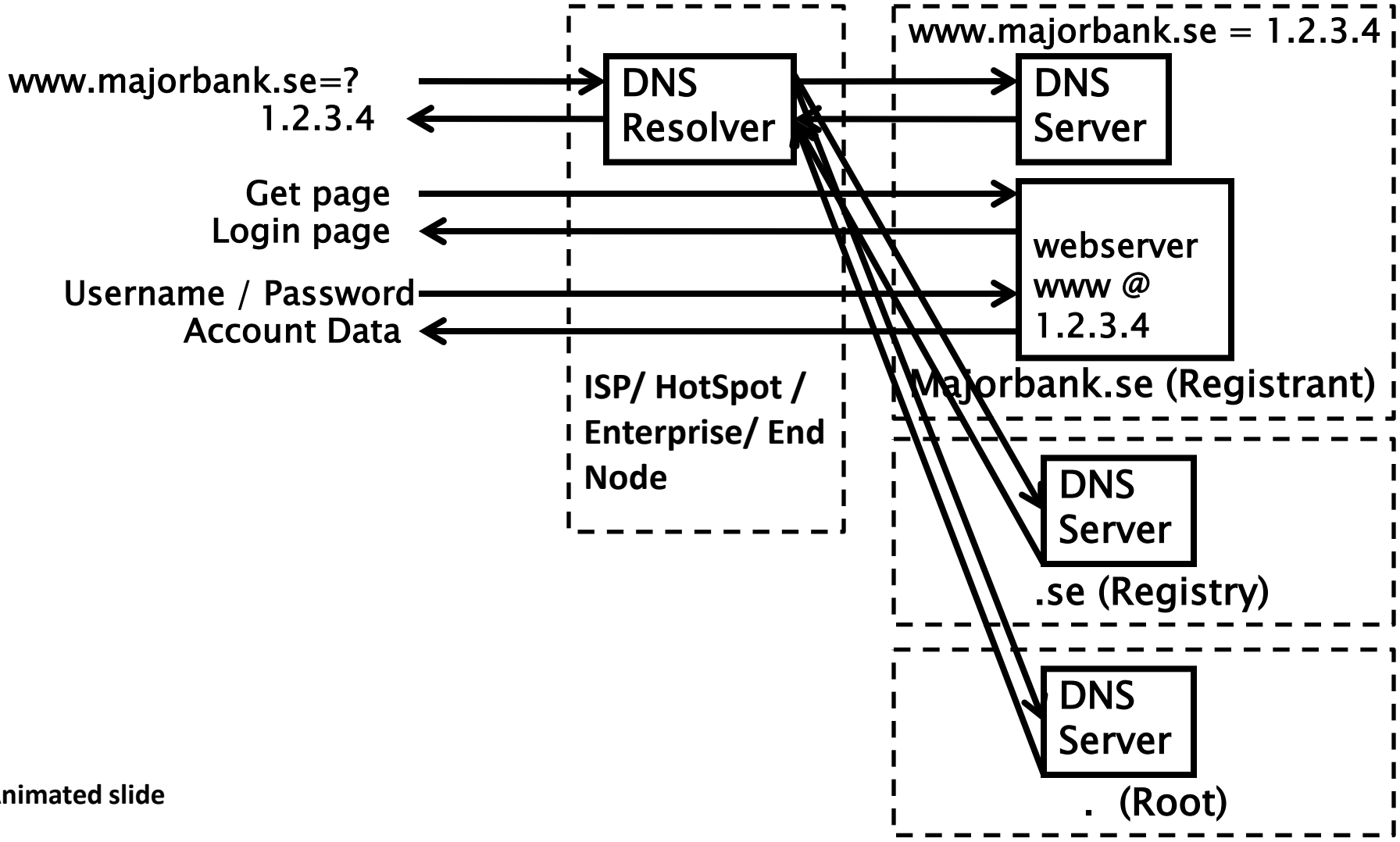
January 27, 2010

ICA

Photos: Kim Davies

DNSSEC: Internet infrastructure upgrade to help address today’s needs and create tomorrow’s opportunity.

The Internet's Phone Book - Domain Name System (DNS+DNSSEC)



Animated slide