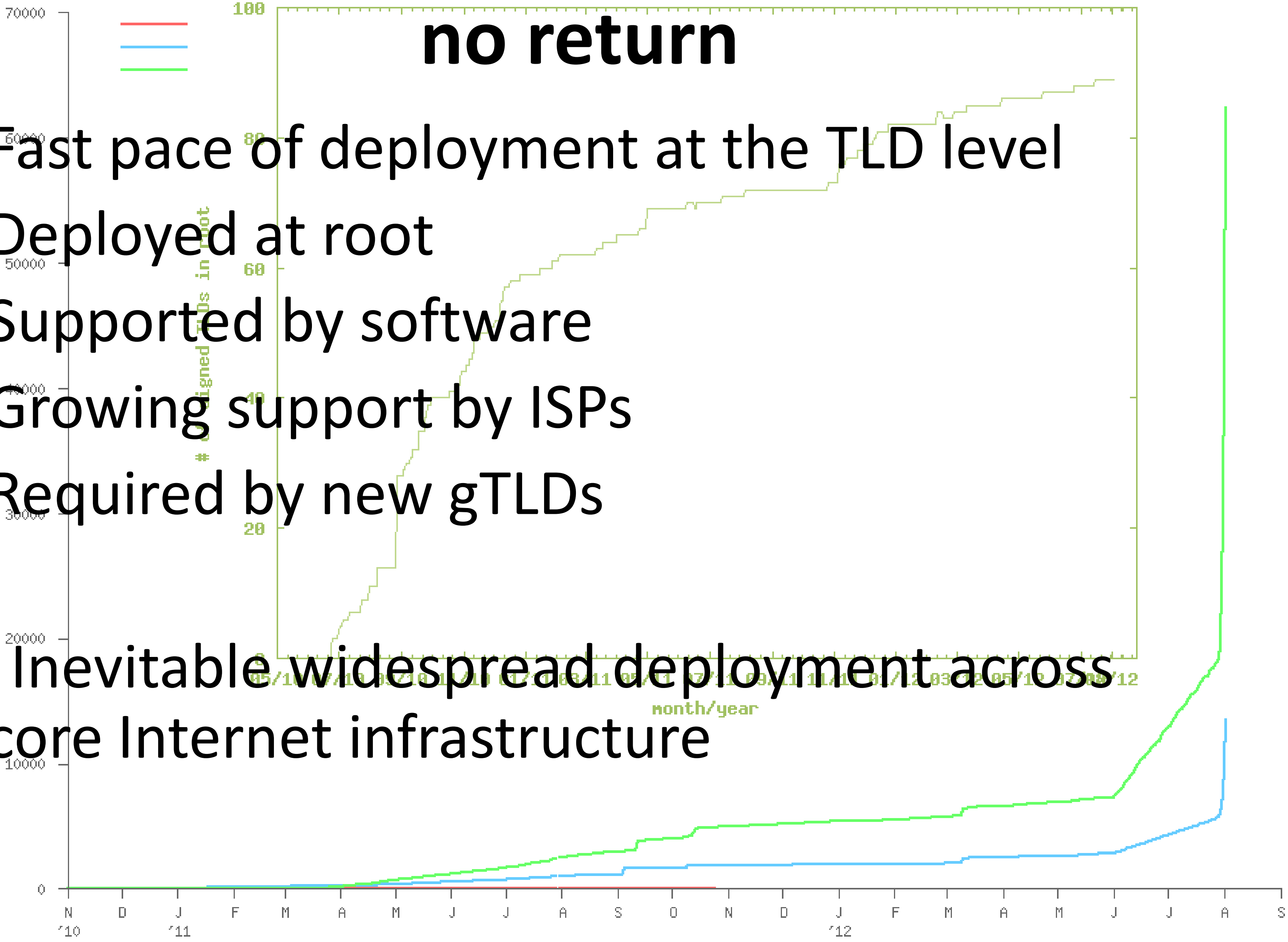
DNSSEC: Where We Are (and how we get to where we want to be)

APNIC 34, Phnom Penh, Cambodia

August 2012

richard.lamb@icann.org

DNSSEC: We have passed the point of no return

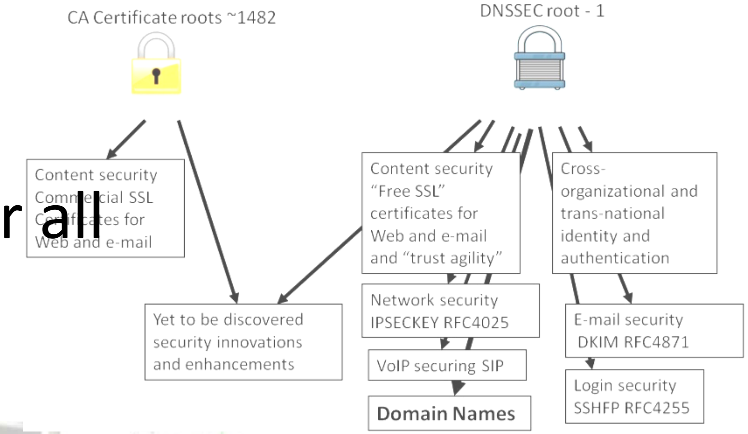


- Fast pace of deployment at the TLD level
- Deployed at root
- Supported by software
- Growing support by ISPs
- Required by new gTLDs

→ Inevitable widespread deployment across core Internet infrastructure

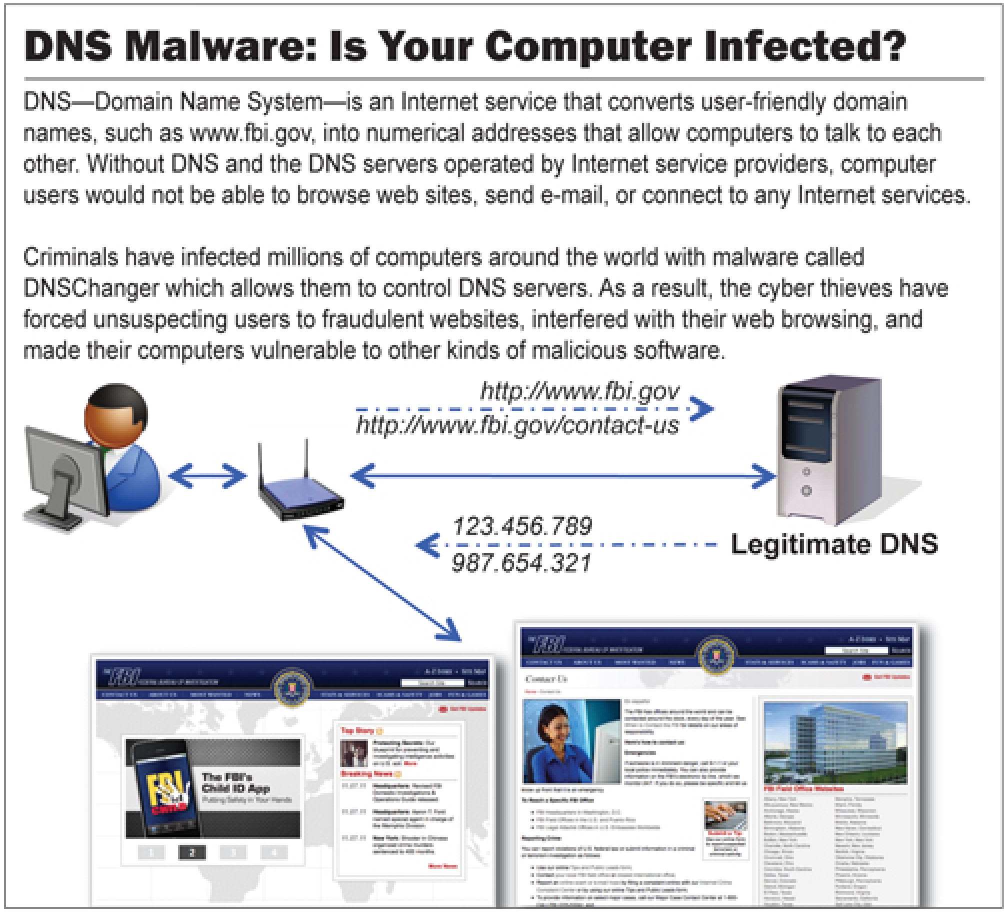
DNSSEC: Plenty of Motivation

- DNSChanger (Nov 2011), calls for deployment by government, etc…
- DANE
  - Improved Web TLS and certs for all
  - Email S/MIME for all
- …and
  - SSH, IPSEC, VoIP
  - Digital identity
  - Other content (e.g. configurations, XML, app updates)
  - Smart Grid
  - A global 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
Yet to be discovered security innovations and enhancements
Network security IPSECKEY RFC4025
VoIP securing SIP
Domain Names
E-mail security DKIM RFC4871
Login security SSHFP RFC4255

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

The BAD: DNSChanger - ‘Biggest Cybercriminal Takedown in History’ – 4M machines, 100 countries, $14M



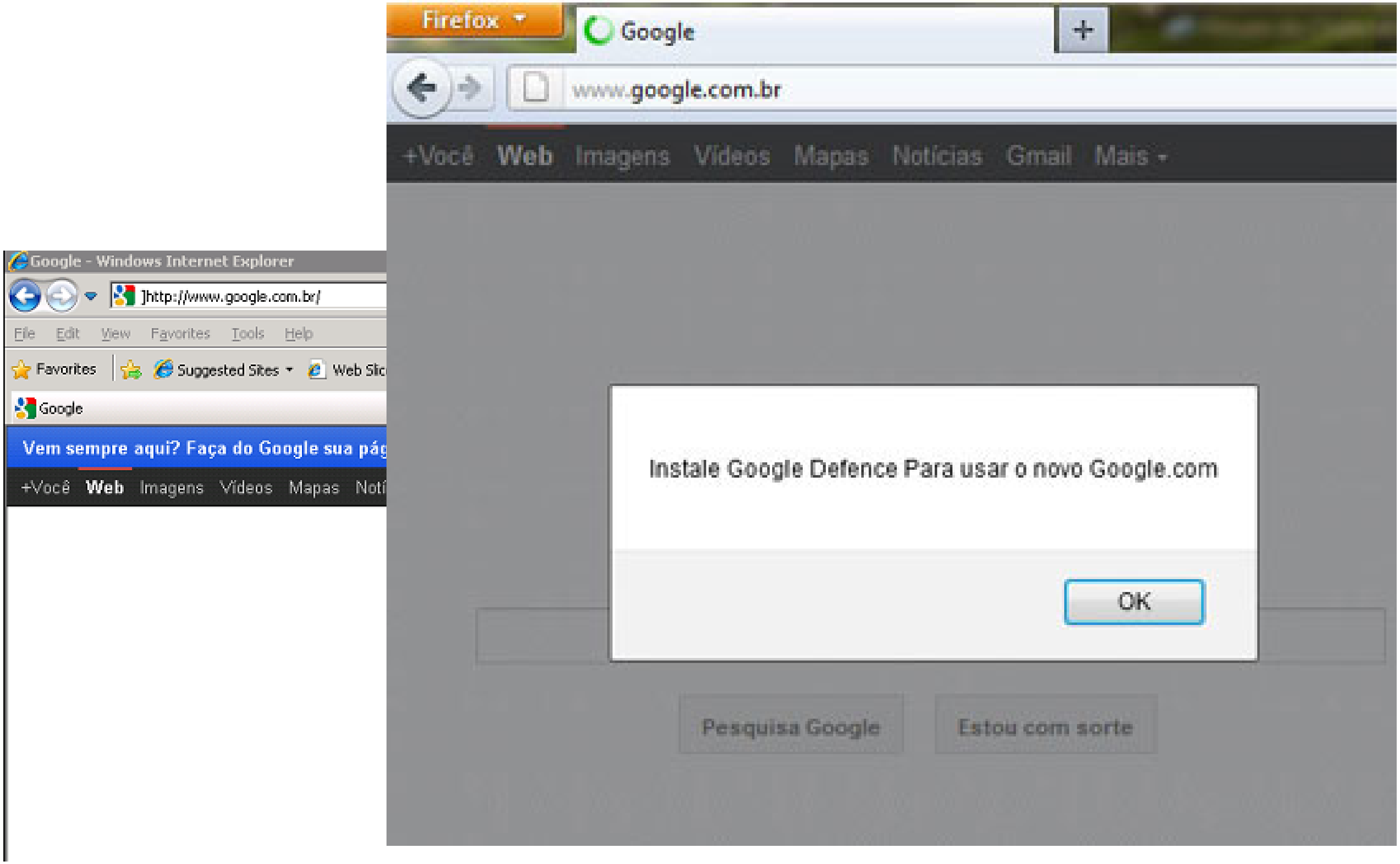
DNS Malware: Is Your Computer Infected?

DNS—Domain Name System—is an Internet service that converts user-friendly domain names, such as www.fbi.gov, into numerical addresses that allow computers to talk to each other. Without DNS and the DNS servers operated by Internet service providers, computer users would not be able to browse web sites, send e-mail, or connect to any Internet services.

Criminals have infected millions of computers around the world with malware called DNSChanger which allows them to control DNS servers. As a result, the cyber thieves have forced unsuspecting users to fraudulent websites, interfered with their web browsing, and made their computers vulnerable to other kinds of malicious software.

Nov 2011 http://krebsonsecurity.com/2011/11/malware-click-fraud-kingpins-arrested-in-estonia/

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


Firefox
Google
www.google.com.br
+Você Web Imagens Vídeos Mapas Notícias Gmail Mais
OK
Pesquisa Google
Estou com sorte
Google - Windows Internet Explorer
]http://www.google.com.br/
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Web Slic
Google
Vem sempre aqui? Faça do Google sua pág
+Você Web Imagens Vídeos Mapas Notí

Instale Google Defence Para usar o novo Google.com

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

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
- 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

DNSSEC support from government

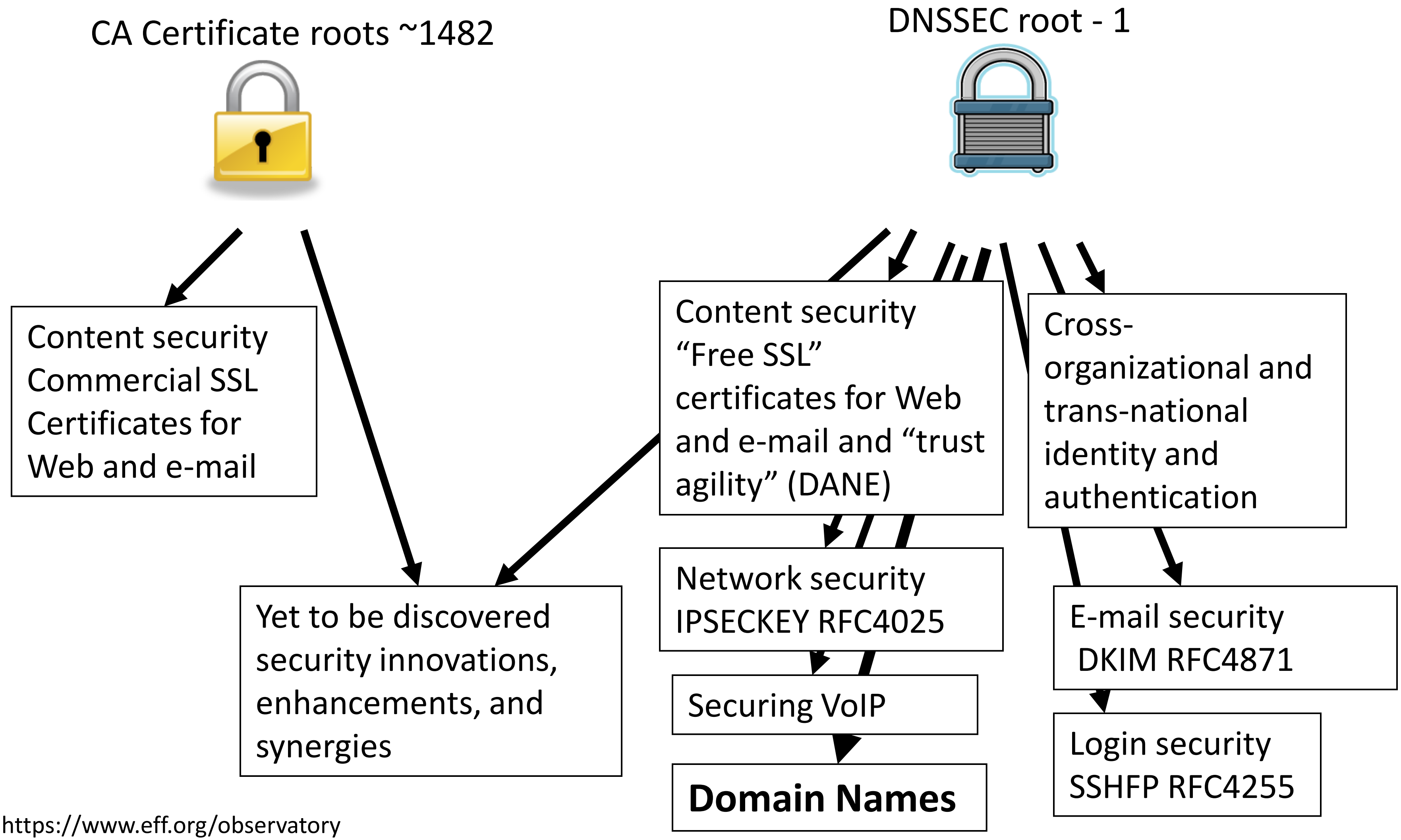
- Sweden, Brazil, and others encourage DNSSEC deployment
- Mar 2012 - AT&T, CenturyLink (Qwest), Comcast, Cox, Sprint, TimeWarner Cable, and Verizon have pledged to comply and abide by US FCC [1] recommendations that include DNSSEC.. "A report by Gartner found 3.6 million Americans getting redirected to bogus websites in a single year, costing them $3.2 billion.,"[2].
- 2008 US .gov mandate. >60% 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

Global PKI



CA Certificate roots ~1482

DNSSEC root - 1

Content security
Commercial SSL
Certificates for
Web and e-mail

Yet to be discovered
security innovations,
enhancements, and
synergies

Content security
“Free SSL”
certificates for Web
and e-mail and “trust
agility” (DANE)

Cross-
organizational and
trans-national
identity and
authentication

Network security
IPSECKEY RFC4025

Securing VoIP

Domain Names

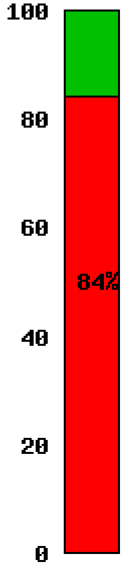
E-mail security
DKIM RFC4871

Login security
SSHFP RFC4255

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

DNSSEC: Where we are

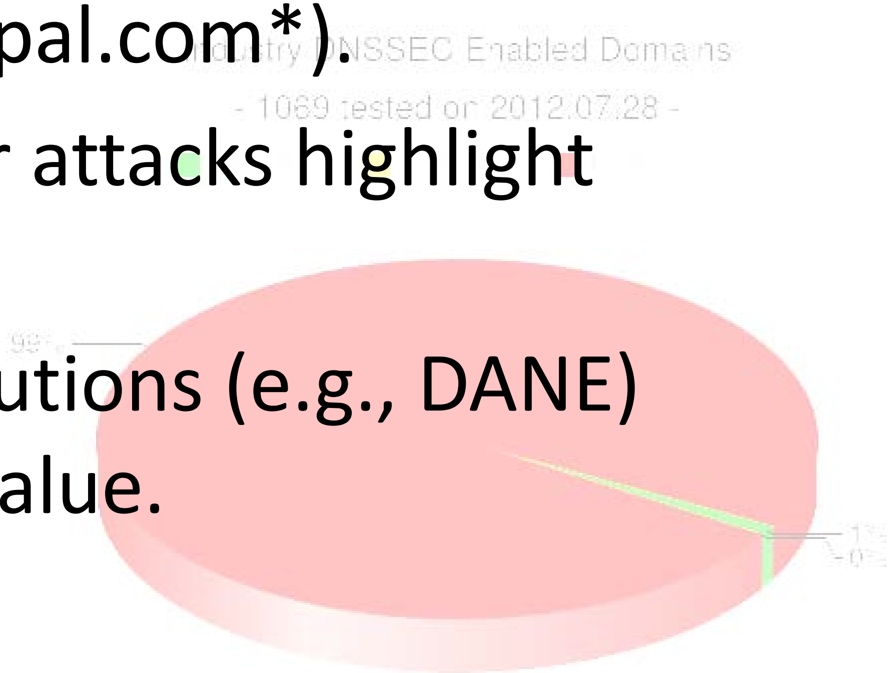
- Deployed on 89/313 TLDs (.asia, .tw 台灣 台湾, .kr 한국, .jp, .in, .lk, .kg, .tm, .am, .mm, .ua, .cr, .cz, .br, .se, .uk, .fr, .com,…)
- Root signed and audited by PwC SysTrust
- >84% of domain names could have DNSSEC
- Growing ISP support*
- 3rd party signing solutions are appearing (e.g., GoDaddy, VeriSign, Binero,…)
- Unbound, BIND, DNSSEC-trigger, vsResolver and other s/w support and secure last-mile
- IETF DANE Certificate support RFC almost out



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

But…

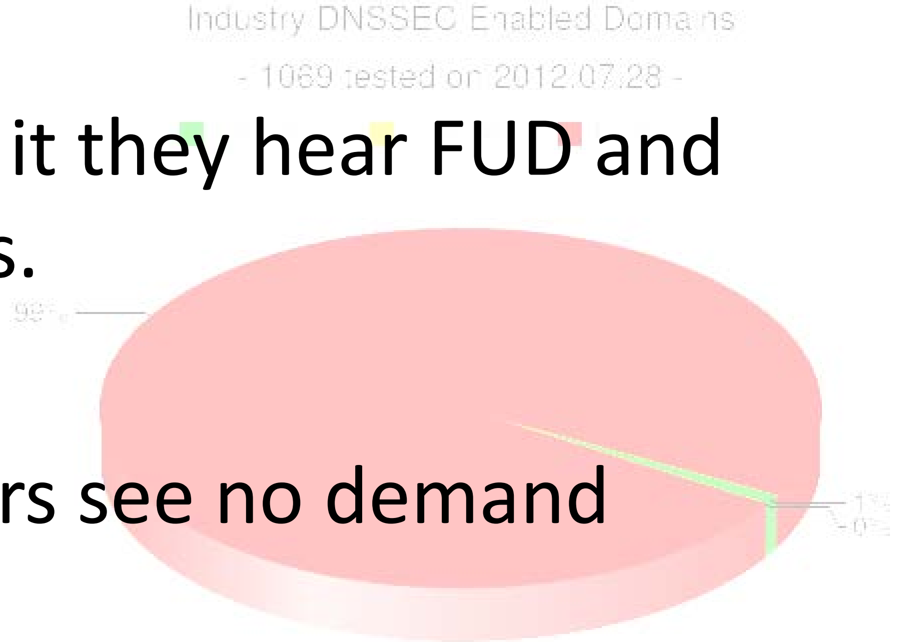
- But deployed on < 1% of 2nd level domains. Many have plans. Few have taken the step (e.g., yandex.com, paypal.com*).
- DNSChanger and other attacks highlight today's need.
- Innovative security solutions (e.g., DANE) highlight tomorrow's value.



* 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 enterprise IT departments know about it or are putting out other fires.
- When they do look into it they hear FUD and lack of turnkey solutions.
- Registrars/DNS providers see no demand



Barriers to success

- Lack of Awareness at enterprise and customer level (e.g., security implications)
- Lack of Registrar support*
  - Chicken and egg
  - Lack of expertise and/or simple solutions
  - Justifying cost
- Implementation F.U.D. by solution provider
  - Security/crypto/key management/complexity
  - Effect on existing enterprise operations: e.g. expiry, LB, CDN, etc..
- Un-trustworthy deployment
  - Yet another security thing to manage: “email the keys to everyone”
  - Insecure practices and processes
  - Garbage in, garbage out - what does signing my zone buy me?

***Partial list of Registrars supporting DNSSEC**
http://www.icann.org/en/news/in-focus/dnssec/deployment

Solutions

- Raise awareness of domain holders, end users, h/w+s/w vendors [1]
  - Point to improved security as differentiator and the disadvantage of not adopting
  - New opportunities for O/S (mobile and desktop) and browser vendors
  - Added security for hardware products (e.g., validator in CPE)
  - Meet with Registrars and DNS providers
- Ease Implementation:
  - Take advantage of DNSSEC training[2] and learn from existing implementations
  - Automate key management and monitoring
  - Crypto: HSM? Smartcard? TPM chip? Soft keys? - all good
  - Seek “click and sign” interface simplicity
  - Start implementation early since to get ahead in learning curve
  - For ISPs, at minimum ensure validation can occur downstream to support end2end security
- Make it trustworthy:
  - Transparent and secure processes and practices
  - Writing a DPS creates the right mindset for:
    - Separation of duties
    - Documented procedures
    - Audit logging
  - Opportunity to improve overall operations using DNSSEC as an excuse [3]

[1] DNSSEC.jp and other groups are excellent examples

[2] APNIC, NSRC, ISOC, ICANN offer training

[3] ENISA report on DNSSEC deployment

Trustworthy Implementation

Learn from CA successes (and mistakes)

- The good:
  - The people
  - The mindset
  - The practices
  - The legal framework
  - The audit against international accounting and technical standards
- The bad:
  - Diluted trust with a race to the bottom (>1400 CA’s)
  - DigiNotar
    - Weak and inconsistent polices and controls
    - Lack of compromise notification (non-transparent)
    - Audits don’t solve everything (ETSI audit)

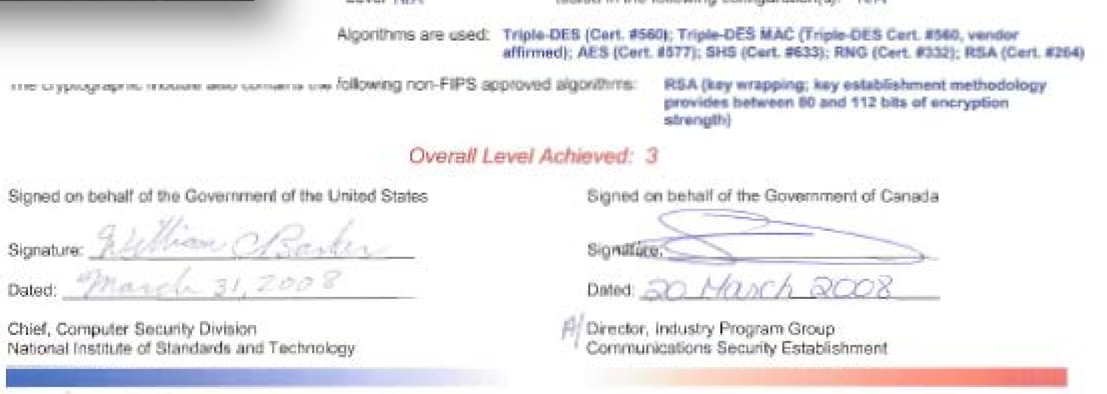
An implementation can be thi$

SysTrust

…or this

TPM

+



FIPS 140-2 Vali

FIPS VALIDATED 140-2 TM

The Communications Security Establishment of the Government of Canada

ive levels of security: Level 1, L
d environments in which cryptog
ign and implementation of a cry
ict identified as:

Athena IDProtect by Athen
AT90SC25672RCT Revision D; I

ting accredited laboratory:

Level 3	C		
Level 3	F		
Level 4	*Cryptographic Key Management:*	Level 3
Level 3	*Self-Tests:*	Level 3
Level 3	*Mitigation of Other Attacks:*	Level 3
Level N/A	*tested in the following configuration(s):*	N/A

Algorithms are used: **Triple-DES (Cert. #560); Triple-DES MAC (Triple-DES Cert. #560, vendor affirmed); AES (Cert. #577); SHS (Cert. #633); RNG (Cert. #332); RSA (Cert. #264)**

The cryptographic module also contains the following non-FIPS approved algorithms: **RSA (key wrapping; key establishment methodology provides between 80 and 112 bits of encryption strength)**

Overall Level Achieved: 3

Signed on behalf of the Government of the United States

Signature: William C. Barker

Dated: March 31, 2008

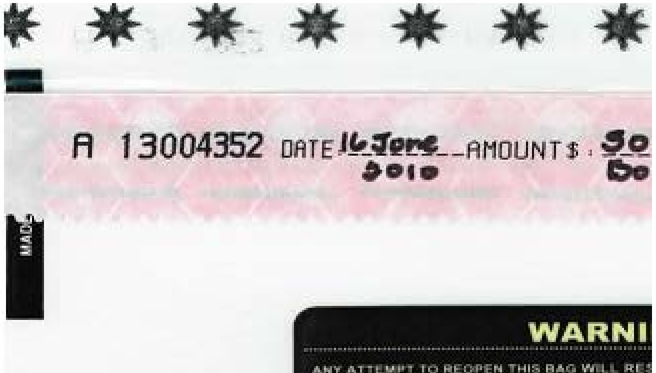
Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

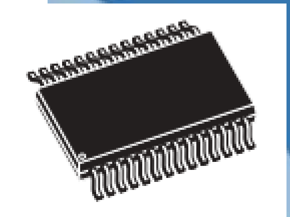
Signature:

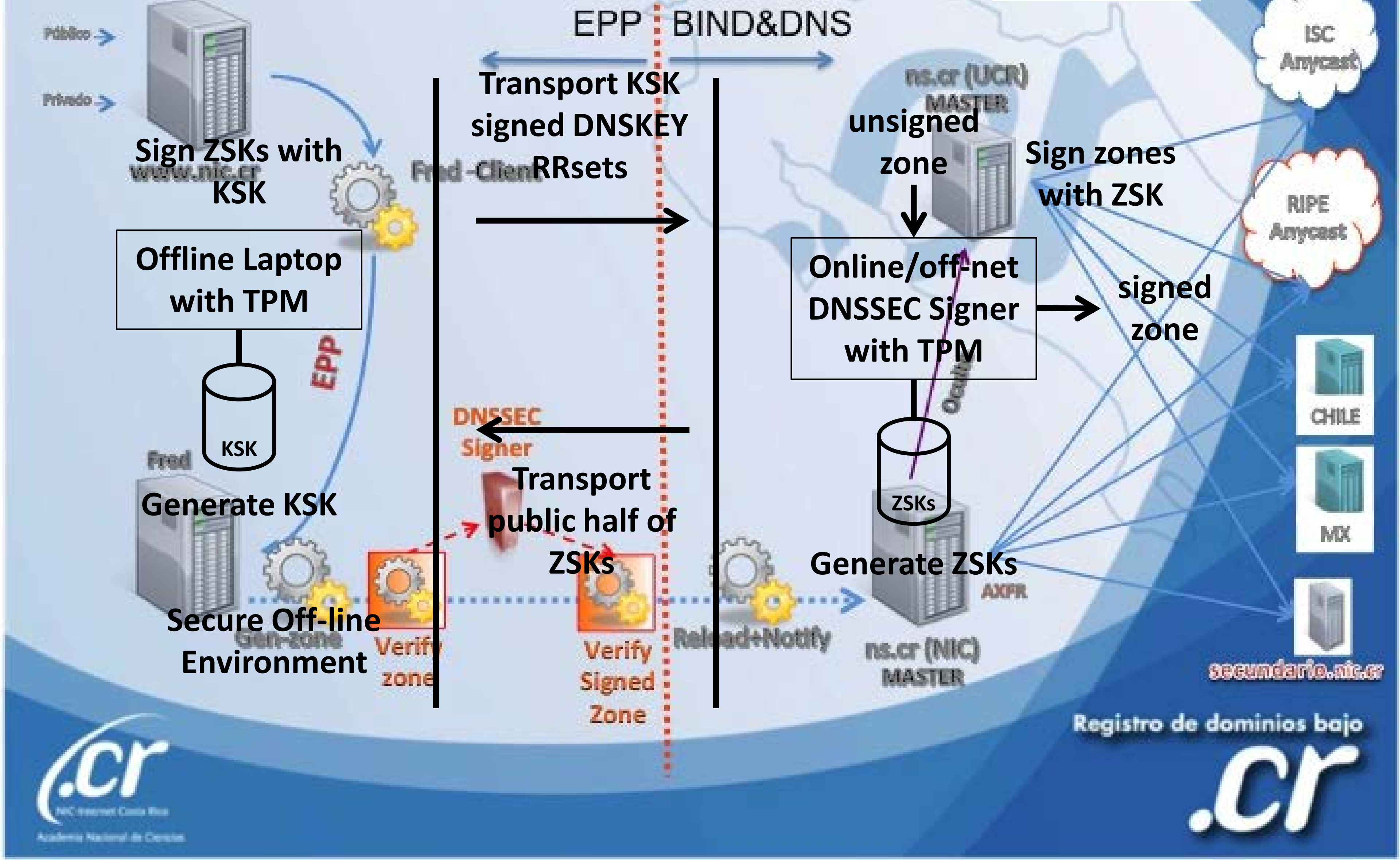
Dated: 20 March 2008

A/ Director, Industry Program Group
Communications Security Establishment


A 13004352 DATE 16 June 2010 AMOUNT $ 50 500
MADE
WARNI
ANY ATTEMPT TO REOPEN THIS BAG WILL RES

..or this (CR NIC)





Sign ZSKs with KSK

Offline Laptop with TPM

KSK

Generate KSK

Secure Off-line Environment

Transport KSK signed DNSKEY RRsets

Transport public half of ZSKs

unsigned zone

Sign zones with ZSK

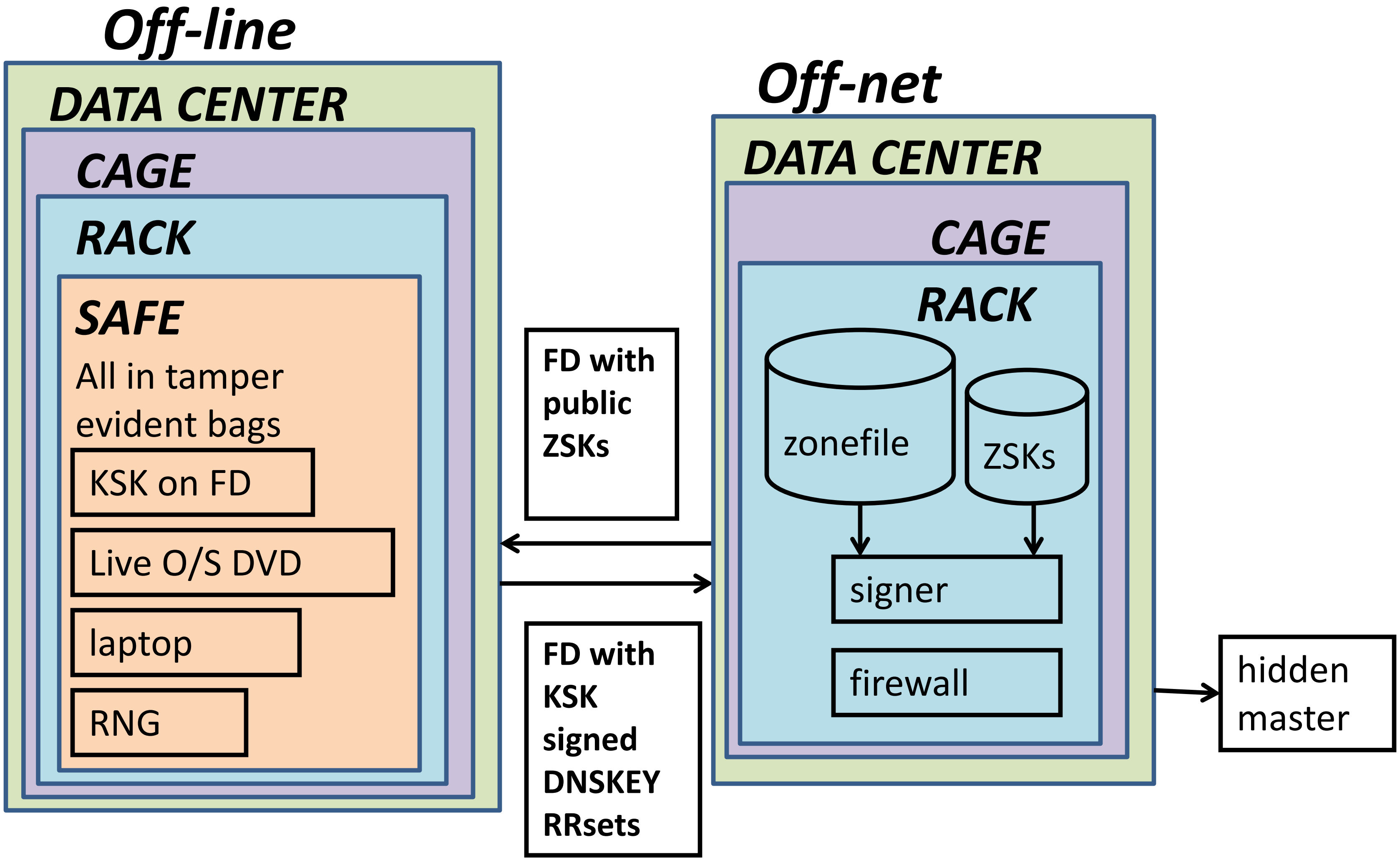
Online/off-net DNSSEC Signer with TPM

signed zone

ZSKs

Generate ZSKs

…or even this

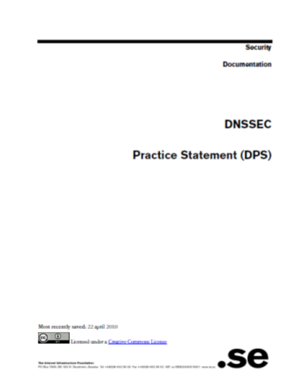


Off-line
DATA CENTER
CAGE
RACK
SAFE
All in tamper evident bags
KSK on FD
Live O/S DVD
laptop
RNG
FD with public ZSKs
FD with KSK signed DNSKEY RRsets
Off-net
DATA CENTER
CAGE
RACK
zonefile
ZSKs
signer
firewall
hidden master

But all must have:

- Published practice statement
  - Overview of operations
  - Setting expectations
    - Normal
    - Emergency
  - Limiting liability
- Documented procedures
- Multi person access requirements
- Audit logs
- Good Random Number Generators

15 Feb 12 – "Ron was wrong, Whit is right"



Security

Documentation

DNSSEC

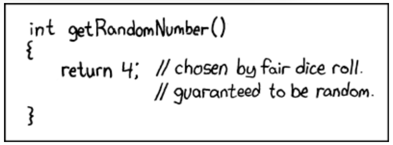
Practice Statement (DPS)

Most recently saved: 22 april 2010

Licensed under a Creative Commons License

The Internet Infrastructure Foundation
[illegible]

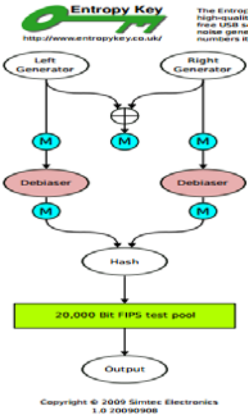
.se



```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

Intel RdRand

DRBGs
FIPS 140



Useful IETF RFCs:
DNSSEC Operational Practices http://tools.ietf.org/html/draft-ietf-dnsop-rfc4641bis
A Framework for DNSSEC Policies and DNSSEC Practice Statements http://tools.ietf.org/html/draft-ietf-dnsop-dnssec-dps-framework

Summary

- DNSSEC has left the starting gate but without greater support by Registrars, demand from domain name holders and trustworthy deployment by operators, it will die on the vine
- Building awareness amongst a larger audience based on recent attacks and increased interest in cyber security may be one solution
- Drawing on lessons learned from certificate authorities and other sources of trust on the Internet can make DNSSEC a source of innovation and opportunity for all

+1-202-709-5262
VoIP

US-NSTIC

DNS is a part of all ecosystems

facebook

eBay

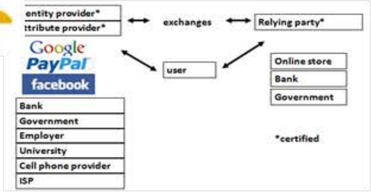
AADHAAR

Google

OpenID

PayPal

OECS ID effort



amazon Prime

e-Passport
symbol

ICP Brasil
O Brasil na era da certificação digital

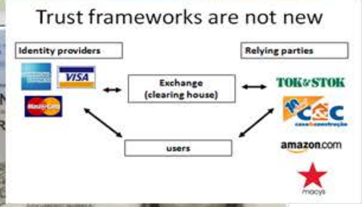
SVERIGE SWEDEN SUÈDE
SVENSK/SWE
O chip permitiria o armazenamento de dados sobre o citadão
O Registro de Identidade Civil seria um número nacional de identificação
REPÚBLICA FEDERATIVA DO BRASIL
MINISTÉRIO DA JUSTIÇA
REGISTRO DE IDENTIDADE CIVIL
ESTADO DE UTOPIA
FERNANDA CARVALHO DA SILVA
UTOPIA / UT
10/05/1975
JOÃO CARVALHO DA SILVA
MARIA CARVALHO DA SILVA
0000000001-9
JUL/JUL 07
JUL/JUL 12

DigiNotar
A VASCO COMPANY

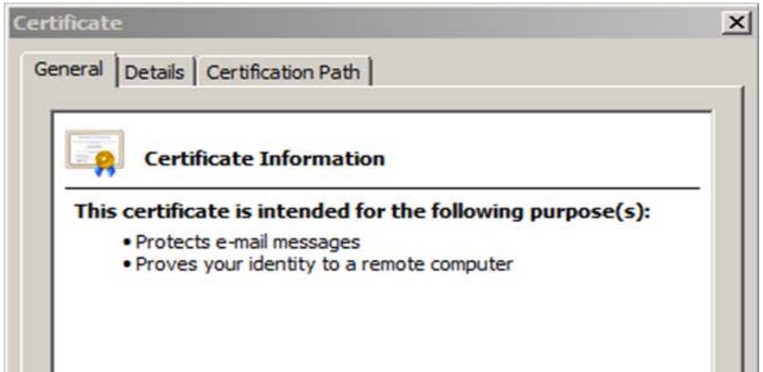
COMODO
Creating Trust Online

Smart Electrical Grid

lamb@xtcn.com


Trust frameworks are not new

ARVALHO<FERNANDA<<<<<<
mydomainname.com


Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):
- Protects e-mail messages
- Proves your identity to a remote computer

Norton SECURED
powered by VeriSign