Deploying DNSSEC: From Content to End-customer

InterOp Mumbai 2012

11 October 2012

richard.lamb@icann.org

Terminology

Registrant (Content)←→Registrar←

→Registry←→Root←

→ISP←→End User (Eyes)

Example:

tata.in (TATA)←→net4.in (Net4)←

→nixi.in (NIXI)←→icann.org (ICANN)←

→Airtel, Sify, etc..←→ISP Customer

Creating a Chain of Trust

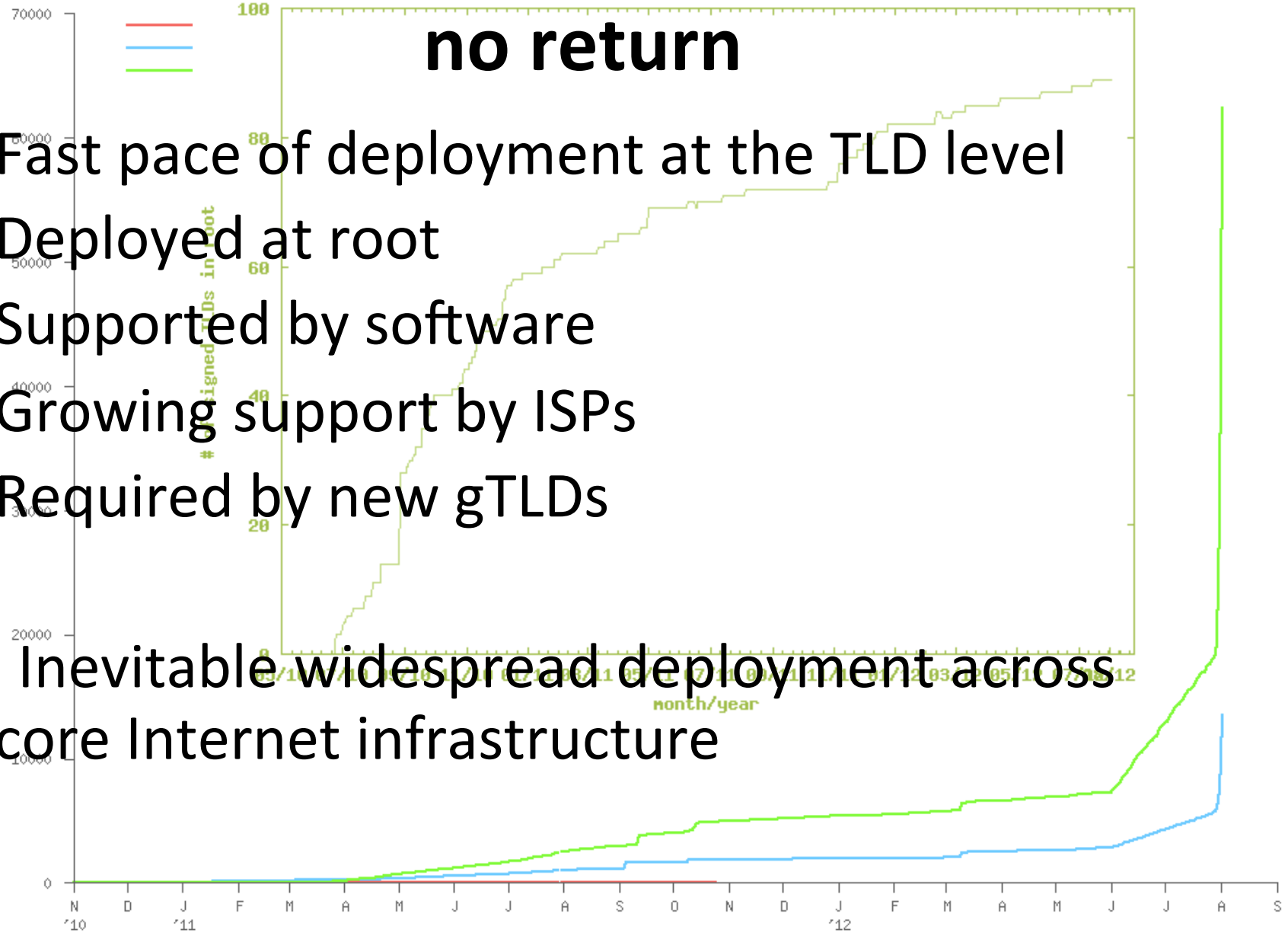
- Registrant generates, signs their records with and publishes key to Registrar.
- Registrar manages key at the Registry on behalf of the Registrant.
- Registry generates, signs Registrant key with and publishes its own key in root.
- The root generates, signs Registry key with and publishes its own key to public.
- ISP/End User validates Registrant DNS record with Registrant key then Registrant key with Registry key and finally Registry key with root key.
- This creates the chain of trust from content provider (Registrant) to end user.

Registrant→Registrar→Registry→Root→ISP→End User

DNSSEC: We have passed the point of no return

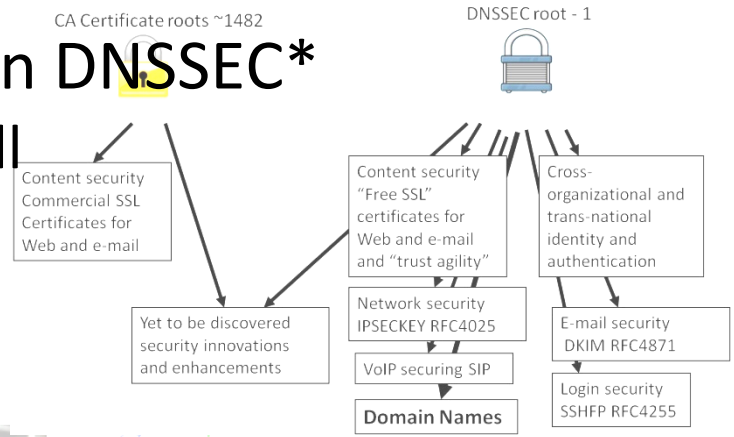
- Fast pace of deployment at the TLD level
- Deployed at root
- Supported by software
- Growing support by ISPs
- Required by new gTLDs

→ Inevitable widespread deployment across core Internet infrastructure



DNSSEC: Plenty of Motivation

- DNSChanger attack, calls for deployment by governments, etc…
- Technology and standards built on DNSSEC*
  - Improved Web TLS and certs for all
  - Secured e-mail (S/MIME) for all
  - SSH, IPSEC, …
- …and new applications
  - VoIP
  - Digital identity
  - Secured content delivery (e.g. configurations, updates)
  - Smart Grid
  - A global PKI
  - Increasing trust in e-commerce

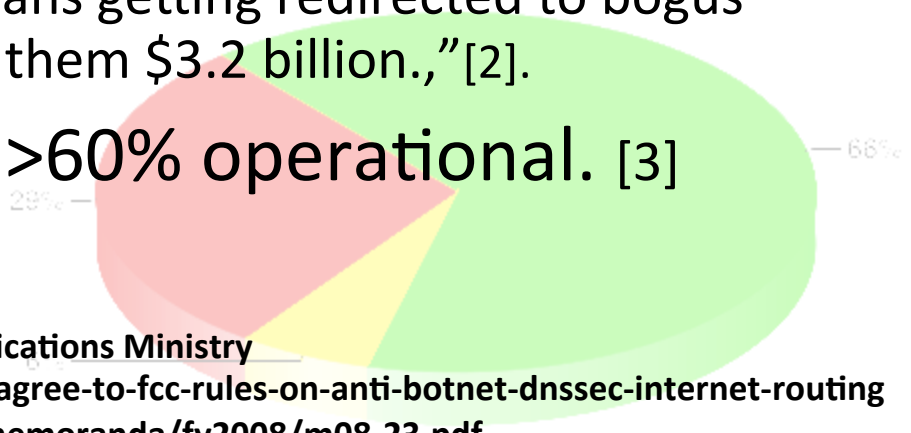


A good ref http://www.internetsociety.org/deploy360/dnssec/

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

DNSSEC interest from governments

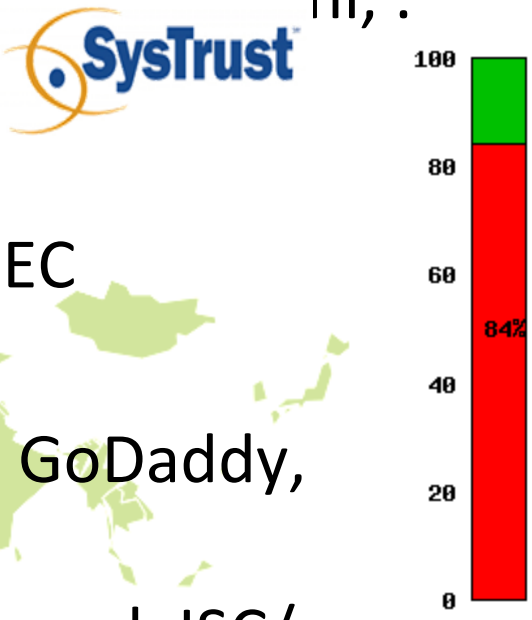
- Sweden, Brazil, Netherlands and others encourage DNSSEC deployment to varying degrees
- Mar 2012 - AT&T, CenturyLink (Qwest), Comcast, Cox, Sprint, TimeWarner Cable, and Verizon have pledged to comply and abide by US FCC [1] recommendations that include DNSSEC.. "A report by Gartner found 3.6 million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

DNSSEC: Where we are

- Deployed on 94/316 TLDs (.in, .lk, .my ملیسیا , .asia, .tw 台灣, .kr 한국, .jp, .kg, .tm, .am, .mm, .ua, .cr, .cz, .bı ' nl, .fr, .com, .tt, .net, .post, …)
- Root signed** and audited
- >84% of domain names could have DNSSEC
- Growing ISP support*
- 3rd party signing solutions are appearing: GoDaddy, VeriSign, Binero, …***
- S/W H/W support: NLNetLabs/NSD+Unbound, ISC/BIND, Microsoft, PowerDNS, Secure64, Xelerence,…
- IETF standard on DNSSEC SSL certificates (DANE)



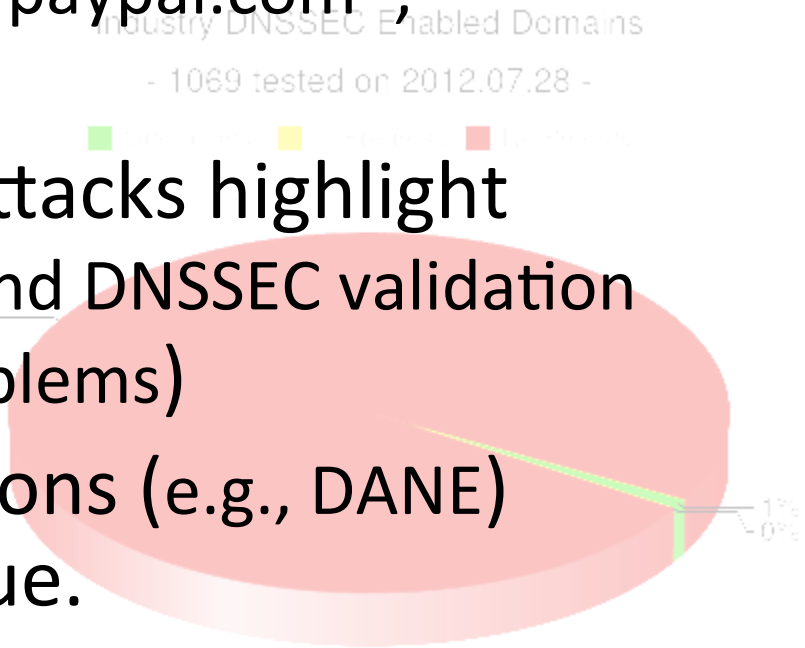
***COMCAST Internet (18M), TeliaSonera SE, Sprint,Vodafone CZ,Telefonica CZ, T-mobile NL, SurfNet NL, SANYO Information Technology Solutions JP, others..**

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

How to implement DNSSEC?

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

"What You Can Do"

- Raise awareness of DNSSEC and its security value in your enterprises. Deploy on your domain names – it is “a feature”.
- Start DNSSEC implementation early, combine with other upgrades. Later, offer hosting as a service.
- At minimum ensure network and resolvers pass DNSSEC responses to end users unscathed to allow validation to occur there.

Trustworthy Implementation

Building in security

- Getting the machinery for DNSSEC is easy (BIND, NSD/Unbound, OpenDNSSEC, etc..).

- Finding good security practices to run it is not.

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

COMODO
Creating Trust Online®

- 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)

DigiNotar®
A VASCO COMPANY

An implementation can be thi$

SysTrust

…or this

FIPS 140-2 Vali

FIPS VALIDATED 140-2

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
ct identified as:

Athena IDProtect by Athen
AT90SC25672RCT Revision D;

ting accredited laboratory:

+

Level 3		
Level 3		
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)

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 Baker

Dated: March 31, 2008

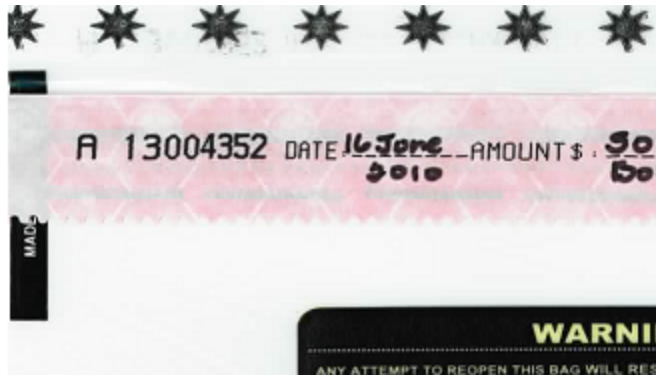
Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

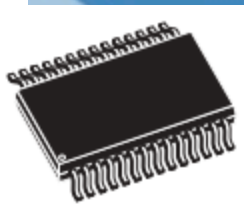
Signature:

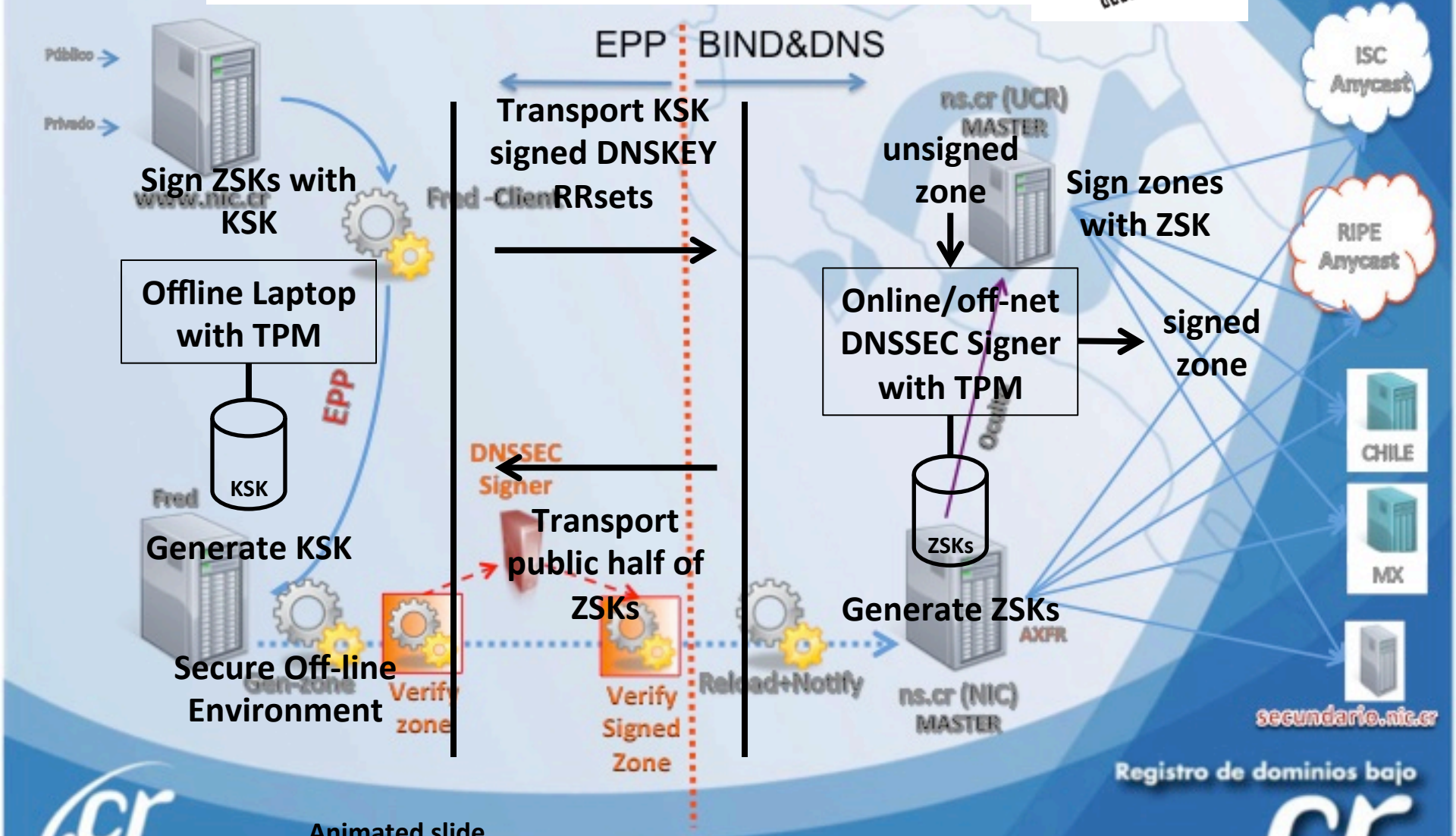
Dated: 20 March 2008

Director, Industry Program Group
Communications Security Establishment



..or this (CR NIC)

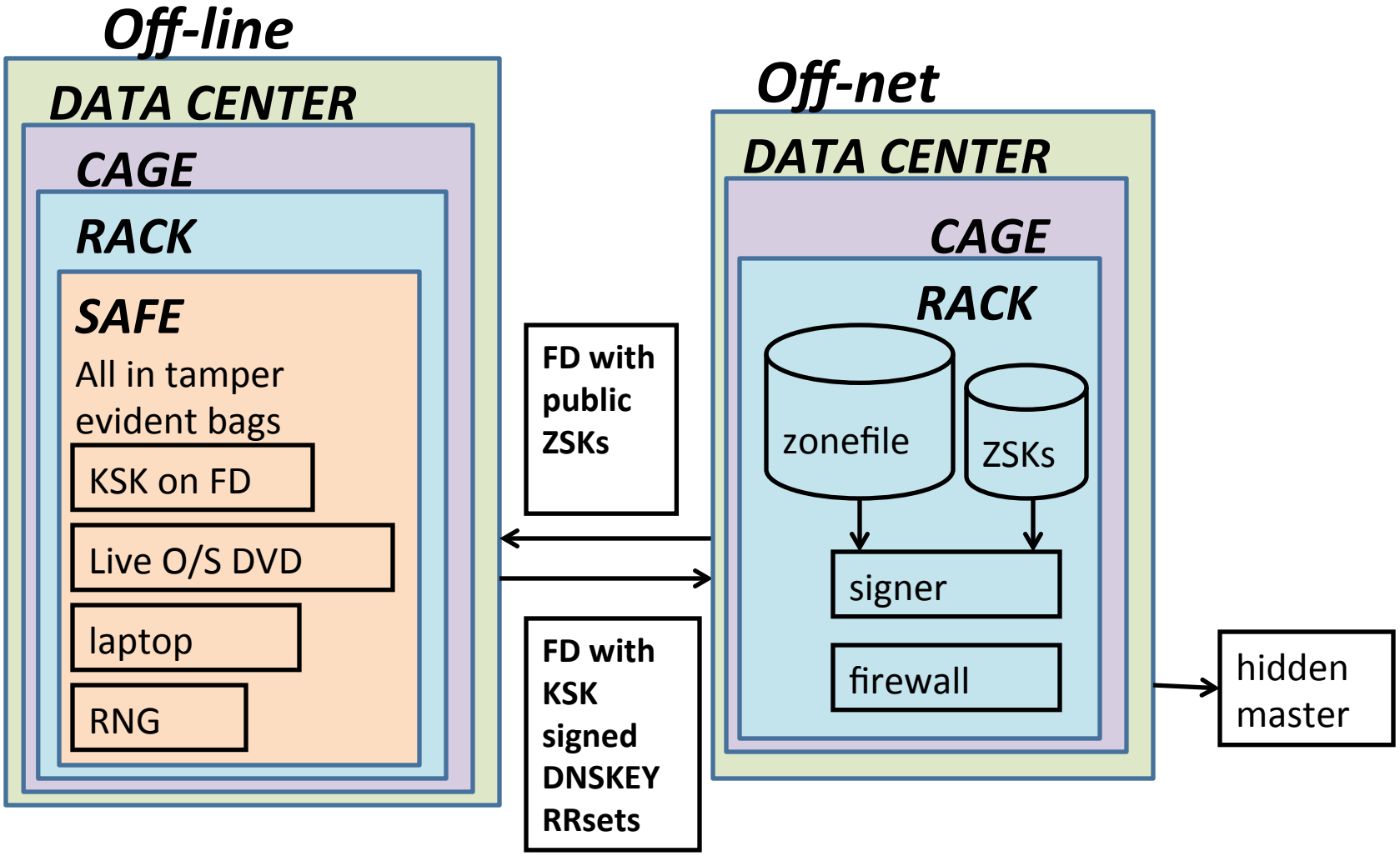




Animated slide

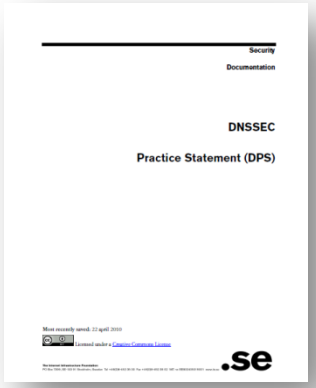
Registro de dominios bajo .cr

…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:

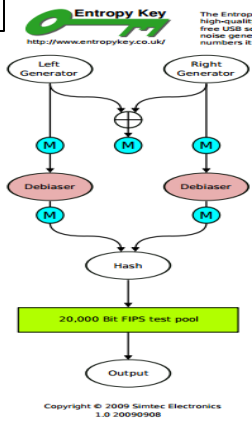
- Published practice statement
  - Overview of operations
  - Setting expectations
    - Normal
    - Emergency
  - Limiting liability
- Documented procedures
- Multi person access requirements
- Audit logs
- Monitoring (e.g., for signature expiry)
- Good Random Number Generators


Security
Documentation
DNSSEC
Practice Statement (DPS)
.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 deployment by domain name holders, support from Registrars, and trustworthy deployment by operators, we may miss the opportunity to improve overall Internet security and develop innovative new security solutions.

+1-202-709-5262
VoIP

US-NSTIC

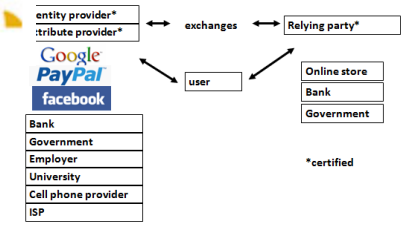
DNS is a part of all IT ecosystems

Google
OpenID

facebook

ebay

AADHAAR



PayPal

OECS ID effort

amazon Prime

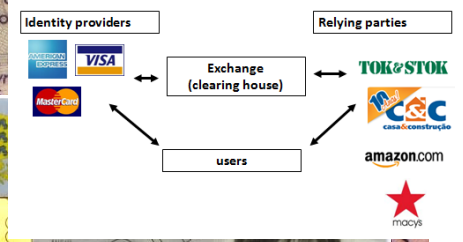
e-Passport symbol

ICP Brasil
O Brasil na era da certificação digital

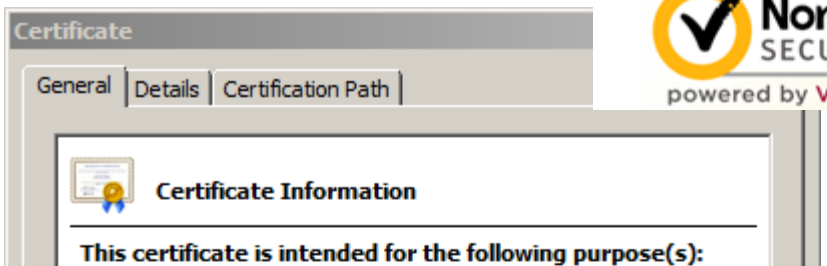
DigiNotar
A VASCO COMPANY

COMODO
Creating Trust Online

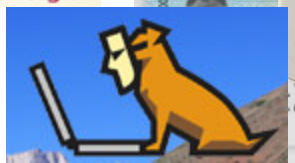
Trust frameworks are not new



Smart Electrical Grid



Norton SECURED
powered by VeriSign



lamb@xtcn.com

mydomainname.com