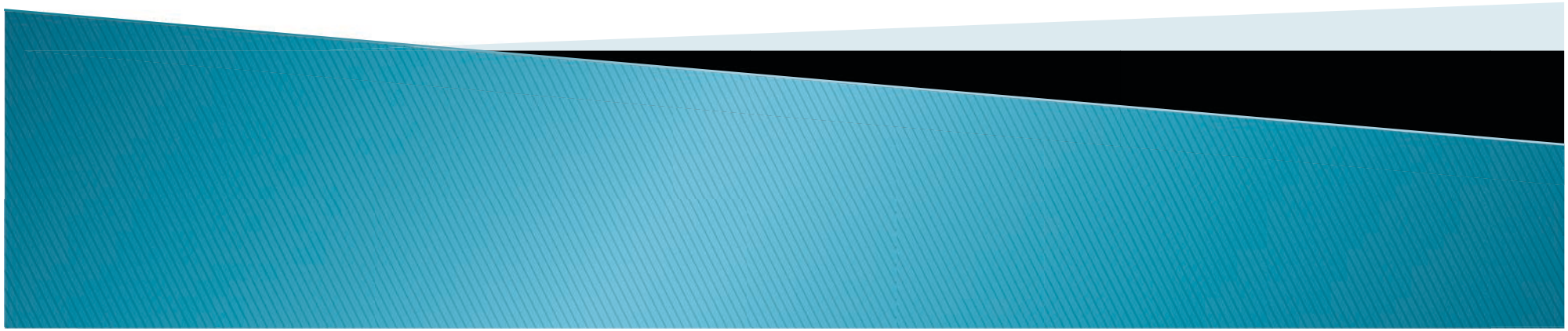
DNSSEC Deployment: Where We Are (and where we need to go)

APRICOT 2012 New Delhi, India
February 21 – March 2

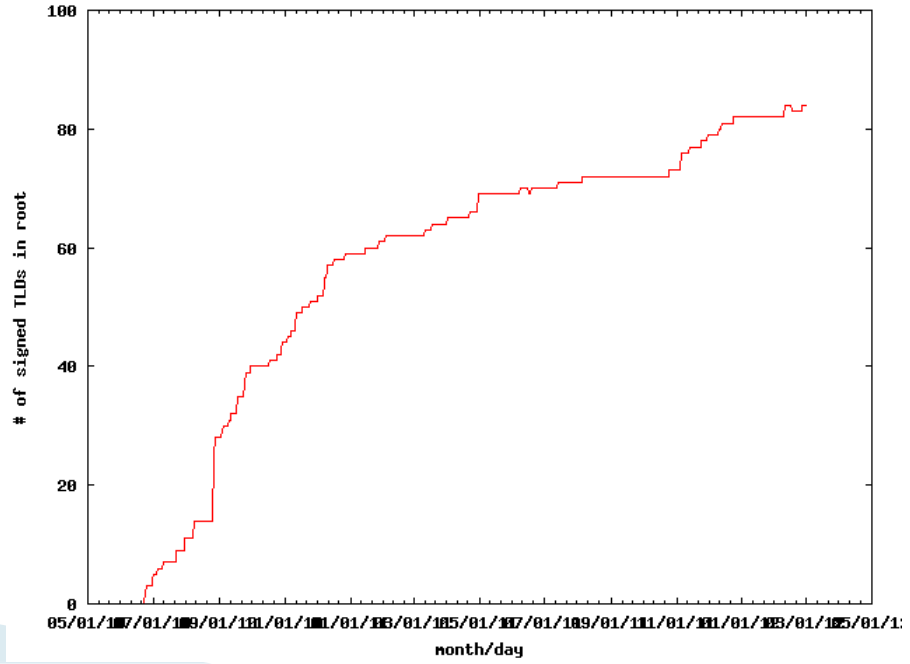
richard.lamb@icann.org



DNSSEC: Passed the point of no return

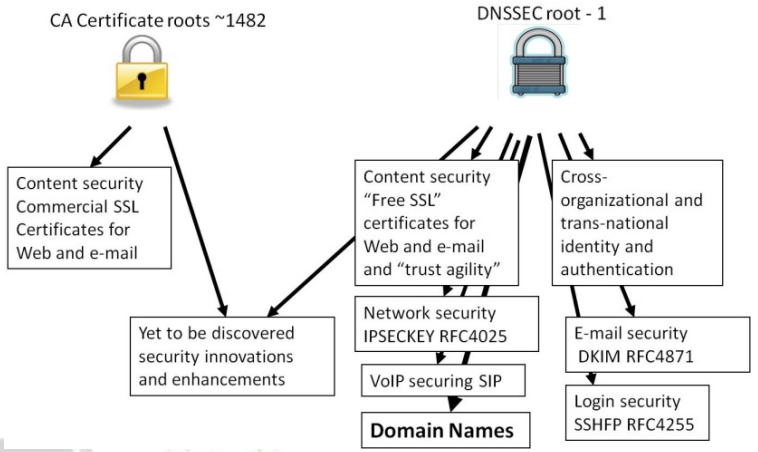
- Fast pace of deployment at the TLD level
- Stable deployment at root

→Inevitable widespread deployment across core infrastructure



DNSSEC: Plenty of Motivation

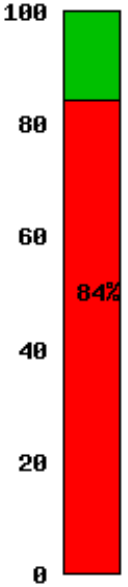
- DNSChanger (10 Nov 2011), Brazilian ISP (7 Nov 2011), etc…
- DANE
  - Improved Web TLS for all
  - Email S/MIME for all
- And…
  - SSH, IPSEC, VoIP
  - Digital identity
  - Other content (e.g. configurations)
  - A global PKI



22 Feb 2012- US FCC Chairman: "A report by Gartner found 3.6 million Americans getting redirected to bogus websites in a single year, costing them $3.2 billion.," … "I urge all broadband providers to begin implementing DNSSEC as soon as possible."

DNSSEC:Where we are

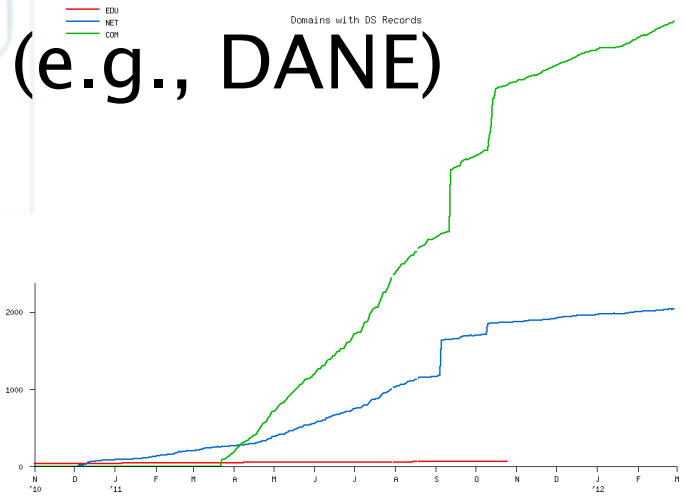
- Deployed on 84/312 TLDs (.asia, .in, .lk, .tw 台灣 台灣, .jp, .nz, .kr, .my, .th, .nc, .nu, .tm, .kg, .mn, .mm, .la, .ug, .na, .com.*)
- Root signed and audited
- 84% of doman names could have could have DNSSEC deployed on them
- Large ISP has turned DNSSEC validation “on”
- A few 3rd party signing solutions (e.g., GoDaddy, VeriSign, Binero,…)
- Unbound, BIND, DNSSEC-trigger, vsResolver and other last mile. DANE work almost done



*10 Jan 2012 – All 18M COMCAST Internet customers. Others..TeliaSonera SE, Vodafone CZ,Telefonica, CZ, T-mobile NL, SurfNet NL

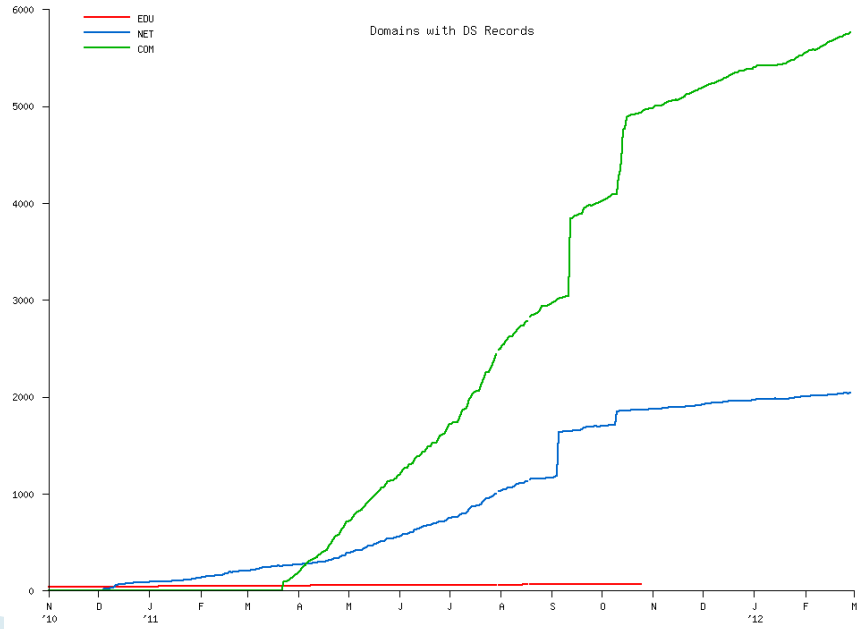
DNSSEC:Where we are

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



What needs to happen

- ISPs need to turn on DNSSEC validation.
- Domain name holders need to sign.
- …all in a trustworthy fashion.



Barriers to success

- Registrar support*
  - chicken and egg
- Ease of implementation
  - security/crypto/management cost/complexity
  - no click and sign
- Trust
  - insecure practices and processes
  - garbage in, garbage out

*www.icann.org/en/news/in-focus/dnssec/deployment

Solutions

- Create demand for DNSSEC: Raise awareness of domain holders (content) and users (eyes)
- Ease Implementation:
  - DNSSEC training drawn from existing implementations*
  - Key management automation and monitoring
  - Crypto: HSM? Smartcard? TPM chip? Soft keys? – all good
- Trust: It is transparent processes and practices that matter
  - 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

*Just talk to me. Its my job!

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

FIPS 140-2 Vali

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	C	
Level 3	Fi	
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

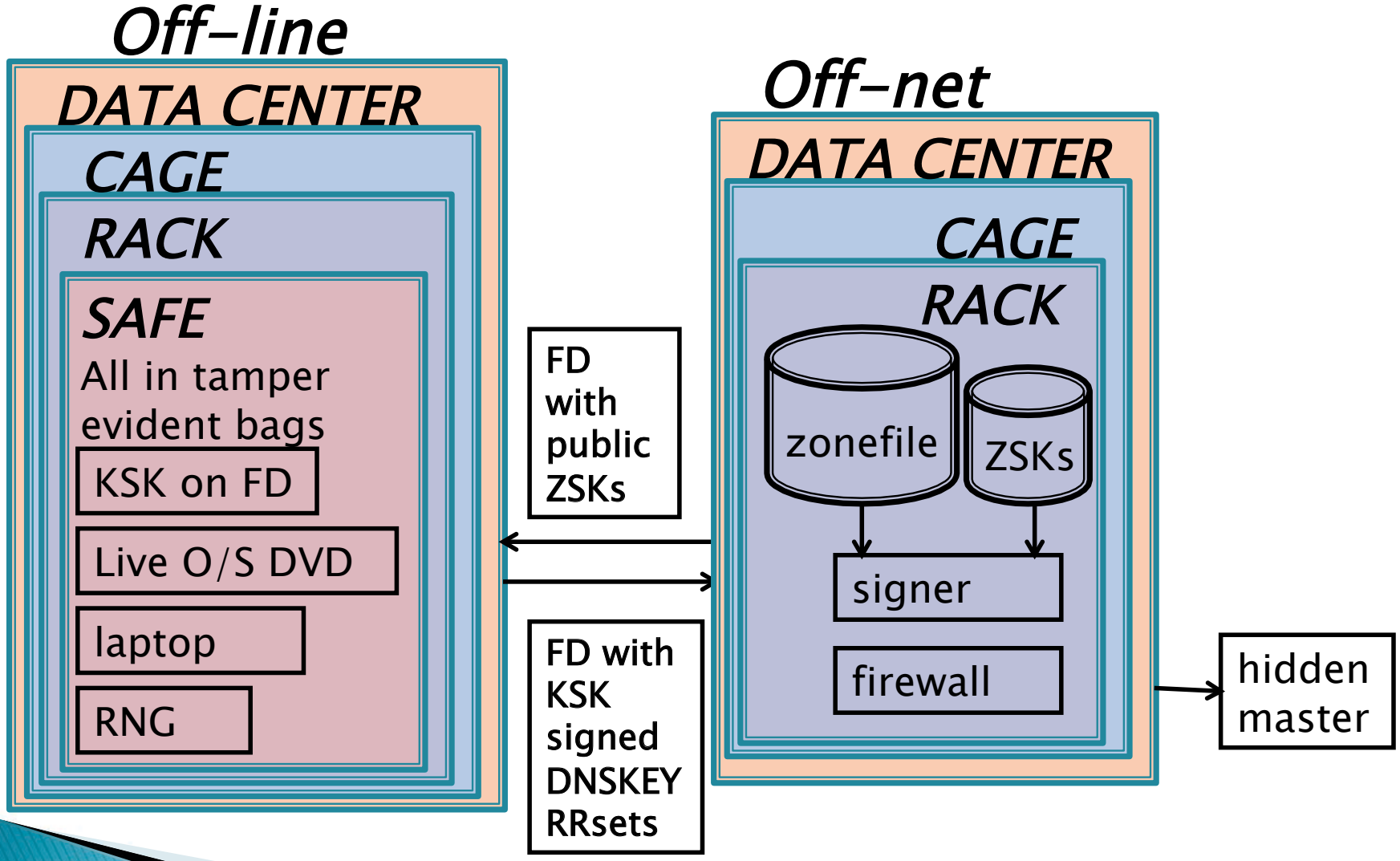
Signed on behalf of the Government of Canada

Signature:

Dated: 20 March 2008

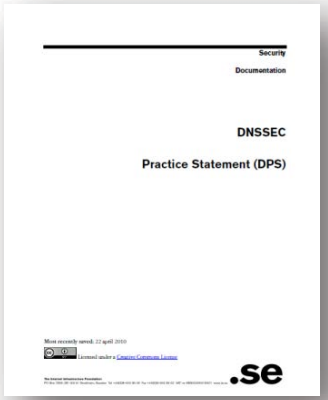
Director, Industry Program Group
Communications Security Establishment

…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

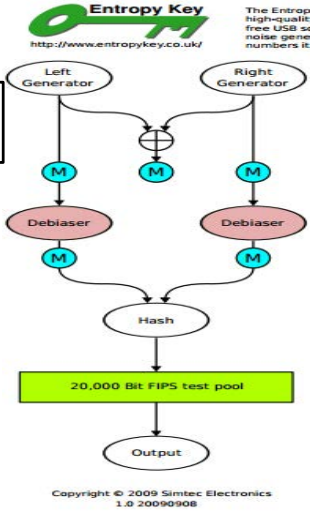
But all must have:

- Published practice statement
  - Overview of operations
  - Setting expectations
    - Normal
    - Emergency
  - Limiting liability



- Documented procedures for each operation
- Multi person access requirements
- Audit logs
- Good Random Number Generators

Intel RdRand



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

DRBGs

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

Summary

- DNSSEC has left the starting gate and is likely to continue to be deployed at an accelerated pace at the TLD level with the benefits well understood by those in the field. However, a number of obstacles and pitfalls must be overcome for DNSSEC to reach its full potential
  - Lack of support by Registrars and ISPs
  - Lack of adoption by domain name holders and interest by end users
  - Un-trustworthy, quick and dirty, DNSSEC deployment
- Increased awareness building driven by the recent reporting of widespread DNS exploits and CA failures should drive a virtuous cycle of secure DNSSEC deployment and support. However, the complexity and cost of a professional DNSSEC implementation are often cited as a barrier.
- By drawing on experience from CAs and current DNSSEC deployments, a trustworthy implementation need not be expensive nor complex if we focus on transparency.
- Given the integral role DNS plays in the Internet and government interest in “doing something” about cyber security, DNSSEC deployment, if properly positioned, may serve as an excuse to upgrade/improve the security of DNS operations as a whole.
- Questions?