DNSSEC Sample Implementation

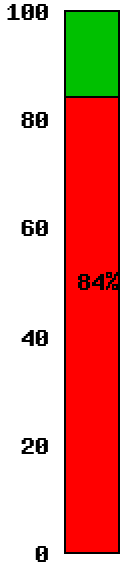
MENOG 10 Workshop

22 April 2012, Dubai

richard.lamb@icann.org

DNSSEC: Where we are

- Deployed on 86/313 TLDs (.uk, .fr, .asia, .in, .lk, .kg, .tm, .am, .tw **台灣 台湾**, .jp, .cr, .com,…)
- Root signed and audited
- 84% of domain 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,

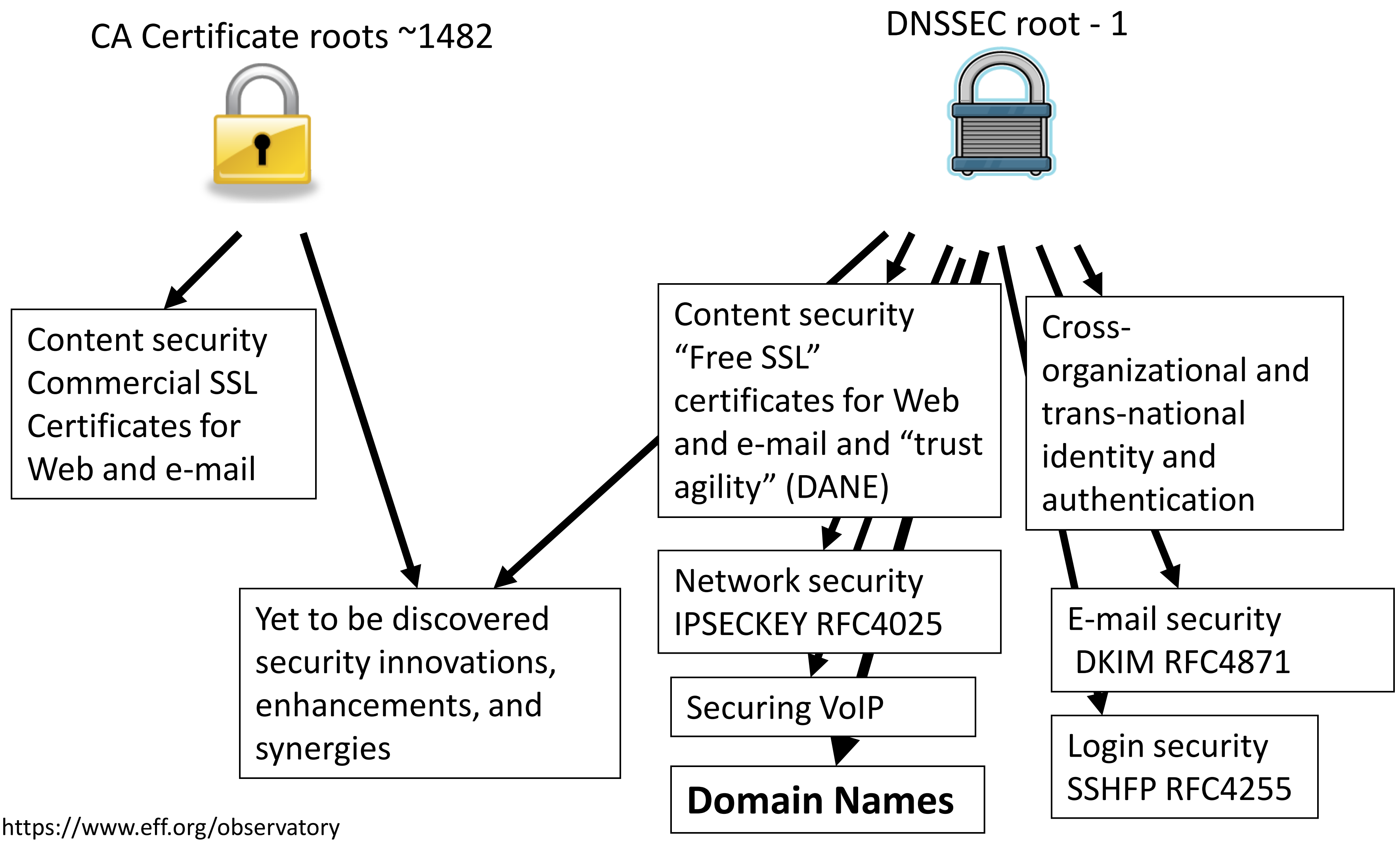
Vodafone CZ,Telefonica, CZ, T-mobile NL,

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

Resultant Global PKI

SSL (DANE), E-mail, VOIP security…



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)

Network security
IPSECKEY RFC4025

Securing VoIP

Domain Names

Cross-organizational and trans-national identity and authentication

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/

Design Considerations

Goals

- Reliable
- Trusted
- Cost Effective (for you)

Cost Effectiveness

Cost Effectiveness

- Risk Assessment
- Cost Benefit Analysis

Business Benefits and Motivation

(from “The Costs of DNSSEC Deployment” ENISA report)

- Become a reliable source of trust and boost market share and/or reputation of zones;
- Lead by example and stimulate parties further down in the chain to adopt DNSSEC;
- Earn recognition in the DNS community and share knowledge with TLD’s and others;
- Provide assurance to end-user that domain name services are reliable and trustworthy;
- Look forward to increasing adoption rate when revenue is an important driver. Deploying DNSSEC can be profitable;

Risk Assessment

- Identify your risks
  - Reputational
    - Competition
    - Loss of contract
  - Legal / Financial
    - Who is the relying party?
    - SLA
    - Law suits
- Build your risk profile
  - Determine your acceptable level of risk

Vulnerabilities

- False expectations
- Key compromise
- Signer compromise
- Zone file compromise

Cost Benefit Analysis

Setting reasonable expectations means it doesn’t have to be expensive

From ENISA Report

- "….organizations considering implementing DNSSEC can greatly benefit from the work performed by the pioneers and early adopters."
- Few above 266240 Euros: Big Spenders: DNSSEC as an excuse to upgrade all infrastructure; embrace increased responsibility and trust through better governance.
- Most below 36059 Euros: Big Savers: reuse existing infrastructure. Do minimum.

Anticipated Capital and Operating Expense

- Being a trust anchor requires mature business processes, especially in key management;
- Investment cost also depends on strategic positioning towards DNSSEC: leaders pay the bill, followers can limit their investment;
- Financial cost might not outweigh the financial benefits. Prepare to write off the financial investment over 3 to 5 years, needed to gear up end-user equipment with DNSSEC.

Other Cost Analysis

- People
  - Swedebank – half a FTE
  - Occasional shared duties for others
- Facilities
  - Datacenter space
  - Safe ~ $100 - $14000
- Crypto Equip ~ $5-$40000
- Bandwidth ~ 4 x

http://www.internetdagarna.se/arkiv/2008/www.internetdagarna.se/images/stories/doc/22_Kjell_Rydger_DNSSEC_from_a_bank_perspective_2008-10-20.pdf

Trusted

Trust

- Transparent
- Secure

Transparency

Transparency

- The power of truth
    - Transparency floats all boats here
- Say what you do
- Do what you say
- Prove it

Say what you do

- Setting expectations
- Document what you do and how you do it
- Maintain up to date documentation
- Define Organization Roles and responsibilities
- Describe Services, facilities, system, processes, parameters

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

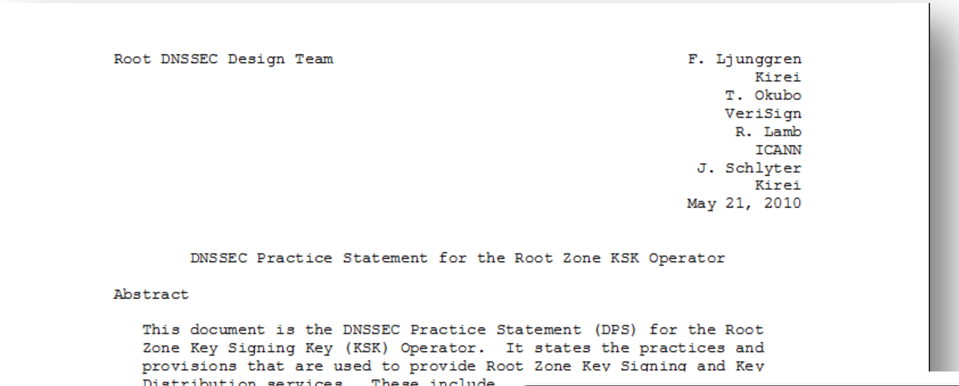
Say What You Do - Learn from Existing Trust Services

- Borrow many practices from SSL Certification Authorities (CA)
  - Published Certificate Practices Statements (CPS)
    - VeriSign, GoDaddy, etc..
  - Documented Policy and Practices (e.g., key management ceremony, audit materials, emergency procedures, contingency planning, lost facilities, etc…)

Say What You Do - DNSSEC Practices Statement

- DNSSEC Policy/Practices Statement (DPS)
  - Drawn from SSL CA CPS
  - Provides a level of assurance and transparency to the stakeholders relying on the security of the operations.
  - Regular re-assessment
  - Management signoff
    - Formalize - Policy Management Authority (PMA)

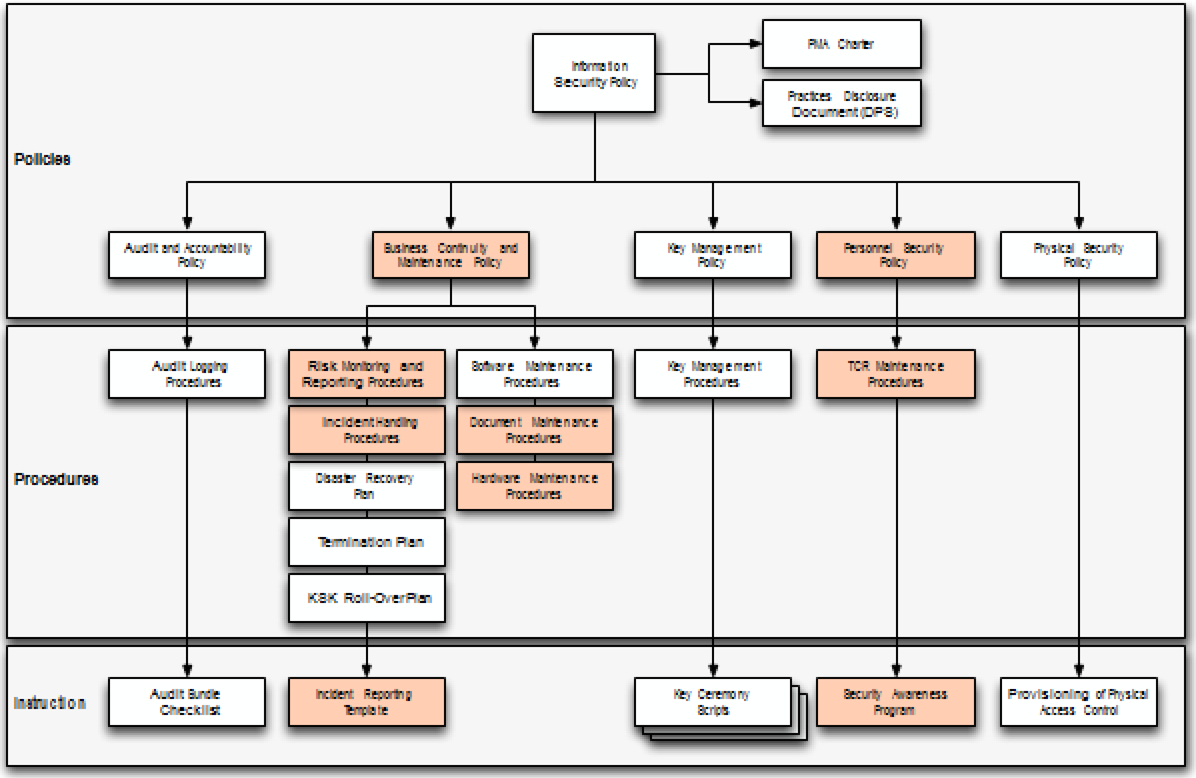
Documentation - Root



```
Root DNSSEC Design Team                                     F. Ljunggren
                                                                   Kirei
                                                                T. Okubo
                                                                VeriSign
                                                                 R. Lamb
                                                                   ICANN
                                                             J. Schlyter
                                                                   Kirei
                                                            May 21, 2010

       DNSSEC Practice Statement for the Root Zone KSK Operator

Abstract

   This document is the DNSSEC Practice Statement (DPS) for the Root
   Zone Key Signing Key (KSK) Operator.  It states the practices and
   provisions that are used to provide Root Zone Key Signing and Key
   Distribution services.  These include,
   issuing, managing, changing and distrib
   with the specific requirements of the U

Copyright Notice

   Copyright 2009 by VeriSign, Inc., and b
   Assigned Names and Numbers.  This work
```

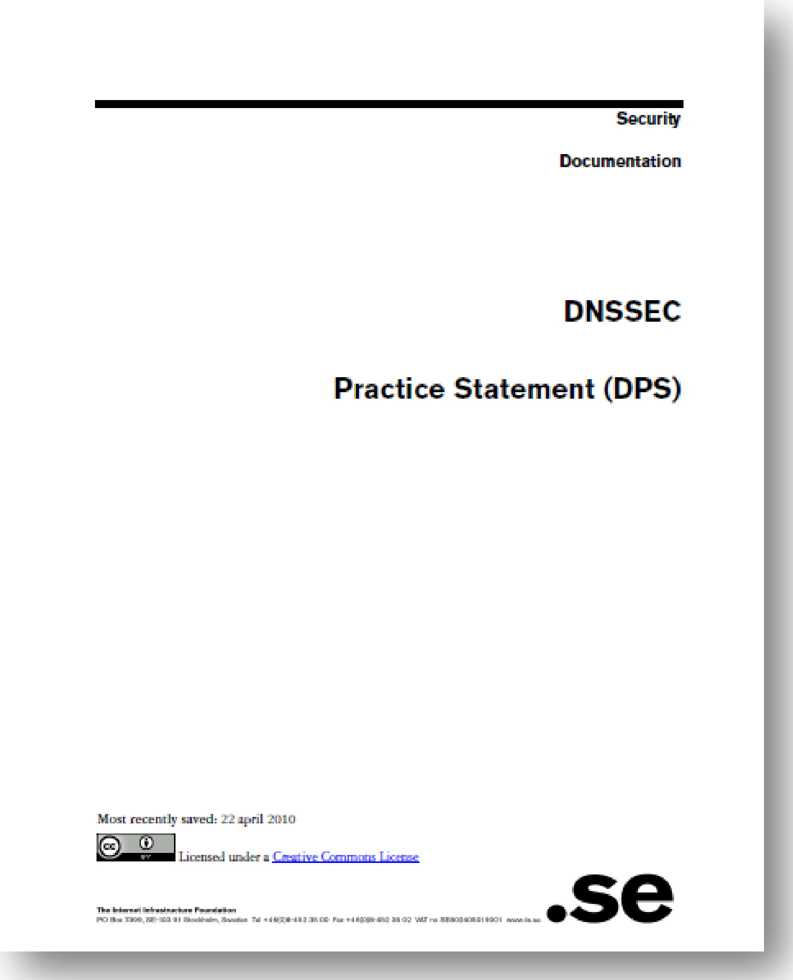
91 Pages and tree of other documents!

Root DPS



Information Security Policy
RMA Charter
Practices Disclosure Document (DPS)
Policies
Audit and Accountability Policy
Business Continuity and Maintenance Policy
Key Management Policy
Personnel Security Policy
Physical Security Policy
Procedures
Audit Logging Procedures
Risk Monitoring and Reporting Procedures
Software Maintenance Procedures
Key Management Procedures
TCR Maintenance Procedures
Incident Handling Procedures
Document Maintenance Procedures
Disaster Recovery Plan
Hardware Maintenance Procedures
Termination Plan
KSK Roll-Over Plan
Instruction
Audit Bundle Checklist
Incident Reporting Template
Key Ceremony Scripts
Security Awareness Program
Provisioning of Physical Access Control

Documentation - .SE



Security

Documentation

DNSSEC

Practice Statement (DPS)

Most recently saved: 22 april 2010

The Internet Infrastructure Foundation
PO Box 7399, SE-103 91 Stockholm, Sweden Tel +46(0)8-452 35 00 Fax +46(0)8-452 35 02 VAT no SE802405601601 www.iis.se

22 pages, Creative Commons License!

.SE DPS

Do what you say

- Follow documented procedures / checklists
- Maintain logs, records and reports of each action, including incidents.
- Critical operations at Key Ceremonies
  - Video
  - Logged
  - Witnessed

Key Ceremony

A filmed and audited process carefully scripted for maximum transparency at which cryptographic key material is generated or used.

Prove it

- Audits
  - 3rd party auditor $$
  - ISO 27000 $$ etc..
  - Internal

Prove it - Audit Material

- Key Ceremony Scripts
- Access Control System logs
- Facility, Room, Safe logs
- Video
- Annual Inventory
- Logs from other Compensating Controls
- Incident Reports

Prove it

- Stakeholder Involvement
  - Publish updated material and reports
  - Participation, e.g. External Witnesses from
    - local Internet community
    - Government
  - Listen to Feedback

Prove it

- Be Responsible
  - Executive Level Involvement
    - In policies via Policy Management Authority
    - Key Ceremony participation

Security

Security

- Physical
- Logical
- Crypto

Physical

- – Environmental
- – Tiers
- – Access Control
- – Intrusion Detection
- – Disaster Recovery

Physical - Environmental

- Based on your risk profile
- Suitable
  - Power
  - Air Conditioning
- Protection from
  - Flooding
  - Fire
  - Earthquake

Physical - Tiers

- Each tier should be successively harder to penetrate than the last
  - Facility
  - Cage/Room
  - Rack
  - Safe
  - System
- Think of concentric boxes

Physical - Tier Construction

- Base on your risk profile and regulations
- Facility design and physical security on
  - Other experience
  - DCID 6/9
  - NIST 800-53 and related documents
  - Safe / container standards

Physical – Safe Tier

Physical – Safe Tier

Physical - Access Control

- Base on your risk profile
- Access Control System
  - Logs of entry/exit
  - Dual occupancy / Anti-passback
  - Allow Emergency Access
- High Security: Control physical access to system independent of physical access controls for the facility

Physical - Intrusion Detection

- Intrusion Detection System
  - Sensors
  - Motion
  - Camera
- Tamper Evident Safes and Packaging
- Tamper Proof Equipment

Physical - Disaster Recovery

- Multiple sites
  - Mirror
  - Backup
- Geographical and Vendor diversity

Logical

- Authentication (passwords, PINs)
- Multi-Party controls

Logical - Authentication

- Procedural:
  - REAL passwords
  - Forced regular updates
  - Out-of-band checks
- Hardware:
  - Two-factor authentication
  - Smart cards (cryptographic)

Logical - Multi-Party Control

- Split Control / Separation of Duties
  - E.g., Security Officer and System Admin and Safe Controller
- M-of-N
  - Built in equipment (e.g. HSM)
  - Procedural: Split PIN
  - Bolt-On: Split key (Shamir, e.g. ssss.c)

Crypto

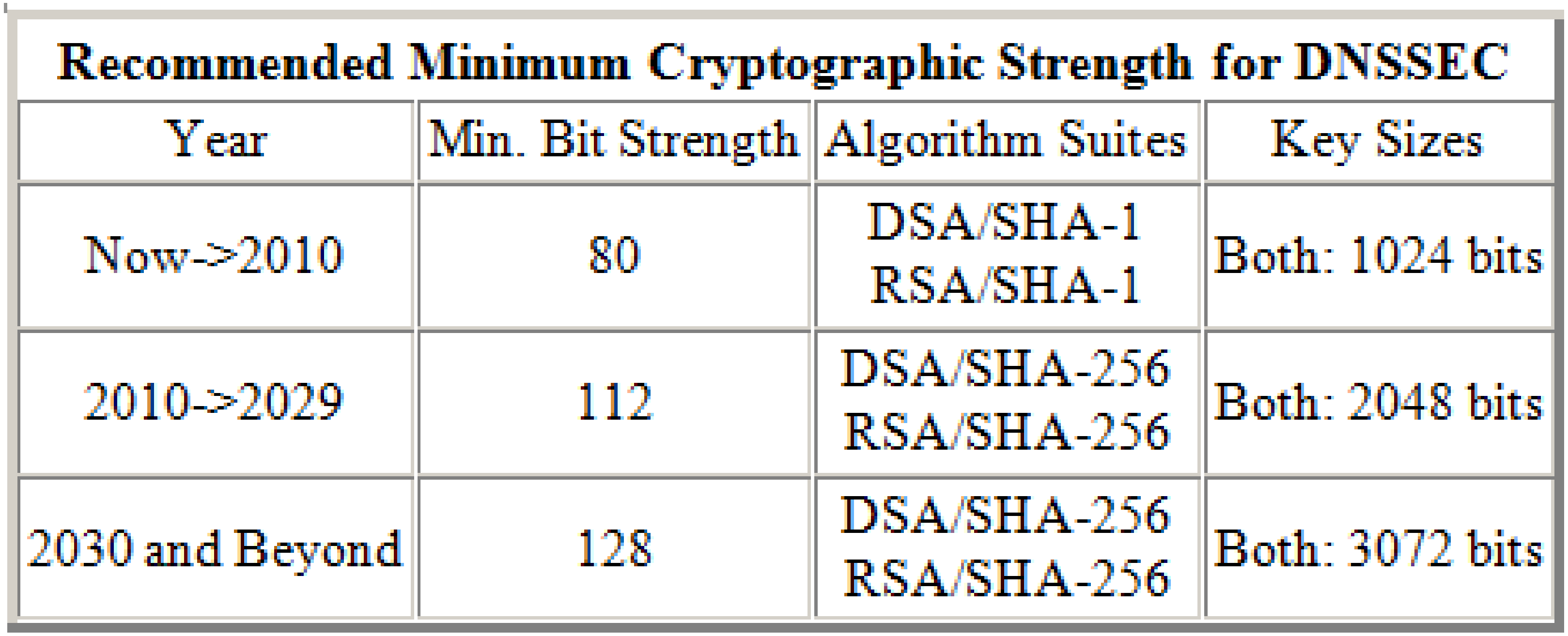
- Algorithms / Key Length
- Crypto Hardware

Crypto - Algorithms / Key Length

- Factors in selection
  - Cryptanalysis
  - Regulations
  - Network limitations

Crypto - Key Length

- Cryptanalysis from NIST: *2048 bit RSA SHA256*



Recommended Minimum Cryptographic Strength for DNSSEC

Year	Min. Bit Strength	Algorithm Suites	Key Sizes
Now->2010	80	DSA/SHA-1 RSA/SHA-1	Both: 1024 bits
2010->2029	112	DSA/SHA-256 RSA/SHA-256	Both: 2048 bits
2030 and Beyond	128	DSA/SHA-256 RSA/SHA-256	Both: 3072 bits

http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf

Crypto - Algorithms

- Local regulations may determine algorithm
  - GOST
  - DSA
- Network limitations
  - Fragmentation means shorter key length is better
  - ZSK may be shorter since it gets rolled often
  - Elliptical is ideal – but not available yet

Crypto - Algorithms

- NSEC3 if required
  - Protects against zone walking
  - Avoid if not needed – adds overhead for small zones
  - Non-disclosure agreement?
  - Regulatory requirement?
  - Useful if zone is large, not trivially guessable (only “www” and “mail”) or structured (ip6.arpa), and not expected to have many signed delegations (“opt-out” avoids recalculation).

Crypto - Hardware

- Satisfy your stakeholders
  - Doesn’t need to be certified to be secure (e.g., off-line PC)
  - Can use transparent process and procedures to instill trust
  - But most Registries use or plan to use HSM. Maybe CYA?
- AT LEAST USE A GOOD Random Number Generator (RNG)!
- Use common standards avoid vendor lock-in.
  - Note: KSK rollover may be ~10 years.
- Remember you must have a way to backup keys!

Crypto - Hardware Security Module (HSM)

- FIPS 140-2 Level 3
  - Sun SCA6000 (~30000 RSA 1024/sec) ~$10000 (was $1000!!)
  - Thales/Ncipher nshield (~500 RSA 1024/sec) ~$15000
- FIPS 140-2 Level 4
  - AEP Keyper (~1200 RSA 1024/sec) ~$15000
  - IBM 4765 (~1000 RSA 1024/sec) ~$9000
- Recognized by your national certification authority
  - Kryptus (Brazil) ~ $2500

Study: http://www.opendnssec.org/wp-content/uploads/2011/01/A-Review-of-Hardware-Security-Modules-Fall-2010.pdf

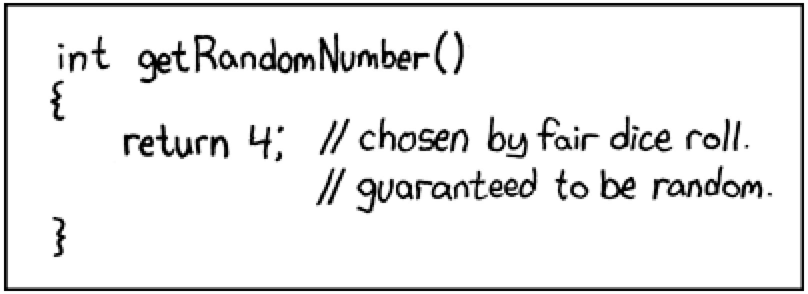
Crypto - PKCS11

- A common interface for HSM and smartcards
  - C_Sign()
  - C_GeneratePair()
- Avoids vendor lock-in - somewhat
- Vendor Supplied Drivers (mostly Linux, Windows) and some open source

Crypto - Smartcards / Tokens

- Smartcards (PKI) (card reader ~$20)
  - Oberthur ~$5-$15
  - AthenaSC IDProtect ~$35
  - Feitian ~$5-10
- Token
  - Aladdin/SafeNet USB e-Token ~$50
  - SDencrypter micro HSM www.go-trust.com
- Open source PKCS11 Drivers available
  - OpenSC
- Has RNG
- Slow ~0.5-10 1024 RSA signatures per second

Crypto -Random Number Generator



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

- rand()
- Netscape: Date+PIDs
- LavaRand
- System Entropy /dev/random
- Quantum Mechanical $
- Standards based (FIPS, NIST 800-90 DRBG)
- Coming soon: Intel atomic

Crypto - FIPS 140-2 Level 4 HSM

Root, .FR, …

Crypto – FIPS Level 3 HSM

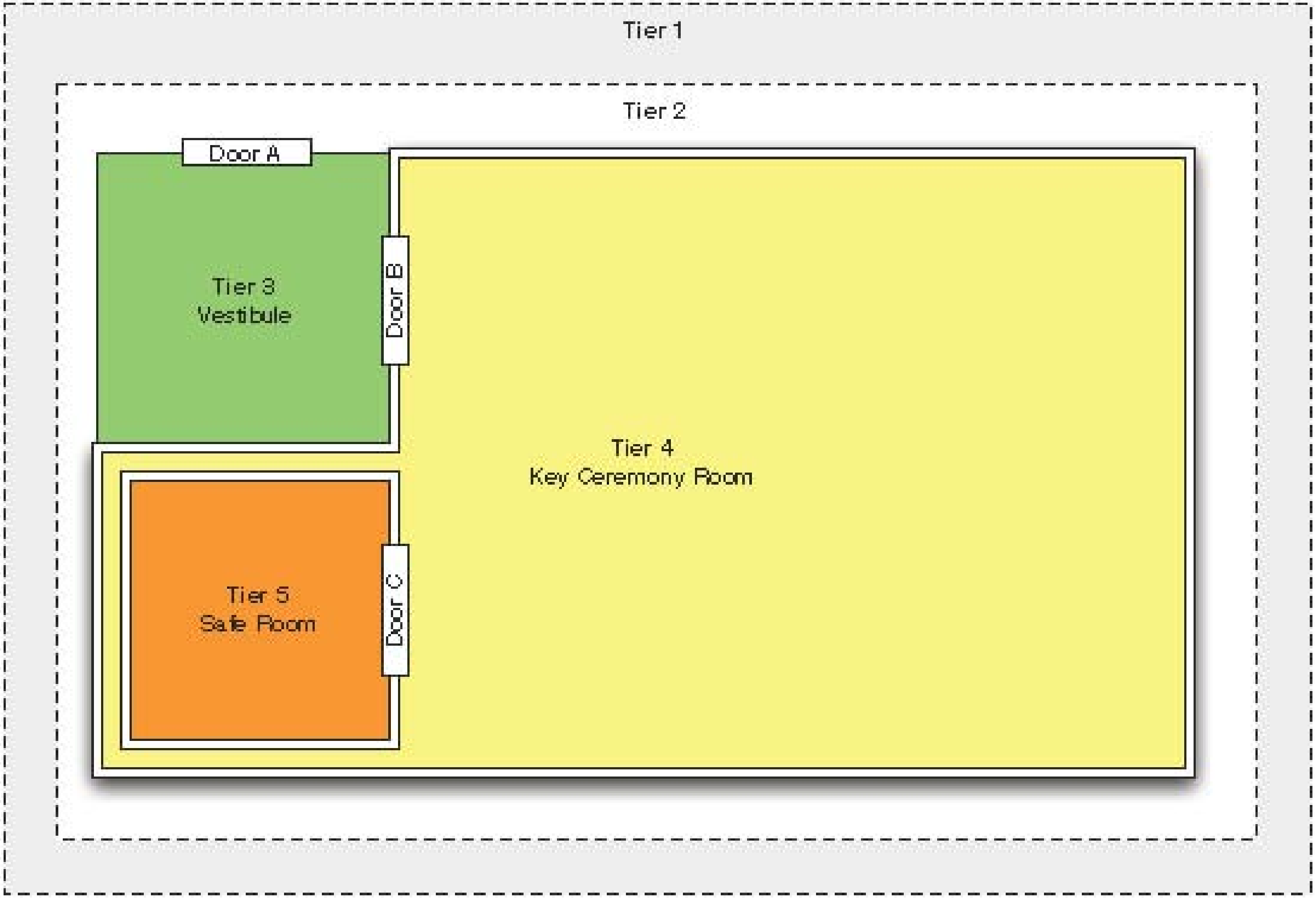
- But FIPS 140-2 Level 3 is also common
- Many TLDs using Level 3 .com , .se, .uk, .com, etc… $10K-$40K

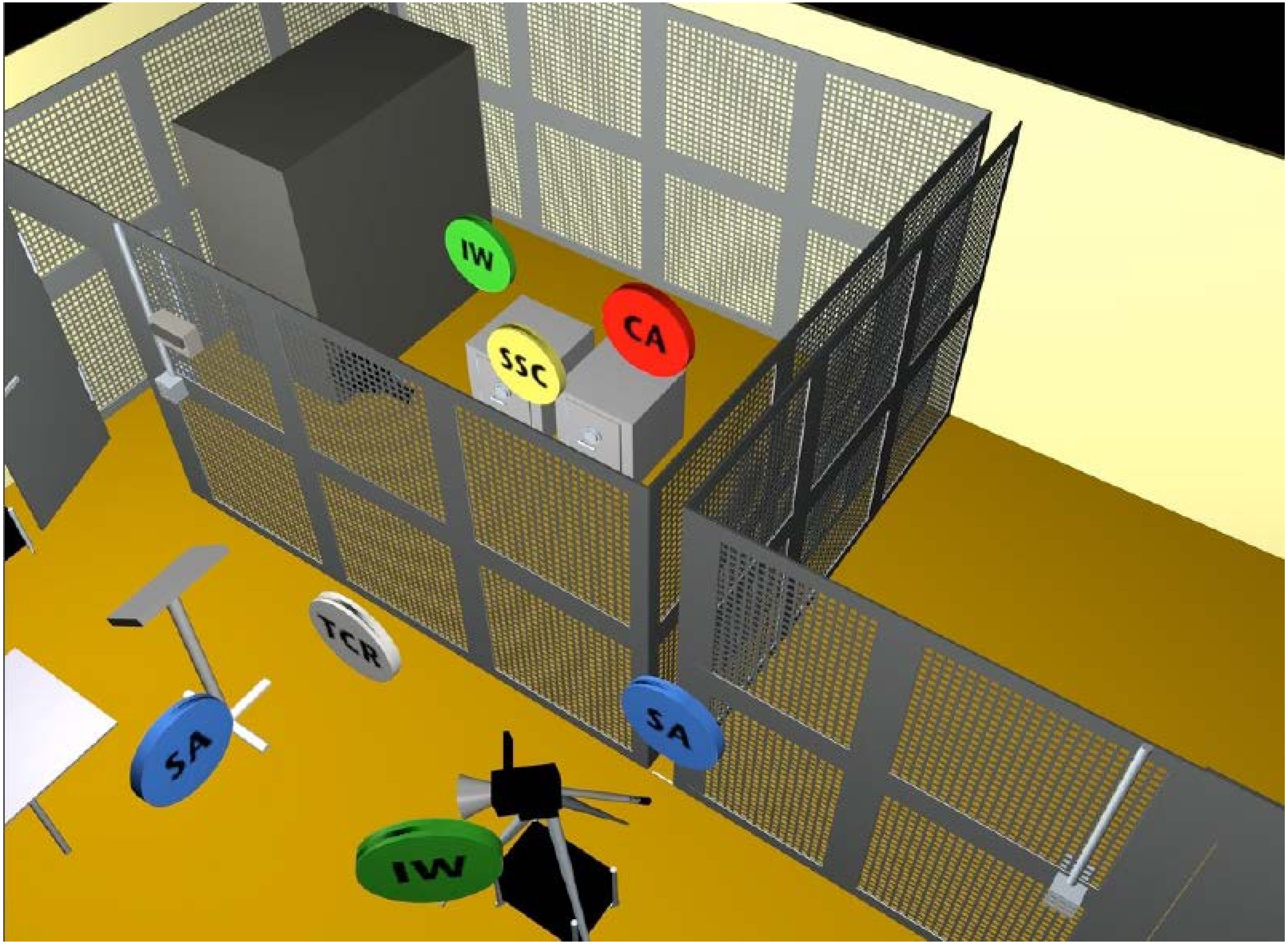
[illegible]

An implementation can be thi$

SysTrust

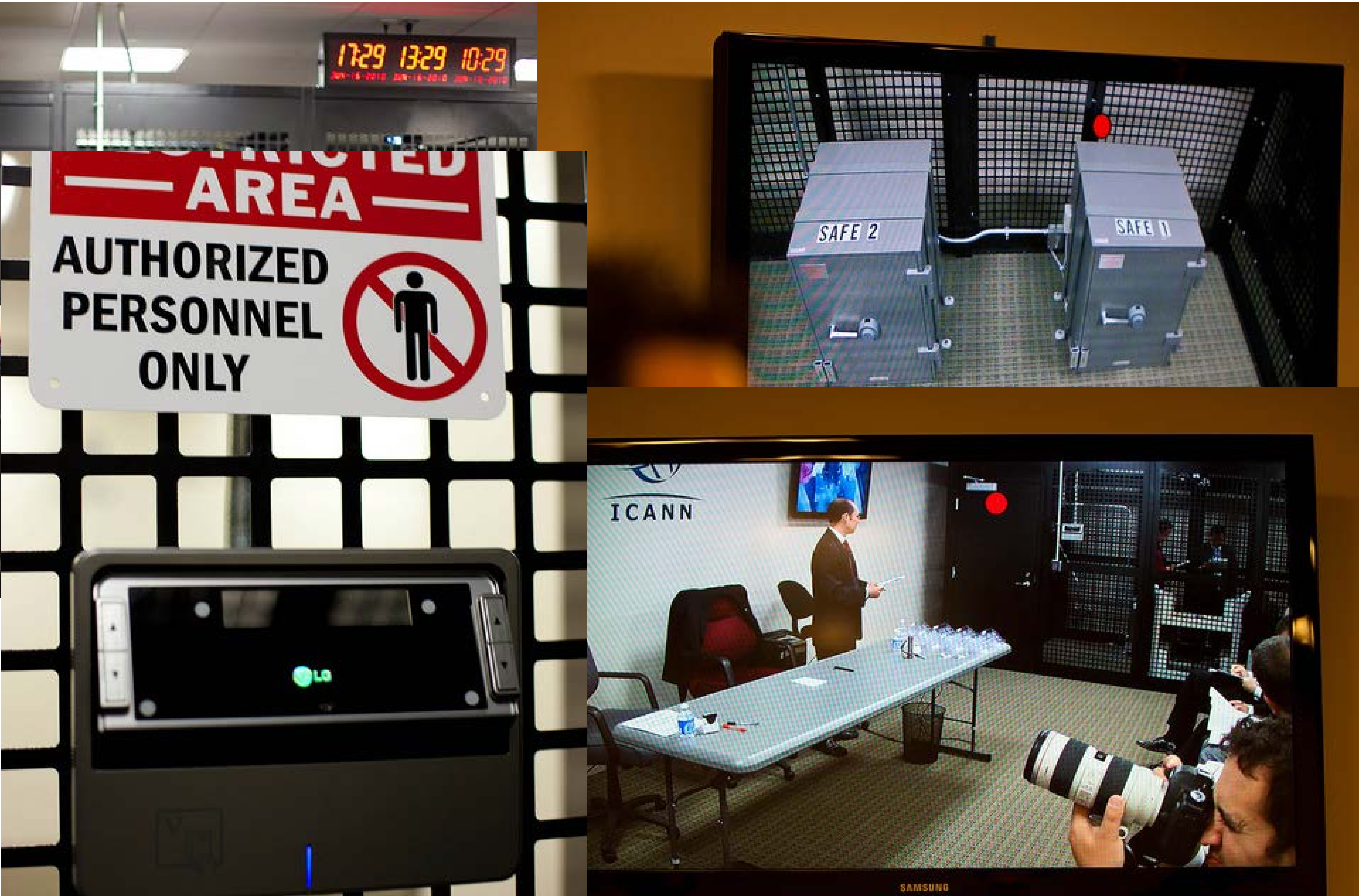
Physical Security

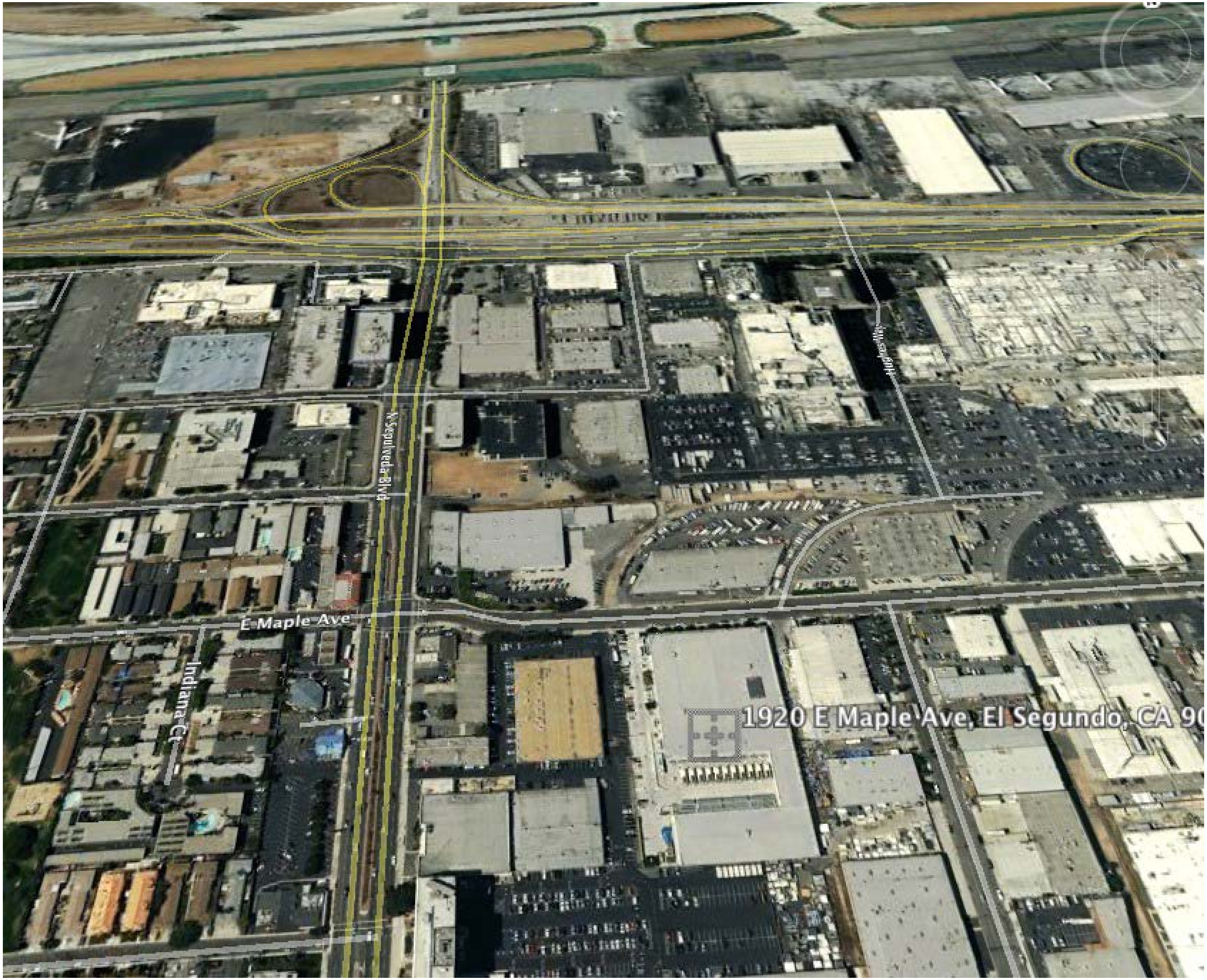




IW
CA
SSC
TCR
SA
SA
IW

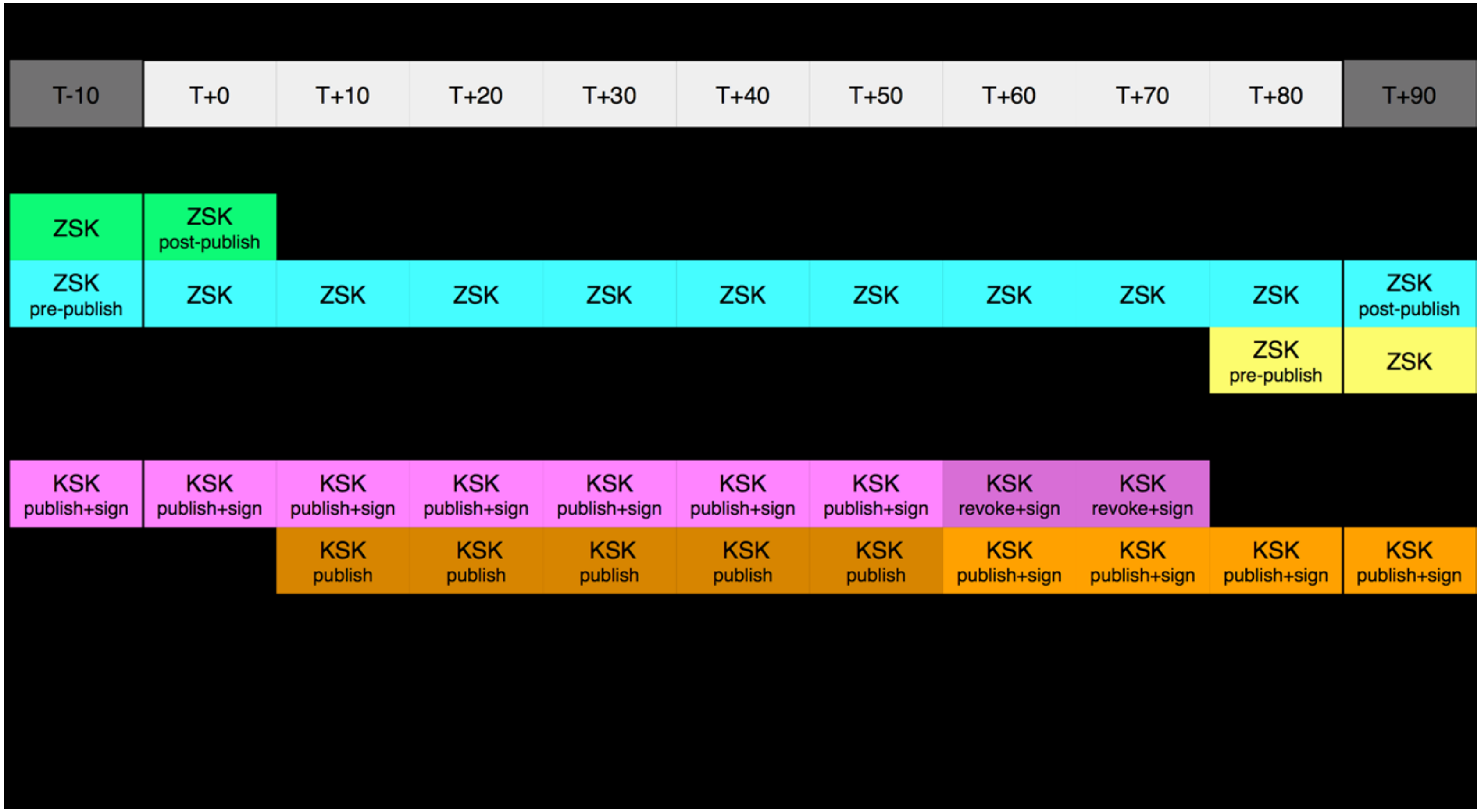
http://www.flickr.com/photos/kjd/sets/72157624302045698/




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

January 27, 2010

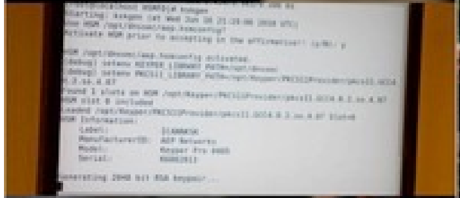
Key Rollover Schedule - Root



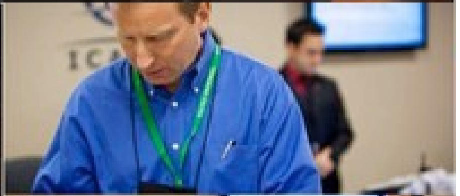
T-10	T+0	T+10	T+20	T+30	T+40	T+50	T+60	T+70	T+80	T+90
ZSK	ZSK post-publish									
ZSK pre-publish	ZSK	ZSK	ZSK	ZSK	ZSK	ZSK	ZSK	ZSK	ZSK	ZSK post-publish
									ZSK pre-publish	ZSK
KSK publish+sign	KSK publish+sign	KSK publish+sign	KSK publish+sign	KSK publish+sign	KSK publish+sign	KSK publish+sign	KSK revoke+sign	KSK revoke+sign		
		KSK publish	KSK publish	KSK publish	KSK publish	KSK publish	KSK publish+sign	KSK publish+sign	KSK publish+sign	KSK publish+sign

https://www.iana.org/dnssec

NOTICE
ALL EMPLOYEES AND VISITORS MUST WEAR IDENTIFICATION BADGES
NOTICE
UNAUTHORIZED PERSONS NOT PERMITTED BEYOND THIS POINT
NOTICE
NOTICE
NO FOOD OR DRINK BEYOND THIS POINT
NOTICE



```
root@localhost HSMS]# keygen
Starting: keygen (at Wed Jun 16 21:29:00 2010 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
Activate HSM prior to accepting in the affirmative!! (y/N): y

HSM /opt/dnssec/aep.hsmconfig activated.
[debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
[debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4
0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:           ICANNKSK
    ManufacturerID:  AEP Networks
    Model:           Keyper Pro 0405
    Serial:          K6002011

Generating 2048 bit RSA keypair...
```



19036

…or this

FIPS 140-2 Valid

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
uct identified as:

Athena IDProtect by Athen
AT90SC25672RCT Revision D; I

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

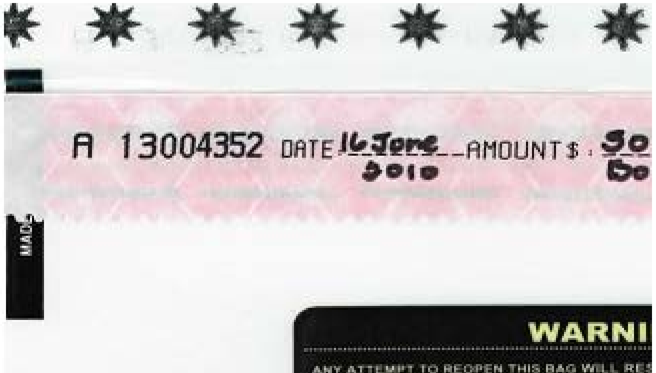
Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

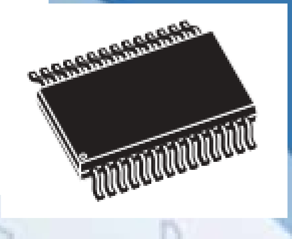
Signature:

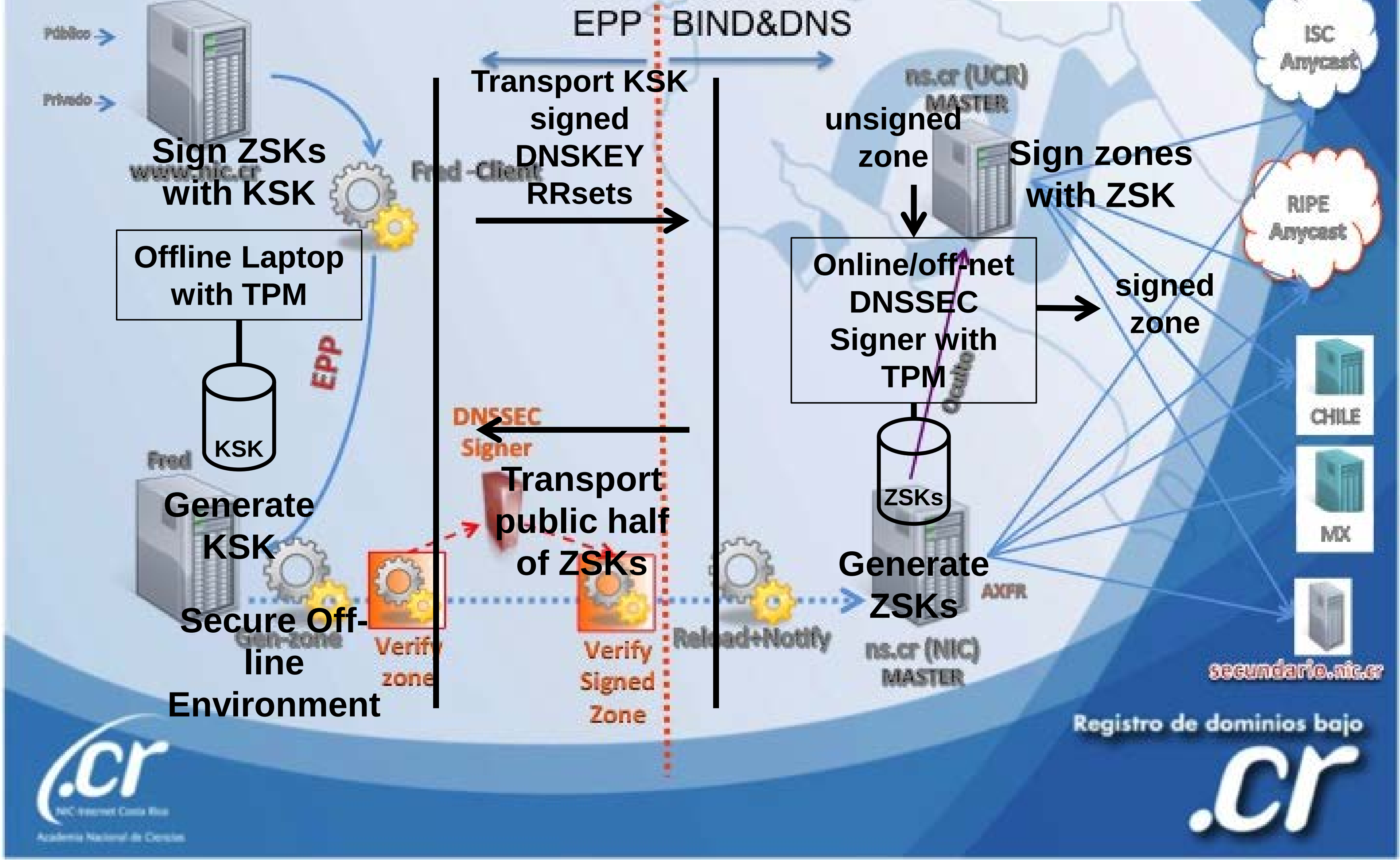
Dated: 20 March 2008

A/ Director, Industry Program Group
Communications Security Establishment


A 13004352 DATE 16 June 2010 AMOUNT $ 50 00
MADE
WARNI
ANY ATTEMPT TO REOPEN THIS BAG WILL RES

..or this (from .cr)





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

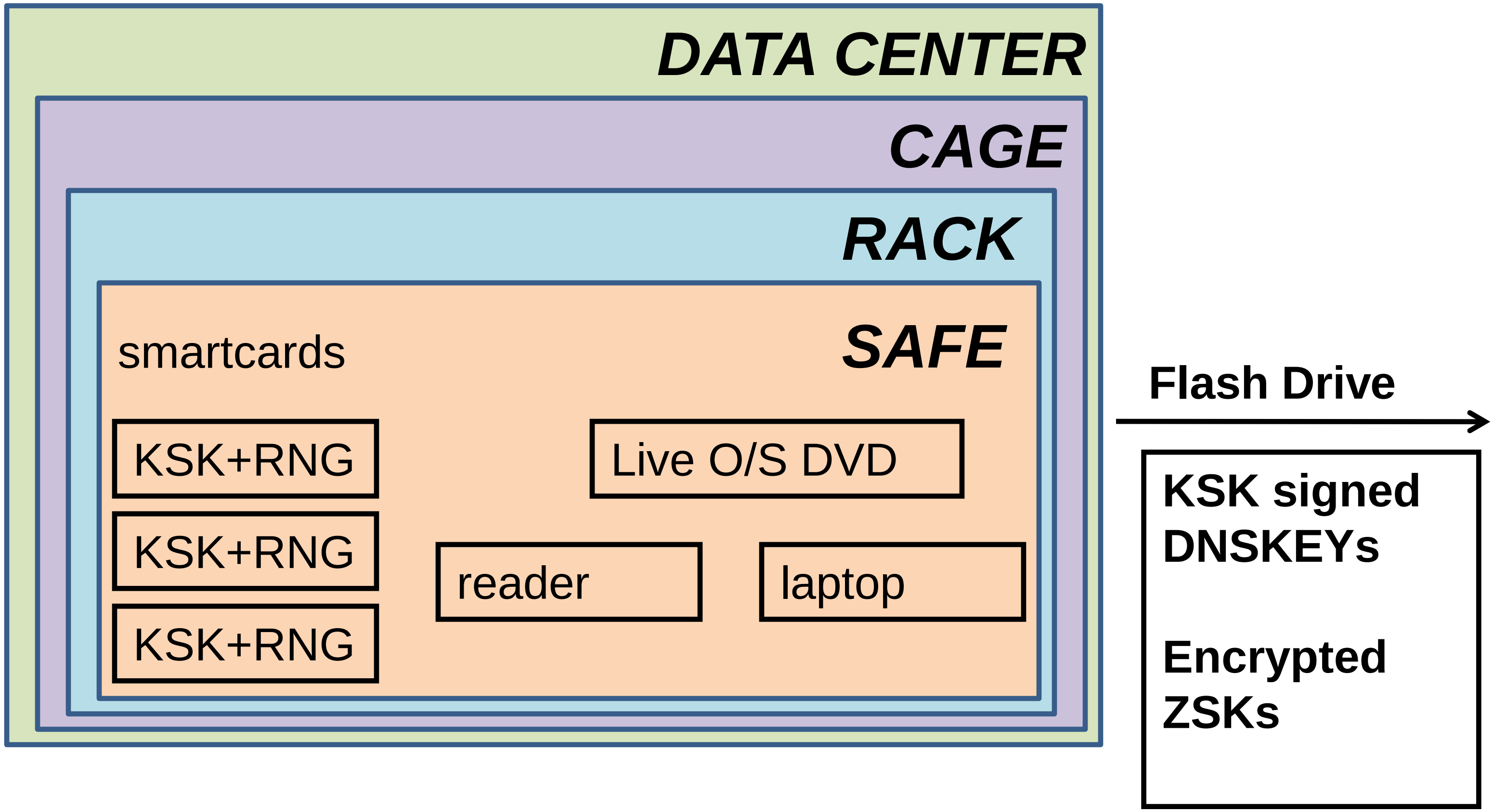
ZSKs

Generate ZSKs

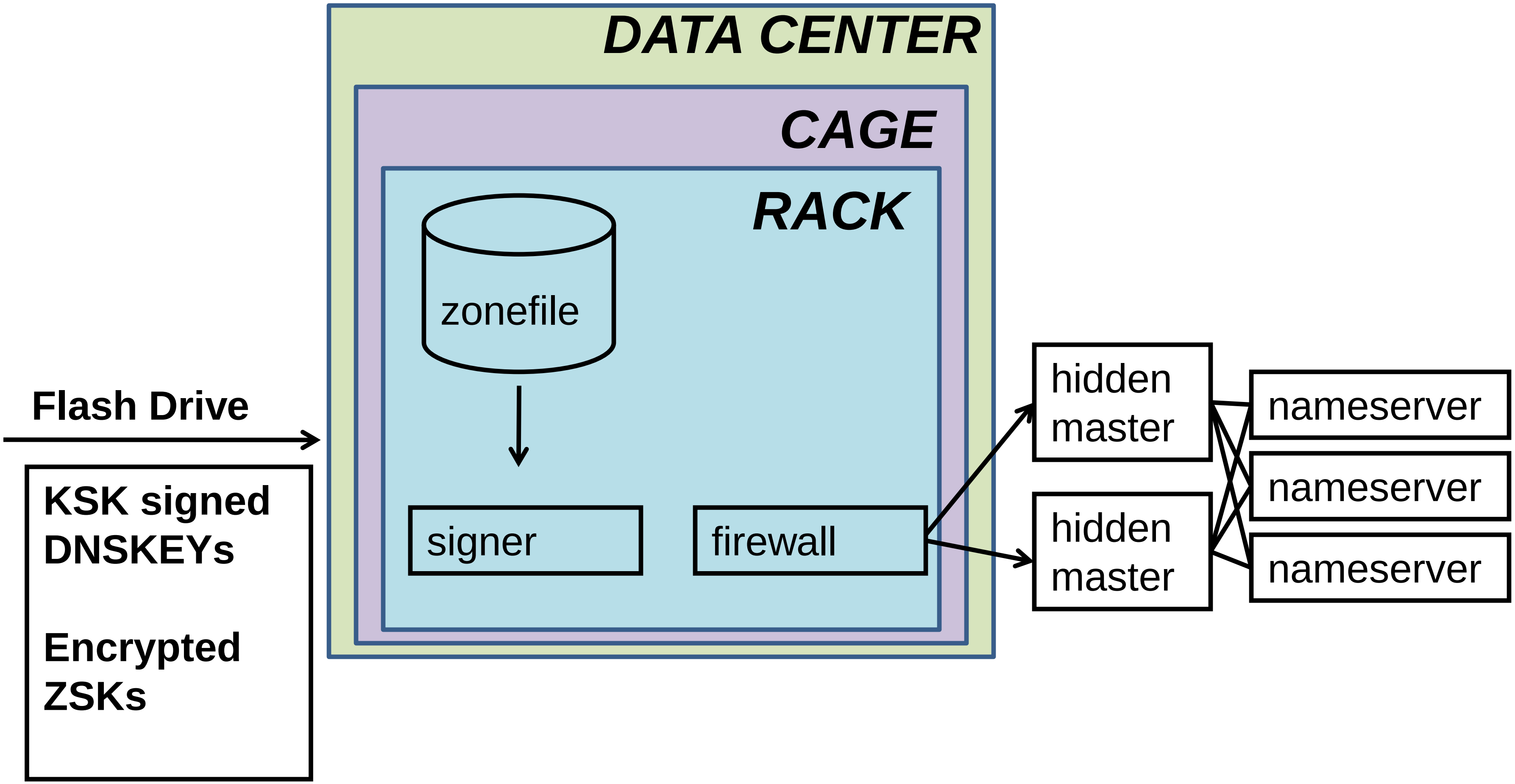
Demo Implementation

- Key lengths – KSK:2048 RSA ZSK:1024 RSA
- Rollover – KSK:as needed ZSK:90 days
- RSASHA256 NSEC3
- Physical – HSM/smartcards inside Safe inside Rack inside Cage inside Commercial Data Center
- Logical – Separation of roles: cage access, safe combination, HSM/smartcard activation across three roles
- Crypto – use FIPS certified smartcards as HSM and RNG
  - Generate KSK and ZSK offline using RNG
  - KSK use off-line
  - ZSK use off-net

Off-Line Key generator and KSK Signer



Off-Net Signer



DATA CENTER

CAGE

RACK

zonefile

signer

firewall

Flash Drive

KSK signed
DNSKEYs

Encrypted
ZSKs

hidden
master

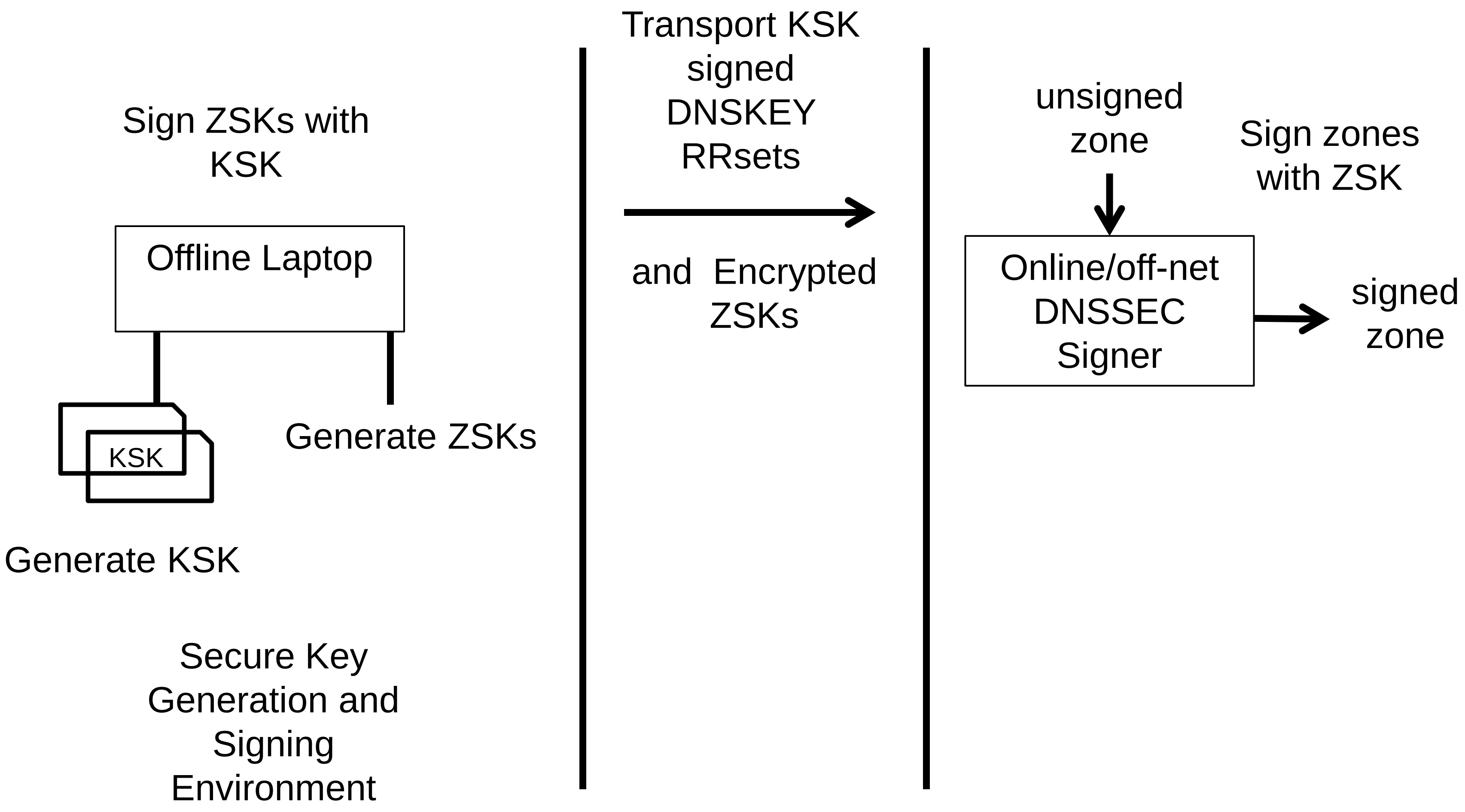
hidden
master

nameserver

nameserver

nameserver

Key Management



Sign ZSKs with KSK

Offline Laptop

KSK

Generate KSK

Generate ZSKs

Secure Key Generation and Signing Environment

Transport KSK signed DNSKEY RRsets

and Encrypted ZSKs

unsigned zone

Sign zones with ZSK

Online/off-net DNSSEC Signer

signed zone