



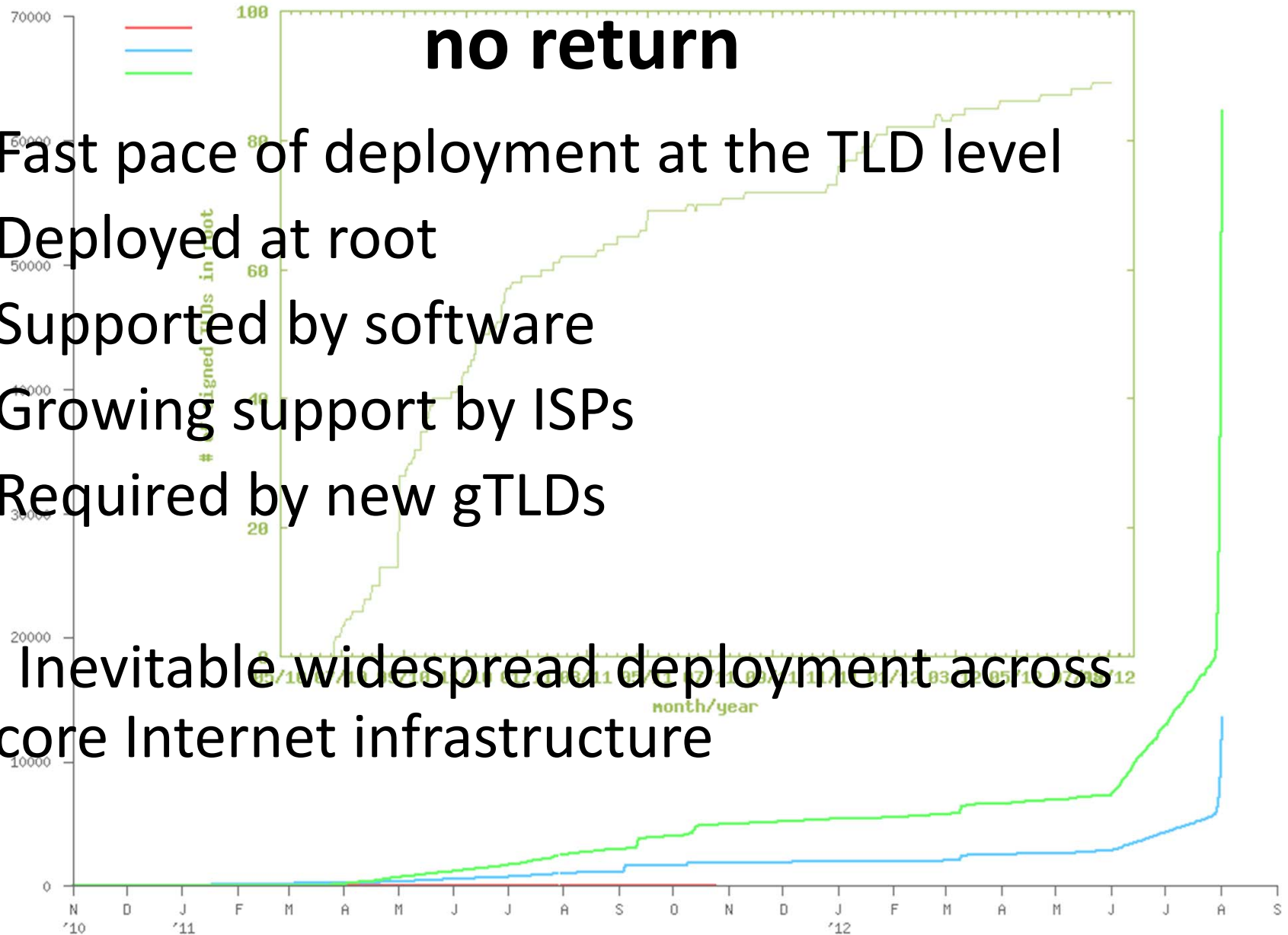
# DNSSEC Implementation Considerations and Risk Analysis

Midrand, South Africa  
8-10 July 2015  
[richard.lamb@icann.org](mailto: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



# Design Considerations

**How do I sign a zone?**

# That's it

**dnssec-signzone mydomain.zone mydomain.zone.signed**

```
www.abc.com. IN A 192.101.186.125
```

```
www.abc.com. IN A 192.101.186.125
```

```
IN RRSIG A 8 3 3600
```

```
20130926030000 20130909030000 32799
```

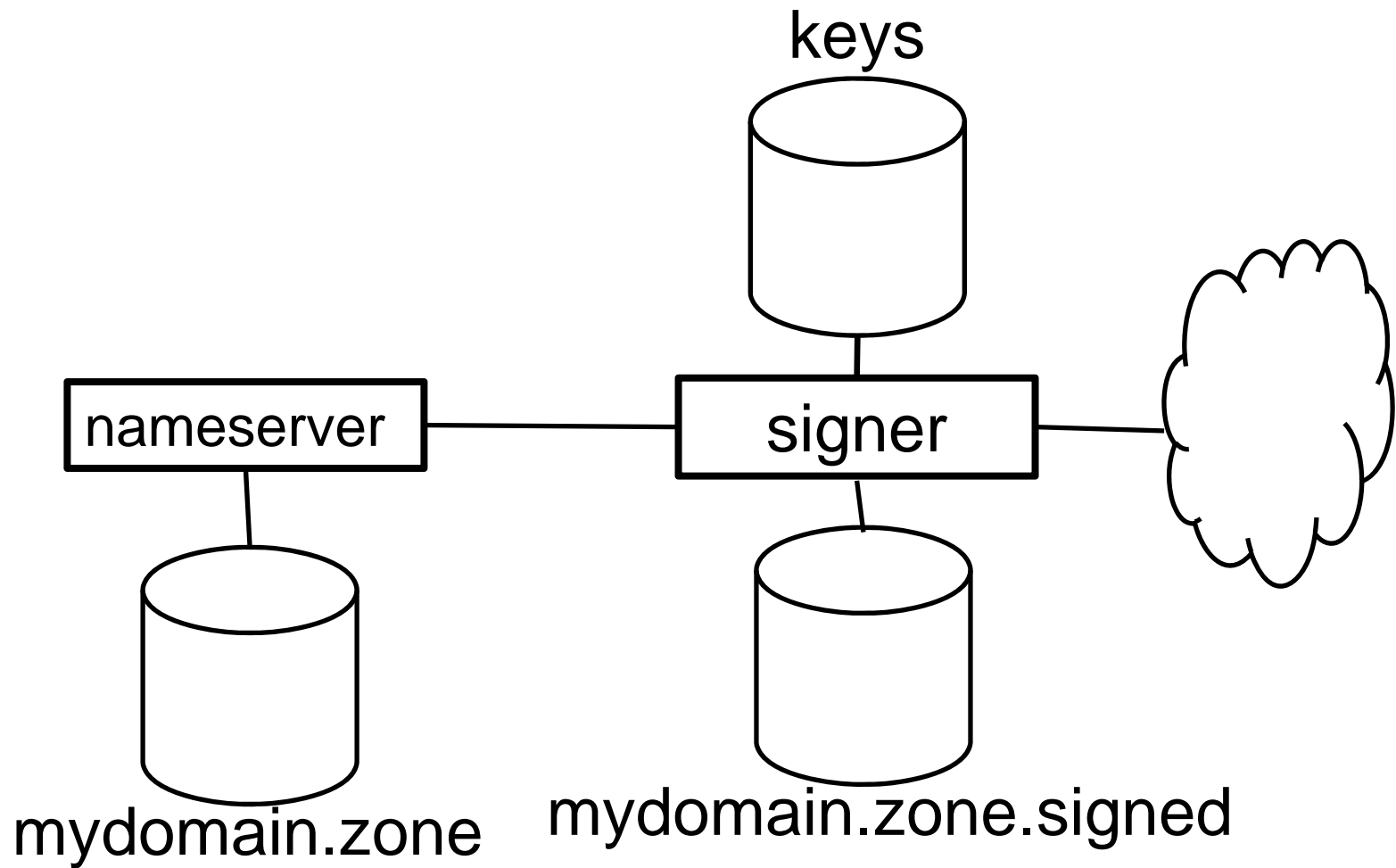
```
www.abc.com. N7upFHNplnIiXAEMOTefeuJrwymNxF
```

```
8D6/poAoRVDThHVOnXniaIj2WuGVbCGvUMjayDhVNk9
```

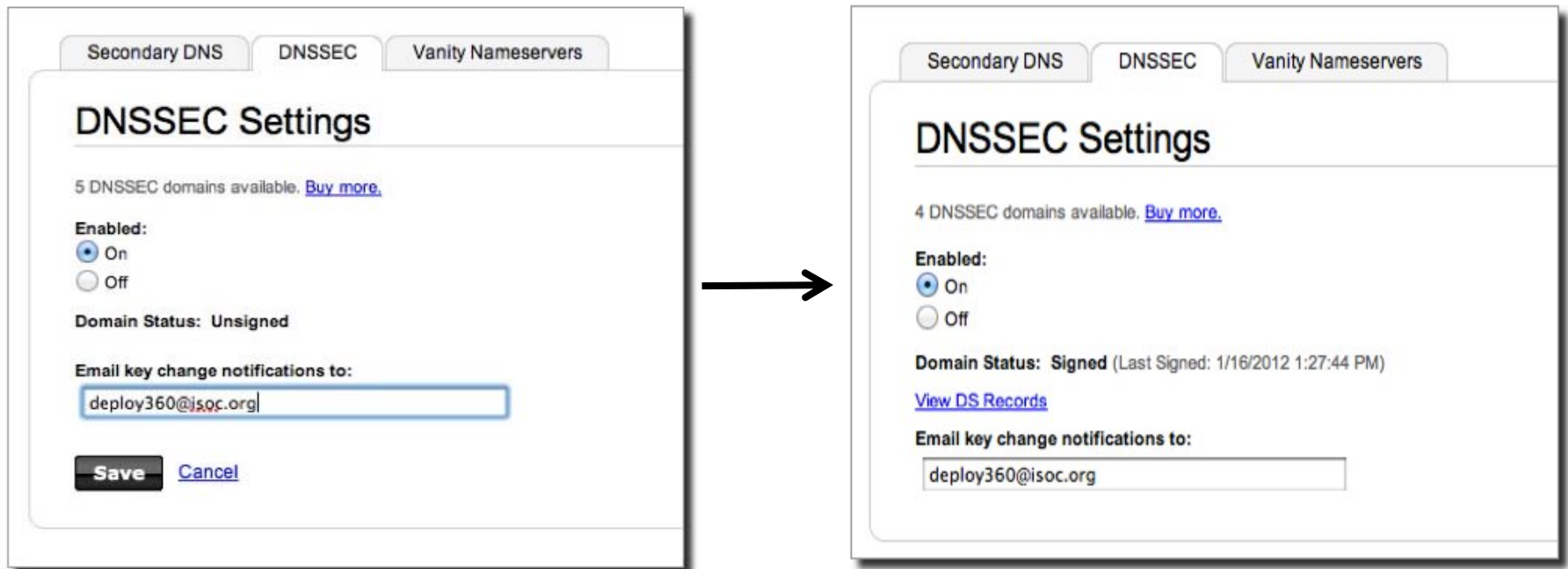
```
vAQtVHUIAnxZXsIlP4ZbtIgtZ/hbTKByySx1Y0u9aRD
```

```
lik=
```

# One way to do this



# or...another



<http://www.internetsociety.org/deploy360/resources/how-to-sign-your-domain-with-dnssec-using-godaddy-com/>

It's a question of risk / trust,  
but it does not have to be expensive



# 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](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



- The bad:
  - Diluted trust with a race to the bottom (>1400 CA's)
  - DigiNotar
    - Weak and inconsistent policies and controls
    - Lack of compromise notification (non-transparent)
    - Audits don't solve everything (ETSI audit)





# 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

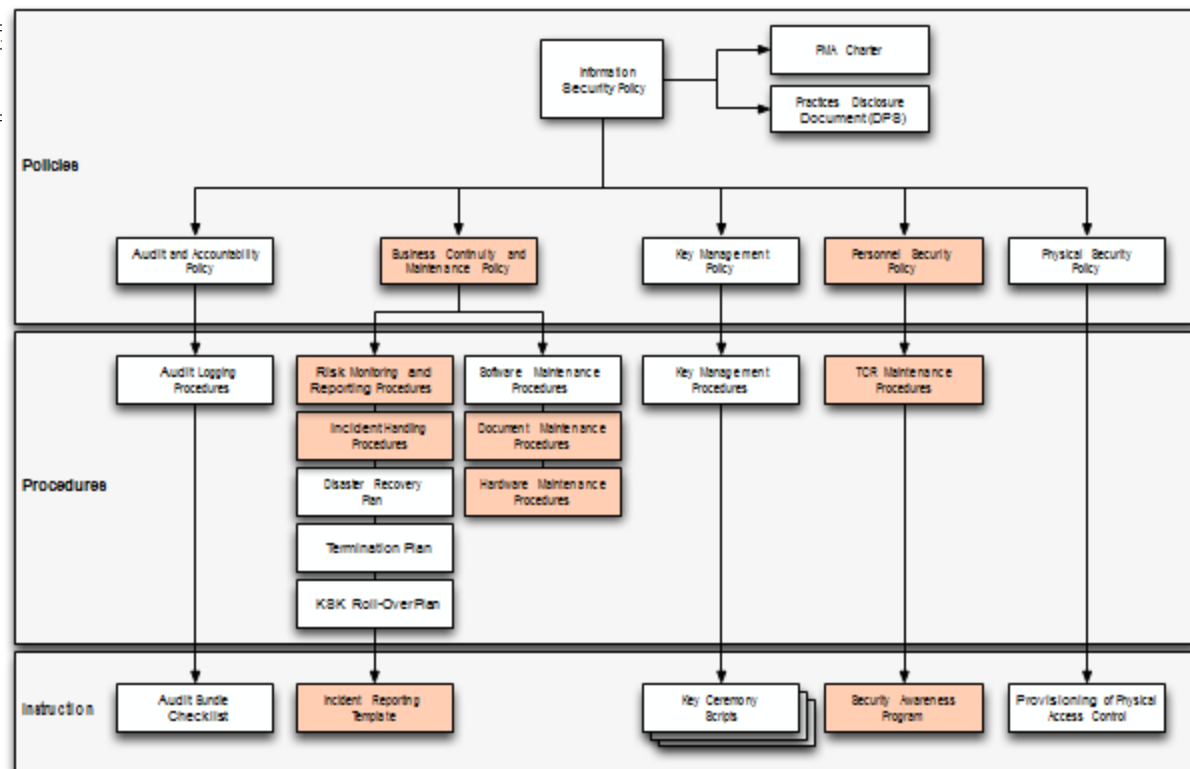
This document is the DNSSEC Practice Statement (DPS) for the Root Zone Key Signing Key (KSK) Operator. It states the practices and provisions that are used to provide Root Zone Key Signing and Key Distribution services. These include, issuing, managing, changing and distributing with the specific requirements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

Copyright Notice

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

91 Pages and  
tree of other  
documents!

## Root DPS



# Documentation - .SE

---

- Security
- Documentation
- DNSSEC
- Practice Statement (DPS)

22 pages, Creative Commons License!

Most recently saved: 22 april 2010



Licensed under a [Creative Commons License](#)

The Internet Infrastructure Foundation  
PO Box 7306, SE-163 81 Stockholm, Sweden Tel +46(0)8-433 36 00 Fax +46(0)8-432 36 02 VAT no SE800404318301 [www.iif.se](http://www.iif.se)

**.se**

**.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

- 3<sup>rd</sup> 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

# Building in security

- Getting the machinery for DNSSEC is easy (BIND, NSD/Unbound, OpenDNSSEC, etc..).
- Finding good security practices to run it is not.

# 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 – Tamper Evident Packaging

Print

DO NOT CUT. HERE TO OPEN **DIEBOLD** DO NOT CUT. HERE TO OPEN **DIEBOLD** DO NOT CUT. HERE TO OPEN **DIEBOLD** DO NOT CUT. HERE TO OPEN **DIEBOLD**

**STOP**

This bag uses a custom, tamper-evident sealing tape. Evidence of tampering may include:

- ✓ Appearance of the words "VOID" in the tape.
- ✓ Appearance of dark red in the heat indicator strip.
- ✓ Stretching or distortion of the tape or any pre-printed area of the bag or seal.

**STOP**

**IF THERE IS ANY EVIDENCE OF TAMPERING, DO NOT OPEN BAG. CONTACT SENDER IMMEDIATELY.**

FROM: BB 501437

Customer Name/Account Number \_\_\_\_\_  
 Store Location/Number \_\_\_\_\_  
 Date \_\_\_\_\_  
 Cash \_\_\_\_\_  
 Checks \_\_\_\_\_  
 Other \_\_\_\_\_

**DEPOSIT SAID TO CONTAIN:**

Participating Bank: \_\_\_\_\_  
 Branch: \_\_\_\_\_  
 Account #: \_\_\_\_\_  
 Date: \_\_\_\_\_

Instructions: At the end of each deposit slip, print name, branch name, date, time, and phone area code.

**INSTRUCTIONS**

- 1 Complete information using a ballpoint pen. Use of metal styluses or tag pen may void your receipt.
- 2 Insert receipt into slot.
- 3 Rotate rollers to engage receipt with tag.
- 4 Press this bag into slot until it seals.

Account #: \_\_\_\_\_  
 Date: \_\_\_\_\_

**is A DIEBOLD**

version 1.0 Page 1 of 18

ITEM # 80051001000A

TO REMOVE CONTENTS - CUT ALONG DASHED LINE

12-11

# 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*

<b>Recommended Minimum Cryptographic Strength for DNSSEC</b>			
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](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 commonplace

# 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
  - Ultimaco
- 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.opendssec.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 ~\$12)
  - AthenaSC IDProtect ~\$30
  - Feitian ~\$5-10
  - Aventura ~\$11
- TPM
  - Built into many PCs
- Token
  - Aladdin/SafeNet USB e-Token ~\$50
- Open source PKCS11 Drivers available
  - OpenSC
- Has RNG
- Slow ~0.5-10 1024 RSA signatures per second

# Crypto -Random Number Generator

X rand()

X Netscape: Date+PIDs

✓ LavaRand

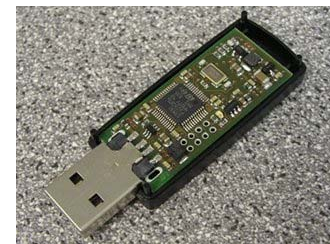
? System Entropy (/dev/random-urandom)

? H/W, Quantum Mechanical (laser) \$\$

✓ Standards based (FIPS, NIST 800-90 DRBG)

✓ Built into CPU chips

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



# Crypto - FIPS 140-2 Level 4 HSM

Root, .FR, .CA ...



# 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



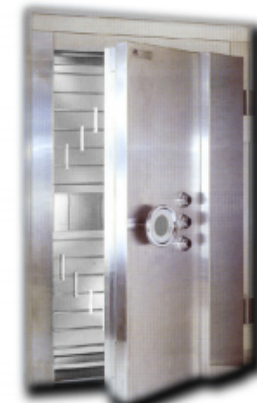
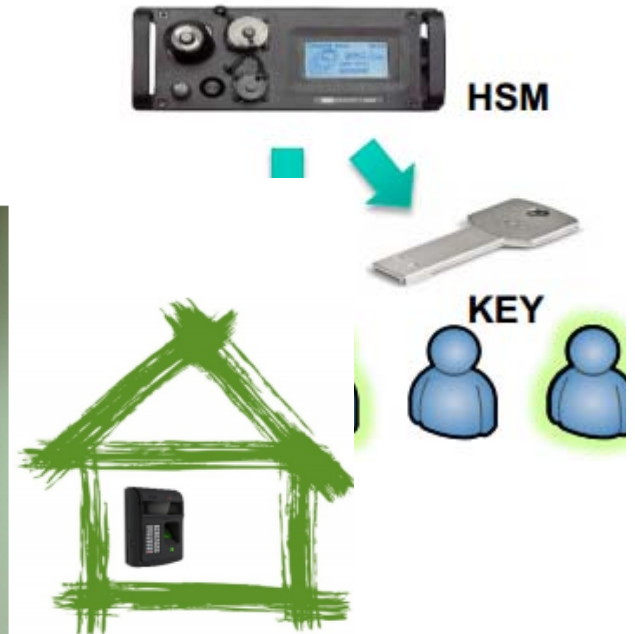
# An implementation can be thi\$



# ...or this

## Physical Security

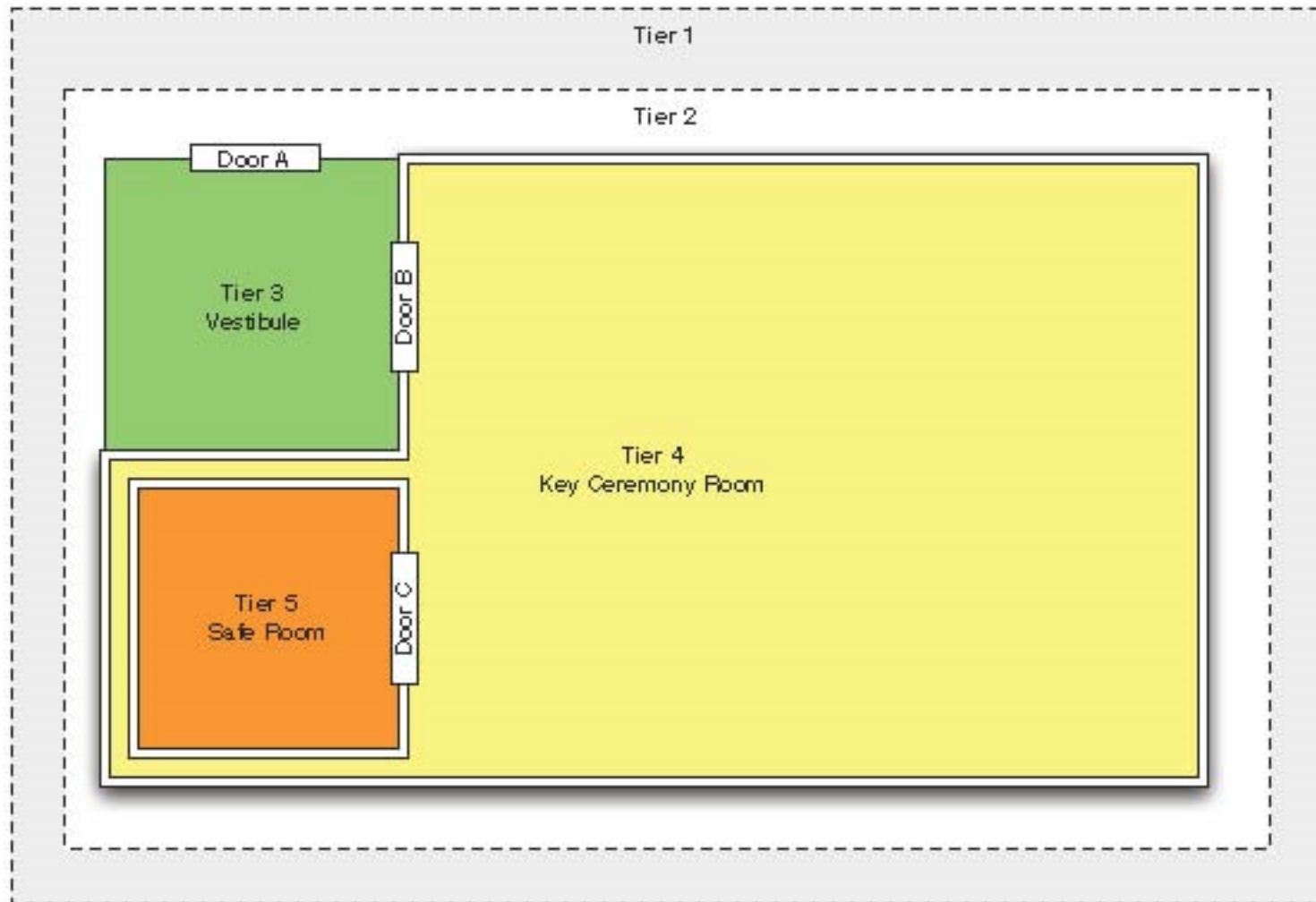
- An electromagnetic shielding datacenter ( following GJBz20219-94 “C” level of PRC) is being used, and only authorized persons may access
- HSMs and hidden master servers are kept in the electro-magnetic shielding datacenter
- A backup system is established in disaster datacenter in Chengdu, with the same security insurance level as that of Beijing

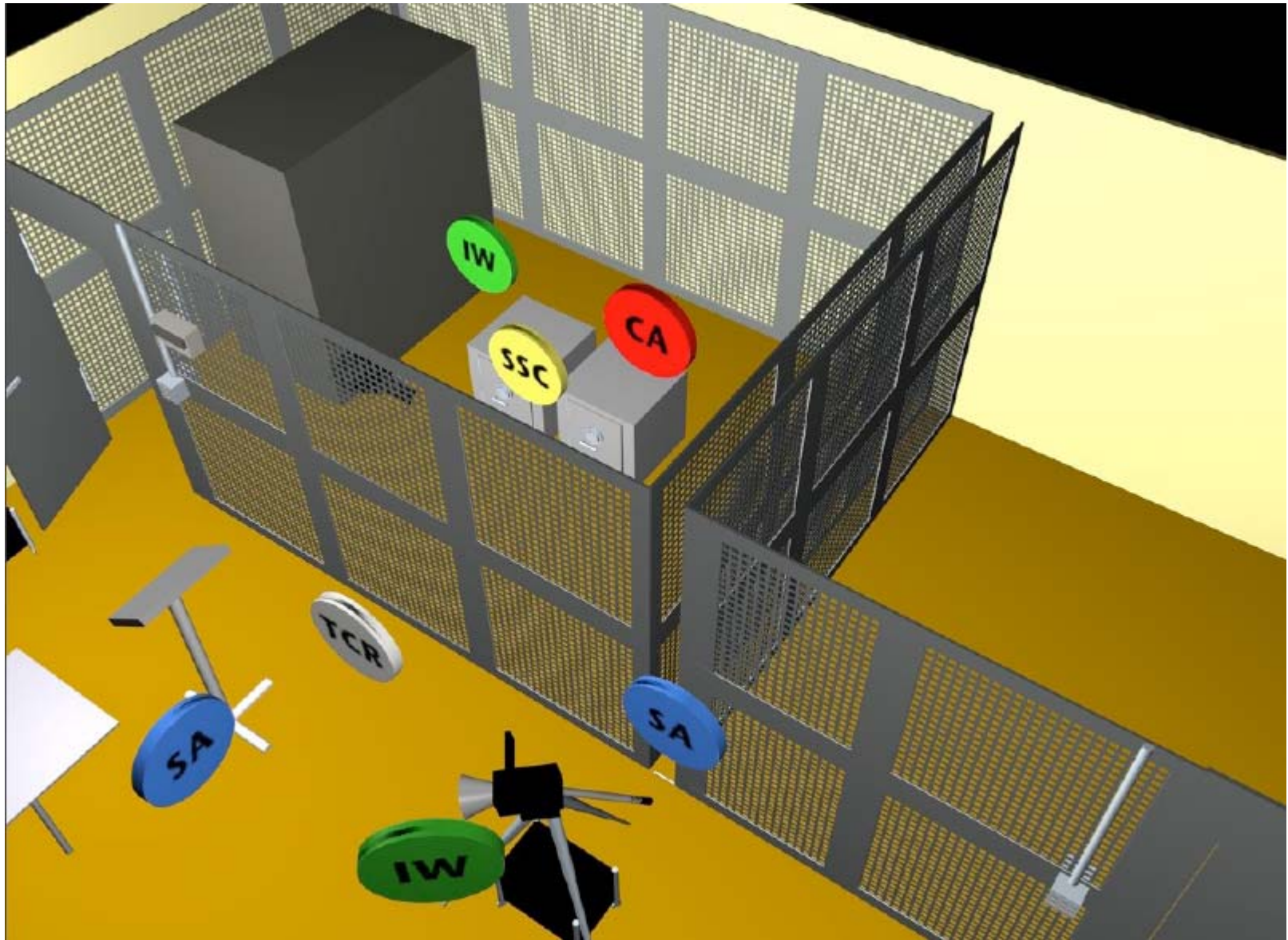


<http://singapore49.icann.org/en/schedule/wed-dnssec/presentation-dnssec-deployment-cn-26mar14-en.pdf>



# Physical Security

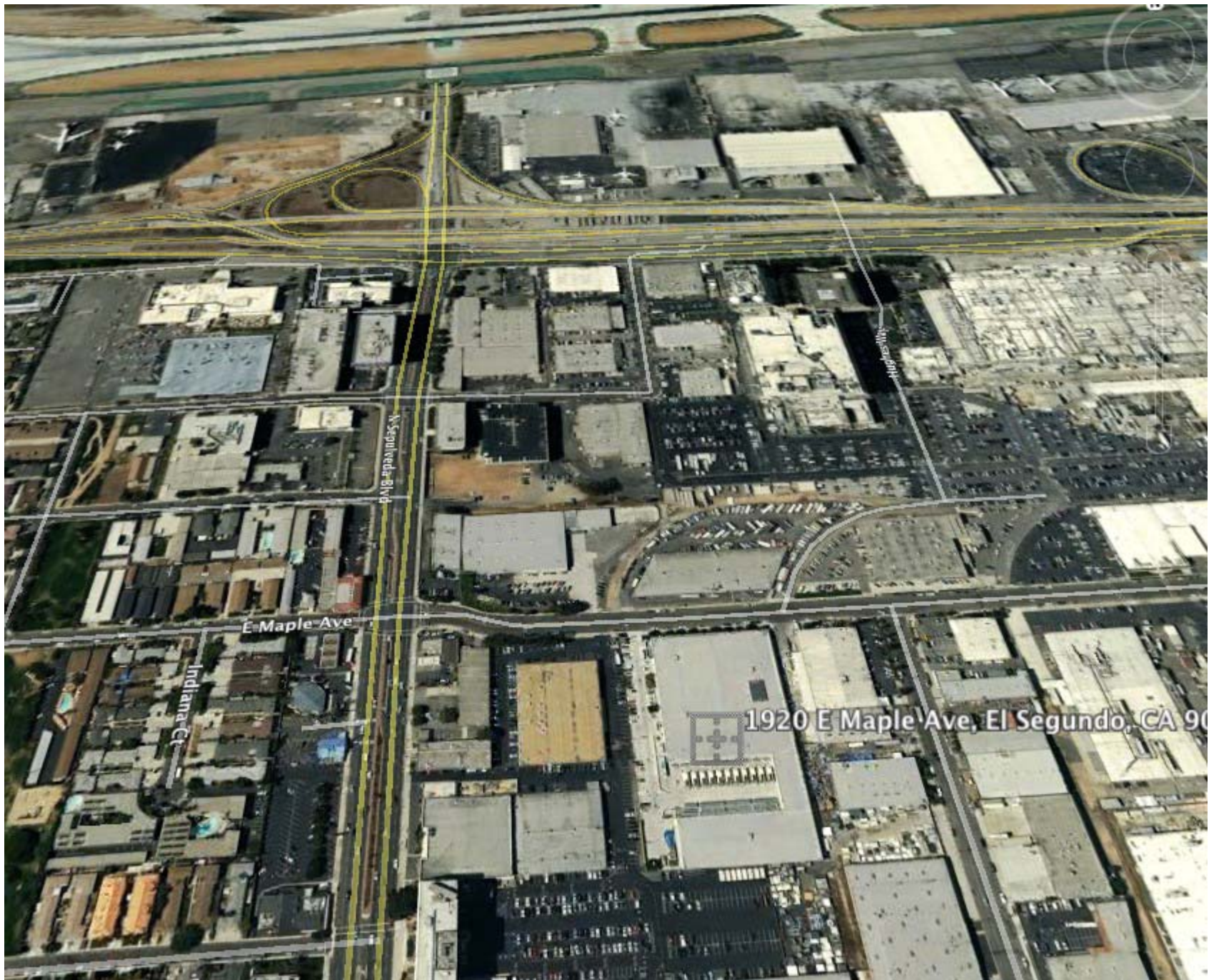




<http://www.flickr.com/photos/kjd/sets/72157624302045698/>







1920 E Maple Ave, El Segundo, CA 90



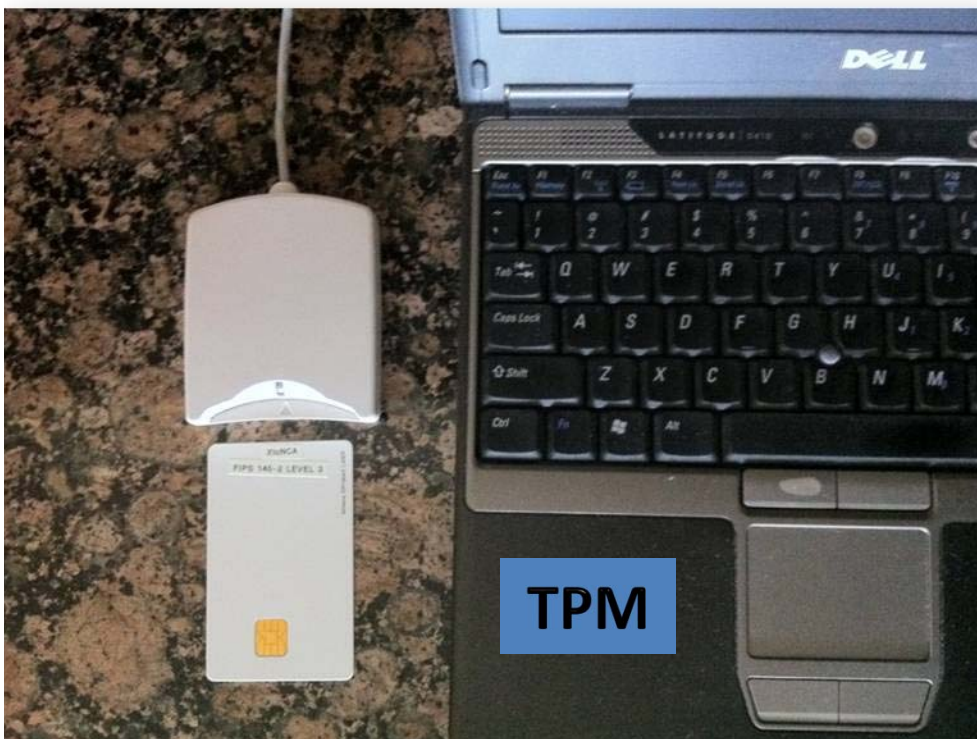








...or this



TPM



FIPS 140-2 Valid



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  
act identified as:

Athena IDProtect by Athen  
'AT90SC2567RCT Revision D) f

ting accredited laboratory: Inf  
DF

- Level 3
- Level 3
- Level 4
- Level 3
- Level 3
- Level N/A



Cryptographic Key Management:	Level 3
Self-Tests:	Level 3
Mitigation of Other Attacks:	Level 3
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 C. Barker*

Dated: *March 31, 2008*

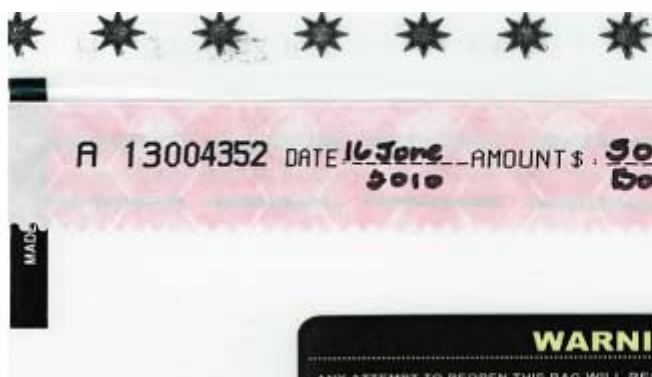
Chief, Computer Security Division  
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

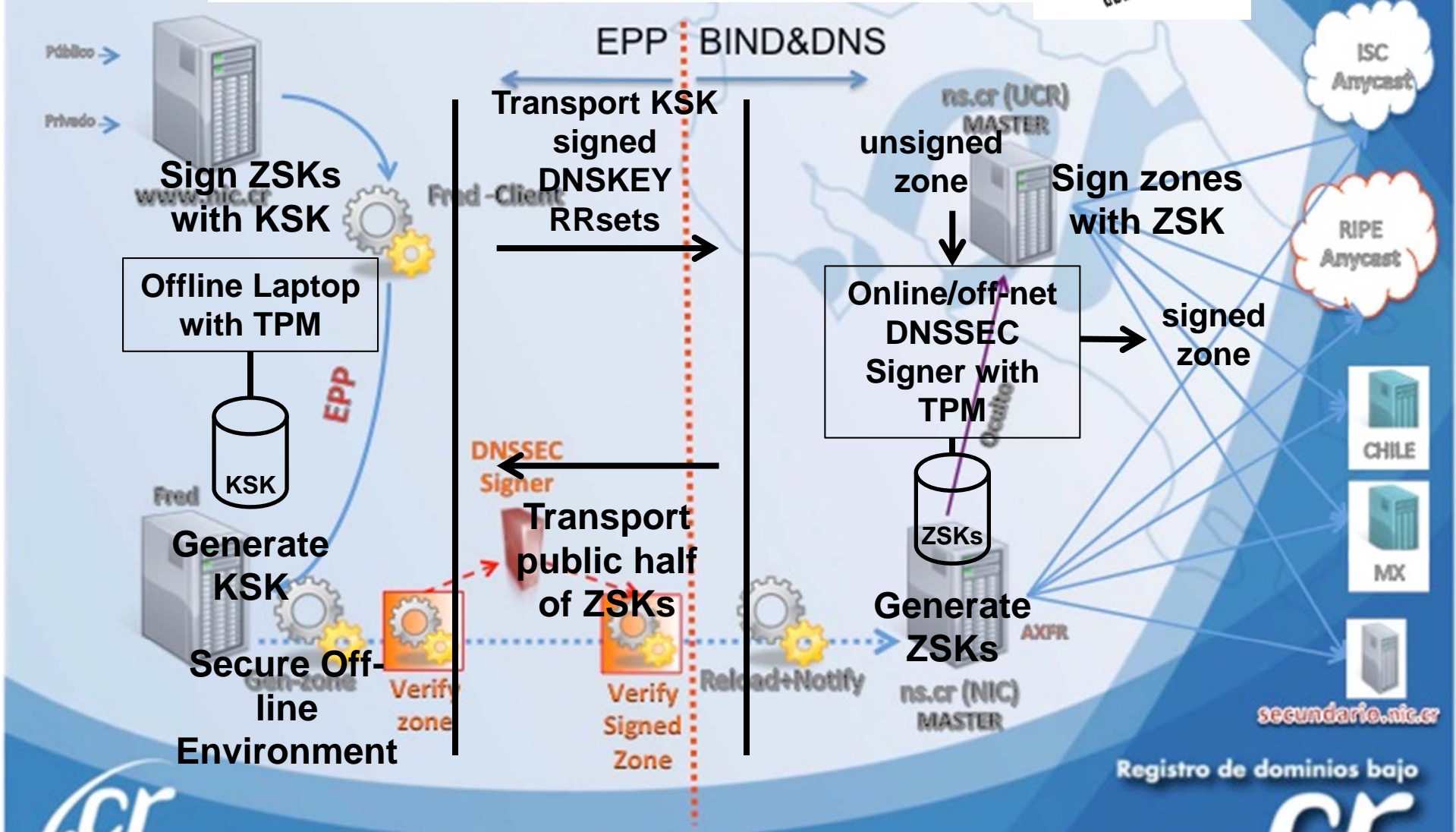
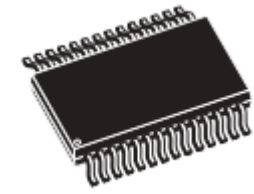
Signature: *[Signature]*

Dated: *30 March 2008*

Director, Industry Program Group  
Communications Security Establishment

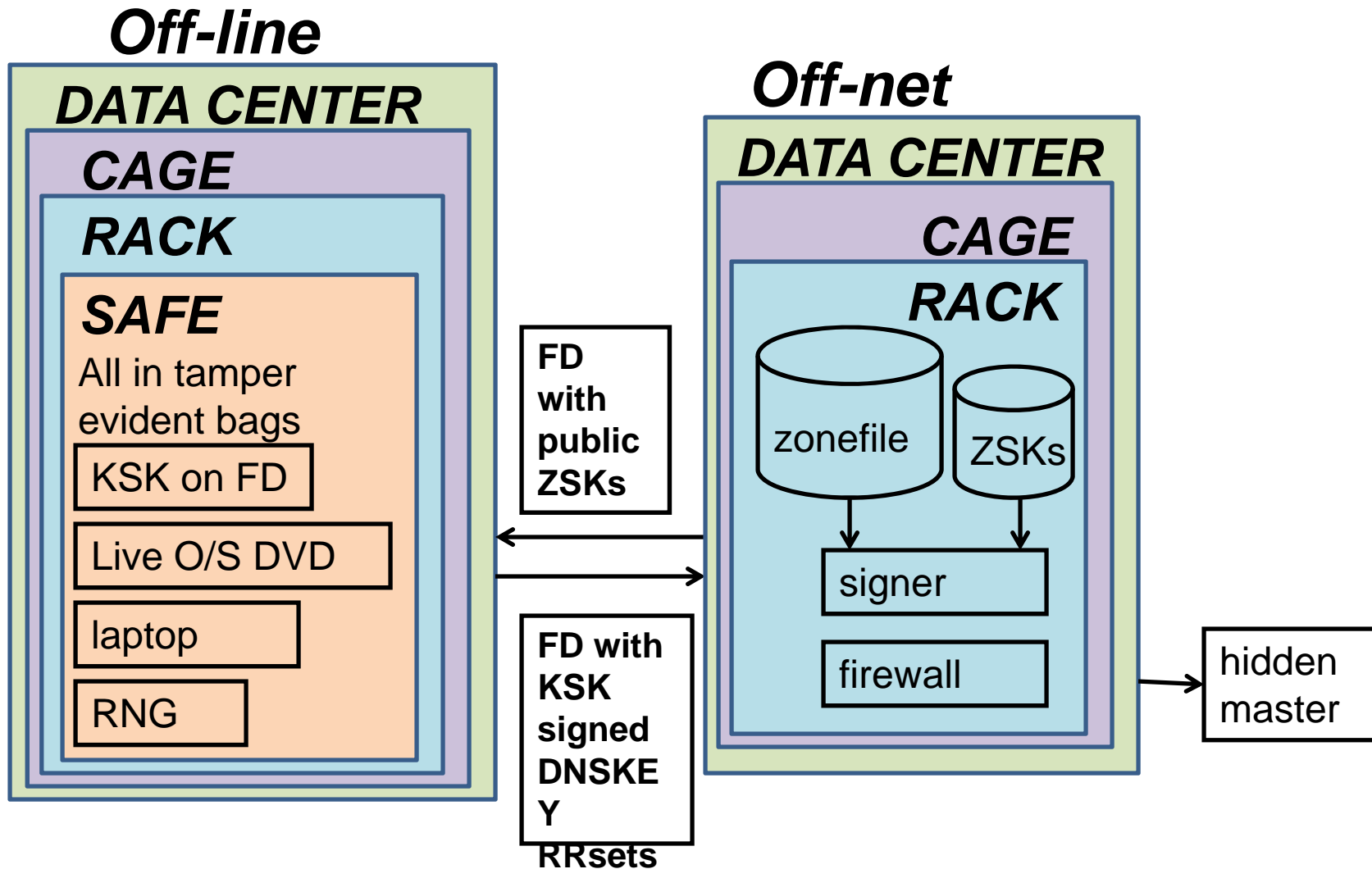


# ..or this (from .cr)



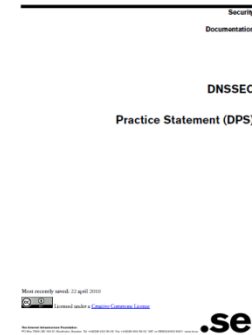


# ...or even this



# But all must have:

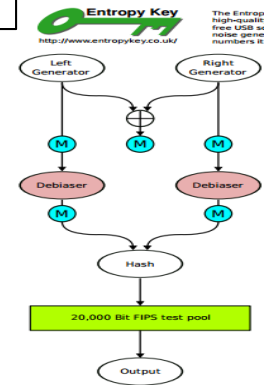
- Published practice statement
  - Overview of operations
  - Setting expectations
    - Normal
    - Emergency
  - Limiting liability
- Documented procedures
- Multi person access requirements
- Audit logs
- Monitoring (e.g., for signature expiry)
- Good Random Number Generators



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

Intel RdRand

DRBGs  
FIPS 140



Useful IETF RFCs:

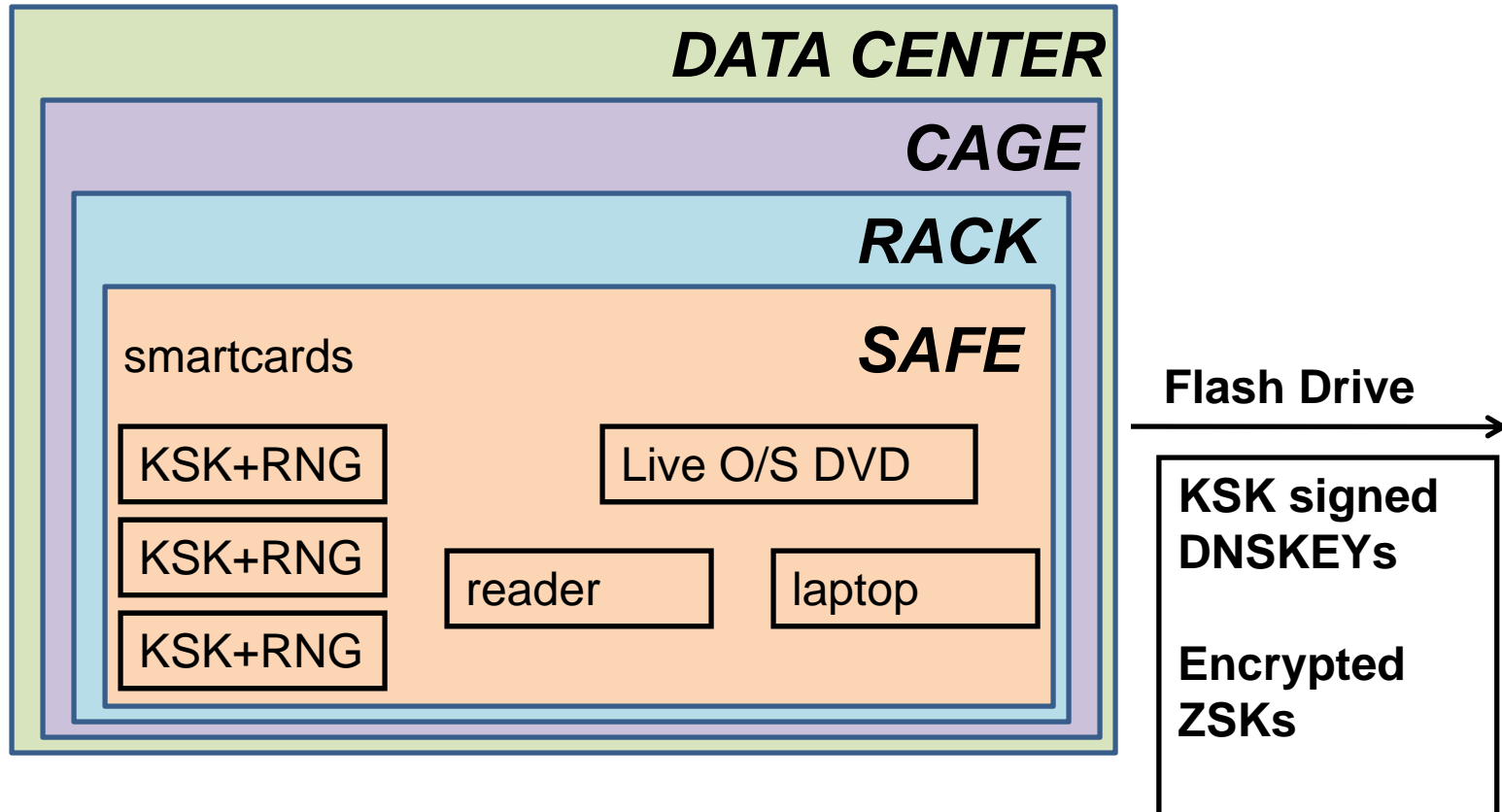
DNSSEC Operational Practices <http://tools.ietf.org/html/draft-ietf-dnsop-rfc4641bis>

A Framework for DNSSEC Policies and DNSSEC Practice Statements <http://tools.ietf.org/html/draft-ietf-dnsop-dnssec-dps-framework>

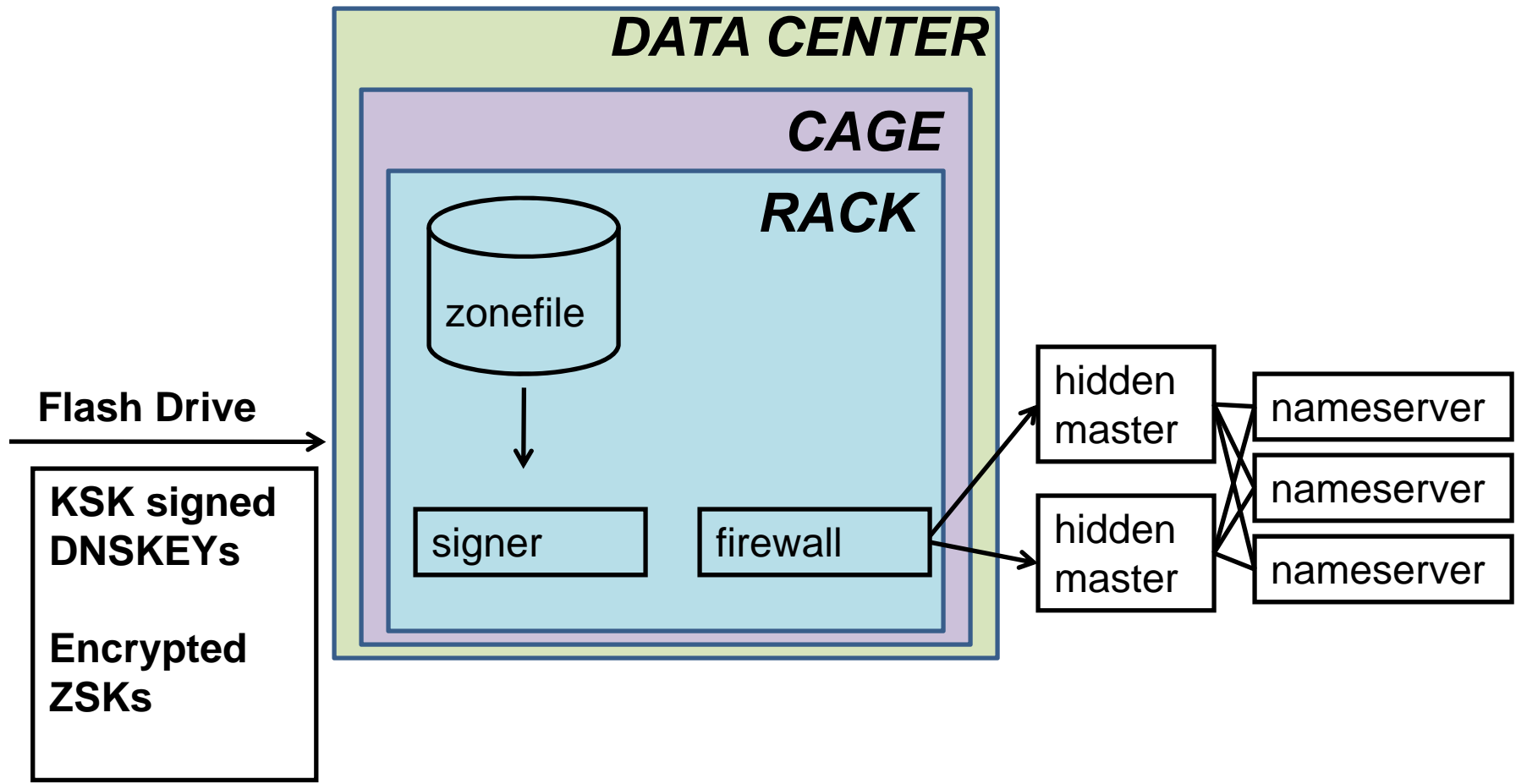
# Demo Implementation

- 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

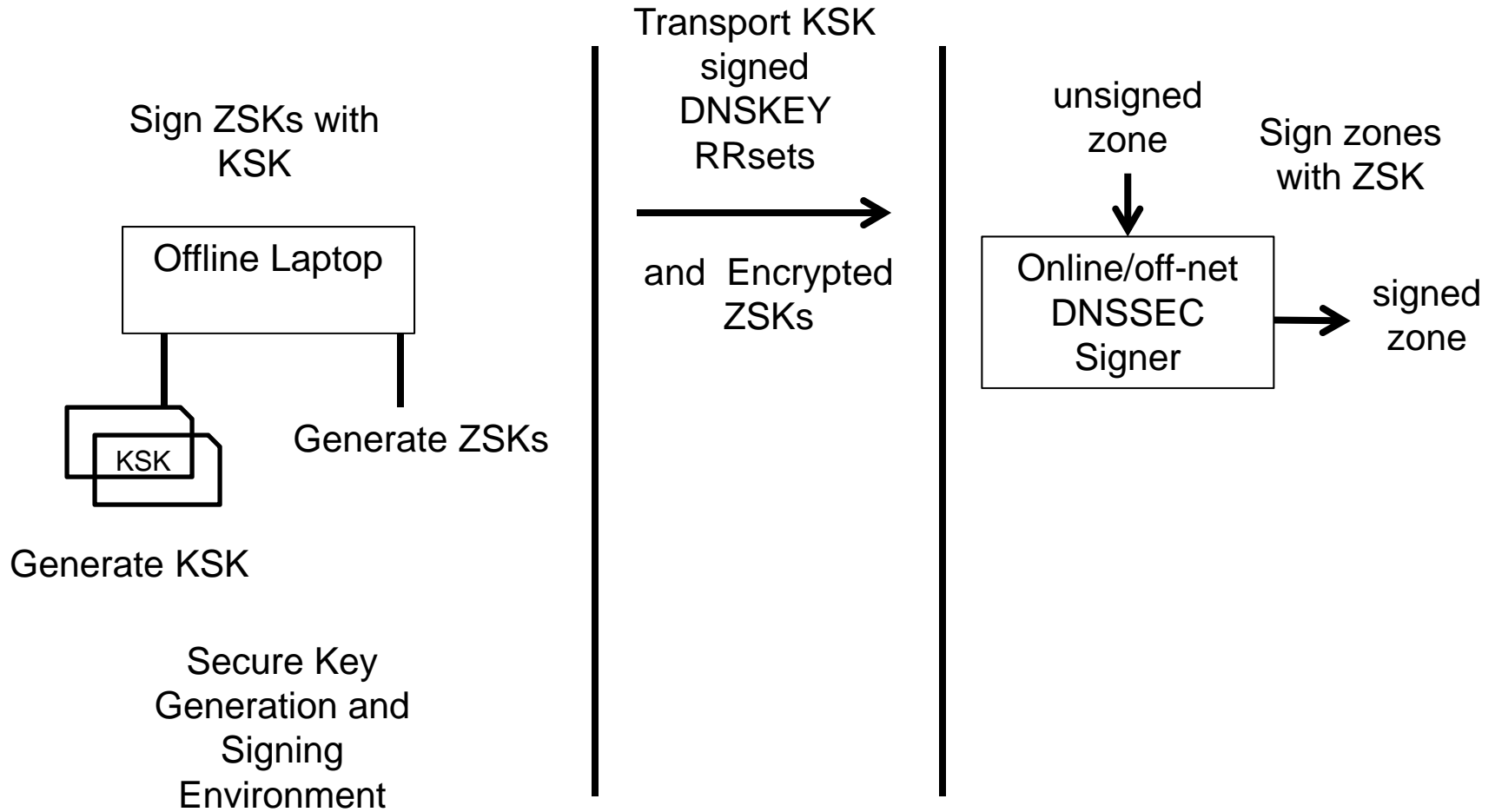
# Off-Line Key generator and KSK Signer



# Off-Net Signer

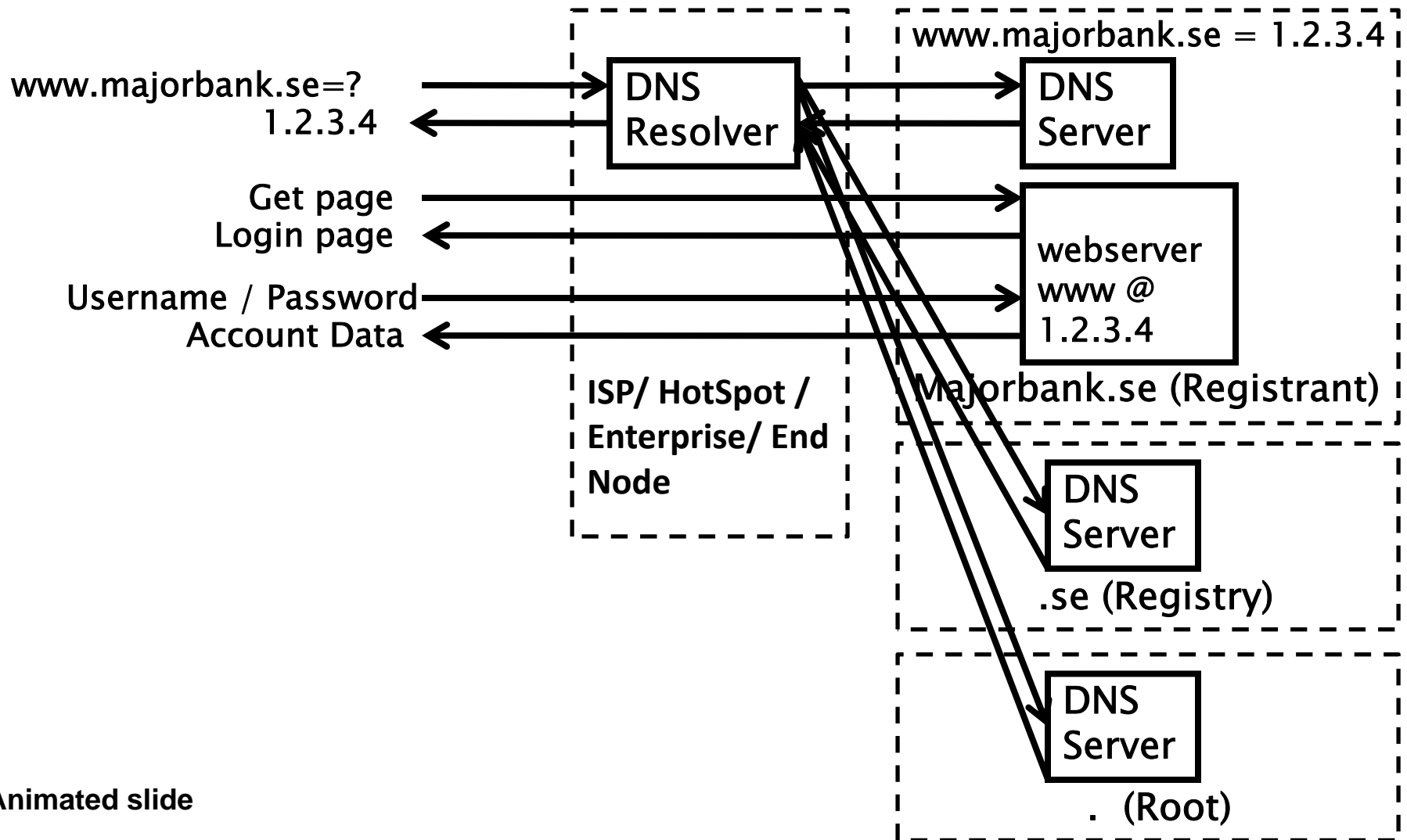


# Key Management



Animated slide

# DNS+DNSSEC



Animated slide

# Simple Key Management Scripts



# Keeping things signed

- If the signatures are going to expire soon, sign the zone
- Define “soon”
- Also sign if a record has changed
- That’s it!

```
while(1) {
    t = time
    if(exp - t) < 5 days {
        inc = t
        exp = t + 10 days
        touch infile
    }
    if new infile {
        cat infile keys > zonefile
        increment zonefile SOA serial
        signzone -s inc -e exp zonefile
                                zsk-current ksk

        rndc reload
    }
    sleep 1 second
}
```

# Rolling keys

- Mind the cache – DNS resolvers have memory
- Publish the new ZSK before signing with it
  - Put the new ZSK in the DNSKEY RRset along with old ZSK and wait until everyone see its
- Sign the zone with the new ZSK until you want to change it
- But do not un-Publish the old ZSK until no one may need it

# 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 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>

```
generate zsk-new
cat zsk-new zsk-current ksk > keys
touch infile
sleep >2xTTL
copy zsk-new zsk-current
touch infile
sleep >2xTTL
cat zsk-current ksk > keys
touch infile
sleep >2xTTL
```

# Some Recent Recommendations..

**“One obstacle for the implementation of DNSSEC is the lack of guidance for individual domain holders regarding which requirements should be defined - in particular for small and medium-sized businesses. In order to remedy that obstacle, .SE has written a guide as an aid and tool for municipalities that have the intention to implement DNSSEC, but this guide also applies to other types of organizations in both the public and private sectors.”**

<https://www.iis.se/english/domains/tech/recommendations-for-dnssec-deployment/>

**Anne-Marie Eklund Löwinder**

**Chief Information Security Officer**

**.SE (The Internet Infrastructure Foundation)**