DNSSEC Implementation Considerations and Risk Analysis

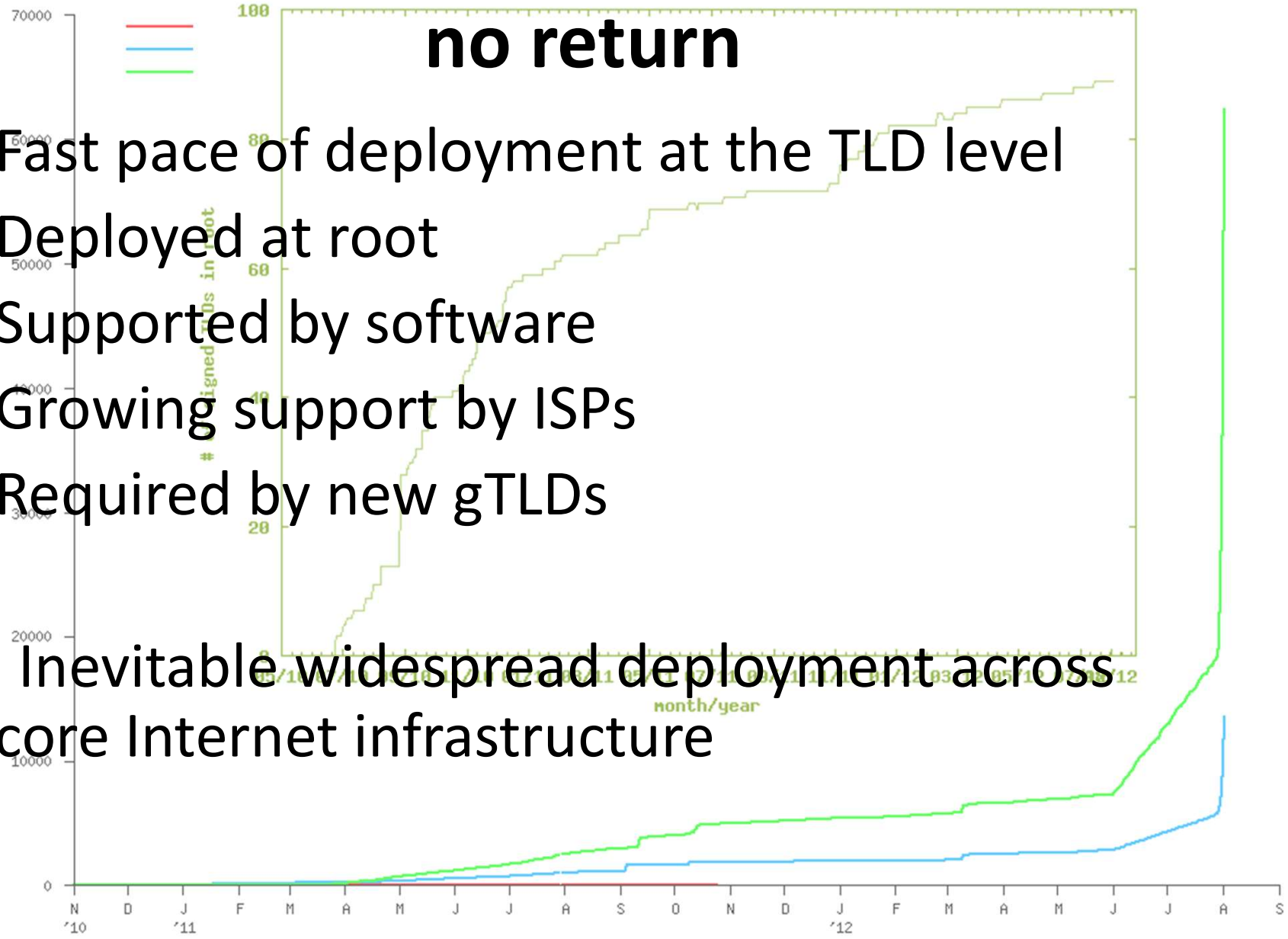
Sep 2017

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?

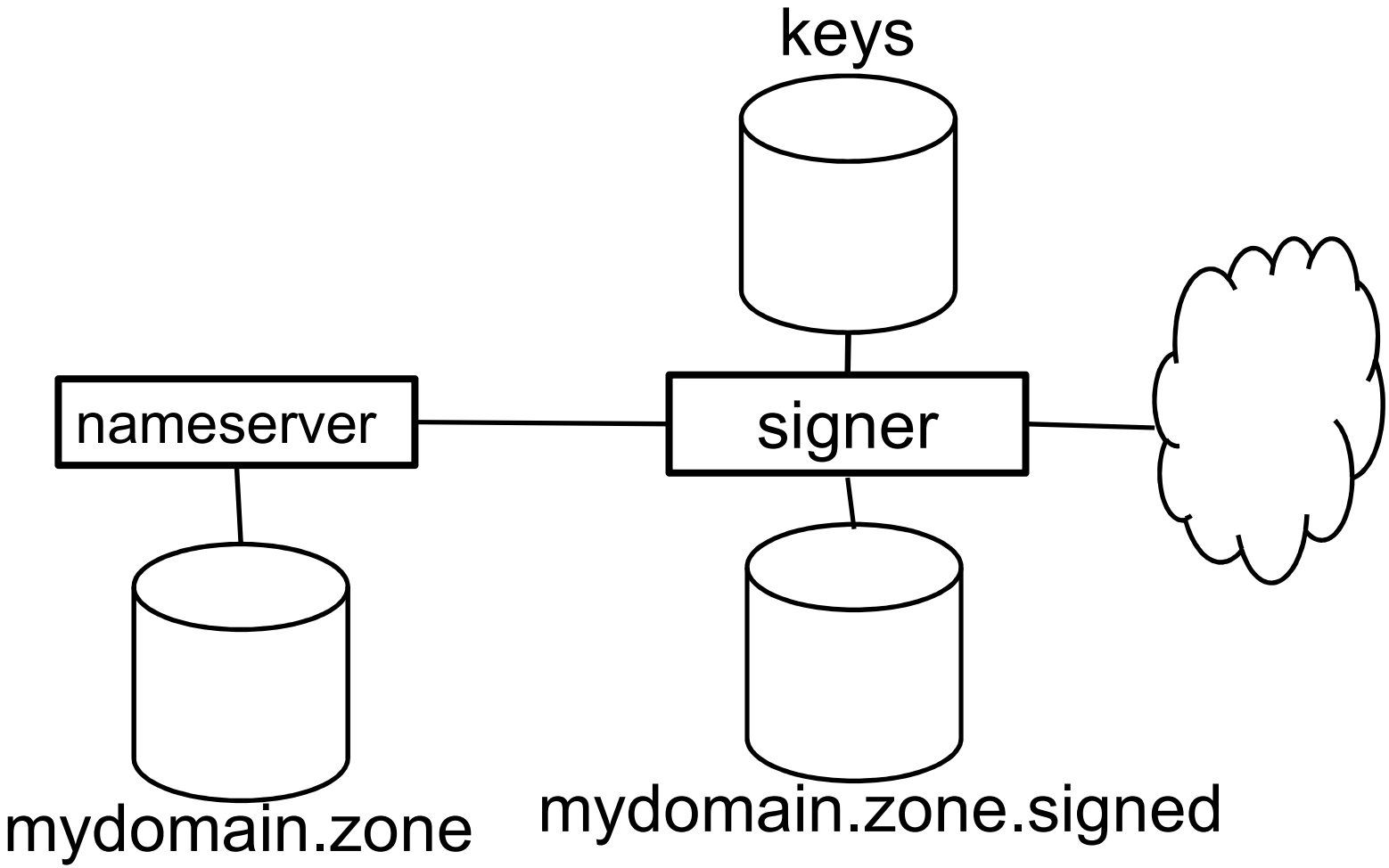
That’s it

dnssec-signzone mydomain.zone mydomain.zone.signed

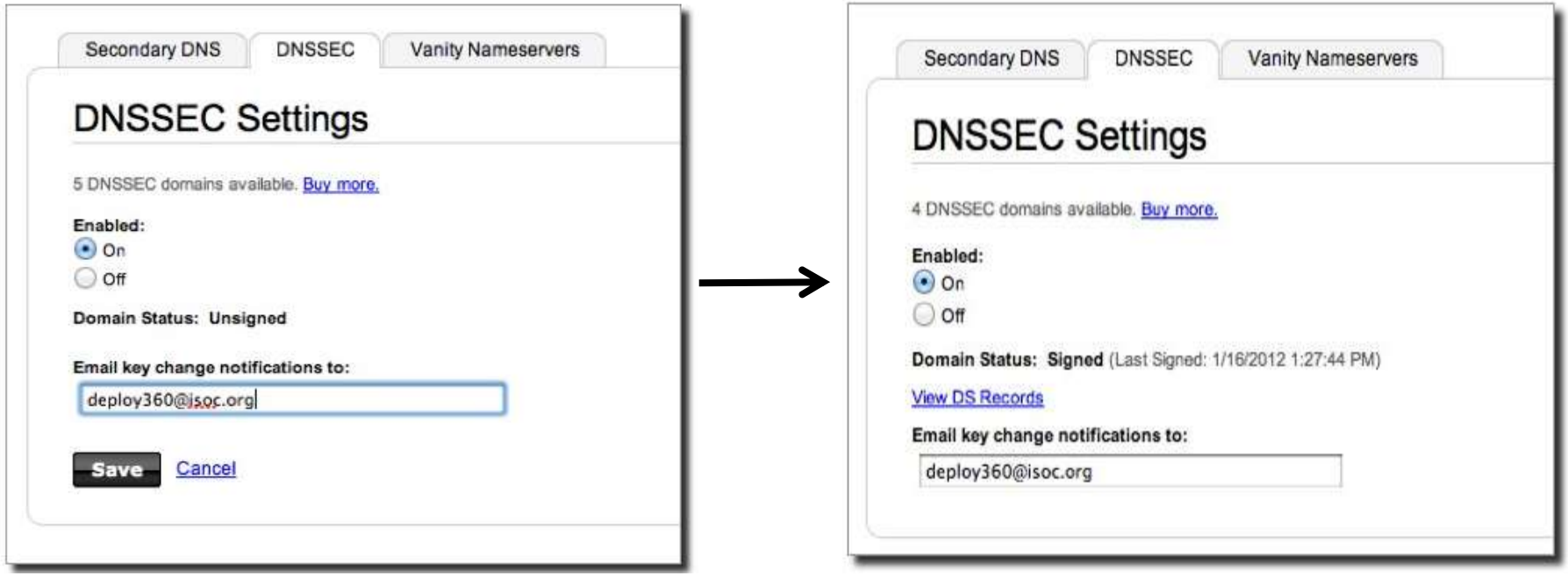
```
www.abc.com. IN A 192.101.186.125
```

```
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
1ik=
```

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 is does not have to be expensive

Goals

- Reliable
- Trusted
- Cost Effective (for you)

Reliable

- Keep design simple
- Monitoring – DNSSEC is time sensitive!
- People – develop checklists and documentation

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

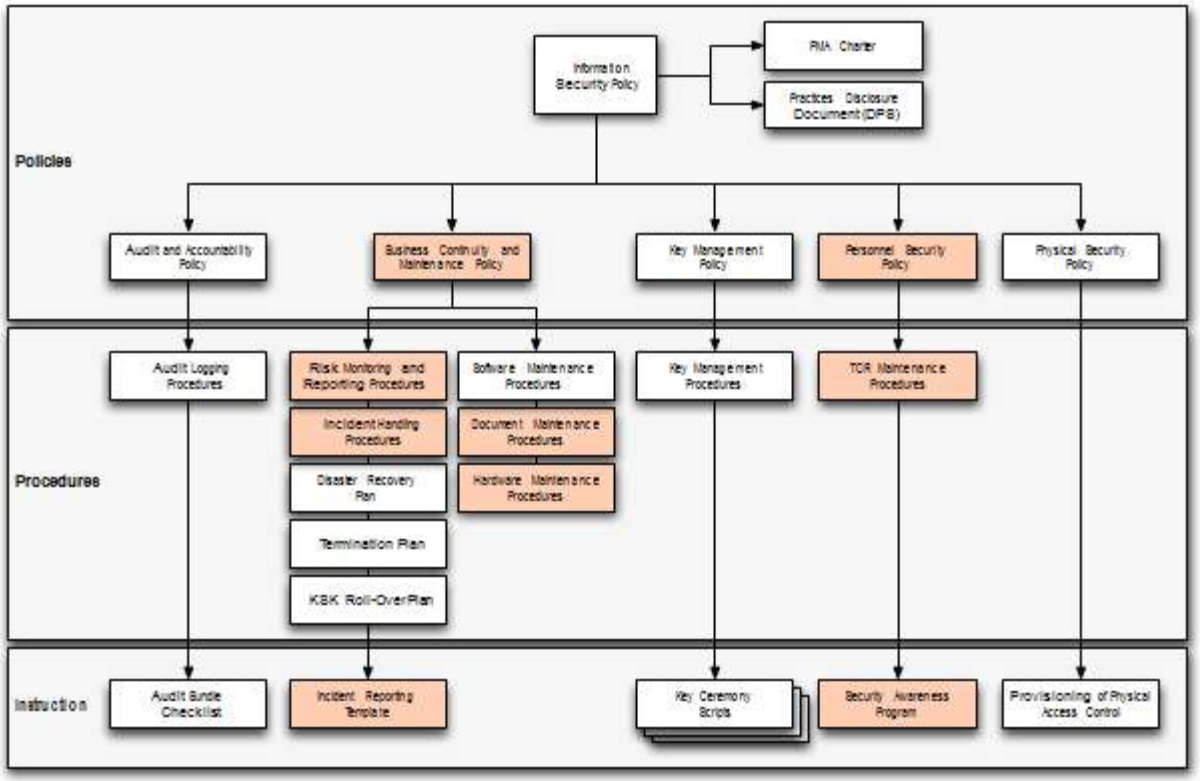
This document is the DNSSEC Practice Statement (DPS) for the Root Zone Key Signing Key (KSK) Operator. It states the practices and provisions that are used to provide Root Zone Key Signing and Key Distribution services. These include, issuing, managing, changing and distrik with the specific requirements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

Copyright Notice

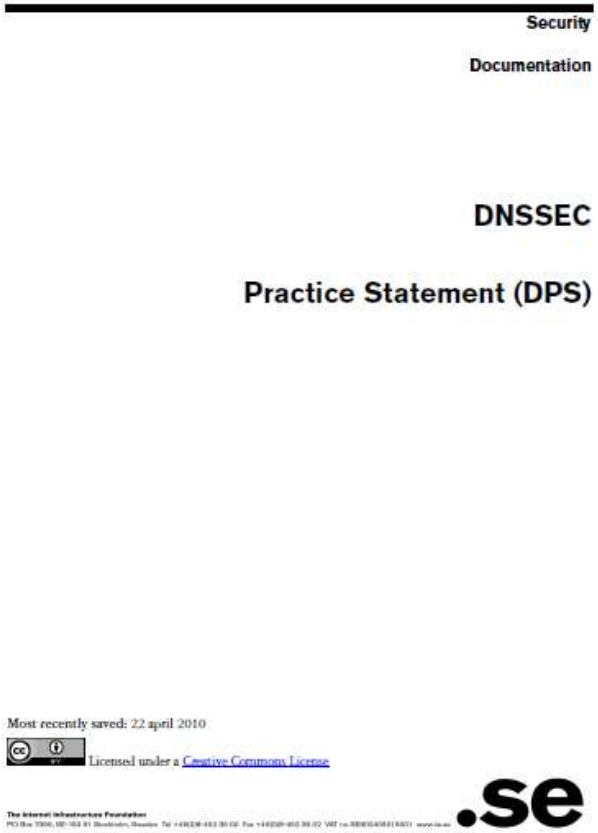
Copyright 2009 by VeriSign, Inc., and k Assigned Names and Numbers. This work

Root DPS

91 Pages and tree of other documents!



Documentation - .SE


Security

Documentation

DNSSEC

Practice Statement (DPS)

Most recently saved: 22 april 2010

The Internet Infrastructure Foundation

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

Building in security

- Getting the machinery for DNSSEC is easy (BIND, NSD/Unbound, Knot, 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

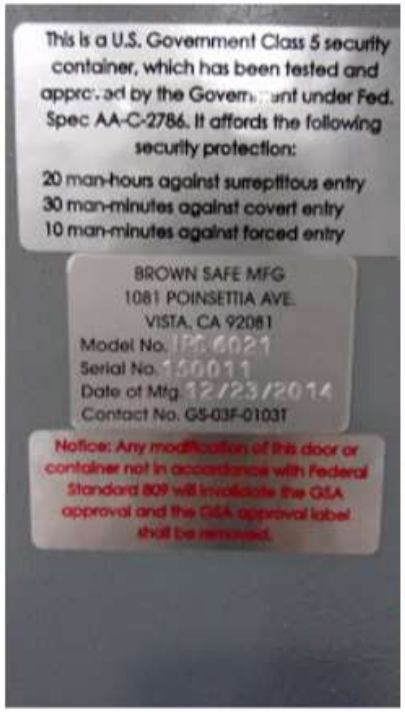
- Each tier should be successively harder to penetrate than the last
  - Facility
  - Cage/Room
  - Rack
  - Safe
  - System
- Think of concentric boxes

Physical - Tier Construction

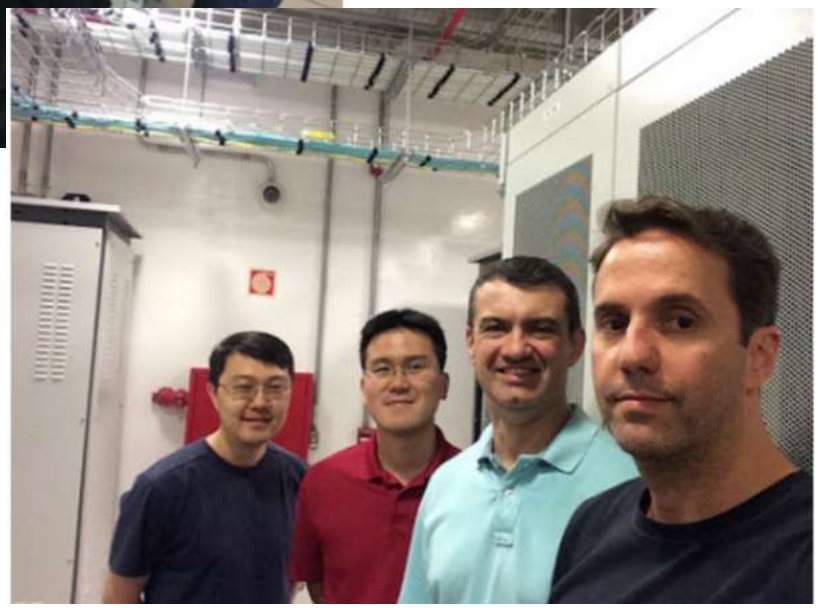
- Base on your risk profile and regulations
- Facility design and physical security on
  - Other experience
  - DCID 6/9
  - NIST 800-53 and related documents
  - Safe / container standards

Physical – Safe Tier

Physical – Safe Tier



Transparency



Physical – Tamper Evident Packaging

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

https://www.keylength.com

ECRYPT is a network of excellence in cryptology. This report [3] is driven by the "Security Level" you want to reach. To each of these levels corresponds a symmetric key size from which equivalent asymmetric key sizes are built in a similar way as the one used in NESSIE.

Level	Protection	Symmetric	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash
1	Attacks in "real-time" by individuals *Only acceptable for authentication tag size*	32	-	-	-	-	-
2	Very short-term protection against small organizations *Should not be used for confidentiality in new systems*	64	816	128	816	128	128
3	Short-term protection against medium organizations, medium-term protection against small organizations *Should not be used for confidentiality in new systems*	72	1008	144	1008	144	144
4	Very short-term protection against agencies, long-term protection against small organizations *Smallest general-purpose level,* *2-key 3DES restricted to 2^{40} plaintext/ciphertexts,* *Should not be used for confidentiality in new systems*	80	1248	160	1248	160	160
5	Legacy standard level *2-key 3DES restricted to 10^6 plaintext/ciphertexts, protection from 2017 to 2020*	96	1776	192	1776	192	192
6	Medium-term protection *3-key 3DES, protection from 2017 to 2030*	112	2432	224	2432	224	224
7	Long-term protection *Generic application-independent recommendation, protection from 2017 to 2040*	128	3248	256	3248	256	256
8	"Foreseeable future" *Good protection against quantum computers, unless Shor's algorithm applies*	256	15424	512	15424	512	512

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
- Update to FIPS 140-2 → ISO/IEC 19790

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)
  - Smartcard HSM ~$15 (DE)
  - Feitian ~$5-10 (CN)
  - Aventra ~$11 (FI)
- TPM
  - Built into many PCs (e.g. Dell)
- 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

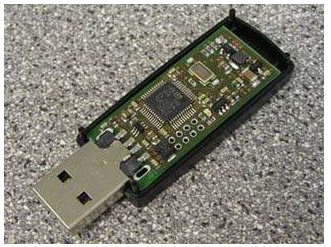
? System Entropy (/dev/random-urandom)

? 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 …

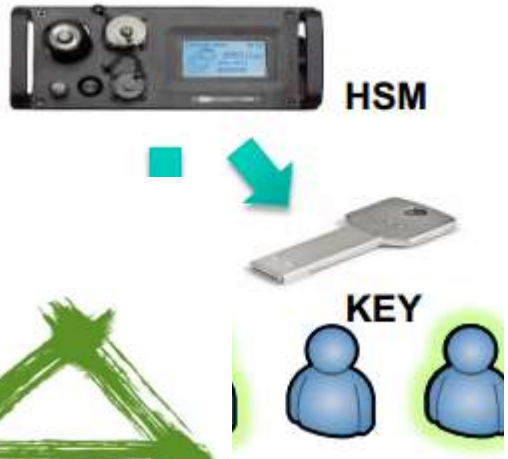
Crypto – FIPS Level 3 HSM

- 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$

SysTrust

…or this

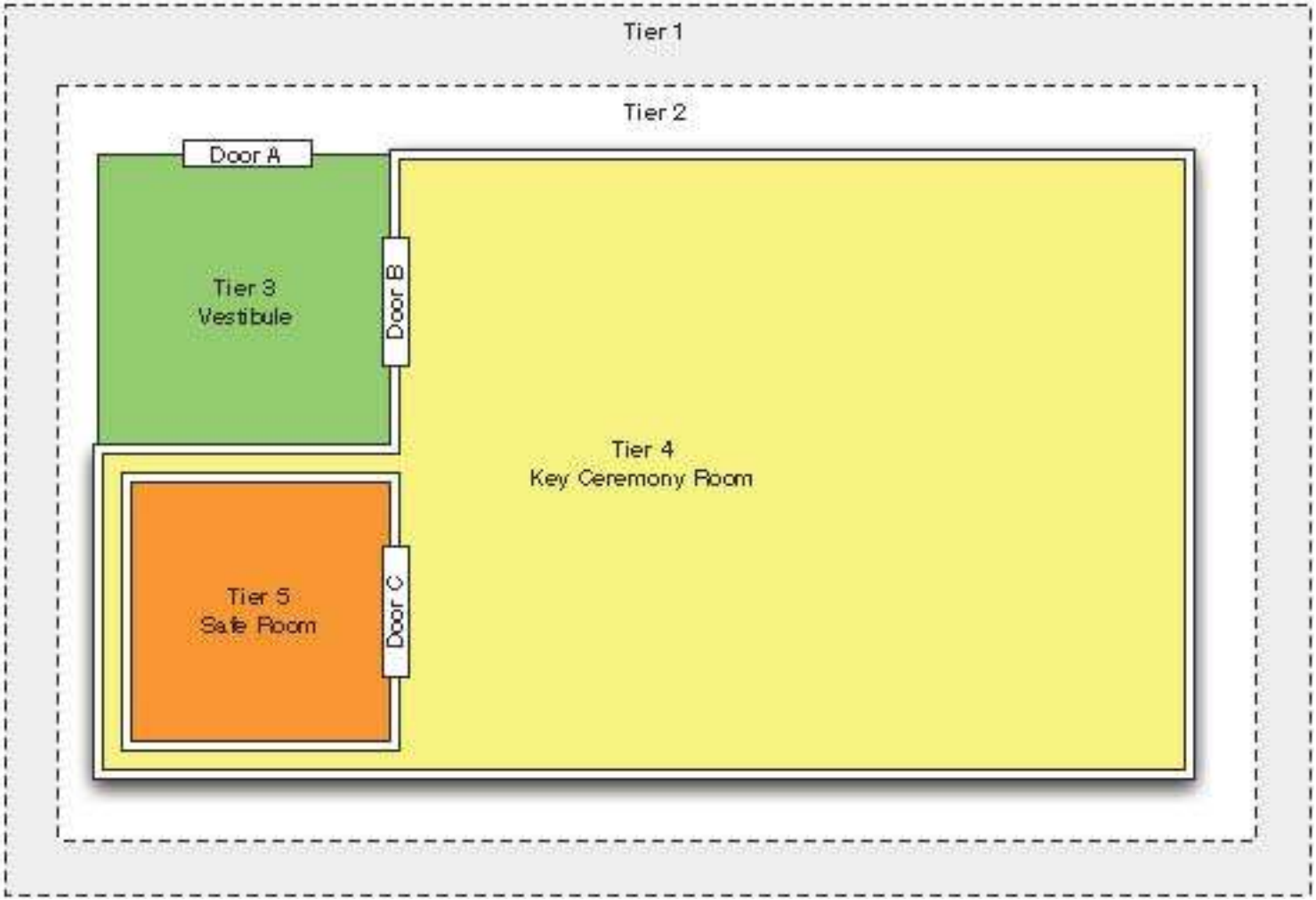


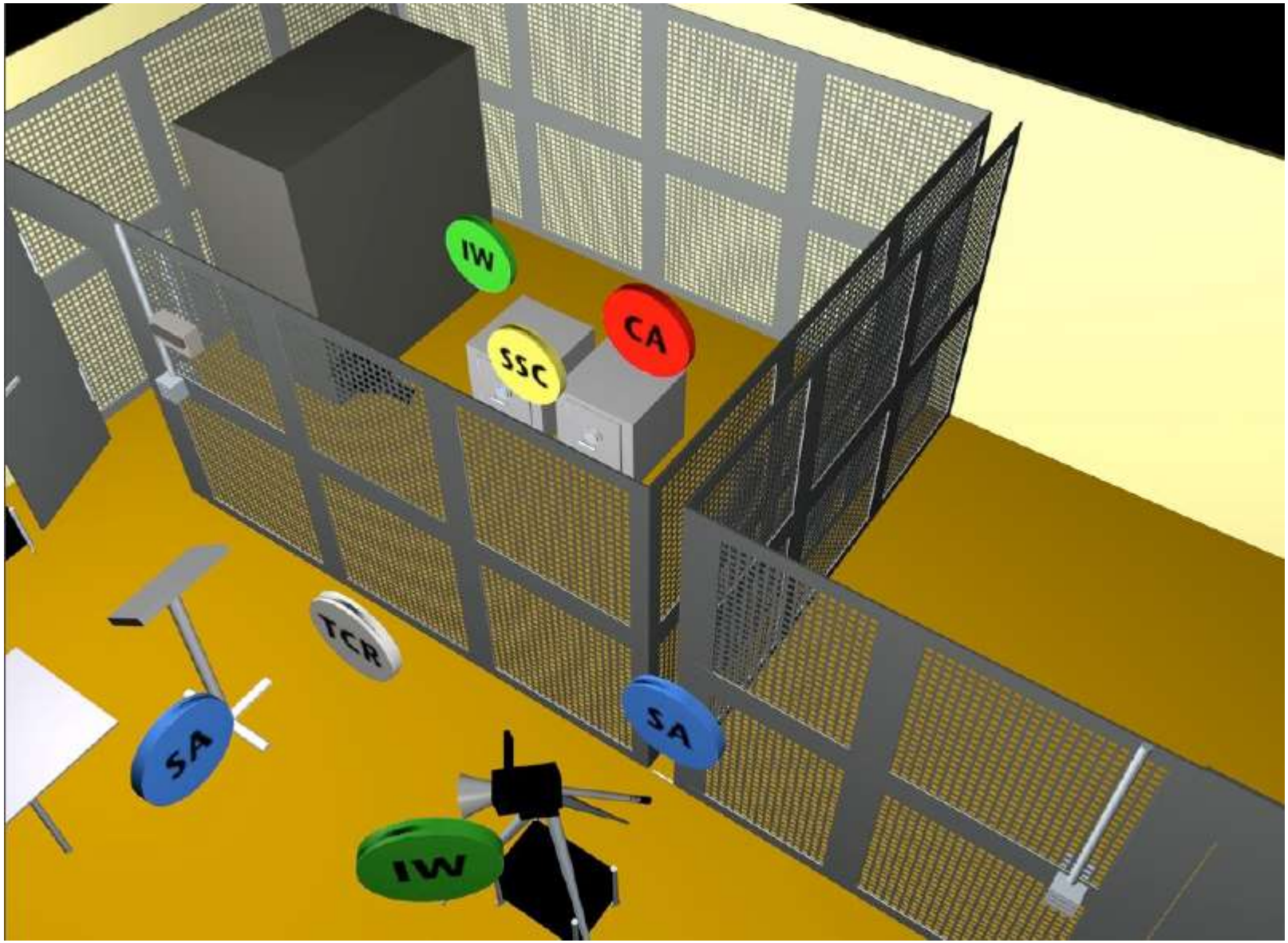
Physical Security

- 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

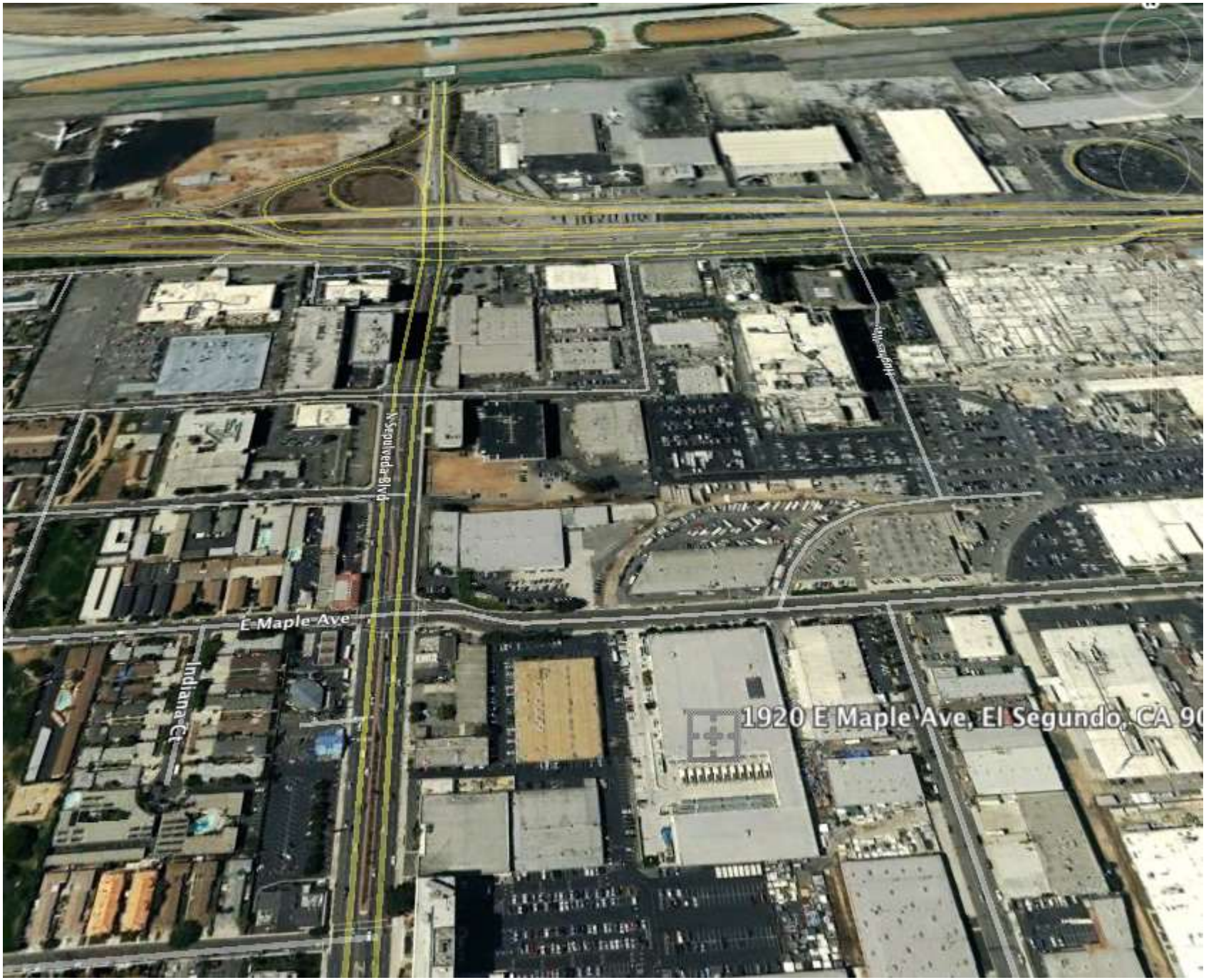
http://singapore49.icann.org/en/schedule/wed-dnssec/presentation-dnssec-deployment-cn-26mar14-en.pdf

Physical Security




IW
CA
SSC
TCR
SA
SA
IW

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


E Maple Ave
Indiana Ct
1920 E Maple Ave, El Segundo, CA 90


January 27, 2010


NOTICE
NOTICE
NOTICE
NO FOOD
OR DRINK
One World. One Internet. Everyone Connected.
19036

…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
environments in which cryptog
ign and implementation of a cry
ct identified as:

Athena IDProtect by Athen
ATSOSC25672RCT 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:

Dated: March 31, 2008

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

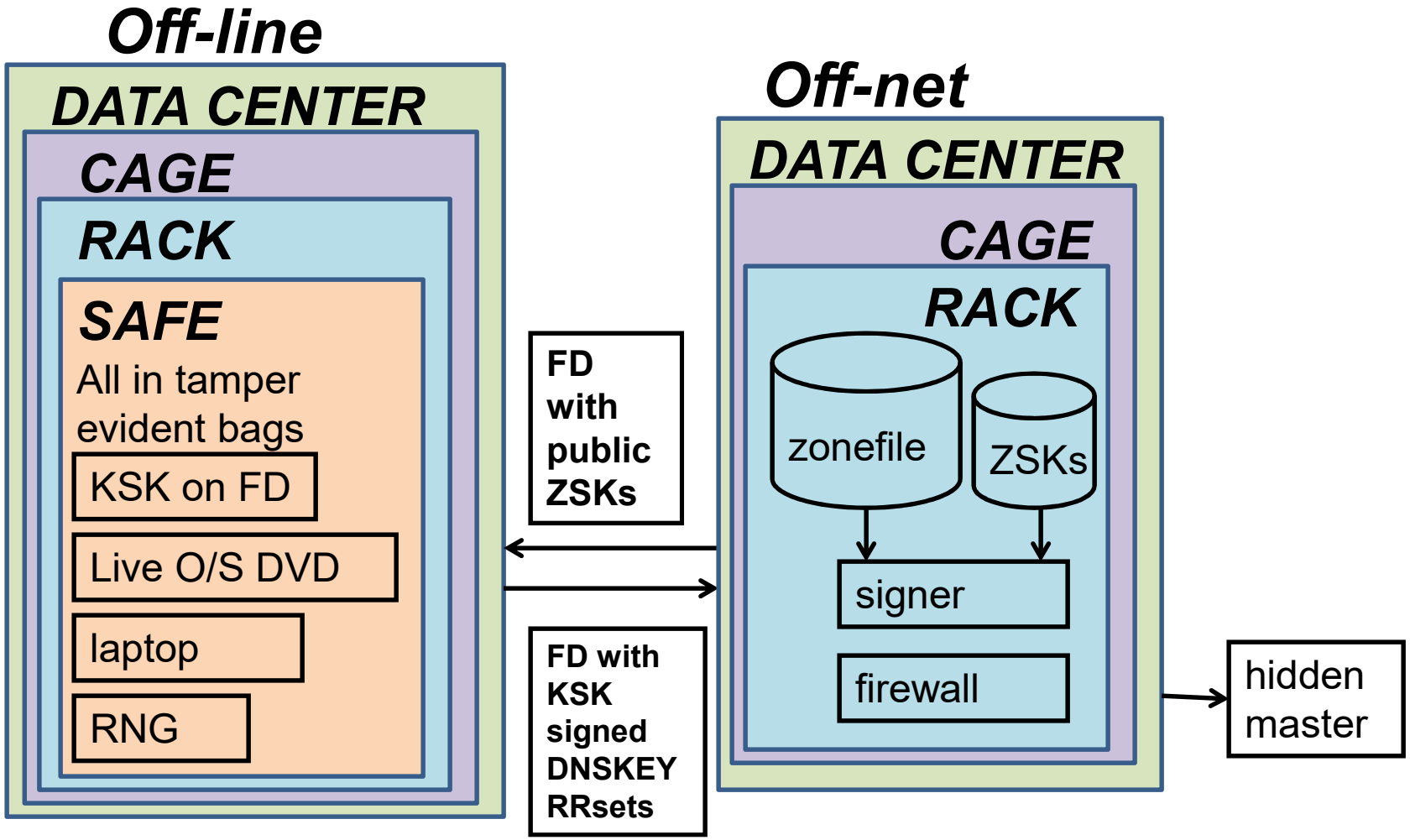
Dated: 20 March 2008

Director, Industry Program Group
Communications Security Establishment

..or this (from .cr .ar)

Animated slide

…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

Learn from others mistakes

ISP's and other validating resolver operators

- Learn from experience of others*. When someone else's DNSSEC system fails, e.g., signatures expire, who gets the phone call? YOU DO.
- It is happening less and less (a few times a year) but have an email response ready and
- If necessary use the Negative Trust Anchor** option found in some resolvers to temporarily disable validating the problematic zone

***COMCAST US ISP ~20M customers**
****Appendix A: https://tools.ietf.org/html/draft-livingood-dnsop-negative-trust-anchors-01**

Signing Operations – DNSSEC and Vacations

- Learn from the experience of others. Technology is easy. Managing people is hard. DNSSEC signatures are time limited. If the signature validity period is too long, you will not be able to recover from a compromise too quickly.
- If the validity period is too short, you might not be able to replace failed equipment or get a hold of your engineers on vacation.
- Therefore many DNSSEC signatures are good for 1 to 2 weeks (about how long someone in the US takes a vacation ☺)

Signing Operations – Monitoring Signature Expiry

- The biggest problem we have seen with DNSSEC deployments has been expired signatures. Do you really want signatures to renew on December 31 ? Who is going to be around if things fail?
- Monitor the expiry time of your zone using a script or an outside service. Send out email/SMS if a DNSSEC signature is about to expire. Plenty of tools*
- The Internet technical community is small but global. Have one of them run a script to monitor your systems and you do the same for them. Just like you might do with secondary name servers.

***http://dnsviz.net/**
http://www.zonecheck.fr/
http://dnscheck.iis.se/ (note:has undelegated option for testing new zones)

Signing Operations – Openness = Trust

- At these early stages of DNSSEC mistakes will happen. Being public about such mistakes and how you fix them builds trust and sets expectations*.
- Sharing those experiences helps others and makes you the expert.
- Being “found out” later can destroy an operation

***http://en.wikipedia.org/wiki/Chicago_Tylenol_murders#Aftermath**
UK http://blog.nominet.org.uk/tech/wp-content/uploads/2010/09/dnssec-incident-report.pdf
FR http://singapore41.icann.org/meetings/singapore2011/presentation-key-deletion-issues-22jun11-en.pdf

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

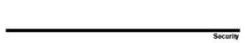
.SE (The Internet Infrastructure Foundation)

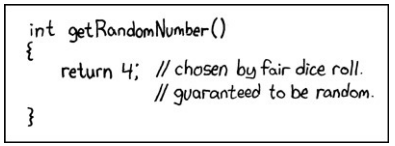
Setting reasonable expectations means it doesn't have to be expensive

You do not need a fortress, just detect if something is touched

But all must have:

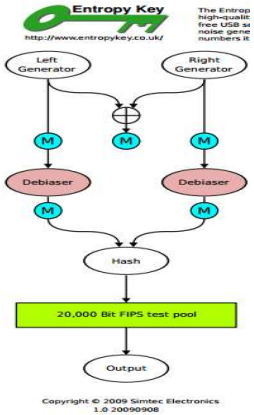
- Published practice statement
  - Overview of operations
  - Setting expectations
    - Normal
    - Emergency
  - Limiting liability
- Documented procedures
- Multi person access requirements
- Audit logs
- Monitoring (e.g., for signature expiry)
- Good Random Number Generators





Intel RdRand

DRBGs
FIPS 140

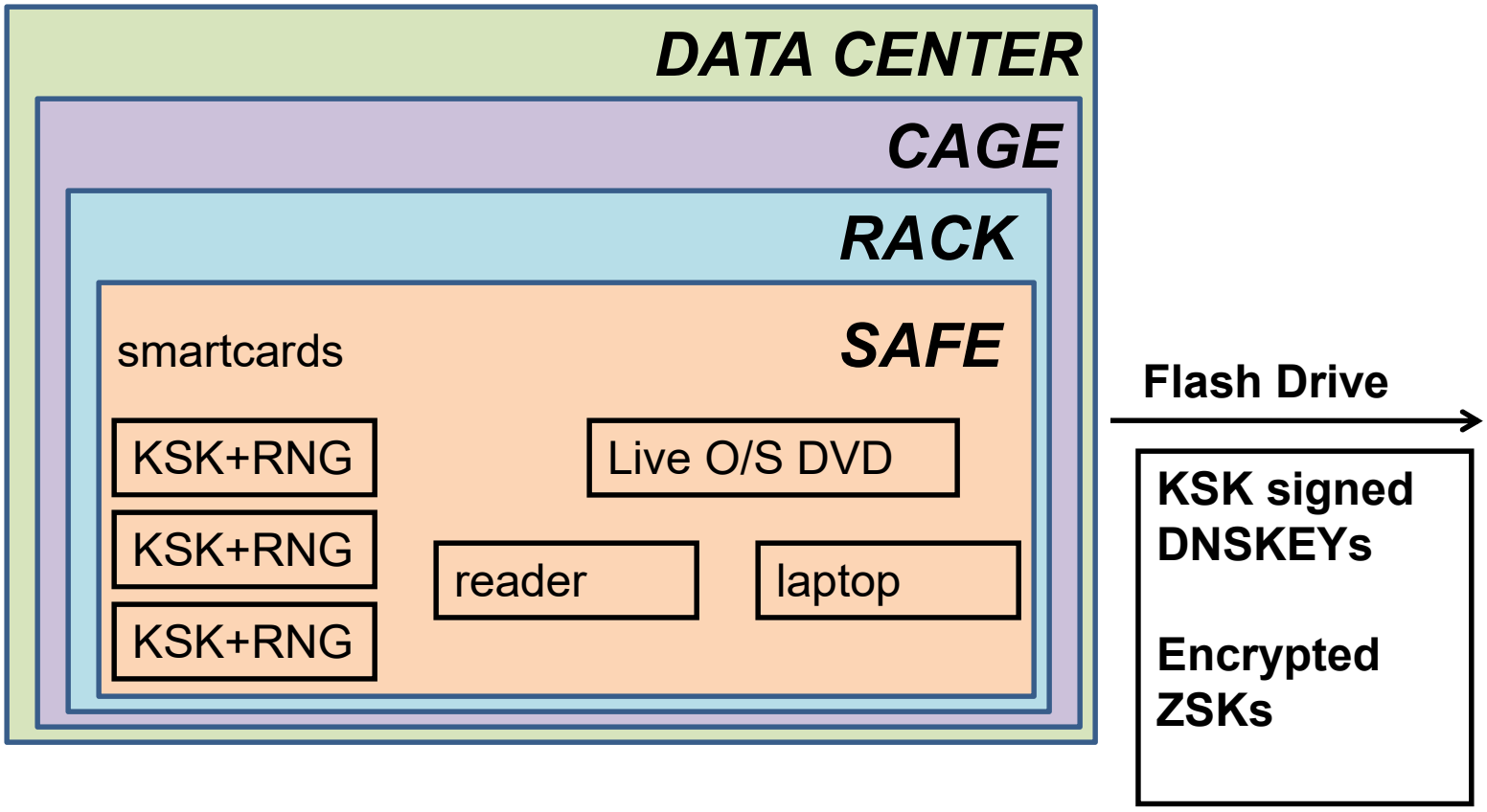


Useful IETF RFCs:
DNSSEC Operational Practices V2 RFC6781
A Framework for DNSSEC Policies and DNSSEC Practice Statements RFC6841

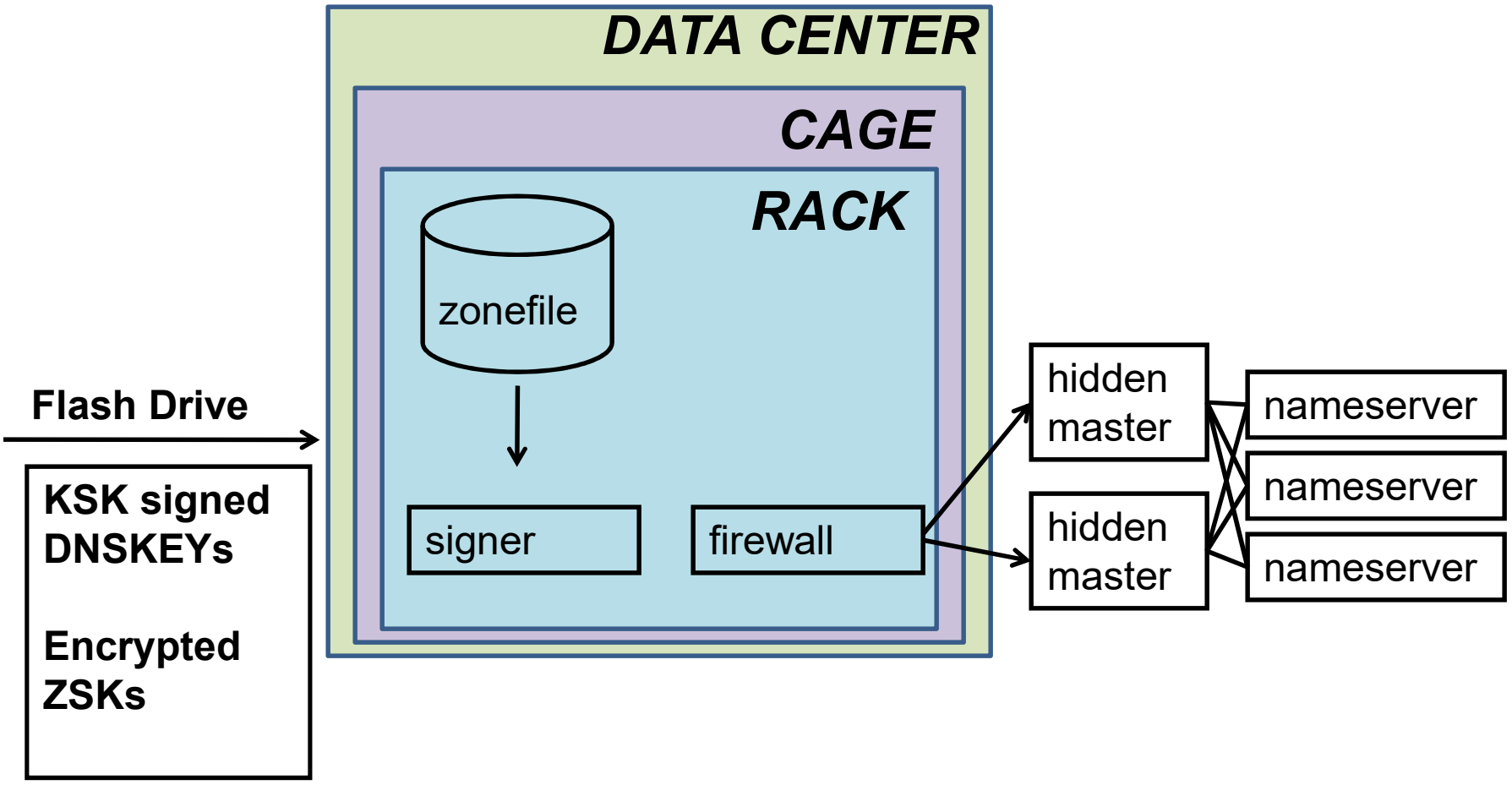
Demo Implementation

- 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

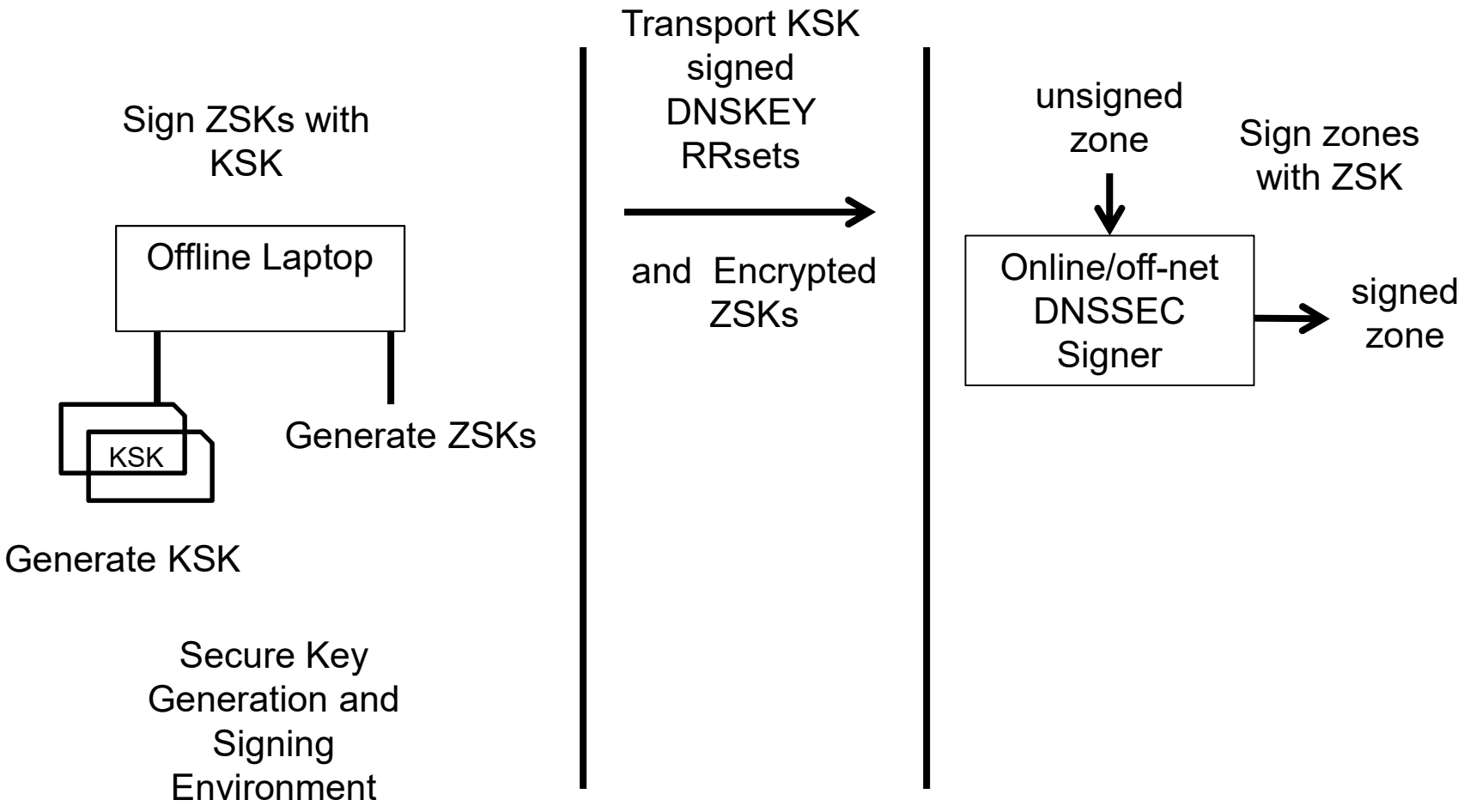
Off-Line Key generator and KSK Signer



Off-Net Signer

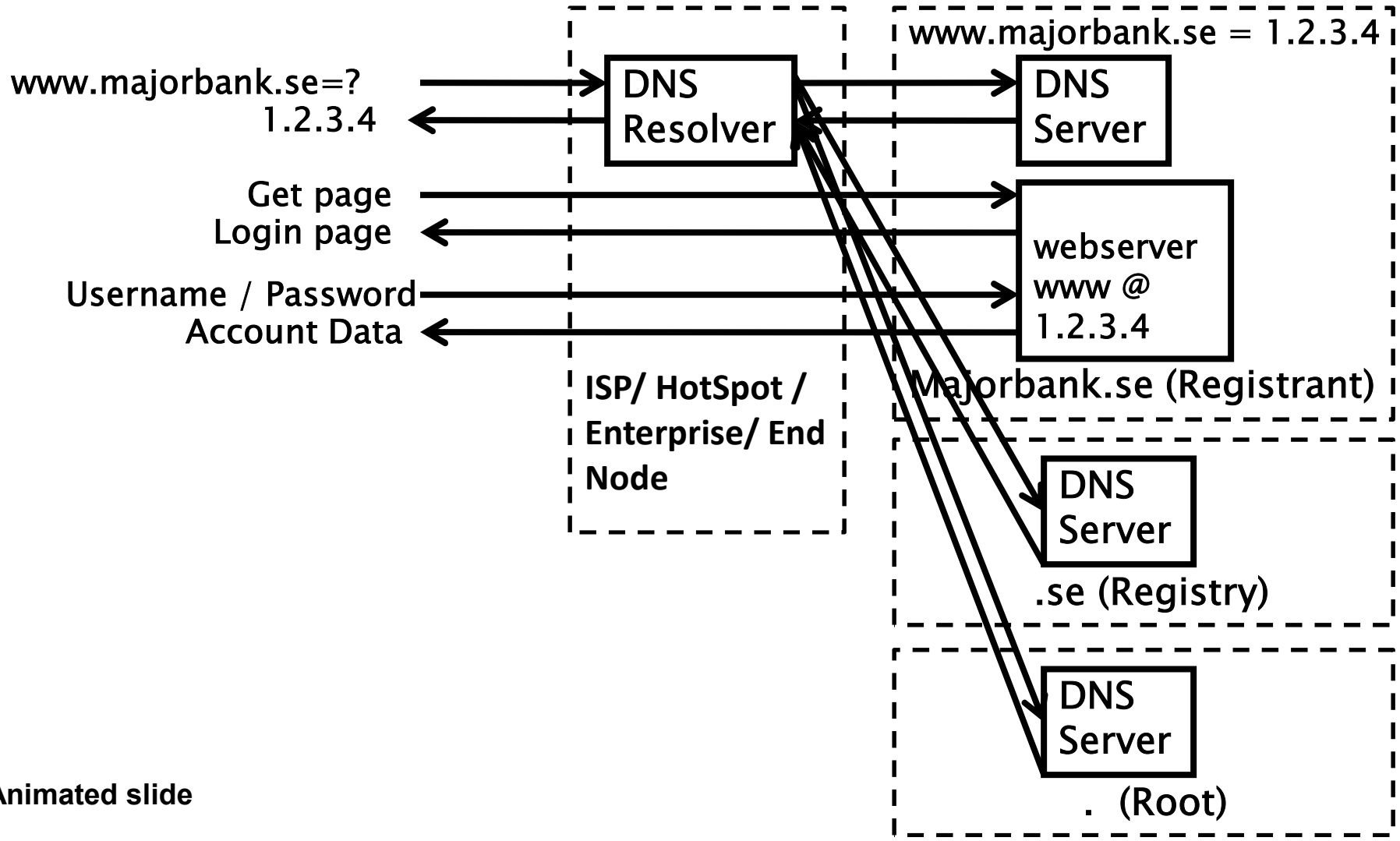


Key Management



Animated slide

DNS+DNSSEC



Animated slide

Simple Key Management Scripts

Keeping things signed

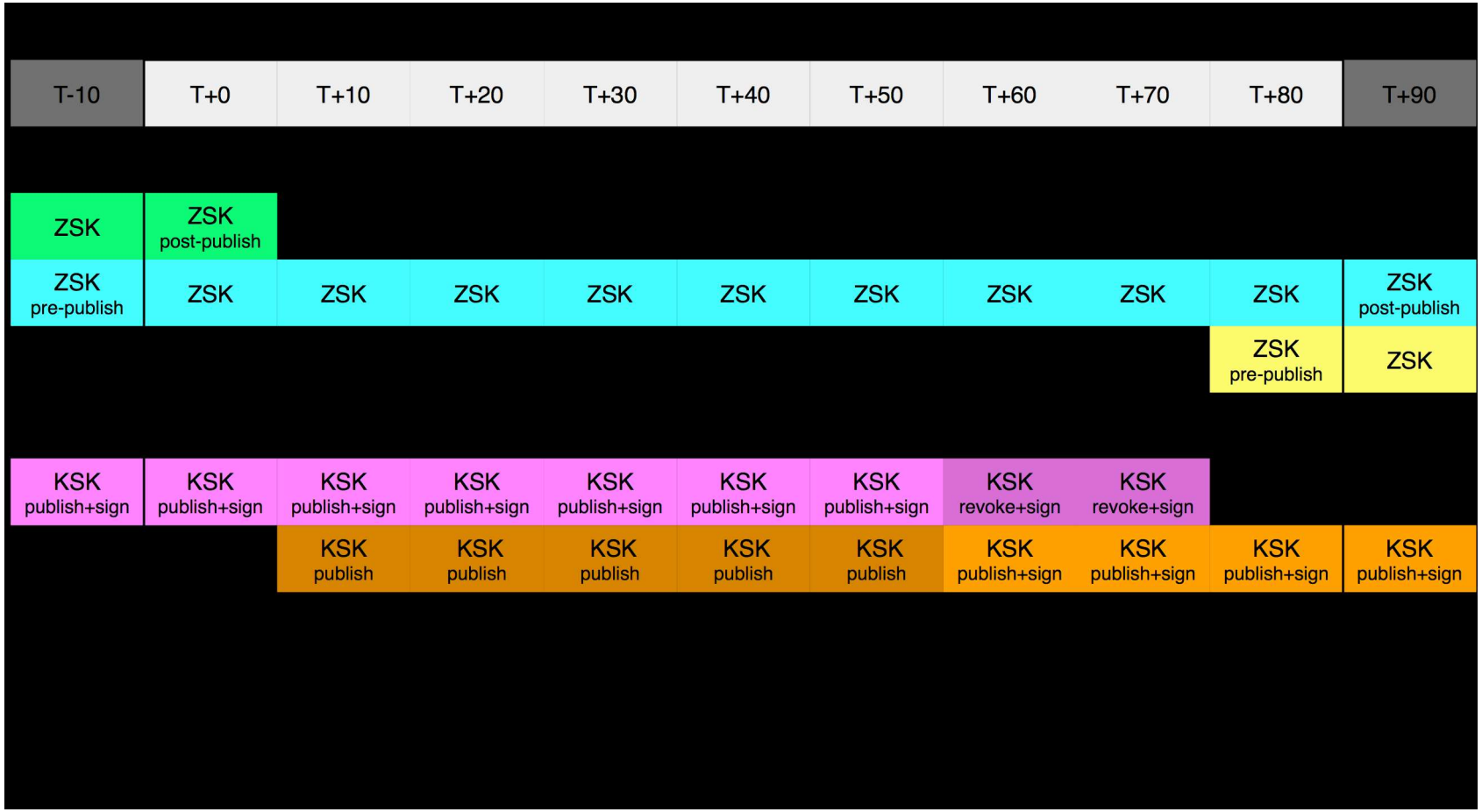
- If the signatures are going to expire soon, sign the zone
- Define “soon”
- Also sign if a record has changed
- That’s it!

```
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



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
```