DNSSEC Sample Implementation

Module 1

DNSSEC Workshop

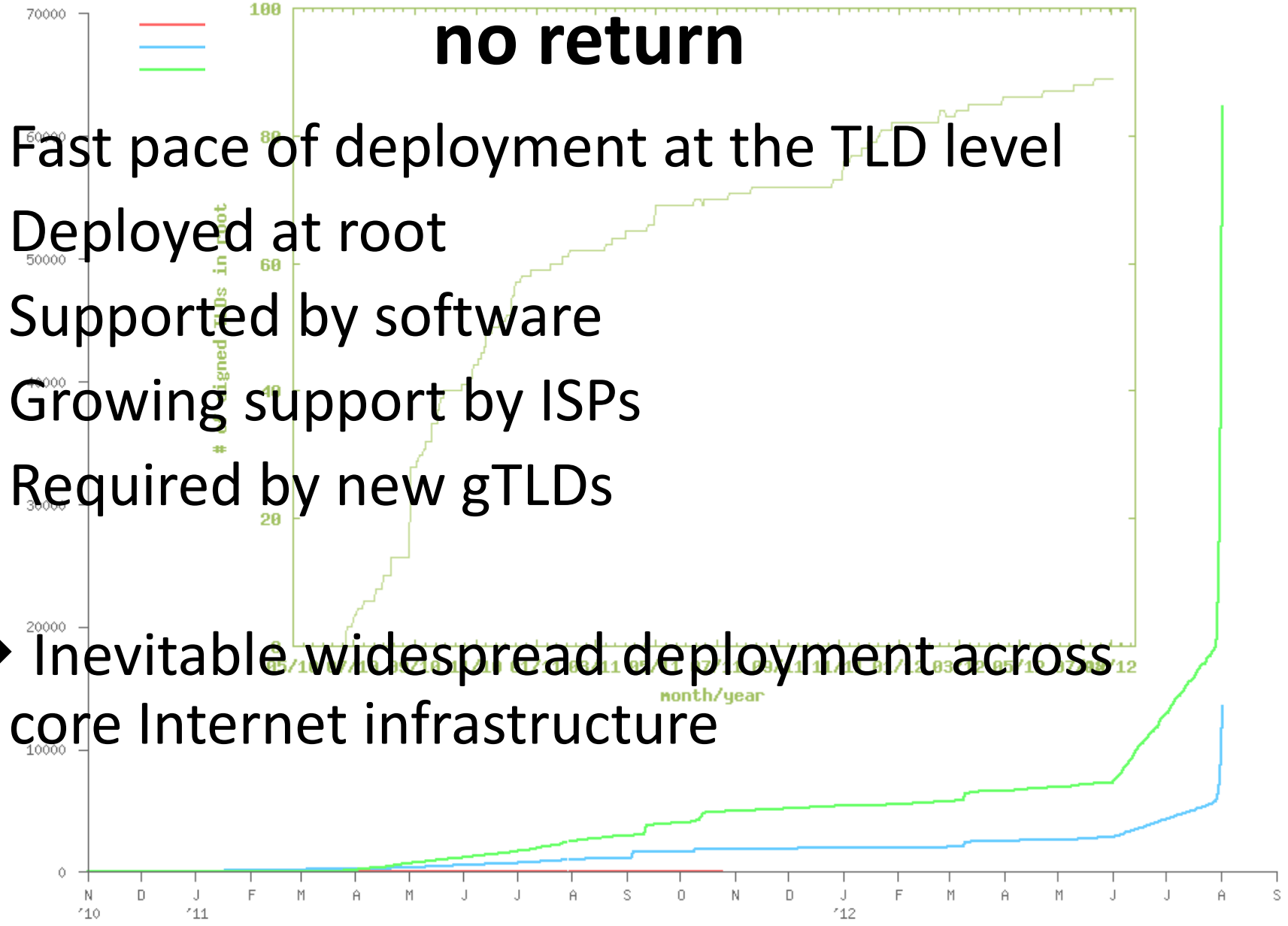
5 May 2013, Medellin, Colombia

richard.lamb@icann.org

DNSSEC: We have passed the point of no return

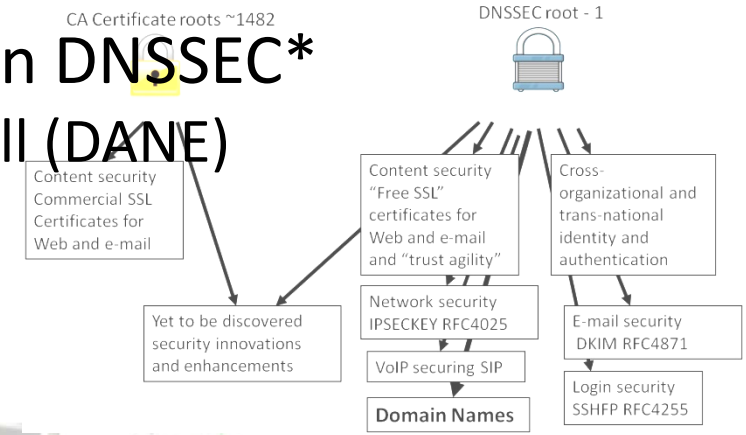
- Fast pace of deployment at the TLD level
- Deployed at root
- Supported by software
- Growing support by ISPs
- Required by new gTLDs

→ Inevitable widespread deployment across core Internet infrastructure



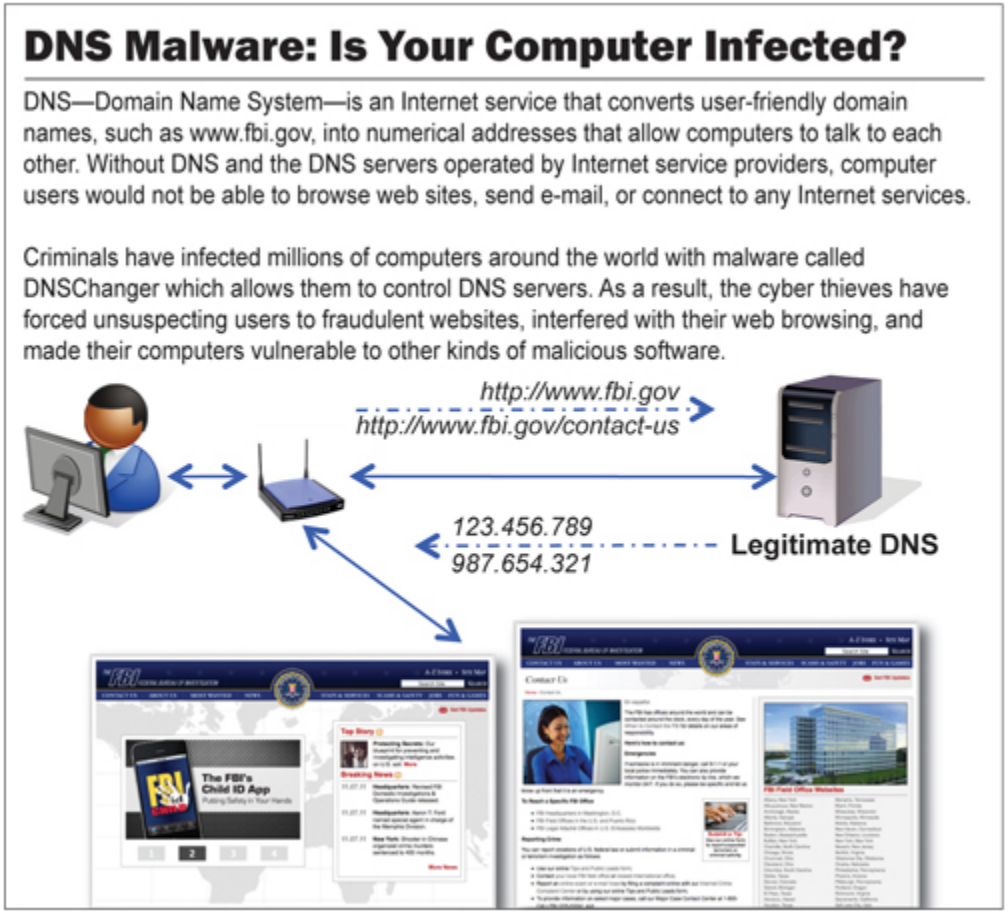
DNSSEC: Plenty of Motivation

- DNSChanger attack, calls for deployment by governments, etc…
- Technology and standards built on DNSSEC*
  - Improved Web TLS and certs for all (DANE)
  - 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**

The BAD: DNSChanger - 'Biggest Cybercriminal Takedown in History' – 4M machines, 100 countries, $14M



Nov 2011 http://krebsonsecurity.com/2011/11/malware-click-fraud-kingpins-arrested-in-estonia/
End-2-end DNSSEC validation would have avoided the problems

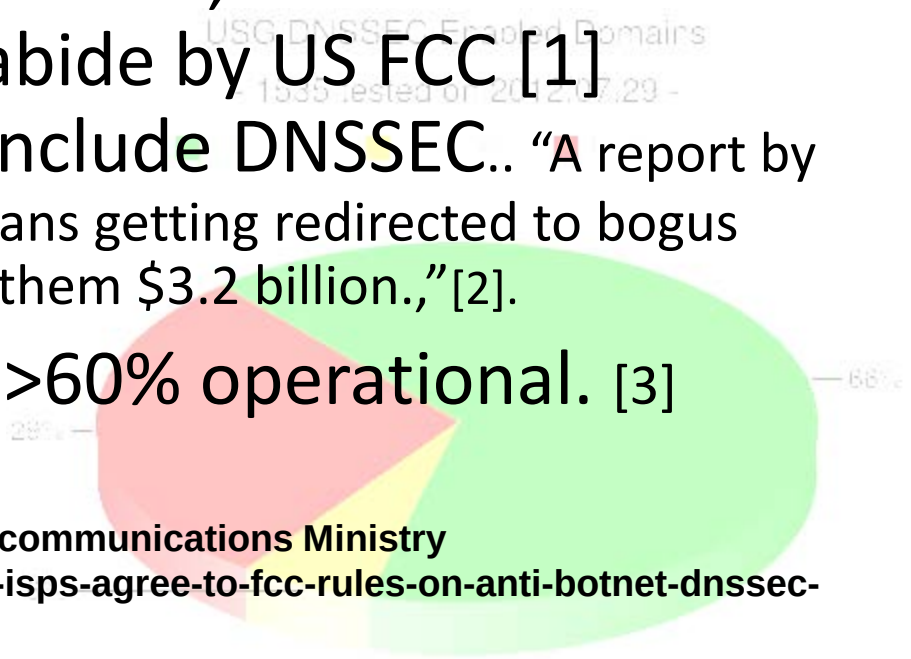
The BAD: Other DNS hijacks*

- 25 Dec 2010 - Russian e-Payment Giant ChronoPay Hacked
- 18 Dec 2009 – Twitter – “Iranian cyber army”
- 13 Aug 2010 - Chinese gmail phishing attack
- 2009-2013 google.* (e.g., .ke, …)
  - April 28 2009 Google Puerto Rico sites redirected in DNS attack
  - May 9 2009 Morocco temporarily seize Google domain name
- 9 Sep 2011 - Diginotar certificate compromise for Iranian users
- SSL / TLS doesn't tell you if you've been sent to the correct site, it only tells you if the DNS matches the name in the certificate. Unfortunately, majority of Web site certificates rely on DNS to validate identity.
- DNS is relied on for unexpected things though insecure.

*A Brief History of DNS Hijacking - Google
http://costarica43.icann.org/meetings/sanjose2012/presentation-dns-hijackings-marquis-boire-12mar12-en.pdf

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

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

SSL Dilution of Trust
DNSSEC = Global “free” PKI

CA Certificate roots ~1482

DNSSEC root - 1

Content security
Commercial SSL
Certificates for
Web and e-mail

Content security
“Free SSL”
certificates for Web
and e-mail and “trust
agility”

Cross-
organizational and
trans-national
identity and
authentication

DANE and other yet to be
discovered security
innovations, enhancements,
and synergies

Network security
IPSECKEY RFC4025

Securing VoIP

Domain Names

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/

DNSSEC - Where we are

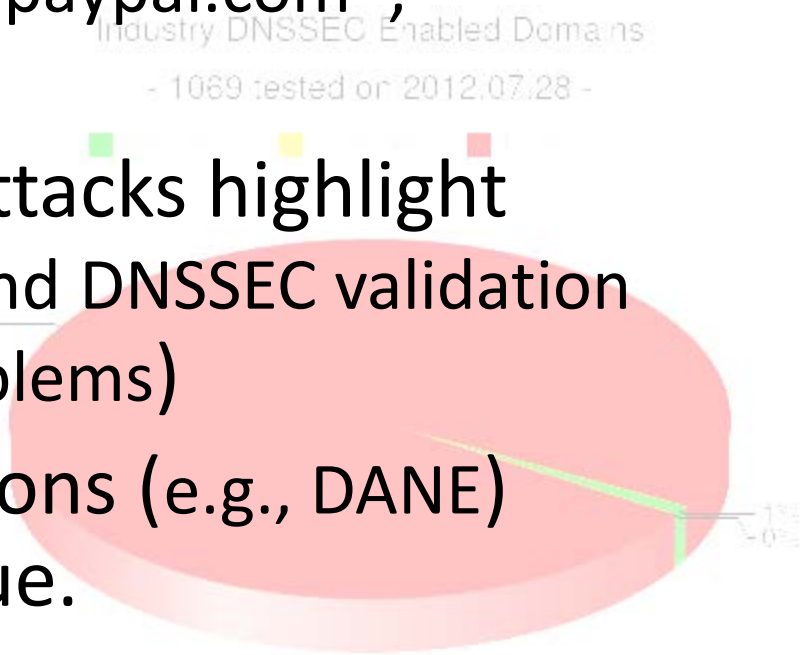
- Deployed on 105/317 TLDs (.lb .lt .tz .in .th .mm .ru .pф .tm .kg .lk .ca .be .uk .nl .fr .br .cz .de .pt .my ملیسیا .asia .tw 台灣, .kr 한국 .com .net, .post, ….cn soon)
- Root signed** and audited
- >86% of domain names could have DNSSEC
- Required in new gTLDs
- Growing ISP support*
- 3rd party signing solutions: GoDaddy, Binero, VeriSign…***
- Growing S/W H/W support: NLNetLabs/NSD+Unbound, ISC/BIND, Microsoft, PowerDNS, Secure64…?openssl, mozilla DANE support?
- IETF standard on DNSSEC SSL certificates (RFC6698)
- Growing support from major players…(IOS, 8.8.8.8,…)

***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.

+1-202-709-1234
VoIP

US-NSTIC

DNS is a part of all IT ecosystems

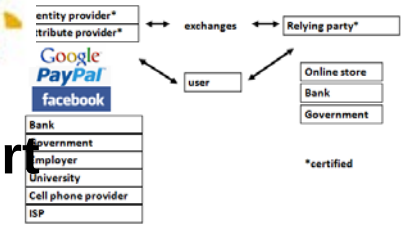
Google
OpenID

facebook

eBay

AADHAAR

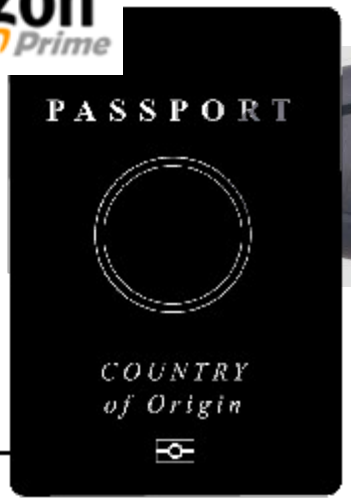
PayPal



OECS ID effort

amazon Prime

e-Passport symbol

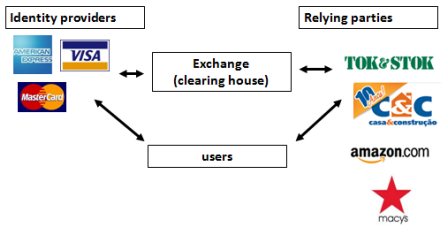


ICP Brasil
O Brasil na era da certificação digital

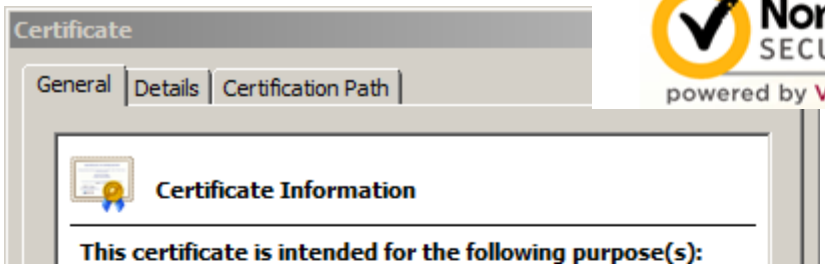
DigiNotar
A VASCO COMPANY

COMODO
Creating Trust Online®

Trust frameworks are not new



Smart Electrical Grid



Norton SECURED
powered by VeriSign

dave@xtcn.com

mydomainname.com

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

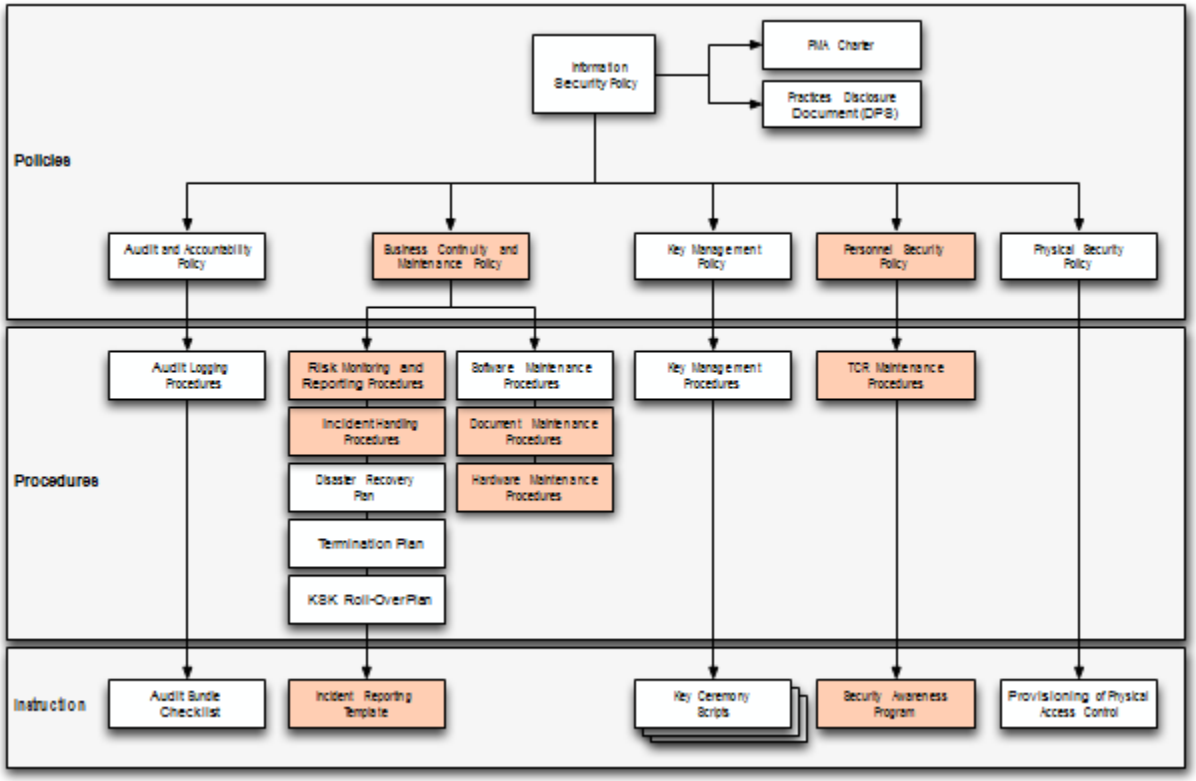
This document is the DNSSEC Practice Statement (DPS) for the Root Zone Key Signing Key (KSK) Operator. It states the practices and provisions that are used to provide Root Zone Key Signing and Key Distribution services. These include, issuing, managing, changing and distrib with the specific requirements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

Copyright Notice

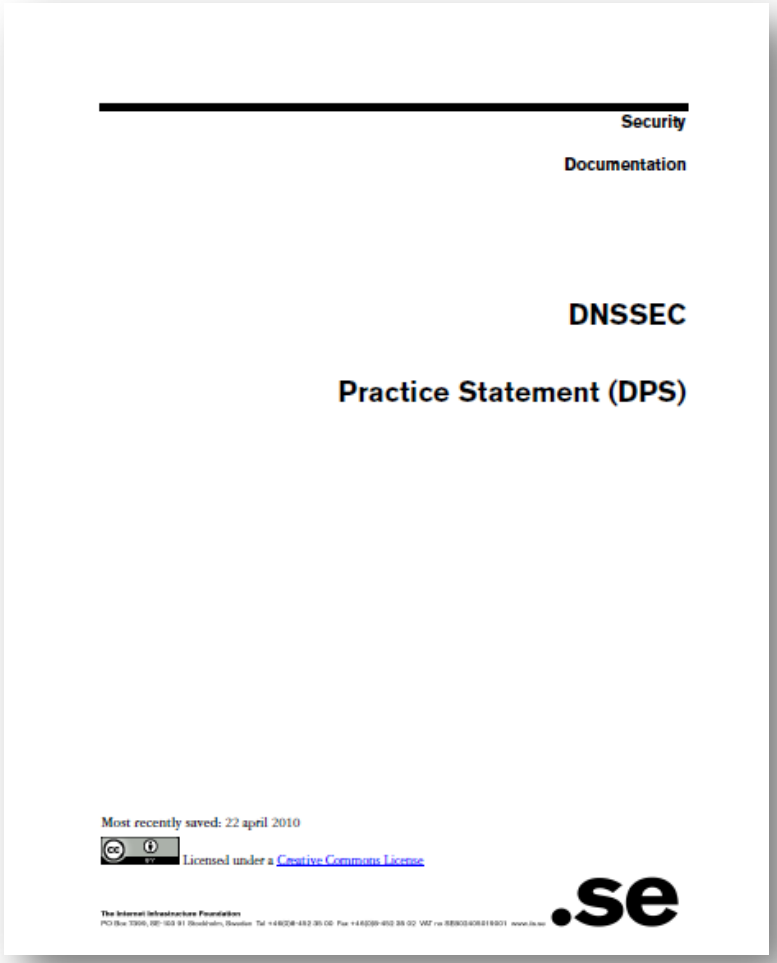
Copyright 2009 by VeriSign, Inc., and b Assigned Names and Numbers. This work

Root DPS

91 Pages and tree of other documents!



Documentation - .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

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

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 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.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 ~$12)
  - AthenaSC IDProtect ~$30
  - Feitian ~$5-10
  - Aventra ~$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 into /dev/random
(FBSD=dbrg+entropy/Linux=entropy?)

✓ 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

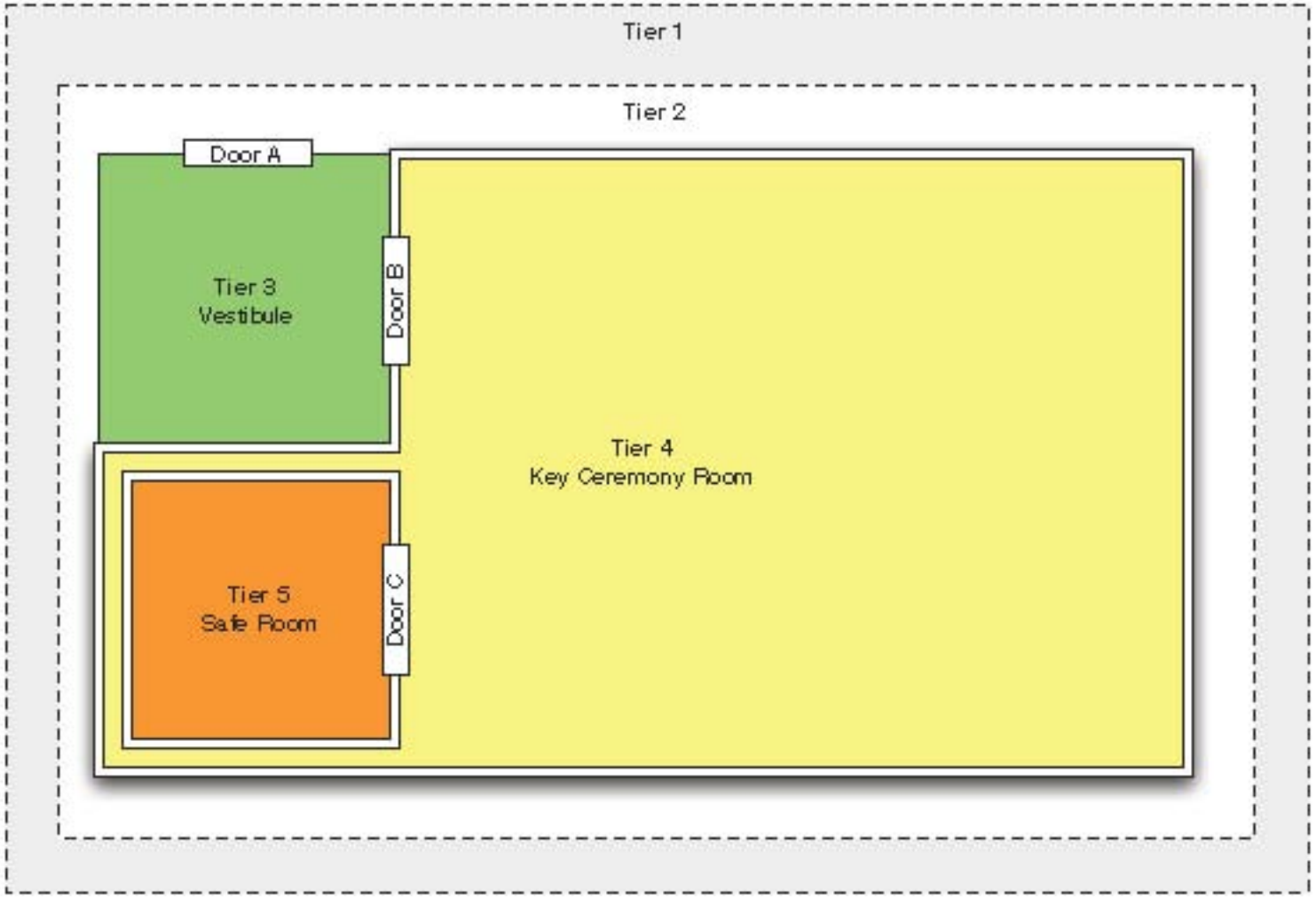
Root, .FR, .CA …

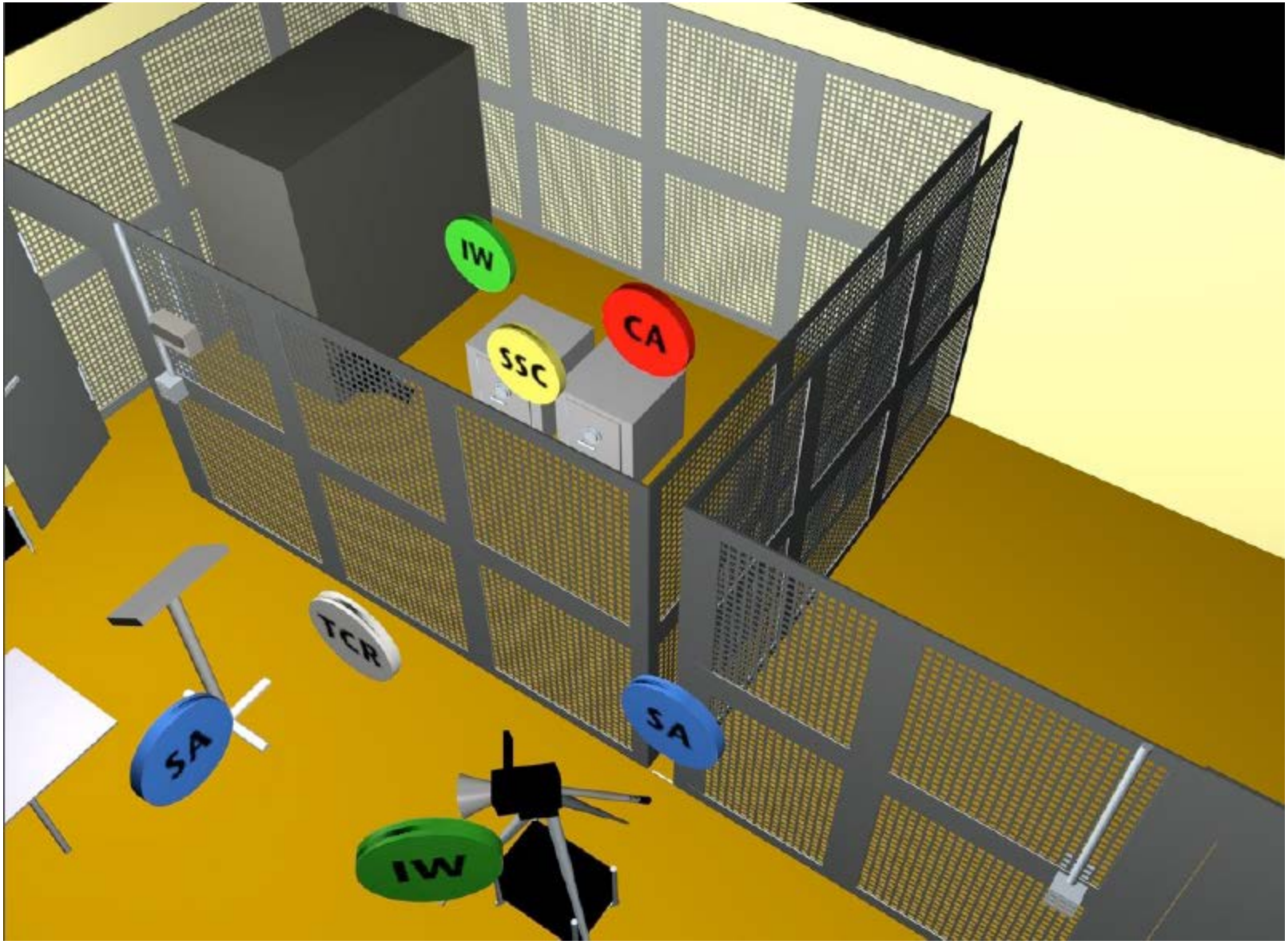
Crypto – FIPS Level 3 HSM

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

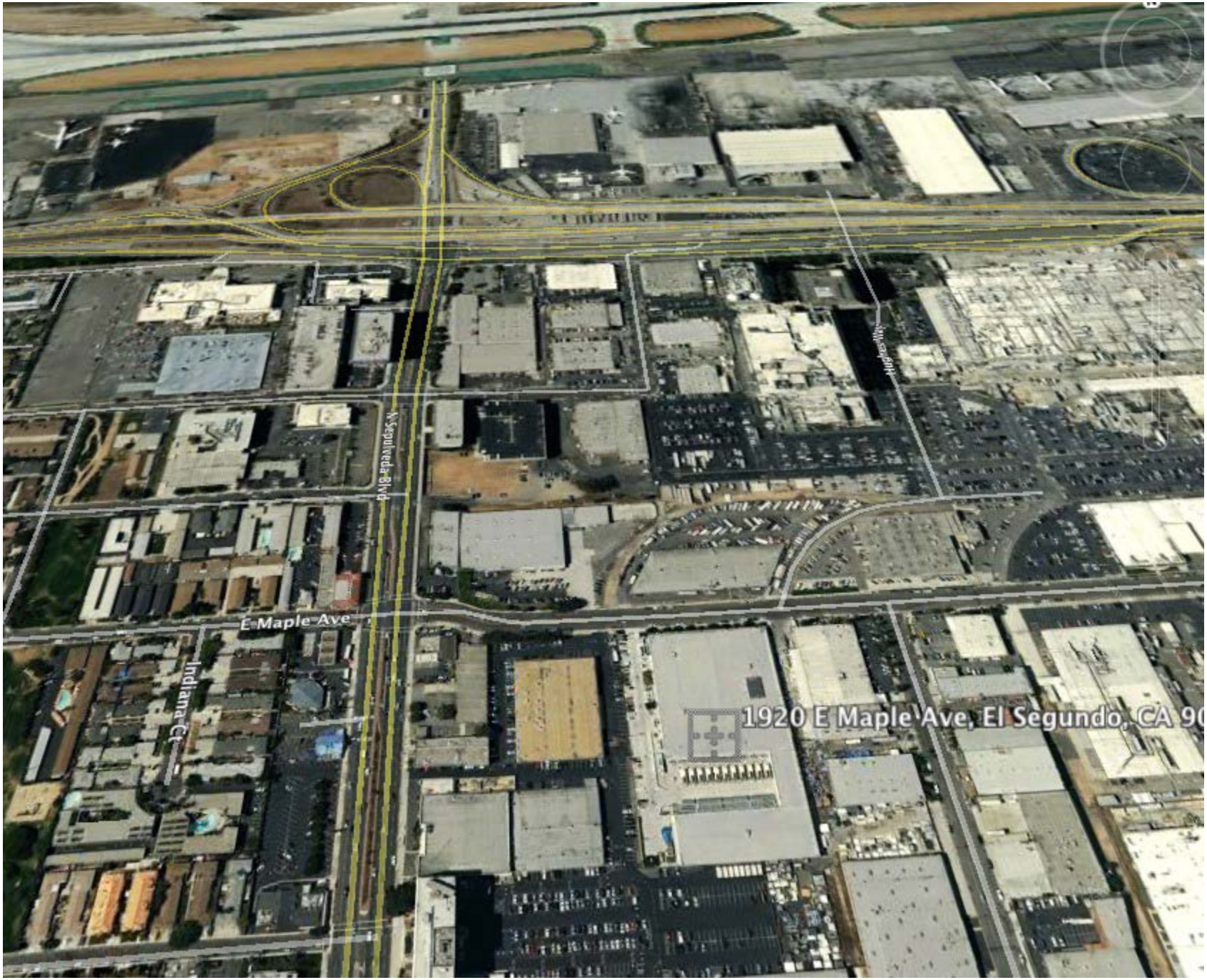
An implementation can be thi$

Physical Security




IW
SSC
CA
TCR
SA
SA
IW

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


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


January 27, 2010


NOTICE
NOTICE
NOTICE
NO FOOD
OR DRINK
NOTICE
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
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)

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

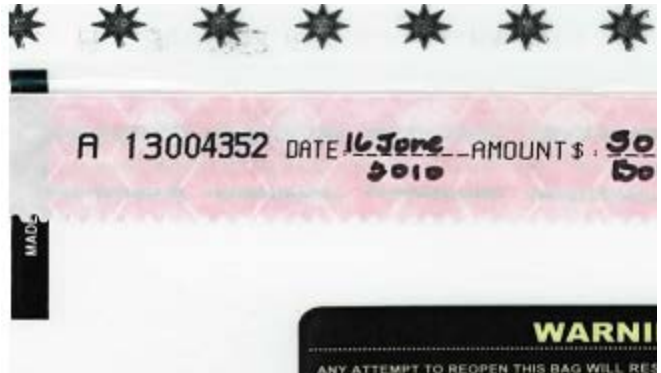
Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

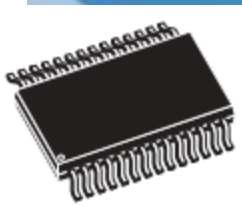
Signature:

Dated: 20 March 2008

Director, Industry Program Group
Communications Security Establishment

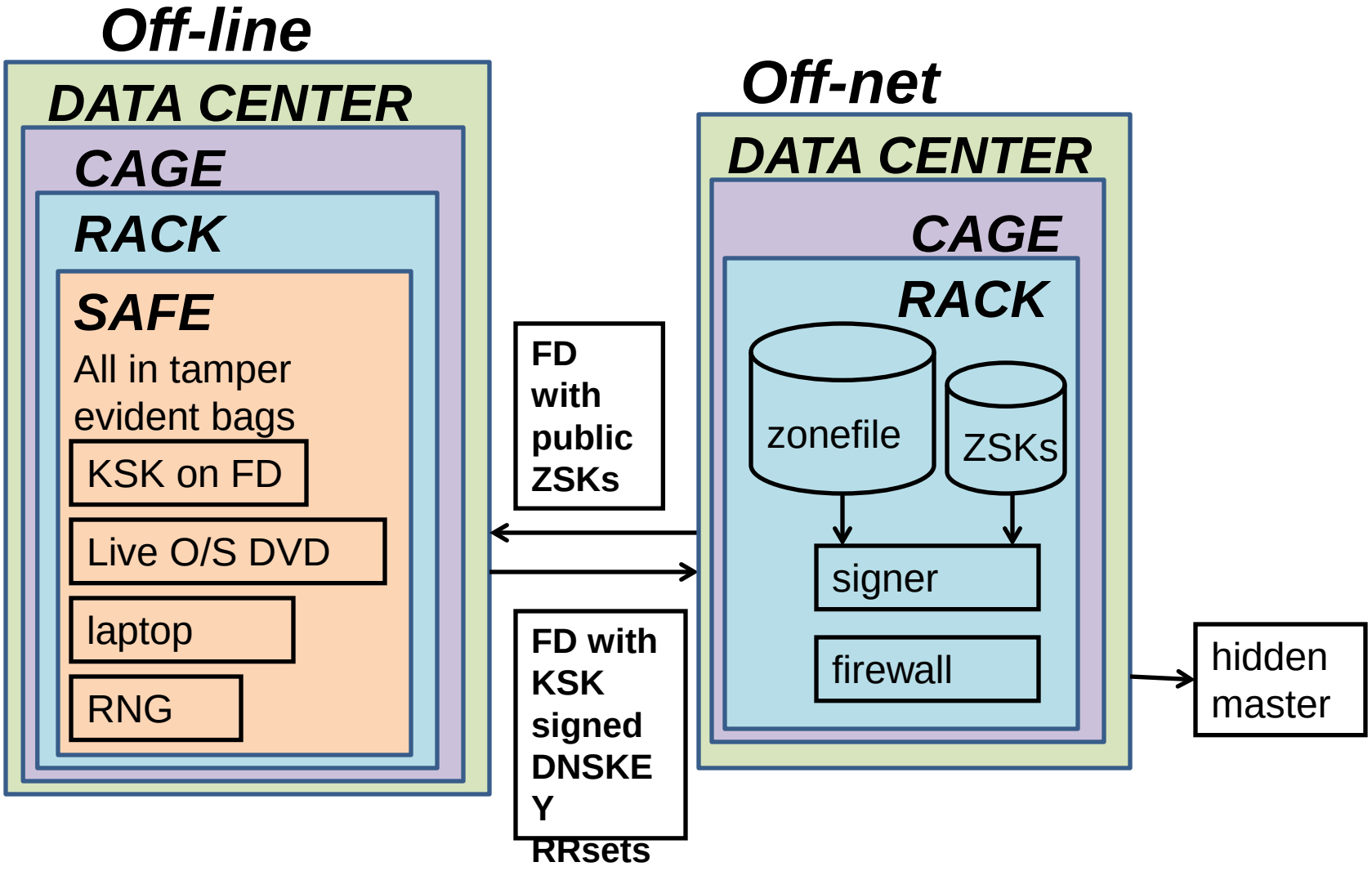


..or this (from .cr)



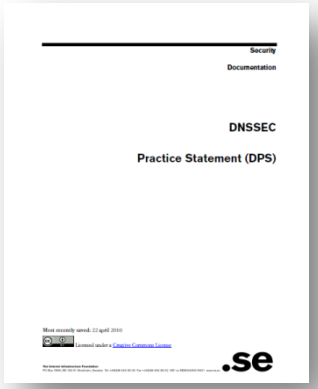
Animated slide

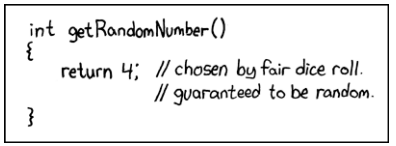
…or even this


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

But all must have:

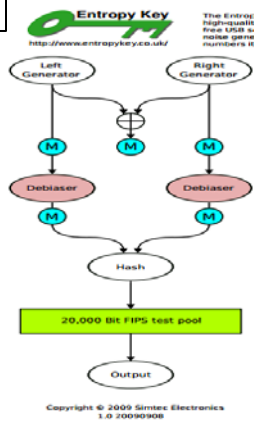
- Published practice statement
  - Overview of operations
  - Setting expectations
    - Normal
    - Emergency
  - Limiting liability
- Documented procedures
- Multi person access requirements
- Audit logs
- Monitoring (e.g., for signature expiry)
- Good Random Number Generators





Intel RdRand

DRBGs
FIPS 140

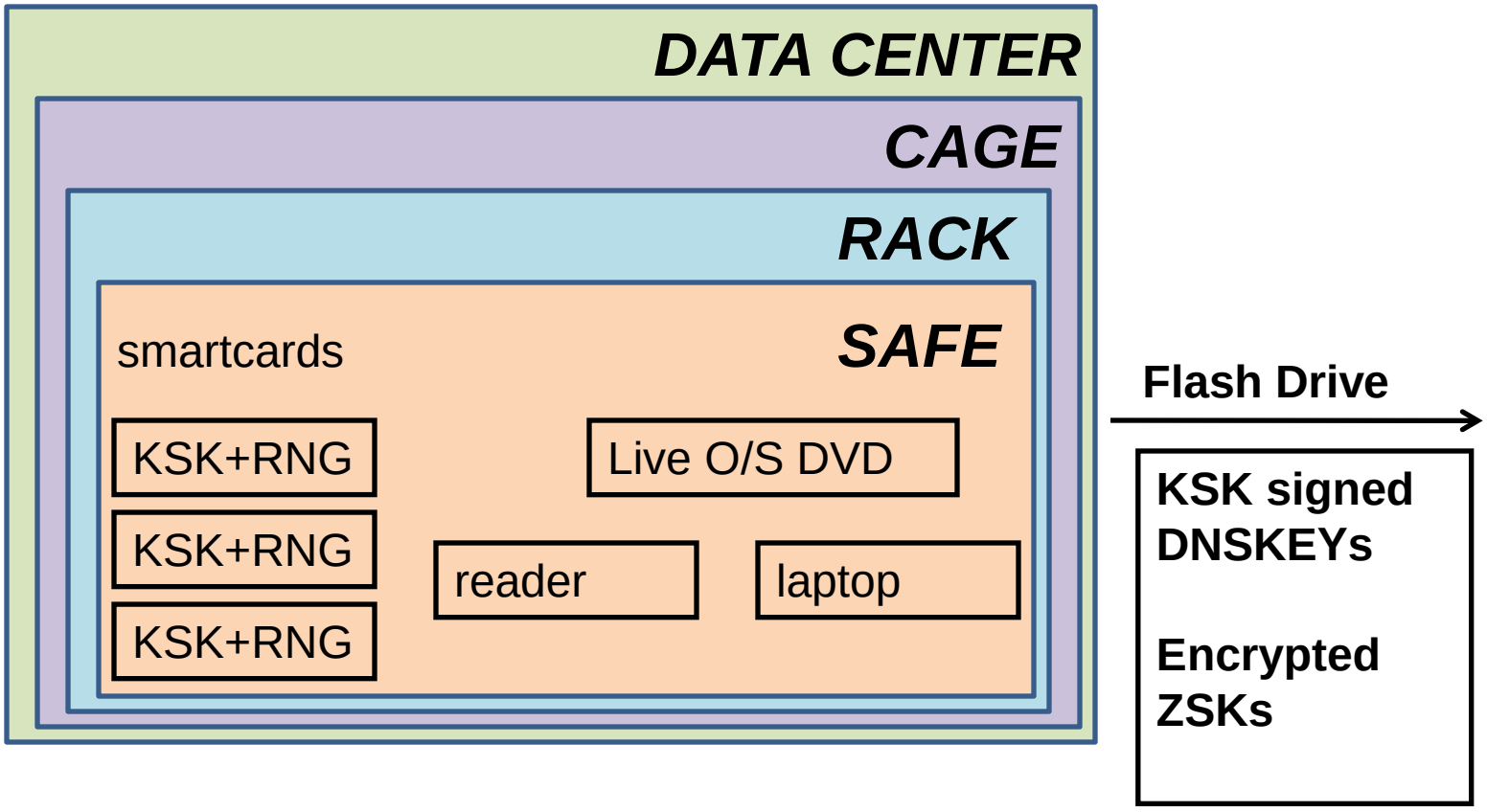


Useful IETF RFCs:
DNSSEC Operational Practices http://tools.ietf.org/html/draft-ietf-dnsop-rfc4641bis
A Framework for DNSSEC Policies and DNSSEC Practice Statements http://tools.ietf.org/html/draft-ietf-dnsop-dnssec-dps-framework

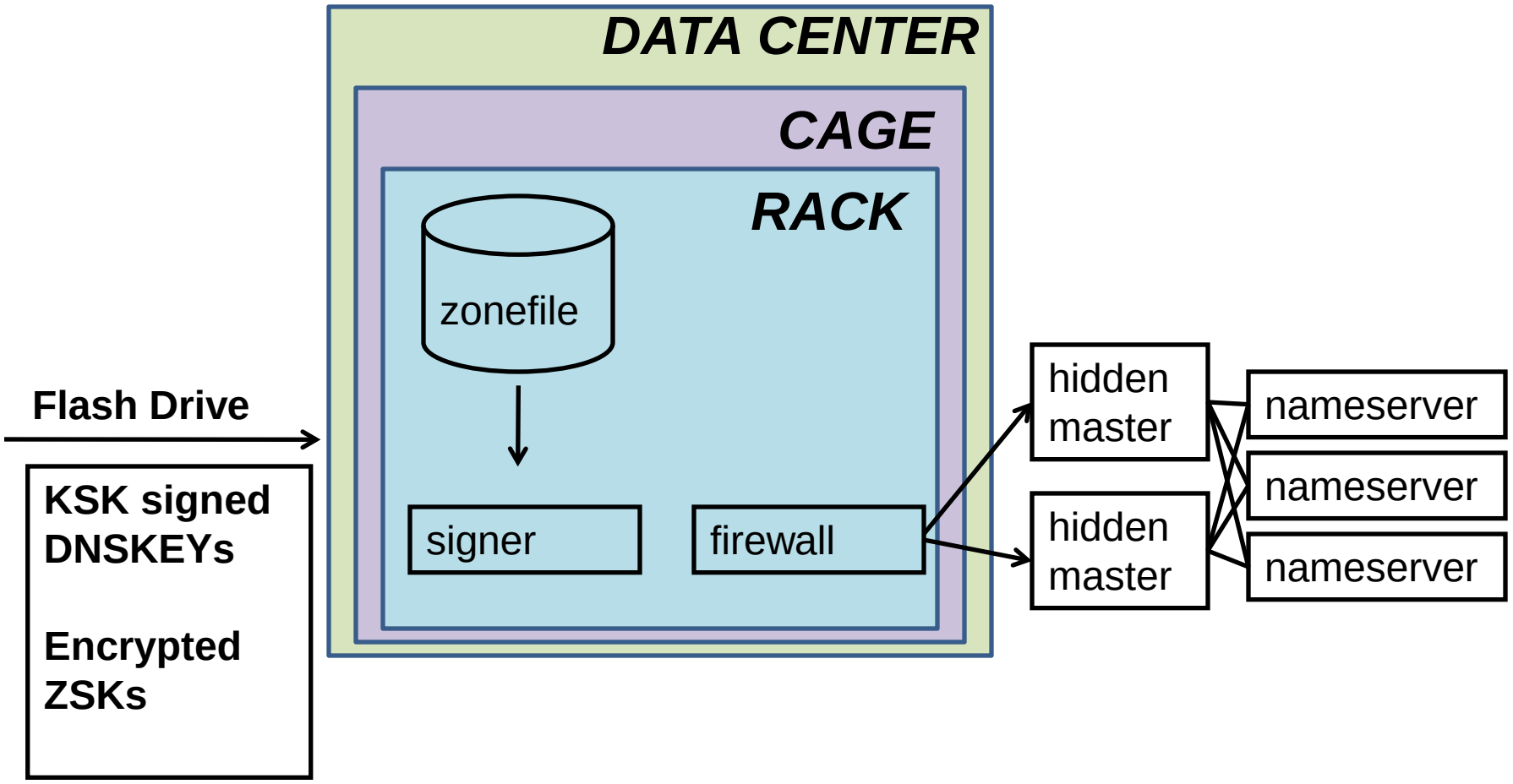
Demo Implementation

- 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

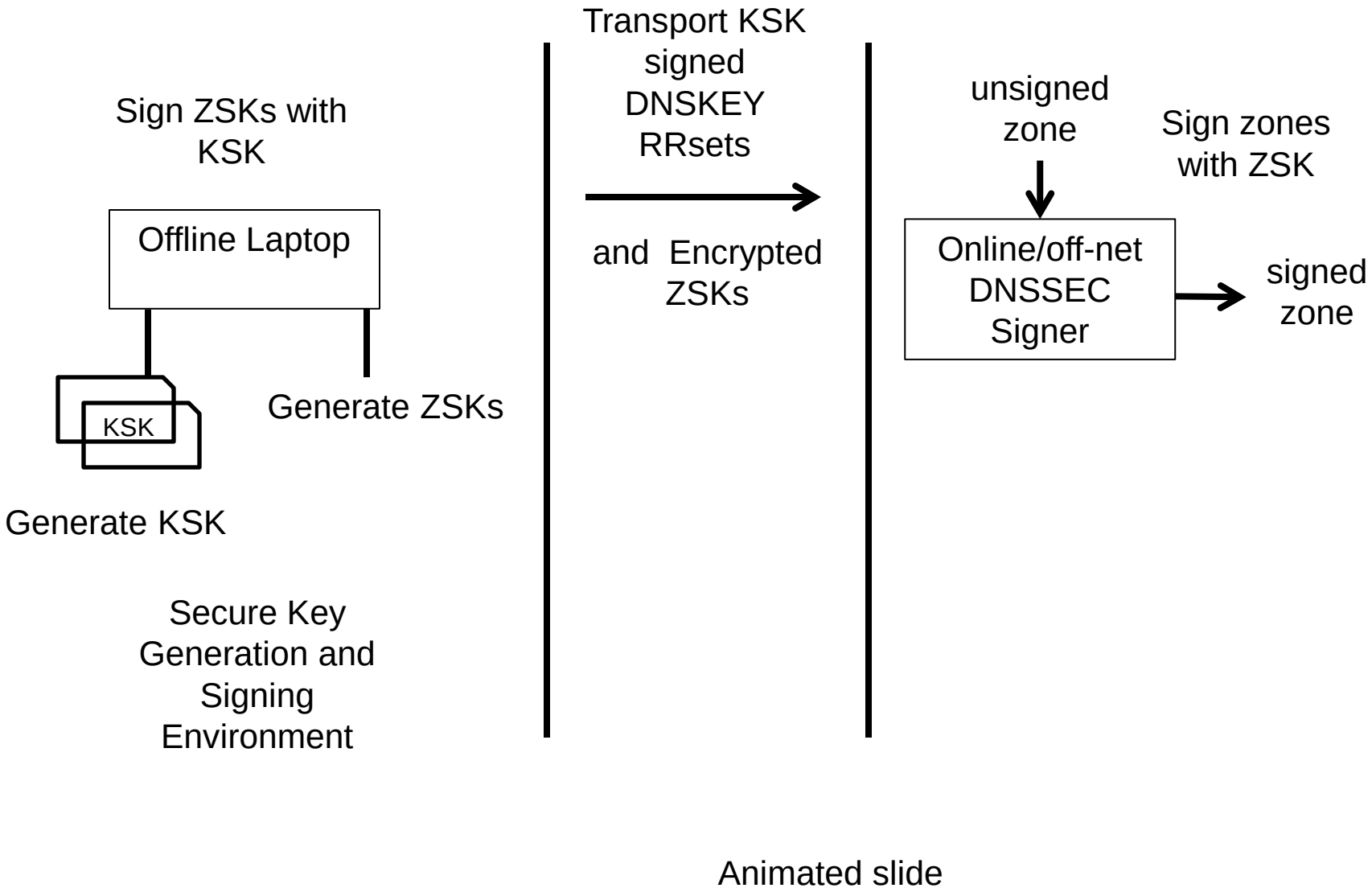
Off-Line Key generator and KSK Signer



Off-Net Signer

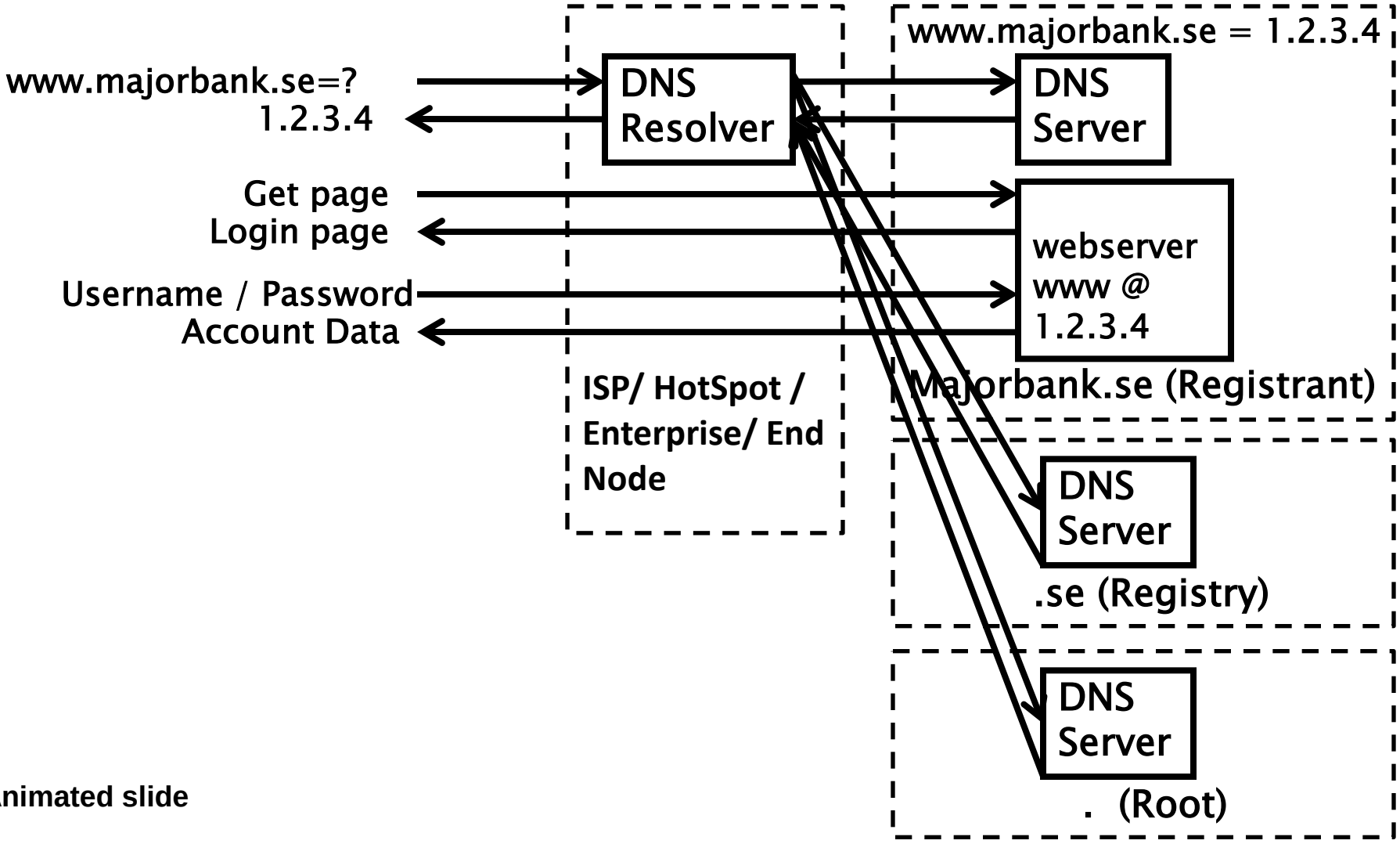


Key Management



Animated slide

DNS+DNSSEC



Animated slide

Simple Key Management Scripts

Keeping things signed

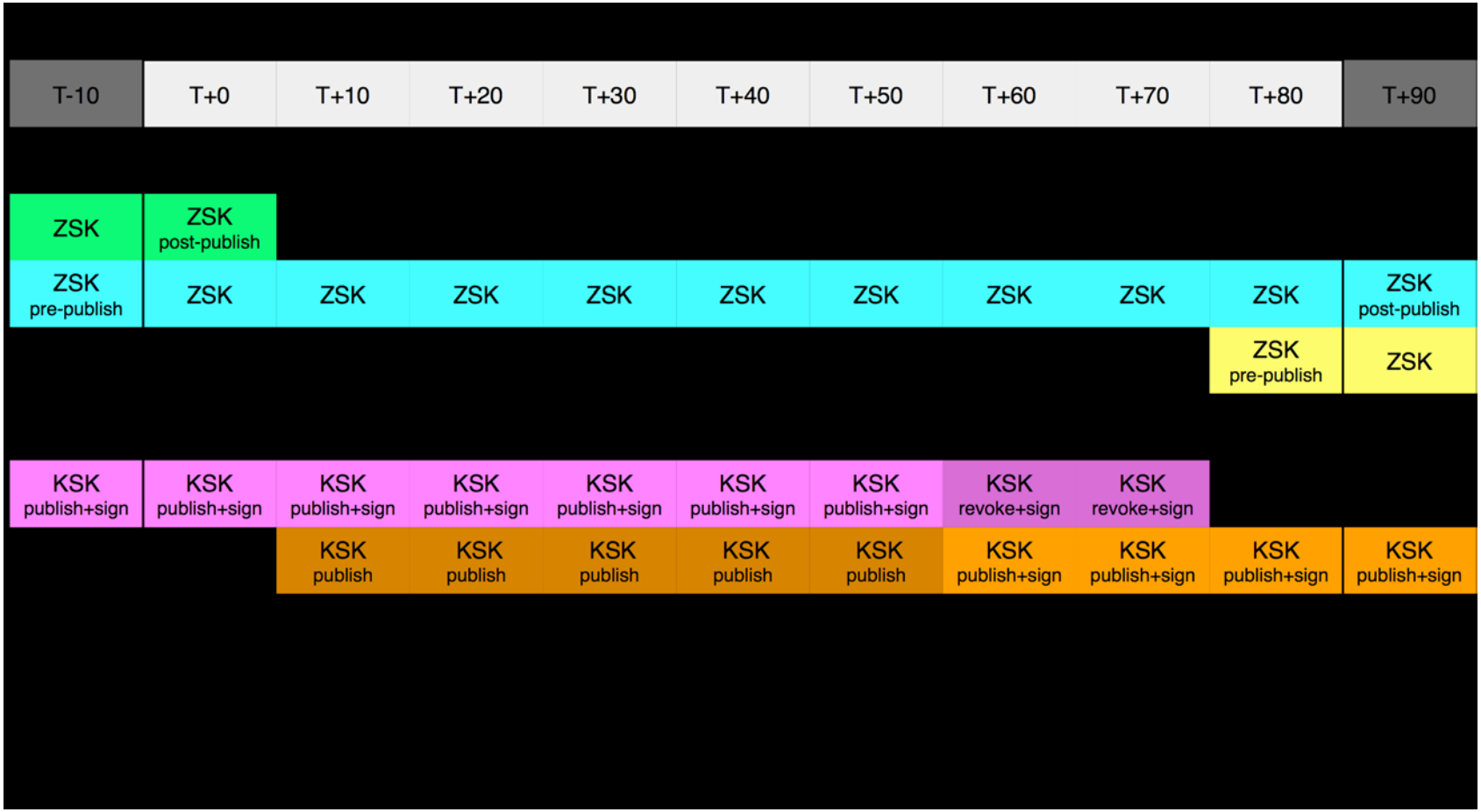
- If the signatures are going to expire soon, sign the zone
- Define “soon”
- Also sign if a record has changed
- That’s it!

```
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



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
```