DNSSEC Implementation Considerations and Risk Analysis

ENOG 12 Yerevan, Armenia Oct 2016
richard.lamb@icann.org

DNS is a part of all IT ecosystems (much more than one expects)

HealthCare.gov

US-NSTIC effort

+1-202-709-5262 VoIP

MasterCard

Google

OpenID

facebook

ebay

AADHAAR

Google PayPal facebook

Identity provider*		exchanges		Relying party*
Attribute provider*				
		user		Online store
				Bank
				Government

Bank
Government
Employer
University
Cell phone provider
ISP

*certified

PayPal

RSA SecurID 159 759.
Secured by RSA

OECS ID effort

SVERIGE SWEDEN SUÈDE
Nationalitet/Nationality
SVENSK/SWE
Kortnummer/Card No. 45123456
Personnr./Personal Id. No. 610321-3499
Innehavarens namnteckning/Holder's signature
SPECIMEN
Längd/Height 177 CM
Kön/Sex MXM
Födelsedatum/Date of birth 21 MAR/MAR 61
Efternamn/Surname SPECIMEN
Förnamn/Given name SVEN
Utfärdat/Date of issue 25 JUL/JUL 07
Giltigt t.o.m/Date of expiry 25 JUL/JUL 12
Myndighet/Authority POLISMYNDIGHETEN I STOCKHOLMS LÄN

amazon Prime

e-Passport symbol

PASSPORT

COUNTRY of Origin

VASCO 554322
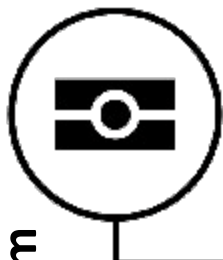
ICP Brasil
O Brasil na era da certificação digital

O chip perm armazenam dados sobre

DATA NASCIMENTO 10/05/1975
FILIAÇÃO JOÃO CARVALHO MARIA CARVALHO

DiGiNotar
A VASCO COMPANY

Trust frameworks are not new

Identity providers		Relying parties
VISA AMERICAN EXPRESS	Exchange (clearing house)	TOK&STOK
MasterCard		C&C casa&construção
	users	amazon.com
		macys

COMODO
Creating Trust Online®

Smart Electrical Grid

Norton SECURED
powered by VeriSign

lamb@xtcn.com

Certificate

| General | Details | Certification Path |

Certificate Information

This certificate is intended for the following purpose(s):

N/F BST 01.01.1971
47101010033
A1410634
21.02.2012

CARVALHO<FERNANDA<<<<<<<

mydomainname.com

The Problem:
DNS Cache Poisoning Attack

www.majorbank.se = 1.2.3.4

www.majorbank.se=?

5.6.7.8

DNS Resolver

DNS Server

Attacker
www.majorbank.se = 5.6.7.8

Get page
Login page

Username / Password
Error

Attacker webserver
www @ 5.6.7.8

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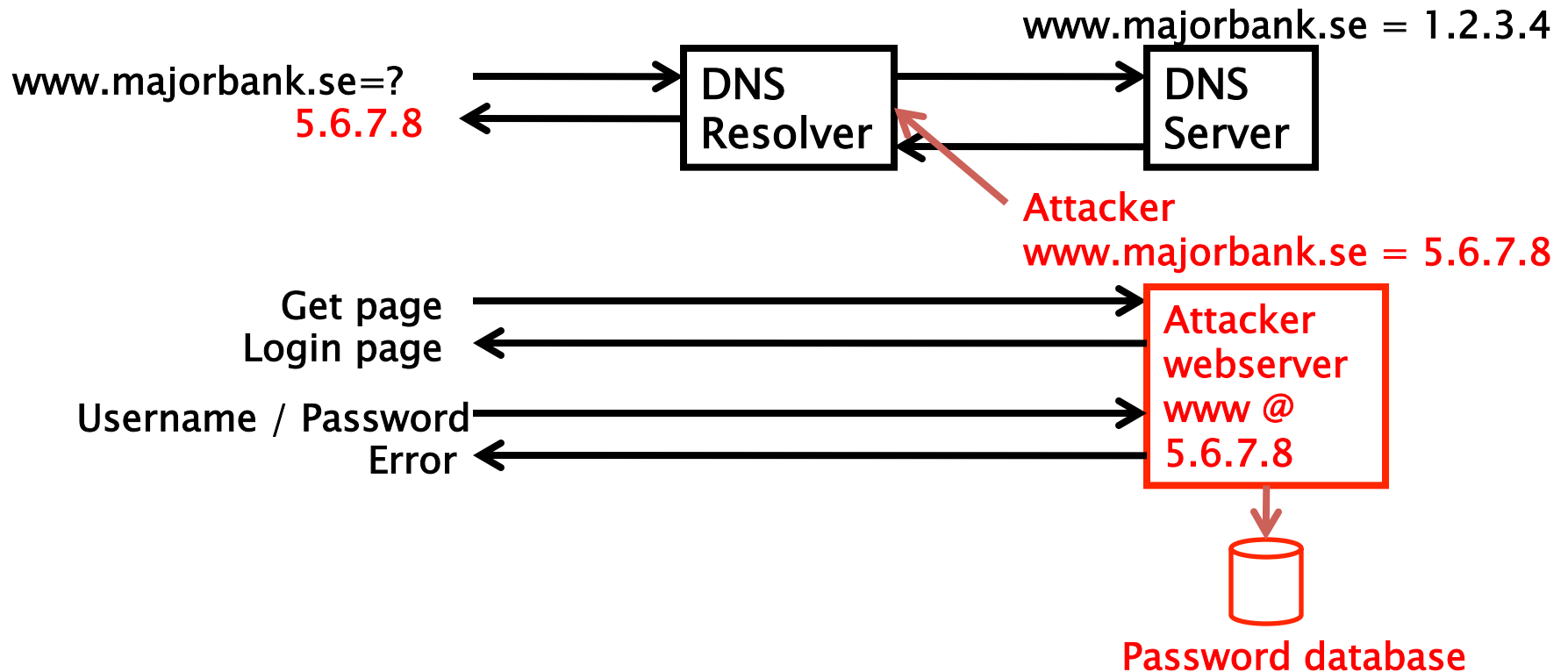
The Bad: DNSChanger - 'Biggest Cybercriminal Takedown in History' – 4M machines, 100 countries, $14M

DNS Malware: Is Your Computer Infected?

DNS—Domain Name System—is an Internet service that converts user-friendly domain names, such as www.fbi.gov, into numerical addresses that allow computers to talk to each other. Without DNS and the DNS servers operated by Internet service providers, computer users would not be able to browse web sites, send e-mail, or connect to any Internet services.

Criminals have infected millions of computers around the world with malware called DNSChanger which allows them to control DNS servers. As a result, the cyber thieves have forced unsuspecting users to fraudulent websites, interfered with their web browsing, and made their computers vulnerable to other kinds of malicious software.

http://www.fbi.gov
http://www.fbi.gov/contact-us

123.456.789
987.654.321

Legitimate DNS

Securing it

- DNS converts names (www.bncr.fi.cr) to numbers (201.220.29.26)

- Make sure we get the right numbers (DNSSEC)
- Verify the identity and encrypt data

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**

- **25 Dec 2010 Tunisia DNS Hijack**

- **2009-2012 google.***

  - **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.**

DigiNotar®
A VASCO COMPANY

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

The Business Case for DNSSEC

- Cyber security is becoming a greater concern to enterprises, government, and end users. DNSSEC is a key tool and differentiator.

- DNSSEC is the biggest security upgrade to Internet infrastructure in over 20 years. It is a platform for new security applications (for those that see the opportunity).

- DNSSEC infrastructure deployment has been brisk but requires expertise. Getting ahead of the curve is a competitive advantage.

DNSSEC interest from governments

- Sweden, Brazil, Netherlands, Czech Republic 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. 85% operational. [3]

USG DNSSEC Enabled Domains

1317 tested on 2013.09.10

Operational In Progress No Progress

12%

3%

85%

[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
http://fedv6-deployment.antd.nist.gov/snap-all.html
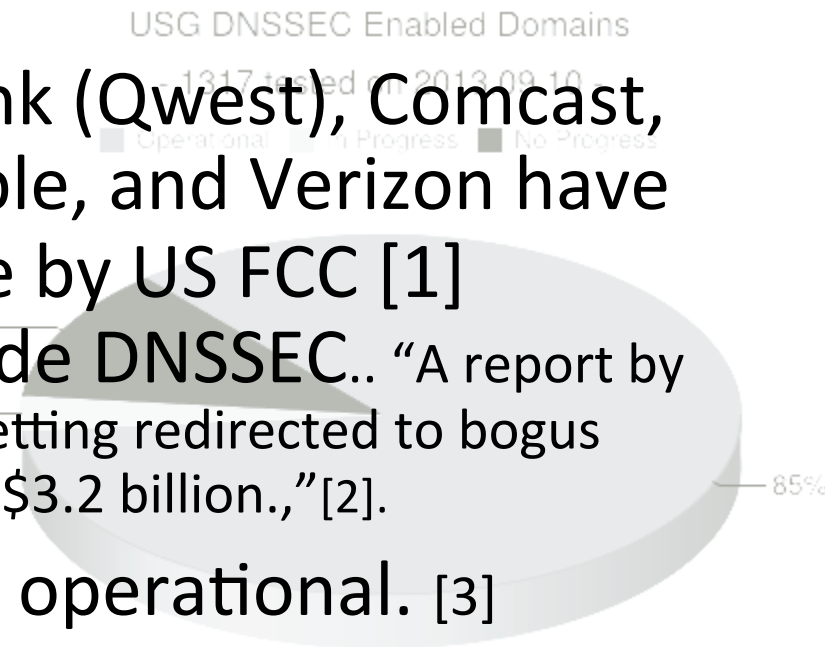
Use of DNSSEC Validation for World (XA)

Thank you Geoff
Huston

Domains with DS Records

COM
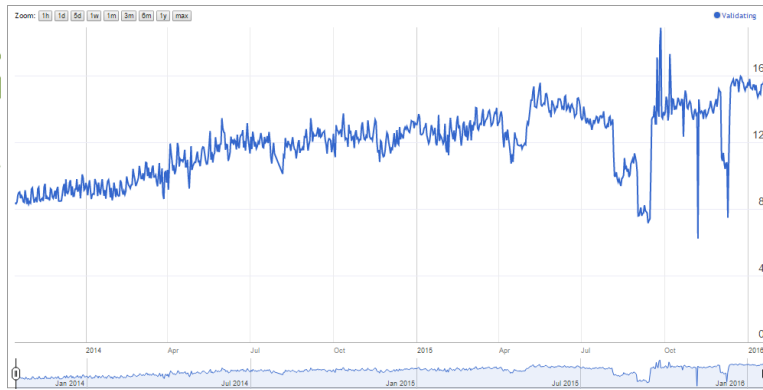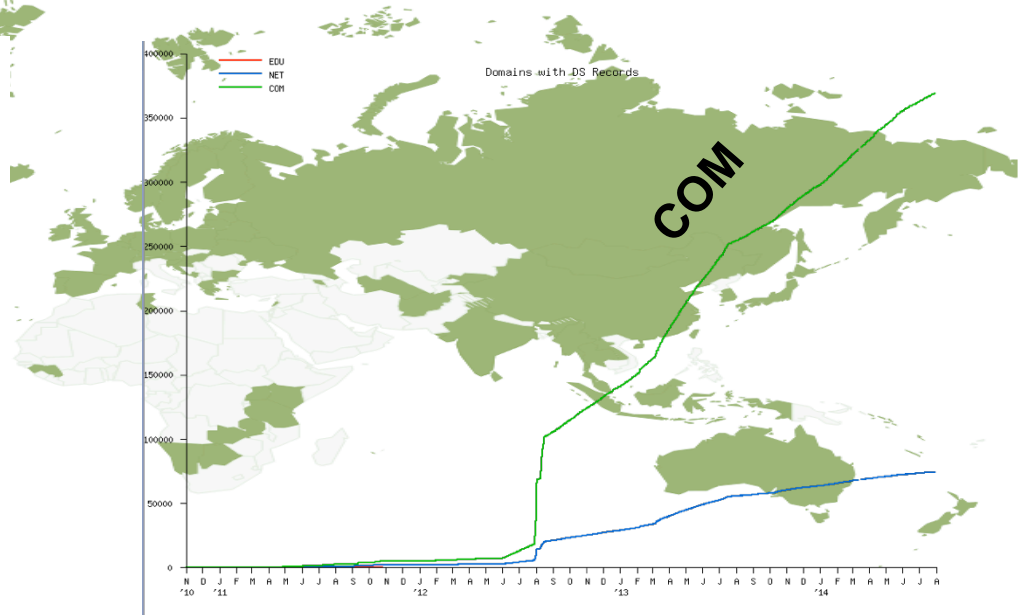
Total number of DNSSEC delegations in the .NL zone: 1766343

NL

Data last updated 33 minutes ago
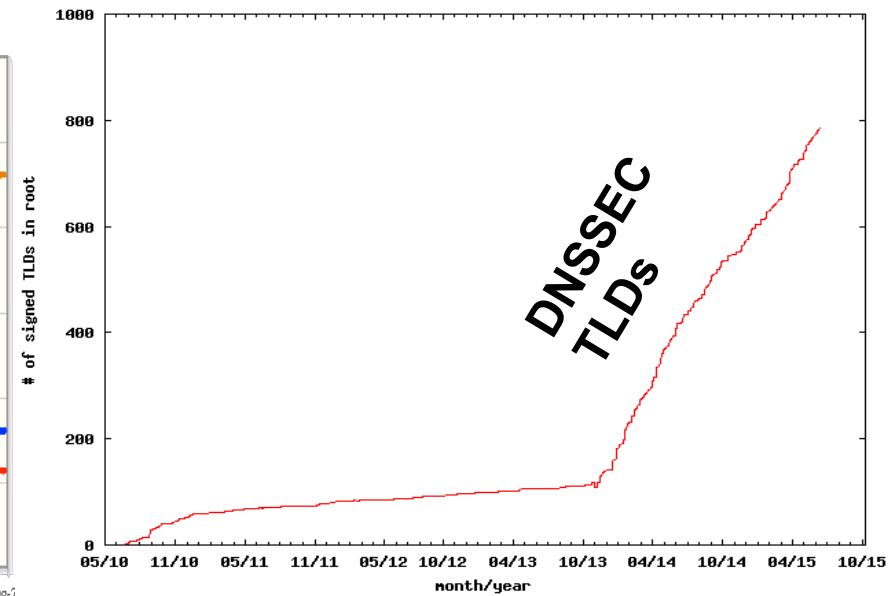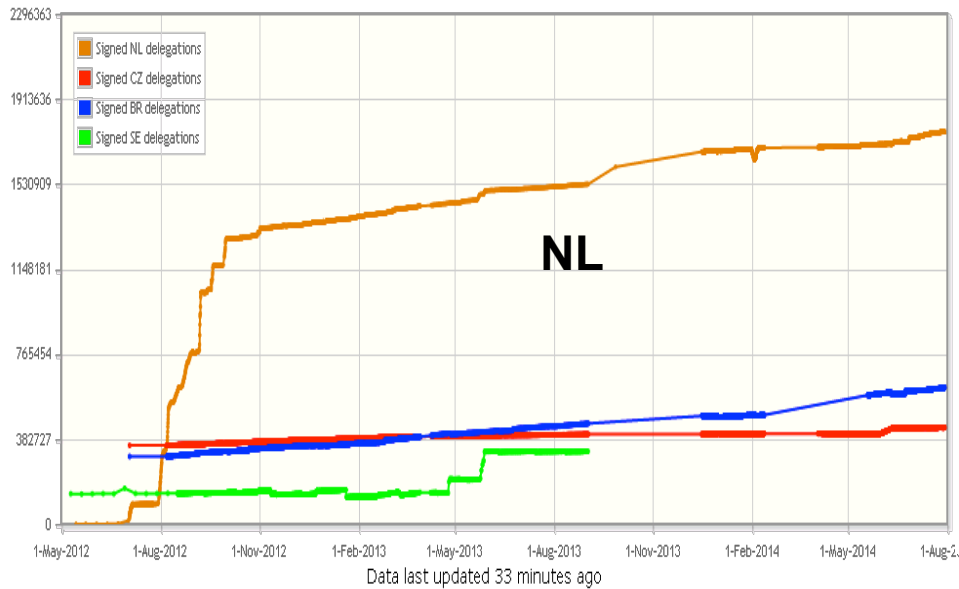
DNSSEC
TLDs

Feb 2011

DNSSEC - Where we are

- Deployed on 1340/1500 TLDs (2 Oct 2016 .am .in .af .tm .kg .cn .se .de .ru .рф .com .uk .nl .fr .in .jp .us .my ماليسيا .asia .tw 台灣, .kr 한국 .net, .org, .post, +ntlds, .ibm .berlin)

- Root signed** and audited

- > 89% of domain names could have DNSSEC

- Required in new gTLDs. Basic support by ICANN registrars

- Growing ISP support* - ~16% end users "validate".

- 3rd party signing solutions***

- S/W H/W support: NLNetLabs, ISC, Microsoft, PowerDNS,KNOT, Secure64…? openssl, postfix, XMPP, mozilla: early DANE support

- IETF standard on DNSSEC TLS certificates (RFC6698) and others

- Growing support from major players…(Apple iPhone/iPad, Google 8.8.8.8, hosting co Cloudflare DNSSEC by default, German email providers…)

Stats: https://rick.eng.br/dnssecstat/

* COMCAST /w 20M and others; most ISPs in SE ,CZ.

**Int'l bottom-up trust model /w 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 only ~3% 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 IT departments know about it or are too busy putting out other security fires.

- When they do look into it they hear old stories of FUD and lack of turnkey solutions and CDN support.

- Registrars*/CDNs/DNS providers see no demand leading to "chicken-and-egg" problems.

*but required by new ICANN registrar agreement
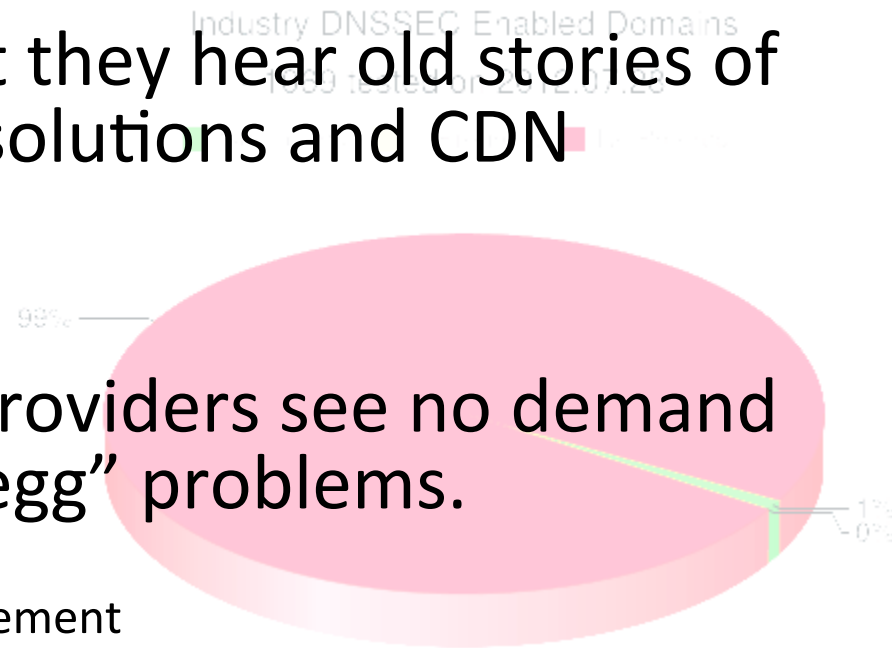
DNSSEC: A Global Platform for Innovation

or..

I* $mell opportunity !

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 (June 2010)

For Techies and other Dreamers

Too many CAs. Which one can we trust? DNSSEC to the rescue….

CA Certificate roots ~1482
Symantec, Thawte, Godaddy

DNSSEC root - 1

Internet of Things
IoT

Content security
Commercial SSL
Certificates for
Web and e-mail

Content security
"Free SSL"
certificates for Web
and e-mail and "trust
agility" **DANE**

Cross-
organizational and
trans-national
authentication and
security

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

Crypto currencies
and e-commerce?

E-mail security SMIME,
DKIM RFC4871

Securing VoIP

Login security
SSHFP RFC4255

Domain Names

https://www.eff.org/observatory
http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/

Opportunity: New Security Solutions

- Improved Web SSL and certificates for all*
- Secured e-mail (SMTP+S/MIME) for all*
- Validated remote login SSH, IPSEC*
- Securing VoIP
- Cross organizational authentication, security
- Secured content delivery (e.g. configurations, updates, keys) – Internet of Things
- Securing Smart Grid efforts
- Increasing trust in e-commerce
- Securing cryptocurrencies and other new models
- First global FREE PKI

A good ref
http://www.internetsociety.org/deploy360/dnssec/
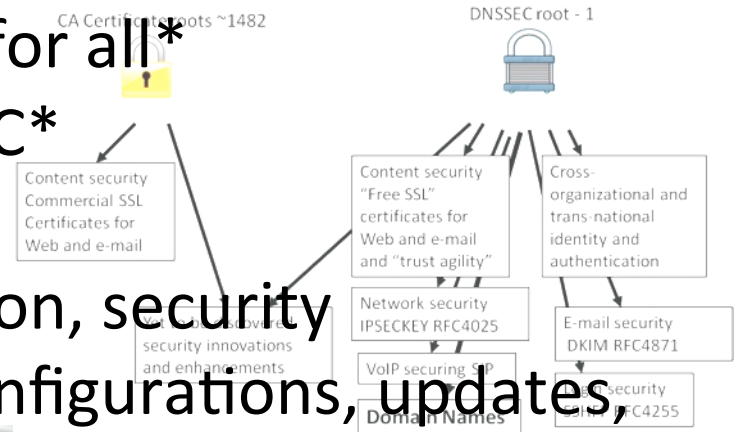
DNSSEC: Internet infrastructure upgrade to help address today's needs and create tomorrow's opportunity.

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
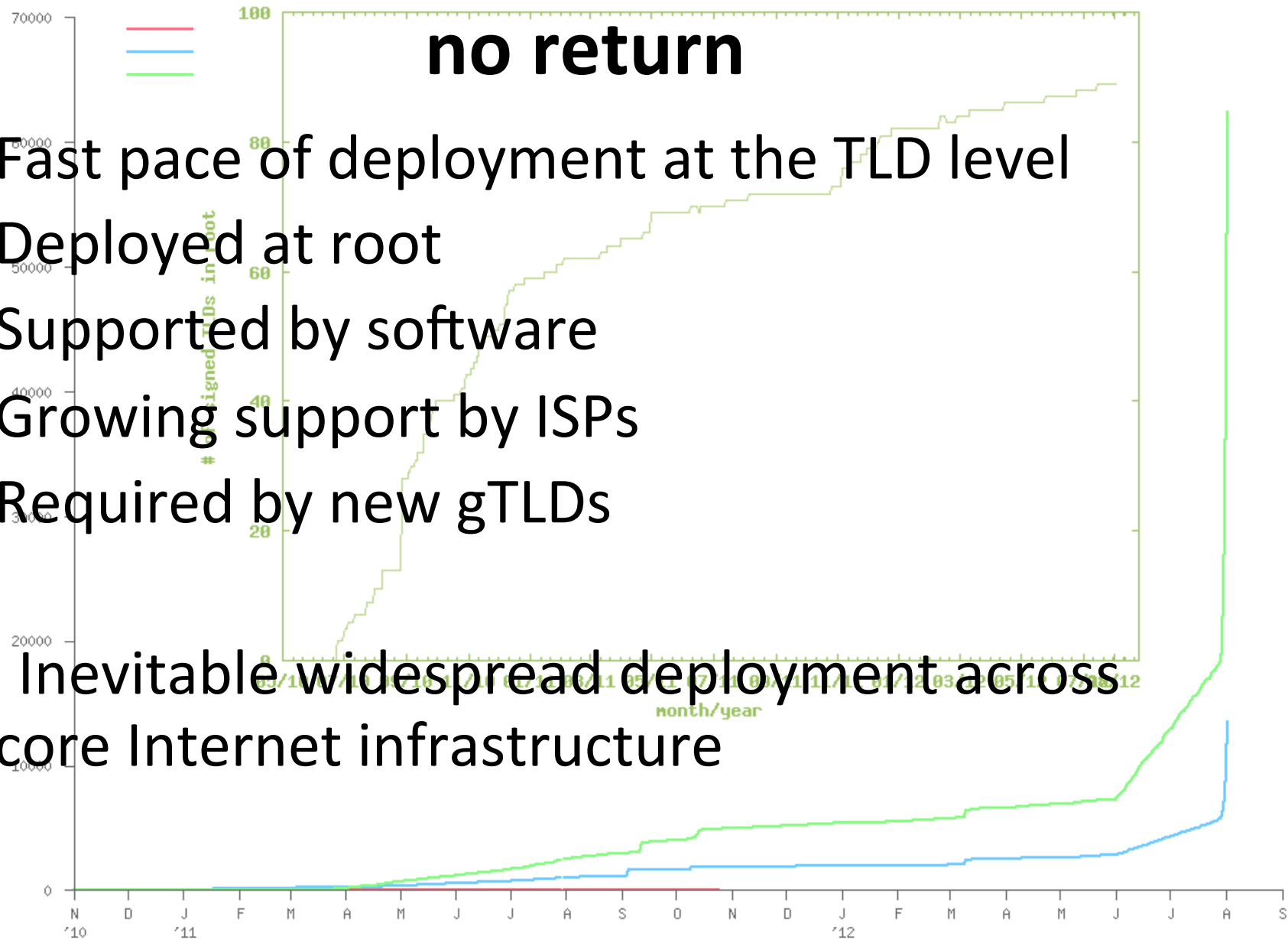
Design Considerations

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/
poAoRVDThHVOnXniaIj2WuGVbCGvUMjayDhVNk9vAQ
tVHUIAnxZXsIlP4ZbtIgtZ/
hbTKByySx1Y0u9aRD1ik=
```

One way to do this

keys

nameserver —— signer

mydomain.zone   mydomain.zone.signed

or…another

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
- 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)

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 DPS

91 Pages and tree of other documents!

Documentation - .SE

Security

Documentation

DNSSEC

Practice Statement (DPS)

Most recently saved: 22 april 2010

Licensed under a Creative Commons License
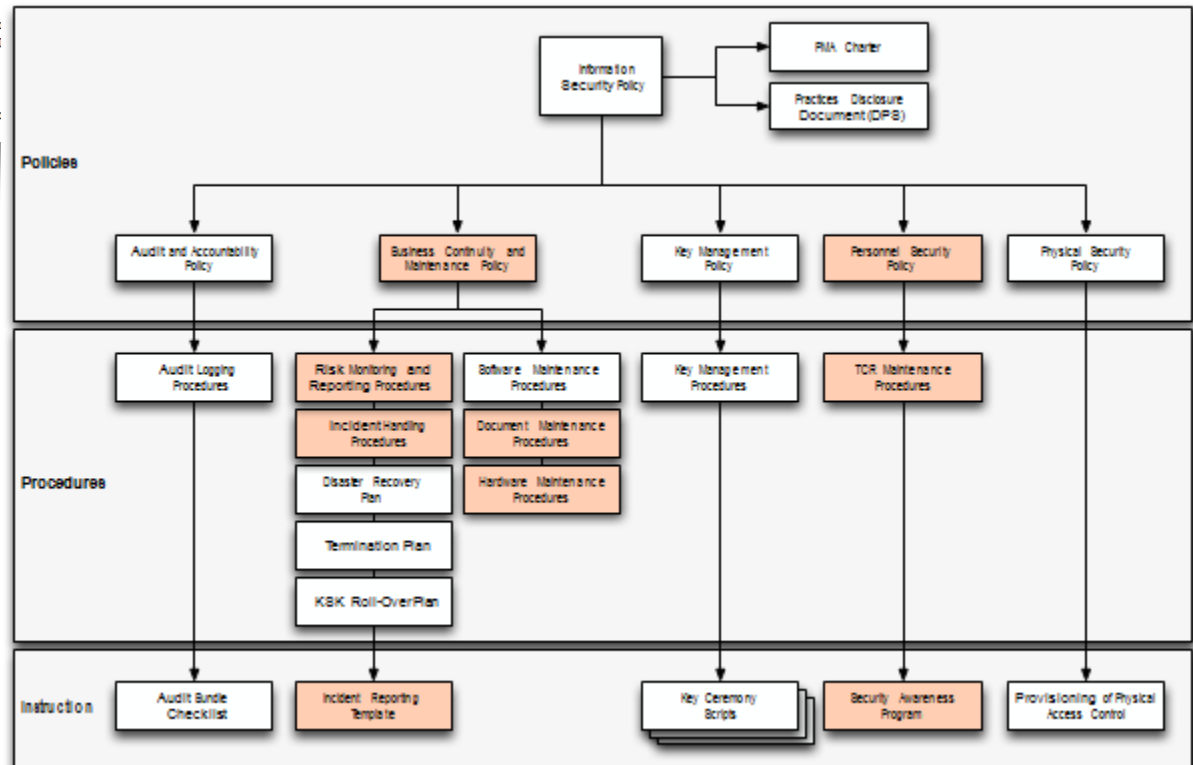
The Internet Infrastructure Foundation

.se
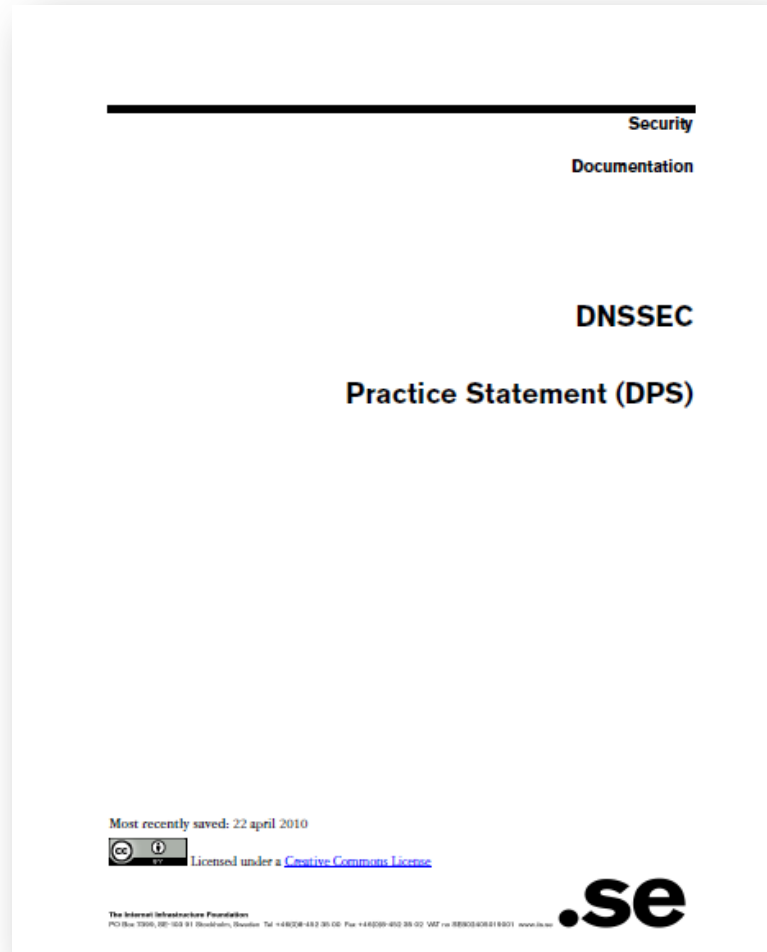
22 pages, Creative Commons License!

.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

SOC³ SysTrust for Service Organizations

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)
  - Smartcard HSM ~$20
  - Feitian ~$5-10
  - Aventra ~$11
- TPM
  - Built into many PCs
- Token
  - Aladdin/SafeNet/Feitian 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 800-90A)

✓ Built into CPU chips


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

https://www.nist.gov/news-events/news/2015/06/nist-revises-key-computer-security-publication-random-number-generation

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$
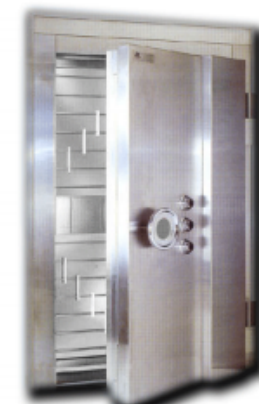
…or this

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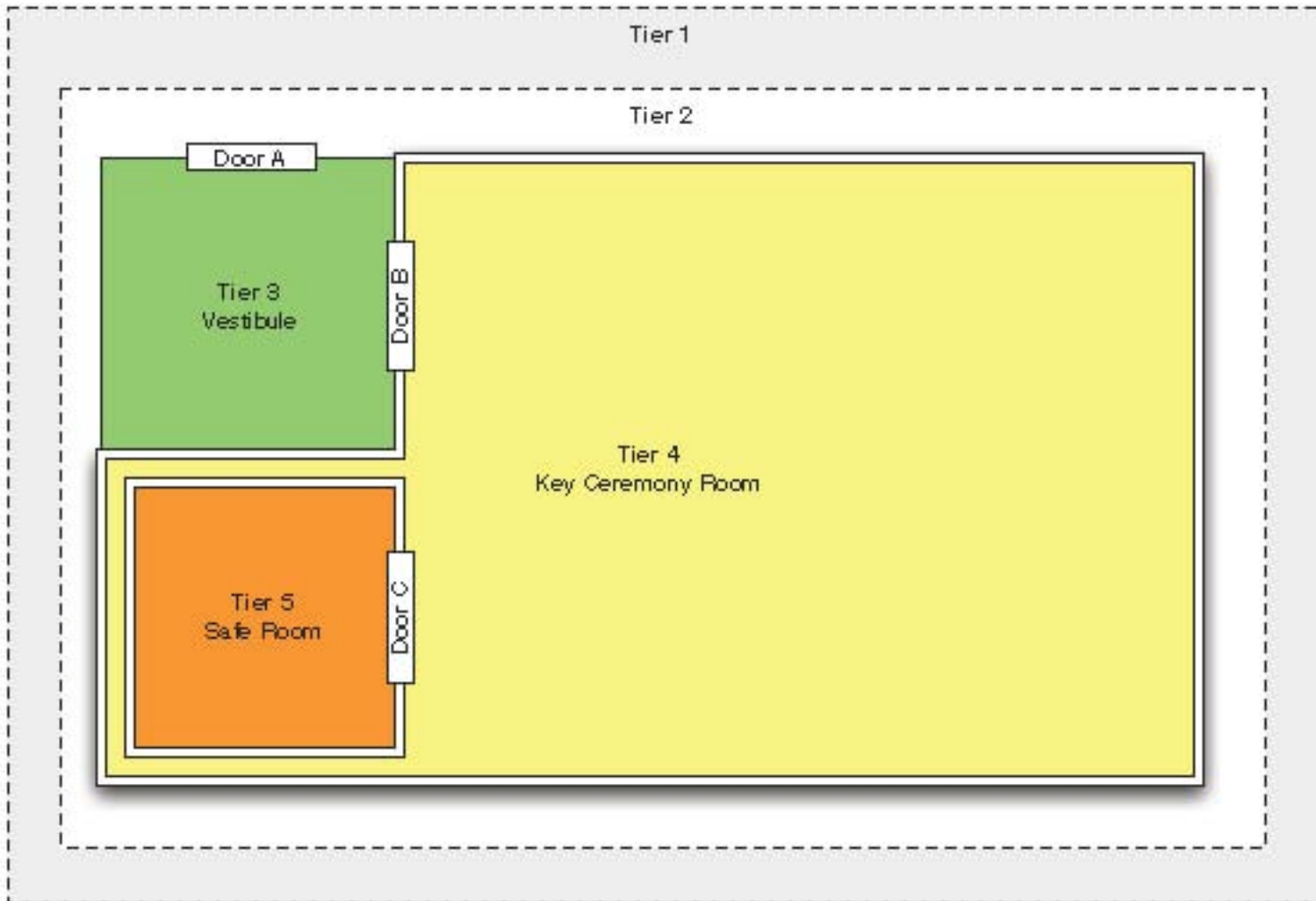
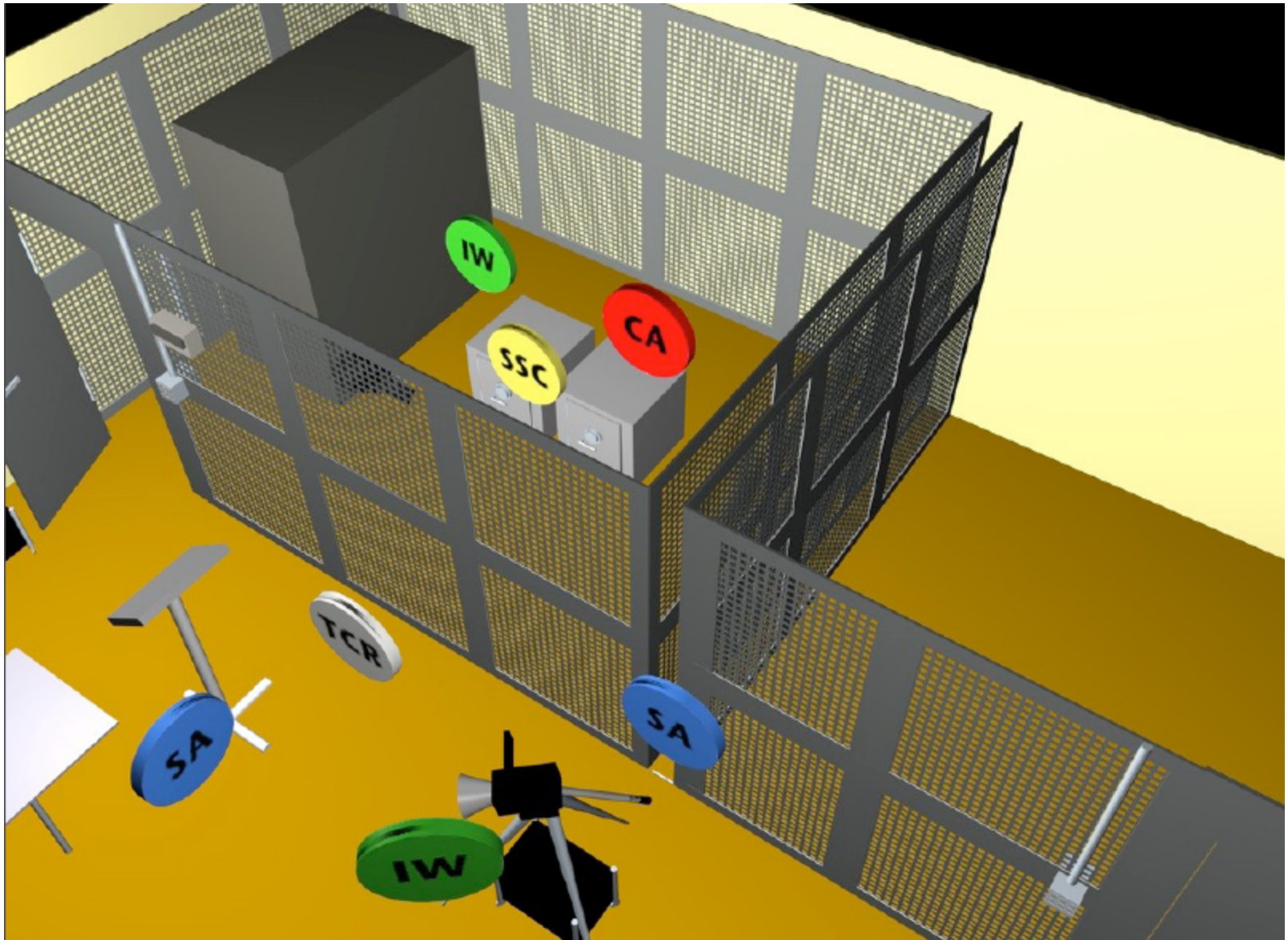http://singapore49.icann.org/en/schedule/wed-dnssec/presentation-dnssec-deployment-cn-26mar14-en.pdf

Physical Security

N Sepulveda Blvd

Hughes Way

E Maple Ave

Indiana Ct

1920 E Maple Ave, El Segundo, CA 90

January 27, 2010

One World. One Internet. Everyone Connected.

19036

…or this

TPM

+

FIPS 140-2 Valid...

five 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 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_

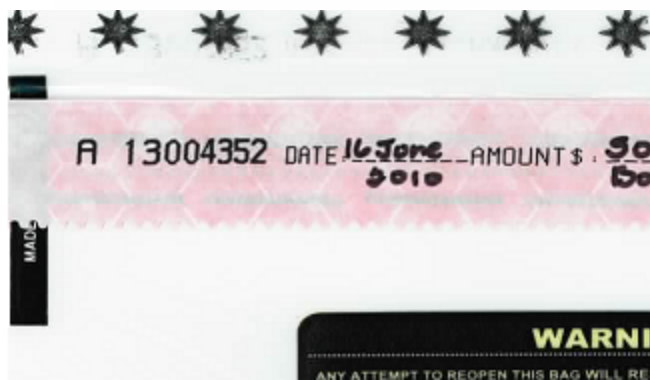Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____
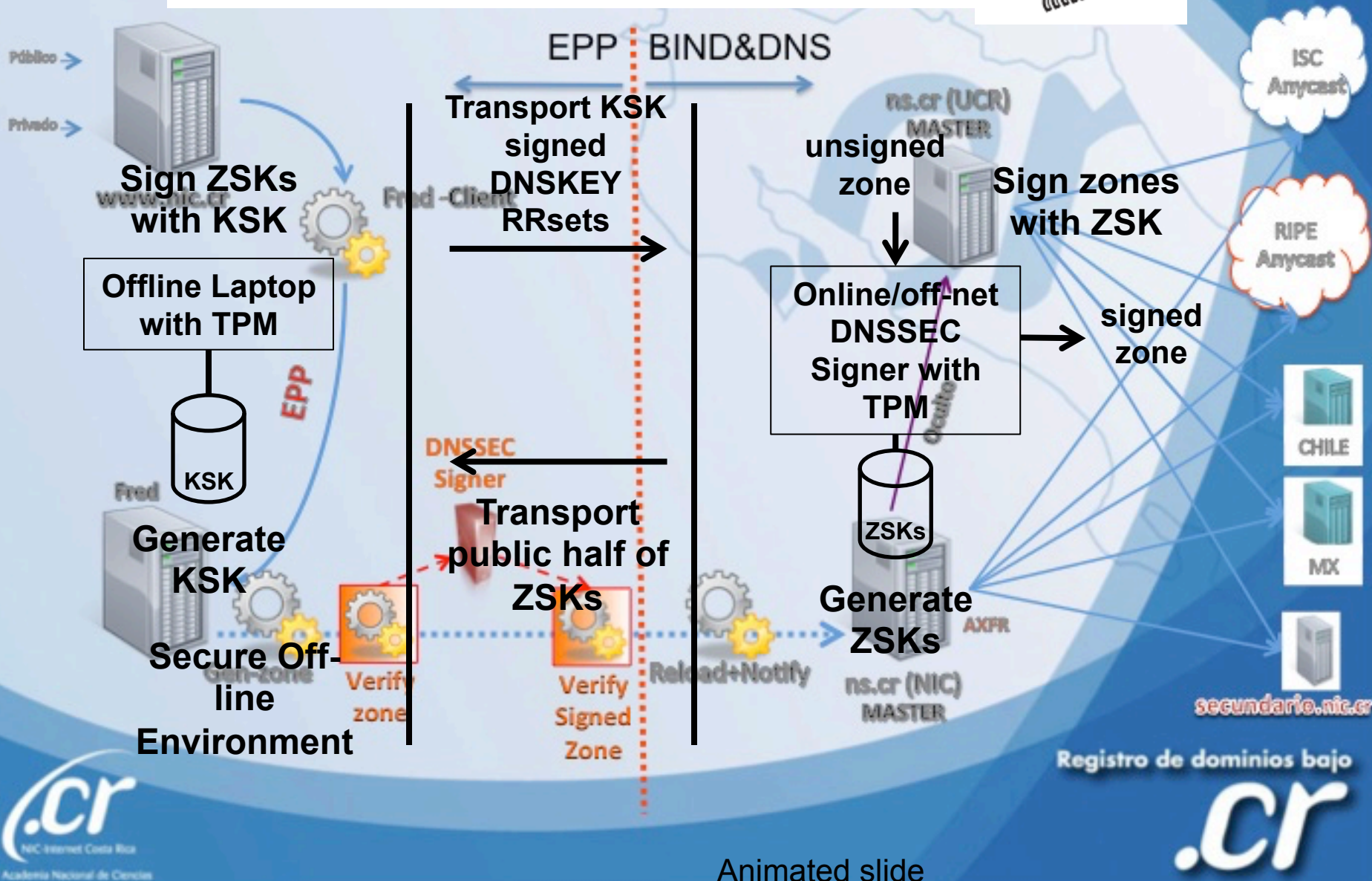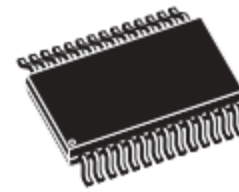
Dated: _20 March 2008_

A/ Director, Industry Program Group
Communications Security Establishment

A 13004352 DATE _16 June 2010_ AMOUNT $ _90.00_

WARNI...
ANY ATTEMPT TO REOPEN THIS BAG WILL RES...

..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

Off-net

DATA CENTER

CAGE

RACK

zonefile

ZSKs

signer

firewall

FD with public ZSKs

FD with KSK signed DNSKEY RRsets

hidden master
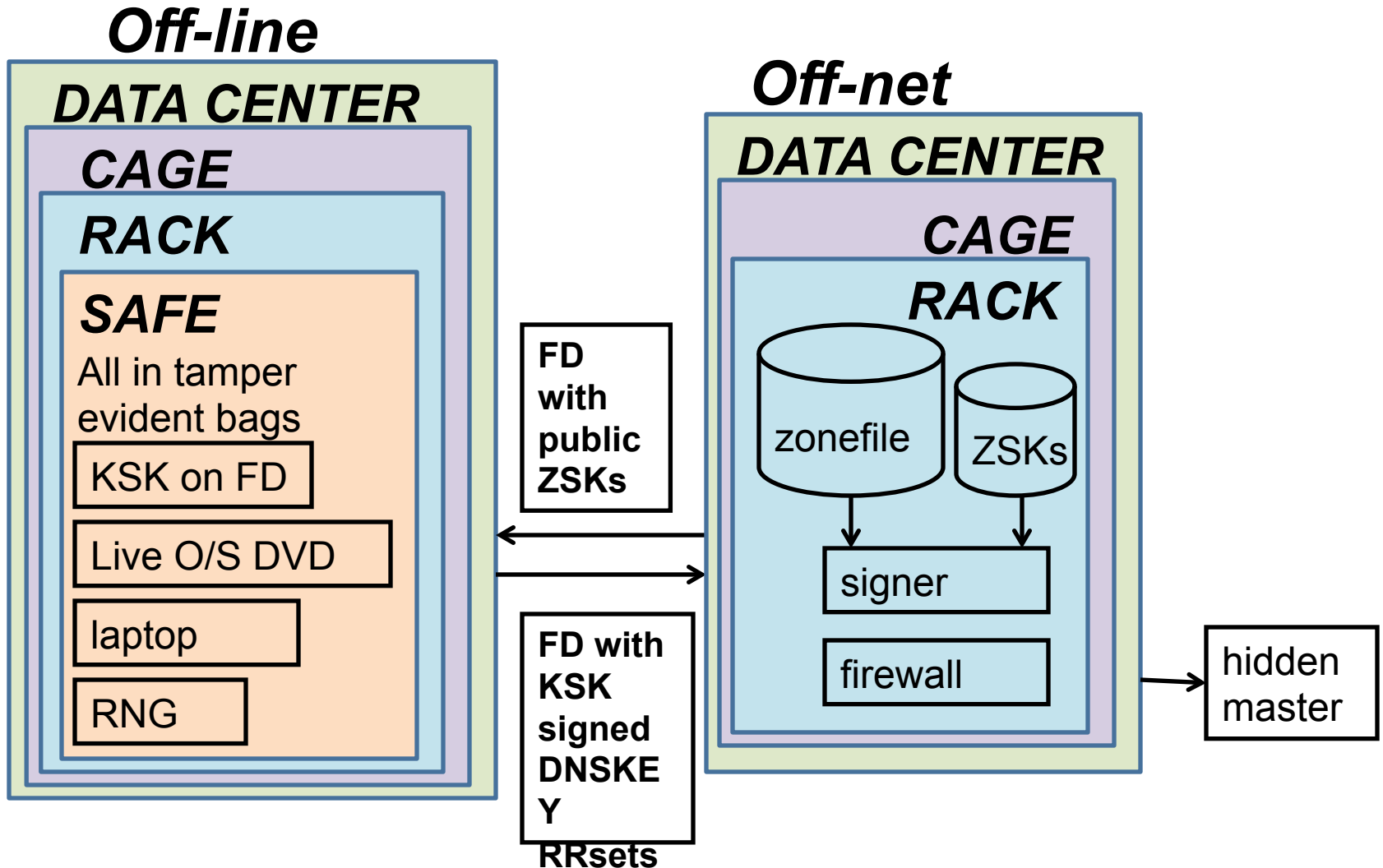
Learn from others mistakes

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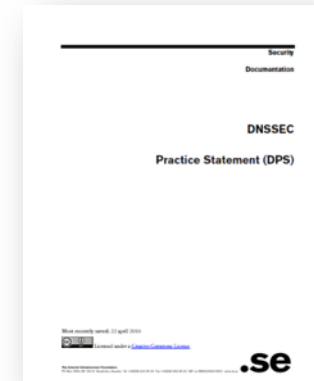
```
int getRandomNumber()
{
    return 4;   // chosen by fair dice roll.
                // guaranteed to be random.
}
```

Intel RdRand

DRBGs
FIPS 140
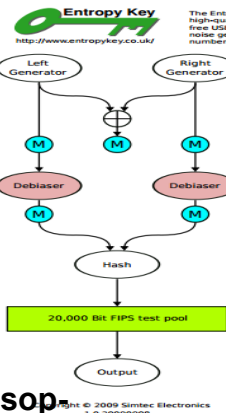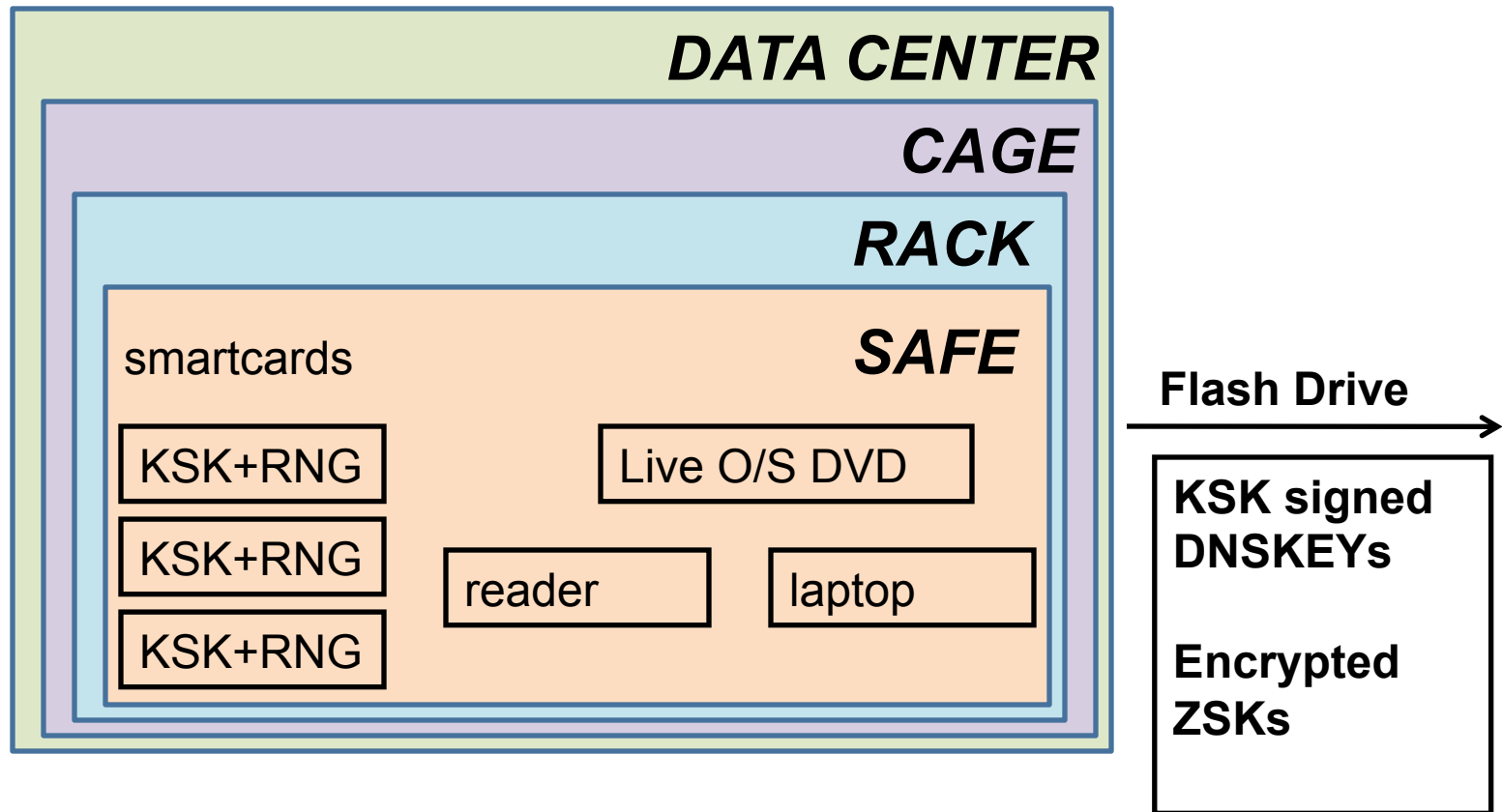
Useful IETF RFCs:
DNSSEC Operational Practices http://tools.ietf.org/html/draft-ietf-dnsop-rfc4641bis
A Framework for DNSSEC Policies and DNSSEC Practice Statements http://tools.ietf.org/html/draft-ietf-dnsop-dnssec-dps-framework
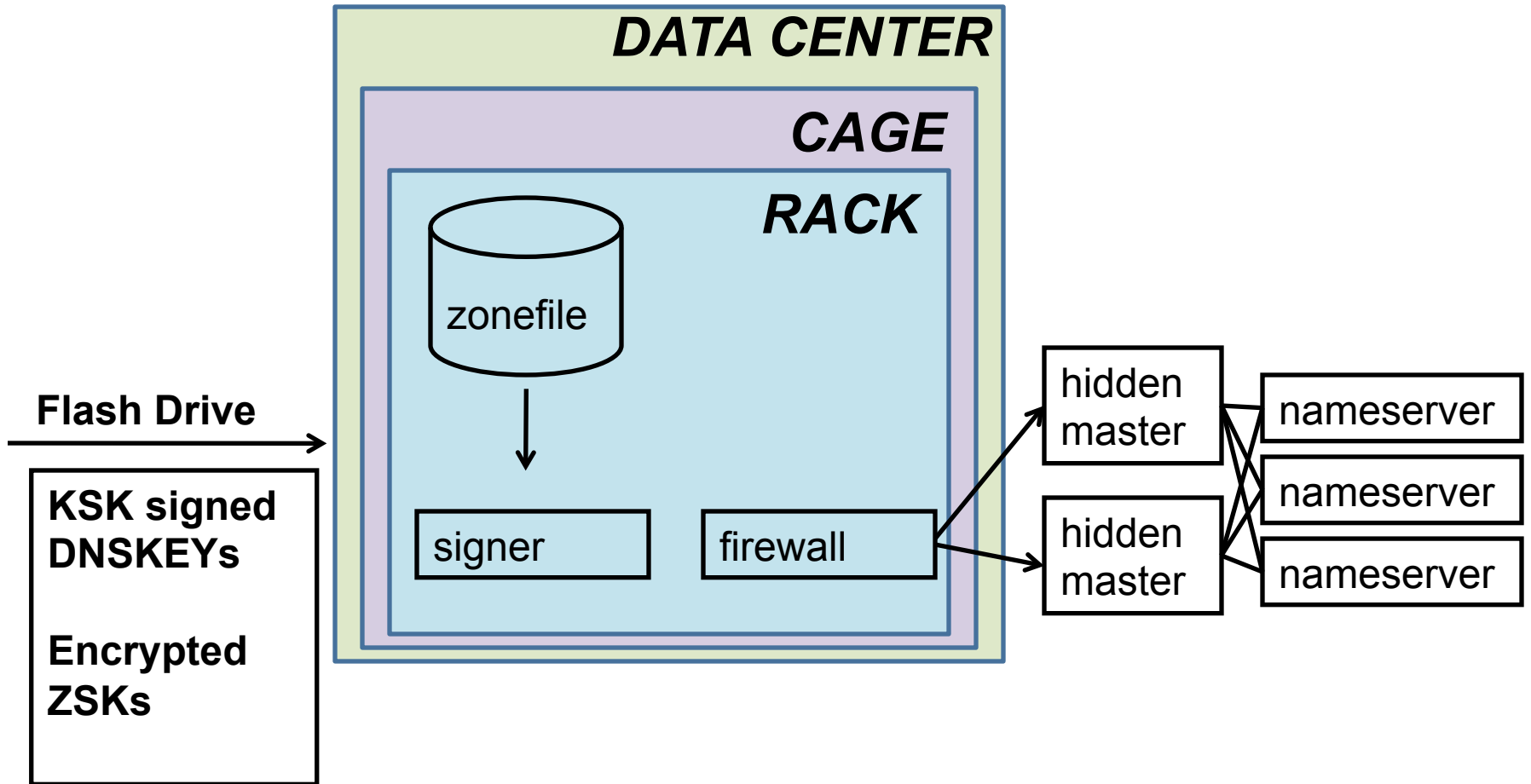
Demo Implementation

- 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

Transport KSK
signed
DNSKEY
RRsets

and Encrypted
ZSKs

Sign ZSKs with
KSK

Offline Laptop

KSK

Generate ZSKs

Generate KSK

Secure Key
Generation and
Signing
Environment

unsigned
zone

Sign zones
with ZSK

Online/off-net
DNSSEC
Signer

signed
zone

Animated slide

DNS+DNSSEC

www.majorbank.se = 1.2.3.4

www.majorbank.se=?

1.2.3.4

DNS
Resolver

DNS
Server

Get page
Login page

webserver
www @
1.2.3.4

Username / Password
Account Data

ISP/ HotSpot /
Enterprise/ End
Node

Majorbank.se (Registrant)

DNS
Server

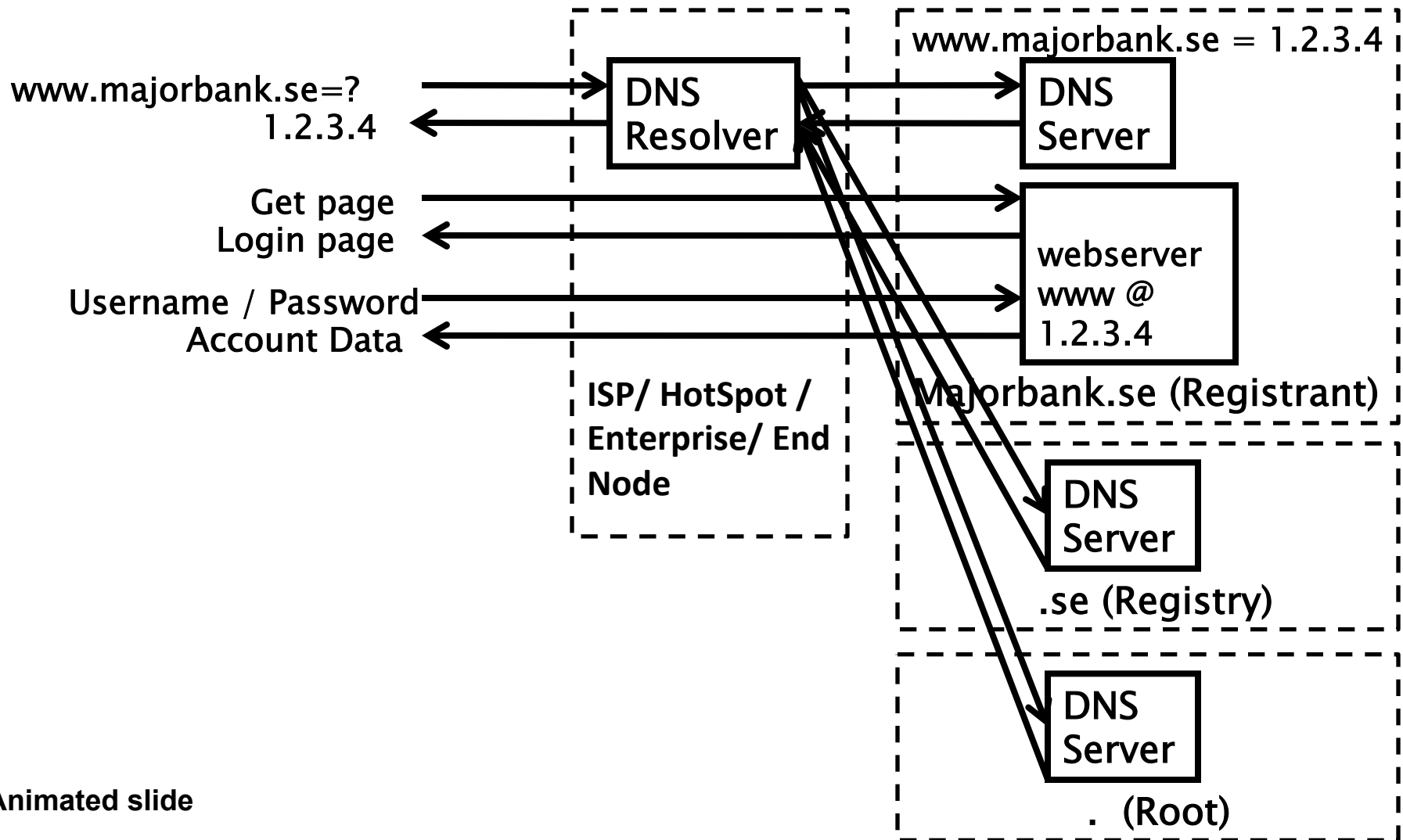.se (Registry)

DNS
Server

. (Root)

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 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
```