DNSSEC Implementation

Module 1

LACTLD Workshop

8 September 2011, Santiago, Chile

richard.lamb@icann.org

Overview

- Design Considerations
- Demo Implementation
- DNSSEC Practices Statement
- Demo
- Outputs
  - Demo Implementation
  - Demo DNSSEC Practice Statement
  - Demo Key Ceremony Scripts

DNSSEC Update

DNSSEC Update

- < 1% DNSSEC still needs to deployed on more domain names.
- 72/310 top level domain (e.g., .com) have DNSSEC deployed. Internal ICANN-only site:
- 81% of domain names can have DNSSEC deployed on them.

BLACKHAT – Jeff Moss, Las Vegas August 04, 2011

- Jeff Moss, told the Black Hat Technical Security conference in Las Vegas that now is the time for corporations and organizations to embrace DNSSEC.
- If you only call us after the house is on fire, you have very few options, Moss told the conference in emphasizing the need for business to prioritize online security, including adoption of DNSSEC.
- If you don’t have a corporate policy or strategy to sign your zone, you should, said Moss, who is the founder of the Black Hat conference. You're not only going to be helping your own organization, you're going to be helping the rest of the Internet.

http://www.itbusinessnet.com/article/ICANN-Security-Chief-Urges-Widespread-Adoption-of-DNSSEC-1620995

Basic HowTo

- For Companies:
  - Sign your corporate domain names
  - Turn on validation on their DNS resolvers
- For Users:
  - Ask ISP to turn on validation on their DNS resolvers. (ISP in US with>18M has turned on validation)
- For ccTLDs
  - Do Yourself / Outsource / Somewhere in between

- More Registrars need to support DNSSEC

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

Opportunity

- Looks like we now have a global, secure database for “free”!
- A globally trusted Public Key Infrastructure
- Enabler for global security applications
- An authentication platform for identification
  - Identifying the threat is a key obstacle for cyber security efforts.
- Cross-organizational and trans-national
- .. A global platform for innovation

Sources of Trust on the Internet

CA Certificate roots ~1482

DNSSEC root - 1

Content security
Commercial SSL
Certificates for
Web and e-mail

Yet to be discovered
security innovations
and enhancements

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

Network security
IPSECKEY RFC4025

VoIP securing SIP

Domain Names

Cross-
organizational and
trans-national
identity and
authentication

E-mail security
DKIM RFC4871

Login security
SSHFP RFC4255

One effort: DANE in IETF

- Free SSL Certificates
  - Currently ~4M out of 255M sites use SSL. Y-not all?
- Improved security for existing and high security (EV) Certificates
  - Extra protection around recent CA mistakes
- Secure e-mail - S/MIME
  - Mature but unused due to difficult PKI deployment.
- Timeframe? ~2 years

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

Opportunity for Indigenous Certification Authorities

- CAs located in only 52 countries
  - 'AE', 'AT', 'AU', 'BE', 'BG', 'BM', 'BR', 'CA', 'CH', 'CL', 'CN', 'CO', 'CZ','DE', 'DK', 'EE', 'ES', 'EU', 'FI', 'FR', 'GB', 'HK', 'HU', 'IE', 'IL', 'IN', 'IS', 'IT', 'JP', 'KR', 'LT', 'LV', 'MK', 'MO', 'MX', 'MY', 'NL', 'NO', 'PL', 'PT', 'RO', 'RU', 'SE', 'SG', 'SI', 'SK', 'TN', 'TR', 'TW', 'UK', 'US', 'UY', 'WW', 'ZA'
- Even then, some countries are not using their own CAs.
- Synergy: Reduced barriers, Alignment with TLD and national interests, DNSSEC operations

Achieving full potential

- Someday critical industries will come to rely on DNSSEC (or not)-:
- Need to focus on weak links in the chain of trust

  Registrant →Registrar →Registry →Root
- This will require secure IT practices and transparency
- …and greater awareness for the consumer

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

Reliability

Reliability

- Availability: Absolute time matters / Signatures expire: can not set and forget.

```
raiz. 135957  IN  RRSIG   DNSKEY 8 0 172800
20110913235959 20110830000000 19036 raiz.
mTOLwTC+jfhKi7P5V/zcLYLwjFUvOqTXGujYQVzeMCJdRlVdlYLxGUmM
..
```

- Complexity: Key management: DNSSEC > DNS

Reliability

- Ensuring Availability
  - Automate
  - Monitor
  - Backup Sites
- Taming Complexity
  - Step-by-step checklists
  - Rely on documented processes - not specialists

Reliability - Automation

- Pre-gen key material and rollover schedules
  - Pre-gen KSK signed DNSKEY RRsets
- Scripts
  - cronjob dnssec-signzone execution
  - check zone before publication

Reliability - Monitor

- Early Warning systems
  - Impending RRsig expiration
  - SOA serial sync between NS

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

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..
    - USHER HEBCA, Dartmouth
  - 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

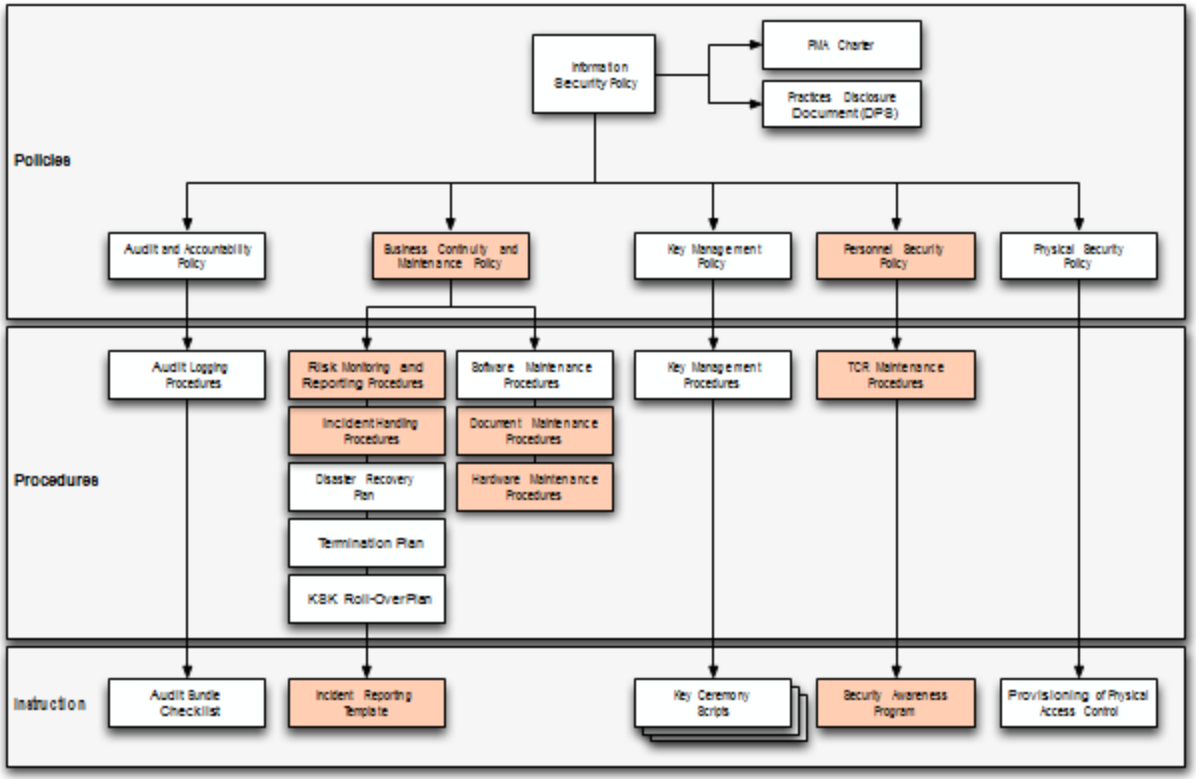
This document is the DNSSEC Practice Statement (DPS) for the Root Zone Key Signing Key (KSK) Operator. It states the practices and provisions that are used to provide Root Zone Key Signing and Key Distribution services. These include, issuing, managing, changing and distrik with the specific requirements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

Copyright Notice

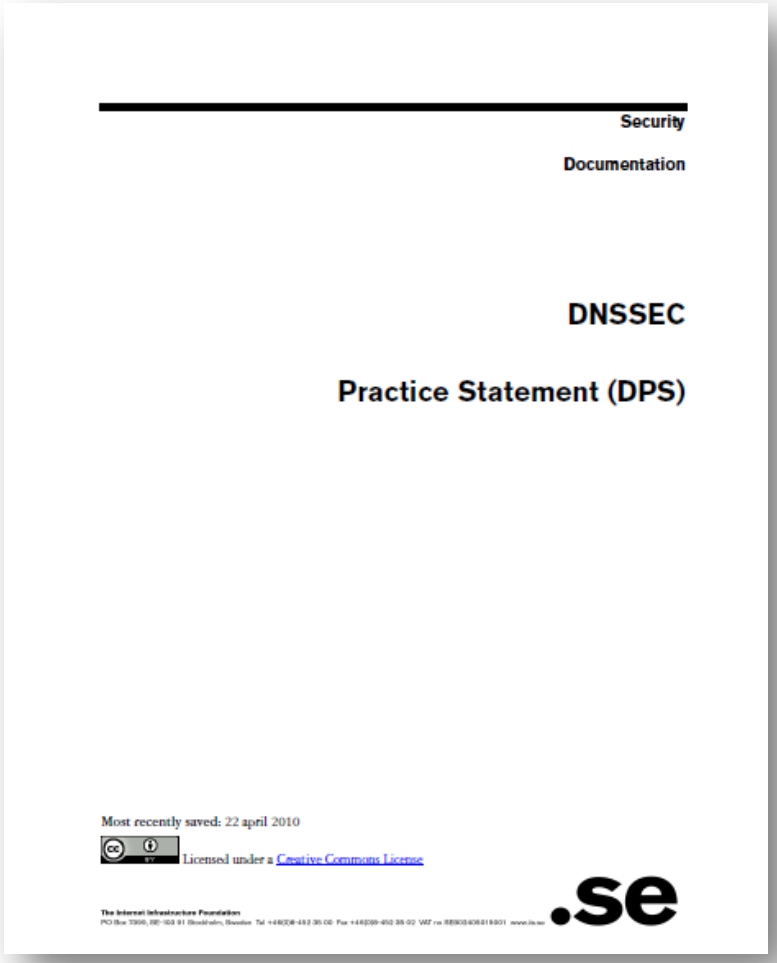
Copyright 2009 by VeriSign, Inc., and k Assigned Names and Numbers. This work

Root DPS

91 Pages and tree of other documents!



Documentation - .SE



22 pages, Creative Commons License!

.SE DPS

Do what you say

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

Key Ceremony

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

Prove it

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

Prove it - Audit Material

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

Prove it

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

Prove it

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

Security

Security

- Physical
- Logical
- Crypto

Physical

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

Physical - Environmental

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

Physical - Tiers

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

Physical - Tier Construction

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

Physical – Safe Tier

Physical – Safe Tier

Physical - Access Control

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

Physical - Intrusion Detection

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

Physical - Disaster Recovery

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

Logical

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

Logical - Authentication

- Procedural:
  - REAL passwords (e.g., 8 characters and mixed)
  - 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
- KSK/ZSK Splitting
- Effectivity (rollover) Period
- Number and Scheduling of keys
- Validity Period
- Crypto Hardware

Crypto - Algorithms / Key Length

- Factors in selection
  - Cryptanalysis
  - Regulations
  - Network limitations

Crypto - Key Length

- Cryptanalysis from NIST: *2048 bit RSA SHA256*

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

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

Crypto - Algorithms

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

Crypto - Algorithms

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

Crypto - KSK/ZSK Split

- Any reasonable sized zone will change frequently enough to warrant the ZSK to be on-line
- Manage compromise risk of on-line ZSK for frequently changing zone
- Flexibility in handling interaction with parent zone
- Not difficult to implement

Crypto – KSK Rollover

- Key length sets upper limit on effectivity (rollover) period
- Earlier cryptanalysis suggests 2048 bit key is good till 2030 so upper limit is ~20 years
- Other factors:
  - Practice emergency rollover
  - HSM operational considerations
  - Trusted employee turnover
  - Hard to roll if Trust Anchor. Easy if not.
  - Automated TA update - RFC5011

Crypto - KSK Rollover (cont)

- Only roll when compromised.
- Counter argument is to need to exercise emergency rollover for compromise recovery
- No widespread agreement
- If the KSK is not used as a Trust Anchor and decision is to do rollovers, not so difficult.
  - RFC4641bis suggests ~ 1 year effectivity period since year time-span is easily planned and communicated.

Crypto – ZSK Rollover

- ZSK more frequently accessed: operational considerations
- ZSK compromise less severe since under zone owner control but rollover should happen soon.
- If online, exposed to various threats: keep off-net and roll.

Number and Schedule of Keys

- 1, 2, or 3 published (DNSKEY) keys for KSK and/or ZSK
  - UDP fragmentation on DNSKEY RRset + RRSIGs
  - Note: DNSKEY RRset does not need to be signed by ZSK

- Pre-publish KSK
  - more work for parent w/ extra steps;
  - cant pre-verify new DS;
  - doesn't work for combined alg rollover
- Double sign for KSK
  - only DNSKEYs signed so doesn't make zone too big

- Generally pre-publish for ZSK. Double sign for KSK.
- For root we use 1 KSK and 1 ZSK. Pre-publish new ZSK during ZSK rollover and double sign with both KSKs during KSK rollover.

Number and Schedule of Keys (cont)

- Example (root)

Crypto - Signature Validity Period

- Short to minimize replay attack - quickly recover from compromise
  - Max validity period < how long wiling to tolerate replay attack
- Long to limit operational risks from equipment failure
  - Min validity period > operational failure recovery time.
- Validity periods overlap to deal with clock skew
- Other Guidelines
  - Avoid expiration in cache: Max TTL < validity period/N where N > 2
  - Secondaries do not serve expired signatures: SOA expiration < validity period

Crypto - Hardware

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

Crypto - Hardware Security Module (HSM)

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

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

Crypto - PKCS11

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

Crypto - Smartcards / Tokens

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

Crypto -Random Number Generator

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

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

Crypto - FIPS 140-2 Level 4 HSM

Root, .FR, …

Crypto – FIPS Level 3 HSM

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

Crypto - But this is also “level 3”

FIPS 140-2 Validation Certificate

The Communications Security Establishment of the Government of Canada

+

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	

The following FIPS approved Cryptographic 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

Director, Industry Program Group
Communications Security Establishment

Crypto - Other Hardware (cont)

- Two-Factor
  - RSA SecureID
  - Vasco “footballs” ~$5
  - NagraID cards ~$30
- Good for registrant-registrar authentication

Miscellaneous

Tools and Software

- BIND
  - BIND 9.8.x dynamic zone signing
  - dig [+sigchase]
  - dnssec-signzone, dnssec-dsfromkey, dnssec-dsfromkey
- LDNS
  - ldns-*
- OpenDNSSEC
- PKCS11
  - Some tools
  - But Not so hard. Plenty of examples out there.
- Test Tools
  - http://dnsviz.net
  - TLDMon - https://www.dns-oarc.net/oarc/services/tldmon
  - DNSMON - http://dnsmon.ripe.net/dns-servmon/

Parental policies

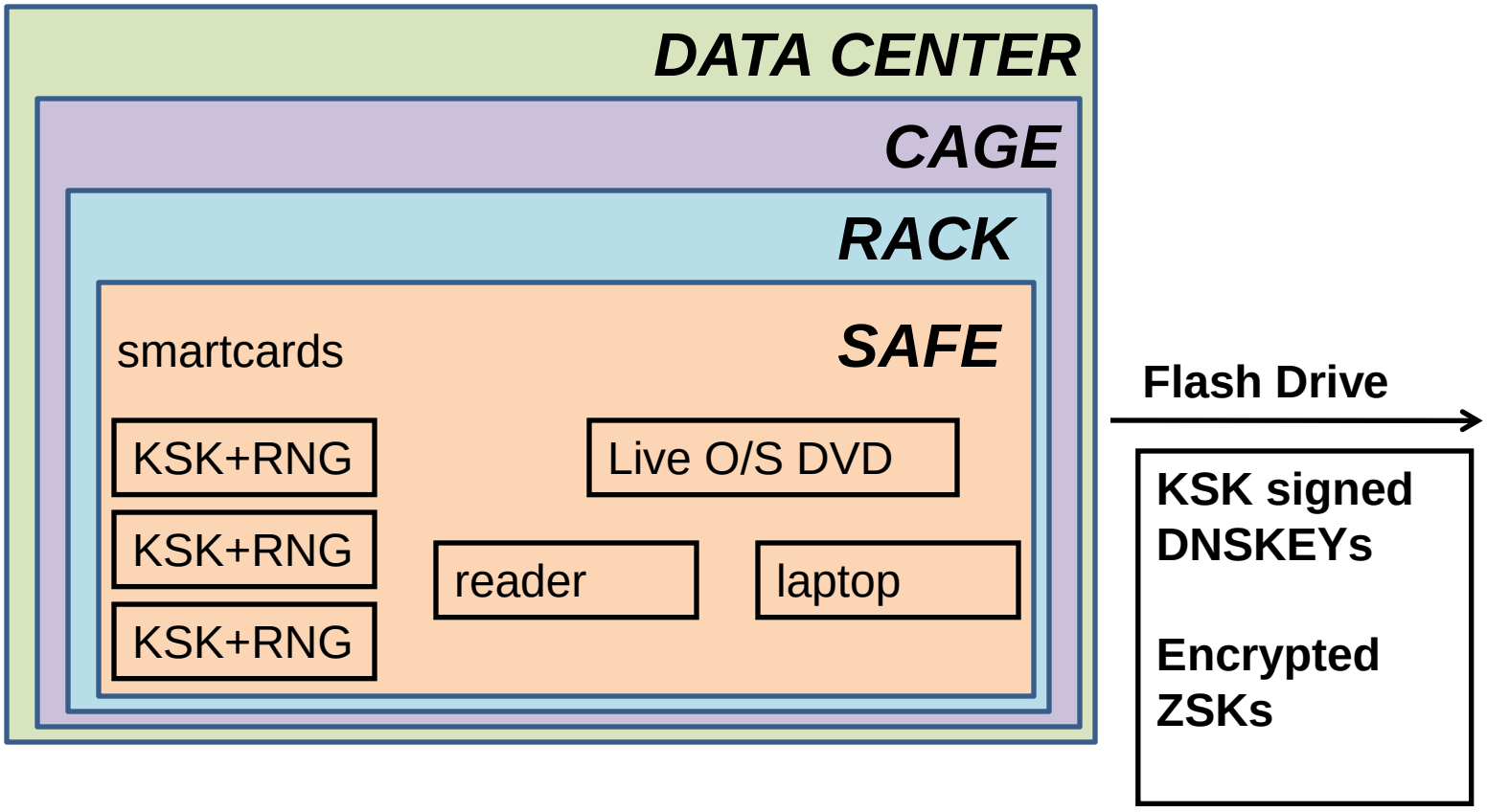
- Initial key exchange
  - Out of band check even if dnskey available
  - Accept DS at minimum
  - Verify matching DNSKEY (root does this)
  - Awaiting simplifying protocols that update DS in band between parent and child using established crypto relationship (non-TA only)
- Avoid security lameness – no matching DNSKEY for DS : “bogus”
  - Child’s careful removal of KSK DNSKEY material
  - Advice to child not to remove the KSK before the parent has a DS record for the new KSK in place (otherwise attacker’s zone valid while yours is not)
- Changing DNS operators
  - Cooperative (double KSK signed + ZSK pre-pub) - publish your policies. Reasonable TTLs ☺
  - Non-cooperative – 10year TTL+validity period for DNSKEY ☹ Solution: ask registry to remove DS
  - Proper contractual relationships between all parties is only solution.

Demo Implementation

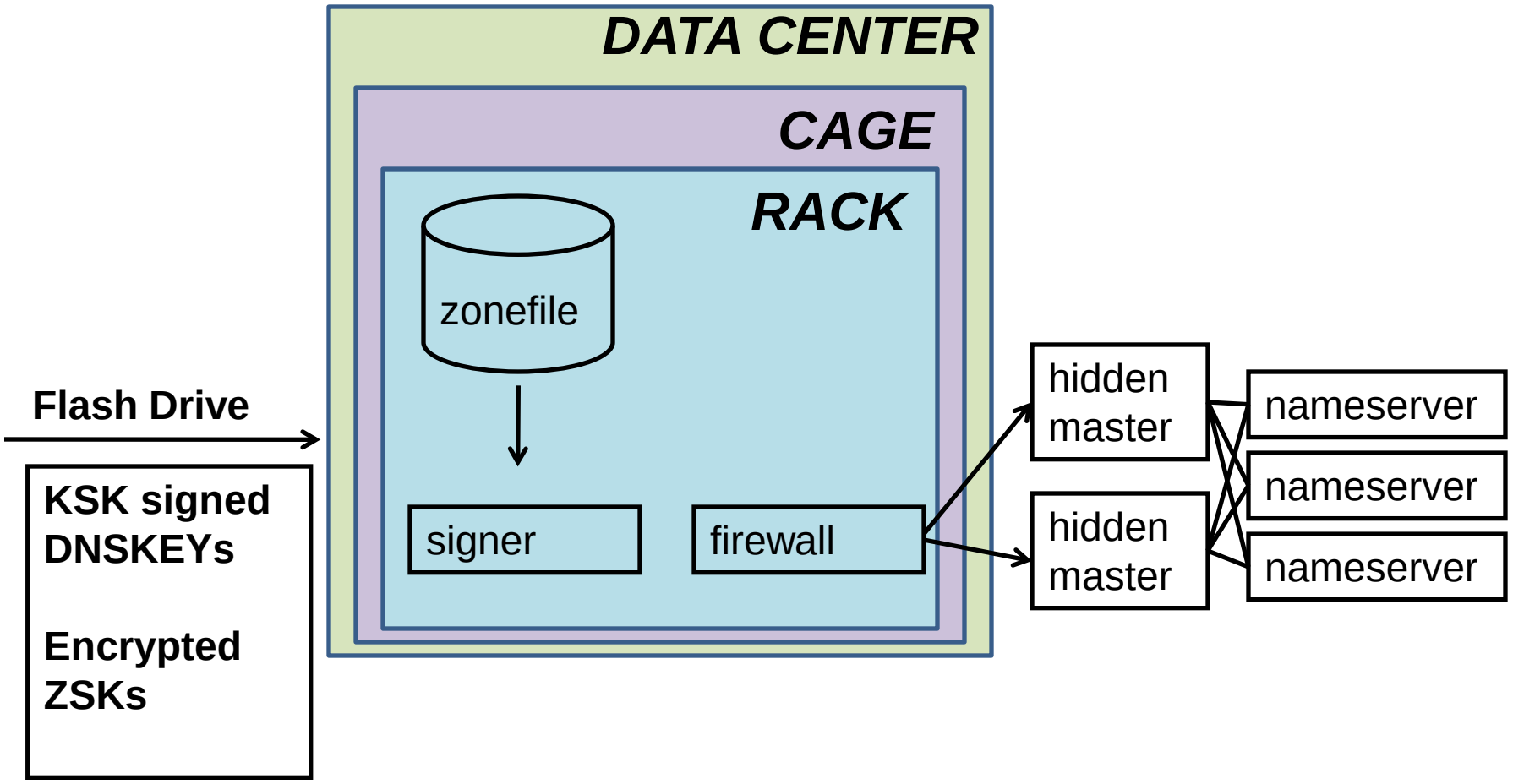
Demo Implementation

- Key lengths – KSK:2048 RSA ZSK:1024 RSA
- Rollover – KSK:as needed ZSK:51 days
- RSASHA256 NSEC3
- Physical – HSM inside Safe inside Rack inside Cage inside Commercial Data Center
- Logical – Separation of roles: cage access, safe combination, HSM 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



Write DNSSEC Practice Statement