Expériences de divers déploiement de DNSSEC

Leçons apprises

- Apprendre des erreurs des autres
- Surveiller, surveiller, surveiller
- Planifier
- Documenter et publier
- Analyses de risques
- Apprendre des Autorités de Certification

Objectifs

- Fiable
- De confiance
- Rentable(pour vous)

Rentabilité

Rentabilité

- Analyse de risques
- Analyse rapport coût-bénéfice

Impacts sur les affaires et motivation

(du rapport ENISA "The Costs of DNSSEC Deployment")

- Devenir une source fiable de confiance et booster la part de marche et/ou la réputation des zones;
- Mener par l'exemple et stimuler les autres parties dans la chaine à adopter DNSSEC;
- Gagner la reconnaissance dans la communauté DNS et partager l'expérience avec les TLDs et autres ;
- Fournir l'assurance aux utilisateurs que les services de noms de domaine sont fiables et de confiance;
- Envisager une adoption plus élevée quand le revenu sera une grande motivation. Déployer DNSSEC peut être profitable;

Analyse de risques

- Identifier vos risques
  - Réputation
    - Compétition
    - Perte de contrats
  - Légal / Financier
    - Qui sont les utilisateurs qui nous font confiance?
    - SLA
    - Poursuite judiciaire
- Construire votre profile de risque
  - Déterminer votre niveau de risque acceptable

Vulnérabilités

- Fausses attentes
- Compromission de clés
- Compromission de l'outil de signature
- Compromission du fichier de zone

Analyse des coûts

« Établir des attentes raisonnables signifie qu'il n'a pas besoin d'être coûteux »

Du rapport ENISA

- "….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.

Anticiper les dépenses CAPEX et OPEX

- Etre “ancre de confiance” demande des pratiques matures, surtout en matière de gestion de clés;
- L’investissement peut aussi dépendre de la stratégie de positionnement à travers DNSSEC: les leaders payent la facture, les autres peuvent limiter leur investissement;
- Le coût financier pourrait ne pas dépasser les avantages financiers. Préparez-vous à amortir l'investissement financier sur plus de 3 à 5 ans.

Autres analyses de coût

- Personnel
  - Swedebank – 1/2 FTE
  - Occasionnellement partager des taches avec d'autres
- Installations
  - Espace Datacenter
  - Coffre-fort ~ $100 - $14000
- Equipement de cryptographie ~ $5-$40000
- Bande passante ~ 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

De confiance

Confiance

- Transparent
- Securiser

Transparence

Transparence

- Le pouvoir de la vérité
  - La transparence fait flotter tous les bateaux ici
- Dites ce que vous faites
- Faites ce que vous dites
- Prouver le

Dites ce que vous faites

- Définir les attentes
- Documenter ce que vous faites et comment vous le faites
- Maintenir la documentation a jour
- Définir les rôles et responsabilités dans l'organisation
- Décrire les services, les installations, les systèmes, les procédures, paramètres..

Apprendre des CA

- Le bon:
  - Les hommes
  - La mentalité
  - Les pratiques
  - Le cadre légal
  - L'audit contre les standards internationaux
- Le Mauvais:
  - Confiance diluée avec une course vers le bas (>1400 CA's)
  - DigiNotar
    - Règles et contrôles faibles et inconsistants
    - Manque de notification des compromissions (non-transparent)
    - Les audits ne règlent pas tout (ETSI audit)

COMODO
Creating Trust Online®

DigiNotar®
A VASCO COMPANY

Dites ce que vous faites – Apprendre des services de confiance existantes

- 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…)

Dites ce que vous faites- DPS

- DNSSEC Policy/Practices Statement (DPS)
  - Construit sur le modèle des CPS des CA
  - Fournit un niveau d'assurance et de transparence aux parties faisant confiance à la sécurité des opérations.
  - Réévaluer régulièrement
  - Gestion
    - Formaliser - Autorité de gestion des politiques

Documentation - Racine

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

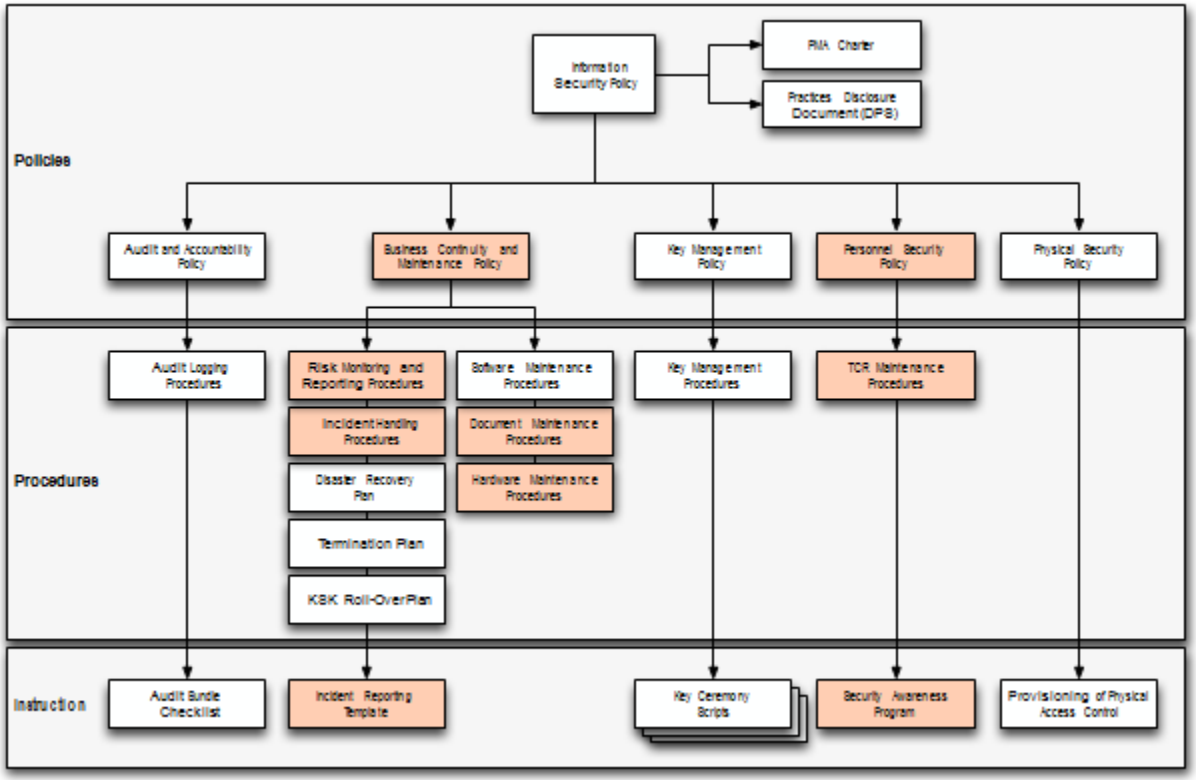
This document is the DNSSEC Practice Statement (DPS) for the Root Zone Key Signing Key (KSK) Operator. It states the practices and provisions that are used to provide Root Zone Key Signing and Key Distribution services. These include, issuing, managing, changing and distrib with the specific requirements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

Copyright Notice

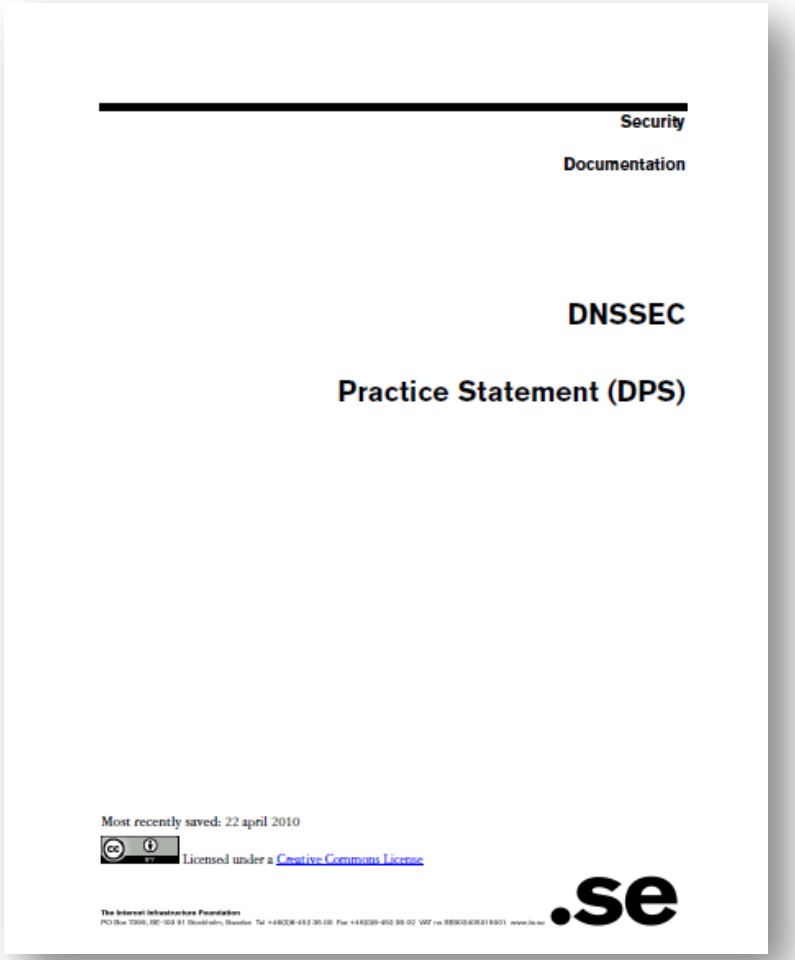
Copyright 2009 by VeriSign, Inc., and b Assigned Names and Numbers. This work

91 Pages and tree of other documents!

Root DPS



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

Faites ce que vous dites

- Suivre les procédures documentées
- Maintenir les logs, enregistrements et rapports de chaque action, ainsi que des incidents.
- Operations critiques pendant les cérémonies de clés.
  - Vidéo
  - Log
  - Témoins

Cérémonies de clés

Un processus filmé et audité, soigneusement orchestré pour une transparence maximale pendant que des clés de cryptographie sont générées ou utilisées.

Prouvez le

- Audits
  - –Externe $$
  - –ISO 27000 $$ ..
  - –Interne

Prouvez le - Matériel d'audit

- Scripts des cérémonies de clés.
- Logs des contrôles d'accès
- Installations, salles, Log des coffre-fort
- Vidéo
- Inventaire annuel
- Rapports d'incident

Prouvez le

- Implication des parties prenantes
  - Publier les rapports et matériels de travail à jour
  - Participation, i.e. témoins extérieurs de
    - La communauté Internet locale
    - Du gouvernement
  - Ecoutez les Feedbacks

Prouvez le

- Soyez responsable
  - Implication du niveau décisionnel
    - Dans la gestion des politiques
    - Participation dans les cérémonies de clés.

Sécurité

Construire la sécurité

- Obtenir la machinerie pour DNSSEC est facile(BIND, NSD/Unbound, OpenDNSSEC, etc..).
- Trouver de bonnes pratiques de sécurité le n'est pas.

Sécurité

- Physique
- Logique
- Cryptographique

Physique

- Environnement
- Les niveaux
- Contrôles d'accès
- Détection d’intrusion
- Reprise après sinistre

Physique - Environnement

- Baser sur votre profile de risques
- Adapter
  - Electricité
  - Climatisation
- Protection contre
  - Inondation
  - Feu
  - Tremblement de terre

Physique - Niveaux

- Chaque niveau doit être plus difficile à pénétrer que le dernier
  - Installations
  - Cage/Salle
  - Rack
  - Coffre-fort
  - Système
- Penser a des boites concentriques

Physique – Construction des niveaux

- Baser sur votre profile de risques et les régulations
- Conception des installations et sécurité physique sur
  - D'autres expérience
  - DCID 6/9
  - NIST 800-53 et autres documents
  - Coffre-fort /contenais standards

Physique – Coffre-fort

Physique – Coffre-fort

Physique – TEB

Physique – Contrôle d'accès

- Baser sur votre profile de risques
- Système de contrôle d'accès
  - Logs des entrées/sorties
  - Double occupation / Anti-passback
  - Permettre les accès d’urgence
- Haute Sécurité : Du contrôle physique d'accès au système Independent de contrôle d'accès physique pour les installations.

Physique – Détection d'intrusion

- IDS
  - Capteurs
  - Mouvements
  - Camera
- TEB
- Equipements « Tamper Proof »

Physique – Reprise après sinistre

- Plusieurs sites
  - Miroir
  - Backup
- Diversité de fournisseurs et géographique

Logique

- Authentification (mots de passe, PINs)
- Contrôle multi-parties

Logique - Authentification

- Procédures:
  - Mots de passe réels
  - Mise a jour régulières forcées
  - Contrôles hors bande
- Matériel:
  - Authentification Two-factor
  - Smart cards (cryptographique)

Logique – Contrôle Multi-Parties

- Séparation des rôles
  - i.e., “Security Officer” et “System Admin” et “Safe Controller”
- M-de-N
  - Au niveau des équipements (HSM)
  - Procédures: division des PIN
  - Boulonner: Division des clés (Shamir, i.e. ssss.c)

Crypto

- Algorithmes / Longueur des clés
- Matériel de Cryptographie

Crypto-Algorithmes/Longueur des clés

- Facteurs de sélection
  - Cryptanalyse
  - Régulations
  - Limites Réseaux

Crypto – Longueur de clé

- 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 - Algorithmes

- La régulation locale peut déterminer l'algorithme
  - GOST
  - DSA
- Les limites du réseau
  - Fragmentation: une clé plus courte est meilleure
  - ZSK peut être plus courte, puisque renouvelée plus souvent
  - ECC est idéal – Mais pas encore très populaire

Crypto - Algorithmes

- NSEC3 si nécessaire
  - Protège contre la diffusion des zones
  - Eviter si pas nécessaire – Ajoute de la complexité pour les petites zones
  - Accord de non diffusion?
  - Régulation ?
  - Utile pour les grandes zones sans beaucoup de délégations signées (“opt-out”).

Crypto - Materiel

- Satisfaire vos parties prenantes
  - Pas besoin de certification pour être sécurisé (i.e., off-line PC)
  - Peut utiliser les procédures transparentes pour construire la confiance
  - Mais beaucoup de registres utilisent ou pensent utiliser HSM. Peut être CYA?
- **Au moins une bonne source de nombres aléatoires (RNG)!**
- Utiliser des standards classiques évite la dépendante constructeur
  - Note: renouvellement de KSK peut se faire ~10 ans.
- Penser au backup des clés

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
- Reconnu par les autorités nationales de certification
  - Kryptus (Brazil) ~ $2500

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

Crypto - PKCS11

- Interface commune pour HSM and smartcards
  - C_Sign()
  - C_GeneratePair()
- Evite la dépendance constructeur
- Les constructeurs fournissent les pilotes (Linux, Windows) et parfois « 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
- Lent ~0.5-10 1024 RSA signatures per second

Crypto –Générateurs de nombres aléatoires

X rand()

X Netscape: Date+PIDs

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

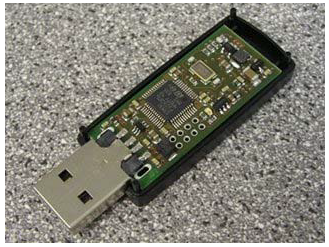
✓ LavaRand

? System Entropy into /dev/random (FBSD=c
+entropy/Linux=entropy?)

✓ H/W, Quantum Mechanical (laser) $

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

✓ Built into CPU chips



Crypto - FIPS 140-2 Level 4 HSM

Root, .FR, .CA …

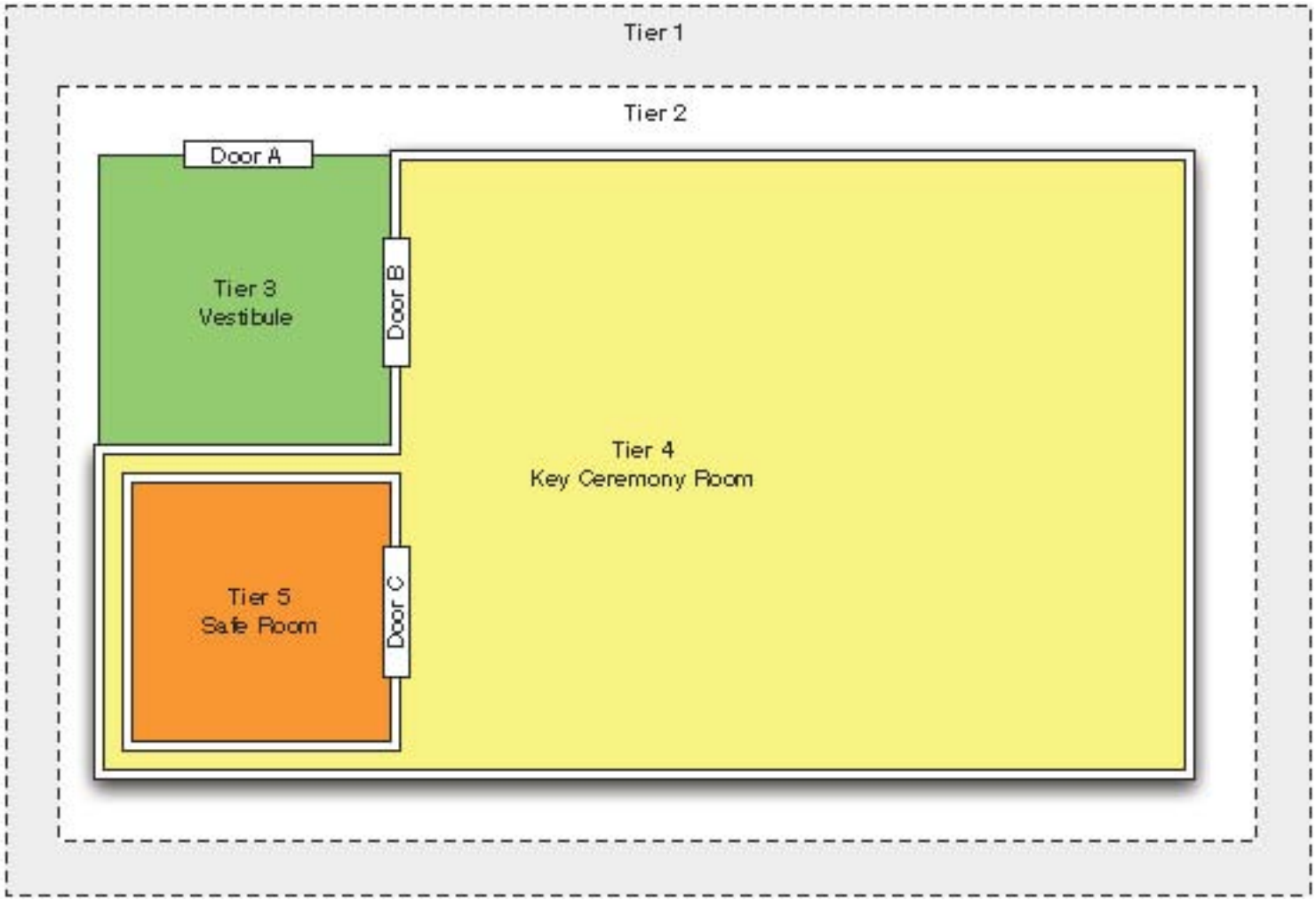
Crypto – FIPS Level 3 HSM

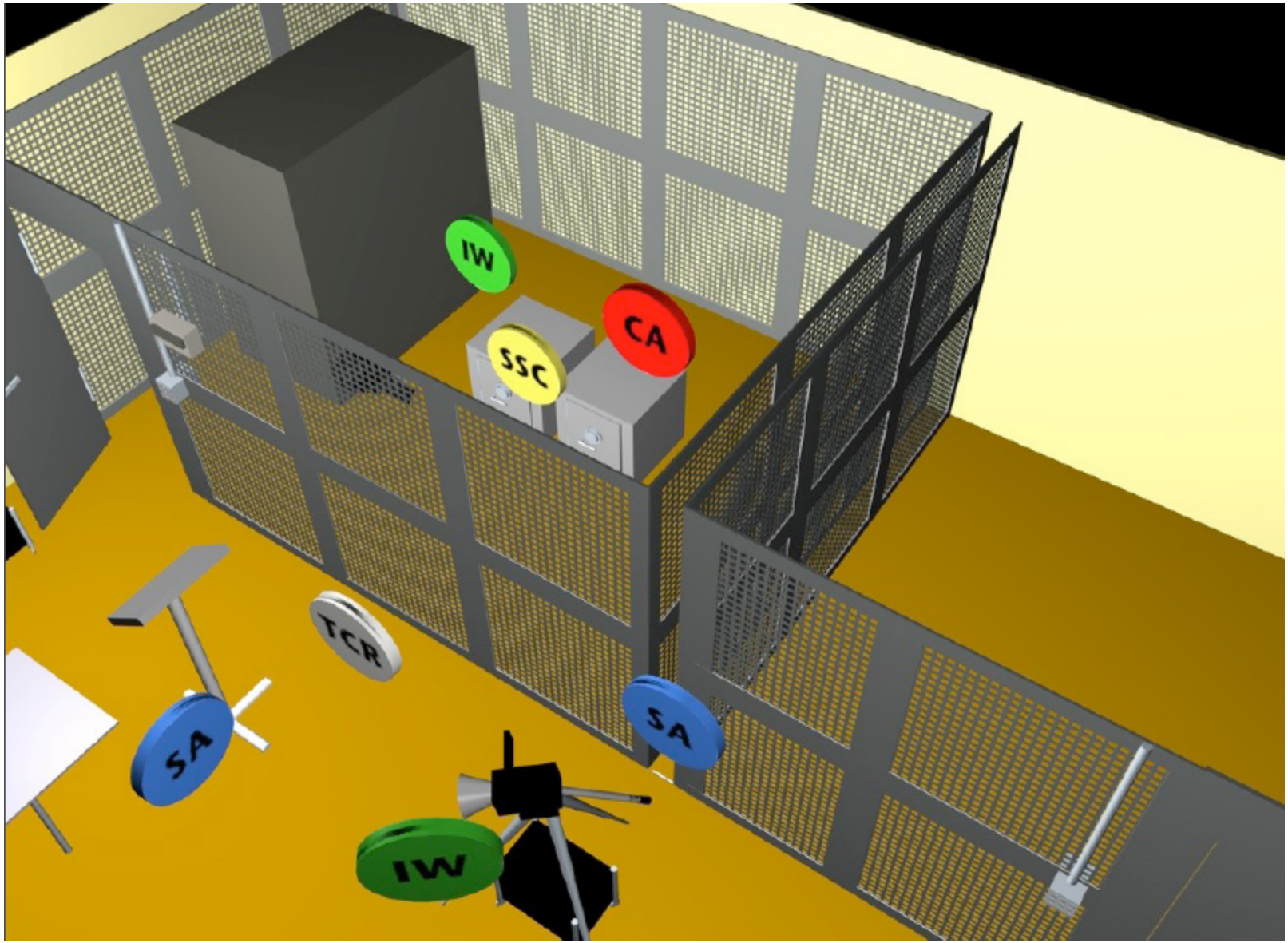
- FIPS 140-2 Level 3 est aussi très utilisé
- Beaucoup de TLDs utilisent level3

  .com , .se, .uk, .com, etc… $10K-$40K

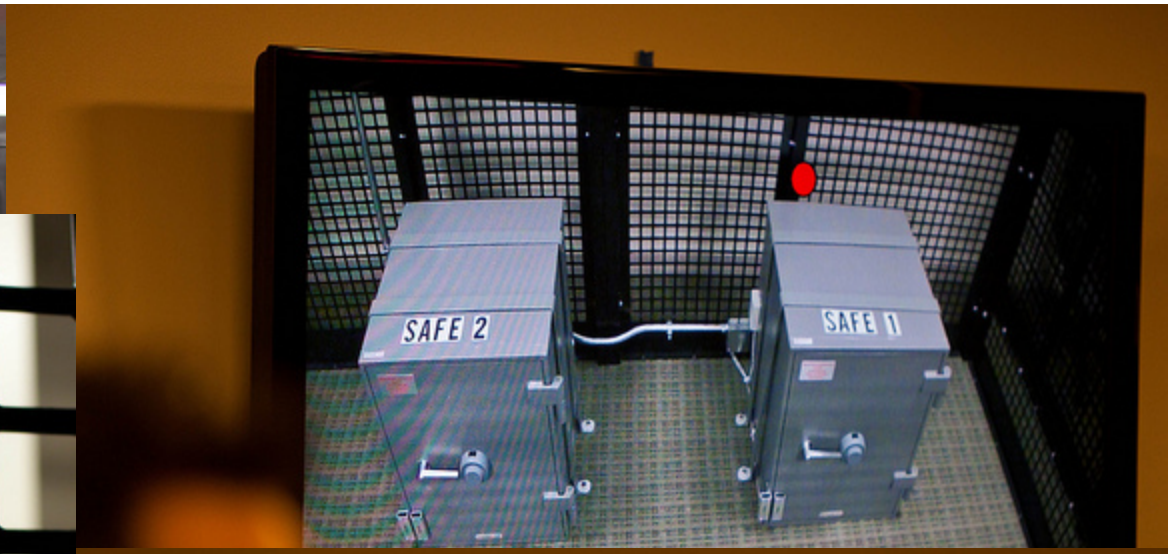
Une implémentation peut être comme..

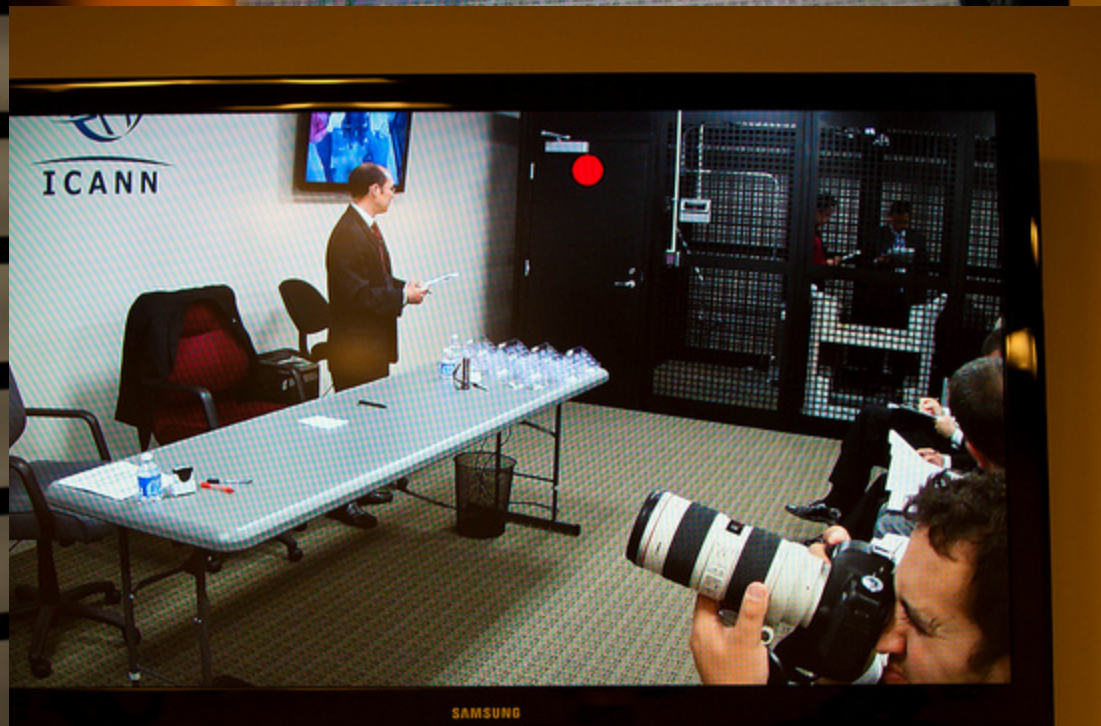
Sécurité physique




IW
CA
SSC
TCR
SA
SA
IW

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

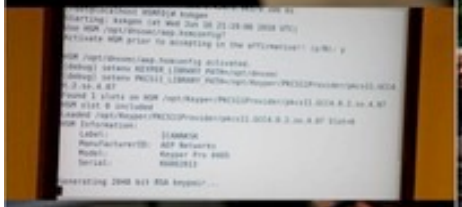





E Maple Ave
N Sepulveda Blvd
Indiana Ct
1920 E Maple Ave, El Segundo, CA 90


January 27, 2010


NOTICE
NOTICE
NOTICE
NOTICE
NO FOOD
OR DRINK




N


One World. One Internet. Everyone Connected.
19036

…ou comme

FIPS 140-2 Valid

FIPS VALIDATED 140-2

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	

Algorithms are used: **Triple-DES (Cert. #560); Triple-DES MAC (Triple-DES Cert. #560, vendor affirmed); AES (Cert. #577); SHS (Cert. #633); RNG (Cert. #332); RSA (Cert. #264)**

following non-FIPS approved algorithms: **RSA (key wrapping; key establishment methodology provides between 80 and 112 bits of encryption strength)**

Overall Level Achieved: 3

Signed on behalf of the Government of the United States

Signature: William Baker

Dated: March 31, 2008

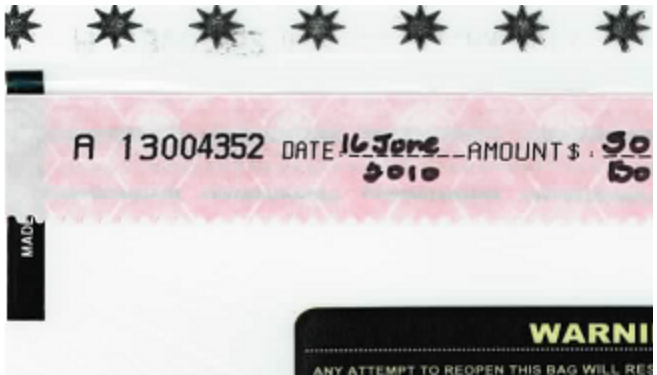
Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

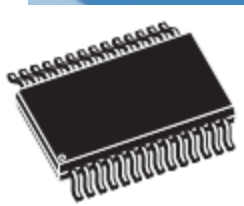
Signature:

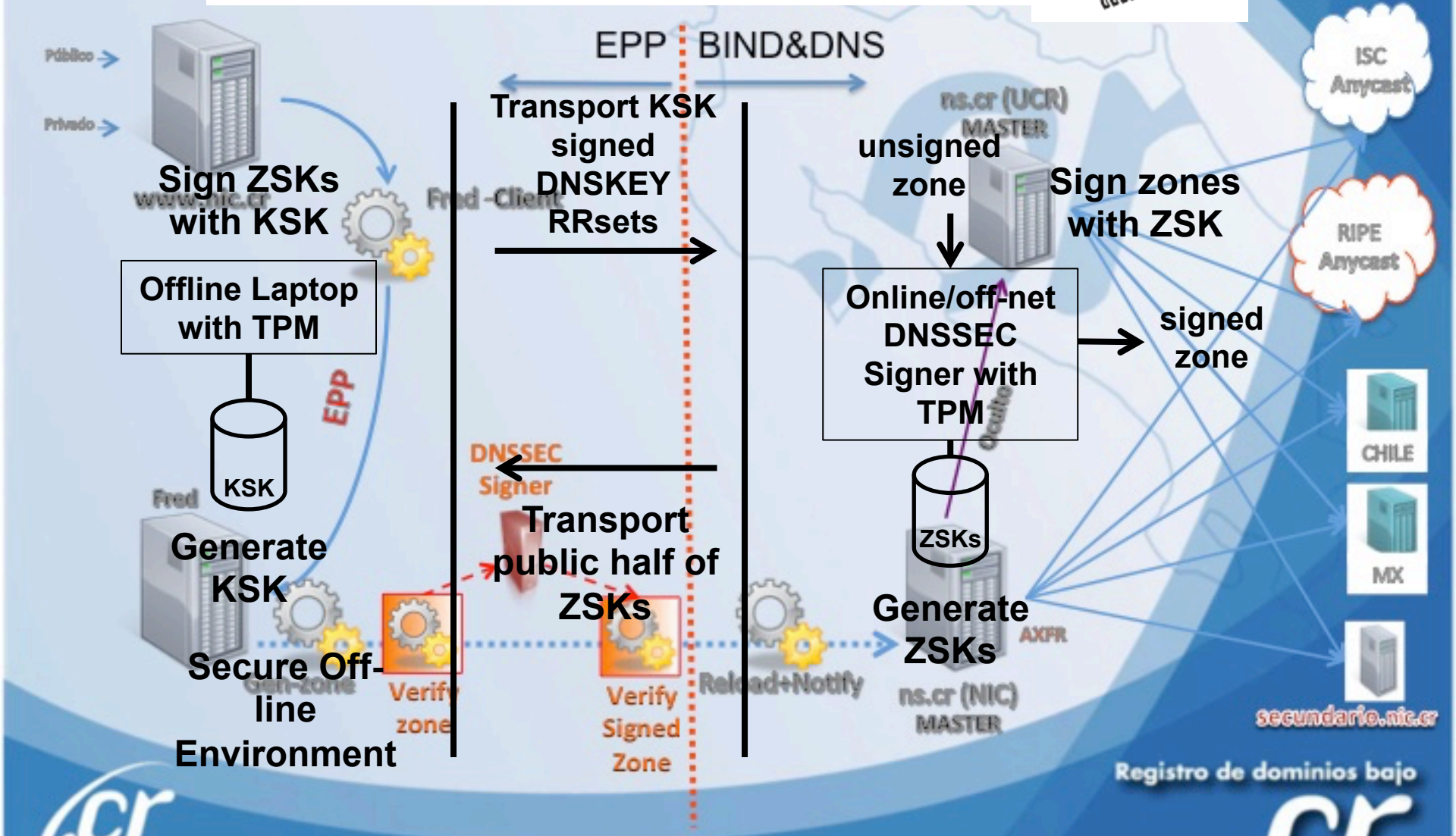
Dated: 20 March 2008

Director, Industry Program Group
Communications Security Establishment



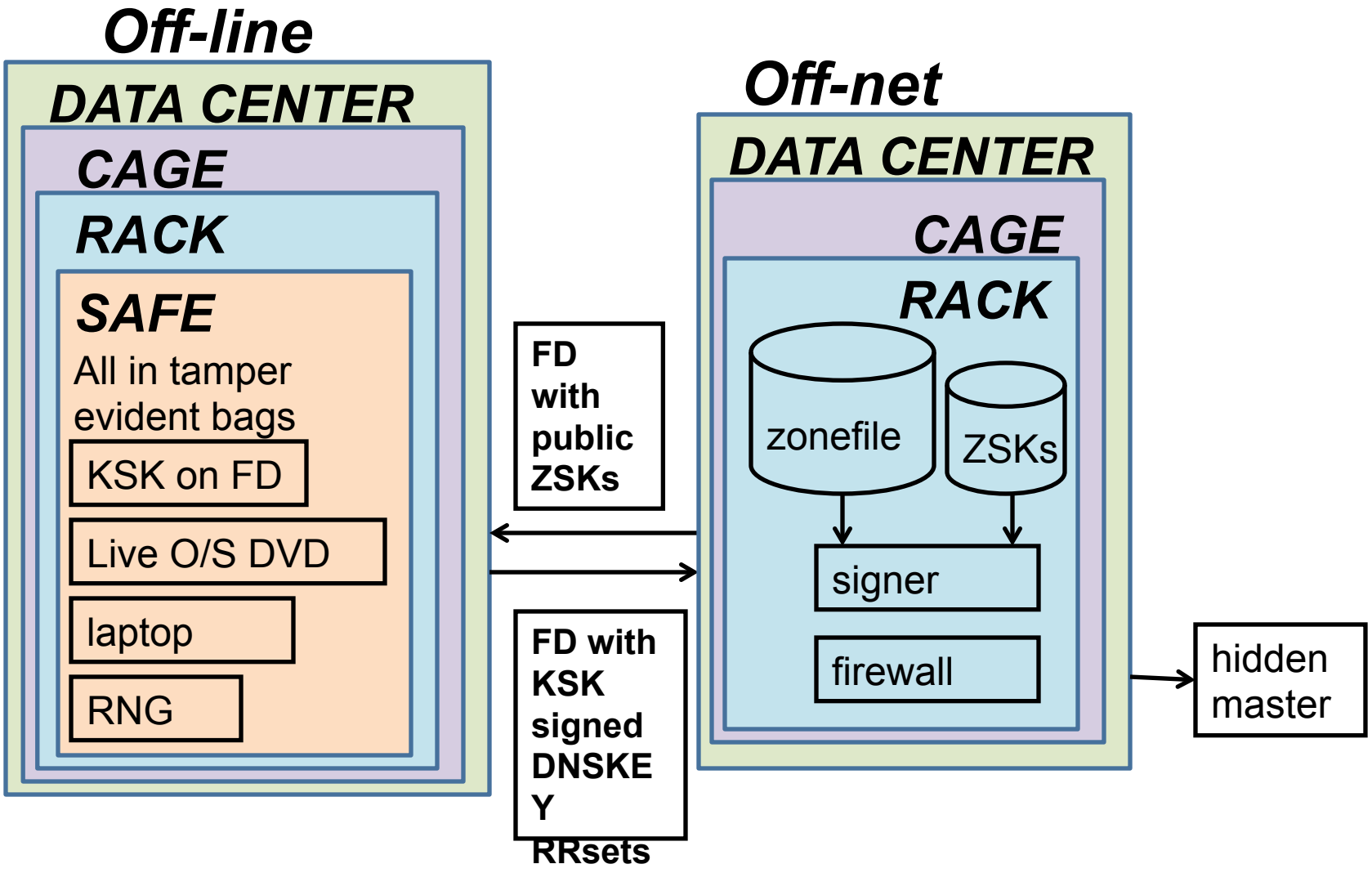
..ou comme (.cr)





Animated slide

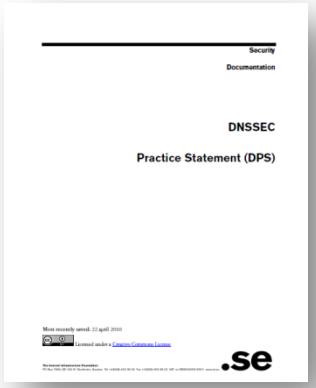
...ou même comme



Questions ?

But all must have:

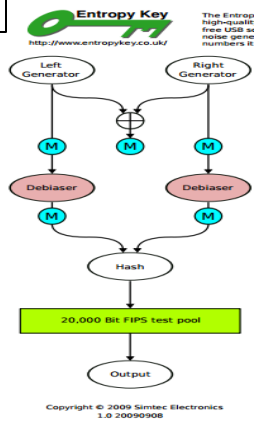
- Published practice statement
  - Overview of operations
  - Setting expectations
    - Normal
    - Emergency
  - Limiting liability
- Documented procedures
- Multi person access requirements
- Audit logs
- Monitoring (e.g., for signature expiry)
- Good Random Number Generators




```
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