aep NETWORKS Ultra ELECTRONICS

Securing Digital Keys

High Quality Key Generation

Highest Level Key Protection

Implementation of DNSSEC

Fadi Cotran, Ph.D.

Director of Technical Business Development

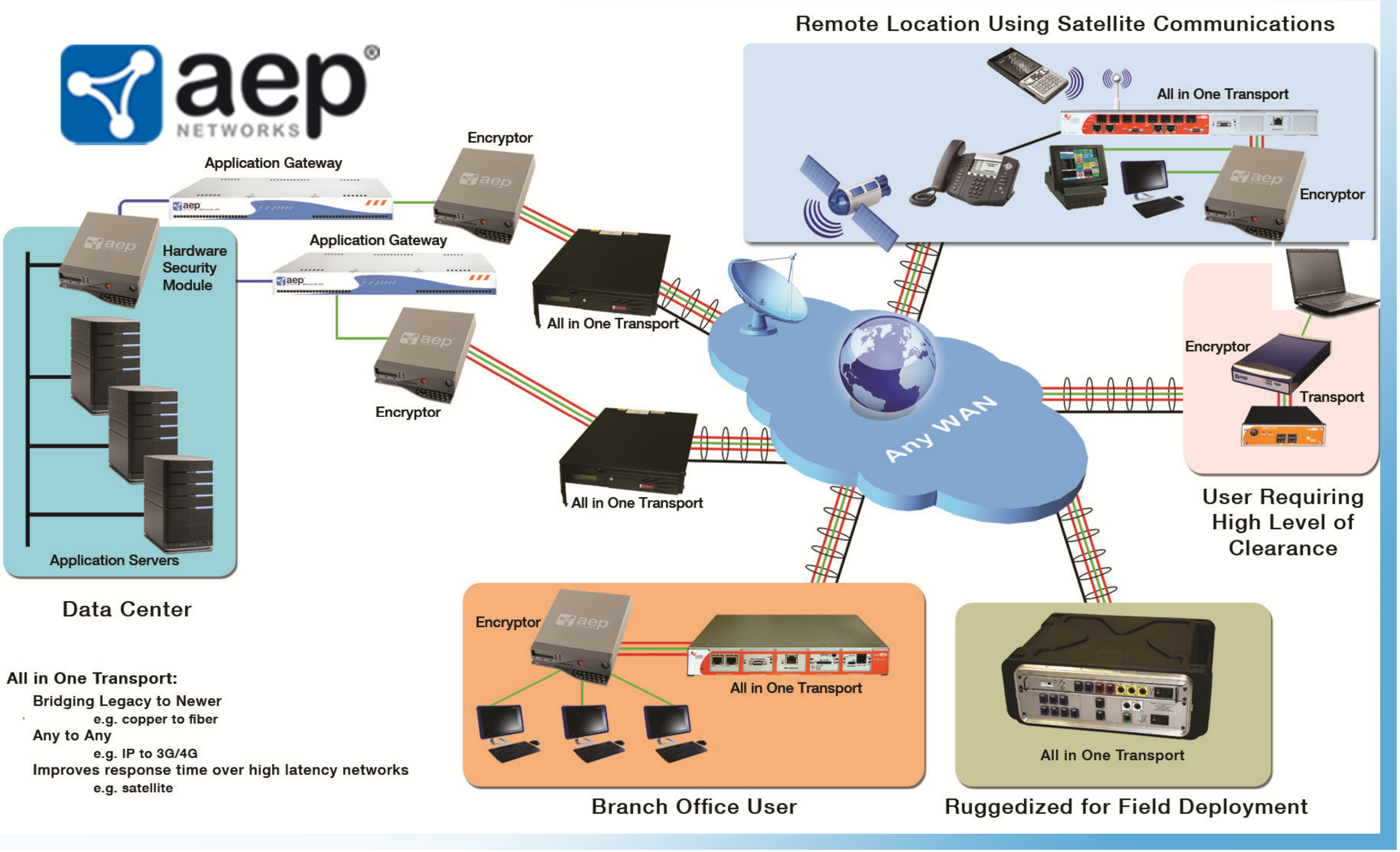
Who Are We and What Do We Do?

Provide **trusted security everywhere** and secure data and voice communication regardless of device, environment or location.

Deliver **proven security architectures** to organizations all over the world including governments, enterprises and carriers.

Now a wholly owned subsidiary of **Ultra Electronics**, a $2B Security and Defense products and services public company.

Communicate Securely From Anywhere



All in One Transport:

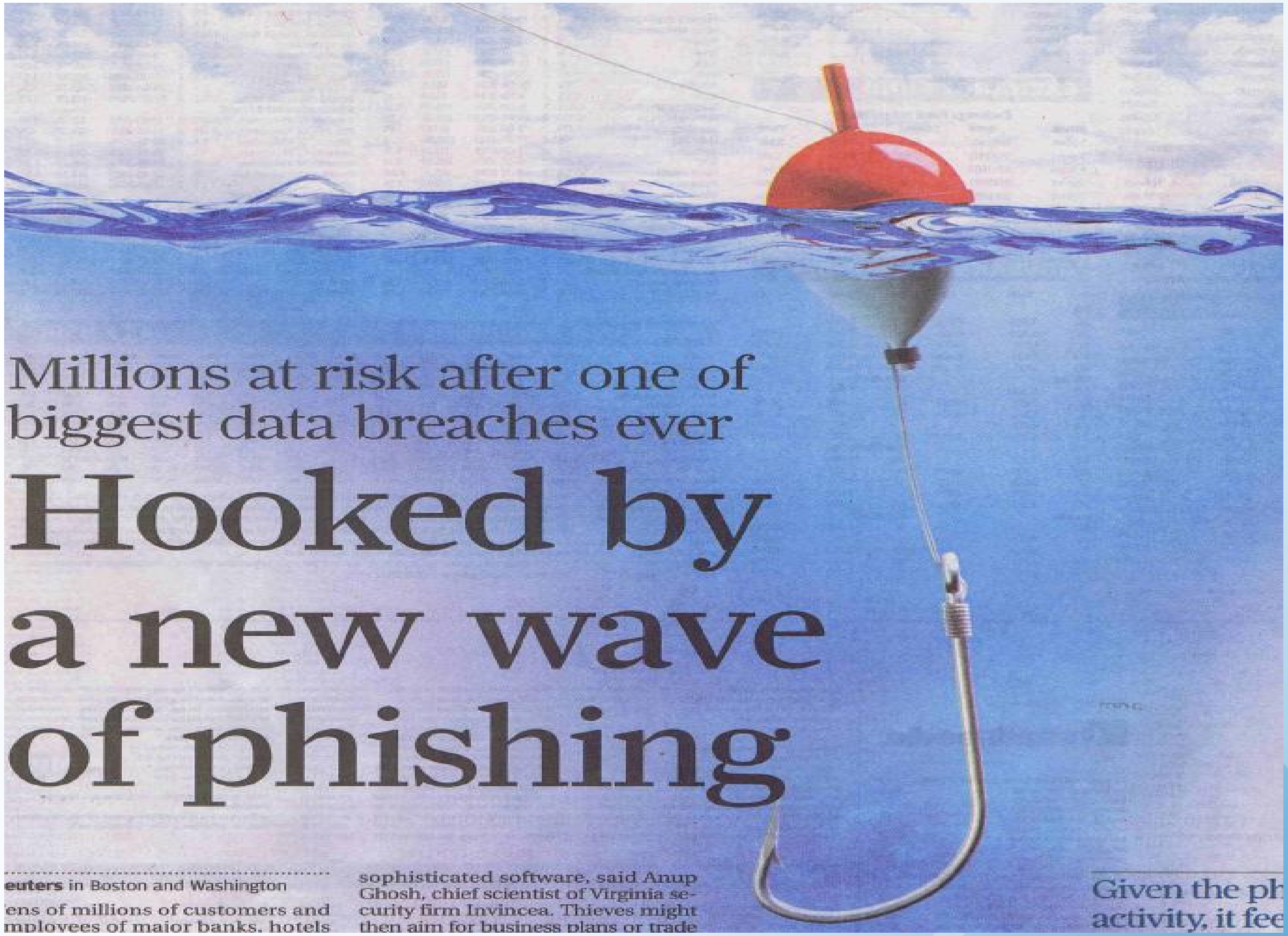
- Bridging Legacy to Newer
  - e.g. copper to fiber
- Any to Any
  - e.g. IP to 3G/4G
- Improves response time over high latency networks
  - e.g. satellite

Ensure the quality and security of digital signing keys used by applications providing security for:

- Government, finance, and telecommunications companies
- Domain Name System Security Extensions (DNSSEC)
- Public Key Infrastructure (PKI) Applications
- Content Providers (music, software, media)
- Electronic Gaming Machines (EGM) Security
- Payment Card Industry (PCI) Compliance
- Supply Chain Security
- Healthcare Electronic Patient Record (EPR) Security

What's DNSSEC ?
And
Why do I need it?

Phishing



Millions at risk after one of biggest data breaches ever

Hooked by a new wave of phishing

euters in Boston and Washington

ens of millions of customers and mplovees of maior banks. hotels

sophisticated software, said Anup Ghosh, chief scientist of Virginia security firm Invincea. Thieves might then aim for business plans or trade

Given the ph activity, it fee

Phishing

- Phishing can be done via email:
  - Attacker makes you think that email is legit
  - Convinces you to click on a link
  - Link looks close to what it's supposed to be:

Bancofamerica.com instead of

Bankofamerica.com

What is DNS?

- DNS is the internet’s phone book
- Translates website name to an IP address
- Distributed and hierarchical
- Relies on thousands of DNS servers at different domains and zones.
- At the top of the pyramid (root of the tree) is the root zone
- DNS is inherently trusted

DNS

- Imagine if the phone book got hacked?
- Imagine if someone slipped a new phone book on your driveway?
- Some important numbers were different, like banks.
- Next time you look up your Bank's phone number, you get a fake number.
- Call that number, it duplicates the phone tree.
- You can imagine the rest…

Why DNSSEC ?

Why DNSSEC ?

Dan Kaminsky

Why DNSSEC ?

- 2008 Black Hat Conference
- Dan Kaminsky demonstrated live how you can exploit a critical flaw in DNS and hijack a website.
- He is credited for developing DNSSEC as the solution to prevent DNS exploits.
- The US Government mandated that all Federal websites implement DNSSEC by end of 2009.

RECENT DNS ATTACKS

- January 2010, websites of **Amazon.com** and **Walmart.com** were brought down due to DNS attacks.
- Not talked about much publicly…
- Their DNS servers were compromised.
- DNS supplier Neustar - UltraDNS

Why DNSSEC ?

Dell Australia customer details stolen in major global data breach

Asher Moses
April 7, 2011 - 12:29PM

- Cyber raids 'threaten British, US stock markets‘ January 31, 2011 - 8:39PM
- EU halts trading after hacking - **Sydney Morning Herald**
- Nasdaq acknowledges hit by hackers February 7, 2011 - 12:01AM NYT
- More than 400 cyber attacks have affected Australian government networks in the past year, figures reveal*.*

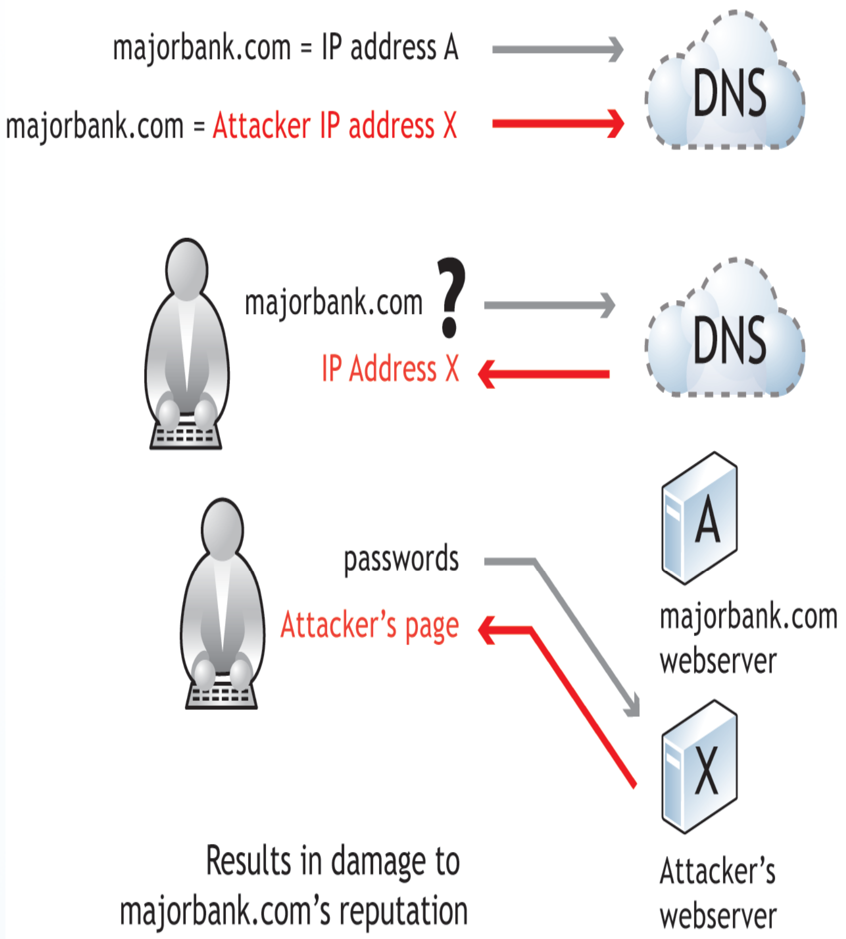
Recent Attacks

- April 26, 2011: Sony admits that 77 million customer emails and private information compromised on PlayStation worldwide network.
- Network out for several months!
- 25 Million user private information published on the internet.

Recent Attacks

- Recently, the targets have been Certification Authorities (CA).
- This is the new international warfare
- Comodo CA attacked
- DigiNotar CA in the Netherlands attacked
- Both performed by Iranian hackers!
- A hacker who gets a certificate for Bankofamerica.com will be able to steal people's passwords and hijack their accounts.

Without DNSSEC



majorbank.com = IP address A

majorbank.com = Attacker IP address X

DNS

majorbank.com ?

IP Address X

DNS

passwords

Attacker's page

A

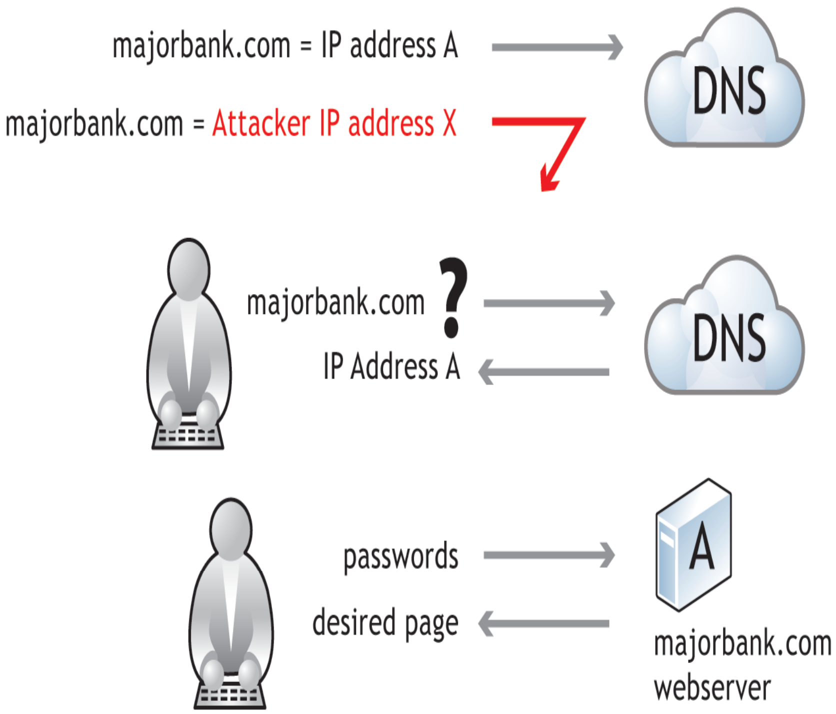
majorbank.com webserver

X

Attacker's webserver

Results in damage to majorbank.com's reputation

With DNSSEC



majorbank.com = IP address A

majorbank.com = Attacker IP address X

DNS

majorbank.com ?

IP Address A

DNS

passwords

desired page

A

majorbank.com webserver

What are DNSSEC benefits?

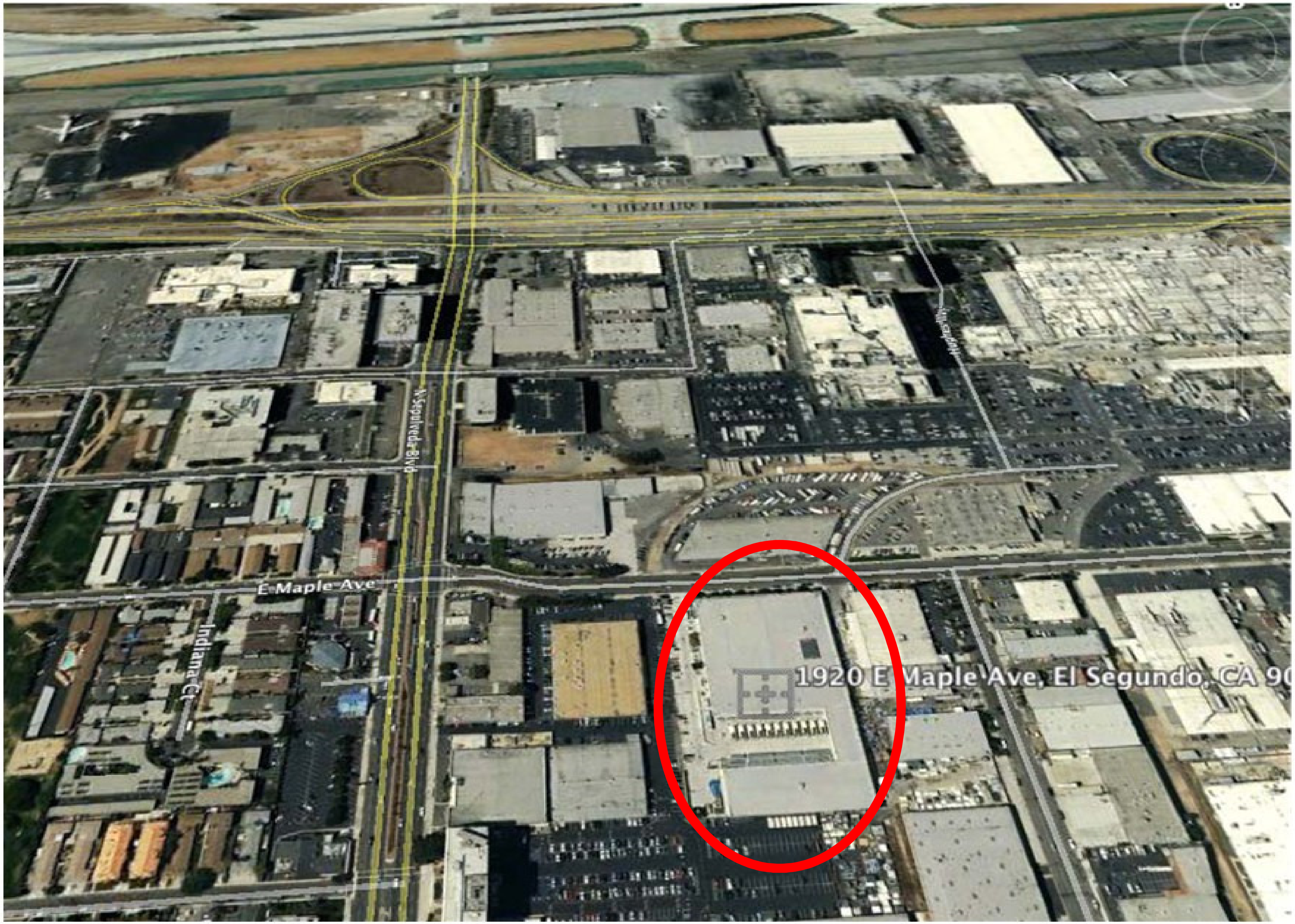
- DNS lookup can be modified in transit to redirect an end user to an imposter or malicious site for password collection.
- Modification attacks carried out en masse at ISP/enterprise = cache poisoning.
- A lookup secured with DNSSEC is protected against modification = primary benefit.
- Greatest benefits may be yet to come. Why not securely distribute more than just DNS info? Other keys? Identification info?
- DNSSEC deployment at root and TLDs set the stage

ICANN DNSSEC Implementation

ICANN

July 15, 2010 ICANN goes live with AEP & ISC DNSSEC solution

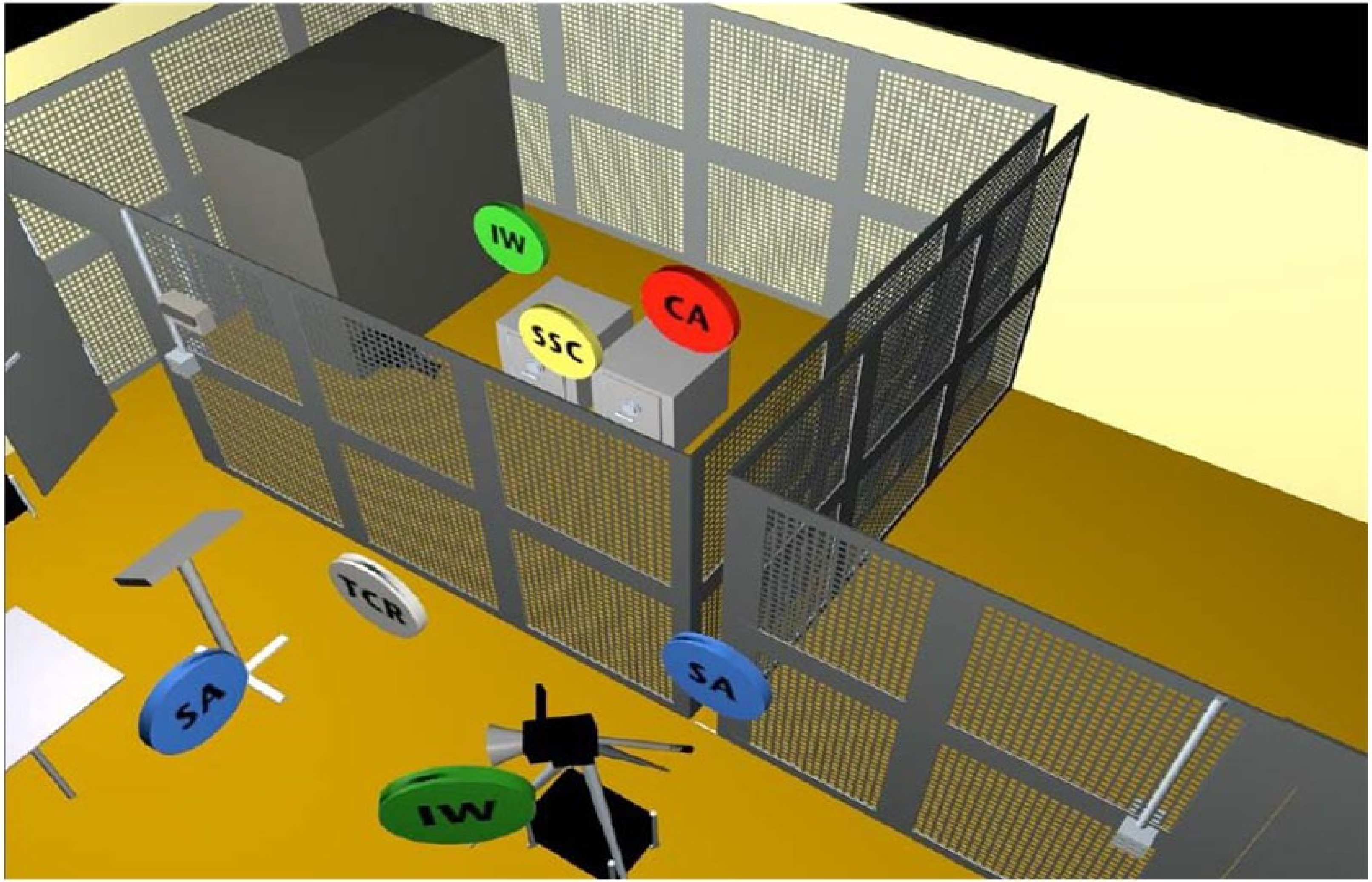
Los Angeles Datacenter



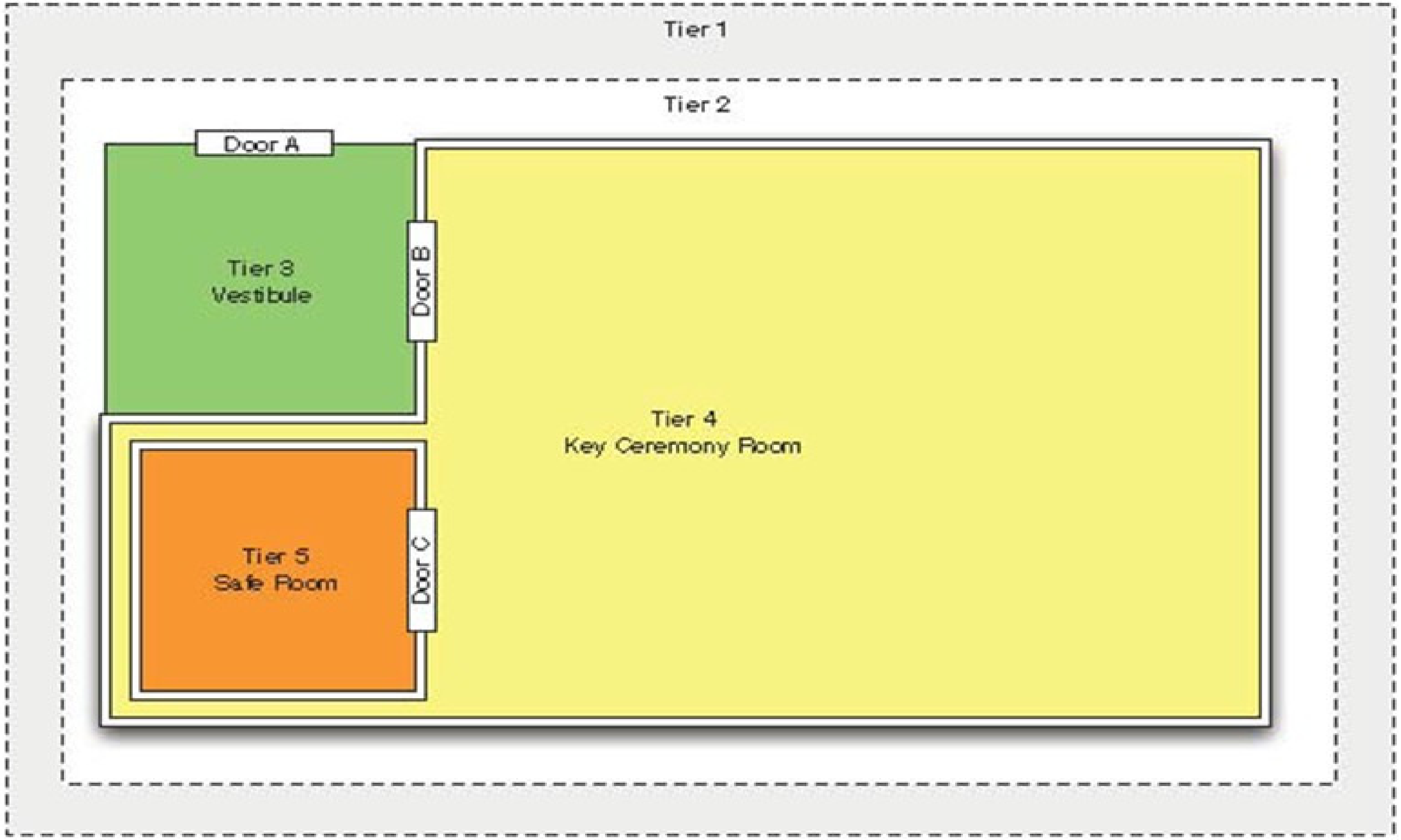
Washington DC Datacenter

January 27, 2010

Secure Cage in Datacenter



Physical Security



17:29 13:29 10:29

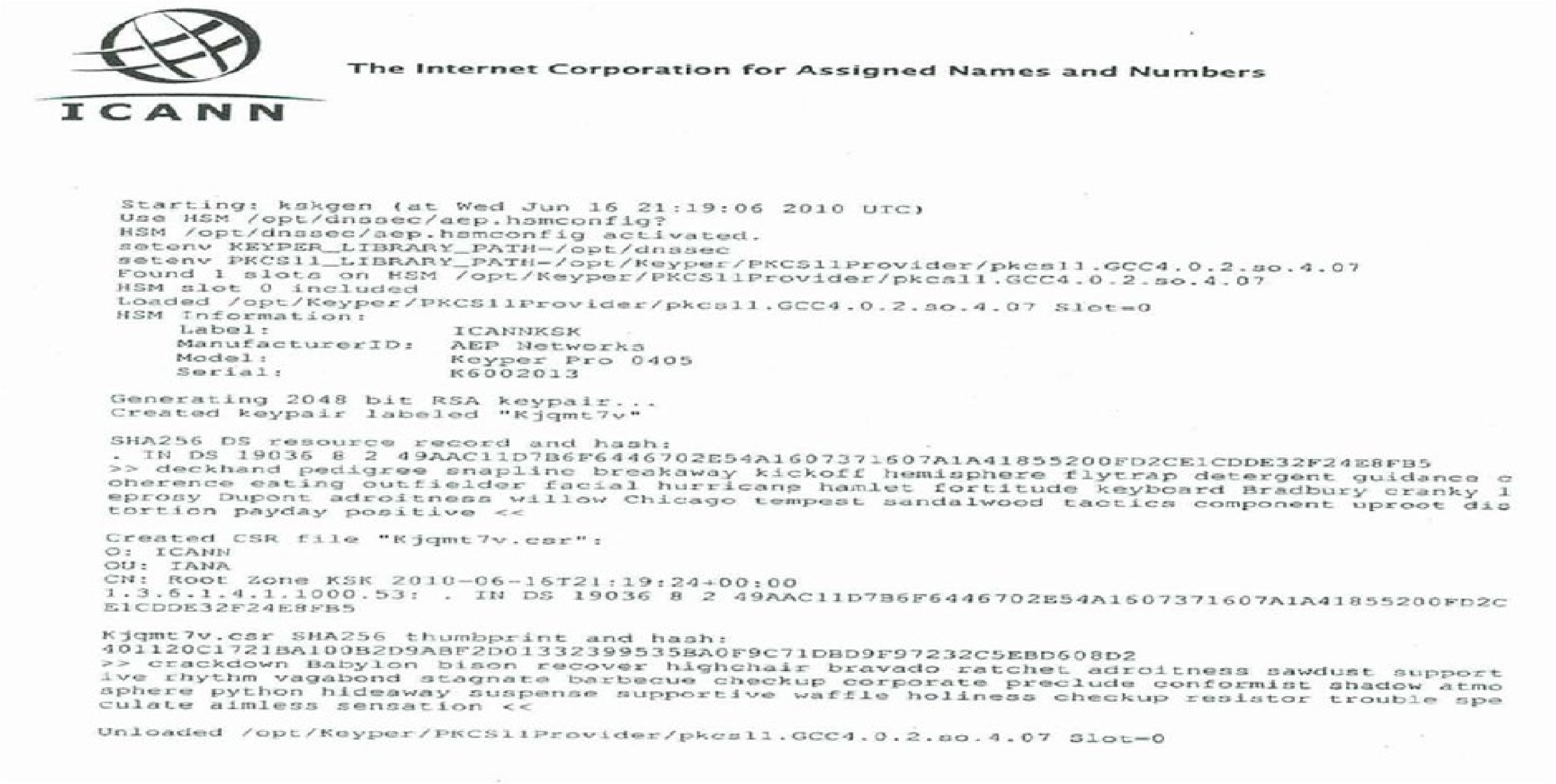
AREA
AUTHORIZED PERSONNEL ONLY
LG

SAFE 2
SAFE 1

ICANN
SAMSUNG

NOTICE
NOTICE
NOTICE
NO FOOD OR DRINK BEYOND THIS POINT
NOTICE
ICANN
SEAHAWKS
3066
ICANN
One World. One Internet. Everyone Connected.
19036

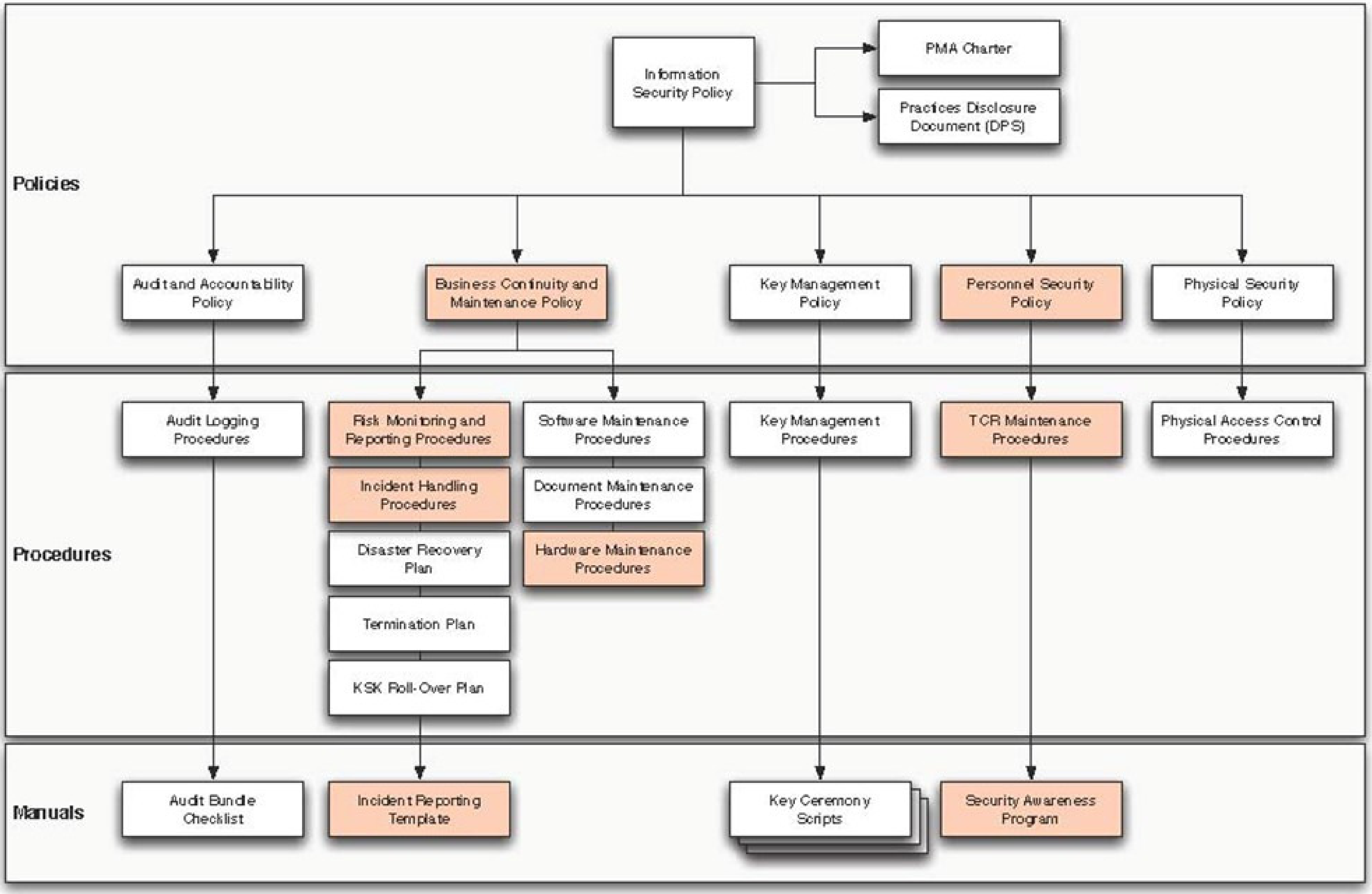
Root Key Generation



ICANN

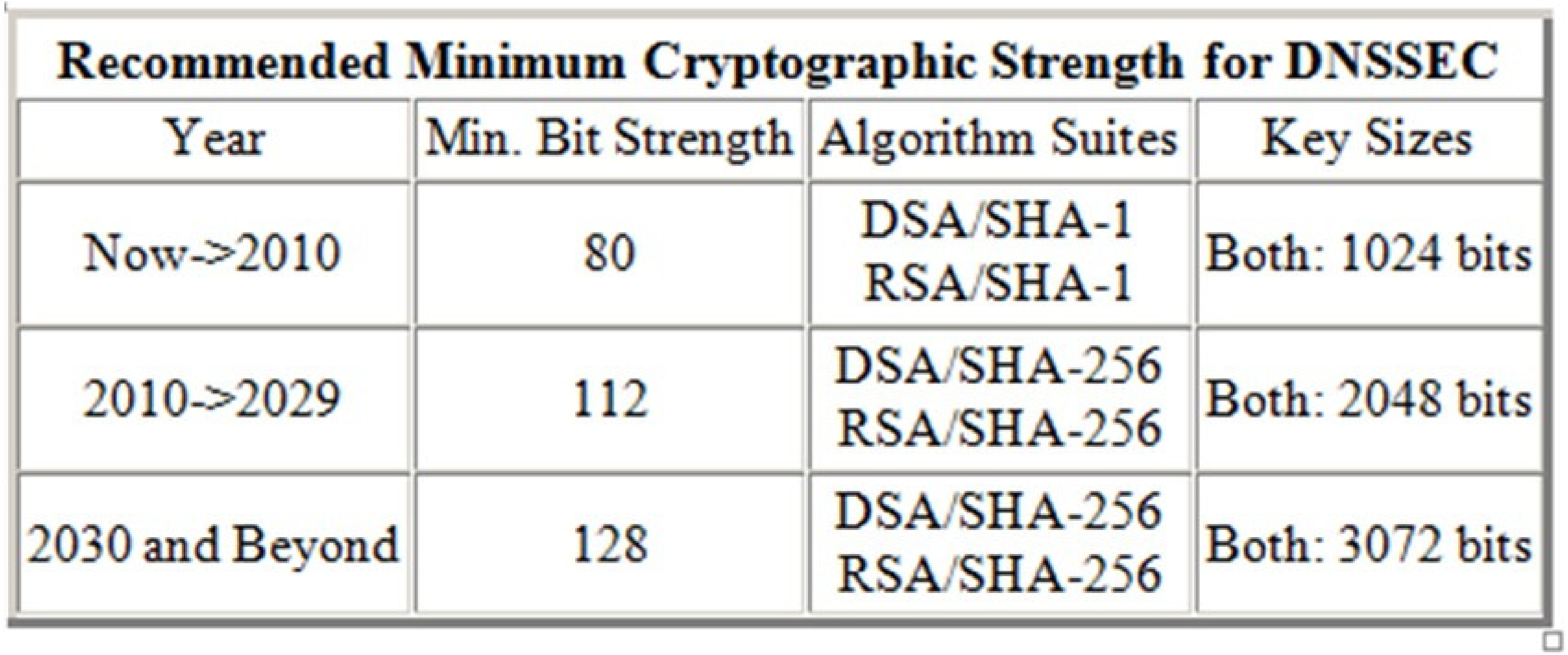
The Internet Corporation for Assigned Names and Numbers

```
Starting: kskgen (at Wed Jun 16 21:19:06 2010 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
     Label:            ICANNKSK
     ManufacturerID:   AEP Networks
     Model:            Keyper Pro 0405
     Serial:           K6002013

Generating 2048 bit RSA keypair...
Created keypair labeled "Kjqmt7v"

SHA256 DS resource record and hash:
. IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5
>> deckhand pedigree snapline breakaway kickoff hemisphere flytrap detergent guidance c
oherence eating outfielder facial hurricane hamlet fortitude keyboard Bradbury cranky l
eprosy Dupont adroitness willow Chicago tempest sandalwood tactics component uproot dis
tortion payday positive <<

Created CSR file "Kjqmt7v.csr":
O: ICANN
OU: IANA
CN: Root Zone KSK 2010-06-16T21:19:24+00:00
1.3.6.1.4.1.1000.53: . IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2C
E1CDDE32F24E8FB5

Kjqmt7v.csr SHA256 thumbprint and hash:
401120C1721BA100B2D9ABF2D01332399535BA0F9C71DBD9F97232C5EBD608D2
>> crackdown Babylon bison recover highchair bravado ratchet adroitness sawdust support
ive rhythm vagabond stagnate barbecue checkup corporate preclude conformist shadow atmo
sphere python hideaway suspense supportive waffle holiness checkup resistor trouble spe
culate aimless sensation <<

Unloaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```


Information Security Policy
PMA Charter
Practices Disclosure Document (DPS)
Policies
Audit and Accountability Policy
Business Continuity and Maintenance Policy
Key Management Policy
Personnel Security Policy
Physical Security Policy
Procedures
Audit Logging Procedures
Risk Monitoring and Reporting Procedures
Software Maintenance Procedures
Key Management Procedures
TCR Maintenance Procedures
Physical Access Control Procedures
Incident Handling Procedures
Document Maintenance Procedures
Disaster Recovery Plan
Hardware Maintenance Procedures
Termination Plan
KSK Roll-Over Plan
Manuals
Audit Bundle Checklist
Incident Reporting Template
Key Ceremony Scripts
Security Awareness Program

Algorithm / 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

ICANN PARAMETERS

- Split KSK and ZSK
- KSK is 2048-bit RSA
  - Rolled as required
  - RFC 5011 for automatic key rollovers
- Signatures made using SHA-256
- ZSK is 1024-bit RSA
  - Rolled once a quarter (four times per year)
- Zone signed with NSEC
- Signatures made using SHA-256

Crypto Officer (CO)

- Have physical keys to safe deposit boxes holding smartcards that activate the HSM
- ICANN cannot generate new key or sign ZSK without 3 of 7 COs
- Able to travel 4 times to US

Recovery Key Shareholder (RKSH)

- Have smartcards holding pieces (M of N) of the key used to encrypt KSK inside HSM
- If both key management facilities fall into the ocean, 5 of 7 RKSH smartcards and an encrypted KSK smartcard can reconstitute KSK in a new HSM
- Backup KSK encrypted on smartcard held by ICANN
- Able to travel to US on relatively short notice. Hopefully never.
- Annual Inventory.

CO

Alain Aina, BJ
Anne-Marie Eklund Löwinder, SE
Frederico Neves, BR
Gaurab Upadhaya, NP
Olaf Kolkman, NL
Robert Seastrom, US
Vinton Cerf, US

Andy Linton, NZ
Carlos Martinez, UY
Dmitry Burkov, RU
Edward Lewis, US
João Luis Silva Damas, PT
Masato Minda, JP
Subramanian Moonesamy, MU

CO BCK

Christopher Griffiths, US
Fabian Arbogast, TZ
John Curran, US
Nicolas Antoniello, UY
Rudolph Daniel, UK
Sarmad Hussain, PK
Ólafur Guðmundsson, IS

RKSH

Bevil Wooding, TT
Dan Kaminsky, US
Jiankang Yao, CN
Moussa Guebre, BF
Norm Ritchie, CA
Ondřej Surý, CZ
Paul Kane, UK

BCK

David Lawrence, US
Dileepa Lathsara, LK
Jorge Etges, BR
Kristian Ørmen, DK
Ralf Weber, DE
Warren Kumari, US

DNSSEC Status - Jan 15, 2012

- Signed root published 15 July, 2010
- 88 TLDs out of 312 total have been signed
- Details: http://stats.research.icann.org/dns/tld_report/
- 8 of 16 gTLD registries are signed: .com, .net, .org, .asia, .biz, .cat, .info, .museum
- 2 of 3 US TLDs are signed: .edu, .gov
- Biggest change to Internet in 20+ years
- Security applications built on DNSSEC

ICANN’s HSM Crypto requirements:

ICANN

⇛ Generate, store and manage cryptographic keys to the highest level of assurance

- Highest level of security (FIPS 140-2 Level 4) required
- Never been compromised
- High quality RNG
- Keys can be backed up

⇛ Track record and customer credibility

⇛ 10 year support for products

Types of HSMs

PCI card

- Limited platform and operating system support due to requirement for drivers
- Tamper evident only protection: does not erase keys if tampered with
- Typically FIPS 140-2 Level 2 or 3 validated

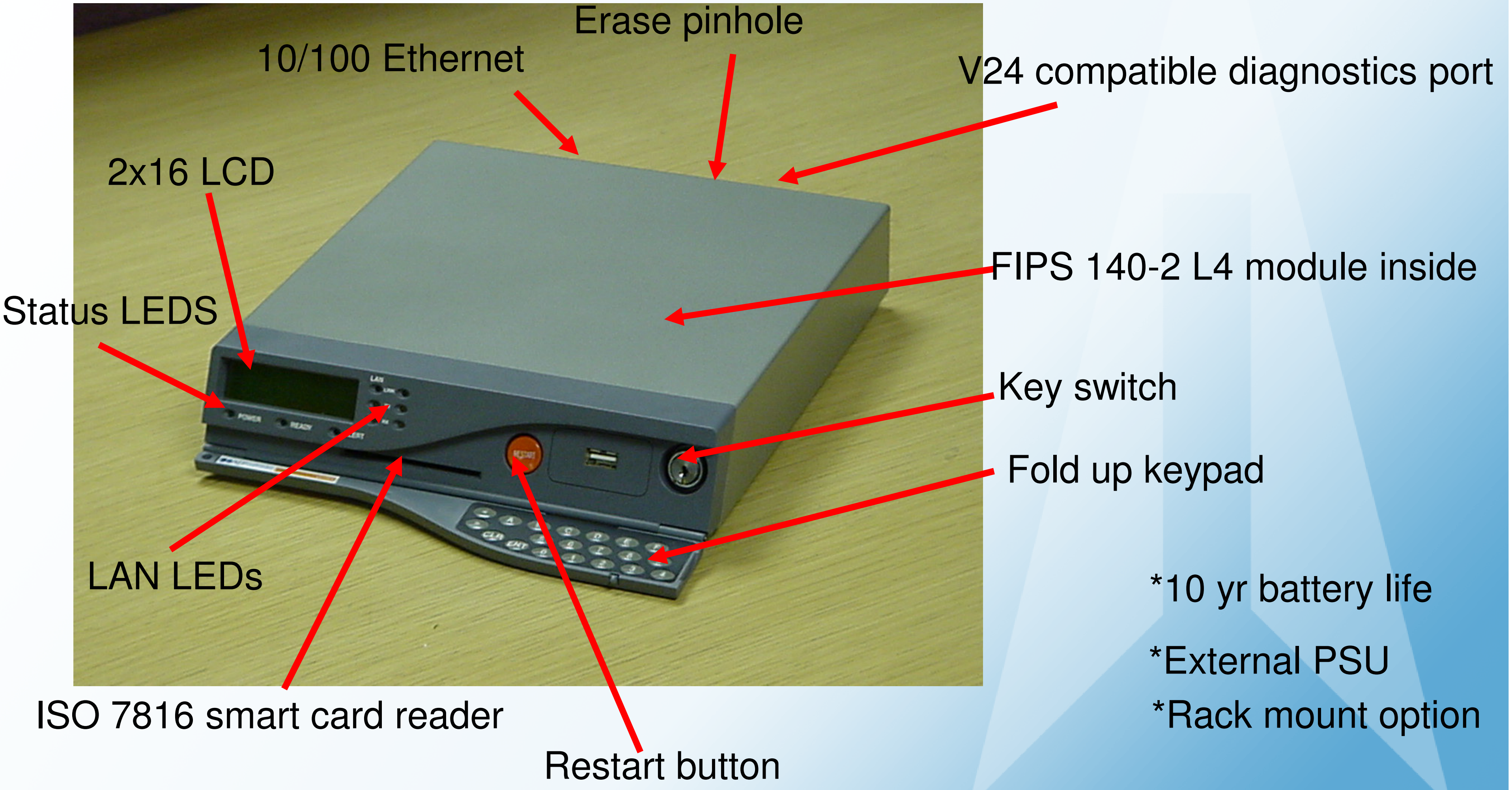
Network-attached PC containing PCI card

- Uses standard general purpose operating systems (FreeBSD, GNU Linux etc) with attendant vulnerabilities
- Contains PCI Card (FIPS 140-2 Level 2 or 3 validated)
- No tamper protection
- No FIPS 140-2 certification

Standalone, network attached HSM

- Hardware/firmware is designed for purpose
- Tamper reaction protection: automatically, positively erases keys if tampered
- FIPS 140-2 Level 4 validated

FIPS 140-2 Level 4 Hardware



*10 yr battery life

*External PSU

*Rack mount option

Why Choose a FIPS 140-2 L4 HSM?

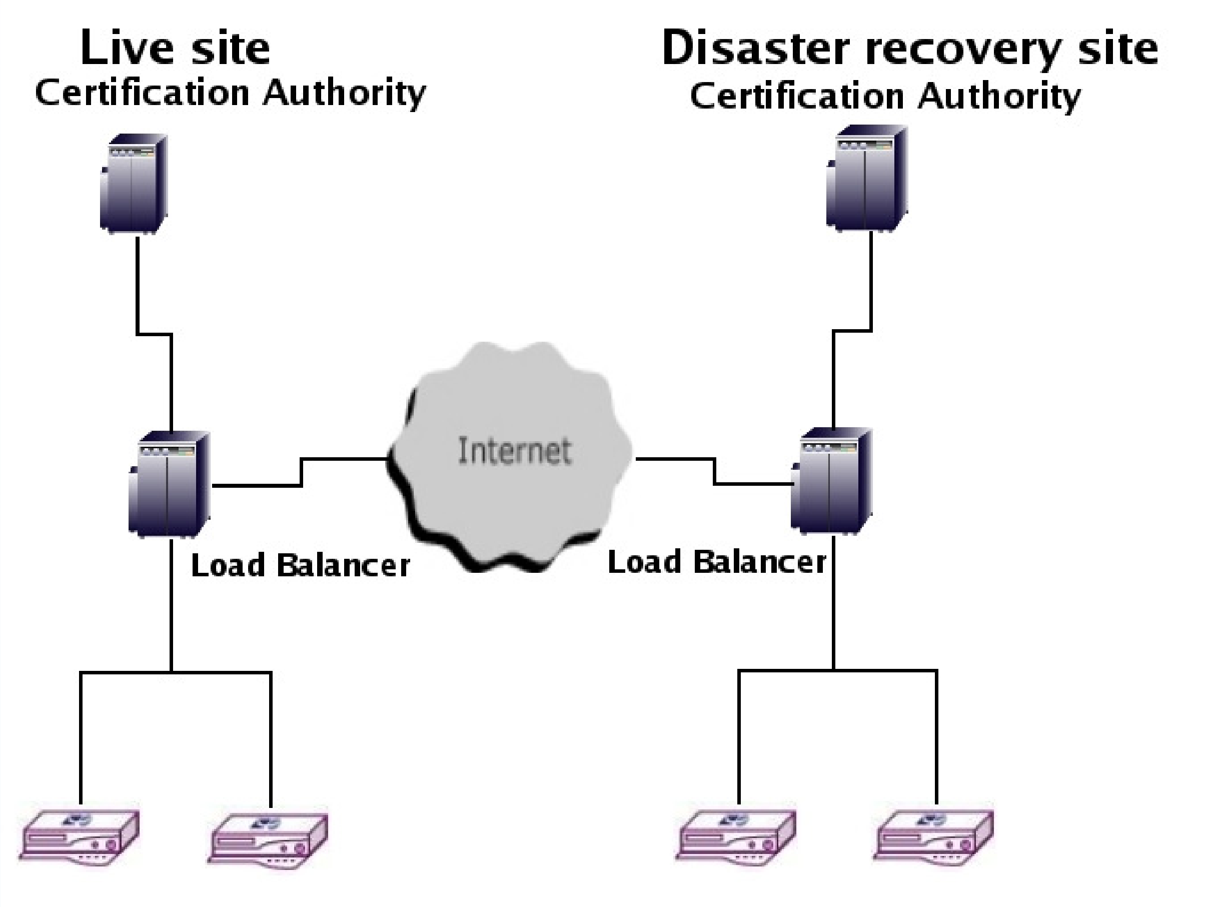
Hacker and virus proof

- Signed downloads
- Separation of code and data
- No PC-based vulnerabilities (not a general purpose OS)
- Never had a vulnerability in its 10+ years history

High reliability and redundancy

- Fully solid state
- No moving parts
- No PC-based vulnerabilities (no general purpose OS)
- High availability
- Load Balancing (up to 16)
- Fault tolerance using all AEP Keypers live (up to 16)
- Hot swappable (up to 16)

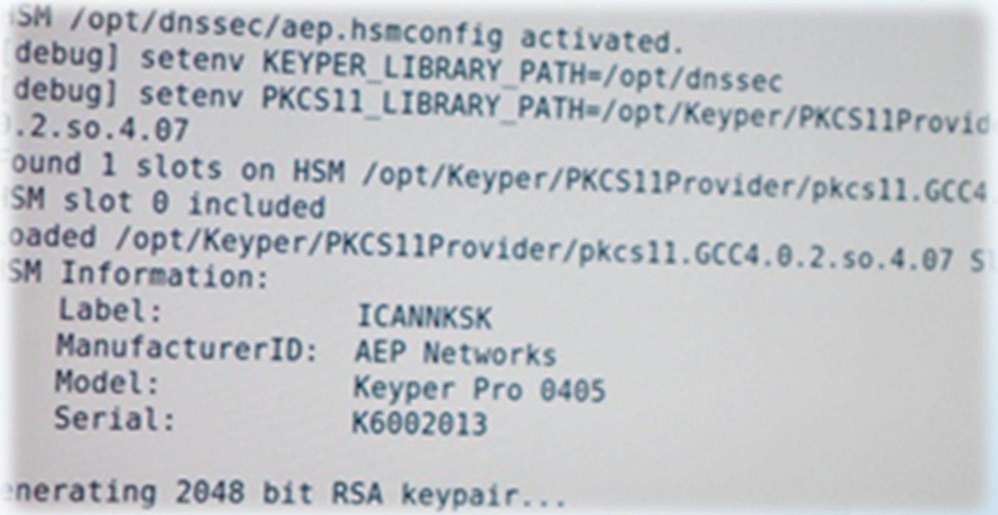
HA + Disaster Recovery



FIPS 140-2 L4 HSM Performance

- 1200 Signing Transactions per Second (1024-bit RSA)
- 500 TPS (2048-bit RSA)
- **100 Million Signing Transactions per Day**
- 42 Million TPD (2048-bit RSA)
- Clustering up to 16 Load Balanced HSM's
- **1.6 Billion Signing Transactions per Day**
- 700 Million TPD (2048-bit RSA)
- Verisign signs **96 Million Domains** under .com and 6 Million domains under .net.

FIPS 140-2 L4 HSM secures Internet DNS Root Zone



```
SM /opt/dnssec/aep.hsmconfig activated.
debug] setenv KEYPER_LIBRARY_PATH=/opt/dnssec
debug] setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provid
.2.so.4.07
ound 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4
SM slot 0 included
oaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 S
SM Information:
   Label:            ICANNKSK
   ManufacturerID:   AEP Networks
   Model:            Keyper Pro 0405
   Serial:           K6002013

nerating 2048 bit RSA keypair...
```

“Security is a critical factor for ICANN’s DNSSEC deployment, … FIPS Level 4 was an easy choice,”

– Richard Lamb, ICANN

If you want to be as secure as the Root of the Internet, then deploy what ICANN implemented for security, a FIPS 140-2 Level 4 HSM

ICANN