DNSSEC Root Signing HowTo, Lessons Learned, and Future Impact
Richard Lamb - ICANN

GTER 30
Sao Leopoldo, Brazil
26 November 2010
richard.lamb@icann.org

DNSSEC Root HowTo

Goal: Transparency

- Processes and procedures should be as open as possible for the Internet community to trust the signed root

Goal: Audited

- Processes and procedures should be audited against industry standards, e.g. ISO/IEC 27002:2005

Goal: High Security

- Root system should meet all NIST SP 800-53 technical security controls required by a HIGH IMPACT system

Goal: Community Involvement

- Trusted representatives from the community are invited to take an active role in the key management process

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

Validity Periods

- DNSKEY-covering RRSIG (by KSK) validity 15 days
    - new signatures published every 10 days
- Other RRSIG (by ZSK) validity 7 days
    - zone generated and resigned twice per day

Root Trust Anchor

- Published on a web site by ICANN as
  - XML-wrapped and plain DS record
    - to facilitate automatic processing
  - PKCS #10 certificate signing request (CSR)
    - as self-signed public key
    - Allows third-party CAs to sign the KSK
    - ICANN signs the CSR producing a CERT

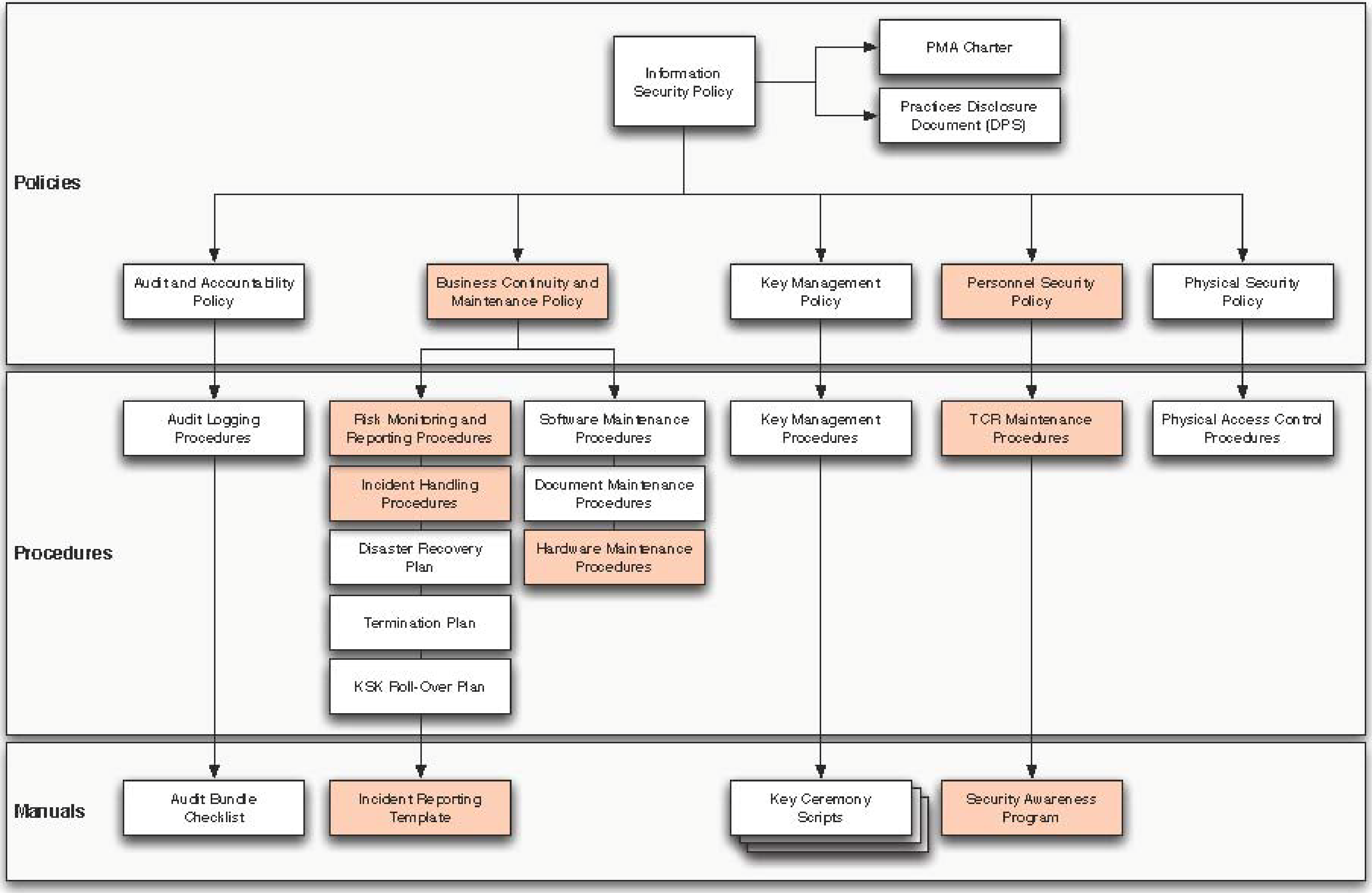
Auditing & Transparency

- Third-party auditors check that ICANN operates as described in documentation
- Other external witnesses may also attend the key ceremonies
- SysTrust audit being performed as we speak

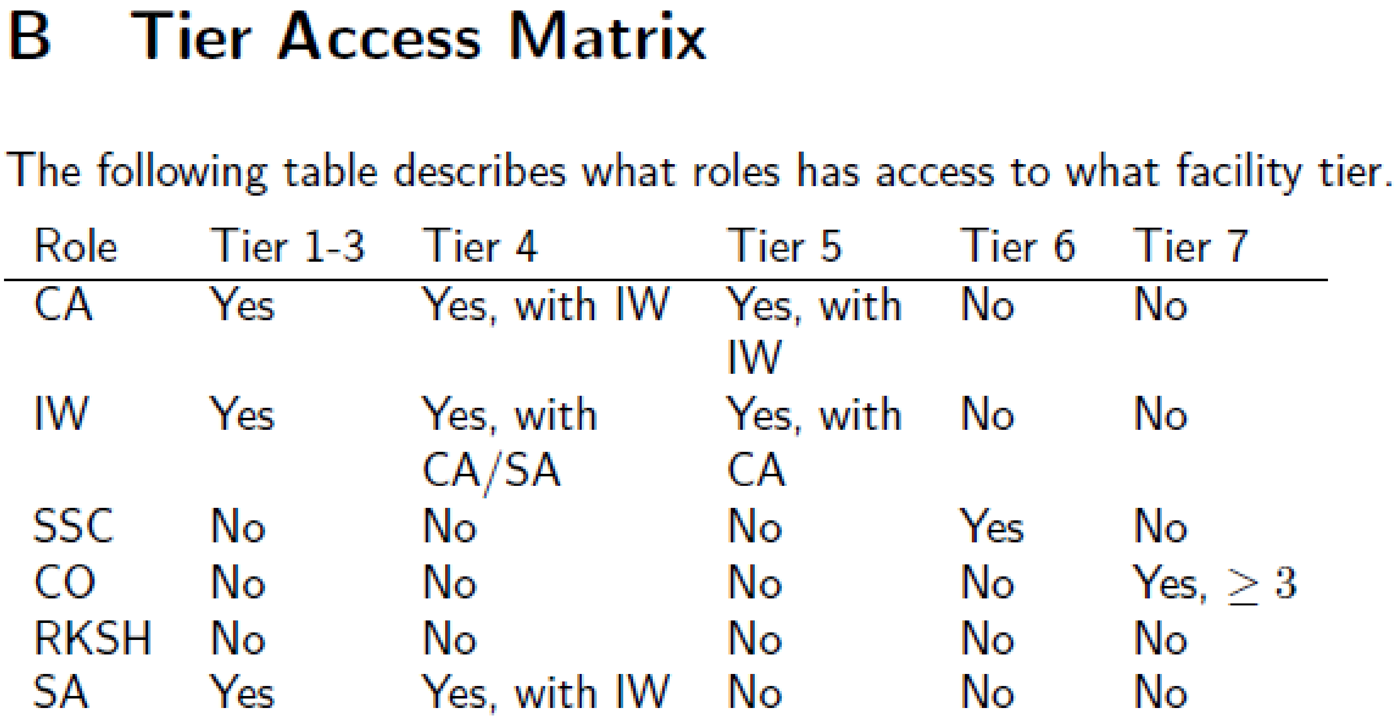
DPS

DNSSEC Practice Statement

- States the practices and provisions that are employed in root zone signing and zone distribution services
  - Issuing, managing, changing and distributing DNS keys in accordance with the specific equirements of the U.S. DoC NTIA
- Comparable to a certification practice statement (CPS) from an X.509 certification authority (CA)


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

Key Management Document

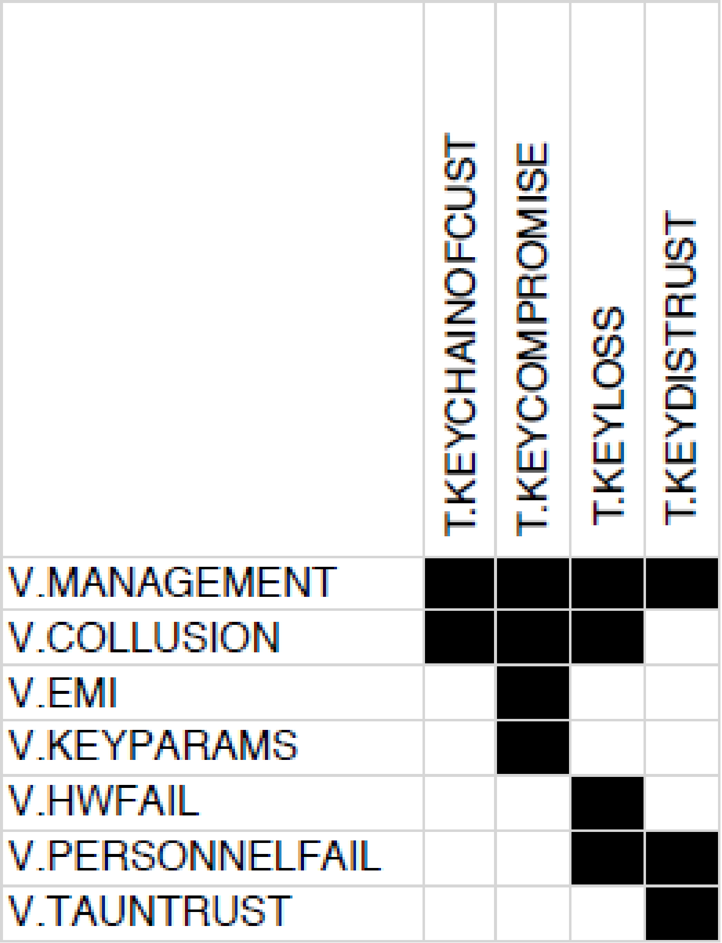


B Tier Access Matrix

The following table describes what roles has access to what facility tier.

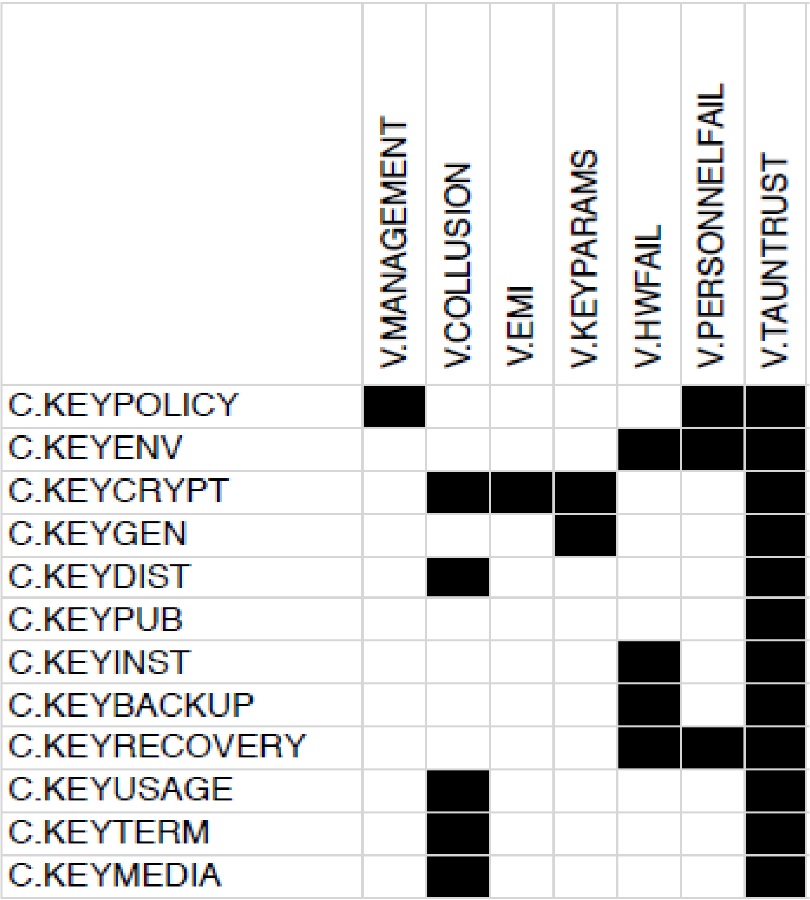
Role	Tier 1-3	Tier 4	Tier 5	Tier 6	Tier 7
CA	Yes	Yes, with IW	Yes, with IW	No	No
IW	Yes	Yes, with CA/SA	Yes, with CA	No	No
SSC	No	No	No	Yes	No
CO	No	No	No	No	Yes, ≥ 3
RKSH	No	No	No	No	No
SA	Yes	Yes, with IW	No	No	No

Threats and Vulnerabilities



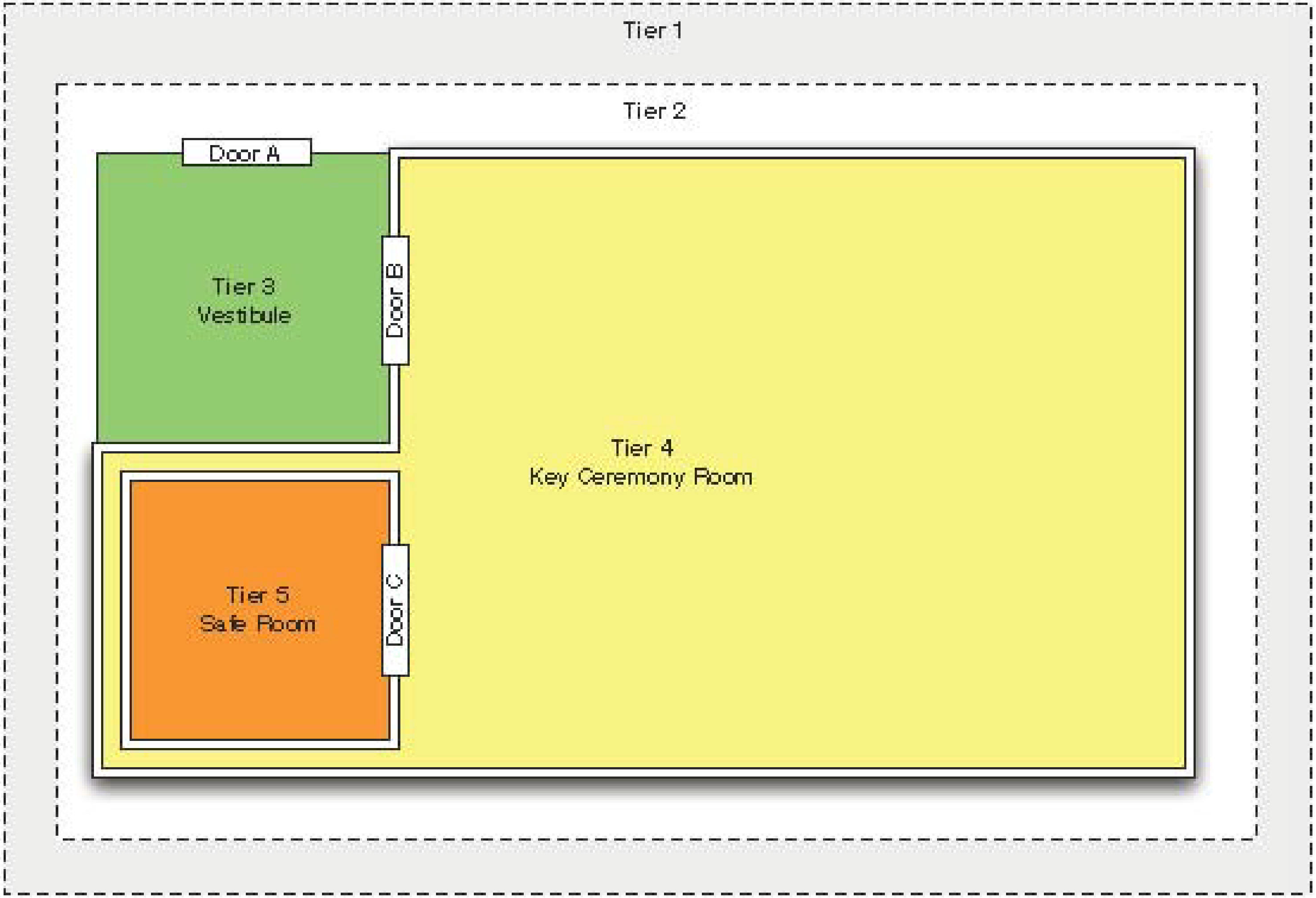
	T.KEYCHAINOFCUST	T.KEYCOMPROMISE	T.KEYLOSS	T.KEYDISTRUST
V.MANAGEMENT	■	■	■	■
V.COLLUSION	■	■	■	
V.EMI		■		
V.KEYPARAMS		■		
V.HWFAIL			■	
V.PERSONNELFAIL			■	■
V.TAUNTRUST				■

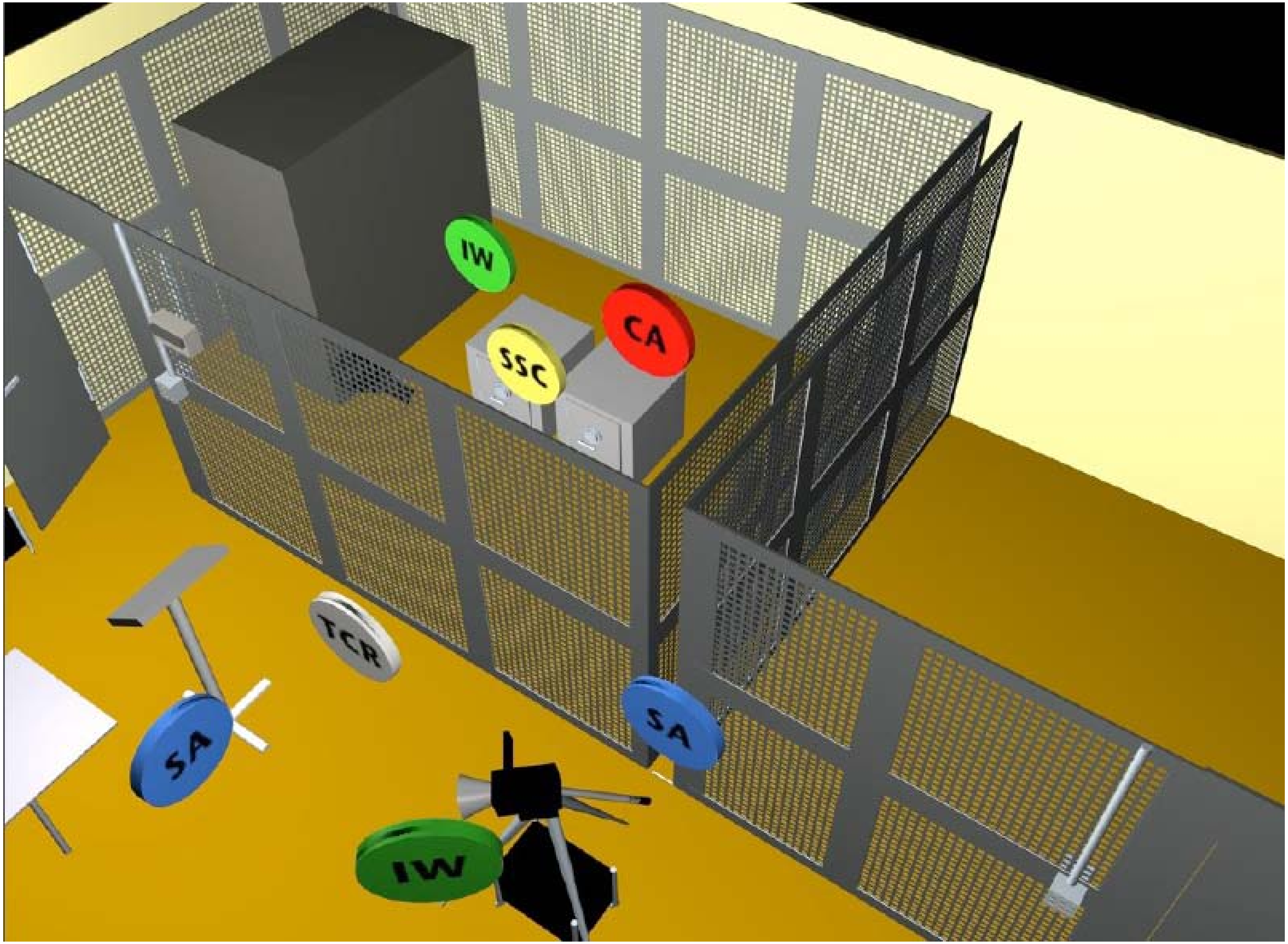
Completeness of Controls



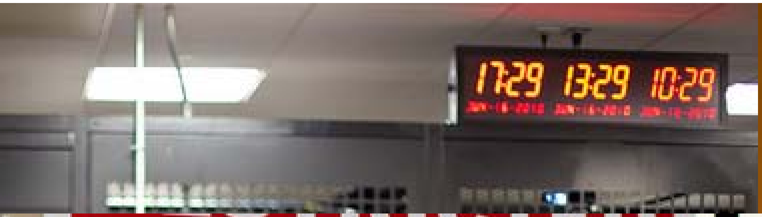
	V.MANAGEMENT	V.COLLUSION	V.EMI	V.KEYPARAMS	V.HWFAIL	V.PERSONNELFAIL	V.TAUNTRUST
C.KEYPOLICY	■					■	■
C.KEYENV					■	■	■
C.KEYCRYPT		■	■	■			■
C.KEYGEN				■			■
C.KEYDIST		■					■
C.KEYPUB							■
C.KEYINST					■		■
C.KEYBACKUP					■		■
C.KEYRECOVERY					■	■	■
C.KEYUSAGE		■					■
C.KEYTERM		■					■
C.KEYMEDIA		■					■

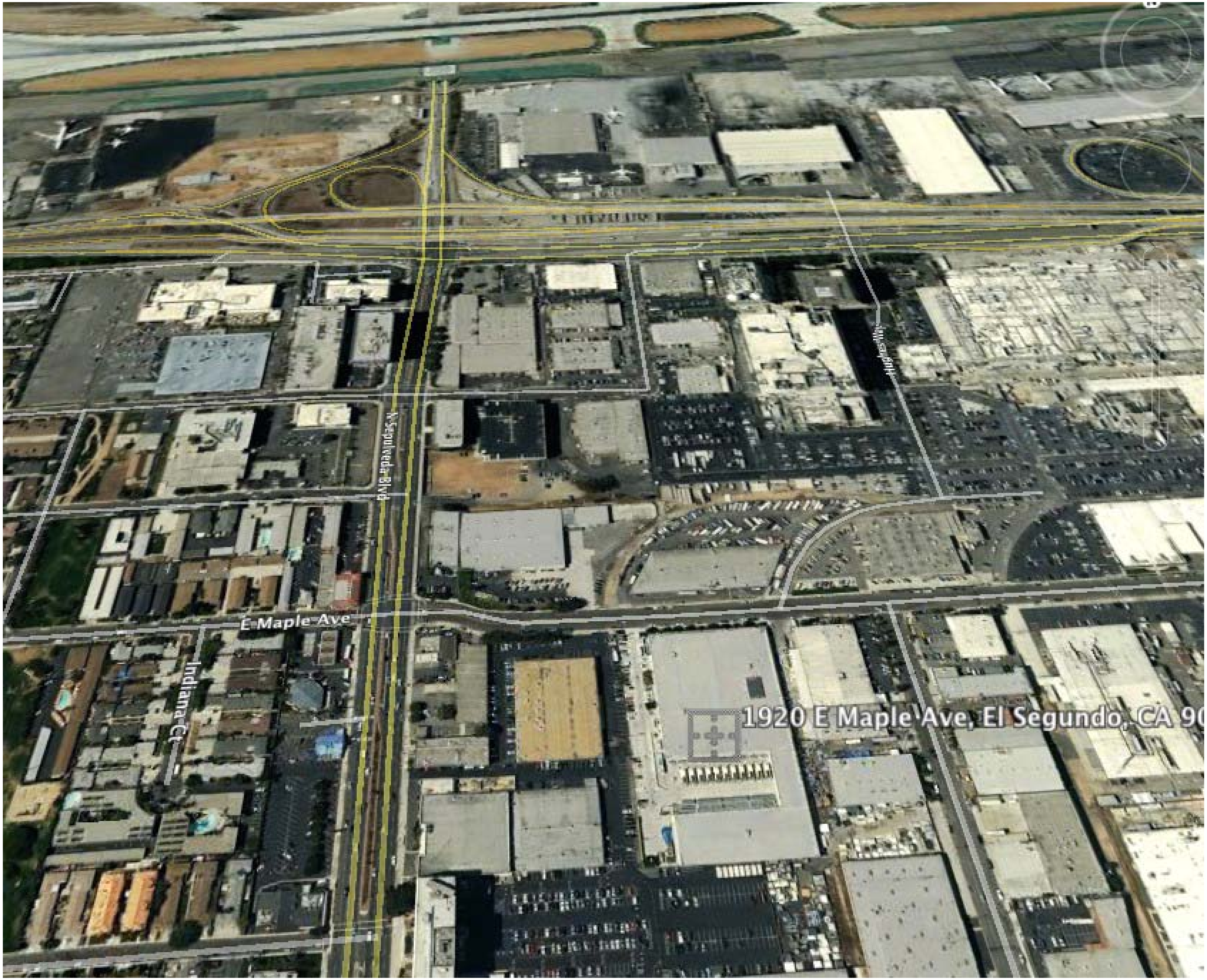
Physical Security




IW
CA
SSC
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

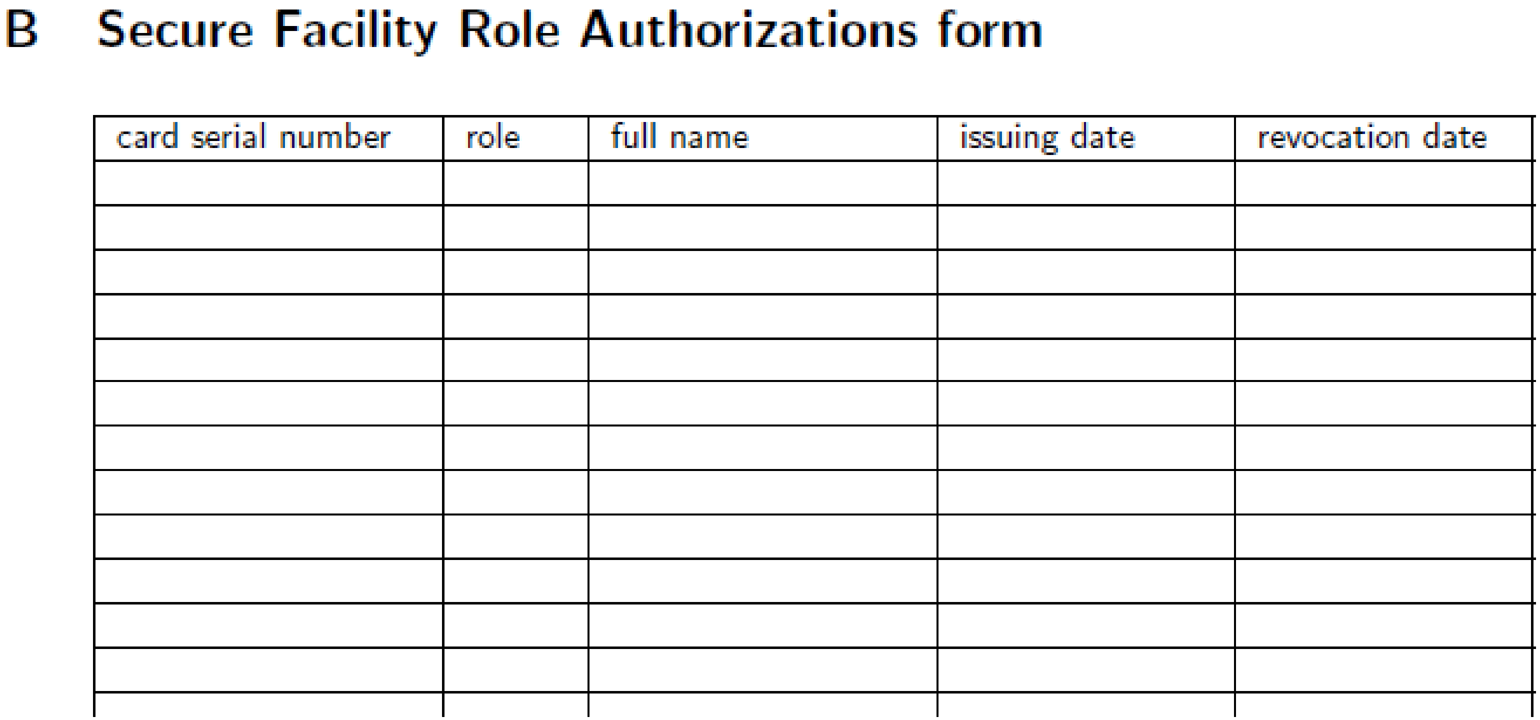
Access and Monitoring

- Facility provider
  - Controls the access on Tier 1 and Tier 2.
  - Monitors all the cameras (Tier 1-5)
  - Has access to Tier 3 for physical verification of the state of the room.
- ICANN
  - Monitors tiers 3-6 actively with state of art alarm system which includes, motion, seismic, environmental sensors.
  - Controls access to Tiers 3,4,5,6
  - Enforces and monitors to dual occupancy.

ACS

- 6 digit PINs.
- X09 locks for Tier 6.
- Motorized hook bolt locks on steel doors.
- MIFARE DESFire EV1 aka MIFARE Evolution. (Random ID/128Bit AES)
- Biometric systems; Iris scanners.

Authorizations form



B Secure Facility Role Authorizations form

card serial number	role	full name	issuing date	revocation date

Trusted Community Representatives (TCRs)

- Have an active roll in the management of the KSK
  - as Crypto Officers needed to activate the KSK
  - as Recovery Key Share Holders protecting shares of the symmetric key that encrypts the backup copy of the KSK

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 up to 4 times a year to US.

Recovery Key Shareholder (RKSH)

- Have smartcards holding pieces (M-of-N) of the key used to encrypt the KSK inside the 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 on relatively short notice to US. 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

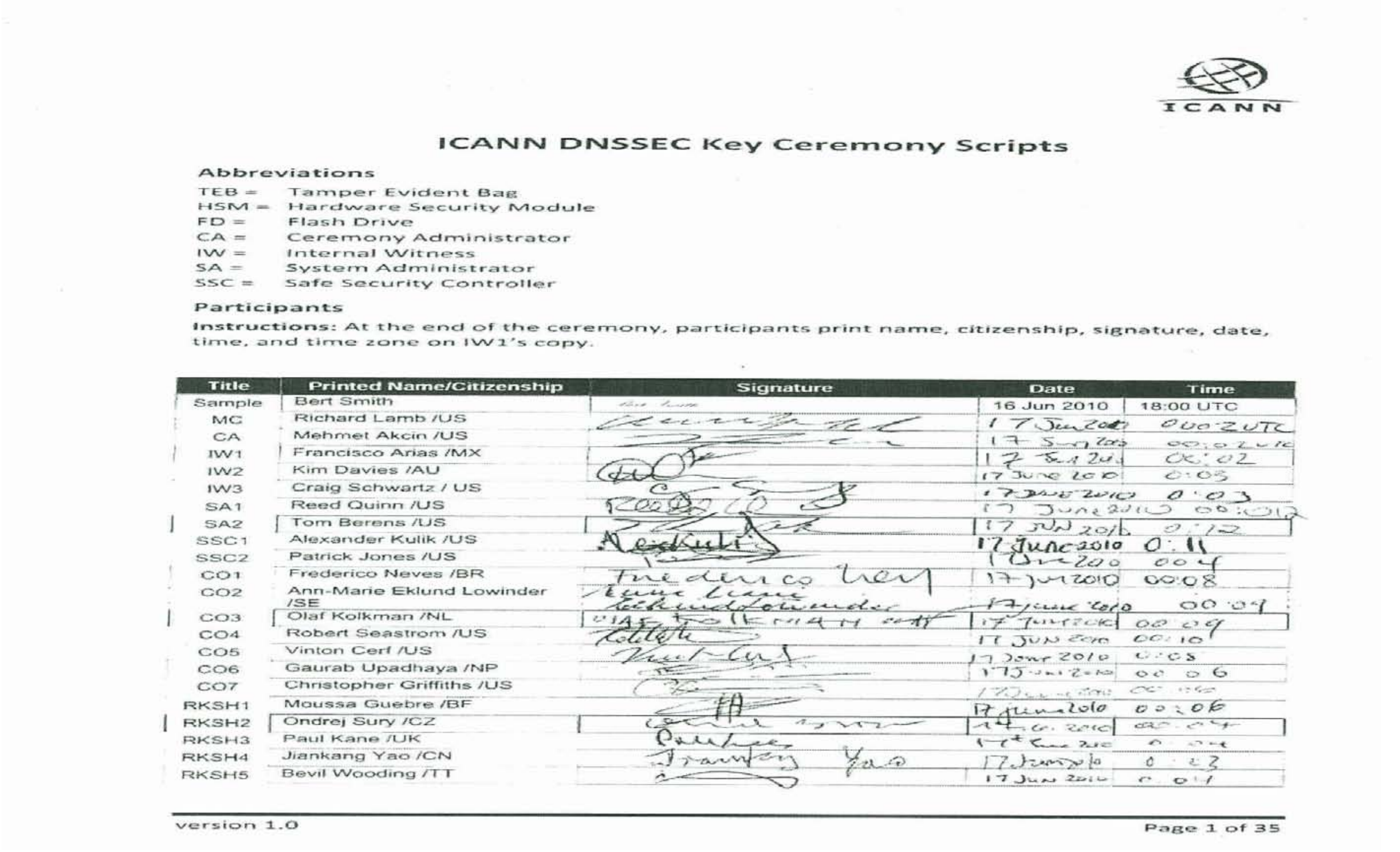
BCK

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

Key Ceremonies

- Key Generation
  - Generation of new KSK
- Processing of ZSK Signing Request (KSR)
  - Signing ZSK for the next upcoming quarter (3-month intervals)
  - Every quarter

Key Ceremony Script



ICANN

ICANN DNSSEC Key Ceremony Scripts

Abbreviations

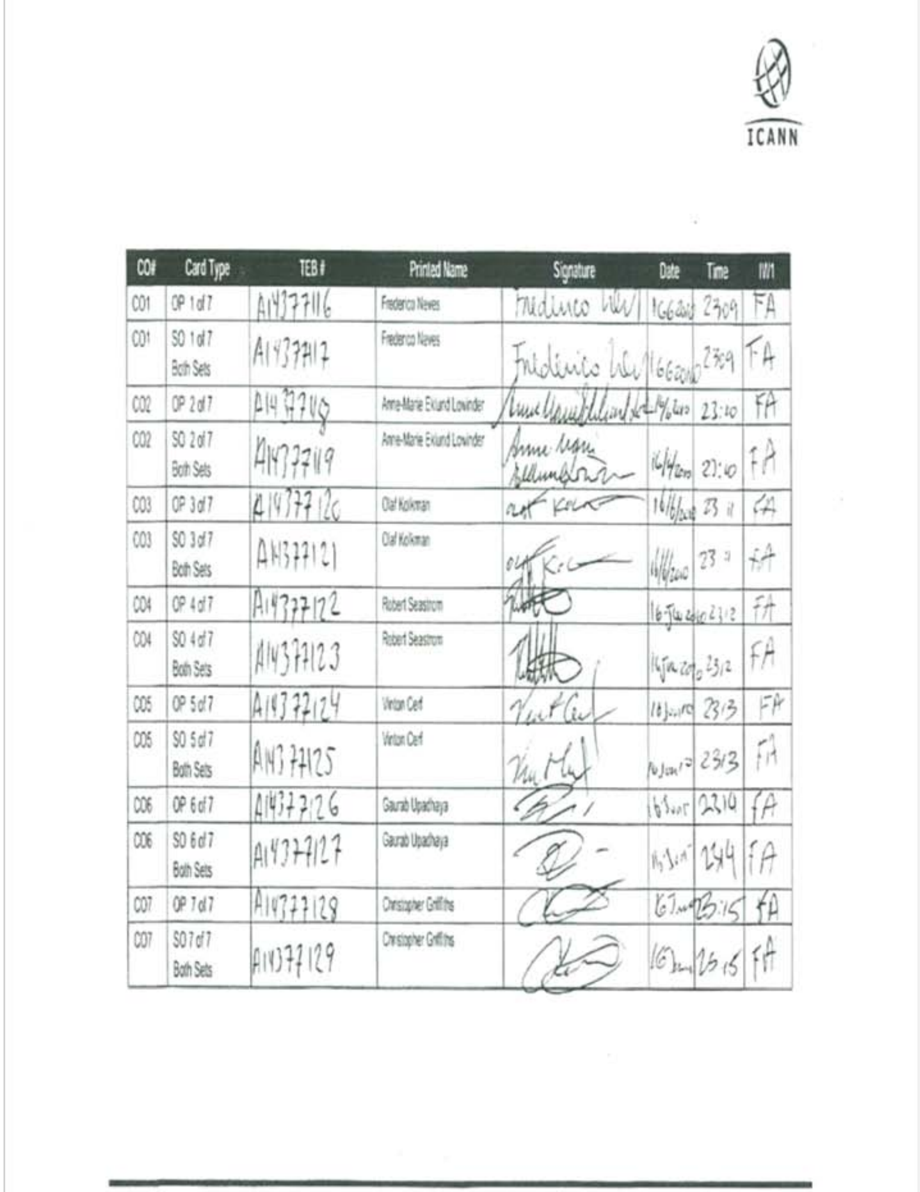
TEB = Tamper Evident Bag
HSM = Hardware Security Module
FD = Flash Drive
CA = Ceremony Administrator
IW = Internal Witness
SA = System Administrator
SSC = Safe Security Controller

Participants

Instructions: At the end of the ceremony, participants print name, citizenship, signature, date, time, and time zone on IW1's copy.

Title	Printed Name/Citizenship	Signature	Date	Time
Sample	Bert Smith	Bert Smith	16 Jun 2010	18:00 UTC
MC	Richard Lamb /US		17 Jun 2010	000Z UTC
CA	Mehmet Akcin /US		17 Jun 2010	00:02 UTC
IW1	Francisco Arias /MX		17 Jun 2010	00:02
IW2	Kim Davies /AU		17 June 2010	0:03
IW3	Craig Schwartz / US		17 June 2010	0:03
SA1	Reed Quinn /US	Reed	17 June 2010	00:012
SA2	Tom Berens /US		17 JUN 2010	0:12
SSC1	Alexander Kulik /US	A Kulik	17 June 2010	0:11
SSC2	Patrick Jones /US		17 June 2010	004
CO1	Frederico Neves /BR	Frederico Neves	17 Jun 2010	00:08
CO2	Ann-Marie Eklund Lowinder /SE	Anne Marie Eklund Lowinder	17 june 2010	00:09
CO3	Olaf Kolkman /NL	OLAF KOLKMAN	17 Jun 2010	00:09
CO4	Robert Seastrom /US		17 JUN 2010	00:10
CO5	Vinton Cerf /US	Vint Cerf	17 June 2010	0:05
CO6	Gaurab Upadhaya /NP		17 Jun 2010	00 06
CO7	Christopher Griffiths /US		17 June 2010	00:06
RKSH1	Moussa Guebre /BF		17 june 2010	00:06
RKSH2	Ondrej Sury /CZ	Ondřej Surý	17.6.2010	00:04
RKSH3	Paul Kane /UK	Paul Kane	17th June 2010	0:04
RKSH4	Jiankang Yao /CN	Jiankang Yao	17 June 2010	0:23
RKSH5	Bevil Wooding /TT		17 Jun 2010	0:04

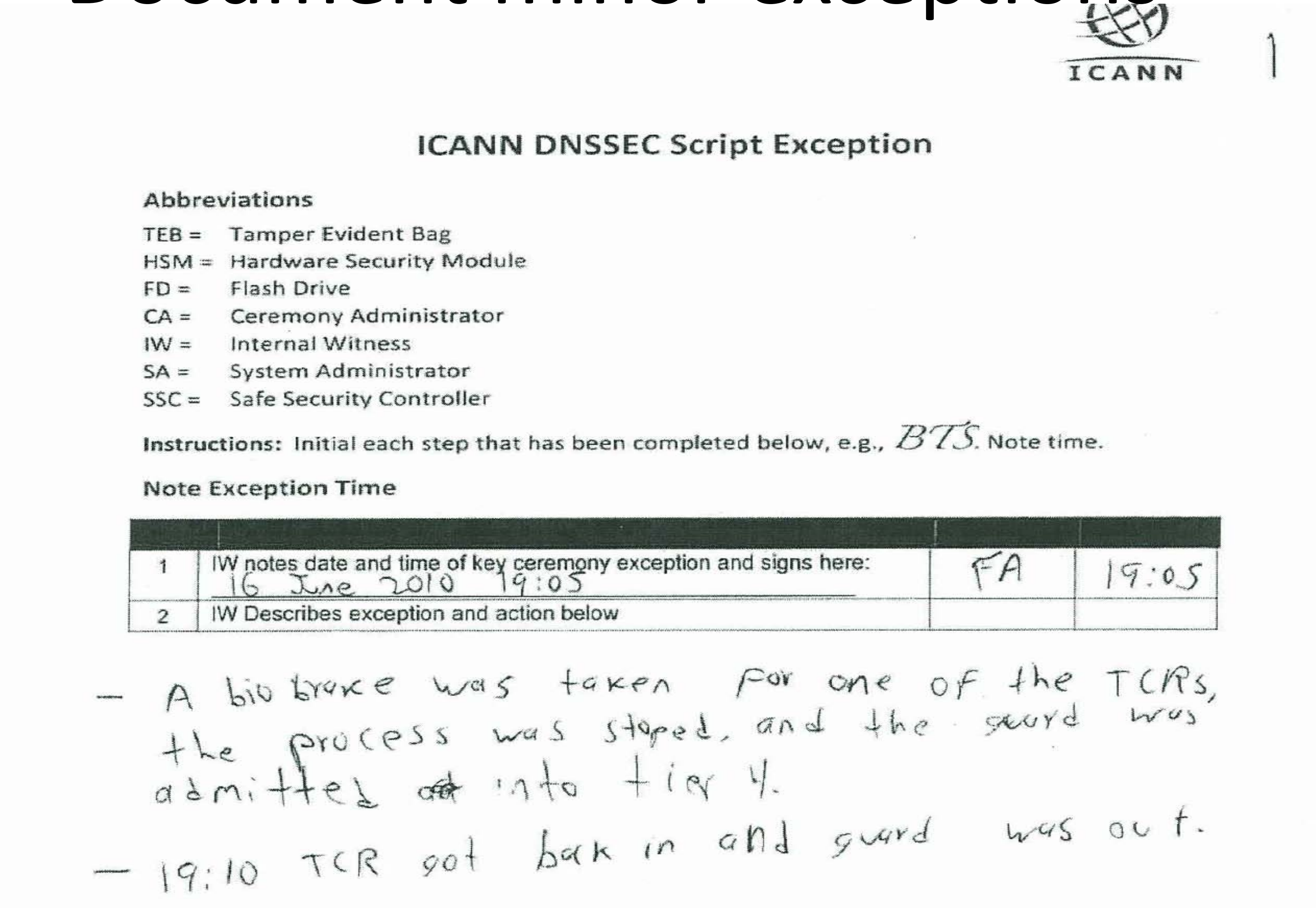
Key Ceremony Scripts (cont)



ICANN

CO#	Card Type	TEB #	Printed Name	Signature	Date	Time	IW1
CO1	OP 1 of 7	A14377116	Frederico Neves	Frederico Neves	16 6 2010	2309	FA
CO1	SO 1 of 7 Both Sets	A14377117	Frederico Neves	Frederico Neves	16 6 2010	2309	FA
CO2	OP 2 of 7	A14377118	Anne-Marie Eklund Lowinder	Anne-Marie Eklund Lowinder	16/6 2010	23:10	FA
CO2	SO 2 of 7 Both Sets	A14377119	Anne-Marie Eklund Lowinder	Anne-Marie Eklund Lowinder	16/6/2010	23:10	FA
CO3	OP 3 of 7	A14377120	Olaf Kolkman	Olaf Kolkman	16/6/2010	23 11	FA
CO3	SO 3 of 7 Both Sets	A14377121	Olaf Kolkman	Olaf Kolkman	16/6/2010	23 11	FA
CO4	OP 4 of 7	A14377122	Robert Seastrom		16-Jun 2010	2312	FA
CO4	SO 4 of 7 Both Sets	A14377123	Robert Seastrom		16 Jun 2010	2312	FA
CO5	OP 5 of 7	A14377124	Vinton Cerf	Vint Cerf	16 June 10	2313	FA
CO5	SO 5 of 7 Both Sets	A14377125	Vinton Cerf		16 June 10	2313	FA
CO6	OP 6 of 7	A14377126	Gaurab Upadhaya		16 June	2314	FA
CO6	SO 6 of 7 Both Sets	A14377127	Gaurab Upadhaya		16 June	2314	FA
CO7	OP 7 of 7	A14377128	Christopher Griffiths		16 June	23:15	FA
CO7	SO 7 of 7 Both Sets	A14377129	Christopher Griffiths		16 June	23:15	FA

No one expects you to be perfect. Document minor exceptions



1

ICANN DNSSEC Script Exception

Abbreviations

TEB =	Tamper Evident Bag
HSM =	Hardware Security Module
FD =	Flash Drive
CA =	Ceremony Administrator
IW =	Internal Witness
SA =	System Administrator
SSC =	Safe Security Controller

Instructions: Initial each step that has been completed below, e.g., *BTS*. Note time.

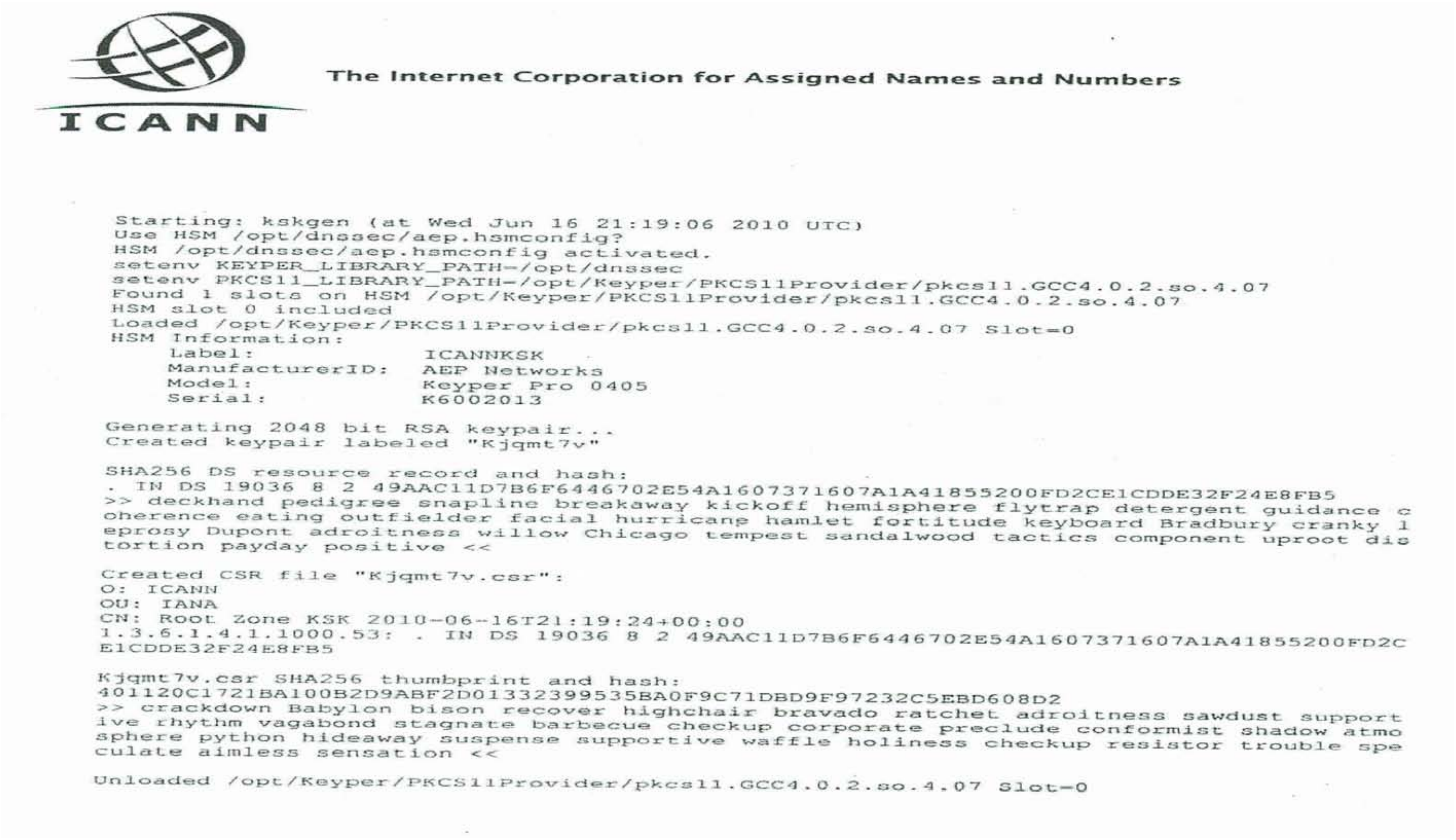
Note Exception Time

1	IW notes date and time of key ceremony exception and signs here: 16 June 2010 19:05	FA	19:05
2	IW Describes exception and action below		

- A bio brake was taken for one of the TCRs, the process was stoped, and the guard was admitted ~~at~~ into tier 4.

- 19:10 TCR got bak in and guard was out.

…for a trusted result



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
```

Key Ceremony Video

- To be inserted here

NOTICE
NOTICE
UNAUTHORIZED PERSONS NOT PERMITTED BEYOND THIS POINT
NOTICE
NO FOOD OR DRINK BEYOND THIS POINT
ICANN
EXIT
One World. One Internet. Everyone Connected.
19036

Deployment

- Communicate Often
- Issues Anticipated Which Affected the Deployment Strategy – DO=1 bit
  - A significant proportion of DNS clients send queries with EDNS0 and DO=1
  - Some (largely un-quantified, but potentially significant) population of such clients are unable to receive large responses
  - Serving signed responses might break those clients

Rollback

- If we sign the root, there will be some early validator deployment
- There is the potential for some clients to break, perhaps badly enough that we need to un-sign the root (e.g., see previous slide)
- Un-signing the root will break the DNS for validators

Deploy Incrementally

- The goal was to leave the client population with some root servers not offering large responses until the impact of those large responses is better understood
- Relies upon resolvers not always choosing a single server

DURZ

- Deploy conservatively
  - It is the root zone, after all
- Prevent a community of validators from forming
  - This allows us to un-sign the root zone during the deployment phase (if we have to) without collateral damage

DURZ

- “Deliberately Unvalidatable Root Zone”
- Sign RRSets with keys that are not published in the zone (but with matching keytag…)
- Publish keys in the zone which are not used, and which additionally contain advice for operators (see next slide)
- Swap in actual signing keys (which enables validation) at the end of the deployment process

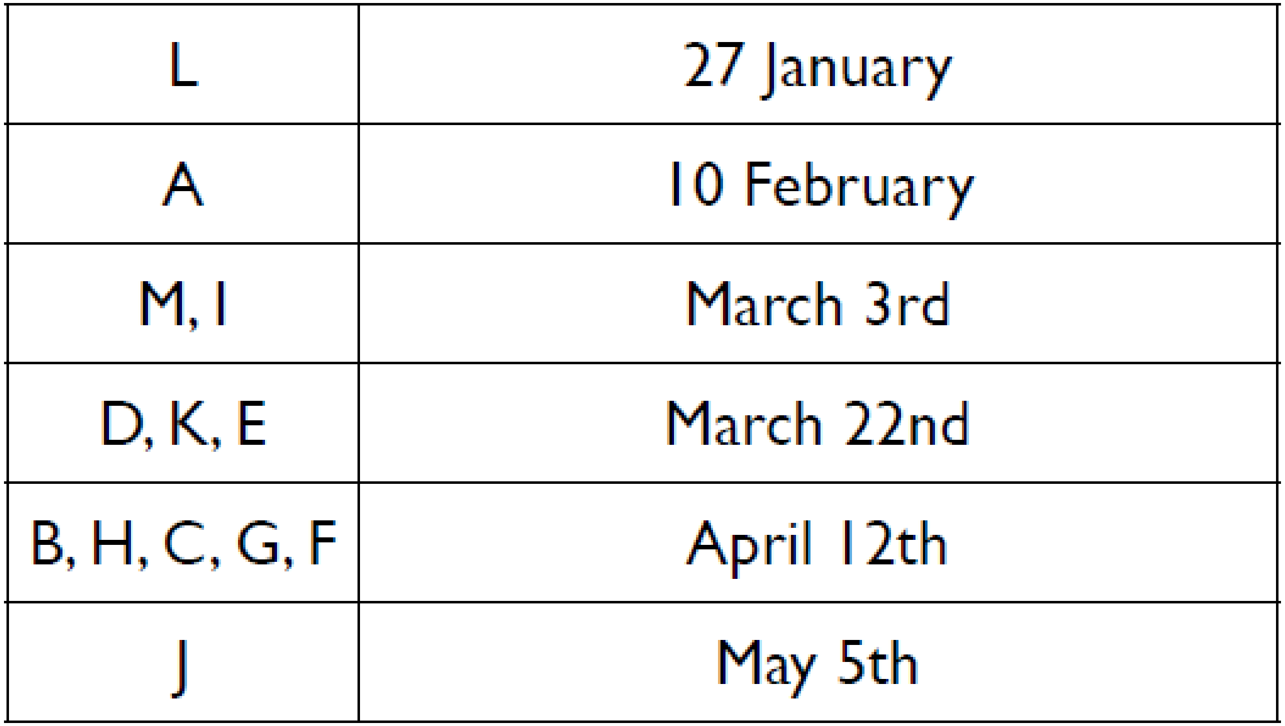
DURZ

```
.  3600 IN DNSKEY 257 3 5 (
   AwEAAa++++++++++++++++++++++++++++++
   ++THIS/KEY/AN/INVALID/KEY/AND/SHOULD
   /NOT/BE/USED/CONTACT/ROOTSIGN/AT/ICA
   NN/DOT/ORG/FOR/MORE/INFORMATION+++++
   ++++++++++++++++++++++++++++++++++++
   ++++++++++++++++++++++++++++++++++++
   ++++++++++++++++++++++++++++++++++++
   ++++++++++++++++++++++++++++++++++++
   ++++++++++++++++++++++++++++++++++++
   ++++++++++++++++++++++/=
   ) ; Key ID = 6477
```

Testing

- A prerequisite for this plan was a captive test of the deployment
    - Test widely-deployed resolvers, with validation enabled and disabled, against the DURZ
    - Test with clients behind broken networks that drop large responses

Deploy Incrementally



L	27 January
A	10 February
M, I	March 3rd
D, K, E	March 22nd
B, H, C, G, F	April 12th
J	May 5th

Measurement

- Full packet captures and subsequent analysis around signing events in addition to long term collection of priming queries
- Dialogue with operator communities to assess real-world impact of changes
- Looking at the data for indications of problems
  - Query rates
  - TCP traffic
  - Message sizes
  - Priming queries

Summary

- No problems evident in the data
- No problems reported by users

Communications

- Project Web Page http://www.root-dnssec.org
  - Status updates
  - Documents
  - Presentation Archive
  - Contact information
- Reaching the technical audiences via mailing lists and other means, such as showing up in person to make presentations
  - IETF DNS lists (e.g. DNSOP)
  - non-IETF DNS lists (e.g. DNS-OARC)
  - General operator lists (e.g. NANOG)

Ceremony Schedule

- Ceremony #1: 16 June 2010, Culpeper, VA
  - Generate KSK and sign Q3 ZSK
- Ceremony #2: 12 July 2010, El Segundo, CA
  - Import KSK into backup site and sign Q4 ZSK
- Ceremony #3: November 1, 2010, Culpeper, VA
  - Sign Q1 2010 ZSK
- Ceremony #4: February 6, 2011, El Segundo, CA
  - Sign Q2 2010 ZSK

Links

- The DPS, trust anchor, scripts, and ceremony recordings available at https://www.iana.org/dnssec/
- Questions & Answers rootsign@icann.org
- Documents at www.root-dnssec.org

Root DNSSEC Design Team

Joe Abley
Mehmet Akcin
David Blacka
David Conrad
Richard Lamb
Matt Larson
Fredrik Ljunggren
Dave Knight
Tomofumi Okubo
Jakob Schlyter
Duane Wessels

..and so many others!!

Lessons Learned

Disclaimer

- Contents are just observations based on experience in and study of current DNSSEC deployments.
- Though expanding quickly, DNSSEC deployment is still in its early stages. Current common practices will evolve.

Who Are You? Who Are Your Stakeholders?

- Who are you?
  - Authoritative Zone Owner
  - Name server operator
  - Registries
  - Registrars
  - Registrants
  - Application Developers
- Who are your customers?
- Who are your users?
- Who are your regulators?
- Who are your contractees?

What Do Your Stakeholders Expect?

- Today
- In the future
- Reliability
- Availability ...and now
- Trust
  - Transparency
  - Security

What are the Risks?

- Identify your risks
  - Reputational
  - Financial
  - Legal
- Build your risk profile
  - Determine your acceptable level of risk

Vulnerabilities give rise to risks

- False expectations
  - Transparency floats all boats here
- Insecure child DS handling
- Zone file compromise
- Signer compromise
- Inability to set correct time
- Insecure parent key handling
  - **KSK compromise**
  - **Undetermined KSK confidentiality**
  - **Un-authorized person accesses ZSK**

Solutions to Satisfy your Stakeholders, Build Trust and Mitigate Risks

- –Building Trust
- –Security
- –Without incurring high cost

Building Trust

- Say what you do
- Do what you say
- External check that you did
- Stakeholder Involvement
  - Incorporate Feedback in updates
  - Participation
- Be Responsible

Building Trust

- Borrow many practices from SSL Certification Authorities (CA)
  - Published Certificate Practices Statements (CPS)
    - VeriSign, GoDaddy, etc..
    - USHER HEBCA, Dartmouth
  - Practices (e.g., key ceremony, scripts, audit, etc…)
  - Also…
  - Facility design (e.g. Access control, building)
  - Crypto

Trust

- DNSSEC Policy/Practices Statement (DPS)
  - Drawn from SSL CA Certificate Policy/Practices Statement
  - Policy: requirements
  - Practice: how you meet them
  - 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)

Trust

- Documented procedures
  - Operations
    - Key ceremony
  - Maintenance
  - Emergency Procedures
    - Pre-defined compromise and/or rollover procedures
- Contingency planning
  - Lost facilities
- Management involvement
- Overall information security policy

Key Ceremony

DNSSEC Key Ceremony: Not some arcane ritual that old men practice at their lodge while drinking beer.   It is a filmed and audited process carefully scripted for maximum transparency at which a cryptographic key is generated or used. In this case the key is the Key Signing Key (KSK) for a protocol called DNSSEC used to secure the DNS.

Key Ceremony Scripts

- Initialization
- Key Generation
- Signing
- Equipment Acceptance
  - Chain of custody
- Maintenance
- Exceptions

Audit Material

- Scripts
- Access Control System logs
- Facility, Room, Safe logs
- Video
- Annual Inventory
- Other Compensating Controls

Trust

- Audit - Check that they match
  - Internal
  - External
  - SysTrust / WebTrust
  - ISO 27000 etc..
  - NIST 800-53 etc…

Security

- Physical
- Logical
- Crypto

Physical

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

Environmental

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

Tiers

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

Tier Construction

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

Access Control

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

Intrusion Detection

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

Disaster Recovery

- Multiple sites
  - Mirror
  - Backup

Logical

- Base on risk profile
- Authentication (passwords, PINs)
- Multi-Party controls

Authentication

- Procedural:
  - REAL passwords (e.g., 8 characters and mixed)
  - Forced regular updates
  - Out-of-band
- Hardware:
  - Two-factor authentication
  - Smart cards (cryptographic)

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

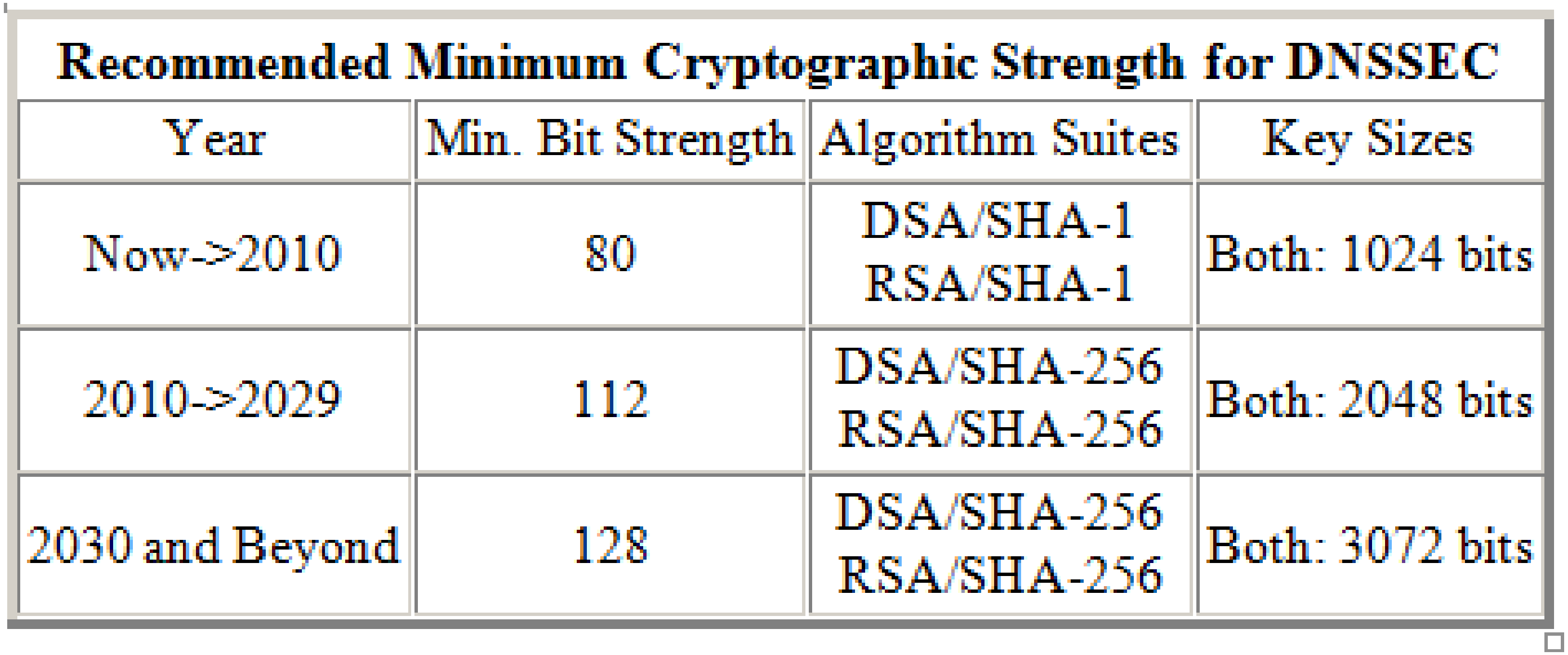
- RFC4641bis is a great source
- Algorithms / Key Length
- Key Splitting
- Effectivity (rollover) Period
- Number and Scheduling of keys
- Validity Period
- Crypto Hardware

Algorithms / Key Length

- Factors in selection
  - Cryptanalysis
  - Regulations
  - Network limitations

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

Algorithms / Key Length

- 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
    - 1024 bit RSA typical for ZSK
  - Elliptical is ideal – but not available yet

Algorithms / Key Length

- 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).

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

Effectivity - KSK

- 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

Effectivity – KSK (cont)

- If KSK is a Trust Anchor, then 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.

Effectivity - ZSK

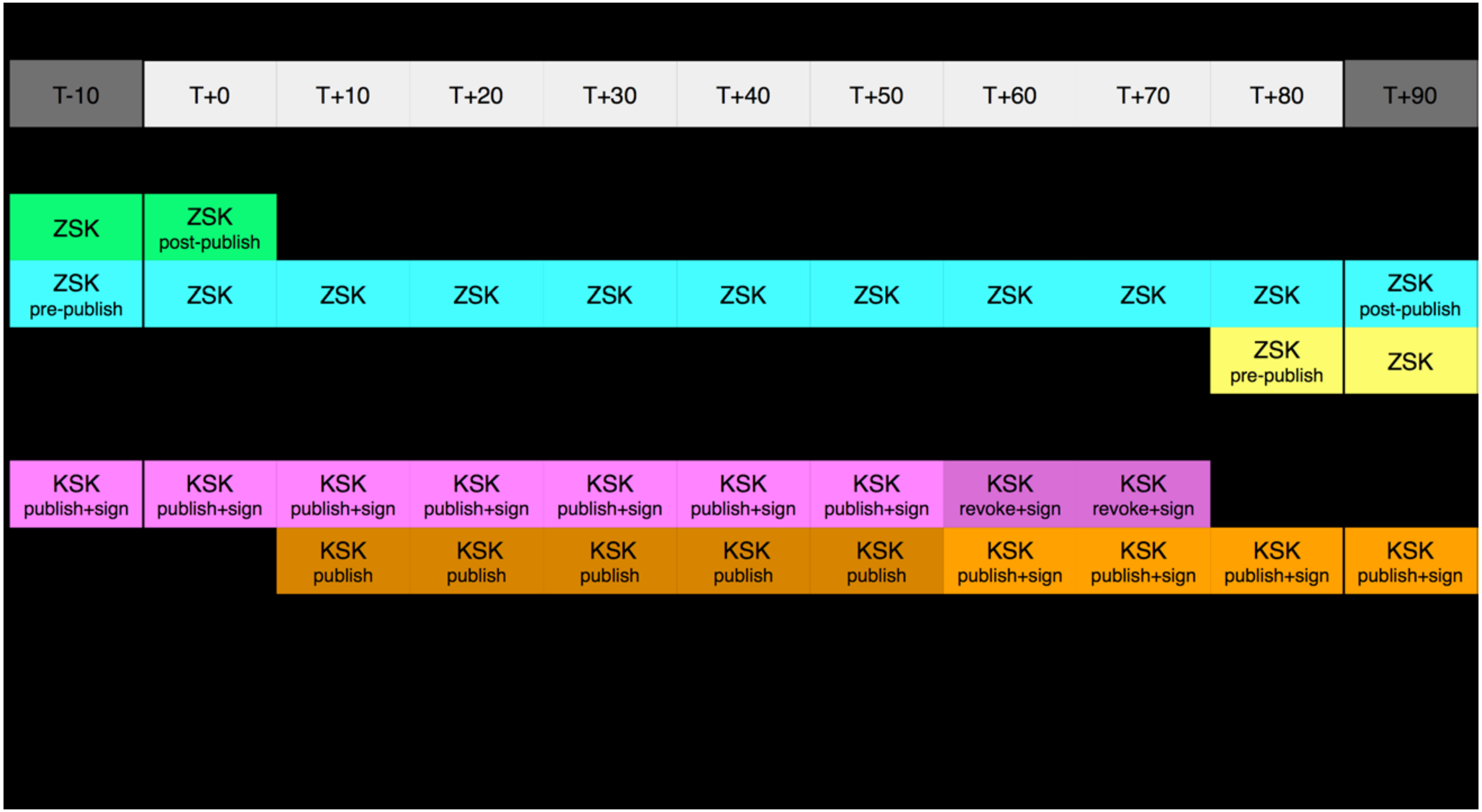
- ZSK more frequently accessed: operational considerations
- ZSK compromise less severe since under zone owner control but rollover should happen soon.
- If online, exposed to various threats: RFC4641bis suggests one month

Number and Schedule of Keys

- 1, 2, or 3 published (DNSKEY) keys for KSK and/or ZSK
  - UDP fragmentation on DNSKEY RRset + RRSIGs
  - CPE study, DO=1 but heard no problems from root
- DNSKEY RRset does not need to be signed by ZSK
- Pre-publish (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)



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

Validity Period

- Short to minimize replay attack - quickly recover from compromise
- Long to limit operational risks from equipment failure
- Max validity period < how long wiling to tolerate replay attack
- Min validity period > operational failure recovery time.
  - Min validity period ~ time to fix failure + how often we refresh sigs
- Validity jitter < signature refresh
- Validity periods overlap to deal with clock skew - increase validity period
- Other Guidelines
  - Max TTL < validity period/N where N > 2
  - SOA Min TTL > 10 min
  - SOA expiration > validity period/M where M = 3-4

Crypto Hardware

- FIPS 140-2 Level 3
  - AthenaSC IDProtect ~$35 + Reader ~$8-$20
  - Aladdin USB e-Token ~$50
  - Sun SCA6000 ~$1000
- FIPS 140-2 Level 4
  - AEP Keyper ~$15000
- Recognized by your national certification authority
  - Kryptus (Brazil) ~ $2500-$25000
- Satisfy for 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
- AT LEAST USE A GOOD RNG! *(rngtest)*
- Remember you must have a way to backup keys!

Crypto Hardware (cont)

- Two-Factor
  - Vasco “footballs” ~$5
  - NagraID cards ~$30
- Smartcards (PKI)
  - Oberthur ~$5-$15
  - AthenaSC ~$35
- Can authenticate with existing cooperative ID efforts (e.g. VeriSign ID protect) or PKIs

DNSSEC Parameters in the Wild

	KSK	ZSK	Apex DNSKEY RRSIG (KSK) Validity Period/TTL	RRSIG (ZSK) Validity Period	Apex NS /G TTL	NS/ glue/ DS TTL	SOA
root	2048 2-5yrs	1024 3Mo (10D)	15D 1D	7-10D	6D 42D	NS/G=2D DS=2D	.5H .25H 7D 1D
br	1280 2-5yrs	1152 1-3Mo	21D 6H	2Mo 7D (DS)	2D	NS/G=2D DS = 1D	.5H .25H 7D .25H
se	2048 as needed	1024 28th D	6-8D 1H	6-8D	2D	NS/G = 1D DS = 1H	.5H .5H 28D 2H
cz	2048 2yrs	1024 3Mo	13D 1H	12-14D	5H	NS/G=5H DS = 5H	.25H 5m 7D .25H
uk	2048 ~5yrs	1024 -	14D 2D	14D	2D	--	2H .25H 28D 2D
org	2048 5yrs	1024 1Mo	14D .25H	14D	1D	NS/G=1D DS=1D	.5H .25H 7D 1D
gov	2048 >1yr	2048 1Mo ?	5D 1D	5D	3D	NS/G=1D DS=1D	1H .25H 21D 1D
edu	2048 >1yr	1024 3Mo	7D 1D	7D	2D	NS/G=2D DS=1D	.5H .25H 7D 1D
kirei.se	2048 4yrs	1024 3Mo	10D 1H	10D	1D 4H		4H 1H 7D 4H

DNSSEC Practices in the Wild

	Published DPS	Audit	KSK	Access Control	Multi-party (minimum)
root	Yes	External (SysTrust)	H/W FIPS 140-2 Level 4	Physical only	3 of 7 community (external) + 5 internal
br	No – Presentations		H/W ASI National Certification	Physical and Logical	4 of 12 internal
se	Yes	External	H/W FIPS 140-2 Level 3	Physical and Logical	1 logical + 1 physical internal
cz	No – Operation Manual		S/W HSM planned	Physical and Logical	Two internal parties
uk	Planning	External	H/W FIPS 140-2 Level 3	Physical and Logical	1 logical + 1 physical internal
org	No – Partial		FIPS 140-2 Level 2		
gov	Planning Contractual (FISMA HIGH)	External	H/W FIPS 140-2 Level 3	Physical and Logical	
edu	Yes	External (SysTrust)	H/W FIPS 140-2 Level 3	Physical	3 of 10? Internal
kirei.se	No	None	S/W	Physical	No

A word about 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.

Cost

- People
  - Swedebank – half a FTE
  - Occasional shared duties for others
- Facilities
  - Datacenter space
  - Safe ~ $500 - $14000
- Crypto Equip ~ $35-$20000
- Bandwidth ~ 4 x

Future Impact

Update

- Signed root published 15 July, 2010
- 51 TLDs: asia. be. bg. biz. br. bz. cat. ch. cz. dk. edu. eu. fi. fr. gi. gov. hn. in. info. lc. li. lk. mn. museum. na. nl. nu. org. pm. pr. pt. re. sc. se. tf. th. tm. uk. us. yt. Plus 11 IDN test zones already in root…more coming
- 8 out of 16 gTLD registries are signed or in the process to be signed. (e.g. .net 2010, .com 2011)
- Biggest change to Internet in 20+ years
- Security applications built on DNSSEC
  - You will have a larger role/opportunity to help secure the Internet.
  - Self Signed SSL certs, S/MIME, SSH

From Black Hat 2010 (Jeff Moss)

- Security has been discussed and debated throughout Black Hat's 13-year history, yet what progress have we made? What real successes can we celebrate? The growth in malicious traffic on the web is higher than the growth in legitimate traffic. The Internet security community, he said, has had no solid accomplishment to show for our efforts – until today. Today DNSSEC is being launched, and just days ago the root of the Internet was cryptographically signed. This is the first major Internet security enhancement since the beginning of Black Hat, and we thank ICANN for this accomplishment.

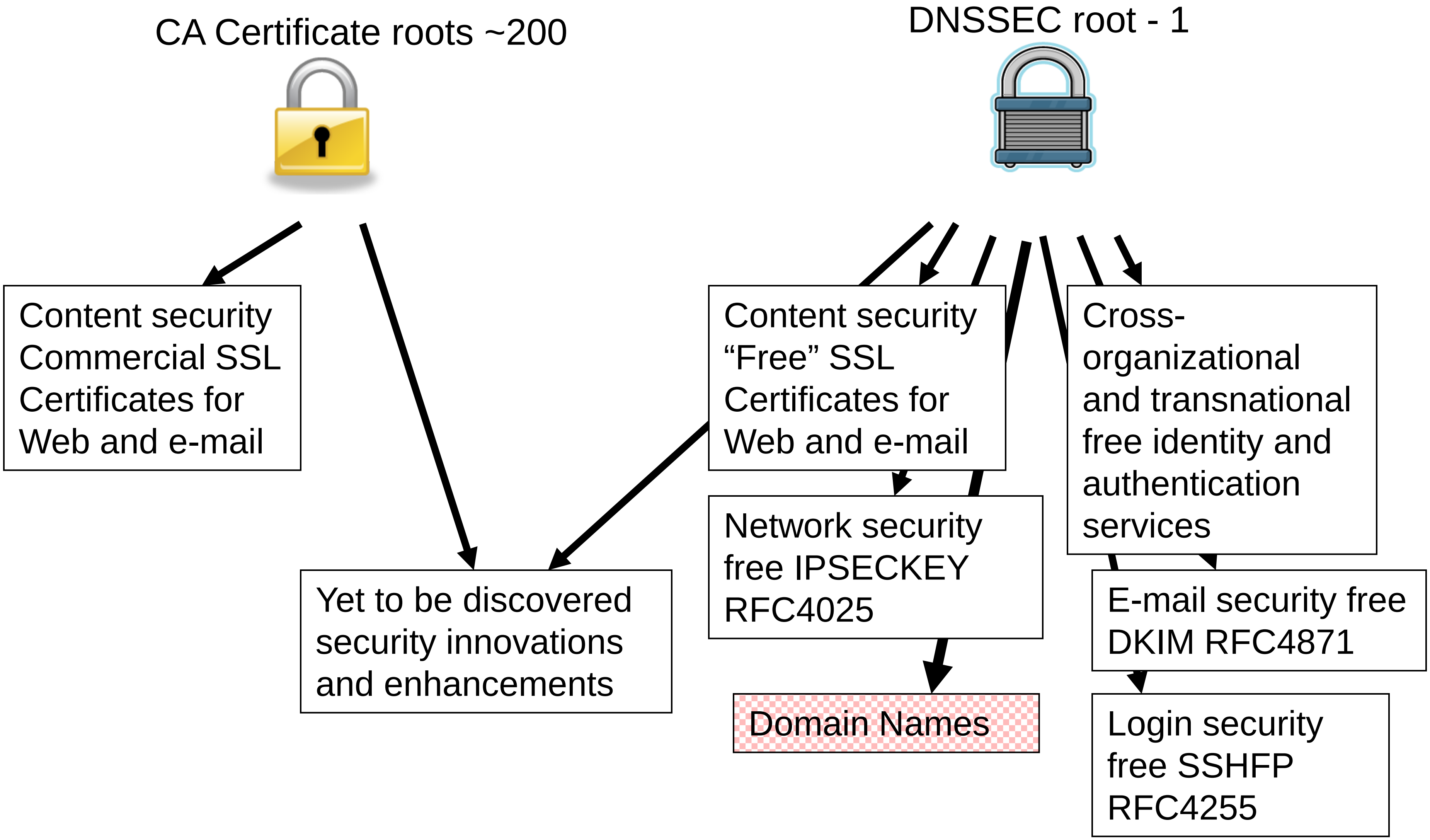
From Black Hat 2010 (Dan Kaminsky)

- For the last *eighteen years,* people have been trying to secure the DNS.
- *Now it's our turn to secure everything else!*

http://tinyurl.com/296mcsn

DNS Operators are now part of a chain of trust shared by administrators of each zone

Opportunity



CA Certificate roots ~200

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

Network security free IPSECKEY RFC4025

Domain Names

Cross-organizational and transnational free identity and authentication services

E-mail security free DKIM RFC4871

Login security free SSHFP RFC4255

Example

Example

- Keys
  - Length Type, Algorithm
    - KSK 2048 RSA
    - ZSK 1024 RSA
    - RSA SHA256
  - Rollover
    - KSK 2 years (not TA)
    - ZSK 3 months (how often willing to manually intervene)
  - Signature Validity Period
    - 7 days (compromise recovery / operational risk)
  - Number
    - 1 KSK, 1 ZSK (minimize effects of UDP fragmentation)
  - Scheduling
    - Double signature for KSK rollover (simplify parental roll)
    - Pre-publish for ZSK rollover

Example

- Misc
  - NSEC
  - Default TTL = 2 days
  - Use BIND dynamic update
  - Zone signer and zone on same machine
  - Machine firewalled - off-net
  - Software drawn from defined SDLC (e.g. BIND tools, PKCS11 utilities)

Example

- Key management
  - Online ZSK (scalable dynamic signing S/W)
  - Offline KSK on smartcard
    - Split PIN
  - Backup KSK also on another smartcard
  - KSK generation equipment destroyed after generation of KSKs at a key ceremony
  - 2 geographically dispersed backup sites with duplicate equipment
  - Backup KSK kept in tamper evident bag inside bank safe deposit box
  - Multi-Person control
    - KSK and backups in safes controlled by Safe Controller
    - Physical access controlled by System Administrator
    - PIN controlled by Crypto Officers – may involve 3rd party to imbue trust

Example

- Key Management (cont)
  - Pre-generate KSK signed DNSKEY RRsets for ZSK rollovers
  - Scripted and Filmed Key Ceremonies every 3 months
  - Audit material duplicated and protected (includes above script and film, access logs, as well as any log files from ZSK signer)
  - Periodically reviewed internally and updates applied
  - Audited by 3rd party

Example

- Facilities
  - Commercial data center with 24hr guard and video monitoring
    - Power, water, air conditioning etc..
    - Must be able to get footage from prior periods
    - Must be able to get copy of facility and cage access logs
  - 2 sites operated by different companies
  - Facility does not have access to rack within cage
    - Log sheet in rack
  - smartcards/laptop/backup in Safe within rack
    - Log sheet in safe
  - Access to facility by System Administrator
  - Access to safe by Safe Controller
  - PIN/Passwords split between two or more other Crypto Officers
  - Off-net zone, ZSK Signer, Hidden Master in separate cage and rack
    - Signed DNSKEY RRsets transported via USB

Review of DPS

- Create a DPS using the .SE DPS and RFC draft framework as a guide
    - http://www.iis.se/docs/se-dnssec-dps-eng.pdf

- Publish on Webpage
- To publicize seek some sort of certification (industry group) and/or audit opinion and/or involve key individuals in Key Ceremonies.

Review of Scripts

- Equipment Acceptance Script
  - http://tinyurl.com/38raqn5
- Key Ceremony Script

  http://data.iana.org/ksk-ceremony/1/ceremony1-script-annotated.pdf
- Safe Log Sheet Examples
  - http://tinyurl.com/35zxfuv
  - http://tinyurl.com/33oge37

Other Documentation

- Document detailed procedures (e.g. scripts, operations, disaster recovery, etc) elsewhere.

- Compromise and disaster recovery
  - Incident Management
  - Compromise of private key recovery
  - Contingency (move operations to backup)
  - Termination

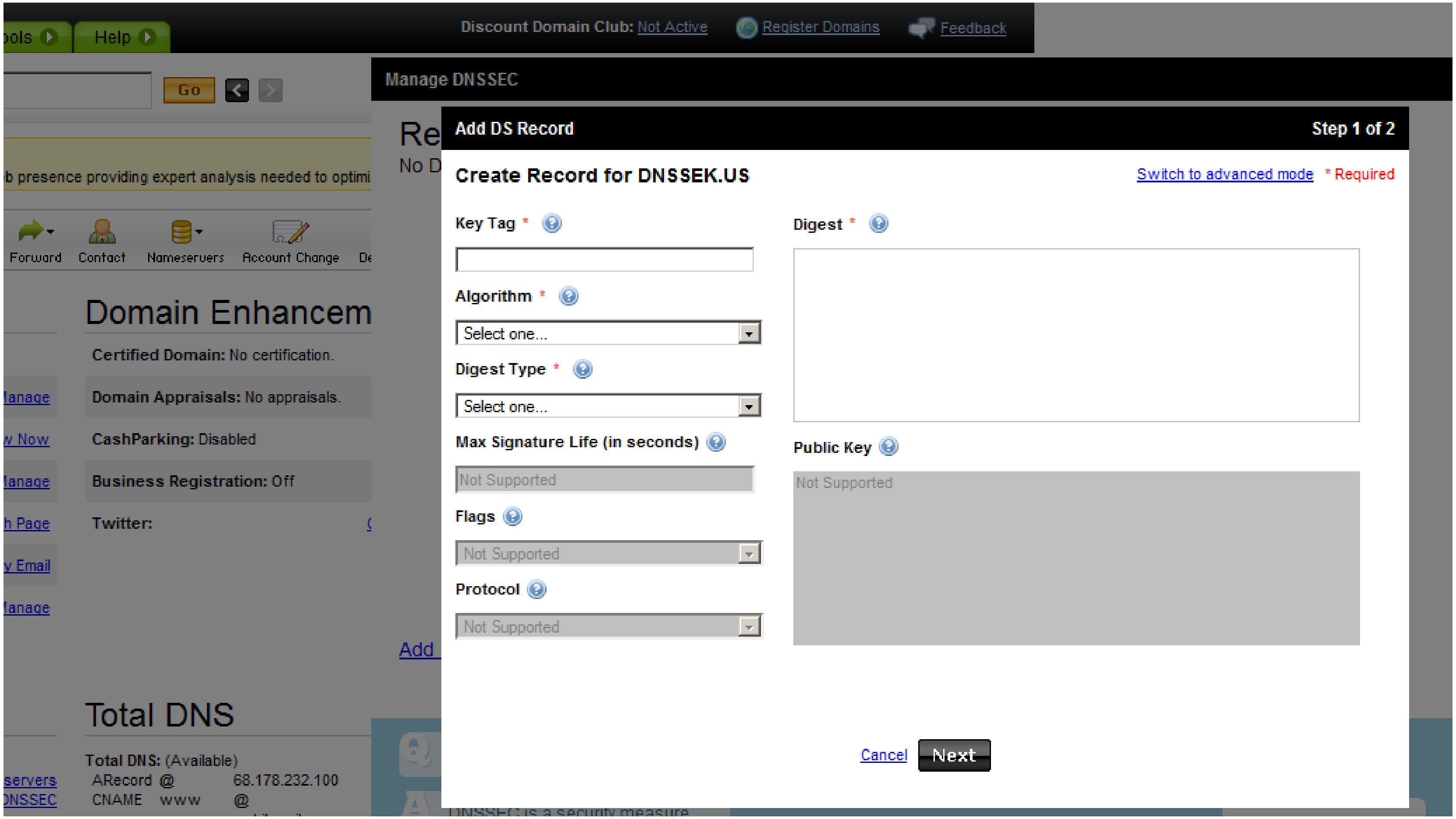
Link to Management

- Create Policy Management Authority
  - Sample http://tinyurl.com/32nnrrt
- Call PMA meeting to get formal signoff from management

DS record handling / Customer Interface

- Accept any child algorithm
- But limit DS digest to SHA1 and SHA256 so that we may calculate
- State removal conditions in DPS
- User interface requiring two-factor authentication or at least secure password requirements
- Out of band verification of initial exchange
- Proof of possession of the private key corresponding to DNSKEY (maybe to differentiate services)

Registrar DS instructions and interface example



b presence providing expert analysis needed to optimi

Domain Enhancem

Certified Domain: No certification.

Domain Appraisals: No appraisals.

CashParking: Disabled

Business Registration: Off

Twitter:

Total DNS

Total DNS: (Available)

ARecord @ 68.178.232.100

CNAME www @

Add DS Record — Step 1 of 2

Create Record for DNSSEK.US

Switch to advanced mode * Required

Key Tag *

Algorithm *: Select one...

Digest Type *: Select one...

Max Signature Life (in seconds): Not Supported

Flags: Not Supported

Protocol: Not Supported

Digest *

Public Key: Not Supported

DNSSEC is a security measure

- http://community.godaddy.com/help/article/6114/
- http://community.godaddy.com/help/article/6115

Summary

- DNSSEC deployment at the TLD level is moving much faster than expected.
- Developers are enthusiastically reconsidering DNSSEC as a global source of authentication. Expect and be a part of the innovation.
- With this DNS Operators are now part of a chain of trust …and part of solutions to Internet security
- As part of the chain, build trust with improved processes, practices and education to differentiate offerings and develop new revenue streams
- Doesn’t have to be expensive, just institutionalized

References

- http://tools.ietf.org/id/draft-ietf-dnsop-rfc4641bis-04.txt
- http://point-at-infinity.org/ssss/
- http://www.iis.se/docs/se-dnssec-dps-eng.pdf
- http://www.pptsearch.net/details-backup-hsm-keys-scott-rea-25010.html
- http://usher.internet2.edu/practices/ca1/cps.pdf
- http://www.internetdagarna.se/arkiv/2008/www.internetdagarna.se/images/stories/doc/22_Kjell_Rydger_DNSSEC_from_a_bank_perspective_2008-10-20.pdf
- http://tools.ietf.org/html/draft-ietf-dnsop-dnssec-dps-framework-02
- http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf
- http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf Appendix F
- http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm
- http://www.root-dnssec.org/documentation/
- http://www.iana.org/procedures/root-dnssec-records.html
- http://nsrc.org/tutorials/2009/apricot/dnssec/
- http://lacnic.net/documentos/lacnicxiii/presentaciones/tutorial-DNSSEC-en-32.pdf
- http://www.dnssec.cz/files/nic/doc/Provozni_manual_DNSSEC_201001_final_angl.pdf
- http://www.isc.org/software/bind/new-features/9.7
- http://data.iana.org/ksk-ceremony/1/ceremony1-script-annotated.pdf
- https://www.iana.org/dnssec/icann-dps.txt

Questions Welcome