DNSSEC Tutorial

APNIC 30
Gold Coast, Australia
24 August 2010
richard.lamb@icann.org

DNSSEC basics

- Assume DNS knowledge

- Can sign a zone with standard tools

Disclaimer

- Tutorial 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.

Update

- Signed root published 15 July, 2010
- .bg .biz .br .cat .cz .dk .edu .lk .museum .na .org .tm .uk .us already in root.
- …more coming (.se .ch .gov .li .my .nu .pr .th)
- 8 out of 16 gTLD registries are signed or in the process to be signed. (e.g. .com 2011)
- Biggest change to Internet in 20+ years
- Security applications built on DNSSEC
  - You will have a greater role in helping secure the Internet. You are now all purveyors of trust on the ‘net

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.

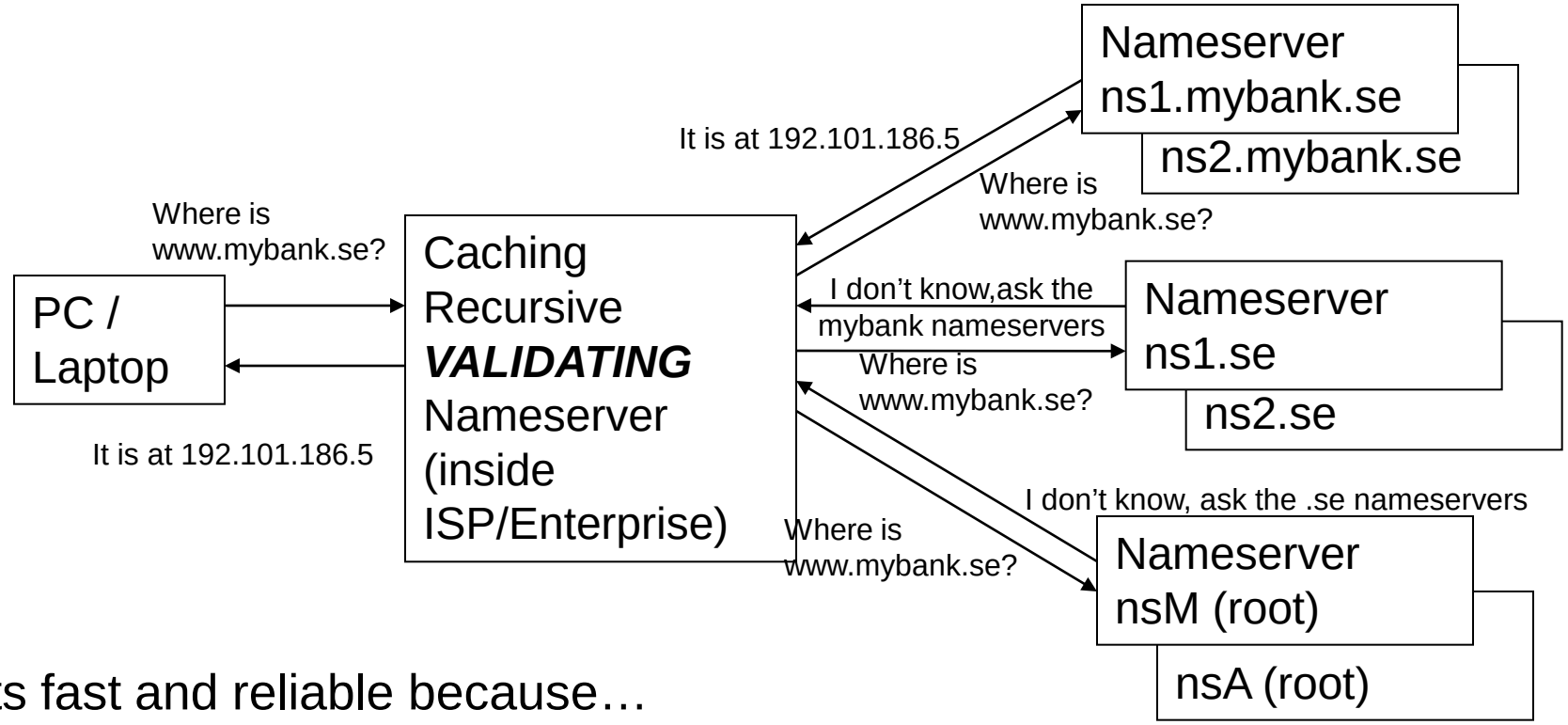
From Black Hat 2010 (Dan Kaminsky)

- 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

DNSSEC Overview



- Its fast and reliable because…
- It remembers…
- …and this is also the vulnerability
- but DNSSEC fixes this
- ...and creates an infrastructure for new Internet security solutions.

Drawbacks

- Absolute time now matters.
- May cause entire sub-domains to become invisible (marked “Bogus”).
- Requires more resources
- But… many new opportunities!

A Chain of Trust

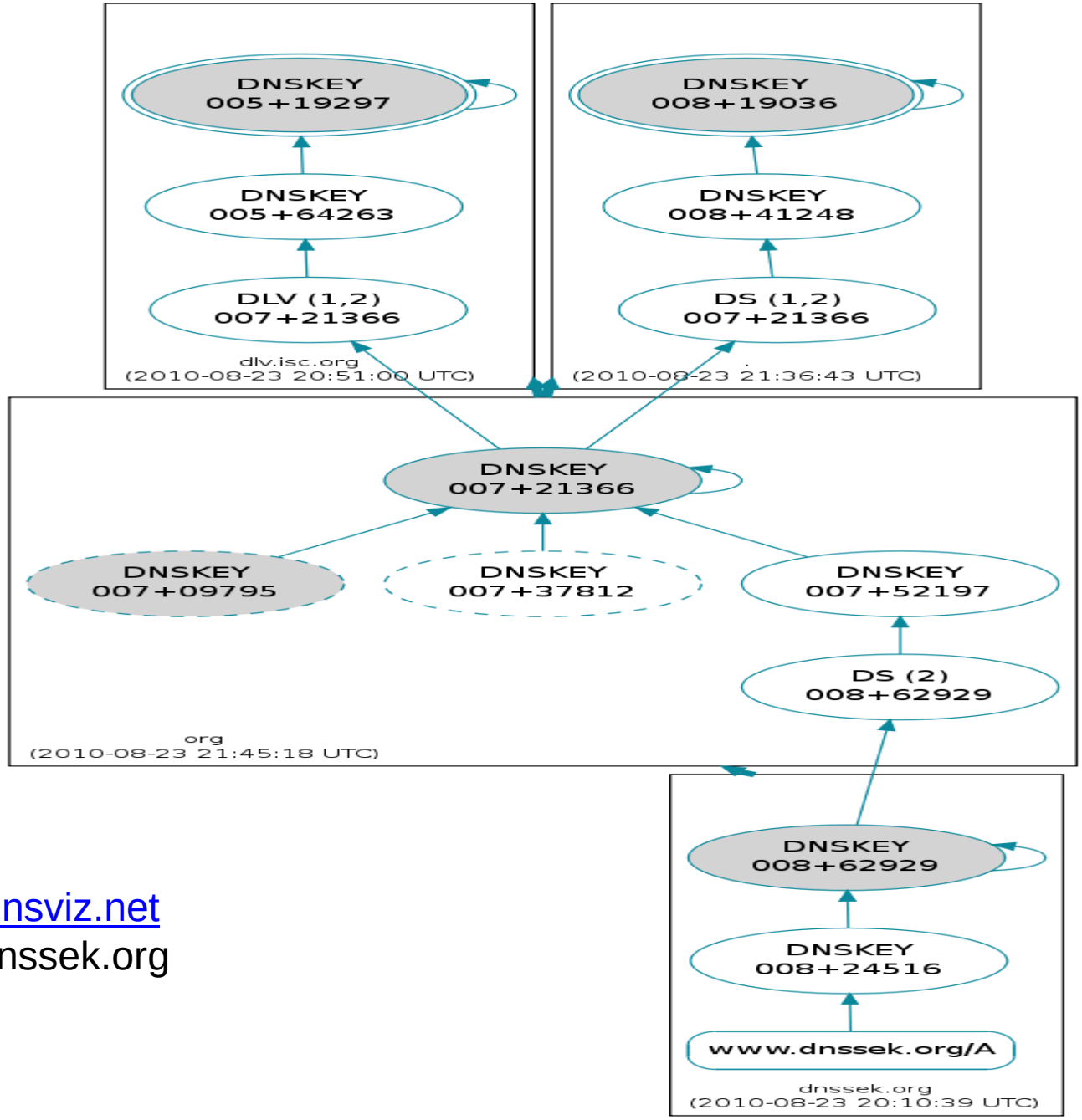
Example: Resource Record = www.mybank.se A 192.101.186.5
Legend: Resource Record ***key used to sign the record***

mybank.se – Registrant or DNS Hosting Registrar
www mybank.se-a ***mybank.se-dnskey-zsk***
mybank.se-dnskey-zsk ***mybank.se-dnskey-ksk***
mybank.se-ds = hash(mybank.se-dnskey-ksk) (child)

se - Registry
mybank.se-ds ***se-dnskey-zsk*** (parent)
se-dnskey-zsk ***se-dnskey-ksk***
se-ds = hash(se-dnskey-ksk) (child)

root
se-ds ***root-dnskey-zsk*** (parent)
root-dnskey-zsk ***root-dnskey-ksk***

resolver – ISP, Enterprise, etc
root-ds = hash(root-dnskey-ksk)



http://dnsviz.net

www.dnssek.org

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

- 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)

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
- 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	1024-1152 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	Planning	External (SysTrust)	H/W FIPS 140-2 Level 3	Physical	3 of 10? Internal
kirei.se	No	None	S/W	Physical	No

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

Tools and Software

- BIND
  - BIND 9.7.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.
- Tools
  - http://dnsviz.net
  - http://dnssec-debugger.verisignlabs.com
  - http://www.dnssec.org.mx/checkdnssec.html
  - http://yazvs.verisignlabs.com/
  - rngtest

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

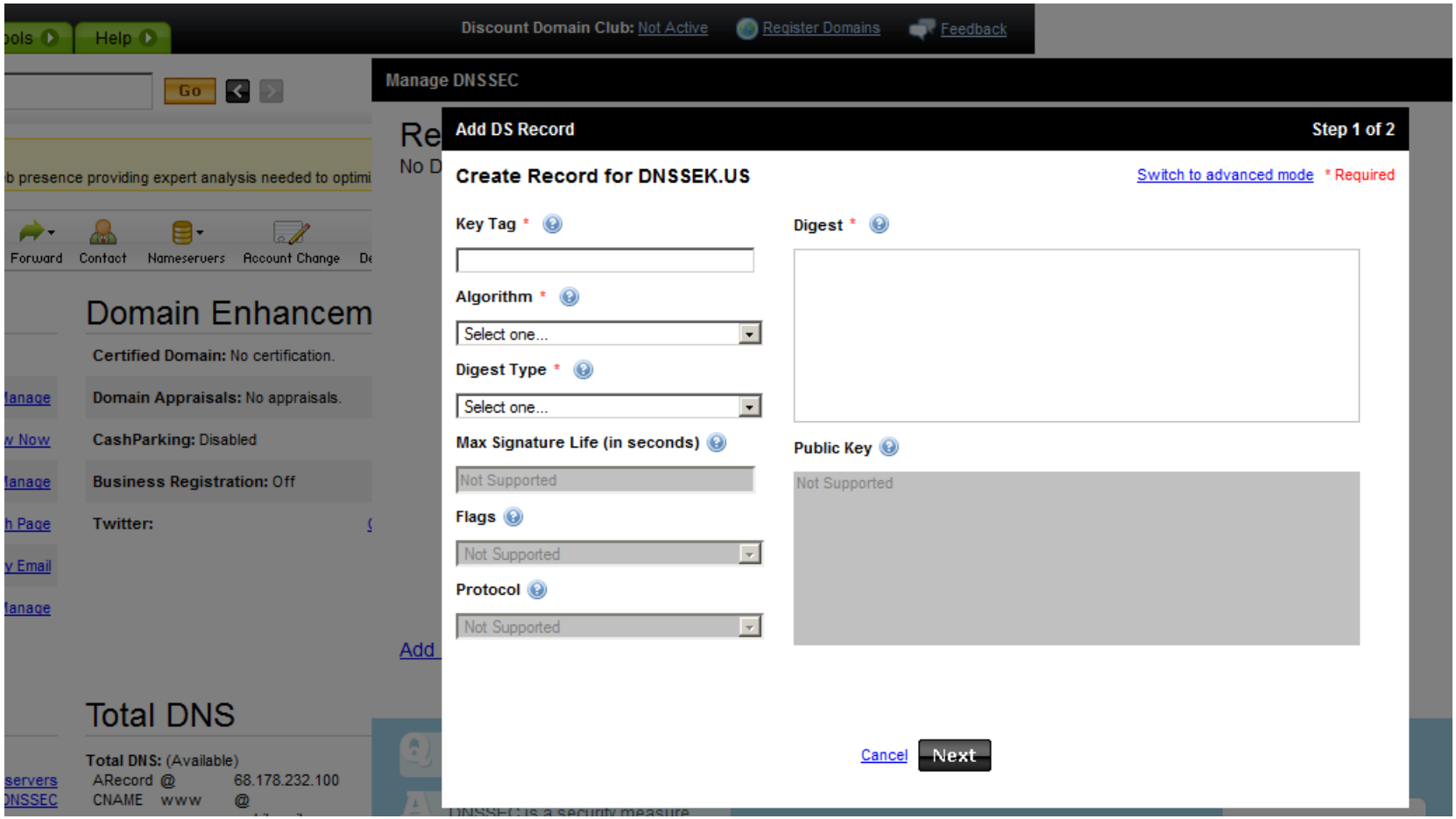
Link to Management

- 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



- 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