DNSSEC Update
27 Aug 2010 Tokyo, Japan

DNSSEC 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

Signed Root - Quick Recap

- Design is the result of a cooperation between ICANN & VeriSign with support from the U.S. Department of Commerce/NTIA
- 2048-bit RSA Key Signing Key (KSK), 1024-bit RSA Zone Signing Key (ZSK)
- Signatures with RSA/SHA-256 hash
- Split ZSK/KSK operations
- Incremental deployment
- Deliberately Unvalidatable Root Zone (DURZ)

Signed Root

- Full production on July 15, 2010
  - Already had DURZ at every root server
  - Keys became un-obscured
  - No problems reported
- Delegation Signer (DS) Record Change Requests
  - DS record requests being accepted by ICANN/IANA now
  - TLD change template now includes DS Records

Trusted Community Representatives (TCRs)

- Crypto Officers (CO)
- Recovery Key Shareholders (RKSH)
- Not from an organization affiliated with the root zone management process
  - ICANN, VeriSign or the U.S. Department of Commerce

Crypto Officers (COs)

Mehmet Akcin, ICANN and Masato Minda, JPRS. Photo by Kim Davies

Crypto Officers (COs)

- Have physical keys to safe deposit boxes holding smartcards that activate the Hardware Security Module (HSM)
- ICANN cannot generate new key or sign ZSK without 3-of-7 COs
- Have to travel up to 4 times a year to US
- Can’t lose the (physical) key

Recovery Key Share Holders (RKSHs)

- 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, but hopefully never
- Annual inventory

Crypto Officers (COs)

U.S. East:

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

U.S. West:

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

Backup COs

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

Recovery Key Shareholders (RKSHs)

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

Backup RKSHs

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

Key Ceremonies

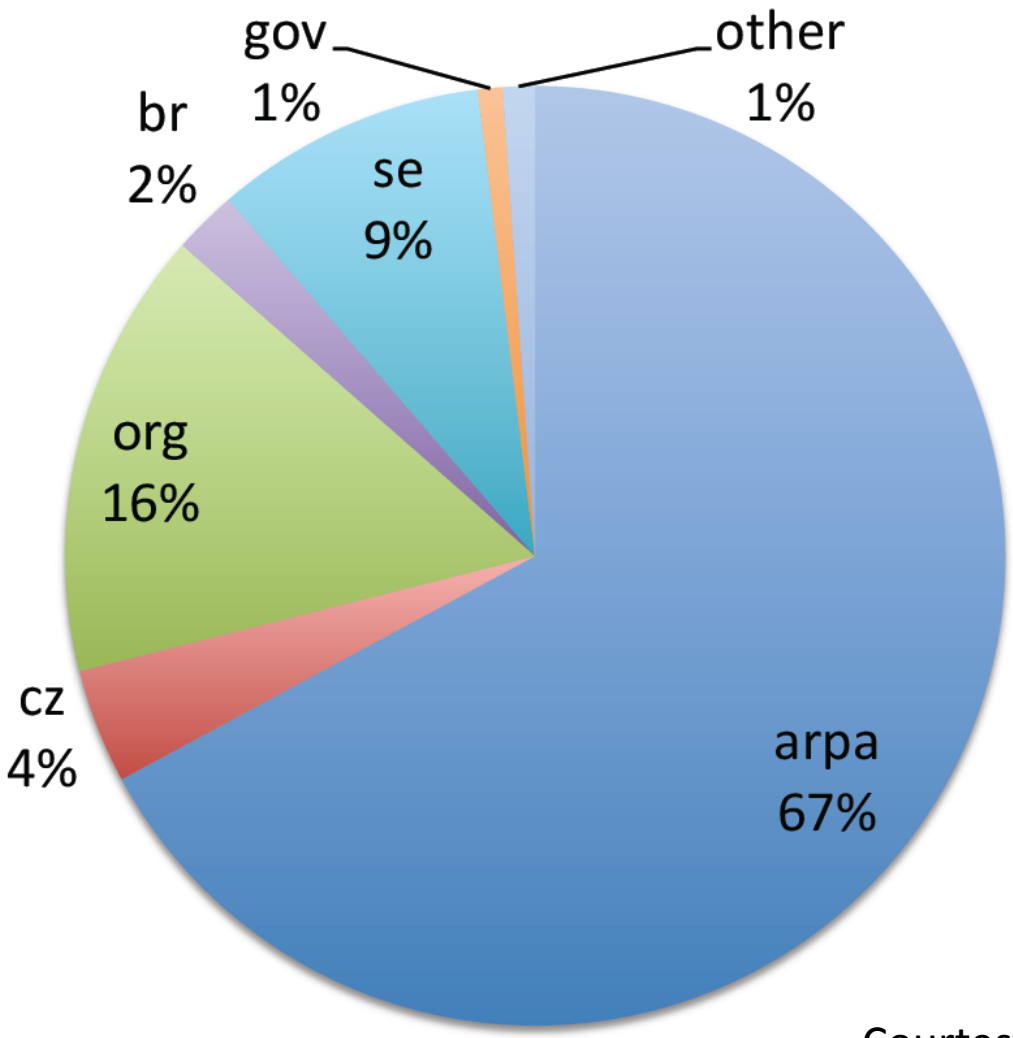
- Ceremony #1: June 16, 2010, Culpeper, VA
  - KSK created, Q3 root DNSKEY RRsets signed
  - Recovery Key Shareholders and East Coast Crypto Officers enrolled
- Ceremony #2: July 12, 2010, Los Angeles, CA
  - KSK installed, Q4 root DNSKEY RRsets signed
  - West Coast Crypto Officers enrolled

THANK YOU!!

Photos by Kim Davies

Key Ceremony Video

TLDs of DS Queries



(Based on data from
2010-07-14
through
2010-07-19)

Courtesy of Duane Wessels

Documentation

Available at www.root-dnssec.org

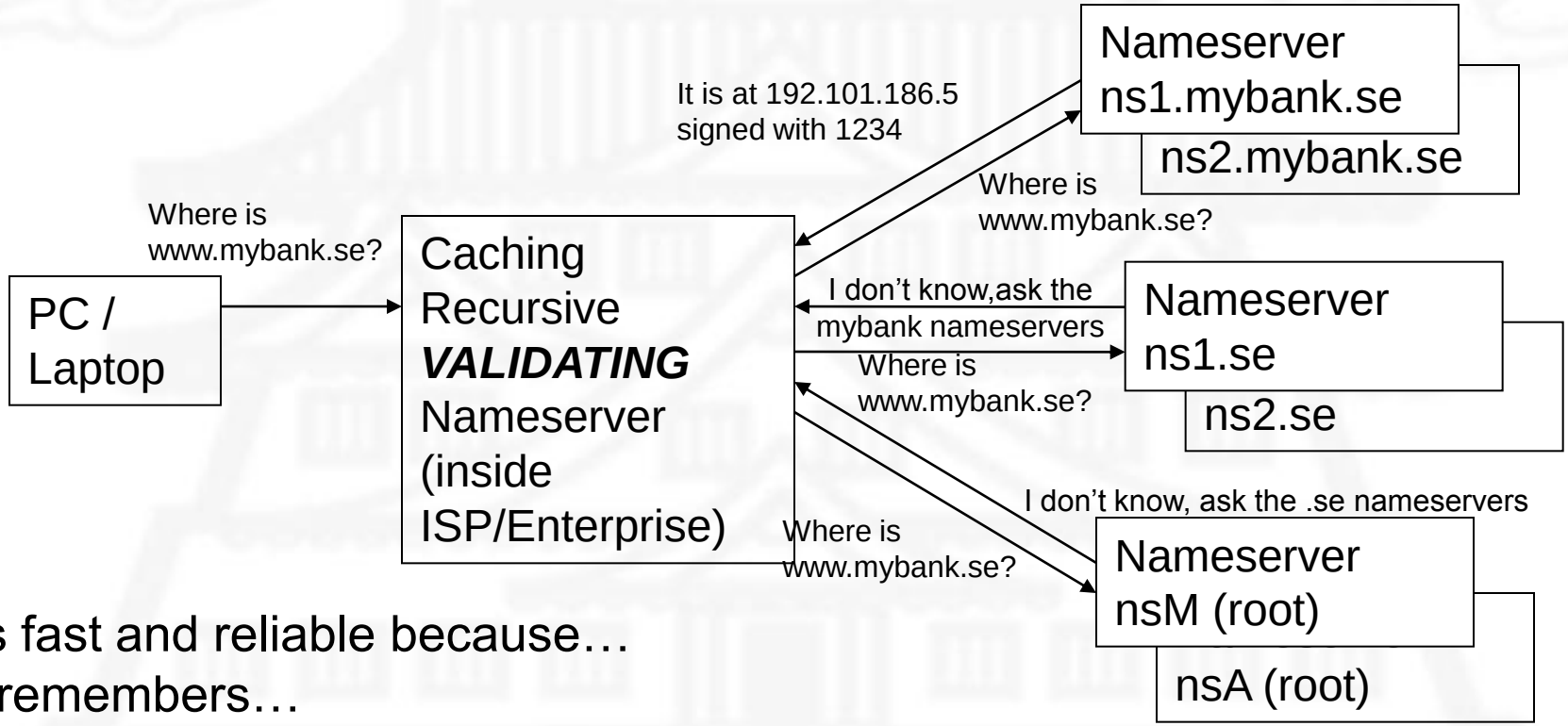
- Requirements
- High Level Technical Architecture
- DNSSEC Practice Statements (DPS)
- Trust Anchor Publication
- Deployment Plan
- KSK Ceremonies Guide
- TCR Proposal
- Resolver Testing with a DURZ

Root DNSSEC Design Team

rootsign@icann.org

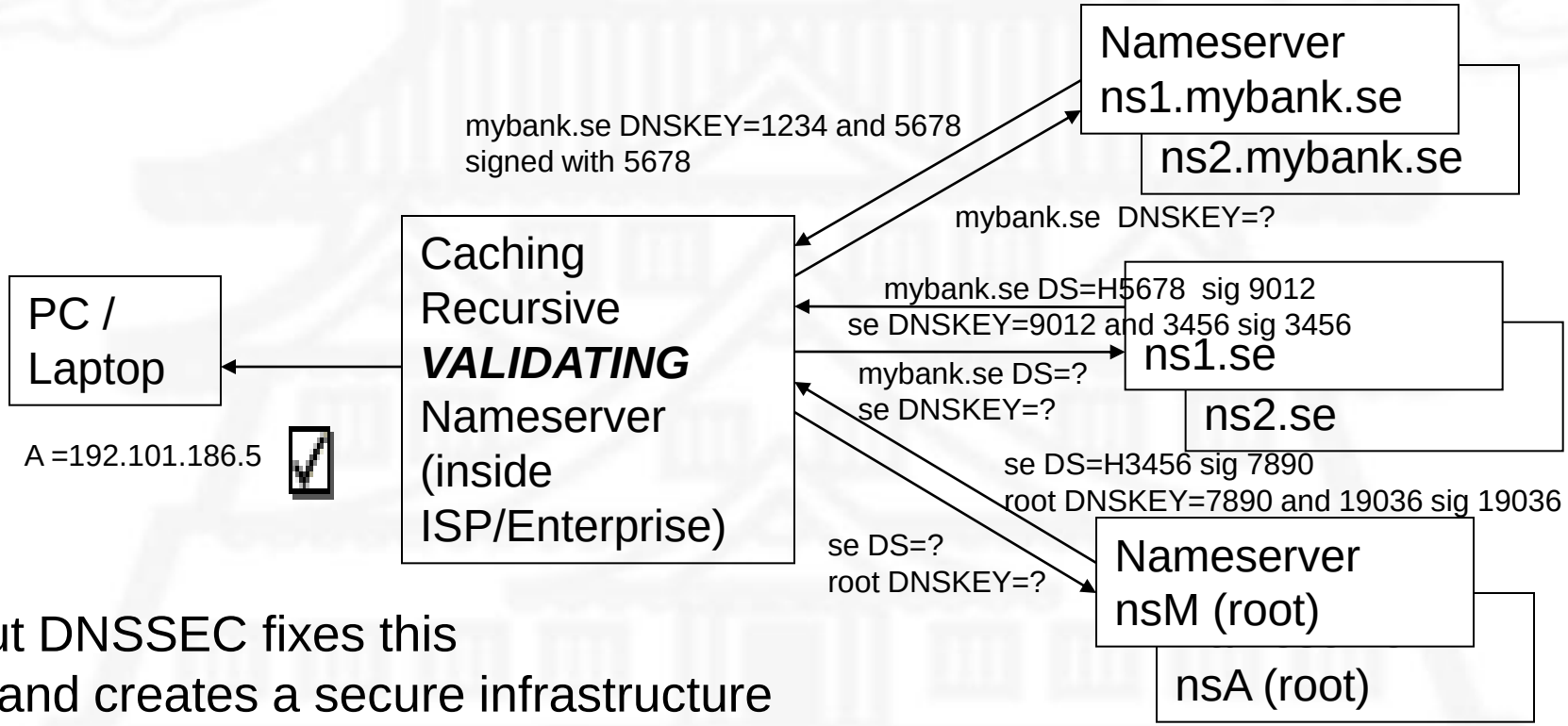
Joe Abley
Mehmet Akcin
David Blacka
David Conrad
Richard Lamb
Matt Larson
Fredrik Ljunggren
Dave Knight
Tomofumi Okubo
Jakob Schlyter
Duane Wessels

DNSSEC Overview



- Its fast and reliable because…
- It remembers…
- …and this is also the vulnerability

DNSSEC Overview (cont)



- but DNSSEC fixes this
- ...and creates a secure infrastructure for new Internet security solutions.

DNSSEC Overview – 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)

se - Registry

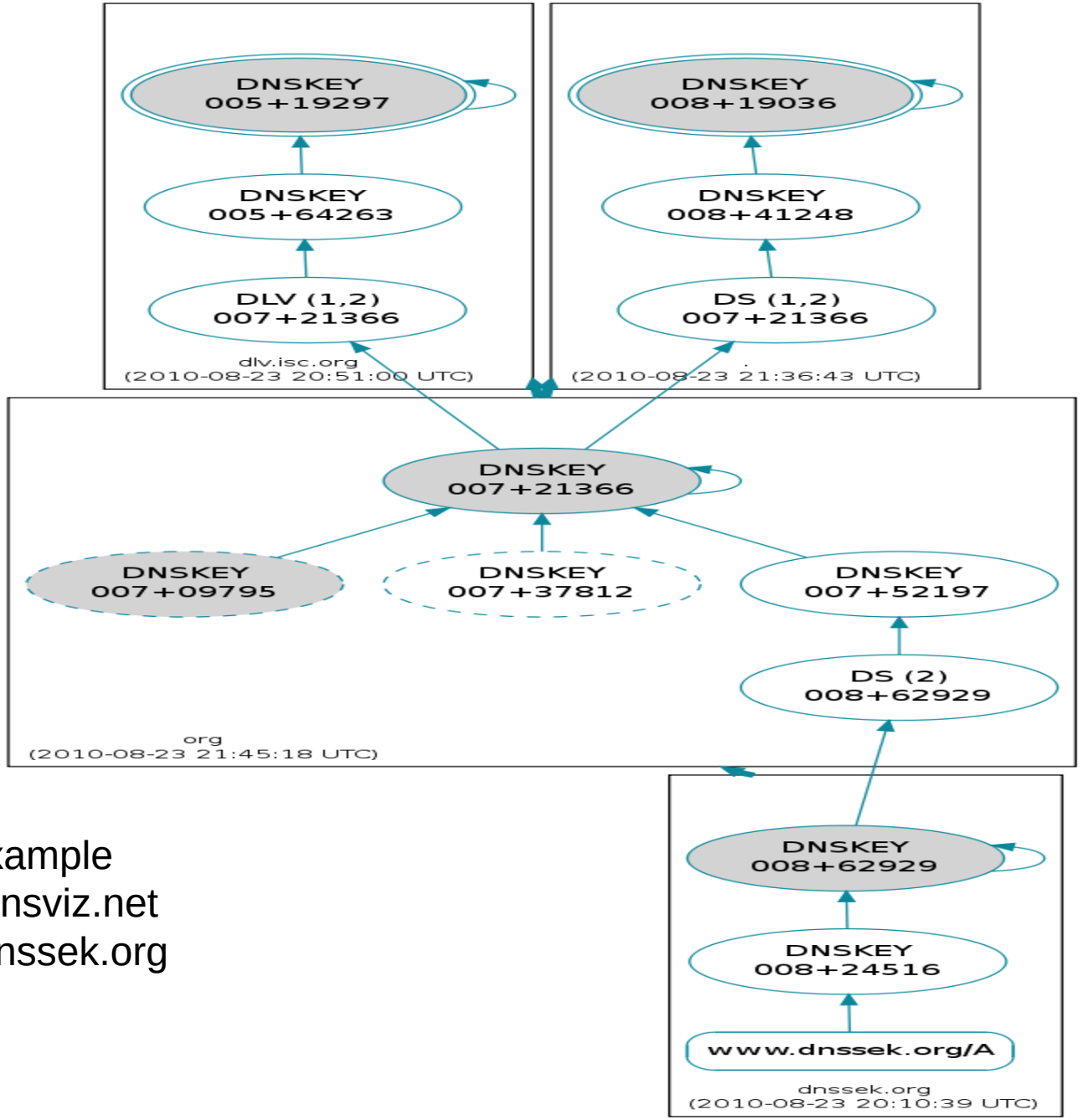
mybank.se-ds ***se-dnskey-zsk***
se-dnskey-zsk ***se-dnskey-ksk***
se-ds = hash(se-dnskey-ksk)

root

se-ds ***root-dnskey-zsk***
root-dnskey-zsk ***root-dnskey-ksk***

resolver – ISP, Enterprise, etc

root-ds = hash(root-dnskey-ksk)



Live example
http://dnsviz.net
www.dnssek.org

DNS is now more than just DNS

- Whole range of applications/products/services will be built and rely on DNS and DNSSEC “chain of trust” (ref: Dan Kaminsky)
- Increased dependence of Registrants on DNS for security
- New product/service revenue potential for all
- Ultimately it is the responsibility of the Registrant to choose Registrar and Registry that reduces risk to an acceptable level.
  - Risks for Registrant
    - Financial
    - Reputational
    - Legal
- Therefore:
  - Security becomes more important
  - Trust becomes more important
- Can be solved with improved processes and practice
  - Not necessarily expensive

Registrar perspective

- Responsible for identifying Registrant
- Responsible for DS records
  - Secure Transmission to Registry (EPP, etc)
  - Checking DS records?
    - Consequences
      - Sub-zone could go dark
      - Chain of trust broken – security solutions fail. Attacks ensue.
    - Verify corresponding private KSK ownership?
    - Scripts and tools to help
      - Compute DS from on-net KSK DNSKEYs and match with supplied DS
      - yazvs (http://yazvs.verisignlabs.com/)
      - dnsviz.net and other on-line tools
    - Can't do all, e.g. GOST keys
    - Out-of-Band verification (e.g. , telephone hash or code. We use this for root)
    - Future: automated DS updates based on established trust
  - Where does DS come from?

Registrar perspective cont.

- Registrant supplied DS
  - Simple but rare
  - Limit number to Registry limit – at least two for rollover (e.g., GoDaddy=10)
- Generation of DS for Registrant
  - More likely (e.g. .CZ ACTIVE24 and WEB4U just DNSSEC for all)
  - Revenue opportunity
  - Differentiation
  - Associated Requirements
    - DPS, documented and audited procedures, different level of trust / $ervice
    - Key transfer policy between registrars
    - Clarification of liabilities / understanding risks
  - Split KSK/ZSK model (messy, unlikely), bump in wire, or host DNSSEC zone for registrant
  - or Outsource the whole thing for a fee (e.g., Afilias one click DNSSEC, name.com)
- Other revenue models

Registry perspective

- You are DNSSEC experts by now – right?
- Just receive DS. Presumed correct.
- May check that at least one valid chain of trust exists (Check that DS-DNSKEY pair validate…root does this)
- Registrar responsible for identifying Registrant
- How many DS records? (e.g., .SE = 6, .EU=4)
- Does not validate that Registrant has private KSK.
- DS record removed by request from Registrar.
  - This deactivates DNSSEC for the zone. No security but everything still works.
  - Only Registrant Tech or Admin Contact has authority to request DS removal
  - Registrar does this on Registrant's behalf
    - How soon does this happen ? - should be made clear since security applications now rely on this.
- Emergency removal by Registrant if can't reach Registrar?

New Solutions – New Opportunities

- Genie is out of the bottle
  - Global PKI
  - Unambiguous domain name based authentication
  - Like all progress – some “creative destruction”
- Security solutions
  - Email (e.g. DKIM RFC4871, S/MIME for all)
  - Self signed certs for all (RFC4398)
  - Improved EV certs. Certificate Authorities still have a very important role.
  - VPN, remote login (RFC4025, RFC4255)
  - Secure IM/chat
  - New RR types
- Opportunity for revenue and differentiation

General Security Improvements

- Unfortunate Registrar Stories
  - CheckFree (SSAC Report 040)
  - Recent DefCon/BlackHat comments. DNSSEC → security solutions… but must focus on weak links in chain of trust
- Building Trust in your organization
  - Customer education
  - Published maintenance procedures (details not necessary)
  - Checked (audited)
  - Internal, SysTrust (Security, Availability, Processing Integrity, Confidentiality, Privacy), ISO27K, NIST 800-53, DPS is a good beginning.
  - Regular review

Building Trust

- Say what you do
- Do what you say
- External check that you did
- Stakeholder Involvement
  - Incorporate Feedback in updates
  - Participation
- Be Responsible
- Good start: DPS - DNSSEC Practices Statements
  - http://www.iis.se/docs/se-dnssec-dps-eng.pdf

General Security Improvements

- Opportunity to benefit from improvements
  - Two-factor authentication
    - Good if your model supports it (e.g., name.com)
    - Uses between registrant-registrar, registrar and registry. ($5 card/token, existing id's, VRSN, PIV card)
    - May help but not all that is necessary nor is it a magic bullet against poor practices or social engineering techniques on a single point of contact
  - Vetted system designs may help (e.g. SQL/cgi attacks)
  - Better practices and procedures (more SW/HW not a must)
    - Documented and scripted practices and procedures – internal and external
    - Out-of-band notifications, e.g. automated phone call? (now mostly email)
    - If username/password only – minimum length/strength requirements? Limit number of tries (add delay). Challenge questions.
    - Support and optionally require multiple points of contact mirroring tech/admin (protects registrant against insider problem, disgruntled employee)
    - Educate the customer about protection measures already in place – call attention to this. This is a great differentiator and trust builder.

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 Registrars and Registries 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

Thank You


ICANN
AsiaPacific
Regional Event of ICANN-Accredited Registrars and gTLD Registries

Dr. Richard Lamb,
richard.lamb@icann.org
Tomofumi Okubo,
tomofumi.okubo@icann.org