IANA and DNSSEC at the Root

APRICOT 2009 Manila

February 25, 2009

richard.lamb@icann.org

Questions

- DNSSEC what is it
- Why do I care
- How will it effect me
- Why is IANA involved
- What I want

What is it?

- Protecting the Internet’s phonebook
- Just like your Web site certificate is signed by your Certificate Authority and whose certificate is stored and trusted by your operating system vendor,
- you have the public keys used to sign your domain signed by the registry you got your domain name from whose public key is stored and trusted by your nameserver.
- www.yourbank.se

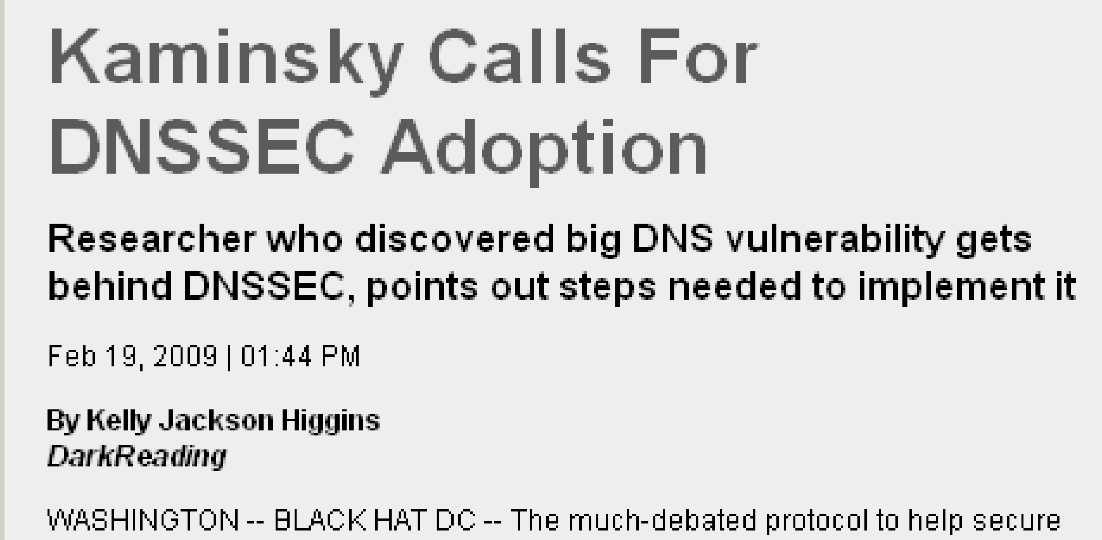
$$\text{www}_{\text{yourbank}} \rightarrow \text{yourbank}_{\text{se}} \rightarrow \text{se}_{\text{root}}$$

A,RRSIG,DNSKEY → DS, RRSIG,DNSKEY → DS,RRSIG,DNSKEY→ DS,RRSIG,DNSKEY

Why do I care?

- DNS cache poisoning in less than a second w/o patch – thank you Kaminsky, Dickenson, and others
- ~6hr after patch. Many resolvers un-patched
- Its coming… community pressure, ccNSO report, .se, .pr, .bg, .br, .cz, .museum… .org, .gov, .uk, .ca …
- I hear you can do cool things with it. E.g., alternate/free source of trust for DKIM, certs, SSL, ipsec, and who knows
- ….but you tell me

Press



Kaminsky Calls For DNSSEC Adoption

Researcher who discovered big DNS vulnerability gets behind DNSSEC, points out steps needed to implement it

Feb 19, 2009 | 01:44 PM

By Kelly Jackson Higgins
DarkReading

WASHINGTON -- BLACK HAT DC -- The much-debated protocol to help secure

- need to make DNSSEC deployable today
- "DNSSEC is the key to fixing the persistent authentication problems plaguing real-world, cross-organizational business for years,”

http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=214501924&cid=RSSfeed

How will it effect me?

- Registrant / domain name operator
  - Cost? (extra ½ time job/year: Swedbank)
  - Complexity but tools continue to be developed
  - Deployment experience building (e.g. .se, .uk, .cz,…)
  - Lessons learned → automation is key (e.g., auto key gen/sign)

http://www.internetdagarna.se/arkiv/2008/www.internetdagarna.se/images/stories/doc/22_Kjell_Rydger_DNSSEC_from_a_bank_perspective_2008-10-20.pdf

How will it effect me?

- Registries (e.g., nz) and Registrars (e.g., GoDaddy)
  - handle DS records in addition to NS records and other info
  - possibly manage keys and signing operations on behalf of customers
  - slow uptake and time may be on our side
  - zone walking issue - NSEC3 is a solution (.ORG)

How will it effect me?

- ISP's
  - 3-12 x bandwidth, validation processing, memory
    http://www.net.informatik.tu-muenchen.de/~anja/feldmann/papers/dnssec05.pdf
  - need to maintain a trust anchor (for signed root) or multiple trust anchors (for unsigned root) in their validating recursive resolver.
  - Secure trust anchor delivery. Maybe ISP's (or a designated organization) part of key generation ceremony?

How will it effect me?

- End user
  - O/S resolvers (i.e. Windows desktop/server)
  - Need to make applications aware. e.g. fallback behavior
  - Securing the last DNSSEC mile.
  - resilience of DNSSEC-- handling new failure modes (key expiry, middleboxes like firewalls and proxies that don't handle the extra data properly)
  - application awareness: what do you do with DNSSEC data, especially if you want to know why/how validation failed if it did?

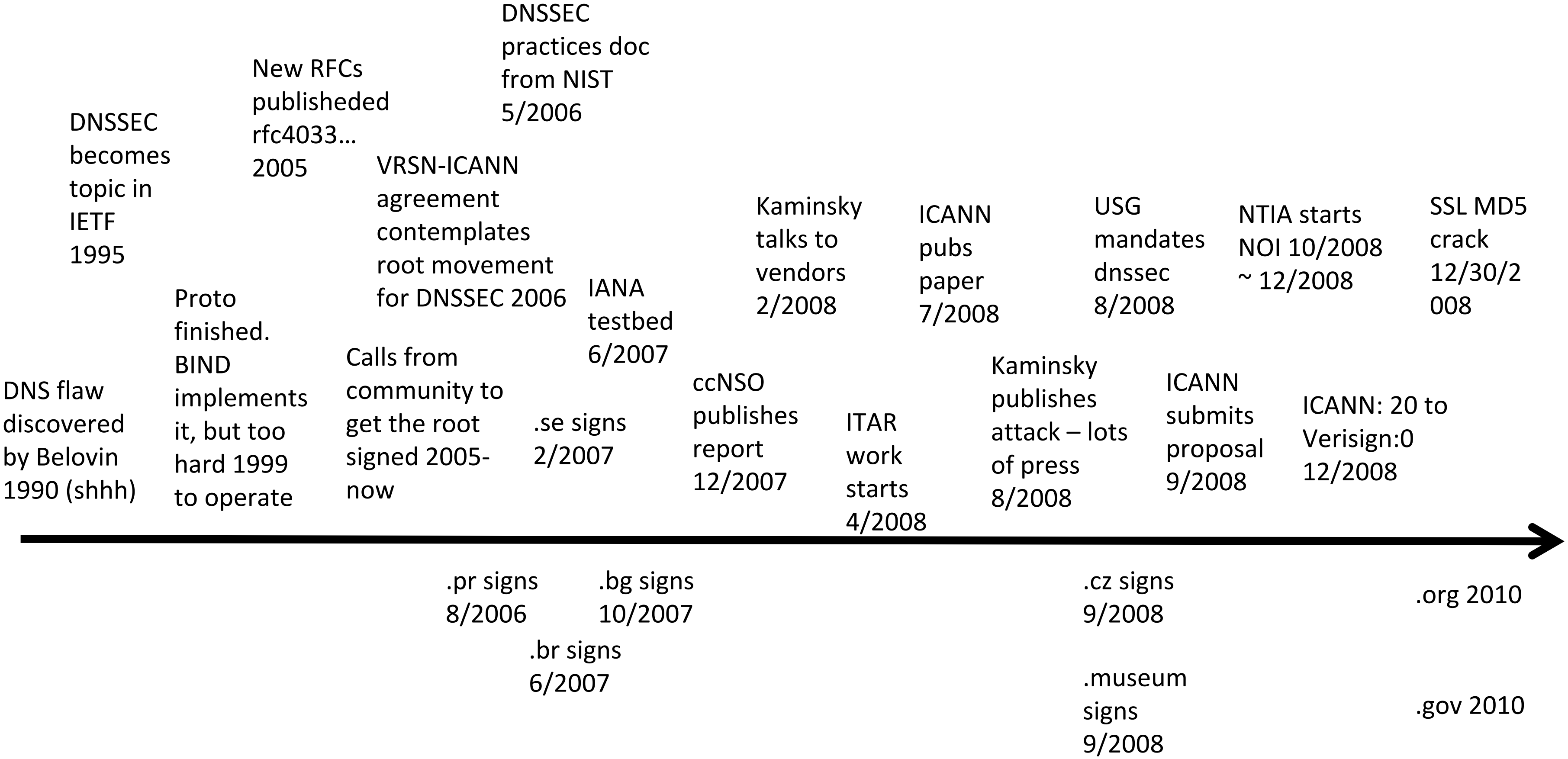
Why is IANA involved?

- We have been asked by the community (APNIC, RIPE, ccTLDs, …). Start the ball rolling. No excuses.
- We are here to serve and are responsible for managing the root

Who cares about a signed root?

- Simplifies DNSSEC configuration
- Compromise recovery….reason for root (or ITAR)
- Maintaining trust from TLD operator to root

Sequence of Events



DNS flaw discovered by Belovin 1990 (shhh)

DNSSEC becomes topic in IETF 1995

Proto finished. BIND implements it, but too hard 1999 to operate

New RFCs publisheded rfc4033… 2005

Calls from community to get the root signed 2005-now

VRSN-ICANN agreement contemplates root movement for DNSSEC 2006

DNSSEC practices doc from NIST 5/2006

.se signs 2/2007

IANA testbed 6/2007

ccNSO publishes report 12/2007

Kaminsky talks to vendors 2/2008

ITAR work starts 4/2008

ICANN pubs paper 7/2008

Kaminsky publishes attack – lots of press 8/2008

USG mandates dnssec 8/2008

ICANN submits proposal 9/2008

NTIA starts NOI 10/2008 ~ 12/2008

ICANN: 20 to Verisign:0 12/2008

SSL MD5 crack 12/30/2008

.pr signs 8/2006

.br signs 6/2007

.bg signs 10/2007

.cz signs 9/2008

.museum signs 9/2008

.org 2010

.gov 2010

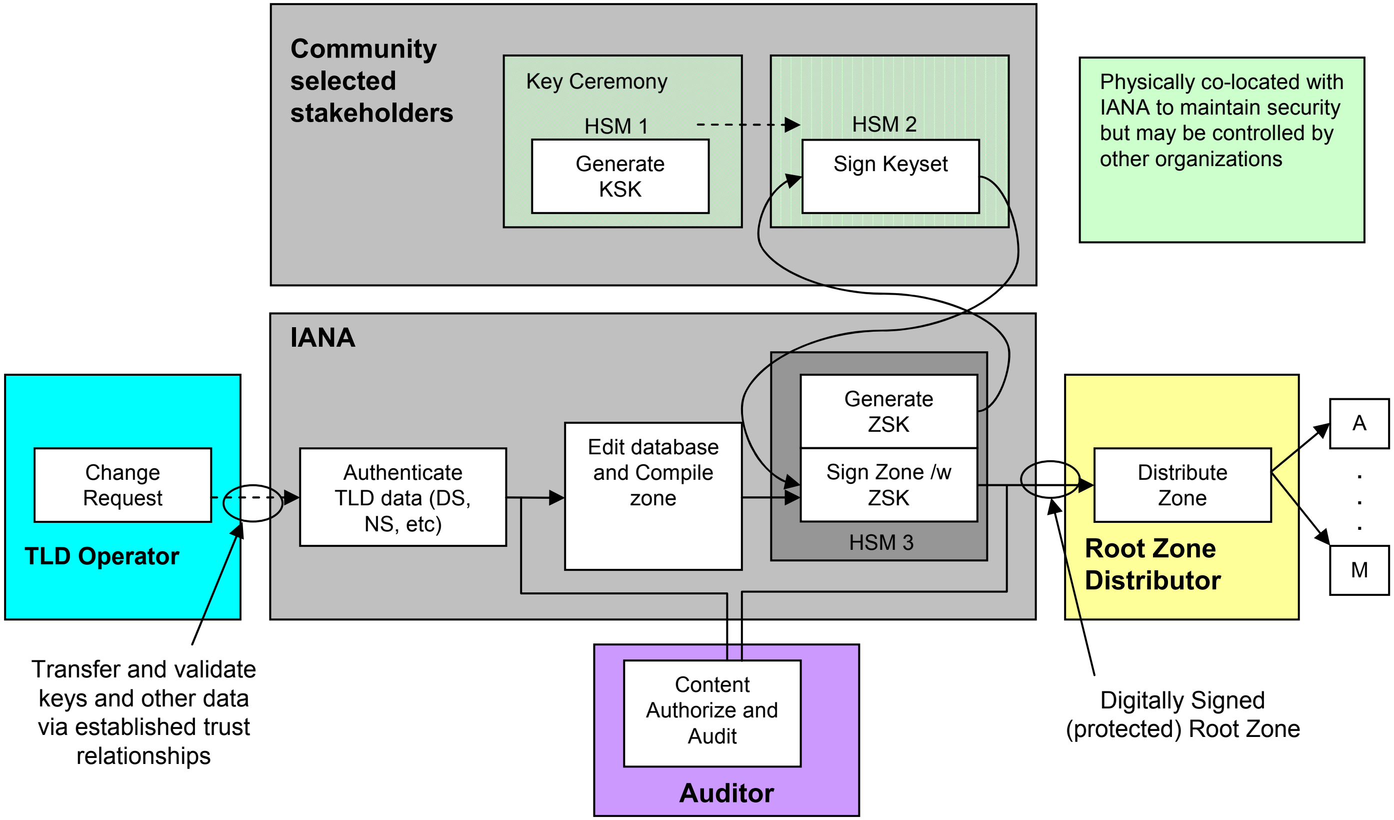
Goal: Trust and Accountability

- Important elements of a root-signing solution are transparency, public consultation, broad stakeholder participation (e.g. key ceremony), flexibility, reliability, and trust;
- Solution has to balance various concerns, but must provide for a maximally secure technical solution and one that provides the trust promised by DNSSEC;
- An open, transparent and international participatory process will allow for root zone management to adapt to changing needs over time as DNSSEC is deployed throughout the Internet and as new lessons are learned.

ICANN’s root signing proposal

- No change in administrative control of content
- Accept no compromises in security: preserve chain of trust
- Designed by Community for Community
- Broad and **continual** international participation
- Root “key” controlled by Internet community – not ICANN
- Regular auditing and reporting
- Timely deployment building on existing signed root and experience
- Maximum reliability through automation
- Flexible to support evolving technologies and policies
- All Open Source

vet, sign - together

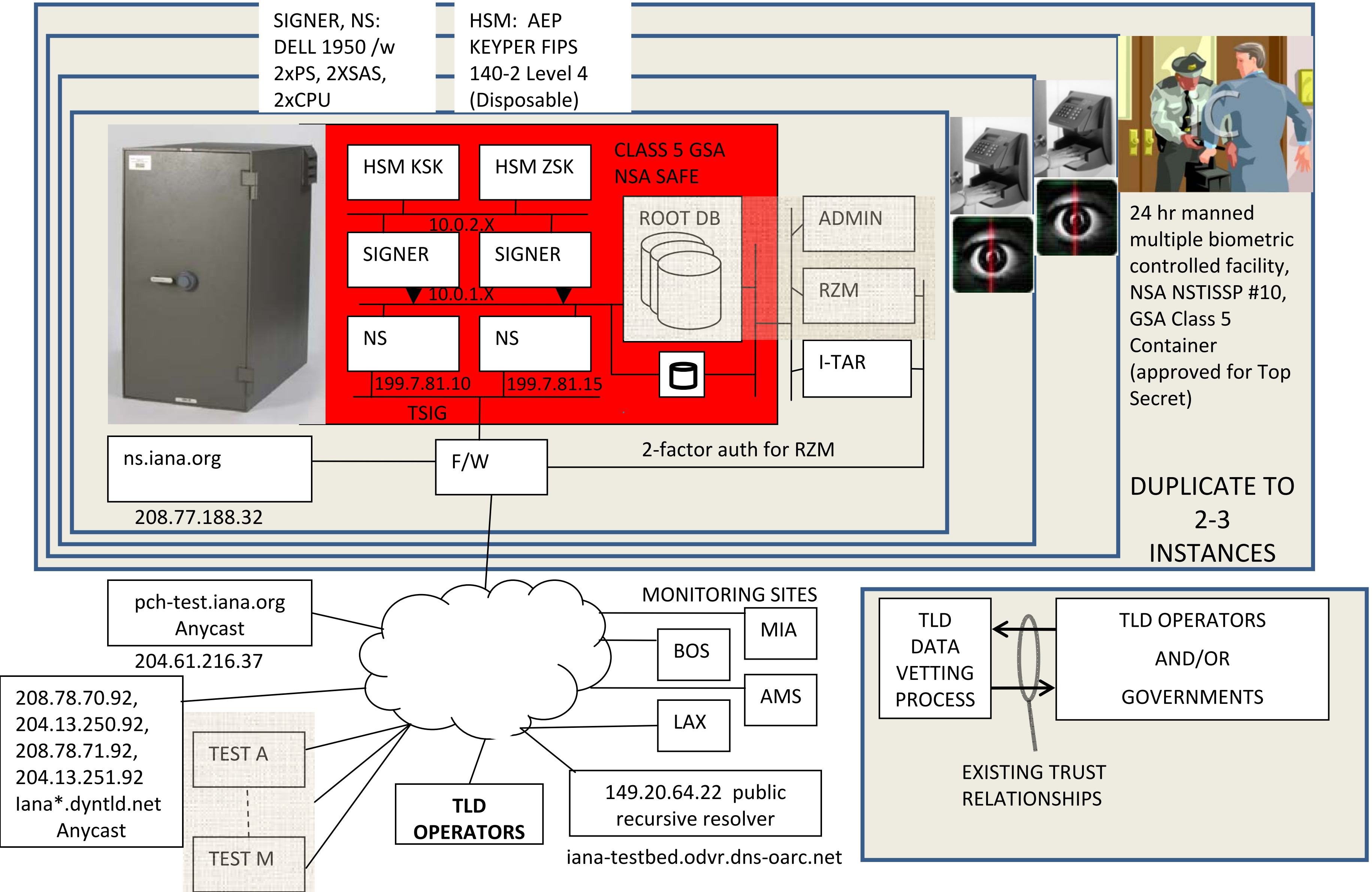

Community selected stakeholders
Key Ceremony
HSM 1
Generate KSK
HSM 2
Sign Keyset
Physically co-located with IANA to maintain security but may be controlled by other organizations
IANA
Change Request
TLD Operator
Authenticate TLD data (DS, NS, etc)
Edit database and Compile zone
Generate ZSK
Sign Zone /w ZSK
HSM 3
Distribute Zone
Root Zone Distributor
A
.
.
.
M
Content Authorize and Audit
Auditor

Transfer and validate keys and other data via established trust relationships

Digitally Signed (protected) Root Zone

Behind our testbed

System status at: https://ns.iana.org/dnssec/status.html
.arpa, in-addr.arpa, ip6.arpa, iris.arpa, urn.arpa, uri.arpa,
.int, xn-"test" (DS: .se, .br, .bg, .pr, .cz, .museum, .gov.)



SIGNER, NS:
DELL 1950 /w
2xPS, 2XSAS,
2xCPU

HSM: AEP
KEYPER FIPS
140-2 Level 4
(Disposable)

24 hr manned
multiple biometric
controlled facility,
NSA NSTISSP #10,
GSA Class 5
Container
(approved for Top
Secret)

DUPLICATE TO
2-3
INSTANCES

Some Features

- Based on trailblazing work of .SE – much help and continue to enlist generous help from DNSSEC deployment experts
- Flexibility to changing policies and tech , e.g., common standards – PKCS11 in crypto boxes.
- Highest level security for key handling – FIPS 140-2 level 4
- Looking into multiple non-US mirror sites
- No compromise in security. no weak links in trust or accountability or in chain
- Draw on all deployment efforts. Benefit from lessons learned from dnssec deployment so far – e.g., maximize automation
- Ready to deploy – fast a possible as requested by NOI but timely – slow takeup is our friend
- Fully funded and budgeted – ICANN is serious about this work – eg stood up operational group to deal with this
- Naturally open source

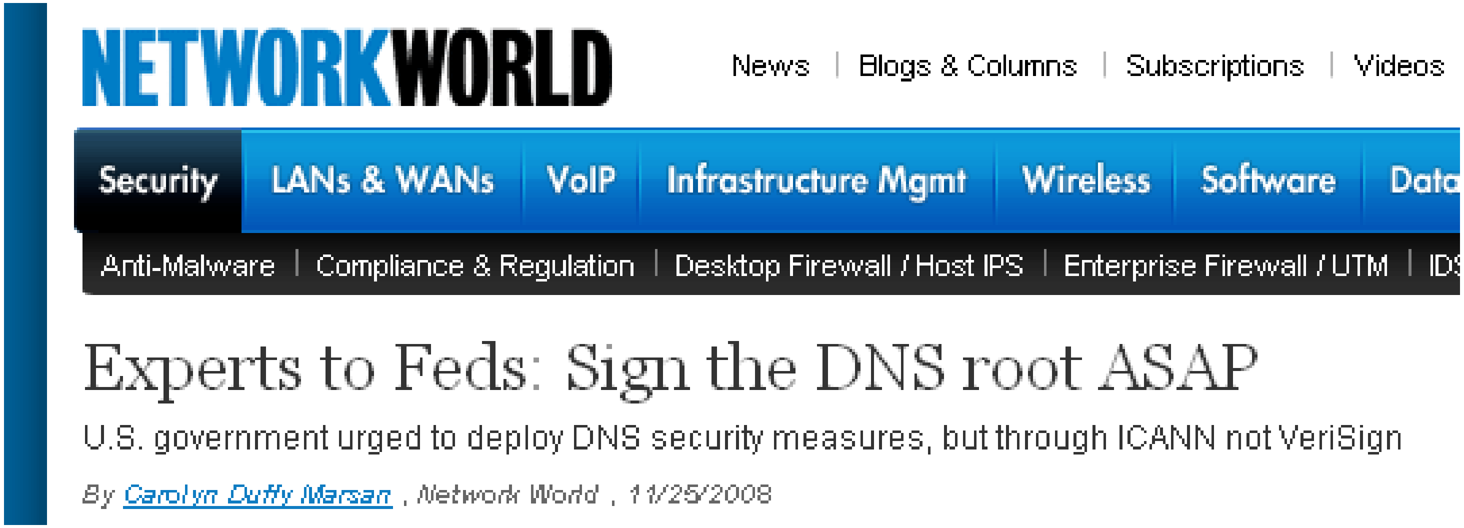
Go ahead – test it!

- Public recursive validating DNSSEC resolver at 149.20.64.22. Thank you OARC / Duane!
- Masters: 208.77.188.32 (ns.iana.org) and Anycast 204.61.216.37 (pch-test.iana.org). Thank you PCH!
- More Anycast masters: 208.78.70.92, 204.13.250.92, 208.78.71.92, 204.13.251.92 Thank you dynect.com!

What are we waiting for?

- Waiting on NTIA (Department of Commerce) decision
- Technically ready. Almost two years of operational public testbed
- (USG HowTo)

Press



Experts to Feds: Sign the DNS root ASAP

U.S. government urged to deploy DNS security measures, but through ICANN not VeriSign

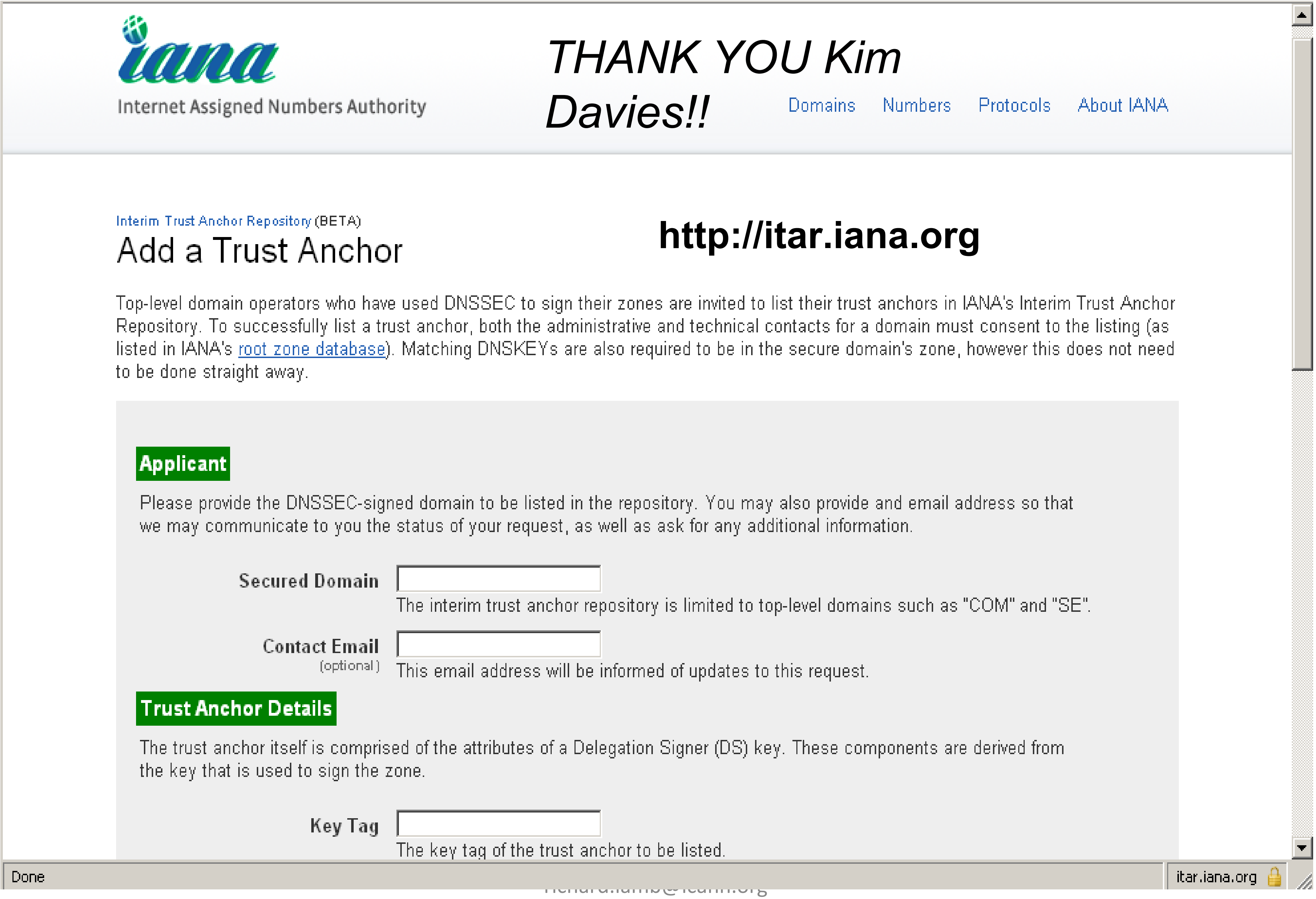
By Carolyn Duffy Marsan , Network World , 11/25/2008

http://www.networkworld.com/news/2008/112508-dns-root.html

http://www.ntia.doc.gov/dns/dnssec.html

http://blog.wired.com/27bstroke6/2008/10/who-should-sign.html

Interim Trust Anchor Repository - ITAR



THANK YOU Kim Davies!!

http://itar.iana.org

Interim Trust Anchor Repository (BETA)

Add a Trust Anchor

Top-level domain operators who have used DNSSEC to sign their zones are invited to list their trust anchors in IANA's Interim Trust Anchor Repository. To successfully list a trust anchor, both the administrative and technical contacts for a domain must consent to the listing (as listed in IANA's root zone database). Matching DNSKEYs are also required to be in the secure domain's zone, however this does not need to be done straight away.

Applicant

Please provide the DNSSEC-signed domain to be listed in the repository. You may also provide and email address so that we may communicate to you the status of your request, as well as ask for any additional information.

Secured Domain ____
The interim trust anchor repository is limited to top-level domains such as "COM" and "SE".

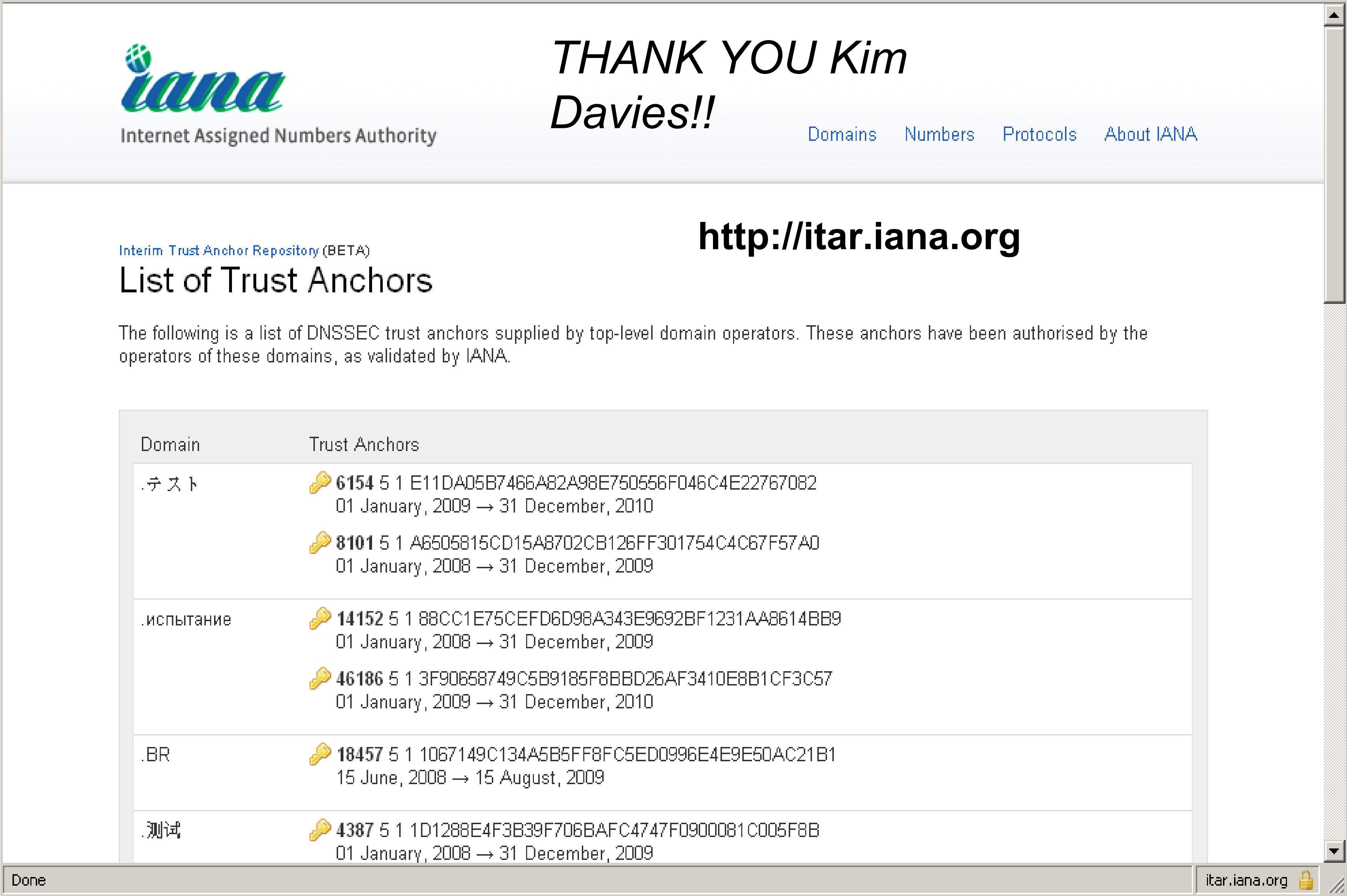
Contact Email (optional) ____
This email address will be informed of updates to this request.

Trust Anchor Details

The trust anchor itself is comprised of the attributes of a Delegation Signer (DS) key. These components are derived from the key that is used to sign the zone.

Key Tag ____
The key tag of the trust anchor to be listed.

Interim Trust Anchor Repository - ITAR



THANK YOU Kim Davies!!

http://itar.iana.org

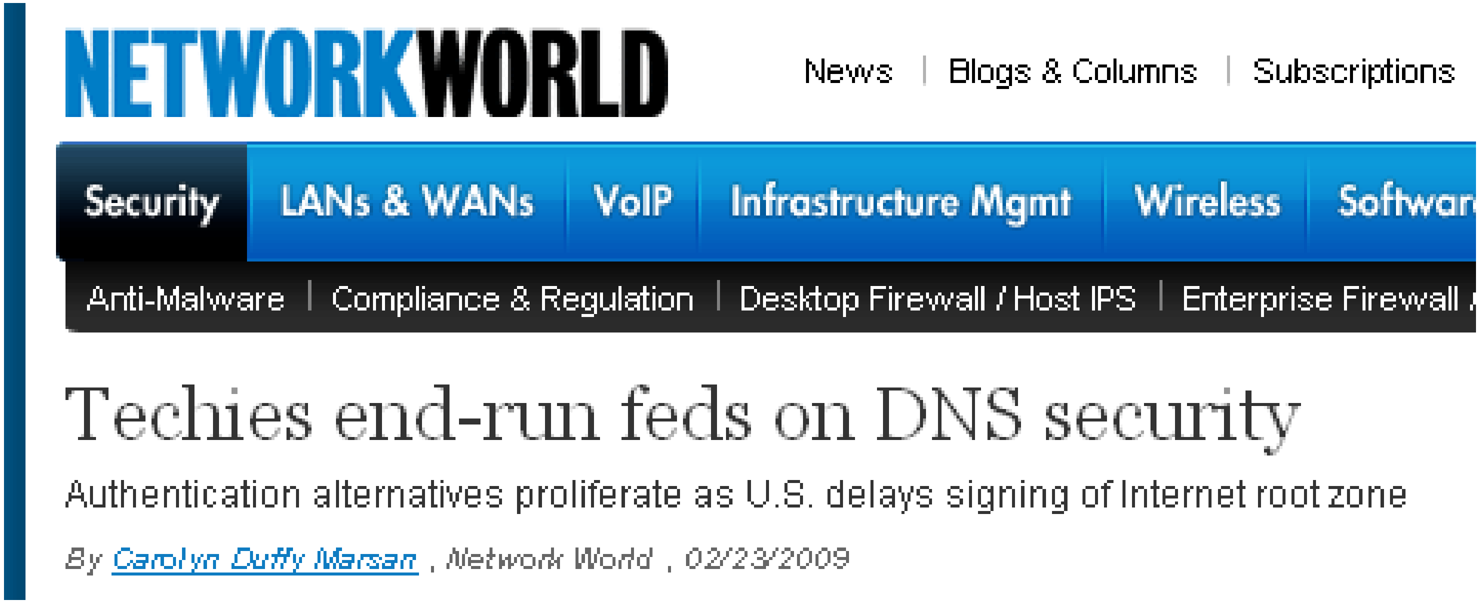
Interim Trust Anchor Repository (BETA)

List of Trust Anchors

The following is a list of DNSSEC trust anchors supplied by top-level domain operators. These anchors have been authorised by the operators of these domains, as validated by IANA.

Domain	Trust Anchors
.テスト	**6154** 5 1 E11DA05B7466A82A98E750556F046C4E22767082 01 January, 2009 → 31 December, 2010 **8101** 5 1 A6505815CD15A8702CB126FF301754C4C67F57A0 01 January, 2008 → 31 December, 2009
.испытание	**14152** 5 1 88CC1E75CEFD6D98A343E9692BF1231AA8614BB9 01 January, 2008 → 31 December, 2009 **46186** 5 1 3F90658749C5B9185F8BBD26AF3410E8B1CF3C57 01 January, 2009 → 31 December, 2010
.BR	**18457** 5 1 1067149C134A5B5FF8FC5ED0996E4E9E50AC21B1 15 June, 2008 → 15 August, 2009
.测试	**4387** 5 1 1D1288E4F3B39F706BAFC4747F0900081C005F8B 01 January, 2008 → 31 December, 2009

Press

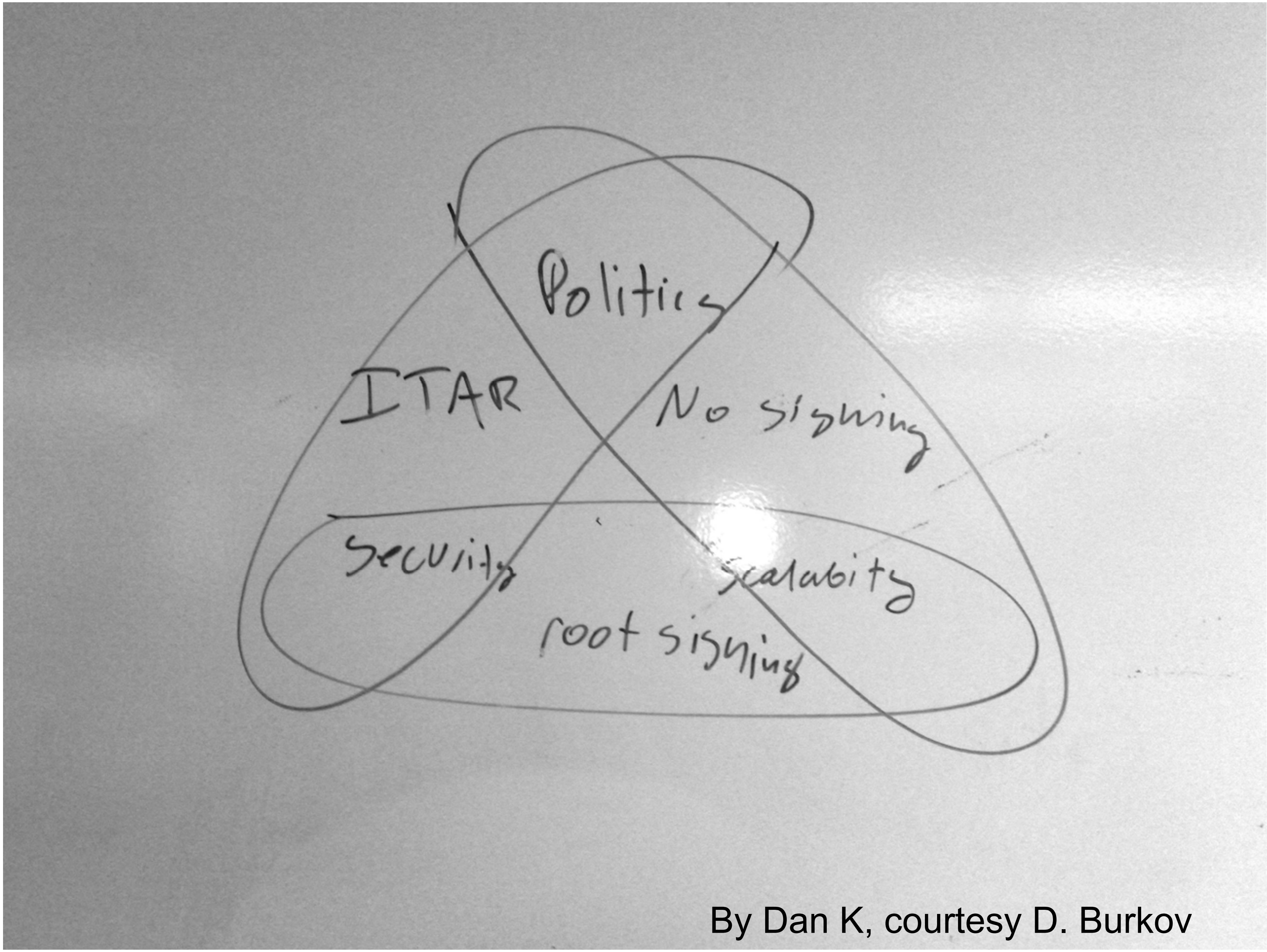

NETWORKWORLD
News | Blogs & Columns | Subscriptions
Security
LANs & WANs
VoIP
Infrastructure Mgmt
Wireless
Softwar
Anti-Malware | Compliance & Regulation | Desktop Firewall / Host IPS | Enterprise Firewall /

Techies end-run feds on DNS security

Authentication alternatives proliferate as U.S. delays signing of Internet root zone

By Carolyn Duffy Marsan , Network World , 02/23/2009

http://www.networkworld.com/news/2009/022309-dns-security.html?hpg1=bn



By Dan K, courtesy D. Burkov

Whats next

- Meanwhile –continue to educate, discuss and exchange ideas with those deploying DNSSEC and operationalize our DNSSEC infrastructure
- New DNS Group headed up by Joe Abley
- Part of overall IT operations headed up by DRC
- Expanding operational capabilities
- Responsible for DNSSEC, L-root, and other DNS
- Some efforts
  - Second safe, backup location, deploy it, publish all operational and design documents
  - Publicize DNSSEC efforts
  - Study gTLD + DNSSEC + IPv6 effects on root –"perfect storm"
  - Fleshing out the current root signer testbed /w Kirei (responsible for .SE and follow on. Processes, security, key dist, ceremony, etc)

Misc

- I-TAR and signed root
  - EV+PGP .vs. ceremony/hints file?
    - discuss
- .arpa (IAB), in-addr.arpa, ip6.arpa (pulling in sub), iris.arpa, urn.arpa, uri.arpa, .int, iana.org, icann.org
- .com+.net by 2011

http://www.networkworld.com/news/2009/022409-verisign-dns-security.html?hpg1=bn

What do I want?

- To thank the APNIC community for its past support.
- And look to your direction, comments, feedback and continued support – its your root.

Thanks to APNIC, Roy Arends (.uk), Patrik Falstrom, Olaf Kolkman, Jakob Schlyter (.se), John Dickinson, David Soltero (.pr), Kim Davies, David Miller, Don Davis, Andy Linton and so many others from the Internet and security communities!!

Questions?