Some of Dr. Richard Lamb's Technical Contributions at ICANN

1. With help from NSRC developed my own teaching kit and material over the years (since 2011). Transitioned from FBSD jails to 90 LXC VMs under Ubuntu. Complete standalone signed root dnssec system and routing infrastructure that fits in a backpack. Under continual improvement to track events. E.g. http://dnssec-deployment.icann.org/training/SGN/

and thanks to and many others for courseware

DNS/DNSSEC Hands-On Training APNIC 2017 Ho Chi Minh City, Vietnam

This is a 5-day, hands-on workshop. The participants will:
Learn to design, deploy, and operate authoritative and recursive DNS architectures
Understand the risks surrounding the DNS, and the role of DNSSEC (DNS security extensions)
Learn how to deploy DNSSEC, including zone signature and key management
Learn about secure registry operations, monitoring and practices.

Workshop Requirements:

Some understanding of DNS and netowrk basics
Some knowledge of Linux/UNIX command line
Participants need to bring a computer that can acess WiFi and capable of running "ssh". Tablet computers will not work.

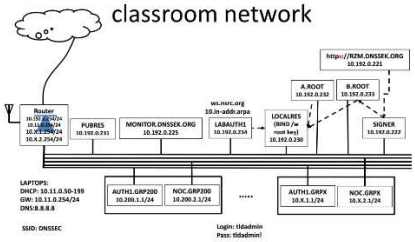
DNS/DNSSEC/NMM Workshop Agenda

Schedule

Session 1	0900-1030
Break	
Session 2	1100-1230
Lunch	
Session 3	1400-1530
Break	
Session 4	1600-1730

Instructors

Name	Email	Organization
Nguyen Trung Kien	Nguyen Trung Kien(at)vnnic.vn	VN NIC
Champika Wijayatunga	champika.wijayatunga(at)icann.org	ICANN
Richard Lamb	richard.lamb(at)icann.org	ICANN



2. Designed/Built/Deployed and maintain multiple root DNSSEC KSK rollover sites in 2015 specially designed to accelerate testing of root KSK rollover using RFC5011. Complete copy of root including PKI signed XML anchors. E.g., https://www.toot-servers.net/root7/ https://icksk.dnssek.info/fauxroot.html

Test minimal root zone with continually rolling KSK and ZSKs (Schedule)
Slightly delayed KSK roll and no missing key Extended Rickroll Final

NOTICES:
22 June 2016: Trust Anchors XML file now tracks introduction, revoke, and removal of KSKs.

11 June 2016: Standalone accelerated 5011 test root server instantiated. One delegation ("test.").

Root server (NSD) Current state indicated by red block in first row. ~60 seconds per slot

Corresponding resolver config:
unbound.conf
root.hints Minimal:

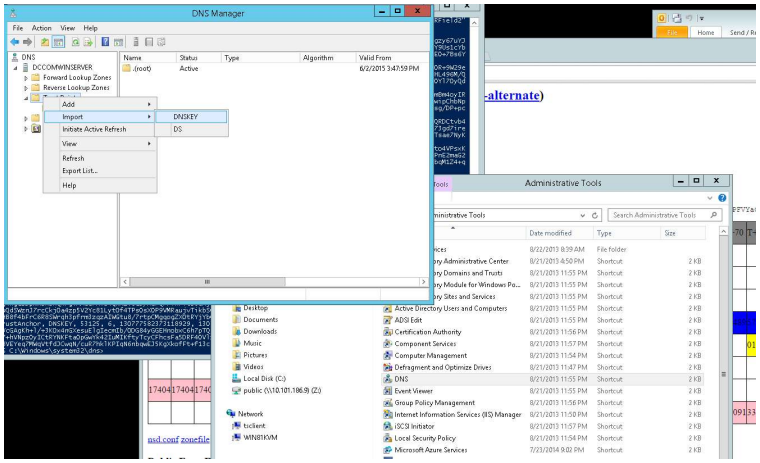
```
.                       12  IN NS    A.TOOT-SERVERS.NET.
A.TOOT-SERVERS.NET.     12  IN A     139.162.162.215
A.TOOT-SERVERS.NET.     12  IN AAAA  2a01:7e01::f03c:91ff:fe28:1ad2
```

Set initial unbound.root.key to:

```
. 12 IN DNSKEY 257 3 8 AwEAAeN5JF++HpbugMqfQdwB01ibIzBgZsTOOgoZV9YhbU4KRzAds8Y6 ogkZCDg+qXd4MceO1hAhGgTsivslxC1M9eDtd6mNkzQpet0D2EVK/yP2 HQNbucTohe7ECHUs1JNbgzf44
```

T+0	T+10	T+20	T+30	T+40	T+50	T+60	T+70	T+80	T+0	T+10	T+20	T+30	T+40	T+50	T+60	T+70	T+80	T+0	T+10	T+20	T+30	T+40	T+50	T+60	T+70	T+80
52083																										
37119	37119	37119	37119	37119	37119	37119	37119	37119	37119																	
								00933	00933	00933	00933	00933	00933	00933	00933	00933	00933	00933								
																	22275	22275	22275	22275	22275	22275	22275	22275	22275	22275
																										37119
03772	03772	03772	03772	03772	03772	03772	03772	03772	03772	03772	03772	03772	03772	03772	03772	03772	03772	03772	03772	03772	03772	03772	03772	03772	03772	
	31255	31255	31255	31255	31255	31255	31255	31255	31255	31255	31255	31255	31255	31255	31255	31255	31255	31255	31255	31255	31255	31255	31255	31255	31255	31255
1139	1139	1139	1139	1139	1139	1139	1139	1414	1414	1139	1139	1139	1139	1139	1139	1139	1414	1414	1425	1425	1425	1425	1425	1425	1425	1139

3. Running public test validating resolver Windows Server, Ubuntu, and BIND systems for above.



4. Design/Built/Deployed free ccTLD DNSSEC HSM based signing system complete with all documents, key ceremonies, rollover tools, and registrar key transition checklists. Operating since 2011 at PCH. Serves many ccTLDs. E.g., https://www.pch.net/resources/Papers/tld-dnssec-platform/tld-dnssec-platform.pdf

5. Advise and work with cryptech (open hardware security module) effort from prior to ICANN funding. Am responsible for design/build/test tamper detection system.

6. With help from NIC.BR built in 2FA system for class Registrar / Registry system to demonstrate importance and simplicity of 2FA security. Shared code with various participants. (ref recent Brazil bank issue)

RZM
Rick's Zone Manager

The Root Management

Token Information

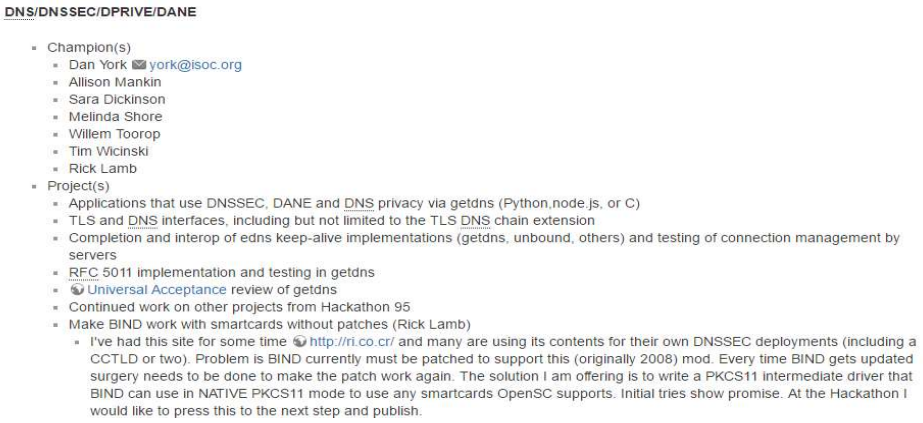
If not done so already, please download the Google Authenticator app onto your smartphone. Then use the information below to initialize the software token on your phone. This can be done by simply scanning the QR code below (reload the page if the scan cannot complete). Write down the "Token Key" for your records. Then enter the next token code and click "Procceed". On subsequent logins, append the changing token code to your password. If you are NOT ready to start using this two-factor authentication system or cannot get the Google Authenticator token working, leave the "Verification Code" field blank and click "Proceed". Once you have a token, click "Signup" next time you login to try again.

Domain name: FOO.
Token Key:
HOEEKTU4RB5VF7KN

Verification Code:
Proceed

Date: 13-APR-2017 04:48 UTC

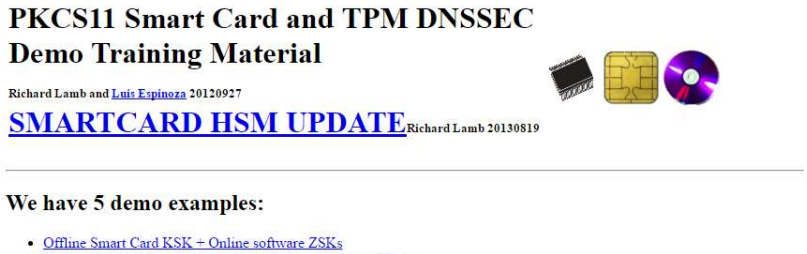
7. Since 2008 added smartcard support into industry standard nameserver BIND. Initially with patches to BIND (that were submitted). Then as with special PKCS11 shim driver that would work with any HSM/smartcard. Led to successfully convincing ISC to support after demonstrating at last IETF Hackathon. E.g., https://www.ietf.org/registration/MeetingWiki/wiki/doku.php?id=96hackathon



DNS/DNSSEC/DPRIVE/DANE

- Champion(s)
  - Dan York york@isoc.org
  - Allison Mankin
  - Sara Dickinson
  - Melinda Shore
  - Willem Toorop
  - Tim Wicinski
  - Rick Lamb
- Project(s)
  - Applications that use DNSSEC, DANE and DNS privacy via getdns (Python,node.js, or C)
  - TLS and DNS interfaces, including but not limited to the TLS DNS chain extension
  - Completion and interop of edns keep-alive implementations (getdns, unbound, others) and testing of connection management by servers
  - RFC 5011 implementation and testing in getdns
  - Universal Acceptance review of getdns
  - Continued work on other projects from Hackathon 95
  - Make BIND work with smartcards without patches (Rick Lamb)
    - I've had this site for some time http://ri.co.cr/ and many are using its contents for their own DNSSEC deployments (including a CCTLD or two). Problem is BIND currently must be patched to support this (originally 2008) mod. Every time BIND gets updated surgery needs to be done to make the patch work again. The solution I am offering is to write a PKCS11 intermediate driver that BIND can use in NATIVE PKCS11 mode to use any smartcards OpenSC supports. Initial tries show promise. At the Hackathon I would like to press this to the next step and publish.

8. Published results of using smartcards as an alternative to HSMs for DNSSEC research. Resulting in release of bootable DVDs and complete key ceremony scripts and other documentation. Popular with ccTLDs and used by NIC.CR and others. E.g., http://ri.co.cr/



PKCS11 Smart Card and TPM DNSSEC Demo Training Material

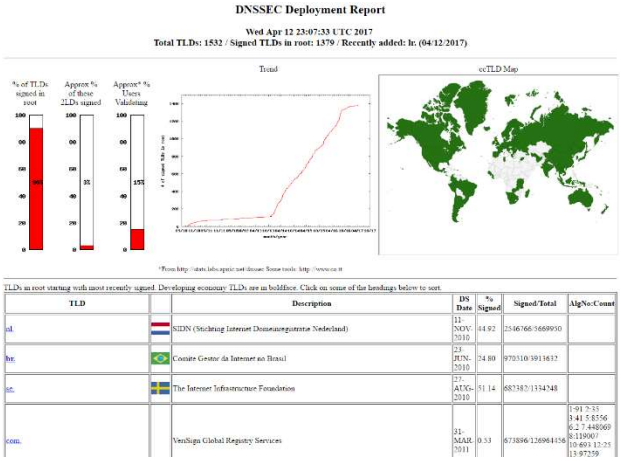
Richard Lamb and Luis Espinoza 20120927

SMARTCARD HSM UPDATE Richard Lamb 20130819

We have 5 demo examples:

- Offline Smart Card KSK + Online software ZSKs
- Offline HSM KSK + Online software ZSKs using fake HSM
- Offline Smart Card KSK + Online Smart Card ZSKs
- Online Smart Card KSK + ZSKs + BIND 9.9 in-line signing
- Online TPM KSK + ZSKs + BIND 9.9 in-line signing

9. Designed/Built/Deployed and maintain DNSSECSTAT since 2010. Referenced and relied on by IGF, ISOC and community since 2010. E.g., https://rick.eng.br/dnssecstat/ (also organized and ran an IGF panel)



DNSSEC Deployment Report

Wed Apr 12 23:07:33 UTC 2017
Total TLDs: 1532 / Signed TLDs in root: 1379 / Recently added: hr. (04/12/2017)

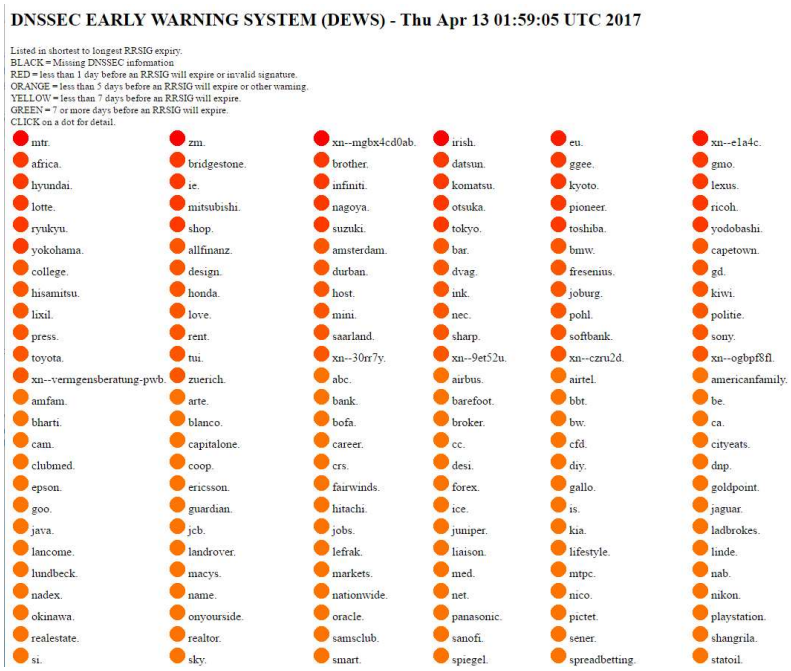
Trend

ccTLD Map

TLDs in root starting with most recently signed. Developing economy TLDs are in boldface. Click on some of the headings below to sort.

TLD		Description	DS Date	% Signed	Signed/Total	Alg/No./Count
nl		SIDN (Stichting Internet Domeinregistratie Nederland)	11-NOV-2010	44.92	2546766/5668930	
br		Comite Gestor da Internet no Brasil	23-JUN-2010	24.80	970310/3913632	
se		The Internet Infrastructure Foundation	27-AUG-2010	51.14	683382/1334748	
com		VeriSign Global Registry Services	31-MAR-2011	0.33	673896/126964158	13-91 7:33 13-41 5:8556 8-2 7:448069 8:119007 10-691 12:25 13:97259

10. Designed/Built/Deployed and maintain TLD Early Warning System in 2010. Auto email warnings. Used often to notify ccTLDs of (impending) failure. E.g., http://www.dnssek.info/

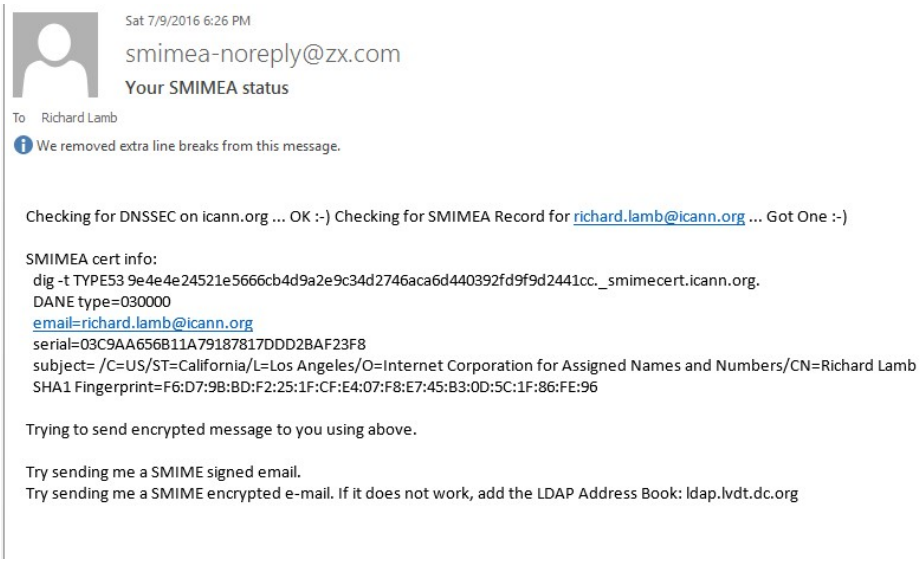


DNSSEC EARLY WARNING SYSTEM (DEWS) - Thu Apr 13 01:59:05 UTC 2017

Listed in shortest to longest RRSIG expiry.
BLACK = Missing DNSSEC information
RED = less than 1 day before an RRSIG will expire or invalid signature.
ORANGE = less than 5 days before an RRSIG will expire or other warning.
YELLOW = less than 7 days before an RRSIG will expire.
GREEN = 7 or more days before an RRSIG will expire.
CLICK on a dot for detail.

mtr.	zm.	xn--mgbx4cd0ab.	irish.	eu.	xn--e1a4c.
africa.	bridgestone.	brother.	datsun.	ggee.	gmo.
hyundai.	ie.	infiniti.	komatsu.	kyoto.	lexus.
lotte.	mitsubishi.	nagoya.	otsuka.	pioneer.	ricoh.
ryukyu.	shop.	suzuki.	tokyo.	toshiba.	yodobashi.
yokohama.	allfinanz.	amsterdam.	bar.	bmw.	capetown.
college.	design.	durban.	dvag.	fresenius.	gd.
hisamitsu.	honda.	host.	ink.	joburg.	kiwi.
lixil.	love.	mini.	nec.	pohl.	politie.
press.	rent.	saarland.	sharp.	softbank.	sony.
toyota.	tui.	xn--30rr7y.	xn--9et52u.	xn--czru2d.	xn--ogbpf8fl.
xn--vermgensberatung-pwb.	zuerich.	abc.	airbus.	airtel.	americanfamily.
amfam.	arte.	bank.	barefoot.	bbt.	be.
bharti.	blanco.	bofa.	broker.	bw.	ca.
cam.	capitalone.	career.	cc.	cfd.	cityeats.
clubmed.	coop.	crs.	desi.	diy.	dnp.
epson.	ericsson.	fairwinds.	forex.	gallo.	goldpoint.
goo.	guardian.	hitachi.	ice.	is.	jaguar.
java.	jcb.	jobs.	juniper.	kia.	ladbrokes.
lancome.	landrover.	lefrak.	liaison.	lifestyle.	linde.
lundbeck.	macys.	markets.	med.	mtpc.	nab.
nadex.	name.	nationwide.	net.	nico.	nikon.
okinawa.	onyourside.	oracle.	panasonic.	pictet.	playstation.
realestate.	realtor.	samsclub.	sanofi.	sener.	shangrila.
si.	sky.	smart.	spiegel.	spreadbetting.	statoil.

11. Designed/Built/Deployed and maintain SMIME-DNSSEC email auto-responder to encourage deployment of the next killer app:email e.g., smimea@zx.com



Sat 7/9/2016 6:26 PM

smimea-noreply@zx.com

Your SMIMEA status

To Richard Lamb

We removed extra line breaks from this message.

Checking for DNSSEC on icann.org ... OK :-) Checking for SMIMEA Record for richard.lamb@icann.org ... Got One :-)

SMIMEA cert info:
dig -t TYPE53 9e4e4e24521e5666cb4d9a2e9c34d2746aca6d440392fd9f9d2441cc._smimecert.icann.org.
DANE type=030000
email=richard.lamb@icann.org
serial=03C9AA656B11A79187817DDD2BAF23F8
subject= /C=US/ST=California/L=Los Angeles/O=Internet Corporation for Assigned Names and Numbers/CN=Richard Lamb
SHA1 Fingerprint=F6:D7:9B:BD:F2:25:1F:CF:E4:07:F8:E7:45:B3:0D:5C:1F:86:FE:96

Trying to send encrypted message to you using above.

Try sending me a SMIME signed email.
Try sending me a SMIME encrypted e-mail. If it does not work, add the LDAP Address Book: ldap.lvdt.dc.org

12. Built system to support CDS experimentation in support of interesting opportunity to simplify and further secure the DNS with DNSSEC.

13. Web site to generate DNSSEC DANE TLSA records to support TLSA deployment. E.g., https://www.co.tt/tlsa4www.cgi

TLSA4WWW

Calculate TLSA for Web Site
Version 0.01.

web site FQDN: Calculate

Date: 13-APR-2017 05:10 UTC

14. Web site to generate DNSSEC DS records to support DNSSEC deployment. https://www.co.tt/ds4dn.cgi

DS4DN

Calculate DS for Domain Name
Version 0.01.

Domain Name:
[OPT]Nameserver: Calculate

Date: 13-APR-2017 05:12 UTC

15. Web site showing daily updated stats on TLD DNSSEC validity period, key sizes, algorithm to help in deployment decisions. E.g., https://www.co.tt/dnssec_scan_val.html
16. Built and maintain list of Registrars supporting DNSSEC (2010). E.g., https://www.icann.org/resources/pages/deployment-2012-02-25-en

Resources

- About ICANN
  - Learning
  - Participate
  - President's Corner
  - ICANN Management Organization Chart
  - Staff
  - Careers
- In Focus
  - Continuity
  - DNSSEC
    - Standards
    - IANA DNSSEC Root Information
    - TLD DNSSEC Report
    - Root Deployment
    - Registrar Deployment
    - Deployment Map
    - Deployment Graph

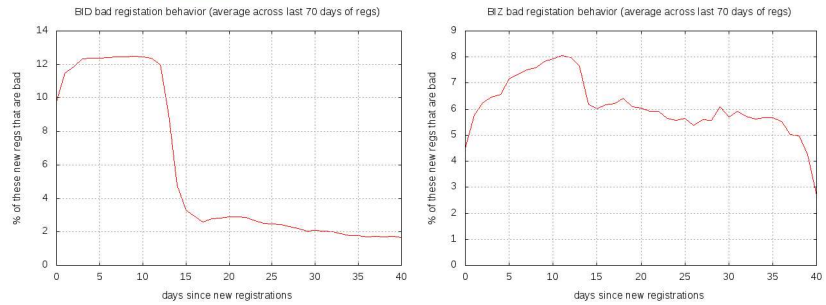
Deploying DNSSEC

Registrars that support end user DNSSEC management, including entry of DS records

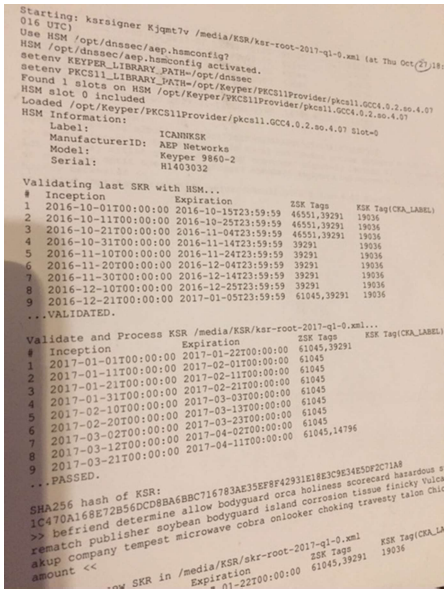
Last updated: 20 May 2016

Registrar	Accepts DS records for	Notes
123domain.eu (DE)	.com .net .org .at .be .ch .cz .de .eu .fr .li .lu .me .se	(1) (2)
AB Name ISP (SE)	.be .biz .com .eu .net .org .se .us	(1) (2)
BigRock (IN)	.com .in .me .net .org	(2) More info at http://manage.bigrock.in/kb/answer/1907
Binero (SE)	.se .eu	All domains are automatically signed. (1) (2)
BIT B.V. (NL)	.com .net .org .nl .be .de .eu .info .biz	(1) (DS via email)
CPS-Datensysteme GmbH (DE)	.at .biz .ch .com .de .eu .info .li .net .org	
CSC Corporate	.com .net org .uk .biz .com.au .net.au .us .eu .be .se .co	

17. Guided by Dave P, built system to track badness in new nTLDs registrations based on blocklists and whois data. E.g. (one of many) https://www.co.tt/badregs/



18. Designed/Built/Deployed and maintain all KSK root software (still!) and test routines. Also created and instituted the TCR approach to ensure trust in a multi-stakeholder environment. Architected whole root KSK system down to safe selection and key ceremonies. Pushing PTI to reduce risk by funding other avenues.



19. Designed/Built/Deployed and maintained live Root DNSSEC testbed that was anycasted and used by large ISP for testing. (2008)
20. Numerous direct engineering assistance to ccTLDs including NP TZ CR …