Overview of Open Source Tools for DNSSEC

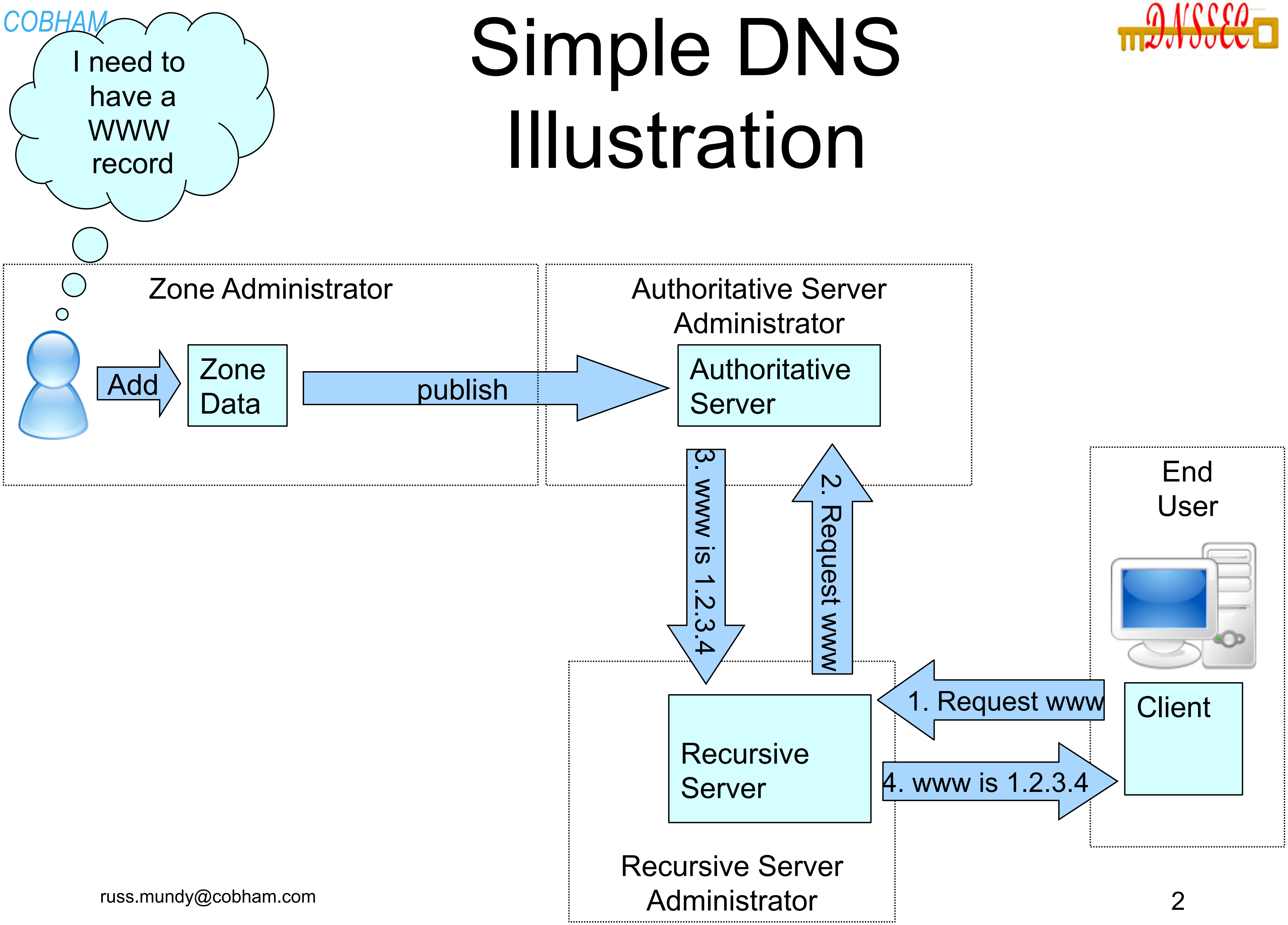
Russ Mundy

Cobham Analytic Solutions

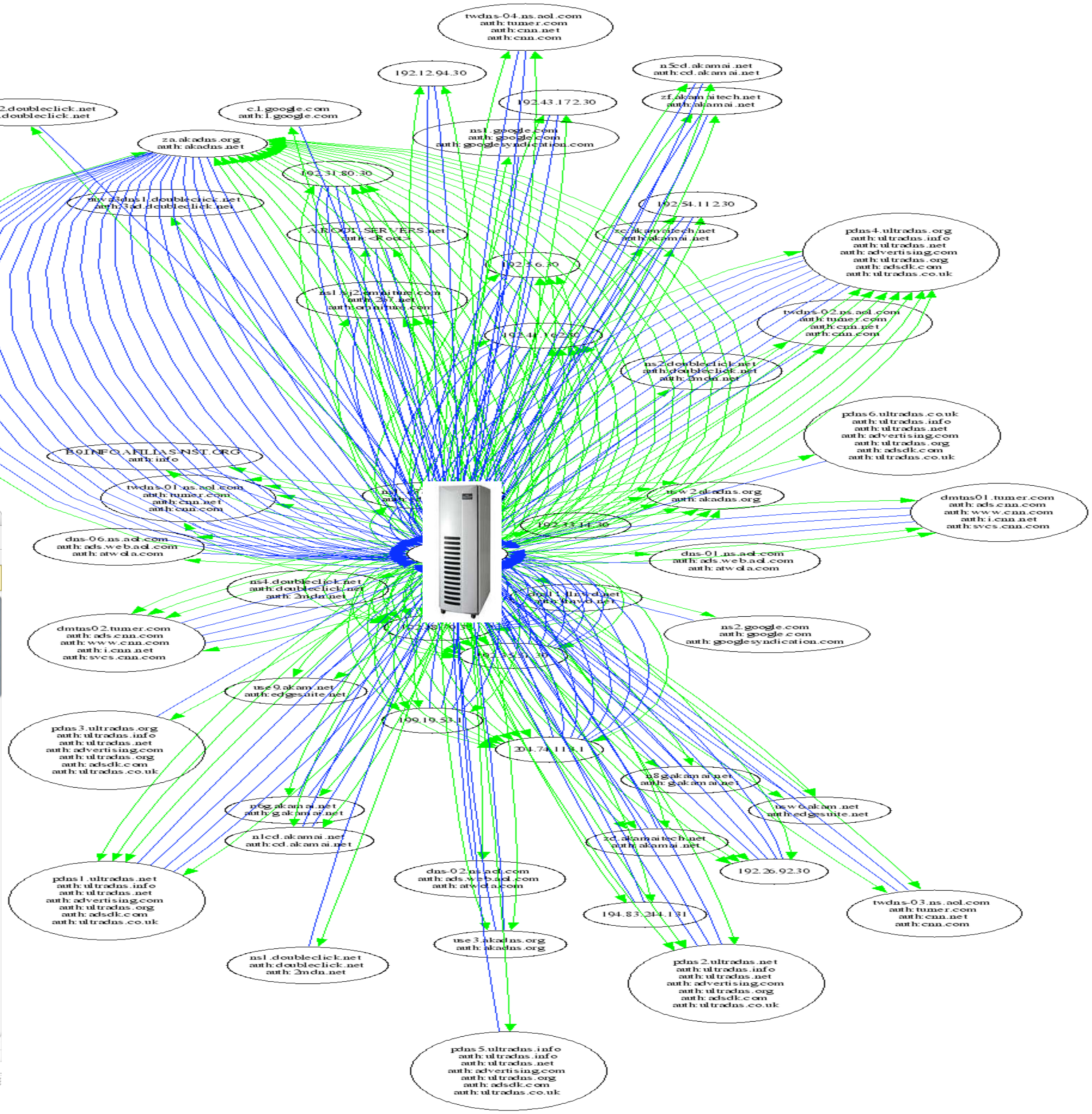
(aka: SPARTA, Inc.)

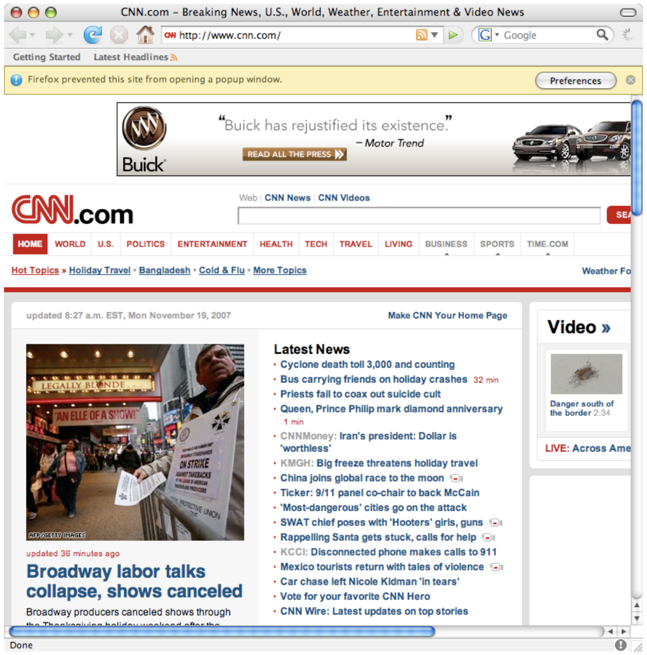
June 23, 2010

Simple DNS Illustration



1 Webpage = Multiple DNS Name Resolutions




CNN.com – Breaking News, U.S., World, Weather, Entertainment & Video News

http://www.cnn.com/

Getting Started Latest Headlines

Firefox prevented this site from opening a popup window.

Hot Topics » Holiday Travel • Bangladesh • Cold & Flu • More Topics Weather Fo

updated 8:27 a.m. EST, Mon November 19, 2007 Make CNN Your Home Page

updated 36 minutes ago

Broadway labor talks collapse, shows canceled

Broadway producers canceled shows through the Thanksgiving holiday weekend after the

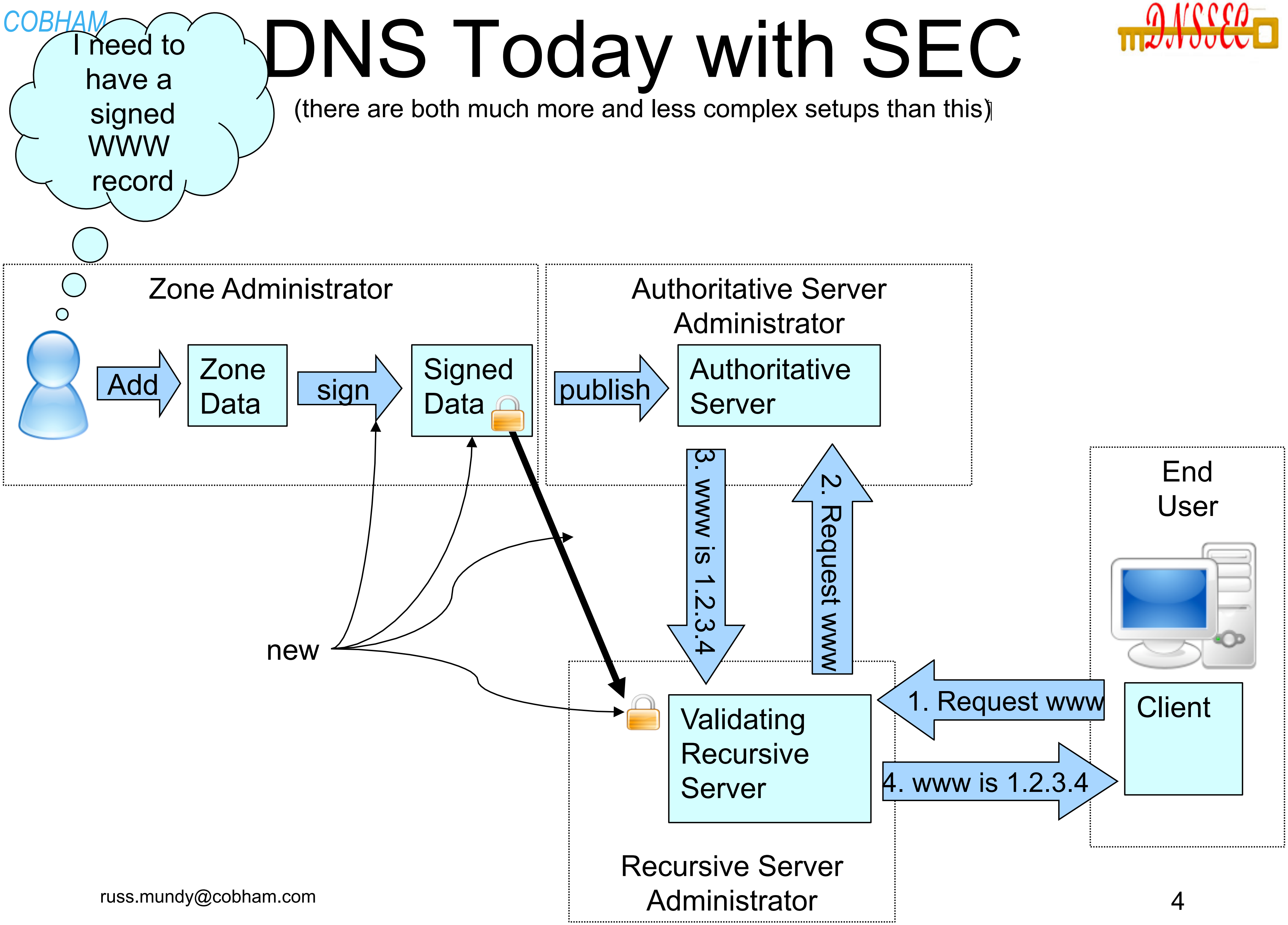
Latest News

- Cyclone death toll 3,000 and counting
- Bus carrying friends on holiday crashes 32 min
- Priests fail to coax out suicide cult
- Queen, Prince Philip mark diamond anniversary 1 min
- CNNMoney: Iran's president: Dollar is 'worthless'
- KMGH: Big freeze threatens holiday travel
- China joins global race to the moon
- Ticker: 9/11 panel co-chair to back McCain
- 'Most-dangerous' cities go on the attack
- SWAT chief poses with 'Hooters' girls, guns
- Rappelling Santa gets stuck, calls for help
- KCCI: Disconnected phone makes calls to 911
- Mexico tourists return with tales of violence
- Car chase left Nicole Kidman 'in tears'
- Vote for your favorite CNN Hero
- CNN Wire: Latest updates on top stories

Danger south of the border 2:34

DNS Today with SEC

(there are both much more and less complex setups than this)



I need to have a signed WWW record

Zone Administrator

Add

Zone Data

sign

Signed Data

publish

Authoritative Server Administrator

Authoritative Server

3. www is 1.2.3.4

2. Request www

new

End User

Client

1. Request www

4. www is 1.2.3.4

Validating Recursive Server

Recursive Server Administrator

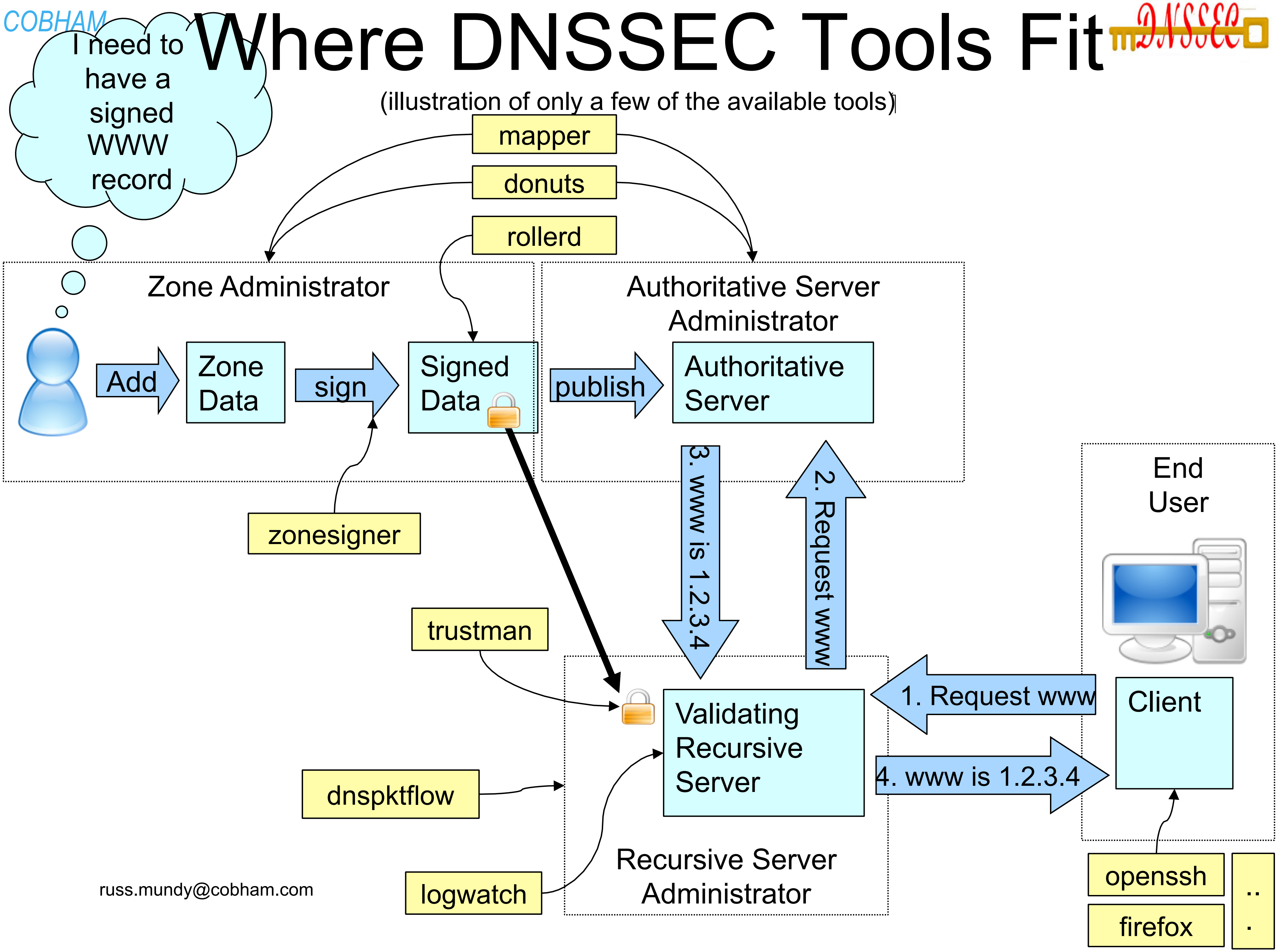
Available Resources

- Various categories of resources are available
  - Tools for zone data administration
  - Tools for secure delegation registration
  - Tools for supporting operations at the validating systems including DNSSEC-capable applications
  - Developer resources
  - Operator guidance documentation
- Some of the available tools are catalogued at https://www.dnssec-deployment.org/index.php/learning-center/survey/
- Existing tools have broad coverage

COBHAM

Where DNSSEC Tools Fit

(illustration of only a few of the available tools)



russ.mundy@cobham.com

Wide Range of Tools

- Taking full advantage of DNSSEC capabilities will occur gradually over time
- Adding DNSSEC capabilities to various DNS related functions will occur gradually
- Large number of tools available
  - Existing tools continue to evolve
  - New tools and capabilities continue to appear

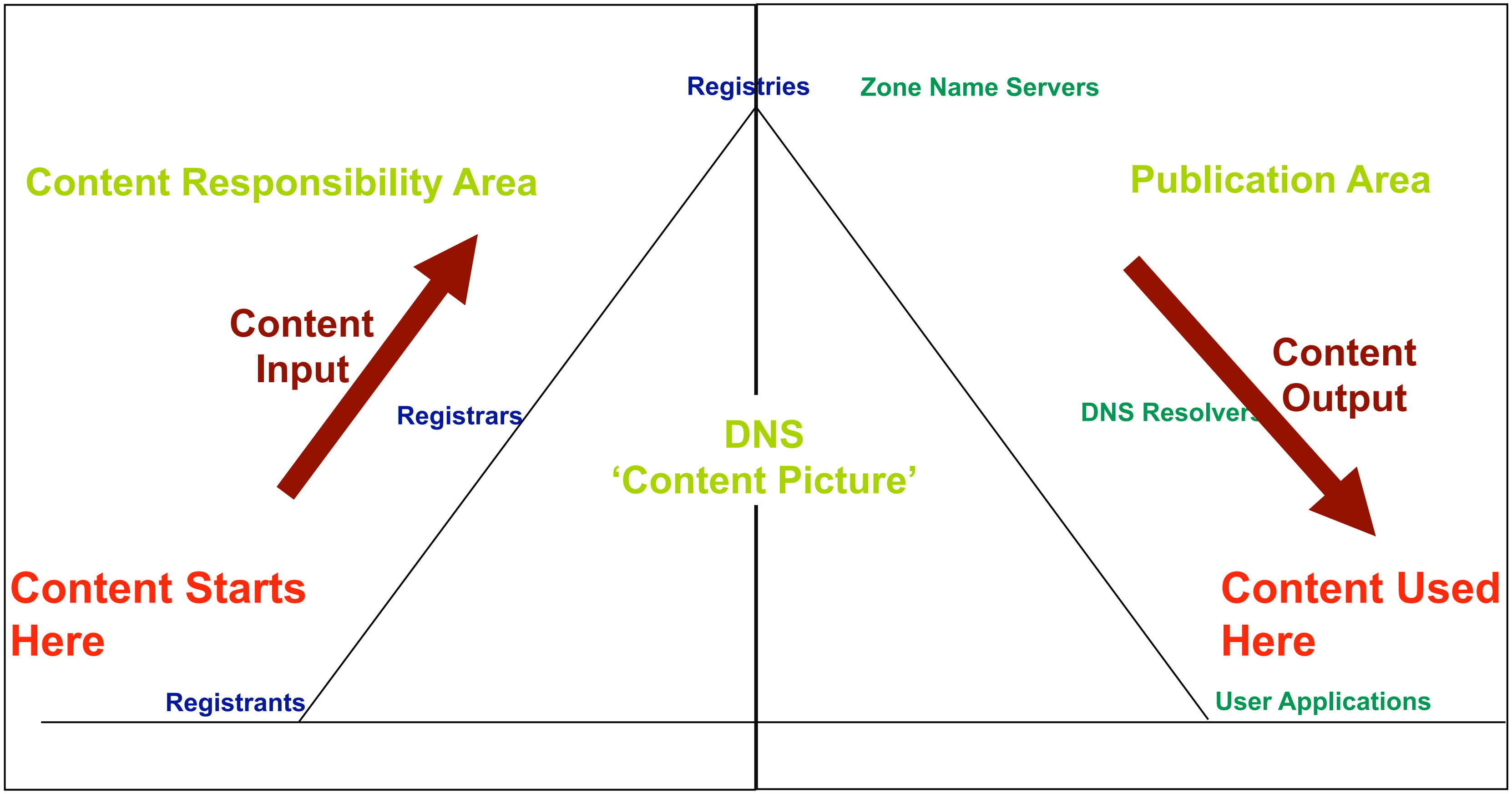
Comments or Questions?

(If time permits)

Questions, comments and other feedback can be sent to
russ.mundy@cobham.com

Backup Slides

DNS Content MATTERS



Resources for Zone Administration

Name Servers

BIND	Authoritative, validating, recursive, and caching open source name server implementation	ISC	www.isc.org
NSD	Authoritative only, open source name server	NLNet Labs	http://www.nlnetlabs.nl/nsd
UNBOUND	Validating, recursive and caching open source name server	NLNet Labs, Verisign, Nominet, Kirei	http://unbound.net/

Key Generation and Zone Signing

dnssec-keygen, dnssec-signzone	Standard tools provided with the BIND distribution	ISC	http://www.isc.org
jdnssec-keygen, jdnssec-signzone	Tools from the jdnssec-tools suite	Verisign Labs	http://www.verisignlabs.com/dnssec-tools/
ldns-keygen, ldns-signzone	Tools from the ldns tool suite	NLNet Labs	http://www.nlnetlabs.nl/ldns/
pdnssec-keygen, pdnssec-signzone,	Tools from the DNSSEC perltools distribution	Roy Arends	http://www.nsec3.org/cgi-bin/trac.cgi/browser/dnssec/perltools/
zonesigner	Wrapper around BIND tools, available in the dnssec-tools suite	Cobham	http://www.dnssec-tools.org/wiki/index.php/Zonesigner
dnssec-zkt and dnssec-signer -	Wrapper around BIND tools	HZNET	http://www.hznet.de/dns/zkt/
ldns-zsplit and ldns-zcat	Tool from the ldns package for enabling parallel signing a large zone	NLNetLabs	http://www.nlnetlabs.nl/ldns/
maintkeydb, dnssigner	Tools from the DNSSEC Key Management Tools suite	RIPE NCC	https://www.ripe.net/projects/disi/dnssec_maint_tool/
OpenDNSSEC	Open-source turn-key solution for DNSSEC	Collaborative effort, see website	http://www.opendnssec.org

Key Rollover

Rollerd and rollctl	Tool from the dnssec-tools package for managing different phases of ZSK and KSK rollover	Cobham	http://www.dnssec-tools.org/wiki/index.php/Rollerd
Maintkeydb	Command line interface to a database containing DNSSEC Keys	RIPE NCC	https://www.ripe.net/projects/disi/dnssec_maint_tool/
OpenDNSSEC	Open source turn-key solution for DNSSEC	Collaborative effort, see website	http://www.opendnssec.org

Hardware Interface

DNSSEC Smartcard Utility	Supports operations for storing keys to Any PKCS#15 smartcard supported by OpenSC and exporting them as DNSSEC records	.SE	http://opensource.iis.se/trac/dnssec/browser/pkcs15-dnssec
pkcs11HSMtools	Modifications to BIND for native PKCS-11 HSM support	IANA	http://www.xtcn.com/~lamb/pkcs11HSMtools.tar.gz
Software for interfacing with crypto hardware	EVP Perl Implementation	Nominet	www.nominet.com

Zone Troubleshooting

SZIT monitor extension	Tests the zone contents against best common practices and overall security	NIST	http://snad.ncsl.nist.gov/dnssec/
donuts and donutsd	A dnslint like application available in the dnssec-tools suite, for analyzing zone files.	Cobham	http://www.dnssec-tools.org/wiki/index.php/Donuts
Mapper	Tool in the dnssec-tools suite that maps DNS realms, color coding the results to allow for easy visual interpretation of the results	Cobham	http://www.dnssec-tools.org/wiki/index.php/Mapper
jdnssec-verifyzone	Verifies all of the signatures in a zone for cryptographic validity	Verisign Labs	http://www.verisignlabs.com/dnssec-tools/
named-checkzone	Standard tool provided with the BIND distribution	ISC, BIND	www.isc.org

Resources for Creating Secure Delegations

DS Record Creation

dnssec-dstool	simple tool for generating DS (or DLV) records from DNSKEY records	Verisign Labs	http://www.verisignlabs.com /dnssec-tools/
ldns-key2dns	DNSKEY to DS conversion	NLNet Labs	http://www.nlnetlabs.nl/ldns/
Key2ds, Net::DNS::Sec	DNSKEY to DS conversion	Olaf Kolkman	http://www.net-dns.org/

Update to Parent

Regsoft	Front-end for updating contents of a registry	Shinkuro, Inc	
CADR	registrar software that can move keys from sub-zones to parent zones	Afilias, Shinkuro, SPARTA, EP.net	http://cadr.rs.net/
libepp-nicbr	library that partially implements the Extensible Provisioning Protocol (EPP), as described in the Internet Drafts RFC3730bis to RFC3734bis and RFC3735	NIC.br	http://registro.br/epp/index-EN.html

Resources for Validating Systems

Fetching Key Information

ISC DLV registry	Trust Anchor Repository constructed through explicit zone owner registration	ISC	https://secure.isc.org/index.pl?/ops/dlv/
Secspider	Trust Anchor Repository populated by a crawler program	UCLA, Colorado State	http://secspider.cs.ucla.edu/
IKS Jena Survey	Trust Anchor Repository populated by a crawler program	IKS Jena	http://www.iks-jena.de/leistungen/dnssec.php
IANA TAR	(Currently) demo Trust Anchor Repository for SEP keys for TLDs	IANA	https://ns.iana.org/dnssec/status.html
ldns-keyfetcher	queries and retrieves DNSKEYs for a given domain	NLNet Labs	http://www.nlnetlabs.nl/ldns/
getdnskeys	Tool in the dnssec-tools suite for fetching, comparing and remembering a list of DNSKEYs from DNS zones	Cobham	www.dnssec-tools.org

Automated TA Rollover

trustman	Implementation of RFC 5011 for automated rollover of trust anchors in validating resolvers. Tool available in the dnssec-tools distribution	Cobham	http://www.dnssec-tools.org/wiki/index.php/Trustman

Troubleshooting

dig	Standard tool provided with the BIND software	ISC	www.isc.org
drill	Debugging/query tool for DNSSEC, similar to dig	NLNet Labs	http://www.nlnetlabs.nl/ldns/
validate	A tool that helps determine the validation status for a DNS record and the reasons for validation failure if any	Cobham	http://www.dnssec-tools.org/wiki/index.php/Validate
dnspktflow	This tool, when combined with tethereal and graphviz, can trace tcpdump/tethereal network packet captures to visually diagram dns packet flows	Cobham	http://www.dnssec-tools.org/wiki/index.php/Dnspktflow
Traffic Monitoring Tool	Tool to capture and analyze DNS traffic to and from a name server	NIST	http://snad.ncsl.nist.gov/dnssec/
dnsdump	Perl script that captures and displays DNS packets seen on the network	The Measurement Factory	http://dns.measurement-factory.com/tools/dnsdump/
dnscap	network capture utility designed specifically for DNS traffic	OARCI	http://public.oarci.net/tools/dnscap
Logwatch	Configuration plugin to have logwatch perform DNSSEc parsing of system logging messages from running BIND name serverq	Plugin provided by Cobham available in the logwatch distribution	http://www2.logwatch.org:81/

DNSSEC Aware Applications

DNSSEC Capable Applications

Firefox	patch that enables DNSSEC checking of DNS lookups done with Firefox	Cobham	http://www.dnssec-tools.org/wiki/index.php/Firefox
Firefox Addon	Checks DNSSEC validity of DNS portion of url bar	Cz nic Labs	https://addons.mozilla.org/en-US/firefox/addon/64247
Thunderbird	patch that enables DNSSEC validation in the Thunderbird mail app	Cobham	http://www.dnssec-tools.org/wiki/index.php/Thunderbird
SSH	patch that contains support for local DNSSEC validation for all DNS lookups	Cobham	http://www.dnssec-tools.org/wiki/index.php/Ssh
Sendmail	patch for adding DNSSEC validation support during lookups	Cobham	http://www.dnssec-tools.org/wiki/index.php/Sendmail
Postfix	patch for adding DNSSEC validation support during lookups	Cobham	http://www.dnssec-tools.org/wiki/index.php/Postfix
libsf2	patch for adding DNSSEC validation support during lookups and adding a new field in the mail header based on the results of the checks	Cobham	http://www.dnssec-tools.org/wiki/index.php/LibSPF
wget	patch to enable DNSSEC validation in wget	Cobham	http://www.dnssec-tools.org/wiki/index.php/Wget
ncftp	patch to enable DNSSEC validation during lookups	Cobham	http://www.dnssec-tools.org/wiki/index.php/Ncftp
proftpd	patch to enable DNSSEC validation during lookups	Cobham	http://www.dnssec-tools.org/wiki/index.php/Proftpd

Developer Resources

Validation Libraries

libval	A C library that provides interfaces for name lookup with DNSSEC validation support.	Cobham	http://www.dnssec-tools.org/docs/tool-description/libval.html
libval_shim	LD_PRELOAD-based approach for transparently adding DNSSEC capability to existing applications	Cobham	http://www.dnssec-tools.org/docs/tool-description/libval_shim.html
ldns library	A C library that provides validation capability	NLNet Labs	http://www.nlnetlabs.nl/ldns/
libunbound	A C library that can be linked against applications to provide validation capability	NLNet Labs, Verisign, Nominet, Kirei	http://unbound.net/

Perl SDKs

Net::DNS::SEC	Extension to Net::DNS with DNSSEC functionality	RIPE NCC	http://www.net-dns.org/
Net::DNS::SEC::Tools	Tools and modules that provide zone signing and key management configuration utilities.	Cobham	http://www.dnssec-tools.org/
Net::DNS::ZoneFile::Fast	provides the ability to parse zone files that BIND8 and BIND9 use, fast.	Anton Berezin and Cobham	http://search.cpan.org/dist/Net-DNS-ZoneFile-Fast/Fast.pm

Validator API

DNSSEC Validator API	Proposed API between applications and security aware validating stub resolvers	Cobham	http://tools.ietf.org/id/draft-hayatnagarkar-dnsext-validator-api-06.txt
libunbound API	API provided by the libunbound library	NLNet Labs, Verisign, Nominet, Kirei	http://www.unbound.net/documentation/index.html

Testing Resources

maketestzone	useful for generating test data which DNSSEC aware software can be tested against	Cobham	www.dnssec-tools.org
Querysim	A DNS traffic replay tool	NIST	http://snad.ncsl.nist.gov/dnssec/
Packet Server	A tool that helps crafting packets with various settings to test the behavior of validating resolvers	Roy Arends	http://www.nsec3.org/cgi-bin/trac.cgi/browser/dnssec/perltools/

Deployment Aids

Operator Guidance Documentation

NIST Special Publication 800-81	Recommendations of the National Institute of Science and Technology, Deployment Guide	NIST	http://csrc.nist.gov/publications/nistpubs/
RFC 4641	DNSSEC Operational Practices	IETF	http://www.ietf.org/rfc/rfc4641.txt
Step-by-Step guides	Guides for signed zone operation	Cobham	http://www.dnssec-tools.org/resources/documentation.html
DNSSEC Howto	A tutorial in disguise	NLNet Labs	http://www.nlnetlabs.nl/dnssec_howto/

Survey of DNSSEC Tools

https://www.dnssec-deployment.org/index.php/learning-center/survey/

DNSSEC Resources

- Cobham (SPARTA) DNSSEC Project page
  - http://www.dnssec-tools.org
  - Tools, Applications, Step-by-step guides.
- DNSSEC Deployment Working Group
  - http://www.dnssec-deployment.org
  - Mailing list: dnssec-deployment@dnssec-deployment.org
- NIST DNSSEC Project page
  - http://www-x.antd.nist.gov/dnssec
  - Links to NIST tools & SNIP effort
- Secure Naming Infrastructure Pilot
  - http://www.dnsops.gov
  - Distributed test domain/training pilot