

So I own a nameserver... What do I do now??

Russ Mundy

Co-Chair DNSSEC Initiative

Cobham Analytic Solutions

(aka: SPARTA, Inc.)

December 6, 2010

DNS Basic Functions

- DNS provides the translation from names to network addresses
- Get the right DNS content to Internet users

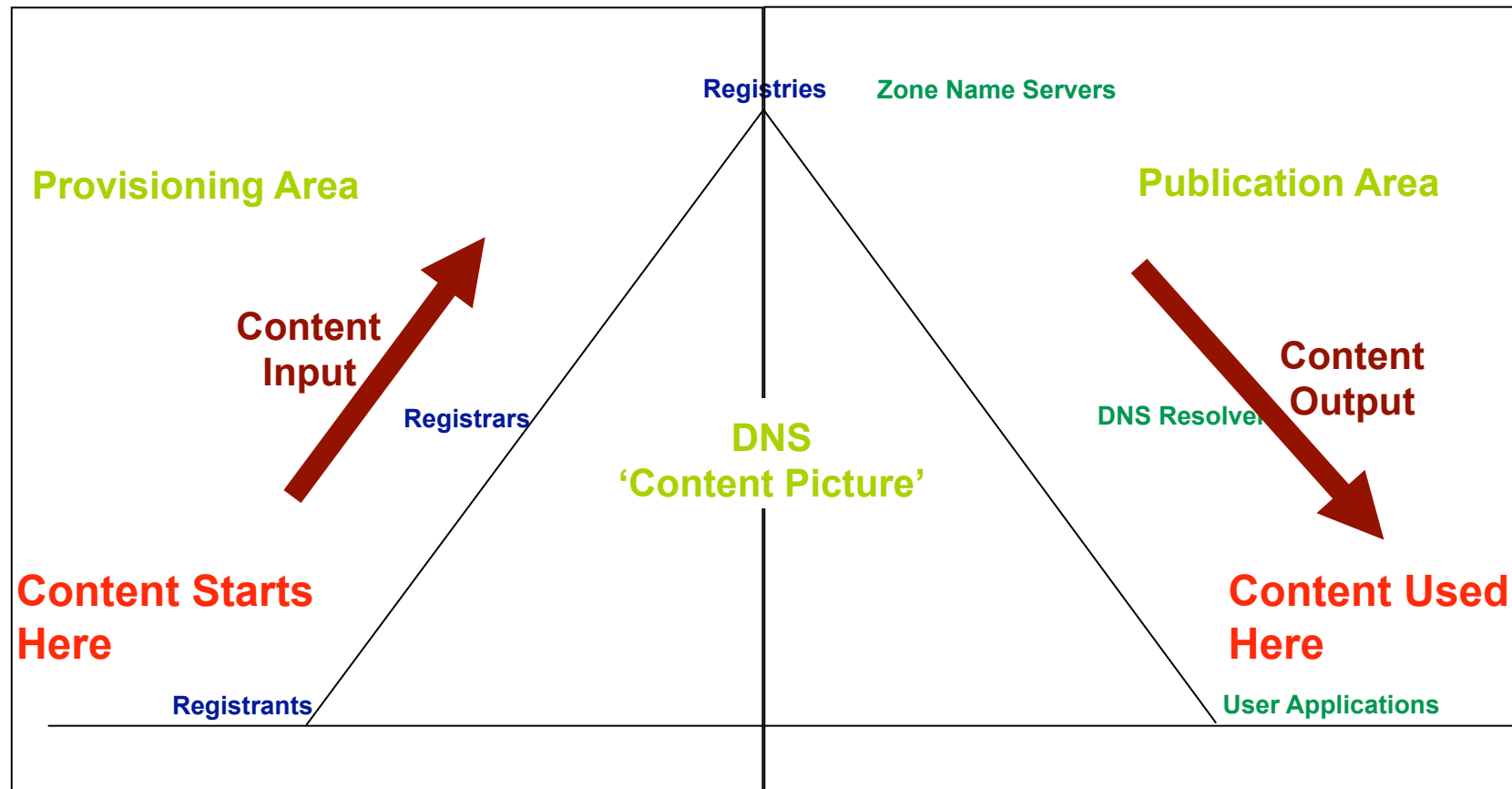
➤ IT'S DNS CONTENT THAT MATTERS!

How Does DNSSEC Fit?

- DNSSEC required to thwart attacks on DNS CONTENT
 - DNS attacks used to attack Internet users applications
- Protect **DNS CONTENT** as much as (or more than) any DNSSEC information
 - Including DNSSEC private keys!!

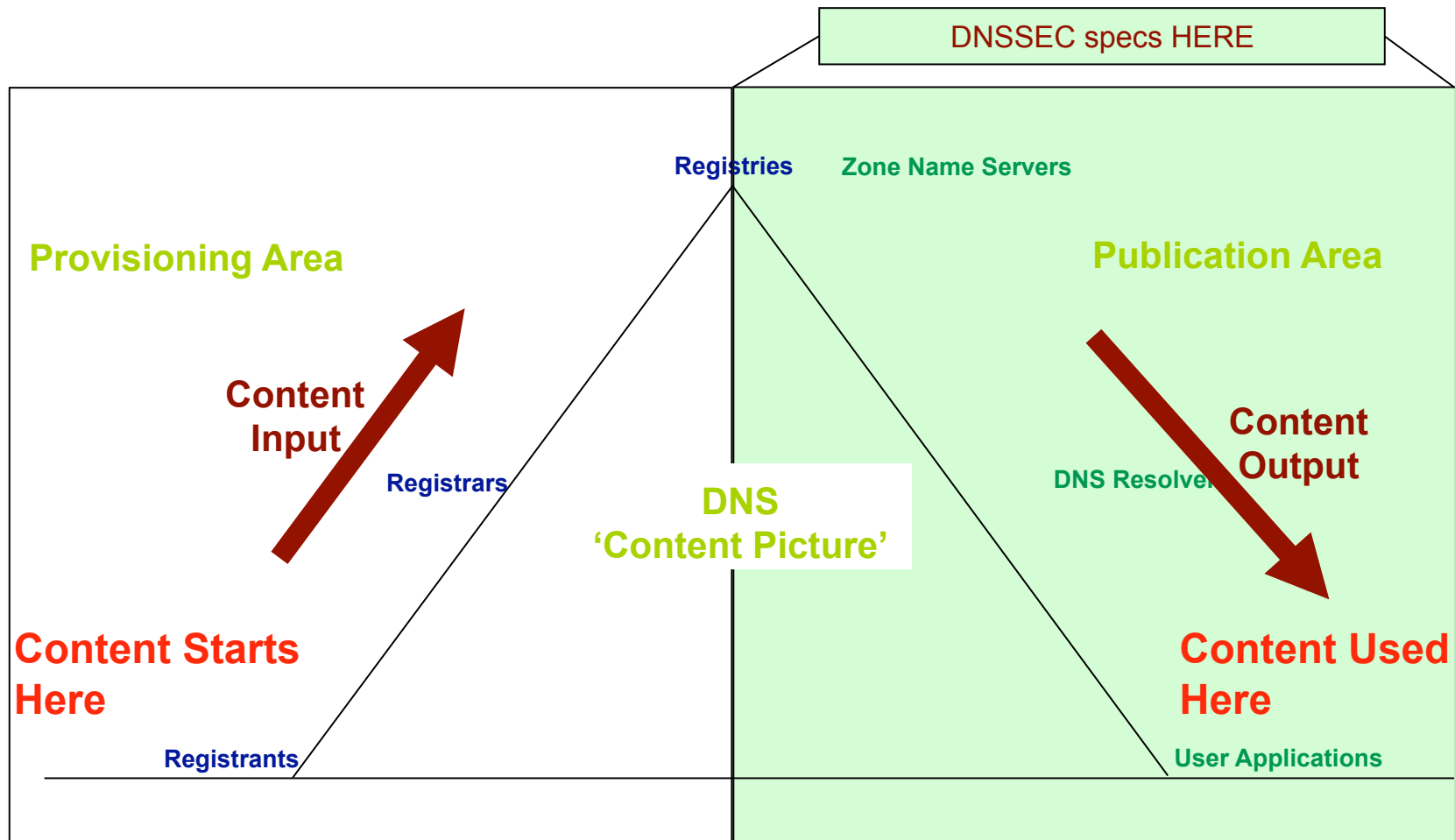
DNS Zone Content Flow

(for example, www.icann.org)

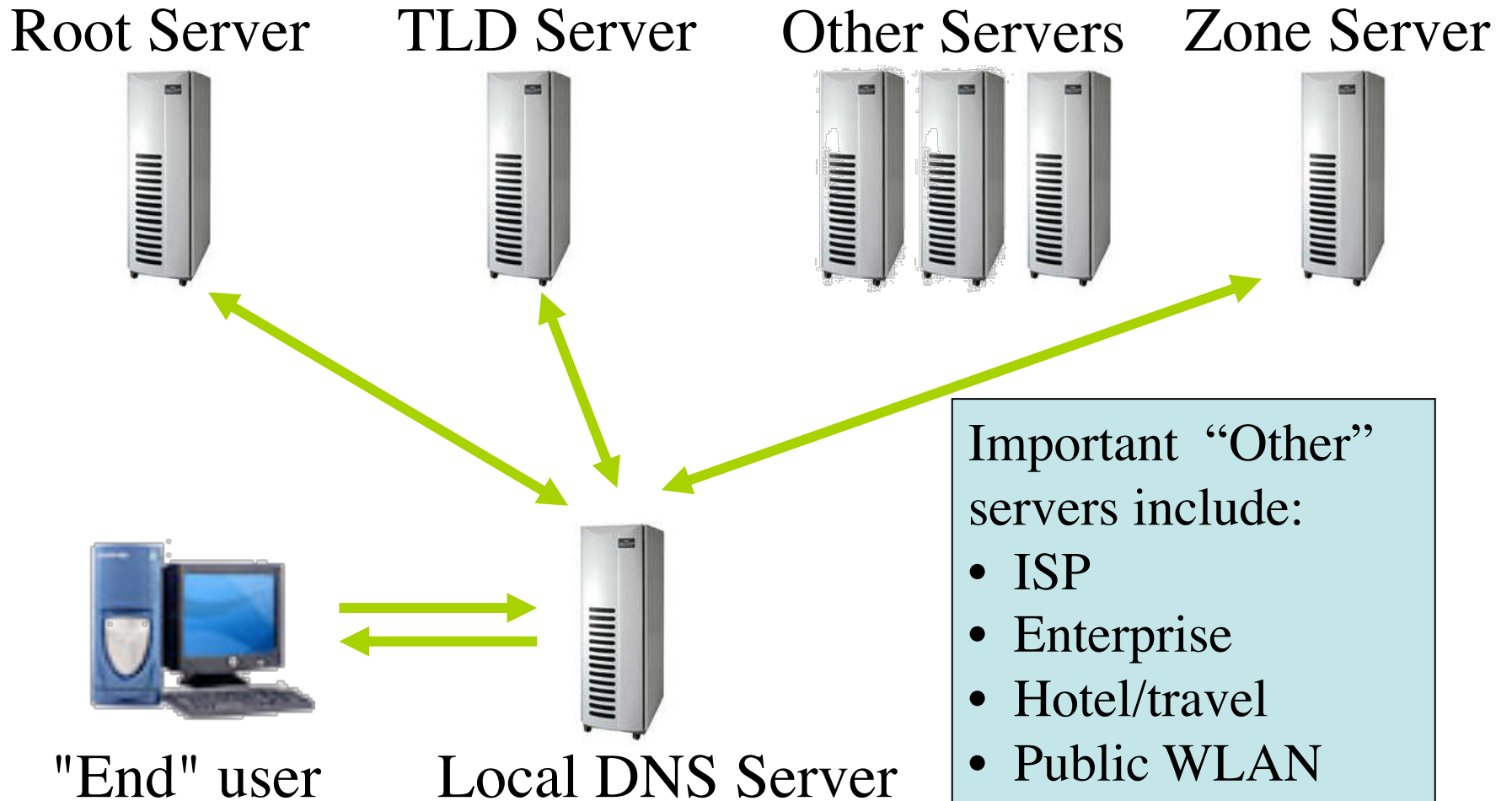


DNS Zone Content Flow

(for example, www.icann.org)



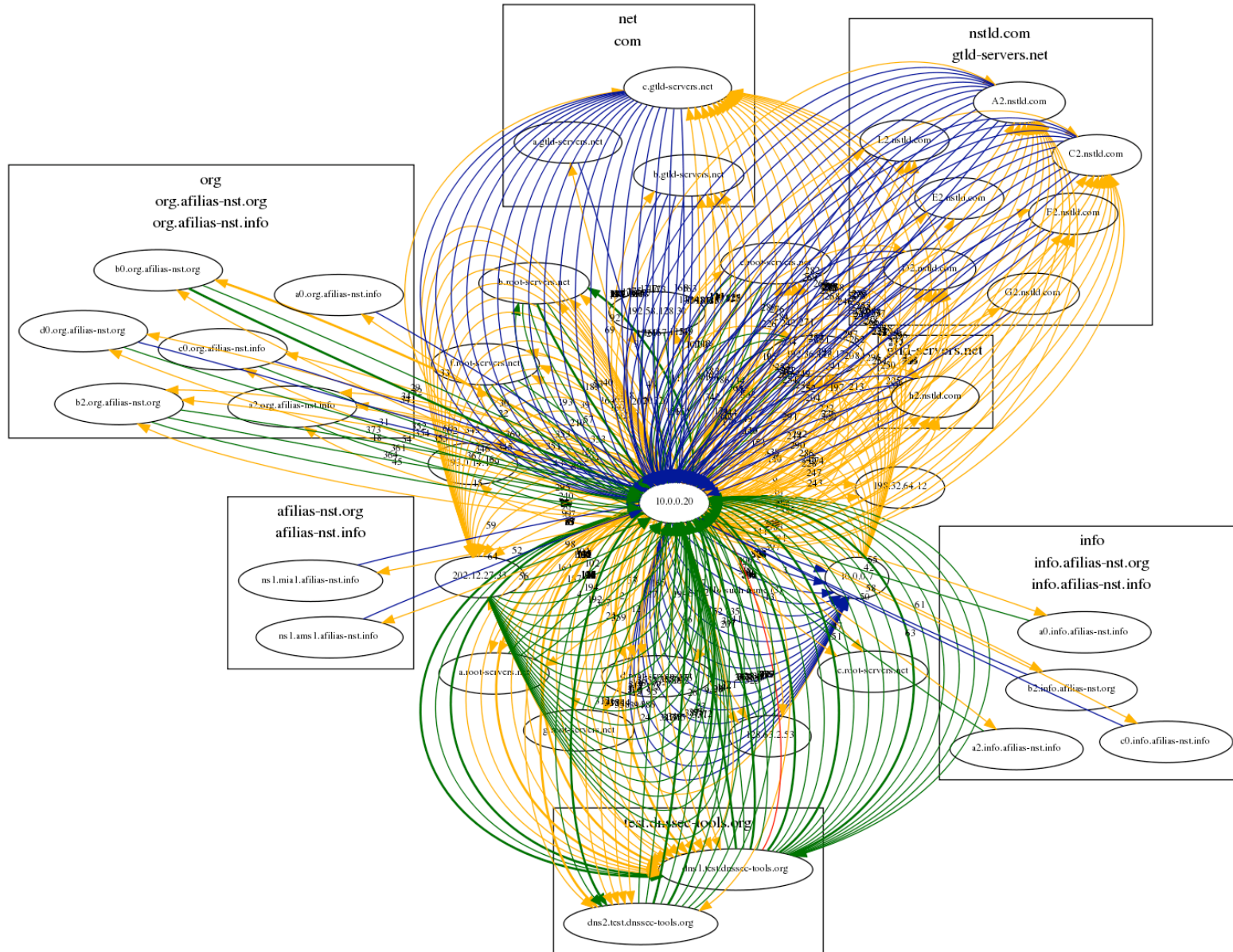
DNS Name Resolution



As owner of a nameserver ...

- But I just have a web site with one name ...
 - e.g., www.dnssec-tools.org
- How many DNS queries can there be?
- More than you probably ever imagined!!

www.dnssec-tools.org



As owner of a nameserver ...

- Decide to protect your nameserver content with DNSSEC
- The Good News:
 - Many nameservers (open source & commercial) currently handle DNSSEC
 - See: <https://www.dnssec-deployment.org/index.php/deployment-resources/survey/>
- The Not So Good News:
 - Some nameservers don't fully handle DNSSEC
 - Ask them to provide it (or change vendors)

Open Source DNSSEC Nameservers

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/
OpenDNSSEC	Open-source turn-key solution for DNSSEC	Collaborative effort, see website	http://www.opendnssec.org

As owner of a nameserver ...

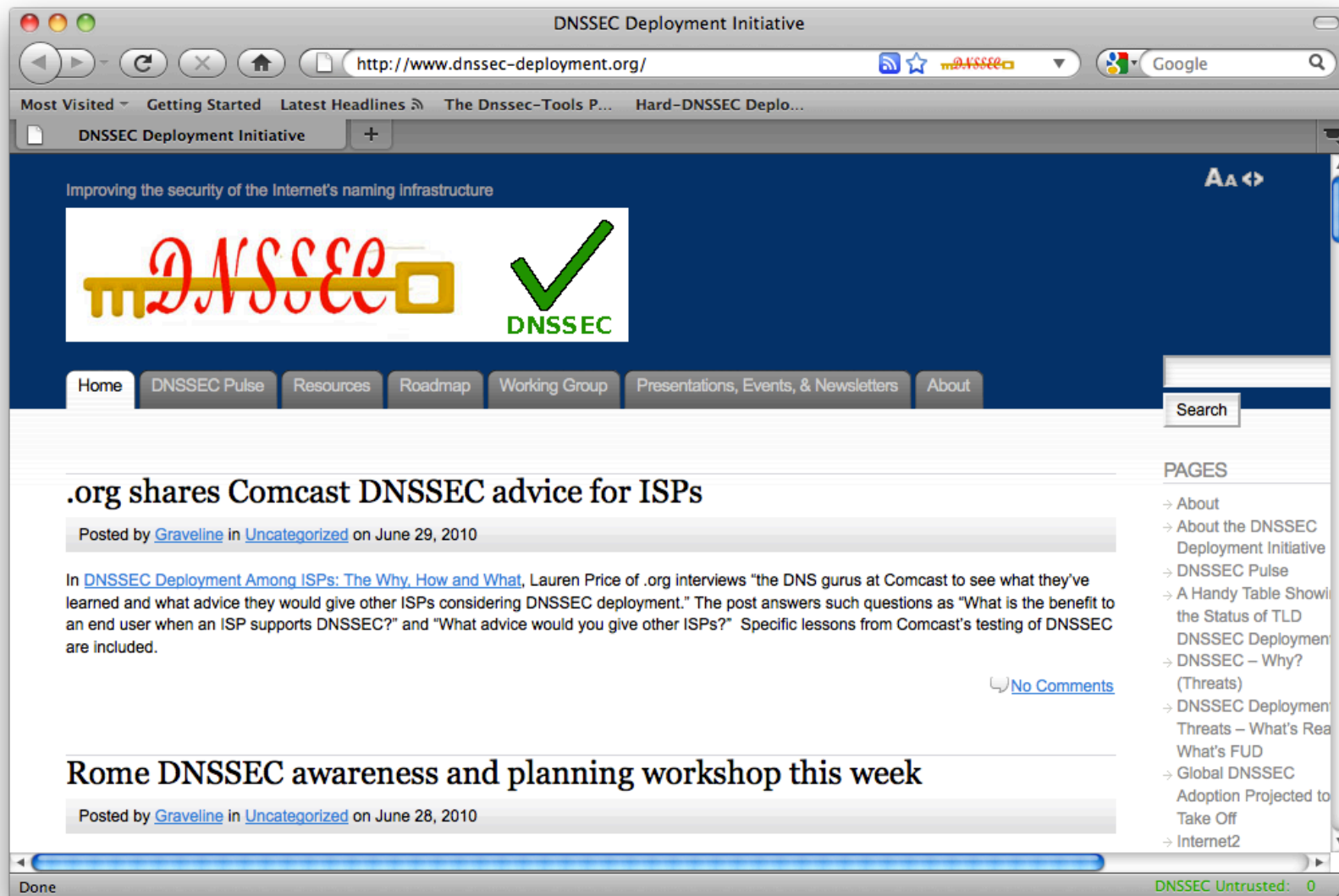
- Use DNSSEC to validate DNS queries
- Choose DNSSEC aware product:
 - Many nameservers currently handle DNSSEC
 - See: <https://www.dnssec-deployment.org/index.php/deployment-resources/survey/>
- Choose DNSSEC aware service provider:
 - Some ISPs and Registrars don't fully handle DNSSEC
 - Ask them to provide it (or change vendors)

As owner of a nameserver ...

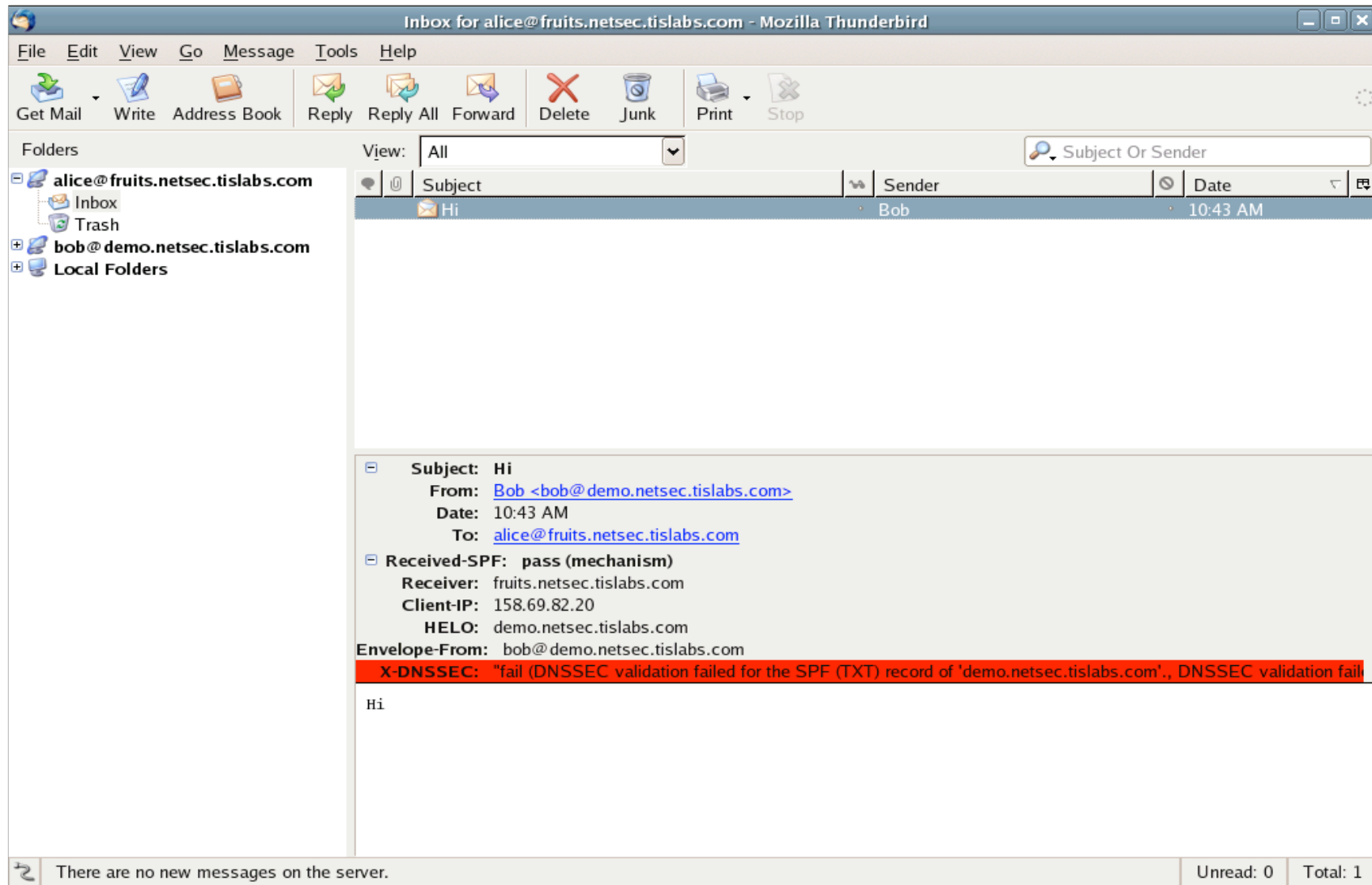
- Begin using DNSSEC applications
- Open source products and extensions currently available:
 - See: <https://www.dnssec-tools.org/>
 - See: <https://www.dnssec-deployment.org/index.php/deployment-resources/survey/>
 - Some examples follow – others available and under development, e.g. Phreebird suite from Dan Kaminsky:
https://media.blackhat.com/bh-ad-10/source/kaminsky/phreebird_suite_1.0.tar.gz

DNSSEC Aware Application Examples

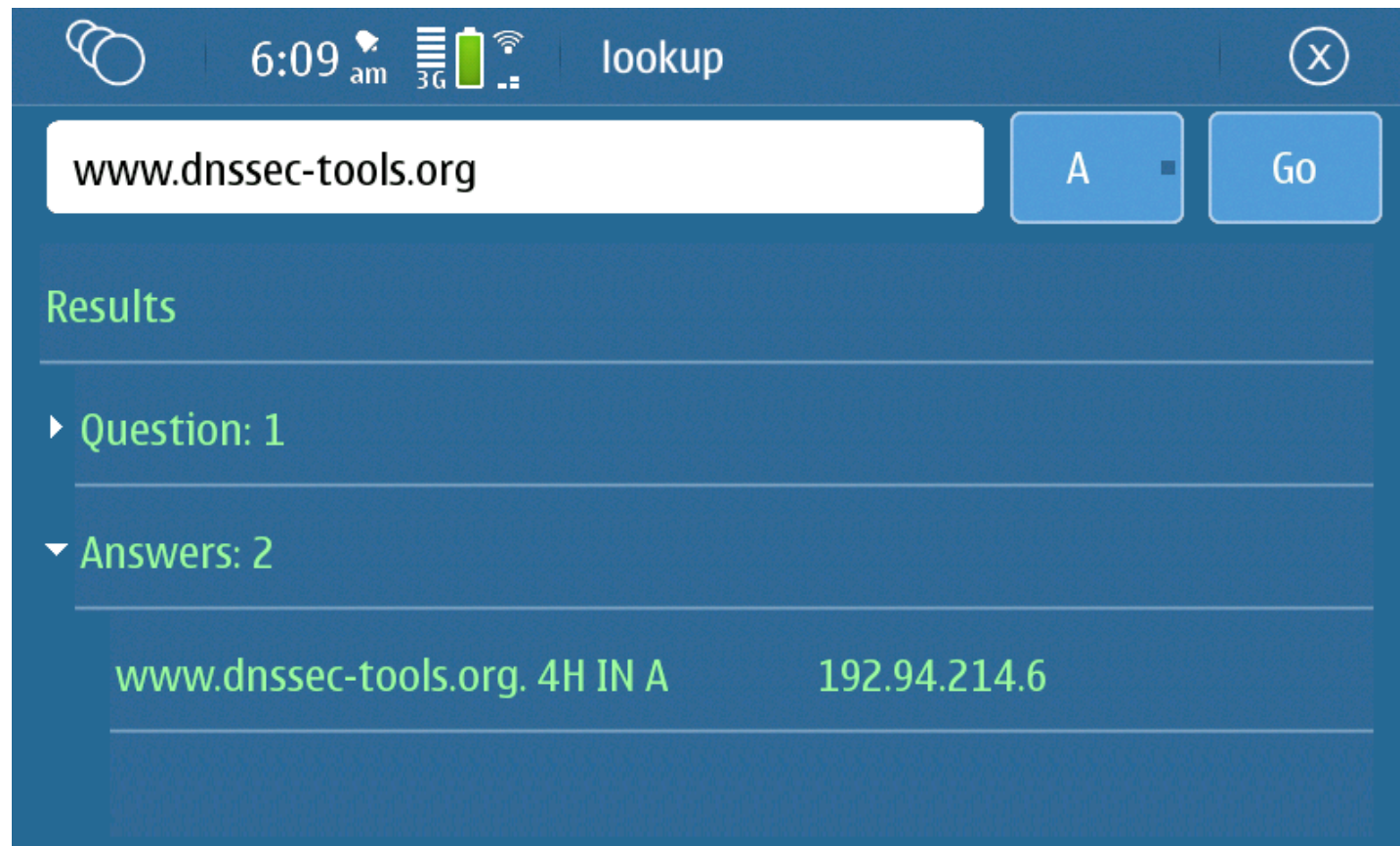
firefox



thunderbird



DNSSEC Aware Phone



N900 Users: it's "lookup" in extras-testing

Comments or Questions?

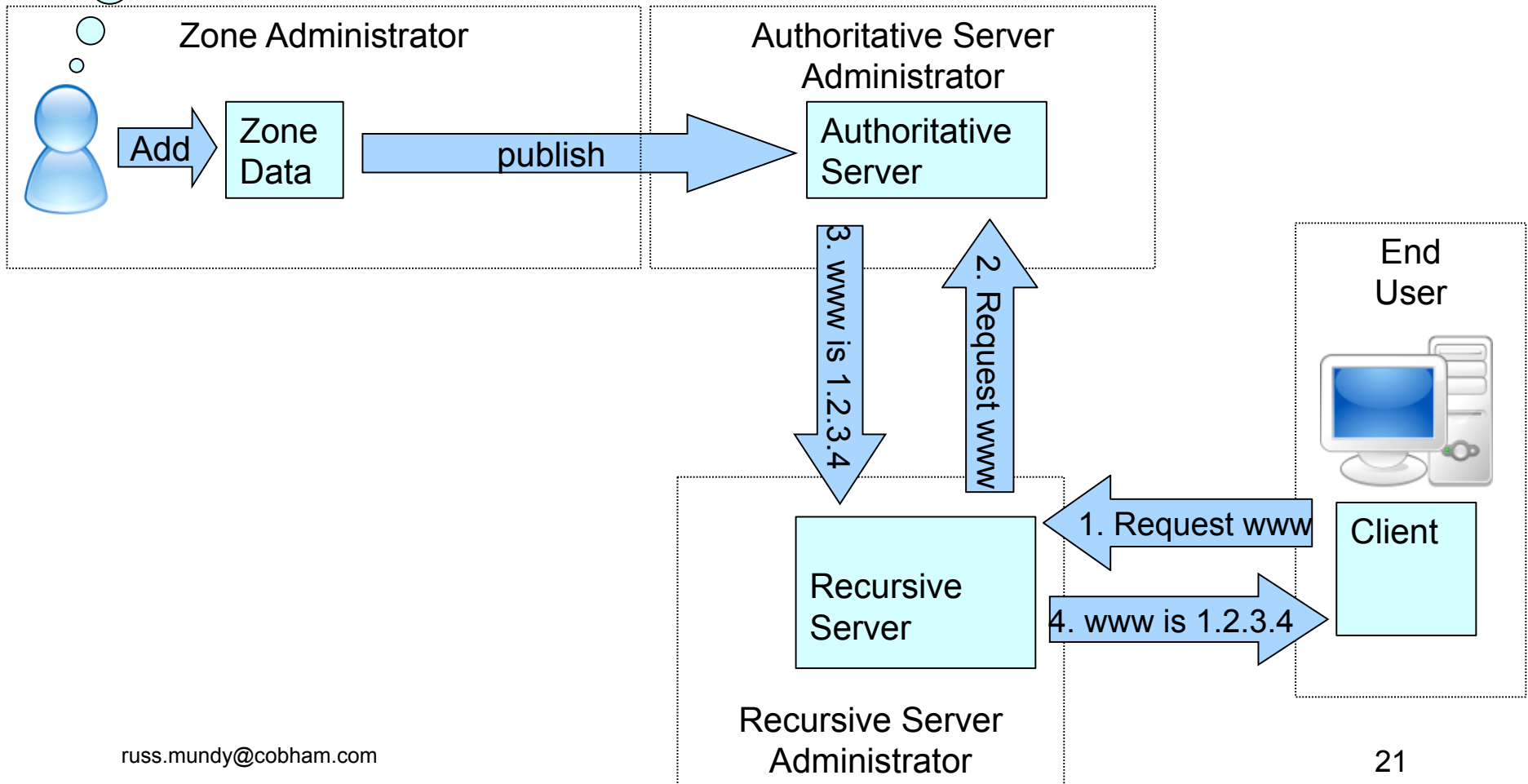
(If time permits)

<http://www.dnssec-tools.org>
<http://www.dnssec-deployment.org>

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

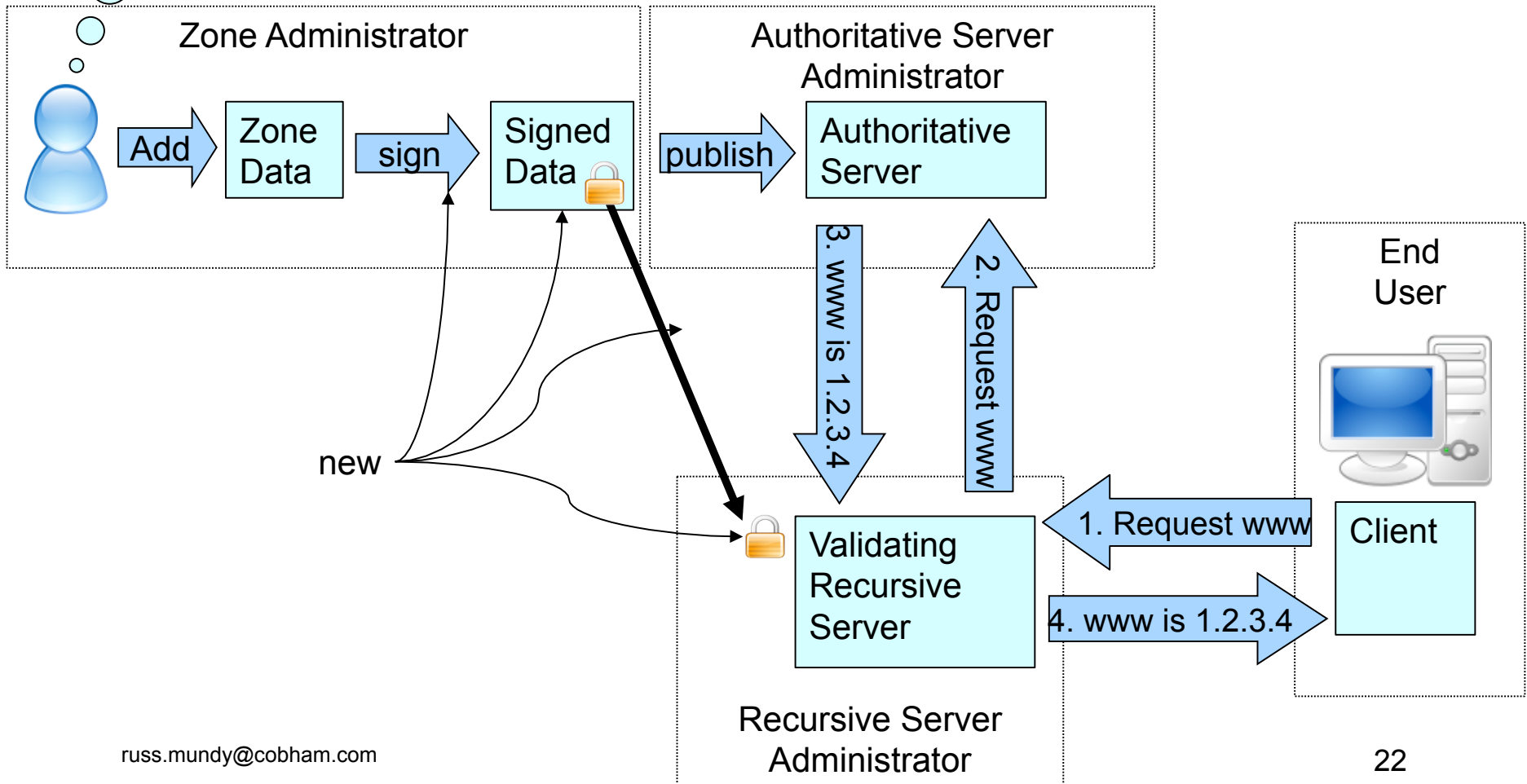
Backup Slides

Simple Illustration of DNS Components



Simple Addition of DNSSEC

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



DNSSEC-Tools Suite

- Suite of tools developed by SPARTA
 - Open Source project sponsored by DHS S&T
 - <http://www.dnssec-tools.org/>
 - **Free! (BSD License)**
- Status
 - Designed to make DNSSEC “easy”
 - Many tools: Pick what you need
 - Grouping of Tools provided on project web site:
<http://www.dnssec-tools.org/>

The Dnssec-Tools Project

http://www.dnssec-tools.org/

Postini 32nd-ICANN Jaap-Bartok'sPlayPen timecard UEMdemo ianaDNSSEC NetSecWiki Worf Infosite Deployment DnssecTools

DNSSEC-Tools

Is your domain secure?

[Sign Your Zone](#) [Tutorials](#) [Install](#)

[Why?](#)

About DNSSEC-Tools

The goal of the DNSSEC-Tools project is to create a set of software tools, patches, applications, wrappers, extensions, and plugins that will help ease the deployment of DNSSEC related technologies.

- [Read the Tutorials](#)
- [Explore the wiki](#)
- [See the Tool Descriptions and ScreenShots](#)
- [Download and Install](#)

To contact the project developers, please write the [dnssec-tools-users AT lists.sourceforge.net mailing list](mailto:dnssec-tools-users@lists.sourceforge.net) or submit bugs to the [bug database](#).

Get Started!

The DNSSEC-Tools DNSSEC software contains many helpful tools. Find the ones you need in order to get started by browsing the tutorial sections listed below:

- [Authoritative Zones](#)
- [Authoritative Servers](#)
- [Recursive Servers](#)
- [Applications](#)
- [Application Developers](#)

Project News

DNSSEC-Tools 1.5.rc2 posted 2009-02-16 23:26 - [dnssec tools](#) [XML](#)
 DNSSEC-Tools 1.5.rc2 contains a few more features than 1.5.rc1, so check it out!
[Read More »](#)

Sign Your Zone

DNSSEC-Tools Resources

- [Main Page](#)
- [Tutorials](#)
- [Tool Descriptions And Screen-Shots](#)
- [Download](#)
- [Additional Documentation](#)
- [Test Zone](#)

Tools For...

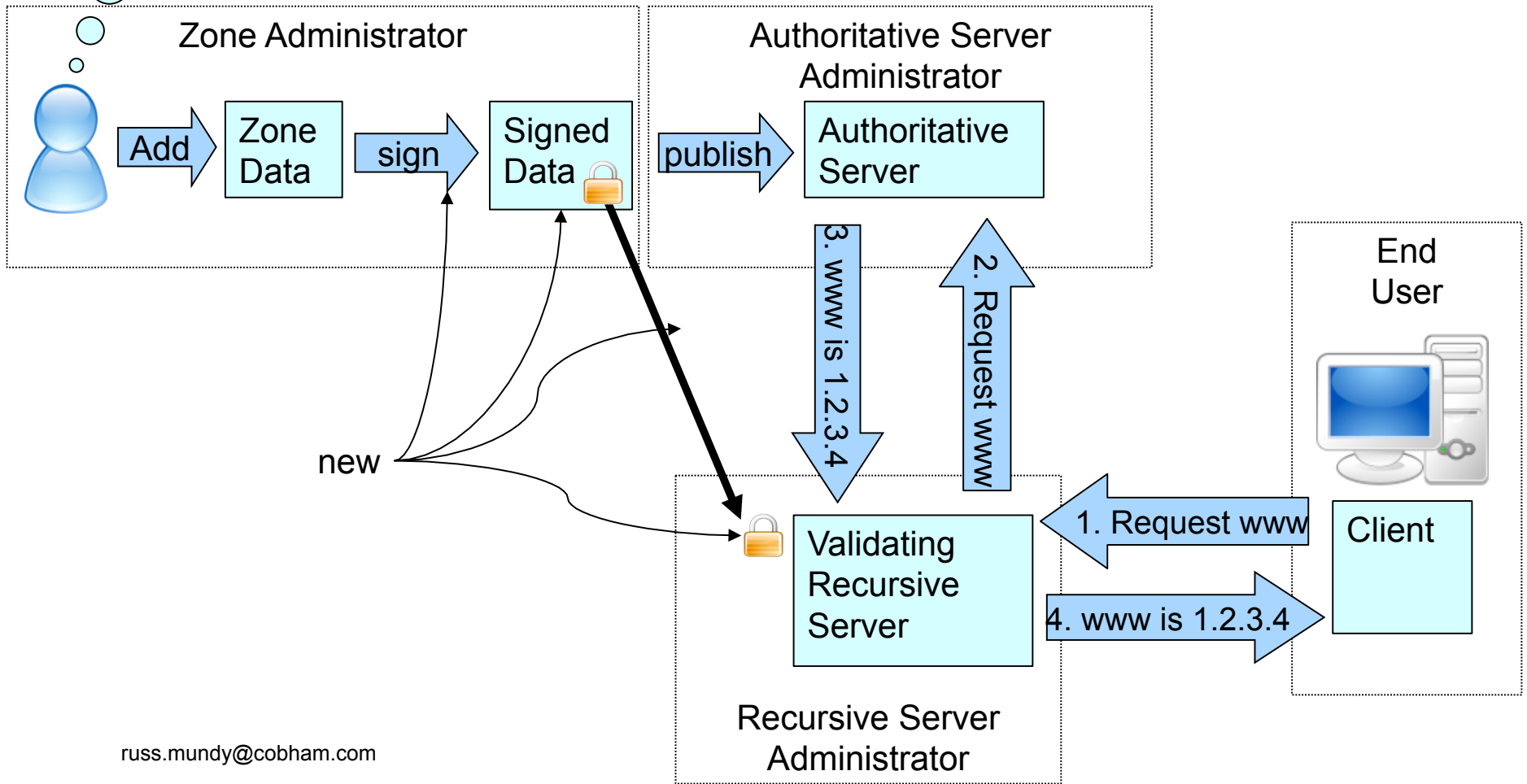
- [Authoritative Zones](#)
- [Authoritative Servers](#)

DNS Today with SEC



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

I need to add a WWW record



Some New Aspects With DNSSEC



- Key maintenance
- Zone Signing Operation
- Provisioning: Memory, CPU, bandwidth
- Parent-child communication of DNSSEC-related information
- Trust Anchor Maintenance
- New error codes in applications
- Additional Troubleshooting

DNSSEC-Tools Components

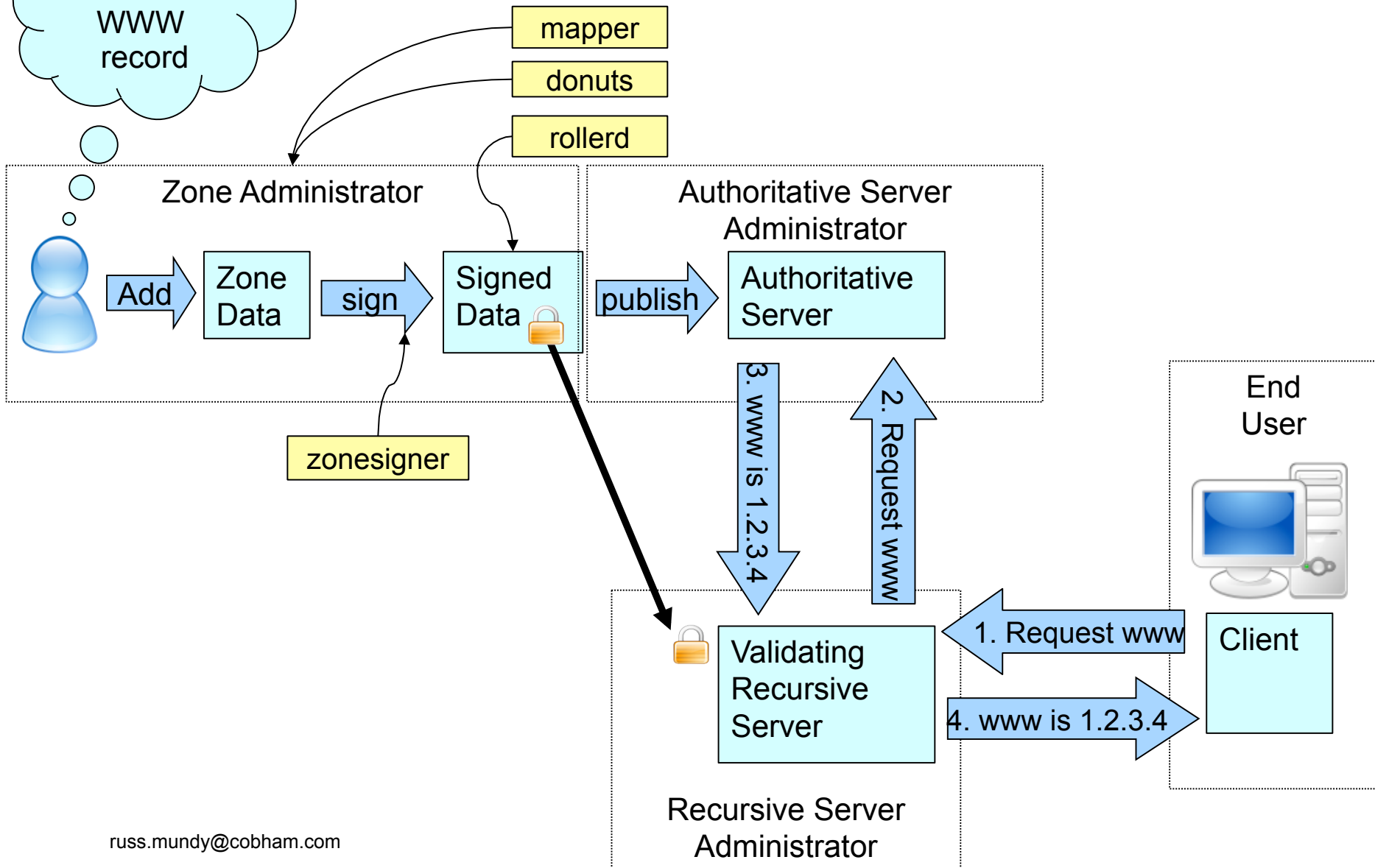
- Infrastructure
 - (Libraries, Perl Modules, ...)
- Tools for managing zones
 - (signers, lint, debug, ...)
- Tools for managing resolvers
 - (trust anchor management)
- Applications
 - (firefox, ssh, ncftp, ...)
- Educational Materials
 - (**tutorials!!!**, documentation)

Zone Administration Tools



- DNSSEC Maintenance:
 - Zonesigner
 - RollerD
- Zone Data Quality Assurance:
 - Donuts
 - Mapper

Zone Admin Tools



zonesigner

- Signs zones in one step
- Defaults do the “right thing”
- Wraps around the bind tools
- Keeps track of state, keys, etc
- Getting started:
 - First time: `zonesigner --genkeys example.com`
 - There after: `zonesigner example.com`

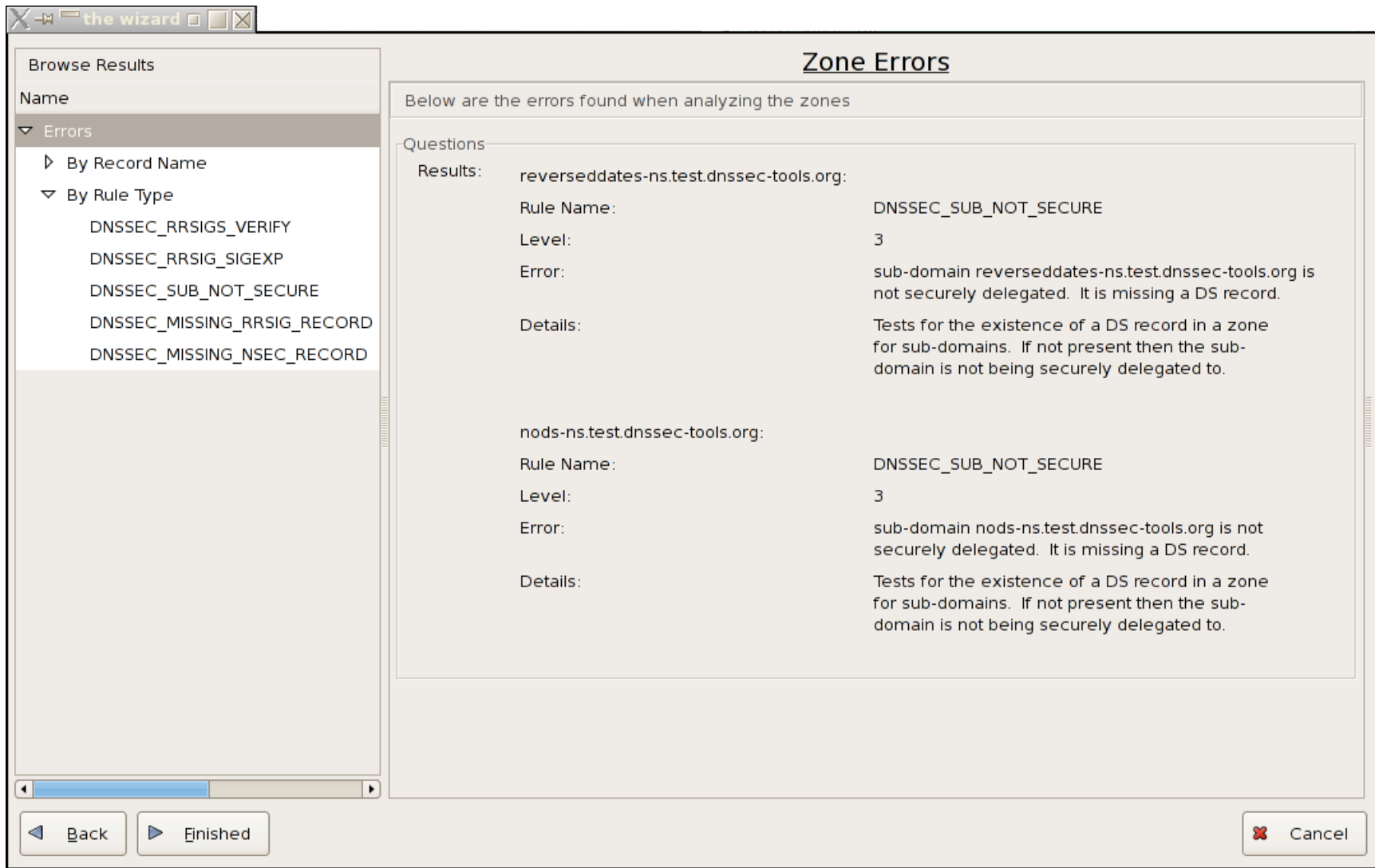
rollerd

- Automatic key-rollover and signing daemon
 - Follows a defined policy for how often to roll keys
 - Handles both ZSK and KSK keys
- Regular scheduled calls to zonesigner
- Runs as a Daemon
- Includes a separate utility to talk to the daemon
 - Check status
 - Start something “now”

donuts

- DNS Zonefile error/lint checker
 - Validates all DNSSEC records
 - donutsd for running on a regular basis
- Extendible:
 - Easily create your own site-specific rules (see tutorial)
 - Site specific configuration
 - Add/Remove specific types of features/checks
- Expects the data to be readable
 - Zone data must be parsible
 - Doesn't report syntax errors

donuts: Browsable GUI example



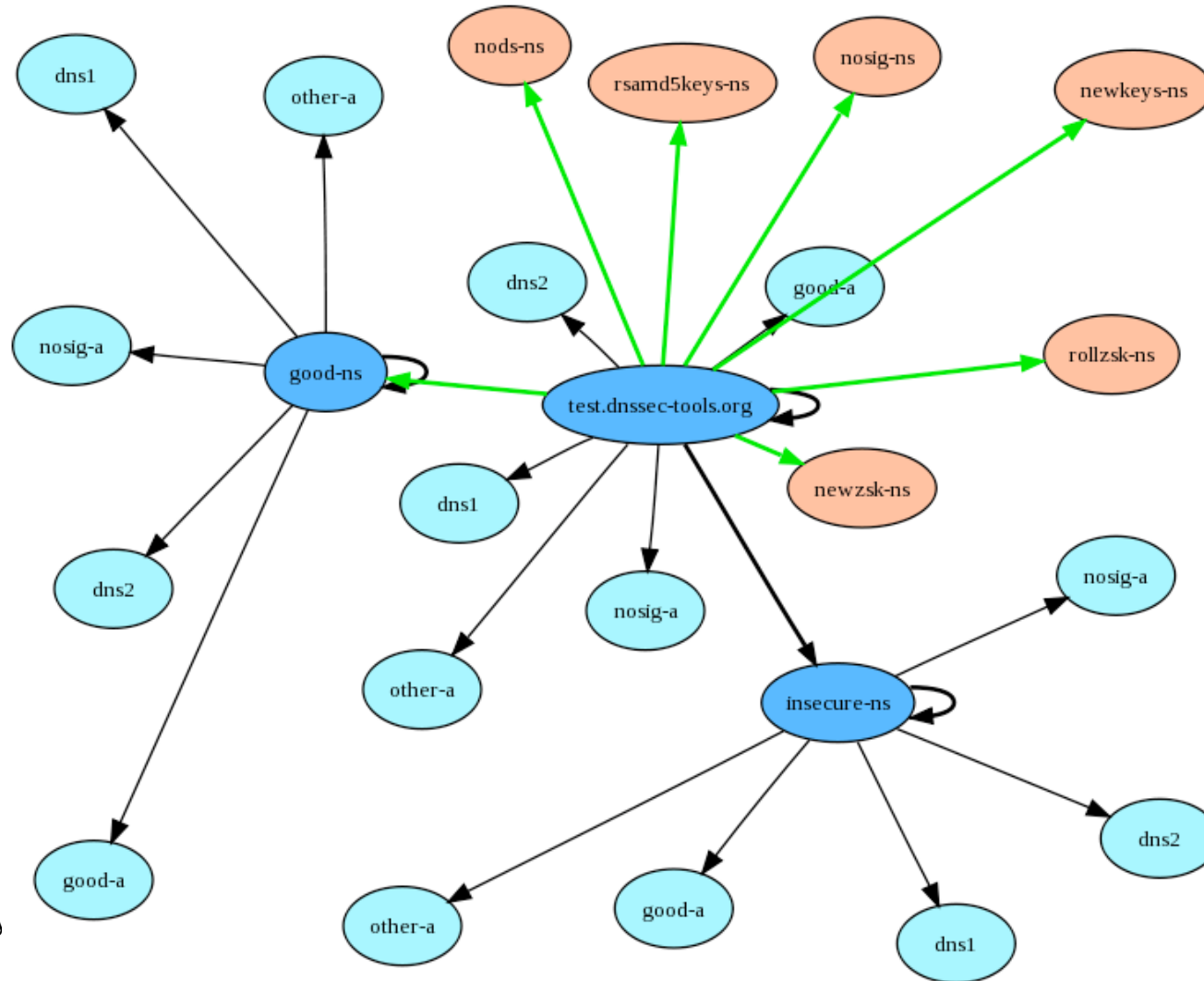
mapper

- Graphical map generator of zone data
- Color codes zone data and relationships
- Understands DNSSEC record types
 - Currently doesn't validate data
 - Just checks for existence and dates

mapper: example



test.dnssec-tools.org



russ.mundy

Authoritative Server Tools

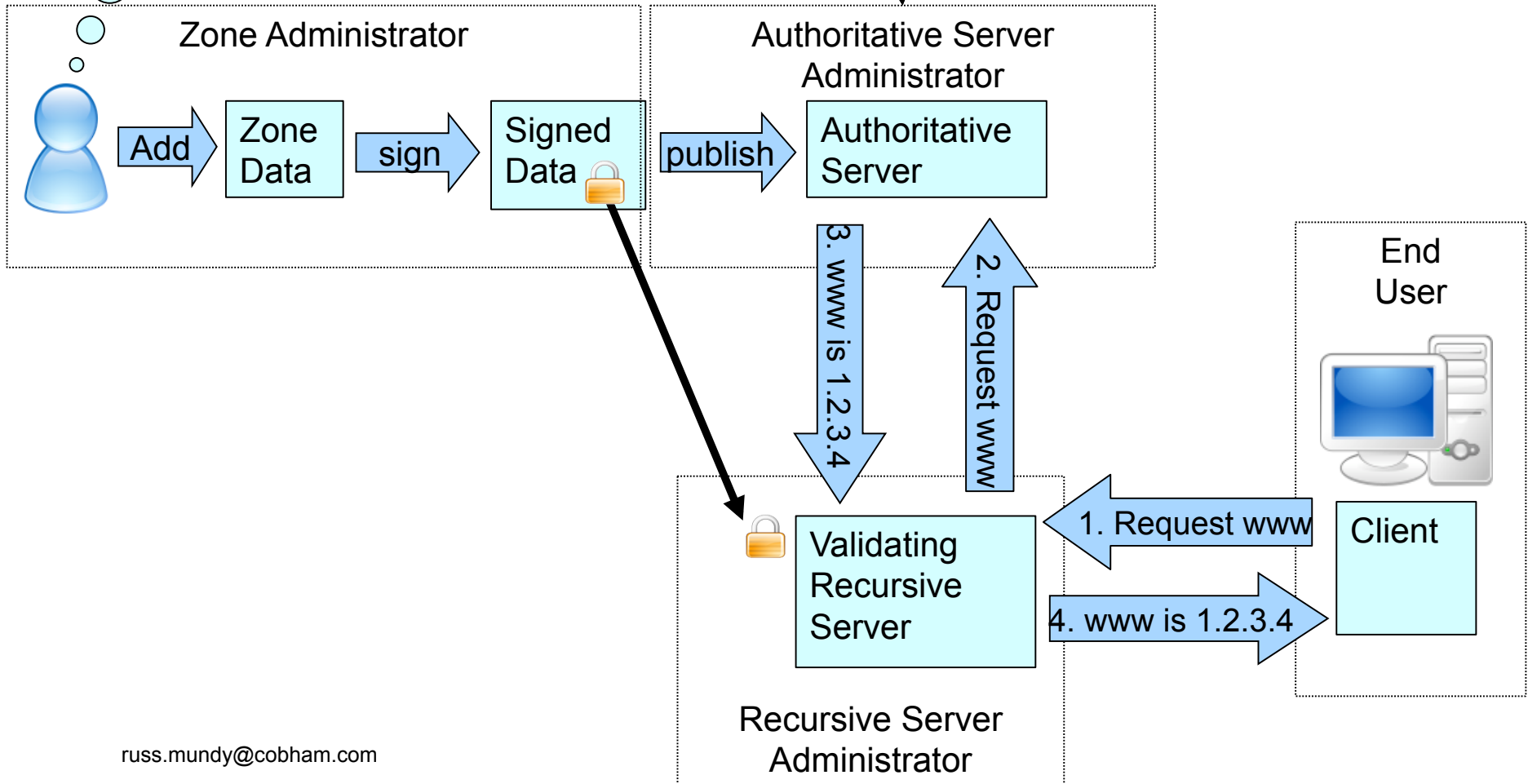
A subset of the Zone owner tools:

- Zone Data Quality Assurance:
 - donuts
 - mapper
- Other tools, discussed later may be useful too:
 - logwatch
 - dnspktflow

Auth Server Tools



mapper
donuts



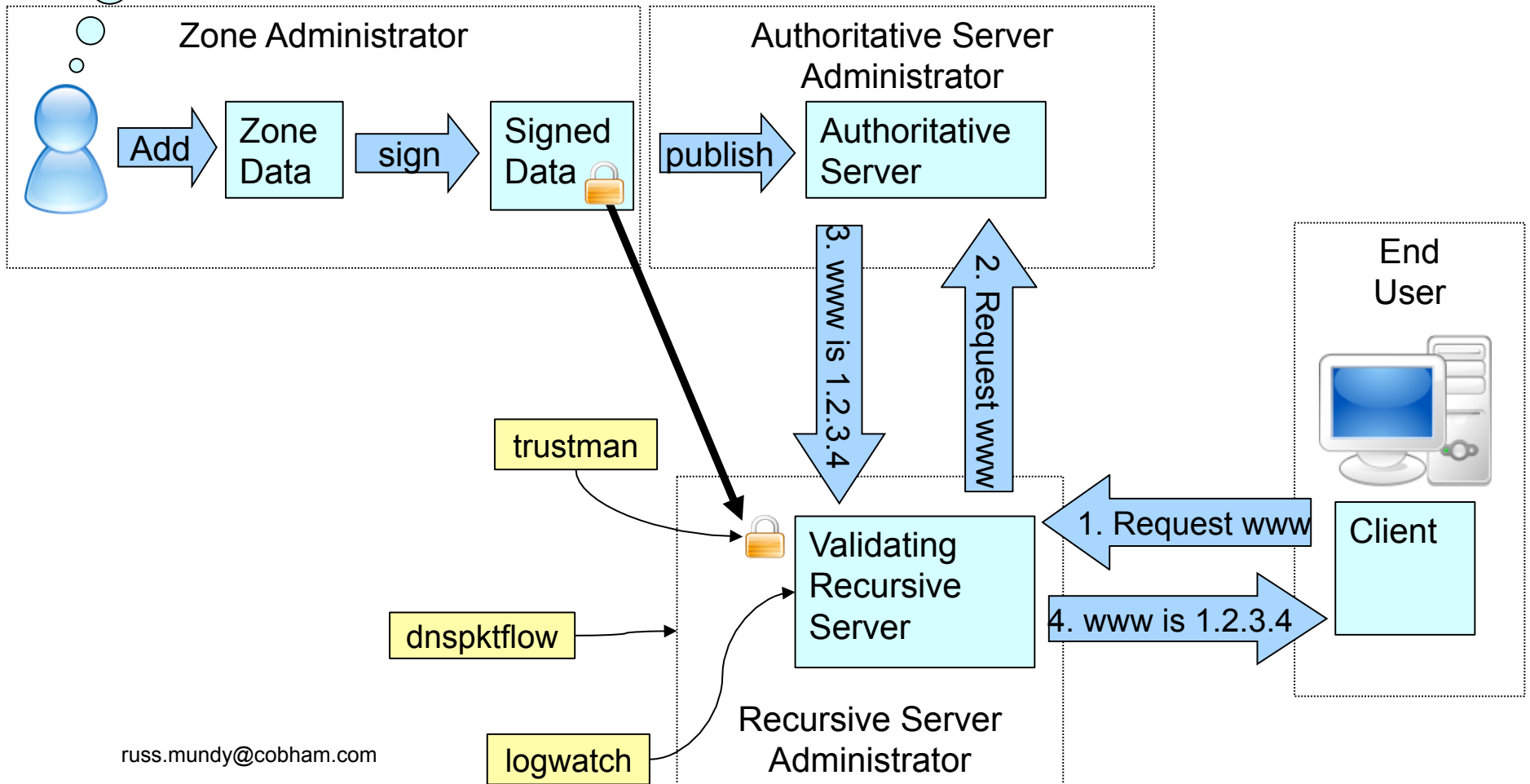
Validating Recursive Server Tools

- Trust Anchor Management
 - Trustman
- Debugging
 - dnspktflow
- Name Server Error Reporting
 - logwatch

V



Validating Recursive Server Tools



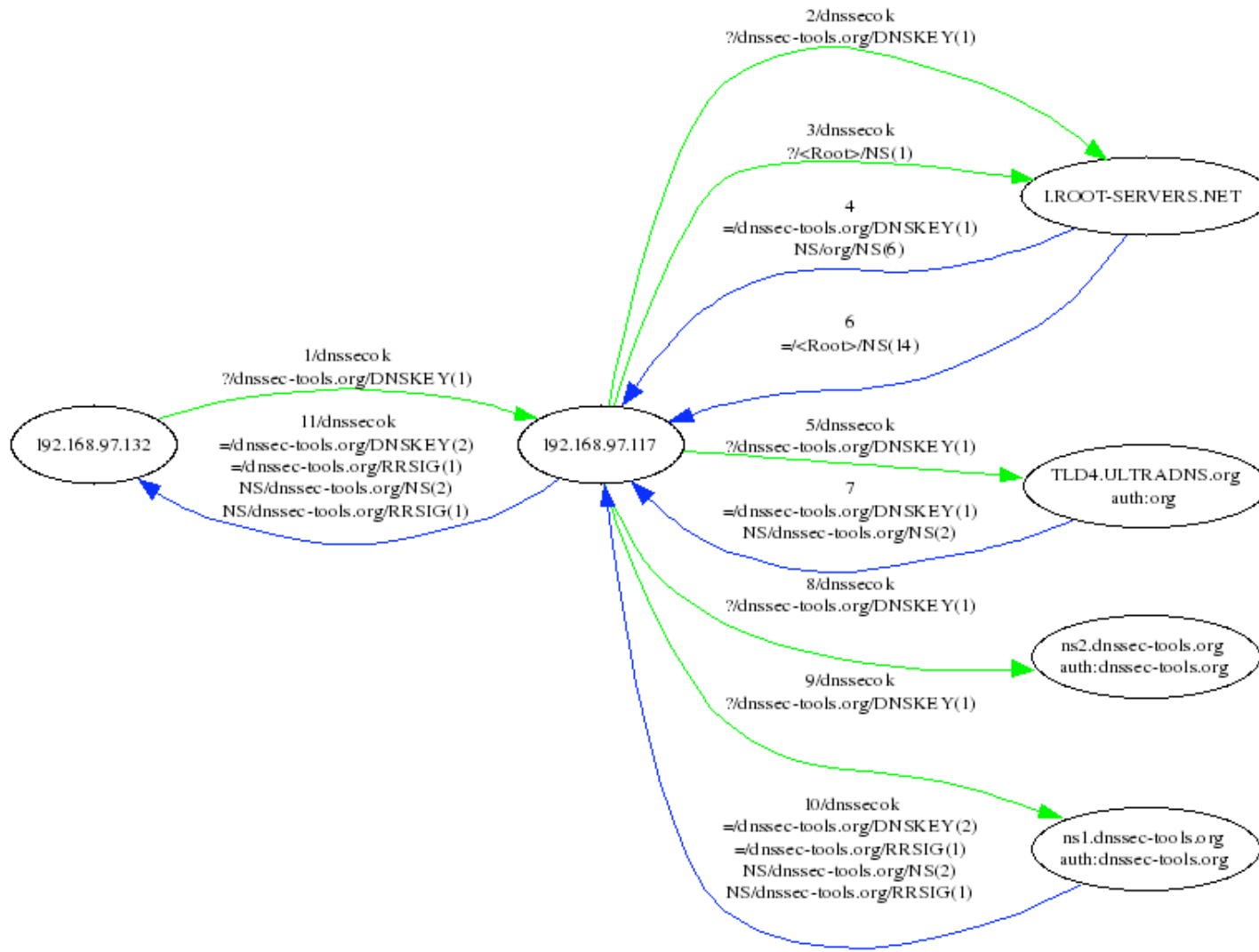
trustman

- Manages validating resolver trust anchors
 - Detects new keys being deployed
 - Updates/Notifies when new zone keys are detected
- RFC5011 compliant
- Runs as a Daemon
 - has a run-once mode

dnspktflow

- Analyzes DNS packets within tcpdump files
- Requires wireshark
 - More importantly: tshark
- Draws a diagram with:
 - Numbered requests/responses
 - Request/response contents
 - Circles, arrows and implements of destruction

dnspktFlow: example



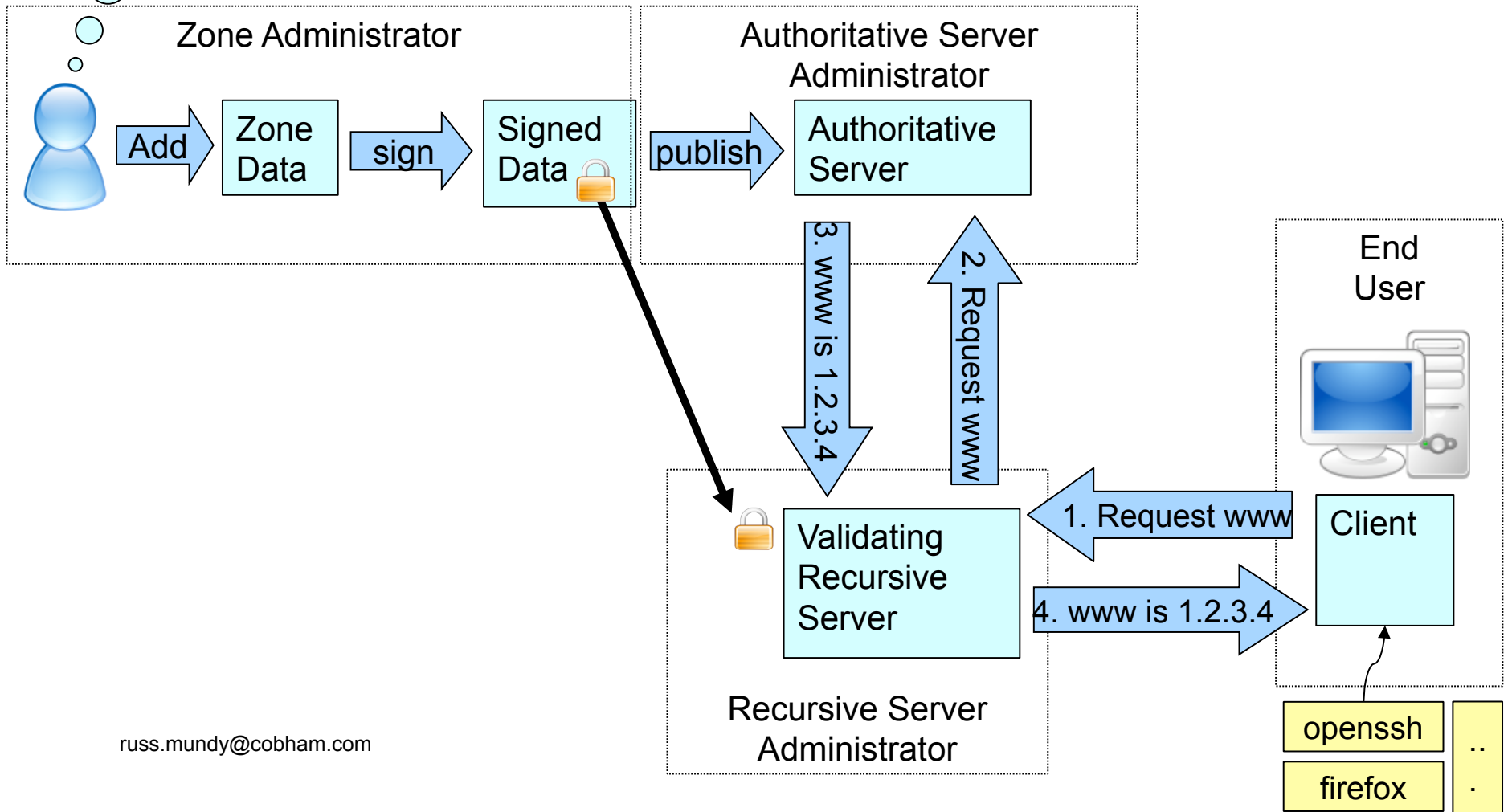
logwatch

- Summarizes DNSSEC related output from bind
- Now included in logwatch 7.1 and beyond

End-User Tools

- Libraries
 - Libval: a validating library for developers
 - Libval_shim:
 - system wide shim library
 - Forces all apps to be DNSSEC capable
- Perl modules
- Command-line troubleshooting utilities
- DNSSEC-enabled applications

End-User Tools



DNSSEC-Tools: Libraries

- DNSSEC validating resolver library - libval
 - Verifies DNS(SEC) data at the library layer
 - Portable-ish (getting more so)
 - Based on libbind
 - Thread-safe
 - Reentrant
 - Can
n
p
pull data directly or from a local caching resolver
 - BSD Licensed

Libval shim

- LD_PRELOAD-based approach for adding DNSSEC capability to existing applications
- The shim library implements most of the commonly-used resolver functions
 - Applications that use these functions can automatically become DNSSEC-capable if they run within an LD_PRELOAD environment with libval_shim.
 - Many applications are known to work out of the box with libval_shim

DNSSEC-Aware Applications

- DNSSEC-Tools contains patches to:
 - firefox
 - thunderbird
 - postfix, sendmail, LibSPF
 - wget, lftp, ncftp, proftpd
 - OpenSSH
 - OpenSWAN (opportunistic encryption)
 - Jabberd
- DNSSEC support provide through libval

Developer Resources

- Test zone test.dnssec-tools.org
 - Contains many DNSSEC “errors” to test against
- Developers guide to using the validator and resolver libraries - work in progress
- PERL modules
 - `Net::DNS::SEC::Tools`
 - `Net::DNS::SEC::Validator`
 - `Net::DNS::Zonefile::Fast`
 - `Net::addrinfo`

Validation Library API

- draft-hayatnagarkar-dnsex-07.txt
 - Defines an API for interfacing with a validation library
 - Allows clients to state their policy
 - Allows clients to get DNS and validation results
 - High-level: `val_gethostbyname`
 - Low-level: `val_resolve_and_check`
 - Policy: `val_istrusted`
 - Implemented in DNSSEC-Tool's libval
- Not yet an IETF Working Group document

postfix/sendmail/libspf



- Protects various attributes of mail processing
 - MX record lookups
 - SPF record lookups

wget/lftp/ncftp

- Protects address lookup

OpenSSH

- Protects address lookup
- Provides key discovery
 - Removes need for leap-of-faith
 - Protects against key reuse for key changes

Documentation

- Step-by-step guide for DNSSEC operation using DNSSEC-Tools
- Step-by-step guide for DNSSEC operation using BIND tools
- Tutorials
- Wiki
- Manual pages
- User Documentation

Survey of Resources Available for DNSSEC

<https://www.dnssec-deployment.org/index.php/deployment-resources/survey/>

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 resources are catalogued at <https://www.dnssec-deployment.org/index.php/deployment-resources/survey/>
 - Approximately 100 tools listed in the catalogue

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/
OpenDNSSEC	Open-source turn-key solution for DNSSEC	Collaborative effort, see website	http://www.opendnssec.org

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/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

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

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/dns/
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 server	Plugin provided by Cobham available in the logwatch distribution	http://www2.logwatch.org:81/

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

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-07.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/

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/

Summary

- DNSSEC adds to cost and complexity but the availability of good tools can reduce much of this.
- DNS operators have diverse environments, so tools should be modular and extensible
 - Possible to envision tool suites that wrap around existing tools and hand-walk an administrator through the process of deploying DNSSEC
- A number of tools that enable DNSSEC deployment for various environments exist **today**; the DNSSEC-Tools suite provides many of them.
- A number of DNSSEC-capable applications are also available
 - Complexity of retrofitting DNSSEC in applications depends on the complexity of the application design.
 - API development work is ongoing.

