

DNSSEC in Practice: Using DNSSEC- Tools to Deploy DNSSEC

Wes Hardaker

Russ Mundy

Suresh Krishnaswamy

{hardaker,mundy,suresh}@sparta.com



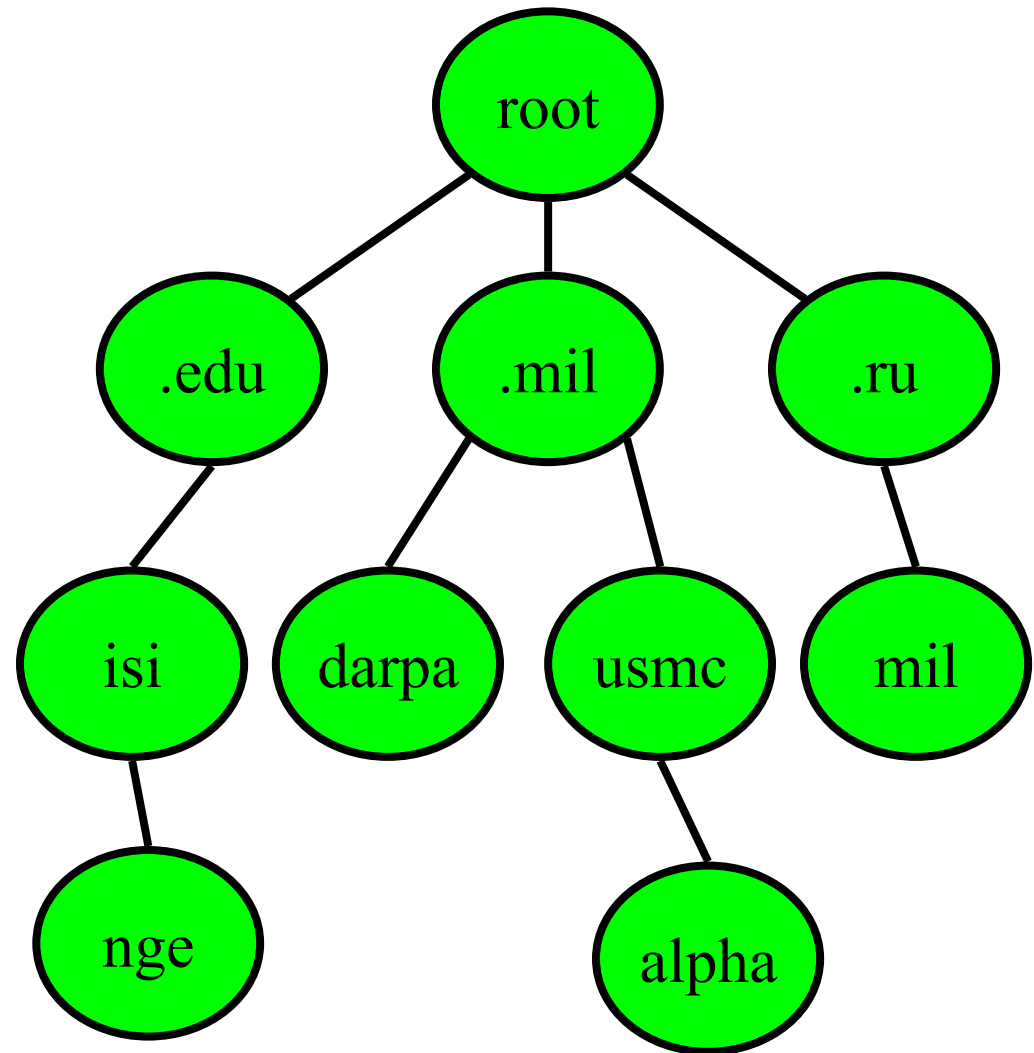
SPARTA, Inc.

Domain Name System and Security

- Critical Internet infrastructure component
 - Virtually every Internet application uses the DNS
- DNS database maps:
 - Name to IP address
 - (for example: www.isi.edu = 128.9.176.32)
 - And many other mappings (mail servers, IPv6, reverse...)
- DNS threats identified in early 1990s
- DNSSEC
 - Cryptographic signatures in the DNS
 - Assures integrity of results returned from DNS queries
 - Protects against tampering in caches and during transmission
 - End-system checks the chain of signatures up to the root

The Domain Name System

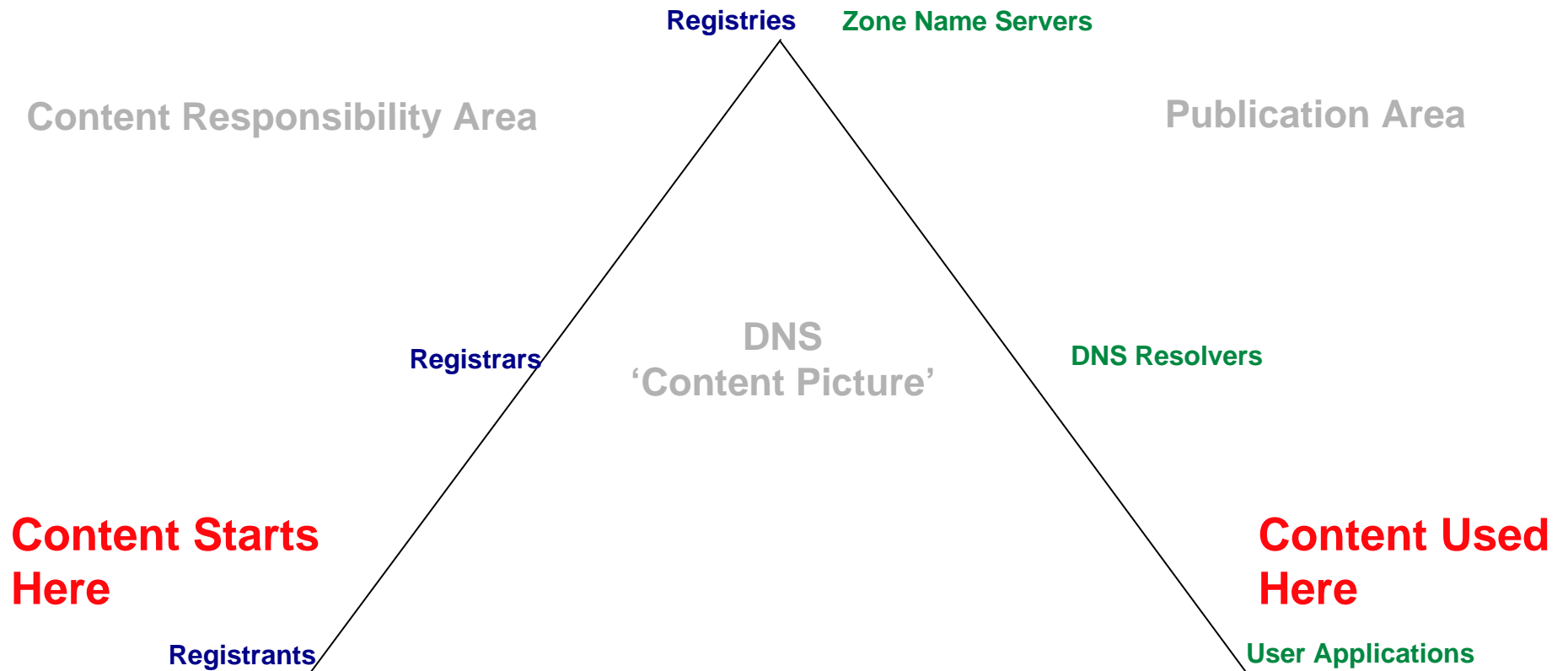
- DNS database maps:
 - Name to IP address
www.dhs.gov = 206.18.104.198
 - And many other mappings
(mail servers, IPv6, reverse...)
- Data organized as tree structure:
 - Each zone is authoritative for its own data
 - Minimal coordination between zone operators



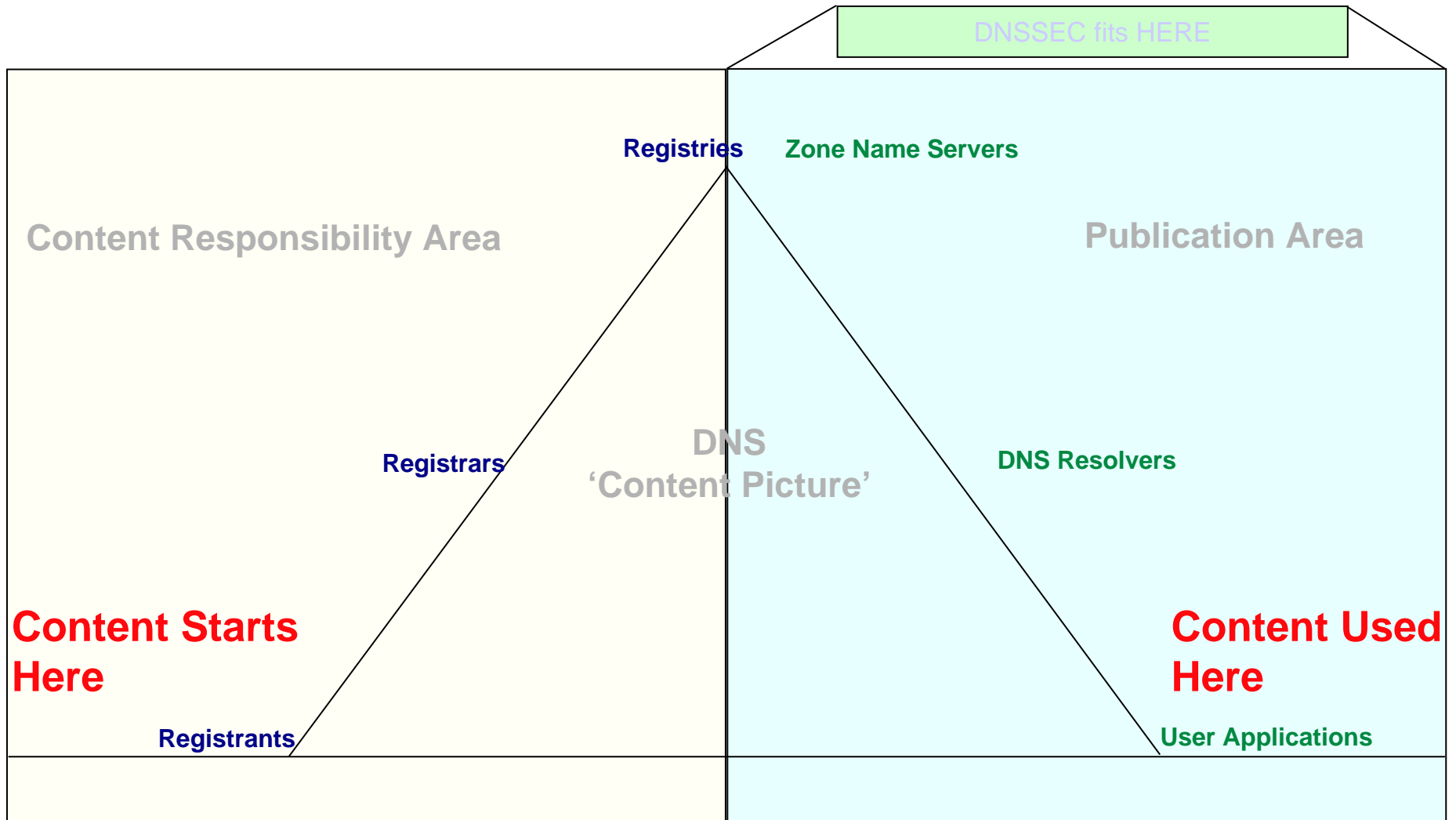
Why is the DNS so Vulnerable?

- Designed in 1980s when threat model was very different from today
- Optimized for fast query/response times
 - Not optimized for authenticity or integrity
 - Trust is implied - legitimate queries and legitimate replies are expected
- Attack the trust model and you can change the way information is found and exchanged on the Internet

What are the DNS Pieces for each Zone?



Where Does DNSSEC Fit?



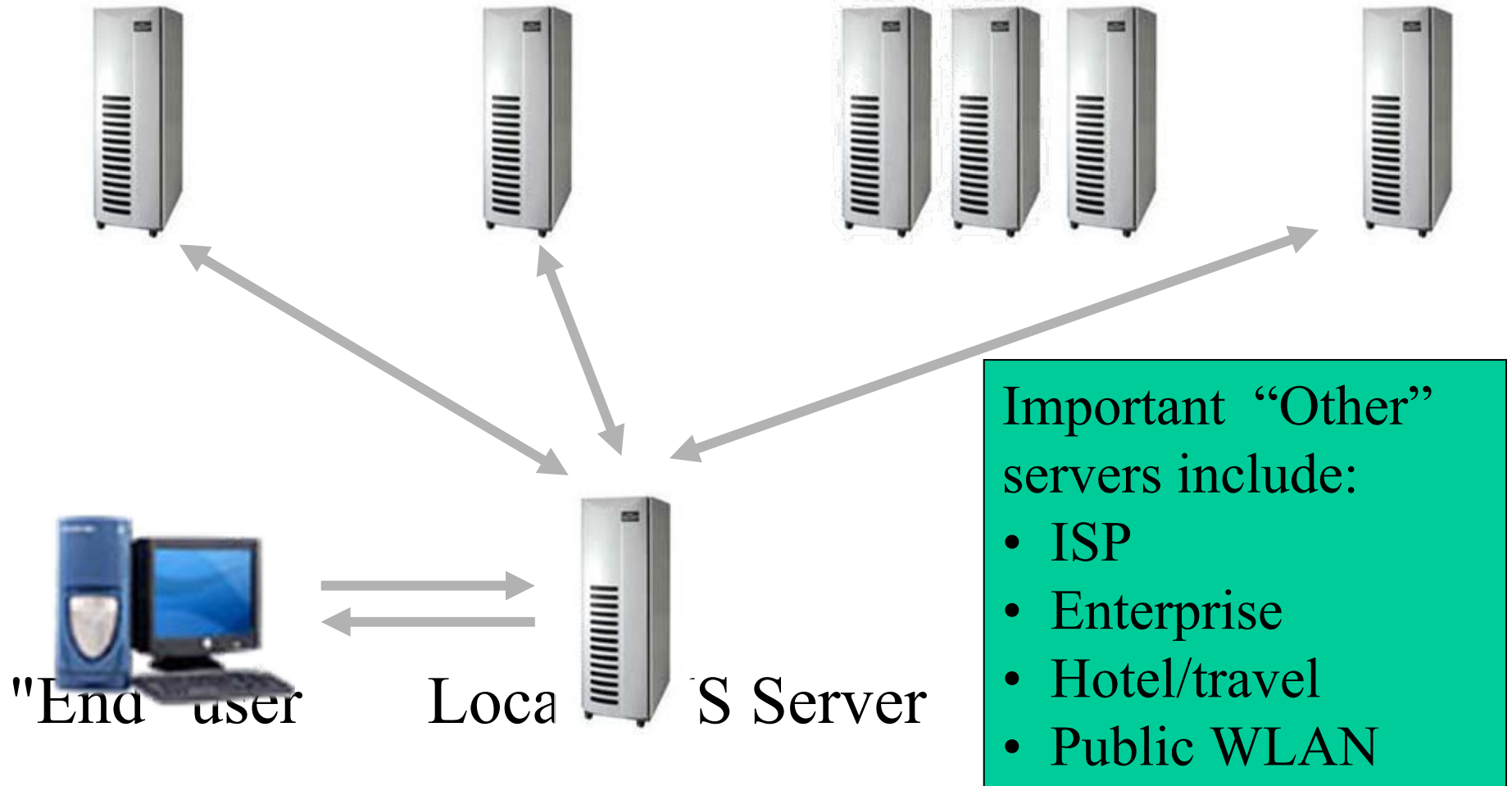
DNS Name Resolution

Root Server

TLD Server

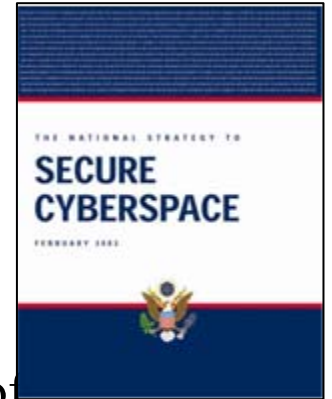
Other Servers

Zone Server



National Strategy to Secure Cyberspace

- The National Strategy to Secure Cyberspace (2003) recognized the DNS as a critical weakness
 - NSSC called for the Department of Homeland Security to coordinate public-private partnerships to encourage the adoption of improved security protocols, such as DNS
 - The security and continued functioning of the Internet will be greatly influenced by the success or failure of implementing more secure and more robust BGP and DNS. The Nation has a vital interest in ensuring that this work proceeds. The government should play a role when private efforts break down due to a need for coordination or a lack of proper incentives.



USG DHS DNSSEC Deployment Initiative

- Recognition of the weaknesses in critical infrastructure protocols
- Calls for the USG to coordinate public-private partnerships to encourage the adoption of improved security protocols
- The DNSSEC Deployment Initiative sponsored by the DHS Science and Technology (S&T) Directorate is one of these partnerships
 - NIST, Shinkuro and SPARTA
- Leading the effort to get the .GOV and other major zones signed

DNSSEC Initiative Activities

- DNSSEC Deployment Roadmap
 - <http://www.dnssec-deployment.org/roadmap.php>
- Multiple workshops held world-wide to facilitate the deployment of DNSSEC
- Active participation in various conferences
 - E.g Upcoming featured presentation at Govsec
- Monthly newsletter
 - <http://www.dnssec-deployment.org/news/dnssecthismonth/>
- Catalog of available tools
 - <http://www.dnssec-deployment.org/tracker>

DNSSEC Initiative Resources

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

DNSSEC Deployment Initiative



DNSSEC This Month

February 2, 2009

Volume 4, Number 2

ISSN 1932-6564

In This Issue:

- [New version of BIND includes DNSSEC upgrades](#)
- [DNSSEC tops U.S. government IT priorities for 2009](#)
- [New ENISA report evaluates DNSSEC](#)
- [Technology Review calls DNSSEC "A New Web of Trust"](#)
- [NANOG offers Comcast, other DNSSEC presentations](#)
- [Winter Internet2 Joint Techs to Texas](#)
- [Homeland Security holds cybersecurity conference in March](#)
- [ICANN to Mexico City in March](#)
- [Reminder! Initiative to present daylong session on DNSSEC deployment at GovSec](#)
- [IETF to San Francisco](#)
- [BlackHat offers DNSSEC workshops in Amsterdam, Las Vegas](#)

New version of BIND includes DNSSEC upgrades: ISC BIND 9.6.0 includes several DNSSEC related improvements, including **full NSEC3 support, automatic zone re-signing, two new DNSSEC tools, and PKCS#11 Cryptoki hardware support.** As an alternative to NSEC, NSEC3 (defined in RFC 5155) can prevent walking of DNSSEC zones and permits optional gradual expansion of delegation-centric zones. New options -- sig-signing-nodes and sig-signing-signatures -- provide incremental re-signing support for dynamic zones. BIND 9.6 can optionally be built to use OpenSSL's PKCS#11 (or Cryptographic Token Interface) support so it can use specialized hardware for securely storing keys and/or generating cryptographic data. The new tool, dnssec-keyfromlabel, uses the hardware device to construct a DNS key pair for use by named and dnssec-signzone. The new tool, dnssec-dsfromkey, can generate DS records from the DNSKEY contained in existing keyset or .key files. In addition, BIND 9.6.0 also includes Holger Zuleger's DNSSEC Zone Key Tool (zkt) in the contrib collection. It provides wrappers around BIND's dnssec-keygen and dnssec-signzone tools to help create and list DNSSEC zone keys, sign zones, do re-signing, and automate key rollovers. Go to the [ISC](#) for more information about BIND and ISC's DNSSEC-related services.

WELCOME

Attacks on the Internet infrastructure are a reality - it's estimated that 10 percent of servers in the network today are vulnerable to domain name system (DNS) attacks. And many technology experts believe that we will see a serious attack on the underlying infrastructure within the next decade.

The [DNS Security Extensions \(DNSSEC\) Deployment Coordination Initiative](#) is part of a global effort to deploy new security measures that will help the DNS perform as people expect it to - in a trustworthy manner. This initiative builds on over a decade of work undertaken by many experts around the world, who developed [the DNSSEC standard](#) that was published by the IETF.

On this site, we have collected important information to help you learn more about the initiative; DNS attacks and their impact on your business, government agency, or home computing; information for adopters and potential adopters; and news and research to keep you informed about progress against this important security threat.

Available Software

- Various categories of tools and software are available
- Some of the available tools are catalogued at <http://www.dnssec-deployment.org/tracker>
- Existing tools have broad coverage
- Some gaps remain and are currently being addressed within the community

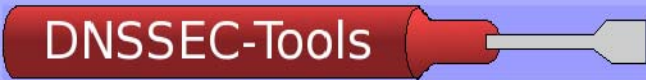
DNSSEC-Tools Suite

- 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
 - Tool robustness: varies with age
 - Each tool has it's own version number
 - Check with -v

The Dnssec-Tools Project


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

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



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 »](#)

DNSSEC-Tools Resources

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

Tools For...

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

DNS Yesterday

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

I need to
add a
WWW
record

Zone Administrator

Authoritative Server
Administrator

End
User

Client

Add

Zone
Data

publish

Authoritative
Server

3. www is 1.2.3.4

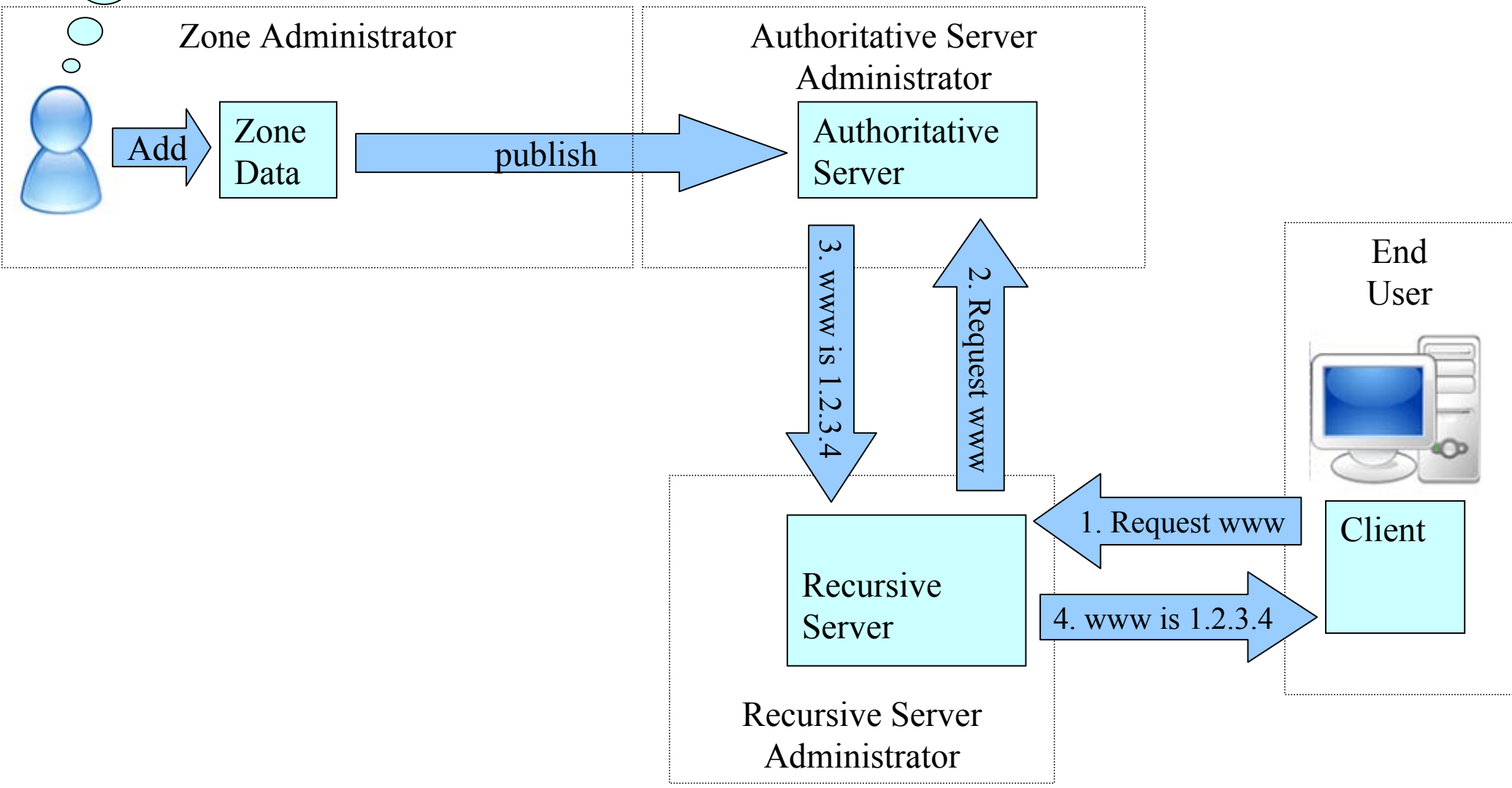
2. Request www

Recursive
Server

1. Request www

4. www is 1.2.3.4

Recursive Server
Administrator



DNS Today with SEC

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

I need to
add a
WWW
record

Zone Administrator

Authoritative Server
Administrator

End
User

Client

Recursive Server
Administrator

Add

Zone
Data

sign

Signed
Data

publish

Authoritative
Server

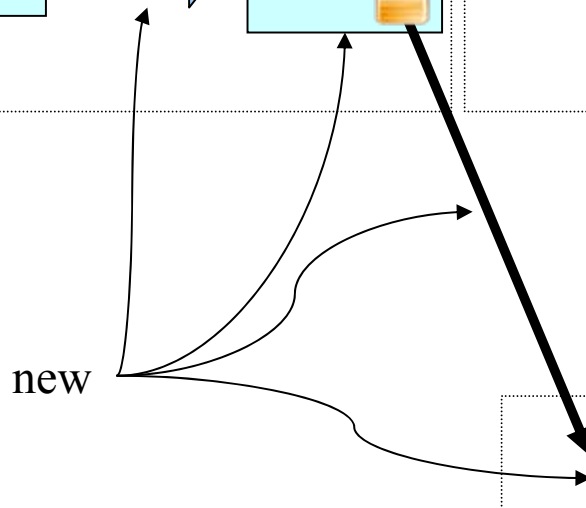
3. www is 1.2.3.4

2. Request www

1. Request www

4. www is 1.2.3.4

new

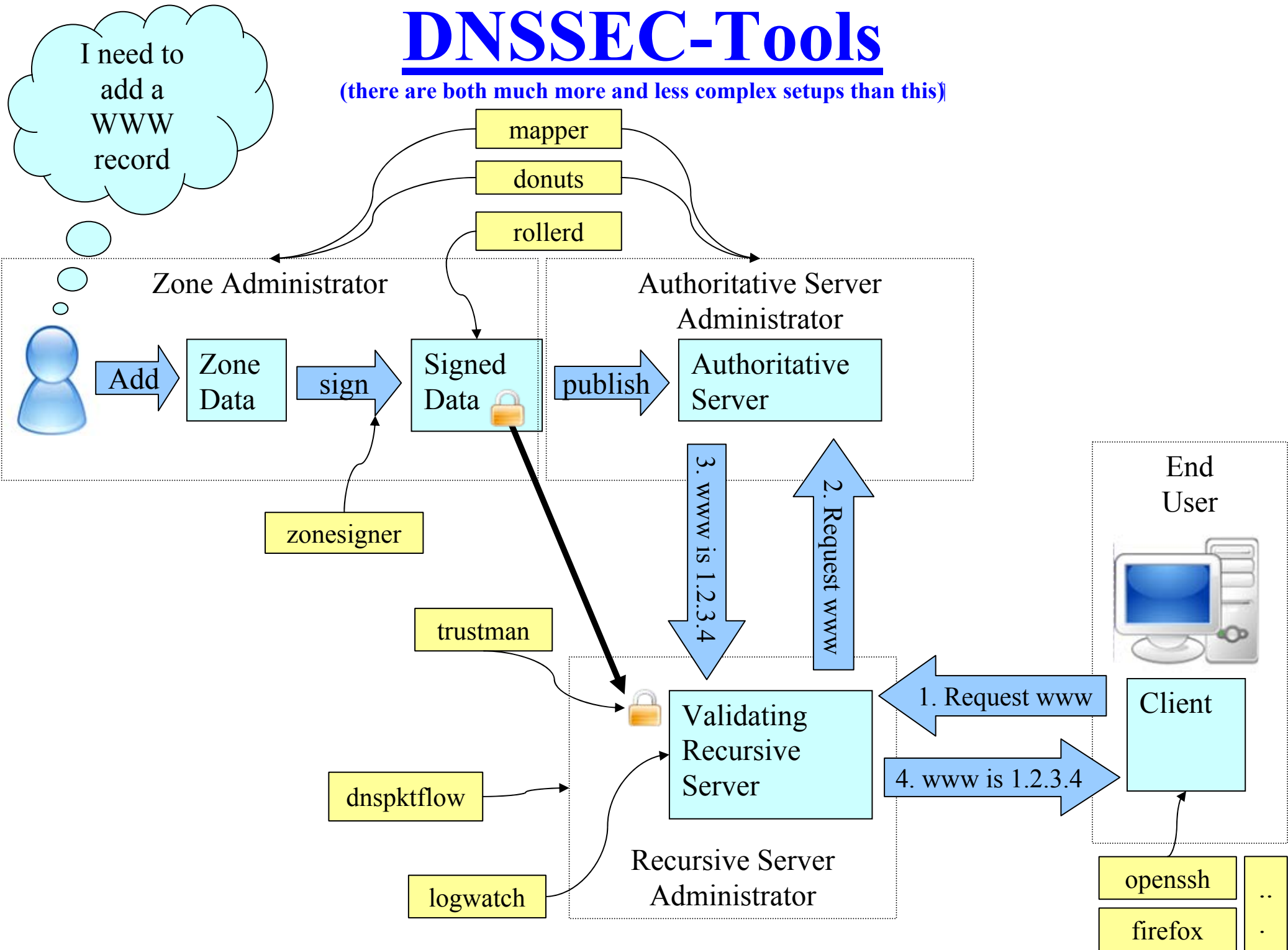


Some New Aspects With DNSSEC

- 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

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



DNSSEC-Tools Components

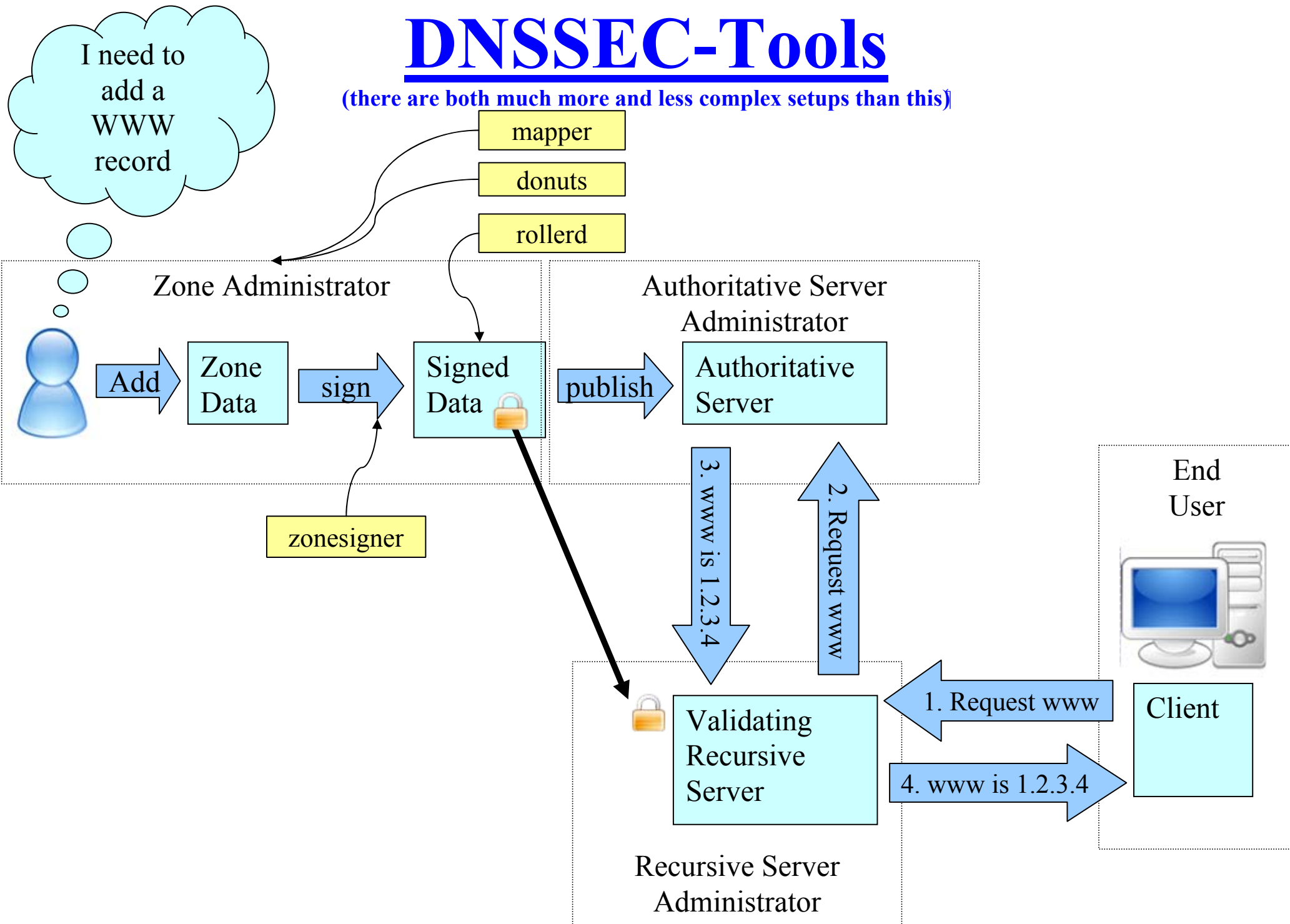
- Infrastructure
 - (Libraries, Perl Modules, ...)
- Tools for managing zones
 - (signers, lint, debug, ...)
- Tools for managing resolvers
 - (trust anchor management)
- Applications
 - (firefox, ssh, ncftp, ...)
- Educational Materials
 - (tutorials!!!, documentation)

Zone Administration Tools

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

DNSSEC-Tools

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



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

zonesigner: example

```
# zonesigner -genkeys example.com

    if zonesigner appears hung, strike keys until the program
completes
    (see the "Entropy" section in the man page for details)↑

zone signed successfully

example.com:
    KSK (cur) 25816  -b 2048  08/21/08      (example.com-signset-3)↑
    ZSK (cur) 54228  -b 1024  08/21/08      (example.com-signset-1)↑
    ZSK (pub) 28878  -b 1024  08/21/08      (example.com-signset-2)↑

zone will expire in 4 weeks, 2 days, 0 seconds
DO NOT delete the keys until this time has passed.
```

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: example

```
# donuts --level 8 -v example.com.signed example.com
```

```
[...]
```

```
--- Analyzing individual records in example.com.signed
```

```
--- Analyzing records for each name in example.com.signed
```

```
example.com:
```

```
Rule Name:    DNS_NO_DOMAIN_MX_RECORDS
```

```
Level:       8
```

```
Warning:     At least one MX record for example.com is suggested
```

```
sub2.example.com:
```

```
Rule Name:    DNSSEC_SUB_NOT_SECURE
```

```
Level:       3
```

```
Error:       sub-domain sub2.example.com is not securely delegated.  It  
             is missing a DS record.
```

```
results on testing example.com.signed:
```

```
rules considered:    28
```

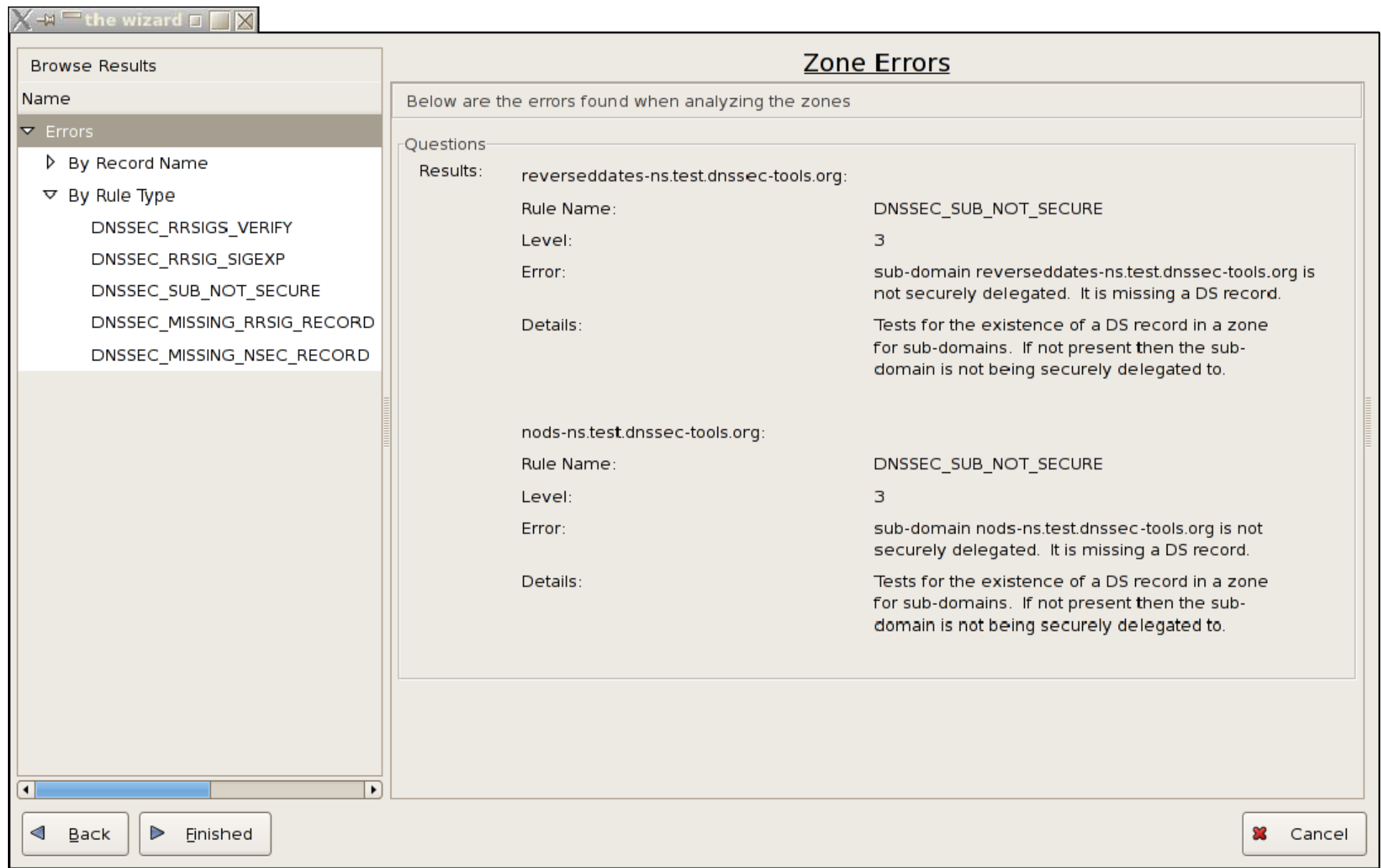
```
rules tested:       25
```

```
records analyzed:   52
```

```
names analyzed:     8
```

```
errors found:       2
```

donuts: Browsable GUI example

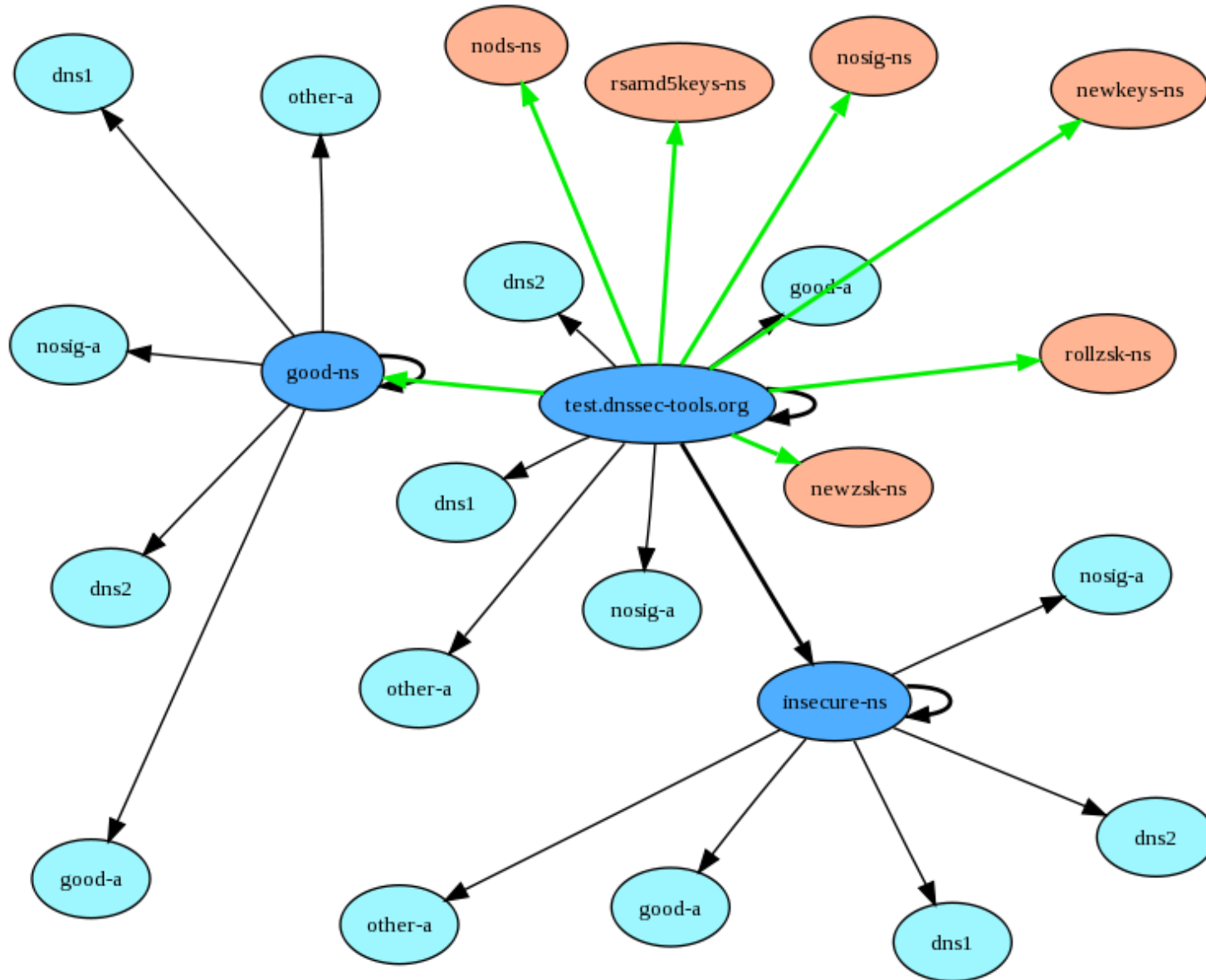


mapper

- 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



Authoritative Server Admin Tools

A subset of the Zone owner tools:

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

DNSSEC-Tools

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

mapper

donuts

I need to add a WWW record

Zone Administrator

Authoritative Server Administrator

End User



Client

Add

Zone Data

sign

Signed Data 

publish

Authoritative Server

3. www is 1.2.3.4

2. Request www

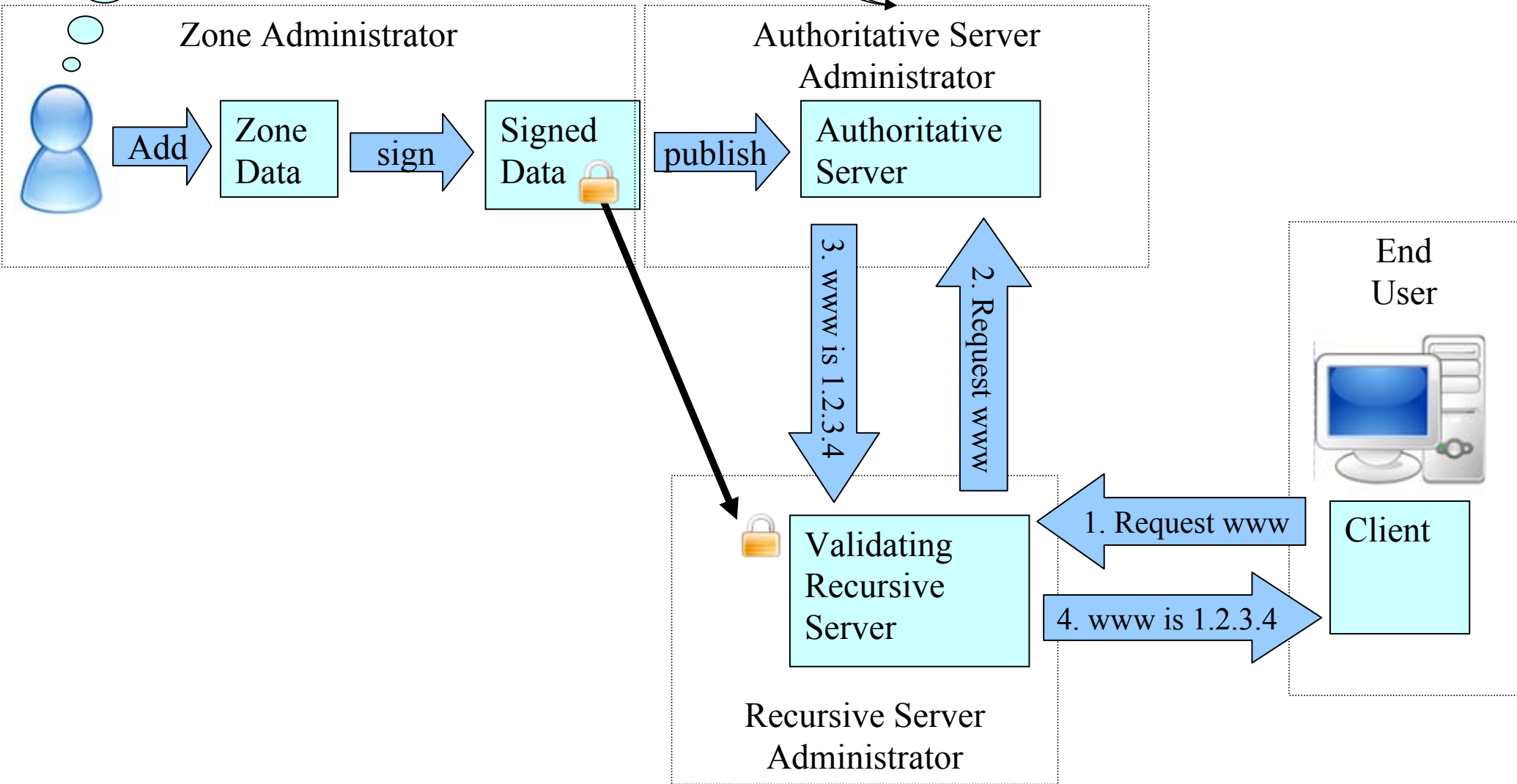


Validating Recursive Server

1. Request www

4. www is 1.2.3.4

Recursive Server Administrator



Validating Recursive Server Tools

- Trust Anchor Management
 - Trustman

- Debugging
 - dnspktflow

- Name Server Error Reporting
 - logwatch

DNSSEC-Tools

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

I need to add a WWW record

Zone Administrator

Authoritative Server Administrator

End User

Client

Recursive Server Administrator

Add

Zone Data

sign

Signed Data

publish

Authoritative Server

3. www is 1.2.3.4

2. Request www

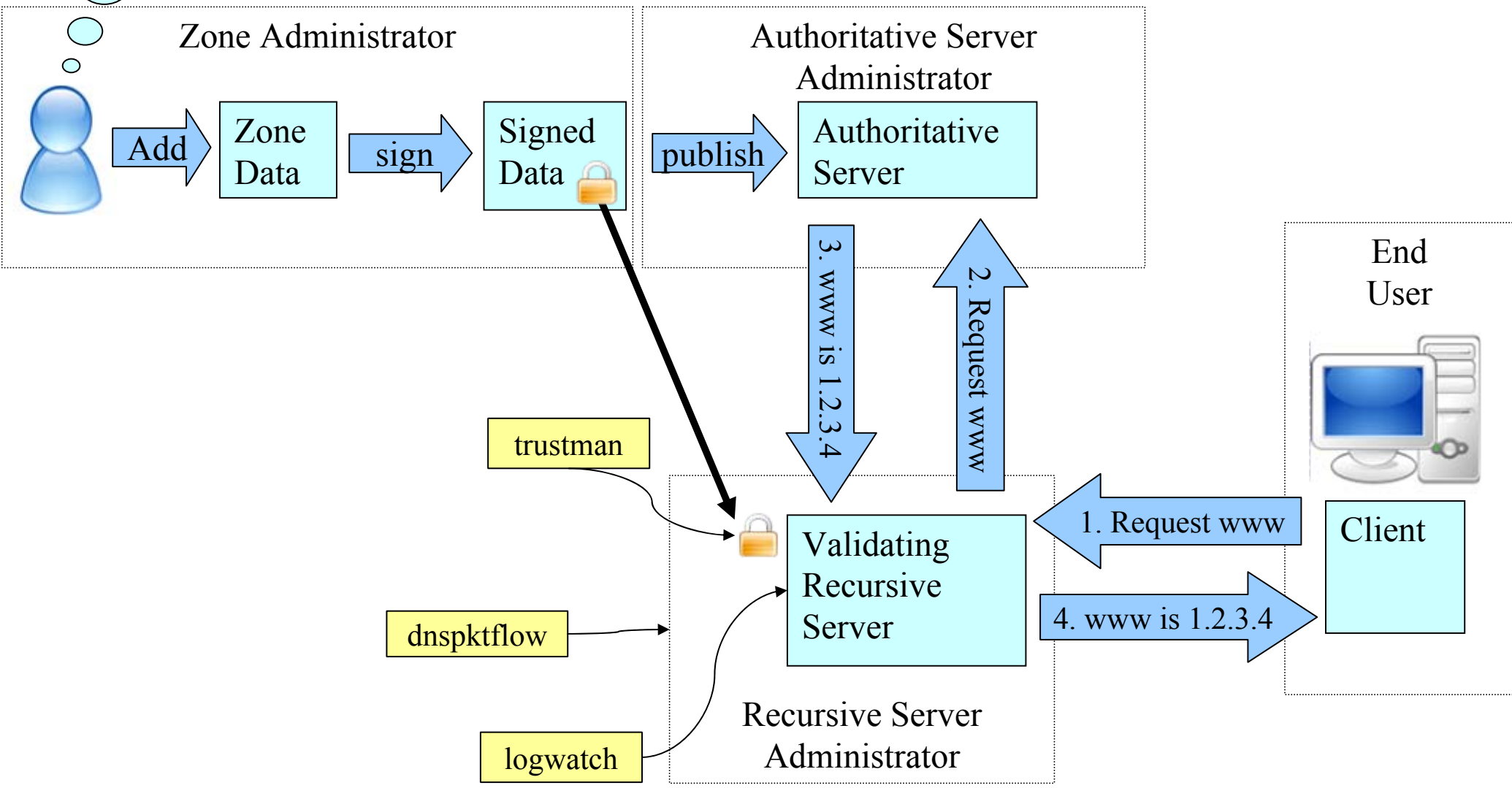
1. Request www

4. www is 1.2.3.4

trustman

dnspktflow

logwatch



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

trustman: example

```
# trustman -f -S -v
```

```
reading and parsing trust keys from /usr/local/etc/dnssec-tools/dnsval.conf
```

```
Reading and parsing trust keys from /etc/dnssec-tools/dnsval.conf
```

```
Found a key for dnssec-tools.org
```

```
Checking zone keys for validity
```

```
Checking the live "dnssec-tools.org" key
```

```
dnssec-tools.org ... refresh_secs=43200, refresh_time=1209637099
```

```
adding holddown for new key in dnssec-tools.org (1209680299 seconds from now)␣
```

```
sending mail to root@example.com
```

```
Writing new keys to /etc/dnssec-tools/trustman.storage
```

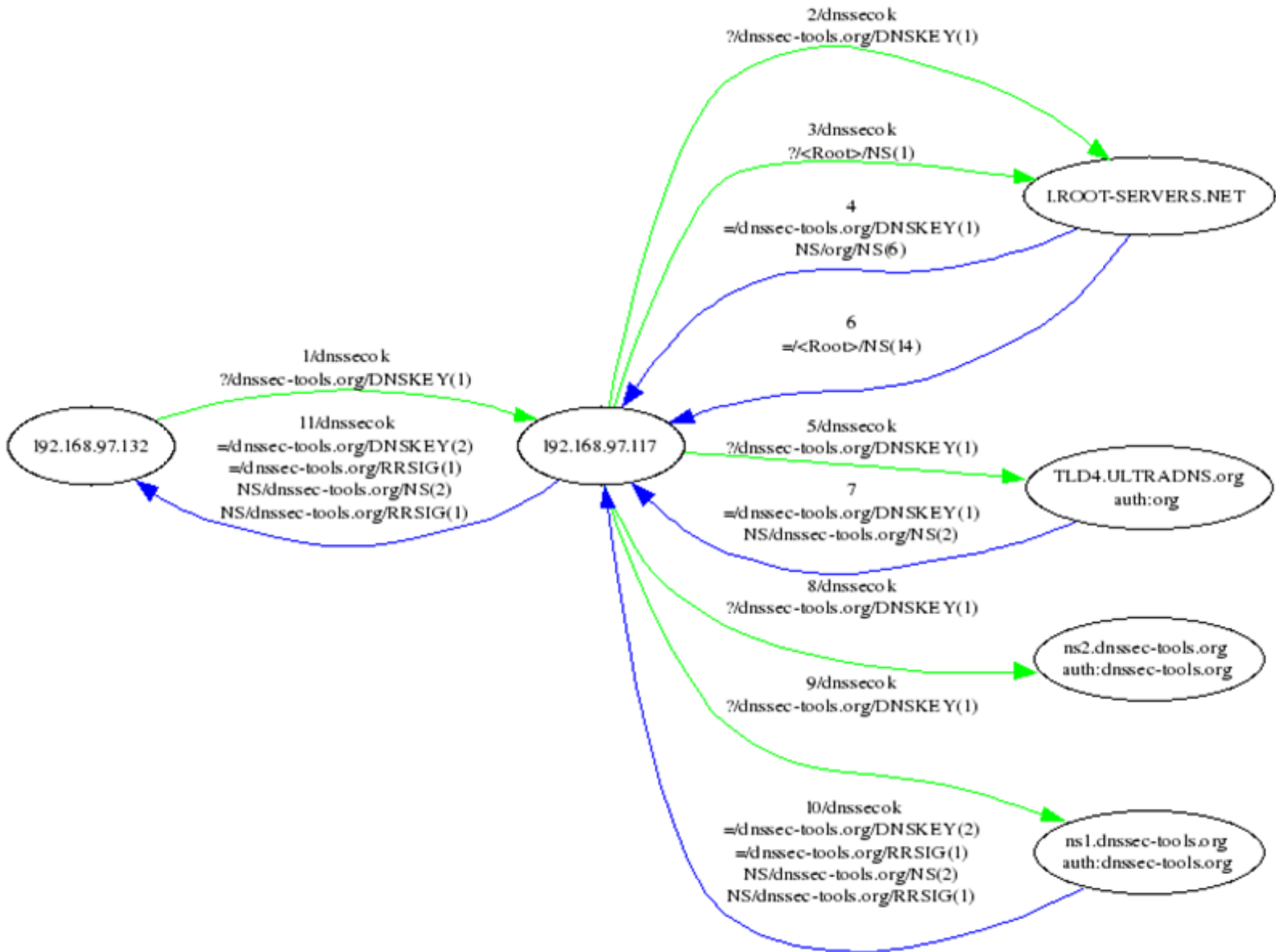
```
checking new keys for timing
```

```
hold down timer for someone.com still in the future (86400 seconds)␣
```

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

logwatch: example

```
##### LogWatch 6.0.2 (04/25/05) #####  
  Processing Initiated: Thu Jul  7 10:13:34 2005  
  Date Range Processed: all  
  Detail Level of Output: 10  
    Type of Output: unformatted  
    Logfiles for Host: host.example.com  
#####
```

----- DNSSEC Begin -----

No Valid Signature received 6 times

Detail >= 5 log messages:

Marking as secure 97 times

Verified rdataset succeeded 97 times

Attempted positive response validation 96 times

Nonexistence proof found 20 times

Attempted negative response validation 18 times

Validation OK 2 times

----- DNSSEC End -----

----- Resolver Begin -----

Received validation completion event 171 times

Validation OK 125 times

Nonexistence validation OK received 46 times

----- Resolver End -----

```
##### LogWatch End #####
```

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
 - Many!

DNSSEC-Tools

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

I need to
add a
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

 Validating
Recursive
Server

Recursive Server
Administrator

1. Request www

4. www is 1.2.3.4

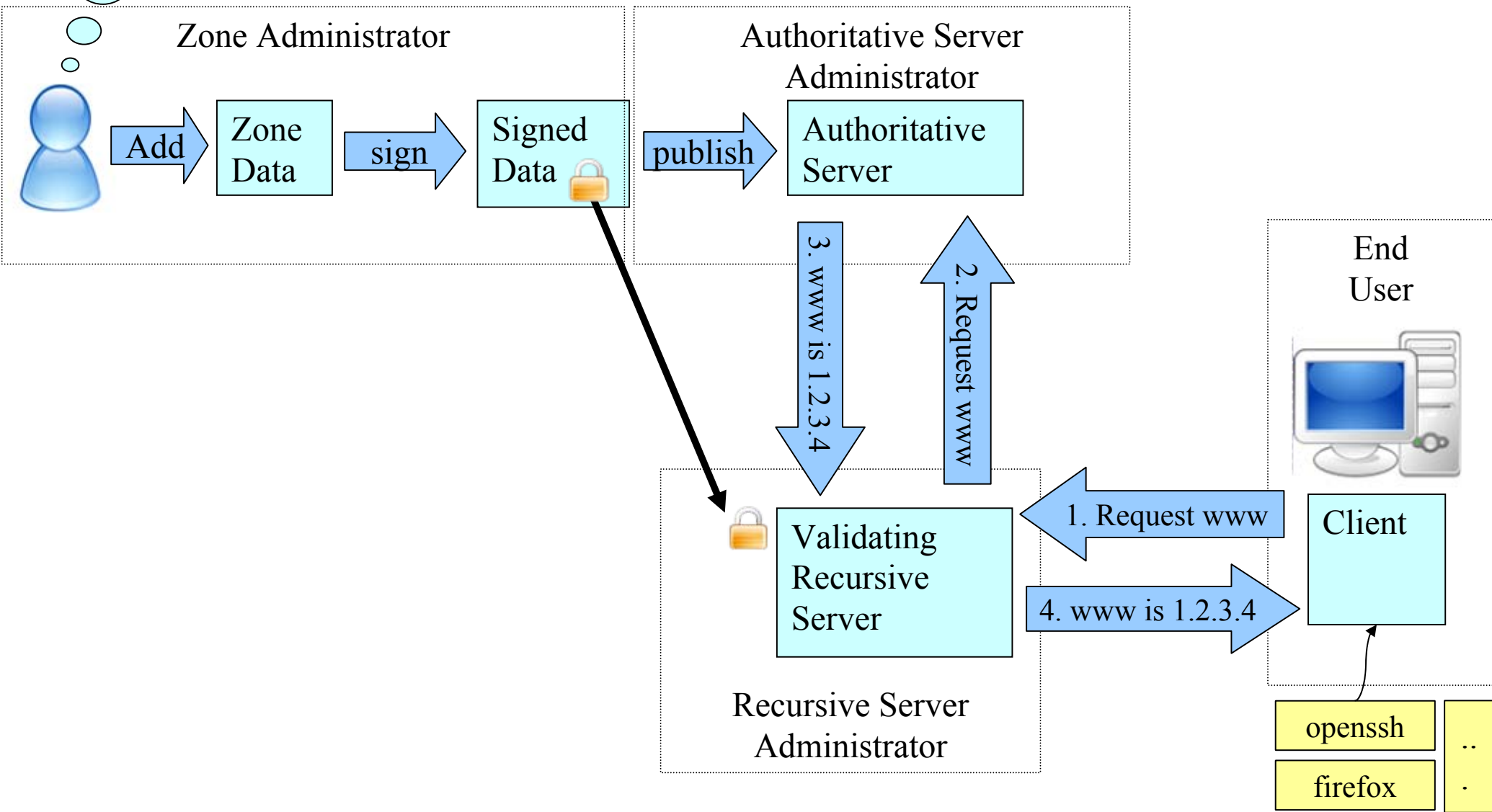
End
User



Client

openssh ..

firefox .



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 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-dnsext-validator-api-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

firefox

The Dnssec-Tools Project

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

Getting Started Latest Headlines

DNSSEC Tools

Is your domain secure?

[Why?](#)

About This Project

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

- [Tool Descriptions and ScreenShots](#)
- [Download](#)

To contact the project developers, please write the dnssec-tools-users_AT_lists.sourceforge.net_mailing_list or submit bugs to the [bug database](#).

Project News

DNSSEC-Tools Resources

- Main Page
- Tool Descriptions And Screen-Shots
- Download
- Additional Documentati
- Test Zone

Project Links

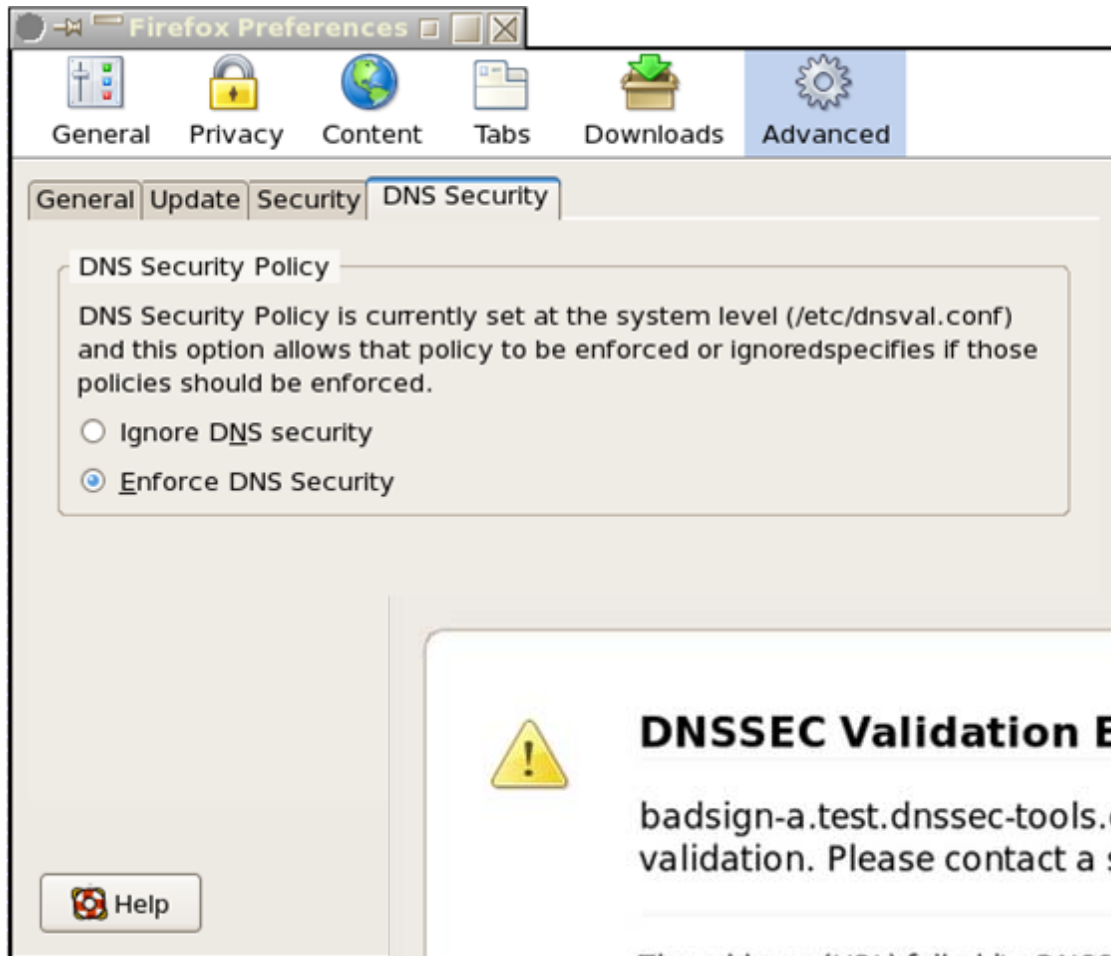
- SF Project Page
- Mailing Lists
- SVN Repository
- Bug Database

Other Useful Si

- Bind Software

Done DNSSEC: Secure: 2 Insecure: 2 Errors: 1

firefox: example



DNSSEC Validation Error

badsign-a.test.dnssec-tools.org failed its DNSSEC security check validation. Please contact a security or system administrator for help.

The address (URL) failed its DNSSEC security check validation. Please contact a system administrator for help.

Try Again

firefox: example

- Blocks inline components



- A summary plugin:



thunderbird

The screenshot shows the Mozilla Thunderbird email client interface. The window title is "Inbox for alice@fruits.netsec.tislabs.com - Mozilla Thunderbird". The menu bar includes File, Edit, View, Go, Message, Tools, and Help. The toolbar contains icons for Get Mail, Write, Address Book, Reply, Reply All, Forward, Delete, Junk, Print, and Stop. The Folders pane on the left shows the account structure for alice@fruits.netsec.tislabs.com (Inbox, Trash) and bob@demo.netsec.tislabs.com (Local Folders). The main pane displays a list of messages with columns for Subject, Sender, and Date. The selected message is from Bob with the subject "Hi", sent at 10:43 AM. The message content shows the following headers:

Subject: Hi
From: Bob <bob@demo.netsec.tislabs.com>
Date: 10:43 AM
To: alice@fruits.netsec.tislabs.com

Received-SPF: pass (mechanism)
Receiver: fruits.netsec.tislabs.com
Client-IP: 158.69.82.20
HELO: demo.netsec.tislabs.com

Envelope-From: bob@demo.netsec.tislabs.com

X-DNSSEC: "fail (DNSSEC validation failed for the SPF (TXT) record of 'demo.netsec.tislabs.com', DNSSEC validation fail"

The body of the email contains the text "Hi".

At the bottom of the window, a status bar indicates "There are no new messages on the server." and shows "Unread: 0" and "Total: 1".

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

Conclusions and Future Work

- DNSSEC adds to cost and complexity but the availability of good tools can reduce much of this.
- Zone operators have diverse environments, so any tools developed must 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.

Questions?

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

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