DNSSEC-Tools

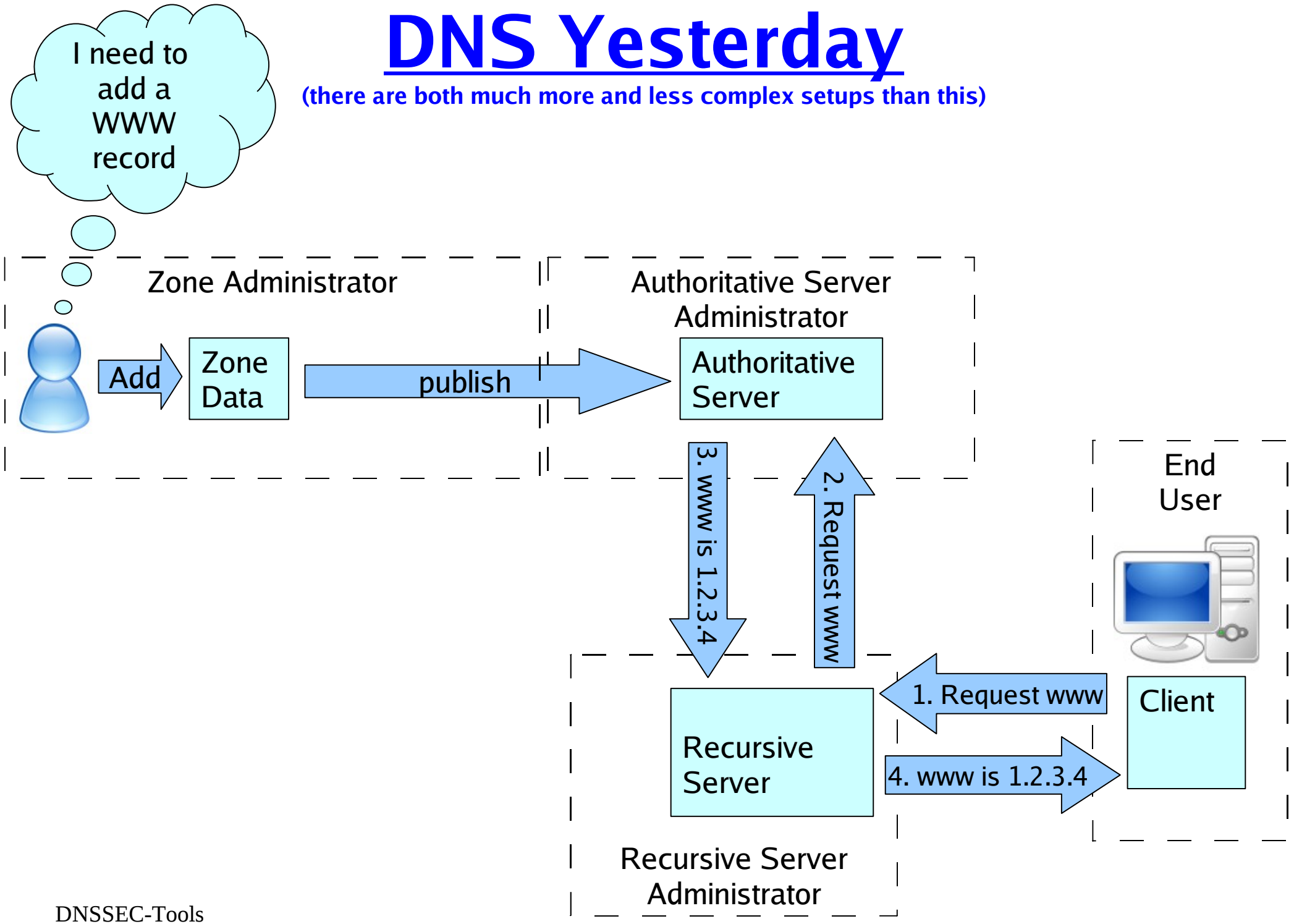
Wes Hardaker
SPARTA, Inc.
<hardaker@sparta.com>

Overview

- DNS Today
- DNS with SEC
- DNSSEC-Tools
  - Background
  - Zone Administrators
  - Authoritative Server Administrators
  - Recursive Server Administrators
  - End-Users

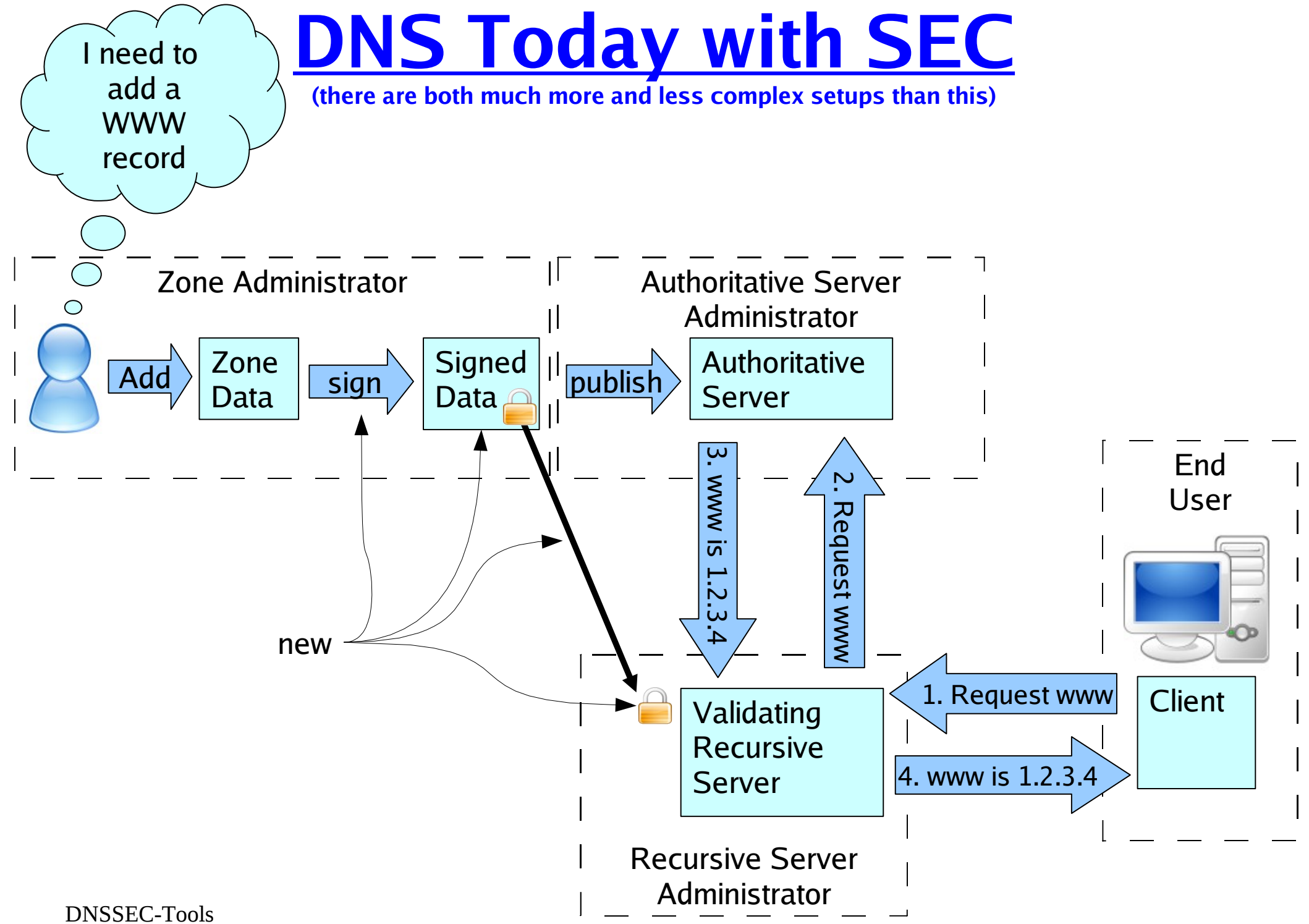
DNS Yesterday

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



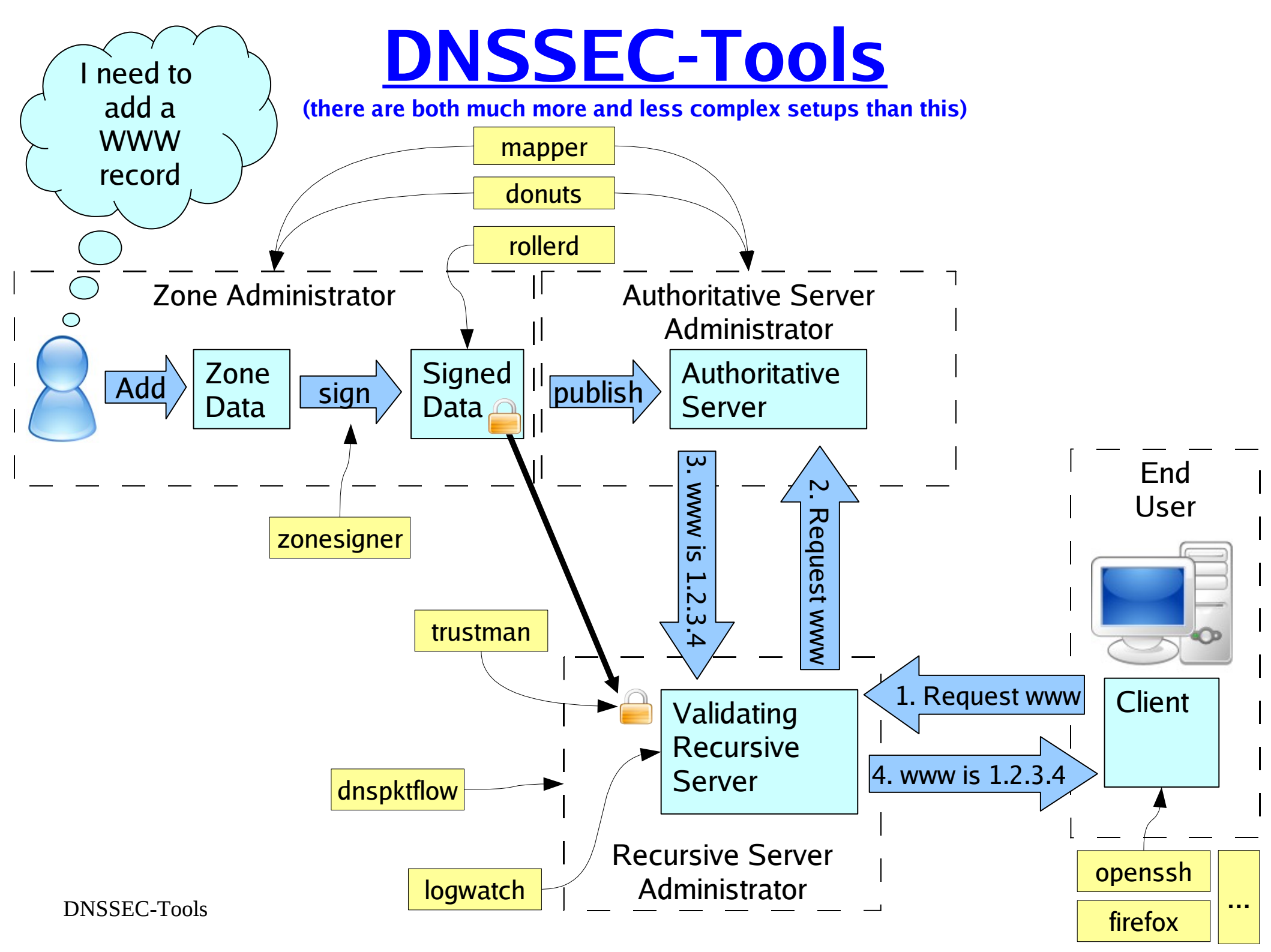
DNS Today with SEC

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



DNSSEC-Tools

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



DNSSEC-Tools

Project Background

DNSSEC-Tools

- SPARTA is developing DNSSEC-Tools
  - http://www.dnssec-tools.org/
  - Open Source Project
  - Sponsored by DHS and is 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

DNSSEC-Tools Components

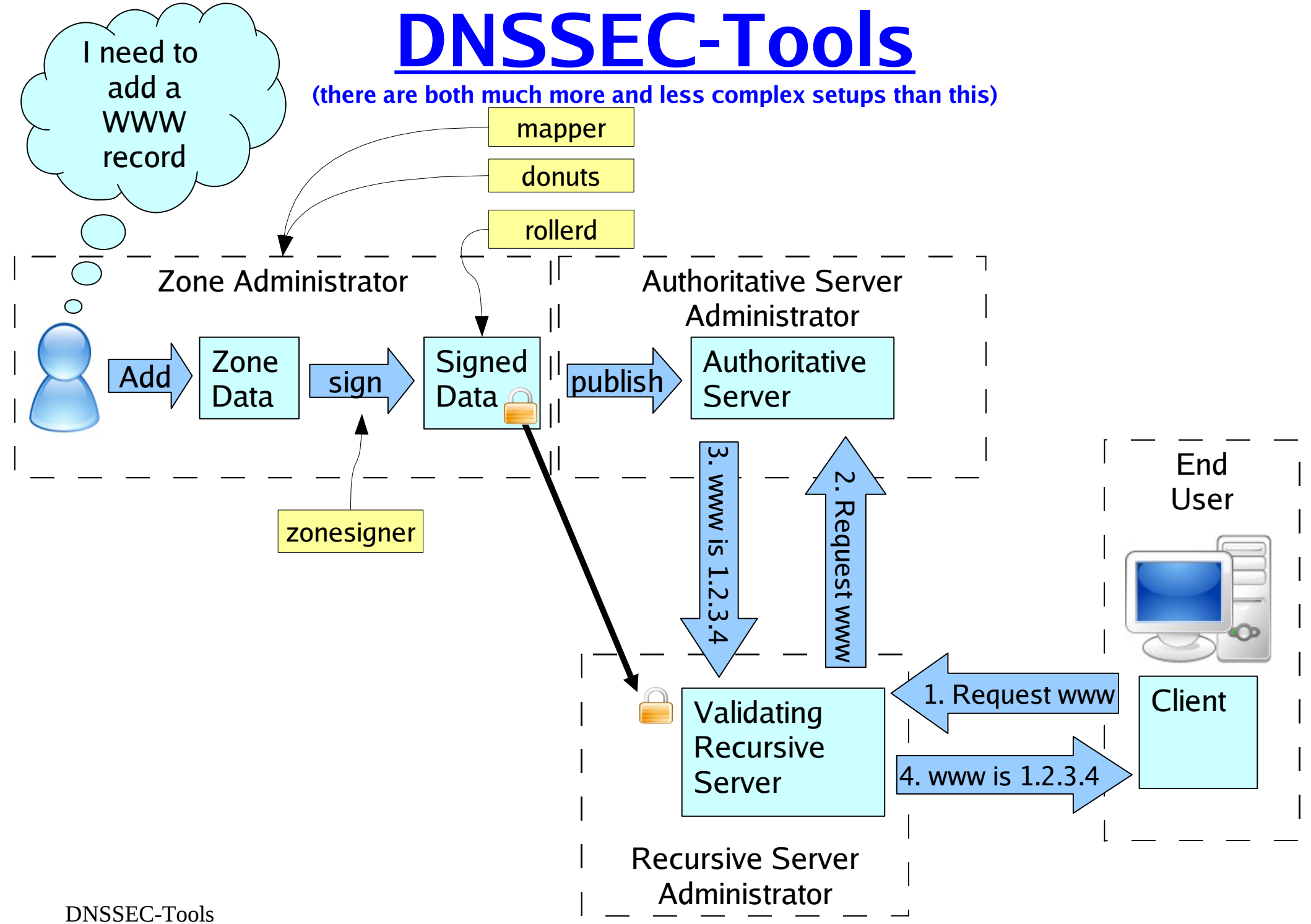
- Infrastructure
  - (Libraries, Perl Modules, ...)
- Tools for managing zones
  - (signers, lint, debug, ...)
- Tools for managing resolvers
  - (trust anchor management)
- Applications
  - (firefox, ssh, ncftp, ...)
- Educational Materials
  - (***tutorials!!!***, documentation)

Zone Administration Tools

- DNSSEC Maintance:
  - 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”

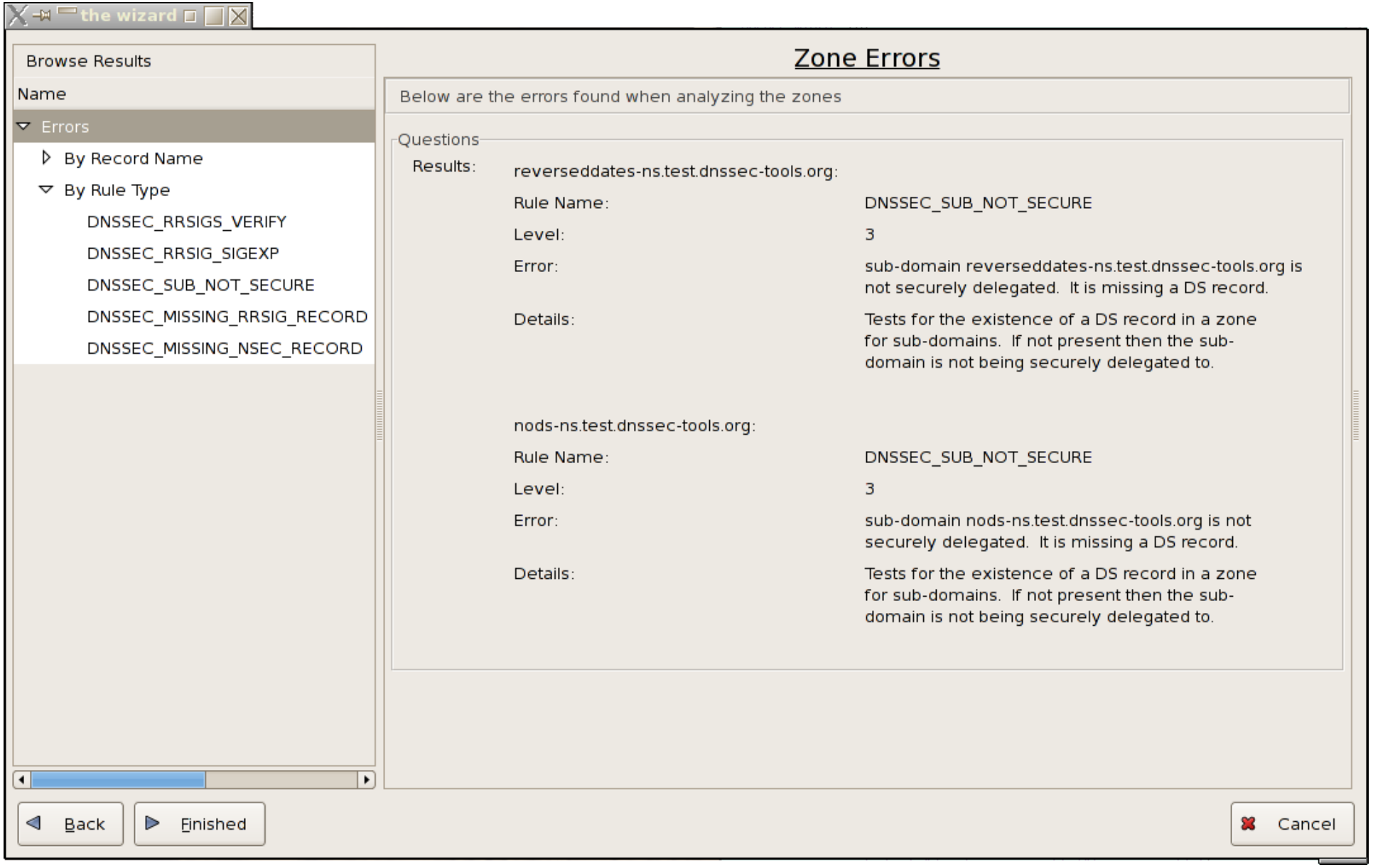
donuts

- 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

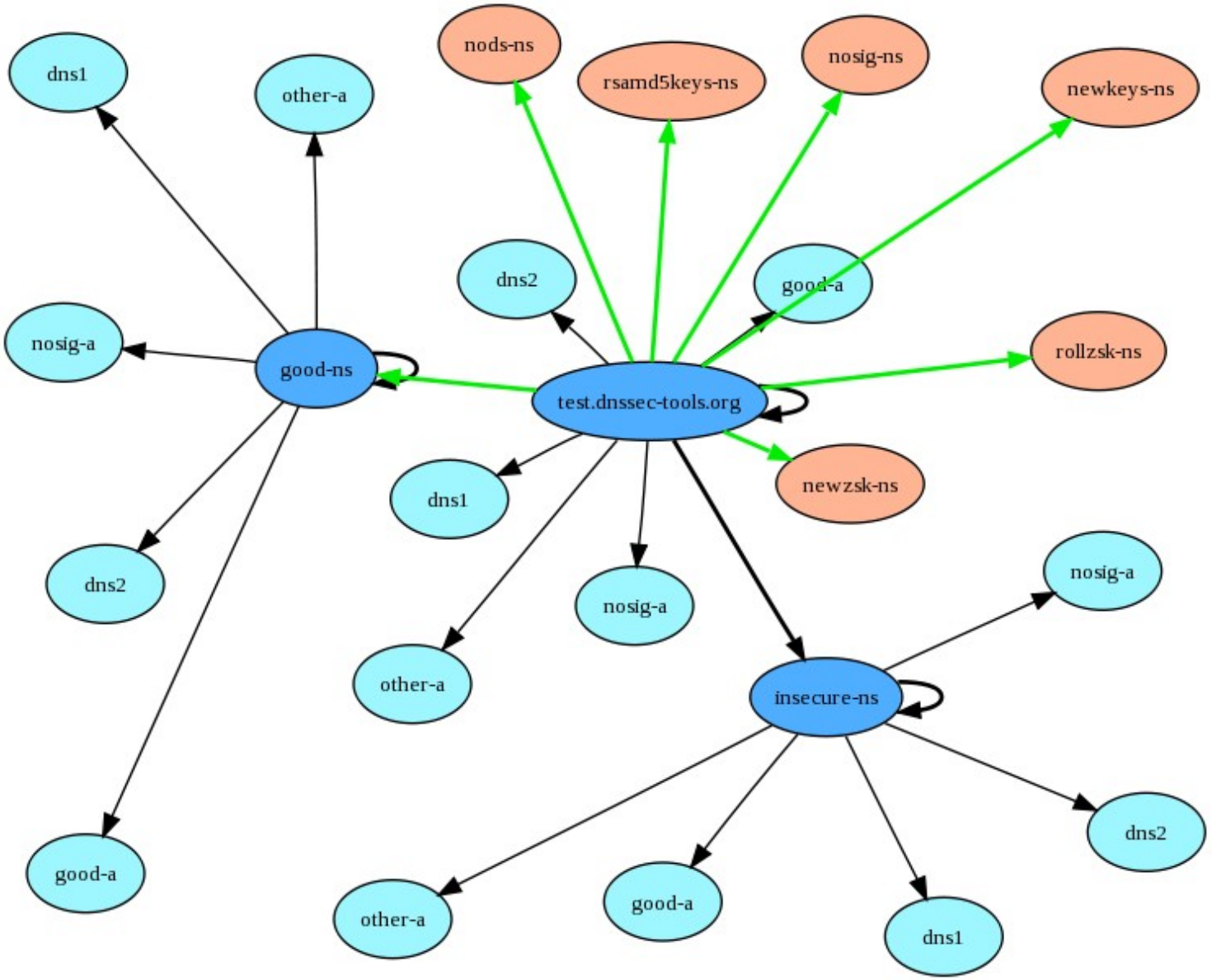


mapper

- 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



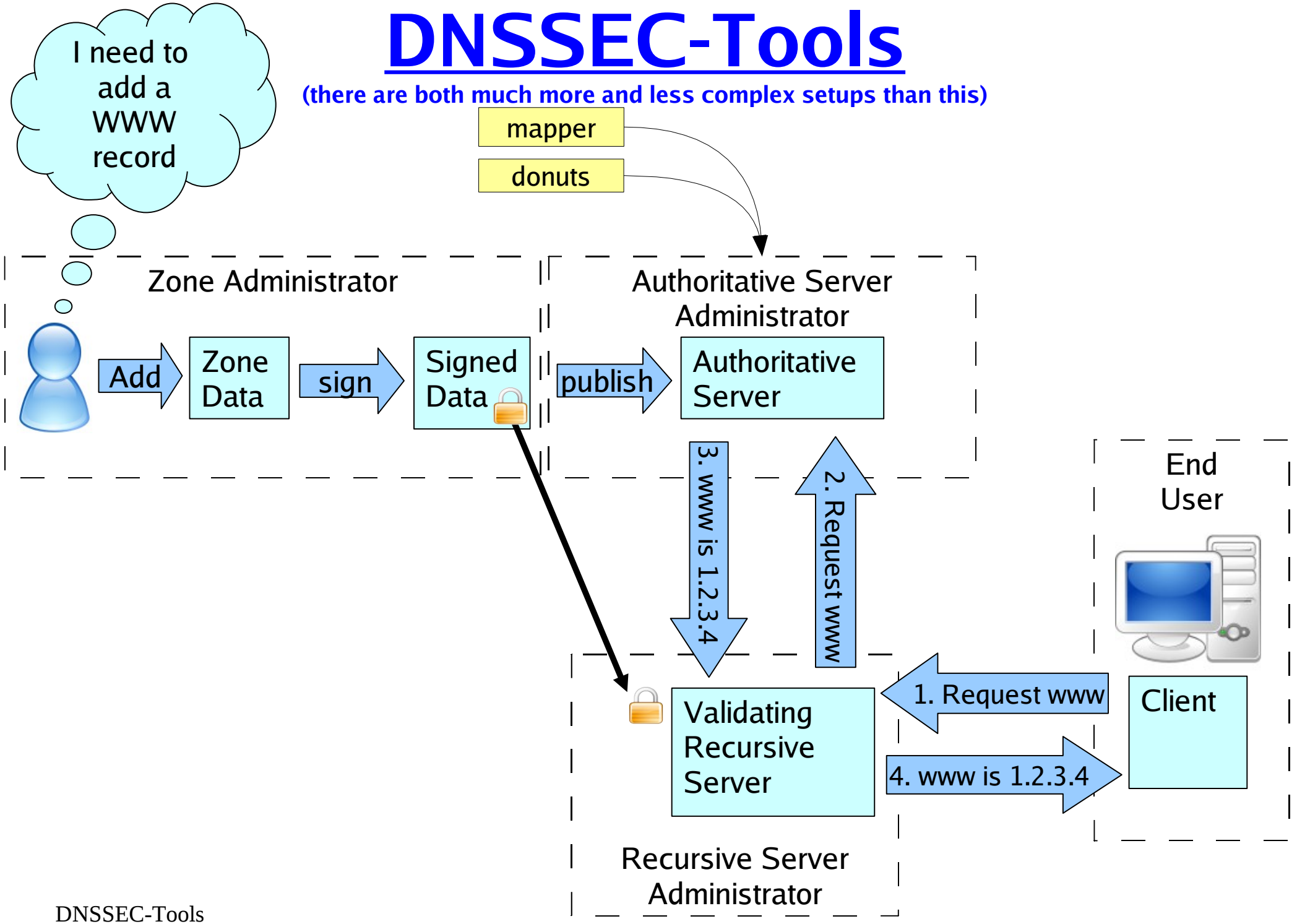
Authoritative Server Admin Tools

A subset of the Zone owner tools:

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

DNSSEC-Tools

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

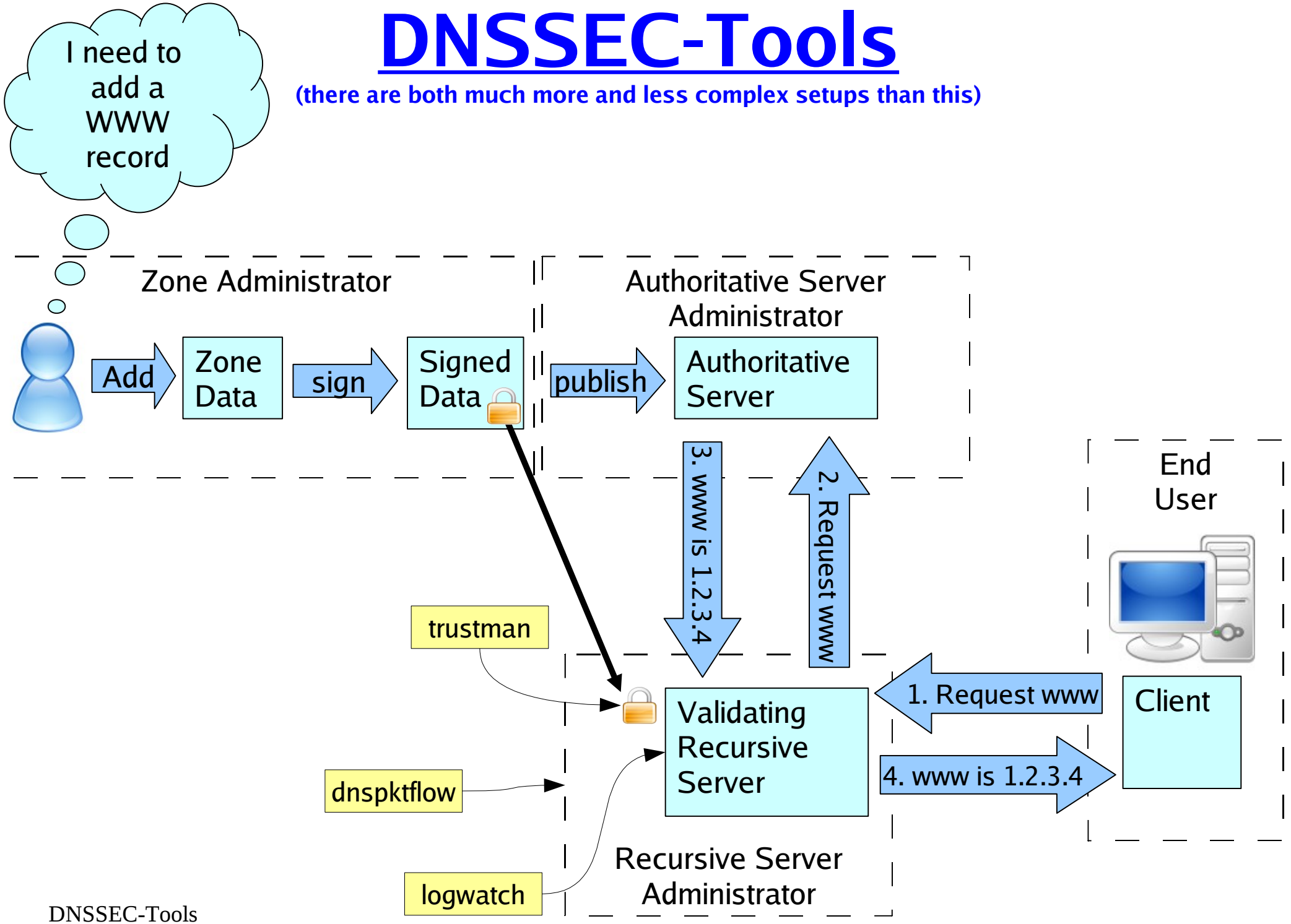


Validating Recursive Server Tools

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

DNSSEC-Tools

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



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

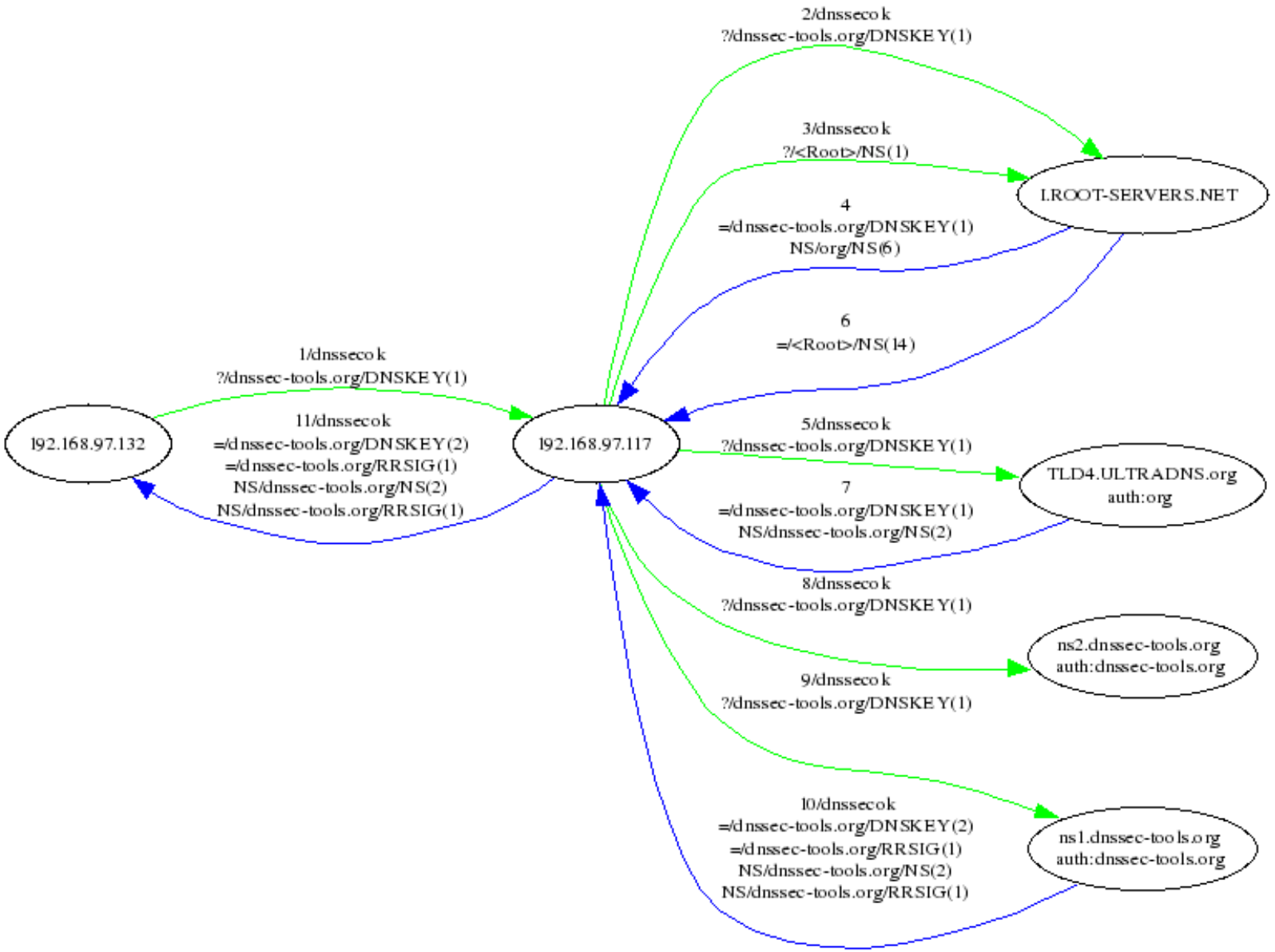
trustman: example

```
# 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 somezone.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

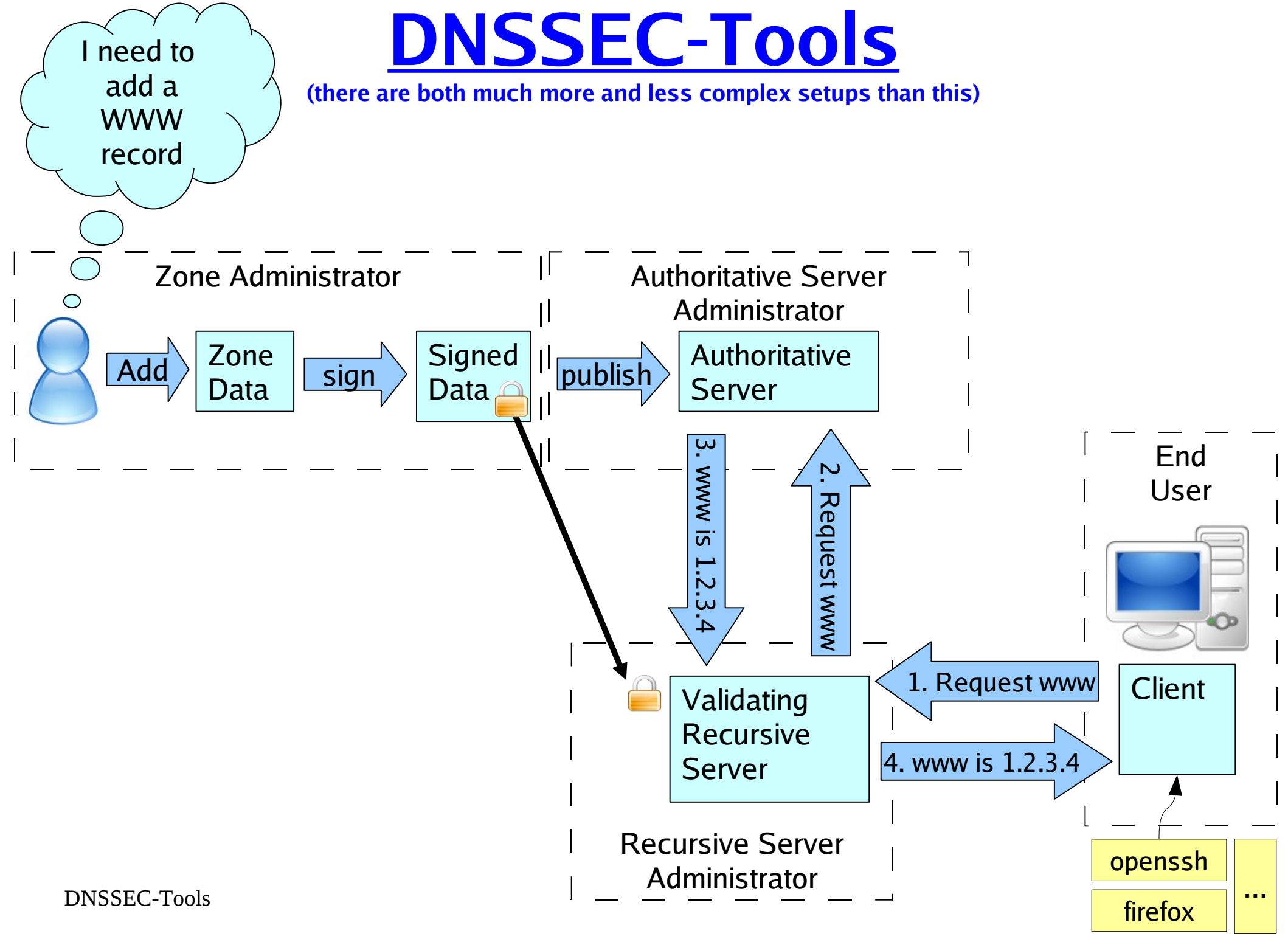
```
################### LogWatch 6.0.2 (04/25/05) ####################
       Processing Initiated: Thu Jul  7 10:13:34 2005
       Date Range Processed: all
     Detail Level of Output: 10
           Type of Output: unformatted
         Logfiles for Host: host.example.com
 ##################################################################

---------- 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

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

DNSSEC-Tools

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



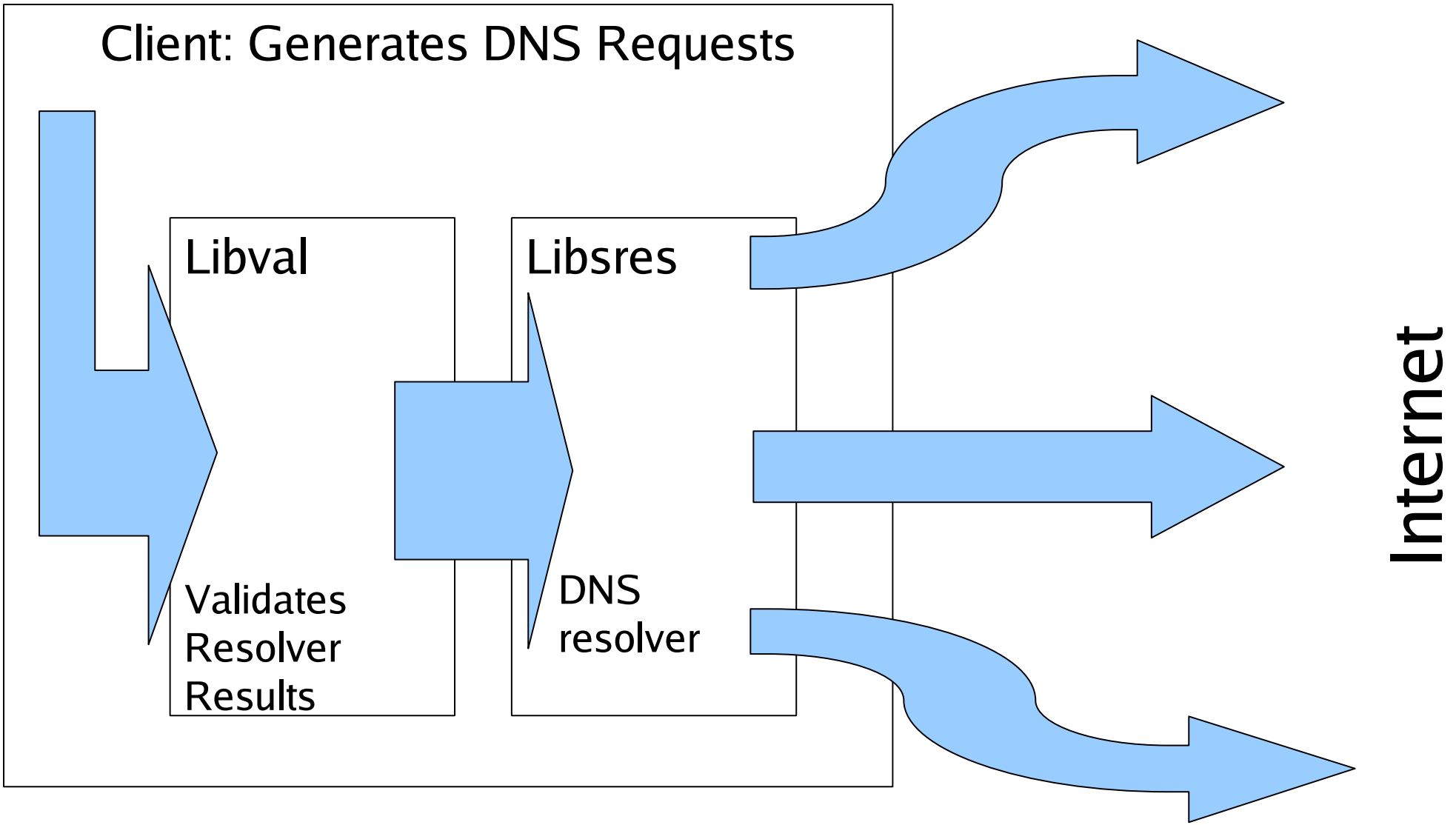
DNSSEC-Aware Applications

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

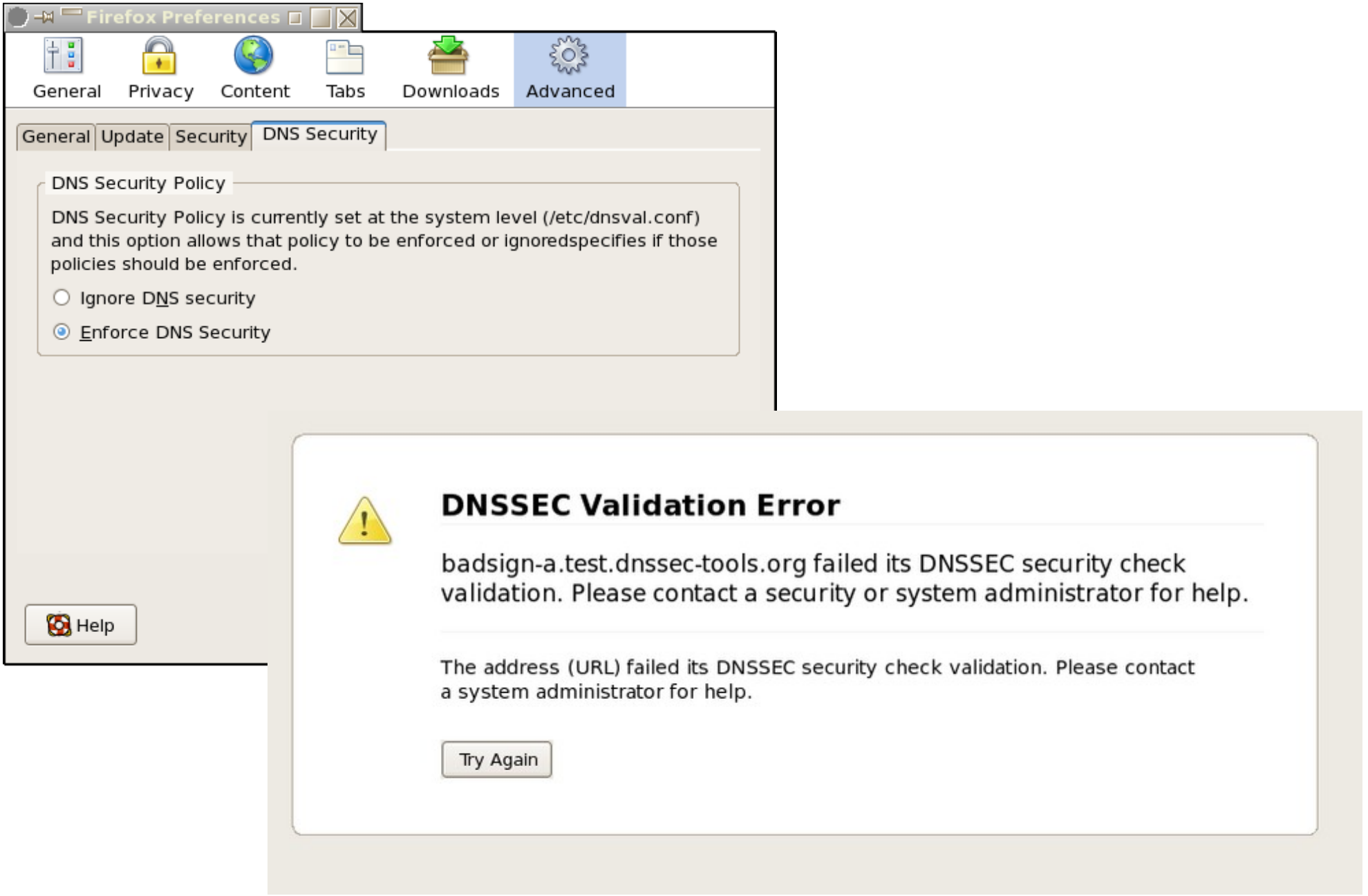
DNSSEC-Tools: Libraries

- DNSSEC validating resolver library
  - 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

DNSSEC-Tools' libval / libsres



firefox: example

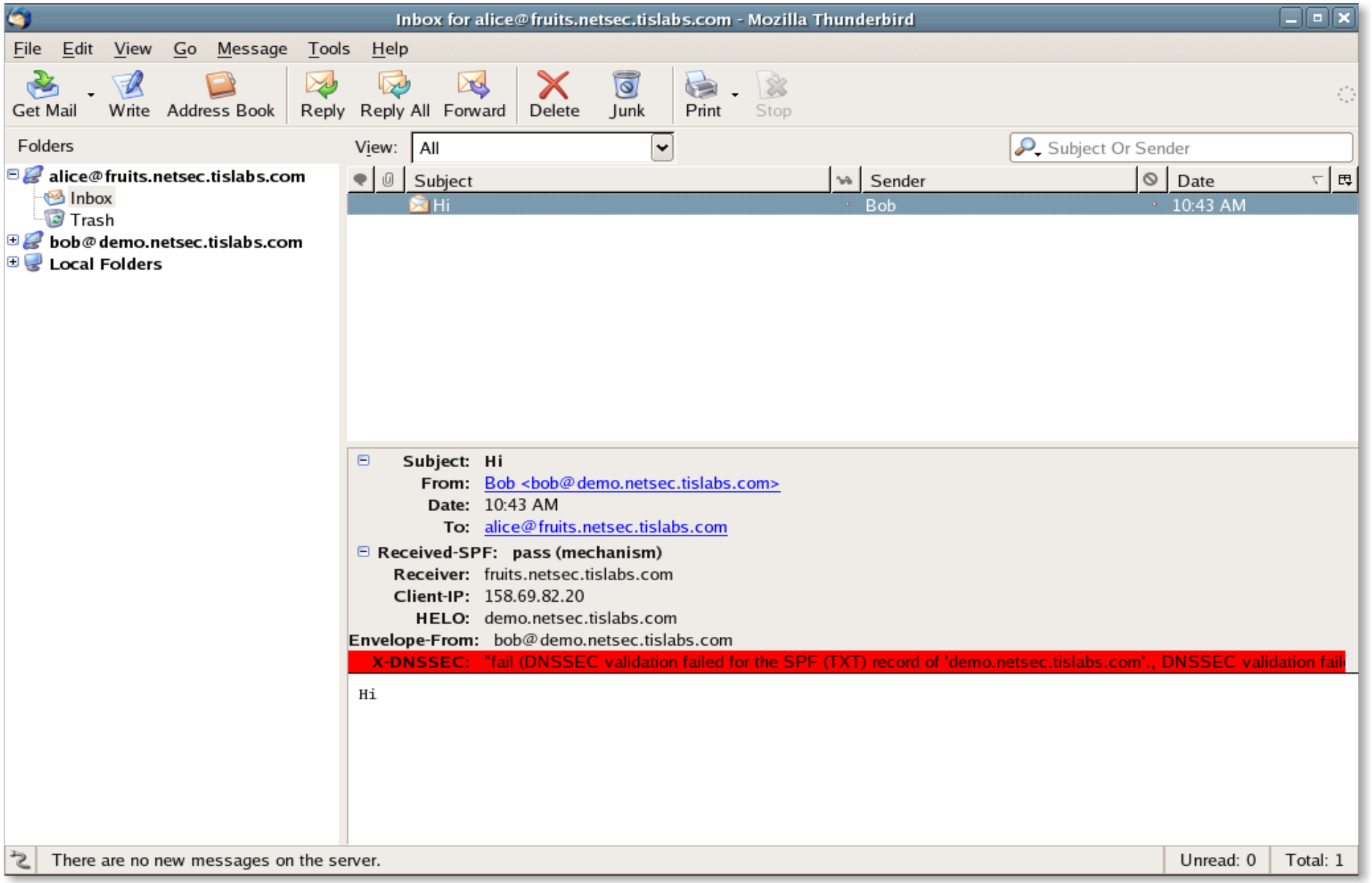


firefox: example

- Blocks inline components

- A summary plugin:

thunderbird



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

Questions?

???