# DNSSEC and DANE Deployment Trends, Tools And Challenges

Dan York, Senior Content Strategist
Internet Society

ENOG 6, Kiev, Ukraine
October 2, 2013

# About Deploy360

## The Challenge:

- The IETF creates protocols based on open standards, but some are not widely known or deployed
- People seeking to implement these protocols are confused by a lack of clear, concise deployment information

## The Deploy360 Solution:

- Provide hands-on information on IPv6, DNSSEC and routing resiliency/security to advance real-world deployment
- Work with first adopters to collect and create technical resources and distribute these resources to fast following networks

# Deploy360 Components

## Web Portal

*(Online Knowledge Repository)*

- Technical documents
- Audience-specific information
- Blogs & social media

## Social Media

*(Constant Audience Engagement)*

- Twitter
- Facebook
- Google+
- YouTube
- RSS Feeds

## Speaking Engagements

*(Come Meet Us or Invite Us to Speak)*

- Consumer Electronics Show
- IPv6 Summits
- Interop
- Network Operators' Groups

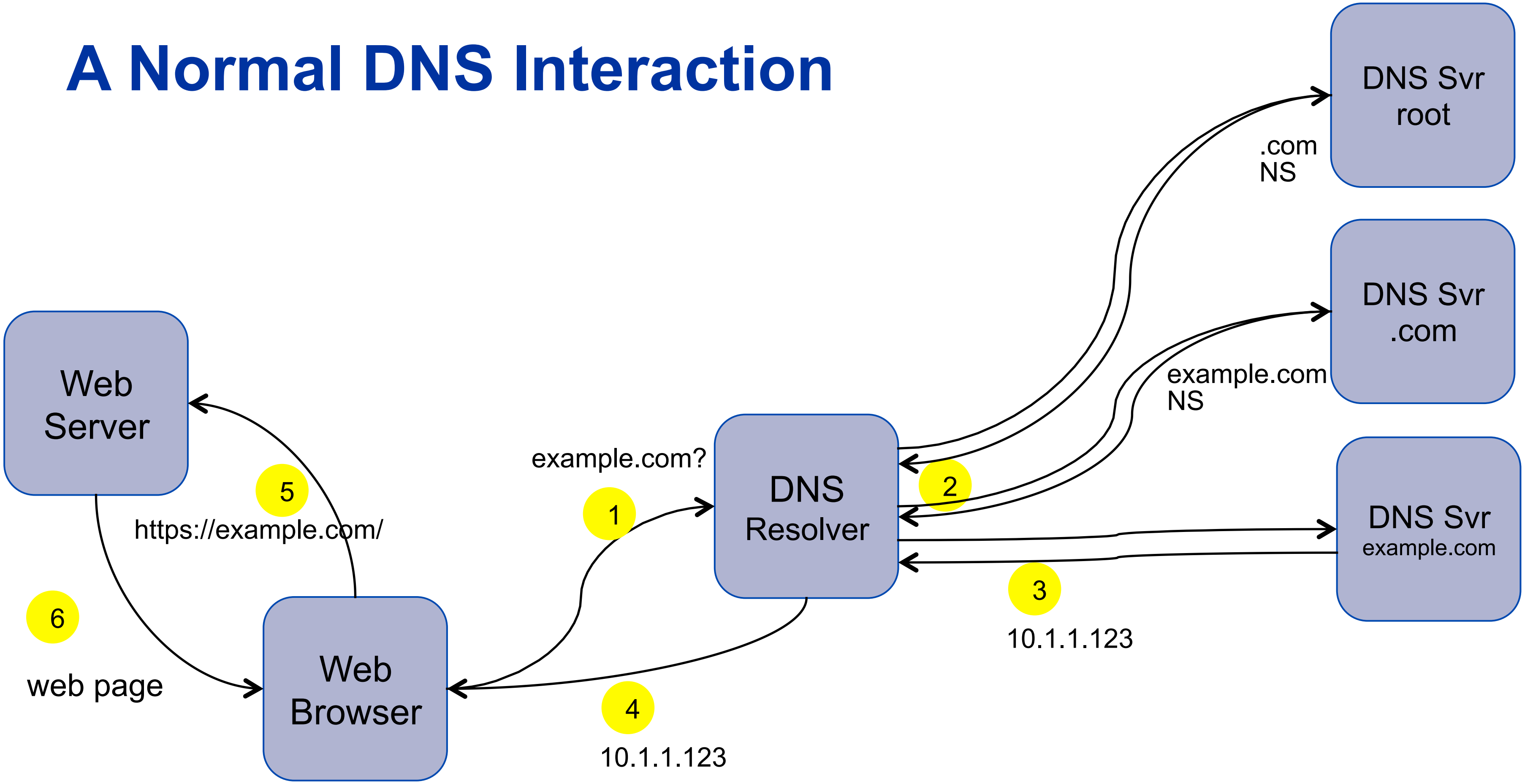
## ION Conferences

*(Hands-on Educational Events)*

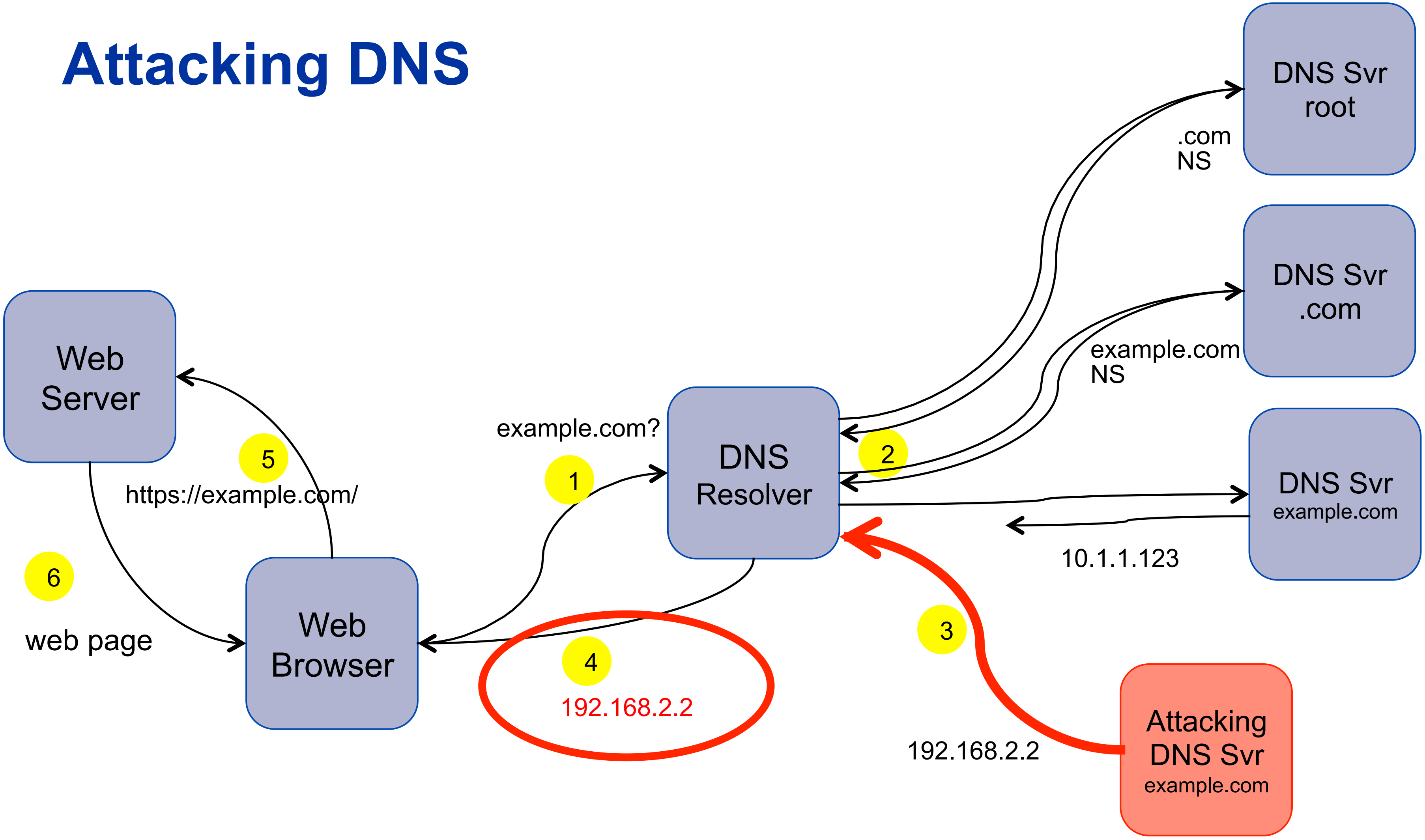
- Slovenia
- India
- USA
- Canada
- Argentina

# A Quick Overview of DNSSEC

# A Normal DNS Interaction

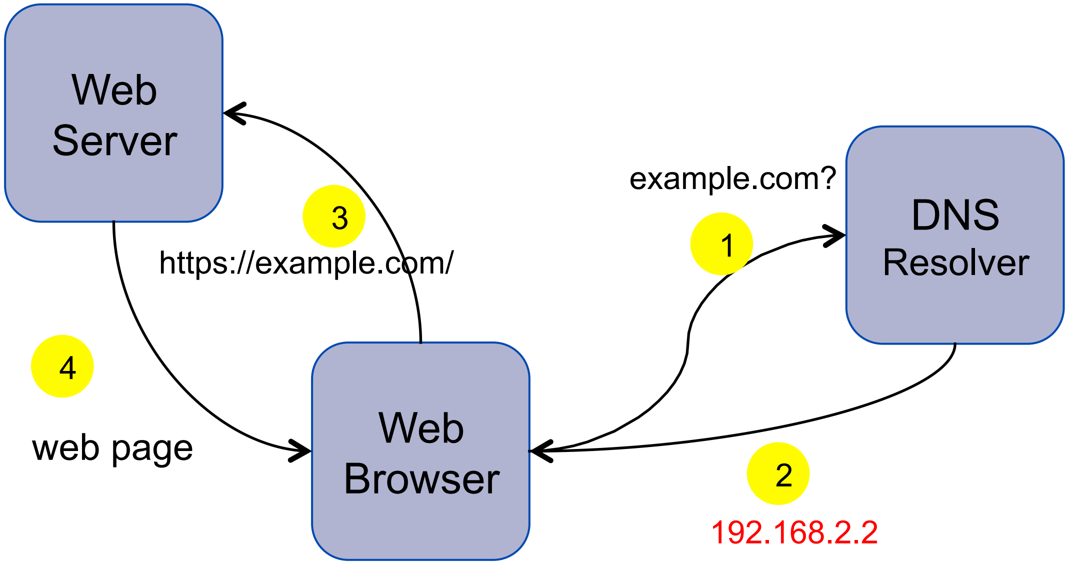


# Attacking DNS



Internet Society™

# A Poisoned Cache

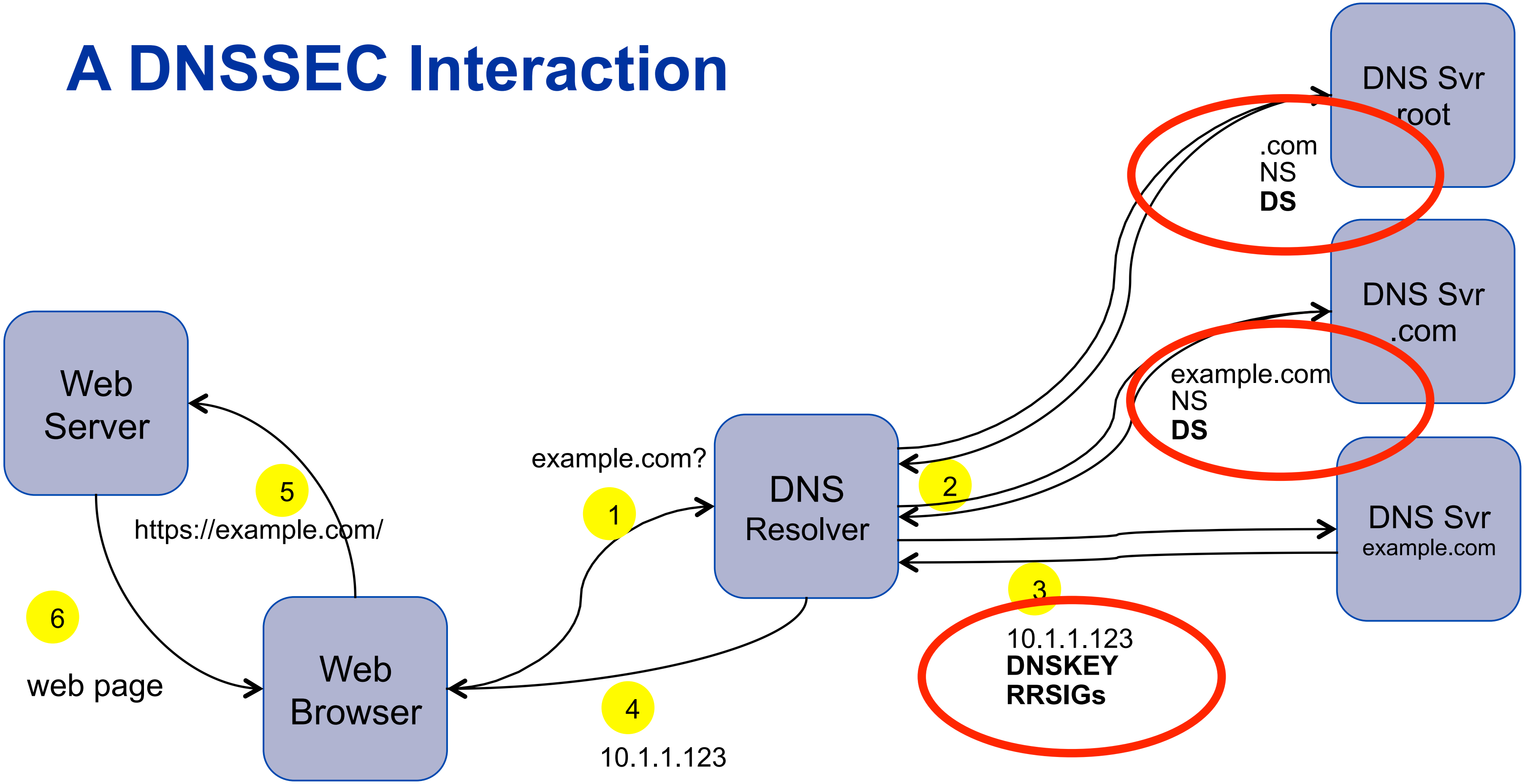


Resolver ***cache*** now has wrong data:

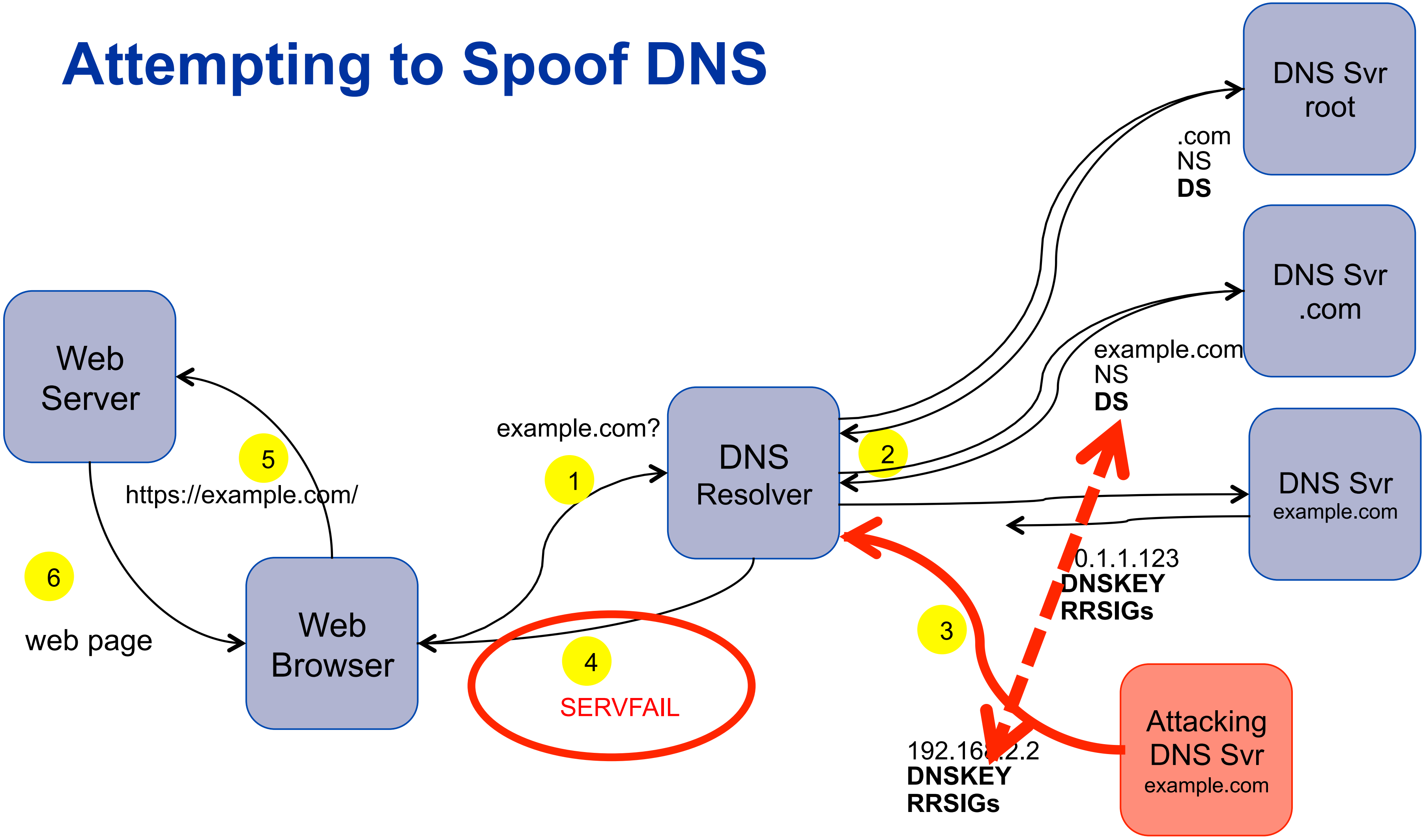
example.com 192.168.2.2

This stays in the cache until the Time-To-Live (TTL) expires!

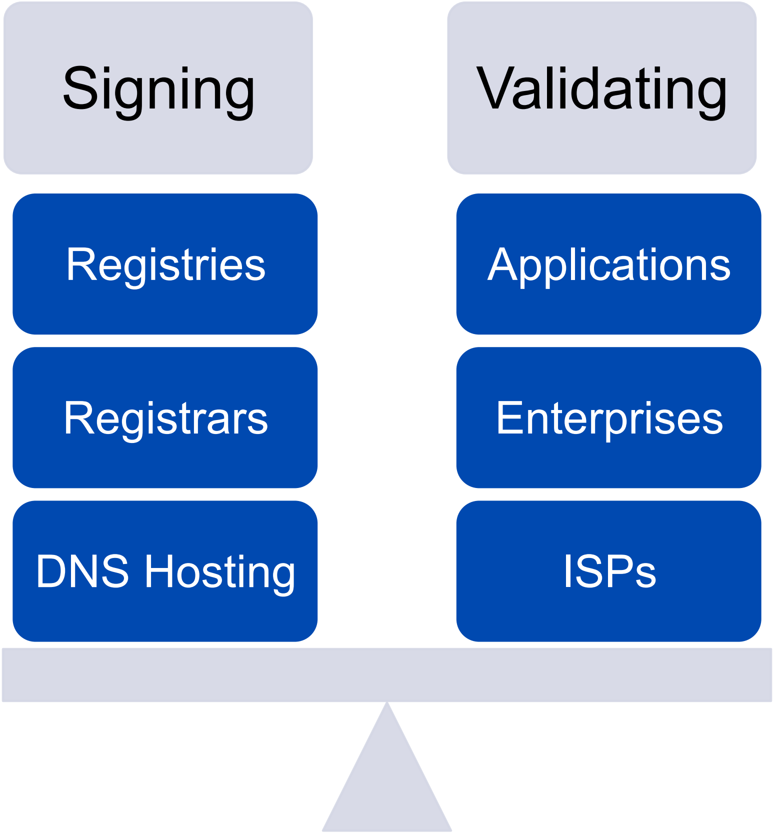
# A DNSSEC Interaction



# Attempting to Spoof DNS



# The Two Parts of DNSSEC



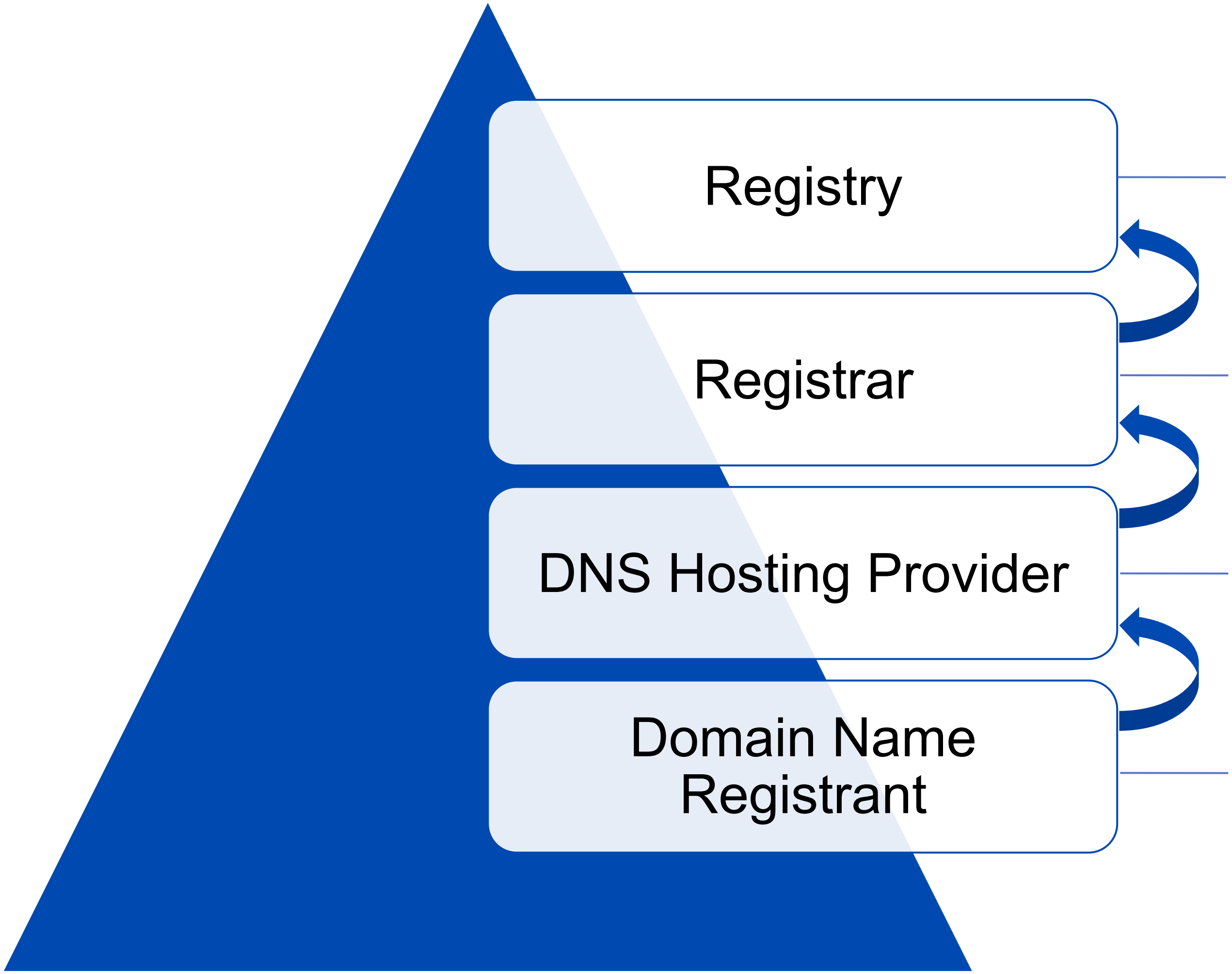
Signing

- Registries
- Registrars
- DNS Hosting

Validating

- Applications
- Enterprises
- ISPs

# DNSSEC Signing  - The Individual Steps



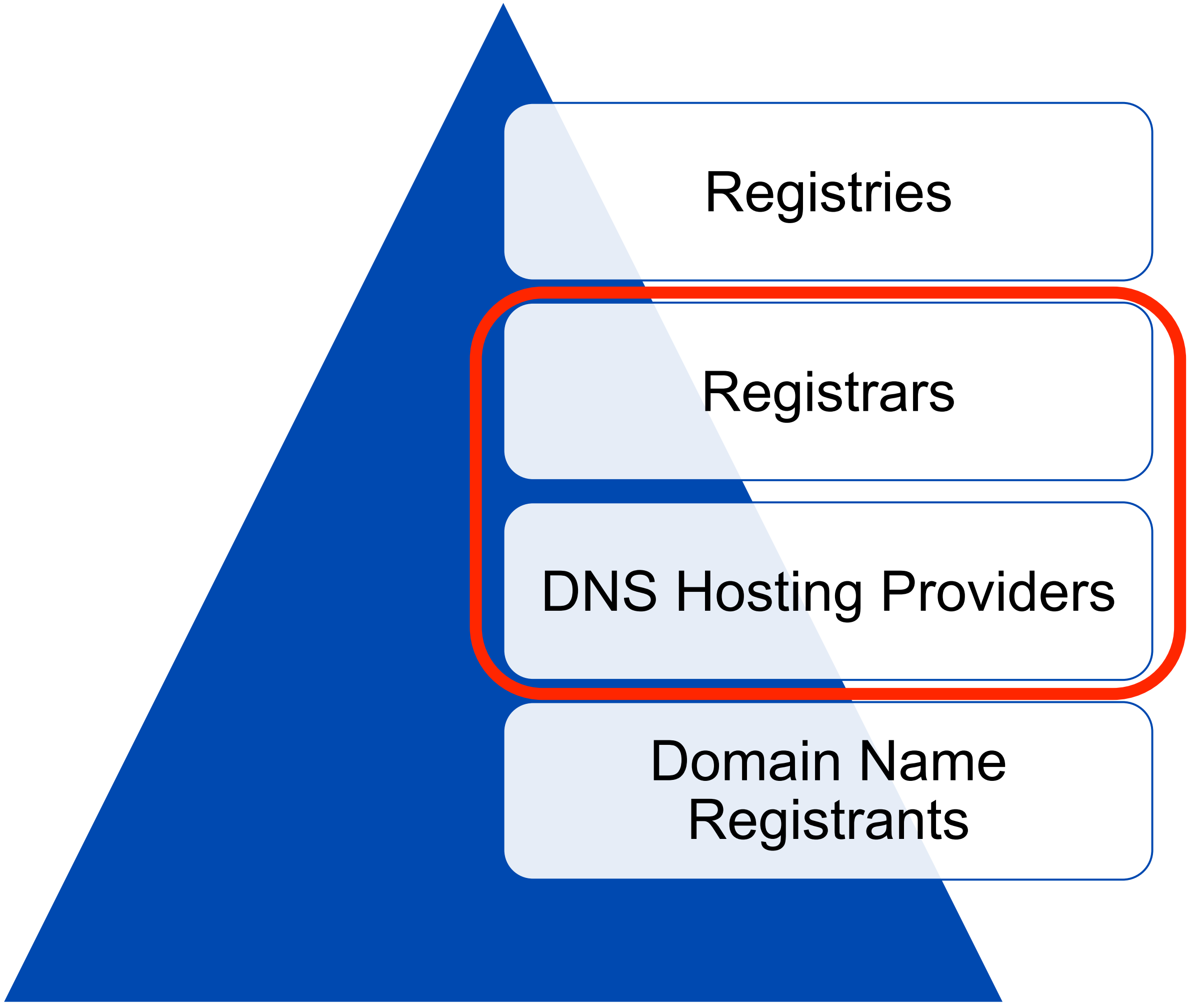
- Signs TLD
- Accepts DS records
- Publishes/signs records

- Accepts DS records
- Sends DS to registry
- Provides UI for mgmt

- Signs zones
- Publishes all records
- Provides UI for mgmt

- Enables DNSSEC (unless automatic)

# DNSSEC Signing - The Players



Registries

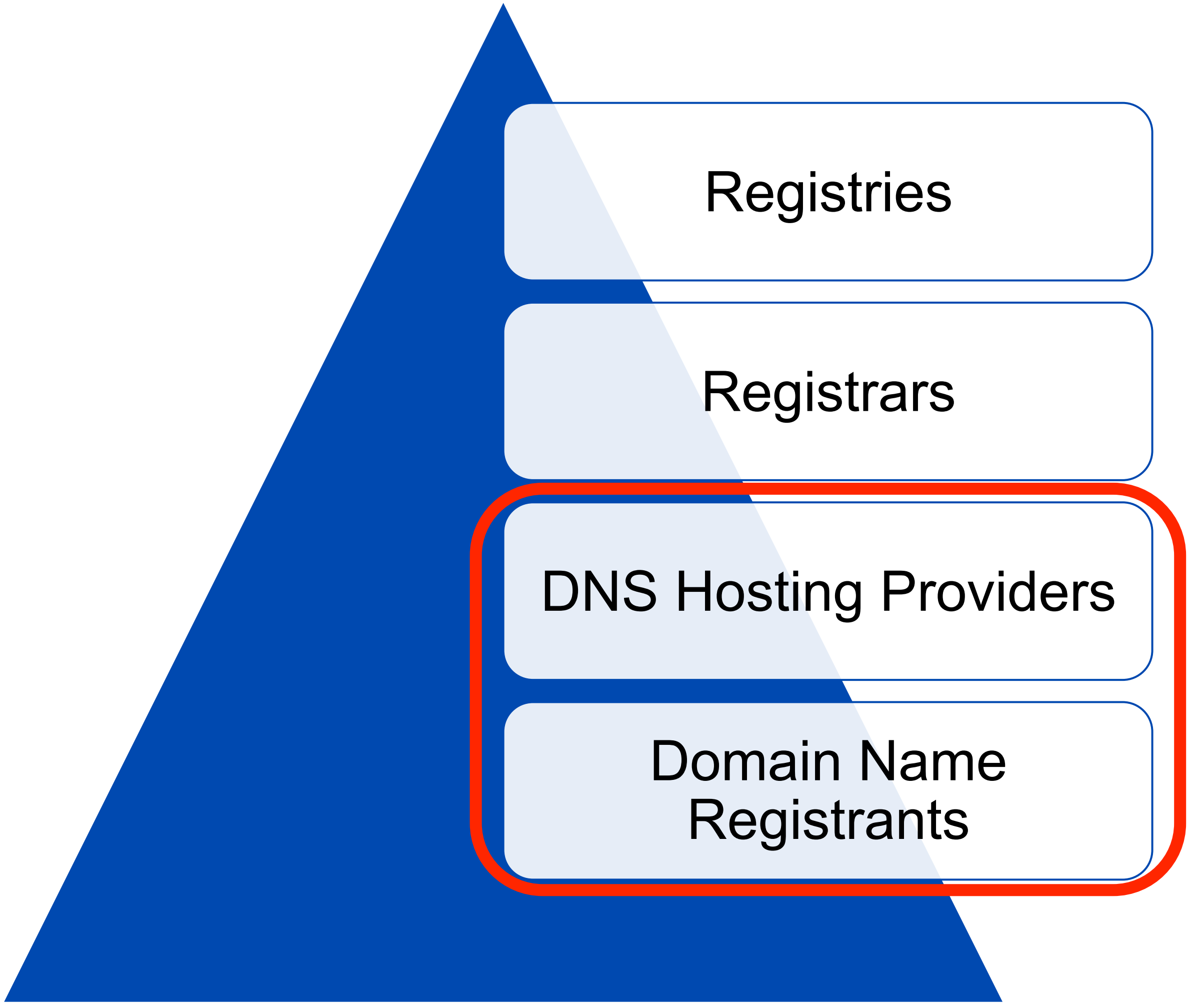
Registrars

DNS Hosting Providers

Domain Name Registrants

Registrar also provides DNS hosting services

# DNSSEC Signing - The Players


Registries

Registrars

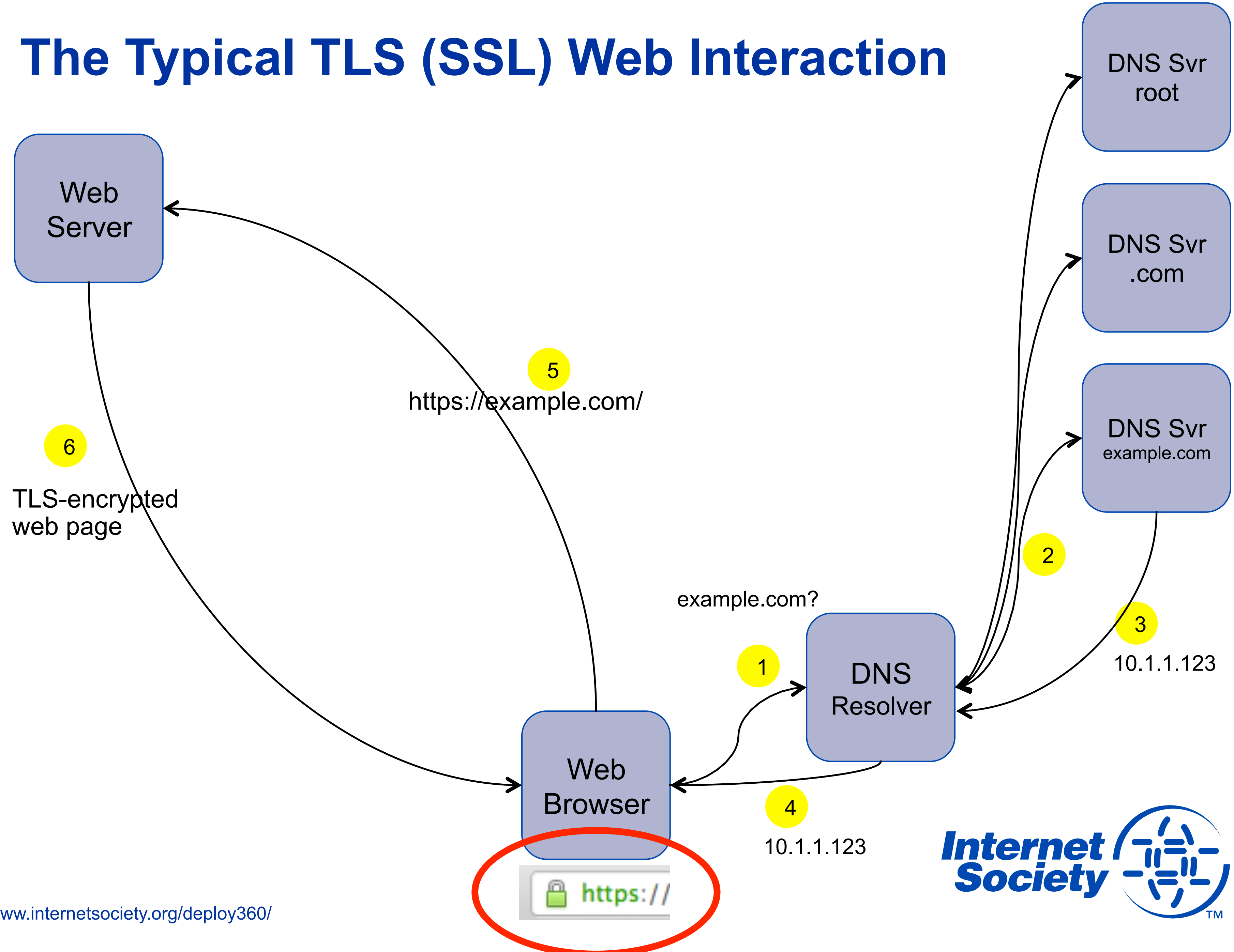
DNS Hosting Providers

Domain Name Registrants

Registrant hosts own DNS

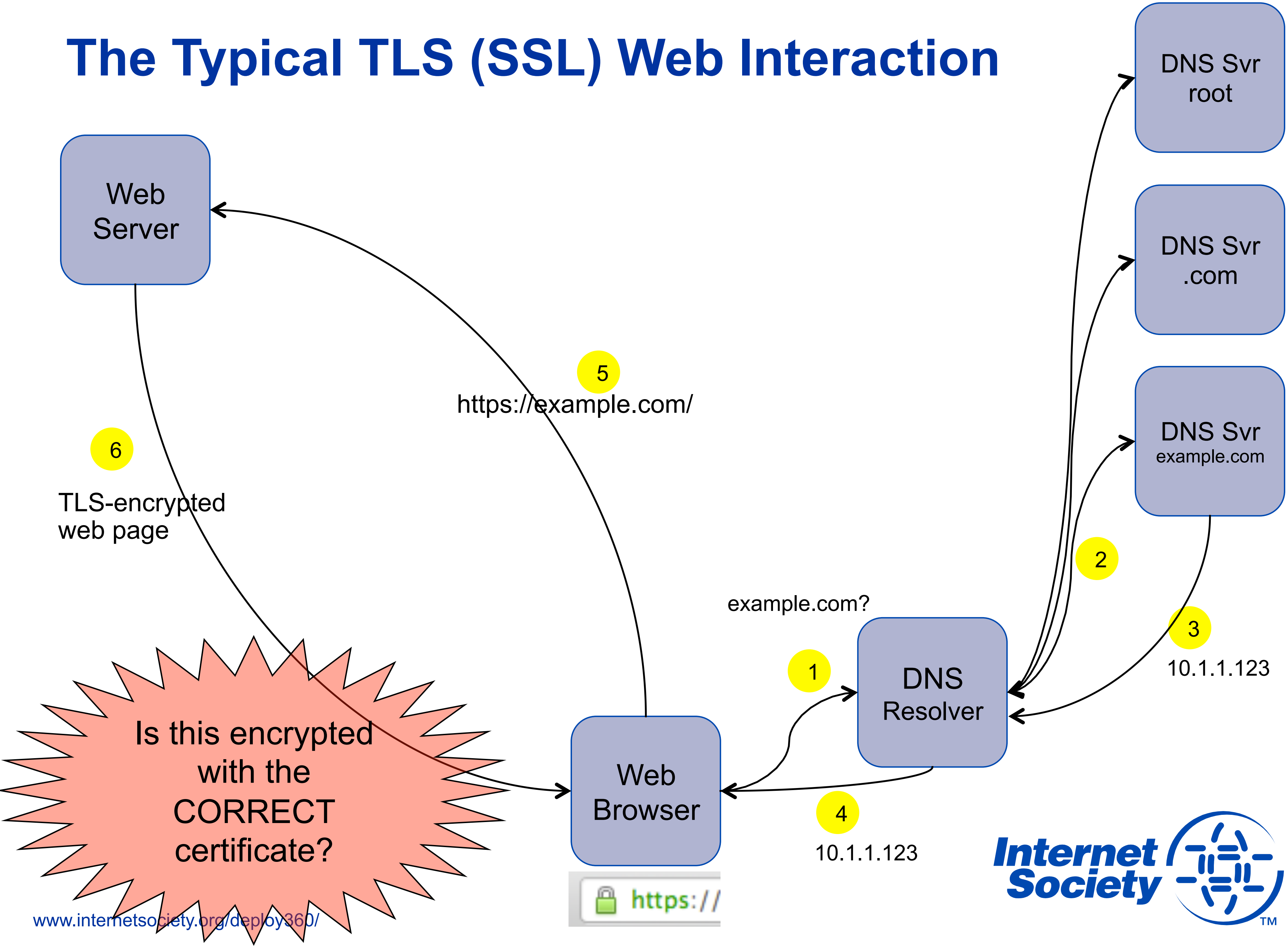
# A Quick Overview of DANE

# The Typical TLS (SSL) Web Interaction



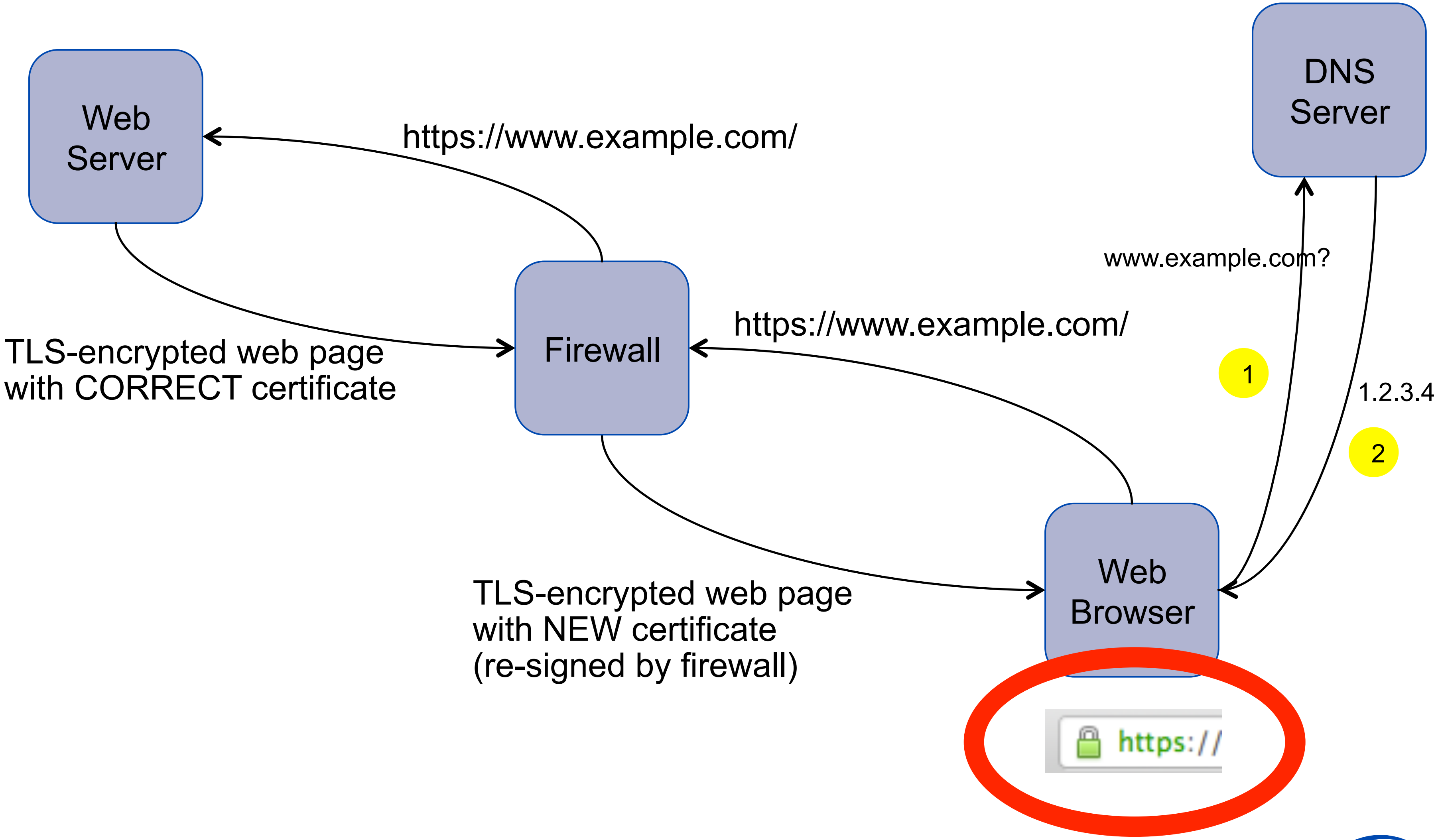
www.internetsociety.org/deploy360/

# The Typical TLS (SSL) Web Interaction



Is this encrypted with the CORRECT certificate?

# Problems?



Web Server

https://www.example.com/

DNS Server

www.example.com?

Firewall

https://www.example.com/

TLS-encrypted web page with CORRECT certificate

1

1.2.3.4

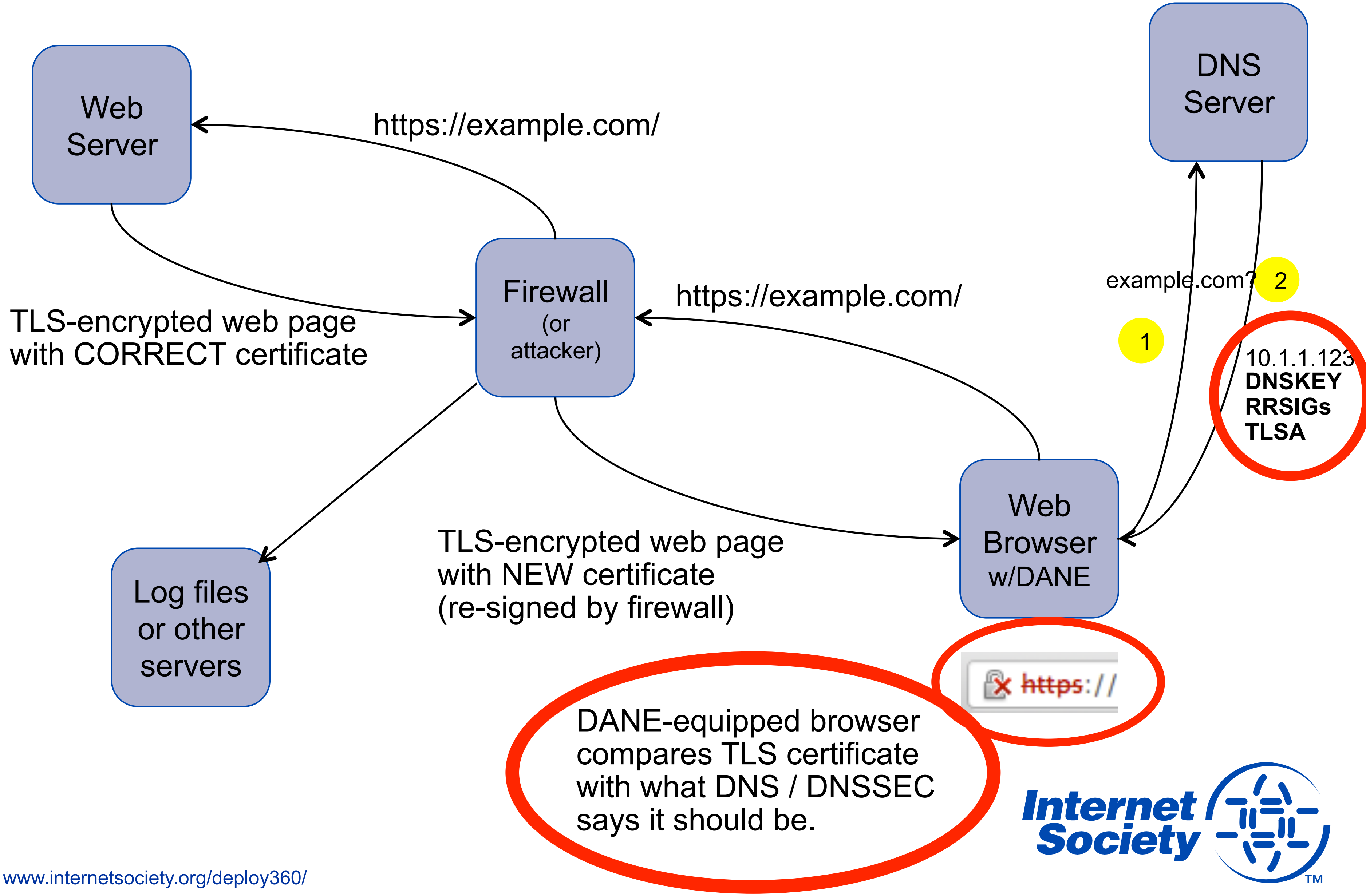
2

Web Browser

TLS-encrypted web page with NEW certificate (re-signed by firewall)

https://

# DANE



Web Server

https://example.com/

TLS-encrypted web page with CORRECT certificate

Firewall (or attacker)

https://example.com/

Log files or other servers

TLS-encrypted web page with NEW certificate (re-signed by firewall)

Web Browser w/DANE

DNS Server

example.com?

1

2

10.1.1.123
**DNSKEY**
**RRSIGs**
**TLSA**

~~https~~://

DANE-equipped browser compares TLS certificate with what DNS / DNSSEC says it should be.

# DNS-Based Authentication of Named Entities (DANE)

- Q: How do you know if the TLS (SSL) certificate is the correct one the site wants you to use?

- A: Store the certificate (or fingerprint) in DNS (new TLSA record) and sign them with DNSSEC.

A browser that understand DNSSEC and DANE will then know when the required certificate is NOT being used.

Certificate stored in DNS is controlled by the domain name holder. It could be a certificate signed by a CA – or a self-signed certificate.

# DANE – Not Just For The Web

- DANE defines protocol for storing TLS certificates in DNS
- Securing Web transactions is the obvious use case
- Other uses also possible:
  - Email via S/MIME
  - VoIP
  - Jabber/XMPP
  - PGP
  - ?

# DANE Resources

DANE and email:

- **http://tools.ietf.org/html/draft-ietf-dane-smtp**
- **http://tools.ietf.org/html/draft-ietf-dane-smime**

DANE Operational Guidance:

- **http://tools.ietf.org/id/draft-dukhovni-dane-ops-01.txt**

DANE and SIP (VoIP):

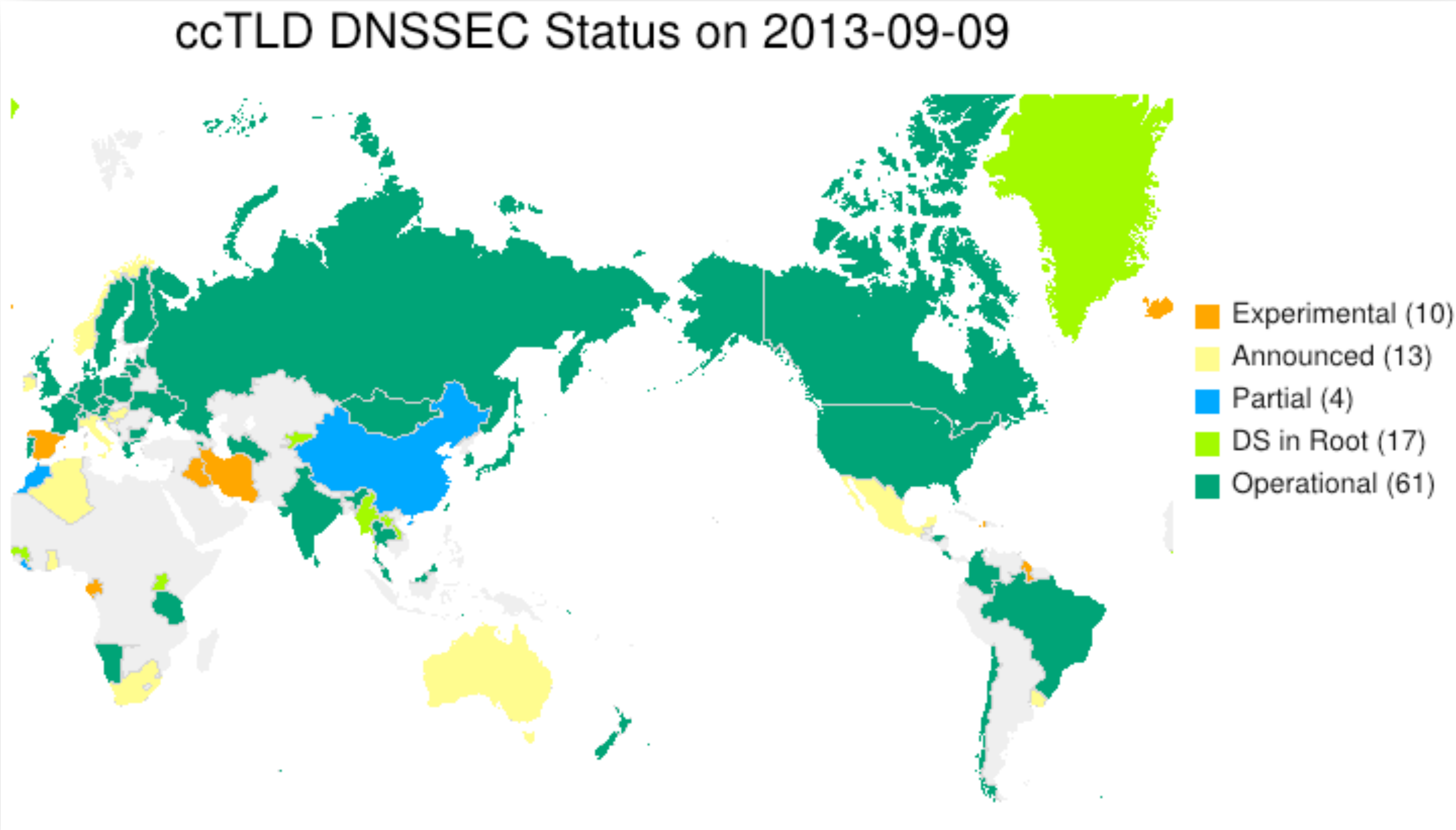
- **http://tools.ietf.org/id/draft-johansson-dane-sip-00.txt**

Other uses:

- **http://tools.ietf.org/id/draft-wouters-dane-openpgp-00.txt**
- **http://tools.ietf.org/id/draft-wouters-dane-otrfp-00.txt**

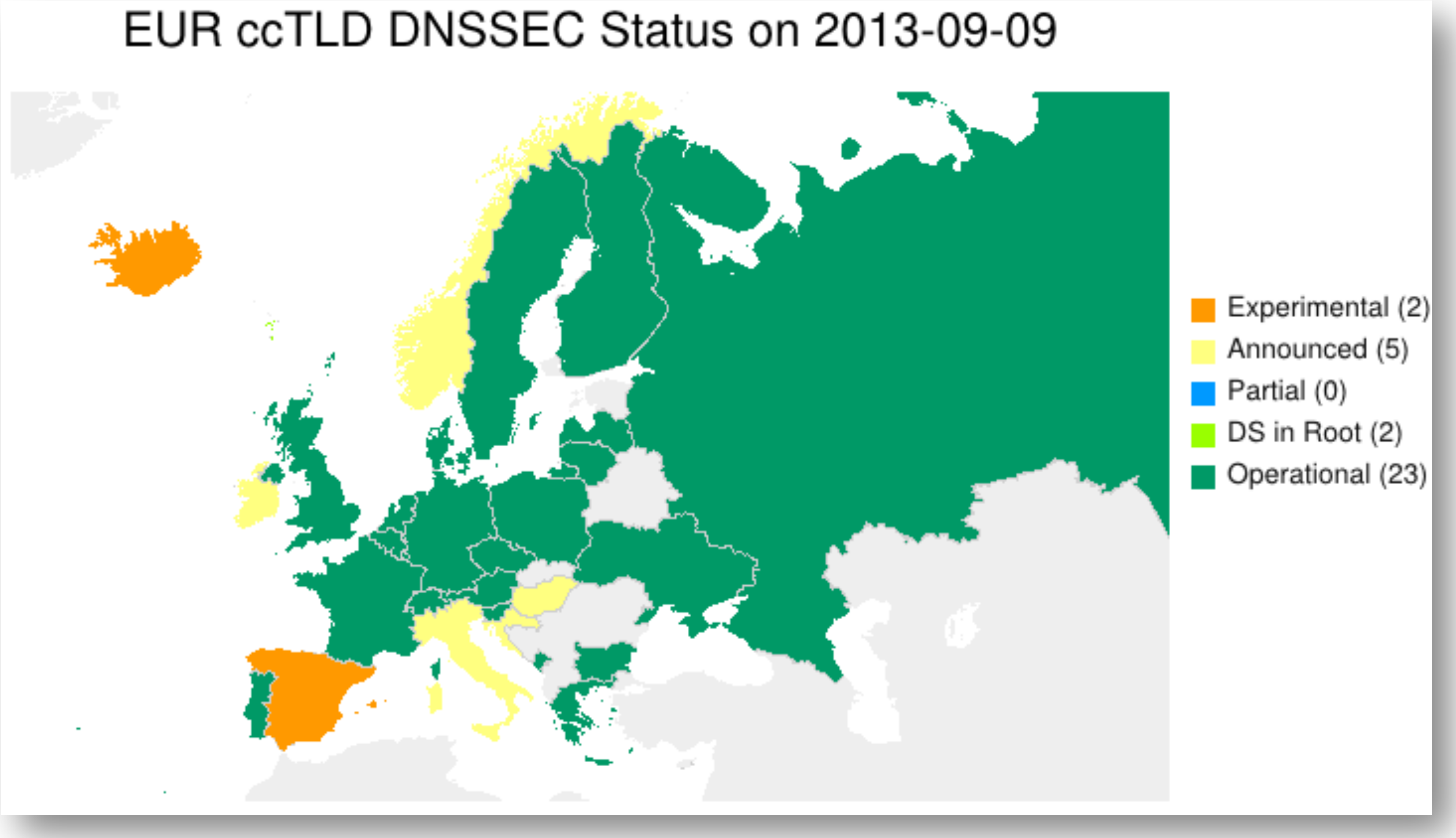
# DNSSEC Deployment Trends - Signing

# DNSSEC Deployment – Top-Level Domains



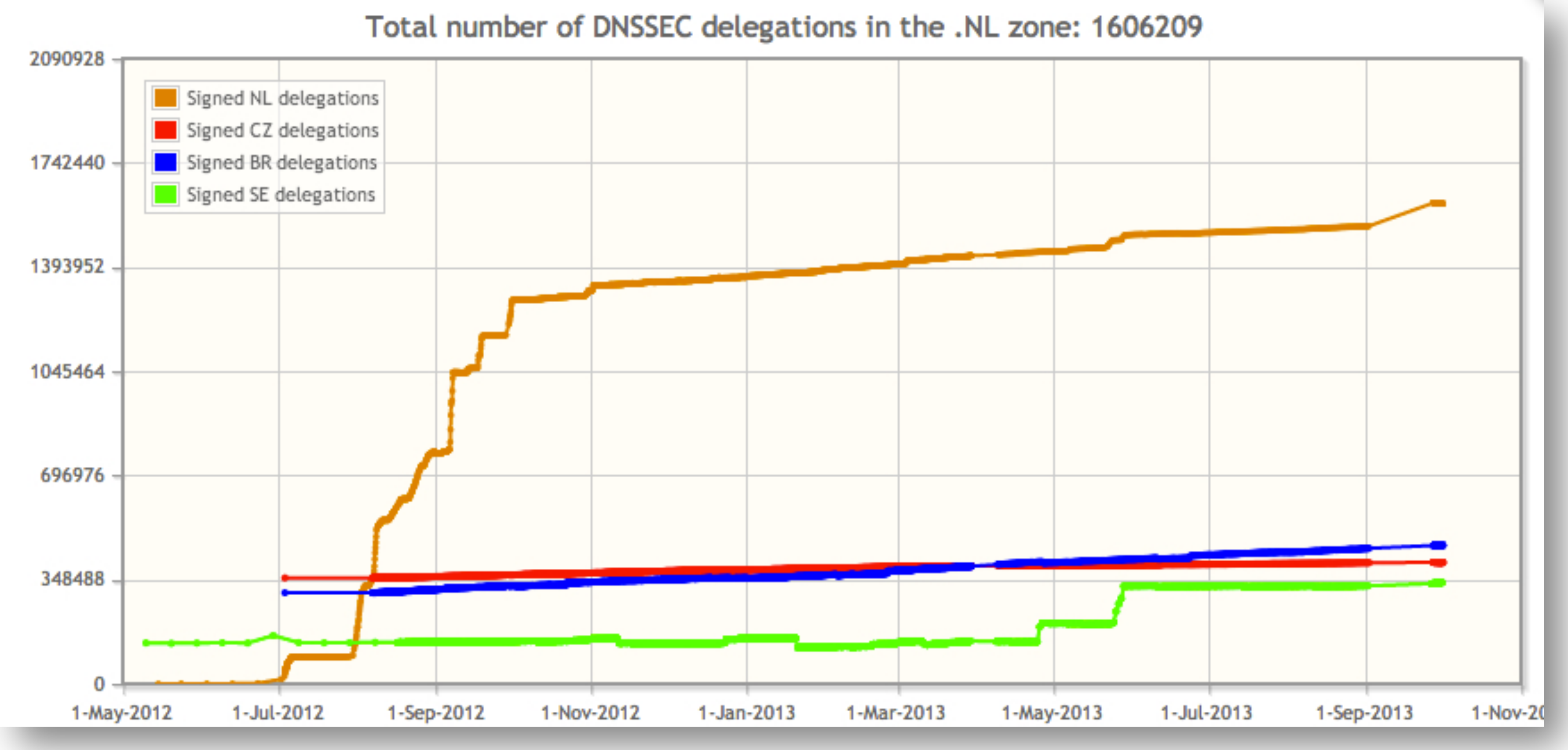
Source: http://www.internetsociety.org/deploy360/dnssec/maps/

# DNSSEC Deployment – Top-Level Domains



Source: http://www.internetsociety.org/deploy360/dnssec/maps/

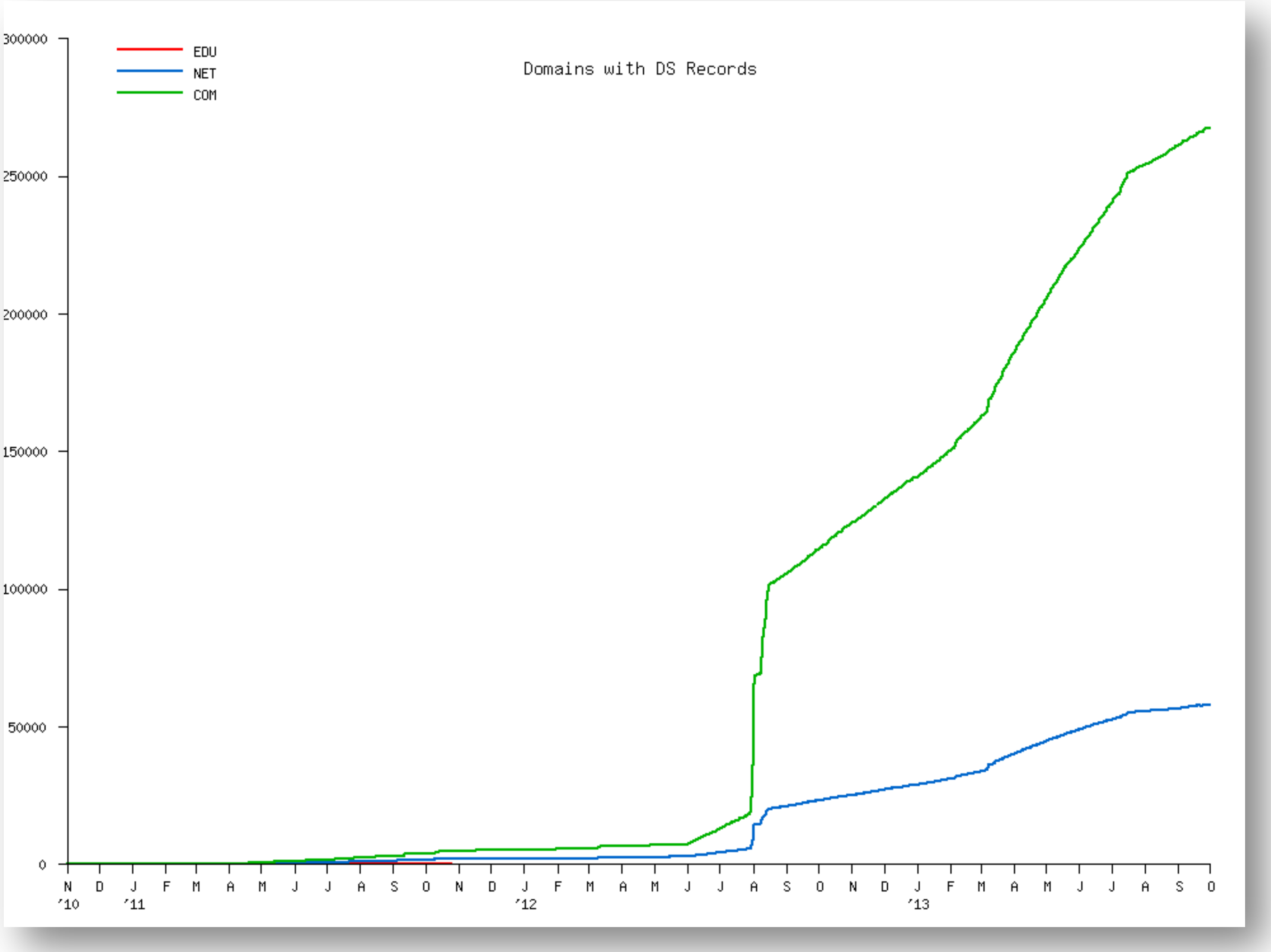
# DNSSEC Deployment – Second-Level Domains



Source: https://xs.powerdns.com/dnssec-nl-graph/

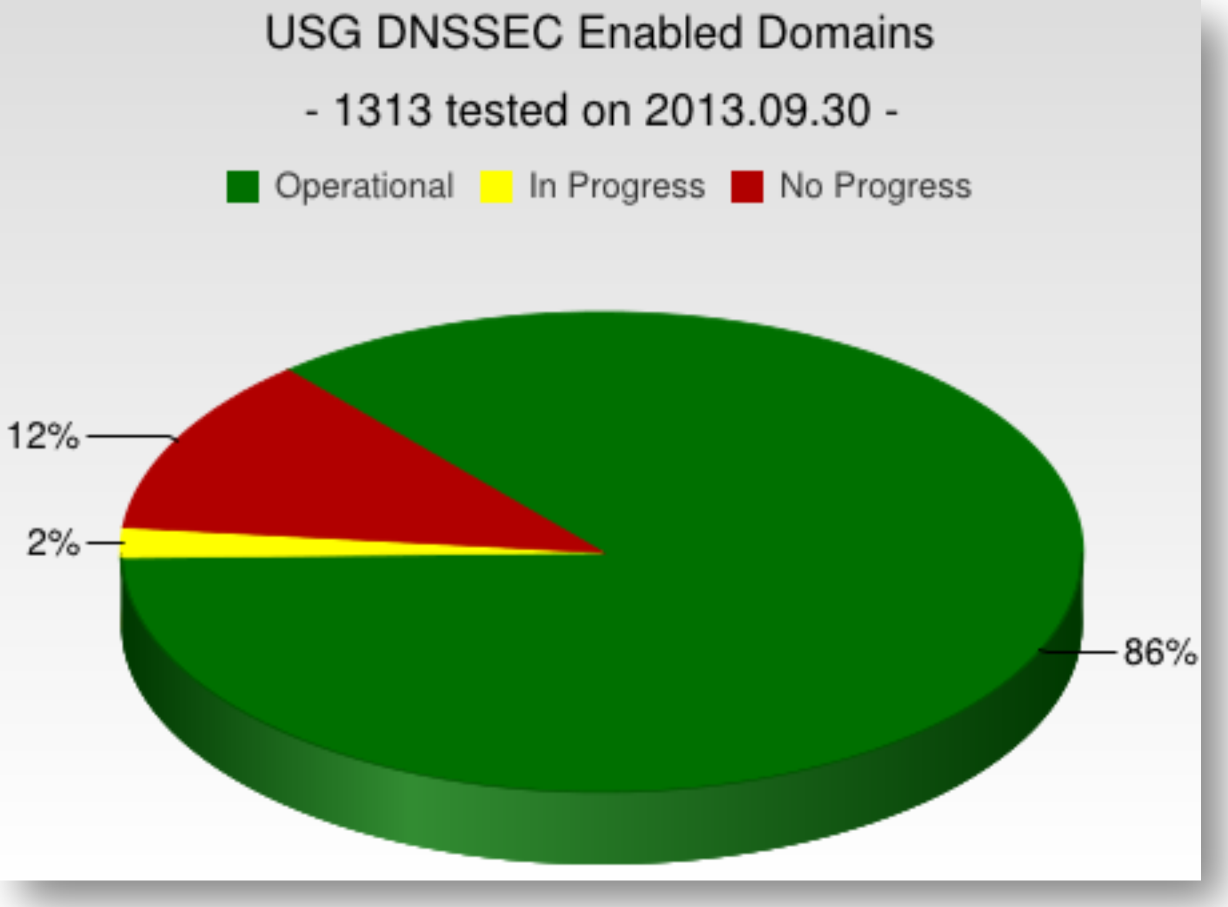
Internet Society™

# DNSSEC Deployment – .COM



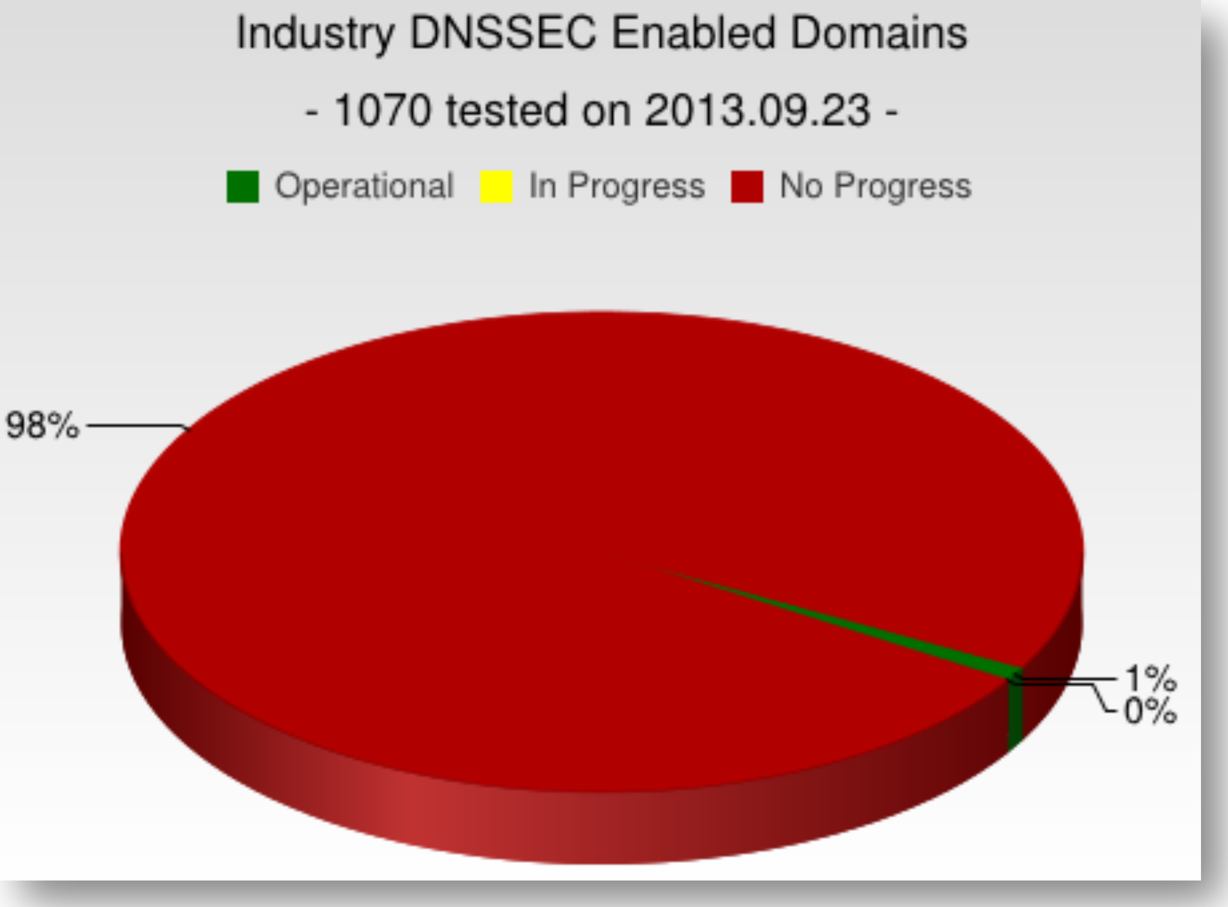
Source: http://scoreboard.verisignlabs.com/count-trace.png

# DNSSEC Deployment – .GOV



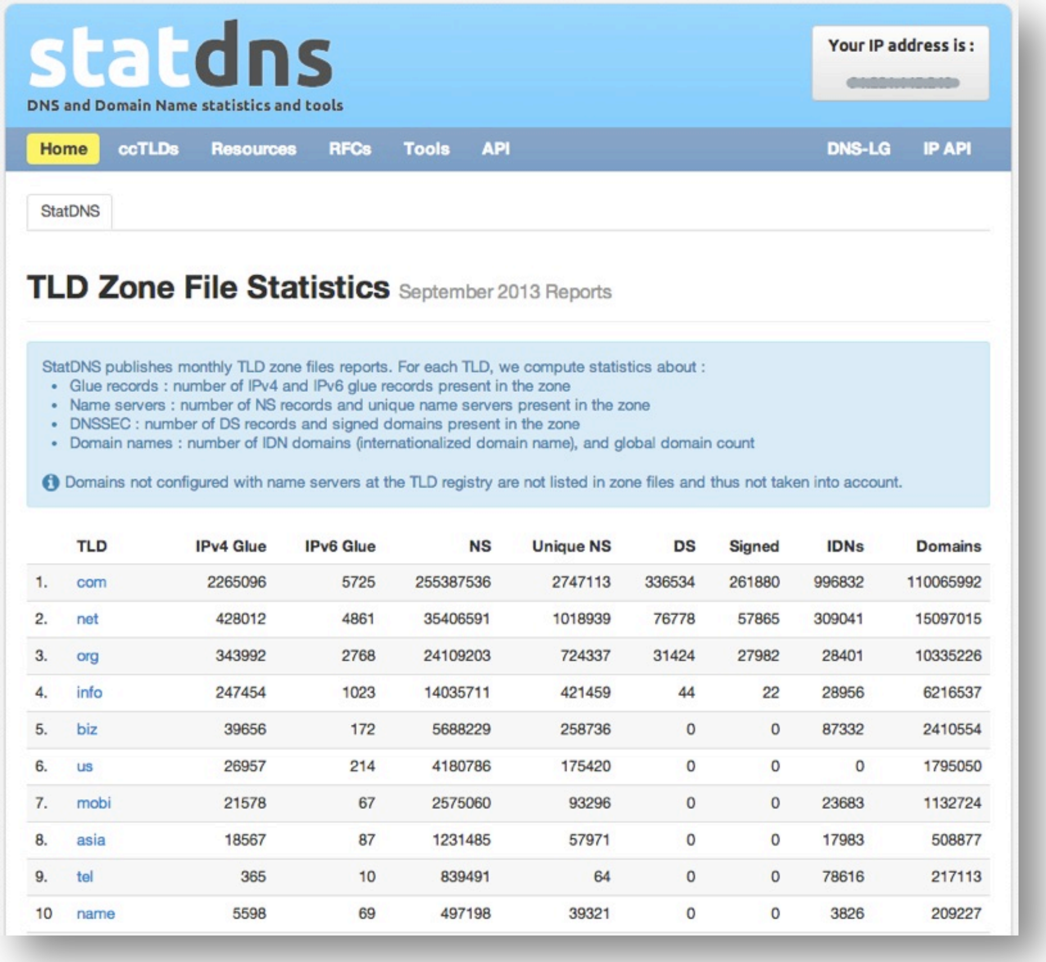
Source: http://fedv6-deployment.antd.nist.gov/snap-all.html

# DNSSEC Deployment – Fortune 1000 and U.S. Alexa Top 100 Sites



Source: http://fedv6-deployment.antd.nist.gov/snap-all.html

# DNSSEC Deployment – New Statistics Site



statdns

DNS and Domain Name statistics and tools

Your IP address is : [redacted]

## TLD Zone File Statistics September 2013 Reports

StatDNS publishes monthly TLD zone files reports. For each TLD, we compute statistics about :

- Glue records : number of IPv4 and IPv6 glue records present in the zone
- Name servers : number of NS records and unique name servers present in the zone
- DNSSEC : number of DS records and signed domains present in the zone
- Domain names : number of IDN domains (internationalized domain name), and global domain count

Domains not configured with name servers at the TLD registry are not listed in zone files and thus not taken into account.

| | TLD | IPv4 Glue | IPv6 Glue | NS | Unique NS | DS | Signed | IDNs | Domains |
|---|---|---|---|---|---|---|---|---|---|
| 1. | com | 2265096 | 5725 | 255387536 | 2747113 | 336534 | 261880 | 996832 | 110065992 |
| 2. | net | 428012 | 4861 | 35406591 | 1018939 | 76778 | 57865 | 309041 | 15097015 |
| 3. | org | 343992 | 2768 | 24109203 | 724337 | 31424 | 27982 | 28401 | 10335226 |
| 4. | info | 247454 | 1023 | 14035711 | 421459 | 44 | 22 | 28956 | 6216537 |
| 5. | biz | 39656 | 172 | 5688229 | 258736 | 0 | 0 | 87332 | 2410554 |
| 6. | us | 26957 | 214 | 4180786 | 175420 | 0 | 0 | 0 | 1795050 |
| 7. | mobi | 21578 | 67 | 2575060 | 93296 | 0 | 0 | 23683 | 1132724 |
| 8. | asia | 18567 | 87 | 1231485 | 57971 | 0 | 0 | 17983 | 508877 |
| 9. | tel | 365 | 10 | 839491 | 64 | 0 | 0 | 78616 | 217113 |
| 10 | name | 5598 | 69 | 497198 | 39321 | 0 | 0 | 3826 | 209227 |

Source: http://www.statdns.com/

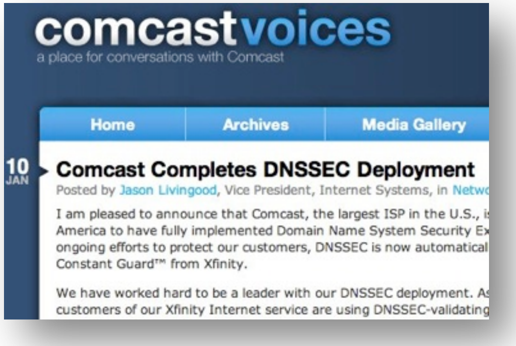
# DNSSEC Deployment Trends - Validation

# Availability of DNSSEC-Validating Resolvers

Consumers need easy availability of DNSSEC-validating DNS resolvers. Examples:

- Google's Public DNS now performing DNSSEC validation by default
- Comcast in North America rolled out DNSSEC-validating resolvers to 18+ million customers
- Almost all ISPs in Sweden provide DNSSEC-validating resolvers

Google



**Comcast Completes DNSSEC Deployment**

Posted by Jason Livingood, Vice President, Internet Systems, in Netwo

I am pleased to announce that Comcast, the largest ISP in the U.S., is
America to have fully implemented Domain Name System Security Ex
ongoing efforts to protect our customers, DNSSEC is now automatical
Constant Guard™ from Xfinity.

We have worked hard to be a leader with our DNSSEC deployment. As
customers of our Xfinity Internet service are using DNSSEC-validating

# Impact of Google Public DNS

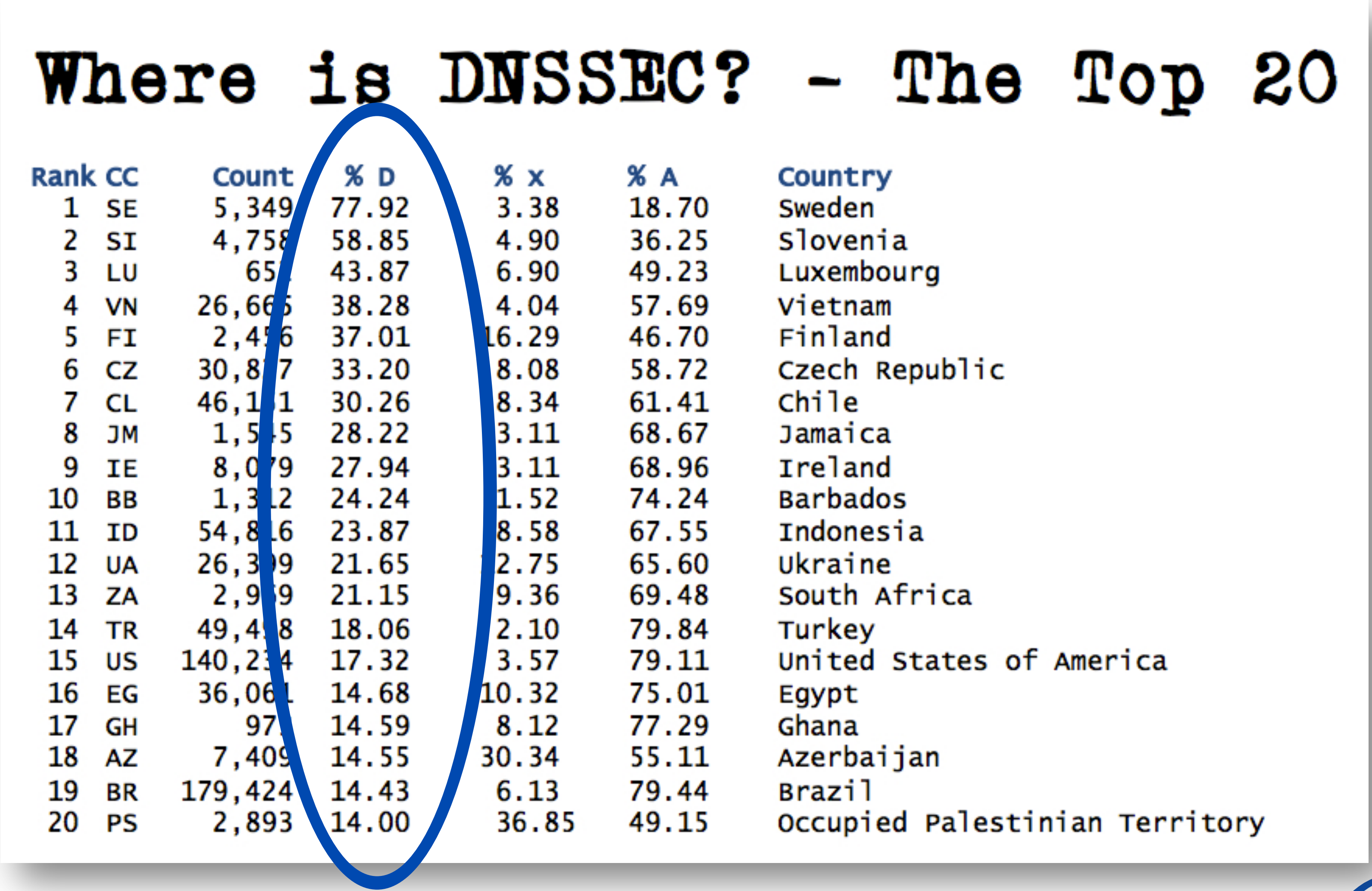
## Geoff Huston's measurements of DNSSEC validation:

- "Since March 2013 we've seen the proportion of end users who use DNSSEC resolvers that perform DNSSEC validation ***rise from 3.3% to 8.1%, or a rise of some 4.7%.***"

- http://www.circleid.com/posts/20130717_dns_dnssec_and_googles_public_dns_service/

- July 2013

# Geoff Huston's Measurements – July 2013



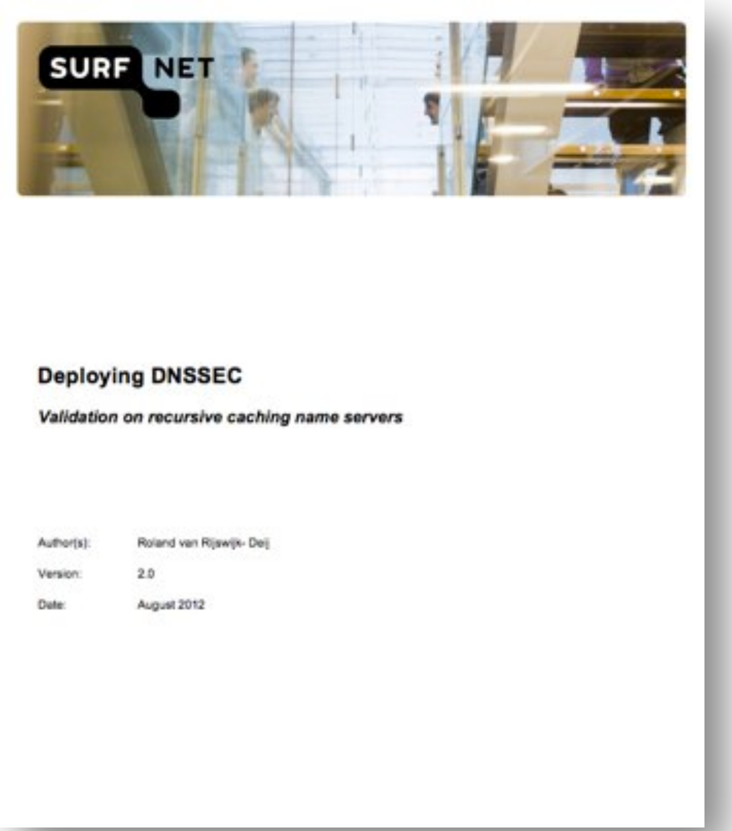
## Where is DNSSEC? - The Top 20

| Rank | CC | Count | % D | % x | % A | Country |
|---|---|---|---|---|---|---|
| 1 | SE | 5,349 | 77.92 | 3.38 | 18.70 | Sweden |
| 2 | SI | 4,758 | 58.85 | 4.90 | 36.25 | Slovenia |
| 3 | LU | 651 | 43.87 | 6.90 | 49.23 | Luxembourg |
| 4 | VN | 26,665 | 38.28 | 4.04 | 57.69 | Vietnam |
| 5 | FI | 2,456 | 37.01 | 16.29 | 46.70 | Finland |
| 6 | CZ | 30,877 | 33.20 | 8.08 | 58.72 | Czech Republic |
| 7 | CL | 46,1[illegible]1 | 30.26 | 8.34 | 61.41 | Chile |
| 8 | JM | 1,545 | 28.22 | 3.11 | 68.67 | Jamaica |
| 9 | IE | 8,079 | 27.94 | 3.11 | 68.96 | Ireland |
| 10 | BB | 1,312 | 24.24 | 1.52 | 74.24 | Barbados |
| 11 | ID | 54,816 | 23.87 | 8.58 | 67.55 | Indonesia |
| 12 | UA | 26,399 | 21.65 | 12.75 | 65.60 | Ukraine |
| 13 | ZA | 2,959 | 21.15 | 9.36 | 69.48 | South Africa |
| 14 | TR | 49,458 | 18.06 | 2.10 | 79.84 | Turkey |
| 15 | US | 140,234 | 17.32 | 3.57 | 79.11 | United States of America |
| 16 | EG | 36,061 | 14.68 | 10.32 | 75.01 | Egypt |
| 17 | GH | 971 | 14.59 | 8.12 | 77.29 | Ghana |
| 18 | AZ | 7,409 | 14.55 | 30.34 | 55.11 | Azerbaijan |
| 19 | BR | 179,424 | 14.43 | 6.13 | 79.44 | Brazil |
| 20 | PS | 2,893 | 14.00 | 36.85 | 49.15 | Occupied Palestinian Territory |

Source: http://iepg.org/2013-07-ietf87/2013-07-28-dnssec.pdf

# SURFnet Validating Server Whitepaper

- http://bit.ly/sn-dnssec-vali
- Steps through cost/benefit, requirements, planning
- Provides instructions for:
  - BIND 9.x
  - Unbound
  - Windows Server 2012



SURF NET

**Deploying DNSSEC**

***Validation on recursive caching name servers***

| | |
|---|---|
| Author(s): | Roland van Rijswijk- Deij |
| Version: | 2.0 |
| Date: | August 2012 |

# DNSSEC Deployment Challenges

# Key Questions

- What needs to be done to get more domains signed with DNSSEC?
- How can DNSSEC validation be more widely deployed?
- Are there technical issues or are the issues more of communication and awareness?
- How can we as a community address these challenges to increase the usage and availability of DNSSEC?

# Opportunities to Accelerate Deployment

1. **Registrar / DNS hosting provider engagement**
   - Encouraging more registrars to provide DNSSEC and making it easier for domain name holders.
2. **Validating name servers**
   - Expanding the deployment of DNSSEC-validating name servers at multiple levels, including ISPs, operating systems and applications.
3. **Enterprise signing of domains**
   - Helping enterprises and other large organizations understand the added security value they can achieve with DNSSEC, particularly with the new capabilities of DANE.
4. **Government activity with DNSSEC**
   - Encouraging governments to expand their promotion and usage of DNSSEC

# Registrars and DNSSEC - RAA

- **New ICANN Registrar Accreditation Agreement (RAA) will have section on DNSSEC**
  - Specifically the "Additional Registrar Operations Specification"
  - http://www.icann.org/en/news/public-comment/proposed-raa-22apr13-en.htm
  - Impact will be that any registrars wishing to continue their ICANN accreditation will need to learn about DNSSEC and accept records
  - Must be implemented by January 1, 2014

# Registrars and DNSSEC - RAA

## New specification states:

### 1. DNSSEC

Registrar must allow its customers to use DNSSEC upon request by relaying orders to add, remove or change public key material (e.g., DNSKEY or DS resource records) on behalf of customers to the Registries that support DNSSEC. Such requests shall be accepted and processed in a secure manner and according to industry best practices. Registrars shall accept any public key algorithm and digest type that is supported by the TLD of interest and appears in the registries posted at: <http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml> and <http://www.iana.org/assignments/ds-rr-types/ds-rr-types.xml>. All such requests shall be transmitted to registries using the EPP extensions specified in RFC 5910 or its successors.

**Specification also covers IPv6 and IDNs.**

# Helping Accelerate DNSSEC Deployment

Public mailing list, “dnssec-coord”, available and open to all:

**https://elists.isoc.org/mailman/listinfo/dnssec-coord**

Focus is on better *coordinating* promotion / advocacy / marketing activities related to DNSSEC deployment.

Monthly conference calls and informal meetings at ICANN and IETF events.

# DNSSEC Resources

# DNSSEC Workshop at ICANN 48

- **November 20, 2013**
  **Buenos Aires, Argentina**

- **Topics to be discussed include:**
  - Automation of DNSSEC
  - Root key rollover
  - Guidance for registrars in supporting DNSSEC
  - Interfaces between registrars and registries
  - Regional activities

- **Will be streamed live over the Internet**

# Resources

**To learn more about DNSSEC and how to get started:**

http://www.internetsociety.org/deploy360/dnssec/basics/

http://www.internetsociety.org/deploy360/resources/dane/

**Specific resources that may be of interest:**

- SURFnet whitepaper about deploying validating servers
- DNSSEC HOWTO
- NIST "Secure DNS Deployment Guide"

# Comcast Case Study

- Presentation at October 2012 DNSSEC Deployment Workshop at ICANN 45

- Slides and audio for workshop:
  - toronto45.icann.org/node/34375

- Comcast presentation:
  - Customer interaction
  - Lessons learned
  - Next steps

xfinity

DNSSEC Activities In North America: Comcast

ICANN 45

October 17, 2012

comcast

NATIONAL ENGINEERING & TECHNICAL OPERATIONS

# Increased Number Of DNSSEC Tools

**Lists of tools:**

http://www.internetsociety.org/deploy360/dnssec/tools/

http://www.internetsociety.org/deploy360/blog/tag/tools/

**DNSSEC Tools Project**

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

# DANE Resources

DANE Overview and Resources:

- **http://www.internetsociety.org/deploy360/resources/dane/**

IETF Journal article explaining DANE:

- **http://bit.ly/dane-dnssec**

RFC 6394 - DANE Use Cases:

- **http://tools.ietf.org/html/rfc6394**

RFC 6698 – DANE Protocol:

- **http://tools.ietf.org/html/rfc6698**

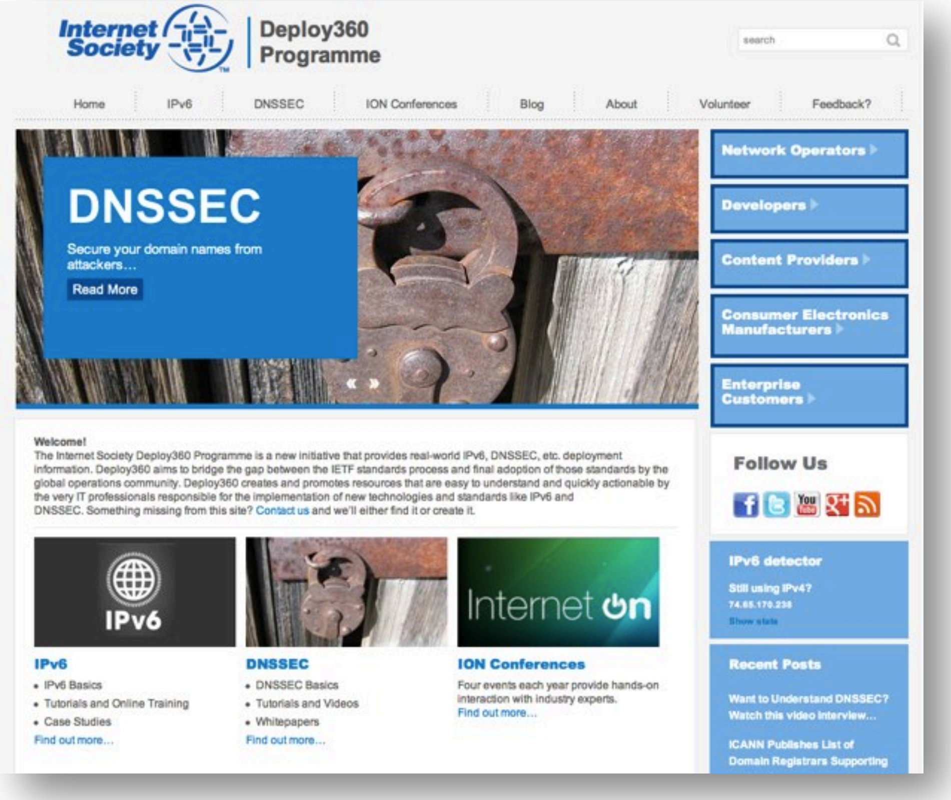
# Three Requests For Network Operators

1. **Deploy DNSSEC-validating DNS resolvers**

2. **Sign your own domains where possible**

3. **Help promote support of DANE protocol**
   - Allow usage of TLSA record. Let browser vendors and others know you want to use DANE. Help raise awareness of how DANE and DNSSEC can make the Internet more secure.

# Internet Society Deploy360 Programme



Internet Society | Deploy360 Programme

search

Home | IPv6 | DNSSEC | ION Conferences | Blog | About | Volunteer | Feedback?

DNSSEC

Secure your domain names from attackers…

Read More

Network Operators

Developers

Content Providers

Consumer Electronics Manufacturers

Enterprise Customers

**Welcome!**

The Internet Society Deploy360 Programme is a new initiative that provides real-world IPv6, DNSSEC, etc. deployment information. Deploy360 aims to bridge the gap between the IETF standards process and final adoption of those standards by the global operations community. Deploy360 creates and promotes resources that are easy to understand and quickly actionable by the very IT professionals responsible for the implementation of new technologies and standards like IPv6 and DNSSEC. Something missing from this site? Contact us and we'll either find it or create it.

**IPv6**

- IPv6 Basics
- Tutorials and Online Training
- Case Studies

Find out more…

**DNSSEC**

- DNSSEC Basics
- Tutorials and Videos
- Whitepapers

Find out more…

**ION Conferences**

Four events each year provide hands-on interaction with industry experts.

Find out more…

**Follow Us**

**IPv6 detector**

Still using IPv4?

74.65.170.238

Show stats

**Recent Posts**

Want to Understand DNSSEC? Watch this video interview…

ICANN Publishes List of Domain Registrars Supporting

**www.internetsociety.org/deploy360/**

## Can You Help Us With:

- Case Studies?
- Tutorials?
- Videos?

## How Can We Help You?

**Dan York**

Senior Content Strategist
Internet Society

york@isoc.org

http://www.internetsociety.org/deploy360/

# Thank You!