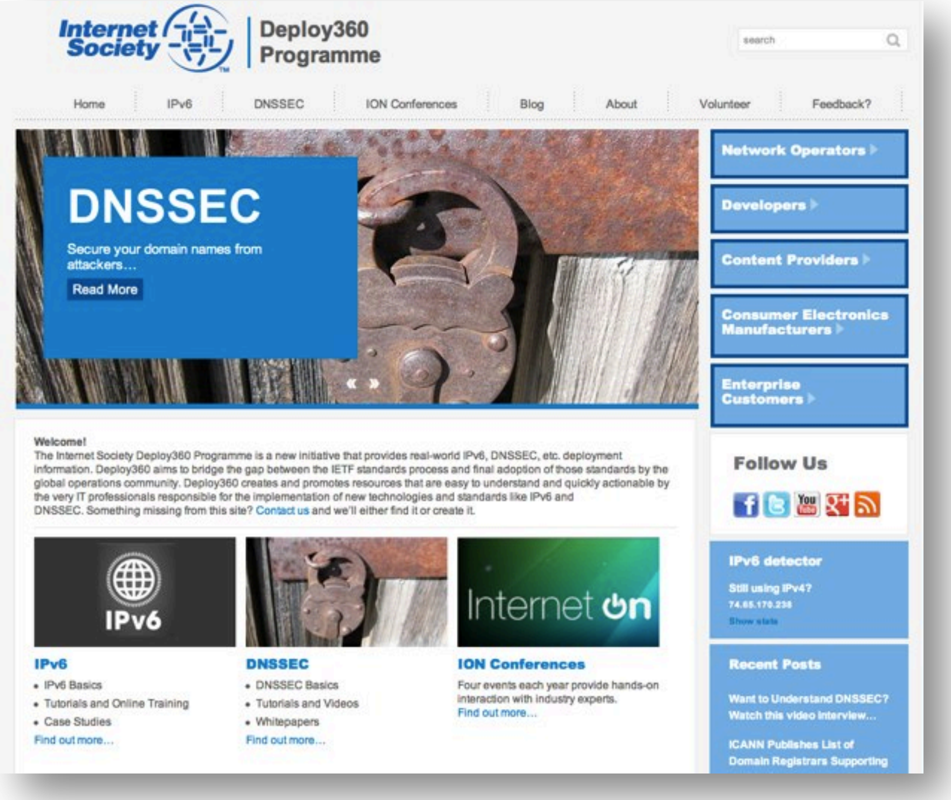
DNSSEC - Why Network Operators Should Care And How To Accelerate Deployment

Dan York, CISSP
Senior Content Strategist, Internet Society

Eurasia Network Operators' Group (ENOG) 4
Moscow, Russia
October 23, 2012

Internet Society ™

Internet Society Deploy360 Programme



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…

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

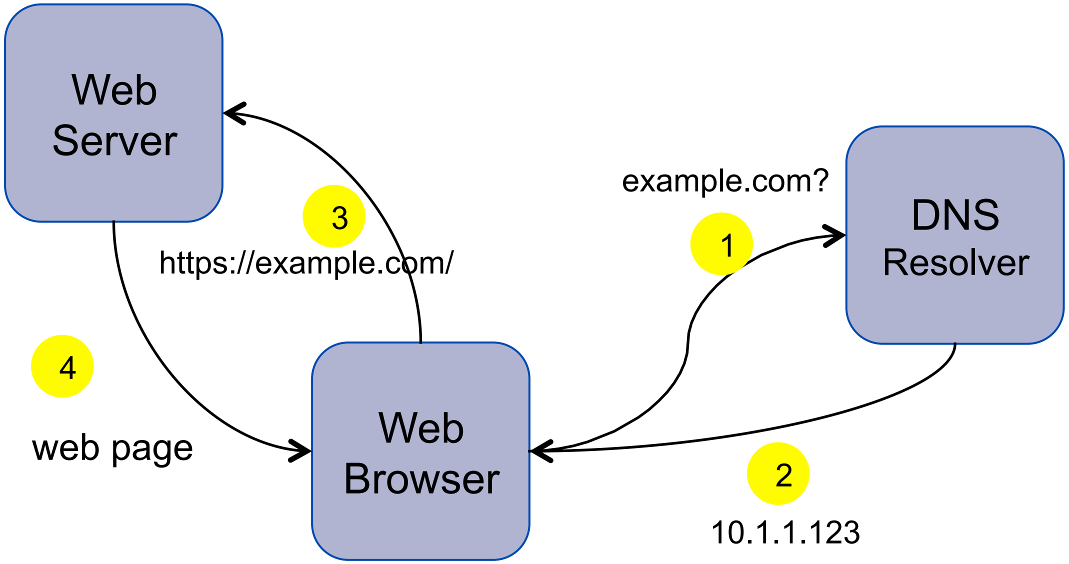
www.internetsociety.org/deploy360/

Providing real-world deployment info for IPv6, DNSSEC and other Internet technologies:

- **Case Studies**
- **Tutorials**
- **Videos**
- **Whitepapers**
- **News, information**

English content, initially, but will be translated into other languages.

A Normal DNS Interaction

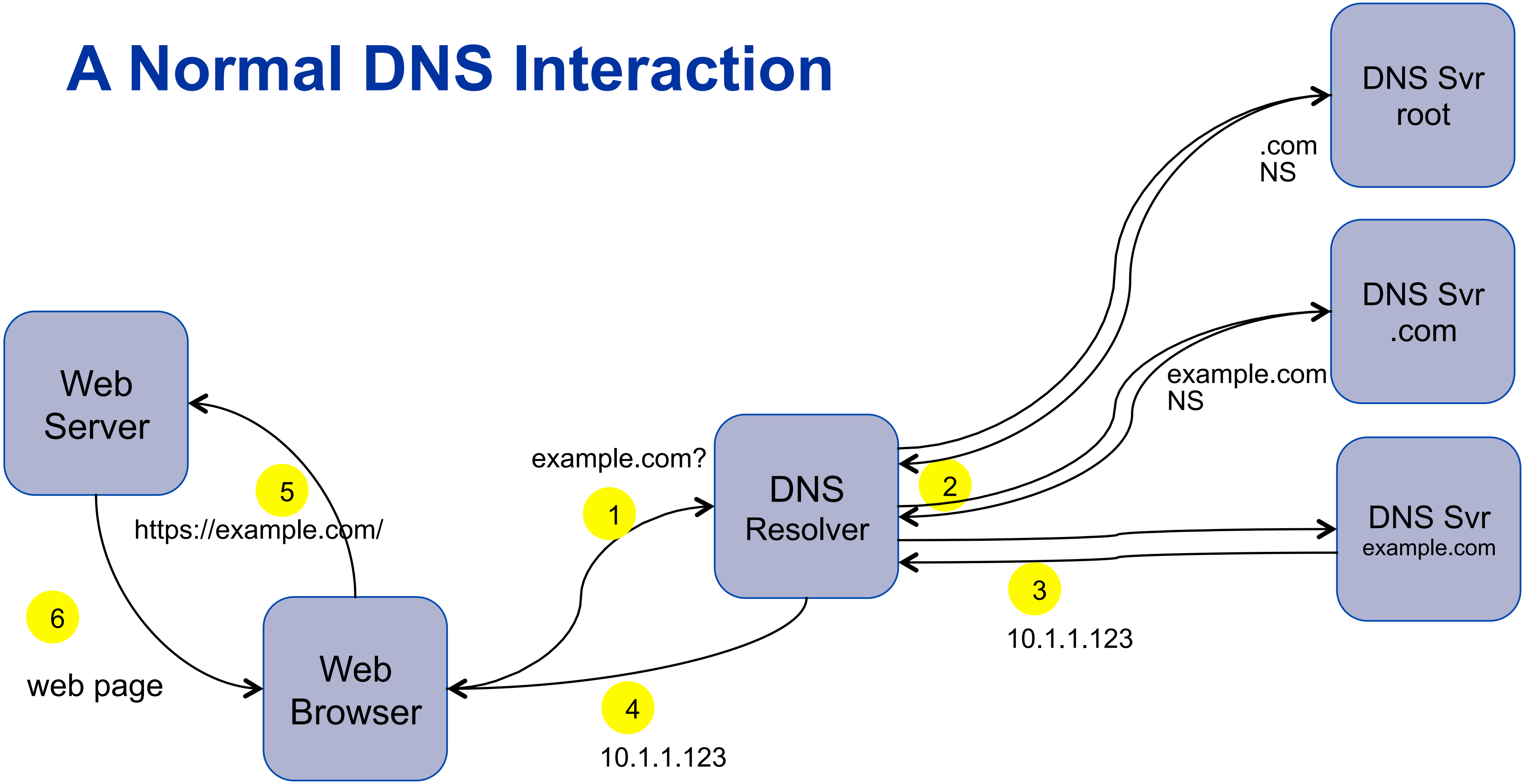


Resolver checks its local *cache.* If it has the answer, it sends it back.

example.com 10.1.1.123

If not…

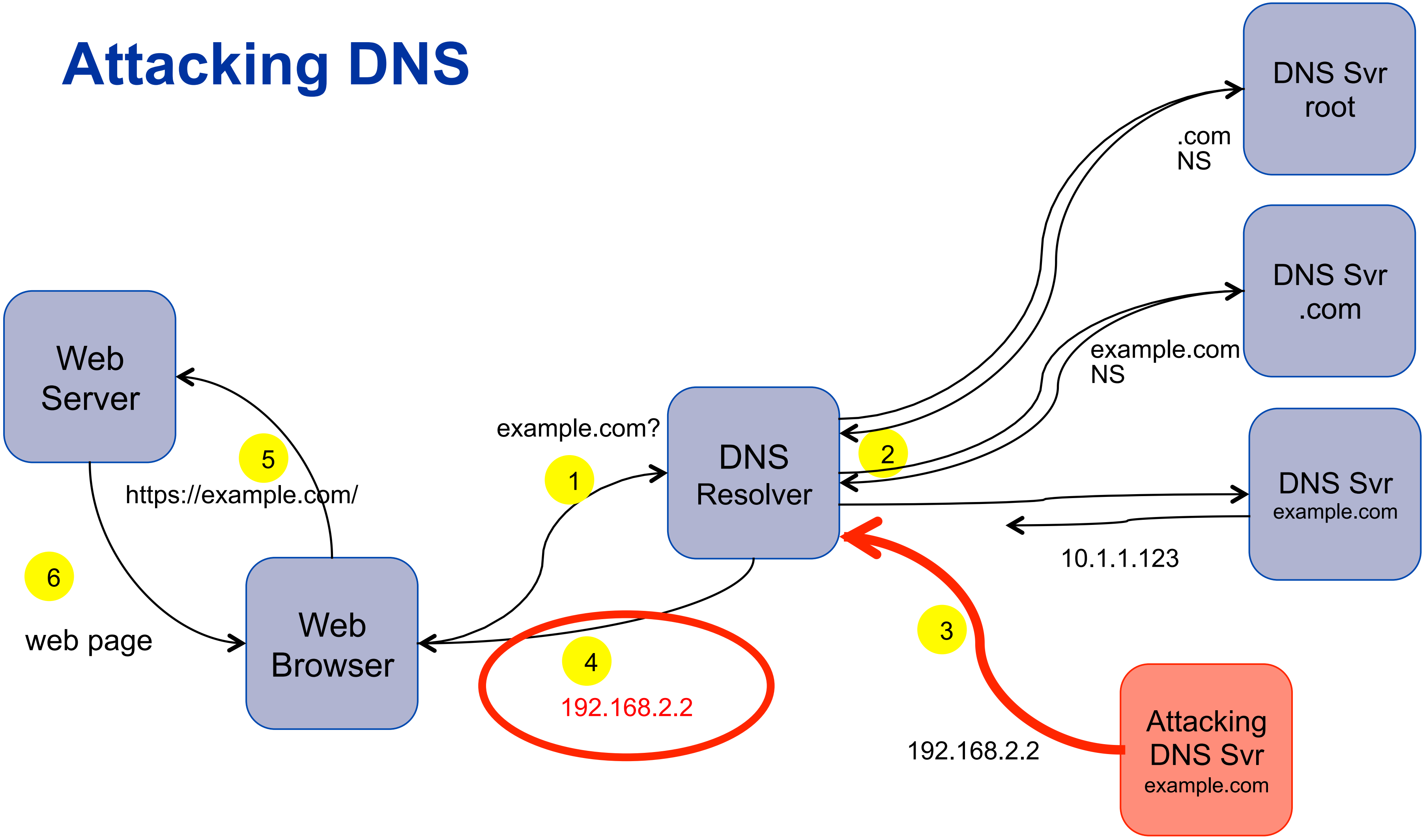
A Normal DNS Interaction



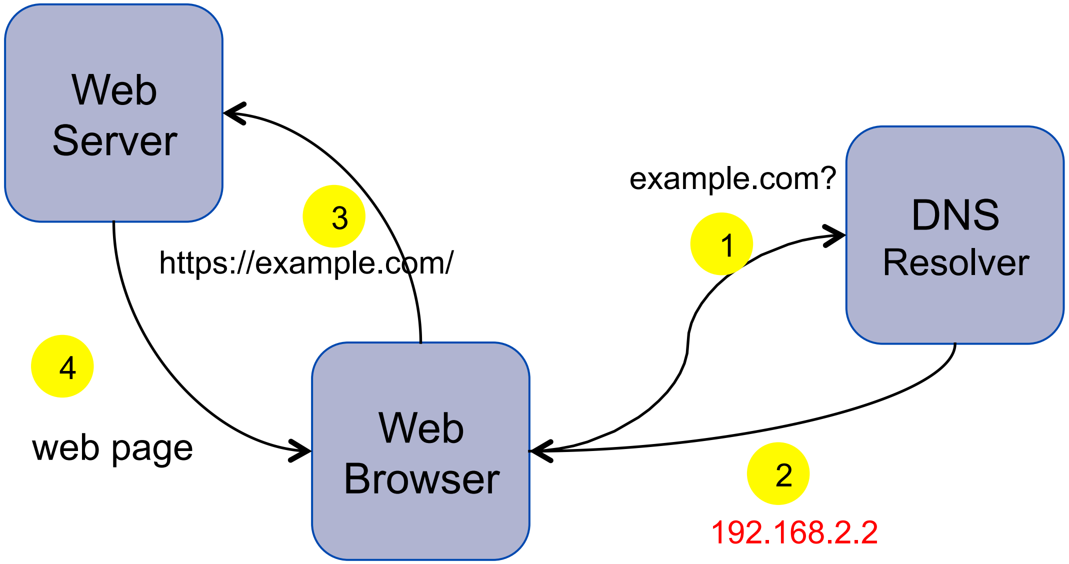
DNS works on speed

First result wins

Attacking DNS



A Poisoned Cache

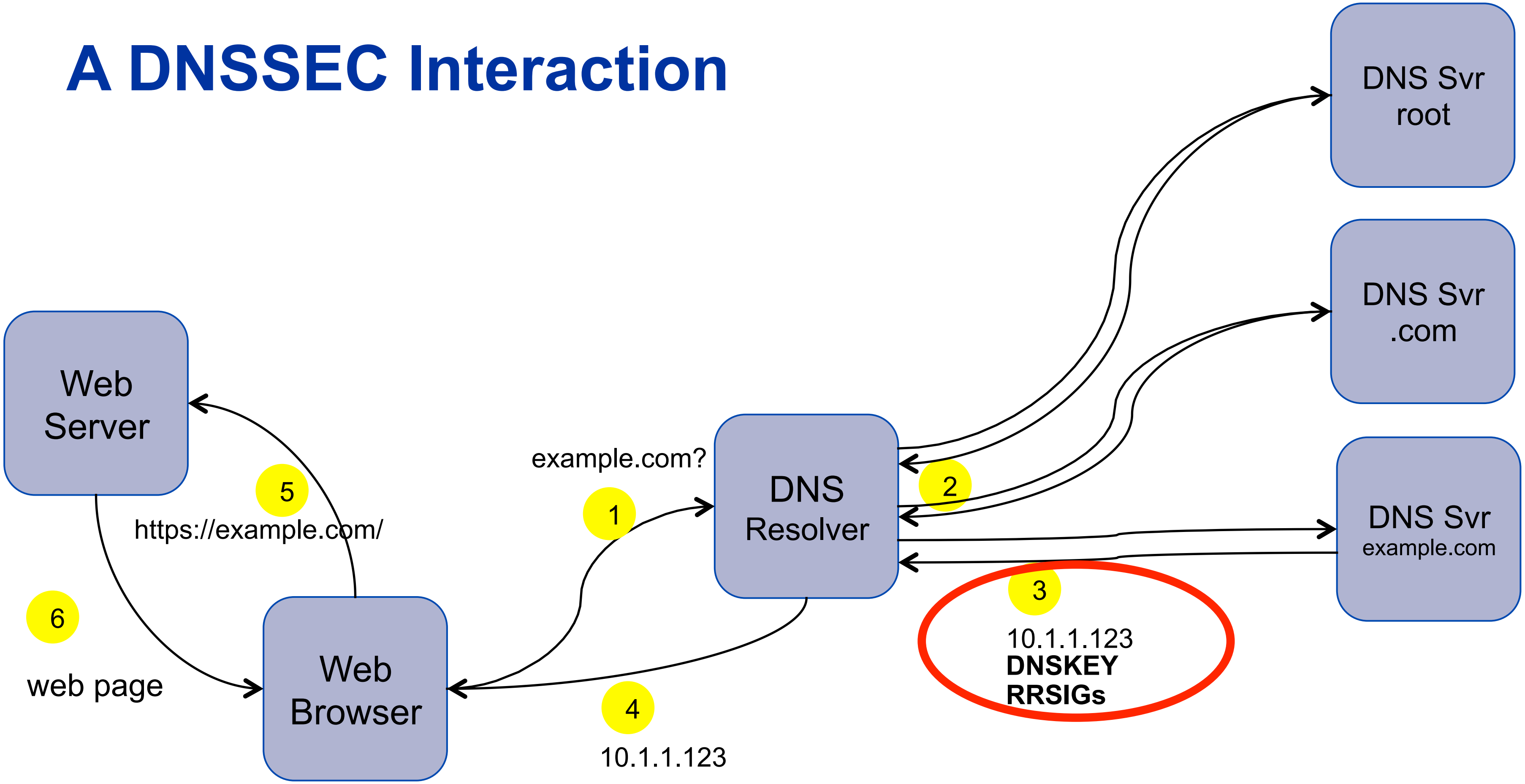


Resolver ***cache*** now has wrong data:

example.com 192.168.2.2

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

A DNSSEC Interaction



DNS Resolver:

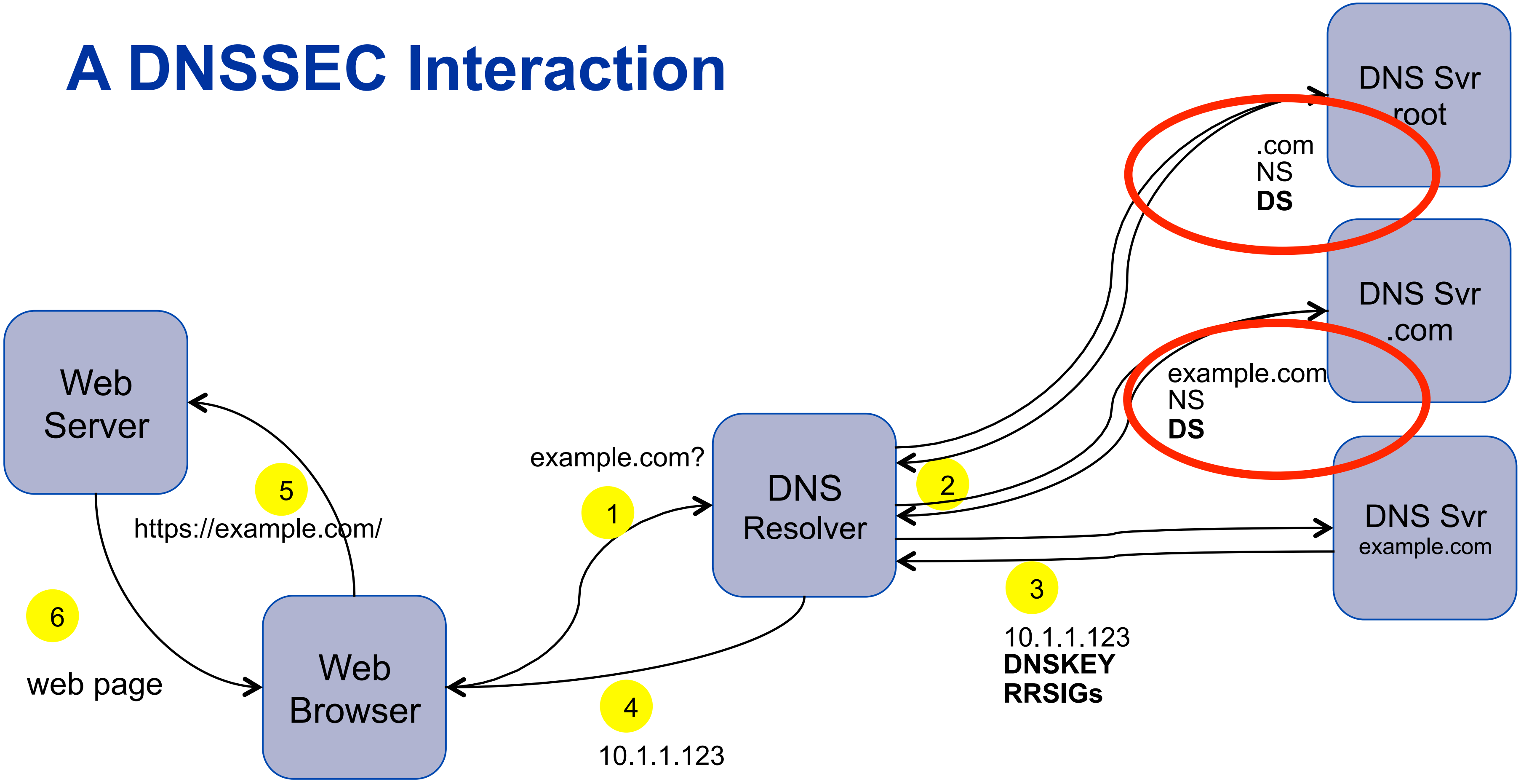
- Uses DNSKEY to perform calculation on DNS records
- Compares result with RRSIG records

Spoof DNSSEC?

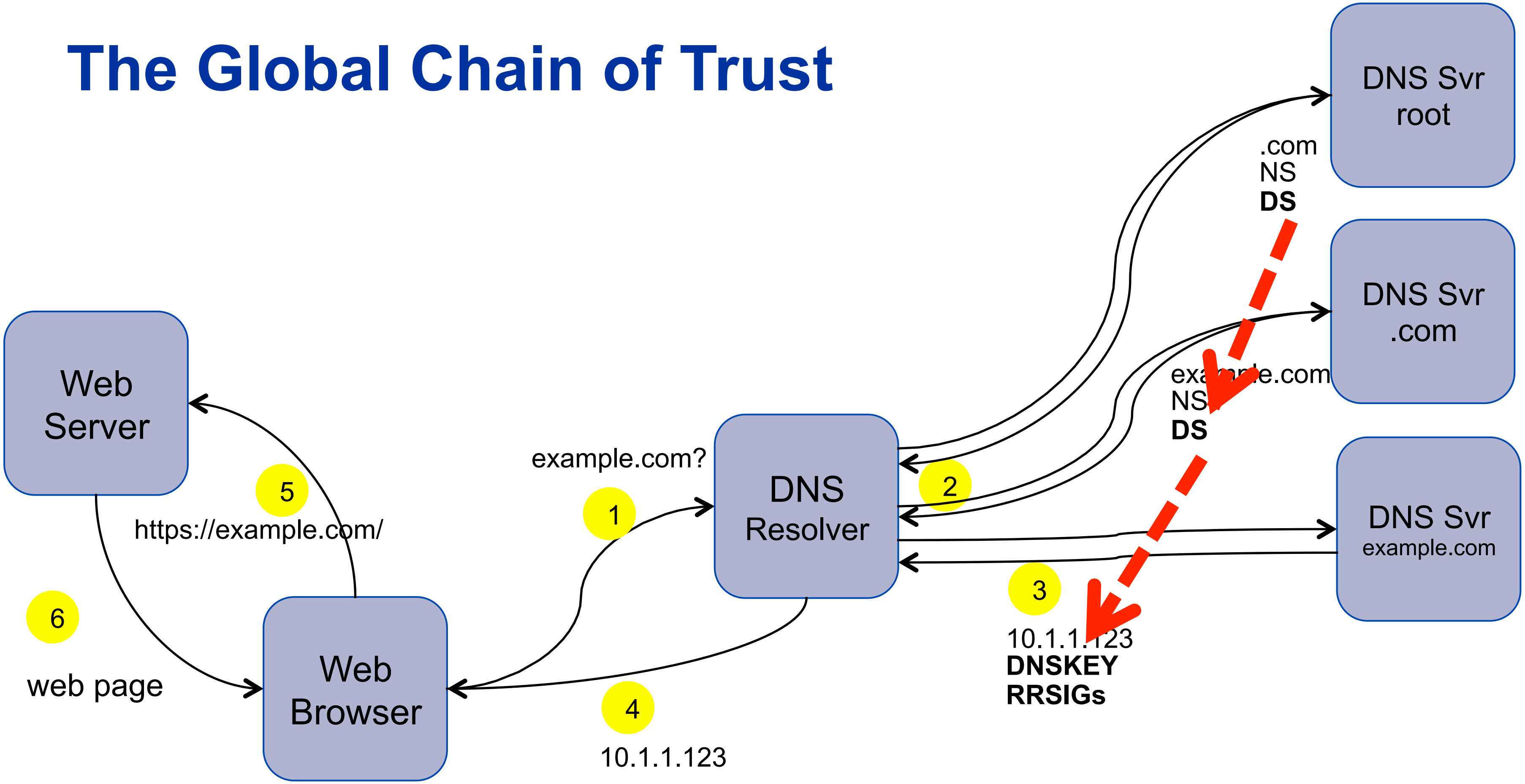
Delegation Signer (DS) Record

Fingerprint of DNSKEY sent to registry

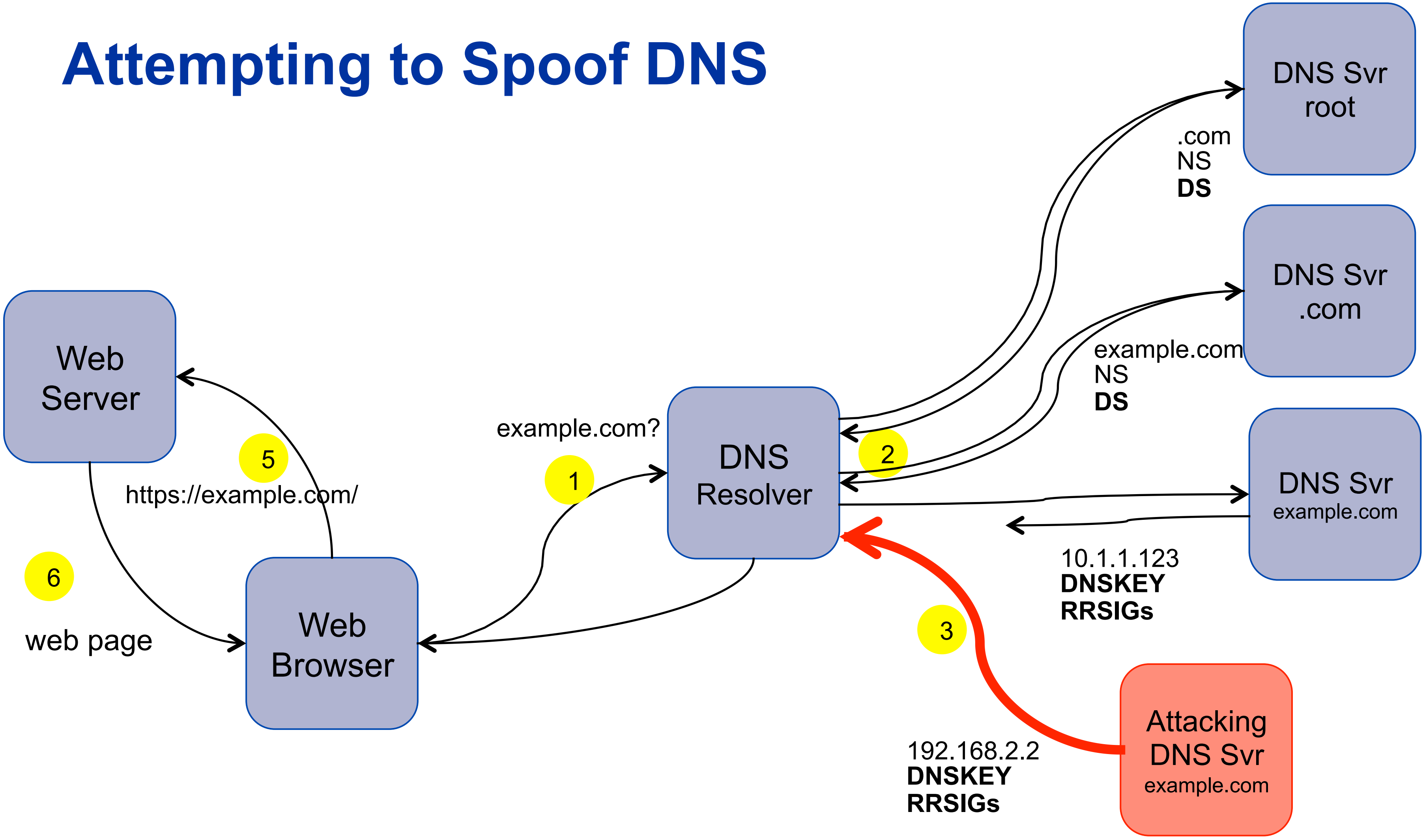
A DNSSEC Interaction



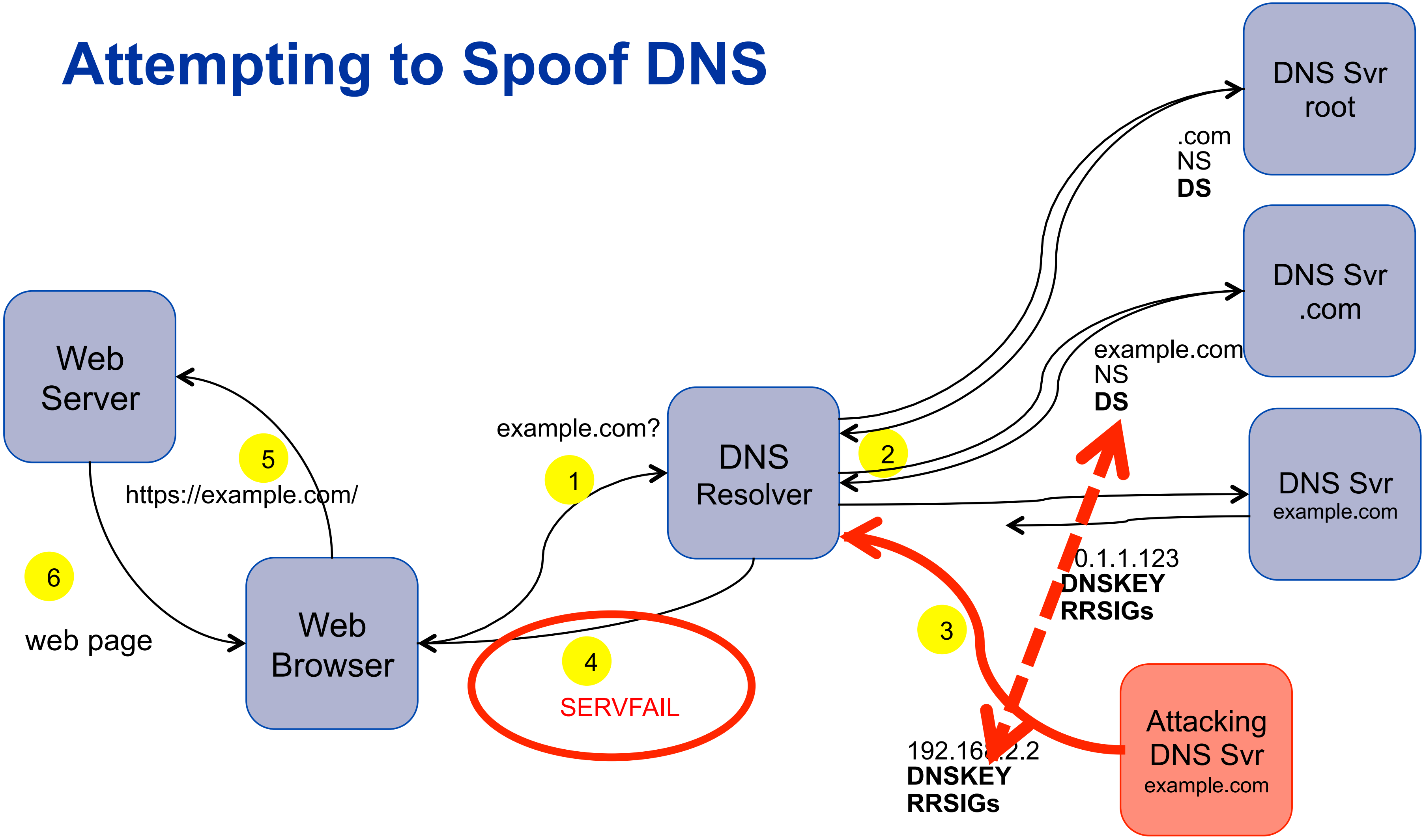
The Global Chain of Trust



Attempting to Spoof DNS



Attempting to Spoof DNS

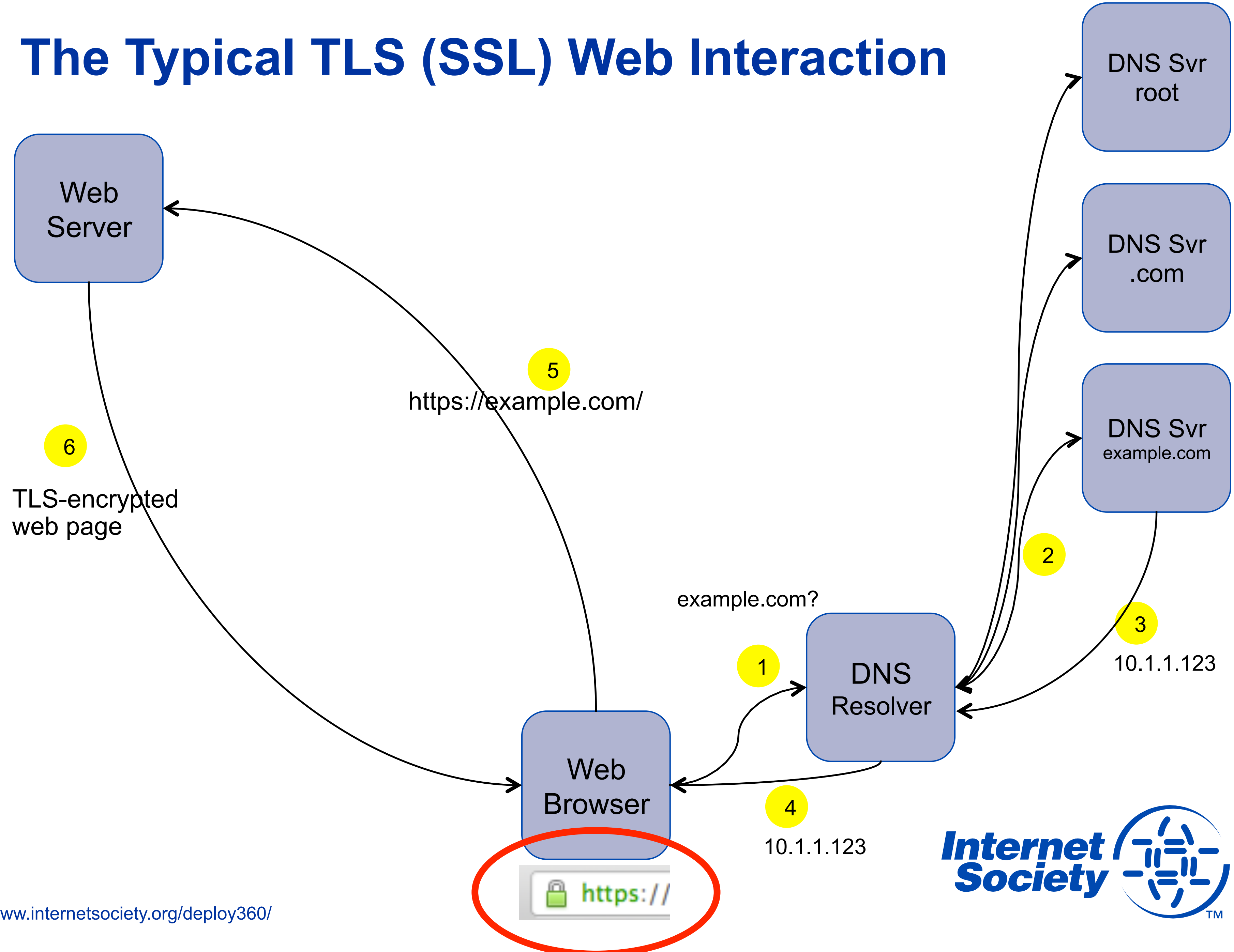


Integrity of DNS answers

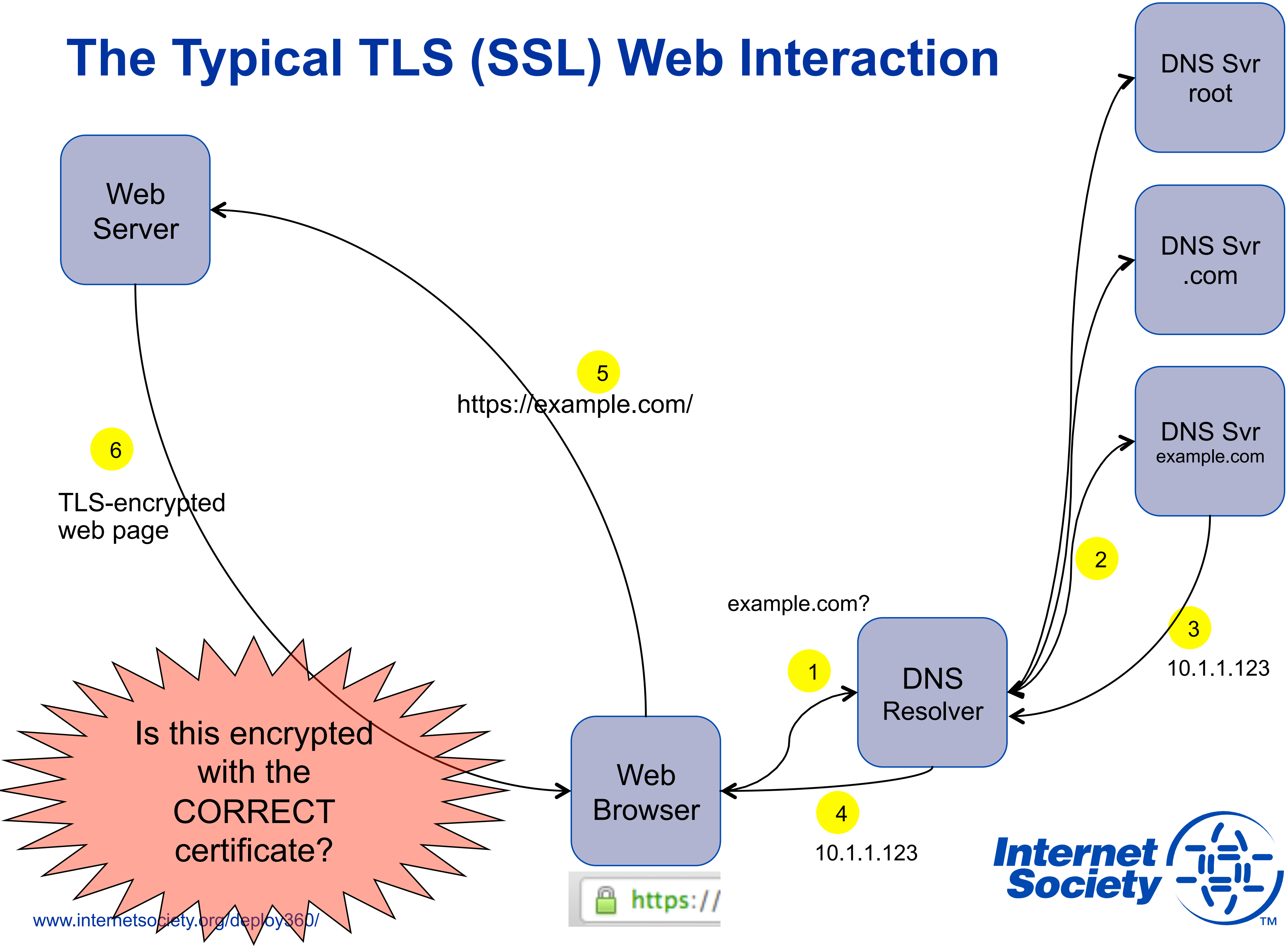
Ensuring info entered into DNS is the **SAME** info end user receives

But if I have SSL (TLS), why do I need DNSSEC?

The Typical TLS (SSL) Web Interaction



The Typical TLS (SSL) Web Interaction



Web Server

DNS Svr root

DNS Svr .com

DNS Svr example.com

5 https://example.com/

6 TLS-encrypted web page

2

example.com?

3 10.1.1.123

1

DNS Resolver

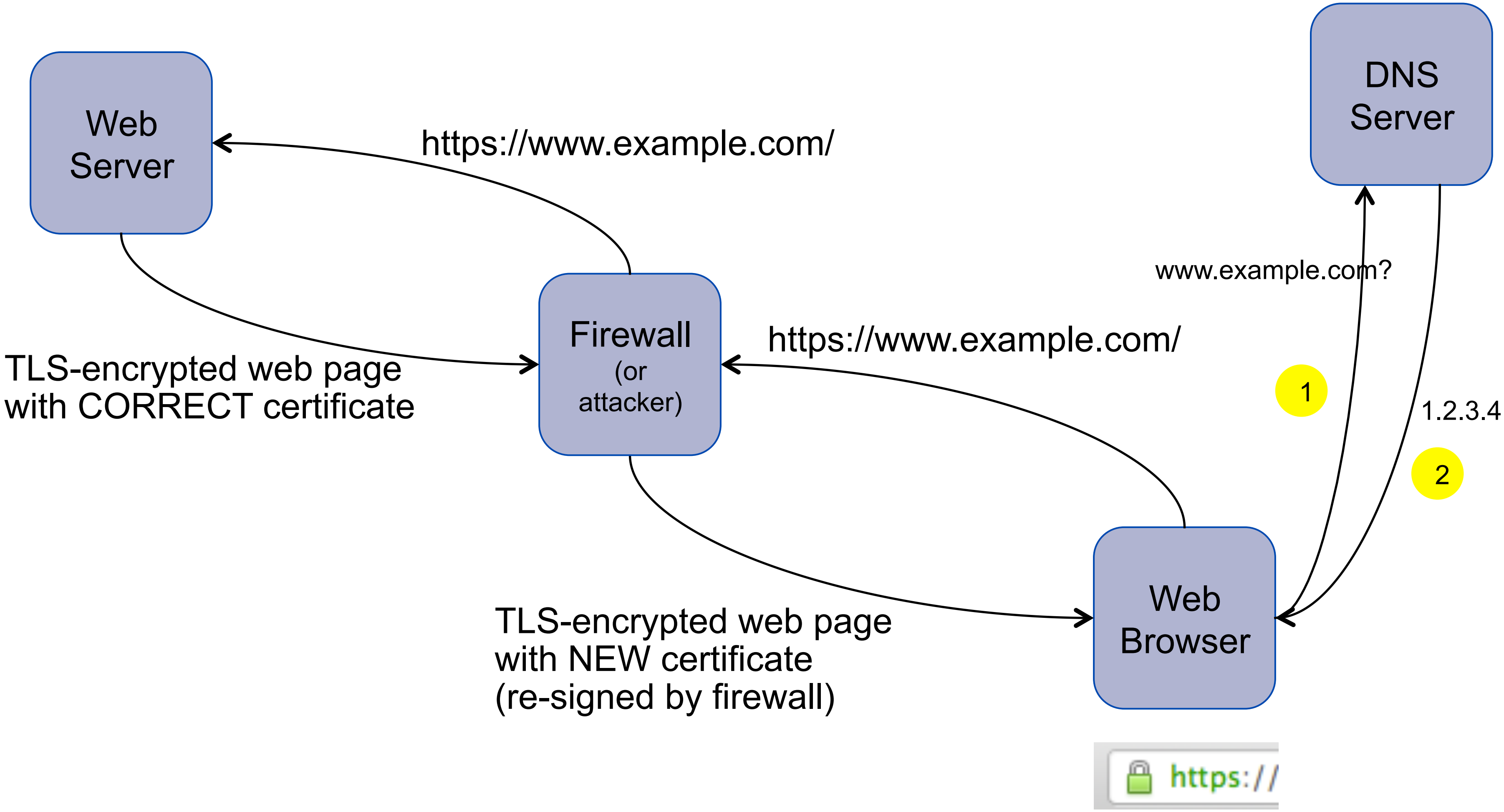
Web Browser

4 10.1.1.123

https://

Is this encrypted with the CORRECT certificate?

What About This?



Web Server

https://www.example.com/

DNS Server

Firewall (or attacker)

www.example.com?

https://www.example.com/

TLS-encrypted web page with CORRECT certificate

1

1.2.3.4

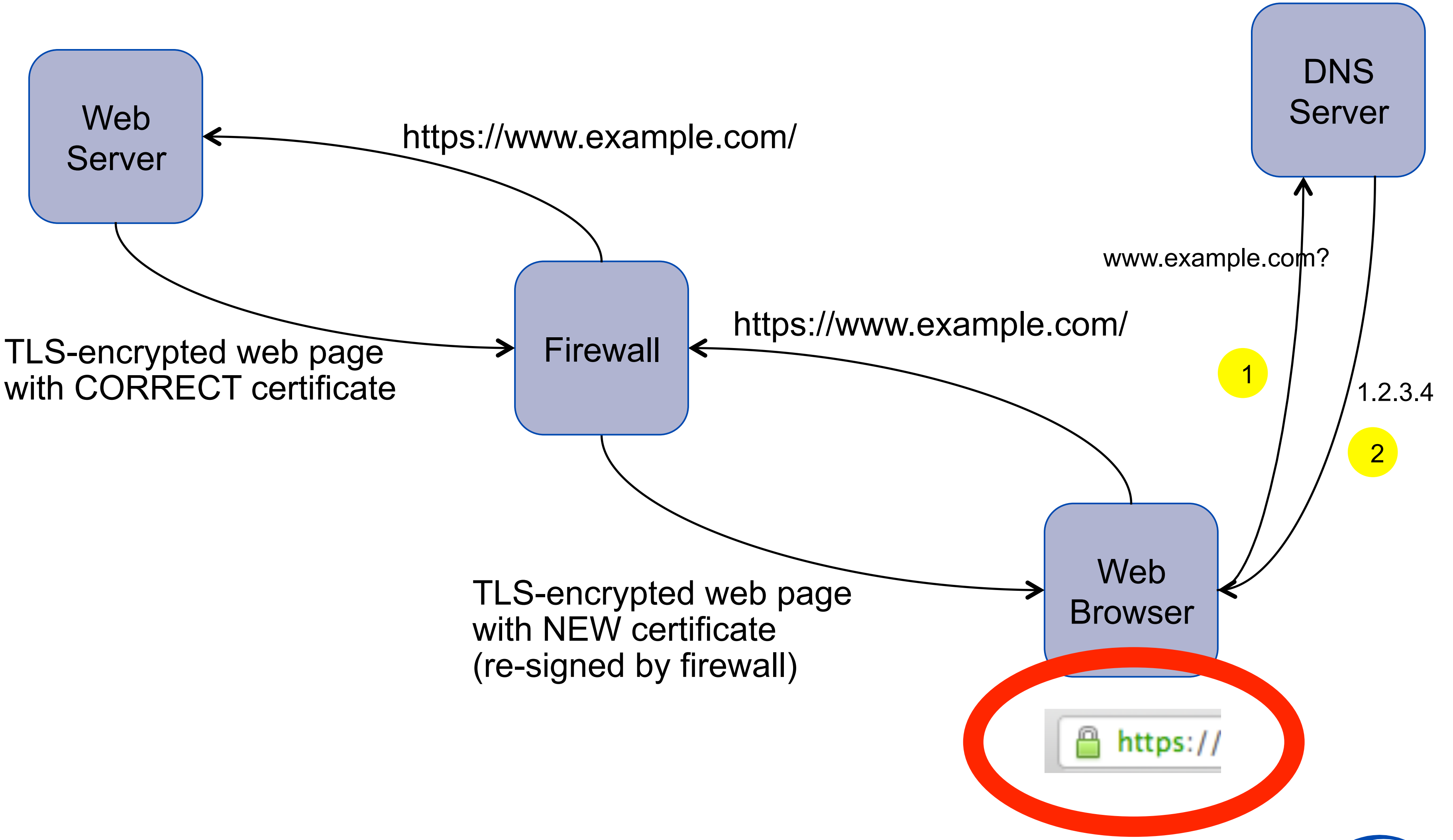
2

Web Browser

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

https://

Problems?



Web Server

Firewall

DNS Server

Web Browser

https://www.example.com/

TLS-encrypted web page with CORRECT certificate

https://www.example.com/

www.example.com?

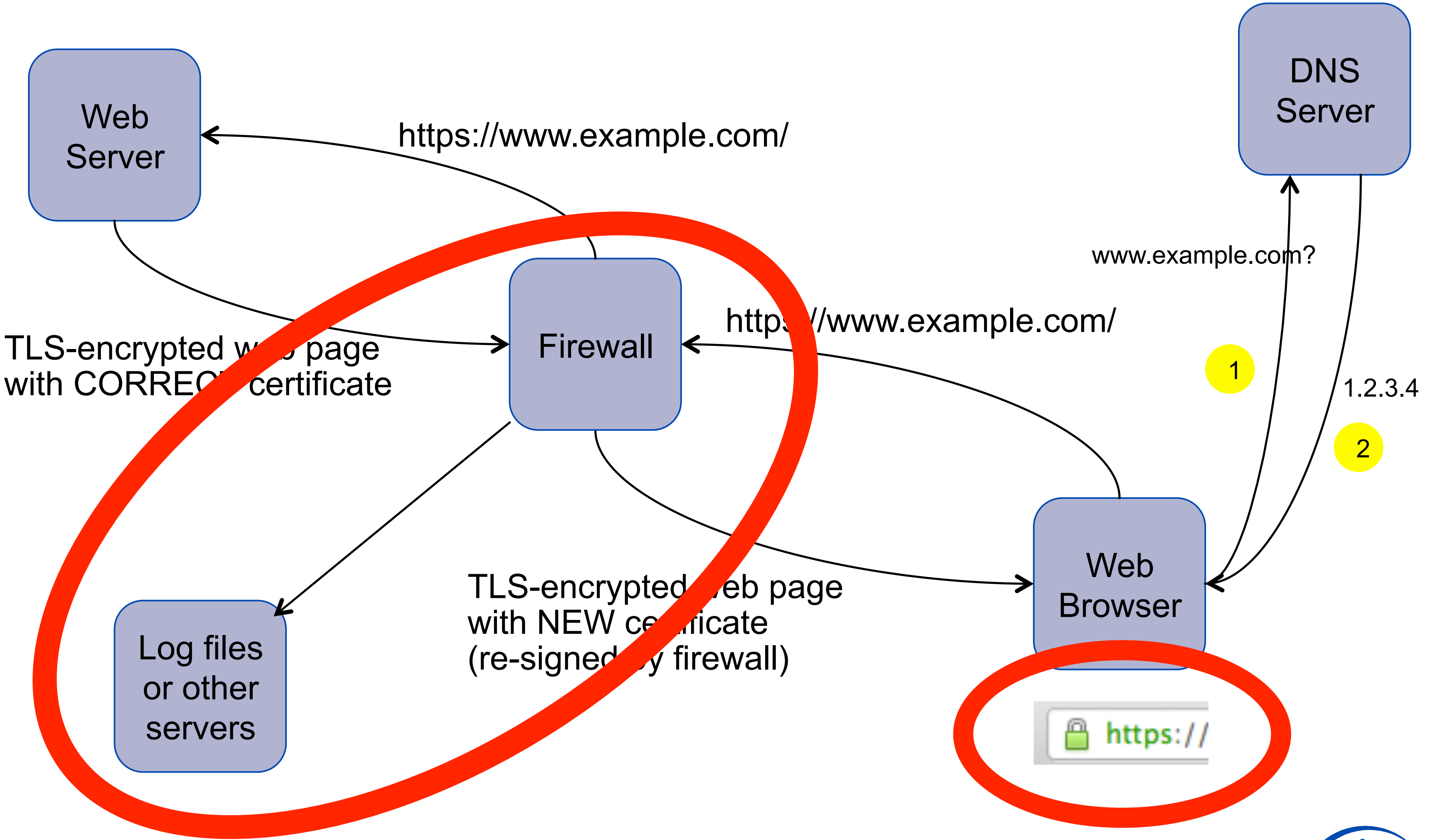
1

1.2.3.4

2

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

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
Log files or other servers
TLS-encrypted web page with NEW certificate (re-signed by firewall)
https://

Potentially including personal information

Issues

A Certificate Authority (CA) can sign *ANY* domain.

Now over 1,500 CAs – there have been compromises where valid certs were issued for domains.

Middle-boxes such as firewalls can re-sign sessions.

TLS = encryption + *limited* integrity protection

DNSSEC = **strong** integrity protection

encryption +
strong integrity
protection?

TLS + DNSSEC =

DANE

DNS-Based Authentication of Named Entities (DANE)

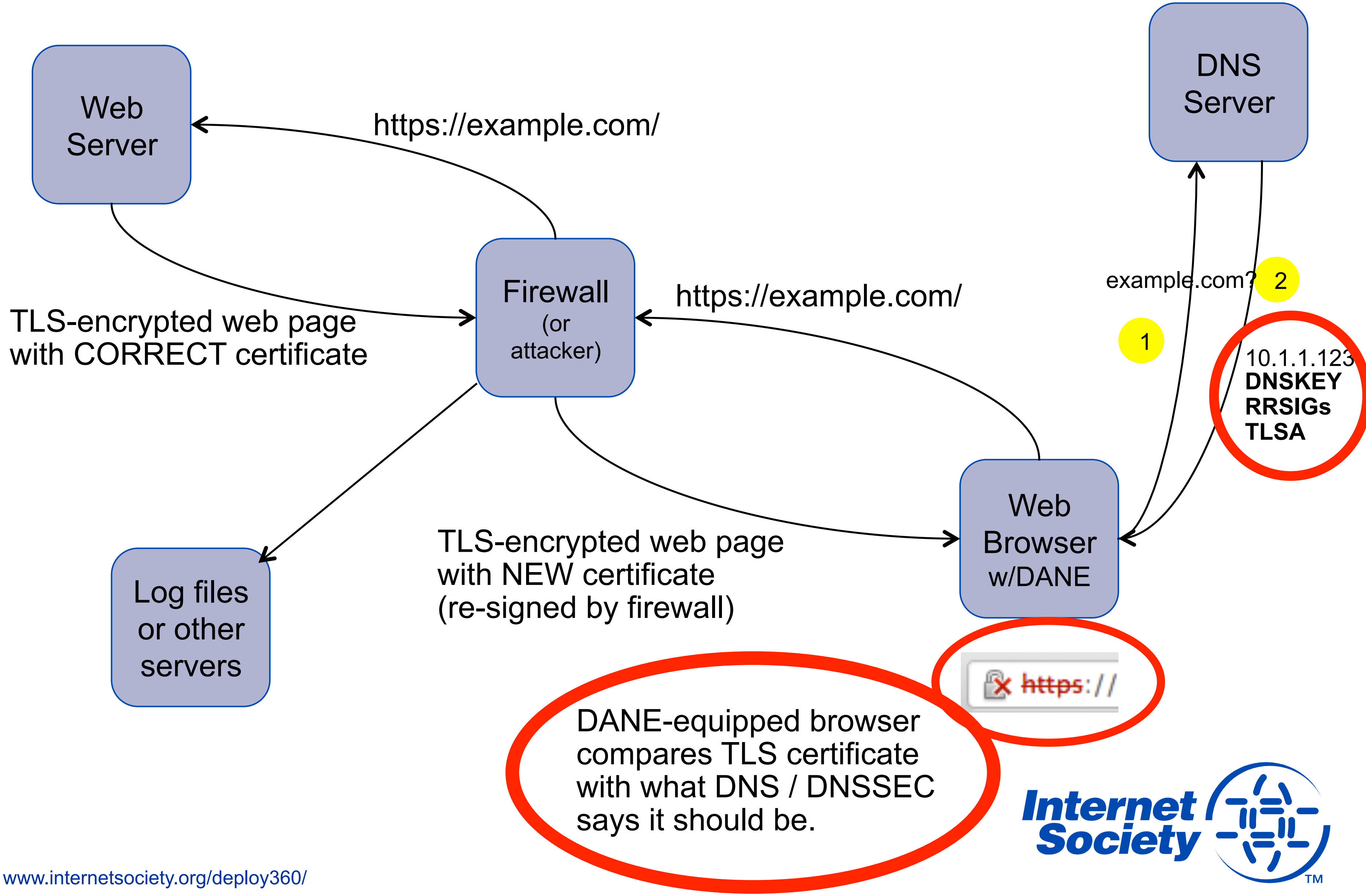
- Q: How do you know if the TLS (SSL) certificate is the correct one the site wants you to use?

- 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



Web Server

https://example.com/

Firewall (or attacker)

TLS-encrypted web page with CORRECT certificate

https://example.com/

DNS Server

example.com?

1

2

10.1.1.123
DNSKEY
RRSIGs
TLSA

Web Browser w/DANE

Log files or other servers

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

~~https~~://

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

Internet Society ™

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
  - ?

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**

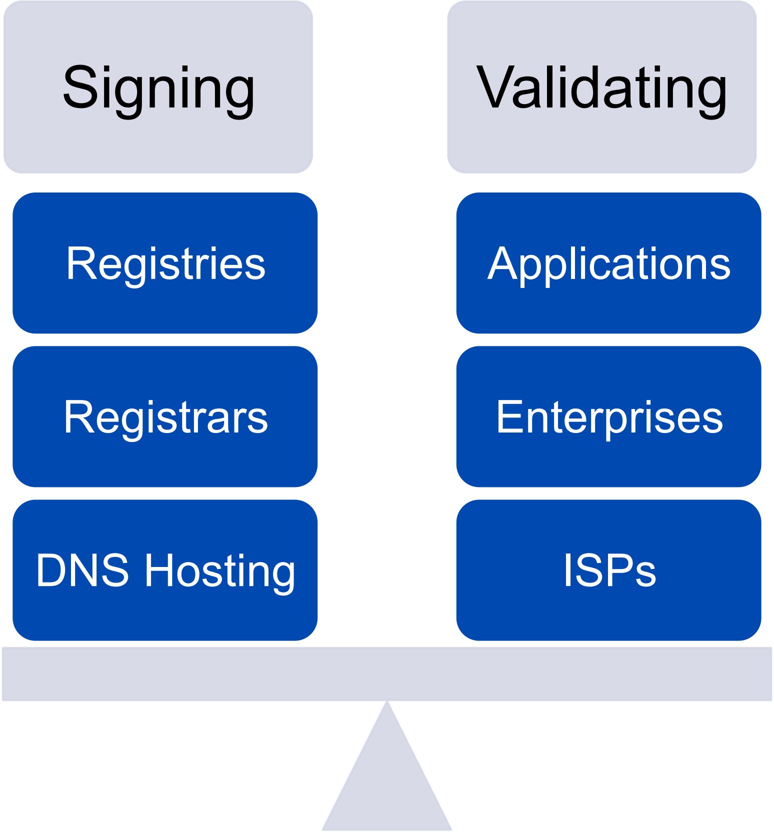
Opportunities

- DANE is just *one* example of new opportunities brought about by DNSSEC

- Developers and others already exploring new ideas

Getting DNSSEC Deployed

The Two Parts of DNSSEC



Key Questions

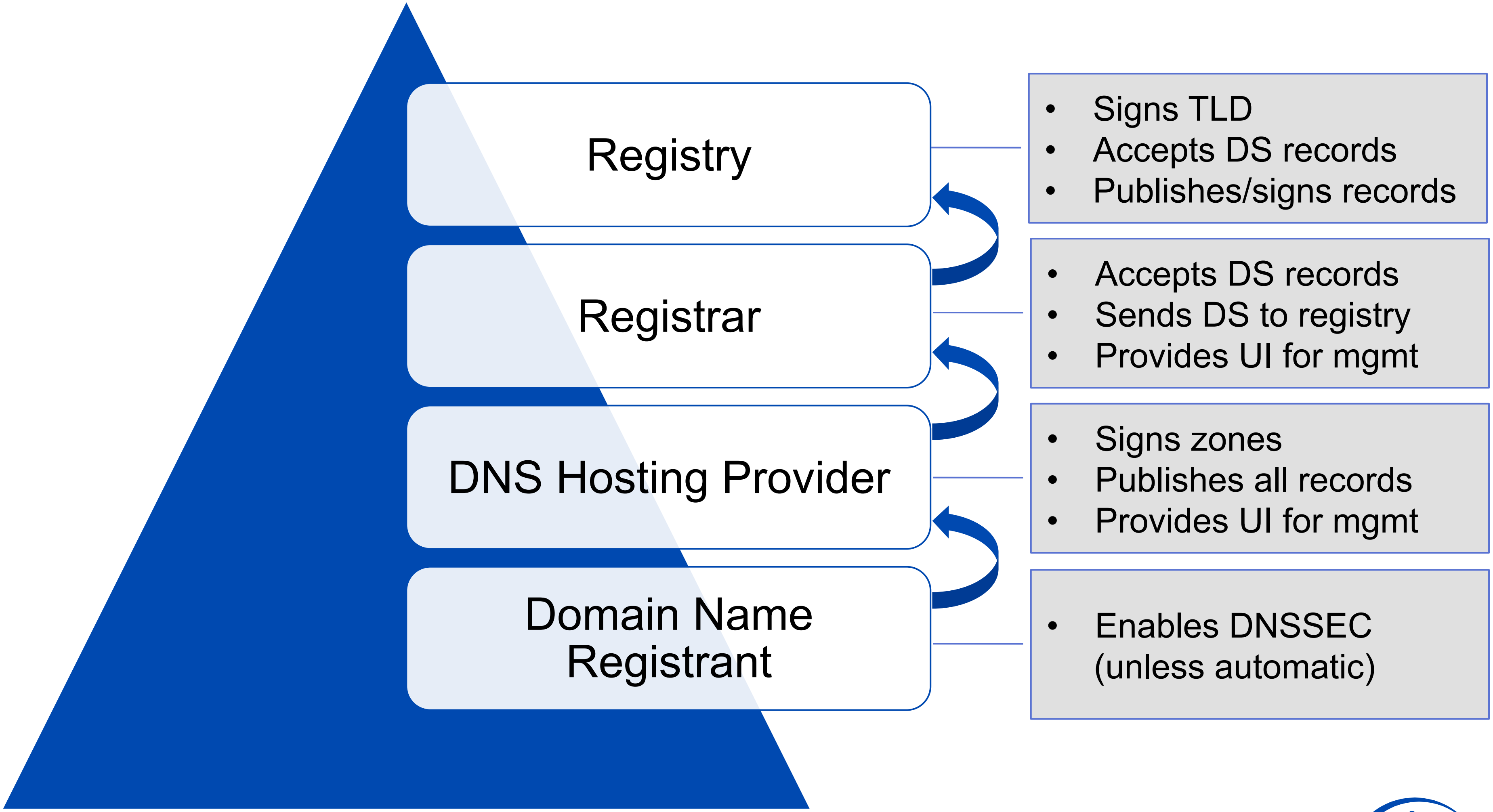
- What needs to be done to get more domains signed with DNSSEC?
- How can DNSSEC validation be more widely deployed?
- Are there technical issues or are the issues more of communication and awareness?
- How can we as a community address these challenges to increase the usage and availability of DNSSEC?

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

Registries / Registrars / DNS Hosting Providers

DNSSEC Signing - The Individual Steps



Registry

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

Registrar

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

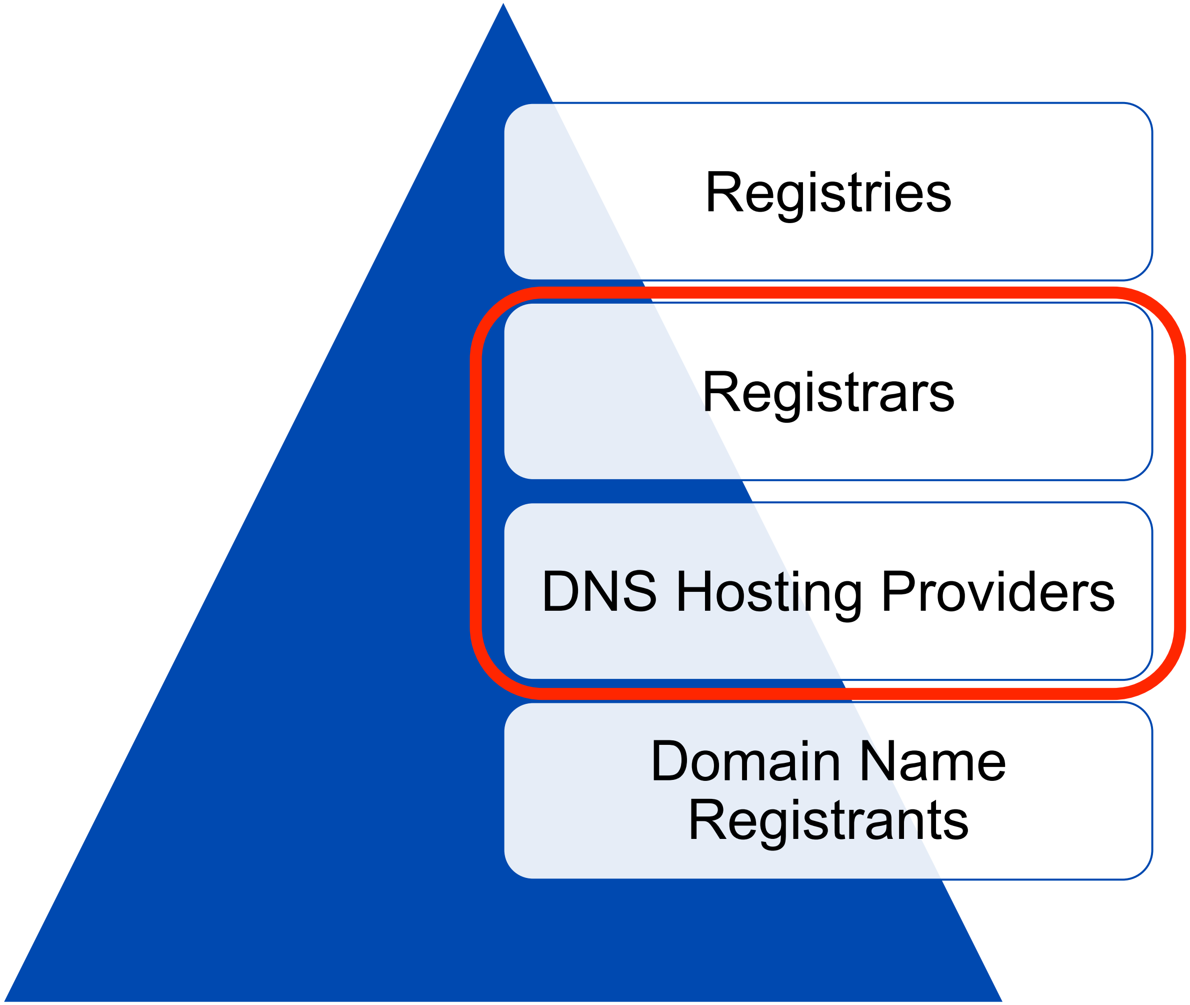
DNS Hosting Provider

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

Domain Name Registrant

- Enables DNSSEC (unless automatic)

DNSSEC Signing - The Players



Registries

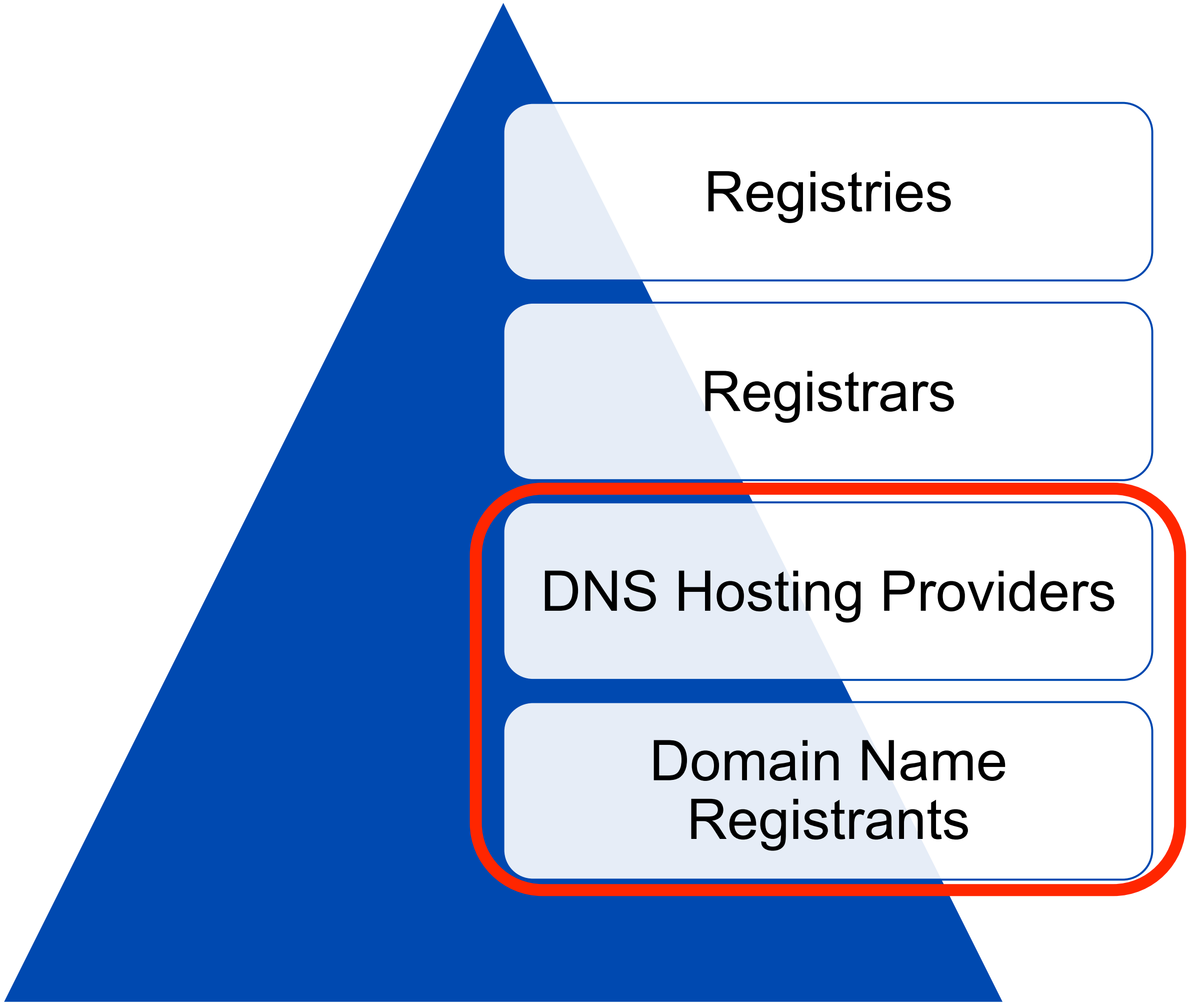
Registrars

DNS Hosting Providers

Domain Name Registrants

Registrar also provides DNS hosting services

DNSSEC Signing - The Players



Registries

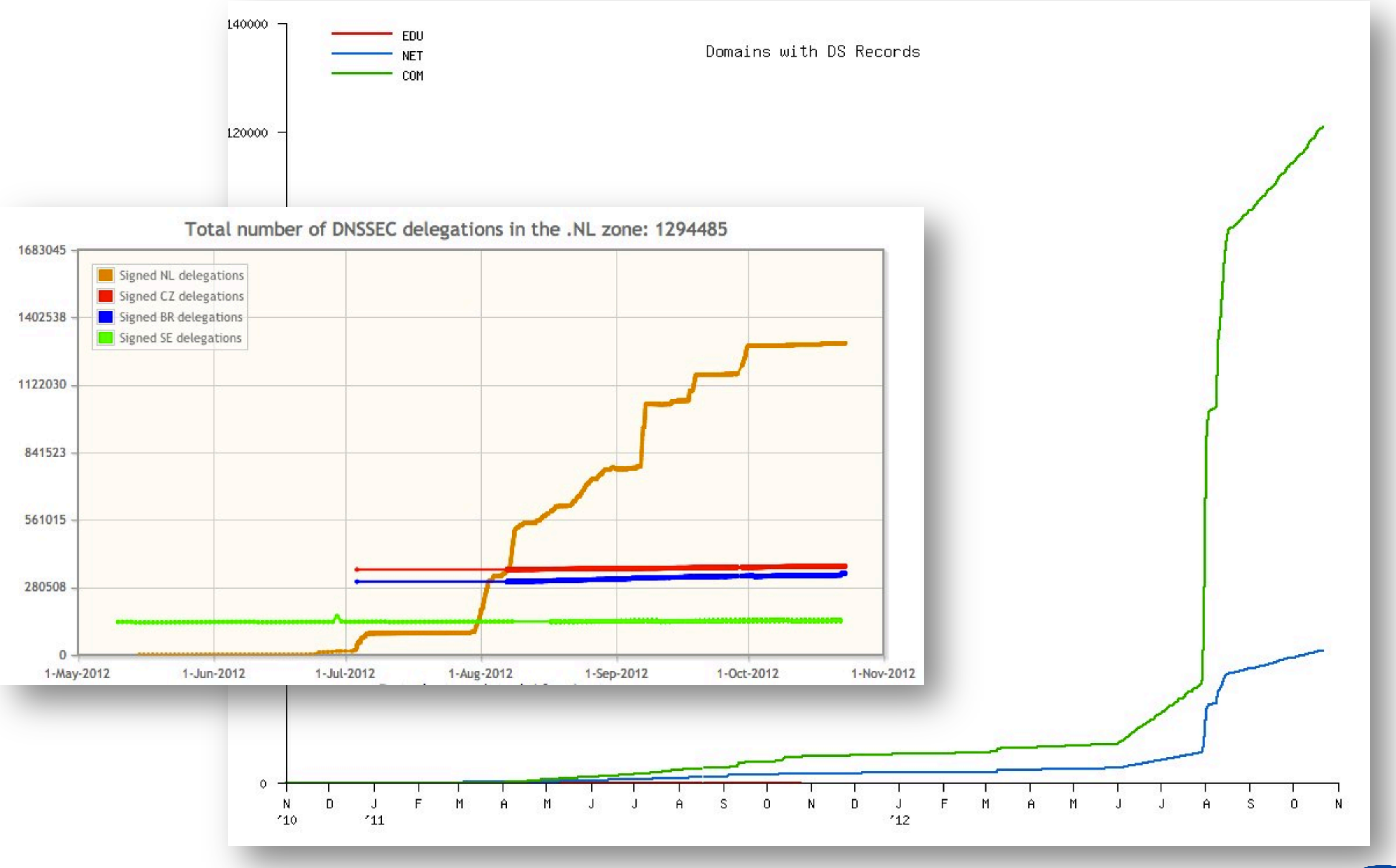
Registrars

DNS Hosting Providers

Domain Name Registrants

Registrant hosts own DNS

Strong Growth In Signed Domains



Sources: PowerDNS and Verisign Labs

www.internetsociety.org/deploy360/dnssec/statistics/

Increasing Number of Domain Name Registrars

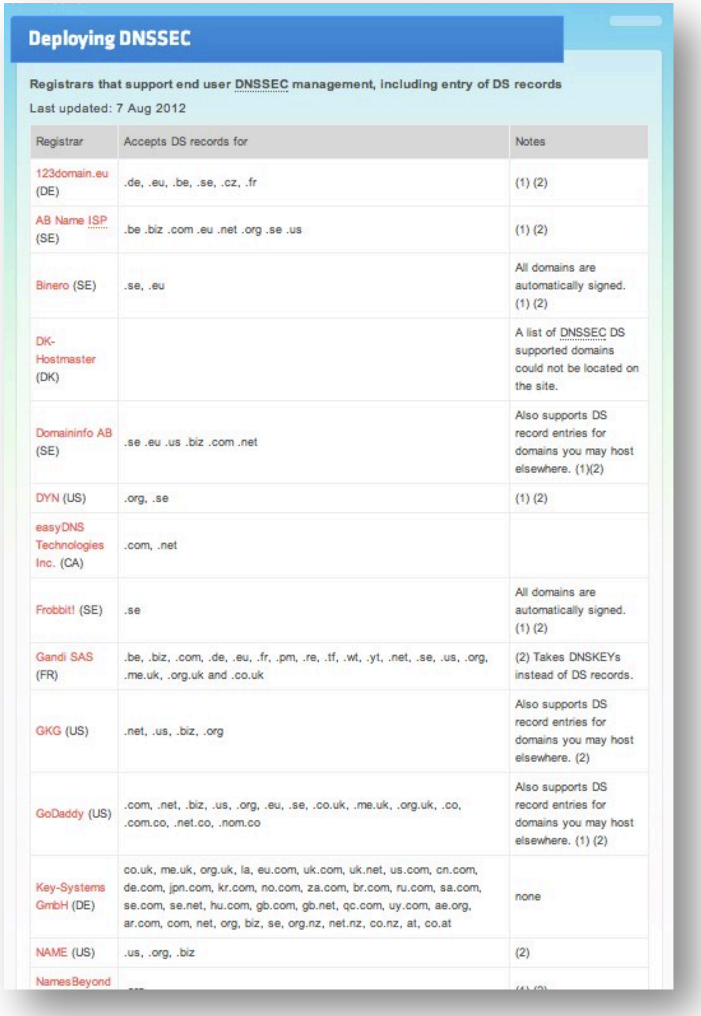
Need to increase number of domain name registrars supporting DNSSEC

- Good news is that the list keeps increasing!

List from ICANN at:

- www.icann.org/en/news/in-focus/dnssec/deployment

If you are a registar and support DNSSEC, you can ask to be added to ICANN's list.



Deploying DNSSEC

Registrars that support end user DNSSEC management, including entry of DS records

Last updated: 7 Aug 2012

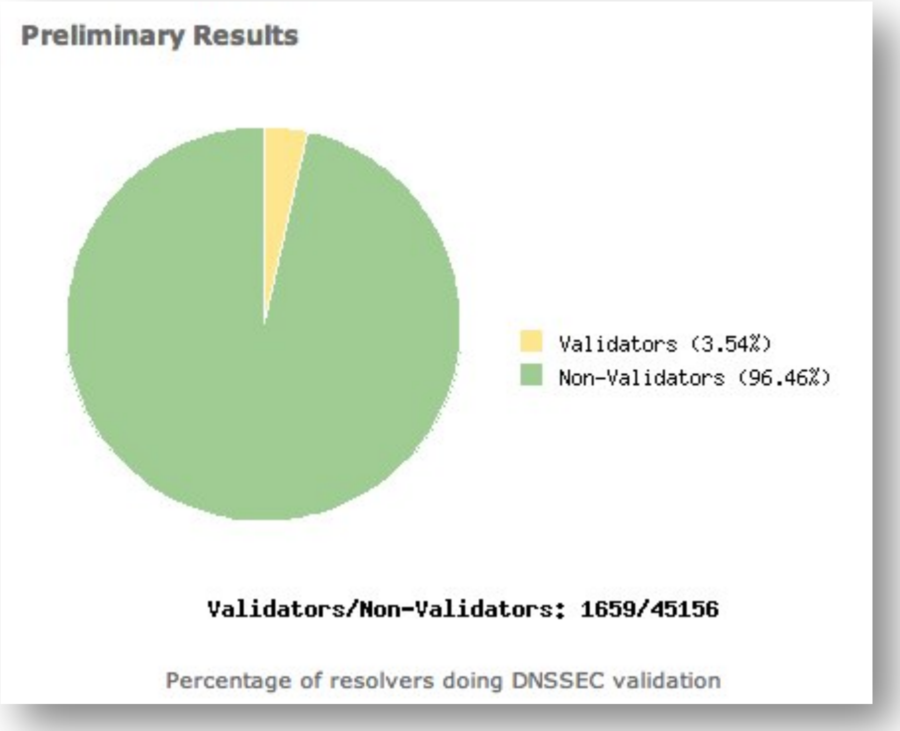
Registrar	Accepts DS records for	Notes
123domain.eu (DE)	.de, .eu, .be, .se, .cz, .fr	(1) (2)
AB Name ISP (SE)	.be .biz .com .eu .net .org .se .us	(1) (2)
Binero (SE)	.se, .eu	All domains are automatically signed. (1) (2)
DK-Hostmaster (DK)		A list of DNSSEC DS supported domains could not be located on the site.
Domaininfo AB (SE)	.se .eu .us .biz .com .net	Also supports DS record entries for domains you may host elsewhere. (1)(2)
DYN (US)	.org, .se	(1) (2)
easyDNS Technologies Inc. (CA)	.com, .net	
Frobbit! (SE)	.se	All domains are automatically signed. (1) (2)
Gandi SAS (FR)	.be, .biz, .com, .de, .eu, .fr, .pm, .re, .tf, .wt, .yt, .net, .se, .us, .org, .me.uk, .org.uk and .co.uk	(2) Takes DNSKEYs instead of DS records.
GKG (US)	.net, .us, .biz, .org	Also supports DS record entries for domains you may host elsewhere. (2)
GoDaddy (US)	.com, .net, .biz, .us, .org, .eu, .se, .co.uk, .me.uk, .org.uk, .co, .com.co, .net.co, .nom.co	Also supports DS record entries for domains you may host elsewhere. (1) (2)
Key-Systems GmbH (DE)	co.uk, me.uk, org.uk, la, eu.com, uk.com, uk.net, us.com, cn.com, de.com, jpn.com, kr.com, no.com, za.com, br.com, ru.com, sa.com, se.com, se.net, hu.com, gb.com, gb.net, qc.com, uy.com, ae.org, ar.com, com, net, org, biz, se, org.nz, net.nz, co.nz, at, co.at	none
NAME (US)	.us, .org, .biz	(2)
NamesBeyond	[illegible]	(1) (2)

Source: www.icann.org/en/news/in-focus/dnssec/deployment

Validating Name Servers

Validating Name Servers

- **How do we increase the percentage?**



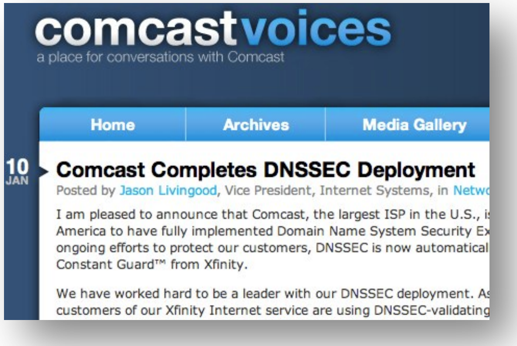
http://validator-search.verisignlabs.com

Availability of DNSSEC-Validating Resolvers

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

- Comcast in North America recently rolled out DNSSEC-validating resolvers to 18+ million customers

- Almost all ISPs in Sweden and Czech Republic provide DNSSEC-validating resolvers



Comcast Completes DNSSEC Deployment

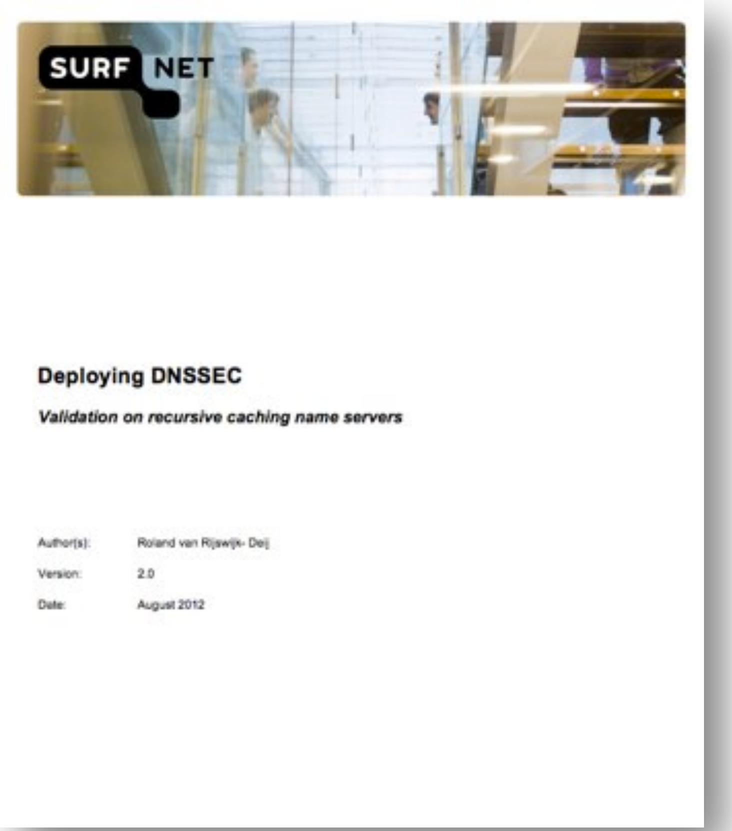
Posted by Jason Livingood, Vice President, Internet Systems, in Netwo

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

SURFnet Validating Server Whitepaper

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



Deploying DNSSEC

Validation on recursive caching name servers

Author(s): Roland van Rijswijk- Deij

Version: 2.0

Date: August 2012

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

Many DNSSEC Tools Now Available

- www.internetsociety.org/deploy360/dnssec/tools/
- www.dnssec-tools.org

Next Steps

New Industry Initiative Forming With Focus On:

1. Deployment Documentation

- What do we need in the way of better documentation/tutorials/etc ?

2. Tools

- What are the missing tools?

3. Unsolved Technical Issues

- What technical issues remain that need to be addressed?

4. Measurement

- How do we measure progress of DNSSEC deployment?
- Can we get more TLDs, ISPs to help provide statistics?

Join The Initial Discussions

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.

Planning for monthly conference calls to support online activities.

Stay tuned for more info… (and join the list!)

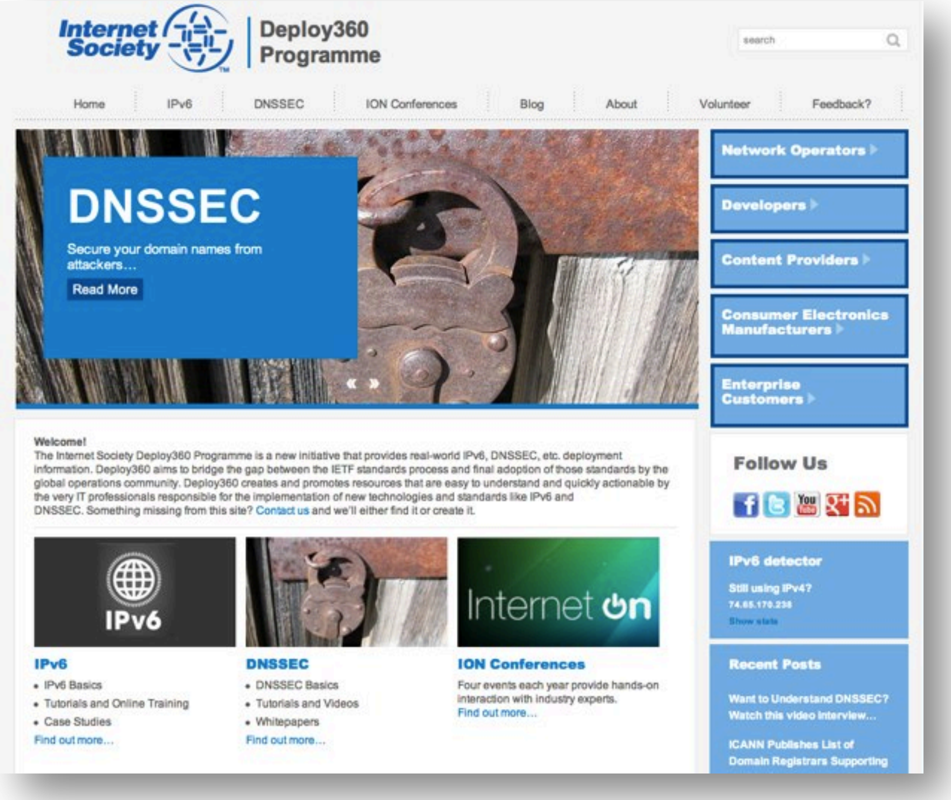
Three Requests For Network Operators

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



DNSSEC

Secure your domain names from attackers…

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 detector

Still using IPv4?
74.65.170.238
Show stats

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…

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, CISSP

Senior Content Strategist, Internet Society

york@isoc.org

www.internetsociety.org/deploy360/

Thank You!

Internet Society™