

# Opportunities For ccTLDs With DNSSEC

Dan York, CISSP  
Senior Content Strategist, Internet Society

ccNSO Meeting, ICANN 45  
Toronto, Canada  
October 16 , 2012

.EH

# market to startups

# Great success!

h.eh

m.eh

GoAw.eh

takeoff.eh

taboul.eh

sorry.eh

pl.eh

# The next Facebook

# THE social network

Pl.eh = ☺



ccTLD = ☺

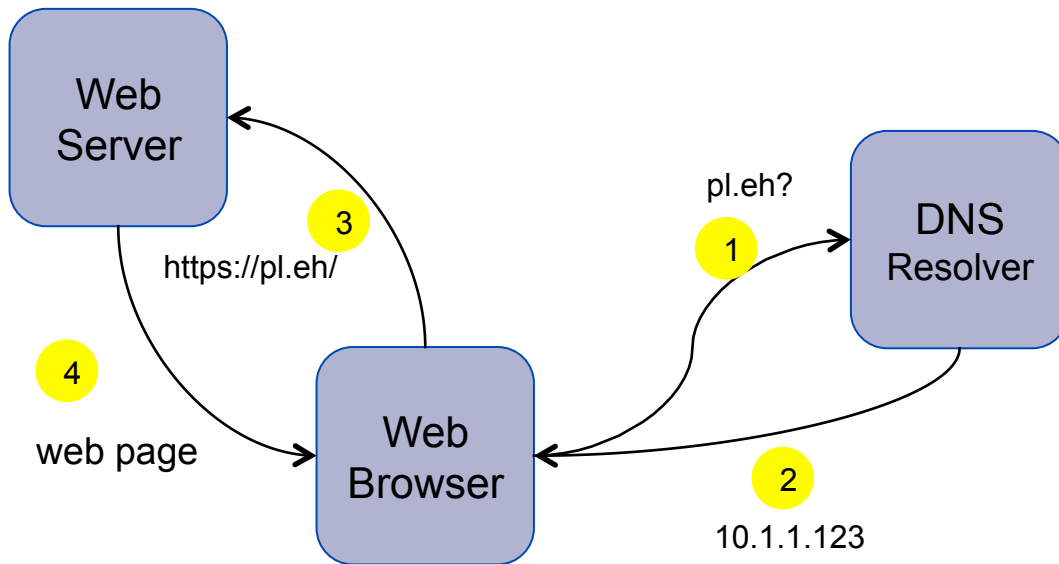
Success = more .EH  
domains



# disrupt

# DNS cache poisoning

# A Normal DNS Interaction

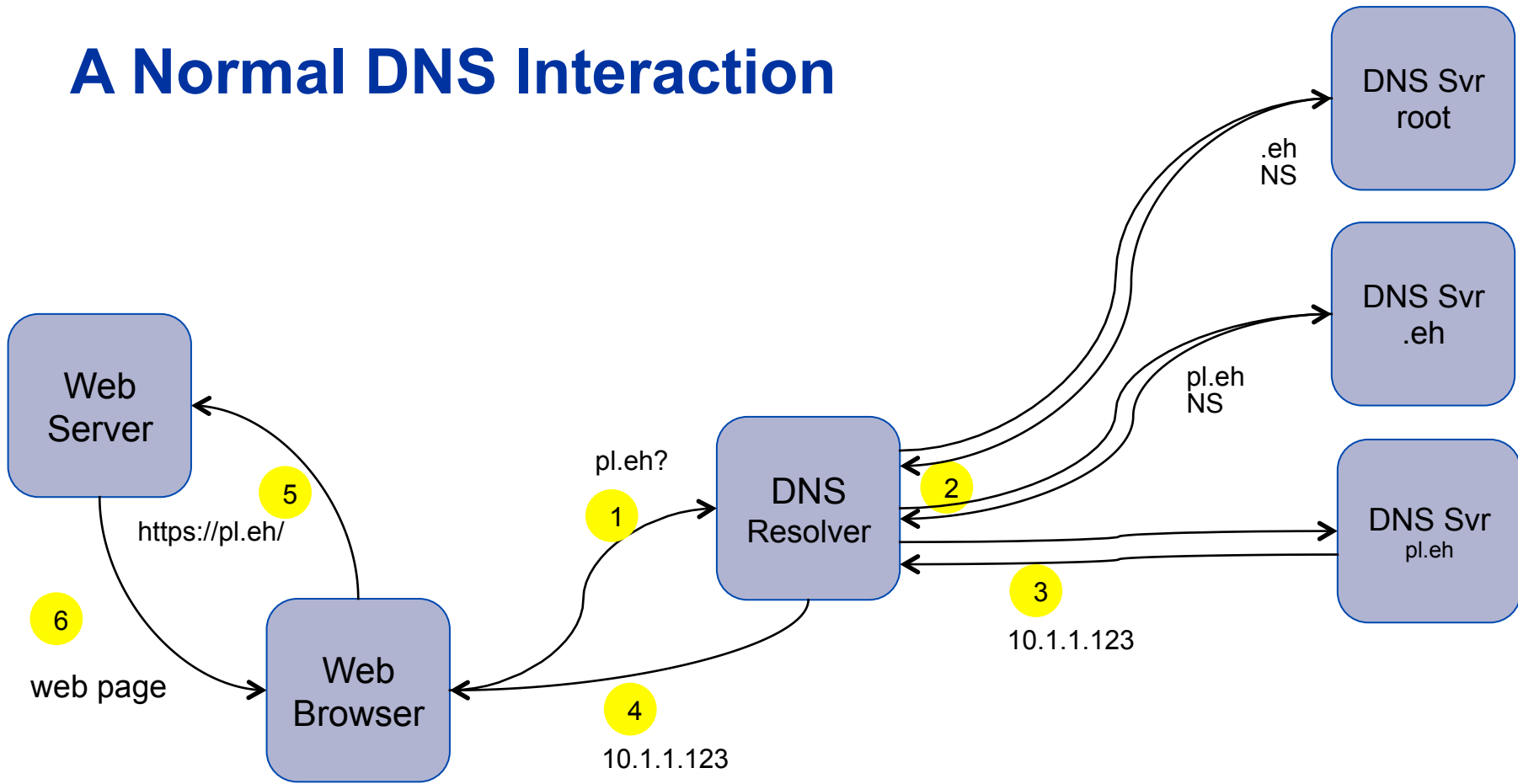


Resolver checks its local *cache*. If it has the answer, it sends it back.

pl.eh 10.1.1.123

If not...

# A Normal DNS Interaction



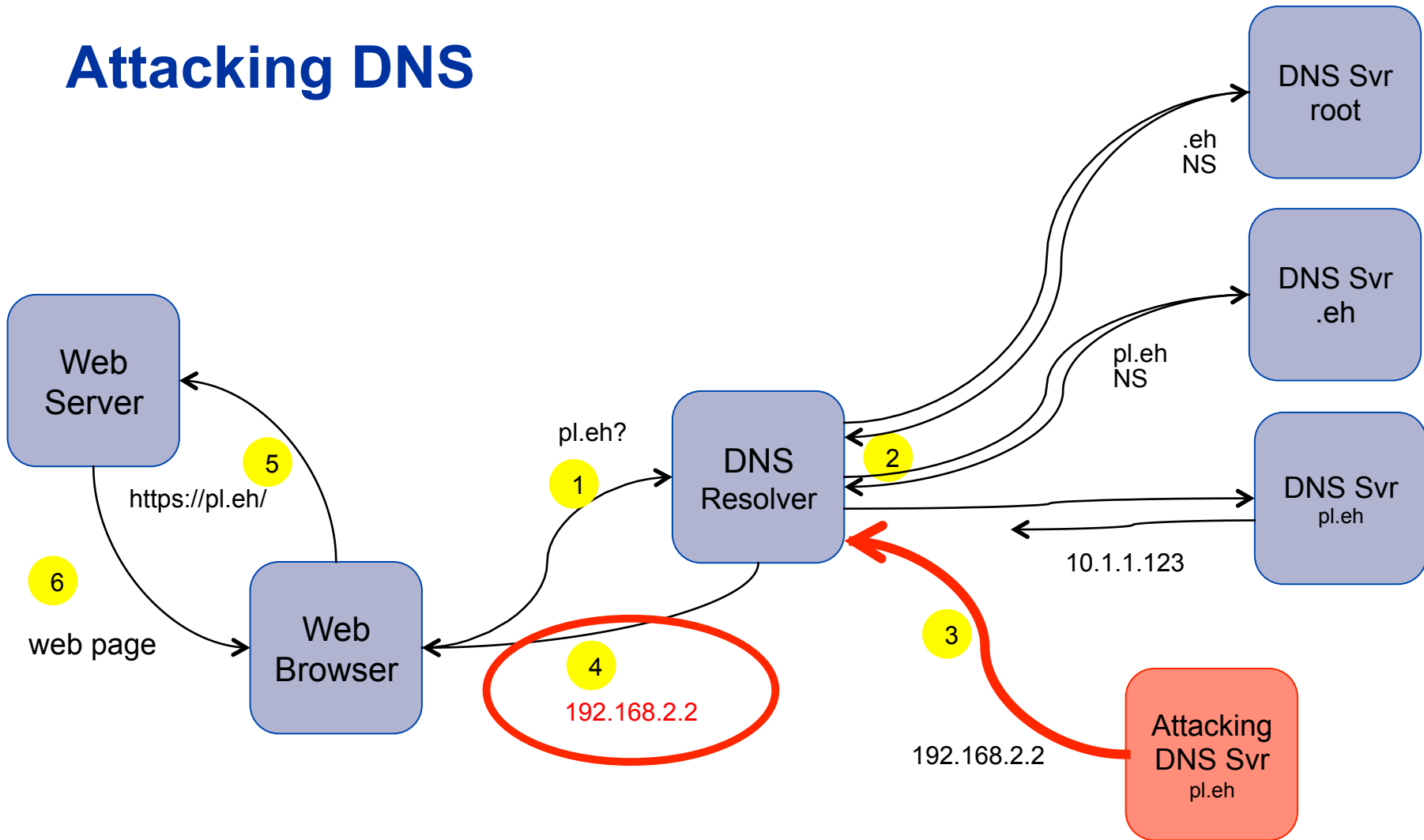
# DNS works on speed

# First result wins

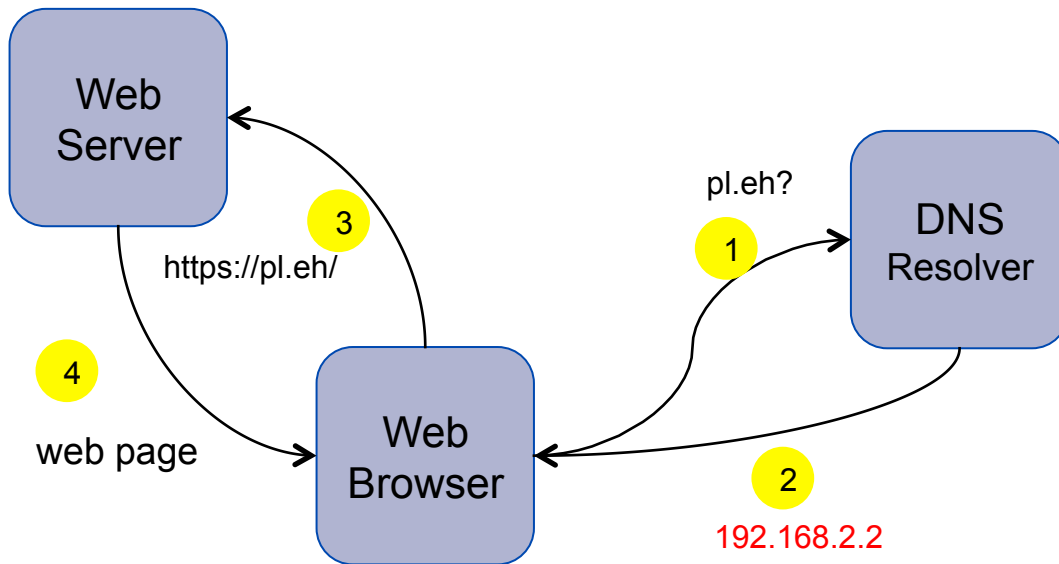


# What if someone else responds first?

# Attacking DNS



# A Poisoned Cache



Resolver **cache** now has wrong data:

`pl.eh` **192.168.2.2**

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

# Oops

# Unhappy Users

# Exposure of personal information

Pl.eh = ☹️

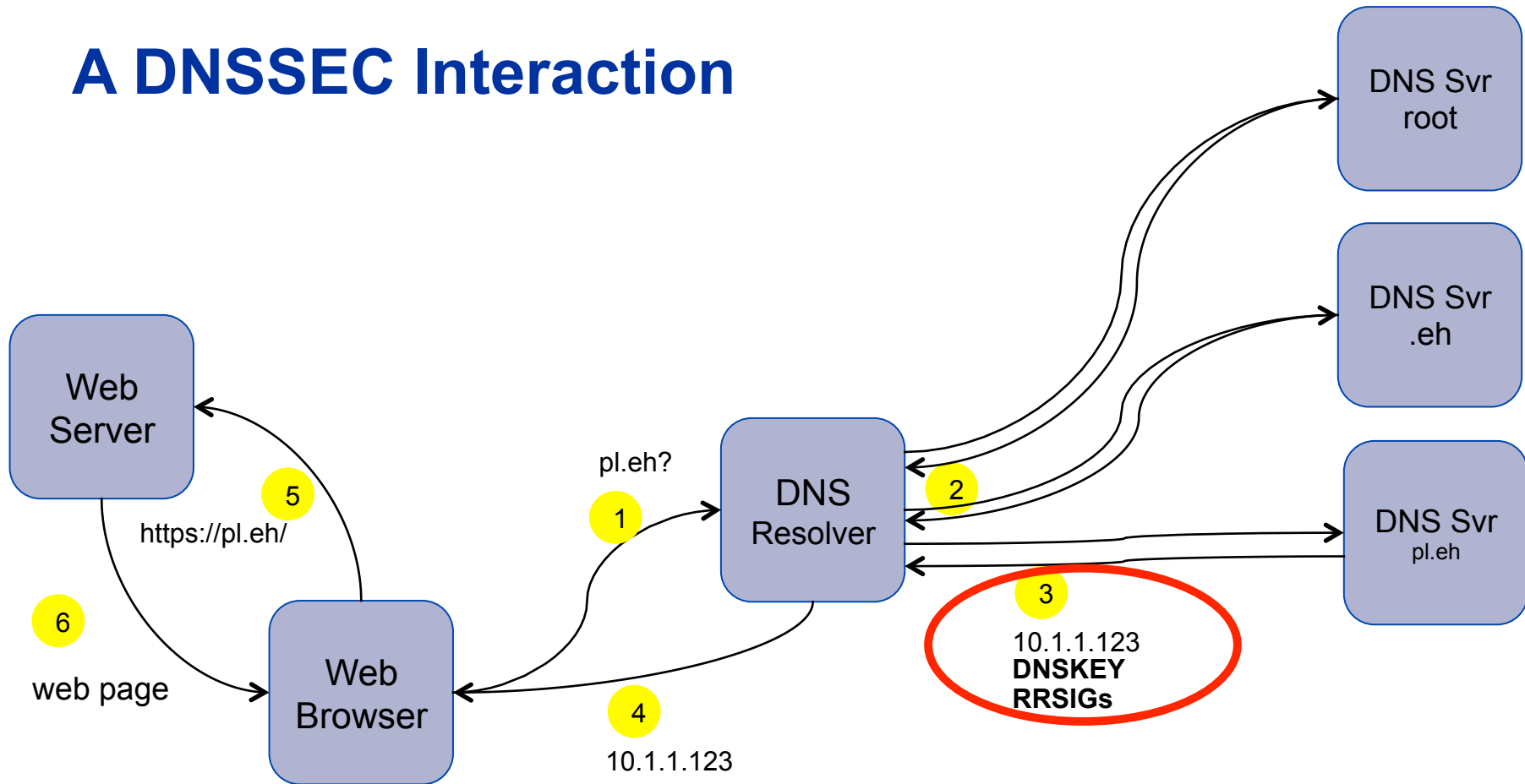
# Aha!



# .eh TLD is signed with DNSSEC

pl.eh  
gets signed

# A DNSSEC Interaction

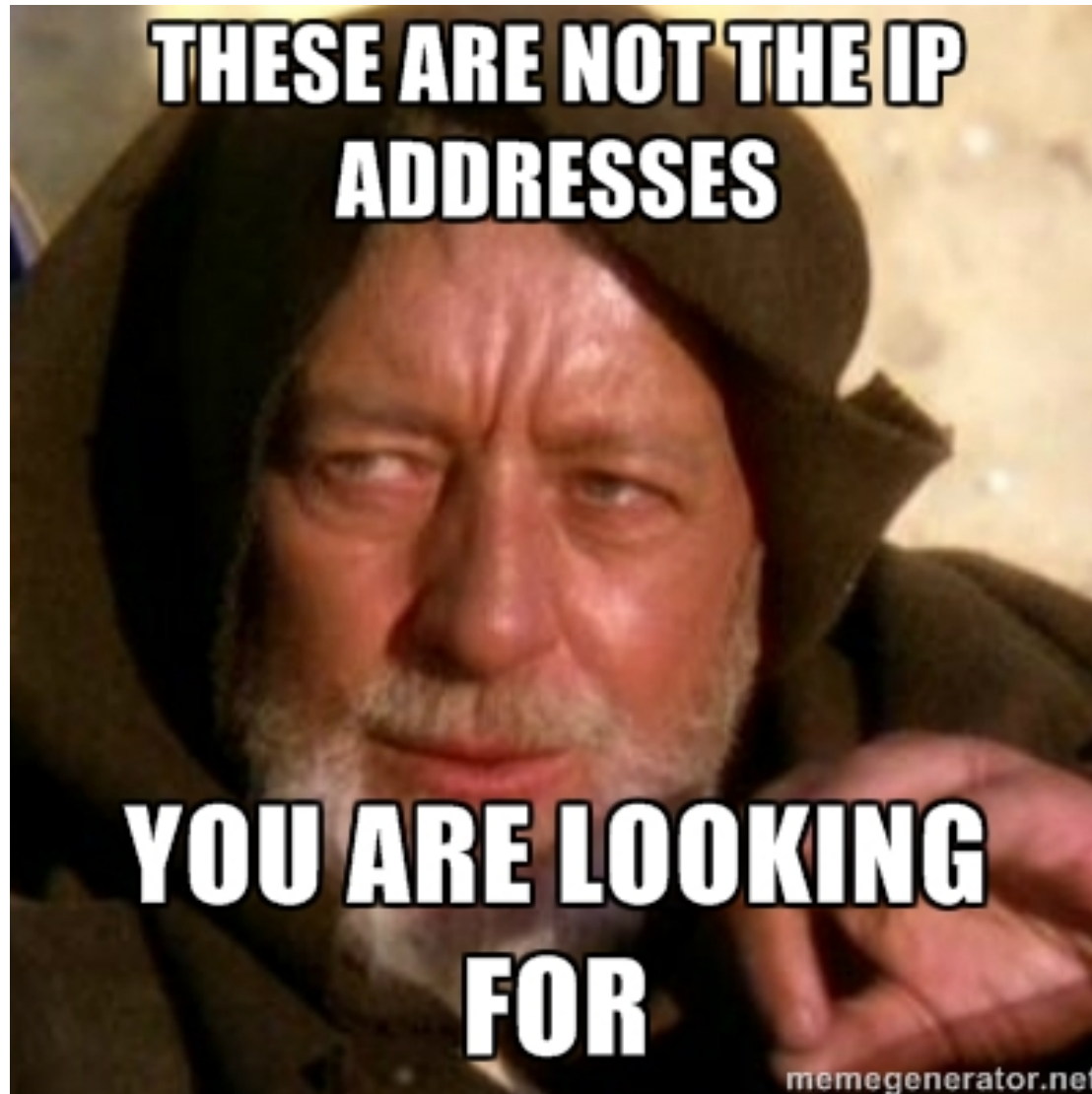


# DNS Resolver:

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

If results match,  
all is good.

If not...



# But wait...

# Spoof DNSSEC?

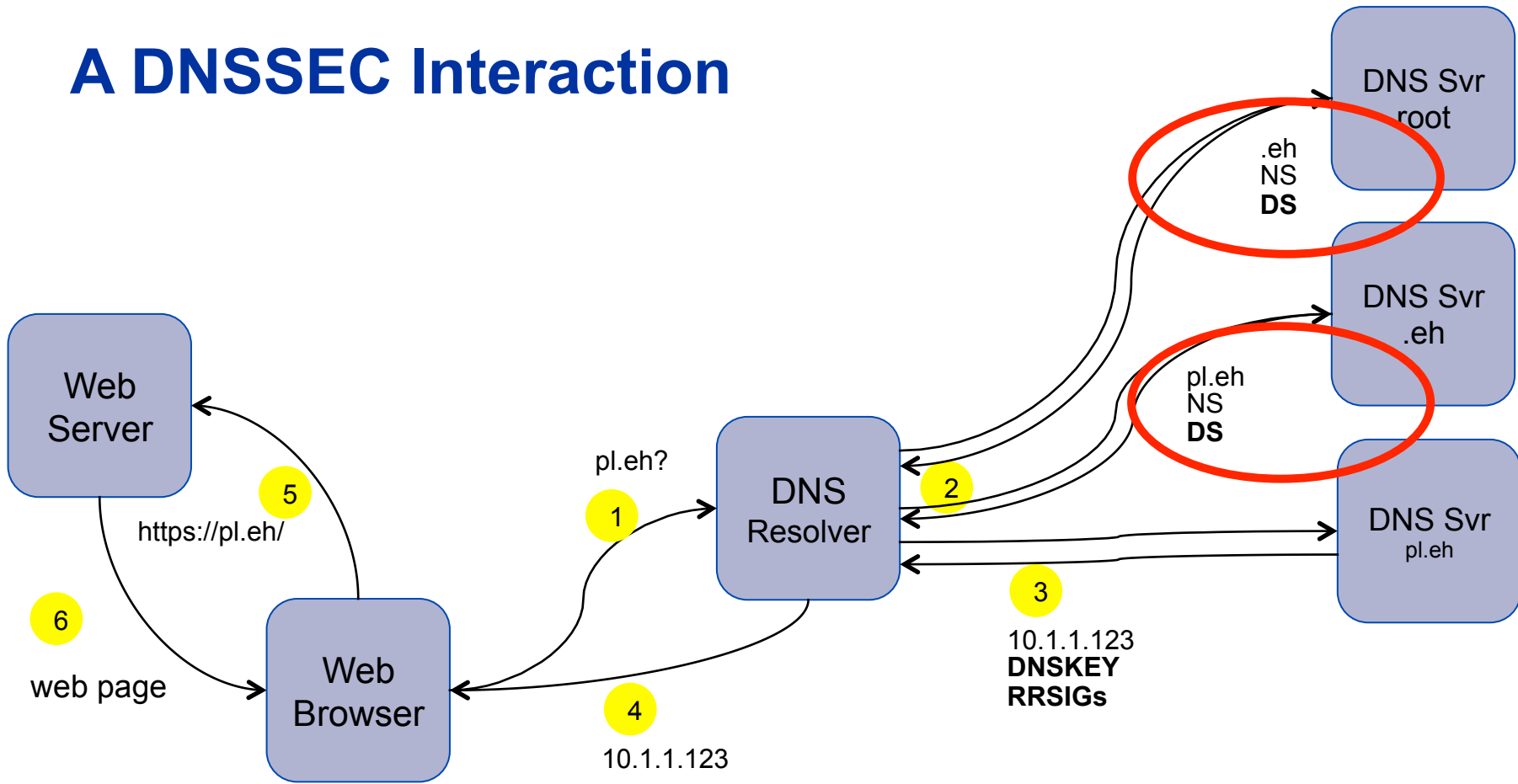


# They can try, but...

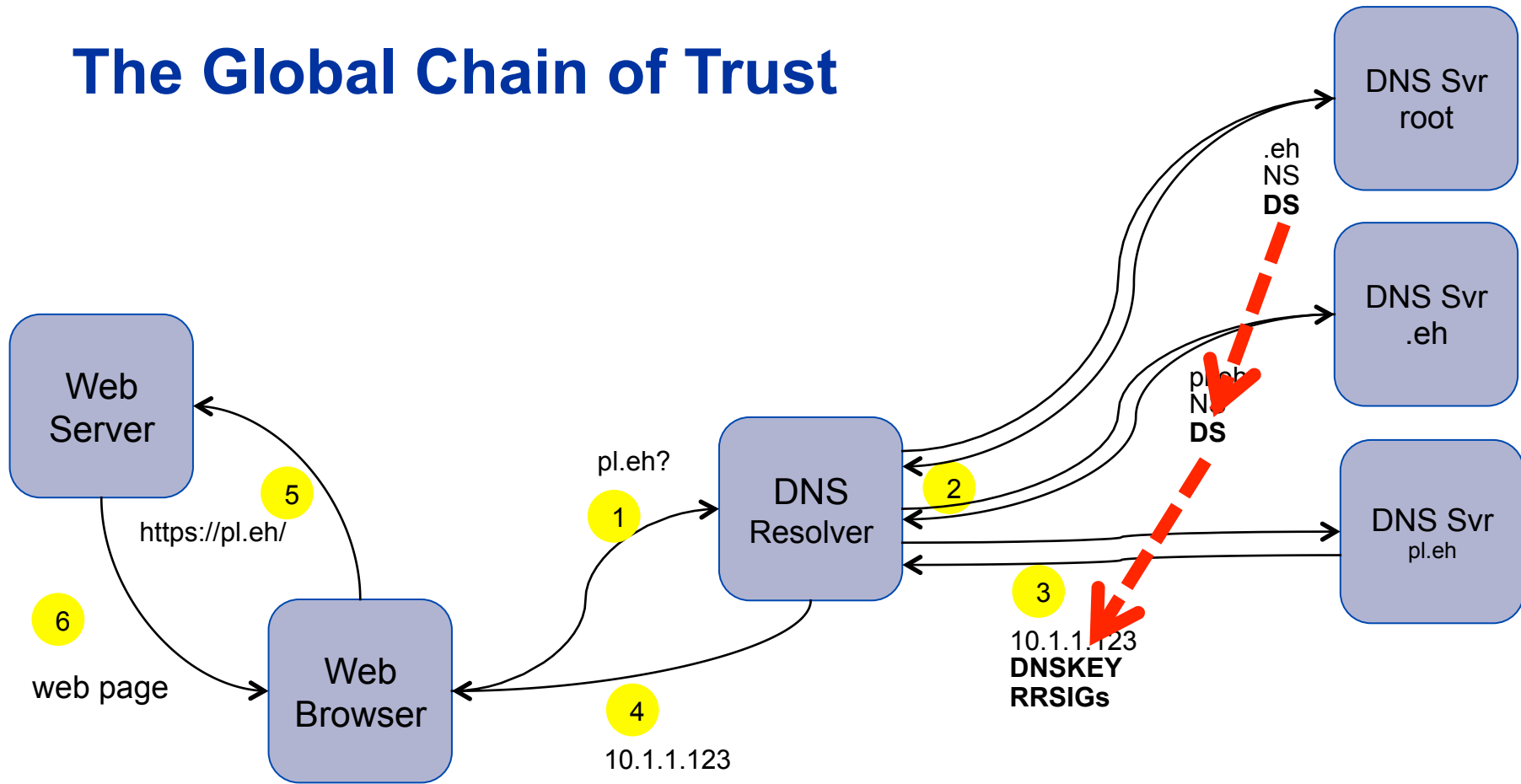
# Delegation Signer (DS) Record

# Fingerprint of DNSKEY sent to registry

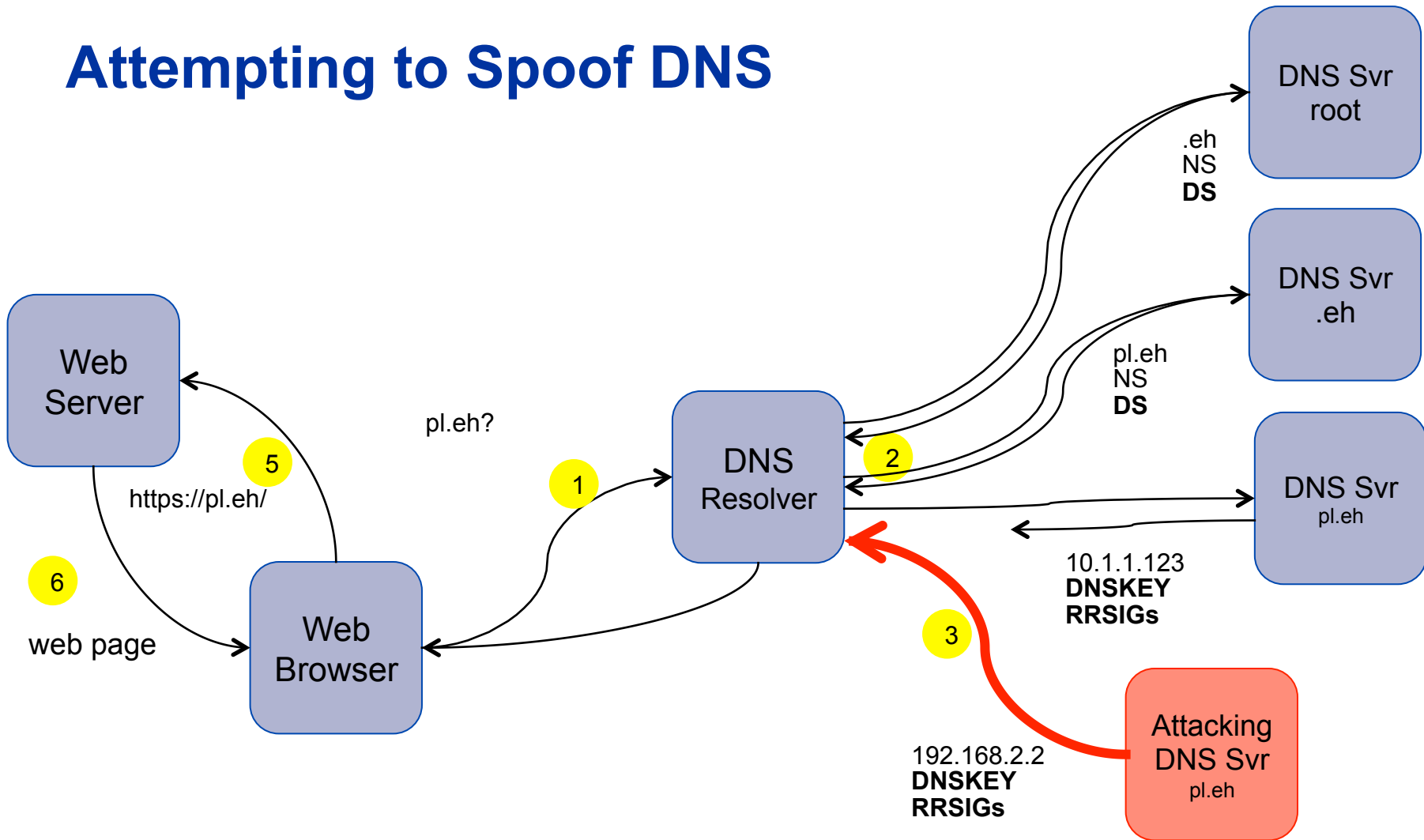
# A DNSSEC Interaction



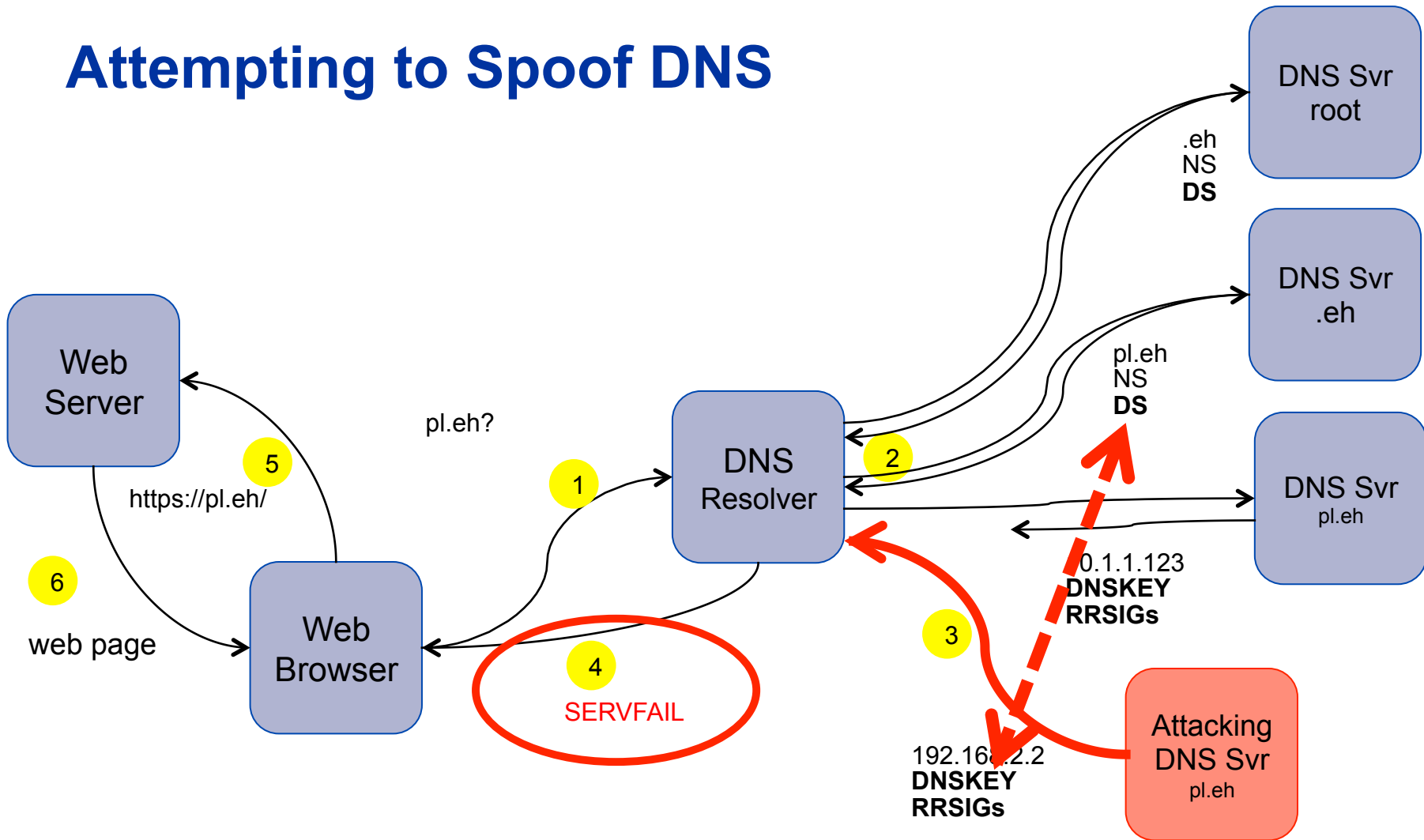
# The Global Chain of Trust



# Attempting to Spoof DNS



# Attempting to Spoof DNS

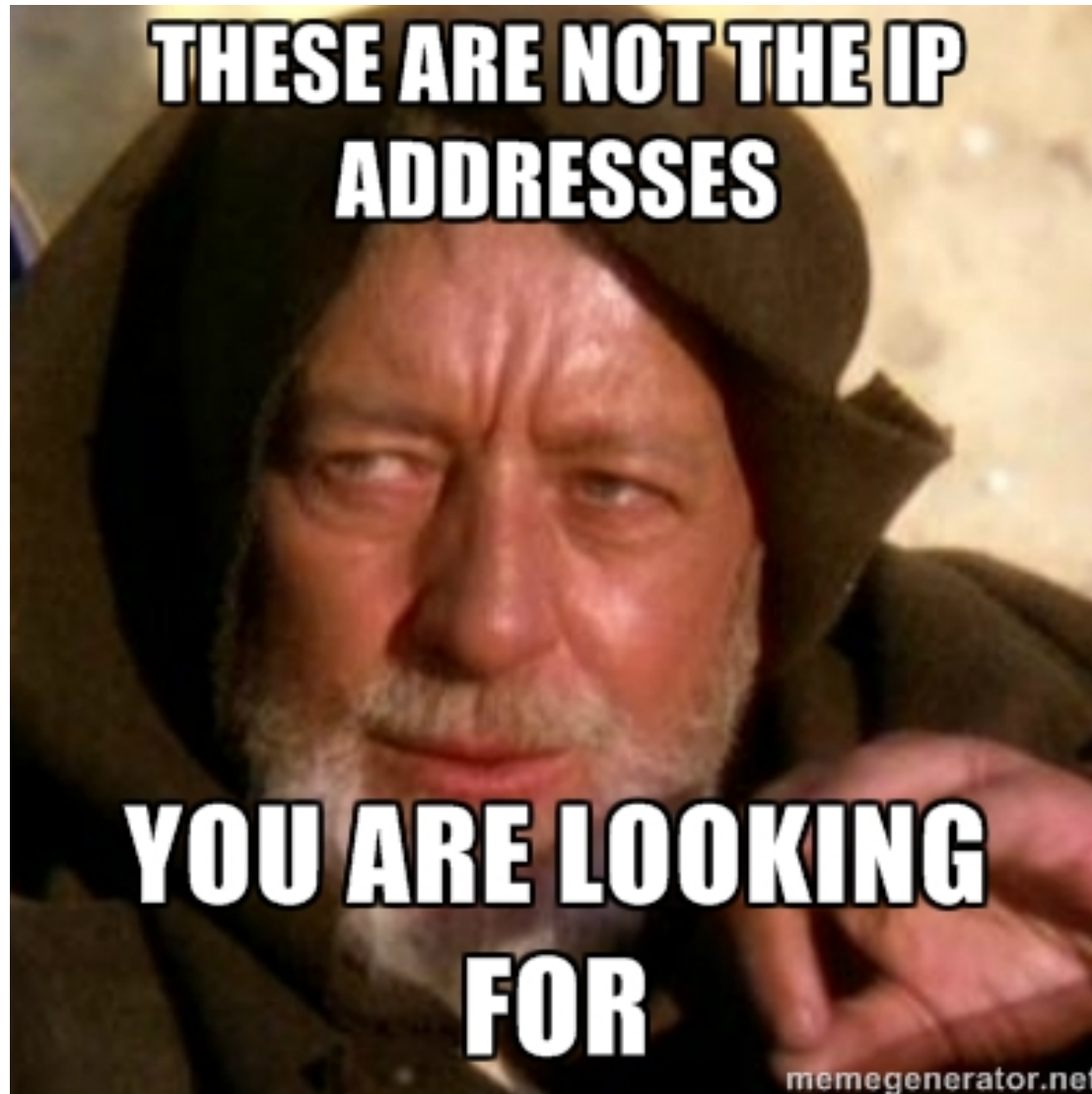


Also addresses leaving  
out DNSSEC



If DS record exists,  
DNSKEY and RRSIGs  
*must* exist

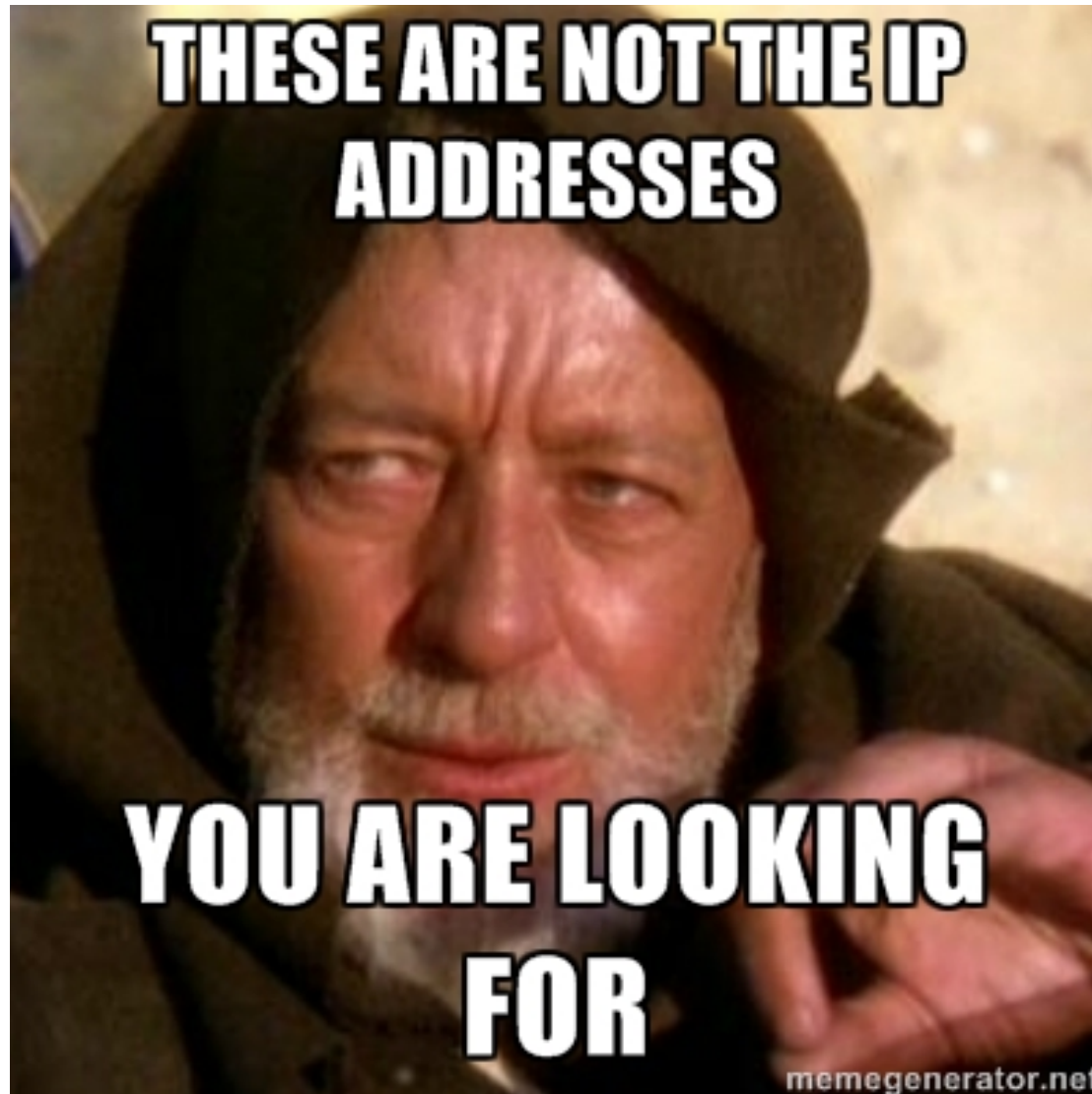
# Global "chain of trust"



# Integrity of DNS answers

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

# NOT about encryption



# But wait...

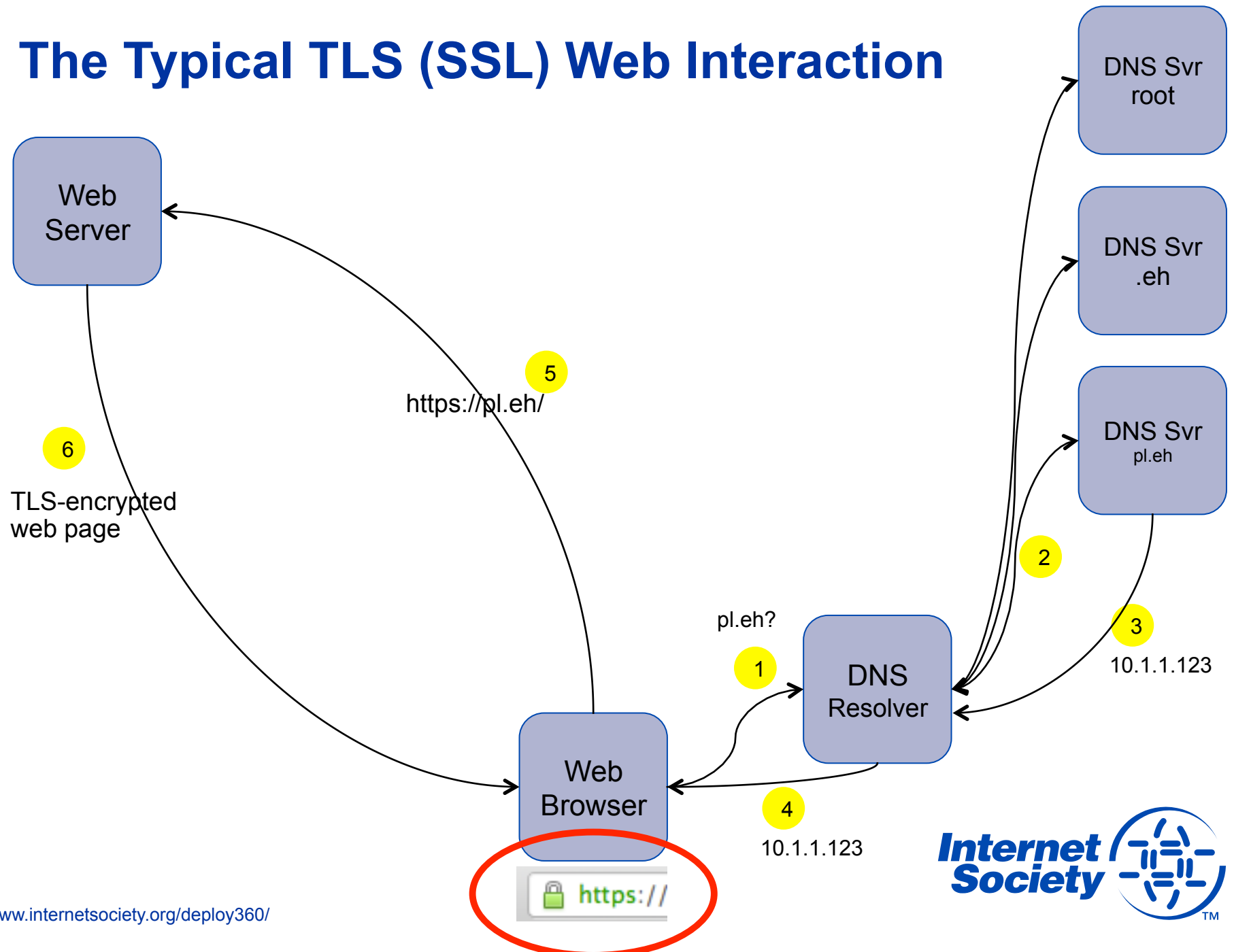


# I've got SSL (TLS)

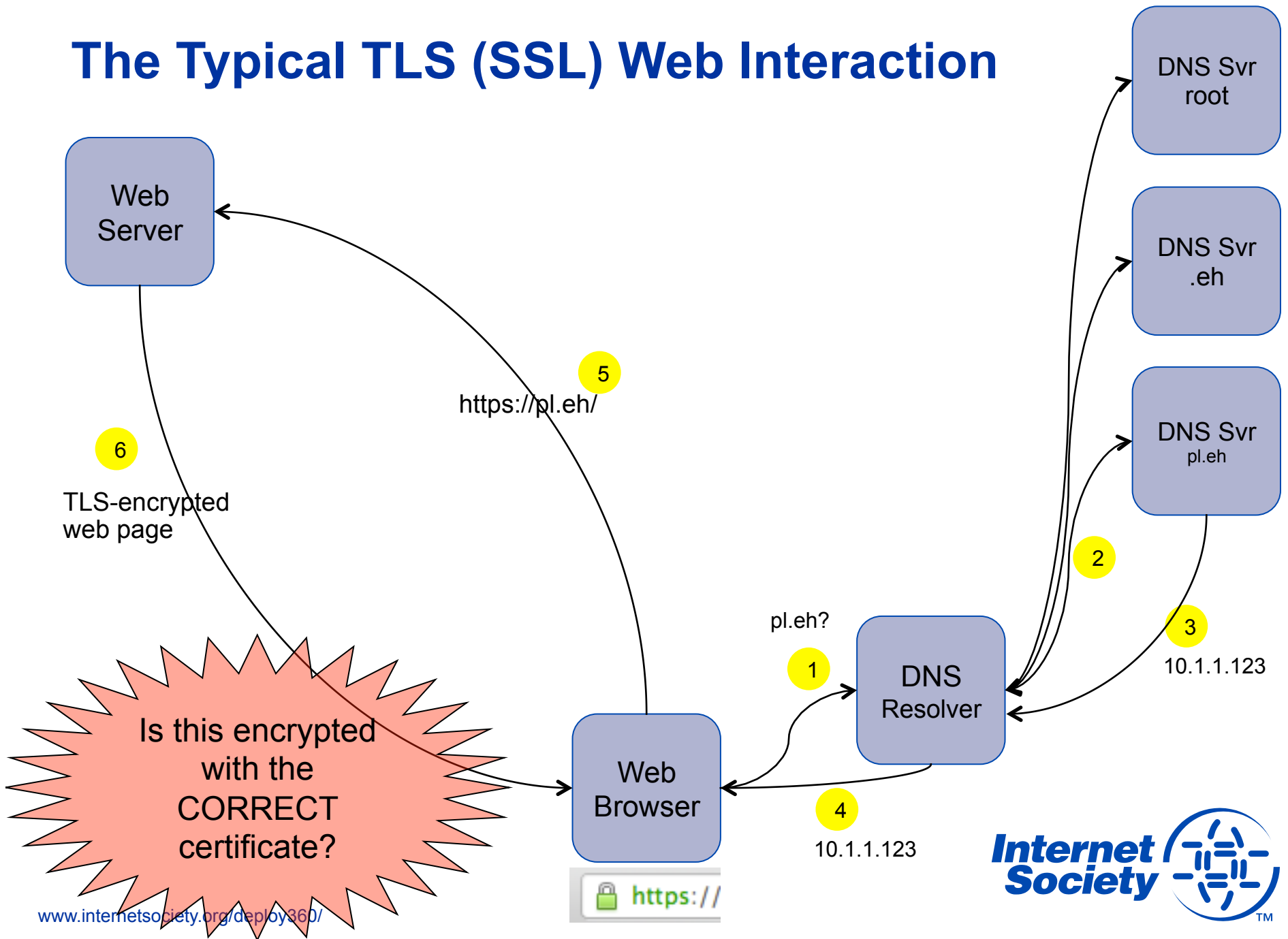
# EV-SSL

# Why do I need DNSSEC?

# The Typical TLS (SSL) Web Interaction



# The Typical TLS (SSL) Web Interaction



TLS = encryption +  
*limited* integrity  
protection

# Certificate Authority (CA)

1,500+ CAs



Any CA can generate  
a certificate for **ANY**  
domain

# compromises

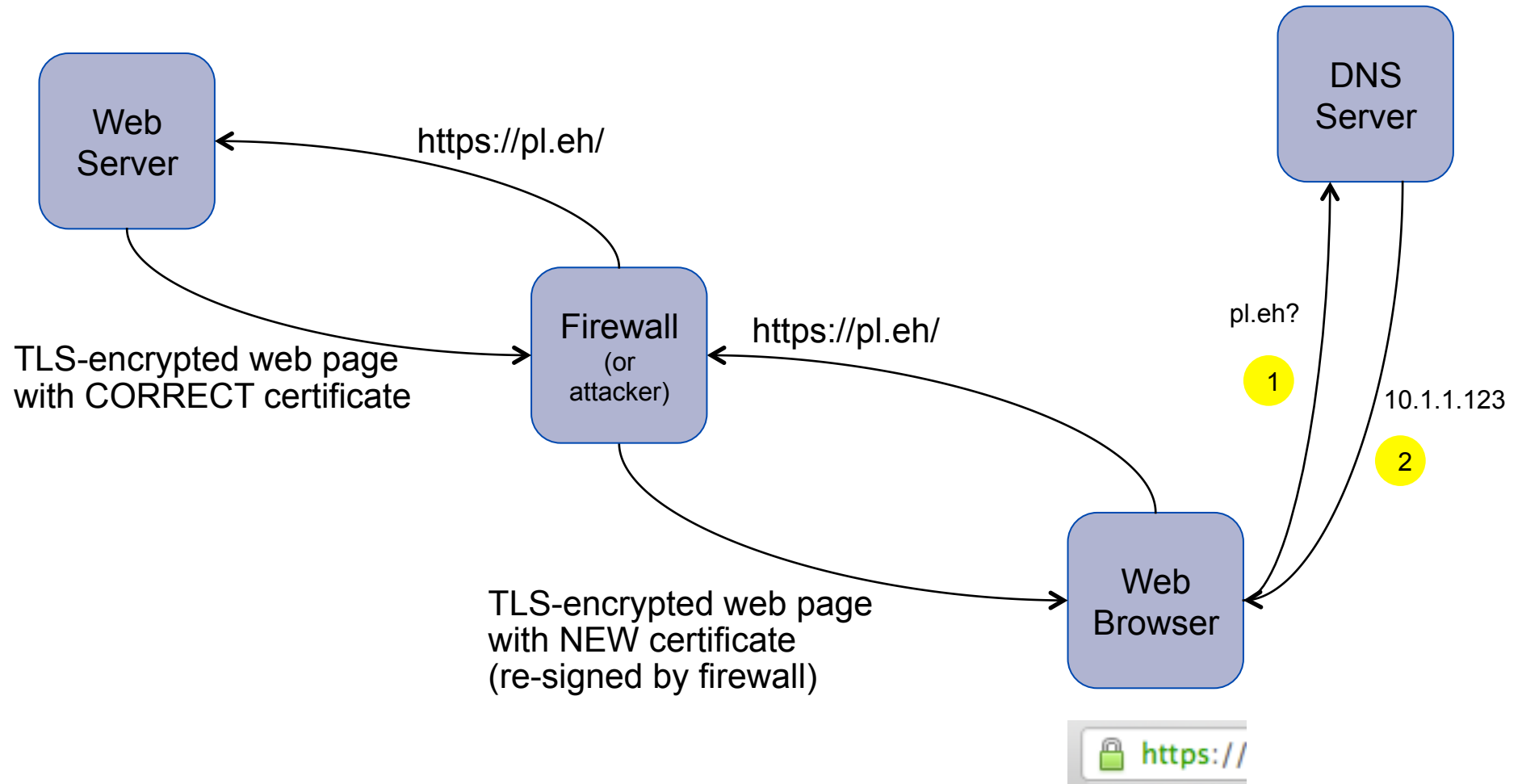
# social engineering

# weak link

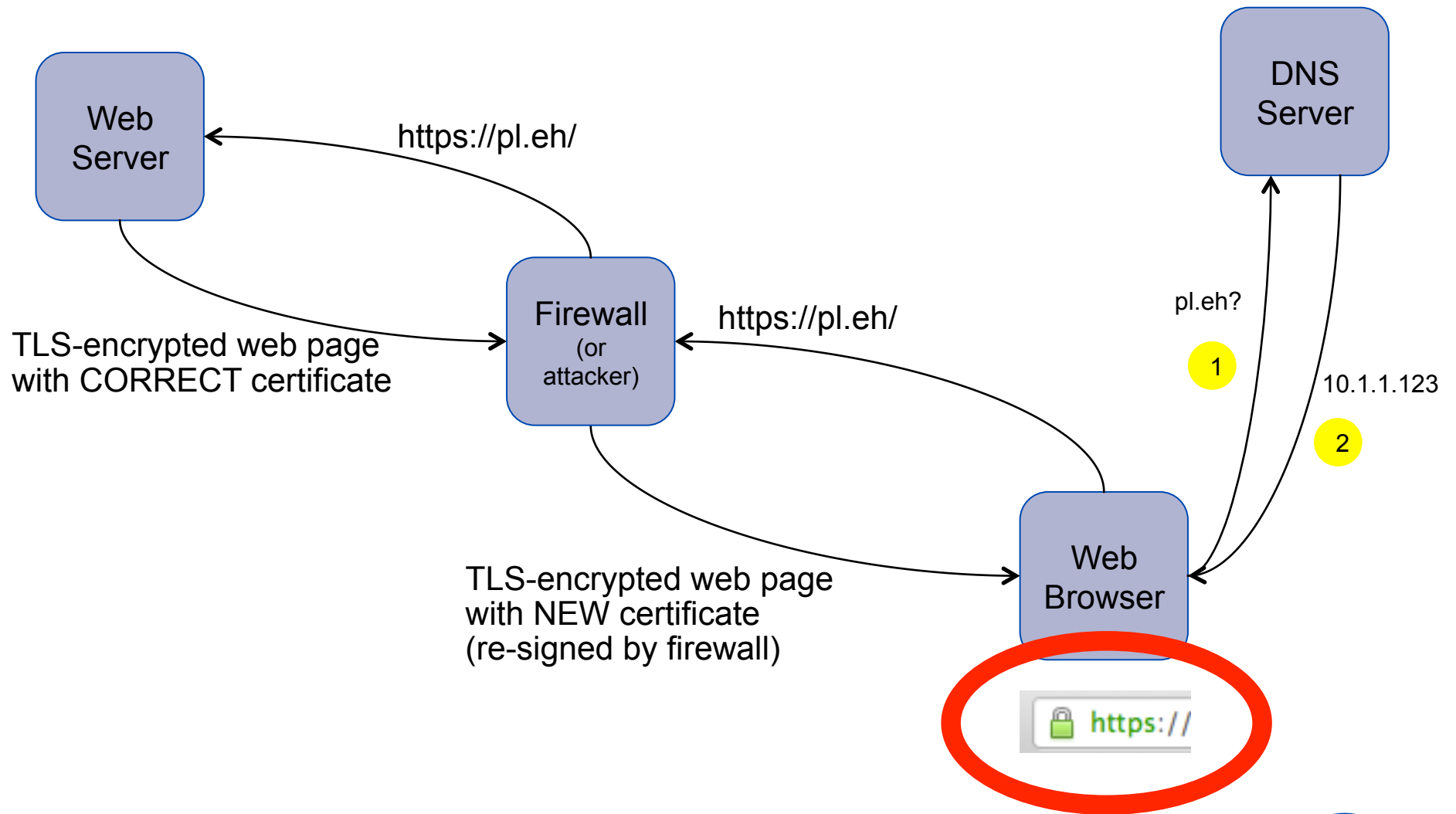
or self-signed cert

# signing cert

# What About This?

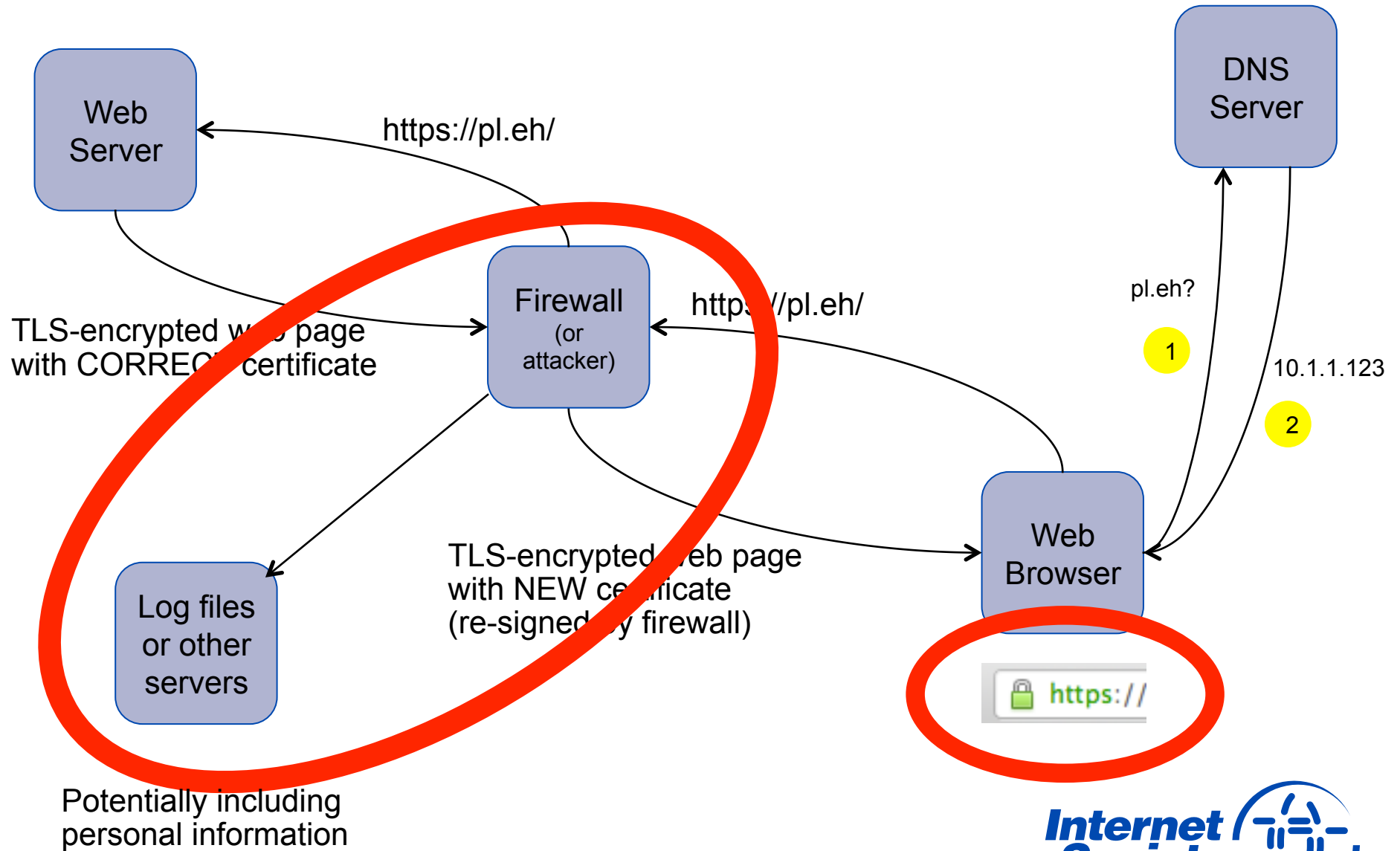


# Oops





# Oops



Hmmm...

TLS = encryption +  
*limited* integrity  
protection

**DNSSEC = strong  
integrity protection**

encryption +  
strong integrity  
protection?

# TLS + DNSSEC ?

**TLS + DNSSEC =**

**DANE**

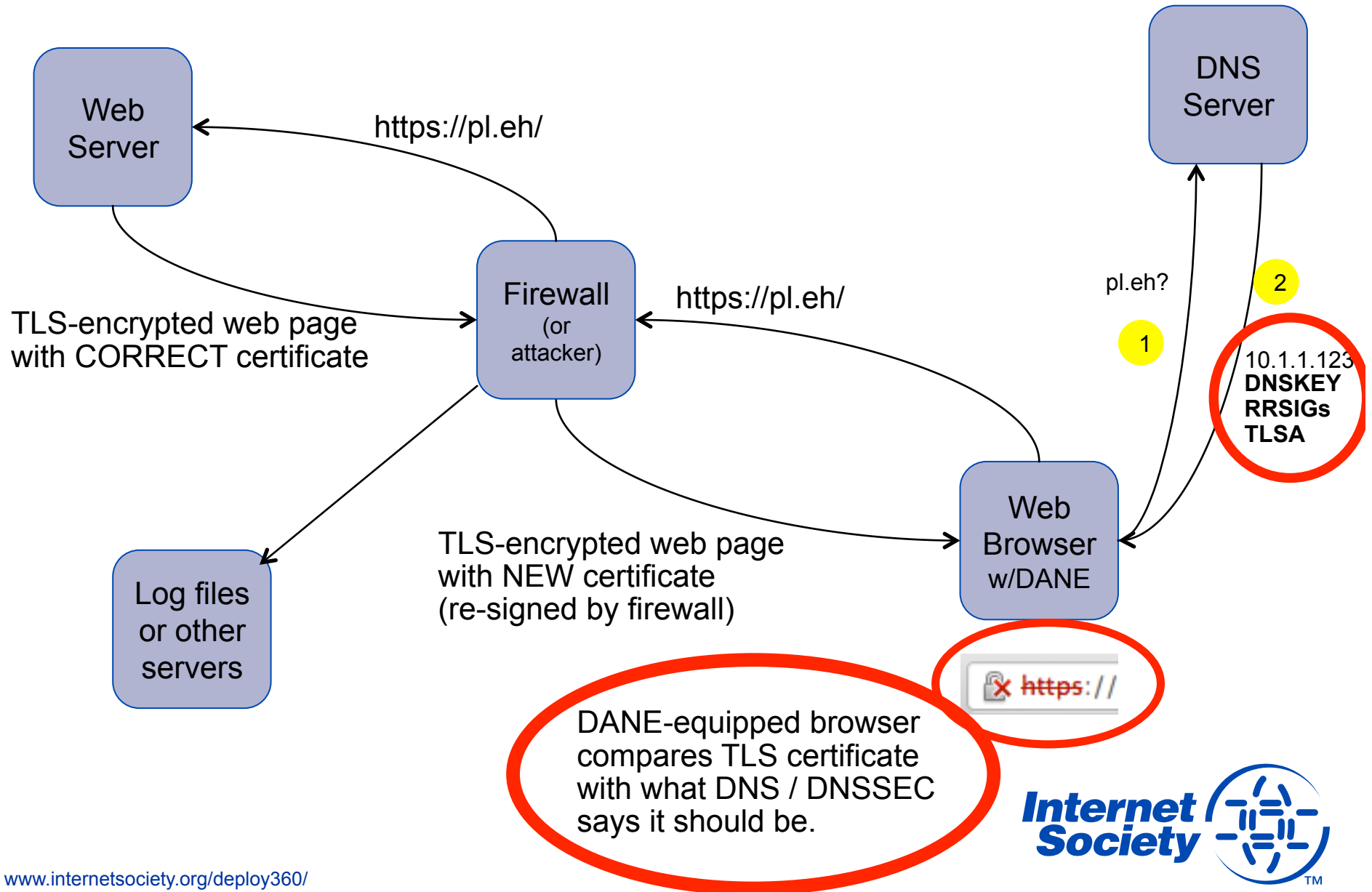
"stuff a TLS cert (or a fingerprint) into DNS"



# new TLSA record

# secured by DNSSEC

# Hurrah!





# RFC 6698

# DANE not just for web

# Email – S/MIME

# VoIP



# Jabber/XMPP

?

*(anything with certs)*

# DANE not just for CA-signed certs

# Also for self-signed certs!

# Beyond DNSSEC and DANE...

Developers are just  
***starting***  
to explore the  
opportunities!

So...

**DNSSEC ensures  
your ccTLD DNS info  
isn't modified**



# DANE upgrades security of Internet services

Together they open  
up a world of  
opportunity

# Sign your ccTLD...

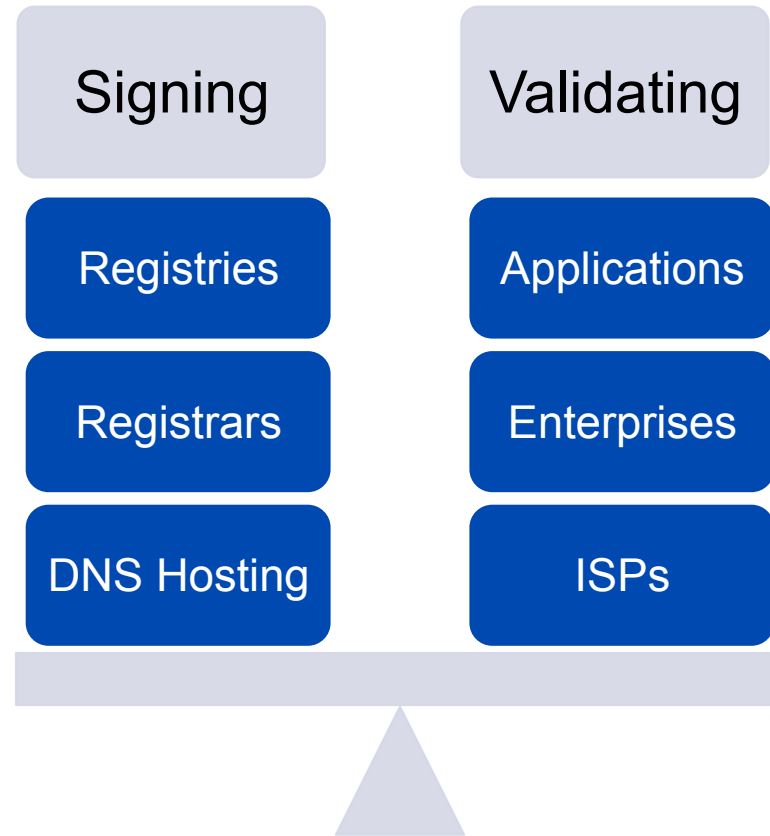
[www.internetsociety.org/deploy360/](http://www.internetsociety.org/deploy360/)



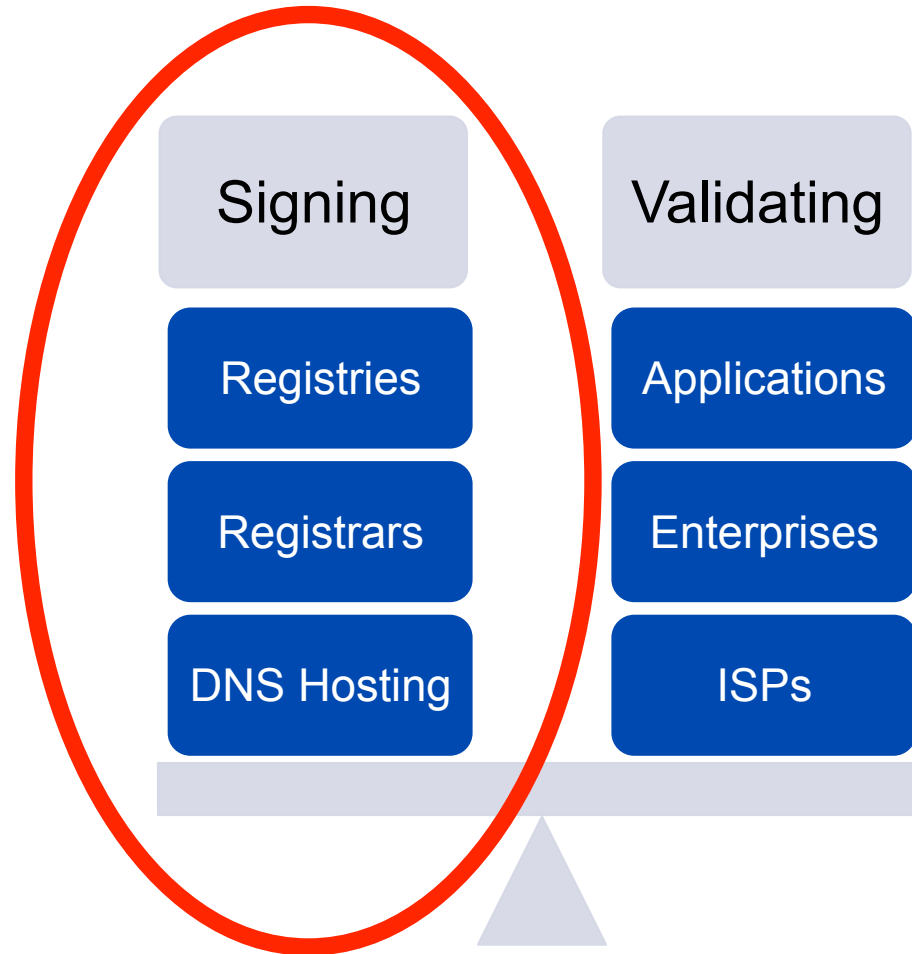
Profit! 😊

# Pretty picture, eh?

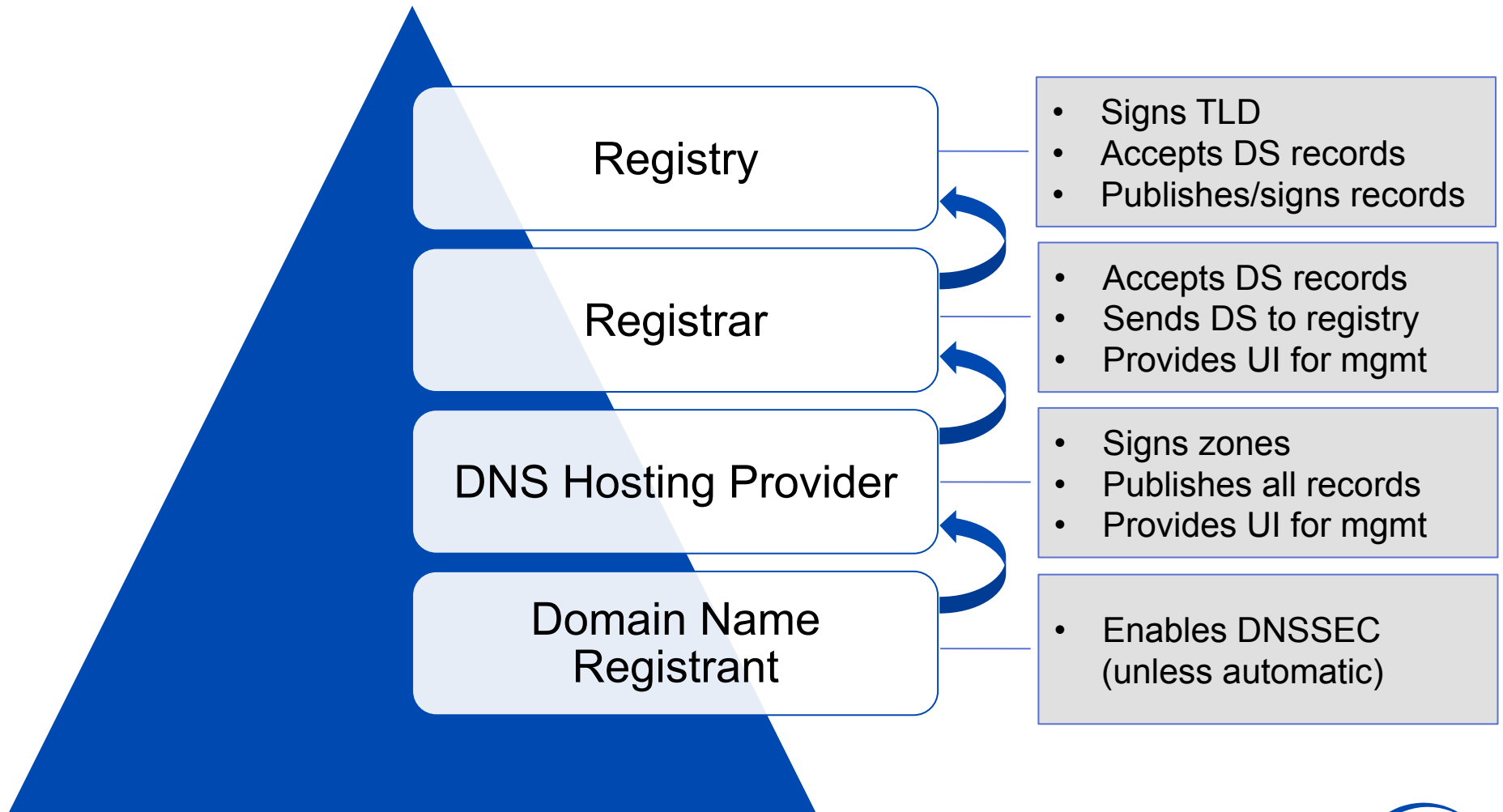
# The Two Parts of DNSSEC



# Today's Focus

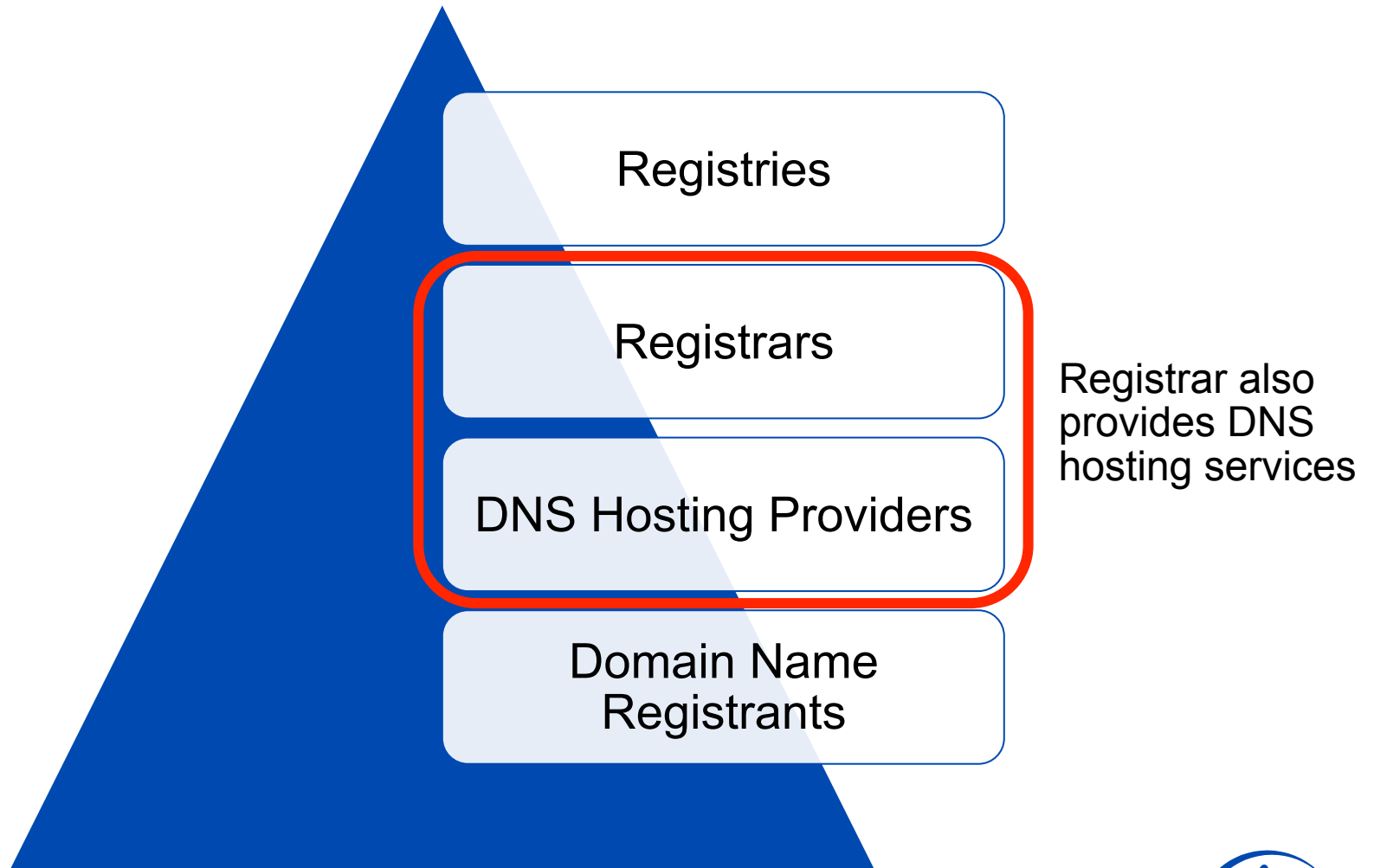


# DNSSEC Signing - The Individual Steps

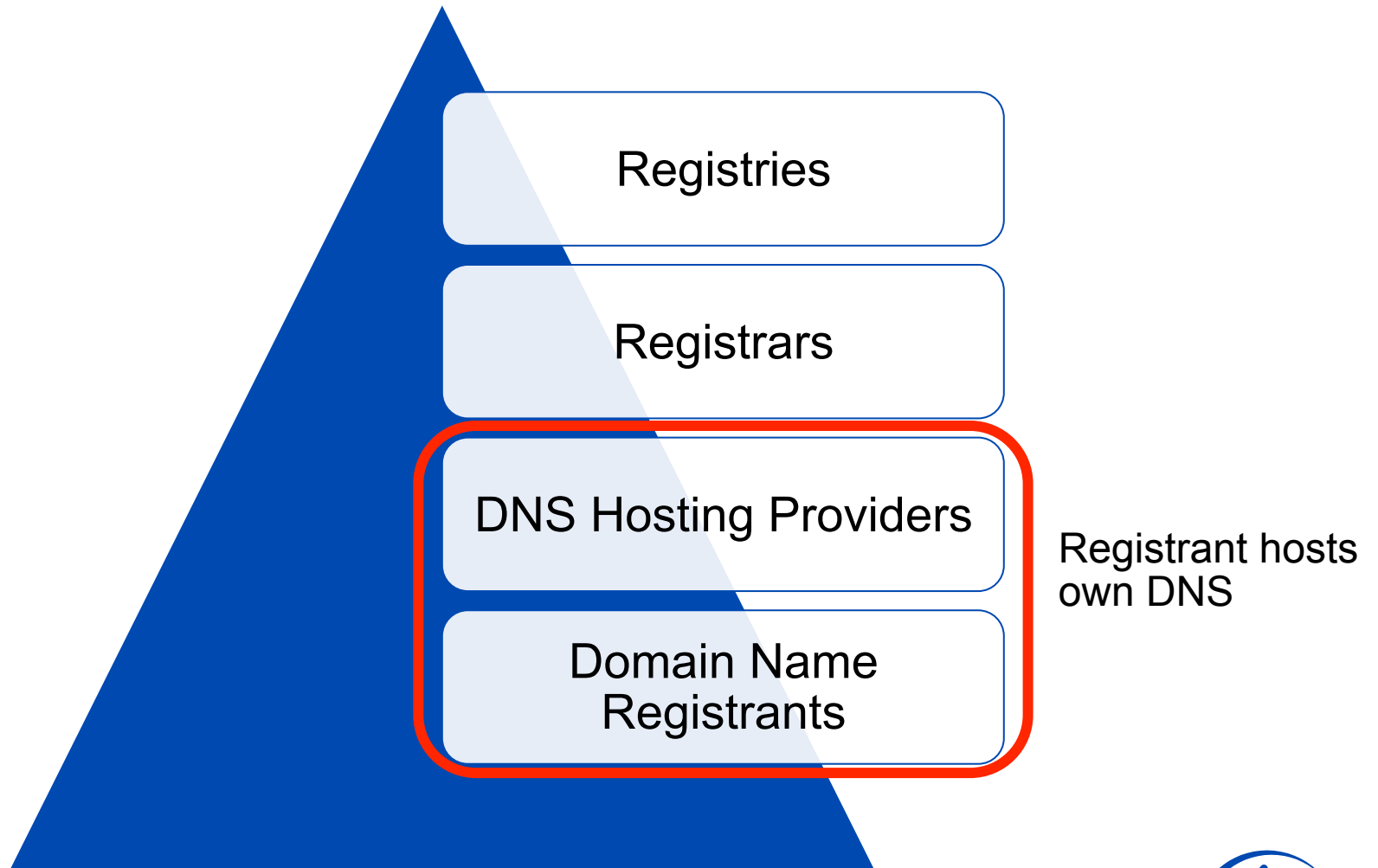




# DNSSEC Signing - The Players



# DNSSEC Signing - The Players



## Three General Points:

1. **Registries** need to make it as simple as possible for registrars to upload Delegation Signer (DS) records
2. **Registrars** need to make it as simple as possible for DNS hosting providers (including domain name registrants who self-host their DNS) to upload DS records
3. **DNS hosting providers** need to make it as simple - and as automated - as possible for domain name registrants to sign domains

# Simplify The Registrar/Hosting Experience

We need to make the DNSSEC-signing process at domain name registrars *easy* for *domain name registrants / holders*.

Examples:

- Binerio in Sweden signs all domains by default
- GoDaddy provides a “one-click” button as part of “Premium DNS” offering
- All keys automatically generated and handled for the domain name holder

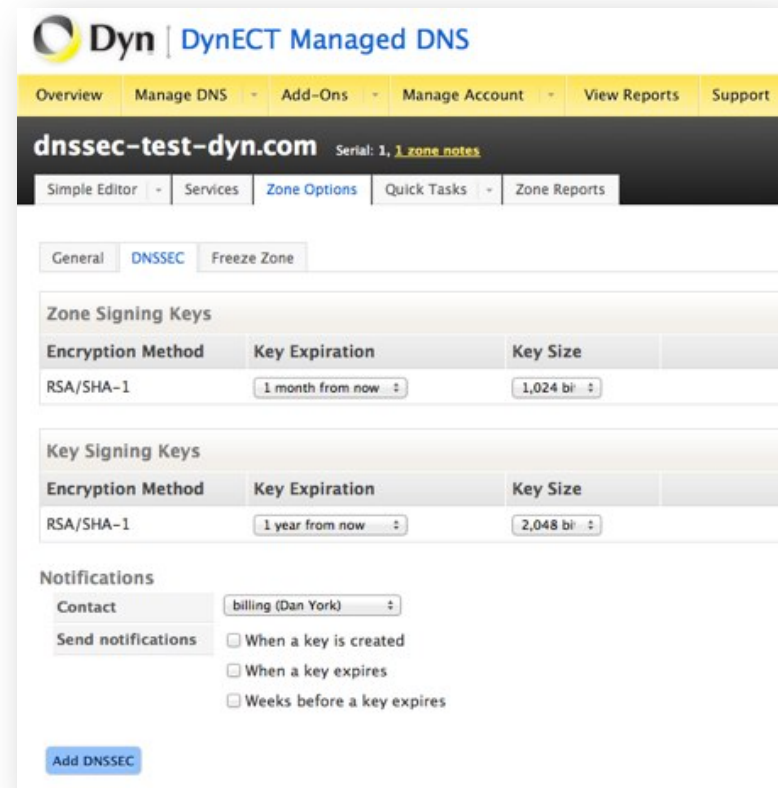
A screenshot of a web interface for DNSSEC settings. At the top, there are three tabs: "Secondary DNS", "DNSSEC", and "Vanity Nameservers". The "DNSSEC" tab is selected. Below the tabs, the heading "DNSSEC Settings" is displayed. Underneath, it says "5 DNSSEC domains available. [Buy more.](#)". There is a section for "Enabled:" with two radio buttons: "On" (which is selected) and "Off". Below that, it says "Domain Status: Unsigned". There is a field for "Email key change notifications to:" containing the text "deploy360@jsoc.org". At the bottom, there are two buttons: "Save" and "Cancel".

# Simplify The DNS Hosting Experience

Another example, Dyn, Inc:

- Provides a simple experience – just click “Add DNSSEC” at the bottom
- Availability of options may be good for technical users but confusing / intimidating for new users

Need this kind of simple interface at more DNS hosting providers



# Simplify/Automate Transfer of DS Records

If DNS is hosted with one provider (including self-hosted), process of getting Delegation Signer (DS) record to registrar is primarily copy / paste between web forms.



The screenshot shows a web form titled "Add Delegation Signer Record" with a dark green background and a yellow header. The form contains the following fields and controls:

- Key Tag:** An empty text input field.
- Algorithm:** A dropdown menu showing "3 - DSA/SHA-1".
- Digest Type:** A dropdown menu showing "1 - SHA-1".
- Digest:** An empty text input field.
- Buttons:** "Add Key" and "Cancel" buttons at the bottom right.

- Ideally needs to be automated to remove this extra step

Some registrars offering API. Example:

- [www.gkg.net/ws/ds.html](http://www.gkg.net/ws/ds.html)

# Registrars / DNS Hosting Providers

## Two technical issues:

- **REGISTRAR TO REGISTRY**
  - Upload of DS records
  - Multiple DS records (to support key rollover)
  - Use of EPP?
- **DNS HOSTING PROVIDER TO REGISTRAR**
  - Upload of DS records
  - No standardized API – mainly propriety APIs or web UI copy/paste

# Increase Number of Domain Name Registrars

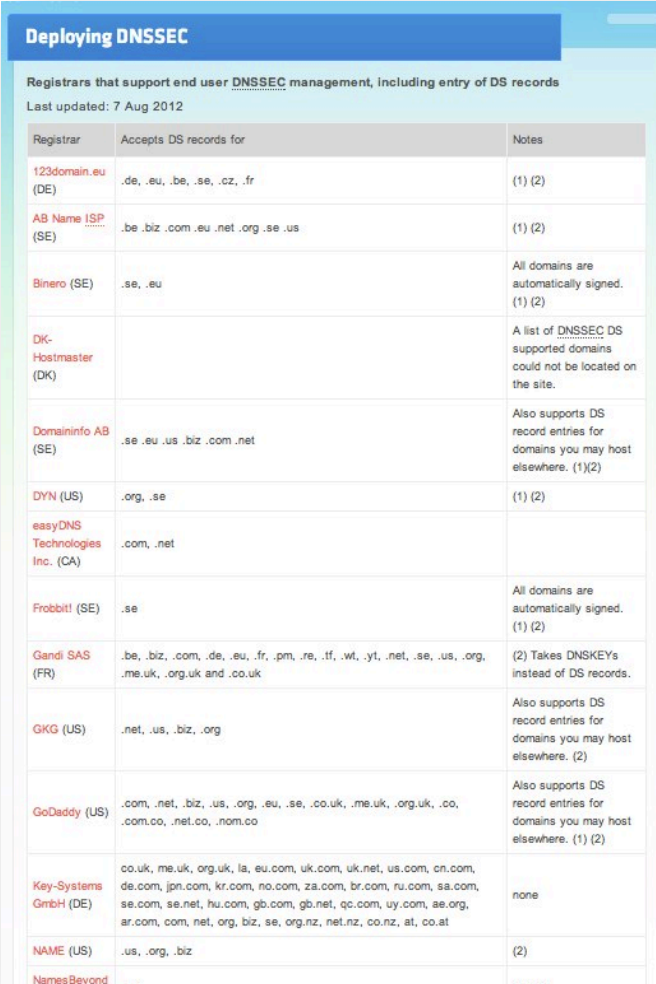
Need to increase number of domain name registrars supporting DNSSEC

- Good news is that the list keeps increasing!

List from ICANN at:

- [www.icann.org/en/news/in-focus/dnssec/deployment](http://www.icann.org/en/news/in-focus/dnssec/deployment)

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



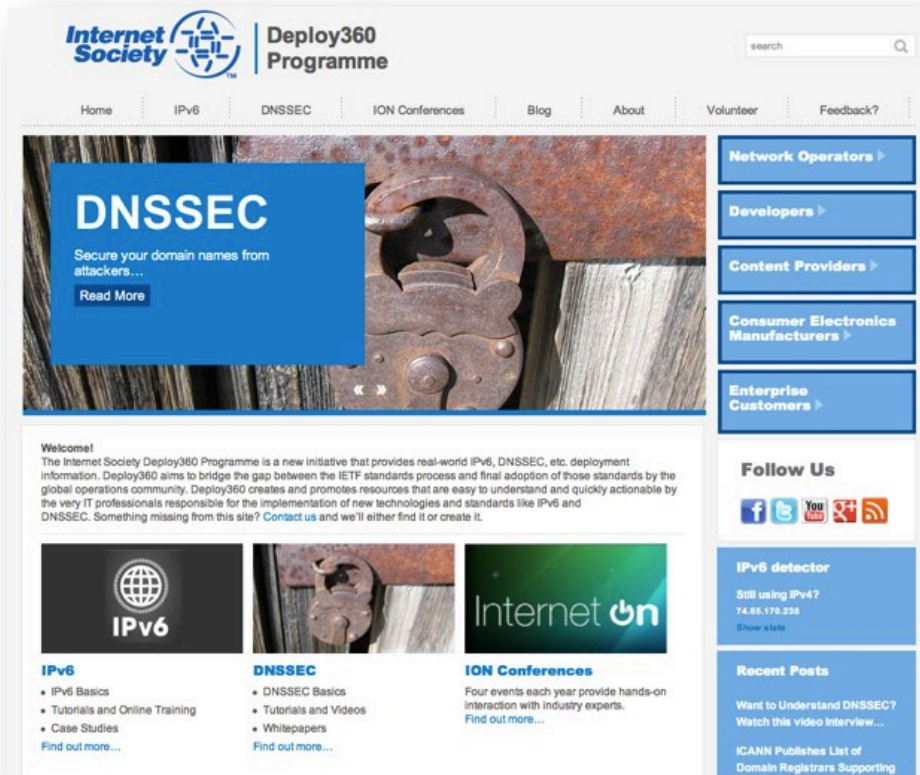
Registrar	Accepts DS records for	Notes
123domain.eu (DE)	.de, .eu, .be, .se, .cz, .fr	(1) (2)
AB Name ISP (SE)	.be, .biz, .com, .eu, .net, .org, .se, .us	(1) (2)
Binero (SE)	.se, .eu	All domains are automatically signed. (1) (2)
DK-Hostmaster (DK)		A list of DNSSEC DS supported domains could not be located 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	
Frobbitt! (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 DNSKEY's 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		(1) (2)

Source: [www.icann.org/en/news/in-focus/dnssec/deployment](http://www.icann.org/en/news/in-focus/dnssec/deployment)



# Next steps...

# Internet Society Deploy360 Programme



[www.internetsociety.org/deploy360/](http://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.

# Three Steps TLD Operators Can Take:

## 1. Sign your TLD!

- Tools and services available to help automate process

## 2. Accept DS records

- Make it as easy as possible (and accept multiple records)

## 3. Work with your registrars

- Help them make it easy for DNS hosting providers and registrants

## 4. Help With Statistics

- Can you help by providing statistics?

**Implement DNSSEC and make your TLD more secure!**

**Dan York, CISSP**

Senior Content Strategist, Internet Society

york@isoc.org

[www.internetsociety.org/deploy360/](http://www.internetsociety.org/deploy360/)

# Thank You!

Want more info?  
Attend the "DNSSEC Deployment Workshop" tomorrow or  
watch the archived recording later.

# Additional Material

# Review Our DNSSEC Content Roadmap

We have posted a roadmap of the content we believe we need to add to Deploy360 site related to DNSSEC (and IPv6):

**[www.internetsociety.org/deploy360/roadmap/](http://www.internetsociety.org/deploy360/roadmap/)**

We would greatly appreciate feedback:

- Anything missing? Are there additional topics we should consider?
- Will this content help you deploy DNSSEC?
- Please send comments to **[deploy360@isoc.org](mailto:deploy360@isoc.org)**

# Download A DNSSEC Whitepaper

“Challenges and Opportunities in Deploying DNSSEC”

**<http://bit.ly/isoc-satin2012>**

## Other Areas (Beyond Those Mentioned Earlier)

- Tools exist to help automate key signing (ex. OpenDNSSEC)
- The “key rollover” process needs to be well-documented (ex. NASA/Comcast issue)
- Guidance can be found in “DNSSEC Policy & Practice Statements” (often abbreviated “DPS”)
  - <http://www.internetsociety.org/deploy360/resources/dnssec-practice-statements/>



# 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>

# How Do We Get DANE Deployed?

## Developers:

- Add DANE support into applications (see list of libraries)

## DNS Hosting Providers:

- Provide a way that customers can enter a “TLSA” record into DNS as defined in RFC 6698 ( <http://tools.ietf.org/html/rfc6698> )
- This will start getting TLS certificates into DNS so that when browsers support DANE they will be able to do so.
- [More tools are needed to help create TLSA records – ex. hashslinger ]

## Network Operators / Enterprises / Governments:

- Start talking about need for DANE
- Express desire for DANE to app vendors (especially browsers)