

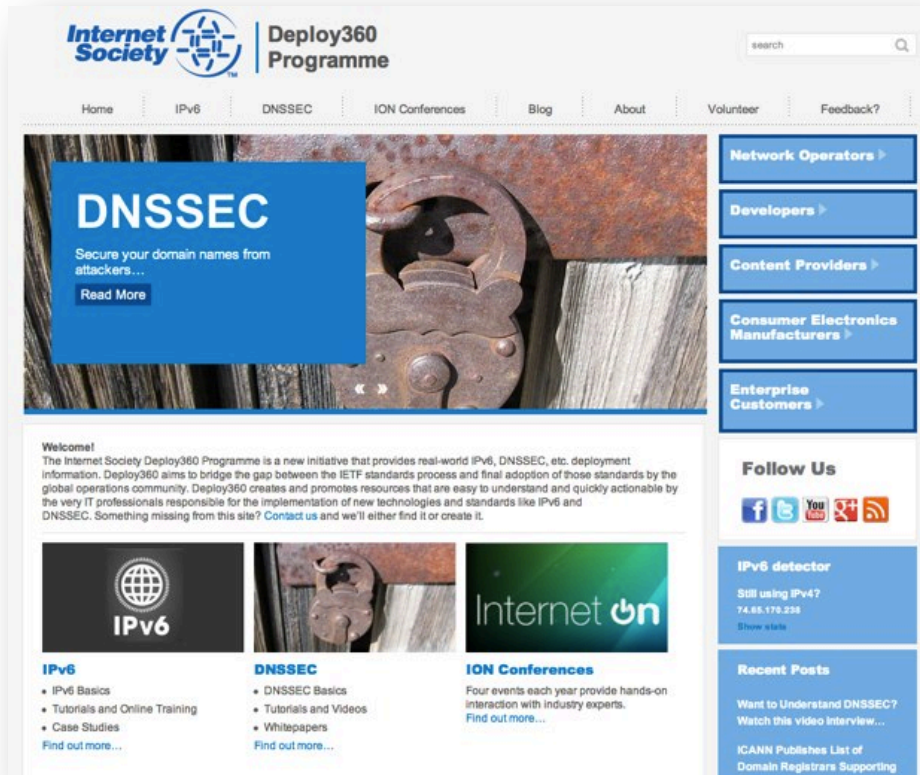
# Key Steps In Accelerating DNSSEC Deployment

Dan York, CISSP

Senior Content Strategist, Internet Society

5th international conference for ccTLD registries and registrars of CIS,  
Central and Eastern Europe  
Budva, Montenegro  
September 12 , 2012

# Internet Society Deploy360 Programme



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

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

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

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

# 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?

# Goals for DNSSEC

## 1. Registrar / DNS hosting provider engagement

- encouraging more registrars to provide DNSSEC and making it easier for domain name holders.

## 2. Validating name servers

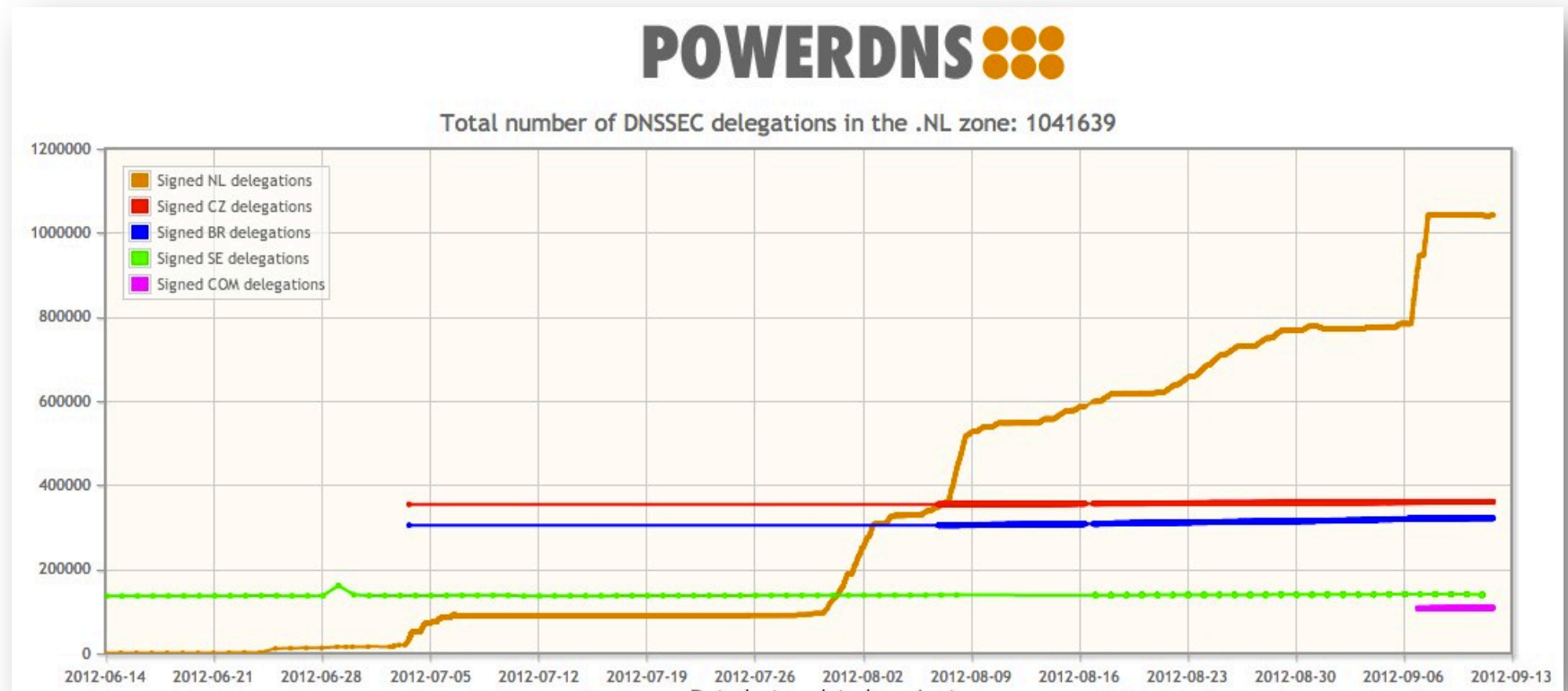
- expanding the deployment of DNSSEC-validating name servers at multiple levels, including ISPs, operating systems and applications.

## 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.

# Registries / Registrars / DNS Hosting Providers

# Case Study – The Growth of .NL



<https://xs.powerdns.com/dnssec-nl-graph/>

# Case Study – The Growth of .NL

- **.NL registry (SIDN) offered discount for signed domains – 2-year discount for each signed domain**
  - Large bulk registrars took advantage of incentive
- **Established <http://dnssec.nl/> website**
- **SIDN provided webinars on DNSSEC to registrars**
- **PowerDNS team provided free technical support (with support from SIDN) to registrars and DNS hosting providers**
- **Strong communication between registry, registrars and DNS hosting providers**
- **Next, SIDN looking to focus on ISPs and validation.**

## 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 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

# Registrars vs DNS Hosting Providers

In documentation and web sites, we need to help average domain name registrant understand difference between:

- Registrar
- DNS Hosting Provider (including hosting DNS yourself)

Many domain name holders do not understand and therefore find process confusing.

**Registrar  
versus  
DNS Hosting  
Provider**

# 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

# DEMO TIME

# Simplify The Registrar Experience

To get more domain names signed with DNSSEC, we need to make the DNSSEC-signing process at domain name registrars *easy for domain name holders*. Examples:

- Binero 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

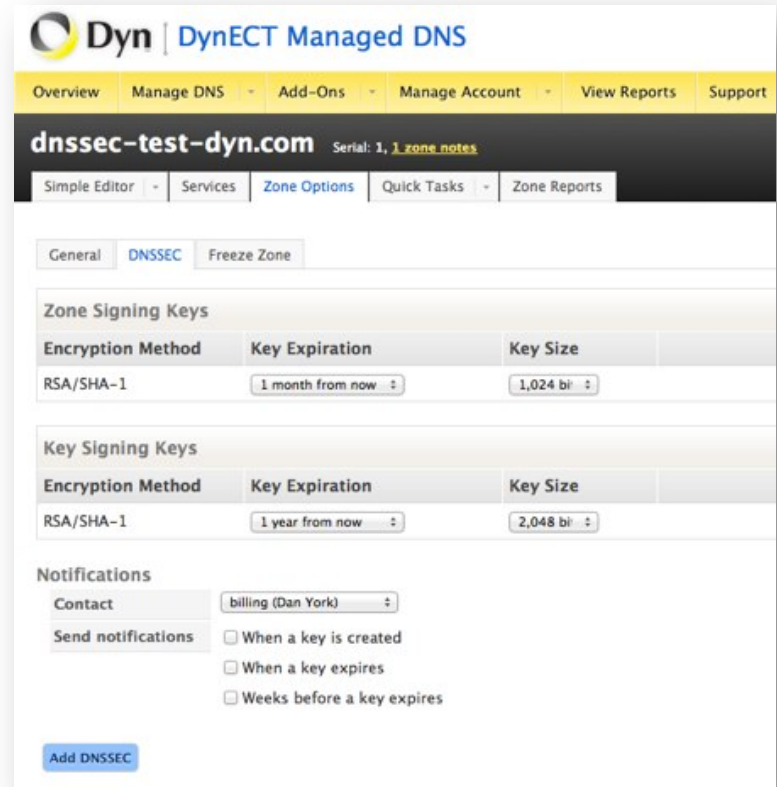
A screenshot of a web interface for DNSSEC settings. At the top, there are three tabs: "Secondary DNS", "DNSSEC" (which is selected), and "Vanity Nameservers". Below the tabs, the title "DNSSEC Settings" is displayed. The main content area shows "5 DNSSEC domains available. [Buy more.](#)". Under the heading "Enabled:", there are two radio buttons: "On" (which is selected) and "Off". Below this, it says "Domain Status: Unsigned". Further down, there is a label "Email key change notifications to:" followed by a text input field containing the email address "deploy360@isoc.org". At the bottom of the form, there are two buttons: a black "Save" button and a blue "Cancel" link.

# Simplify The Registrar 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 registrars



The screenshot shows the DynECT Managed DNS interface for the domain **dnssec-test-dyn.com**. The interface has a yellow navigation bar with links: Overview, Manage DNS, Add-Ons, Manage Account, View Reports, and Support. Below the navigation bar, there's a dark header with the domain name and a "Serial: 1, 1 zone notes" link. A secondary navigation bar includes "Simple Editor", "Services", "Zone Options", "Quick Tasks", and "Zone Reports".

The main content area has three tabs: "General", "DNSSEC" (selected), and "Freeze Zone". Under the "DNSSEC" tab, there are two sections:

- Zone Signing Keys**: A table with columns "Encryption Method", "Key Expiration", and "Key Size". It shows "RSA/SHA-1", "1 month from now", and "1,024 bi".
- Key Signing Keys**: A table with columns "Encryption Method", "Key Expiration", and "Key Size". It shows "RSA/SHA-1", "1 year from now", and "2,048 bi".

Below these is a "Notifications" section with a "Contact" dropdown set to "billing (Dan York)" and a "Send notifications" section with three checkboxes: "When a key is created", "When a key expires", and "Weeks before a key expires". At the bottom left, there is a blue "Add DNSSEC" button.

# 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.

A screenshot of a web form titled "Add Delegation Signer Record". The form has a yellow header bar with the title. Below the header, there are four input fields: "Key Tag:" with a text box, "Algorithm:" with a dropdown menu showing "3 - DSA/SHA-1", "Digest Type:" with a dropdown menu showing "1 - SHA-1", and "Digest:" with a text box. At the bottom right of the form are two buttons: "Add Key" and "Cancel".

- 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)

*Note: If you are not aware, a DS record ties the DNSSEC-signed DNS zone into the global "chain of trust".*

# 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.



**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	
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 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, on.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)

## 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/>

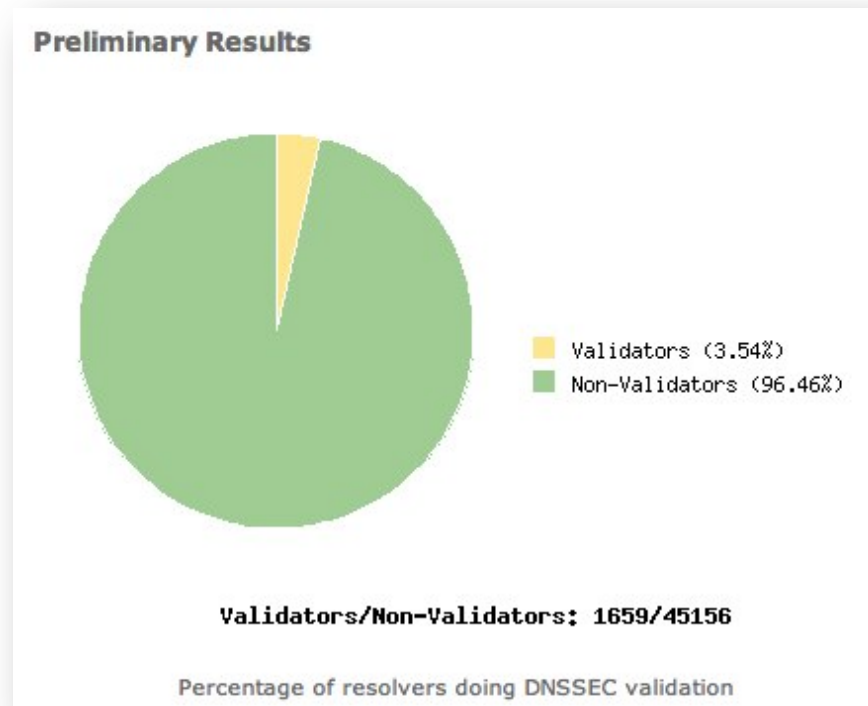
## Three General Points:

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 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

# Validating Name Servers

# Validating Name Servers

- How do we increase the percentage?



<http://validatorsearch.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

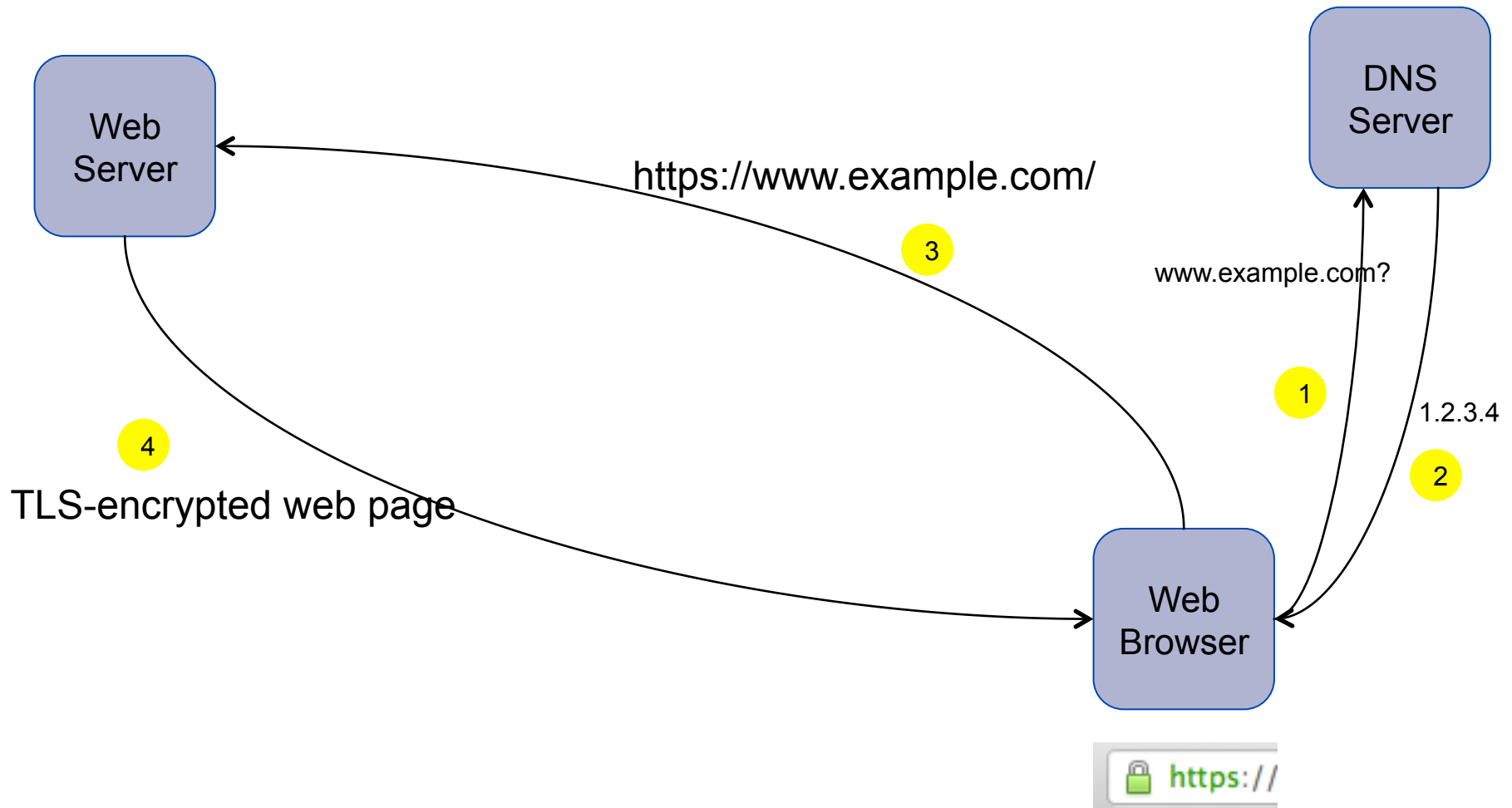


# Enterprises / Domain Name Holders

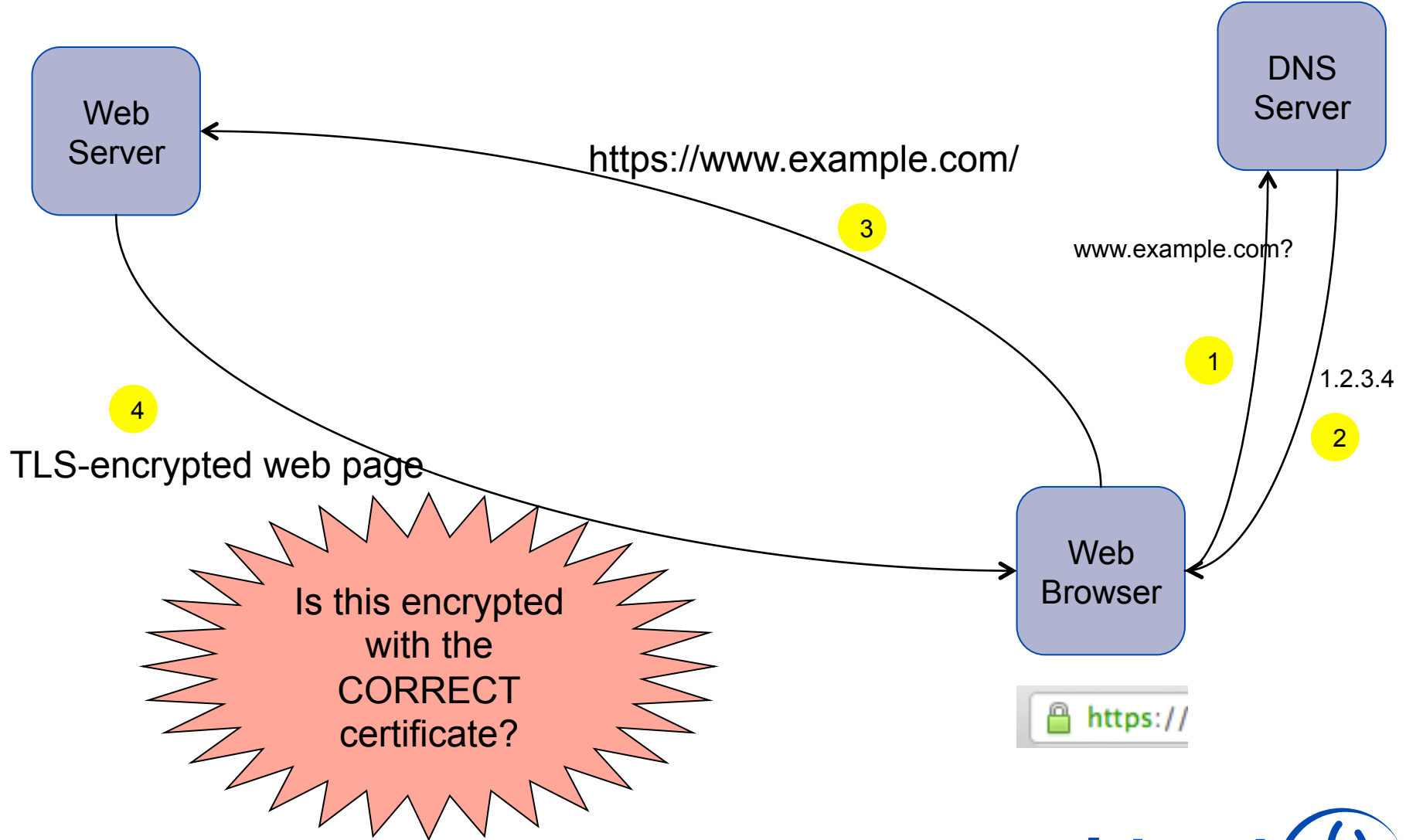
# Key Steps for Enterprises / Domain Name Holders

- Simplification of registrar / DNS hosting experience
- Education about basics of DNSSEC and the value
- More articles in mainstream IT media, more presentations at IT conferences
- DANE...

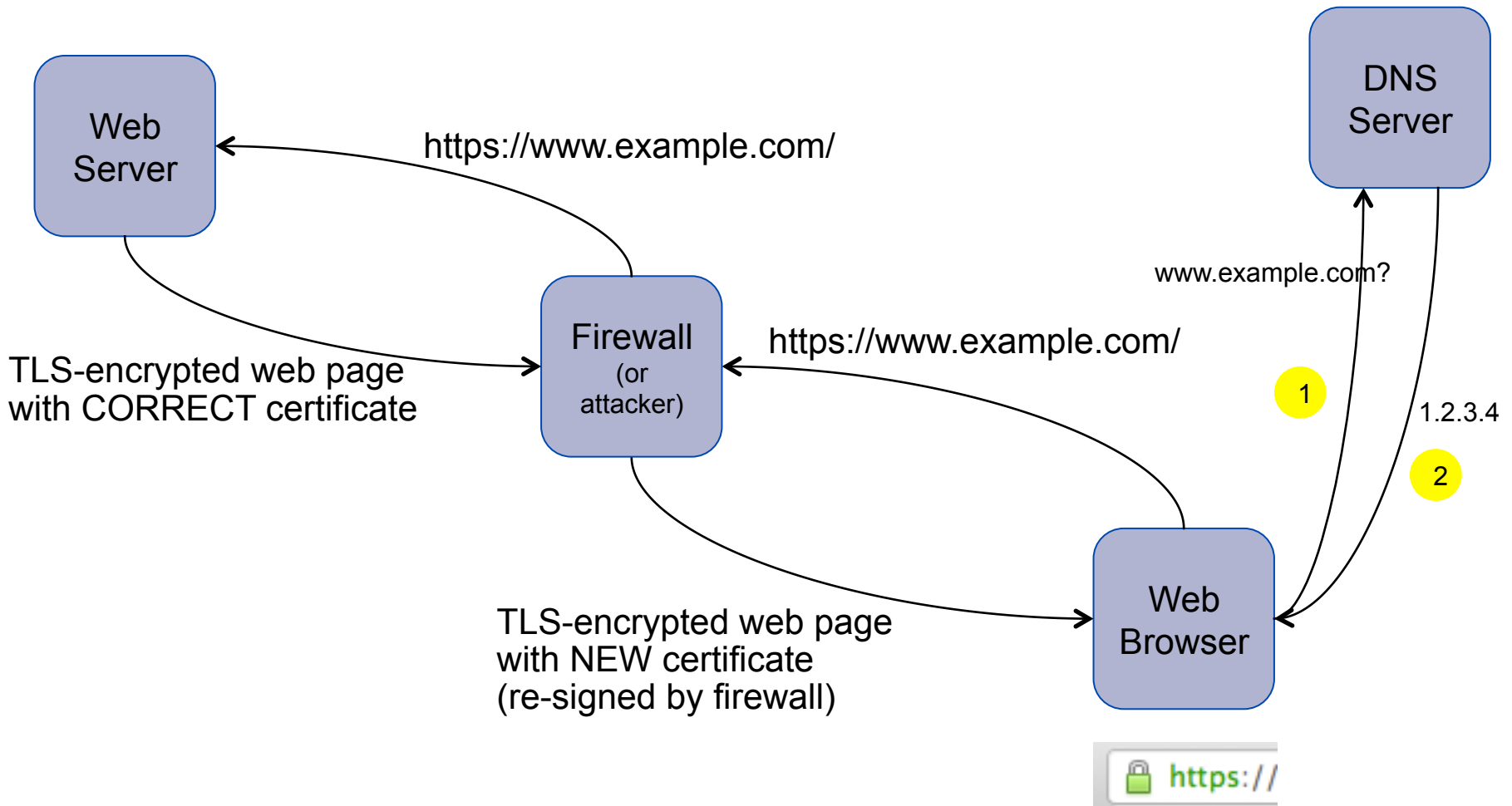
# The Typical TLS (SSL) Web Interaction



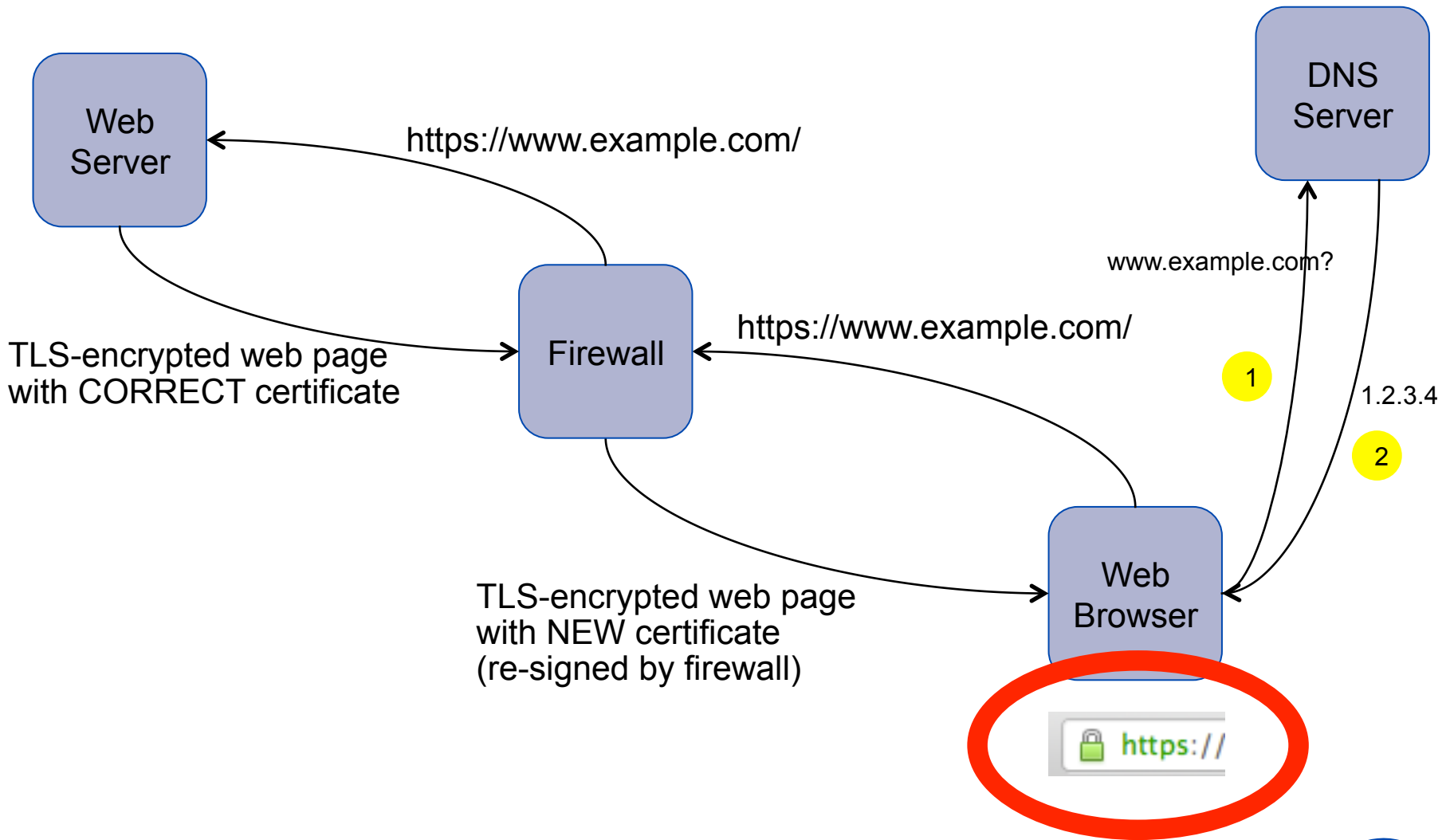
# The Typical TLS (SSL) Web Interaction



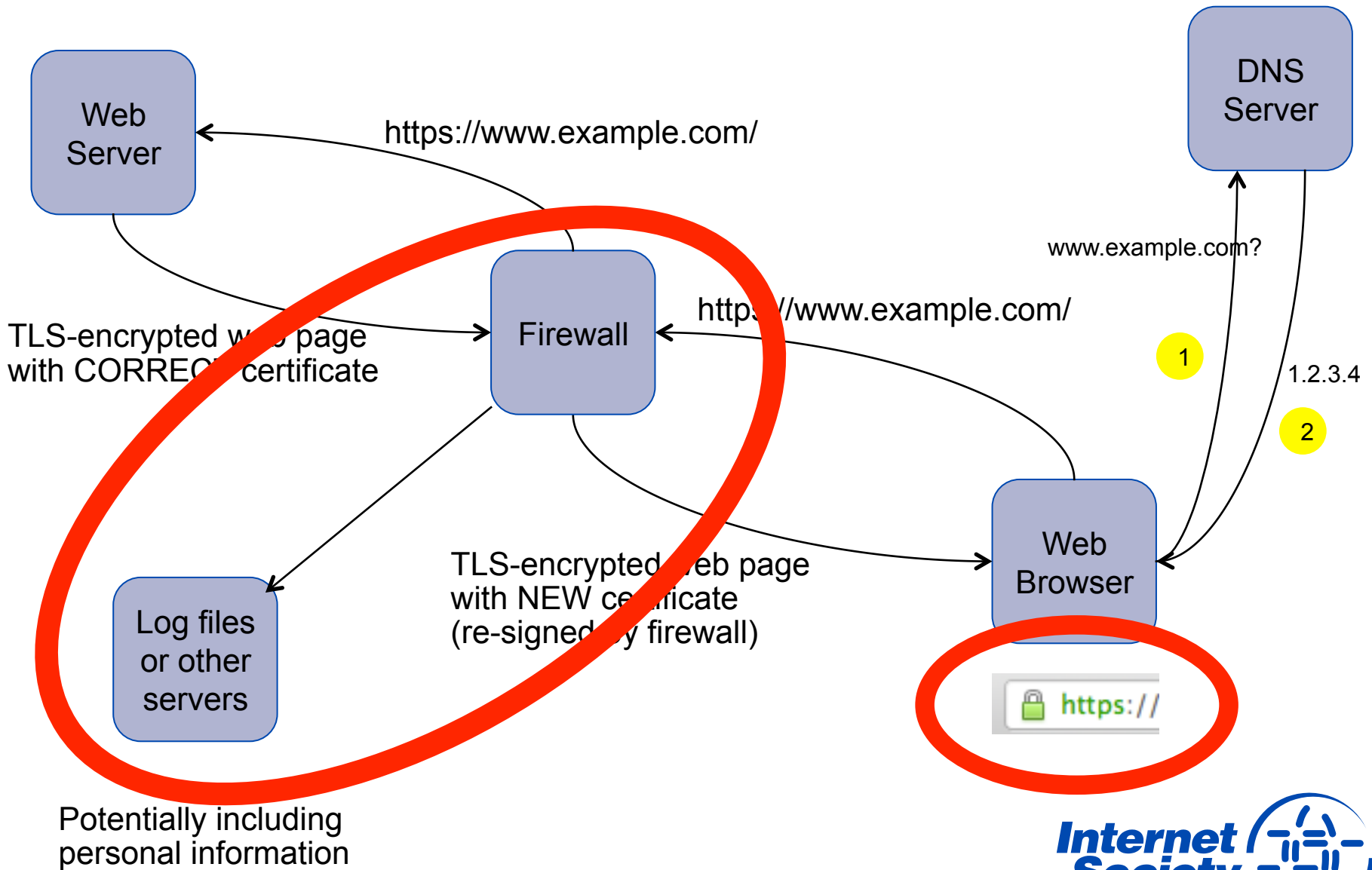
# What About This?



# Problems?



# Problems?



# 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.

# DNS-Based Authentication of Named Entities (DANE)

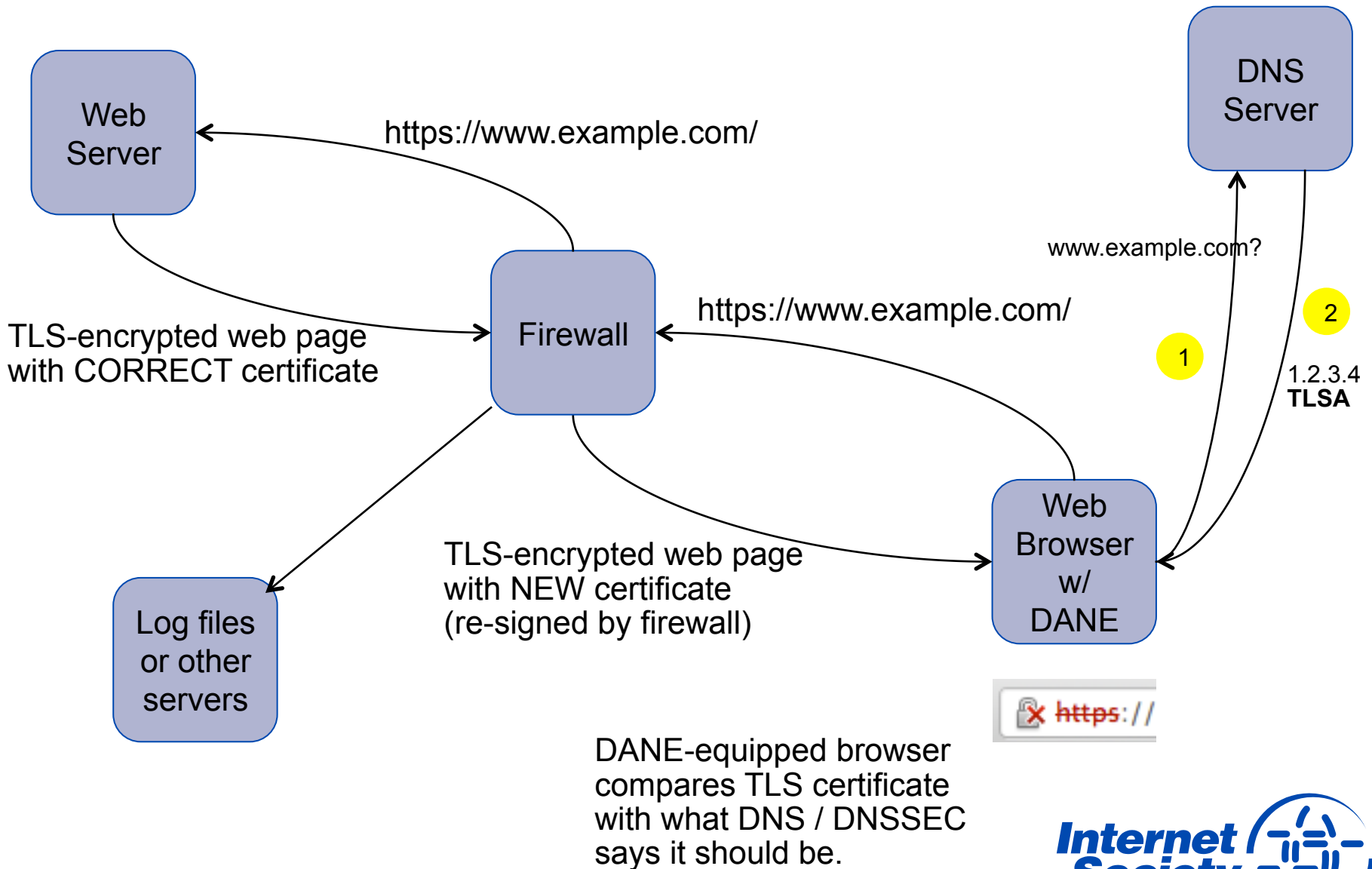
Q: How do you know if the TLS (SSL) certificate is the correct one the site wants you to use?

A: Store the certificate (or keys used) in DNS 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.

# Problems?



# DANE Resources

IETF Journal article explaining DANE:

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

DANE Working Group:

- <http://datatracker.ietf.org/wg/dane/charter/>

RFC 6394 - DANE Use Cases:

- <http://tools.ietf.org/html/rfc6394>

RFC 6698 – DANE Protocol:

- <http://tools.ietf.org/html/rfc6698>

# DNS Hosting Providers – How You Can Help

How can you help get DANE deployed?

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.

Have your customers be among the first to be more secure!

# The Deploy360 Programme

# Download A DNSSEC Whitepaper

“Challenges and Opportunities in Deploying DNSSEC”

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

# Review Our DNSSEC Content Roadmap

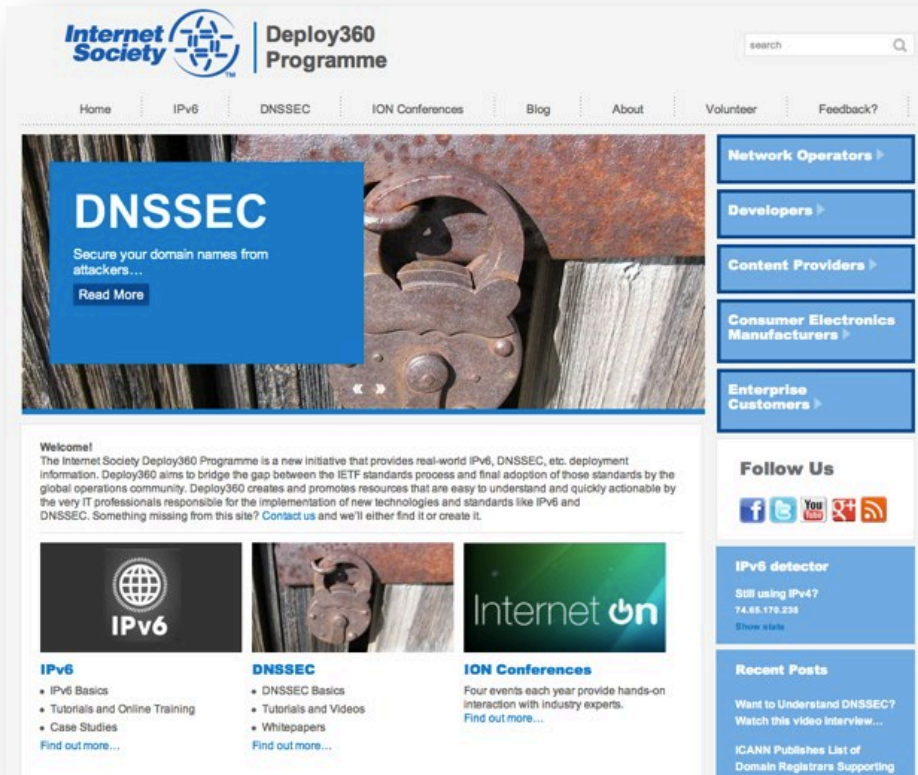
We have posted a roadmap of the content we believe we need to add to Deploy360 site related to DNSSEC (and IPv6):

**[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)**

# Internet Society Deploy360 Programme



Can You Help Us With:

- Case Studies?
- Tutorials?
- Videos?

How Can We Help You?

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

**Dan York**

Senior Content Strategist, Internet Society

york@isoc.org

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

**Thank You!**