

# Next Steps In Accelerating DNSSEC Deployment

DNS-OARC Spring Forum 2013  
May 12, 2013

Dan York  
Internet Society

# Internet Society Deploy360 Programme

**Internet Society** | Deploy360 Programme

Home IPv6 DNSSEC ION Conferences Blog About Volunteer Feedback?

## DNSSEC

Secure your domain names from attackers...

[Read More](#)

**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...](#)

### Network Operators

[Developers](#)

[Content Providers](#)

[Consumer Electronics Manufacturers](#)

[Enterprise Customers](#)

### Follow Us

f t You+ g+ r

### IPv6 detector

Still using IPv4?  
14.85.178.238

[Show stats](#)

### Recent Posts

Want to Understand DNSSEC?  
Watch this video interview...

ICANN Publishes List of  
Domain Registrars Supporting

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

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

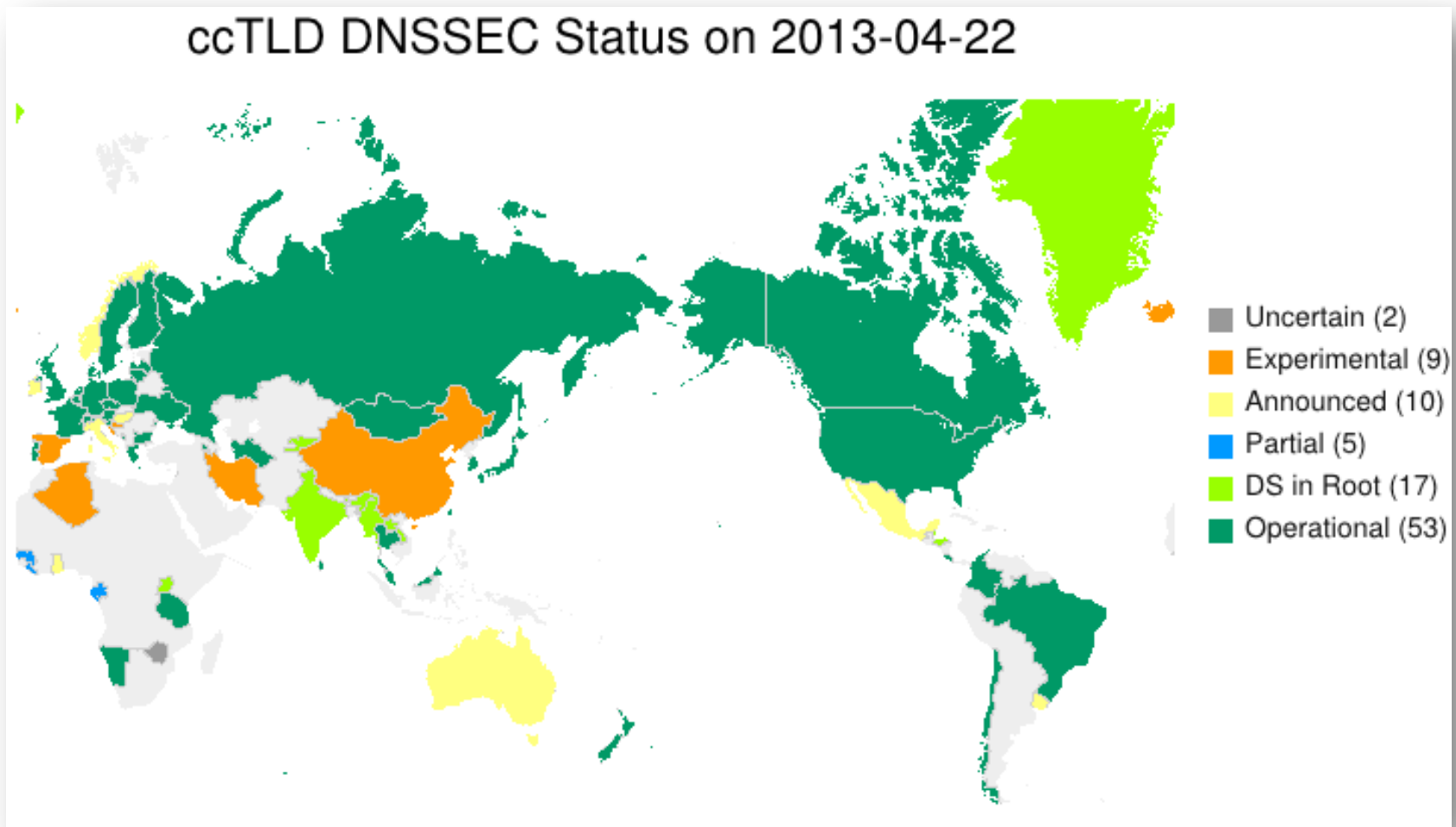
[www.internetsociety.org/deploy360/](http://www.internetsociety.org/deploy360/)

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

# DNSSEC Deployment Status – Signing Side

- All major generic TLDs signed (.com, .org, .net ... )
- 105 TLDs (of 317) signed as of April 25, 2013:
  - [http://stats.research.icann.org/dns/tld\\_report/](http://stats.research.icann.org/dns/tld_report/)
- DNSSEC is *mandatory* for the 1,900+ proposed new gTLDs
- Tools have become greatly automated
- Developer libraries now support DNSSEC
- Struggling a bit with registrar support:
  - <http://www.icann.org/en/news/in-focus/dnssec/deployment>

# DNSSEC Deployment Status



# DNSSEC Deployment Status – Validation Side

## DNSSEC validation is easily enabled for major DNS resolvers:

- BIND 9.x
- Unbound
- Microsoft Windows Server 2012

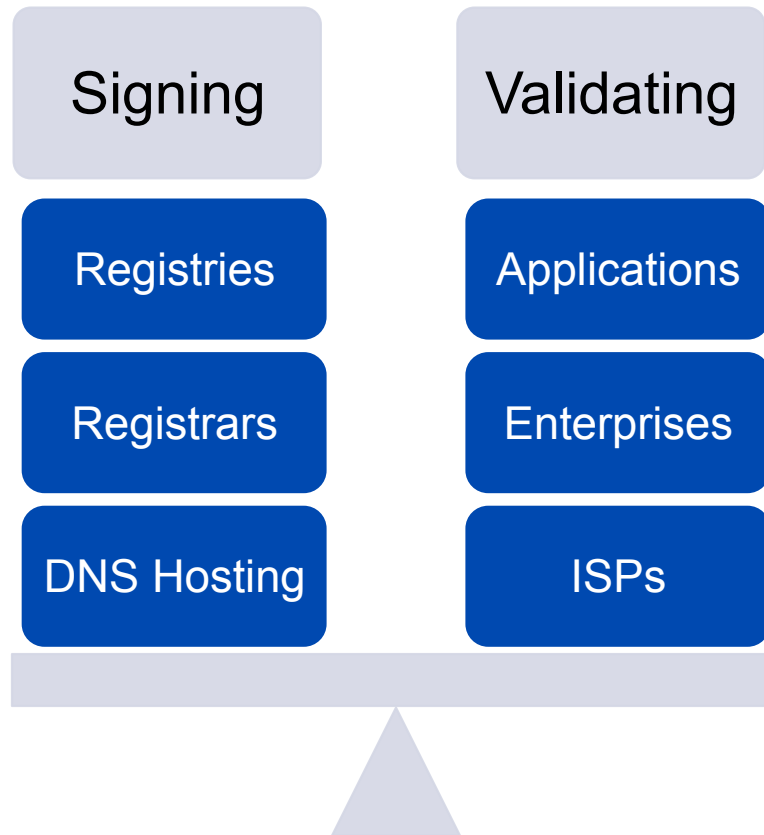
## See SURFnet white paper:

- [http://www.surfnet.nl/Documents/rapport\\_Deploying\\_DNSSEC\\_v20.pdf](http://www.surfnet.nl/Documents/rapport_Deploying_DNSSEC_v20.pdf)

## Large-scale deployments:

- Comcast deployed DNSSEC validation to their 18 million customers
- Most ISPs in Sweden, Czech Republic, Netherlands, Brazil
- Google's Public DNS (8.8.8.8, 8.8.4.4 and IPv6 versions) now support full validation of DNSSEC

# The Two Parts of DNSSEC

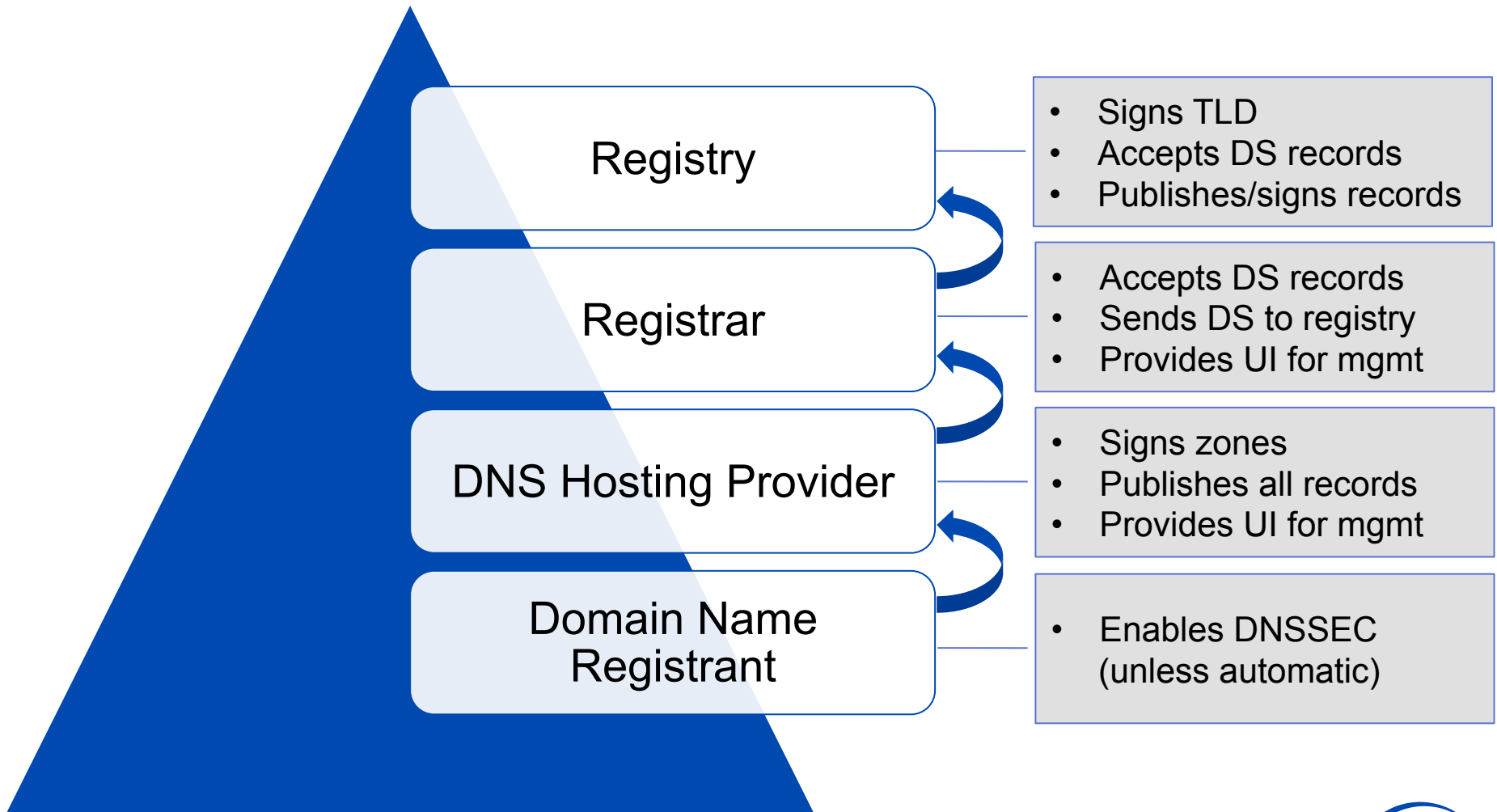


# DNSSEC Validation

- **Fairly simple – just enable DNSSEC validation in your DNS caching resolver**
  - DNS resolver will return a SERVFAIL if there is a validation error. User will not receive any results
- **Question is more where does DNSSEC validation occur?**
  - ISP's DNS resolvers
  - Public DNS resolvers
  - Local network DNS resolver
  - Local computer (i.e. operating system)
  - Application

(answer is that it could occur in any of the locations)

# DNSSEC Signing - The Individual Steps





# Registrars and DNS Hosting Providers Supporting DNSSEC

# Signing *Can* Be Simple

Secondary DNS   DNSSEC   Vanity Nameservers

## DNSSEC Settings

5 DNSSEC domains available. [Buy more.](#)

**Enabled:**  
 On  
 Off

**Domain Status:** Unsigned

Email key change notifications to:

**Save** [Cancel](#)

### Add Delegation Signer Record

**Key Tag:**

**Algorithm:** 3 - DSA/SHA-1

**Digest Type:** 1 - SHA-1

**Digest:**

**Add Key** **Cancel**

Dyn | DynECT Managed DNS

Overview   Manage DNS   Add-Ons   Manage Account   View Reports   Support

## dnssec-test-dyn.com

Serial: 1, [1 zone notes](#)

Simple Editor   Services   Zone Options   Quick Tasks   Zone Reports

General   **DNSSEC**   Freeze Zone

### Zone Signing Keys

Encryption Method	Key Expiration	Key Size
RSA/SHA-1	1 month from now	1,024 bit

### Key Signing Keys

Encryption Method	Key Expiration	Key Size
RSA/SHA-1	1 year from now	2,048 bit

### Notifications

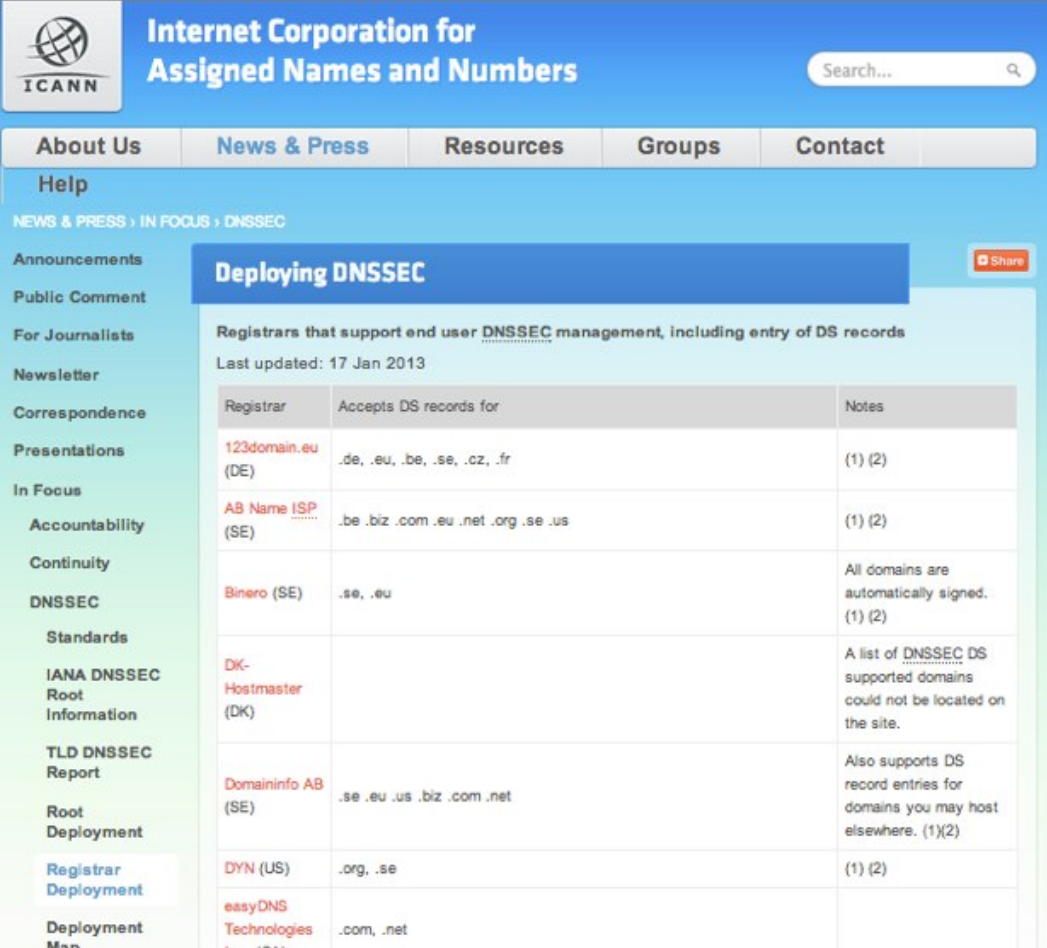
**Contact:** billing (Dan York)

**Send notifications:**

- When a key is created
- When a key expires
- Weeks before a key expires

**Add DNSSEC**

# ICANN's List of Registrars



Internet Corporation for Assigned Names and Numbers

Search...

About Us News & Press Resources Groups Contact

Help

NEWS & PRESS > IN FOCUS > DNSSEC

Announcements Public Comment For Journalists Newsletter Correspondence Presentations In Focus Accountability Continuity DNSSEC Standards IANA DNSSEC Root Information TLD DNSSEC Report Root Deployment Registrar Deployment Deployment Map

## Deploying DNSSEC

Share

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

Last updated: 17 Jan 2013

Registrar	Accepts DS records for	Notes
<a href="#">123domain.eu</a> (DE)	.de, .eu, .be, .se, .cz, .fr	(1) (2)
<a href="#">AB Name ISP</a> (SE)	.be, .biz, .com, .eu, .net, .org, .se, .us	(1) (2)
<a href="#">Binerio</a> (SE)	.se, .eu	All domains are automatically signed. (1) (2)
<a href="#">DK-Hostmaster</a> (DK)		A list of DNSSEC DS supported domains could not be located on the site.
<a href="#">Domaininfo AB</a> (SE)	.se, .eu, .us, .biz, .com, .net	Also supports DS record entries for domains you may host elsewhere. (1)(2)
<a href="#">DYN</a> (US)	.org, .se	(1) (2)
<a href="#">easyDNS Technologies</a>	.com, .net	

<http://www.icann.org/en/news/in-focus/dnssec/deployment>

## 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

# "DS Upload"

- **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

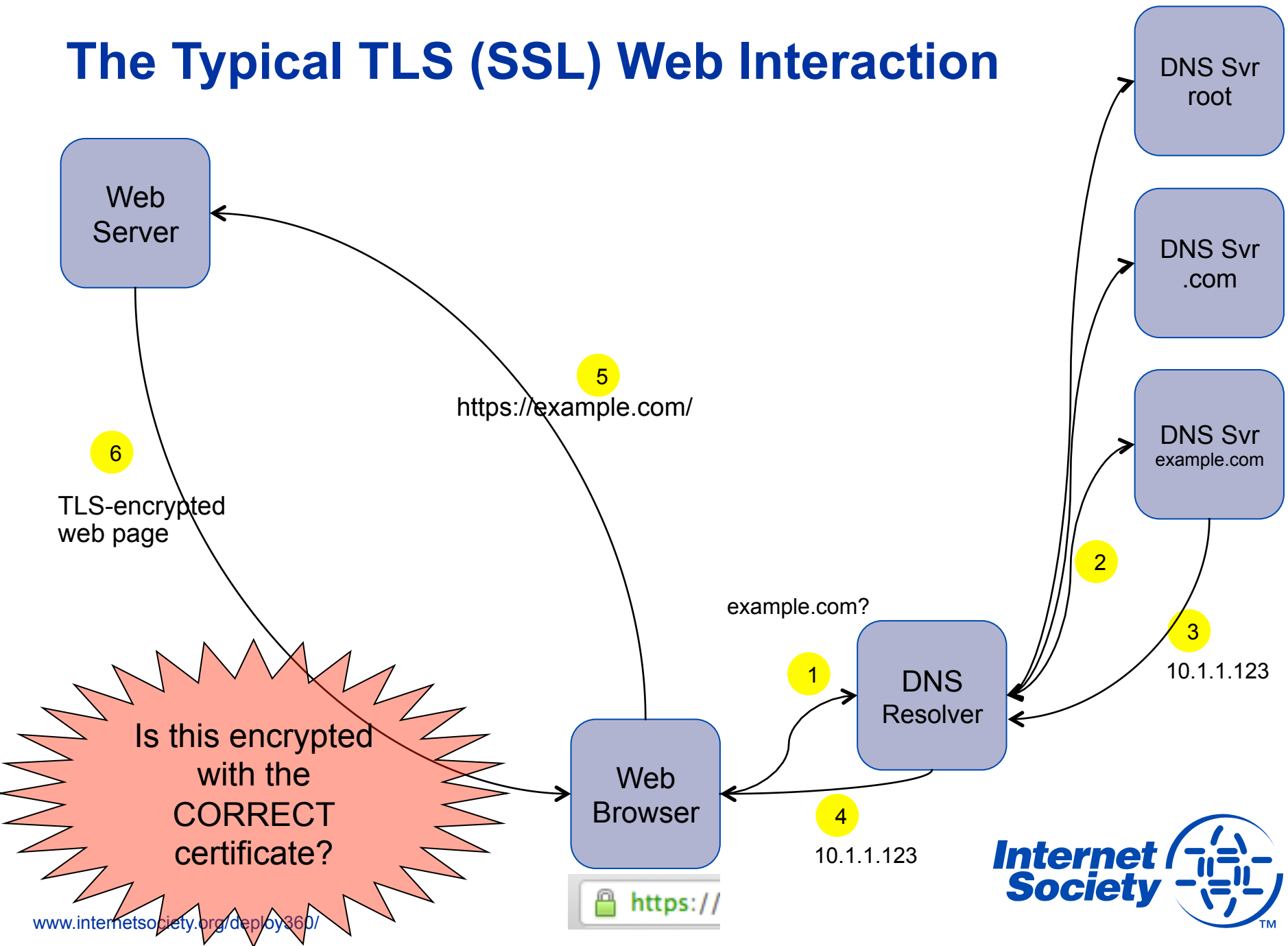
**Multiple proposals exist for solutions**

# A Business Case For DNSSEC – DANE?

# A Powerful Combination

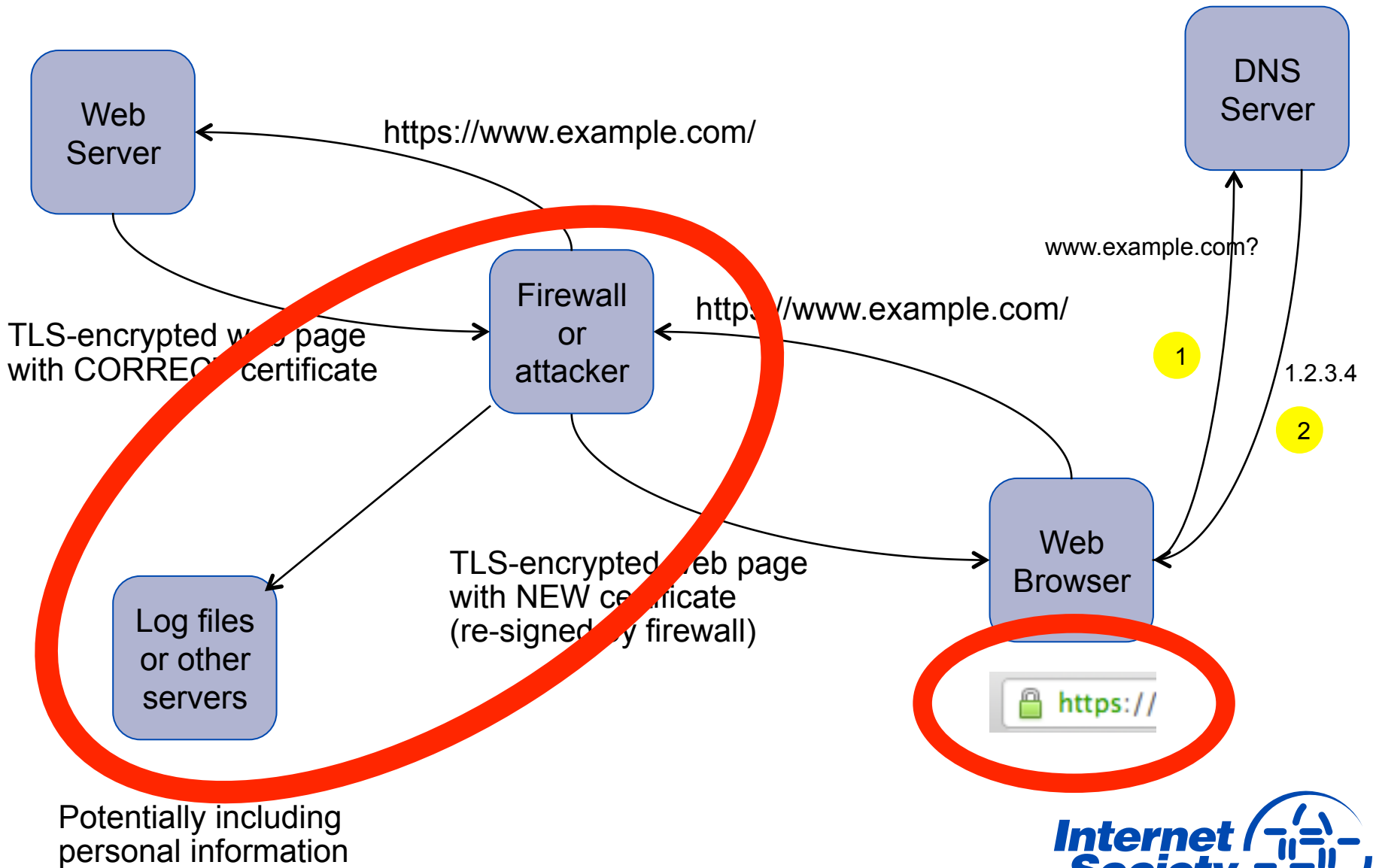
- TLS = encryption + *limited* integrity protection
- DNSSEC = strong integrity protection
- How to get encryption + strong integrity protection?
- TLS + DNSSEC = **DANE**

# The Typical TLS (SSL) Web Interaction





# Problems?



Potentially including personal information

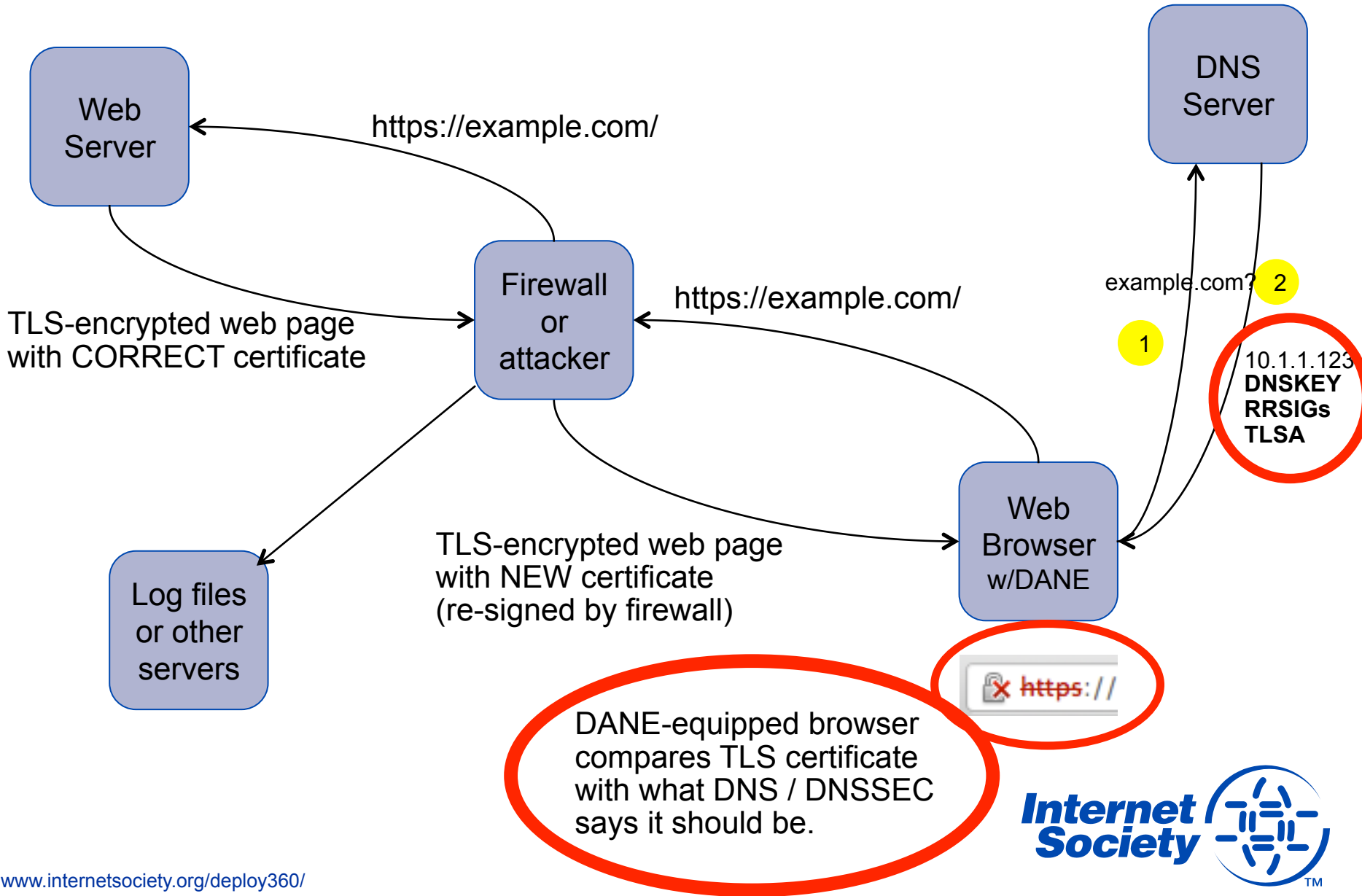
# Issues

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.

# DANE



# DANE

**DANE as an "upgrade to the 'trust layer' of the Internet**

**Complementing existing certificates to add an additional layer of integrity and security**

# How Do We Get DANE Deployed?

## Developers:

- Add DANE support into applications (see list of libraries)
- Note: VoIP developers don't need to wait for browser vendors!

## 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.

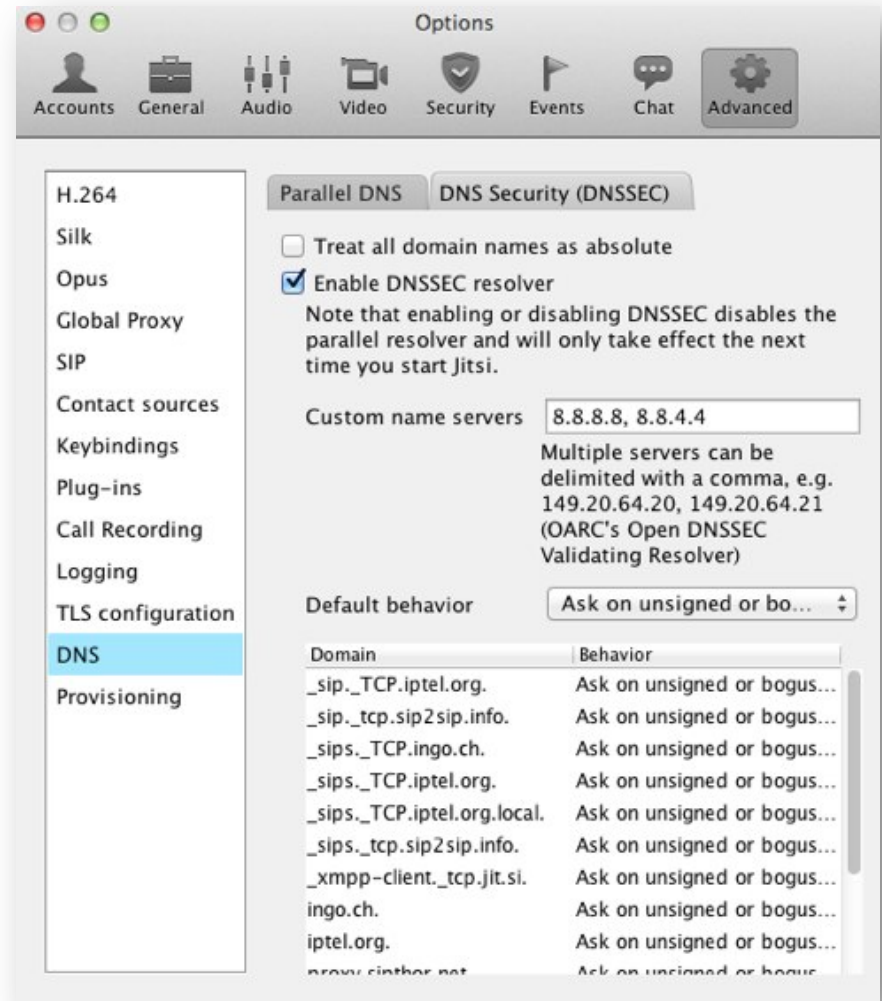
## Network Operators / Enterprises / Governments:

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

# Expanding Into New Areas Example: DNSSEC and VoIP

# Example: Jitsi softphone

- [www.jitsi.org](http://www.jitsi.org)
- Includes DNSSEC resolver
- Generates warning message with DNSSEC failures
- Currently works in Jitsi 2.2



# Example: Kamailio SIP Server

- **New DNSSEC module**
- **Tutorial:**  
<http://www.kamailio.org/wiki/tutorials/dns/dnssec>



The screenshot shows the Kamailio SIP Server Wiki page for the DNSSEC module. The page title is "Kamailio with DNSSEC". The main content area contains the following text:

The **dnssec** module in Kamailio was added during the development of v4.1.0 (expected to be released later in 2013). Therefore this tutorial presents how to add DNSSEC module in the default configuration file of Kamailio, following GIT installation guidelines.

In short, this tutorial focuses on:

- install Kamailio development version from GIT repository on Ubuntu 12.04 32b
- enable user authentication and persistent location service using MySQL server
- add DNSSEC support to configuration file

Below the main content, there is a "Table of Contents" section with the following items:

- Kamailio with DNSSEC
  - About DNSSEC
    - DNSSEC Tools Installation
    - DNSSEC Tools Devel Libraries Installation
  - Kamailio Installation
    - Prerequisites
    - Fetch Sources from GIT Repository
    - Compile and Install
    - Installation Details
    - Kamctl Setup
    - Database Setup
    - Adding SIP Users

The page also features a search bar, a navigation menu on the left, and a sidebar on the right with icons for search, clock, and link.



# My "Asks" At Conferences

# Three Requests For Network Operators (ISPs)

**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.

# Three Requests For Website/Content Owners

## 1. Sign your domains

- Work with your registrar and/or DNS hosting provider to make this happen.

## 2. Ask your IT team or network operator about DNSSEC validation

## 3. Help promote support of DANE protocol

- Let browser vendors and others know you want to use DANE. If you use SSL, deploy a TLSA record if you are able to do so. Help raise awareness of how DANE and DNSSEC can make the Internet more secure.

# DNSSEC Resources

Deploy360 Programme:

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

DNSSEC Deployment Initiative:

- [www.dnssec-deployment.org/](http://www.dnssec-deployment.org/)

DNSSEC Tools:

- [www.dnssec-tools.org/](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>

# Your Participation

**Visit and explore**

**<http://www.internetsociety.org/deploy360>**

## **Create Content**

- Help us develop materials based on your experiences
- We will credit your work

## **Define New Features**

- Tell us what you need to get started on your own deployment
- We have the flexibility to make changes/additions

**Contact us: [deploy360@isoc.org](mailto:deploy360@isoc.org)**

**Dan York, CISSP**

Senior Content Strategist, Internet Society

york@isoc.org

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

**Thank You!**