

# Challenges and Opportunities in DNSSEC Deployment and Usage – A 2014 View

Dan York  
Senior Content Strategist  
Internet Society

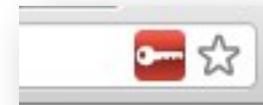
ICANN 50, June 23, 2014, London England

(Original presentation in March 2012 at ICANN 43)

# What Should The End User Experience Be?



Mixed. The end user experience is still not determined... but I sense a growing view that we don't want the TLS/SSL error warning experience.



# DNSSEC-Validating Resolvers

Good News – More deployment of DNSSEC-validating resolvers. Google Public DNS and others helped here. Still more work to do.



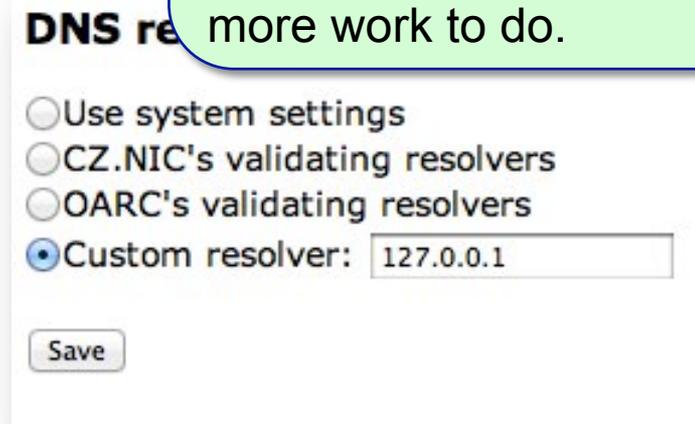
**comcastvoices**  
a place for conversations with Comcast

Home Archives Media Gallery

**10 JAN** **Comcast Completes DNSSEC Deployment**  
Posted by [Jason Livingood](#), Vice President, Internet Systems, in [Network](#)

I am pleased to announce that Comcast, the largest ISP in the U.S., is pleased to have fully implemented Domain Name System Security Extension (DNSSEC) on its network. As part of our ongoing efforts to protect our customers, DNSSEC is now automatically enabled for all Comcast customers using Constant Guard™ from Xfinity.

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



**DNS re**

- Use system settings
- CZ.NIC's validating resolvers
- OARC's validating resolvers
- Custom resolver:



# Application Developer Libraries

Good News – DNSSEC appearing in more libraries – and the release of the getDNS API is a big step

## DNSSEC Developer Libraries

At the current time we are aware of the following libraries for developers seeking DNSSEC support to their applications:

### C

- [ldns](#) from NLnet Labs
- [libval](#) from the DNSSEC-Tools Project
- [libunbound](#), a component of the [Unbound DNS resolver](#) that can be used in applications

### Erlang

- [dns\\_erlang](#)

### Go

- [godns](#)

### Java

- [dnsjava](#)
- [DNSSEC4J](#) (based on the DNSSEC primitives in dnsjava)

### Perl

- [Net::DNS](#) and [Net::DNS::SEC](#)
- [Perl modules from the DNSSEC-Tools Project](#)

### Python

- [dnspython](#) – available at [dnspython.org](#) and on [Github](#)
- [python-dnssec](#)
- [PyUnbound](#) – a python wrapper for the libunbound library (mentioned above under C)

### Ruby

- [dnruby](#)

Source: [www.internetsociety.org/deploy360/resources/dnssec-developer-libraries/](http://www.internetsociety.org/deploy360/resources/dnssec-developer-libraries/)

# Domain Name Registrars

Good News – More registrars supporting at least *some* DNSSEC info.

2013 R.A.A. major source of action here.

Deploying DNSSEC

Registrars that support end user DNSSEC management, including entry of D

Last updated: 27 May 2014

Registrar	Accepts DS records for	Note
123domain.eu (DE)	.de, .eu, .be, .se, .cz, .fr	(1)
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)
BIT B.V. (NL)	.com, .net, .org, .nl, .be, .de, .eu, .info, .biz	(1) (DS via email)
CSL Computer Service Langenbach GmbH dba JOKER.COM (DE)	.de, .nl, .com, .net, .cc, .tv, .me, .org, .biz, .us, .at, .uk, .eu	(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)	.com, .net, .org, .biz, .info, .se	(1) (2)
Dynadot (US)	.com, .net, .org, .biz, .be, .cc, .de, .eu, .in, .co, .in, .net, .in, .org, .in, .fr, .in, .com, .in, .ind, .in, .in, .it, .me, .nl, .com, .nl, .net, .nl, .org, .nl	(2)

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

# User Experience at the Registrar / DNS Hosting?

Secondary DNS | DNSSEC | Vanity Nameservers

## DNSSEC Settings

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

Enabled:  
 On  
 Off

Domain Status: Unsigned

Email key change notifications to:

[Cancel](#)

### Add Delegation Signer Record

Key Tag:

Algorithm:

Digest Type:

Digest:

Mixed. Better at some registrars and DNS Hosting Providers. Still a good bit of work to do. Still too much copy-and-paste.

Dyn | DynEC

Overview | Manage DNS

## 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:

Send notifications

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



# Awareness of DNSSEC Information

Good News – More and better information. Still more work to do, but getting better.

**NLnet**  
**DNSSEC HOWTO**  
NLnetLabs | Projects | Publications | Support

**NIST**  
National Institute of Standards and Technology  
Technology Administration  
U.S. Department of Commerce

## Secure Domain Name (DNS) Deployment Guide

### DNSSEC HOWTO, a tutorial in disguise

Olaf Kolkman  
Revision 134

July 4, 2009

Download the most recent PDF release from:  
[http://www.nlnetlabs.nl/dnssec\\_howto/dnssec\\_howto.pdf](http://www.nlnetlabs.nl/dnssec_howto/dnssec_howto.pdf)

About This Howto: Improving the security of the Internet's naming infrastructure



Home | Calendar | About | Resources | DNSSEC Pulse | Papers, Presentations, & Newsletters

## We have Wiki!

Posted by [Mark Feldman](#) in [Uncategorized](#) on February 24, 2012

We try to keep ourselves and you informed about all things related to the deployment of DNSSEC, but we can't do it alone. We also publish useful information from a variety of points of view, and we try to bring those to the attention of the community. One source of information that is often overlooked in these blog posts and web sites is you. We appreciate the information you provide. Deploying DNSSEC is on the leading edge (yes, it is).

Our solution, which hasn't been given the spotlight it deserves, is to create an account, and help us document the DNSSEC

**DNSSEC-Tools**

**Is your domain secure?**

**Sign Your Zone Tutorials Install**

Deploying DNSSEC  
Good practices guide  
January 10

Good practices guide for deploying DNSSEC

enisa  
European Network and Information Security Agency

# Rationale for Deploying DNSSEC?



Good News – DANE a major help. Seeing DANE/DNSSEC deployment in XMPP, SMTP, IM – and interest for web sites. Heartbleed vulnerability increased interest in securing TLS.

Snowden revelations also increased interest in overall Internet security.

# (New) Solving The "DS Upload" Issue

**How to communicate to the parent zone that a new DNSSEC key has been published**

- **Potential solutions**

- <http://tools.ietf.org/html/draft-ietf-dnsop-delegation-trust-maintainance>
- <http://tools.ietf.org/html/draft-ietf-dnsop-child-synchronization-01>

# (New) Secure Transfer of Domains Between Registrars

Once a domain is signed, what is the best way to transfer it between registrars?

- **Potential solution:**
  - <http://tools.ietf.org/html/draft-ietf-ppext-keyrelay>

# **(New) Network Infrastructure**

**Roadblocks in terms of middle boxes, non-compliant resolvers, etc.**

## **draft-ietf-dnsop-dnssec-roadblock-avoidance**

- <http://tools.ietf.org/html/draft-ietf-dnsop-dnssec-roadblock-avoidance>

# What Else?



**Dan York**

Senior Content Strategist, Internet Society

york@isoc.org

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

**Thank You!**