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

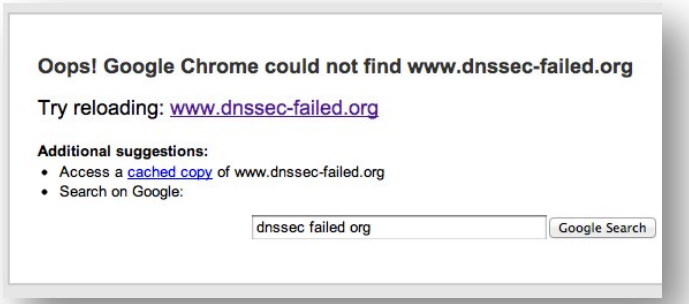
Dan York
Senior Content Strategist
Internet Society

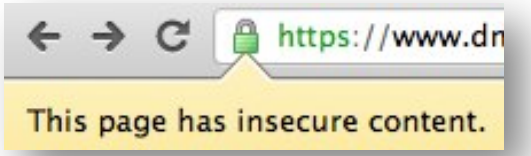
ICANN 50, June 23, 2014, London England

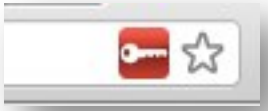
(Original presentation in March 2012 at ICANN 43)

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.

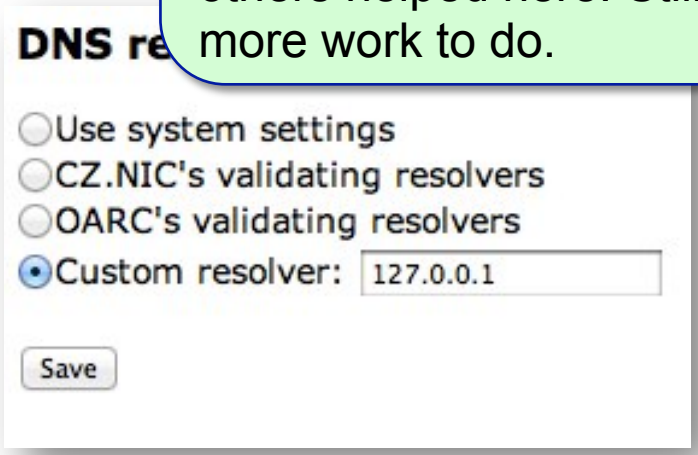






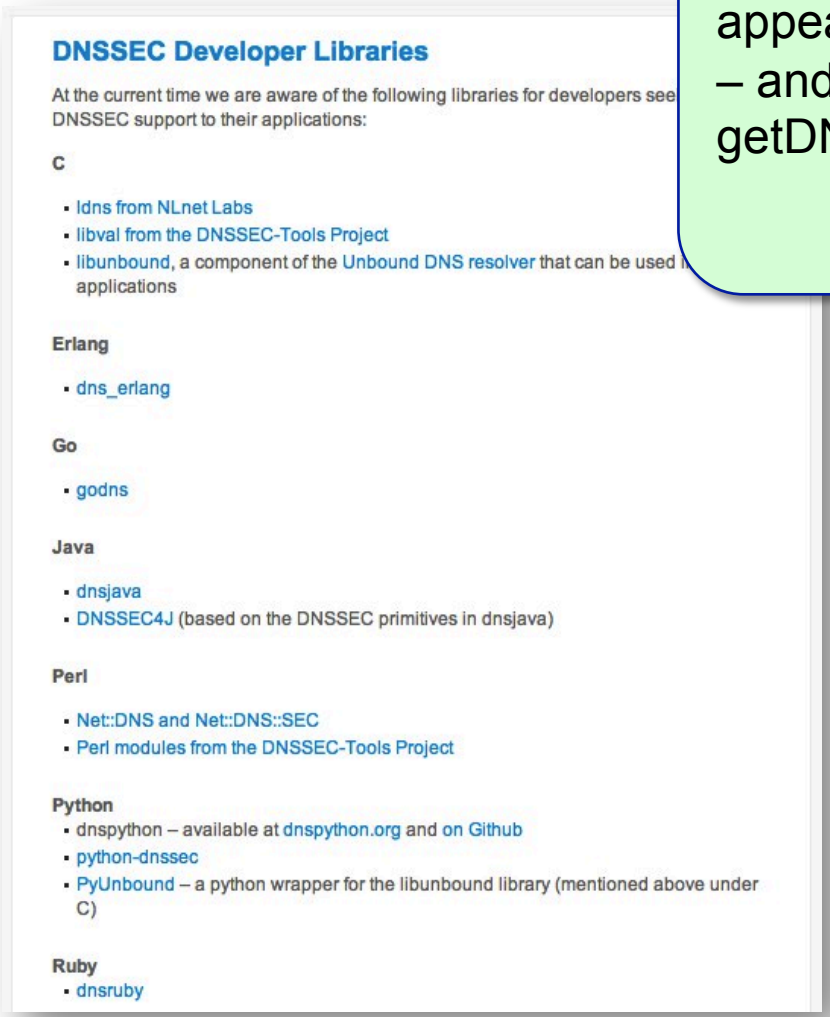
DNSSEC-Validating Resolvers

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



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 see 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 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

- dnsruby

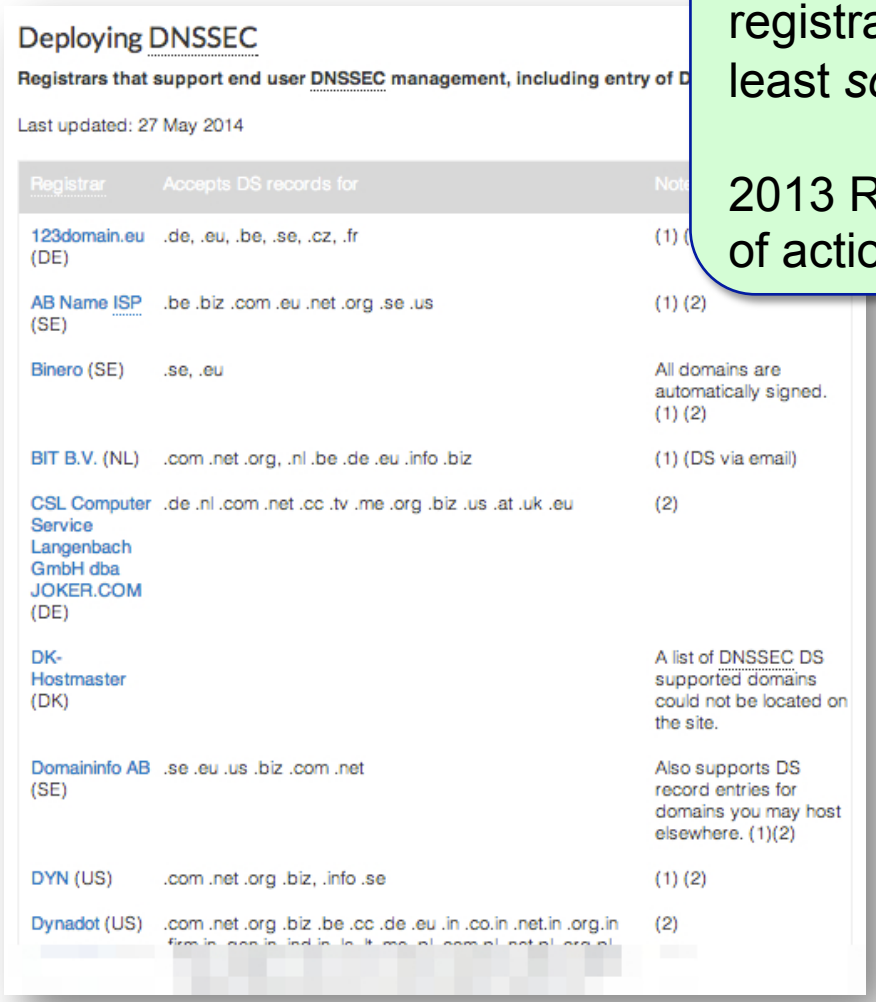
Source: www.internetsociety.org/deploy360/resources/dnssec-developer-libraries/

Internet Society™

Domain Name Registrars

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

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



Deploying DNSSEC

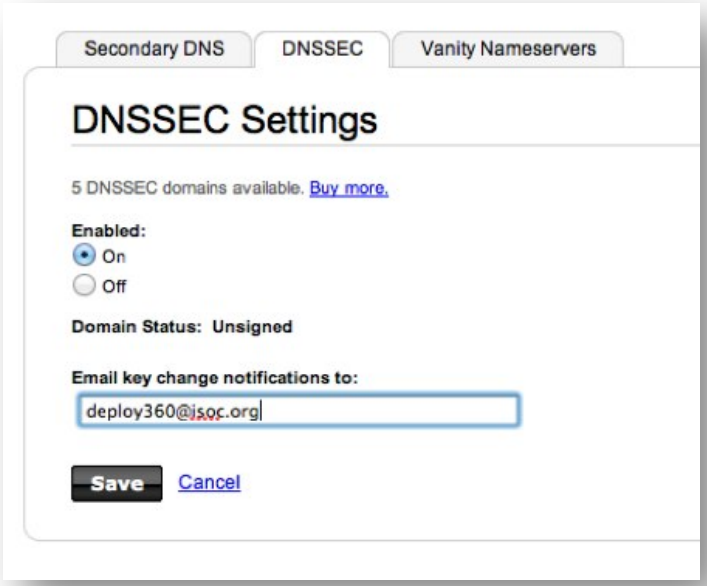
Registrars that support end user DNSSEC management, including entry of D

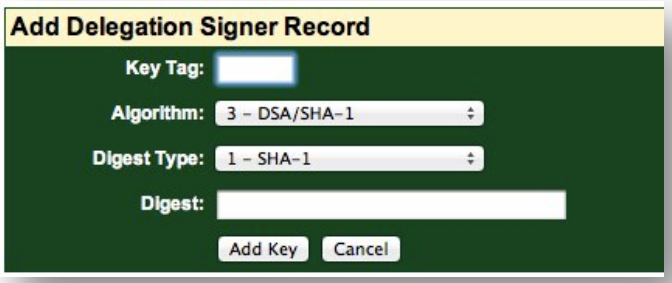
Last updated: 27 May 2014

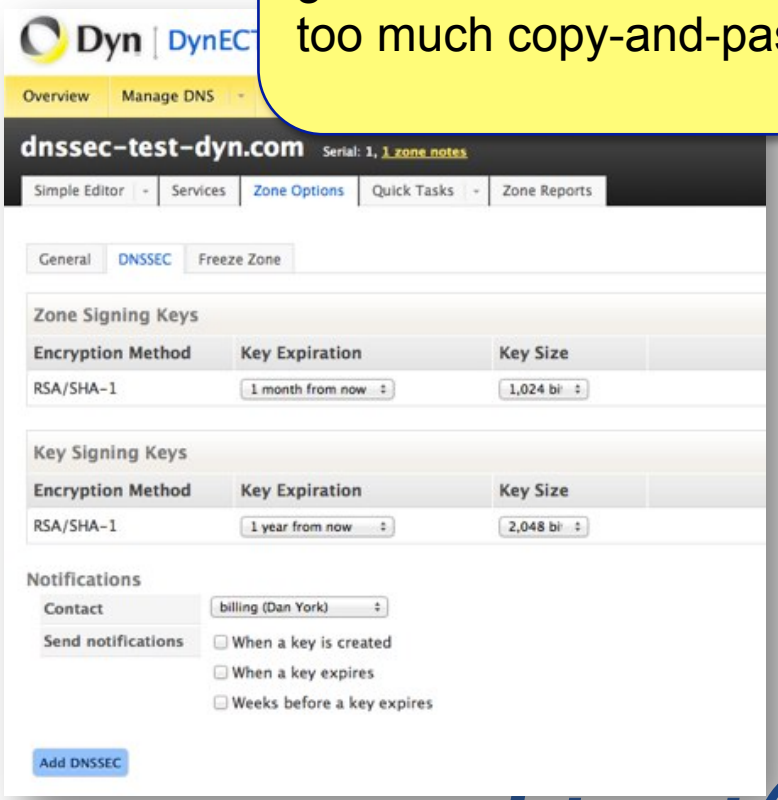
Registrar	Accepts DS records for	Not
123domain.eu (DE)	.de, .eu, .be, .se, .cz, .fr	(1) (
AB Name ISP (SE)	.be .biz .com .eu .net .org .se .us	(1) (2)
Binero (SE)	.se, .eu	All domains are automatically signed. (1) (2)
BIT B.V. (NL)	.com .net .org, .nl .be .de .eu .info .biz	(1) (DS via email)
CSL Computer 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	(2)

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

User Experience at the Registrar / DNS Hosting?

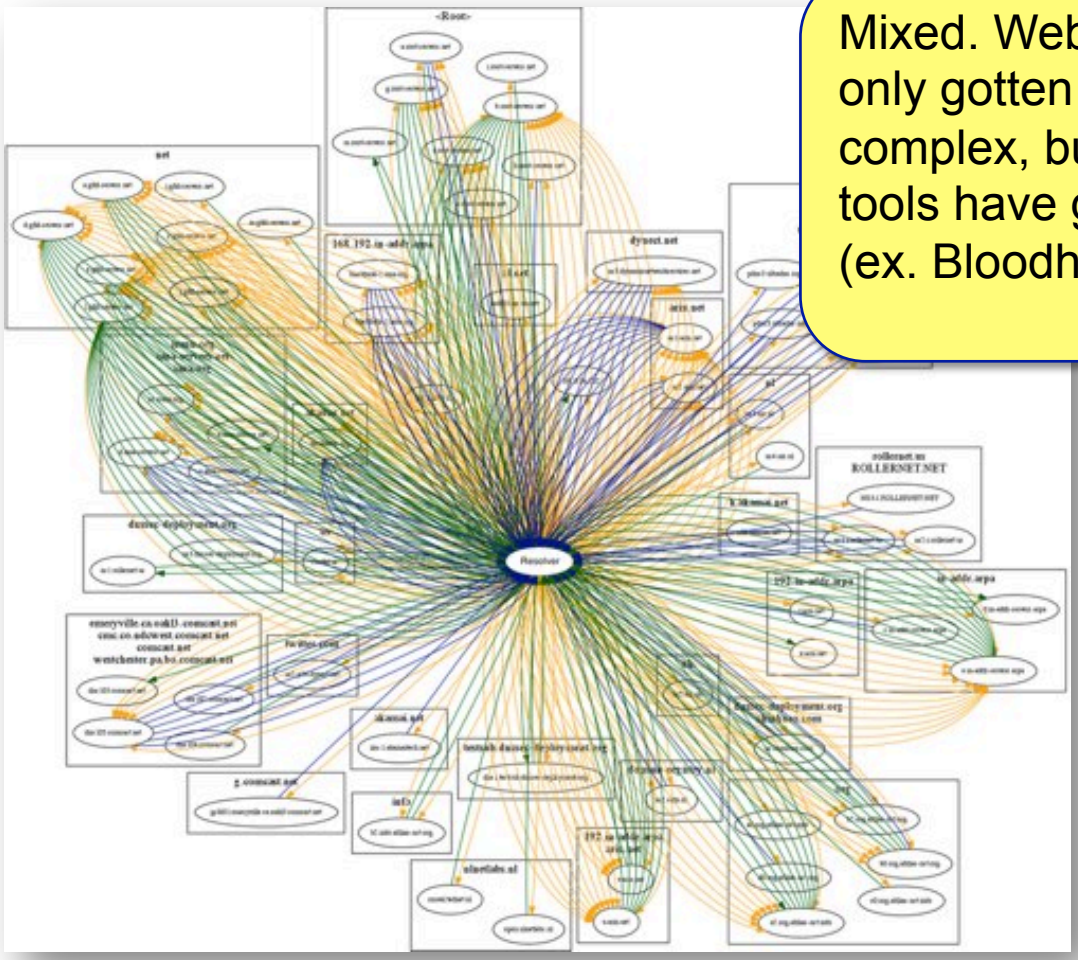






Mixed. Better at some registrars and DNS Hosting Providers. Still a good bit of work to do. Still too much copy-and-paste.

Complexity of Modern Web Sites



Mixed. Web sites have only gotten MORE complex, but some of our tools have gotten better (ex. Bloodhound).

Source: www.dnssec-deployment.org/index.php/2012/02/are-you-secure/

Internet Society™

Awareness of DNSSEC Information

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

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-syncronization-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-eppext-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?

Internet Society™

Dan York

Senior Content Strategist, Internet Society

york@isoc.org

www.internetsociety.org/deploy360/

Thank You!