Key Steps To Accelerating DNSSEC Deployment

Dan York
Senior Content Strategist
Internet Society

Eurasian Network Operators Group (ENOG) 2012
May 22, 2012

Internet Society™

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?

Three Areas of Focus

1. *Domain name consumers* – entities (people or organizations) that are going to *use* domain names, for instance in applications or web browsers.

2. *Domain name holders* – entities that register domain names and wish to sign them with DNSSEC.

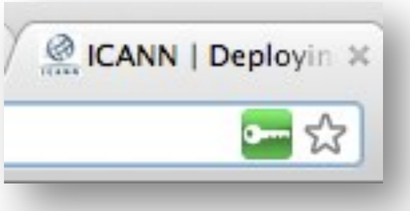
3. *Domain name infrastructure operators* – entities that operate components of the domain name infrastructure such as domain name registrars, DNS hosting providers and content delivery networks

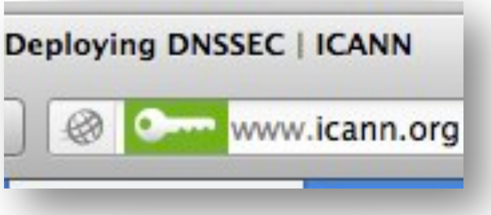
Domain Name Consumers

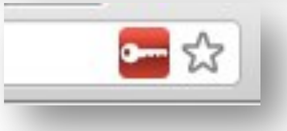
What Should The End User Experience Be?

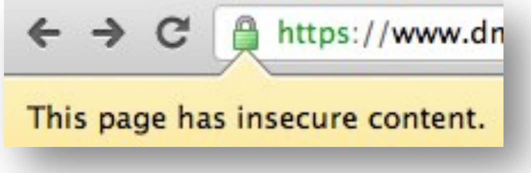
As an industry, we need to be clear on what "DNSSEC" should look like to "average" user:

- *Should* there be any visible sign?
- Should there be a new icon? Or more data added to lock icon?
- Or should the DNS lookup simply fail?
- If so, should we have a new error message back to browsers?

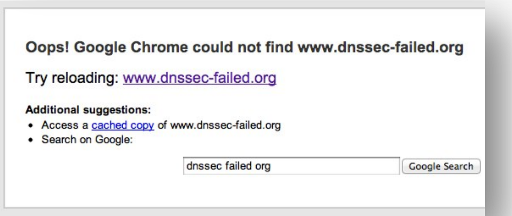








This page has insecure content.



Oops! Google Chrome could not find www.dnssec-failed.org

Try reloading: www.dnssec-failed.org

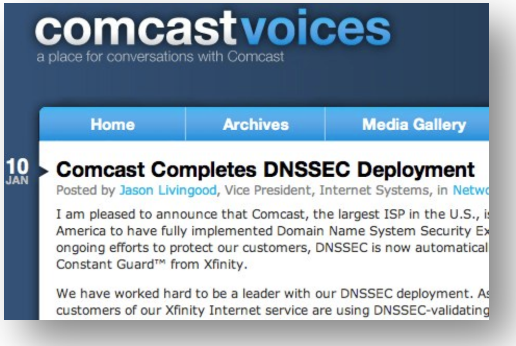
Additional suggestions:
- Access a cached copy of www.dnssec-failed.org
- Search on Google:

dnssec failed org | Google Search

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



10 JAN

Comcast Completes DNSSEC Deployment

Posted by Jason Livingood, Vice President, Internet Systems, in Netwo

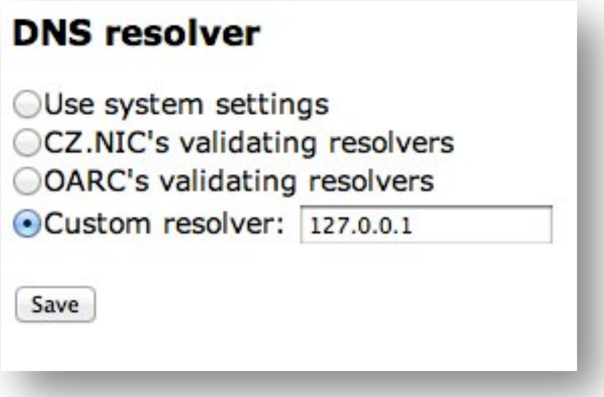
I am pleased to announce that Comcast, the largest ISP in the U.S., i America to have fully implemented Domain Name System Security Ex ongoing efforts to protect our customers, DNSSEC is now automatical Constant Guard™ from Xfinity.

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

- Almost all ISPs in Sweden and Czech Republic provide DNSSEC-validating resolvers

Availability of DNSSEC-Validating Resolvers

End users *can* install local DNSSEC-validating resolvers, or configure their system to use known resolvers. Examples:



DNS resolver

○ Use system settings
○ CZ.NIC's validating resolvers
○ OARC's validating resolvers
● Custom resolver: 127.0.0.1

- CZ.NIC's browser plugins
- DNSSEC-Trigger from NLNet Labs

This, though, requires users to go through these steps.

Availability of DNSSEC-Validating Resolvers

Larger questions for industry discussions:

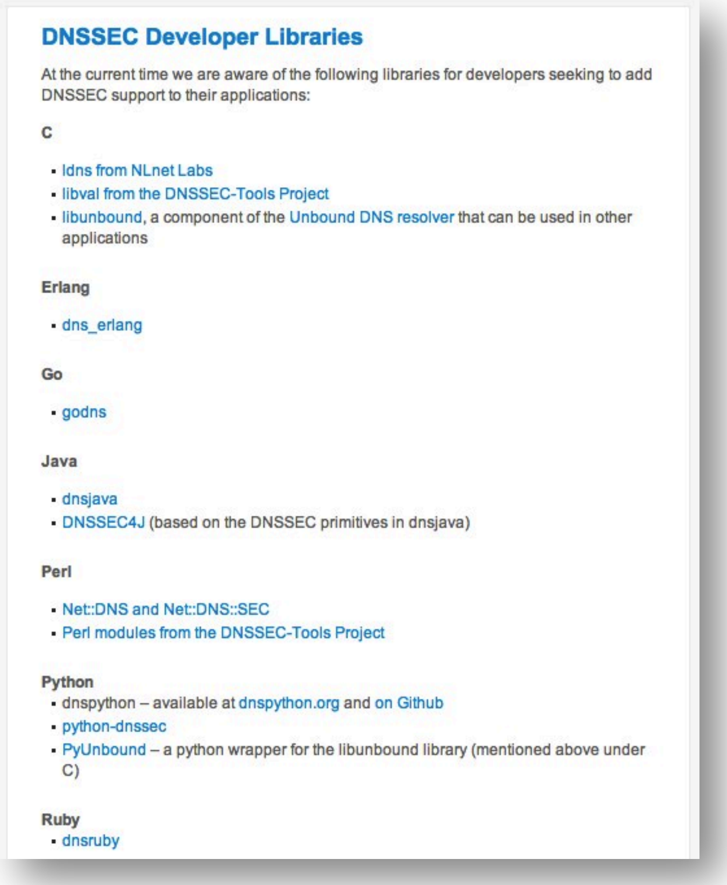
- *Where* should DNSSEC-validation occur?
- Is a DNSSEC-validating resolver at the ISP “good enough”?
- Or should the DNSSEC-validation occur on the user’s local network? Or even in the operating system of their local machine?

Reality is that DNSSEC rollout will probably occur in phases, with initial deployments of DNSSEC-validating resolvers at ISPs and then moving to local networks and computers

Application Developer Libraries Are Available

Good news is that many / most DNS libraries for developers include DNSSEC support.

- Developers need to understand value of DNSSEC
- Question again of end-user experience:
  - Should a developer need to care? Or should the operating system simply take care of DNSSEC?



DNSSEC Developer Libraries

At the current time we are aware of the following libraries for developers seeking to add 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 other 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

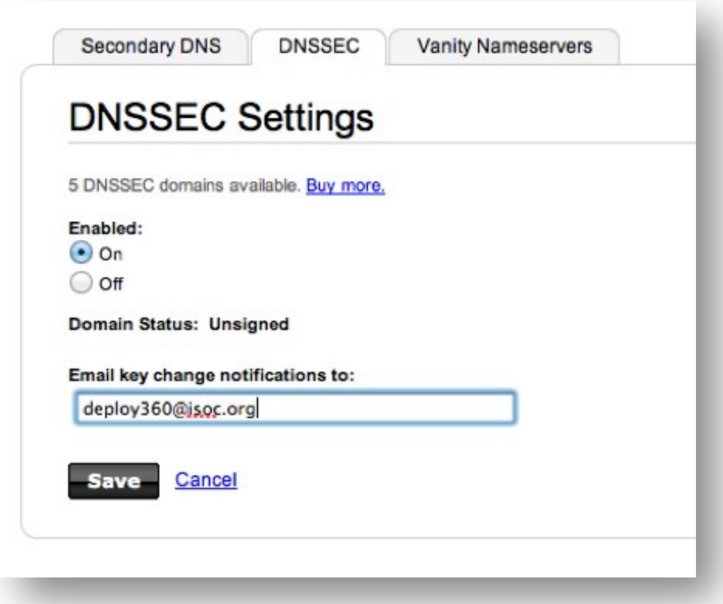
Source: www.internetsociety.org/deploy360/resources/dnssec-developer-libraries/

Domain Name Holders

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



DNSSEC Settings

5 DNSSEC domains available. Buy more.

Enabled:
● On
○ Off

Domain Status: Unsigned

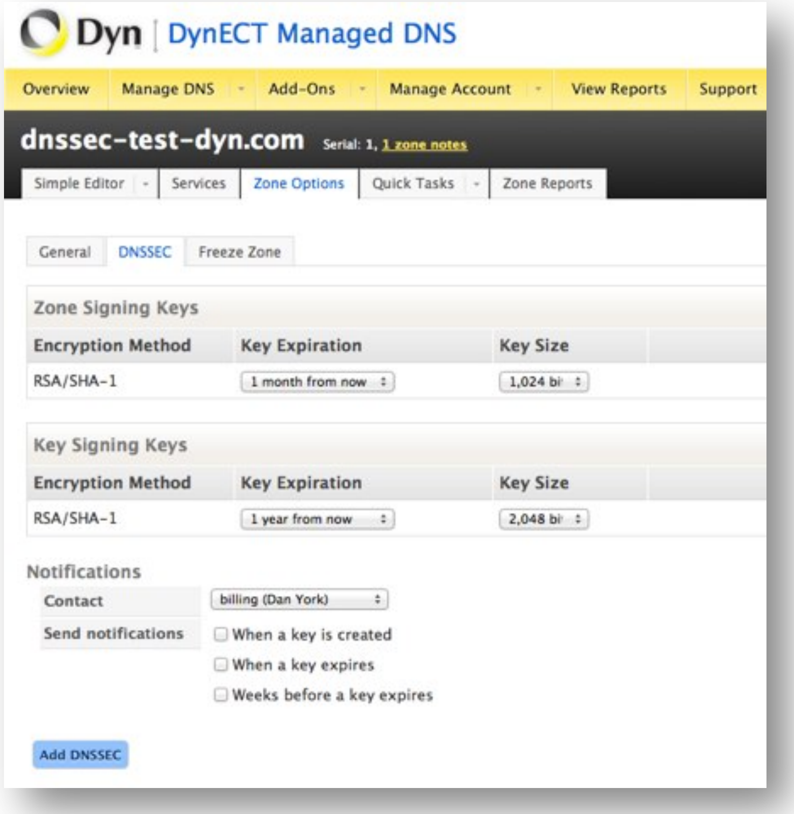
Email key change notifications to:
deploy360@isoc.org

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



dnssec-test-dyn.com Serial: 1, 1 zone notes

Zone Signing Keys

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

Key Signing Keys

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

Notifications

Contact: billing (Dan York)

Send notifications:
□ When a key is created
□ When a key expires
□ Weeks before a key expires

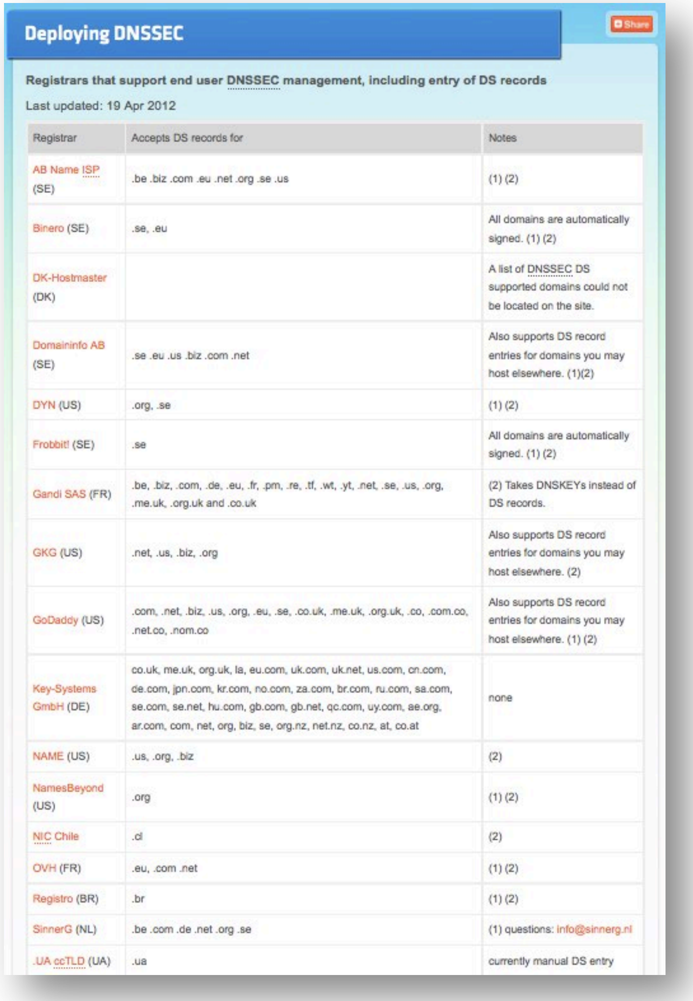
Increase Number of Domain Name Registrars

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



Deploying DNSSEC

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

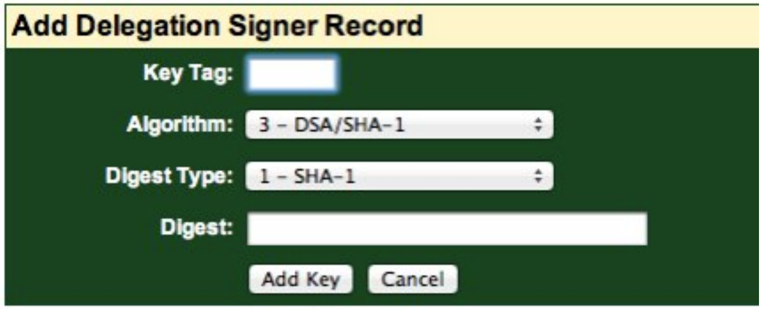
Last updated: 19 Apr 2012

Registrar	Accepts DS records for	Notes
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)
Frobbit! (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, 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 (US)	.org	(1) (2)
NIC Chile	.cl	(2)
OVH (FR)	.eu, .com .net	(1) (2)
Registro (BR)	.br	(1) (2)
SinnerG (NL)	.be .com .de .net .org .se	(1) questions: info@sinnerg.nl
.UA ccTLD (UA)	.ua	currently manual DS entry

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

Simplify/Automate Transfer of DS Records

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



Add Delegation Signer Record

Key Tag:

Algorithm: 3 - DSA/SHA-1

Digest Type: 1 - SHA-1

Digest:

- Ideally needs to be automated to remove this extra step

Some registrars offering API. Example:

- 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".

Simplify/Automate Transfer of DS Records

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

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

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

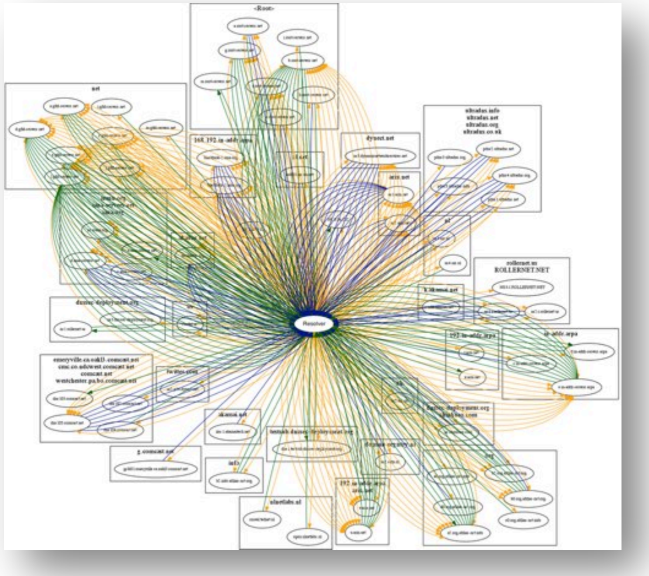
Registrar

versus

DNS Hosting Provider

Recognize Complexity of Modern Web Sites

Modern websites are not simple group of pages. Now much more complex. Examples:



- Content from multiple sites
- Use of web hosting providers (with CNAME usage)
- Use of Content Delivery Networks (CDNs)

Full DNSSEC validation requires DNSSEC support in all providers.

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

Complexity of Modern Web Sites - CNAMEs

Example – pointing a domain to WordPress.com involves:

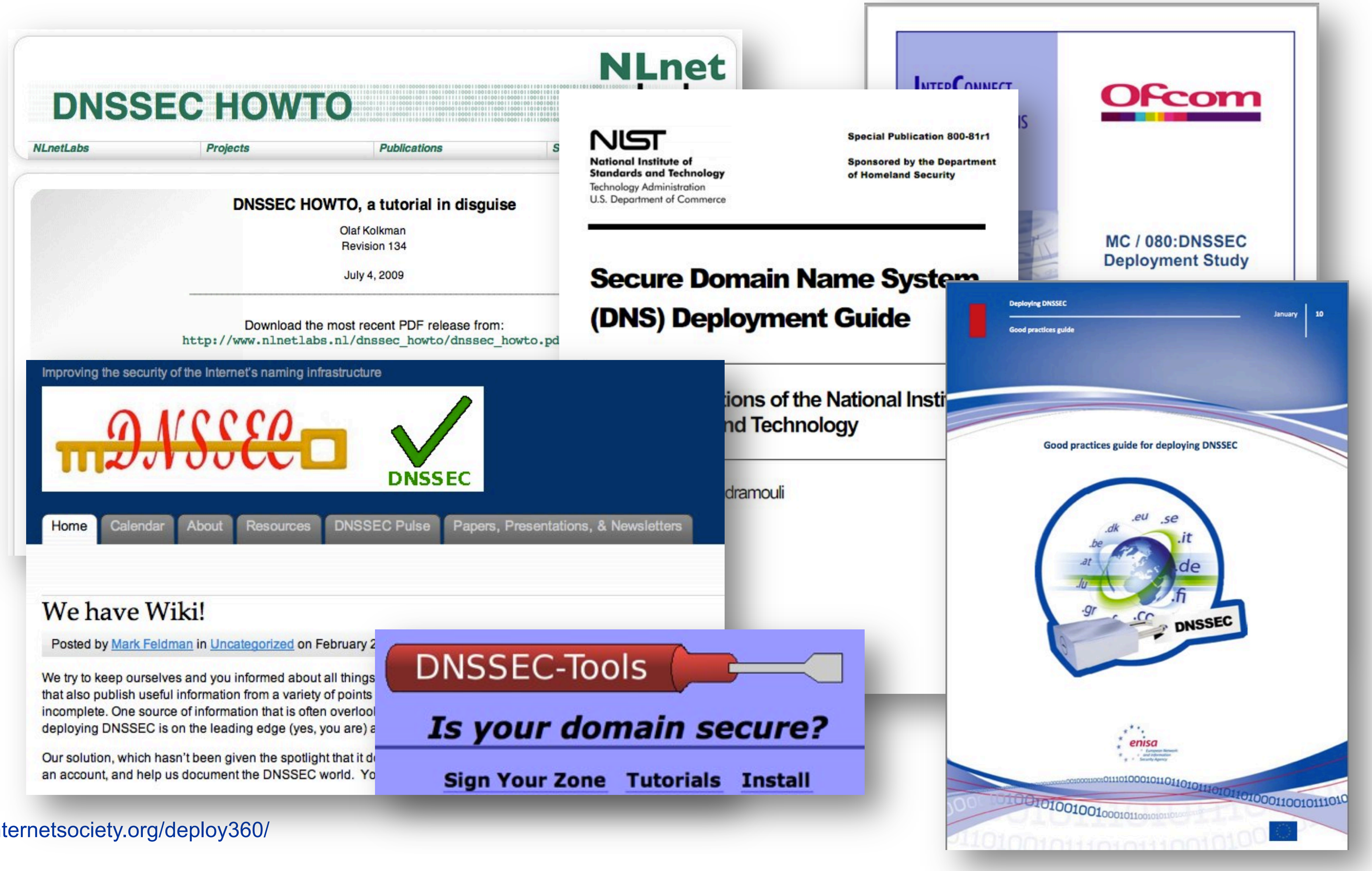
```
www.example.com. IN CNAME yourblog.wordpress.com.
```

- DNSSEC validation on “www.example.com” proceeds fine until it hits this record
- Now must go through DNSSEC validation for “yourblog.wordpress.com”
- Requires that hosting providers support DNSSEC

Domain Name Infrastructure Operators

Awareness of DNSSEC Information

Great amount of content *already* available!



NLnet

DNSSEC HOWTO

NLnetLabs Projects Publications S

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.pd

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

Special Publication 800-81r1

Sponsored by the Department of Homeland Security

Secure Domain Name System (DNS) Deployment Guide

ions of the National Insti
nd Technology

dramouli

InterConnect
IS

Ofcom

MC / 080:DNSSEC Deployment Study

Deploying DNSSEC
Good practices guide
January | 10

Good practices guide for deploying DNSSEC

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 2

We try to keep ourselves and you informed about all things
that also publish useful information from a variety of points
incomplete. One source of information that is often overloo
deploying DNSSEC is on the leading edge (yes, you are) a

Our solution, which hasn't been given the spotlight that it d
an account, and help us document the DNSSEC world. Yo

DNSSEC-Tools

Is your domain secure?

Sign Your Zone Tutorials Install

Other Areas (Beyond Those Mentioned Earlier)

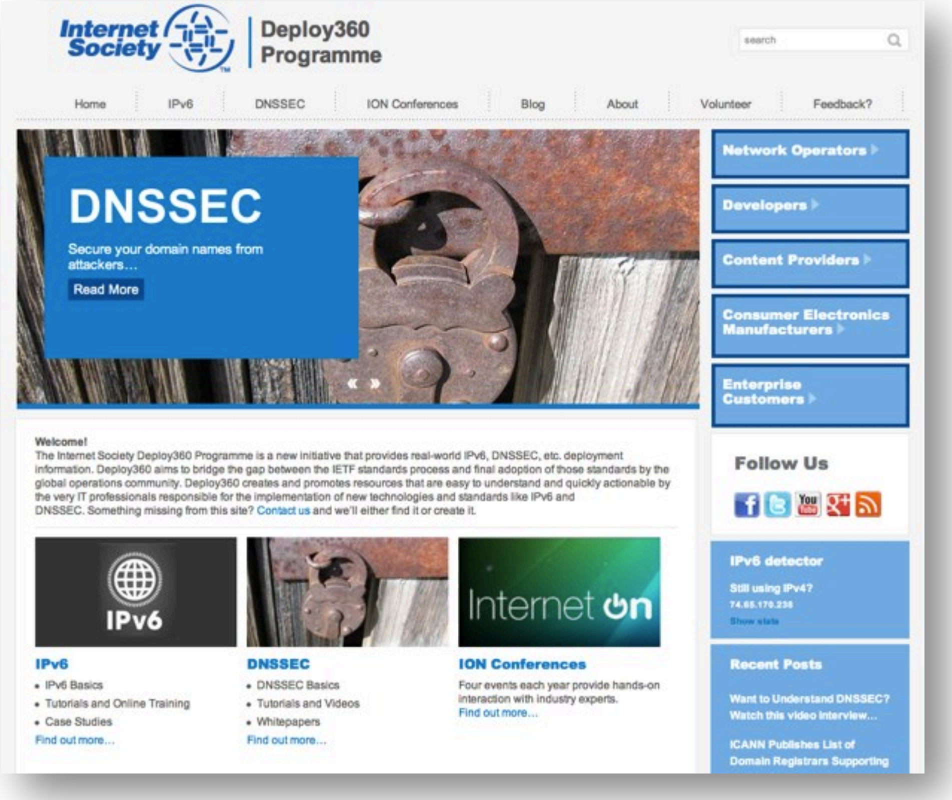
- Tools exist to help automate key signing (ex. OpenDNSSEC)
- Your “key rollover” process needs to be well-documented (ex. NASA/Comcast issue)
- Guidance can be found in “DNSSEC Policy & Practice Statements” (often abbreviated “DPS”)

Key Steps For Network Operators To Consider:

- Can you provide DNSSEC-validating DNS resolvers to your customers?
- If you provide a domain name registrar function, can you make it easy for domain name holders to sign their domain? Can you even automate it entirely? (or if you don't directly, can you work with registrars in your area?)
- Can you help simplify/automate the DS record process?
- Can you work with web hosting providers and CDNs to provide DNSSEC-signing of their records?

The Deploy360 Programme

Internet Society Deploy360 Programme



DNSSEC

Secure your domain names from attackers…

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…

IPv6 detector

Still using IPv4?

74.65.170.238

Show stats

Recent Posts

Want to Understand DNSSEC? Watch this video interview…

ICANN Publishes List of Domain Registrars Supporting

Providing real-world deployment info:

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

www.internetsociety.org/deploy360/

Download A DNSSEC Whitepaper

"Challenges and Opportunities in Deploying DNSSEC"

bit.ly/isoc-satin2012

Review Our DNSSEC Content Roadmap

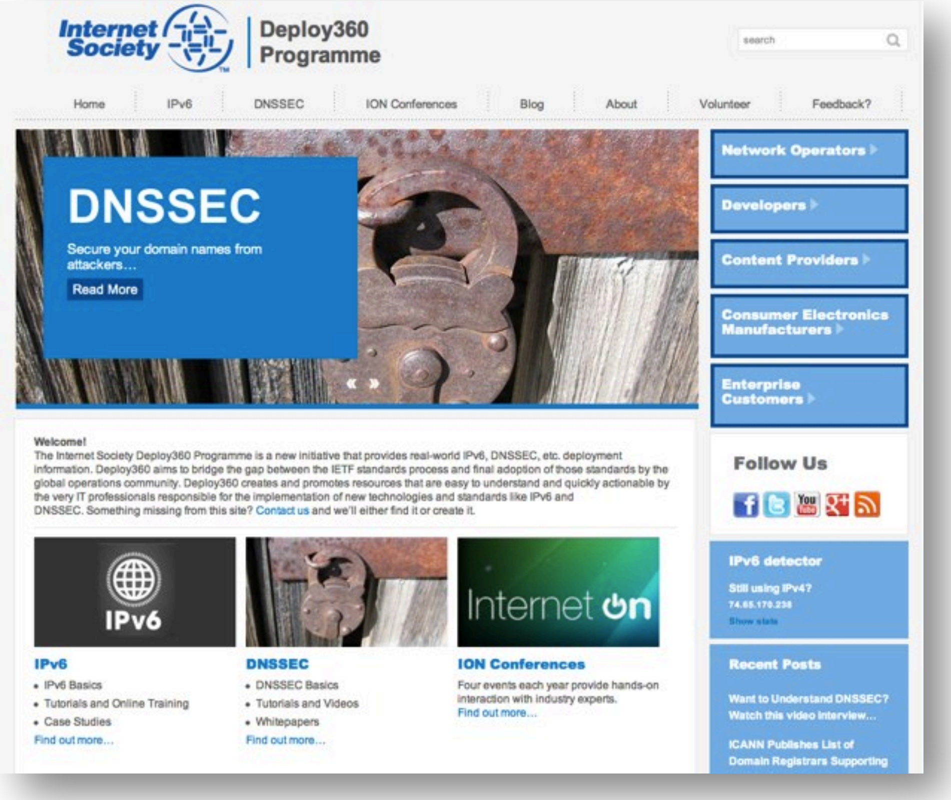
We have posted a roadmap of the content we believe we need to add to Deploy360 site related to DNSSEC (and IPv6):

www.internetsociety.org/deploy360/roadmap/

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**

Internet Society Deploy360 Programme



DNSSEC

Secure your domain names from attackers…

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…

IPv6 detector

Still using IPv4?
74.65.170.238
Show stats

Recent Posts

Want to Understand DNSSEC? Watch this video interview…

ICANN Publishes List of Domain Registrars Supporting

www.internetsociety.org/deploy360/

Can You Help Us With:

- Case Studies?
- Tutorials?
- Videos?

How Can We Help You?

Dan York

Senior Content Strategist, Internet Society

york@isoc.org

www.internetsociety.org/deploy360/

Thank You!

Internet Society ™