Next Steps In Accelerating DNSSEC Deployment

Dan York, CISSP
Senior Content Strategist, Internet Society

DNSSEC Deployment Workshop, ICANN 45
Toronto, Canada
October 17, 2012
Internet Society Deploy360 Programme

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

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

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?
Opportunities to Accelerate Deployment

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.

4. Government activity with DNSSEC
   • Encouraging governments to expand their promotion and usage of DNSSEC
DNSSEC Signing - The Players

- Registries
- Registrars
- DNS Hosting Providers
- Domain Name Registrants
DNSSEC Signing - The Individual Steps

- **Registry**
  - Signs TLD
  - Accepts DS records
  - Publishes/signs records

- **Registrar**
  - Accepts DS records
  - Sends DS to registry
  - Provides UI for mgmt

- **DNS Hosting Provider**
  - Signs zones
  - Publishes all records
  - Provides UI for mgmt

- **Domain Name Registrant**
  - Enables DNSSEC (unless automatic)
DNSSEC Signing - The Players

- Registries
- Registrars
- DNS Hosting Providers
- Domain Name Registrants

Registrar also provides DNS hosting services
DNSSEC Signing - The Players

- Registrars
- Registries
- DNS Hosting Providers
- Domain Name Registrants

Registrant hosts own DNS
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

*Note: If you are not aware, a DS record ties the DNSSEC-signed DNS zone into the global “chain of trust”.*
Simplify The Registrar/Hosting Experience

We need to make the DNSSEC-signing process at domain name registrars easy for domain name registrants / 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
Simplify The DNS Hosting 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 DNS hosting providers
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.

• Ideally needs to be automated to remove this extra step

Some registrars offering API. Example:

• www.gkg.net/ws/ds.html
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
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

If you are a registrar and support DNSSEC, you can ask to be added to ICANN’s list.

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

• How do we increase the percentage?

http://validator-search.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
Validating Name Servers – How To Get There

• Education about value in DNSSEC validation
• Requests from customer base (i.e. larger education)
• Education about available tools and better automation within tools wherever possible
• More case studies, tutorials
Enterprises / Domain Name Holders
Key Steps for Enterprises / Governments

Steps:
1. Sign domain(s)
2. Enable/install DNSSEC-validating name servers

Needed:

- 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
- More tutorials, more tools
- DANE…
DANE
The Typical TLS (SSL) Web Interaction

2. The DNS Server responds with the IP address `1.2.3.4`.
3. The Web Browser then sends an HTTPS request to `https://www.example.com/` to the Web Server.
4. The Web Server returns the TLS-encrypted web page to the Web Browser.
The Typical TLS (SSL) Web Interaction

1. The Web Browser resolves the domain name "www.example.com" to an IP address (1.2.3.4).
2. The Web Browser connects to the IP address and requests the URL "www.example.com".
3. The DNS Server returns the IP address for "www.example.com".
4. The Web Browser establishes a secure connection (TLS-encrypted) to the Web Server and requests the page from "https://www.example.com/".

Is this encrypted with the CORRECT certificate?
What About This?

Web Server

https://www.example.com/

DNS Server

www.example.com?

1.2.3.4

Firewall (or attacker)

TLS-encrypted web page with CORRECT certificate

Web Browser

TLS-encrypted web page with NEW certificate (re-signed by firewall)
Problems?

- Web Server
- DNS Server
- Firewall
- Web Browser

TLS-encrypted web page with CORRECT certificate

TLS-encrypted web page with NEW certificate (re-signed by firewall)

1. www.example.com?
2. 1.2.3.4

https://www.example.com/
Problems?

Web Server

https://www.example.com/

TLS-encrypted web page with CORRECT certificate

Firewall

https://www.example.com/

TLS-encrypted web page with NEW certificate (re-signed by firewall)

Log files or other servers

Potentially including personal information

DNS Server

www.example.com?

1 1.2.3.4

Web Browser

TLS-encrypted web page

1

Log files or other servers

Potentially including personal information

www.internetsociety.org/deploy360/
**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.
DANE

Web Server

https://www.example.com/

DNS Server

Log files or other servers

Firewall

1.2.3.4 TLSA

Web Browser w/ DANE

TLS-encrypted web page with CORRECT certificate

https://www.example.com/

DANE-equipped browser compares TLS certificate with what DNS / DNSSEC says it should be.

1

2

TLS-encrypted web page with NEW certificate (re-signed by firewall)

www.example.com?
DANE – Not Just For The Web

• DANE defines protocol for storing TLS certificates in DNS
• Securing Web transactions is the obvious use case
• Other uses also possible:
  • Email via S/MIME
  • VoIP
  • Jabber/XMPP
  • ?
DANE Resources

DANE Overview and Resources:

• http://www.internetsociety.org/deploy360/resources/dane/

IETF Journal article explaining DANE:


RFC 6394 - DANE Use Cases:

• http://tools.ietf.org/html/rfc6394

RFC 6698 – DANE Protocol:

• http://tools.ietf.org/html/rfc6698
How Do We Get DANE Deployed?

Developers:
• Add DANE support into applications (see list of libraries)

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.
• [More tools are needed to help create TLSA records – ex. hashslinger ]

Network Operators / Enterprises / Governments:
• Start talking about need for DANE
• Express desire for DANE to app vendors (especially browsers)
Next Steps
New Industry Initiative Forming With Focus On:

1. Deployment Documentation
   • What do we need in the way of better documentation/tutorials/etc?

2. Tools
   • What are the missing tools?

3. Unsolved Technical Issues
   • What technical issues remain that need to be addressed?

4. Measurement
   • How do we measure progress of DNSSEC deployment?
   • Can we get more TLDs, ISPs to help provide statistics?
Join The Initial Discussions

Public mailing list, “dnssec-coord”, available and open to all:

https://elists.isoc.org/mailman/listinfo/dnssec-coord

Focus is on better coordinating promotion / advocacy / marketing activities related to DNSSEC deployment.

Planning for monthly conference calls to support online activities.

Stay tuned for more info… (and join the list!)
Internet Society Deploy360 Programme

Can You Help Us With:

• Case Studies?
• Tutorials?
• Videos?

How Can We Help You?

www.internetsociety.org/deploy360/
Thank You!
Additional Material
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
Download A DNSSEC Whitepaper

“Challenges and Opportunities in Deploying DNSSEC”

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/