Challenges and Opportunities In Deploying DNSSEC

A progress report on an investigation into DNSSEC deployment

Dan York
Internet Society
york@isoc.org

March 23, 2012

***Abstract*—In the process of building a web portal[1] focused on providing real-world deployment information about DNS Security Extensions (DNSSEC), Internet Society staff identified a number of areas where DNSSEC deployment can be simplified for domain name holders, domain name infrastructure operators and domain name consumers (i.e. users of DNSSEC-signed domains). Some areas were predictably around the need for more education of consumers, businesses, developers and network operators about DNSSEC. Other areas, though, were more involved with the process involved in signing domains and also in bootstrapping the overall process of using DNSSEC. This paper outlines the challenges identified so far and offers suggestions on how to overcome those challenges.**

I. Introduction

What needs to be done to get more domains signed with DNSSEC? How can DNSSEC validation be built into more applications? What are the challenges preventing more widespread deployment at a network operator, developer, content provider, enterprise and consumer level? 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?

These were the types of questions asked during the development of the Internet Society Deploy360 Programme web portal[1] that focuses on providing information and resources to accelerate the deployment of DNSSEC and IPv6. Since the signing of the DNS root domain in July 2010, over 80 top-level domains (TLDs) signed and thousands of second- and third-level domains have now been signed. This new Internet Society programme was created to build on the success of DNSSEC deployment to date and expand that deployment to the wider industry.

The Deploy360 site was launched in December 2011 and consists of both reviews of deployment-related content already available on the Internet as well as content specifically created by Internet Society staff or partners. The content is curated and reviewed by full-time Internet Society employees with the assistance and advice of subject matter experts within the industry.

The site will not simply be built and left as a static site. The Internet Society has dedicated full-time employees to ensure that the content is constantly updated as new materials and information become available. Staff associated with the site also engage with interested parties through a variety of social media and other channels to encourage discussion and resolution of DNSSEC deployment challenges and opportunities.

During the first half of 2012, the site is under heavy active development and DNSSEC-related content is being added on a constant basis. This paper is a report on the opportunities identified thus far in the process of collecting and creating the DNSSEC deployment content available today. As the site continues to mature and evolve and more content is developed, it is expected that further opportunities for simplification will be identified as well as tools and processes to overcome challenges identified in this paper. This effort, then, should be viewed as a work in progress.

The Deploy360 Programme is targeted broadly at accelerating DNSSEC deployment by the following audiences:

- Network operators, service providers, carriers
- Developers of applications and software
- Content providers (e.g. website operators)
- Consumer electronics manufacturers
- Enterprise customers

However, for the purpose of this paper the deployment challenges are grouped into three areas:

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.

This paper looks at each of those three areas individually and then concludes with some final thoughts.

II. Domain Name Consumers

Domain name "consumers" is a broad category including any person or any application that is using a domain name as part of a task. In this paper the primary focus is on users of web browsers who are connecting to websites via domain

names. A consumer also could be an application using domain names to connect to other sites or services. Other uses not directly addressed in this paper could be mail applications or real-time communications applications such as instant messaging (IM) or Voice over IP (VoIP).

A consumer of domain names generally types a domain name into the application, or chooses one from a contact list, and expects to be able to connect to the chosen address using the application.

A. *Applications Are Not DNSSEC-Aware*

From an end-user point of view, the challenge with DNSSEC is that there are few end-user applications currently using DNSSEC. There are a good number of DNSSEC-related tools for system/network administrators, but for a "regular" user on a computer there are few options.

For web browsers, CZ.NIC Labs has created extensions for Google Chrome[2] and Mozilla Firefox[3] that provide a "key" icon in the browser address bar that changes shape and color based on the status of the DNSSEC validation. The DNSSEC-Tools project similarly provides an extension for Firefox that displays DNSSEC-related information[4]. An issue with these browser extensions is that they do require the user to initiate the installation. At the time of this paper, the project team has not identified other applications that an end-user would typically use that are DNSSEC-aware.

B. *Uncertain End-User Experience*

To this point, one interesting consideration that requires additional exploration within the DNSSEC community is exactly what the "user experience" *should* be for someone working with a DNSSEC-aware application. For instance, the CZ.NIC extensions for Firefox and Chrome currently add another icon (a key) to the browser address bar. Is adding *another* icon the right experience for a browser user? Or will that only lead to further confusion? Is somehow adding more functionality to the "lock" icon in a browser the right path to take? Or will that again cause more confusion?

Alternatively, should DNSSEC validation not be specifically called out to the end-user? For instance, in a web browser use case, if the site has an invalid DNSSEC signature, should the web browser simply display a warning message to the user through a pop-up window or web page?

Outside of a web browser, for instance in a mail client or VoIP client, what is the user experience there?

This is an area that needs further exploration within the DNSSEC community and recommendations for guidance to application developers.[5]

C. *Application Developer Libraries*

For application developers who want to add DNSSEC support into their applications, the good news is that a number of organizations and individual developers have created a variety of libraries for DNSSEC in languages such as C, Java, perl, python and ruby[6]. Some of the available libraries are quite comprehensive while others are basic.

The opportunity here is really one of helping the wider application developer community understand what they need to do to add DNSSEC to their applications and the benefits they will gain in doing so. The creation of additional tutorials and examples for available libraries would assist in this.

There is also an opportunity for someone in the DNSSEC community to take an inventory of the existing application developer libraries and identify areas that need further development. Are there enhancements that could be made to existing libraries to make them easier to use with DNSSEC? Are there new libraries in other languages that could be created? Are there ways to make the libraries more consistent across languages so that developers can easily work with DNSSEC in multiple languages?

It is worth noting that there has been some ongoing work[7] within the DNSEXT working group of the Internet Engineering Task Force (IETF) to standardize an application programming interface (API) for DNSSEC. The proposed API would allow applications to communicate with the local DNS resolver to control the DNSSEC validation process and obtain validation results. If this proposal moves forward within the IETF it could provide a means to offer a more consistent developer interface for interacting with DNSSEC.

D. *DNSSEC-Aware DNS Resolvers Need To Be More Widely Deployed*

If an end-user had a DNSSEC-aware application or if a developer wanted to make an application DNSSEC-aware, the unfortunate reality is that the vast majority of users would not be able to *use* DNSSEC because of the lack of "DNSSEC-aware" or "DNSSEC-validating" local DNS resolvers.

The issue here is that for DNSSEC to work, the user's application must be able to send out a DNS query and receive back the query along with DNSSEC-related information. Most users typically use the DNS server operated by their Internet Service Provider (ISP) - and most of those DNS servers do not currently support DNSSEC.

Comcast is one of the first cases of widespread DNSSEC deployment within North America. In January 2012 they completed the deployment of DNSSEC-validating DNS servers in their customer-facing infrastructure[8]. Their 17.8 million broadband customers now automatically (and without any customer configuration) receive responses to DNS queries that have been validated with DNSSEC. There are also examples of ISPs validating DNS responses on behalf of their customers in Sweden and some other European countries. With these successful deployments as examples, other large ISPs will hopefully follow.

Without easy access to a DNS resolver that supports DNSSEC, someone seeking to use DNSSEC-related apps or services has these alternatives:

1. Switch the computer's DNS servers to use other public resolvers that support DNSSEC. For instance, the DNS Operations Analysis and Research Center (OARC) operates open DNSSEC-validating resolvers.[9] Additionally, Google's Public DNS servers, while not yet validating DNSSEC will at least forward DNSSEC information so that an application could validate the query[10].

2. Install a local DNSSEC-validating resolver and point the computer to use that resolver. An example would be the DNSSEC-Trigger server developed by NLnet Labs.[11]

3. Use an application that includes its own built-in support for external DNSSEC-validating resolvers. For instance, the CZ.NIC extensions for Google Chrome[2] and Mozilla Firefox[3] include an option to use either the OARC or CZ.NIC DNS servers.

The challenge is that all of these solutions involve extra work on the part of the user and may require a level of technical sophistication in the case of installing a local DNSSEC-validating resolver. As more ISPs follow the Comcast route of deploying DNSSEC-validating resolvers to all customers, DNSSEC-aware applications and services will be able to "just work".

Note that an argument can be made that by relying on a DNSSEC-validating resolver at an ISP there is still the potential that the ISP's resolver could be compromised. Performing the DNSSEC-validation on the local computer can provide the highest level of security. For that to work, though, the upstream DNS resolver at the ISP (or other location) must correctly pass DNSSEC records to the local resolver.

III. DOMAIN NAME HOLDERS

Domain name "holders" are the people or organizations who have registered a domain name and, in the context of DNSSEC, want to sign the domain.

A. Signing a Domain Needs Simplification

The major opportunity to accelerate DNSSEC usage by domain name holders is to look at ways to simplify the process of signing a domain name.

In compiling a list of domain name registrars that support DNSSEC[12], the project team found a wide disparity in the user experience of "signing a domain". As one example of extreme simplicity, the registrar and DNS hosting provider Binero in Sweden simply signs *all* domains hosted (currently only for .SE and .EU) and there is nothing for a user to do. Registro.br in Brazil performs a similar automatic signing service for all .BR domains that they host and directly register. While not that automatic, the registrar GoDaddy has reduced the process down to essentially a single click of a radio button[13]. DNS hosting provider Dyn, Inc. has similarly made the process just a few clicks in its DynECT managed DNS service.[14]

Unfortunately, most registrars today are simply not yet offering DNSSEC services. Or if they do, it is primarily related to accepting Delegation Signer (DS) records or potentially allowing the user to enter self-created DNSSEC records.

For mass adoption of DNSSEC and signing of domains, this step of the process must be made much easier for corporate / government / organization IT staff and individuals to undertake. The automation of signing and key management provided by companies such as Binero, GoDaddy and Dyn, Inc. needs to be expanded to the many other registrars and DNS hosting providers.

It is also obvious that for wider DNSSEC deployment far more registrars and DNS hosting providers need to support DNSSEC. Otherwise domain name holders wishing to sign their domains and have their domains participate in the global chain of trust have to evaluate the effort involved with transferring their domain registration to a registrar who supports DNSSEC. Similarly, they need to evaluate the effort involved in moving the hosting of their DNS records to a DNS hosting provider that supports DNSSEC-signing of domains.

B. Separation Between Registrars And DNS Hosting Providers

Another challenge is that many domain name holders do not fully understand the differences in the function between a domain "registrar" that registers a domain name and a "DNS hosting provider" that may manage the actual DNS records. This confusion is not helped by the fact that many registrars are *also* DNS hosting providers (e.g. GoDaddy.com).

However, the two distinct roles address different aspects of the DNSSEC signing process and both are required to obtain the full value of DNSSEC. The DNS hosting provider hosts all of the domain's DNS records and in the most convenient setting for a domain name holder may handle all the DNSSEC key generation, signing, rollover, etc. The registrar, on the other hand, handles the Delegation Signer (DS) record that ties the holder's signed domain zone into the upper level domains in the global chain of trust.

The issue here is that the two functions may be performed independently and currently may involve a manual step to pass the required data between the two functions.

For example, in the research for the site, the project team noted that Dyn, Inc's DynECT DNS hosting platform handled all the signing of keys, generation of the DS record, etc. The author then needed to copy/paste the relevant information into a DS record at the registrar for the domain - even if the domain was hosted at Dyn's own DynDNS registrar. The process was not difficult but did involve a series of steps to complete.[13]

This is clearly an area where there is an opportunity to greatly simplify the user experience..

C. Simpler Process for Self-Hosted DNS Servers

The good news for people who operate their own DNS server is that there is plenty of documentation out there around how to configure DNSSEC for whatever DNS server they use. There are also sites like the DNSSEC-Tools project[16] that provide tools to assist in the process and software like OpenDNSSEC[17] that can automate a significant portion of the process. The other good news is that very often network administrators who operate their own DNS servers typically have the technical background to work through the steps required to sign a zone and publish the records.

The process *does*, though, still involve a number of steps and is an area where further automation could greatly assist the process.

D. Complexity of Modern Websites

Finally for domain holders, the reality of how companies, governments and organizations actually deploy websites and services in 2012 adds complexity to the DNSSEC-signing process. Specifically, many entities do not host their own web servers on their own network but rather use web hosting providers located somewhere on the Internet.

Additionally, an organization may no longer have simply a single website, but may have an entire series of different websites each of which may be hosted on separate services or may be hosted on a common platform that may or may not be operated by the organization itself. As an example, companies may establish external "micro-sites" consisting of a few landing pages to be used as part of marketing campaigns. There are any number of startups out there that will host these websites for companies.

Similarly many organizations have moved their email services from their own network to a hosted email provider. Many vendors, both large and small, are now offering "cloud" services that allow for the outsourcing of network infrastructure and services while maintaining the "brand" - and domain name - of the entity contracting for those services.

Most of these new services may be very compatible with DNSSEC as they require no substantial changes to DNS and may simply involve new A, AAAA, MX or SRV records added to the zone file. The zone file can still be signed with DNSSEC in the normal manner.

Other services, though, may introduce complications to the DNSSEC signing process. Three examples are given below.

1) CNAME Usage

A particular concern for online content providers is the widespread usage of a CNAME record to map a domain name to a web hosting provider. Typically when you sign up with a web hosting provider the instructions involve adding a CNAME to your domain pointing "www" (or whatever the chosen subdomain is) over to a domain name at the web hosting provider. The web server then routes an incoming HTTP request to the appropriate hosted website based on the requested domain name. For example, WordPress.com instructs users to create a DNS record similar to this[18]:

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

The issue from a DNSSEC perspective is that while the holder can sign their own zone file, including the CNAME record, when the DNSSEC-validating resolver or other application goes down the chain of trust and hits the CNAME it must then go through the DNSSEC validation process for this second domain.

And if, as is common right now, the web hosting provider does not support DNSSEC, then the holder's website will not be able to be validated as fully signed. The chain of trust will break as soon as it hits the CNAME pointing to the unsigned domain.

Until the web hosting providers are fully signed with DNSSEC, all the domains that use CNAMEs to point to those web hosting providers will not be able to provide a complete DNSSEC-signed domain.

2) Web Hosting Providers Who Also Provide DNS Hosting

Rather than mapping a subdomain to a web hosting provider, some domain holders choose to move their complete online presence to a hosting provider and in doing so turn the management of DNS records over to the hosting provider as well. For example, WordPress.com, host of literally millions of websites, provides very easy instructions[19] for changing a domain's name servers and is used in this manner by many sites including large media sites such as TechCrunch.com.

The issue here is that the domain holder's web hosting provider is now their DNS hosting provider and, as mentioned previously, needs to support DNSSEC in order for the domain to be signed. Given that many web hosting providers are focused more on the web hosting than DNS hosting, they may or may not be planning to make DNSSEC available.

3) Content Delivery Networks (CDNs)

To speed up access to their online content, many organizations make use of "content delivery networks" (CDNs), also sometimes called "content distribution networks." These CDNs cache an organization's online content in their global network and make it available to end-users through "edge servers" that are close to the users on the network.

The concern from a DNSSEC perspective is that a CDN needs to control the DNS records for a domain in order to route end-users to the appropriate edge server to get the content.

Therefore, just as with a web hosting provider mentioned earlier, the CDN needs to support DNSSEC within its infrastructure. One of the largest CDNs, Akamai, started promoting DNSSEC in 2010 complete with fully automated signing as part of its Enhanced DNS services[20]. At an ICANN workshop in March 2011 an Akamai representative provided a progress report and noted the need for further education of the larger industry on the benefits of DNSSEC[21].

This type of effort needs to be encouraged within other CDN providers as their deployment of DNSSEC will then enable all domains making use of those services to sign their domains.

IV. Domain Name Infrastructure Operators

Domain name "infrastructure operators" are people or organizations that provide the actual service behind the Domain Name System and have a role to play in the DNSSEC signing and validation processes. Examples include domain name registries, domain name registrars, DNS hosting providers and at a base level the Internet Service Providers (ISPs) that provide local DNS resolvers. People or

organizations that operate their own DNS servers and host their own domains also fall into this category in addition to being domain name holders.

A. Awareness of DNSSEC Operational Guidelines

The DNSSEC community to date has developed a significant amount of documentation around guidelines for deploying and operating a DNSSEC environment. Documents such as RFC 4641bis[22] capture the experiences and recommendations of early adopters at a network operator and zone administrator level. Other documents such as the "DNSSEC Policy & Practice Statement Framework"[23] concisely outline questions that a domain name infrastructure operator needs to consider. Multiple examples of such policy statements can be found online in various formats[24][25][26].

Many infrastructure operators, however, are simply not aware of these documents. Additionally, when operators do see these documents they immediately become concerned about the complexity of properly implementing the processes around DNSSEC.

There exists a need for more tutorial-level documentation that can help domain name infrastructure operators understand the steps they need to move through to get involved with DNSSEC.

B. Complex Setup Process

To implement large-scale signing of domains or to provide a very automated end-user experience is not a trivial process to set up. One domain registrar contacted by the author indicated it was not on their plans anytime soon because the process was viewed as far too complex. Tools such as OpenDNSSEC[17] can greatly assist with that process, but in many cases domain name infrastructure operators are not yet aware of these tools.

C. Key Rollover Process

The key rollover process, particularly with the Key Signing Key (KSK), is an area where domain name infrastructure providers need to pay careful attention. The KSK is typically valid for a longer time period (often a year) and so there is a greater potential that people will not be familiar with the KSK rollover process given the infrequent usage.

In January 2012 a live example of the potential issue was given when administrators for the NASA.gov domain made an error in the KSK rollover process that resulted in the domain not having a valid DNSSEC signature tied into the chain of trust. Comcast's DNSSEC-validating DNS servers, upon encountering this error, proceeded to block access to the NASA.gov domain for Comcast's 17.8 million customers. While the situation was quickly remedied, the blockage of NASA's website did create a public relations challenge for Comcast. Comcast's DNS Engineering team wrote up a detailed analysis[27] of exactly what went wrong, how they attempted to mitigate the issue and how it was ultimately resolved.

As DNSSEC becomes more widely deployed this is an area where the project team expects to see greater automation and extension of operational practices to address these key rollover issues.

D. Communication Between Registrar and DNS Hosting Functions

As mentioned previously, in current operations where a domain name holder engages with a registrar or DNS hosting provider to sign a domain, there exists this issue of communicating the DS record from the DNS hosting provider to the domain name registrar. In many cases, the author found that DNS hosting providers made it very easy to obtain the required information to enter a DS record with a registrar. Similarly, the author found that many registrars provided an easy web interface to enter DS records.

The issue right now is that the domain name holder generally must manually copy and paste the required information from the DNS hosting provider's web interface over to the web interface of the domain registrar. As noted previously, this can be the case even if the same company provides both functions. Alternative methods are being explored. The author found one registrar who provided a web-based API for communication of DS records[28].

This is an area where the author expects to see increased automation as domain name infrastructure operators become aware of the issue and as examples of a simplified user experience become widely known.

V. Additional Opportunities

Outside of the technical and process issues outlined above for domain name consumers, holders and infrastructure operators, the author and project staff identified another area where education can greatly assist DNSSEC deployment.

In the research for the site the author found that the larger industry has a lack of understanding about the value that DNSSEC brings:

- *why* should a company, network operator or anyone else go through the effort of deploying DNSSEC?

Much of the messaging around DNSSEC outside the DNSSEC community to date has made statements such as that "DNS wasn't built with security in mind" and that DNSSEC addresses the issues. But what does that simple statement mean to a corporate or government IT manager? What are the actual threats? What is the security risk to an organization? Some of the messaging talks of "cache poisoning" and "spoofing", but again it is not necessarily clear to an IT manager how direct these concerns are to his or her domain names and infrastructure.

This is particularly true given that there is now extremely widespread usage and understanding of SSL/TLS. People are confused by the difference between SSL and DNSSEC. Comments the author heard in discussions included:

- "I already have SSL securing the connection to my site, why do I need DNSSEC?"
- "People will see a warning if my SSL certificate isn't there. What will DNSSEC do to help?"
- "Given that SSL encrypts the connection and DNSSEC doesn't, why should I bother?"

There seems to be a lack of understanding of how SSL/TLS and DNSSEC can complement each other to provide a much higher level of security.

This also goes to the user experience. End-users now understand that their web connection is "secure" if they see a lock icon in their browser window. They may even understand that if their browser bar is green that means the site is even more secure (courtesy of an Extended Validation Certificate).

Users and IT personnel already believe they have a "secure" web experience and therefore feel little or no urgency to consider something like DNSSEC.

The opportunity, then, for the industry is to more clearly communicate the very real benefits and opportunities that are enabled by DNSSEC. With regard to SSL, people need to understand the different roles played by DNSSEC and SSL and how they can complement each other to provide a significantly more secure environment.

Beyond SSL, people need to understand the benefits of what DNSSEC can offer in terms of providing a more secure infrastructure and in further enabling innovation.

For instance the DANE working group within the IETF[29] is developing ways in which DNSSEC can enable DNS to effectively work as a global public key infrastructure (PKI). This work will provide a way for enterprises and organizations to not only provide an additional layer of security for traditional certificates issued by Certificate Authorities (CAs) but also will provide a way for entities to securely use certificates they issue themselves without a CA and entirely under their own control. The opportunity here is for companies and organizations to more rapidly innovate and provide new and more secure services.

Similarly, there are opportunities where DNSSEC can enable more secure usage of email, instant messaging, voice-over IP (VoIP) and other forms of real-time communications.

Wider communication within the larger industry of these opportunities for innovation enabled by DNSSEC and the benefits that DNSSEC can provide for a more secure infrastructure will help companies understand the value and benefits of deploying DNSSEC.

VI. Conclusions

The opportunities and challenges identified in this paper are typical of a technology that is in the early stages of wide deployment. Further educational materials, tutorials and other content to help domain name consumers, holders and infrastructure operators may potentially overcome many of these challenges. Other challenges may be addressed as deployment tools mature and greater levels of automation are introduced.

A somewhat larger challenge with the deployment of DNSSEC is the proverbial "chicken and egg" situation. In conversations, project staff found that application developers and some infrastructure operators were reluctant to spend any effort on DNSSEC as so few domains have been actually signed – while on the opposite end domain holders saw little value in signing their domains as there are very few actual consumers of DNSSEC validation.

It also became clear to the project staff during the site development that the benefits and opportunities of using DNSSEC do need to be made more understandable to those outside the DNSSEC community. Many people within the wider industry are still very unfamiliar with what DNSSEC is – and even more so with the very real value it can bring.

Over the course of 2012, the Internet Society Deploy360 Programme will address the opportunities and challenges documented in this paper and assist in accelerating the deployment of DNSSEC. This effort will involve not only the project website, but also regional deployment-focused conferences, speaking at various industry events and continuous outreach through social media and other online tools.

The project staff expects that through this continued effort additional challenges and opportunities for DNSSEC deployment will be identified and further progress reports such as this will be produced for DNSSEC community events. The author and the rest of the project staff look forward to working with the larger DNSSEC community to further accelerate the deployment and bring about a more secure Internet.

References

[1] Internet Society, “Deploy360 Programme." [Online]. Available: http://www.internetsociety.org/deploy360/

[2] Internet Society Deploy360 Programme, "How To Add DNSSEC Support to Google Chrome." [Online]. Available: http://www.internetsociety.org/deploy360/resources/how-to-add-dnssec-support-to-google-chrome/

[3] Internet Society Deploy360 Programme, "How To Add DNSSEC Support to Mozilla Firefox." [Online]. Available: http://www.internetsociety.org/deploy360/resources/how-to-add-dnssec-support-to-mozilla-firefox/

[4] W Hardaker and S Krishnaswamy, "Enabling DNSSEC in Open Source Applications," SATIN 2011. [Online.] Available: http://conferences.npl.co.uk/satin/papers/satin2011-Hardaker.pdf

[5] Internet Society Deploy360 Programme, "What is the correct 'user experience' for DNSSEC in a web browser?" [Online]. Available: http://www.internetsociety.org/deploy360/blog/2012/01/what-is-the-correct-user-experience-for-dnssec-in-a-web-browser/

[6] Internet Society Deploy360 Programme, "DNSSEC Developer Libraries" [Online]. Available: http://www.internetsociety.org/deploy360/resources/dnssec-developer-libraries/

[7] S. Krishnaswamy and A. Hayatnagarkar, "DNSSEC Validator API" [Online.] Available: http://tools.ietf.org/html/draft-hayatnagarkar-dnsext-validator-api

[8] Internet Society Deploy360 Programme, "Comcast Gives 17.8M Customers Access to DNSSEC Validating DNS Servers" [Online.] Available: http://www.internetsociety.org/deploy360/blog/2012/01/comcast-gives-17-8m-customers-access-to-dnssec-validating-dns-servers/

[9] Domain Name System Operations Analysis and Research Center (DNS-OARC), "OARC's Open DNSSEC Validating Resolver" [Online.] Available: https://www.dns-oarc.net/oarc/services/odvr

[10] Google, Inc., "Google Public DNS – Frequently Asked Questions" [Online.] Available: http://code.google.com/speed/public-dns/faq.html#dnssec

[11] NLnet Labs, "DNSSEC-Trigger" [Online.] Available: http://nlnetlabs.nl/projects/dnssec-trigger/

[12] Internet Society Deploy360 Programme, "How To Sign And Secure Your Domain With DNSSEC Using Domain Registrars" [Online]. Available: http://www.internetsociety.org/deploy360/resources/dnssec-registrars/

[13] Internet Society Deploy360 Programme, "How To Sign Your Domain With DNSSEC Using GoDaddy.com" [Online]. Available: http://www.internetsociety.org/deploy360/resources/how-to-sign-your-domain-with-dnssec-using-godaddy-com/

[14] Internet Society Deploy360 Programme, "How To Sign Your Domain with DNSSEC Using Dyn, Inc" [Online]. Available: http://www.internetsociety.org/deploy360/resources/how-to-sign-your-domain-with-dnssec-using-dyn-inc/

[15] Internet Society Deploy360 Programme, "Step-By-Step: How To Use A DNSSEC DS Record To Link a Registrar to a DNS Hosting Provider" [Online]. Available: http://www.internetsociety.org/deploy360/resources/step-by-step-how-to-use-a-dnssec-ds-record-to-link-a-registar-to-a-dns-hosting-provider/

[16] DNSSEC-Tools Project. [Online.] Available: http://www.dnssec-tools.org/

[17] OpenDNSSEC Project [Online.] Available: http://www.opendnssec.org/

[18] WordPress.com, "Domain Mapping – Map A Subdomain" [Online.] Available: http://en.support.wordpress.com/domain-mapping/map-subdomain/

[19] WordPress.com, "Domain Mapping – Map An Existing Domain" [Online.] Available: http://en.support.wordpress.com/domain-mapping/map-existing-domain/

[20] Akamai Technologies, Inc., "Akamai Enhanced DNS" [Online.] Available: http://www.akamai.com/html/technology/products/enhanced_dns.html

[21] D. Lawrence, "DNSSEC at Akamai Technologies," ICANN Silicon Valley DNSSEC Workshop, March 2011. [Online.] Available: http://svsf40.icann.org/meetings/siliconvalley2011/presentation-dnssec-akamai-16mar11-en.pdf

[22] O. Kolkman and W. Mekking, "DNSSEC Operational Practices, Version 2," proposed updates to RFC 4641. [Online]. Available: http://tools.ietf.org/html/draft-ietf-dnsop-rfc4641bis

[23] F. Ljunggren, A-M. Eklund-Lowinder and T. Okubo, "DNSSEC Policy & Practice Statement Framework" [Online.] Available: http://tools.ietf.org/html/draft-ietf-dnsop-dnssec-dps-framework

[24] Internet Infrastructure Foundation, "DNSSEC Practice Statement (DPS)" [Online.] Available: https://www.iis.se/docs/se-dnssec-dps-eng.pdf

[25] RIPE NCC, "DNSSEC Policy and Practice Statement" [Online.] Available: http://www.ripe.net/data-tools/dns/dnssec/dnssec-policy-and-practice-statement

[26] F. Ljunggren, T. Okubo, R.Lamb and J.Schlyter, "DNSSEC Practice Statement for the Root Zone KSK Operator" [Online.] Available: http://www.root-dnssec.org/wp-content/uploads/2010/06/icann-dps-00.txt

[27] Internet Society Deploy360 Programme, "Comcast Releases Detailed Analysis of NASA.gov DNSSEC Validation Failure" [Online.] Available: http://www.internetsociety.org/deploy360/blog/2012/01/comcast-releases-detailed-analysis-of-nasa-gov-dnssec-validation-failure/

[28] GKG.net, "DNSSEC Delegation Signer Webservice API" [Online.] Available: http://www.gkg.net/ws/ds.html

[29] DNS-based Authentication of Named Entities (dane) Working Group, Internet Engineering Task Force. [Online.] Available: https://datatracker.ietf.org/wg/dane/charter/