DNSSEC Roadmap

Prepared for:
Department of Homeland Security
DNSSEC Deployment Initiative

Prepared by:
Shinkuro Inc.
February 13, 2013

Version 21

Table of Contents

List of Appendices

List of Figures

List of Tables

1 Executive Summary

Since its inception, the DHS DNSSEC Deployment Initiative has served a vital role in determining and developing the critical tools, technologies and partnerships that have been the springboard for the successes in DNSSEC adoption to date. The state of that adoption is explained in greater detail in Section 2 and beyond, but for readers who are already familiar with the complex DNSSEC landscape, below are the top five priorities for the Initiative to reach its goal—*for all zones to be signed and all DNS queries to be checked*. This is followed by a high-level summary of what remains to be done and, if Initiative action is appropriate, how the Initiative will promote DNSSEC adoption, arranged by strategic areas of focus.

Top Priorities

- Develop tools that enable mass signing of zones
- Develop tools that will help reduce occurrences of common DNSSEC provisioning errors, and reduce the time to recover from any errors
- Increase registrar support for DNSSEC, and make it easy for users to request and enable DNSSEC support for their zones
- Persuade ISPs to increase support for DNSSEC by either fully validating or, at a minimum, being DNSSEC-aware but non-validating
- Identify a standard set of fallback techniques that would enable DNSSEC validation software to work around certain error conditions that currently make adding DNSSEC support within certain end-applications prohibitive

Persuade

- Registrars and DNS hosting providers to sign customers' zones *en masse* and pass their DNSSEC information through to registries, perhaps with the help of an incentive system such as has been used by the .se and .nl ccTLDs
- Developers of desktop and mobile operating systems, Web and mail browsers, and hosting services of the benefits of building DNSSEC signing and validation capabilities into their software, hardware and services
- Firewall and router manufacturers that their products must be at least DNSSEC-aware enough to not drop DNSSEC packets, and to deploy DNSSEC-aware resolvers in these devices if they contain resolvers within them
- ISPs to *at a minimum* offer support for queries of signed records and for DNSSEC key records via a DNSSEC-aware resolver, and set a roadmap for additional levels of service, including full validation at the ISP level
- Fortune 500 companies to require their supplier networks to sign and validate their zones

Develop

- Tools that facilitate DNSSEC signing and validation for registries, registrars and network operators
- Methods to help operators determine and plan for any DNSSEC-associated increases in memory and/or bandwidth usage within their environments

- DNSSEC-capable end-user products for individuals and organizations that perform validation *and* accommodate the applications that will depend on that validation
- A demonstration project for the DANE protocol, which will govern applications built on top of DNSSEC capabilities
- Best practices for DNSSEC adoption geared toward U.S. government and private-sector CIOs
- Demonstration scenarios showing attacks on various targets (corporate LAN, home network, bank Web site) and the use of DNSSEC as a remedy

Coordinate

- Among U.S. government agencies, federal contractors, business enterprises, associations and trade groups, private-sector players, and Internet governing bodies to require DNSSEC signing and validation as a default
- With registrars, registries and associations endorsing DNSSEC deployment to eliminate redundancies and to work in unison to accelerate adoption
- With the Internet Society's Deploy360 Programme, which has agreed to play a lead role in raising public and organizational awareness of the need for DNSSEC

Engage

- With developers regarding the possible types of new, secure applications that DNSSEC enables
- In U.S. government, private-sector and Internet governance working groups to produce new rules and RR types that ease DNSSEC adoption and pave the way for the applications that will be built on top of it

Determine

- Accurate figures for DNSSEC uptake in both public- and private-sector zones, and establish deployment benchmarks
- Accurate figures for DNSSEC impact on network bandwidth, CPU and memory utilization for servers and validating resolvers, and network latency for different deployment scenarios

Educate

- ISPs on the benefits of enabling DNSSEC validation and the practicality of doing so, as evidenced by the successful deployment of DNSSEC by large ISPs
- Developers and others about the ecosystem of beneficial applications that can be built on top of DNSSEC-secured networks, which are not currently possible without it
- Major ISPs, trade associations, critical infrastructure enterprises (e.g. banks), and others on the importance of securing their own domain name, how to get their zones signed, and how to validate access

2 Overview

This Roadmap's goal is to show the steps that can be taken globally to further DNSSEC signing and validation and detail those areas in which the Department of Homeland Security and the DNSSEC Deployment Initiative can be most effective in furthering DNSSEC adoption.

DNSSEC adoption has begun but is far from complete. The growing interest and information available today through Internet and information technology (IT) security associations and groups to assist in outreach signals positive momentum; with the Initiative's strategic guidance and coordination, DNSSEC adoption will eventually predominate and secure the DNS for substantially all online communications, protecting against attacks at the DNS level as a complement to efforts to secure other layers of the Internet Protocol (IP) stack.

Since its inception in 2004, the DNSSEC Deployment Initiative has achieved significant progress toward its original and continued primary goal of having all Domain Name System (DNS) entries signed and all DNS requests validated.

The landscape of DNS Security Extensions (DNSSEC) adoption has evolved from the last DNSSEC Roadmap publication in 2007, when neither the root nor the major top-level domains (TLDs) were signed and very few large enterprises had signed their domains. At that time, validation was almost non-existent in either the public or private sectors, and the question most frequently heard about DNSSEC was "Why?"

Today, the root and major TLDs have been cryptographically signed; the U.S. federal government mandates signing for its agencies' domains and is expected to mandate validation; and a small but growing number of Fortune 500 companies either have adopted or plan to adopt DNSSEC in their zones' operations.

(Please see Appendices 1 and 2 for explanations of the DNS and DNSSEC, respectively.)

As the number of DNSSEC deployments has steadily grown in both government and enterprise, "Why?" is giving way to the more practical "How?" and "When?"

These events signal two tipping points, the first of which has already occurred: the point at which DNSSEC signing becomes the workaday norm for government zones rather than the exception. Roughly 57 percent of .gov zones have been signed, and new Federal Information Security Management Act (FISMA) requirements will shortly mandate validation as well. These two factors provide an opportunity for the Initiative's portfolio of .gov work to expand from persuading zones to sign to providing aid in both signing *and* validating .gov zones. DNSSEC signing is rapidly becoming the norm for the U.S. government, and validation is expected to follow.

However, the second tipping point—where DNSSEC adoption is the norm for enterprises as well—has not yet been reached. The Initiative has begun to uncover

strategically important enterprises and non-government organizations (NGOs) to partner with that are starting to focus on DNSSEC deployment in the private sector, such as the Internet Society and its Deploy360 Programme. However, to build this initial enthusiasm into true momentum warrants a continued but separate drive to bring DNSSEC security to this largest sector of the U.S. economy.

The Initiative will also emphasize DNSSEC validation more than in past efforts. While there has been significant progress in persuading operators to *sign* their zones, the *validation* side of the equation is only just beginning in both the public and private sectors. There are examples in other countries, such as Sweden, where all fixed-access providers (FTTH, cable, DSL) validate, as do all mobile providers, whether 2G, 3G or 4G, showing that large-scale validation by all major access providers is possible. (All of Sweden's large combined registrar/DNS hosting providers sign customers' zones, including the largest, TeliaSonera).

At the individual level, it has only recently become possible for end users to request that Internet service providers (ISPs) perform validation on their behalf, let alone possible for them to perform such validation on their own.

Because the challenges and opportunities surrounding validation differ from those surrounding signing, this Roadmap is really an entwinement of two distinct roadmaps, one outlining efforts and plans to increase signing in enterprise zones and the remaining unsigned .gov zones, and the other covering progress in validating relative to four successively more aggressive objectives:

- Validation by ISPs
- Validation at the edge of the enterprise
- Validation by end-user systems
- The emergence of the ecosystem of DNSSEC-aware applications that will develop as DNSSEC becomes nearly ubiquitous, especially on mobile platforms

2.1 Dept. of Homeland Security (DHS) Leadership in the Deployment Initiative

The DHS role in the DNSSEC Deployment Initiative is broad and deep. DHS:

- Works to promote U.S. domestic coordination in matters relating to DNSSEC deployment and maintenance
- Cultivates in-house expertise on DNSSEC within the federal government, smoothing the way for the imminent requirement to validate in the .gov zone
- Proposes draft regulations within the U.S. government
- Sponsors work on technical issues related to zone transfer, the timing of key rollover, and

The Signing of the Root
The signing of the root zone at two sites, one each in Virginia and California, was accomplished in a manner that combined extraordinary documentation and publicity with security levels normally reserved for nuclear launch codes or presidential visits. You can see annotated scripts for the ceremony (one nearly 200 pages long) as well as video and other documentation at https://www.iana.org/dnssec/ by following the link for "KSK Ceremony Materials".

other technical considerations
- Is an "ambassador" fostering international cooperation on DNSSEC adoption worldwide
- Leads workshops and tutorials relating to DNSSEC
- Contracts the development of tools that aid both U.S. government agencies and other DNS operators in adopting DNSSEC

In the private sector, DHS seeks to influence early adopters to become the leading edge of enterprise adoption of DNSSEC, then to ensure that DNSSEC deployment becomes standard practice for the proper operation of an enterprise's network presence. Success is defined as the point at which IT-security auditors check for the presence of DNSSEC signing and validation as a matter of course, and where DNS operators act on the idea that good DNS security is vital to their network's, and their brand's, health.

The Initiative is, however, beginning to consider measures of effectiveness (MOEs) by which to benchmark its progress. For example, specific, relevant metrics must be devised to measure:

Table 1: Most important DNSSEC-related metrics

Metric	Estimated Years to Tipping Point
Number of enterprises with signed zones	5
Registrars supporting DNSSEC	2–3
ISPs operating B- or A-level resolvers*	5

* Please see Table 4 below.

The "Estimated Years to Tipping Point" column is a rough guess as to how long it will take before these items will become accepted standard practice.

2.2 Landscape of the DNSSEC Deployment Effort

At first glance, the large numbers of players involved at different areas in the DNSSEC landscape, and the deployment effort's relatively long timeline, make it appear quite complex. However, this complexity can be reduced to a model with just a few "layers," and it is through this lens that we examine the future of DNSSEC deployment efforts.

The DNSSEC ecosystem of players, protocols and products is divided into five groupings according to the following criteria (note that some items may overlap layers since they perform more than one function):

Tools and implementations are programs that perform discrete, important tasks related to signing or validation but are not themselves stand-alone systems. These are intended for developers and others with deep technical expertise, to be connected and bundled into larger, user-oriented systems.

Products and services are defined as bundles of tools and implementations that have been packaged in such a way—i.e. with user interfaces and some integration of their

actions—as to be usable by less technically skilled operators to enable and maintain DNSSEC operations.

Documents and regulations include legislation, governmental and non-governmental regulations, protocol standard specifications, and background and best-practice documents that combine to form the space of what is possible in deploying and operating a DNSSEC-enabled system. Documents and regulations increasingly mold what is normal or accepted practice as DNSSEC deployments tend to converge toward or adopt standards; they tend to define the opportunities and boundaries of the DNSSEC ecosystem rather than to push technological development. They may be geared toward policymakers, programmers, DNS operators, or other audiences.

Deployment and operations include hardware, software and practices that ease DNSSEC deployment and operations and maximize DNSSEC's utility to operators of registries, registrars and ISPs. The "deployment" part of this layer includes decision-making, planning and resources, while the "operational" side includes performance monitoring, re-signing, and other aspects related to the smooth functioning of DNSSEC. These items are largely geared toward programmers and operators.

Applications are tools and products that can be built on top of a system that has largely adopted DNSSEC, and that thus can rely on DNSSEC signing and validation. These can include new types of email and credentialing systems that rely on an identity established via DNSSEC-secured records, enabling the DNS to become a repository for trusted information. These items are intended for use either by end users or system administrators to take advantage of the increased level of trust that DNSSEC enables.

These five groupings are arranged as layers in a chart in which audience size (or user base) increases from the bottom layer to the top layer. In other words, the activities and products in the bottom layer are useful almost exclusively to programmers and IT-security experts, while those in the top layer are turnkey products usable by system administrators and end users.

In addition, discussion of each grouping is also divided into a signing side having to do with technologies for establishing DNSSEC resource records (RRs) with the appropriate registry, and a validation side discussing items that help to cryptographically check DNSSEC signatures.

These layers and sides of DNSSEC deployment can be visualized as follows. Note that the lower layers are most relevant to and have the most benefit for programmers; that registries and registrars tend to develop and derive benefit from items in the two middle layers; and that end users will tend to only be concerned about (and benefit from) the topmost layer:

Figure 1: The five "layers" of the DNSSEC landscape

As stated above, each layer contains both signing and validation components, given that the two are separate activities that can be conducted independently, although the goal is to have every zone signed and every lookup validated.

On both the signing and validation sides, the first layer consists of DNSSEC Tools & Implementations that can be embedded in products and software. These are useful component parts that do not form usable products on their own, but are necessary for the creation of products that do stand on their own.

The second layer has two parallel sections, which are duplicated on both the signing and validation sides:

- DNSSEC Products & Services that are typically used by registrars and registries to enable and maintain DNSSEC operations
- Documents & Regulations affecting DNSSEC deployment, including U.S. government mandates, rules set by Internet standards bodies, messaging advocating deployment, and tutorials, manuals, and best-practices documents that ease and smooth deployment and operation

Documents & Regulations do not depend on lower-level technologies and so are visualized at the same level as, but to one side of, DNSSEC Products & Services.

These first two layers feed into a third layer, Deployment & Operations, which is concerned with the deployment and maintenance of DNSSEC functions, both in the U.S. and internationally.

Finally, there is a fourth, currently developing layer of Applications that is being built on top of DNSSEC and that contributes to an emerging public-key infrastructure (PKI). The discussion of these applications represents what will become possible once DNSSEC is

widely deployed and end-user validation is common; widespread signing by ISPs and validation by end users is a given for their use.

In the pages to follow we will address facets of each of the layers above and how they contribute to the overall picture for the signing and validation sides of DNSSEC deployment.

3 First Layer: DNSSEC Tools & Implementations

Figure 2: Tools & Implementations layer highlighted within the DNSSEC landscape

At the outset of this Roadmap's description of the DNSSEC landscape we believe it is helpful to list vendors' and other organizations' known DNSSEC-capable authoritative nameservers and recursive resolvers, partially as a demonstration of how far DNSSEC deployment has come.

Table 2: Known authoritative nameservers and recursive resolvers

Vendor/Developer	Authoritative Nameserver	Recursive Resolver
BT Diamond	IPControl	IPControl
Cisco	--	Prime Network Registrar (utilizes Unbound)
cz.nic	knot-dns	---
EURid	Yadifa	---
F5	Big-IP Global Traffic Manager[1]	
Infoblox	Infoblox	Infoblox
ISC	BIND	BIND
Microsoft	Windows Server 2012	---
NLnet Labs	NSD	Unbound
Nominum	Nominum ANS	Vantio Caching Platform
PowerDNS	PowerDNS Authoritative Server	---
Secure64	DNS Authority	DNS Cache
Verisign	ATLAS[2]	---

[1] This is a load balancer to be used in front of either an authoritative nameserver or recursive resolver.
[2] Available as a service for Verisign customers rather than as a software or software/hardware implementation

3.1 Signing Side

3.1.1 Tools

In providing greater security for those who adopt it, DNSSEC introduces an additional layer of complexity to DNS transactions. Tools are available that help address that complexity, and can be used to create, check or automate various aspects of the DNSSEC signing process. They tend to perform highly specific tasks, and are best thought of as stand-alone modules that can be combined into more complex products that help get a zone signed and keep it signed.

Signing-side DNSSEC tools perform tasks such as the following:

- Automate "rolling" of keys
- Check for expired DNSSEC signatures
- Check public nameservers for DNSSEC metadata
- Check syntax of signed zone files
- Generate and distribute keys
- Sign DNS zone files
- Solve misconfigurations/inconsistencies
- Test zone contents against best practices and overall security
- Verify signatures for cryptographic validity

See also Appendix 3, "Lists of Tools & Implementations," for partial lists of exemplary tools that developers (both DHS-funded and not) have created for deployment and for ongoing operations. They are important components for creating DNSSEC products usable by a wider constituency at registrars, content delivery networks (CDNs), ISPs, and others involved in DNSSEC signing efforts. In addition, an even more extensive list is currently available at https://www.dnssec-deployment.org/wiki/index.php/Tools_and_Resources.

Note however that more tools and more classes of tools are needed to facilitate DNSSEC adoption, including to:

- Support the signing of large numbers of domains to encourage name-server operators—typically registrars—to sign large numbers of zones at once
- Help those adopting DNSSEC for their zones ("registrants") check their domains' DNS and DNSSEC status as well as that of their parent zone
- Aid third-party monitoring to ensure DNS and DNSSEC integrity (e.g. further tools such as .se's dnscheck, which lets both the registrant and the party signing the zone check its DNSSEC status even before the zone is delegated)
- Distribute (publish) keys from child zone to parent zone

3.1.2 DNS Servers

There has been progress in this area because the major DNS-server offerings—including BIND, NSD and Unbound—now incorporate DNSSEC into their operation. Importantly, these products are themselves being incorporated into other, more complex software, signaling that software developers view DNSSEC as more than an end in

itself, but as the basis for other products that require high security at a low level in the IP stack (see discussion in Section 4, "Second Layer: DNSSEC Products & Services," below).

3.2 Validation Side

3.2.1 Tools

Please see Appendix 3 for a partial list of tools and implementations that developers have promulgated for troubleshooting validation.

3.2.2 Validation Libraries

Please see Appendix 3 for a partial list of software libraries that developers can use to perform DNSSEC validation.

3.2.3 Browsers

Since users access Web pages through browsers, those browsers ought to be able to benefit from DNSSEC validation. However, developers of browsers (e.g. Apple's Safari, Microsoft's Internet Explorer, Mozilla's Firefox, Opera Software's Opera) have taken few steps to integrate DNSSEC into their products' operation to complement the Secure Sockets Layer (SSL) technology that secures Web-based communication at the browser level. This may be because developers believe DNSSEC validation adversely affects browser performance by slowing page-loading speed—a major discriminator and market factor.

However, some browser developers currently advocate third-party, non-operating-system add-ons to provide DNSSEC protection[3] (something we believe is not as effective as validation of all queries), while others believe DNSSEC validation is something that must be incorporated into operating systems, not browsers.[4]

Potential first steps in an effort to persuade U.S. and international browser developers to adopt DNSSEC include the creation of practical pro-DNSSEC arguments targeted at them, along with associated lobbying. This effort can be expected to take between months and years, even given that browser-development cycles are somewhat faster than operating-system development cycles.

3.2.4 Operating Systems

The incorporation of DNSSEC into major operating systems (OSs) will both lighten the computational burden on existing recursive resolvers and nearly eliminate the need for stand-alone applications to handle DNSSEC validation independently. The strongest motivator for DNSSEC incorporation into operating systems, however, is that it shrinks

[3] Such extensions include CZ.NIC's DNSSEC Validator and University of Amsterdam System and Network Engineering Students' Extended DNSSEC Validator (currently at proof-of-concept stage); see "Mozilla" presentation at http://svsf40.icann.org/node/22163. or University of Amsterdam/NLnet PDF at https://www.os3.nl/_media/2010-2011/courses/rp1/p19_presentation.pdf.

[4] In October 2011, Olafur Gudmundsson/Shinkuro related an Opera Software official's remark that the Opera browser will not incorporate DNSSEC for this reason.

the proverbial "last mile" between the component performing validation and the application consuming those results (i.e. to within the local host). This provides a foothold for any application running on the OS that is interested in establishing end-to-end security mechanisms.

Such DNSSEC-enabled operating systems represent a major step forward in making DNSSEC adoption ubiquitous across applications running on the host system, and will enable operating-system vendors and application developers to provide a consistent way of handling DNSSEC-related status and error conditions.

Currently, no commercial OS vendor supports DNSSEC validation in its default distributions. (Some OS vendors distribute a validating caching nameserver in lieu of a system validating library in order to support local DNSSEC validation.) A number of third-party DNSSEC validator libraries exist, most of which are portable across a variety of OS platforms including certain hand-held devices.

Note, however, that the collaborative open-source Fedora Project does include DNSSEC in its distribution of Fedora. Red Hat frequently adopts technologies from Fedora after their use has been proven, and at the time of this writing was incorporating DNSSEC via the use of Unbound in its upcoming release of Red Hat Enterprise Linux.[5]

In addition, some emerging applications will need to fetch and validate DNS records directly. Hence, one of the missing pieces for OS developers is the availability of a standardized DNSSEC application programing interface (API) to allow such applications to act appropriately and securely under a variety of conditions. There is ongoing activity within the DNSSEC community to define and standardize such an API.

3.2.5 Mobile Operating Systems

As end users increasingly communicate and receive information via mobile devices, it will be equally important that mobile OS developers worldwide incorporate DNSSEC into their offerings to ease end-user validation and provide the springboard for the development of an end-to-end DNSSEC-secured Applications space. While NLnet Labs has developed an iOS version of Unbound and tools such as DNSSEC-Nodes and DNSSEC-Check work with Android, our discussions with mobile OS developers indicate that they have generally made very little progress on this front. The Initiative plans to discuss DNSSEC adoption more urgently with these strategically important firms as soon as possible.

[5] Communication of Paul Wouters/Red Hat with Paul Kretkowski/Shinkuro, 15 July 2012.

4 Second Layer: DNSSEC Products & Services

Figure 3: Products & Services layer highlighted within the DNSSEC landscape

Much progress has been made in this area because many developers have produced tools, products and services that ease the adoption of DNSSEC by various actors, although these third-party items may also add complexity to the overall DNS system.

4.1 Signing Side

4.1.1 Managed DNS Services

Several firms provide services that include DNSSEC signing and management for TLDs, registries and their customers. A partial list of these firms is contained in Appendix 3.

4.1.2 DNSSEC Hardware

In addition to numerous smart cards, universal serial bus (USB) tokens, and trusted platform modules, certain hardware products incorporate DNSSEC into their operation either by enabling functions important to DNSSEC (e.g. AEP's Keyper) or functioning as self-contained appliances (e.g., Infoblox). Note however that their interactions, and how they work together with DNSSEC using PKCS#11, require further study.[6] A partial list of these products is contained in Appendix 3.

4.2 Validation Side

4.2.1 Mobile Apps

At the time of this writing the most widely known DNSSEC-validation app is VeriSign's DNSSEC Analyzer, an iPhone and Android app that allows consumers to immediately analyze the DNSSEC status of any site they visit on the Web. While it does not perform validation, it does let users trace a Web site's DNSSEC status, if any, back to the root.

[6] .se commissioned such a study in 2010; the PDF of their consultants' report is available here.

5 Second Layer: Documents & Regulations

This layer represents the advocacy, policies and guidance that go into DNSSEC deployment and operation. On the signing side this includes the laws, regulations, agency mandates, messaging, and standards bodies' directives and protocol specifications that hasten DNSSEC deployment, as well as the manuals, workshops, tutorials, and best-practices documents that enable DNS operators to deploy and operate DNSSEC in their organizations. In particular, the regulatory environment surrounding DNSSEC has improved considerably although it remains a patchwork of mandates and recommendations across both the private and public sectors.

On the validation side are the case studies, messaging, tutorials and best practices that persuade and enable ISPs and, ultimately, end users and applications to perform DNSSEC validation.

Overlaying the Documents & Regulations layer is the need for advocacy, broadly defined—the promotion of DNSSEC through initiating or maintaining a presence at conferences and standards bodies, conducting educational sessions and how-to demonstrations, creating tutorials, and initiating contact with those the Initiative hopes to persuade to play a more active role in adopting DNSSEC.

Figure 4: Documents & Regulations layer highlighted within the DNSSEC landscape

5.1 Signing Side

5.1.1 Progress Overview: U.S Federal Government

In 2008, the Office of Management and Budget (OMB) issued OMB-08-23, mandating that DNSSEC be deployed on all Executive Branch .gov delegations and the .gov top-level domain (TLD) itself.[7] The .gov TLD (operated as a contract from the General

[7] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-23.pdf

Services Administration [GSA]) officially deployed DNSSEC in January 2009 for both the registry and registrar functions.

DNSSEC was first added to the FISMA auditing controls in National Institute for Standards and Technology (NIST) regulation SP 800-53r1. Since then, these controls were modified in NIST SP 800-53r3 to both tighten them and to require DNSSEC signing for all federal information systems. However, validation is still only required for systems identified as "high" impact, according to the Federal Information Processing Standards (FIPS) 199 definition.

To address the slow uptake of deployment within .gov, the Federal Chief Information Officers (CIO) Council has created an interagency "tiger team" to develop a continuous monitoring system (maintained by DHS) to perform weekly checks on DNSSEC deployment within the .gov space. This has led to both an increased rate of adoption and a reduced error rate within signed .gov zones. The tiger team has also produced a report with recommendations and lessons learned about deployment and sent it to the Federal CIO Council; it contains recommendations on how to foster adoption of DNSSEC and encourages DNSSEC deployment in support of other security protocols, such as email validation.

5.1.2 Best Practices, Tutorials and Manuals

To aid agencies in deployment, NIST issued SP 800-81, “Secure Domain Name System Deployment Guide,” which includes guidance on deploying DNSSEC on an enterprise zone.[8] This document was revised in 2010 to include guidance on recent additions to the DNSSEC protocol specifications. In addition, the DHS Federal Network Security (FNS) branch published a DNS reference-architecture document that builds on NIST SP 800-81 to provide a set of architecture recommendations for organizations that want to either set up a DNS deployment or redesign or update an existing DNS infrastructure. Additional documentation in this vein, specifying use cases and best practices for DNSSEC adoption in non-governmental contexts, will be helpful.[9]

DNSSEC Uptake in .gov
The signing of zones within .gov (the U.S. government's zone) has accelerated dramatically since 2008, when OMB-08-23 mandated that agencies do so—from nearly zero to nearly 57 percent in just four years, according to NIST. This rapid pace of adoption is much faster than enterprise adoption but is leavened by the need to increase low levels of validation in the .gov zone. However, validation in .gov is expected to accelerate as well with the publication in February 2012 of NIST SP 800-53r4, which mandates DNSSEC validation as part of agencies' FISMA compliance.

There are other examples of best-practice manuals produced by other ccTLDs; for example, the Internet Engineering Task Force (IETF) DNSSEC Policy & Practice Statement Framework grew directly out of Sweden's experience in setting up the .se ccTLD for DNSSEC and working on developing the root zone DNSSEC practice statement (DPS), and includes a lengthy list of strategic

[8] See http://www.csrc.nist.gov/ or download PDF here.
[9] The 2009 Shinkuro/Sparta document "DNSSEC Operations: Setting the Parameters" (PDF here) is one example of such a document.

and technical questions for domain managers, zone operators and others to answer as they plan for DNSSEC adoption. In addition, the Swedish government provided free consulting time to its governmental name-service operator to motivate it to adopt DNSSEC, and also provided funding for Swedish municipalities to adopt as well under the rationale that DNS security was a vital national interest. The result between 2005 and today is that about 10 percent of the .se zone file has been signed.

In addition, at this writing it appears that DNSSEC Operational Practices, Version 2 will shortly be published as an RFC, making the current relevant guidelines in RFC 4641 obsolete.

Other NGOs have their own DNSSEC adoption initiatives, such as the Internet Society's Deploy360 Programme, and CENTR's effort to arrange workshops, benchmarking and statistics relating to DNSSEC among European ccTLDs. We intend to search for and conduct increased outreach to them to help coordinate their efforts.

5.1.3 What Needs to Happen: U.S. Federal Government

The newest FISMA control, NIST SP 800-53r4, has tightened the validation requirement within .gov, and DNSSEC validation will now be mandatory for all federal information systems that fall under FISMA reporting requirements (see sidebar above). This will be the driver for deploying validating resolvers within the federal DNS community. NIST SP 800-81 will need to be revised again to add guidance and recommendations for deploying validating resolvers in an enterprise, and the Initiative will contribute to this process.

The current policy documentation for the .gov TLD maintained by GSA needs revision to provide a clear, concise set of policy guidelines for DNSSEC deployment within the federal government. The current policy documents for the .gov TLD were produced before the OMB mandate and FISMA controls and do not provide DNSSEC guidance to .gov delegation holders. Examples of the type of guidance needed include specification of approved cryptographic algorithms and key lengths,[10] and of key-management requirements such as key lifetimes and rollover planning. One approach to updating these documents involves adapting relevant language from the IETF's DNSSEC Policy & Practice Statement Framework (mentioned above) to .gov-specific needs.

Finally, with large amounts of government work being outsourced to contractors, federal contracting rules can be interpreted so as to require potential contractors to deploy DNSSEC for security purposes, with FISMA (or in the case of healthcare information, the Health Insurance Portability and Accountability Act or HIPAA) as the underlying justification. (This is not a new approach; note that contractors in the Managed Trusted Internet Protocol Services [MTIPS] program are required to perform DNSSEC validation.) Appropriate language pertaining to this requirement can be inserted into

[10] Some communities are interested in or require the use of cryptographic algorithms other than RSA or ECC. The DNSSEC protocol accommodates other algorithms, e.g. Russian algorithms described in the GOST documents, but there has not been any visible testing of these; such testing is needed.

requests for proposal (RFPs) or relevant contracting documents, and the Initiative will examine how such a requirement can be brought into being.

5.1.4 Progress Overview: Other U.S. and International DNS Rulemakers

Among non-governmental rule-making bodies, the Internet Corporation for Assigned Names and Numbers (ICANN) has made DNSSEC integration a condition for the assignment of any future TLD.[11] ICANN now requires that the would-be registry operator detail how it will deploy DNSSEC on the newly created TLD. This indirectly highlights a problem with existing policies in that none specify or standardize what information registrars must pass on to registries.

The U.S. financial-services industry views DNSSEC as a potential key component for increasing trust in e-commerce and online banking. To this end, the Financial Services Sector Coordinating Committee (FSSCC) has signed a joint Memorandum of Understanding (MOU) with NIST and DHS's science-and-technology division that forms a private-public relationship to foster the deployment of new technologies to aid in building trust online.[12]

DNSSEC has also been deployed internationally at both the ccTLD level and at lower levels of the DNS tree (see dnssec-deployment.org for a map showing the timeline of international adoption since early 2006). Some nations have embraced DNSSEC as the basis for a trusted online infrastructure; for example, Brazil has completely signed subtrees for its financial industry and the Brazilian Judiciary Branch of the State, which operate under the .br ccTLD as b.br and jus.br, respectively.[13]

5.2 Validation Side

5.2.1 Progress Overview: Building on DNSSEC

In 2010, the U.S. government created the National Strategy for Trusted Identity in Cyberspace (NSTIC).[14] Its goal is to address a key shortcoming in efforts to build trust on the Internet, which NSTIC identified as "the online authentication of people and devices," noting that the President's Cyberspace Policy Review had "established trusted identities as a cornerstone of improved cybersecurity." The strategy document is a roadmap to foster public-private cooperation to meet the goal of having "individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation."

Securing the integrity of DNS lookups via DNSSEC is a key component of the global infrastructure needed to build confidence on the Internet in both human and non-human

[11] See requirements guidebook for new generic top-level domains (gTLDs) at http://newgtlds.icann.org/en/applicants/agb.
[12] https://www.fsscc.org/fsscc/reports/2010/FSSCC_DHS_NIST_MOU_12062010.pdf
[13] http://www.registro.br/
[14] http://www.nist.gov/nstic/

entities (i.e. servers and software components), and two initiatives—one from an international NGO and one from the U.S. government—aim to use DNSSEC to generate that confidence.

The IETF's DNS-based Authentication of Named Entities (DANE) Working Group is developing new RR types to store transport-layer security (TLS) certificates as well as policy statements concerning which certificate authority given services use. Its initial goal was to have a means for browsers to obtain TLS certificates via the DNS or provide a means for a browser to get information via the DNS to determine whether a certificate is authentic or not. Since the DNS is protocol-agnostic, this work can be extended to support other applications such as email (e.g. S/MIME),[15] Voice over Internet Protocol (VoIP), and so on. At the time of this writing, work on this specification is complete and the RFC embodying this new resource record (RR) type is ready for implementation. The DANE Working Group is meanwhile switching its focus to S/MIME and to securing other protocols (e.g., Jabber).

The Federal CIO Council tiger team for DNSSEC deployment is also looking at the deployment of various email authentication technologies in .gov, specifically including the Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). SPF authenticates authorized mail servers by publishing their IP addresses, and it can announce a domain's recommended disposition policy for mail received from unauthorized servers. DKIM establishes a responsible identity by associating a distinct, authenticated domain name with a message; it publishes a public key for that domain and signs messages with the associated private key.

In addition, a new specification, DMARC, allows a sender to indicate that their valid emails are protected by SPF and/or DKIM, and tells a receiver what to do if neither of those authentication methods passes for a received message. It also provides a way for the email receiver to report back to a domain owner about messages that contain the domain name in the author's From: field.[16]

All three technologies rely on the DNS for publication, by using specialized TXT RRs. DNSSEC can provide a greater degree of assurance that the domain's information is valid. (Note that the .se ccTLD supported an implementation of DKIM validation using DNSSEC, called OpenDKIM, in 2008; a report on OpenDKIM is available here.)

5.2.2 What Needs to Happen: Building on DNSSEC

As new RR types and protocol extensions are specified to support different applications such as email and Web surfing, guidance documents will need to be updated. The majority of these documents were produced before widespread DNSSEC deployment; for example, NIST Special Publication documents on securing application servers (e.g.

[15] Secure/Multipurpose Internet Mail Extensions

[16] Note that dnssec-tools.org lists tools that are available to add DNSSEC validation to outbound e-mail in both Sendmail and Postfix.

for the Web, email, etc.) must be revised to include guidance on how to use new features with DNS to support a given application protocol.

Documentation and guidance on how to use DNSSEC in applications are needed to aid application developers who do not yet understand the new level of service that DNS with DNSSEC enables. The nature of this guidance in turn depends on the existence of the APIs that are available either as a separate library or as part of an OS or application.

6 Third Layer: Deployment and Operations

This effort is divided into Deployment Considerations, which include strategy setting, decision making, planning, and resources, and Operational Considerations, which include performance monitoring, re-signing and other activities related to the continued smooth functioning of DNSSEC in an organization.

Figure 5: Deployment & Operations layer highlighted within the DNSSEC landscape

As noted in the Overview, the Deployment Initiative has four major goals:

- All zones signed
- ISP validation (i.e., widespread validation by ISPs; see Table 3 below)
- End-system validation
- DNSSEC-capable applications that integrate DNSSEC validation into the delivery of non-security-related services

The following table helps elucidate how actions by operators, application developers and others contribute to fulfilling these four goals. For example, ISP validation (or at least DNSSEC awareness) is necessary for all the validation-related goals, but other actions are needed to fully realize each of them:

Table 3: Validation-related categories and requirements

	ISP Validation Enabled	Enterprise or SOHO Network Validation Enabled	End-System Validation Enabled	Applications Enabled
ISPs Validate DNS Queries in Recursive Resolvers	•			
Enterprise DNS Recursive Resolvers Validate	•	•		
Local Systems Validate			•	•
Browsers Validate			•	•
Email Validates			•	•
DANE and Other Application Frameworks				•

Thus, the goal of a *basic* level of validation requires that a usefully large number of zones be signed, that ISPs validate DNS queries in recursive resolvers, and that enterprises run DNS recursive resolvers. End-system validation also requires that a usefully large number of zones be signed, but in addition is a state in which local systems, browsers and mail programs are DNSSEC-capable as well. The final set of goals is an Applications ecosystem in which all zones are signed and local systems validate, but where DNSSEC-capable applications are widely used for purposes other than DNS security (e.g. mail, consumer communication with banks, etc.).

The majority of large ISPs in countries such as Sweden and the Czech Republic are already providing ISP-level validation,[17] and progress has also recently been made in U.S. ISPs' acceptance of the need to, at a minimum, be transparent to DNSSEC traffic so that customers and others may conduct their own validation. Specifically, in a 2012 report by the Federal Communications Commission's (FCC's) Communications Security, Reliability, and Interoperability Council (CSRIC) Working Group 5, a wide range of ISPs endorsed the idea of becoming DNSSEC-aware as soon as possible, and additionally that "key industry segments, such as banking, credit cards, healthcare and others, sign their respective domain names with DNSSEC."

This report also detailed the various levels at which ISPs validate or otherwise handle DNSSEC traffic, as illustrated in the following table:

[17] Ondrej Sury/cz.nic e-mail with Paul Kretkowski/Shinkuro, 9 July 2012.

Table 4: Categories of DNSSEC validation service levels in ISPs

Category	DNSSEC service
A	Fully validating, where the ISP performs all validation on the end user's behalf (although the validating server can be configured in two distinct modes)[18]
B	DNSSEC-aware but non-validating, so that end systems may validate but the intermediate resolver doesn't
C	DNSSEC-unaware but able to handle large (e.g., EDNS0, IPv6) packets
D	DNSSEC-unaware but unable to handle large packets (this category is becoming obsolete but is included for the sake of completeness)

As mentioned previously, ISPs must be at least at category B in order for wide DNSSEC adoption to take place. At this level, validation is handled by end users or other non-ISP entities such as enterprise firewalls.

The Czech Experience
The Czech Republic serves as an innovative example of how ccTLDs can encourage DNSSEC adoption through pricing. In 2010, the Czech Republic encouraged its largest registrars to work with registries on getting all the registrars' zones signed. In this case there were 600,000 domains in the .cz space and registrar/registry cooperation enabled the registrars to sign 100,000 zones essentially at once. As of May 17, 2012, a remarkable 36 percent of the 944,000 zones in .cz were signed (see current figures at CZ.NIC), a byproduct of registries charging registrars less for signed domains, according to Jaromir Talir, technical manager for .cz.

6.1 Deployment Considerations: Signing Side

6.1.1 Root and Top-Level Domains (TLDs)

The root and nearly all the "major" ccTLDs have been signed (except .cn, which has begun the process). Meanwhile, the generic TLDs with the greatest numbers of zones have been signed, including .com, .org, .net and .gov. The signing of the .com TLD by itself accounted for nearly half of all existing zones, a major step that enabled an unbroken chain of trust to potentially stretch from the root to .com to roughly 100 million end users' zones.

6.1.2 The .gov Space

As noted above, in 2008 the U.S. federal government mandated DNSSEC signing on .gov and all .gov delegations (e.g., fcc.gov, state.gov). The Initiative has begun tracking the percentage of .gov delegations that are signed[19], and as of June 13, 2012, 906 .gov delegations were signed while 3,938 remained unsigned.[20]

[18] A fully validating resolver can be configured in two modes: strict or permissive. Strict mode will prevent an answer from being returned to a client when validation fails. Permissive mode will return a non-validated answer to the client, but will not set the authenticated-data flag. Permissive mode only offers security protections for DNSSEC-aware client-side software, but does not prevent access to non-DNSSEC-aware applications when DNSSEC validation fails, either due to misconfiguration or security abuse. Permissive mode is considered a transitory setting with the end goal considered to be strict mode, and some argue that permissive mode should not be used at all.
[19] http://usgv6-deploymon.antd.nist.gov/cgi-bin/generate-gov
[20] Olafur Gudmundsson/Shinkuro, 13 June 2012.

6.1.3 The Enterprise Space

Despite the signing of the root, .com, .org and .net, DNSSEC signing has generally been slower in the U.S. private sector beneath the level of these gTLDs.[21] While only a handful of Fortune 500 companies are signed, two of those that are—Comcast and PayPal, in the ISP and payment-processing businesses, respectively—have an outsized influence on others. (As one might expect, IT-industry companies tend to have an above-average rate of DNSSEC signing.)

Part of the enterprise signing lag stems from the fact that enterprises have had few easy ways to pass DNSSEC information through their registrars to registries, although this is changing as more registrars realize the value of providing DNSSEC signing as a service. Still, more efficient processes and tools must be created and implemented to speed enterprise adoption.

Beyond their importance to individual enterprise DNSSEC deployments, registrars have the power to facilitate DNSSEC adoption for very large numbers of enterprises. This has already been demonstrated in several European countries, with remarkable results in terms of the ease of subsequent DNSSEC signing. For example, the Czech Republic encouraged its largest registrars to work with registries on getting all the registrars' zones signed, with remarkable success (see sidebar, "The Czech Experience," above).[22] By encouraging similar models of cooperation, the Netherlands and Sweden have produced similar successes, with the Netherlands in particular benefiting from a large number of operators using PowerDNS, which performs online signing and eases deployments for a large number of zones.

Registrars, then, can be a very high-leverage part of the DNSSEC deployment equation; once they create simple mechanisms for passing customers' public keys to registries, adoption will accelerate rapidly—and from the bottom up as well as the top down (in terms of domain size) as small domains realize DNSSEC's security benefits.

We plan to specifically target registrars to both accelerate their own deployment and ease customer enterprises' adoption of DNSSEC. This will involve working with the registrars in concert with ICANN and registries to make DNSSEC support standard practice for registrars. In addition, we plan to consult with hosting providers to

Signature-Checking Tools
Signature validity is a major operational concern in DNSSEC deployment, and signatures must be managed actively—a major change from the set-it-up-and-forget-it reliability of DNS. A wide array of tools are available to check the validity of items such as key length, exponent size, algorithm support, number of NSEC3 iterations, signature presence, and other important factors. Signature-checking tools can help check several or all of these items; see Appendix 3: Lists of Tools & Implementations.

[21] As of January 4, 2012, 5,933 in .com, 1,532 in .org, and 6,038 in .net were signed, according to monitoring by Olafur Gudmundsson/Shinkuro.
[22] Personal communication of Steve Crocker/Shinkuro with Jaromir Talir, technical manager for cz.nic; Talir reported that 314,088 of 894,033 domains were signed as of 31 January 2012.

persuade them to create standardized tools for passing DNSSEC information to registrars and so on to registries.

We also plan to work with ISPs through their umbrella organization, the North American Network Operators Group (NANOG), and through FCC CSRIC Working Group 5 (mentioned above), to get more large ISPs to deploy DNSSEC throughout their networks and begin validating, as Comcast and Sprint have done (albeit in "permissive" mode, in Comcast's case, at the time of this writing). Success is defined as persuading non-validating ISPs to move to at least level B as noted on Table 2, "Categories of DNSSEC validation service levels in ISPs," and to move to level A if they are already at level B. That persuasion hinges on the further marshaling of arguments that DNSSEC is good for ISPs' brand, their customers, their operations and, when deployed as a premium service, their bottom line.

Several other types of organizations also present high-leverage opportunities to the extent that they can be persuaded to sign their zones, because the integrity of their domains is vital to their brand as well as their business operations. Examples include:

- Banks and other financial institutions, which have a very high need for security to protect their own and their customers' transactions
- Universities, which tend to have very high traffic, large numbers of delegations, and a relatively inexperienced user base[23]
- Associations and trade groups that both highlight DNS-related issues and persuade or require their members to adopt DNSSEC, such as BITS (the Technology Policy Division of the Financial Services Roundtable), INTA (the International Trademark Association), MPAA (the Motion Picture Association of America), and others
- CDNs and "cloud" services, since they provide large and critical Web-site functionality for influential enterprises

6.1.4 Configuration and Operational Considerations

Once a zone operator decides to deploy DNSSEC, configuration and operational considerations that come into play include (but are not limited to):

- DNS parameters, including times-to-live (TTLs) for records
- Key length and algorithm
- Zone re-signing frequency
- Key rollover frequency for key-signing keys (KSKs) and zone-signing keys (ZSKs)
- Signature expiration date
- Validity times for a zone and its signing keys
- Use of Next Secure (NSEC) vs. NSEC3 records

Zone operators must decide on and set parameters for the above items that are appropriate for their zone, taking into consideration factors such as zone size, the importance of any given delegation, operational availability, alignment of the times-to-

[23] Additionally, universities are the core of the Internet2 development effort.

live of the zone and its keys, and the zone's general need for security or secrecy. Standard settings in the above categories are converging toward what appear to be median values, but they are currently far from stable.[24]

In addition, more work needs to be done to establish standard procedures for when a DS record published in a parent zone that no longer matches any DNSKEY in the child zone, a problem that could have significant effects on the zone's availability as validation becomes widespread.[25]

The need for the above-noted types of basic standards, procedures and guidance indicate that some maturation in DNSSEC operations and processes is needed, including more examples of the types of thorough guidance evidenced in the draft RFC 4641bis-04, "DNSSEC Operational Practices, Version 2," before signing and validation can become truly widespread.[26]

6.1.5 "Completeness" of Signing

We have gradually realized that the definition of a "signed zone" is not as simple as we'd first thought, particularly for large enterprise sites. An enterprise that signs its zone (www.example.com) can still leave several avenues on its Web site through which it hosts other, unsigned zones or their content. We propose that the definition of a fully signed site be one in which:

- The enterprise has signed its subdomains (e.g., sales.example.com).
- Its Web pages incorporate only content from CDNs or other parties whose zones are signed, such as a weather map from example.net that is then embedded on example.com.
- The site features links only to external zones that are signed.

While at first the task of fully signing a site appears daunting, numerous link-checking programs already help operators ensure that their site's links work properly. We need to encourage and help developers to create tools that can check these links' DNSSEC status (and the zones from which embedded content is imported), such as by using the DNSSEC-Nodes graphical debugging utility.

6.2 Validation Side

6.2.1 The .gov Space

It is difficult to measure validation in the .gov space accurately without information from the many .gov recursive resolvers. However, it is still possible to get information on validation from various federal agencies; if the Initiative persuades one of the agencies that acts as a touchstone for all the other agencies—such as the Office of Personnel Management (OPM) or the OMB—to share information on whether incoming queries

[24] Paul Kretkowski/Shinkuro email with Richard Lamb/ICANN, 1 February 2012
[25] Some progress is being made on this problem, as in tools such as dnssec-kskro-frp, described here.
[26] In particular, one reviewer of this Roadmap noted a need for solid processes to handle DNSSEC-signed names in the Extensible Provisioning Protocol (EPP) process.

are validating or not, this will give an accurate picture of whether, for example, the FCC or the National Aeronautics and Space Administration (NASA) are validating as well as signing. From these statistics it is also possible and desirable to monitor the aggregate quality and stability of DNSSEC signing and validation in .gov over time, providing a useful snapshot of DNS security throughout government.

6.2.2 ISPs

The drive to encourage ISPs to embrace DNSSEC has also just begun. While companies such as Comcast (in the U.S.) and TeliaSonera (in Sweden) are at the forefront of both deployment and advocacy, and Sprint has deployed the necessary hardware and software with little fanfare, other major U.S. ISPs are only at the beginning of their deployment efforts. Comcast and Sprint are both capable of validating DNSSEC signatures, although only Comcast is currently doing so. The Initiative must make the case to ISPs that DNSSEC adoption is inevitable, necessary, will help secure their networks, does not impose as large a computational overload as they estimate, and provides them with additional opportunities to generate revenue (for example, by touting DNSSEC as a premium service, although this may not lead to the widest possible adoption).

ISPs' DNSSEC Concerns
Some ISPs have voiced concern that DNSSEC only increases the amount of damage that attackers can do through DNS amplification attacks, since DNSSEC replies are larger than other types of DNS replies (although large-scale adoption of BCP 38 ingress filtering would likely help assuage ISPs' concerns in this area). The Initiative believes that studies are needed to determine whether this is so and the overall risk:reward ratio of DNSSEC adoption by ISPs.

It may also be helpful for U.S. ISPs to follow the Swedish example of creating or chairing a reference group composed of ISPs, registrars, registries and other interested parties that can aid those groups in reaching consensus regarding DNSSEC adoption, as well as facilitate the development of best practices among them.

6.2.3 End-User Resolvers

The first tools for end-user validation have begun to emerge, the most prominent of which at this writing is NLnet Labs' DNSSEC-Trigger.[27] This validating, caching nameserver allows the end user's computer to either determine whether the DNS servers it is using are DNSSEC-capable and either use those servers or, alternately, the root nameservers as their starting point for validating signatures.[28] (If need be, DNSSEC-Trigger can choose from a list of Unbound servers provided by NLnet Labs.)

We expect DNSSEC-Trigger to be the first of a wave of more consumer-friendly products that enable DNSSEC validation at the network edge, further opening the way to the Applications end point discussed below.

[27] http://nlnetlabs.nl/projects/dnssec-trigger/
[28] http://jpmens.net/2011/10/21/automating-unbound-for-dnssec-on-your-workstation/

6.2.4 Firewalls and Routers

Enterprise and personal firewalls and routers lie between ISPs and end-user resolvers. These seem both a natural and a largely unexplored point at which to handle validation, which seems to fit nicely with firewalls' and routers' current missions. We plan to discuss the possibility of incorporating DNSSEC functionality into firewalls and routers with manufacturers, as well as with the ISPs that serve enterprise and home networks that therefore have great influence on these devices' specifications.

The Initiative will also hold discussions with software developers to determine whether there are robust software additions that device manufacturers can incorporate, and persuade them to create these additions if not.

At the very least, all these parties need to be made aware that their products may need to be modified if they currently consider DNSSEC packets to be harmful or "too large" and so discard them; DNSSEC awareness in these devices is critical.

7 Fourth Layer: DNSSEC-Based Applications

The Applications layer is both at the apex of the DNSSEC development process and the slowest part of the DNSSEC ecosystem to develop, depending as it does on DNSSEC being used by a sufficient number of domains to render the applications useful. However, steady progress is being made on validation-side applications that the advent of a DNSSEC-secured network infrastructure will make possible.

Herein lies a major unrecognized business opportunity: The creation of commercial applications that will build on DNSSEC and the DANE protocol to provide security to millions of users who haven't even heard of it, just as billions once had never heard of the Internet. The search for a "killer app" utilizing DNSSEC as its security foundation has begun, and the market-opportunity "carrot" that such an application creates may generate the consumer pressure for DNSSEC adoption that has long been missing from debates over the protocol.

Among the logical first entrants into the competition to create a DNSSEC-based killer app would be certificate authorities that may see their current business model as threatened, but who may instead find that the transition to DNSSEC creates an entirely new consumer-oriented business for them.

We expect that some of the first new applications to be built atop DNSSEC will include DKIM e-mail as well as DNSSEC-signed SSHFP records, which will assure users that they are connecting not just to example.com as intended, but logging into a specific computer at example.com.

Figure 6: Applications layer highlighted within the DNSSEC landscape

7.1 Signing Side

This category includes products that will enable different types of information products to be stored in resource records; for example, each individual employee stores a DNSSEC signature in the employer's system once they're hired, enabling employees to authenticate their actions and correspondence later. The tools that can perform this function—of "signing on" an employee to his/her employer by creating a record

corresponding to a DNSSEC signature, for example—are still largely undeveloped. This prospect depends on the creation of standardized DNSSEC-signing processes that can be incorporated into commercial software. An early effort in this direction involves using DNSSEC with Secure Shell (SSH) to publish key fingerprints, as described at http://www.ietf.org/rfc/rfc4255.txt.

7.2 Validation Side

7.2.1 DANE Working Group

This IETF-chartered group[29] is developing standard ways for domains to secure and publicly present their domains' security using DNSSEC. The DANE protocol is capable of using a DNSSEC underpinning to secure Web, e-mail and other traffic against attempts to tamper with addressing; however, prototypes must be created and experiments conducted to take a DANE standard from promising idea to reality.

For DANE to work in this context, a Web site must be in a signed DNS zone; the Web site must publish its DANE records in the zone; and the user trying to access the site must have a browser that supports DANE processing and DNSSEC validation (or have access to a trusted DNSSEC validator). Initiative members are active in the DANE Working Group and continue to work vigorously to develop this protocol and applications derived from it.

7.2.2 DKIM

DKIM is a standard for cryptographically associating a domain name with an email address, which could be especially useful with DNSSEC (although this is not required). Combining DKIM with DNSSEC provides a much higher assurance that the DKIM signature is valid. We believe DKIM will evolve and become more popular through a combination of wider DNSSEC usage and the development of tools and processes for the validation of DKIM record lookup, including the development of error codes for DNSSEC validation.

7.2.3 DMARC

DMARC adds policy and reporting capabilities for email services using SPF and DKIM authentication. It was recently developed by an informal, private industry consortium that included many large email service providers and has already been adopted by a number of them.

[29] http://datatracker.ietf.org/wg/dane/charter/

8 Next Steps for DNSSEC Deployment: The Road Ahead

The Initiative acknowledges that although great strides have been made in encouraging DNSSEC signing and validation, much remains to be done to move DNSSEC deployment forward. Here is a visualization of which areas—in the stages between the root and end-users' applications—the Initiative has put its efforts to date, and whether it must devote more, less or the same attention to that stage:

Table 5: Past, current and future areas of Initiative focus

Stage in Flow (from Root to End-User)	Effort to 2012 (Low, Medium, High)	Future Effort (Increase, Same, Decrease)
Root	High	Decrease
TLDs	High	Same
Registrars	Low	Increase
DNS Operators	Low	Increase
ISPs	Medium	Increase
Last Mile (Firewalls & Routers)	Low	Increase
Operating Systems	Low	Increase
Applications	Medium	Increase

This remainder of this section compiles this Roadmap's recommendations and notes the remaining challenges and where the Initiative and/or other parties must devote their resources to maximize their impact. Because this Roadmap is intended as strategic guidance, specific programs that put this guidance into action may not yet have been created.

8.1 Tools & Implementations

8.1.1 Signing Side

- Continue development of tools that close gaps in various parties' ability to deploy DNSSEC, particularly tools that automate provisioning and/or management of authoritative DNSSEC nameservers (e.g. setting parameters for key rollover, key length, time-to-live considerations, etc.), especially those that provide the capability of signing and managing zones *en masse*
- Encourage and aid developers to create tools that can check the DNSSEC status of subdomains, links to their site, and zones from which embedded content originates
- Encourage and aid developers to establish metrics and tools that allow registrants, DNSSEC operators and third parties to measure the overall quality of a site's DNS and DNSSEC operations

8.1.2 Validation Side

- Cultivate and continue dialogue with OS developers to improve query flow and caching models, and encourage inclusion of DNSSEC in future versions of major operating systems
- Educate browser and other application developers regarding the need to not rely on third-party add-ons for DNSSEC validation. Studies are needed of DNSSEC's effects on browser performance which, while we expect them to be small, must be measured
- Investigate the prominence of DNS use in industrial/infrastructural operations (i.e. as part of SCADA-controlled operations) and promote DNSSEC use among those operators
- Develop a standard set of fallback techniques that would enable DNSSEC validation software to work around certain error conditions that currently inhibit DNSSEC validation within end-applications

8.2 Documents and Regulations

8.2.1 Signing Side

- Contact NIST to determine the feasibility of including DNSSEC signing and validation as a standard part of federal contracting procedures
- Through NIST, provide input to GSA policy documentation in support of OMB's mandate to adopt DNSSEC
- Work with ICANN to facilitate deployment of DNSSEC through its contracts and best practices with registries and registrars, which currently include mandating DNSSEC adoption by new gTLDs
- Work with ICANN and DNS operators to specify what information registrars must pass on to registries, including DS records, and encourage operators to create standard interfaces through which they may pass DS or DNSKEY data to registrars for distribution to registries
- Develop free educational materials on DNSSEC adoption that are geared toward registrants and zone-signing parties, and examine the possibility of providing them with financial incentives for DNSSEC adoption

8.2.2 Validation Side

- Through NIST, act on interagency "tiger team" recommendations to the Federal CIO Council as appropriate
- Support the DANE Working Group's efforts to develop DANE protocols by continuing to engage in the approval and specification process leading to their publication, especially specifications for publishing DANE records in a signed zone
- Continue to work with the DNSSEC validator community in order to come up with a single API that applications can use to process DNSSEC results

8.3 Products & Services

8.3.1 Signing Side

- Raise and discuss with registrars the possibility of signing zones *en masse* as .cz .se and other registrars have done; discuss with Dept. of Commerce how this can be accomplished for the .edu and .us zones, and whether any incentives such as those used by the .se and .nl ccTLDs are feasible
- Persuade hosting services to offer signed DNSSEC service and encourage them (and registrars and ISPs generally) to self-monitor to ensure their services are working properly so they can take action in case of any DNSSEC-related problems

8.3.2 Validation Side

- Encourage ISPs to (at a minimum) offer validation as a service, emphasizing that ISPs' ability to recognize and pass DNSSEC packets is crucial to end-to-end validation; persuade them to move from level B to level A if they already have validation capabilities in place
- Discuss with manufacturers the possibility of incorporating DNSSEC functionality into firewalls and routers, at least to the point where such products are DNSSEC-aware

8.4 Deployment and Operations

8.4.1 Signing Side

- Meet with/deepen contacts with trade associations, banks, universities, ISPs and other high-leverage organizations to encourage them to agree to deploy DNSSEC both internally and to members and customers; subsequently, provide them with implementation guidance
- Encourage Fortune 500 companies that use large supplier networks (e.g. auto manufacturers, big-box retailers) to require suppliers to sign and validate their zones
- Through improvements to Initiative Web sites and other collateral materials, and through the Initiative's recent collaboration with the Internet Society's Deploy360 Programme, develop and offer information and education on DNSSEC for signing parties

8.4.2 Validation Side

- Meet with mobile-OS developers and press them to include DNSSEC validation capabilities in upcoming releases (such as NLnet Labs' iOS version of libunbound)
- Through discussions to raise awareness of OMB and NIST mandates, press .gov CIOs to begin validation of other .gov signatures
- Organize ways to measure and gauge DNSSEC uptake in .gov or elsewhere

8.5 Applications

8.5.1 Signing Side

- Explore possibilities for storing authentication information for other protocols in resource records, i.e. leverage the work done in DANE using DNSSEC for S/MIME user's certificate with the intended domain name or mail-submitter certificates

8.5.2 Validation Side

- Create the applications necessary for end-user validation (e.g. improvements on/successors to DNSSEC-Trigger), including preferable actions of applications in response to validation errors
- Test emerging tools and give developers feedback designed to make those tools more reliable and easy to use
- Create end-user products, including email authentication technologies such as SPF, DKIM and DMARC, potentially modeled on .se's OpenDKIM.
- Create a demonstration project to showcase the DANE protocol's capabilities and potential applications, priming the pump of the search for a DNSSEC-based "killer app"

Appendix 1: The Domain Name System

Brief overview of the DNS

The Domain Name System (DNS) is a distributed hierarchical database that contains a listing of Internet resources and various types of information associated with those resources. Although the DNS has a variety of uses, its most important function is to bind user-friendly names of Internet resources to corresponding IP addresses of the systems that host those resources. This allows end users to conveniently depict and access Internet resources using recognizable names. The DNS also creates a logical linkage between the name of an Internet resource and its IP address, allowing a resource to retain the same name, even though its IP address and point of attachment to the network changes over time.

Structure of domain names

A domain name denotes an Internet resource, such as a Web site, a database server, or any machine or service that is accessible through the Internet. Domain names are hierarchically organized in a tree structure as shown in Figure 7. Each node in the hierarchy represents a domain and has a label associated with it. A domain may be the parent of subordinate domains (subdomains). The root of the DNS tree has no formal name, but is generally referred to as the DNS root domain or "the root." Below the root domain are the top-level domains (TLDs) that comprise the first-level group of domains. The TLDs include generic top-level domains (gTLDs) such as .com, .net, .org, .edu, etc. and country code top-level domains (ccTLDs) such as .us, .uk, .br, .de and .se.

The next subordinate levels in the tree structure include the second-level domains, third-level domains, fourth-level domains, etc. There can be up to 127 levels of subordinate domains in the hierarchy.

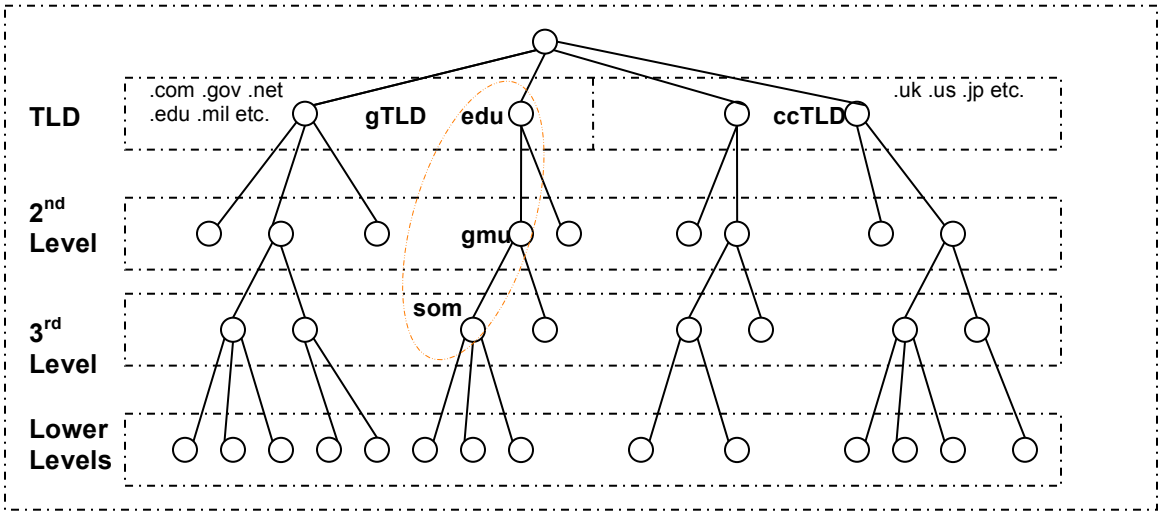

Figure 7 – Generic structure of DNS namespace

The administration of the DNS is decentralized. Each domain or subdomain can be managed by a separate organization. A domain administrator can delegate management of some of its subdomains to other entities—and this domain decomposition and delegation process can be enacted recursively. Parent domains maintain only pointers to servers that contain information about their subdomains so that DNS queries can be referred to the appropriate data sources. Each autonomously managed domain is called a zone. The syntax of a domain name consists of a sequence of labels (designating nodes in the namespace) separated by dots. Essentially, a domain name is an index entry in the DNS database. For example “som.gmu.edu” refers to the “som” subdomain under “gmu” in the “edu” gTLD.

The DNS database is distributed across a very large number of geographically dispersed nameservers that are managed by independent organizations. Each nameserver contains information pertaining to one or more DNS zones. Nameservers store data associated with domain names in resource records (RRs). Broadly speaking, there are two types of nameservers: (1) authoritative and (2) caching. An authoritative server has complete knowledge about a subset of the domain namespace, while caching servers improve query response time by locally caching a subset of global DNS data for a specified time interval.

Appendix 2: DNSSEC in a nutshell

For those unfamiliar with DNSSEC, here is a brief explanation of what it is and how it works. It is useful to think of the DNS as providing a service that is similar to that provided by calling the telephone directory assistance number 411. To place a call to Roger Smith of Nashville, Tennessee without knowing Roger's phone number, a caller can dial 411 and ask the operator to look Roger's phone number up. When the operator tells the caller the number, he or she can then dial that number to talk to Roger. Note that without Roger Smith's phone number, the caller can't call him.

Similarly, when an end user wants to access the Web page at www.example.com, their Web browser must first ask some other authority (typically the user's ISP) what numeric Internet Protocol (IP) address (e.g. 181.04.4.4) www.example.com translates into. The IP address is similar to the phone number in the Roger Smith example—without it, the browser cannot contact www.example.com.

This is because the DNS, which governs how information is located on the Internet, is set up so that the browser has no prior way of knowing the correct IP address for www.example.com. (Please see Appendix 1, "The Domain Name System," for a detailed explanation of the DNS.) Even if the browser did know the "correct" address, domain names change or are transferred, are created or destroyed, or their hardware and software updated so that IP addresses can change over time; they are never "fixed" in the way that landline phone numbers are.

The system that answers the question "what numeric address does www.example.com translate into" is called a recursive resolver. It may reside at the end user's ISP (in a *caching resolver*) or on the end user's system. In either case, its job is to query a succession of servers (caching or *authoritative*). Eventually one of the queried resolvers or nameservers returns the appropriate numeric address and the user's browser can then get the example.com Web page.

However, an inherent lack of security in the original DNS means that criminals and others can intercept the request to translate www.example.com into the correct numeric address. The criminals might instead provide a bogus numeric address that sends the request to their own servers, which can then respond with an unwanted page (typically an advertisement) or worse, a carefully crafted—but fake—example.com Web page designed to capture the user's innocently input credentials. This type of exploit is called a "man in the middle" attack (also commonly known as a Kaminsky attack) and the user may not realize they have revealed important information until it is too late.

DNSSEC addresses this problem; it is an enhanced level of security that allows Web sites (and other applications and protocols) and ISPs to validate that domain names in query responses have not been tampered with between the authoritative server and the resolver. For example, with DNSSEC, a domain name such as example.com can be cryptographically signed in the DNS. Then, when an end user tries to connect to that Web site, an ISP's DNS servers will check that the domain name and its security

signature are verified and have not been tampered with by hackers. End users will then only be connected if this security verification has been passed. (This entire transaction occurs so quickly that end users do not even notice that it is being performed.)

So when DNSSEC is used for the example.com domain, the user's ISP (if it is DNSSEC-aware) asks www.example.com for its resource records and the public keys required for verifying the signatures accompanying those resource records. It forwards www.example.com's content back to the end user as a DNSSEC-validated response only if it is able to construct a DNSSEC "authentication chain" from a DNSSEC trust anchor (a locally configured starting point for validation) to the verified signatures.

Because of DNSSEC, the user and example.com can interact with much greater security and little threat of DNS-based attacks. Eventually, individual users will harness DNSSEC-enabled applications to perform the ISP's function on their own, pushing responsibility for DNS security all the way to the edge of the worldwide network.

Appendix 3: Partial lists of tools, implementations, hardware and software

Signing Side: Deployment

Tool	Developer	Function
OpenDNSSEC	.se, Cira, Nominet	Checks all public nameservers for zone DNSSEC meta-data, and checks that the zone is validatable at all times (including during rollovers)
dnssec-keygen	ISC	"Generates keys for DNSSEC (Secure DNS), ... [and] can also generate keys for use with TSIG "
dnssec-signzone	ISC	"Signs a zone. .... Generates NSEC and RRSIG records and produces a signed version of the zone"
ldns-keygen, ldns-signzone	NLnet Labs	Tools from the ldns-tool suite
pdnssec-keygen, pdnssec-signzone	Roy Arends	Tools from the DNSSEC perltools distribution
Secure64 DNS Signer	Secure64	"Fully automates DNSSEC key generation, key rollover, zone signing and re-signing processes." In addition, its DNS Cache caching nameserver is specifically designed to handle any increased load imposed by DNSSEC validation.
Zonesigner	Sparta, Inc.	Allows zone administrators to sign DNS zone files easily
Rollerd	Sparta, Inc.	Automates the "rolling" of zone-signing keys and key-signing keys
jdnssec-keygen, jdnssec-signzone	Verisign Labs	Tools from the jdnssec-tools suite

Signing Side: Operations

Tool	Developer	Function
dnscheck	.se	"...Help people check, measure and hopefully also understand the workings of the Domain Name System. ... other sanity checks, for example measuring host connectivity, validity of IP-addresses and control of DNSSEC signatures will also be performed."
validns	Anton Berezin, sponsored by AFNIC	"In addition to basic syntactic and semantic zone checks, includes DNSSEC signature verification and NSEC/NSEC3 chain validation."
Measurement Naming System	GCSEC	Framework that "proposes to design a layered and multi-perspective framework for the

(MeNSa)		measurement and benchmarking of the DNS SSR level"
SZIT Monitor Extension	NIST	Tests zone contents against best common practices and overall security
Donuts	Sparta, Inc.	Syntax-checks signed zone files for DNSSEC
ZoneCheck	AFNIC Team	Open-source program that helps solve misconfigurations or inconsistencies
Nagios Plugin	The Measurement Factory	Checks for expired DNSSEC signatures
SecSpider	UCLA, Colorado State, Verisign	Checks DNSSEC compliance and reachability, and tests for PMTU[30] problems of zones from globally distributed pollers; the oldest such tracking system
jdnssec-verifyzone	Verisign Labs	Verifies all of the signatures in a zone for cryptographic validity

Validation-Side Tools[31]

Tool	Developer	Function
Dig	ISC	DNS lookup utility; "flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried"
DNSviz	Sandia National Laboratories	"Provides a visual analysis of the DNSSEC authentication chain for a domain name and its resolution path in the DNS namespace, and it lists configuration errors detected by the tool"
DNSSEC-Nodes	Sparta	"Graphical debugging utility that allows administrators to watch the data being logged into a libval or bind logging file"
DNSSEC-Check	Sparta	"Examines the system's configured recursive resolvers for client-side DNSSEC support" and performs tests based on its findings, displaying the results using red, yellow or green lights
logwatch	Sparta	"Collects output on a regular basis from syslog messages and summarizes them so they're easier to scan through," reporting on DNS and DNSSEC errors
lookup	Sparta	Graphical DNS lookup and validation tool

Applications Using DNSSEC

Tool	Developer	Function
DNSSEC	CZ.NIC	"[Will] check the DNSSEC status of a page you

[30] Path maximum transmission unit
[31] See also the more technically oriented list of validation-side tools at https://www.dnssec-deployment.org/wiki/index.php/Tools_and_Resources - DNSSEC_on_the_End_System.

Validator (web-browser extension)		are visiting and ... present status of DNSSEC security using color keys and information texts in the URL bar"
DNSSEC-Trigger	NLnet Labs	Allows the end user's computer to determine whether the DNS servers it is using are DNSSEC-capable and either use those servers or, alternately, the root nameservers as their starting point for validating signatures
DKIM Milter	Open-source community effort	Part of OpenDKIM package; "milter-based filter application that can plug in to any milter-aware MTA[32] to provide that service to sufficiently recent sendmail MTAs and other MTAs that support the milter protocol"
Open SSH	Open-source community effort	"Free SSH/SecSH protocol suite providing encryption for network services like remote login or remote file transfer" and includes DNSSEC capabilities
DNSSEC-Tray	Sparta	"System-tray application that monitors log files (e.g. libval, or bind/named and unbound logfiles) for DNSSEC error messages that should be displayed to the user"

(See also the Internet Society's Deploy360 Programme list of libraries.)

Validation Libraries

Library	Developer	Function
Net::DNS::SEC	CPAN	"DNSSEC extensions to Net::DNS". No validation library as yet.[33]
libunbound	NLnet Labs	“Can be used to convert hostnames to IP addresses, and back, and obtain other information from the DNS. The library performs public key validation of results with DNSSEC.”
Perl Net::DNS	NLnet Labs	"DNS resolver implemented in Perl. It allows the programmer to perform nearly any type of DNS query from a Perl script"
dnspython	Nominum	"Supports almost all record types. It can be used for queries, zone transfers, and dynamic updates. It supports TSIG authenticated messages and EDNS0"
vsresolver	Shinkuro	"DNSSEC validating stub resolver that exposes a software API for python programs to query DNS and validate results.”
libval, libsres	Sparta	"DNSSEC Validating library that allows applications to issue DNS queries and verify that the responses returned are trusted.”

[32] Mail transfer agent
[33] Olaf Kolkman/NLnet Labs email with Paul Kretkowski/Shinkuro, 6 July 2012.

libval_shim	Sparta	"... Implements wrappers for a number of DNS related functions and in turn calls equivalent DNSSEC-aware validating functions from 'libval', mapping the results to return codes recognized by the original functions. In this way a wide variety of applications can be made DNSSEC aware without code changes and recompilation."

Managed DNS Services

Service	Producer	Description
OneClick DNSSEC, Afilias Managed DNS	Afilias	Various registry and managed DNS services for top-level domains[34]
EURid DNSSEC Signing Service	EURid	Manage and automate information necessary for DNSSEC operation and maintenance, and for zone transfers
Premium DNS service	GoDaddy.com	Provides a check box through which users can enable DNSSEC signing of their GoDaddy-hosted domain (step-by-step instructions here)
SNS	ISC	"Infrastructure service for publication of DNS zone data to the global Internet with maximum availability and minimum delay"; includes DNSSEC signing/maintenance as a feature
DNSSEC Signing Service	Nominet	"Takes unsigned zones and returns signed zones"[35]
Shared ccTLD DNSSEC Signing Platform	Packet Clearing House (PCH)	Runs a program to securely handle signing of country-code top-level domains (ccTLDs) on their behalf, then transition management to the ccTLD as it gains experience[36]
Verisign Managed DNS	Verisign	"Makes the complex process of managing DNSSEC easier by signing all zone files in a customer's account, continually checking the status of DNSSEC keys to ensure they are valid, and automatically publishing new keys after the existing ones expire"

[34] Presentation by Jim Galvin/Afilias at March 2011 ICANN DNSSEC Workshop; http://svsf40.icann.org/meetings/siliconvalley2011/presentation-accelerating-dnssec-16mar11-en.pdf
[35] Presentation by Simon McCalla/Nominet at March 2011 ICANN DNSSEC Workshop; http://svsf40.icann.org/meetings/siliconvalley2011/presentation-dnssec-signing-service-16mar11-en.pdf
[36] Presentation by Bill Woodcock/PCH and Richard Lamb/ICANN at March 2011 ICANN DNSSEC Workshop; http://svsf40.icann.org/meetings/siliconvalley2011/presentation-shared-platform-14mar11-en.pdf/

DNS Hardware Devices

Product	Manufacturer	Description
Keyper	AEP	"Allows the FIPS[37]-certified Security Officer and authorized user to generate, store and use high quality keys within a tamper reactive, Ethernet-connected HSM"[38]
Sapphire Sx20	BT Diamond	"Supports a dedicated DNSSEC administrator login to configure DNSSEC key and signature policies, including key types, algorithms, lengths, and rollover as well as key generation and lifetime management as well as signature expiration times. The Sapphire Sx20 also automatically links parent zone Delegation Signer (DS) records to simplify key rollover for managed zones." Tested/certified with AEP Keyper
4765 Cryptographic Coprocessor Card	IBM	"Specialized hardware performs AES, DES, TDES, RSA, SHA-1, SHA-224 to SHA-512[39], and other cryptographic processes, relieving the main processor from these tasks"
Compact HSM	Kryptus	"Execute digital signatures on solutions which use PKCS#11[40] ... Generate and store certificates ... Communications encryption/safe links"
SCA6000 Crypto Accelerator card	Oracle	"Accelerates SSL cryptographic functions ... [by offloading] SSL functions for any application, including IPSec,[41] from host processors"
Luna CA4, Luna SA appliance	SafeNet	CA4 "protects the PKI root key and performs all key management, key storage, and key operations (such as digital signing) exclusively within hardware"; SA does "high-performance signing and acceleration of SSL cryptographic functions for any application"
nShield Solo and nShield Connect	Thales	"Protects private DNSSEC signing keys and assures the integrity of the DNSSEC validation process using high assurance, FIPS-certified, tamper-resistant hardware security modules (HSMs)."[42]
CryptoServer HSM	Utimaco (Sophos Group)	Cryptographic HSM that additionally deletes keys and certificates if tampered with

[37] Federal Information Processing Standards
[38] Hardware security module
[39] AES=Advanced Encryption Standard, DES=Data Encryption Standard, TDES=Triple DES, RSA=acronym for RSA, Inc. encryption standard, SHA=Secure hash algorithm
[40] Public-key cryptography standard
[41] Internet Protocol security
[42] Lisa Kramer/Thales email to Paul Kretkowski/Shinkuro, 23 July 2012.

DNSX Secure Signer	Xelerance Corp.	Automates DNSSEC management tasks
DNSX Secure Resolver	Xelerance Corp.	Adds security to caching and resolving nameservers

Appendix 4: "Players" in the DNSSEC ecosystem (and messaging to them)

The following is a list of actual or potential players (besides the Initiative itself) within the DNSSEC ecosystem; the Initiative does not currently engage with all these parties but acknowledges that all of them have some influence on the DNSSEC ecosystem and on the Initiative's work. (Note: The groupings below are a work in progress and subject to change.)

Class	Examples	Action Desired	Message to Them
Govt./NGO Funders, Labs, Rulemakers	DHS, NIST, OMB, ICANN	Include DNSSEC as either a requirement or a standard best practice	Provide evidence that DNSSEC prevents hijacking of DNS responses at relatively low bandwidth/CPU cost and increases DNS robustness
gTLD Registries	Verisign; Public Interest Registry (PIR); Neustar, Inc.; Afilias Ltd.	Sign their zones and provide pathway for registrars to insert and maintain delegation signer (DS) records	Collate best-practices information from TLD peers on what it takes to successfully deploy
gTLD Registrars	Go Daddy.com, NamesBeyond, Dyn	Provide DNSSEC interface to customers; provide DNSSEC service. Make it easy for customers to choose DNSSEC as a default with little/no charge	Note desire for DNSSEC from customers, peers, ICANN. Cost and/or modification of existing operations will be minimal
ccTLD Registries	.br, .ca, .cn, .de, .fr, .in, .it, .jp, .kr, .nl, .pk, .ru	Sign their zones and require their registrars to enable DNSSEC service	Emphasize importance of DNSSEC and registries' key role
DNS Service Providers	Afilias, Nominet, PCH, ISC, UltraDNS	Provide DNSSEC service both for primary and secondary operations	DNSSEC capability (and automating provision of new record types, e.g. the proposed TLSA record)is a factor when customers choose between service providers. Provide deployment strategies and key-management techniques
DNS Software Providers	ISC, NLnet Labs, PowerDNS, various router and firewall vendors	Implement DNSSEC in their primary and secondary authoritative nameservers and validation in their resolvers. Fix broken guidance that	Emphasize government and industry requirements, plus business opportunity in new apps that will utilize DNSSEC

		recommends limiting DNS packets to UDP size[43]	
DNSSEC Appliance Vendors	Secure64, Xelerance, Oracle, Thales, AEP, IBM, SafeNet, Kryptus	Make their products easy to use and cost-effective; ensure compliance with standards	Note government and industry requirements, new business opportunity in DNSSEC-capable HSMs, new apps that will utilize DNSSEC
Browser Vendors	Mozilla, Microsoft, Opera Software, Apple, Google	Add DNSSEC to the resolvers they have in their browsers (i.e., local validation capability); consider how DNSSEC capability can improve error messages for users	Note business opportunity in technologies that bootstrap over DNSSEC
Operating System Vendors	Microsoft, Apple, Linux, mobile platforms (Mac iOS, Android, Windows Mobile, RIM QNX)	Implement and, by default, have validation turned on	Best common practices for DNSSEC in OSs are necessary and will help take advantage of opportunities that DANE, etc. will enable
Content Distribution Networks	Akamai, Cotendo, Limelight	Implement DNSSEC on the signing side	Deploy DNSSEC, even if as a for-pay service; note demand from brand-savvy enterprises
Industry Leaders	Google, Amazon, key news organizations (*N.Y. Times*, *Wash. Post*, CNN), Facebook, LinkedIn	Sign their zones and tout having done so	Promote perceptions of your enterprise as a technology leader while securing your DNS operations and brand
Industry Thought-Leader Organizations	INTA, BITS (banking), American Bar Association (attorneys), AMA or others (medical), MPAA, NCTA, others	Include DNSSEC as a recommended practice for their members	Emphasize safety, and cachet of being able to tout increased security to members—and their customers, who are likely quite sensitive to such issues
Corporate Network Managers	CIOs of Fortune 500 companies and the U.S. government	Sign their zones; require their trade partners to do the same	Note that DNSSEC will make supply and distribution chains stronger and protect Fortune 500 companies' brands
ISPs	AT&T,	Permit, or not hamper,	Describe competitive

[43] Generally less than 8,000 bytes, with a best-practice limit of 4,000 bytes due to the danger of larger-sized packets being dropped as they traverse longer network distances

	Cablevision, CenturyLink, Comcast, Cox, Sprint, Time Warner Cable, Verizon	validation on end systems and provide validation service for customers, i.e. level B or A per U.S. FCC report (download PDF here)	pressure from early-adopting ISPs and potentially, pressure from regulatory agencies
DNS Lookup Services	OpenDNS, Google, Amazon	Permit, or not hamper, validation on end systems and provide validation service for customers, i.e. level B or A per U.S. FCC report (download PDF here)	Describe competitive pressure from early-adopting services and potentially, pressure from regulatory agencies

Appendix 5: List of acronyms

AES	Advanced Encryption Standard
API	Application programming interface
ccTLD	Country-code top-level domain
CDN	Content delivery network
CIO	Chief information officer
CSRIC	Communications Security, Reliability, and Interoperability Council
DANE	DNS-based Authentication of Named Entities
DES	Data Encryption Standard
DHS	Department of Homeland Security
DKIM	DomainKeys Identified Mail
DLV	DNSSEC Look-aside Validation
DNS	Domain Name System
DNSKEY	DNS public key
DNSSEC	Domain Name System Security Extensions
DPS	DNSSEC practice statement
DS	Delegation Signer
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FSSCC	Financial Services Sector Coordinating Committee
GSA	General Services Administration
HIPAA	Health Insurance Portability and Accountability Act
HSM	Hardware security module
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol security
ISP	Internet Service Provider
IT	Information technology
KSK	Key-signing key
LDNS	Local domain name server
MOU	Memorandum of understanding
MTA	Mail transfer agent
NASA	National Aeronautics and Space Administration
NIST	National Institute for Standards and Technology
NSEC	Next Secure (data format)
NSEC3	Next Secure 3 (data format)
NSTIC	National Strategy for Trusted Identity in Cyberspace
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OS	Operating system
PCH	Packet Clearing House
PKCS	Public-key cryptography standards
PKI	Public-key infrastructure

PMTU	Path maximum transmission unit
RFP	Request for proposal
RR	Resource record
RSA	Encryption standard developed by RSA, Inc.
SHA	Secure hash algorithm
SPF	Sender Policy Framework
SSL	Secure Sockets Layer
TDES	Triple Data Encryption Standard
TLD	Top-level domain
TLS	Transport layer security
TTL	Time to live
USB	Universal serial bus
VoIP	Voice over Internet Protocol
ZSK	Zone-signing key