



Registrar DNSSEC Readiness Report

A survey of domain name registrars' readiness to provide Domain Name System Security Extensions services to domain name owners.



www.afilias.info

August 2010

Introduction

2010 has seen significant advancement in the deployment of Domain Name System Security Extensions (DNSSEC). Indeed, a key driving factor in DNSSEC adoption over the last few years has been the efforts of .ORG, The Public Interest Registry and their strategic initiatives to improve the security of the .ORG domain by deploying DNSSEC.

As technical services provider to .ORG, Afilias helped PIR craft and rollout a careful and smooth introduction of DNSSEC for the .ORG domain. But even with significant media attention and advancements such as deploying DNSSEC in the Internet root zone, DNSSEC adoption among domain name registrars is still in a nascent stage.

It is Afilias' belief that the next wave of DNSSEC effort must be geared towards registrars, helping them deploy DNSSEC for their customers and helping them tackle the technology changes required within the registration process. Without support from registrars, DNSSEC can never be broadly adopted by domain name owners and organizations who will never receive the ultimate security benefits if provides.

To assess registrar readiness and identify areas where Afilias may help, Afilias conducted an electronic survey of registrars across all 15 top-level domains (TLDs) for which Afilias provides domain name registry and DNS services. Our **Registrar DNSSEC Readiness Report** details the findings of this research survey and outlines the state of deployment, adoption and interest in DNSSEC among domain name registrars worldwide.

Methodology

Afilias conducted an electronic survey between August 9 and August 16, 2010. Invitations to participate in this survey were sent via e-mail to all registrar contacts for the gTLD and ccTLD domain name registries that Afilias supports. Our database included over 3000 contacts inclusive of administrative, technical and executive members of registrar organizations that register domain names. Afilias received 71 responses to the electronic survey, for a response rate of 2.13 percent, in line with expectations.

Executive Summary

Afilias' survey confirms that, while registrars support DNSSEC, most do not yet feel fully prepared to offer DNSSEC services to domain name owners. In fact, registrants likely will not see broadscale availability of DNSSEC services from their registrars before 2011, or even later.

Registrars cite a number of factors influencing their deployment timing for DNSSEC. In addition to the expected technical training and development issues, most registrars cite a current lack of user demand for these services which makes immediate investment in DNSSEC a lower priority for the business.

Highlights of our research include:

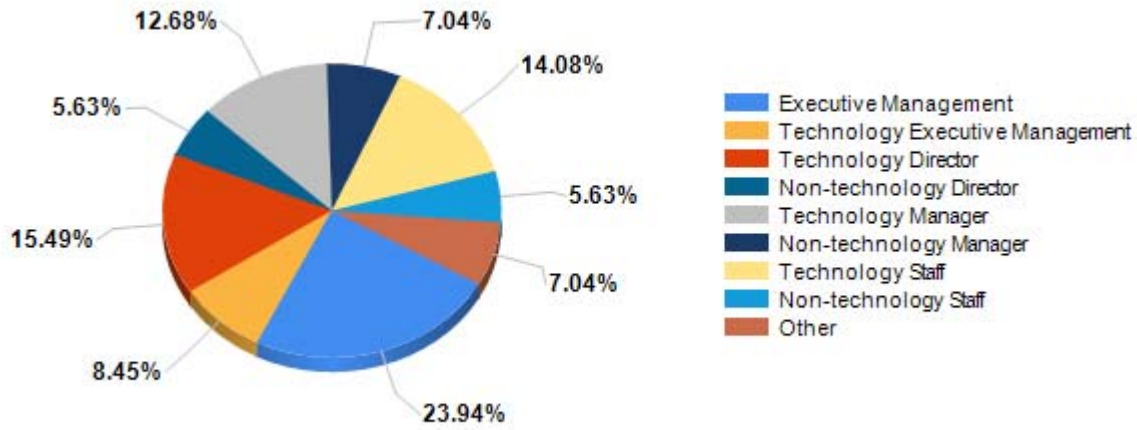
- **Registrars think DNSSEC is a good idea, but are not yet fully prepared to offer consumer services.** 80% of registrars believe that top-level domain (TLD) registries should offer DNSSEC. However 90% of registrars currently feel completely unprepared or only somewhat prepared to actually offer DNSSEC services to their customers at this time.
- **69% of Registrars plan to offer DNSSEC services in 2011 or beyond.** 32% have no plan to introduce DNSSEC within the next 12 months. Less than 3% of registrars indicated that DNSSEC was an extremely high priority for them. In fact, a combined total of 70% rated the priority of DNSSEC as average or lower.
- **Registrars are not yet experts in DNSSEC.** Most respondents rated both their own and their technical team's knowledge of DNSSEC as *Intermediate* or *Somewhat knowledgeable*. Overall, technical teams were rated as having more knowledge of DNSSEC (42% rated their Technical teams as Intermediate) than the individual respondent (36% rated themselves as Intermediate).
- **Consumer demand is the biggest challenge for registrars.** 56% cite a lack of consumer demand as their biggest challenge impeding their DNSSEC implementation. Other top issues that are standing in the way of registrars' plans to rollout DNSSEC include project prioritization and developing a process of key management, including storage and rollover.
- **Registrars also cite issues with deploying DNSSEC technology.** While user-demand for DNSSEC services was ranked as the number one concern by the greatest percentage of registrars (29.5%), key management (19.7%) and DNSSEC technology and expertise (18.3%) also factored as registrars' number one concern. Many registrars (over 36%) indicated that they were still in the planning stages and did not know exactly how they would sign domains.

In summary, DNSSEC represents an historic enhancement to Internet security, but much more work is needed before the domain distribution channel, a key to broadscale acceptance, is prepared to deploy. This research shows not only the extent of preparedness, but suggests areas of focus that can accelerate deployment.

Respondent Demographics

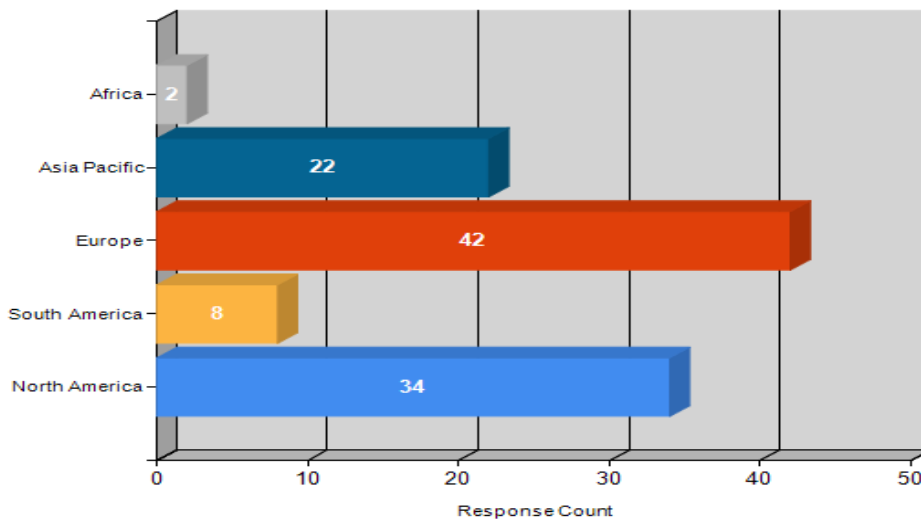
Respondents to this survey represented a variety of roles within the organization. The greatest number of responses were from Executive Management (23.94%), Technology Directors (15.49%) and Technology Staff (14.08%). This data confirms that the survey results represent both the business and technical issues of DNSSEC deployment, as this distribution of respondents contains the key groups of decision makers for new product development, business strategy and technical capability to deploy DNSSEC.

What is your role in the organization?



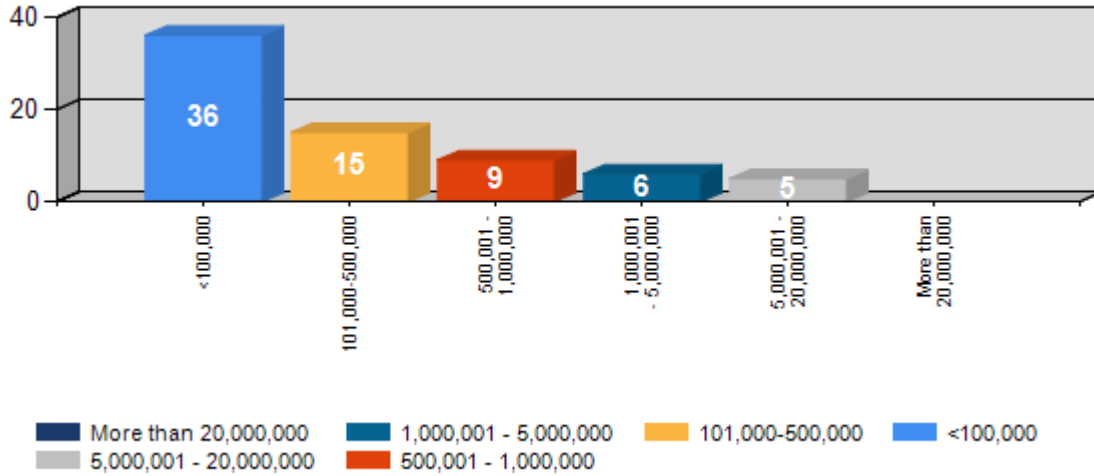
Survey respondents also represent the world’s largest registration markets. The majority of respondents do business in Europe and North America. This correlates to both the highest registration markets and the geographies that have seen the most attention toward DNSSEC. However, some of our respondents do business in Asia Pacific and South America. Nearly none of the respondents do registration business in Africa.

What region(s) of the world is your primary source of business?



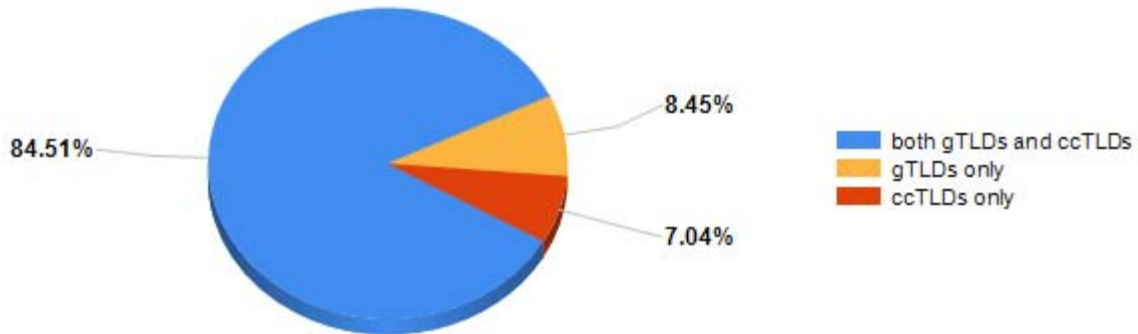
Responses to this survey were obtained from all sizes of registrars, from those with a few thousand domains under management, to those with over 5 million. Interestingly, the largest respondent group was registrars with less than 100,000 domains under management.

How many domain name registrations does your registrar manage (including reseller portfolios)?



Survey respondents also represented the majority of the available domain names in the registration market. Nearly 85% of respondents offer both gTLD and ccTLD registration services.

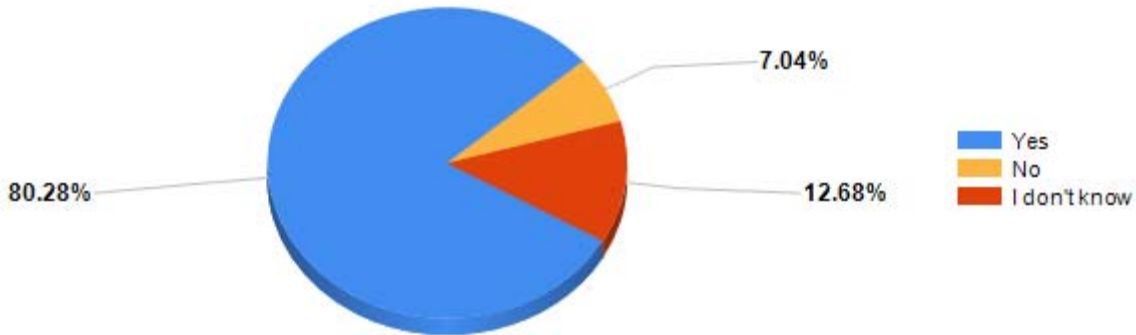
Which top-level domains does your registrar offer for sale?



Registry Support for DNSSEC

There is general support for the work that many TLD registries have already put into DNSSEC deployment. The majority of registrars, over 80%, think that TLD registries should offer DNSSEC.

Do you think TLD registries should offer DNSSEC?



Although .ORG already offers signed second level delegations (the ability for domain name registrants to deploy DNSSEC for their specific name), we also asked Registrars which TLDs should offer this service as well. Not surprisingly, registrars consider .COM to be the most important TLD to offer signed delegations. Of those respondents that said TLD registries should offer DNSSEC, over 91% indicate .COM as the most important to offer second level signed delegations followed by .NET at 80%, .ORG at over 73%, and ccTLDs at over 59%. .INFO followed closely at nearly 58%.

If you think registries should offer DNSSEC, which top-level domains in particular are the most important to offer second level signed delegations?

Choice	Response Percent
.com	91.23 %
.net	80.70 %
.org	73.68 %
.info	57.89 %
.biz	45.61 %
Other gTLDs	28.07 %
ccTLDs	59.65 %
None in particular	5.26 %

Knowledge and expertise

Most respondents rank both their own, as well as their technical team’s, knowledge of DNSSEC as *Intermediate* or *Somewhat Knowledgeable*. Overall, technical teams were rated as having more knowledge of DNSSEC (42% rated as *Intermediate*) than the individual respondent (36% rated as *Intermediate*).

While an *Expert* rating was much lower, it is encouraging that only about 5 percent of either group indicated that there was no knowledge at all within their organization about DNSSEC.

Please rate your personal knowledge of DNSSEC.

Choice	Response Percent
Expert	9.86 %
Intermediate	36.62 %
Somewhat knowledgeable	47.89 %
No knowledge at all	5.63 %

Please rate the DNSSEC knowledge of your technical team.

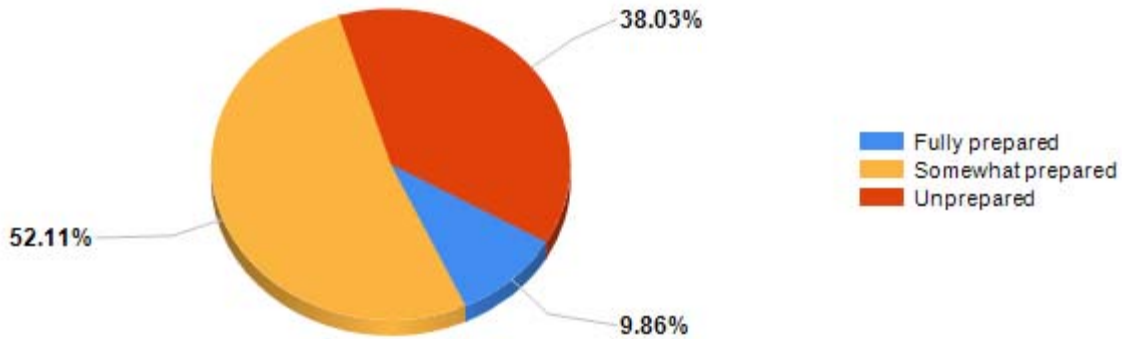
Choice	Response Percent
Expert	19.72 %
Intermediate	42.25 %
Somewhat knowledgeable	32.39 %
No knowledge at all	5.63 %

Registrar Preparedness

Only less than 10% of registrars feel fully prepared to offer DNSSEC services to registrants today.

The majority of registrars (90%) feel that they are only somewhat prepared (52%) and over 38% feel that they are completely unprepared to offer these services.

How prepared is your registrar to offer DNSSEC services to your registrants TODAY?



Market Availability of DNSSEC services

Most registrars (69%) will not offer DNSSEC services until 2011 or beyond. Of our respondents, 37% indicated they planned to offer DNSSEC in 2011, and another 32% indicated they had no plan to offer DNSSEC within the next 12 months. Approximately 15% indicated that they would offer DNSSEC services by the end of 2010.

When is your registrar likely to offer DNSSEC services to registrants?

Choice	Response Percent
2010	15.49 %
2011	36.62 %
We have no plan to offer DNSSEC within the next 12 months.	32.39 %
We already offer DNSSEC services	15.49 %

In addition, nearly 30% of registrars rated DNSSEC as a high or extremely high priority for their business in 2010 and 2011. However, nearly 20% rated DNSSEC as a low priority.

Combined, 70.42% rated the priority of DNSSEC as average or lower.

Less than 3% indicated that DNSSEC was an extremely high priority.

Where does implementing DNSSEC fall in your registrar's business priorities for 2010 or 2011?

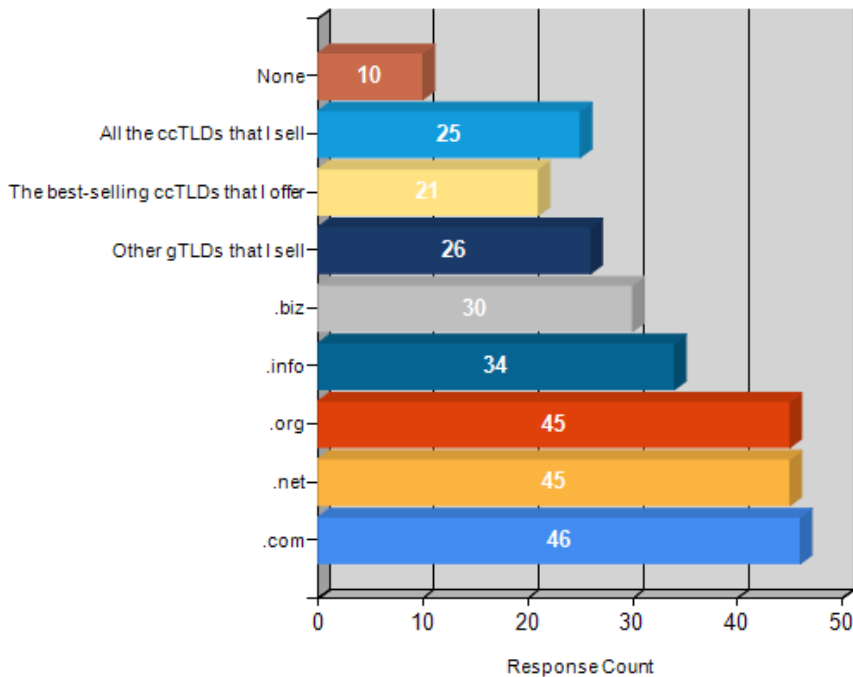
Choice	Response Percent
Extremely high	2.82 %
High	26.76 %
Average	36.62 %
Somewhat important	14.08 %
Low	19.72 %

DNSSEC availability among domains

Interest in offering DNSSEC services appears to be highest in .COM, .NET, and .ORG, with .INFO not far behind. This result, however, is not surprising, as it follows in line with overall registration volume. This directional information indicates that registrars plan to provide DNSSEC services for the most popular domains.

Interestingly though, we did seek to find out whether the registrars indicated any perceived difference in whether “best selling ccTLDs” that do more volume would be better candidates for DNSSEC services than simply their entire ccTLD portfolio. More registrars indicated that they would offer DNSSEC across all their ccTLDs, than only their best selling ones. This trended closely with the percent that would offer DNSSEC in gTLDs other than .COM, .NET, .ORG, .INFO, and .BIZ.

Among which top-level domains do you plan to offer DNSSEC services?



Choice	Response Percent
.com	64.79 %
.net	63.38 %
.org	63.38 %
.info	47.89 %
.biz	42.25 %
Other gTLDs that I sell	36.62 %
The best-selling ccTLDs that I offer	29.58 %
All the ccTLDs that I sell	35.21 %
None	14.08 %

Factors impeding DNSSEC implementation

While there are a considerable number of factors that registrars say are impeding their implementation, in our survey just a few stood out as the most influential factors. These are:

1. Lack of customer demand
2. That other projects have a higher priority
3. Developing a process of key management, including storage and rollover

The technical effort needed to develop a signing technology and lack of in-house resources also appear to be significant constraints for registrars.

While user demand may evolve as more TLDs are signed, clearly registries must do a good job of making DNSSEC implementation easy for registrars so that it can fit into their busy development and release schedule. It is our belief that additional education regarding key management can help registrars in determining the best software and hardware solutions.

What do you consider the main problems impeding your DNSSEC implementation?

Choice	Response Percent
Developing signing technology	21.13 %
Developing a process for key management including storage and rollover	39.44 %
Redesigning our customer user interface	26.76 %
Lack of customer demand	56.34 %
Other projects have a higher priority	46.48 %
DNSSEC is too expensive to implement	7.04 %
I can't convince upper management of the value of DNSSEC	7.04 %
Lack of in-house resources	25.35 %
Lack of in-house expertise	14.08 %
We have no technical problems preventing our delivery of DNSSEC services	8.45 %
We already provide DNSSEC services	11.27 %
Other	7.04 %

We also asked registrars to rank order some significant DNSSEC issues by their concern level. User-demand for DNSSEC services was ranked as the number one concern by the greatest percentage of registrars (29.5%). However, key management (19.7%) and DNSSEC technology and expertise (18.3%) also factored as registrars number one concern.

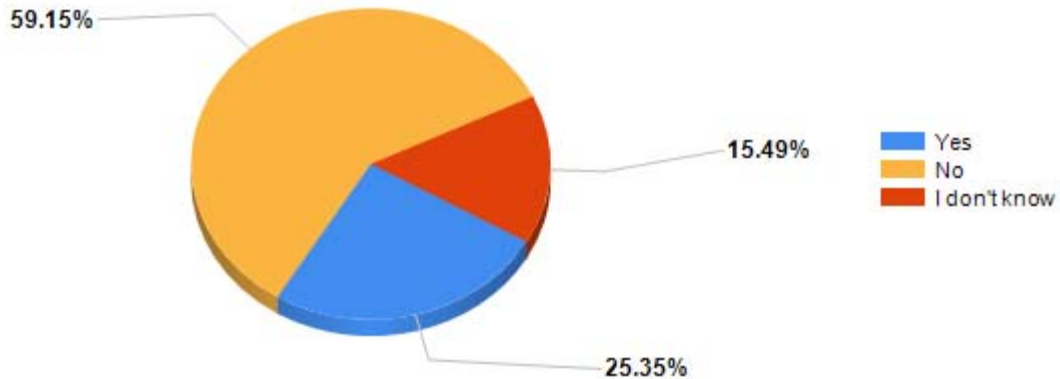
It is important to note that the effect of DNSSEC on DNS queries and traffic was most often ranked the least item of concern (32.4% of respondents).

Important issues like DNS and domain name ownership transfers fall somewhere in the middle. This is perhaps because the first step in the implementation process is tackling the deployment issues themselves.

Thinking about DNSSEC Deployment, how would you rank issues you are most concerned about (1 to 7), 1 being most concerned, 7 being least concerned

	Total for 1	Total for 2	Total for 3	Total for 4	Total for 5	Total for 6	Total for 7	Total Selected
DNS queries/traffic	8	7	4	7	8	14	23	71
DNS transfers	3	14	18	18	6	6	6	71
DNSSEC technology and expertise	13	7	12	17	8	11	3	71
Domain transfers	9	17	12	9	10	7	7	71
Key management (generation, storage, rollover)	14	14	8	9	14	9	3	71
User Interface design	3	6	13	7	11	17	14	71
User-demand for DNSSEC services	21	6	4	4	14	7	15	71

Does your customer base exhibit any demand for DNSSEC services?

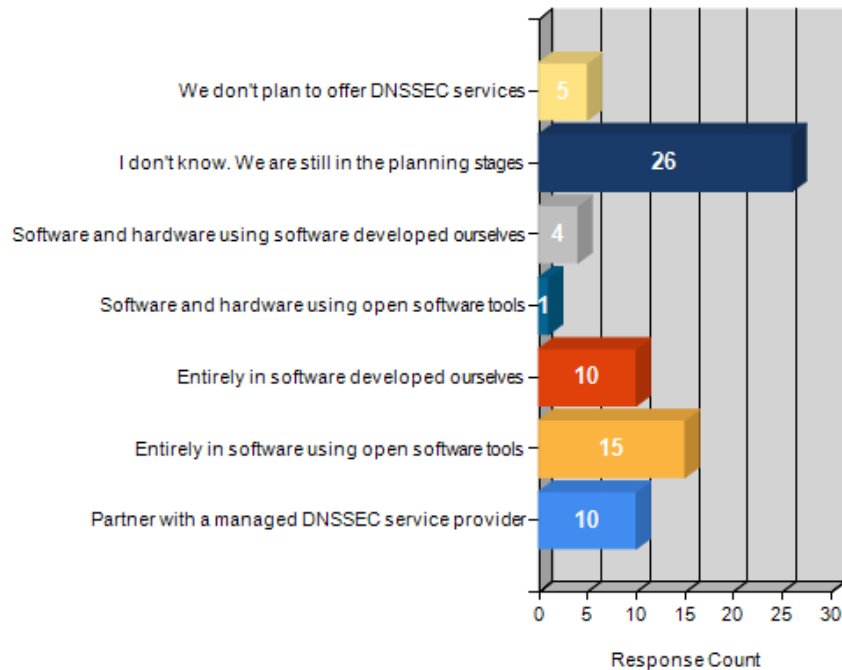


Technology Deployment

Registrars have a number of technical challenges in deploying DNSSEC, not least of which is delivering an end-user service that integrates with their existing registration services and meets their usability needs. We therefore asked registrars how they expected to sign their customers' domains with DNSSEC. Most registrars (over 36%) indicated that they were still in the planning stages and did not know exactly how they would sign domains.

The next largest group (over 21%) indicated that they would entirely use software, or software-based tools to do their signing. Exactly the same percentage of registrars plan to buy as plan to build. That means that just as many registrars are considering buying a managed service to fulfill their DNSSEC needs, as are considering developing software themselves.

How do you expect to sign domains with DNSSEC?



Choice	Response Percent
Partner with a managed DNSSEC service provider	14.08 %
Entirely in software using open software tools	21.13 %
Entirely in software developed ourselves	14.08 %
Software and hardware using open software tools	1.41 %
Software and hardware using software developed ourselves	5.63 %
I don't know. We are still in the planning stages	36.62 %
We don't plan to offer DNSSEC services	7.04 %

Conclusion

Afilias believes that this directional research confirms that, while DNSSEC is an endeavor supported by the industry, registrars require more technical tools, training and resources before they will be fully prepared to roll out DNSSEC services to registrants.

The timing indicated by registrars for future availability of these services may mean that they are waiting for a tipping point with the .COM registry until they consider devoting more resources to its deployment.

Afilias expects that the additional efforts of domain name registries to sign their TLDs with DNSSEC in 2010 and 2011 will contribute to the expansion of DNSSEC awareness and that registrars will begin to see increases in user demand for these services.

Most concerning to Afilias is that 90% of registrars currently feel completely unprepared or only somewhat prepared to actually offer DNSSEC services to their customers as this time. Also concerning are a low *Expert* level rating of DNSSEC knowledge, and key challenges of key management and technology deployment.

Afilias believes that these results indicate the need for more outreach, education, and tools for registrars to help ease their implementation burden. Further, registries would be wise to ensure that their DNSSEC deployments are as uniform as possible so that registrars can minimize their development efforts and have the greatest expectation that DNSSEC best-practices will work the same across the domain name landscape.