Report on the ccNSO's DNSSEC Survey 2009

Background Information

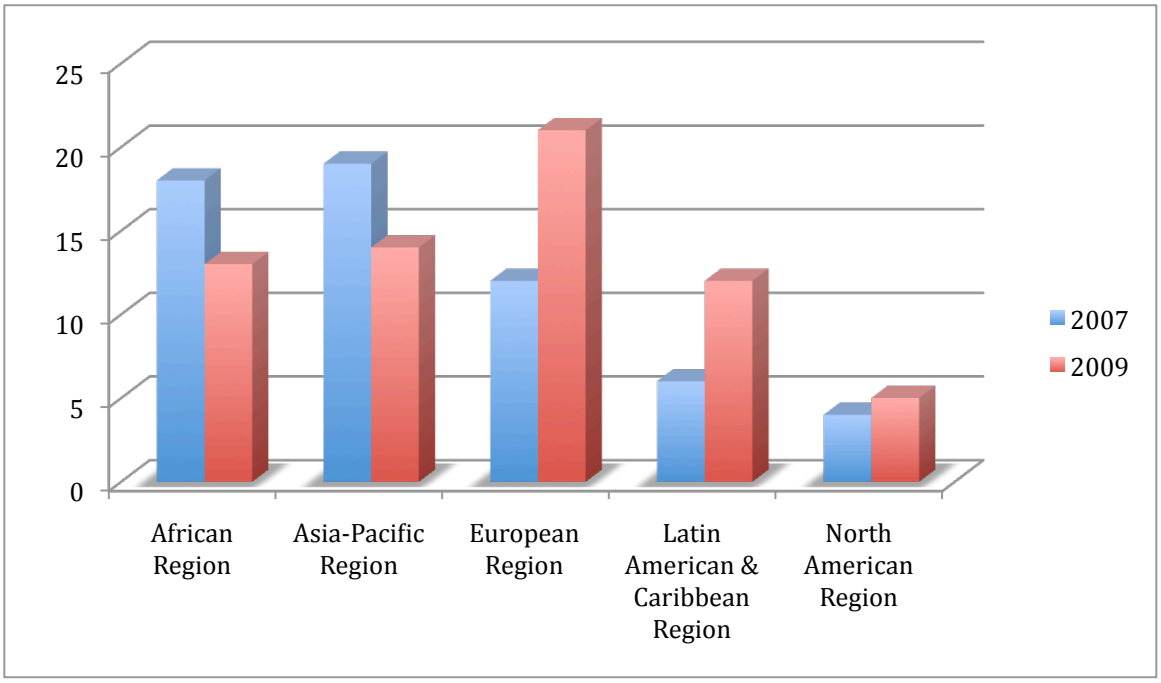
The 2009 DNSSEC Survey was initiated after.SE, the Swedish registry and ENISA, the European Network and Information Security Agency requested updated information to the DNSSEC survey conducted by the ccNSO in 2007.

The ccNSO Council approved the re-launch of the survey in May 2009 and suggested a slight re-draft in order to better reflect the current situation. As a result, some questions were added, others slightly reformulated.

The 2009 survey was implemented using an online survey tool, whilst the 2007 survey was compiled manually. This might have a slight effect on some questions, as the 2007 survey gave the respondents a higher flexibility of adding "alternative" answers outside the pre-defined options

The survey was launched on the 24th June 2009 and closed on the 7th September 2009.

1. Your Top Level Domain

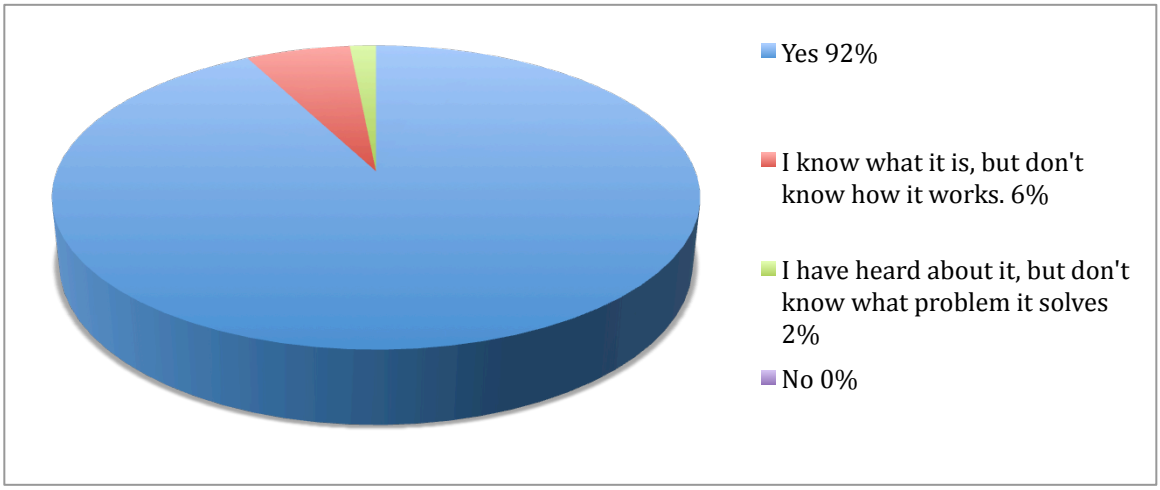


In total 65 valid replies were received, a small improvement to the DNSSEC survey from 2007, which received 61 valid replies. Whilst there were noticeably more replies from the European and Latin American regions, the African and Asia-Pacific regions contributed less than in 2007.

According to the ICANN regions, the spread of the replies was as follows (the numbers from 2007 in brackets);

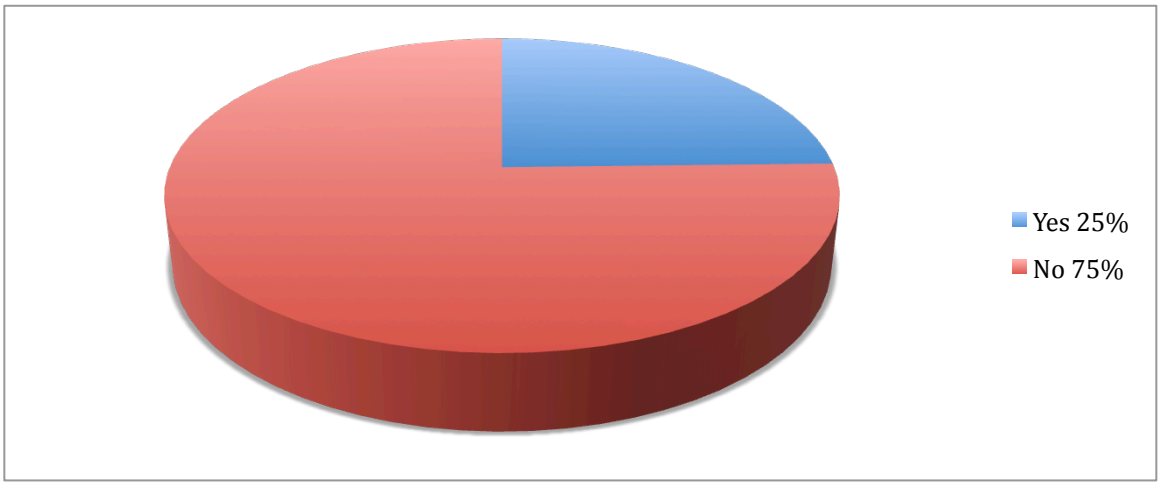
African Region: 13 (18)
Asia-Pacific Region: 14 (19)
European Region: 21 (12)
Latin America and Caribbean Region: 12 (6)
North American Region: 5 (4)

2. Do you know what DNSSEC is?



The awareness of what DNSSEC is and how it works has improved slightly compared to 2007's results. Only 8% in total indicated they do not feel confident on the subject, but no one indicated they had never heard of it. In 2007, this number was 5%.

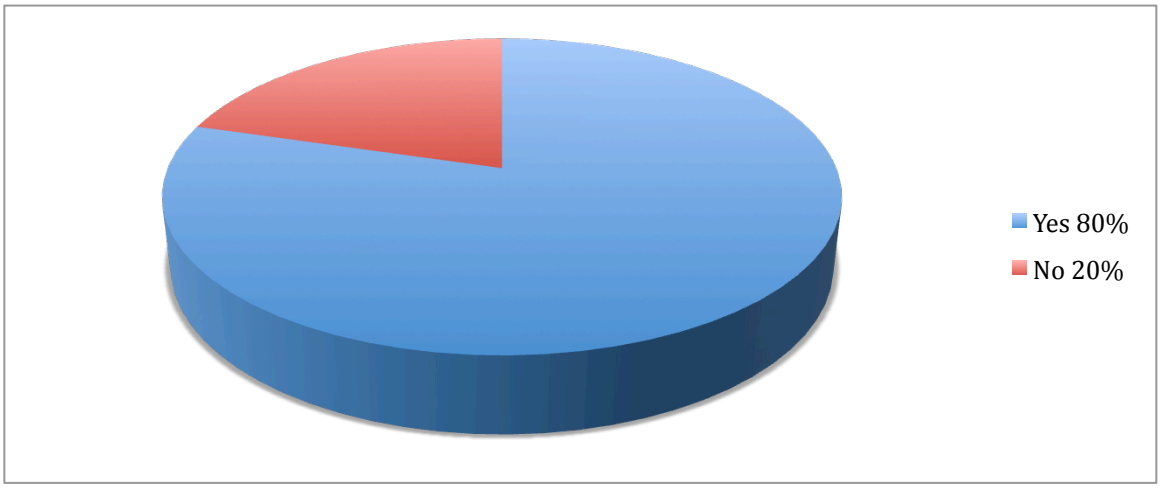
3. Has your registry implemented DNSSEC, or is actively implementing DNSSEC?



25% of the respondents indicated they had, or are actively implementing DNSSEC - a clear increase since 2007, where only 7% indicated they had implemented DNSSEC, another 5% were in a testing phase.

The second part of the question *("/…/ or is actively implementing DNSSEC")* was added to the question in the 2009 survey and could have some impact on the replies.

4. Do you plan to implement DNSSEC?



Amongst the respondents who had not implemented DNSSEC, a clear majority still indicates they intend to implement DNSSEC (80%). This number was somewhat higher in 2007 (85%), probably because some of the respondents then already use DNSSEC today.

However, the group of registries who do not intend to implement DNSSEC has clearly become larger: 20% in 2009's survey, compared to 10% in 2007 (another 6% indicated they were "unsure" in 2007).

All of the respondents from the North American region had, or had plans to implement DNSSEC in their region, followed by 93% of the respondents from the African region and 83% of the Latin American & Caribbean region. 81% of the European respondents indicated they either had, or were planning to implement DNSSEC, followed by the Asia-Pacific region, were 79% indicated they had, or would do so.

5. Please, briefly explain why you do not intend to implement DNSSEC in the next three years:

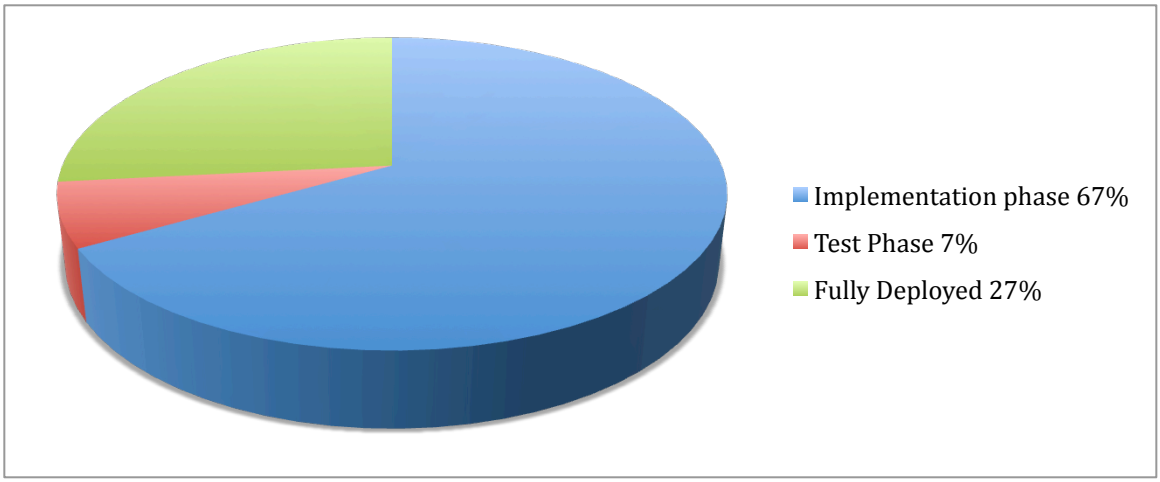
Whilst many of the respondents declared that they might implement DNSSEC within a few years, they often indicated that the registry either had other priorities at the moment, or that there was a lack of technical and financial resources for such a project (both mostly mentioned by minor registries).

Other frequently mentioned issues were that there was no actual demand for the service, that it was overly complicated and that there were several technical and operational issues left to be solved before it would become useful.

One respondent waited for the outcome of the ongoing internal test bed before they would decide how to proceed.

Compared to the DNSSEC survey from 2007, the reasons mentioned are close to those mentioned two years ago, with the exception that the lack of a signed root zone no longer is an issue.

6. [NEW] For DNSSEC, what implementation phase are you in now?



This question was added to 2009's survey, in order to find out how far the implementation of DNSSEC had proceeded amongst those who indicated they either had, or were actively implementing DNSSEC.

The vast majority either had already fully deployed DNSSEC, or was in the implementation phase.

7. Please, briefly describe the technical environment you use for DNSSEC:

The responses to this question varied to a high degree, however, following tendencies could be defined:

- Various UNIX based platforms were used
- Several utilised OpenDNSSEC
- Most rely on BIND
- Most use HSMs or smartcards

Compared to the 2007 survey, there were no notable changes in methodology except the use of better tools (e.g. OpenDNSSEC).

The individual answers to this question are attached in appendix 1 (randomly presented, with the name of the ccTLD removed).

8. Please, briefly describe your experience in implementing DNSSEC:

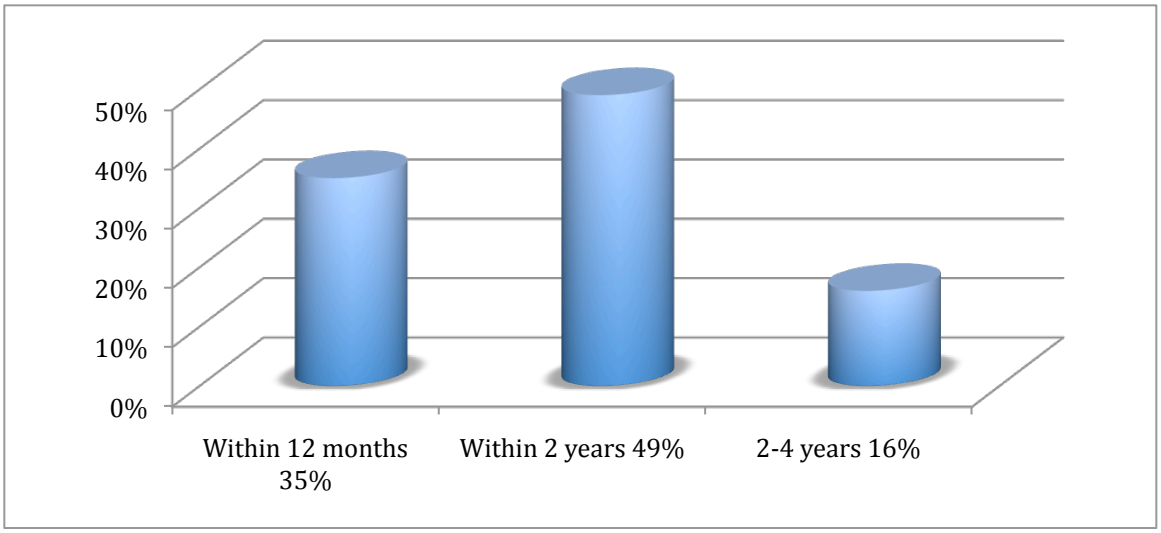
The general feeling was that it was relatively easy to deploy DNSSEC and that it created less work than expected. Some of the respondent had a test deployment prior to production, which was perceived being useful.

However, there were also directly contradicting opinions, indicating that the implementation phase was cumbersome, mainly caused by a low interest from registrars. The deployment of NSEC3 was also hard due to lack of third party support. There was furthermore a lack of general documentation and poor software support.

It was also mentioned that the registries had to implement new policies and procedures when deploying DNSSEC.

The nature of the replies from 2009 compared to 2007 suggests that thinking has matured somewhat on DNSSEC, with more experience in DNSSEC deployment and the challenges more about educating other groups like registrars, rather than registries themselves learning the techniques.

9. What is the planned timeline for implementing DNSSEC?



Almost half of the respondents indicated they plan to implement DNSSEC within the next two years, 35% plan to implement it within the next 12 months. This means that 84% of the respondents in total foresee DNSSEC to be implemented in 2011, latest.

In 2007, 45% estimated to have DNSSEC implemented within one to two years (33% within 12 months, 12% within two years). Today, we can see that only 18% actually did manage to implement it within two years (see replies to question 3 *"Has your registry implemented, or is actively implementing DNSSEC?").*

Some of the reply options slightly changed compared to the 2007 survey, ("3 years" was an option instead of "2-4 years" and "No set timeline" was an additional option).

10. Please, describe the technical environment you plan to use to implement DNSSEC:

A large part of the respondents did not have their technical environment defined yet, including several of those who had indicated they plan to implement DNSSEC within the next 12 months.

However, those who had defined their technical tools were mostly looking to deploy their own solutions in line with those already deployed. A minority is planning to outsource the job of signing to a vendor.

Noticeably, most respondents only referred to the signing process for their zone, and little on registry interfaces, such as how to accept customer's keys.

The same kinds of issues in the 2009 survey were raised in the 2007 survey. There does seem to be more outsource vendor support for DNSSEC now, so registries can rely on third parties to do more DNSSEC work for them rather than doing it alone.

The individual answers to this question are attached in appendix 2 (randomly presented, with the name of the ccTLD removed). Those indicating they had not yet defined their technical environment are not presented.

11. Please, describe how strategically important you consider DNSSEC to be. (Please, explain what the principle drivers are, the goals you would like to achieve with DNSSEC and the main threats and opportunities you foresee):

Not surprisingly, the improvement of DNS security was the most frequently mentioned reason for the deployment of DNSSEC. Issues such as the cache poisoning and pharming were frequently brought up. Some ccTLDs also indicated "securing IDNs" as one of the principle drivers for using DNSSEC. A few registries mentioned that they had to respond to demands from their country's authorities that were interested in seeing DNSSEC deployed. Some registries thought that using DNSSEC was a good way of being able to offer "modern service" to their clients and that DNSSEC is the best option for common security problems available today.

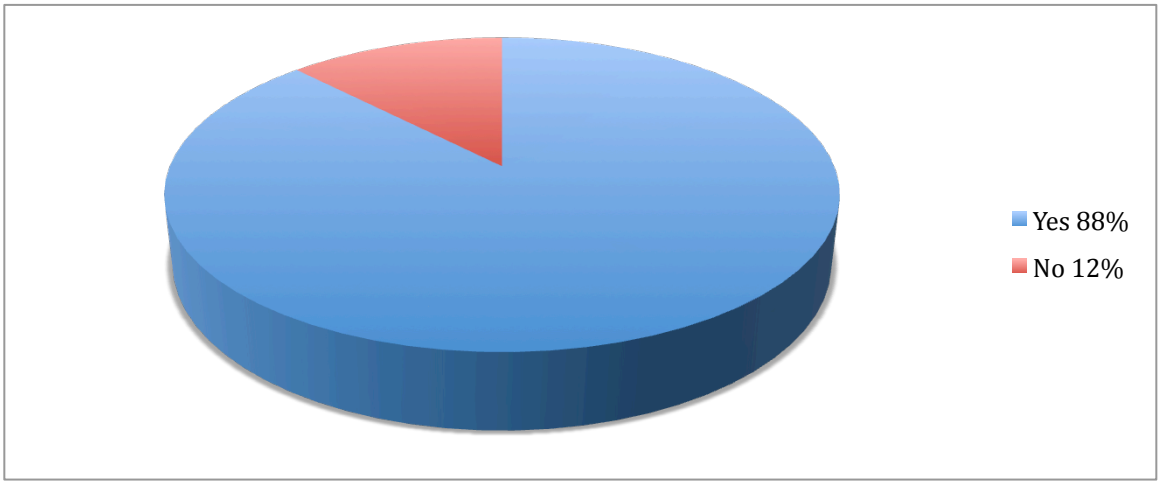
The most frequently mentioned 'major threat' that registries perceived, was a too great expectation in what DNSSEC actually is able to solve. The belief that DNSSEC can fix all security problems was envisaged to be a security problem in itself.

Other issues mentioned were cooperation problems with registrars and ISPs and the complexity in implementing DNSSEC. Furthermore, it was frequently mentioned that the registry actually cannot see any demand in the country; some even considered DNSSEC being a "marketing gimmick".

The replies from 2007 are mentioning similar issues except that "the lack of a signed root zone" was one of the most frequently mentioned problems then. This is not an issue today. Another noticeable change is the fact that much less respondents today mentioned they lack understanding in the technology, compared to two years ago.

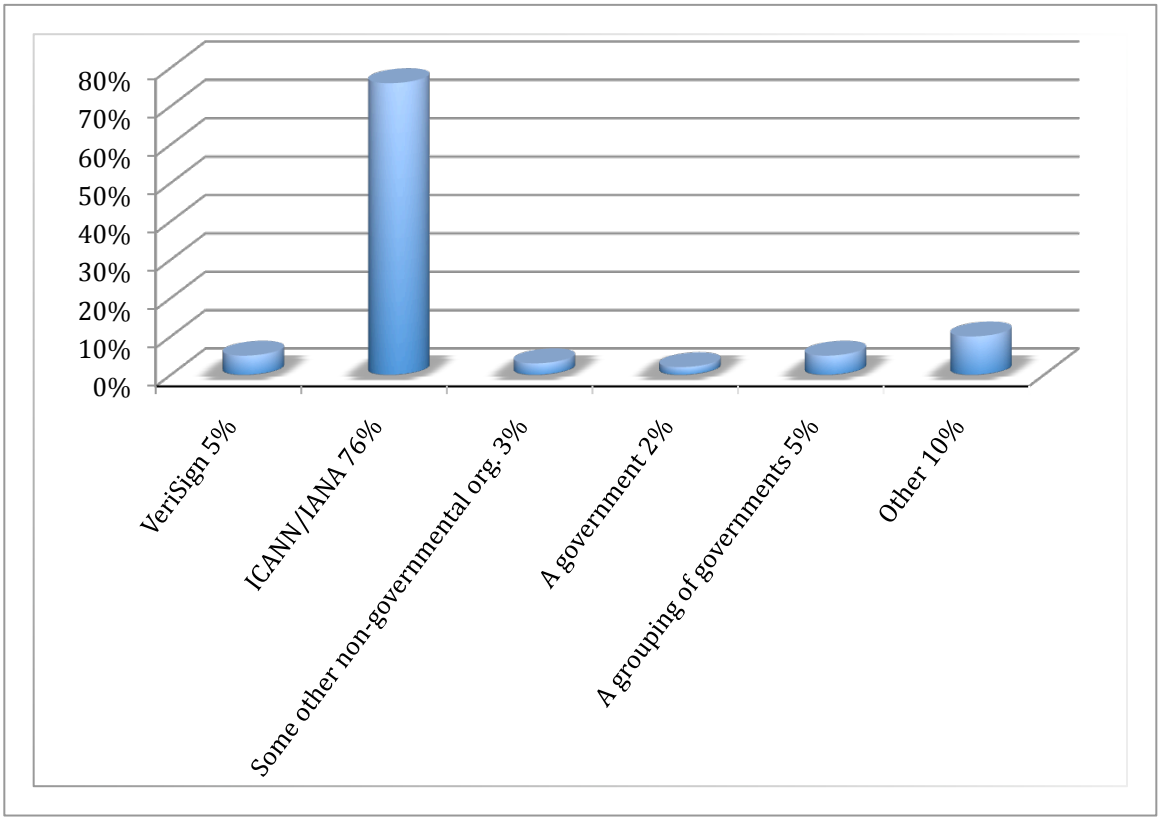
The individual answers to this question are attached in appendix 3 (randomly presented, with the name of the ccTLD removed).

12. Is it important to you that the DNS root zone is signed?



The opinion on the importance of a signed root zone is stable – the vast majority still considers this being important, with a slight increasing tendency – 88%, compared to 84% in 2007.

13. Who, in your opinion, should be the signer of the DNS root zone?



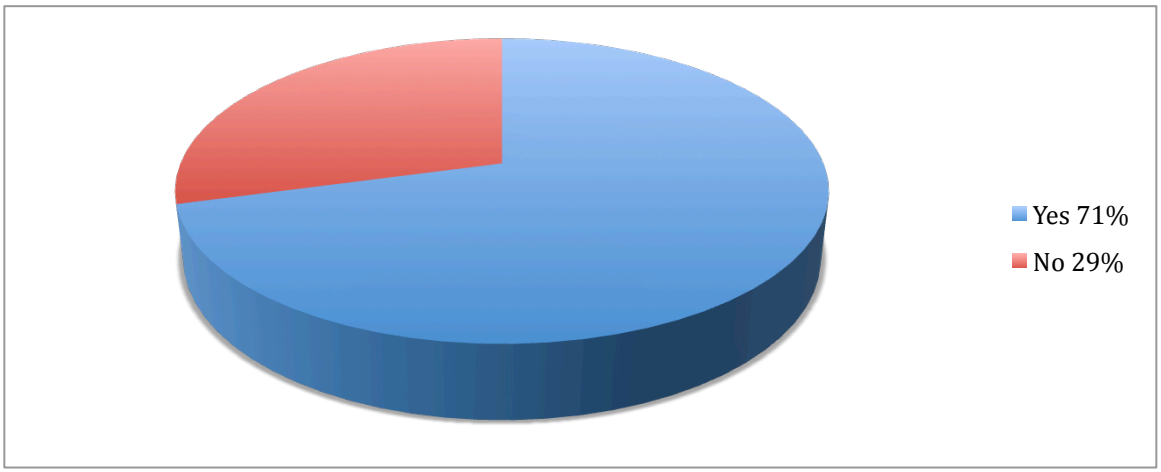
Just like in the 2007 survey, an overwhelming majority of the respondents represents the opinion that ICANN/IANA should be the signer of the root zone. The support for ICANN/IANA has even clearly increased compared to the previous study – from 68% in 2007 to 76% in 2009.

VeriSign was added as a new option in this year's survey, to reflect the U.S. Department of Commerce's announcement that VeriSign would manage and have operational responsibility for the Zone Signing Key in the interim arrangement to get the root zone signed. However, only 5% of the respondents supported VeriSign's role in this arrangement.

Whilst the support for ICANN/IANA as the root zone signer dominated in most regions, the African region differed considerably in this respect: Almost 40% of the respondents from this region declared they would like to see someone else than ICANN/IANA signing the root.

There was no clear trend in what the 10% of the respondents who had replied "Other" wished for. Some indicated they were happy with the current arrangement, others suggested that the root zone management should be split between IANA and VeriSign. Some called for a neutral and non-for profit organisation to manage the root zone signing, another respondent thought the signer should be "internationally agreed".

14. [NEW] Are you aware of the Interim Trust Anchor Repository (ITAR) provided by IANA?



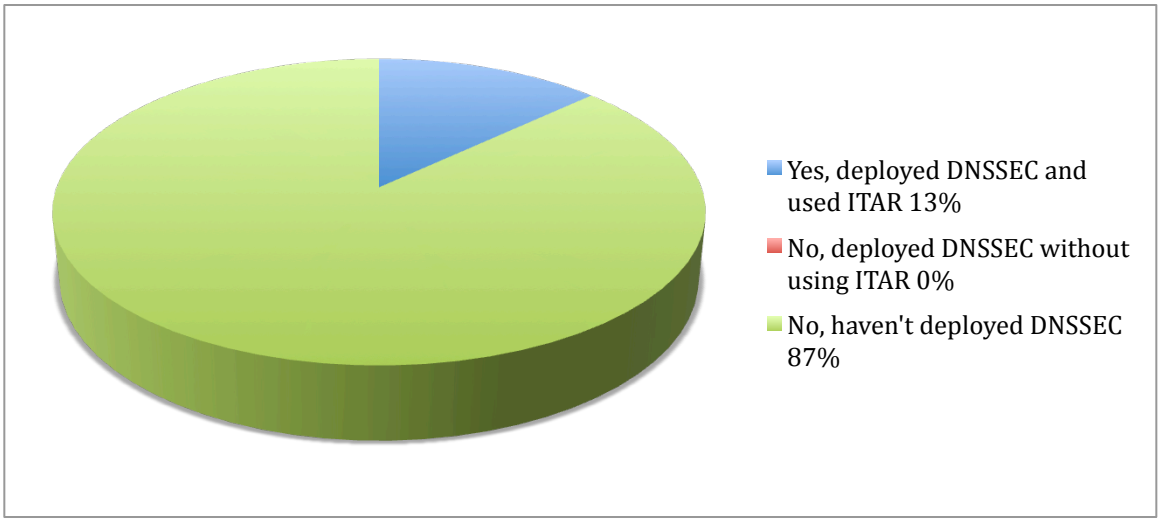
IANA's Interim Trust Anchor Repository (ITAR) was launched in January 2009, after a testing period involving a subset of TLDs in late 2008. It was announced on DNS operations mailing lists, DNSSEC-specific mailing lists, as well as at TLD operator forums like CENTR and ccNSO meetings.

Most of the respondents (71%) had heard about it, however almost 30% had not. The latter group contains a crosscut of minor to large registries, and almost 70% of these declared they are planning to implement DNSSEC.

The awareness of ITAR per region, according to the respondents:

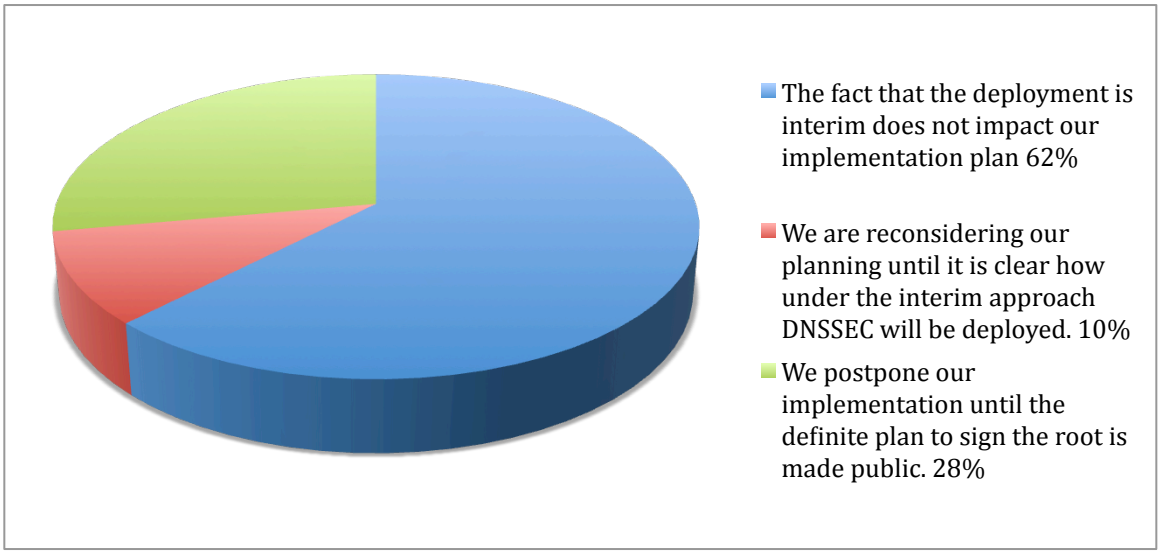
African Region: 69%
Asia-Pacific region: 57%
European Region: 81%
Latin American Region: 58%
North American Region: 100%

15. [NEW] Are you using ITAR for your registry?



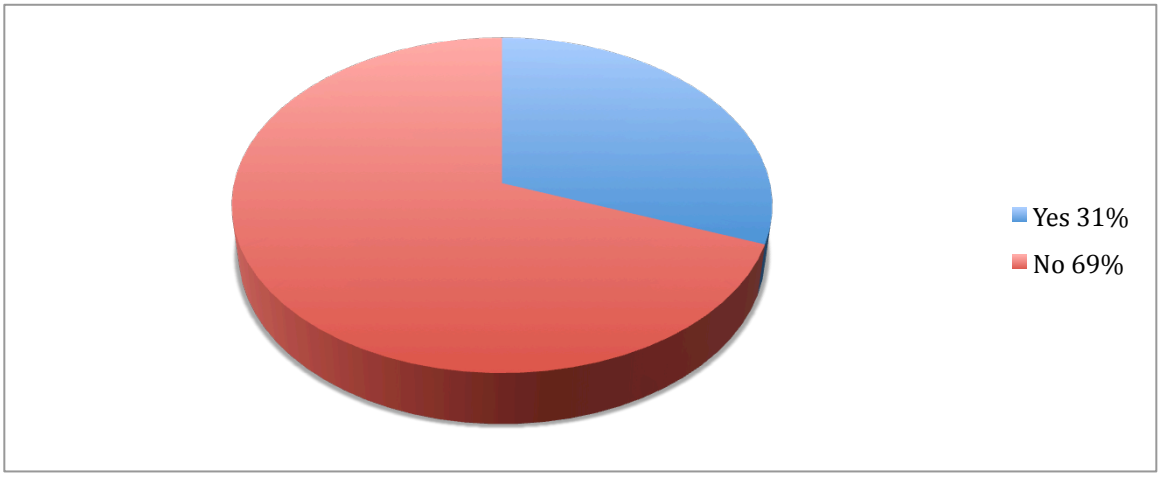
All of the respondents who had deployed DNSSEC were using ITAR.

16. [NEW] It was announced on 3 June that two agencies of the U.S. Department of Commerce, ICANN and VeriSign are working on an interim approach to deployment, by year's end, of DNSSEC at the authoritative root zone. What is your view?



Although most of the respondents indicated that the interim deployment plan of the U.S. Department of Commerce will not have any impact on their implementation plan (62%), a not to ignore amount of ccTLDs (38% in total) represent the opinion that the presented arrangement is concerning enough to either reconsider or postpone their implementation plans until the definite plan is presented.

17. [NEW] It was also identified that VeriSign will manage and have operational responsibility for the Zone Signing Key in the interim arrangement, and that ICANN will manage the Key Signing Key process. ICANN will work closely with VeriSign regarding the operational and cryptographic issues involved. Does the proposed arrangement concern you?



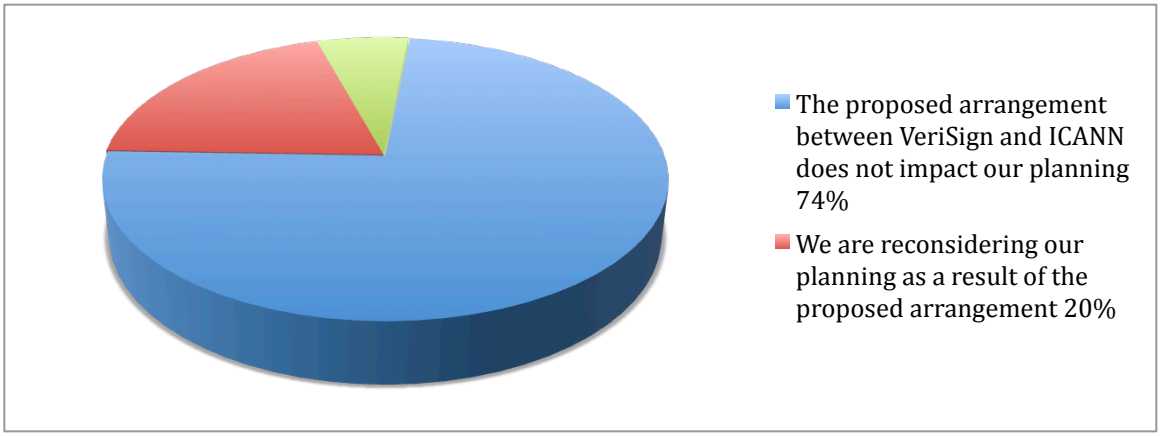
The proposed arrangement for signing the root zone does not concern the clear majority of the respondents. However, almost one-third of the respondents indicated that this poses concern for their registry.

18. [NEW] Please, explain your concerns about the proposed signing arrangement:

The main concern ccTLDs see in the arrangement seems to be VeriSign's commercial nature. It is felt that it is inappropriate that a for-profit company should be able to have control of the root zone, where sovereign countries are represented. Some registries say they do not even have any understanding for why VeriSign should have a role at all. Another concern is that the arrangement will force the moving of data back and forth, which creates additional possible points of failure.

The individual answers to this question are attached in appendix 4 (randomly presented, with the name of the ccTLD removed).

19. [NEW] Please, choose your view



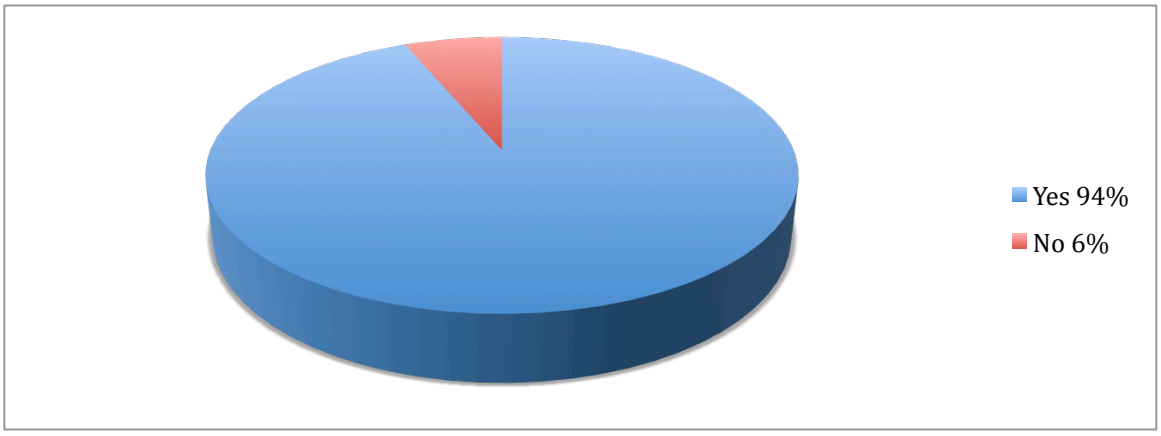
Quite corresponding to the results of the replies to question 16 and 17, almost 3/4th of the respondents (74%) indicated the proposed arrangement between VeriSign and ICANN does not impact their planning. 26% in total declared they will either reconsider their planning (20%), or even defer from implementing DNSSEC (6%).

20. [NEW] Please, explain your concerns that is causing you to reconsider or not deploy DNSSEC

The most frequently mentioned reason was that the debate is still ongoing and the outcome and implications are unsure. However, many also mentioned they were unhappy that the process was outsourced outside ICANN/IANA, for the reasons mentioned in the reply to question 18 (*"Please, explain your concerns about the proposed signing arrangement"*).

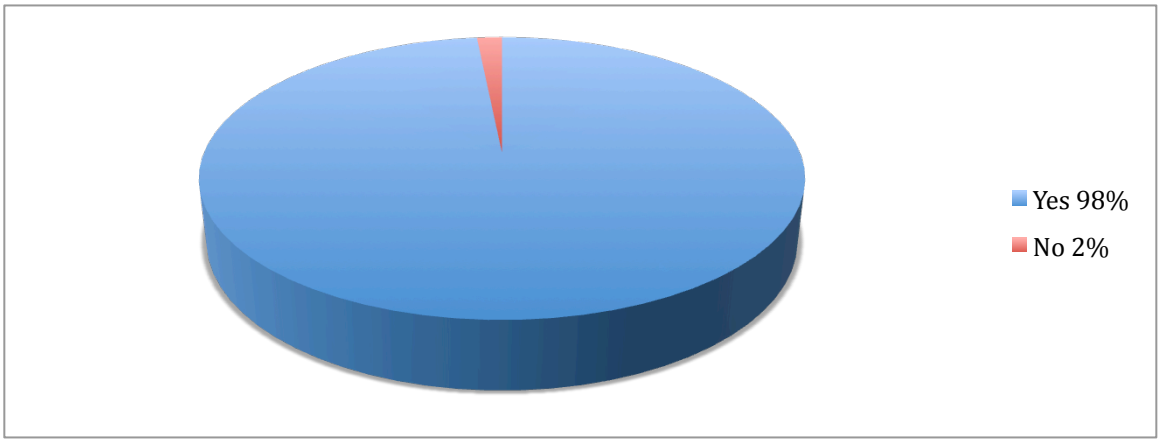
One of the respondents stated they were going to speed up the deployment of DNSSEC because of the proposed arrangement.

21. [NEW] Would it be of any interest to you to have updated and relevant statistics about the total number of signed zones, worldwide (or as far as applicable)?



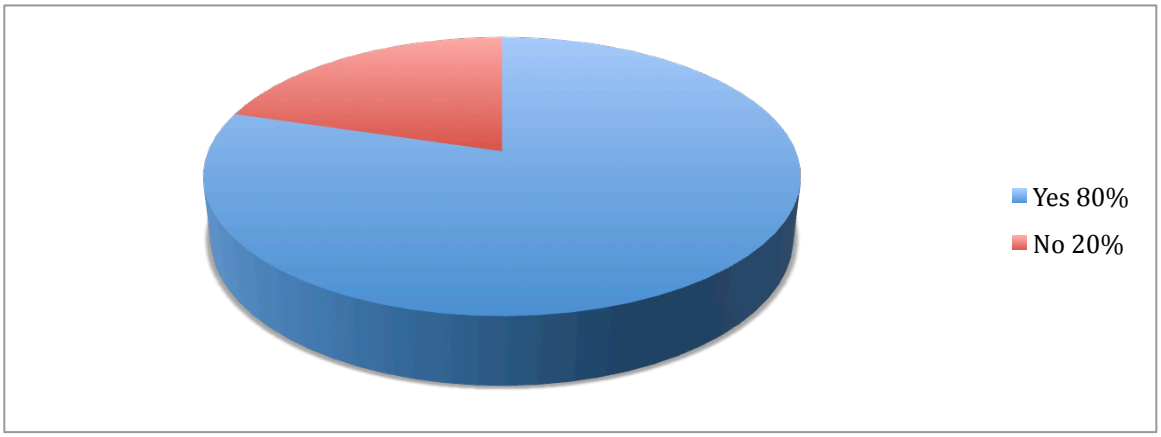
The vast majority of the respondents (94%) felt that it would be of interest to receive updated DNSSEC statistics.

22. Do you think there is a need to exchange DNSSEC experiences between ccTLD managers?



Almost all respondents (98%) felt that it is important to share information and experiences between the ccTLD managers – a clear increase since 2007, where only 84% clearly stated they think there is a need for this.

23. Do you think the ccNSO should actively promote the deployment of DNSSEC?



An increased amount of ccTLDs believe the ccNSO should actively promote the deployment of DNSSEC – 80% in 2009, compared to 62% in 2007.

24. Please, explain how you think the ccNSO should promote DNSSEC:

Most respondents thought that the ccNSO should take an active lead on internal as well as external education on the topic. Very frequently it was mentioned that the ccNSO should organise regional DNSSEC workshops and training sessions, some suggested this should be done in cooperation with the regional organisations.

It was also suggested that an entire ccNSO meeting should be devoted to DNSSEC issues, or that DNSSEC at least becomes a standing item on the ccNSO programme for the next 2-3 years. The Tech Day was also mentioned to be a useful forum for discussing DNSSEC. It was felt that it would be especially useful if registries that already have implemented DNSSEC report on their experiences. The ccNSO should also strive to develop guidelines and best practices in this area.

Furthermore, it was felt that it would be useful if the ccNSO could formulate easy to understand arguments and answers to why DNSSEC is needed which could be used to educate the outside public. It was even suggested to print leaflets or guidebooks on the topic. These would not only be especially useful to ccTLDs who can't attend the meetings, but could also serve as educational material to ISPs, as it was felt there is a need to promote the adoption of DNSSEC amongst them.

Another suggestion was the development of a website devoted to DNSSEC issues, where practical information could be gathered and training material posted. It was also called for accurate statistics and continued surveys on the topic.

Finally, it was suggested that the ccNSO could sponsor or assist the development of software or other shared DNSSEC tools.

The responses to this question were quite similar in the survey from 2007, however, the most frequently mentioned issue then was to “push for getting the root zone signed”, which is not a topic today.

The huge urge for regional workshops and a general exchange of information remain the same. The most noticeable change to the replies from two years ago is the call for help in external education, primarily of ISPs.

Appendix 1
Question 7

7. Please, briefly describe the technical environment you use for DNSSEC
We have developed our own (GPL licensed) registration system, that fully supports DNSSEC. The data flow is the same as before. All the DNSSEC related are passed to the central registry through EPP interfaces. So we do not interact with end users directly.
CoCCATools **Bind9** **Perl Provisioning Scripts**
Currently assessing performance and security aspects of various options for cryto and impact of DNSSEC the DNS secondary platform
Our goal is to implement NSEC3 with two KSKs, three ZSKs.
Key Generation Hardware **θ Hewlett Packard DL140 Intel Xeon 2.4 GHz, 512 MB RAM** **http://www.hp.com/** **θ Axalto Cryptoflex Smartcard (FIPS 140-1 Level 2 Certification)** **http://www.gemalto.com/** **θ Axalto e-gate Desktop Connector (smartcard reader)** **http://www.gemalto.com/** **θ Araneus Alea I True Random Number Generator** **http://www.araneus.fi/products-alea-eng.html** **Key Generation Software** **θ Ubuntu Linux (i386)** **http://www.ubuntu.com** **θ ISC BIND – dnssec-keygen** **http://www.isc.org/** **θ OpenSSL – openssl genrsa** **http://www.openssl.org/** **θ OpenSC – pkcs15-init & smart card libraries** **http://www.opensc-project.org/** **θ OpenCT – smart card driver** **http://www.opensc-project.org/openct/** **θ NIC-SE DNSSEC Tools – pkcs15-dnssec** **http://opensource.iis.se/trac/dnssec/wiki/PKCS15-DNSSEC** **θ NIC-SE DNSSEC Tools – keytool** **Signer Hardware** **θ Hewlett Packard DL385 Dual AMD64 Opteron 2.4 GHz, 2 GB RAM** **http://www.hp.com/** **Signer Software** **θ Ubuntu Linux (i386)** **http://www.ubuntu.com** **θ ISC BIND – dnssec-signzone & named-checkzone** **http://www.isc.org/** **θ .SE DNSSEC Tools – mksigned**
We use OpenDNSSEC as a solution, Solaris as platform, SCA6000 to securely store the keys.
BIND 9.6 and/or NSD on FreeBSD, OpenDNSSEC for signing using smart cards or SoftHSM, probably fully automated
Combination between different HW servers + SW with bind 9.6.1 over CentOS linux
We developed a script that automatically uses the RSA-SHA-1 algorithm to generate the key pair with which we sign every zone. It also regenerates the ZSK with 1028 bits every 3 months and the KSK every 12 months.
We will use DNSSEC with NSEC3 and publish our keys with ITAR until the root zone will be signed.
Domain Provisioning (WEB/EPP) and DNS publishing system (IXFR/SIGNER) completely developed internaly

following IETF standards. .COM.BR and .ORG.BR signed using NSEC3.
In-house developed tools, BIND nameserver software, testing with Hardware HSMs
Before implementing in real servers, we are planning to testbed server , where its possible to identify the complications and other compatibility issues. We have not prepared the implementation plan so far . We are planning to have a open discussion by inviting all the ISPs and network operators within this year.

Appendix 2
Question10

10. Please, describe the technical environment you plan to use to implement DNSSEC:
BIND and Linux
Tier-1 signing with opendnssec
Build in in our current registration system which uses a webinterface and EPP interface.
Upgrade our current registry and then use bind
BIND and other DNS servers with DNSEC support. Custom/registry software for signing zones/ exchanging keys.
Awaiting details from UltraDNS regarding their setup; also considering Autonomica. Precise configuration of the primary server is not yet set.
NSEC3
OpenDNSSEC
We plan to use our own resources.
Cisco based equipment
Own developed IXFR daemon that uses a Safe net Luna HSM for signing and key storage.
It will probably be outsourced
We will implement DNSSEC on FreeBSD servers and BIND9
We currently run our registry using BIND 9.3 under Sun Solaris.
DNS servers running bind of different versions.
We would like to implement it on our UNIX servers running BIND9
We depends to ISPs, domain hosting and end users to enable DNSSEC at their environment and have a basic knowledge how to configure DNSSEC, signing zone and maintain the DNSSEC keys (KSK & ZSK)
BIND on virtual or physical Linux servers acting as secondaries to the registry's hidden root.

Appendix 3
Question 11

Note: In order to keep the replies anonymous, small changes to the replies were made: where the registry or country name was mentioned, this was changed to “our registry” and “our country”.

11. Please briefly describe how strategically important you consider DNSSEC to be. (Please explain what the principal drivers are, the goals you would like to achieve with DNSSEC, and the main threats and opportunities you foresee).
We wanted to bring a response to the so-called Kaminsky attack. So the main driver was security.
DNSSec as a techonology gives confidence to the security & stability of the DNS. Security & other e-crimes are important drivers towards our registry considering DNSSec implementation.
Improvement of DNS security
Marketing Gimmick
Marketing
The main driving force is to gain a higher level of security even though not all problems involved are solved for example for secure online business processes. **Problems are cost, customer acceptance, ISP/registrar acceptance, complexity, difficult trouble shooting, insufficient tool and knowledge**
The DNS protocol does not permit to check the validity of DNS data which can be spoofed. >> DNSSEC protects against data corruption and from certain attacks, such as DNS cache poisoning
We consider it´s very important because we can provide a more secure service.
Ensuring the integrity of DNS. **Improve security transactions in the Internet, and possibly help to minimize fraudulent use of the Internet.**
A known flaw exists within the DNS protocol (Kaminsky vulnerability) and DNSSEC is the sole standard that can address that. That makes DNSSEC essential to the security and stability of the DNS. While there are additional opportunities with DNSSEC, such as the lookup of 509 certificates within DNS, there are also some risks such as lack of support in CPE devices (eg, home routers).
We hope to improve security on DNS by protecting cache poisoning. One of the threats is difficulty in key management. Also DNSSEC applied applications such as email, internet browser should be developed for user.
Finally demand from customers after Kaminski. **We want DNSSEC to become robust before deploying, making efforts do contribute to that.** **Major threat is increased operational procedures and revised roles (registry, registrar, registrant AND dns-operators)**
Although not all technical issues are resolved, it seems to be the best possible way to enhance security
We consider it to be very important. Our principle drivers were to increase the integrity of the DNS and to increase security for our registrants and their users. It is looked upon as a countermeasure against pharming and other DNS MITM attacks and an infrastructure strengthening technique. **A contemplated use of DNSSEC is for authenticated distribution of public keys for other security schemes.** **Moreover, it was called upon by some state authorities.** **We regarded it as necessary to support new critical applications, like ENUM**
As of now this is not really a top priority strategically important issue for us, we have a few other more urgent matters requiring our attention
Not important
Deploying DNSSEC is the right thing to do to help protect our constituency. The main threat is cache-poisoning attacks. The attack is trivial, the result can be disastrous. With the root signed in a foreseeable timeframe, now is the time to implement DNSSEC.

There is no demand for DNSSEC from the community; however, we would like to offer such service to our customers. On the other hand we also would lie to stress and explain to the internet users that DNSSEC alone will not solve all security issues of the Internet. So, by promoting DNSSEC we will stress that this is just one link in the security chain. If we can provide this link we do that - this is our responsibility. Main threats - 1) human error especially in respect of the key management; 2) people relying on DNSSEC and forgeting about other aspects of security; 3) people expecting miracles from the technology. Opportunities: to make people think about security

DNSSEC adds a little to DNS security, but in the same time adds more administrative complexity for customers/registrars/registry.

We don't see demand from local internet community for DNSSEC, but we have to prepare if such demand will rise. The goals of DNSSEC are to make hard to forge DNS response, make DNS service more secure, but OS providers have to implement DNSSEC support from their side too, as last mile from customer DNS server to end user computer has to be protected too.

In light of the recent incidents regarding the operation and security of the DNS, and the possibility of the imminent signing of the root zone, we think that the natural step is to achieve the implementation as soon as possible. In this way we will study and understand DNSSEC, and we will be prepared to give our customers a better service.

So far, we have not received any requests from our customers

We see this as an increasingly critical requirement --both for our customers and in terms of overall ccTLD Registry "best practices". It's become obvious over the past year that the DNS is compromised without it.

DNSSEC is important part of infrastructure. We would need to increase the security level of our DNS network.

We want to provide the customer with a feeling of security, trustworthiness, integrity, and availability. Basically the main threat we foresee of using DNSSEC is the threat of DNS WALKS. By walking the zone, a list of all the records can be obtained.

DNSSEC its the main project in our registry for 2009.

We think that DNSSEC is important and a top level registry have to support it.

Principal drivers: to enhance security.

Threats - slow adoption by the registrars - no efficient management tools for key recovery.

The main driver for DNSSEC implementation is public pressure. The biggest threat is outsourced implementation because of the lack of own human resources.

Not yet considered

General purposes

We consider DNSSEC as strategically important. The principal driver for implementation is the future use of dnssec by banks, government and education institutions.

Very important because of the need for improved security

The main importance to the deployment of DNSSEC is enhancing DNS security.

Continual improvment of the DNS infrastructure. Possibility of creation of safe-havens for special zones.

Eliminate security vulnerabilities in DNS spoofing

It is important for us, because we think that through DNSSEC, we can give security to the zone

DNSSEC protect Internet resolvers (clients) from forged DNS data, such as that created by DNS cache poisoning. DNSSEC can only authenticate that the data is truly from or not available from the domain owner. DNSSEC does not provide confidentiality of data, also DNSSEC does not protect against DoS attacks directly.

*** Our Registry thrives to implement state of the art technology to ensure the privacy and satisfaction of our clients**

*** Our registry is in a phase of implementing IDNs in Arabic. Since the IDN world will introduce lots of cyber squatting online, DNSSec will minimize the impact and ensure better privacy and trade mark issues**

Although we see it as important, we are not using any registrars, and our operation is small, so we think we could wait a little longer.

Actually, we discuss about our registry redelegation

The main reason would be security.

1. As the ccTLD, we believe this will set a pace for Secure DNS in our country

2. Secure our root servers from attacks that can affect registrants
3. Build confidence in the DNS management in the country

Secure DNS and authenticate DNS records

ISPs, banks, internet regulator, our resellers and domain hosting providers - principal drivers.
Goal to achieve with DNSSEC:
1) ISPs to enable DNSSEC at their cache servers.
2) Internet banking to have DNSSEC in their domains.
3) To have clear policy on key management for our ccTLD and customers.
4) To educate people about internet threats and have DNSSEC as one of the ways to prevent such threats (Example cache poisoning can lead to other attacks such as phishing, pharming and etc)
Opportunities:
1) Making ecommerce online experience safer
2) Accelerate adoption of DNSSEC in software development including browsers leading to standardization of DNSSEC

Medium importance to strategy, will be implemented as natural evolution of the ccTLD root. Goal is to be able to offer modern DNS services according to the prevailing requirements. Instability and complexity resulting in security problems is the biggest perceived threat.

It is clear that security is a major issue for all Internet users, technical contributors and governance participants. In particular there is increasing realisation that technical protocols that have been in use for many years needs a fundamental overhaul to provide security features that were unnecessary when they were first developed. DNS is critical to this process because it is one of the foundation-layer technical protocols on which other protocols rely.
It is therefore an absolute necessity that DNSSEC should be implemented in order to facilitates the securing of dependent layers of technology in pursuit of our common goal of a secure and trusted Internet.

To secure the our name zones as much as possible

DNSSEC is demanded by the authorities

DNSSEC is important, but there are so many barriers in our country to online commerce (identity theft, lack of payment gateway providers etc). Once these barriers are overcome and the public is comfortable transacting commercially online, then the need for dnssec will arise.

We still do not recognize DNSSSEC as mandatory for our registry.

DNSSEC is very important for the prevention of cache poisoning.

We think that DNSSEC is very important and that the deployment will improve the security of our domain by preventing attacks such as dns cache poisoning

Considering the inherently bad security of DNS, DNSSEC comes in as a solutions to most of the threats that have eaten slowly on the infrastructure.

The knowledge of the attack mechanisms available to hackers makes it imperative that DNSSEC be deployed asap. The ultimately goal we should look forward to is a more secure DNS infrastructure.

The little knowledge and experience in DNSSEC in the public domain poses a delay on implementations; also the rate at which formalities are happening with the large root and TLD's is another show stopper.

Important to maintain the stability and reliability of the DNS system

Securize our zone exchange

Somewhat important.
Important because it provides a platform to enhance the utilisation and uses for DNS. Our main driver (goal) for implementing DNSSEC is ensuring the stability and security of our ccTLD - one of our core responsibilities as registry operator. The main threats are the aforementioned problems with
vendor support and lack of documentation. A failure to develop a practical, appropriate solution for signing the DNS root zone is also a threat.

Strategically DNSSEC is very important to implement from the registry point of view and at the same time it’s challenging for us to implement. We will timely plan for its actions and it need different stake holders into account.

Prevent attacks related to DNS

To prevent the DNS resolution service from being compromised by hackers.
Threats are impact on performance, operational difficulties

Appendix 4
Question 18

18. Please, explain your concerns about the proposed signing arrangement:
We do not see any good reason for Verisign involvement. We wanted IANA to take care of this. We commented this publicly to NTIA.
We can not accept the proposed scheme of deployment
We see no reason why VRSN should be involved in root zone signing. We strongly believe that this should be ICANN's responsibility.
Depending on how well the process of signing the root is handled, the functionality of DNSSEC-ready ccTLDs might be affected.
It is critical to perform all cryptographic functions in a single environment. The vetting of the data starts at IANA. Signing that data should be done immediately after the data is vetted. The current solution has a serial element where data is moved back and forth twice in order to get signed. This is prone to errors and delays and will be cumbersome in times of an emergency key rollover, or an emergency DS update from a TLD.
I do not see the reason why should Verisign be involved in the process. ICANN is responsible for keeping Internet secure, stable and interoperable. What is Verisign?
if signing arrangement of TLD is then fine , if its for ccTLD , how it will be and the main concern is that the nature of deal between ICANN and verisign. Thank you
The potentially complicated, multi-party arrangement may create additional points-of-failure. The involvement of a for-profit corporate stakeholder in a core security process is also of concern.
Verisign is a commercial concern driven by increasing shareholder values. The root zone contains ccTLDs which represent sovereignty of countries. It is inapproriate for a commercial concern to take full control of such a critical internet infrastructure.
Verisign to be involved, what about other root zone operators, we support a international approach for root zone signing
We would prefer a non-for-profit organisation to sign and publish the ZSK
I think the process of signing the key should include more stakeholders. Who in ICANN will be responsible for this is one question that comes to mind.
It should be internationally agreed
Looks that it is important to be in line with local rules
I don't like the idea of beeing so dependent on a company for-profit (Verisign).