DNSSEC Survey Results

Background Information

The DNSSEC survey was initiated at the request of the ccNSO Council to *"/…/ find out what the cc community has done so far individually regarding DNSSEC, and to take part of their experiences on the matter."* (ccNSO Council meeting minutes San Juan 27th June 2007)

The questions were drafted in cooperation with the Swedish registry.

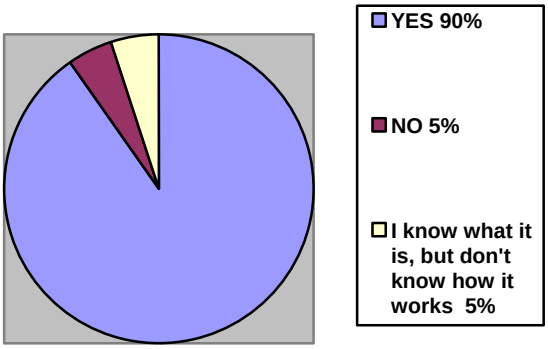
The survey was conducted between 12th September – 12th October 2007. It was sent out to the ccNSO members list and the wwTLD list. The survey was also conducted in Spanish and French, and respondents had the opportunity to reply in Arabic, Spanish, French, Russian and German.

In total, 61 replies were received. The spread of the responses was as follows:

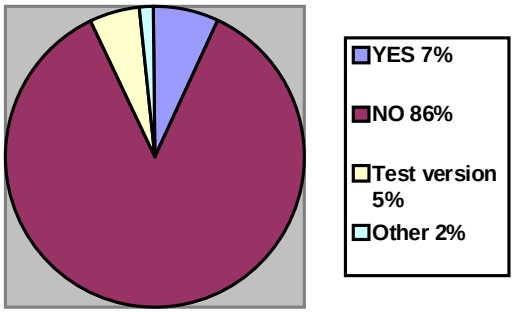
Africa: 18
Asia-Pacific: 19
Europe: 12
Latin America: 8
North America: 4

(following the ICANN Regions)

1) Do you know what DNSSEC is?



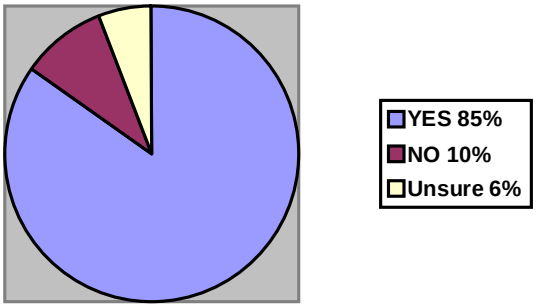
2) Has your registry implemented DNSSEC?



Whilst the vast majority of the respondents had not implemented DNSSEC, several registries had developed an internal "test-version" which was more or less ready to go into production, but for several reasons the registry decided to wait. Some of the reasons mentioned were zone walking issues and the lack of a signed root zone.

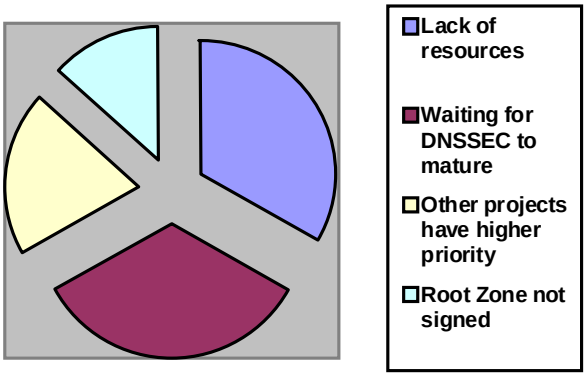
One respondent ("Other") had implemented DNSSEC under ENUM and was ready to implement it on the ccTLD level as soon as the zone walking issue was solved.

3) If you have not implemented DNSSEC, do you plan to?



Many of the registries who replied "No" mentioned that although the registry doesn't *plan* implementing DNSSEC at the moment, they know it is important and that it will probably happen at some point in the future. Some of them also mentioned that some existing problems first need to be solved – such as Zone Walking, or having an IETF standard developed. A few also stated they don't see a point in implementing DNSSEC as long as the root has not been signed.

4) If you have not, or do not intend to implement DNSSEC in the next three years, please briefly explain why you do not intend to do so:



The question was open-ended. In the overview the most "frequently mentioned" reasons are shown.

5) If you have implemented DNSSEC, please briefly describe the technical environment you use:

Because of the highly varied nature of responses, it was not possible to classify them into groups.

A summarising overview shows that some were doing fully manual signing, however most had developed systems to help sign their zones. Most used a combination of known software applications (BIND and/or NSD) on UNIX compatible platforms. Some used Hardware Signing Modules. The use of particular diagnostic tools was recommended, such as the 'drill' application.

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

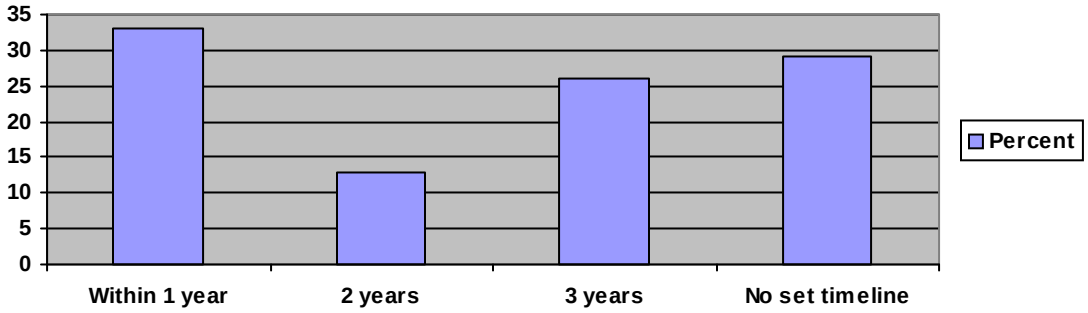
6) If you have implemented DNSSEC, please briefly describe your experience:

Experiences typically reflected that there was little to no adoption of DNSSEC, either in production or in testing. Some noted the limited end-user application support as a factor in failed adoption, and others noted that the tool-chain for the registry was also immature and limited.

The ability to walk the zone to collect a list of names was considered a problem to a number of respondents. They did not want to deploy DNSSEC if it allowed the list of registered names to be made available.

It was noted that key management procedures were crucial and needed careful thought. Additionally, a lot of effort was required to train staff and implement appropriate systems to properly support the technology.

7) If you are planning to implement DNSSEC, what is the planned timeline?



Several of the respondents had already started work on implementing DNSSEC within the next year.

Many of those who had no set timeline stated they will wait until some of the issues (zone walking, root zone signed) have been solved.

8) If you are planning to implement DNSSEC, please briefly describe the technical environment you use:

There were a variety of responses, some detailing hardware choices, others on software and procedural systems. Many needed to develop systems to accept DNSSEC material – such as adapting EPP to have the added functionality. Some had looked to extend the existing solutions, as well as funding well-known software vendors to add the required support to their products. Most mentioned operating system/software was BIND and Linux. Several respondents had not yet decided what system to use.

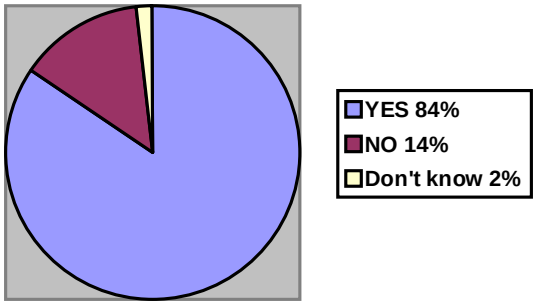
The individual answers to this question are attached in appendix 2 (randomly presented, with the name of the ccTLD removed).

9) Please describe how strategically important you consider DNSSEC to be:

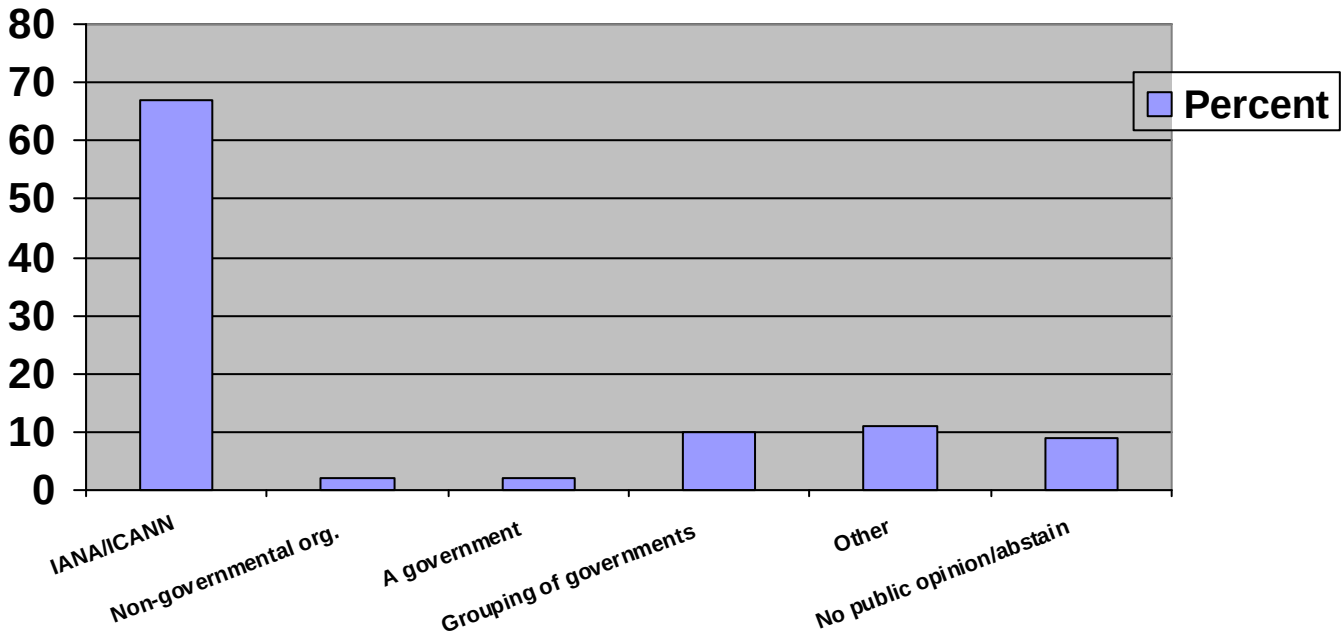
Most responses circled on the direct improvement to the DNS of ensuring the integrity of the answer during transmission. More generally it was expected the technology could improve business confidence in the Internet, and possibly help to minimise fraudulent use of the Internet. Some had received enquiries from business to implement the technology.

The fact the root is not signed was considered an obstacle by some. The complexity of the technology – particularly for the end user – was also a common theme. There seemed to be a lack of user understanding for the technology. Some reported that the technology would overly complicate the relationships the registry has with the registrar.

10) Is it important to you that the DNS root zone is signed?

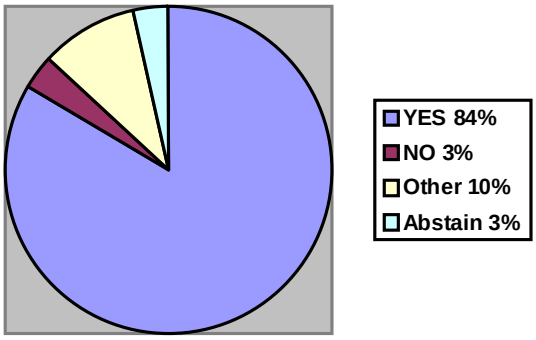


11) Who should be the signer of the root zone?



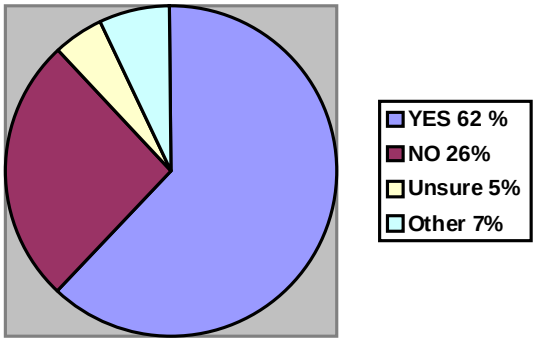
Many of the respondents under “Other” suggested models with multiple signers - such as ICANN/IANA + non-governmental organisation, ICANN/IANA + government(s) or ICANN/IANA + gNSO + ccNSO + RIRs. Other suggestions included ISOC, such as having a board of ISOC appointed trustees signing the root.

12) Do you think there is a need to exchange DNSSEC experiences between TLD managers?



Under “Other” replies were counted which did not clearly take any position.

13) Should the ccNSO actively promote the deployment of DNSSEC?



Many of the respondents who replied “No” did not think the ccNSO should *actively promote* DNSSEC, they much rather thought the ccNSO should provide a platform for exchange of information on the topic. Some respondents also pointed out that the ccNSO should not promote DNSSEC until an IETF standard has been created, or before some of the technical problems, such as zone walking, have been solved.

14) How should the ccNSO promote DNSSEC?

The most frequently mentioned replies of this open-ended question were:

- Organise regional DNSSEC dedicated workshops; preferably in a language spoken in the region.
- Actively push to get the root zone signed
- Produce an information brochure on different aspects of DNSSEC in a simple way so that also non-technical people can understand.
- Collect and share information regularly.

APPENDIX 1

Question 5: If you have implemented DNSSEC, please briefly describe the technical environment you use:

Please, note that not all individual replies are displayed. In cases where the nature of the reply did not make it possible to keep the anonymity, it was left out.

The order of the displayed replies is random.

There are now five servers operated for DNSSEC demonstration service. Two of them are used for SLD DNSSEC service, and another two servers are used for user DNS server. The last one is used for DNSSEC recursive name server. We are currently using BIND 9.4.1 as a DNS software.	We have done it for a few zones, but not the ccTLDs. Freebsd, bind 9.4, the usual stuff. Manually signed.	For the testbed we have: ZSK (1024 bits) stored on HSM, KSK (2048 bits) stored on smartcard stored on safe. Central server signs the zone and sends the information to DNS servers using an in-house IXFR and AXFR implementation. In the Registrar system we ask for the public key and generate the DS records. We are also working on a DNSSEC online signing solution while NSEC3 takes off.

Web and EPP interfaces for the provisioning of DS records. [AI]XFR and Signer servers internally developed for the DNS provisioning. BIND and NSD for the Authoritative Servers	Answer for ENUM, not ccTLD: Registry system developed inhouse + Bind	Our DNSSEC trial was provisioned via DNSSEC extensions to EPP, BIND name servers.

We have not yet implemented DNSSEC. However, we have setup test-beds for the same. Using a simulation of our DNS infrastructure, we have successfully implemented TSIG and zone signing.	DNSSEC involves that the user when requesting a name resolving in DNS may decide if the returned answer is from a valid source and that the information has not been altered on its way back (data integrity and authentication). We also recommend the usage of the Mozilla Firefox Drill Extension which performs DNSSEC lookups for the main hostname of the current page in firefox. This extension uses Drill to chase the signatures up to a trusted key. The user can specify trusted keys by putting them in a directory of his choice.	Linux

APPENDIX 2

Question 8: If you are planning to implement DNSSEC, please briefly describe the technical environment you plan to use:

Please, note that not all individual replies are displayed. Replies such as “Do not know yet” have not been listed.

The order of the displayed replies is random.

Linux RHLE 4.0 or 5.0	We do not plan to purchase any special hardware. Our zone includes about 340 domains and our test shows, that we can sing this zone in 5 minutes after the generation. So we just plan to modify our registry system to include domain holders keys and the zone generator to add dnssec signing.	BIND 9 and some zone key management software that we are yet to determine.
BIND on Linux	Signed zones and using TSIG to secure transactions.	We are planning to use NSD on FreeBSD and BIND on Debian.
Linux	Bind 9 based on FreeBSD	We’ll first use a main local, in which we’ll simulate a WAN in order to test the secured delegation between parent and children zones. (ROOT and two TDLs at least)
BIND especially	BIND	Debian, Bind
Software BIND and some nameservers	i) Secure shared registry system a. Key management server b. Hidden primary server with DNSSEC-enabled + zone signing (not listed in the zone as an authoritative name server for the domain in question) c. DNS server (primary and secondary) with DNSSEC-enabled d. Zone transfer between primary and secondary server (signed zone) ii) Secure datacenter dual stack network performance monitoring	As I know about DNSSEC there is no need to change the technical environment (in terms of servers or network equipments). Identified steps : - bind configuration (dnssec-enable yes) creation of the ZSK and the KSK - zone signing - creation of the DS RR from the parent zone to build the trust chain

National DNS system running on BIND 9, Unix OS, in the north, south and the middle of [country name].	Operating system - Debian Sarge/Etch Database - Postgres DNS - BIND Registry - In house software (SRS)	We already have dynamic updates so we will be adding to that a hardware crypto device that can generate signatures for each dynamic update. Additionally we are paying ISC to amend BIND so that it can re-sign RRs that are not updated, before their signatures expire. Finally, we have a two layer security architecture for KSKs and ZSKs with KSKs being held in FIPS compliant HSMs.

Our Registry system + Bind	Will use existing softwares and/or services for DNS servers. Will use effective and NSEC3 capable zone signer. Will use automatic key management system. May use self-developed DS and/or KSK public key registration system.	High-level plan includes addressing a high volume, high churn zone with dispersed slave name servers.

Linux + Bind	Globally Anycasted instances of diversed hardware/os/dns software	BIND/LINUX

Waiting for NSEC3 to be deployed and supported in multiple nameserver implementations. Need to redesign registry system and processes, zone generation and key management, which is currently in-house developed.	* 2 engineers for the first three steps and 4 for the next two, and one to three plus a marketing specialist for the last one. * 2 to 4 computer stations (depending on the state of the art). * Virtualization SW, Linux and UNIX OS. * Internet connectivity through IPv4 and IPv6 native, to make tests. * Budget to buy new devices, software or services determined by the state of the art studies we would do (Key generation HW, SW, etc.)	DNS server software: BIND9, I think we will use BIND9.3 or BIND9.4 Key algorithm: RSASHA1 Key size: 1280 for KSK and 1024 for ZSK