DNSSEC @ ICANN
Signing the root zone: A way forward toward operational readiness

The purpose of this document is to a) articulate ICANN's initiatives toward operational readiness for DNSSEC signing; and b) as directed in the July 2008 – June 2011 ICANN Strategic Plan help determine the right structures in preparation to "[consulting] with stakeholders, be prepared to digitally sign the root using DNSSEC technology by late 2008".

Specifically, this document is *not* a roadmap for DNSSEC deployment. Ultimately, this roadmap will be developed by a community consultation process, and require relevant approvals through ICANN's IANA functions contract with the U.S. Department of Commerce. The document does summarize ICANN actions to prepare for DNSSEC signing activities should they be called upon to implement this protocol, and communicates staff and expert views on the implications of DNSSEC, and on various signing models.

Executive Summary

The primary benefit of the DNS Security Extensions protocol (DNSSEC)[1] is that it provides a way for software to validate that DNS data have not been modified during Internet transit. This is done by incorporating public-private signature key pairs into the DNS hierarchy to form a chain of trust originating at the root zone. DNSSEC is backward compatible with existing DNS, leaving records as they are – unencrypted - but ensuring their integrity through the use of digital signatures. Users of the DNS who choose not to adopt DNSSEC will be able to access the root zone just as they do today with no changes on their part, however those wishing to validate the DNS data received will be able to do so.

Recently, there has been increased interest in the ICANN community for getting the root of the DNS signed, particularly with the discovery of inherent weaknesses in the DNS protocol in the face of technological advances. ICANN has provided, since June 2007, a publicly available signed root through a testbed.[2] This work grew out of ICANN's previous commitment to the Internet Architecture Board (IAB) to deploy DNSSEC on the .ARPA infrastructure zone[3]. Production deployment of DNSSEC-signing of .ARPA, and a possible ICANN role in DNSSEC-signing of the root zone will involve planning with and approval by the U.S. Department of Commerce under the IANA functions contract.

Looking forward, ICANN's position on the production of a DNSSEC-signed root can be summarized as follows:

- ICANN believes that it should be possible for root zone data to be validated independently of how the data are obtained. For this reason, ICANN's strategic plan calls for the root zone to be DNSSEC-signed.

[1] See RFCs 4033, 4034, and 4035
[2] See https://ns.iana.org/dnssec/root.zone.signed and https://ns.iana.org/dnssec/status.html
[3] See http://www.iab.org/documents/correspondence/2006-05-15-IAB-request-to-IANA-to-sign-DNSSEC-zones.html

- A DNSSEC signed root zone need not affect the operation of any existing TLD and does not necessitate DNSSEC deployment anywhere else on the Internet. In this sense, if the root zone is DNSSEC signed, DNSSEC deployment beyond the root zone remains optional.
- A signed root does not require a change in the current administrative or control structure of the root zone since DNSSEC only adds a validation mechanism for the same data.
- It is not technically necessary for ICANN to be the owner, operator or DNSSEC signing key holder. Still there are some security advantages to ICANN maintaining an unbroken chain of trust from TLD operator to signed root zone.
- DNSSEC is not a panacea that addresses all Internet security ills, rather it is a tool that can address certain forms of attack today and may provide additional security-in-depth for the Internet as a whole in conjunction with other security measures to aid against future attacks.

Background

DNSSEC, a series of DNS protocol extensions defined in RFCs 4033, 4034, and 4035, ensures the integrity of data returned by domain name lookups by incorporating a chain of trust into the DNS hierarchy. The chain is built using public key cryptography with each link in the chain consisting of a public-private key pair. Once fully deployed, validating software could verify that the DNS data received is the same as that contained in the originating DNS server using a single "trust anchor" or public key for the root of the DNS. Securing the DNS using DNSSEC could protect users from attacks such as cache poisoning where an attacker would reply to DNS queries with a bogus DNS response that could, for example, send subsequent users to the attacker's Web pages for account/password collection. Recent discoveries of inherent DNS protocol deficiencies have made such attacks easier for the would-be attacker to implement. Being able to protect against this attack is among the primary motivations for deployment of DNSSEC.

Recognizing these benefits, there are also concerns about DNSSEC deployment. Possible impacts include larger data responses to DNS queries, increased resource requirements, complex key management, and creation of an additional single point of failure for the Internet. Furthermore, the problems that DNSSEC was designed to address can often be handled by using modern DNS software, following best practices, and through user education (e.g., HTTPS / SSL usage).

Notwithstanding these concerns, new DNS attack vectors and requests made to ICANN for DNSSEC deployment at the root by certain portions of the technical community are increasing and will continue to increase. In June 2007, the RIPE community[4] sent a letter requesting ICANN to get the root zone signed "as soon as realistically possible" [attachment 1]. This was followed by requests in October 2007 from major Swedish (.SE) stakeholders interested in DNSSEC [attachment 2] and Nominet (the .UK registry) asking ICANN to instruct staff to "take the necessary steps" to sign the root zone [attachment 3]. Currently DNSSEC is deployed by four (4) TLD operators (.SE, .BR, .BG, .PR) with others preparing for deployment (.ORG [attachment 4], .UK. .CZ, and .GOV[5]). Finally, a recent survey of ccTLD operators also indicates a clear expectation of DNSSEC adoption and root zone signing by ICANN/IANA [attachment 5].

[4] RIPE, Réseaux IP Européens, is "a collaborative forum open to all parties interested in wide area IP networks in Europe and beyond". See http://www.ripe.net/ripe/index.html.
[5] http://www.gcn.com/online/vol1_no1/46262-1.html Note: NIST 800-81 refers to DNSSEC

Partly due to slow progress and partly due to the sense that the larger TLDs will not deploy DNSSEC right away, work has continued on a number of what appear to be inferior alternatives that, once established, may be difficult to undo.

"DNSSEC Lookaside Validation" (DLV) is one such alternative that would create a non-hierarchical, non-scalable, third party authentication system with its own security mechanisms and trust models that continues to use the DNS protocol. Developed by the Internet Systems Consortium (ISC), DLV was recently built into one of the most popular nameserver implementations (ISC's BIND). Another alternative, one requested by the RIPE community, and in response being implemented by ICANN, is a TLD-only "Interim Trust Anchor Repository" (ITAR) comprised of a simple list of DS records and accessible via a non-DNS protocol, (e.g., HTTPS). In theory, the operation of the DLV registry and/or the ITAR would end after there is sufficient DNSSEC adoption for the former or the root zone is signed for the later.

In the interim ICANN will continue to discuss this issue with the Internet community and monitor developments closely.

Attached:
1. Letter from RIPE to ICANN re: DNSSEC (12 June 2007)
(http://www.icann.org/correspondence/pawlik-to-cerf-07jun12.pdf)
2. Letter from .SE to ICANN (26 October 2007) (http://www.iis.se/docs/brev_iana_pdf.pdf)
3. "Signing the Root", Nominet Position Paper (29 October 2007)
(http://www.nominet.org.uk/digitalAssets/25692_Signing_the_Root.pdf)
4. Letter from PIR to ICANN re: .org DNSSEC (2 August 2006)
(http://www.icann.org/correspondence/viltz-to-dam-02aug06.pdf)
See also PIR presentation on .ORG https://par.icann.org/files/paris/RaadDNSSEC.pdf
5. ccTLD DNSSEC Survey Results (October 2007)
(http://ccnso.icann.org/surveys/dnssec-survey-report-2007.pdf)

Key Points

1. ICANN believes that it should be possible for root zone data to be validated independently of how the data are obtained. For this reason, ICANN's strategic plan calls for the root zone to be DNSSEC-signed.

2. There are multiple DNSSEC operational models regarding roles for owner, operator or key holder of the signing system. However, based on lessons learned from DNSSEC experts who currently operate or will be deploying DNSSEC (.SE, .UK, etc), there could be security advantages for ICANN to both compile and sign the root together with its current role of receiving and processing requested changes to the authoritative root zone file. As noted elsewhere, this change in role for ICANN would require approval from the U.S. Department of Commerce and coordination with other parties.

3. To be effective, DNSSEC deployment, at the root or otherwise, must be carried out with respect to carefully considered security plans and follow best practices such as those found in RFC 4641.

4. A signed root does NOT require the current administrative or control structure of the root zone to change since DNSSEC primarily provides a way to verify DNS data received have not been modified in-transit.

5. DNSSEC deployment is optional. A signed root zone need not affect the operation of any existing TLD and does not necessitate DNSSEC deployment anywhere else on the Internet. Not signing the root zone though may have an impact on security for the TLDs that have made the decision to sign their zones by making verification against a single point in the hierarchy difficult[6]

6. ICANN expects market factors and/or other forces to determine how and to what extent DNSSEC is deployed.

7. DNSSEC is not a panacea that addresses all Internet security ills, rather it is a tool that can address certain forms of attack today and may provide additional security-in-depth for the Internet as a whole in conjunction with other security measures to aid against future attacks.

8. DNSSEC is relatively new from a deployment viewpoint. ICANN will continue to closely engage with and look to the DNS community as deployment experience matures.

9. ICANN continues to enhance capabilities so as to be technically prepared to sign the root zone and has been demonstrating this capability since June 2007 with an experimental signed root zone publicly available at ns.iana.org (see https://ns.iana.org/dnssec/status.html), albeit operational requirements (such as designation of secondaries) for the signed root still need to be addressed if this service is to go into production.

10. The U.S. Department of Commerce must authorize whether DNSSEC is implemented at the root pursuant to the IANA Functions contract. ICANN staff will work with the U.S. Department of

[6] E.g., Without a "parent", compromised key recovery for TLD's is a lengthy and error prone process. See PIR .ORG RSTEP report: http://www.icann.org/registries/rsep/rstep-report-pir-dnssec-04jun08.pdf "Many of the stability issues analyzed in this report would either not exist at all, or would be much more tractable, if the root were already signed."

Commerce and the broad group of stakeholders to arrive at a clear, technologically sound, secure implementation of DNSSEC.

.

11. Regarding questions surrounding DNSSEC key control:

a. DNSSEC does not provide any additional level of control over zone data. It only allows DNS data received in response to a DNS query to be validated to ensure that data has not been modified in flight. Control of the contents of the root zone would remain **unchanged**.
b. DNSSEC does not enhance ICANN's ability to attest to the contents of the zone file. This remains **unchanged**.
c. DNSSEC does not encrypt DNS data. It is designed to be backward compatible.
d. DNSSEC does not eliminate the potential of deployment of alternate roots, since DNS root zone data is public by its very nature. This remains **unchanged**. Users of alternate roots would simply install the trust anchor published by that root.
e. DNSSEC does protect the DNS against certain attacks, namely "cache poisoning attacks", that, though rare, have been demonstrated to be easily advanced.
f. In a typical secured DNSSEC implementation[7] the private half of DNSSEC's long term "Key Signing Key" (KSK) is known to no one since, for security reasons, it is generated inside a tamper proof cryptographic device and is never available in unencrypted form.
g. Since KSKs are required to sign new Zone Signing Keys (ZSKs) on a frequent basis and would need to be re-generated immediately in the face of compromise, "N of M" key splitting techniques not only reduce the **security** of a DNSSEC installation by externalizing private key material but also reduce the **stability** of the DNS by relying on the physical availability of N of the M key fragment holders. Should the key fragment holders not be available to update a signature, recover from a compromised key, or rollover a key, DNSSEC users will see a failure.
h. In order to instill confidence in the KSK generation and publication process, it should be performed as part of an annual (or even less frequent) Key Ceremony where the various roles are performed by multiple entities and witnessed by interested stakeholders. This would be akin to what typical Certification Authorities do today when they generate their root SSL keys. By doing this the public can be assured that the keys for the root zone can be trusted and are faithfully deployed.

12. The DNSSEC effort undertaken by staff was initiated as a result of a request from the Internet Architecture Board (IAB) to deploy DNSSEC on the .ARPA infrastructure zone. This request is independent of DNSSEC deployment on the root zone and there do not appear to be any major technical barriers to successfully completing this request. Initial deployment of DNSSEC-signing for the .ARPA zone is currently being discussed by the IAB, ICANN and the U.S. Department of Commerce.

13. With respect to .ARPA, staff have completed development work and are currently developing an operational plan for DNSSEC deployment which includes, among other elements, selection of secondary DNS providers with specific service level agreements.

---

[7] ICANN's testbed signed root uses a FIPS-140-2 Level 4 certified tamper proof cryptographic device

14. ICANN has and will continue to be committed to maintaining complete transparency in its DNSSEC development and any deployment efforts (as demonstrated by the multiple presentations[8] on technical design details[9] that have been given during the development phase).

15. ICANN takes seriously the requests for DNSSEC deployment at the root thus far from RIPE and major Swedish stakeholders in DNSSEC as well as the position paper from the .UK registry. We continue to encourage input from all stakeholders on how to proceed.

16. ICANN will continue to closely monitor DNSSEC deployment as it unfolds, and we will reevaluate our efforts and modify plans accordingly.

17. ICANN will continue its outreach efforts to understand the needs of the Internet community and draw on their expertise.

[8] IETF 69 Chicago, DNSSEC-DEPLOYMENT.ORG, RIPE 55 Amsterdam, ICANN Los Angeles

[9] We have been and will continue to be open sourcing software developed in the course of our DNSSEC deployment efforts and have been working with those experimenting with the IANA demo signed root zone.

ICANN
Dr. Vinton Cerf
Dr. Paul Twomey
4676 Admiralty Way, Suite 330
Marina del Rey, CA 90292-6601
USA

12 June 2007

RE: RIPE Community Request for ICANN to Sign DNS Root

Dear Dr. Cerf and Dr. Twomey,

At the RIPE 54 meeting in Tallinn the DNS Working Group discussed various options for the creation of a repository for DNSSEC keys. Frustration was expressed at the slow progress towards getting the root zone signed and there was concern that this was leading to adoption of ad-hoc workarounds. The DNS Working Group felt there was a need for a public comment on this issue and the statement below was unanimously agreed. The DNS Working Group decided it should request endorsement for the statement from the wider RIPE community. It was presented at the closing plenary session where it was unanimously supported.

The statement, which I quote in full, is as follows:

> The lack of progress towards the deployment of DNSSEC is undermining the stability and security of the internet. Operators and implementers are compelled to adopt ad-hoc, short-term solutions which will create long-term problems. The RIPE community urges ICANN to speed up and improve its efforts to get the root zone signed.

We fully understand that there are issues that need to be resolved before ICANN can sign the root of the DNS. However, on behalf of the members of the RIPE NCC and the RIPE community, we would like to call on ICANN to solve these issues and to sign the root of the DNS as soon as is realistically possible.

We thank you in advance for your urgent consideration of this request and look forward to a prompt announcement of a schedule for signing of the root zone.

Sincerely,

Axel Pawlik	Rob Blokzijl	Jim Reid
Managing Director	Chairman	Chairman
RIPE NCC	RIPE	RIPE DNS Working Group

Stockholm, October 26th, 2007

Dear Dr. Cerf and Dr. Twomey,

The signatories of this letter wish to recognise the efforts made by ICANN to improve the IANA functions. It is of great importance that the IANA functions are operated in an open and transparent manner.

We believe it is essential to have open publication of the IANA policies and processes, and we support the development of a secure, efficient and more automated operation of the IANA.

However, as one of the very early adopters of DNSSEC on a TLD level, .SE, we are concerned about the slow progress of the DNSSEC deployment efforts. We believe that the successful deployment of DNSSEC is crucial for the continued stability and security of the Internet. As this is contingent upon a signed DNS root zone, we urge ICANN to speed up and improve its efforts to quite rapidly migrate to a signed root zone.

We are fully aware that the discussions relating to the signing of the root have been taking place over the last 3-4 years. We believe that the Internet now has reached a point where the absence of a signed root zone is no longer only merely unfortunate. Rather, the absence of a signed root zone directly contributes to the development of inferior alternatives, thereby confusing the community and jeopardising the long term success of DNSSEC deployment.

We strongly recommend that ICANN without further delay takes the decision to sign the root zone, and in doing so sets a firm target date for the deployment of a signed root zone, that ICANN urgently publishes a road map for reaching that goal, that ICANN immediately enters into necessary negotiations with involved parties, and that ICANN instructs the IANA to take the necessary steps to implement that road map.

Stockholm, October 26th, 2007

The signatories below represent the major Swedish stakeholders in DNSSEC deployment and this document represents our shared and stated position in this issue.

We thank you in advance for considering our recommendation. We look forward to your response and to the announcement of a road map for a signed zone in the immediate future.

Sincerely,

Autonomica AB (i.root-servers.net)
Frobbit AB (SE-DNSSEC registrar)
Kirei AB
Loopia AB (SE-DNSSEC registrar)
SNUS - Swedish Network Users' Society
Swedbank AB
Swedish Administrative Development Agency (Verva)
Swedish University Computer Network (SUNET)
TeliaSonera Sverige AB
The Foundation of Internet Infrastructure (.SE)
The Swedish Bankers' Association
The Swedish Urban Network Association (SSNf)

Signing the Root

A Nominet position paper

Contents

1. Introduction

In this paper we examine the issues currently preventing widespread adoption of DNSSEC with a special focus on the issues involved in signing the root zone. After considering the pertinent concerns, we suggest a solution to signing the root that we believe balances the requirements of all concerned.

1.1 A key point in time

DNSSEC is currently not widely deployed, as there are a number of unresolved issues, both technical and political, which are limiting its deployment.

Until now, the major barriers to technical implementation have been:

- Zone-file enumeration
- Support for DNSSEC in application software
- The impact on resources of fully signing a large zone.

These barriers are close to being overcome, thanks in part to the input of Nominet through the Internet Engineering Task Force (IETF), with the imminent approval of improvements to DNSSEC called NSEC3.

The resolution of outstanding technical issues focuses attention on another key step which must be completed prior to the successful implementation of DNSSEC: the signing of the root zone, the so-called “trust anchor”.

In this paper, we provide our solution for overcoming this remaining barrier to the widespread adoption of DNSSEC.

1.2 Who needs DNSSEC anyway?

It is clear that DNSSEC has not captured the public imagination. End users of DNS are not raising a clamour for the introduction of DNSSEC. However, this should not lead to a misapprehension that DNSSEC is not needed or wanted.

There is a significant desire amongst all Internet users including government, industry and civil society for a more secure and trustworthy Internet. It is clear that this will only be achieved by a combined approach of multi-layered technical developments and multi-layered policy developments.

The received technical wisdom is that a secure DNS is a fundamental layer in that technical development, on which many other layers depend. But it is a layer of technology that many are unaware of and will remain so, even while the public embodiment of DNS, domain names, remain a high profile concern.

It is our view that it is imperative for TLD registries to lead the implementation of DNSSEC, raising awareness amongst other users of DNS, with the aim that a secure DNS becomes a ubiquitous feature of the Internet.

1.3 What comes after DNSSEC?

Once implemented, DNSSEC will provide very real benefits. When errors can be detected, what is left is a highly trustworthy distributed database, which will provide a secure foundation for many of the new uses of the DNS.

One good example is Domain Keys Identified Mail (DKIM). This is a technology that adds cryptographic signatures to emails, to prevent address spoofing and utilises the DNS to publish the keys for signature checking. With DNSSEC securing the delivery of those keys, the effectiveness of DKIM is increased and the techniques available to distributors of spam are reduced.

2. DNSSEC, the basic purpose

It is important to remember that DNSSEC was designed to protect Internet users from security threats such as DNS cache poisoning – the introduction of fake DNS data into caching DNS servers, and so-called `man-in-the-middle' attacks – supplying fake data that usurps genuine responses to DNS queries.

DNSSEC provides protection by enabling a computer to check whether the information contained in a given DNS response has come from a trusted source and whether it has been tampered with in transit.

DNSSEC is essentially error detection, where the 'error' could be introduced by a malicious entity, which without DNSSEC would remain undetected.

2.1 The impact of DNSSEC on delegation-only zones

The zones managed by TLDs are normally delegation-only. That means that they contain only nameserver records that delegate domains down the DNS hierarchy.

The normal registry process is for the TLD to receive the nameserver data from the owner of the sub-domain, possibly to run this through some checks before accepting the data, and then to publish it in the TLD zone.

With DNSSEC this model will change slightly as the TLD will additionally need to receive the key identifiers needed to construct Delegation Signer (DS) records. The TLD will then sign the DS record and now publish the nameserver data, the key identifier for the child zone and the TLD signature of this key identifier.

It should be noted that the delegation nameserver data is not signed in DNSSEC because the parent zone is not deemed to be authoritative for the nameserver data, only the child can authoritatively publish its own nameservers.

2.2 What does it mean when someone signs a delegation-only zone?

In this context we examine what it means when a TLD signs a delegation data. It could either mean:

1. We are using the signature to warrant that we have checked the delegation data we are publishing and it can be trusted; or
2. We are using the signature to transmit securely the delegation data supplied to us, but make no warranty as to the trustworthiness of the data.

In our view, wherever a zone is situated in the DNS hierarchy, the meaning of signing a zone should be consistent across the DNS. In other words, we would not make any requirements on the root zone, or our users, that we ourselves were not prepared to meet.

For any zone where the owner of that zone is different from the owner of the parent, the parent would be unable to guarantee the truth of statement (1) above. This is the position of all TLD managers as they are not the owners of the zones for the domains they delegate and so they could not guarantee the truth of statement (1).

Statement (2) is consistent with the DNSSEC standard, which was developed with the limited purpose of enabling secure transmission of DNS data.

Therefore, the entity that signs delegation data in a zone makes a limited promise: that the data received is the same as the data published within the relevant zone.

It should be noted that this is exactly the promise currently made by the publishers of delegation data in zones, but without DNSSEC they cannot transmit that data securely.

3. The challenges of implementing DNSSEC

The implementation challenges remaining to us can be summarized as:

- the chain of trust
- secure key management
- signing changes
- automated re-signing
- managing resource usage

3.1 The chain of trust

In order for DNSSEC to be fully deployed, an unbroken chain of trust needs to be established, down from the root at the top, through the TLD, down to individual registrants. All zones need to be authenticated by "signing", i.e. the publisher of a zone signs that zone prior to publication and the parent of that zone publishes the keys of that zone.

To achieve this we need the root signed and procedures in place at each step to enable the secure transmission of keys between parties.

3.2 Secure key management

Currently registries only make minimal use of keys within DNS transactions as part of the ordinary operations of the registry. Managing DNSSEC keys requires a registry to implement a new infrastructure for the secure storage and transmission of keys, including both suitable equipment and procedures.

3.3 Signing changes

In common with a few of the larger TLD registries, Nominet currently provides near synchronous zone file publication. This means that new domain name registrations are entered into the DNS within minutes and can work almost immediately.

Signing a large zone, like co.uk which has over 6 million registrations, would be a highly involved and maintenance-intensive task. Given the frequency of updates to the records within co.uk, which can peak at 300,000 per day, signing a large, fast-changing zone in real time will require significant cryptographic processing power and reliability

3.4 Automated re-signing

With any zone it is likely that the signatures will expire before the DNS records are updated. Zone operators therefore require a means to automatically re-sign DNS records before these signatures expire. This functionality is dubbed 'continuous signing' and is not yet a feature of common nameserver implementations.

Nominet is therefore providing financial assistance to the Internet Standards Consortium (ISC) to fund the development of continuous signing within BIND, one of the most popular nameserver implementations in deployment.

3.5 Managing resource usage

Signed DNS records are considerably larger than unsigned records, with a fully signed zone being an order of magnitude greater in size than an unsigned zone. Some registries have expressed concern at the impact this will have on their infrastructure and possibly limit their involvement with DNSSEC as a consequence.

However a solution for this exists with NSEC3, the enhancements to DNSSEC that are close to becoming an RFC. This solution is called 'opt-out' and enables a zone operator to only sign those delegations that need DNSSEC. A registry that uses this can manage the increase in resources in line with the gradual uptake of DNSSEC, rather than being forced into an all-or-nothing upgrade.

Traditional capacity management for registries has been based around the number of domains within the zone. However, future capacity planning will need to incorporate the additional factor of the number of signed zones to ensure that a true picture of resource requirements is developed.

4. Signing the root

The IANA root zone is both the authoritative list of TLDs and the starting point for delegation data to locate those TLDs. Without a single point (the root), the world would have to find TLD locations individually, without using the DNS and without any certainty that the TLDs were genuine. This clearly does not scale and is intensive and potentially error prone.

Although a single root is not a technical necessity, it is the Nominet view that, in practice, it is essential for the stability of the Internet.

The DNS root database is managed by ICANN through the IANA function. IANA staff are responsible for updating the database of TLD managers. Currently, each update that is made to the DNS root database is reviewed by the US Department of Commerce prior to going live. This function has caused substantial debate at the international level, particularly during and after the World Summit on the Information Society.

Once the root database has been updated, the data that needs to change in the root zone is sent to the Root Zone Manager (RZM), currently Verisign Inc., who then propagates this through the Internet to the other root server operators.

4.1 Why is it important to sign the root?

DNSSEC requires a trust anchor to work. That is, a point in the DNS hierarchy that a DNS user explicitly trusts and from which they can start the chain of trust that continues down the hierarchy.

Without a single origin of trust, those wishing to use DNSSEC would need to identify multiple trust anchors and monitor them continuously. Again this does not scale and is intensive and potentially error prone.

Experience shows that for successful deployment of new technology, end-users should be required to do very little. In this case, the system administrators around the world who configure DNS servers should be able to make them use secure DNS as simply as possible.

For this to happen, we contend that there should be a single trust anchor and that this should be at the same point as the single authoritative list of TLDs. This can only be achieved by signing the root. Indeed, the standard has been designed on this assumption. Anything else would be splitting the root.

Whilst a number of registries have pioneered the deployment of DNSSEC by signing their own zones and establishing themselves as trust anchors, this is not a stratagem that can be extended beyond these early adopters. As explained before, using multiple trust anchors does not scale and is likely to inhibit the growth of DNSSEC rather than promote it by making the management of DNSSEC too complex.

We therefore recommend that any TLD considering signing its zones and becoming a trust anchor, carefully weighs the wider implications of participating in a mechanism that does not scale.

4.2 What are the options for signing the root?

The identity of the organization or entity that signs the root has been troubling the Internet community for some time. Several options are currently under discussion within the community:

- The current manager of the root zone – the IANA
- The outsourced Root Zone Maintainer, Verisign Inc.
- A trusted third party

In order to evaluate the options, we consider the relevant factors:

- Although the root zone is relatively stable, and does not have nearly the same volume of ongoing updates that affect larger zones (eg .co.uk), implementing DNSSEC will bring a higher degree of complexity and technical maintenance to management of the root zone than previously.
- The consequences of errors in signing a zone could be severe, but are no worse than the current consequences of a mistake in managing the root zone data.
- Even with relatively stable data, there will be a need for signatures to be replaced regularly and so generate a far higher volume of changes to the root zone than there is currently. This signature rollover needs to happen on a regular basis, regardless of how often the root zone is updated with regular DNS changes.
- To introduce an unrelated third party would potentially add delay, cost and complexity, and thereby inhibit DNSSEC take-up.

4.3 How it should work?

From our analysis of these factors, we believe that the following proposal is the best possible solution to this apparently intractable problem.

IANA should be responsible for creating and maintaining the Key Signing Keys (KSKs) used for the root zone. IANA and IANA alone should have the private portions of the keys and use those for the generation of Zone Signing Keys (ZSKs).

IANA should send to the RZM the public portions of the KSKs and the public and private portions of the ZSKs for the RZM to use.

The RZM should be responsible for publishing the public portions of both keys in the root zone and for using the ZSKs to create signatures following agreed algorithms that maintain the balance between security and manageability.

We believe this maintains the appropriate balance of security and practicality of implementation, whilst reflecting the current separation of responsibilities between IANA and the RZM.

To be clear, we do not believe there is any role for a third party in this process.

4.4 Interplay with Internet Governance

Whilst we are aware that the role of IANA, and in particular the role of the US Department of Commerce in reviewing each zone file update, has provoked international controversy for example during the World Summit on the Information Society. Mechanisms incorporated into the Tunis Agenda, such as the process towards enhanced cooperation, together with ongoing discussions within the Internet Governance Forum, should incorporate the expanded root management function, including DNSSEC signing.

Our proposal would not alter (or strengthen) the role currently undertaken by the US Government. It would leave day-to-day technical management in the hands of a technical body.

5. Is there an alternative to signing the root?

Without a signed root, each Top Level Domain that enables DNSSEC will have to arrange for the distribution of their trust anchor to security-enabled nameservers worldwide. A scheme called DNSSEC Lookaside Validation (DLV) has been proposed as a way of doing this.

Theoretically, the concept of DLV side-steps the issue of "who signs the root" by creating an authentication point at an unrelated part of the DNS hierarchy. Furthermore DLV can support multiple points of validation across the DNS.

However, we believe that DLV should not be considered a credible alternative to signing the root, for the following reasons:

- We believe that a trust anchor root that is separate from the authoritative TLD root introduces a level of complexity that is too much for widespread public adoption. There are questions of how TLDs are to be authenticated into a DLV root, who is responsible for it and which of many DLV roots is the right one to trust.
- DLV is technically problematic. It requires a high level of traffic to the DLV root and a dependency on the DLV root being available at all times. Widespread adoption of DLV would therefore introduce fragility to DNS that has never existed before. It is widely accepted that the robustness of DNS has been a major contributor to its success and DLV in its current form could undermine that.

It should be noted that DLV is not a standard and is unlikely to become one whilst it remains technically problematic.

We are working with others on an alternative DLV proposal that would fix the technical problems with DLV, but still would not make DLV an alternative to signing the root.

6. Our proposals in brief

- There should be a single root that combines the authoritative list of TLDs and the start of the DNSSEC chain of trust for those TLDs.
- Sign the root as soon as possible, with IANA responsible for creating and managing keys and the RZM responsible for adding signatures to the root zone data.
- Deal with oversight issues for the IANA function as a whole, through the ongoing process towards enhanced cooperation arising out of the Tunis Agenda.
- Avoid DLV.

7. Glossary

BIND

The Berkeley Internet Name Daemon is the most common DNS nameserver implementation in use worldwide. Whilst BIND is open source, it is developed and maintained by the Internet Systems Consortium, a highly professional and capable organisation who make BIND available for multiple platforms and languages. Recognising the importance of BIND to our work, we are a major contributor of fund to ISC for the ongoing support and development of BIND.

DKIM
Domain Keys Identified Mail is a technology that allows a cryptographic signature to be added to outgoing emails, thereby allowing the recipient to verify they were genuinely sent from the address that is given as the sender in the message. Without DKIM spammers will continue to be able to send email where the sender address has been faked and the recipient will be unable to detect this through automated means.

DLV
Domain Lookaside Validation, is a scheme to publish trust anchors for zones, outside of the Domain Name System's hierarchy, hence the term 'lookaside'. This allows for aggregation of TLD trust anchors on various locations, avoiding the necessity to have a single signed root.

KSK and ZSK
A Key Signing Key is a fundamental component of DNSSEC. This is a cryptographic key that is used solely to sign other keys as part of a chain of trust.

A Zone Signing Key is a key used to sign the data published in a zone. A ZSK is signed by a KSK and is generally a shorter lived (and possibly cryptographically weaker) key than a KSK.

By splitting the usage of keys between KSKs and ZSKs a balance is made between the processing required to verify a signature, the lifetime a key is in use, and the frequency with which a user of the zone needs to retrieve and verify new keys.

NSEC3
An enhancement to DNSSEC that changes the way answers on non-existent or insecured delegations are given. It prevents the practice of zone file enumeration, where a miscreant can use NSEC records (the precursor to NSEC3) to gain an entire copy of a zone file remotely. NSEC3 also adds support for opt-in, whereby a zone publisher can choose whether insecure delegations are signed or unsigned.

RZM
The Root Zone Maintainer (RZM) is the organisation contracted to manage updates to the root zone and to distribute those to the root server operators. The RZM at the time of writing is Verisign.

TLD
A Top Level Domain is a domain immediately below the root, such as .uk or .com.

Public Interest Registry SM

1775 Wiehle Ave.
Suite 102A
Reston, VA 20190

PHONE: +1-703-464-7005
FAX: +1-703-464-7006
WEB: www.pir.org

August 2, 2006

Tina Dam, Chief gTLD Registry Liaison
ICANN
4676 Admiralty Way, Suite 330
Marina del Rey, California 90292-6601

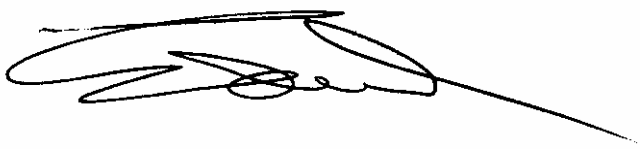
Dear Tina:

This letter is written to advise that PIR intends to implement DNSSEC in accordance with the IETF standards. While PIR does not yet have a specific timeline, we are actively working to prepare our systems and procedures to provide this service.

Please provide guidance on what coordination, approval and/or operational adjustments are required by ICANN in order for us to implement and deploy this service.

Thank you.

Yours very truly,



Edward Viltz
President & CEO

cc: Karen Lentz, gTLD Registry Liaison
Patrick Jones, Registry Liaison Manager
Kurt Pritz, Vice President – Business Operations

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.

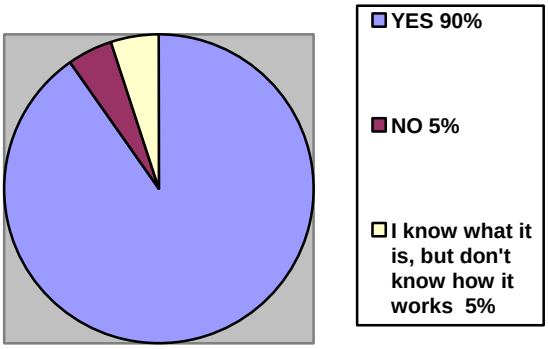
The survey was conducted between 12th September – 12th October 2007. It was sent out to the ccNSO members list and the wwTLD list. The survey was also conducted in Spanish and French, and respondents had the opportunity to reply in Arabic, Spanish, French, Russian and German.

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

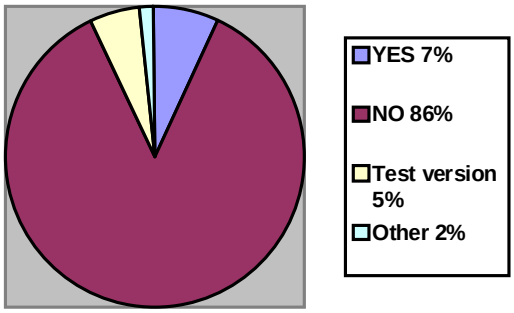
Africa: 18
Asia-Pacific: 19
Europe: 12
Latin America: 8
North America: 4

(following the ICANN Regions)

1) Do you know what DNSSEC is?



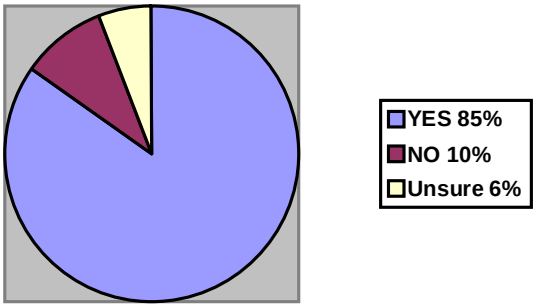
2) Has your registry implemented DNSSEC?



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.

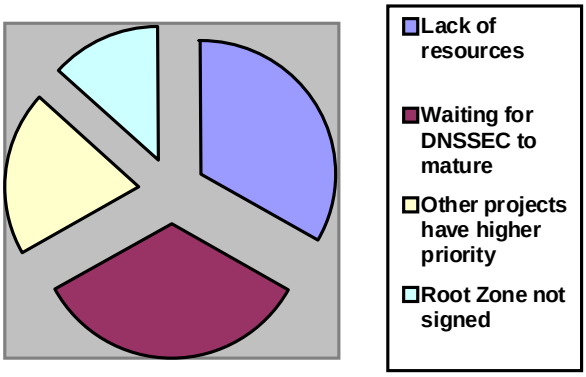
One respondent ("Other") had implemented DNSSEC under ENUM and was ready to implement it on the ccTLD level as soon as the zone walking issue was solved.

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).

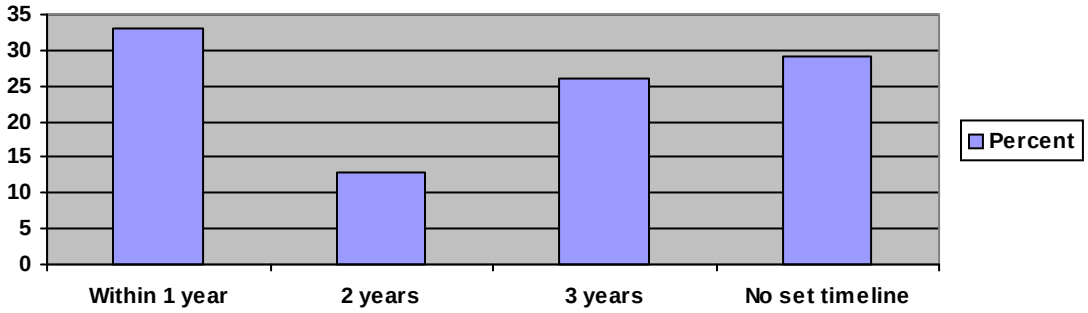
6) If you have implemented DNSSEC, please briefly describe your experience:

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.

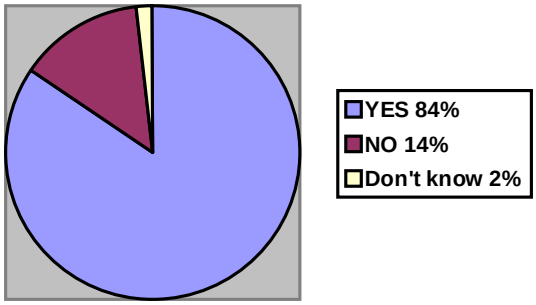
The individual answers to this question are attached in appendix 2 (randomly presented, with the name of the ccTLD removed).

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

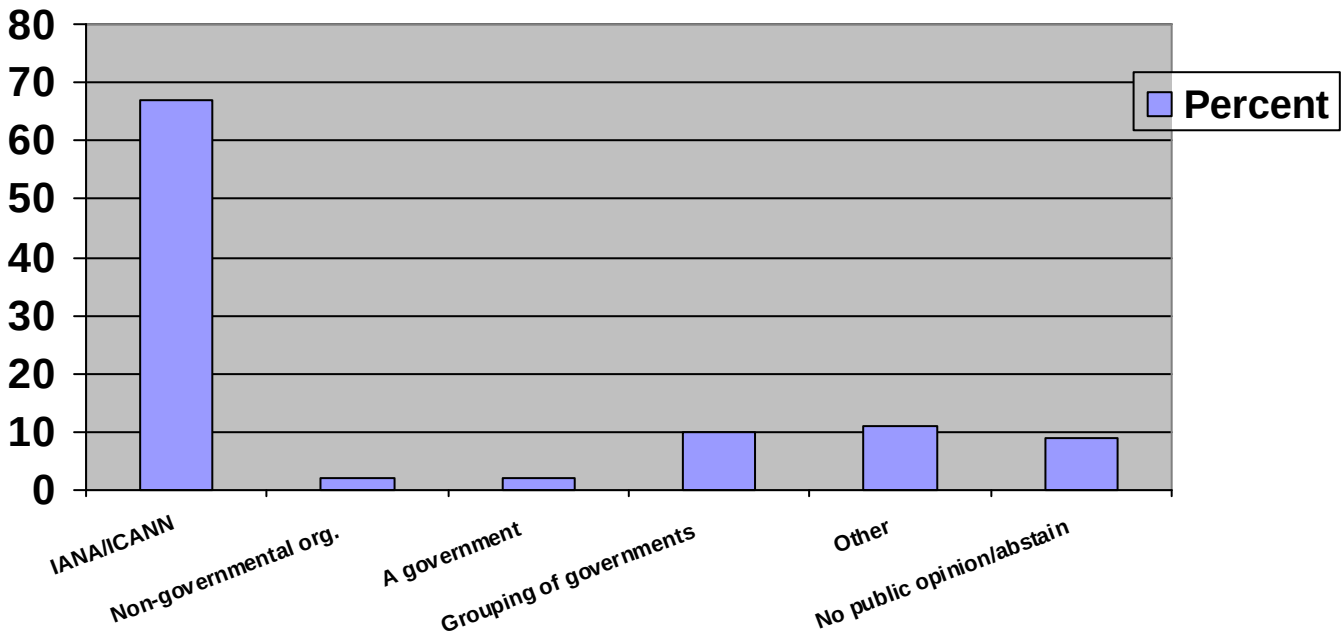
Most responses circled on the direct improvement to the DNS of ensuring the integrity of the answer during transmission. More generally it was expected the technology could improve business confidence in the Internet, and possibly help to minimise fraudulent use of the Internet. Some had received enquiries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

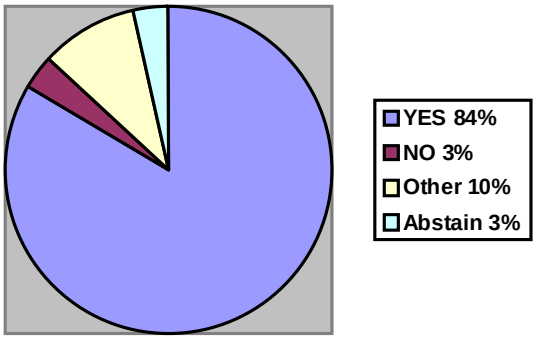


11) Who should be the signer of the root zone?



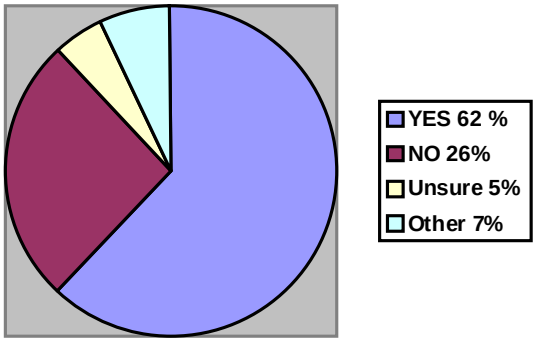
Many of the respondents under “Other” suggested models with multiple signers - such as ICANN/IANA + non-governmental organisation, ICANN/IANA + government(s) or ICANN/IANA + gNSO + ccNSO + RIRs. Other suggestions included ISOC, such as having a board of ISOC appointed trustees signing the root.

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