Retouradres: Postbus 5022, 6802 EA Arnhem

Office of International Affairs
National Telecommunications and Information Administration
US Department of Commerce
Ms. Fiona Alexander
1401 Constitution Avenue / Room 4701
Washington DC 20230
USA

Address
Utrechtseweg 310
6812 AR Arnhem
The Netherlands
P.O. Box 5022
6802 EA Arnhem
t. +31 (0)26 352 55 00
f. +31 (0)26 352 55 05
info@sidn.nl
www.sidn.nl

KvK Arnhem 41215724
BTW nr. NL8048 02 671 B.01
ABN AMRO 60.18.67.165

Date	24 November 2008
Subject	Notice of Inquiry regarding DNSSEC implementation at the root zone
Reference	
Your reference	
Our reference	2008051
Attachment	

Dear Ms. Alexander,

SIDN is the registry for the .nl country-code top level domain, which, with over three million registered domains, is one of the world's largest and most successful ccTLDs. SIDN also manages the Netherlands' ENUM zone 1.3.e164.arpa.

Since its creation in 1996, SIDN has been closely collaborating with the global internet community with the objective to assure availability, accessibility, stability, security, overall quality and further development of the Internet in general and the .nl name-space (and, since 2007 the 1.3.e164.arpa space) in particular.

We believe that the original principles of stability, interoperability, competition and private bottom-up coordination continue to gain additional relevance in light of the developments such as the advance in Internet technology, the expanded global reach of the Internet, and the international dialogue.
We also believe in a DNS that is managed by the private sector and an Internet that is coordinated, not controlled.

Date 24 November 2008
Our reference 2008051

As the Chief Executive of SIDN, I welcome the opportunity for stakeholders to give comments regarding DNSSEC implementation at the root zone.

With this submission SIDN does not aim to individually address the questions raised in the Notice of Inquiry published by the NTIA, as we do not have an appropriate answer to all the questions listed. We would however like to take the opportunity to provide input that will help in reaching consensus on at least part of the issues involved.

SIDN ran the first DNSSEC testbed (SECREG) with real registry data in 2002-2003 after operating an even earlier testbed with an older version of the DNSSEC protocol. The results of these experiences are documented in a report by NLnetLabs (http://www.nlnetlabs.nl/downloads/publications/dnssec/dnssecnl/secreg-report.pdf).

SIDN will implement DNSSEC at the Netherlands ENUM zone in early 2009. Deployment of DNSSEC at the .nl ccTLD zone has not yet been planned, as this will be decided after we have gained enough operational experience with the ENUM zone to be confident that DNSSEC can be deployed for the fairly large and frequently updated .nl zone without any risk to the stability of the zone and the trust of it's present operation.

Current deployment of DNSSEC mostly lacks proven automation of signing frequently updated and/or large zones at TLD registries and maintenance of a large number of zones by registrars/DNS service providers.
Testing and signing of zones as small and slowly updated as the root zone, have succesfully been done numerous times already.

On the whole, we see no technical reasons why DNSSEC could or should not be deployed at the root.
On the contrary, we would welcome a signed root as this would support our efforts on the ENUM zone, and would ease a possible future deployment of DNSSEC for the .nl ccTLD with a single trust anchor.

We are not aware of any feasible alternatives to DNSSEC that could be a sufficient solution to address cache polluting and that work end-to-end.
SIDN favors an end-to-end solution like DNSSEC to maintain the open communication and innovation opportunities it delivers.

We do see an opportunity in deploying DNSSEC at the root in the sense that when the root is signed and secure delegations are made, certain root zone management procedures can be facilitated much better. For example, changing nameservers or glue records for TLD's can be authenticated automatically over DNSSEC at the choice of the TLD manager without manual procedures like approaching administrative and technical contacts for approval. This will facilitate a much desired faster provisioning of requests or emergency changes from TLD managers which improves the consistency of the DNS and stability of the Internet.

Lastly, I would like to strongly stress my opinion that DNSSEC and the management of the keys used therein is not, and should not be, about control, but about data authenticity and integrity.
The deployment of DNSSEC in the root should not be used to change or establish authority of parties over the creation, modification or confirmation of entries in the root zone management system.
Management of the DNSSEC keys is an operational task with a higher level of security to prevent compromising or losing the keys, but does not deliver a different level of trust on the organizations responsible for the key management or root zone maintenance.

SIDN trusts the multi-stakeholder organizations ICANN and IANA and considers them adequately independent for root-zone management process maintenance.
We feel that these organizations are the most stable entities in the current root zone management process and would find it appropriate if the key management was be maintained by either one.
Management of the root zone should be shielded from the heat of day-to-day politics as well as from strong commercial influences.

Date 24 November 2008
Our reference 2008051

Yours sincerely,

Roelof Meijer
CEO SIDN