nominet®

Fiona Alexander
Associate Administrator
Office of International Affairs
National Telecommunications
and Information Administration
US Department of Commerce
1401 Constitution Avenue NW
Room 4701
Washington DC
20230
USA

Contacting us

Phone: 01865 332211
Fax: 01865 332288
Email: nominet@nominet.org.uk
Write to: Nominet UK, Minerva House, Edmund Halley Road,
Oxford Science Park, Oxford, OX4 4DQ
Web: www.nominet.org.uk

24 November 2008

DNSSEC: Nominet's Response to the NTIA Consultation

Dear Ms Alexander,

Nominet is the registry for .uk Internet domain names. With over seven million registered domain names, we are one of the largest top-level domains in the world. As the ccTLD for the UK, we believe that we have an important role and responsibility to provide the right environment for the secure and stable development of the UK Internet economy.

We strongly support the need for the root to be signed, and we would urge there to be rapid progress towards achieving this.

We welcome the NTIA consultation on DNSSEC and hope that this will open the way to implementing a signed root: we strongly believe that a signed root will provide the fundamental layer for a more secure and trusted Internet. It is needed for the wider Internet infrastructure industry to be able to provide innovative tools and applications for business and consumers to help address some kinds of Internet fraud.

Nominet, in its position paper of 28 October 2007[1] clearly identified that we believe that there should be a single root that combines the authoritative list of Top-Level Domains (TLDs) and the start of the DNSSEC chain of trust for those TLDs.

This remains our position. However, since the 2007 position paper, the potential for attacks to hijack large amounts of namespace has become public knowledge. This reinforces our concern about the need for early action and increases the urgency for introducing a signed root.

Security and trust are of increasing concern to business and other users of the Internet and it is incumbent on the Internet industry to put in place the necessary tools to help safeguard Internet transactions.

Even when the root is signed, much work will still need to be done to develop applications that use the technology and, in particular, to develop confidence in, and uptake of, these new solutions. Bearing in mind economic and social dependence on the Internet, delay carries the risk of failing to prevent significant and unnecessary harm. But without commitment to signing the root, it is difficult to convince businesses to commit the significant investment needed.

We strongly believe that the approach to signing the root should not alter – either strengthen or weaken – the role of verification and authorisation currently undertaken by the US Government as administrator of the authoritative root-zone management process. Oversight

---

1. Signing the Root, A Nominet Position Paper, http://www.nominet.org.uk/digitalAssets/27762_Signing_the_Root.pdf

issues for the IANA function as a whole should be dealt with through the ongoing process towards enhanced cooperation arising out of the Tunis Agenda.

Introducing additional steps or operators will increase the complexity of the process, without improving oversight. It will make it more difficult for TLD operators to identify the bottlenecks in the process, reducing trust in the system. The operation of the IANA process has improved considerably over recent years: we would not want to see these benefits lost by increasing the complexity of the process for updating the root zone file.

As such, we would like to see a clear process that focuses on a single operator with the responsibility for generating keys and signing the root and zone brought together with the IANA function. The fourth proposed process flow model (Appendix A of the consultation - http://www.ntia.doc.gov/DNS/DNSSECproposal4.pdf) is, we believe, the simplest and gives the best clarity on responsibility and accountability, without throwing into question the role of the administrator in verifying root change requests. We do not believe that it is necessary for the administrator to take an additional role, although we would not have any strong objections to it verifying or authorising the root signing key update request, if this allowed early adoption.

One of the key features of the operation of the IANA function is its relative independence from the operators. This separation has been important in engendering trust in the way that the domain name system operates. We would have concerns if the introduction of DNSSEC led to a system that did not have sufficient separation of functions to guarantee at least the same level of trust as the present system. While we recognise VeriSign's technical competence, putting it in a central position in signing the root would require the introduction of independent oversight to ensure effective functional separation both with its business as the largest TLD operator and with its security activities.

We also see the automation of the IANA – the e-IANA – as an important step in ensuring that the management of the authoritative root zone is as effective and assured as possible. The introduction of a signed root could usefully be supported by the e-IANA, which we believe has successfully completed its testing. Both can be introduced independently, and we would not envisage any issues if they were introduced within the same timeframe.

In conclusion, we recognise and welcome the high priority that the US Government has given to the security and stability of the Internet. The introduction of DNSSEC is important for improving the security of the DNS against certain kinds of malicious attack, and we would welcome the early introduction of a signed root.

Nominet is committed to work with NTIA and others on issues associated with implementation or in helping to address technical concerns.

Yours Sincerely,

Lesley Cowley
CEO Nominet