Comments of the Internet Governance Project
on
Enhancing the Security and Stability of
the Internet's Domain Name and Addressing System
(Docket Number: 0810021307-81308-01)
submitted to
The National Telecommunications and Information Administration
U.S. Department of Commerce
November 24, 2008

The Internet Governance Project (IGP) welcomes the opportunity to comment on the possible deployment of Domain Name Security Extensions (DNSSEC) at the root zone level of the Domain Name System (DNS). IGP is an international alliance of academics with expertise in international governance, Internet policy, and information and communication technology. IGP's research and advocacy upholds the values of a global and free Internet, individual human rights and democratic governance.

Deployment of DNSSEC at the root zone would create globally unique digital signatures that would be used to identify, authenticate, and provide denial of existence of root zone resource records. As noted in the Notice of Inquiry (NOI), the deployment of DNSSEC at the root zone and the creation of a single trust anchor could simplify resolver validation and provide incentive for broader DNSSEC adoption. However, these benefits will only be achieved if the process flow for creating a single trust anchor is accepted by the global Internet community.

The act of signing the DNS root raises political and economic issues as well as technical ones. While the DNSSEC protocol has been refined technically over more than a decade within the IETF and elsewhere, discussion and analysis of the political and economic dimensions of DNSSEC deployment have just begun.

Our analysis of the root signing proposals flows from recognition of this basic fact:

1. *Deployment of DNSSEC at the root zone, if it led to widespread reliance on a single trust anchor, would dramatically increase the switching costs associated with any attempt to defect from, or provide an alternative to, the existing DNS root. In effect, DNSSEC root signing presents a risk of locking in existing DNS root zone management arrangements.*[1]

This fact raises both political concerns and competition policy concerns. Our first two comments elaborate on the political and economic concerns, respectively. Our last point proposes interim steps that could be taken to enable DNSSEC deployment while avoiding these problems.

---

[1] While another entity would still be able to retrieve, sign and publish the resource records contained in the ICANN root using their own key, they would not be able to replicate the digital signature(s) generated by the authoritative root zone signing device, and thus could not offer a secured DNS based on the currently distributed root key. As noted in Mueller, 2002, replicating the legacy root zone is easy, it is the very strong network externalities created when the entire world uses a specific root for coordination that make DNS registries dependent on the ICANN root.

2. *Support a process flow that recognizes diverse national interests in a secure DNS root*

Because the root zone file sits atop the logical DNS hierarchy, it is a structural bottleneck for resolving queries in the global Internet. The history of bottlenecks within global communications networks demonstrates that they can become points of control and contention, particularly when policy choices concerning them can affect national security or commercial interests.[2] More than 200 TLD operators rely on the root zone, including rapidly-growing ccTLD namespaces. Internet-supported economies and governments are developing around the world. Thus, if it wants DNSSEC to succeed, the U.S. Department of Commerce must ensure that any process flow for deploying DNSSEC at the root zone considers and serves not only the interests of the United States government, but also the interests of the global Internet community.

The current VeriSign proposal for signing the root (reflected in the Department's Proposed Process Flow #6) would distribute signing authority to the Root Server Operators using an "M of N" scheme. **The VeriSign proposal is flawed in that it does not require sufficient regional or political diversity. By suggesting only 5 root server operators to constitute "M", it would allow U.S. based root server operators to sign the root zone without any support from other regions.**

The Department expressed in August 2008 that it has no plans to undertake discussions regarding changes to the respective roles of ICANN, VeriSign or the Department in the management of the authoritative root zone file.[3] And in fact, all of the process flows currently being considered reflect a continued authorization role for the Department in securing the root zone. **While this NOI does not specifically consider the issue of oversight, it is the opinion of the IGP that the Department's authorization role in the deployment of DNSSEC at the root zone unnecessarily politicizes what should be a technical coordination activity.**

3. *Do not institute a process flow that creates competition policy problems*

From an economic perspective, deployment of DNSSEC at the root zone raises competition policy concerns with respect to possible vertical integration of root zone management functions with either root zone Key Signing Key (KSK) activities or Zone Signing Key (ZSK) activities. Depending on if and how these functions are integrated, there is the potential for them to be controlled to gain an advantage over competitors in an adjacent or downstream market.[4] Discriminatory behavior could include tampering with or refusing to sign a TLD operator's resource records, effectively excluding the TLD

---

[2] See e.g., Desai (2008); Diffie and Landau (2007); Headrick (1991)

[3] See Department of Commerce*, Public Comments: Improving Institutional Confidence in ICANN,* (July 30, 2008), available at http://www.ntia.doc.gov/comments/2008/ICANN_080730.pdf

[4] For a helpful discussion of competition policy issues surrounding ICANN and the root zone, see Froomkin and Lemley (2003), for a more general discussion of bottleneck and network effects issues see Faulhaber (2005).

zone and its users from benefits provided by a secured authoritative root. Unfortunately, this risk is reflected in the current proposals put forth by ICANN and VeriSign.

The ICANN proposal for signing the root (reflected in the Department's Proposed Process Flow No. 4) suggests that control of KSK operations may be assigned to other organizations. **However, the ICANN proposal is insufficiently developed in that it offers no specifics regarding to whom KSK operations would be distributed or how they would be conducted.**

The current VeriSign proposal for signing the root (reflected in the Department's Proposed Process Flow No. 6) suggests that they edit, generate, sign (i.e., using the ZSK) and distribute the root zone file. **Although VeriSign performs its root zone management activities under contract with the Department, the proposal is flawed in that it potentially allows the operator of the world's largest TLD zone to adversely affect competing TLD operations.**

The typical remedy for vertical integration problems is structural separation. With respect to KSK activities, this would entail selecting a process flow that clearly establishes independent, globally representative Root Key Operators that are jointly responsible for KSK operations. With respect to ZSK activities, it is acknowledged that root zone edits, generation and ZSK activities should remain within a single organization. However, ZSK operations should not reside with an organization that competes directly with other TLD operators.

4. *Support the deployment of a Trust Anchor Repository as an interim step in securing the DNS root*

Given the important and irreversible changes that would be affected by signing the root zone, and the obvious flaws in the two major proposals (ICANN and VeriSign) before the Department, there is no need to rush the choice of an optimal method. Fortunately, a viable interim solution exists: a Trust Anchor Repository (TAR).

A TAR would store and provide access to TLD operators' secure entry points. This solution should be deployed by IANA. Given the relatively small number of TLD operators currently signing or expressing interest in deploying DNSSEC, a TAR is an adequate interim solution. It will enable registries and resolver operators to experiment with DNSSEC and deploy the technology if they choose. It is recognized that a TAR might not provide a long-term solution because of scalability concerns expressed by resolver operators.[5] However, a TAR does not prevent or conflict with the pursuit of DNSSEC deployment at the root zone. In fact, it is viewed as a possible component of one proposed process flow.[6] **Perhaps most importantly, an interim TAR would avoid the current political and economic issues of deployment of DNSSEC at the root,**

[5] Scalability concerns center on the possible number of trust anchors contained in a TAR and the ability of resolver operators to configure resolvers properly when those trust anchors are rolled over.

[6] See section 2.2, VeriSign Inc., *Root Zone Signing Proposal*, (Sep 22, 2008), available at http://www.ntia.doc.gov/DNS/VeriSignDNSSECProposal.pdf

since IANA could 1) develop the procedures for its operation (e.g., authentication of TAR data) with the global Internet community within the ICANN process and, 2) deploy it without the oversight of a U.S. government agency or operational involvement of a TLD operator.

As noted in the Notice of Inquiry, the ICANN Board approved a TAR proposal in April 2008, and a recent presentation by IANA staff indicates that a functioning TAR is near completion and could be opened to TLD operators by end of November 2008.[7] While ICANN's approved TAR is proposed as an interim measure, no arbitrary restrictions should be imposed on its lifetime. Instead, its lifetime should be based "on the level of benefit it provides to the community at any given point in time."[8] Deploying a TAR would allow time for development and implementation of a process flow that encourages convergence by the global Internet community on a single DNS root trust anchor. It is the view of the IGP that the Department should encourage and not inhibit this activity.

5. References

Cowhey, P., & Mueller, M. Delegation, Networks and Internet Governance. In *Networked Politics* (2008). Cornell University Press.

Desai, A. C. Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy. *Stanford Law Review*, *60*(2), 553-594.

Diffie, W., & Landau, S. (2007). *Privacy on the Line: The Politics of Wiretapping and Encryption* (2nd ed.). The MIT Press.

Faulhaber, G. (2005). Bottlenecks and Bandwagons: Access Policy in the New Telecommunications. In *Handbook of Telecommunications, Technology Evolution and the Internet, Vol. 2* (pp. 488-517). Elsevier.

Froomkin, A. M., & Lemley, M. A. (2003). ICANN and Antitrust. *University of Illinois Law Review*, *1*.

Headrick, D. R. (1991). The Invisible Weapon: Telecommunications and International Politics, 1851-1945. Oxford University Press, USA.

Mueller, M. L. (2002). Competing DNS Roots: Creative Destruction or Just Plain Destruction? *Journal of Network Industries*, *3*(3).

National Research Council. (2005). *Signposts in Cyberspace: The Domain Name System and Internet Navigation*. National Academies Press.

---

[7] See Lamb, R., *ICANN proposal to sign the root*, (November 5, 2008) available at http://cai.icann.org/files/meetings/cairo2008/lamb-dnssec-05nov08.pdf

[8] See Sparta Inc., Shinkuro Inc., and National Institute of Science and Technology, *Statement of Needed Internet Capability: Trust Anchor Repositories,* (Jun 9, 2008) available at http://www.dnssec-deployment.org/tar/