From: IAB Chair <iab-chair@ietf.org>
To: <DNSSEC@ntia.doc.gov>
Date: Tue, Nov 18, 2008 2:46 PM
Subject: DNSSEC deployment at the Root.

Dear Ms. Alexander,

The IAB appreciates the assistance of NTIA, or any other organization, in the rapid deployment of DNSSEC. Hence, we are happy to provide our feedback to the Notice of Inquiry regarding "Enhancing the Security and Stability of the Internet's Domain Name And Addressing System" as published in the Federal Register Vol 73, No 197, d.d. October 9, 2008.

This reply contains a number of observations and statements related to the questions posed in the inquiry.

=== Expedient deployment of DNSSEC at the Root.===

When people use any Internet service, it almost always involves one or more DNS lookups. The base DNS is vulnerable to data corruption and data replacement. DNSSEC is the only standards-track mechanism to prevent corruption and replacement of the DNS data on its path through the Internet. As such, DNSSEC is one of the mechanisms needed to maintain, or even improve, the level of trust with which people use the Internet.

While the administrators of DNS zones must follow certain technical standards so that the overall system works, they also maintain a striking degree of policy autonomy. DSNSSEC has been designed to respect that. At the same time, the DNS, in itself, is technically and operationally hierarchical, and there are many advantages in aligning the DNSSEC chains of trust with that hierarchy, not least of which is the global trust that can come from the general acceptance of a single trust anchor. In other words, because of the inherently hierarchical nature of the DNS, the DNSSEC protocol can only be used efficiently when the protocol is deployed at the root of the DNS hierarchy. Expedient deployment of DNSSEC in the root zone is expected to boost the global deployment of DNSSEC. In that same spirit, and with a reference to appendix A of RFC3172, the IAB is working with IANA to get the .ARPA zone signed.

=== Trust in the System, Confidence, and DNSSEC.===

Consumers of DNS data actively put their trust in the root DNS registry through the configuration of root DNS servers that make that data available. The introduction of DNSSEC provides confidence that DNS data is not modified while it travels between servers and consumers. Adding DNSSEC should not change the trust in the domain name system as a whole, nor in the institutions involved with the management thereof.

To expand on this point:

The consumers of DNS data are typically the devices of the end-users e.g. their PCs or smartphones. Those devices send DNS queries to network components called Recursive Nameservers. These Recursive Nameservers are typically deployed by operators of IP networks such as Internet service providers, network services groups within companies, and sometimes even by individual end-users.

While we do not know the exact number of Recursive Nameservers deployed in the Internet, estimates place their number well into the millions. These Recursive Nameservers need to be configured by their system administrators with the IP addresses of the DNS servers that make the root of the namespace available: the DNS root-servers. It is possible for administrators to configure a set of IP addresses for root-servers that, in fact, do not serve the namespace as administered by IANA. This would cause all sorts of issues detrimental to the stability and security of the Internet, as described in "IAB Technical Comment on the Unique DNS Root" [RFC2628]. The fact that an overwhelming majority of Recursive Nameservers point to the DNS root-servers that serve the root as maintained by the IANA registry is an indication that the system is trusted by the end-users: Their experience has been that the institutions involved in the management of the DNS (the registry and nameserver operators) have provided domain name mappings that are coherent, stable, and as expected. With the introduction of DNSSEC the operators of Recursive Nameservers have to, in order for validation to occur, configure a public key that corresponds with the "Key-signing key"(KSK) with which the mapping as maintained by the registry is signed. This public key is tied to namespace in much the same way as the IP addresses of the root-servers are tied to the namespace. That is, trust in the DNS root-servers depends on administrator configuration, and DNSSEC simply includes a new parameter to the configuration. Configuration is more likely to happen if key custodianship is aligned with DNS registry maintenance in such a way that DNSSEC deployment does not become an issue of control and ownership but remains a matter of data-integrity and authenticity.

=== Process flow===

We acknowledge that introducing DNSSEC in a zone without proper planning and care can involve a new degree of complexity and thereby bring the risk of parts of the system becoming more fragile. However this is normal with any new technology and experience is already being gained with zones which are significantly bigger than the root zone. However, some of the proposals in the notice of inquiry involve data travelling around the system and introduce more parties than are currently involved in the root-zone generation. Initial experience with DNSSEC operations has indicated that zone-generation and zone-signing are two functions that are best performed by the same party, avoiding the need for unsigned zone or key data to change hands, or the introduction of another security mechanism to protect the yet-to-be signed zone or key data as it changes hands.

It should also be noted that during initial deployment the number of customers of DNSSEC data will be relatively small. Because of that the stakes are relatively low, and the design of the system allows for relatively simple procedures. These considerations allow for flexibility, and should be taken into account when designing the key generation procedures, the storage mechanisms, and disaster recovery protocols

=== Rolling of the DNSSEC Key Signing Key ===

DNSSEC has been designed with the notion that keys used in the process are replaced once in a while for security reasons. The deployment of DNSSEC at the root should take this into account. These key rollovers should take place regularly so that a clear expectation is built for the administrators of Recursive Nameservers. A key rollover policy should be developed and discussed in an appropriate open forum. The development of that policy does not need to block deployment as long as it is clear that a KSK rollover will occur.

A system where the change of the KSK custodian does not necessarily need to result in a roll of the key has preference

=== Summary===

The IAB expects expedient and successful deployment of DNSSEC if the following points are taken into account:

* Care should be taken that DNSSEC deployment remains about data, integrity, and authenticity, and not about control.

* The implementation of DNSSEC in the root can and should align with the functions involved in the root-zone maintenance, generation and audit. The implementation of DNSSEC, however, need not today nor for the foreseeable future be cause to permanently fix the roles involved.

* After the main policy decisions have been made, further details about the implementation, such as key rollover, in particular the rollover of the root "key signing key" pair (KSK-pair), and possible key custodianship, should be decided upon within the context of the multi-stakeholder process, as currently embodied in ICANN. This would ensure involvement of all stakeholders through well established mechanisms.

* Regular key rollover should always be part of normal operational practice. A key rollover policy for the root should be discussed and developed in an appropriate open forum.

* Simplicity of the system should be a design criterion. Aligning zone generation and zone signing is one example of such design choice.

The IAB will be happy to answer any further questions you may have.

For the IAB

--Olaf Kolkman
IAB Chair

About the IAB

The Internet Architecture Board has a long history but is currently viewed as a senior committee in the IETF which has both technical (architectural) functions and oversight functions for the development of the Internet. The latter include oversight of IANA functions performed for the IETF. See http://www.iab.org/.

CC: <IAB@iab.org>