From: Rob Blokzijl <k13@nikhef.nl>
To: <dnssec@ntia.doc.gov>
Date: Sun, Nov 23, 2008 3:54 PM
Subject: Comments regarding the signing of the DNSSEC root

The RIPE community thanks the NTIA for its consultation on proposals to sign the root and is pleased to offer the following response to that consultation. We urge the adoption of a solution that leads to the prompt introduction of a signed root zone. Our community considers the introduction of a signed root zone to be an essential enabling step towards widespread deployment of Secure DNS, DNSSEC. This view is supported by the letter from the RIPE community to ICANN as an outcome of discussions at the May 2007 RIPE meeting in Tallinn: http://www.ripe.net/ripe/wg/dns/icann-root-signing.pdf.

It is to be expected that a community as diverse as RIPE cannot have a unified set of detailed answers to the NTIA questionnaire. However several members of the RIPE community will be individually responding to that questionnaire. We present the following statement as the consensus view of our community about the principles that should form the basis of the introduction of a signed DNS root.

1. Secure DNS, DNSSEC, is about data authenticity and integrity and not about control.

2. The introduction of DNSSEC to the root zone must be made in such a way that it is accepted as a global initiative.

3. Addition of DNSSEC to the root zone must be done in a way that does not compromise the security and stability of the Domain Name System.

4. When balancing the various concerns about signing the root zone, the approach must provide an appropriate level of trust and confidence by offering an optimally secure solution.

5. Deployment of a signed root should be done in a timely but not hasty manner.

6. Updates from TLD operators relating to DNSSEC should be aligned with the operational mechanisms for co-ordinating changes to the root zone.

7. If any procedural changes are introduced by the deployment of DNSSEC they should provide sufficient flexibility to allow for the roles and processes as well as the entities holding those roles to be changed after suitable consultations have taken place.

8. Policies and processes for signing the root zone must be transparent and trustworthy, making it straightforward for TLDs to supply keys and credentials so the delegations for those TLDs can benefit from a common DNSSEC trust anchor, the signed root.

9. There is no technical justification to create a new organisation to

oversee the process of signing of the root.

10. No data should be moved between organisations without appropriate authenticity and integrity checking, particularly the flow of keying material between a TLD operator and the entity that signs the root.

11. The public part of the key signing key must be distributed as widely as possible.

12. The organisation that generates the root zone file must sign the file and therefore hold the private part of the zone signing key.

13. Changes to the entities and roles in the signing process must not necessarily require a change of keys.

Sincerely,

Rob Blokzijl
RIPE Chairman