November 24, 2008

Ms. Fiona Alexander
Associate Administrator
Office of International Affairs
National Telecommunications and Information Administration
United States Department of Commerce
1401 Constitution Avenue N.W., Room 4701
Washington, DC 20230
by email: DNSSEC@ntia.doc.gov

Dear Ms. Alexander:

The Internet Society (ISOC) is pleased to respond to the National Telecommunications and Information Administration Docket # 0810021307-81308-01, "Enhancing the Security and Stability of the Internet's Domain Name and Addressing System."

In considering the questions posed in this Notice of Inquiry, ISOC recommends that the decision about how to implement DNSSEC be based on the best technical approach to achieving the desired ends of widely deployed, trusted security for the DNS. These comments complement and support the Internet Architecture Board submission to this Notice of Inquiry, without duplicating its content. Instead, our comments aim to highlight the principles and technical considerations we believe must be kept in mind when deciding on the way forward. A technical annex is included to explain the thinking behind the points that follow.

ISOC believes that the implementation of Domain Name and Addressing System Security Extensions (DNSSEC) at the root zone level is of great importance to preserve the security and stability of the DNS and, in turn, of the Internet itself. We would like to contribute 3 important points to the discussion of implementing DNSSEC by signing the root zone of the DNS:

1. it is important to act now
2. it is imperative to preserve the global trust model of the DNS
3. decisions made now should enhance, not reduce, the ability of the DNS support system to evolve over time

ISOC believes that DNSSEC is an effective technology that will improve the security of the DNS in the future, and that it is important to implement it quickly

and carefully. The Internet community has the means to implement DNSSEC, and ISOC believes that it should be a priority to sign the root as soon as possible, but without undue haste. This will be an important step to facilitate and encourage the deployment of DNSSEC by others.

In taking steps to enable DNSSEC at the root, it is important to preserve global trust in the DNS. Today, there is a single trusted root of the DNS (where responsibility for the root zone file contents rests). All users of the Internet implicitly trust that zone. The root of trust in DNSSEC should not be different than that of the DNS.

Also, absent a signed root, TLD operators that are moving forward with DNSSEC today are storing key validation material in trust-anchor repositories outside the DNS itself. However, as this means there are many different sources of trust anchors, the possibility of multiple disparate “views” of the DNS is introduced. If DNSSEC is not implemented at the root soon, causing alternative trust anchor systems to become entrenched, the existing model of trust in DNS and a single view of the Internet’s naming system may be impossible to restore. This is not consistent with providing a single, global Internetwork.

ISOC believes that it is important not only to determine an implementation of DNSSEC that works today, but also to ensure that the systems (and organizations) that implement it are sound, robust and able to evolve as competencies and the Internet’s requirements change over time. It must be possible to improve DNSSEC deployment and reassign roles as may become appropriate going forward. To illustrate this point: once the root zone is signed, the requirements for distribution may be different from today. Integrity of the root zone content is provided by the signatures on the records, and does not depend on the distribution channel. There is no technical requirement for a single distributor of its contents. Implications of having a larger root zone and implications of more frequent updates, suggest a new distribution mechanism might be appropriate. For example, having multiple distributors not only protects against localized failure, but also enables root-server operators to rely on parties they trust. Parallel operation wherever practical reflects the design value inherent in the DNS.

A further principle may seem obvious, but it is important to emphasize nonetheless. Simple solutions are better than complex solutions, for both technical and security reasons.

Applying this rule to the question of how to enhance the security and stability of the DNS, ISOC recommends that whatever system is established for signing the root, the number of organizations that can act as a bottleneck should be kept as small as possible. It is best to design the system to maximize the number of processes that can be done in parallel, because they create fewer potential bottlenecks; and to minimize the number of processes that have to be done serially, because they create the potential for confusion, conflict and delay.

On reviewing the text of the NOI, and the accompanying supplementary information, ISOC is of the view that several kinds of issues are being raised: some technical, some organizational and some political. We believe that attempting to address these different types of question in the implementation following this consultation could be a distraction from the pressing technical need to accelerate DNSSEC deployment by signing the root as soon as possible. ISOC suggests that instead of elaborating various models of the possible assignment of roles among the organizations currently involved, more progress may result from putting the focus on the information flow implied by the DNS protocol and operation itself. The technical annex to these comments explains this point in greater detail.

Following the line of reasoning shown in the annex, and freed from trying to design in a role for organizations simply because they are involved now, it becomes apparent that it would be possible to arrange the management of changes to the DNS root in different ways after DNSSEC is implemented. For example, the purpose of the administrative oversight function is to provide an external, unbiased, transparent and accountable verification of proposed changes to the root. This could be accomplished in a number of ways, and by different constellations of organizations, but the political question of how that is done does not need to be settled immediately to implement DNSSEC.

As a matter of principle, ISOC believes that the more the DNS is operated by an organization or organizational system that involves all technically competent and legitimately interested global participants in an open, transparent bottom-up process, the better. But discussions of the precise form that might take, or how a variety of actors could become involved in operation of the root key, are extraneous to deployment of DNSSEC. They are important components of the discussion of the ongoing evolution of the stability and acceptability of the DNS system and its operation, but the implementation of DNSSEC should not be delayed because these problems are hard to solve. ISOC continues to advocate that the DNS system should evolve in the direction of enhancing the internationalization of the private sector led, multi-stakeholder approach to the management of the DNS system, as advocated by the NTIA since the original White Paper of 1998.

In conclusion, and to repeat, ISOC believes that it is of the greatest importance that the DNS root be signed as soon as possible, to encourage DNSSEC implementation by all necessary parties in support of the stability and security of the DNS and the Internet as a whole.

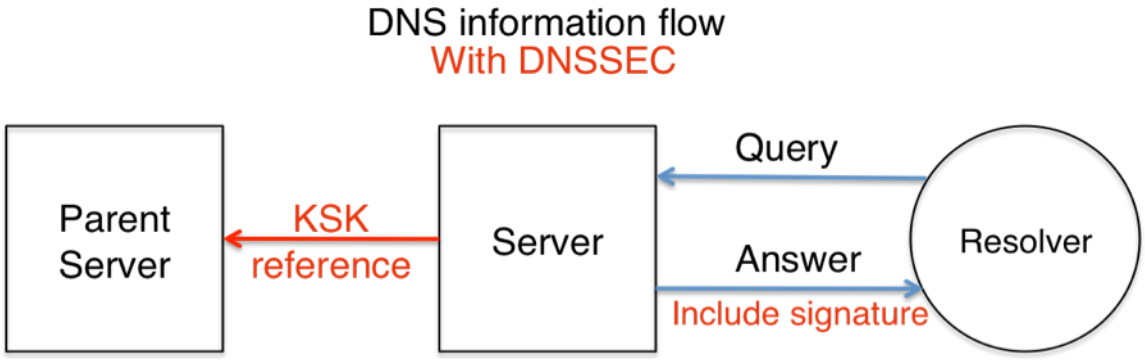
Sincerely yours,

Lynn St. Amour
President and Chief Executive Officer

Technical Annex

ISOC recommends that the design of the process for signing the root focus on the information flow implied by the protocol and operation of DNS, rather than on specific roles of contractors, historical or new. The goal of providing the broadest trust in DNS names is served by transparent operation of the system.

As shown in the following diagram of DNS information flow, DNSSEC (in red) includes cryptographic signatures in answers, which enables resolvers to validate records they receive, possibly through independently operated caches. Resolvers can query many different servers in order to follow referrals from servers that are not authoritative for a name, and to validate signatures. In order to validate answers, the resolver starts at an anchor it trusts and proceeds along a chain of trust established by signed keys along the path of zone delegations.



In addition to zone-signing keys, which produce the signatures for contents of the zone, a DNSSEC server employs key-signing keys (KSK), which produce signatures indicating that the zone has been signed. A reference to this KSK is stored in the parent zone so that a validation chain can be constructed. Validation chains follow the same hierarchy as the DNS names themselves. Key-signing keys are separate from zone-signing keys because changing the keys is expected to be more frequent for zone-signing keys inside the zone than for key-signing keys that are communicated up the chain of trust.

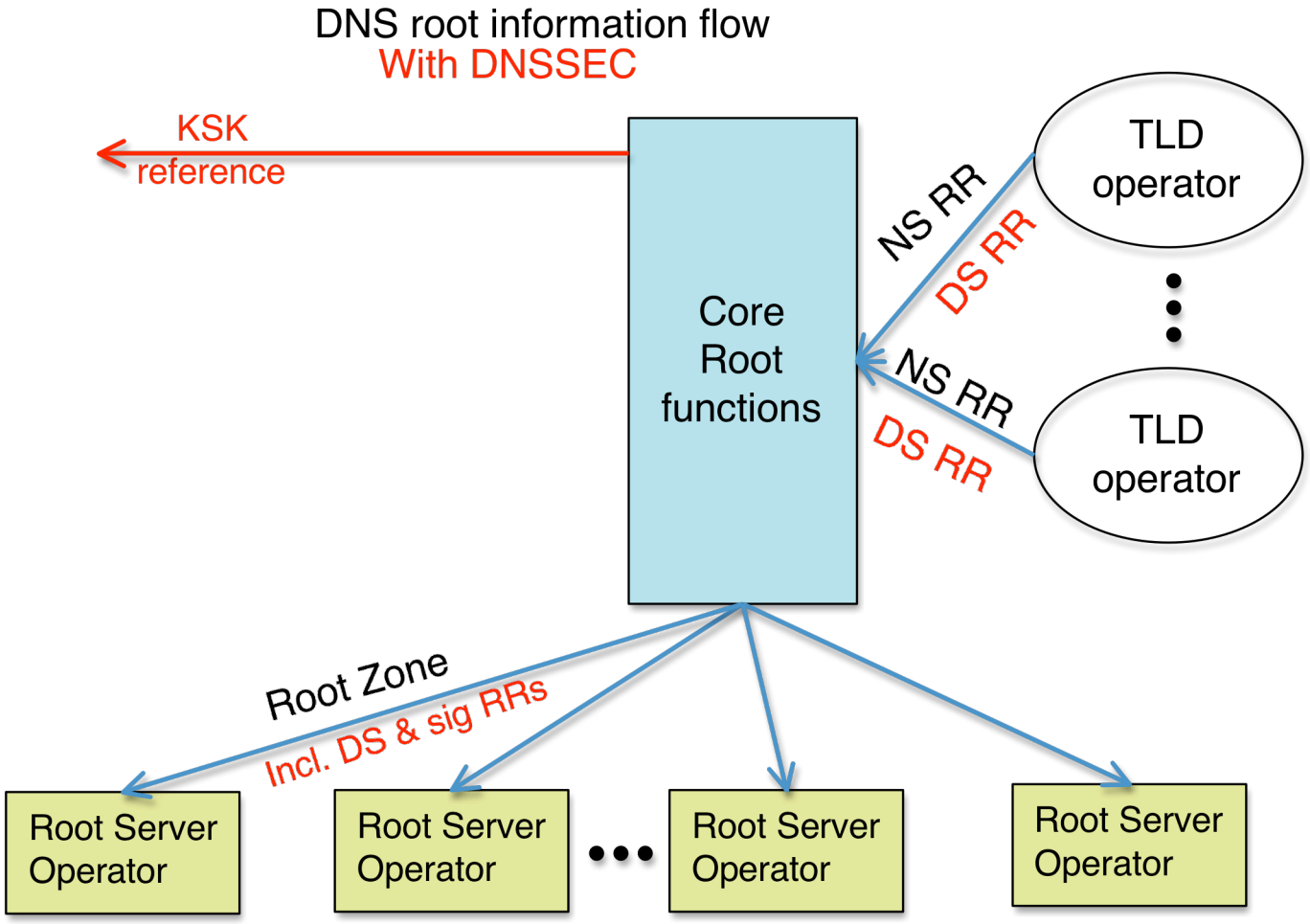
It is worth noting that key validation can also be stored in trust-anchor repositories where a signed zone lacks a signed parent zone, but then resolvers need information about how to reach the trust anchor repositories, different resolvers may use different trust anchors, thereby allowing the possibility of multiple disparate “views” if the DNS. This is not consistent with providing a single, global Internetwork.

The DNS root is special because it has no parent zone. Its trust anchor needs to be available to all validating resolvers, which can be accomplished through widespread publication. The following figure illustrates the information flow for the DNS root (functions colored as in the process flows included in the NOI).

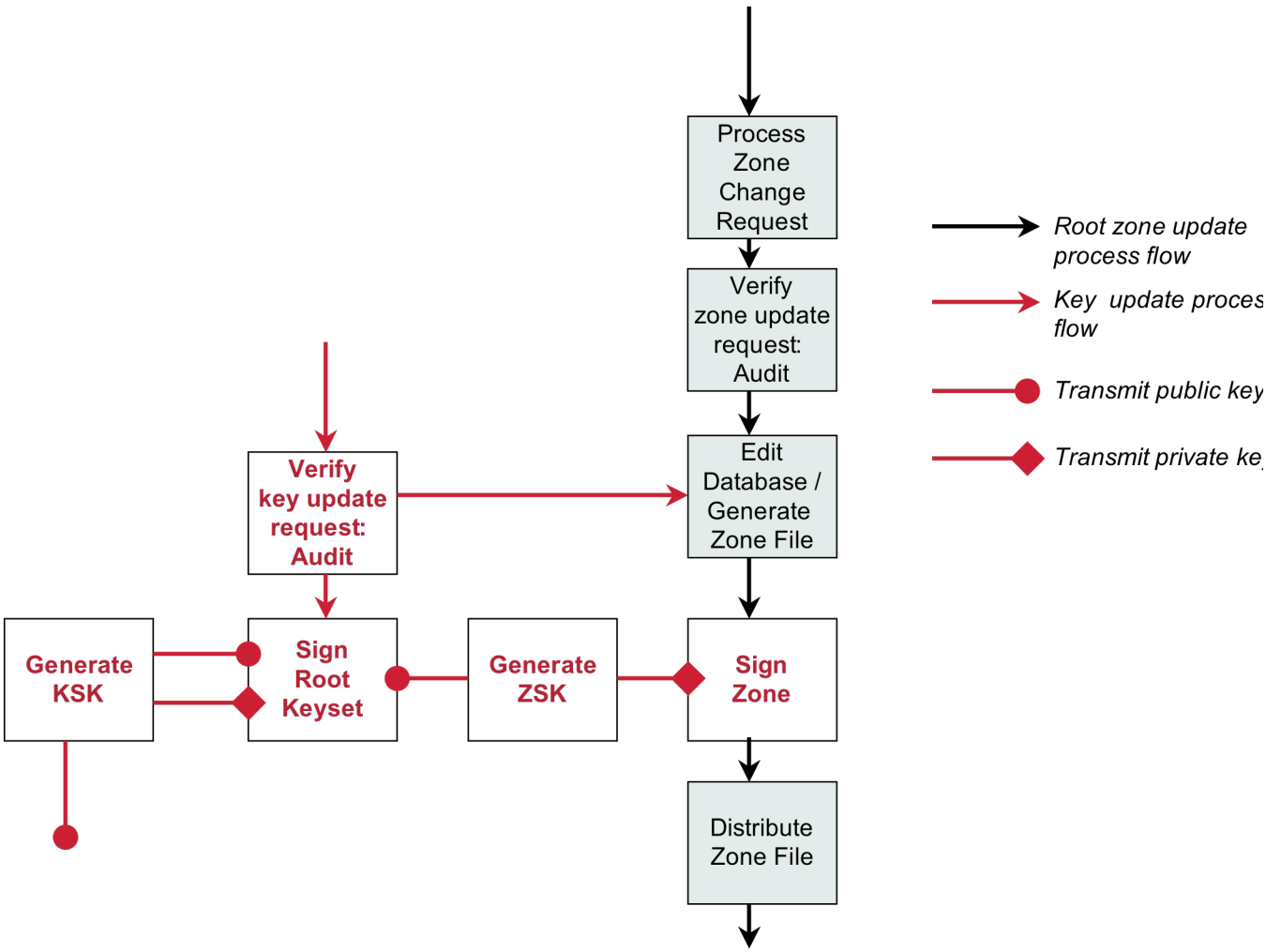
The Core Root (CR) functions are to accept valid changes to the root zone from Top Level Domain (TLD) operators, sign the resulting resource records, and

distribute the root zone. There are technical reasons to not separate some of these functions: private keys and unsigned zone contents should not be transferred unnecessarily because the transfer itself introduces security risks. Other functions, such as oversight and root file distribution can be separated and possibly duplicated.

In addition to installing the name server (NS) records (and glue) into the root zone, CR has to install delegation signer (DS) records in the root zone. A close operational relationship between the CR and TLD operators is required to facilitate both routine and emergency key changes.



In more detail, the Core Root functions are outlined below, without reference to any entity or entities that are or should carry them out.



Global trust in the root's content, including the KSK reference, and the integrity of the root's keys and signatures is imperative. Although the diagram implies nothing about which functions are carried out by what organizations, there are some fundamental requirements to ensure the integrity of and trust in the global DNS and the use of DNSSEC:

- the entire process (including root zone and key updates) must be effected in a way that ensures integrity of the data that is passed from step to step, so that the root zone that is eventually signed is, in fact, as intended by the contributing TLD operators
- the entire process should be undertaken in an organization or organizational system that is supported by the contributing TLD operators
- transmitting private keys requires particular attention to security mechanisms. Currently, the best forms of security are implemented by not transmitting them outside of a single organization: concentrating these operations minimizes exposure of both the keys and the zone data to compromise and avoids transmission delay when recovery from compromise is urgent
- the components of the process may be implemented differently in the

future. For example, we note that any audit function is improved by open and transparent operation – of the oversight process and of the root zone.

Finally, to emphasize the point, once the root zone is signed, the requirements for distribution may be different from today. Integrity of the root zone content is provided by the signatures on the records, and does not depend on the distribution channel. There is no technical requirement for a single distributor of its contents. Implications of having a larger root zone and implications of more frequent updates, suggest a new distribution mechanism might be appropriate. For example, having multiple distributors not only protects against localized failure, but also enables root-server operators to rely on parties they trust. Parallel operation wherever practical reflects the design value inherent in the DNS.