November 24, 2008

Fiona Alexander,
Associate Administrator,
Office of International Affairs, National Telecommunications and Information Administration,
U.S. Department of Commerce,
1401 Constitution Avenue, N.W., Room 4701,
Washington, DC 20230

Foreword

Intel would like to thank the Department of Commerce and the National Telecommunications and Information Administration (NTIA) for the opportunity to comment on the October 9, 2008 Notice of Inquiry Docket Number 0810021307-81308-01. We offer the following comments in response to the NOI.

General Comments

Intel supports the goal of enhancing the security and stability of the Internet's domain name addressing system. Furthermore, we believe that implementing DNSSEC at the root zone, as proposed in the NOI, is an essential step toward that goal. We believe this for the following reasons:

1. DNSSEC is a well architected and well understood protocol that can be implemented without delay.
2. New attack vectors have demonstrated that "patching" the DNS infrastructure is not sufficient to protect against a class of attacks that spoof DNS data.
3. By using public key cryptography, DNSSEC offers complete protection from the spoofing of DNS data.
4. Implementing DNSSEC at the root zone is a necessary precursor to further implementation throughout the DNS hierarchy.
5. Successful examples of DNSSEC deployment can be witnessed in the .se, .br, and .pr country code top level domains (CCTLDs).

Response to specific questions posed in the NOI

Questions on DNSSEC Deployment Generally

1. *In terms of addressing cache poisoning and similar attacks on the DNS, are there alternatives to DNSSEC that should be considered prior to or in conjunction with consideration of signing the root?*

   In the more than a decade since DNSSEC was standardized, many alternatives have been explored however the majority of experts have demonstrated that DNSSEC is the best available option for comprehensively solving the problem of data integrity.

2. *What are the advantages and/or disadvantages of DNSSEC relative to other possible security measures that may be available?*

   DNSSEC is a well architected and well understood protocol that can be implemented without delay. While we recognize that it does not solve all security related problems associated with the DNS infrastructure, Intel believes it provides the best available solution to solve the problem of

Intel Corporation
2200 Mission College Bl
Santa Clara, CA 95052

the data integrity in the DNS and we should not delay the implementation of DNSSEC at the root zone for these reasons.

We note that some deployment issues such as DNSSEC's complexity, increase in size for response packets, potential performance tradeoffs and response time increases due to signature validation or complications created by the use of the hierarchical trust model may exist and should be addressed in a timely fashion by stakeholders and implementers.

3. *What factors impede widespread deployment of DNSSEC?*

   Widespread deployment of DNSSEC is currently impeded by the fact that DNSSEC is not currently implemented at the root zone level. Other implementers of DNSSEC cannot realize the security benefits of DNSSEC signing their zones absent a signed root zone.

4. *What additional steps are required to facilitate broader DNSSEC deployment and use?*

   The domain name service industry has to fully implement DNSSEC and the Internet community must work together to standardize the response to invalid DNS responses.

5. *What end user education may be required to ensure that end users possess the ability to utilize and benefit from DNSSEC?*

   No direct end user education is needed; DNSSEC should be a transparent process to the end user.

   As noted above, Intel recognizes the need for the Internet community to standardize the information that the end user is presented with in the event of invalid DNS responses.

General Questions Concerning Signing of the Root Zone

1. *Should DNSSEC be implemented at the root zone level? Why or why not?*

   Intel supports implementation DNSSEC at the root zone level because it provides well understood and well tested solution to the very immediate problem of the integrity of DNS data.

2. *What is a viable time frame for implementation at the root zone level?*

   Intel supports immediate implementation of DNSSEC at the root zone and we believe that ICANN is best positioned to achieve this.

3. *What are the risks and/or benefits of implementing DNSSEC at the root zone level?*

   The obvious risk to DNSSEC, or any other public key cryptography solution, is a potential compromise of the keys that are used to sign the root. However, we feel strongly that the benefit of protecting the integrity of the DNS from a class of attacks that that fundamentally undermine the integrity of DNS data outweighs the risk of compromised keys. Furthermore, we believe that an effective method can be implemented to protect the keys and thus significantly reducing the main risk associated with DNSSEC.

4. *Is additional testing necessary to assure that deployment of DNSSEC at the root will not adversely impact the security and stability of the DNS? If so, what type of operational testing should be required, and under what conditions and parameters should such testing occur? What entities (e.g., root server operators, registrars, registries, TLD operators, ISPs, end users) should be involved in such testing?*

Intel Corporation
2200 Mission College Bl
Santa Clara, CA 95052

Intel does not believe that any additional testing is necessary as DNSSEC has been an IETF standard for more than a decade. Numerous testbeds have been in operation for sometime as referenced on the IETF's website[1]:

- The Secure Naming Infrastructure Pilot (SNIP) - A joint project involving NIST, SPARTA Inc, and the Dept. of Homeland Security
- DNSSEC test deployment at IANA
- Public Interest Registry (PIR) Testbed - Testbed for the .org domain
- Nominet UK DNSSEC Testbed - DNSSEC Testbed for the .uk domain (co.uk, org.uk, net.uk, ltd.uk, plc.uk, me.uk and sch.uk)
- DNSSEC testbed in Russia (.ru) - Includes signed view, as well as secure delegations
- DNSSEC Deployment in Puerto Rico (.pr) -Real DNSSEC Deployment for the .pr ccTLD
- DNSSEC testbed in Mexico (.mx) - DNSSEC testbed for the .mx ccTLD
- CZ.NIC Testbed - Testbed for the .cz ccTLD
- NLnet Labs SECREG Testbed
  DNSSEC testbed in the Netherlands (.nl) (no longer active) - NIC-SE / IIS DNSSEC Deployment in Sweden (.se)
- Register.BG DNSSEC Deployment - DNSSEC in Bulgaria (.bg)
- Registro.BR DNSSEC Deployment - DNSSEC in Brasil (.br)
- DLV Registry (DNSSEC Look-aside Validation) at ISC - DLV is a technology initiative meant to enable DNSSEC deployment
- Comcast DNSSEC Trial - DNSSEC-capable resolver at Comcast to test against.
- Root Server Testbed Network - Coordinated, persistent facility to evaluate major changes to the DNS
- Verisign Opt-In DNSSEC Pilot - DNSSEC Opt-In testbed (deprecated)
- University of Murcia DNSSEC testbed (SEINIT) - Partners: Alcatel, BT, Deutsche Telekom, et al
- MYNIC DNSSEC Deployment (.my ccTLD) - DNSSEC Deployment in Malaysia

5. *How would implementation of DNSSEC at the root zone impact DNSSEC deployment throughout the DNS hierarchy?*

   Implementing DNSSEC at the root zone is a necessary precursor to further implementation throughout the DNS hierarchy.

6. *How would the different entities (e.g., root operators, registrars, registries, registrants, ISPs, software vendors, end users) be affected by deployment of DNSSEC at the root level? Are these different entities prepared for DNSSEC at the root zone level and /or are each considering deployment in their respective zones?*

   While we cannot predict how DNSSEC might affect every possible stakeholder, we are unaware of any adverse affect to zone operators who choose not to implement DNSSEC at this time. We also note that some entities around the world are ready or have already deployed DNSSEC.

Operational Questions Concerning Signing of the Root Zone

1. *The Department recognizes that the six process flow models discussed in the appendix may not represent all of the possibilities available. The Department invites comment on these process flow models as well as whether other process flow model(s) may exist that would implement deployment of DNSSEC at the root zone more efficiently or effectively.*

   After reviewing all process flow models proposed in the NOI, Intel supports process flow model 4 as we believe it provides the most logical solution to the question of implementation. However, we do not see the need for a separate root zone distributor as shown in the diagram because

[1] http://www.dnssec.net/projects

Intel Corporation
2200 Mission College Bl
Santa Clara, CA 95052

there is no functional or technical need to have the signed root zone file distributed by an additional entity. We believe having a model that includes an additional entity presents another point of failure which is unnecessary for the process to be completed.

Intel believes that process flows 1,2,3 and 5 as presented in the NOI unnecessarily complicate the process of signing the root and introduce additional points of weakness where the system can be attacked. We believe that minimizing the points of failure in the model is the best way to ensure the security and stability of the DNS. Furthermore we believe that ICANN, in implementing the IANA functions, has demonstrated the expertise to execute this process. They are the only entity in the process that can validate the information as they receive the information from the TLD operator. Process flow models 1,2,3 and 5 reduce the IANA function to merely relaying information from one entity to another and places all the technical functions in the hands of a root zone maintainer and/or key operator who does not have the relationships or knowledge necessary to determine whether the information is correct. These models are unnecessarily complex and allow for too many points of failure from the issuance of a change request to distribution of the zone file.

With regard to process flow model 6, Intel finds that it also presents an unnecessarily complex solution. Furthermore, like process flows 1,2,3 and 5, process flow 6 separates the function of signing the root from the entity who receives the zone information.

The application of the zone signing key (ZSK) and the generation of the key signing key (KSK) should not be an overly complicated process. The issue of primary importance is the invalidation of the KSK and all six proposals fail to address the important issue of KSK invalidation. It is critical that this issue be addressed as it fundamentally affects the architecture of the system. Intel strongly supports a model in which multiple entities come together to invalidate the ZSK.

2. *Of the six process flow models or others not presented, which provides the greatest benefits with the fewest risks for signing the root and why?*

   Process flow 4 for the above stated reasons.

3. *Specifically, how should key management (public and private key sets) be distributed and why? What other factors related to key management (e.g., key roll over, security, key signing) need to be considered and how best should they be approached?*

   Intel supports a model in which the function of generating both the ZSK and KSK sits in IANA operator who has the knowledge that the data is correct as they receive the information. The rollover of the ZSK should be a frequent occurrence and therefore that responsibility should also rest in the IANA function.

   KSKs must be generated at the time of initial implementation. While the NOI doesn't cover this area specifically, Intel believes it will be prudent to generate a fixed and relatively small number of KSKs initially. The process of invalidating and rolling over between the limited number of KSKs should be made by a consensus group (of more than one member) in a public way. We believe this group should be comprised of multiple entities with expertise in DNSSEC, cryptography and security.

4. *We invite comment with respect to what technical capabilities and facilities or other attributes are necessary to be a Root Key Operator.*

   Intel believe that the most important qualification is that the root key operator must be the direct and authoritative holder of the knowledge regarding the correctness of the data. Furthermore, the entity must demonstrate the ability to follow the IETF standard RFC 4641, September 2006 – "DNSSEC Operational Practices". Intel supports ICANN in fulfilling this function as they possess both the data and because they have demonstrated through their ability to implement DNSSEC.

Intel Corporation
2200 Mission College Bl
Santa Clara, CA 95052

5. *What specific security considerations for key handling need to be taken into account? What are the best practices, if any, for secure key handling?*

   Suggested reference the IETF standard RFC 4641, September 2006 – "DNSSEC Operational Practices".

6. *Should a multi-signature technique, as represented in the M of N approach discussed in the appendix, be utilized in implementation of DNSSEC at the root zone level? Why or why not? If so, would additional testing of the technique be required in advance of implementation?*

   Intel believes that process flow 6 presents an overly complex model for maintaining the ZSK. However, Intel fully supports a similar technique for the process of invalidating the KSK in the event of compromise. We believe that multiple entities should be required to come together in order to invalidate the KSK.

Intel Corporation
2200 Mission College Bl
Santa Clara, CA 95052