

From: "Jeffrey A. Williams" <jwkckid1@ix.netcom.com>
To: Glen de Saint Géry <Glen@icann.org>, doc/ntia DNSSEC
<DNSSEC@ntia.doc.gov>
Date: Fri, Oct 10, 2008 5:45 AM
Subject: Re: [ga] Proposal To Sign the Root Zone Made Public

Glen and all,

Again thank you for this proposal announcement.

This is a good move by ICANN, but ensuring the security of the internet for stakeholders/users will only be partly protected. What's far more important is to require that all Registrars, and Registries as well as Domain Name holders have DNSSEC fully implemented.

We are still reviewing this proposal and will have further comments in it's regard fairly soon. We have some doubts as to Paul Twomey's attestation to any ICANN selected "Group of DNSSEC experts" review.

Glen de Saint Géry wrote:

> [To: council[at]gnso.icann.org; liaison6c[at]gnso.icann.org]
> [To: ga[at]gnso.icann.org; announce[at]gnso.icann.org]
> [To: regional-liaisons[at]icann.org]
>
> Proposal To Sign the Root Zone Made Public
> <http://www.icann.org/en/announcements/announcement-2-09oct08-en.htm>
>
> 9 October 2008
>
> A proposal [PDF, 276K]
<http://www.icann.org/en/announcements/dnssec-proposal-09oct08-en.pdf>
> to sign the root zone file with Domain Name System Security Extensions, or DNSSEC, technology was released by ICANN today.
>
> DNSSEC provides a way for software to validate that Domain Name System (DNS) data have not been modified during Internet transit. This is done by incorporating public-private signature key pairs into the DNS hierarchy to form a chain of trust originating at the root zone. Importantly, DNSSEC is not a form of encryption. It is backward compatible with existing DNS, leaving records as they are - unencrypted. DNSSEC ensures record integrity through the use of digital signatures that attest to their authenticity.
>
> This proposal has been written by ICANN staff, as authorized by ICANN's Board, with the goal to proceed with appropriate speed and deploy DNSSEC at the root level as a step towards improving the overall security of the DNS.
>
> "The proposal has already been reviewed by a group of global DNSSEC experts. The feedback ICANN received from this group indicates that the proposal is technically sound, and appropriate" ICANN's President and CEO Paul Twomey said.
>

> At the core of DNSSEC is the concept of a 'chain of trust'. ICANN's proposal builds on that notion and, based on security advice, recommends that the entity responsible for making changes, additions and deletions to the root zone file and confirming those changes are valid (ICANN presently performs this function - called the IANA function - under contract from the United States Department of Commerce), should generate and digitally sign the resulting root zone file update. This signed file should then be passed to another organization (presently VeriSign Corporation) for distribution. In other words, the organization responsible for the initial basis of trust - validating root zone changes with top level domain operators - should also authenticate the validity of the final product before it is distributed.

>

> The release occurs as the United States Department of Commerce also announced a Notice of Inquiry on the concept of signing the Root Zone. Details can be found here: <http://edocket.access.gpo.gov/2008/pdf/E8-23974.pdf> [PDF, 72K].

>

> "ICANN has more than a year of experience in producing a signed root zone that has already been widely tested by DNS software vendors and the interested DNSSEC community. ICANN also has "built-in" the participation of a group of world-class DNS experts" Dr Twomey said.

>

> "This is a moment of challenge and opportunity in addressing the overall stability and security of the DNS system - the mission around which ICANN was formed" he added.

>

> A set of questions and answers

> <http://www.icann.org/en/announcements/dnssec-qaa-09oct08-en.htm>

> on what DNSSEC is and why it is important is also published to assist with the reading of the proposal.

>

> Glen de Saint Géry

> GNSO Secretariat

> gnso.secretariat@gnso.icann.org

> <http://gnso.icann.org>

Regards,

Spokesman for INEGroup LLA. - (Over 281k members/stakeholders strong!)

"Obedience of the law is the greatest freedom" -

Abraham Lincoln

"Credit should go with the performance of duty and not with what is very often the accident of glory" - Theodore Roosevelt

"If the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: i.e., whether B is less than PL."

United States v. Carroll Towing (159 F.2d 169 [2d Cir. 1947])

=====

Updated 1/26/04

CSO/DIR. Internet Network Eng. SR. Eng. Network data security IDNS.
div. of Information Network Eng. INEG. INC.

ABA member in good standing member ID 01257402 E-Mail

jwkckid1@ix.netcom.com
My Phone: 214-244-4827

CC: Ga <ga@gnso.icann.org>, GAC Rep <ssene@ntia.doc.gov>,
"twomey@icann.org" <twomey@icann.org>