Subject: **Re: Addendum to VeriSign RSEP submission - Modification of algorithm to sign .net / .com**
Date: Tuesday, April 13, 2010 10:35 AM
From: Pat Kane <pkane@verisign.com>
To: Patrick Jones <patrick.jones@icann.org>

Dear Patrick:

VeriSign wishes to notify you of a change to the October 22, 2009 RSEP (Registry Services Evaluation Process) submission. In the interest of securing the zones, VeriSign intends to sign the .net and .com zones with RSASHA256. This is a technical modification from our RSEP submission which indicated that the zones would be signed with RSASHA1-NSEC3-SHA1.

Given the recent publication of RSASHA256 standards (in late October, 2009, in RFC 5702, shortly after VeriSign's DNSSEC RSEP submission), this modification will:

- increase security - RSASHA256 is a stronger algorithm combination than RSASHA1-NSEC3-SHA1. Security experts are recommending moving away from SHA1 to SHA256;
- eliminate the need to rollover from RSASHA1-NSEC3-SHA1 and the corresponding requirement of signing with two cryptographic algorithms simultaneously during the transition period; and
- align the .net/.com DNSSEC implementation with the root zone implementation currently being signed with RSASHA256.

Sincerely,

Pat

Patrick S. Kane
Vice President
VeriSign Naming Services
pkane@verisign.com
(o) +1.703.948.3349