Viktor Dukhovni

March 15, 2018

Dear ICANN,

Thank you for the opportunity to present at the DNSSEC/DANE workshop at the ICANN61 conference. It is my hope that the presentation will prove useful to would-be adopters of DNSSEC/DANE—the attendees in the room, remote attendees, and those who come across it after the fact—when planning the implementation of these technologies for their email systems.

In the spirit of promoting increased adoption of DNS and email security, I'd like to note the the icann.org domain is in part leading by example as it has already adopted DNSSEC and its MX records are signed with the icann.org DNS signing keys. That said, there are not yet DANE TLSA records for the icann.org MX hosts, leaving icann.org email subject to man-in-the-middle downgrade attacks.

The main obstacle to DANE adoption is implementation of DNSSEC. Having done that, the DANE implementation is comparatively simple (see the slides from the presentation). ICANN's promotion of DANE would carry more weight if icann.org were a domain where DANE is already deployed.

Please implement DANE/TLSA records for the icann.org MX hosts. I am more than happy to answer any questions that the ICANN email operations team may have about key-rotation best-practices, monitoring tools, etc.

Sincerely yours,

Viktor Dukhovni