IANA SESSION

DNSSEC

Signing the Root

Background

(IANA WG)

- DNSSEC is a protocol designed to improve DNS security ;

- DNSSEC implementation in the public DNS tree is a question that has been discussed for years across the community ;

- In July 2007, the IANA Working Group was “asked for help in providing input to the [ccNSO] Council on Root Zone signing from a technical perspective”: http://ccnso.icann.org/about/minutes/ccnso-minutes-31jul07.pdf

- The IANA WG set up an inclusive ccTLD group to write a paper on DNSSEC with the goal to increase awareness about this technology and respond to the Council request;

- See last IANA WG DNSSEC presentation : https://delhi.icann.org/files/guillard-ccnsoianawg-dnssec_11Feb08.pdf

Some feedback from CCs

- A survey on DNSSEC was conducted last year. It shows that although very few CCs have deployed this technology, many believe that DNSSEC will be deployed in the future :
http://losangeles2007.icann.org/files/losangeles/presentationccnsodnssecsurveyresultsschittek30oct07.pdf

- Those TLDs that have signed their zone are looking forward to the root zone being signed to facilitate their DNSKEY dissemination (RIPE has sent a formal request to IANA for their KEY to be published) ;

- Some TLDs have expressed concerns about DNSSEC ;

complex and heavy to deploy for unclear benefit, sends a wrong signal to the market that the DNS would be perfectly secured with DNSSEC, side effects (zone walking now fixed with NSEC3), lack of available tools, at the time of design the DNS context was not the same as today (DNS limitations and holes that were present 10 years ago have now been fixed);

Yet other CC feedback

- Following a discussion in CENTR, CCs were consulted by e-mail : "*would you have any problem for the root zone to be signed, from a technical point of view ?"*

17 responses up to now (so very few at this stage):

14 responded that they didn't see any problem for the root to be signed

2 expressed concerned:
one asking for additional information about the DNSSEC technology as such
another one for documentation about the procedures that would be implemented for the root to be signed.

1 response was received indicating that the question was not understood so that no answer could be provided.

RRSAC

- Question to the RSSAC :

  “ would there be an issue for root servers operators if a signed root zone was to be published? ” :

- Response from Matt Larson :

  - Root server operators have informally indicated that they would be ready at this time to serve a signed root zone if they were asked for ;

  - The question will be explicitly raised in the agenda at the Dublin meeting ;

  - The RSSAC will respond more formally to our question after Dublin ;

Other indications

- SSAC prudently "*recognize that any technology deployment on a global scale is apt to reveal issues not considered in protocol design and development and in controlled (test) environments*": http://www.icann.org/committees/security/sac026.pdf ;

- SSAC has also launched last April a "Survey of DNSSEC Capable DNS Implementations": http://www.icann.org/committees/security/sac030.htm ;

- RFC 5155 is now published (March 2008): practically, standardization process for DNSSECbis (that includes NSEC3) is now fulfilled;

IANA Test Bed

- IANA DNSSEC test bed : https://ns.iana.org/dnssec/status.html

  - Report about the test bed ?

  - Additional information about how would a signed root zone file be operated if DNSSEC@root was implemented ?

  - How would TLD KEYS be collected ?

IANA TAR

(Trust Anchor Repository)

- Last April, ICANN has “authorized the creation of DS Key registry for Top Level Domain DNSSEC keys” (Trust Anchor Repository) : http://www.icann.org/minutes/minutes-30apr08.htm

⇒ TAR looks like a good initiative since it would help those TLDs and DNS cache operators that want to deploy/use DNSSEC, without exposing the others to any risk ;

⇒ Stays some open questions :

- Which format would be used to publish KEYS and which protocol would be used to update and gather them ?
- What would the cost be for IANA to set up such a repository ?
- Will this TAR effectively be used (avoid waste of IANA resources) ?