

# Proposal for activities

## *Introduction*

During TNC 2009, a BoF session was held regarding DNSSEC. This meeting was organised by Milan Sova under the flag of TF Mobility. Goal of the meeting was to discuss what activities are taking place with respect to DNSSEC at the various NRENS.

In this discussion it became clear that there certainly is an interest in DNSSEC but that the level of knowledge and know-how varies between NRENS and that the focus of the attendees on DNSSEC came from many different viewpoints, for example:

- Some NRENS operate their country's top-level domain and are deploying DNSSEC;
- Some NRENS operate the ccTLD but are not (yet) deploying DNSSEC;
- There are people who are interested in leveraging DNSSEC to store certain metadata (for instance server certificates for use in Eduroam);
- Other people are interested in pushing the deployment of DNSSEC for their country's top-level domain;
- etc.

There is a worldwide interest in DNSSEC deployment at the moment, mainly because of the current security issues with DNS (think: Kaminsky):

- Some ccTLDs already sign their zones (.cz, .se in Europe for instance) or have plans
- Some generic TLDs are signed (.org, .museum, .gov) or have announced plans (.com, .net)
- ICANN has announced that the root zone will be signed this year (<http://www.icann.org/en/announcements/announcement-2-03jun09-en.htm>)

During the meeting at TNC 2009 it was decided that it should be investigated whether or not there is an interest in setting up a DNSSEC activity (working group) under TF-Mobility. In this short memo, several possible actions that such a group could undertake have been outlined.

## *Action proposals*

### **Action 1a – General DNSSEC knowledge dissemination**

At the meeting it became clear that the level of knowledge and know-how varies between NRENS. Apart from that, it is important to also inform non-DNS operators and decision makers in the NREN community about the current security issues in DNS and about the implications of deploying DNSSEC.

For this reason, the first action that a DNSSEC activity under TF-M could perform is setting up a comprehensive DNSSEC education track. A possible outline for such a track could consist of the following course modules:

- Current DNS security and vulnerabilities
- DNS security current best practices
- Basic DNSSEC (explains the basic principles behind DNSSEC)
- Advanced DNSSEC (detailed technical explanation)
- DNSSEC operation best practices

## **Action 1b – DNSSEC hands-on training**

In Action 1a a general course track was proposed; following from this and from the experience of DNS operators who already deploy DNSSEC it would be useful to set up hands-on training for DNSSEC operators, focusing on:

- How to run and administrate a DNSSEC signed zone
- Sharing experiences between TLD operators (which some of you are)
- How to enable and manage DNSSEC validation on your resolvers

## **Action 2 – DNSSEC evangelisation**

Many TLD operators are currently not deploying DNSSEC. Some of these TLD operators are NRENs themselves and some NRENs depend on TLD operators that do not deploy DNSSEC.

As DNSSEC WG, we should discuss the necessity of deploying DNSSEC. Most NRENs play a leading role in their respective country's Internet community and as such can set an example by both deploying DNSSEC as well as advocating the adoption of DNSSEC by their country's TLD thus furthering the worldwide deployment of DNSSEC.

This action could include:

- Organising information meetings for the Internet community
- Actively engaging in a debate with (cc)TLD registries about the deployment of DNSSEC
- Speaking with one voice on behalf of the European NREN community towards both (cc)TLD registries as well as to EU organisations such as ENISA

## **Action 3 – DNSSEC tool development**

One of the main issues hampering DNSSEC deployment is the poor availability of good tools for operating DNSSEC signed zones. Some open source initiatives have been started but it takes time before these become mature.

A DNSSEC WG could play a role in the development of good tools by:

- Contributing to open source initiatives such as OpenDNSSEC
- Testing tooling and offering test beds
- Documenting tooling where such documentation is unavailable (for instance: HOWTOs)
- Testing (new) commercial offerings such as DNSSEC appliances and sharing the test results among the WG

## **Action 4 – DNSSEC research**

During the meeting some of the participants expressed an interest in using DNSSEC as a platform for metadata distribution (such as certificates used for Eduroam servers). There are more areas in which DNSSEC can be leveraged as a platform (such as ENUM and distribution of other metadata, for instance in federations or confederations).

A fourth – more general – action could be the pursuit of research in these areas. Currently ongoing research in this area can be shared and new research initiatives can be discussed and set up jointly.

## ***Feedback***

Any feedback on this proposal is welcome; please discuss any remarks or ideas on the DNSSEC BoF mailinglist ([bof-dnssec@terena.org](mailto:bof-dnssec@terena.org)). If you are not on the list but would like to join it you can send an e-mail to [listmanager@terena.org](mailto:listmanager@terena.org) with 'subscribe bof-dnssec "Your name <youremail@domain.com>"' in the body of the message.

You are also requested to pass this proposal on to anyone within your organisation who may have an interest in DNSSEC. If you feel you would like to join and/or organise one of the actions listed in this proposal please communicate this on the list.