The Office of International Affairs
National Telecommunications and Information Administration
U.S. Department of Commerce
Ms. Fiona Alexander

Comments on Docket Number 0810021307-81308-1, Enhancing the Security and Stability of the Internet's Domain Name and Addressing System

The Swedish Post and Telecom Agency (PTS), as the authority which oversees the telecom sector and the Internet Infrastructure Foundation (.SE), as the administrator of the Swedish country code top level domain, appreciate the NTIA's consultation on proposals to sign the root and have concluded on the following joint response.

Background

PTS and .SE recognise the earlier efforts made by ICANN to improve the IANA functions. It is of great importance that the IANA functions within ICANN are operated in an open and transparent manner. We believe that it is essential to have an open publication of policies and processes, and we support the development of a secure, efficient and automated operation of the IANA functions.

Need of a signed root zone for the progress of DNSSEC

.SE, ass one of the very early adopters of DNSSEC on the TLD level and PTS as the first state authority to sign its zone on the subdomain level, have together with several other important stakeholders from the local Internet Community in Sweden, expressed our concern about the slow progress of the DNSSEC deployment efforts in a letter to ICANN in October 2007[1].

We believe that the successful deployment of DNSSEC is crucial for the continued stability and security of the Internet. As this is contingent upon a signed DNS root zone, in the letter we urged ICANN to speed up and improve its efforts to quite rapidly migrate to a signed root zone.

.SE, altogether with several other top-level domain registries, have already started to sign our domains, and more have announced their ambition to do so. The deployment by individual TLD's means a proliferation of individual trust anchors that ends up as isolated islands of trust, which in the end will make the transition to a signed root zone more dangerous and more complex by each TLD trust anchor added.

[1] http://www.iis.se/docs/brev_iana_pdf.pdf

Moreover, the absence of a signed root zone directly contributes to the development of inferior alternatives, thereby confusing the Internet community and jeopardising the long term success of the DNSSEC deployment. It will no doubt be difficult to convince Internet users and Internet service providers to do the investments needed without a clear commitment to sign the root.

PTS and .SE are therefore concerned that the issues in the Notice of Inquiry implies that the NTIA may take a long time to decide who should be the Root Zone Signer, prioritising the balancing of competing interests of various stakeholders before prioritising the actual and urgent need to get the root zone signed as soon as possible.

We are fully aware that the discussions relating to signing the root have been taking place over the last 3-4 years. We believe that the Internet now has reached a point where the absence of a signed root zone is no longer only merely unfortunate. Our belief is also emphasised by the recently detected methods to attack the DNS infrastructure through cache poisoning, against which DNSSEC offers the only long term and standardised protection. An unsigned root zone is one of the main reasons why the deployment of DNSSEC is held back.

Definitions

To clarify the responsibilities and roles we are using the following definitions:

Root Zone Manager: The entity responsible for the contents of the root zone. At the time of writing, this entity is the IANA function within ICANN.

Root Zone Auditor: The entity responsible for auditing the changes to the root zone. At the time of writing, this entity is the NTIA of the U.S. DoC.

Root Zone Maintainer: The entity responsible for editing and compile the root zone. At the time of writing, this entity is Verisign.

Root Zone Signer: The entity responsible for signing zone. There is currently no root zone signer.

Who should sign the root?

Even though signing the root isn't enough, our opinion is that having the root zone signed in a nearby future by an entity already trusted by the Internet community is much more important than spending a long time evaluating the various parties who might want the assignment. We believe that the party who are currently trusted to administer and run the root zone, the IANA function within ICANN, are fully aware of the severity connected to the task to sign the root zone. They have also been running a DNSSEC test bed for a while now.

Furthermore, we find it very unlikely to be able to find a new and unknown party to trust within a short period of time, with the assignment to sign the root, and that are trusted by the Internet community. We think that the IANA function within ICANN as the Root Zone Manager has proved its abilities and deserves our trust in this matter.

Even though it might be tempting to change the whole process of creating and administering the root zone, signing the root zone doesn't change this process a lot. It adds one more step to it. It is more important that the root zone is signed in a stable and secure environment, before the stability of the DNS is weakened by getting too many different TLD trust anchors in the configuration files of the recursive name servers all over the world.

Key ownership vs. key management

PTS and .SE strongly recommend the NTIA to differentiate between ownership and management for each type of key (KSK/ZSK) when making up the model of the root zone signing and key management. Who will have the ability to manage the key must be determined by the owner of that key. Such conceptualization of functions allows the assignment of specific entities to each role.

TRUST ANCHOR CONTROL / KEY SIGNING KEY

It is of our opinion that the ownership of the key signing key, KSK, should be held by the entity responsible for the root zone, i.e. the root zone manager. At the time of writing, this entity is the IANA function within ICANN.

ZONE SIGNING KEY

It is of our opinion that the ownership of the zone signing key, ZSK, should be held by the Root Zone Maintainer, which also should perform the signing of the root zone. At the time of writing this is Verisign.

The main reason for this is that the day to day signing of the root zone requires ownership of the ZSK, as the root zone signer (RZS) must be able to access the private part of the ZSK key pair. Control of the ZSK is not contentious, and must be considered independent of the control of the KSK.

Key Signing Key

From our point of view the root zone's KSK public key management and distribution process should be designed to minimize the impact on name servers throughout the Internet in the event that changes are made to the operators involved.

We consider it very important that it is possible to change holder of KSK without being forced to make a KSK key rollover.

If the Internet community in common find it to be problematic with IANA as the single entity to manage the KSK, it is possible to put together a group of third parties trusted by the community managing "m out of n" presence to get key access, even though PTS and .SE don't hink that is necessary. Howsoever, the IANA function within ICANN is already and will still be in control of the content of the root zone anyway.

Summary

To conclude, our recommendation is for NTIA to strongly consider allowing the IANA function within ICANN to sign the root zone including key management, editing, compiling and signing, with no further delay.

PTS' and .SE's opinion is that IANA should be in control of the KSK and that IANA should have mandate to decide with whom they will interact if they come to the conclusion that they will contract another party to handle the zone editing and signing, including ZSK management.

Even though Verisign's proposal delegates KSK access to the roots operators, it still creates a "lock in" in the sense that Verisign will not be easily replaced. PTS and .SE are not willing to accept Verisign's proposal of them being in charge of the zone signing.

Finally, PTS and .SE find it important for NTIA to set a firm target date for the deployment of a signed root zone and to make that date known to the public. In our opinion that process involves firstly publishing of a road map for reaching that goal with all the details on different policy issues like for instance frequency of key rollover, routines for emergency key rollover, responsibilities and technical environment. Secondly, it involves the parties concerned to immediately enter into necessary negotiations and thirdly that the IANA function within ICANN get instructions to take the necessary steps to implement that road map.

Anders Johanson
Director, Network Security Department
PTS

Danny Aerts
CEO
.SE