CZ.NIC - Comment on NTIA
docket number
0810021307–81308–01

To:
Fiona Alexander,
Associate Administrator,
Office of International Affairs,
National Telecommunications and Information Administration,
U.S. Department of Commerce

To whom it may concern:

Introduction

CZ.NIC is an interest association of legal entities within the Czech Republic, whose main activity is the operation of .CZ, ccTLD and 0.2.4.e164.arpa (ENUM) domains. Currently we register about 500.000 .cz and 5000 ENUM domains. The number of domains has rapidly increased in the past few years. Current annual growth is 36% for .cz. CZ.NIC is considered to be a part of the critical state infrastructure of the Czech Republic. At the end of September 2008 we fully deployed DNSSEC end user registration for both domains and we also signed both zones. DNSSEC is seen as an important security feature among the internet users and we observed the steady increase in the number of DNSSEC enabled domains (a few hundred after about two months of DNSSEC full production operation) and number of DNSSEC aware ISPs and end users. The situation when a root zone is not signed causes significant problems and issues not only to us as the ccTLD operator, but also for all Internet users in the Czech Republic who would like to secure their services or who would like to be secure when using them. Hence we are strongly interested in the initiative to get root zones signed. We would like to express our position on DNSSEC deployment into the root zone and answer NTIA's Notice of Inquiry.

Background

Recently discovered and disclosed methods of attacks on DNS (such as Dan Kaminski, August 2008) and after further research and testing showed again an alarming fact that such a core internet infrastructure as Domain Name System is vulnerable to security compromise (DNS replies spoofing), which may lead to various possibilities of abuse. We think that secure and stable operation of the Domain Name System is extremely important. We believe that DNSSEC is the only solution for completely eliminating the risk of DNS abuse from such attacks. All other alternatives can only lower the risk instead of its complete elimination.

DNSSEC requires establishment of so called chains of trust within the DNS domain tree. Each level of this tree must digitally sign its own DNS record and publish their public key checksum into the parent level of the tree where the signatures will be validated when the particular domain name is used anywhere on the Internet. Only a successful validation at every level of the tree provides the safety – the information from DNS was not spoofed and is trustworthy. Without all DNS levels signed including the root zone, there is no single secure entry point and all DNSSEC users face the problem of a not fully closed chain of trust and must workaround its non-existence by administering lower level domain keys manually or by creating various key repositories.

Some alternative solutions instead of root zone signature have emerged so far, for instance separate registries for DS records such as DLV or TAR. They suggest storing keys in separate systems outside of the root zone to avoid the requirement of root zone signature. In our opinion any of these solutions are just workarounds of the issue. They do not solve the fundamental question of technical and organizational competence as they require the similar technical knowledge and experience as root zone signature, because the consequences of mismanagement would be the same – the particular sub-part of the domain name tree (with all domain names within that part) would disappear from the Internet for DNSSEC enabled users. They just put in additional complexity in DNSSEC system where signing the root zone would be simple and clean solution which is also defined and expected by DNSSEC standard itself.

Situation in the Czech Republic

As mentioned before CZ.NIC has already deployed DNSSEC for .cz and .0.2.4.e164.arpa zones. Instead of doing a simple step to publish DS records for .cz into a root zone, we had among the other actions to introduce other ways how to securely publish keys, setup the keys in DLV and teach the users the complex process how setup their servers to be able to import key and manage it later. We were able to publish ENUM DS records to .e164.arpa zone maintained by RIPE NCC, but as the chain of trust again does not end in the root zone, we had to teach users the necessary steps how to workaround it for .arpa again (by using DLV or manually), but a slightly different way as the source of the key was different in this case. Users must later on spend the extra effort on key management instead of rely on standard representation by the signed root zone. The key management may be different for each TLD, which makes it virtually impossible to use DNSSEC for all existing TLDs. All of those extra steps, extra effort, extra costs and overhead would be made unnecessary with root zone signed.

We truly believe that root zone signature is the only viable option in the long term. It creates a standard, transparent, less error prone and of course the same DNSSEC environment for all domains and Internet users. None of the root zone signature proposals attached to NTIA's Notice of Inquiry, does not add any other authority to the process flow. Also, Root zone signature or DNSSEC itself do not add any new levels of control over the root zone, because it's only about form, integrity and authenticity of the data in the root zone. Thus root zone signature process becomes purely technical issue. The technology has been known for years and the process of signing and administering zones is proven by more different entities (for example by the TLD operators who already signed their zones or by Internet Assigned Numbers Authority which runs root zone signature testing within DNSSEC root zone testbed etc.). We believe, there are no technical doubts, objections or further technical testing necessary regarding root zone signature. Moreover signed root zone does not bring any actions to be taken or extra costs to those TLD operators, domain holders or end users who do not want to use DNSSEC at the moment. For them everything will stay the same as it is now. Therefore we think the root zone signature process should be defined as soon as possible and we call for fast implementation of this process later. Not only because we consider signed root zone to be crucial step towards widespread deployment of DNSSEC, but it will certainly remove a huge part of complexity of current DNSSEC usage for all DNSSEC enabled users as well and there is no benefit for anybody from root zone being unsigned.

Recommendation

CZ.NIC particularly supports the proposal of Internet Corporation for Assigned Names and Numbers (ICANN) because of the following reasons: ICANN works with the international DNS community which ensures the involvement of all interested stakeholders in the area, making the process of root zone signature clear, transparent and done in a way, which can be generally accepted by TLD operators. Internet Assigned Numbers Authority (IANA), body operated by ICANN who are responsible for root zone management, demonstrated its competence to deploy and manage DNSSEC in the root zone by successful operation of DNSSEC root zone testbed since 2007. Keeping the root zone management within a single organization including DNSSEC signing makes the process less prone to organizational type of problems (such as communication between involved parties, different interests etc.) which may occur if more organizations are involved (remind this does not mean root zone key administration to be done by a single organization, involvement of more entities is desirable here).

On behalf of CZ.NIC association
Ondrej Filip, CEO

Ondřej Filip

About CZ.NIC
CZ.NIC, z. s. p. o., was founded in 1998 by leading providers of Internet services. The association currently has 57 members. The key activities of the association include operation of the domain name registry for the .CZ domain and the 0.2.4.e164.arpa (ENUM) domain, operation of the CZ top-level domain and public education in the area of domain names. The association is now intensively working on development of the ENUM system, extension and improvements of the domain administration system, DNS, DNSSEC and support of new technologies and projects beneficial to the Internet infrastructure in the Czech Republic. CZ.NIC is an active member of many international organizations uniting similar organizations around the world (like CENTR, ccNSO and more).