domain.wire

THE DOMAIN NAME NEWSLETTER FROM CENTR
*www.centr.org*

# DNS Security & Stability

INSIDE

*DNSSEC, IPv6, Anycast*
*Internet Governance Forum*
*Investing in the Internet Community*

# Index

# Welcome!

Dear Reader,

This year we are facing a crisis in the banking and financial sector followed by a general slowdown of the economy in many countries.
A crisis which reminds us of similar problems the internet industry was facing in 2000 and 2001 when the "dot-com bubble" exploded and everyone learned the hard way that the "new economy" was subject to the same rules as the old one. This lesson is one of the reasons why the internet sector today seems relatively unaffected by the current problems.
The other reason is that the underlying infrastructure is managed on two sturdy principles: stability and security. Managers of country code Top Level Domain (ccTLD) registries have consistently chosen those principles as the sound basis on which they provided their customers, e-communities and governments with reliable services.

The Domain Name System (DNS) is a key element in the functioning of the internet and is in particular important for the eCommerce industry. As Top Level Domain registries we play an important role in the stability of the DNS and therefore must ensure the safety of our domains. With this goal in mind, CENTR members have over the years focused much of their attention and resources on improved security, business contingency and financial stability of their organisations. As a result, they have been able to provide uninterrupted services and a very high level of security.

The DNS is built and managed to withstand natural disasters and massive cyber attacks (such as the ones in Estonia in 2007 and Georgia in 2008). This high level of resilience can only be achieved by continued investment in technical infrastructure and redundancy across all our business units.
I would invite other stakeholders in the Internet Society such as Internet Service Providers and software developers to start an open dialogue on how we can achieve the same level of security across the whole internet industry.

I hope you enjoy this edition of Domain Wire.

*Dr. Andrzej Bartosiewicz, CENTR Chairman*

# DNSSEC TO SECURE DNS

*By Anne-Marie Eklund Löwinder, Quality & Security Manager, .SE (The Internet Infrastructure Foundation)*

*Have you ever reflected if the web site you are visiting really is the one you intended to visit? Web addresses may be counterfeited and still look genuine. However, there is a technique that is able to eliminate some serious threats towards the domain name system.*

DNS – the Domain Name System – that makes it possible to use domain names instead of IP addresses on the Internet, was invented in 1983 by Paul Mockapetris, although it was not until 1986 that it received IETF standard status. At that time, there was no World Wide Web and the Internet was hardly used at all outside the academic world. However, in the beginning of the 90s, when the web started to appear, it was discovered that DNS suffered from several vulnerabilities. At that time, work was begun to develop a more secure version of DNS.

DNSSEC stands for DNS Security Extensions and represents an enlargement of DNS in order to make it more secure. DNSSEC originated in the work that was started in the beginning of the 90s, but it was not until 1999 that the protocol standard was in such a condition that it was possible to implement and use in tests.

The DNS is still far from secure. There are a lot of known vulnerabilities and there is no doubt that all users of applications and services on the Internet are very strongly dependent on the domain name system to work properly. That is the main reason why Sweden has been a leading country and an early adopter of DNSSEC.

**New threats to DNS**

Lately, new threats to DNS have made DNSSEC more topical. One of the biggest threats is represented by the rather newly announced Kaminsky bug which creates a possibility to attack the DNS, for instance, with the aim to redirect web sites traffic to another bogus web site. In practice, that means that a bank's web site can be redirected to another server without the visitor even noticing. To the user it still looks like he is on the bank's site.

**What is DNSSEC good for?**

You may say that DNSSEC is the Internet's answer to DNS identity theft. It protects users from and makes systems detect DNS attacks. Almost everything in DNSSEC is digitally signed, which allows authentication of the origin of the DNS data and ensures the integrity of the DNS data. Digitally signed means that DNSSEC uses Public Key Cryptography, with a Secret Private Key and an Open Public Key used together. DNS Messages are scrambled using the Private Key – the Public Key is needed to unscramble it. You will now know who sent the message. If the data is modified, mangled, or otherwise compromised en-route, the signature is no longer valid and you will be able to discover it.

DNSSEC protects from different types of tampering with DNS queries and answers during the communication between servers within the DNS. The main function is lookups from domain names to IP-addresses with signed DNS answers. An extended use of DNSSEC could also act as an enabler of other security measures as, for instance, to use DNS as a container to distribute other security related keys or parameters.

## The world's first adoption

Hitherto it has been a long journey for DNSSEC, and a lot of work still remains. Sweden and .SE was the world's first top level domain to deploy a working implementation of DNSSEC, commencing in September 2005. As the first Top Level Domain (TLD) in the world, .SE (the Swedish TLD) also started to offer DNSSEC as a service through a number of Registrars. It was launched in February 2007 as an additional service to its Registrants (domain name customers). The aim was that .SE's DNS service should not only be highly robust and available, but also trustworthy.

.SE's vision for 2011 is that DNSSEC shall be a natural part of DNS, used by all important .SE domains and supported by several applications.

So, why did .SE decide to deploy DNSSEC in the first place? Since we considered that DNSSEC was required to be able to trust new and critical applications in the future, it was a strategic decision. DNSSEC increases the data integrity in DNS, which means it increases security for .SE's Registrants and the Internet community as a whole. It is a counterweapon against pharming and other attacks to DNS and it reinforces the Internet infrastructure. Moreover, it was also called upon by the responsible Swedish authority, the Post and Telecom Agency. This also, by the way, happens to be the first Government Agency to sign its own zone.

## Cost-effective

It doesn't necessarily cost a lot of money for an organisation to get its zone secured by DNSSEC. First of all, make sure that DNSSEC is enabled on all your name servers, which all modern software with the right configuration does support.

Secondly, make sure that you have skilled staff that understand the importance of managing DNSSEC. The zone of the child zone must be signed by its keys, and the keys must be signed by the parent zone. In that way, others may control the validity of the DNS data by verifying through the parent's key, which should be considered as the trust anchor in the security chain.

## Considerations

The deployment of DNSSEC necessitates a legal analysis. What risk exposure will the deployment imply? To what extent will we need contractual restrictions for those responsible for customers and third parties who are expected to rely on the DNSSEC?

An obvious aim is that the level of responsibility should be perceived as reasonable for any partner involved. .SE will take no responsibility for the subdomains keys or the administration thereof. This fact is one area mentioned in the .SE DPS – DNSSEC Policy and Practice Statement, which must be presented and made known to the public. The DPS describes the routines of verification, .SE's administrative and technical routines as well as the overall key management in .SE. The DPS aims to make it possible for others to decide what level of trust they are prepared to put in .SE's DNSSEC key management and administration.

To proceed with DNSSEC within an organisation means that you need to:

- Make someone responsible for the administration of the inhouse domain name management.
- Map all domains available within the organisation.
- Check on name servers – DNS basic configuration must be up to date and compliant with standard RFC's.
- Select which domains to start with and decide on a progress plan.
- Specify requirements (system, resources, competence).
- Devise a time schedule.
- Strive to achieve automatization.

## Key management is essential

The DNS management becomes more complex with DNSSEC, although it is only a slight difference. Mainly, it concerns key management and how to take care of the keys in a secure manner. In addition, you must resign the zone on a regular basis. The key of the parent zone will also change over time through key rollover, and it is important for the child to keep track of changes of the parent's keys. As well as the need for a technical environment for key management, you will also need to set up routines for:

- Key generation
- Key storage
- Key usage
- Key rollover (regularly and on emergency)
- Key distribution and publishing

**Lack of DNSSEC support in applications**
Even though more and more top level domains are deploying DNSSEC there are very few applications which support it, so the benefits are not that obvious, at least not yet. Nevertheless, it still remains important for organisations with critical functions in society to get started and use DNSSEC as soon as possible, before we are faced with a really severe attack against DNS, which could prove to be even more serious than the Kaminsky bug mentioned earlier.

**Real challenges**
There are some real challenges associated with deploying DNSSEC on a large scale.

Firstly, the need to get the root zone signed, which would totally simplify the key management. This issue is on the ICANN agenda, but unfortunately it is far from solved.

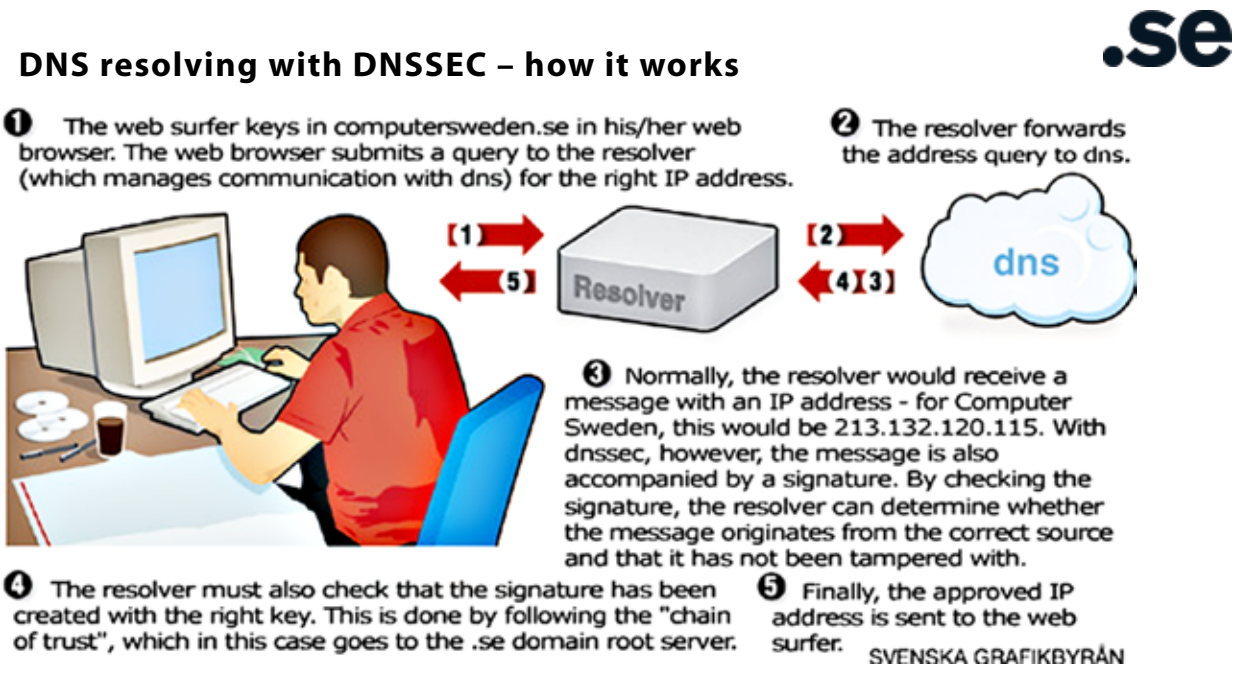
Secondly, all TLD's should be signed. Today only a small number of TLD's are signed, some of them only for test purposes. Last, but not least, all important domains within every TLD should be signed.

The slow development of the DNSSEC standards has been an obstacle. Many have doubted that it would ever happen, others point to the aversion among the Internet Service Providers to adopt DNSSEC. The Internet Service Providers very rarely make any improvements without a clear demand from their customers.
Another challenge is to make responsible decision makers within different areas aware of the fact that DNSSEC exists and eliminate some very serious threats against the Internet infrastructure.

DNSSEC is not the solution to every top priority security issue on the Internet, like malicious code and malware such as trojans and worms distributed through phishing and spam. Nevertheless, it is an important new layer of infrastructure. DNSSEC increases the ability to support different defense methods. Furthermore, like all new infrastructures, the value increases with the number of active users.

The real value of DNSSEC is obtained when the Internet users actually validates the answers from the DNS look-ups to ensure that they originate from the right source. This can be done in different ways. One common wish is that the validation should be made by the end user's application and that the end user by some means should be informed of the result, similar to the lock that is shown in the web browser when it has established a SSL session. Applications do exist that are performing DNS look-ups and DNSSEC validation, but DNSSEC is not supported by our most common applications.

The validation can also be made by the user's local DNS resolver. For the ordinary broadband customer, this resolver is typically provided by the user's ISP. For the Swedish DNSSEC project it has really been encouraging that the leading Swedish ISPs have switched on DNSSEC in their resolvers and are actually doing DNSSEC validation on behalf of their customers. This is indeed a good start, while we are awaiting DNSSEC support to become commonplace in the users' applications.



# IPv6: A Challenge To Any Registry

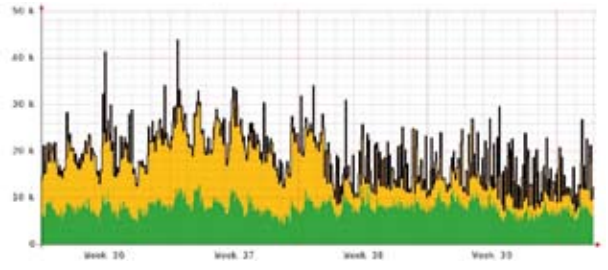
*by Dr. Jörg Schweiger, Member of the Executive Board, DENIC eG, Germany*

In recent years, the Internet has grown tremendously, and with it the number of users and demand for IP addresses. If the Internet continues to grow at the current pace, there will soon be a shortage of IP addresses of the Internet Protocol version 4. To face this foreseeable bottleneck in the evolution of the Internet the IPv6 protocol was developed which, in contrast to its predecessor IPv4, supports a much larger number of addresses. As to this the permitted address length is extended from 32 bit (IPv4) to 128 bit (IPv6). As a consequence, the address space increases to 3.4*10^38 addresses. Switching to this new standard represents an essential step towards a vital expansion of the Internet in order to be able to meet the future demand of additional IP addresses.

Thus, IPv6 constantly gains importance, not only for providers but also for registries. Besides the implementation of IPv6 in the DNS, numerous other services of a registry are affected. Mail servers, web servers, even the registration systems and many more must be made fit for IPv6.

DENIC as the registry for .de has started to roll out IPv6 already a few years ago. Initially, this was focussed on the DNS service. In 2004, DENIC installed an IPv6 (unicast) name server in Frankfurt, in 2005 a second one in Vienna followed. With these two name servers DENIC laid the foundation for the use of IPv6 in the production environment. Future challenges, however, will go beyond that scope, and so DENIC started to set up an IPv6 anycast cloud. This IPv6 anycast cloud is now operated from the locations Amsterdam, Frankfurt, Miami, Stockholm and Vienna on an experimental basis. DENIC thus is the only registry of a Top Level Domain that is already collecting first experiences with the operation and management of IPv6 anycast clouds. For the first quarter of 2009, it even plans to further expand its IPv6 name server service. Besides continuing operation of the currently productive unicast instances, it intends to start regular operation of the IPv6-compatible anycast clouds.

Chart: DNS queries to the IPv6 unicast name servers of DENIC



*The chart shows the number of DNS queries addressed to the two IPv6 unicast name servers of DENIC within one month. In peak periods, the two servers answer up to 40,000 queries per second. The setup accessible via IPv4 addresses, in contrast, processes up to 9 million queries in the same period. If the current distribution of IPv6 addresses is taken into consideration, however, the number of queries received by these servers is quite high.*

DENIC's IPv6 strategy envisages complete accessibility via the new protocol on the transport level. RIPE NCC has already allocated a specific IPv6 block to the registry, and some central services like outgoing mails are also being made available via IPv6. In the next step, the support of IPv6 shall be extended to all services of the registry system. This does not only imply a new architecture for the network that is to be set up but also changes to programs and policies. IPv6 glue records shall be processed automatically, to give one example. Moreover, policies for name server tests that become necessary and rules for delegation must be worked out and implemented.

The whole internal network shall be switched to the new protocol, too. This means that not only the personal computers but in particular the mail and web servers must support IPv6 in parallel to IPv4. DENIC is well prepared for the migration, however, since the office equipment already is IPv6-compatible. Existing testing features will help to identify potential error sources in hard- and software.

Of course the change-over is not an end in itself. It rather represents DENIC's desire to make available in a timely manner all its services in the IPv6 format to all those proactive users who have already switched to the new protocol. This shall encourage users to migrate soon. When other ccTLDs start to switch to IPv6, DENIC will be glad to assist them on the basis of the experiences it has made. DENIC considers this support part of its duty to serve the German and the international Internet Community.

# Introduction to the anycast technology

*by Krzysztof Olesik, DNS Technical Team Manager, NASK*

## Introduction

Broadly speaking we can describe Anycast as a technology that allows multiple hosts (which constitute a so called anycast cloud) to share one common IP address and act as a single device, despite physical separation. In the anycast routing scheme, data is routed to the "nearest" destination as viewed by the routing topology. So the choice of the "nearest" destination depends on network topology, protocols used to make forwarding decisions and the associated administrative policies within a particular network (Autonomous System). An anycast routing scheme is a useful technique for providing redundancy and load sharing to specific types of network services on the Internet.

For a better understanding of anycast and of the differences between communication schemes like unicast, broadcast and multicast we will provide below a short description of each term.

On the Internet, the hosts can be uniquely identified by Internet Protocol (IP) addresses. The IP address which is assigned as a unique identifier to a host's network interface is referred to as unicast address. A unicast address can be used either as the source or destination address in an IP datagram. In a unicast routing scheme, where each IP address uniquely identifies a single host, data is routed from one source host to only a single destination host.

Broadcast addresses are used for information delivery to all hosts in a given IP network. Datagrams sent to an IP broadcast address are delivered to all hosts on a particular physical data link network or IP subnet, in other words each destination (broadcast) address identifies a group of receiver hosts, to which all information is replicated. Broadcast addresses are used in the destination address field of an IP header.

In multicast, an IP address is also associated with a group of receiver hosts. Such a group can consist of any number of hosts, even including all hosts on the network. Like the broadcast addresses, multicast addresses can only be used in the destination address field of an IP header. In a multicast routing scheme each destination address identifies a set of receiver hosts, to which all information is replicated.
Now we can see that anycast like broadcast and multicast has one-to-many associations between IP addresses and hosts: each destination address identifies a set of receiver endpoints, but only one of them is chosen at any given time to receive information from any given sender. An anycast address can be used as either a source or destination address, but no longer uniquely identifies a single host or service. Anycast addresses are assigned from the same address space from which unicast addresses are allocated. Therefore, unlike private address space, one cannot visually differentiate a unicast address from an anycast address.

## Anycast routing

Now we should take a closer look at anycast routing and find an answer on how multiple hosts can share the same IP address without - network conflicts.

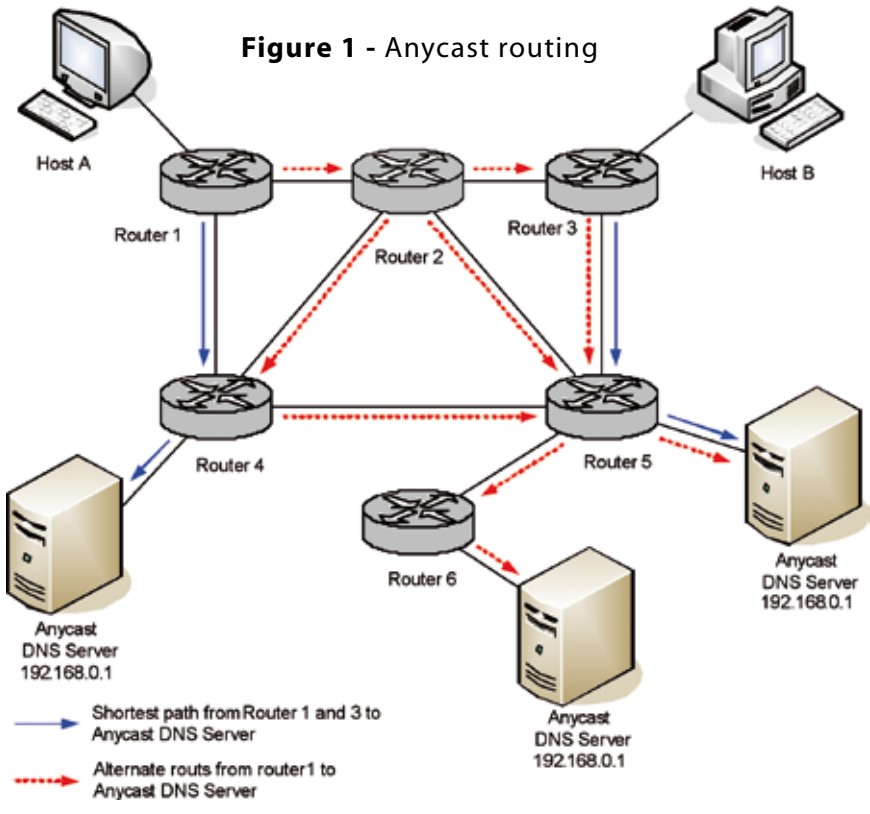
The Internet is a global system of interconnected computer networks that interchange data. It may be perceived as a "network of networks". A group of connected networks under the control of one or more network operators that presents a common, clearly defined routing policy to the Internet is called the Autonomous System (AS). Such a network is identified in the Internet by Autonomous System Number (ASN). At the border of each network there are devices called border or edge routers which advertise netblocks (address space, for example 195.0.1.0/24), also known as prefixes, which indicate what subnetworks are behind a particular router. Anycast address spaces (anycast netblocks) are advertised by routers in the same way as unicast netblocks but anycast netblocks are advertised from multiple origin points. From a routing topology view, it looks as if an anycast netblock is multi-homed at different points of the network. An anycast netblock is often just a host route (/32 in CIDR notation) within an autonomous system (AS). The important feature of the anycast routing is that it uses dynamic routing protocols without any modifications of network protocol standards and do not require any specific routing concepts to implement.

Anycast technology is broadly used in conjunction with the DNS service. That is why we explain anycast routing from the DNS perspective in this example. Let's consider the example in Figure 1.

Host A sends a DNS query to the anycast DNS server which anycast address is for example 192.168.0.1. The single IP address is shared by three physically separate servers providing the same DNS service. Therefore, it does not matter which of three DNS servers (node of anycast cloud) receive the DNS query. According to the anycast routing scheme the DNS query should be delivered to the "nearest" anycast DNS server. Here the main role is played by the routing metrics, which define the best route to the destination. The metric is computed by a routing algorithm like BGP, IGP or OSPF

and may cover such information as: bandwidth, network delay, hop count, path cost, load, MTU, reliability, and communication cost. In our scenario we will use only hop count as a metric for simplicity reasons. As illustrated in Figure 1, the decision how the DNS query from Host A should be delivered to the anycast DNS server belongs to Router 1. Router 1 uses a routing table which is computed based on at least one or more possible routes and their metrics to the destination anycast address. In the latter case Router 1 may forward the DNS query to Router 4 or Router 2. Of course it will chose the route via Router 4 because the anycast DNS server (homed behind Router 4) is only two hops away from Router 1 (the shortest path). The same is true for Host B. It will use the shortest path to DNS Server via Router 3 and Router 5.

**Figure 1** - Anycast routing




One may ask what will happen if the anycast DNS server behind Router 4 is down. The answer for this question depends on how routers are configured. Routers can be configured with static routes or dynamic routes. Let's assume that Router 1 in our example has defined a static route to deliver all datagrams to address 192.168.0.1 via Router 4. Then it will always send the datagrams to address 192.168.0.1 via Router 4. In case of link failure to Router 4, the static routing provides no automated alternate routing. Such example situation would be fixed, if the administrator of Router 1 manually set up the alternate route. Here comes in handy the dynamic routing which provides mechanisms to advertise the reachability of the destination address. Now let's assume, that the anycast DNS server homed behind Router 4 runs a routing software which transmits reachability updates to Router 4. Thus, if the server fails and stops transmitting routing updates to Router 4 then Router 4 will update its routing table with the appropriate metric that the destination 192.168.0.1 homed behind Router 4 is no longer available and pass this information to other routers via the mechanisms of routing protocols. Therefore, Router 1 knows that the anycast DNS server is now reachable via Router 2 and still via Router 4 but now with a less preferable metric. Router 4 knows it has to forward datagrams for address 192.168.0.1 to Router 5. The best solution in this example would be if the routing daemon was linked with the status of the DNS service so it can communicate the anycast DNS server failure also when the DNS service is down. Such an approach provides high availability of the anycast DNS service and its high performance thanks to the shortest path routing.

It is worth to mention that there are two types of anycast: the global anycast and the local anycast. The global anycast uses the BGP routing protocol to announce the same destination anycast address from various places in the Internet. The local anycast uses routing protocols like OSPF, EIGRP, IS-IS. The announcement of the destination anycast address is confined within the local area – an autonomous system. As for the root servers, both F and K root name servers use local and global anycast nodes.

Benefits of Anycast Technology

The introduction of anycast technology, especially to DNS yields number of benefits:

- diversity of ISPs hosting nodes of an anycast cloud (operational regimes, business robustness, diversity in network operation),
- diversity of hardware and software platforms (providers of anycast DNS solutions run proprietary software, use different hardware),
- high availability DNS service,
- better resolution performance (the DNS queries are delivered to the "nearest" anycast DNS server),
- one name server in the delegation of a domain name – multiple physical instances (512B UDP packet size no longer limit the number of physical name servers supporting a domain name),
- resilience against distributed denial of service (DDoS) attacks. (the DDoS traffic flow is distributed amongst the closest anycast nodes. Proved during attack on the root server system on 6 February 2007, see the ICANN's report - DNS Attack Factsheet 1.1 http://www.icann.org/en/announcements/announcement-08mar07.htm).

The anycast technology is an innovative technology for providing a high performance and a high availability of the DNS service. It becomes more popular among the ccTLD registries. According to the author's investigation among CENTR members the following ccTLD registries have deployed at least one anycast cloud: .ca, .cz, .fi, .fr, .ie, .jp, .lt, .lu, .nl, .no, .pl, .se, .uk.

# Looking ahead to the third Internet Governance Forum

*by Emily Taylor, Director of Legal and Policy at Nominet*

*Emily Taylor, Director of Legal and Policy at Nominet, the country code registry for .uk, and member of the Internet Governance Forum's Multi-stakeholder Action Group, looks ahead to the next IGF in Hyderabad and explains how national processes are beginning to have an impact on shaping the discussion.*

We are fast approaching the third meeting of the United Nations' Internet Governance Forum, a multi-stakeholder forum that debates a range of issues relating to Internet governance and works with all stakeholders to create a safe, fair and inclusive Internet experience. This year's event in early December will be held in Hyderabad, India and as well as attending meetings as a member of the IGF's multi-stakeholder action group I will be part of a UK delegation of parliamentarians and stakeholders from industry and civil society.

Nominet, working with other partners, has been at the heart of preparing the UK for the Internet Governance Forum. We see it as crucial to engage constructively with the IGF process, both in contributing to the discussions with ideas and in identifying examples of how to get the best out of the Internet. With other UK stakeholders we are identifying "messages from the UK" and best practice case studies, using a partnership approach to making the Internet a better place, and keeping UK stakeholders engaged in the IGF process.

This approach has developed over the life of the IGF, and led us to launch the UK IGF in March this year. This is an open partnership that provides a light and flexible framework for British stakeholders to work together to make the IGF a success.

Last year Nominet worked with an all-party delegation of parliamentarians who attended the IGF in Rio. The UK delegation was able to share many encouraging examples of the successful partnership approach and multi-stakeholder cooperation that already exists within the UK. We took the opportunity to host Best Practice workshops – well received by our colleagues from other countries who expressed an interest in following a similar approach.

The European Parliament resolution on the Rio IGF meeting stressed the importance of engaging national and regional interests in the IGF process in order to form 'local' IGFs. Rt Hon Alun Michael MP, one of our delegation, had already made the commitment to the international community in Rio to establish a UK IGF and I was delighted when this vision became a reality in March this year. The UK IGF was the first such national process, and to a great extent it is now viewed as the benchmark. A collaborative partnership between Nominet, the UK Department for Business and key parliamentarians, it is modelled on the lightweight, open structure of the international IGF – there is no "membership" and no-one is excluded. It provides an umbrella in which to reflect on relevant initiatives, such as the Crime and Disorder Reduction Partnership and Nominet's Best Practice Challenge.

Nominet launched the Best Practice Challenge as a way of celebrating success and achievement, rather than concentrating on threats and concerns. Now in its second year, the Best Practice Challenge highlights

examples from the UK of excellence in the IGF themes of security, access, diversity and openness. It highlights the work of industry, civil society and governmental organisations in addressing today's challenges, such as security, industry standards, access to the Internet for the disabled or those affected by the digital divide.

This year's Challenge produced even more entries from a wider spectrum of businesses and organisations. Amongst the winners was Barclays Bank with a device called PINsentry that has significantly increased online security for its customers. Other winners included voluntary organisations such as Common Knowledge in Glasgow and ACE IT in Edinburgh dedicated to bridging the technological gap faced by people with significant cognitive learning difficulties and elderly people respectively. These are real examples of individuals' and organisations' initiatives making a real difference to people's lives.

Why is the UK keen on advancing a self-regulatory Internet industry? Simply, as we see clearly from the Best Practice Challenge, from the Internet Watch Foundation, and from the recent creation in the UK of the Council for Child Internet Safety, the Internet benefits greatly from organisations' abilities to provide flexible, adaptable solutions. It is very encouraging to see real examples of this happening within the UK Internet community and in particular how to a great extent challenges are being solved through voluntary action.

The challenge for the UK IGF is to create intelligent, collaborative solutions to problems of Internet governance and the outcomes of the Best Practice Challenge clearly demonstrate to our international colleagues that we are making great strides in this area.

One of the key messages to emerge from the first UK IGF meeting is that the UK is taking a leading role in Internet governance, and that other countries are seeing what we are doing and beginning to start running their own processes at the national level.

Each national process will of course be different, reflecting local priorities and concerns. We will be running a workshop in Hyderabad in collaboration with colleagues from Brazil, Finland and France to explore different national IGF approaches.

The UK is proving to the rest of the world that the Internet Governance Forum works, as a collaborative partnership between Government, business, civil society and academia, because it is not subject to Government legislation and is free from bureaucracy.

One key aspect of the UK's engagement in the IGF is to work with parliamentarians. This has been crucial in helping us develop our messages – in particular in helping understand the concerns and interests of the citizens. Working with parliamentarians has helped us to focus our work on these key issues – like child Internet safety or fighting crime – and to engage with top decision makers from industry and civil society. One British MP has been leading a multi-stakeholder dialogue using the IGF model to improve e-crime reduction in the UK.

I am also chair of the CENTR IGF working group, and have been focusing on how we can engage with the IGF process in the most effective way. For the Rio meeting, and for the IGF in Hyderabad, this group has collaborated with other regional ccTLD organisations (such as apTLD, LACTLD) to prepare workshops which support the IGF themes and introduce delegates to the diversity of ccTLD arrangements, which reflect different national conditions and priorities.

This year, CENTR (in collaboration with the other regional groups) is presenting a workshop "Around the World in 8 ccTLDs". The speakers will each address a topical issue, such as business continuity, interaction with the Internet community, governance structure and internationalised domain names. We aim to use this workshop to educate the wider audience on these topics, whilst demonstrating the diversity in ccTLD organisational structures and how this links with the varying needs of the local communities we serve.

These various initiatives – the UK IGF and the CENTR IGF work – are crucial in providing a positive lead for the IGF: we have an opportunity to shape our future and make the Internet a better, safer environment, without losing the innovation, the benefits and the sheer fun that have contributed so strongly to the economy and society.

nominet

Centr

COUNCIL OF EUROPEAN NATIONAL TOP LEVEL DOMAIN REGISTRIES
WWW.CENTR.ORG

## INTERNET COUNTRY CODE TOP-LEVEL DOMAINS

THE CENTR MEMBERS
THE CENTR ASSOCIATE MEMBERS

| | |
|---|---|
| .ac | Ascension Island |
| .ad | Andorra |
| .ae | United Arab Emirates |
| .af | Afghanistan |
| .ag | Antigua and Barbuda |
| .ai | Anguilla |
| .al | Albania |
| .am | Armenia |
| .an | Netherlands Antilles |
| .ao | Angola |
| .aq | Antarctica |
| .ar | Argentina |
| .as | American Samoa |
| .at | Austria |
| .au | Australia |
| .aw | Aruba |
| .ax | Åland Islands |
| .az | Azerbaijan |
| .ba | Bosnia and Herzegovina |
| .bb | Barbados |
| .bd | Bangladesh |
| .be | Belgium |
| .bf | Burkina Faso |
| .bg | Bulgaria |
| .bh | Bahrain |
| .bi | Burundi |
| .bj | Benin |
| .bl | Saint Barthelemy |
| .bm | Bermuda |
| .bn | Brunei Darussalam |
| .bo | Bolivia |
| .br | Brazil |
| .bs | Bahamas |
| .bt | Bhutan |
| .bv | Bouvet Island |
| .bw | Botswana |
| .by | Belarus |
| .bz | Belize |
| .ca | Canada |
| .cc | Cocos (Keeling) Islands |
| .cd | Congo, The Democratic Republic of the |
| .cf | Central African Republic |
| .cg | Congo, Republic of |
| .ch | Switzerland |
| .ci | Cote d'Ivoire |
| .ck | Cook Islands |
| .cl | Chile |
| .cm | Cameroon |
| .cn | China |
| .co | Colombia |
| .cr | Costa Rica |
| .cu | Cuba |
| .cv | Cape Verde |
| .cx | Christmas Island |
| .cy | Cyprus |
| .cz | Czech Republic |
| .de | Germany |
| .dj | Djibouti |
| .dk | Denmark |
| .dm | Dominica |
| .do | Dominican Republic |
| .dz | Algeria |
| .ec | Ecuador |
| .ee | Estonia |
| .eg | Egypt |
| .eh | Western Sahara |
| .er | Eritrea |
| .es | Spain |
| .et | Ethiopia |
| .eu | European Union |
| .fi | Finland |
| .fj | Fiji |
| .fk | Falkland Islands (Malvinas) |
| .fm | Micronesia, Federated States of |
| .fo | Faroe Islands |
| .fr | France |
| .ga | Gabon |
| .gb | United Kingdom (Great Britain) |
| .gd | Grenada |
| .ge | Georgia |
| .gf | French Guiana |
| .gg | Guernsey |
| .gh | Ghana |
| .gi | Gibraltar |
| .gl | Greenland |
| .gm | Gambia |
| .gn | Guinea |
| .gp | Guadeloupe |
| .gq | Equatorial Guinea |
| .gr | Greece |
| .gs | South Georgia & the South Sandwich Islands |
| .gt | Guatemala |
| .gu | Guam |
| .gw | Guinea-Bissau |
| .gy | Guyana |
| .hk | Hong Kong |
| .hm | Heard and McDonald Islands |
| .hn | Honduras |
| .hr | Croatia |
| .ht | Haiti |
| .hu | Hungary |
| .id | Indonesia |
| .ie | Ireland |
| .il | Israel |
| .im | Isle of Man |
| .in | India |
| .io | British Indian Ocean Territory |
| .iq | Iraq |
| .ir | Iran |
| .is | Iceland |
| .it | Italy |
| .je | Jersey |
| .jm | Jamaica |
| .jo | Jordan |
| .jp | Japan |
| .ke | Kenya |
| .kg | Kyrgyzstan |
| .kh | Cambodia |
| .ki | Kiribati |
| .km | Comoros |
| .kn | Saint Kitts and Nevis |
| .kp | Korea, Democratic People's Republic |
| .kr | Korea, Republic of |
| .kw | Kuwait |
| .ky | Cayman Islands |
| .kz | Kazakhstan |
| .la | Laos |
| .lb | Lebanon |
| .lc | Saint Lucia |

.li Liechtenstein
.lk Sri Lanka
.lr Liberia
.ls Lesotho
.lt Lithuania
.lu Luxembourg
.lv Latvia
.ly Libya
.ma Morocco
.mf Saint Martin
.mc Monaco
.md Moldova
.me Montenegro
.mg Madagascar
.mh Marshall Islands
.mk Macedonia, The Former Yugoslav Republic of
.ml Mali
.mm Myanmar
.mn Mongolia
.mo Macao
.mp Northern Mariana Islands
.mq Martinique
.mr Mauritania
.ms Montserrat
.mt Malta
.mu Mauritius
.mv Maldives

.mw Malawi
.mx Mexico
.my Malaysia
.mz Mozambique
.na Namibia
.nc New Caledonia
.ne Niger
.nf Norfolk Island
.ng Nigeria
.ni Nicaragua
.nl Netherlands
.no Norway
.np Nepal
.nr Nauru
.nu Niue
.nz New Zealand
.om Oman
.pa Panama
.pe Peru
.pf French Polynesia
.pg Papua New Guinea
.ph Philippines
.pk Pakistan
.pl Poland
.pm Saint Pierre and Miquelon
.pn Pitcairn Island
.pr Puerto Rico

.ps Palestinian Territories
.pt Portugal
.pw Palau
.py Paraguay
.qa Qatar
.re Reunion Island
.ro Romania
.rs Serbia
.ru Russian Federation
.rw Rwanda
.sa Saudi Arabia
.sb Solomon Islands
.sc Seychelles
.sd Sudan
.se Sweden
.sg Singapore
.sh Saint Helena
.si Slovenia
.sj Svalbard and Jan Mayen Islands
.sk Slovak Republic
.sl Sierra Leone
.sm San Marino
.sn Senegal
.so Somalia
.sr Suriname
.st Sao Tome and Principe
.su Soviet Union (being phased out)

.sv El Salvador
.sy Syrian Arab Republic
.sz Swaziland
.tc Turks and Caicos Islands
.td Chad
.tf French Southern Territories
.tg Togo
.th Thailand
.tj Tajikistan
.tk Tokelau
.tl Timor-Leste
.tm Turkmenistan
.tn Tunisia
.to Tonga
.tp East Timor
.tr Turkey
.tt Trinidad and Tobago
.tv Tuvalu
.tw Taiwan
.tz Tanzania
.ua Ukraine
.ug Uganda
.uk United Kingdom
.um United States Minor Outlying Islands
.us United States
.uy Uruguay
.uz Uzbekistan

.va Holy See (Vatican City)
.vc Saint Vincent and the Grenadines
.ve Venezuela
.vg Virgin Islands, British
.vi Virgin Islands, U.S.
.vn Vietnam
.vu Vanuatu
.wf Wallis and Futuna Islands
.ws Samoa
.ye Yemen
.yt Mayotte
.yu Yugoslavia
.za South Africa
.zm Zambia
.zw Zimbabwe

The TLD registries for .biz, .cat, .com, .info, .mobi, .net & .org are CENTR Associated Members

Information Source:
IANA TLD Database

December 2008

# European ccTLDs – overview

*by Wim Degezelle, Communications Manager, CENTR*

*CENTR members have a tradition of sharing information and surveys have proven to be one of the most successful tools to gather and convey information on actual, practical and sometimes pressing questions.*

*In the first quarter of 2008 CENTR organised a broad survey on the practices and domain name principles amongst CENTR members.*
*The CENTR 2008 A-level survey is a follow up on the 2002 and 2005 surveys.*

This article gives you an overview of the main results.

43 CENTR members answered the survey. All together, the participants in the survey were responsible for 52 different country code domains and one generic domain.

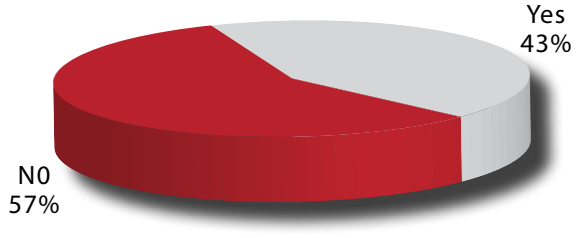
### The ccTLD registry

- The surveyed ccTLDs represented more than 38 million domains registrations on 1st January 2008, what was more than 66% of the total base of ccTLD domains world wide at that moment.
- 57 % of the ccTLD registries in the survey classified themselves as *private organisations*. 43% answered that they were *public entities*.

### Domain names

- 50% of the registries allowed registrations both directly under the top level (e.g. centr.##) and under a second level domain (SLD) (e.g. centr.xyz.##). 33% of the registries only allowed registrations on the second level and 17% only on the third level.
- The registries offered 129 different SLDs (regional and geographic SLDs not included). 105 of the SLDs in the list were unique, for example translations in the local language. The most popular SLDs were *org.##*, *.com.##* and *.net.##*.
- Internationalised domain names (IDNs) could be obtained with 43% of the registries.

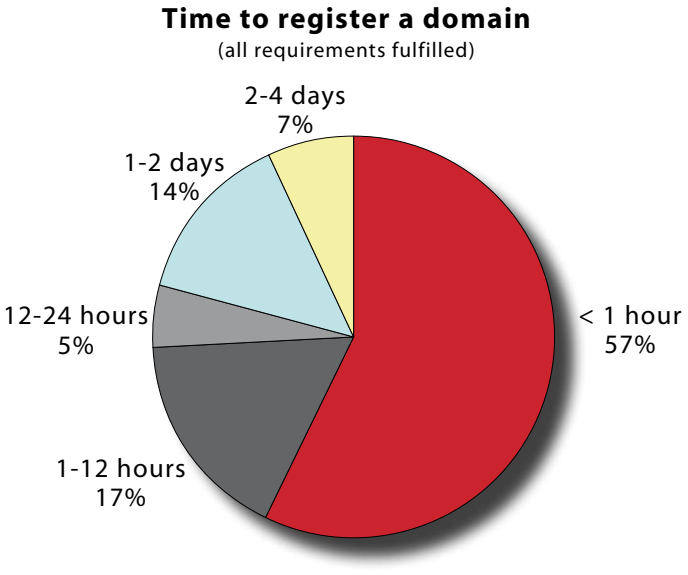
**IDN registrations**




| ccTLD registries register IDN domain names | |
|---|---|
| only as IDNs | 50% |
| only under xn-- form | 22% |
| both as IDN and under the xn—form | 28% |

### Domain Registration

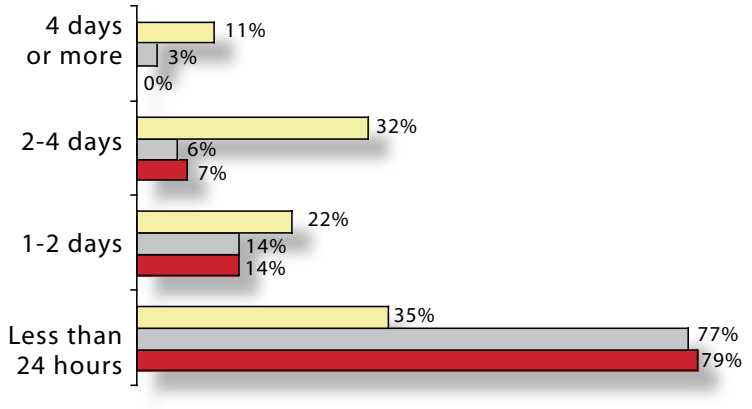
- 79% of the registries strictly applied the *'first come first served'* principle; most others followed *'first come first served'* as main principle with some exceptions.
- Most registries (69%) offered registrations for one year. A smaller number (10% and of 2%) offered standard periods of 2 and 3 years. 19% of the registries had no time limit on domain registrations.
- 41% of the registries require the domain holder to have a presence in the country.
- For most registries, when all requirements are fulfilled it takes less than one hour to register a domain name (57%). Three out of four registries (79%) register domain names within 12 hours and nine out of ten (93%) do it within 2 days.




| Time needed to register a domain name (all requirements fulfilled) | | |
|---|---|---|
| | | **Cumul %** |
| Less than 1 hour | 57% | **57%** |
| 1 – 12 hours | 17% | **74%** |
| 12 – 24 hours | 5% | **79%** |
| 1 – 2 days | 14% | **93%** |
| 2 – 4 days | 7% | **100%** |

- If one compares the time needed to register a domain name in 2008 with the findings of the 2002 and 2005 CENTR A-level surveys there is an enormous improvement between 2002 and 2005/2008. The number of registries that can register a domain name in less than 24 hours more than doubles from 35% to 77% and 79%.

**Time to register 2002 / 2005 /2008**




- Anno 2008, almost 60% of the registries registered a domain name in less then 1 hour.

- A registered domain is visible in the DNS in less than 1 hour said 42% of the registries. 19% of the registries answered that the domain is active in less than 5 minutes.

## Registry / Registrar model

- Three out of four registries worked with a registry-registrar model
- The total number of registrars per registry varied between 4 and 3,621.

## Dispute resolution

- An internally developed ADR (43%) was the most popular dispute resolution service provided, followed by an UDRP based system (24%) .
- 8 registries answered that they were not providing a dispute resolution service.

## Additional services

- Most registries (93%) provided a publicly available Whois service. The information available in the Whois differed from registry to registry.
- 54% of the registries gave the registrant the possibility to hide data in the Whois.
- 38% of the registries were involved in their country's ENUM registry. 10 said they were running the ENUM registry for their country.

For more information, please contact secretariat@centr.org .

# Nominet Foundation

*by Lesley Cowley, CEO of Nominet*

*Lesley Cowley, CEO of Nominet, the country code registry for .uk, talks about the creation of the Nominet Charitable Foundation , an organisation that will fund projects within the UK Internet industry.*

Over the past year we have been working hard to establish the Nominet Charitable Foundation, which will fund education, research and development initiatives in the Internet industry.

At the heart of our decision to begin this project is the fact that Nominet is a not-for-profit organisation. This prevents us from distributing any surpluses that we make to our members but we can use them to make charitable donations.

The idea of a Nominet Foundation was first floated in 2005 though in fact its origins can be traced even further back. Over twelve years ago, as part of the discussions about the kind of organisation that would be formed to take on the role that Nominet now performs, there was a suggestion that a not-for-profit management company would be formed. As part of its main objectives it would establish a charitable trust and pay it any annual surplus not required for the prudent ongoing management of the operation. The trust would use its income for research for the industry and provide it with other educational benefits. This was dropped from later drafts as it was thought unlikely that Nominet would ever make any surpluses, particularly as it was envisaged that our charges would match operating costs.

However, Nominet has been profitable almost since its earliest years and these profits have been used to fund the development of the business and accumulate reserves. The level of reserves we need to cover two years of running costs has been met since 2003 and since then we have been considering what we can best use these funds for.

Following detailed discussions at Board level during April and May 2007 we formulated a consultation document that laid out a proposed structure and purpose for the charitable organisation. We conducted a three-month public consultation with our members and wider stakeholders to gauge support for the initiative. We received some very positive feedback on our proposal, as well as some interesting suggestions for how the money could be used.

The next steps in the process were to draw up the Memorandum and Articles of Association, apply for charitable status for the Foundation and appoint a board of Trustees.

This process took several months to complete, as we were very conscious that the future success of the enterprise depends on us getting these details absolutely right.

We have appointed a board of six trustees. I will act as the Nominet Board representative, my colleague James Kemp is the Nominet staff representative, and Stephen Dyer, Chairman and founder of Energetics Ecology Ltd is the Nominet membership representative. The other three trustees are Vanessa Miner, and advisor to the DCSF on new school partnerships; Ian Ritchie, non-executive Chairman of Iomart plc and Jonathan Welfare, Chief Executive of Elizabeth Finn Care. My fellow trustees are all high calibre candidates with a wealth of experience in fundraising and oversight of charitable trusts and I am confident that together we have the abilities to ensure that the Nominet Charitable Foundation will make a real impact in helping us to shape the future of the Internet in the UK and beyond.

The idea of Nominet establishing a Foundation that will support education, research and development projects within the Internet industry is consistent with other initiatives we have undertaken recently. Since 2007 we have been running the annual Nominet Best Practice Challenge, which has seen us take a leading role in promoting best practice in the UK Internet industry. Past winners of these awards include organisations such as Barclays, the Internet Watch Foundation and the British Library, as well as a number of small businesses and charitable organisations.

Nominet has made an initial donation to the Foundation of £5 million for the first year, and we are planning to invite potential projects to apply for funding in early 2009. We look forward to announcing full details of this process nearer the time. For more information about the Nominet Charitable Foundation, please visit our web site at http://www.nominetfoundation.org.uk/

We believe that the Foundation can be used to strengthen the confidence and trust of UK Internet users in the online environment and will support the wider industry's role in addressing the needs of individual users, businesses and society. The investment we are making and our engagement with the industry on this project will make a real contribution to enabling the UK to remain a global leader in the fast paced world of the Internet.

nominet


# About trust in the Web

*by Roelof Meijer, CEO SIDN*

Over last decades, the internet, with over 100 million websites and an estimated 10 billion public web pages, has developed from a small experimental data network into an all encompassing medium for commerce, communication and data exchange. As such, in a short space of time, the internet has become fundamental to the global economy and social life.

The easy access, low costs of publication and, as a consequence, the virtually unlimited information available on the internet enrich our lives, but also have their downsize. Spam, identity theft and illegal content are some of the virtual world varieties of "real" world crime.
As a result, demands with regard to the protection of economies and consumers sharpen while governments' involvement through oversight and regulation increases.

Ensuring a safe Internet is not just good business. Neither is it just a government (of for that matter "the other guy's") issue. It is the responsibility of all stakeholders since trust and confidence of users in the internet is crucial for the further evolution of the Internet to its full potential and that trust can only be ascertained through collaboration.

As manager of the .nl top level, SIDN is responsible for the proper functioning and development of the .nl name space. However, it should not end there. As an integral part of our strategy and based on a sense of shared stakeholders' responsibility and dedication, we invests significantly in initiatives that aim to stimulate use, increase security and trust and discourage abuse of the Internet.

Ample initiatives exist, both in our own country as well as abroad. Examples of our involvement are the sponsoring of the "Digibewust" campaign (promoting responsible use of the internet amongst all age groups in The Netherlands), "Meldpunt Kinderporno" (for reporting internet child pornography) and "Fraudemeldpunt" (for reporting internet fraud). SIDN was one of the initiators of the recently adopted "code of conduct for Notice and Take Down" for access and hosting providers in The Netherlands.

In the international arena, SIDN is part of a diverse group of Internet related companies that, again out of a sense of shared responsibility, decided to join forces to form the Registry Internet Safety Group or "RISG". During the CENTR GA in Viareggio, Italy, in October 2008, this group presented itself to the membership and welcomed members to join.

The primary purpose of RISG is to facilitate dialogue, affect change, and develop best practices to address Internet identity theft including "phishing" and all of its related forms. RISG members are attempting to create methods to share data among member companies that will enhance the understanding of phishing and malware and further the mission of RISG to eliminate them. RISG members respect and value user privacy as an ideal that must be preserved in any plan designed to prevent Internet identity theft.

RISG seeks to function collaboratively with other Internet industry groups possessing similar objectives. RISG is designed to complement, and not duplicate, the efforts of other industry groups already working to eliminate phishing and malware distribution. RISG is not setting binding policy or engaging in content control or censorship. The exclusive focus of RISG is prevention of identity theft in the form of phishing and abuse of domain names to facilitate phishing.

Current RISG members include Nominet (.UK), Afilias (.info), SIDN (.NL), GoDaddy, FBI, Symantec, Cyveillance, Shinkuro, PIR (.ORG), Neustar (.BIZ), Network Solutions, CNNIC (.CN) and Mark Monitor. Alexa Raad of .ORG currently serves as RISG Chairperson, Roelof Meijer of .NL is Vice Chairperson and Greg Aaron serves as Board Secretary. RISG membership is open to anyone who shares the ideals of responsible Internet practices and agrees to work cooperatively in the RISG group. RISG has also recently created an observer status if a company desires to observe a meeting prior to applying for membership. RISG meets telephonically for one hour each month and the group also meets at the conclusion of each ICANN Conference. Persons interested in RISG membership may contact .ORG team member Adam Palmer at apalmer@pir.org for more information.

SIDN

# The "Internet of Things" viewed from the "Object Naming Service" Angle

*by Mohsen Souissi, R&D team leader at AFNIC*

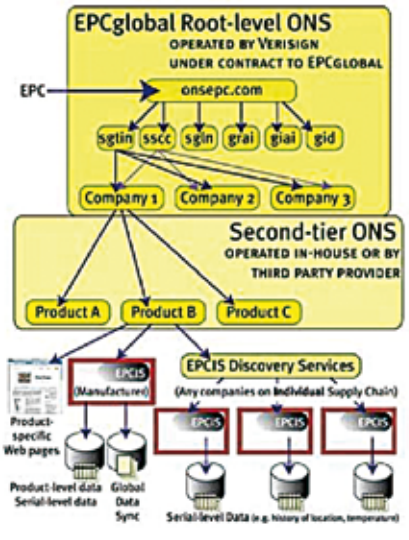
*The "Internet of Things" is quite a new paradigm which encompasses several meanings depending on the communities/technologies being involved. The current Internet infrastructure can be used to connect to the real world of physical objects, using technologies like RFID, Near Field Communication (NFC) and sensor networks, either directly or indirectly.*

For new commonplace devices (aka "objects"), *direct* connections to the Internet may be simply enabled by means of a (minimal) IP stack and some type of layer-2 connectivity (Wi-Fi, GPRS, UMTS, Edge, Ethernet...). As for *indirect* connections to the Internet, they may be enabled via some *intermediate equipment*. The latter is typically a smart device that can handle communications at two levels: on the one hand with those non-IP-capable devices (by using some short-range communication technology such as RFID, Bluetooth, NFC...), and on the other hand, with the IP network, thus bridging between non-IP and IP worlds.

In the context of this article, when dealing with "objects", we will only focus on RFID-capable devices, typically equipped with an RFID tag. An RFID tag stores a unique identification number called Electronic Product Code (EPC). The EPC will serve as the identifier for the physical object carrying the tag. The information about the object is not stored in the tag itself but stored in different servers distributed across the network. The network of physical objects achieved by integrating an EPC to each object is called the EPC network.

### 1. ONS Technology Overview

The Object Naming Service (ONS) [ONS] is an EPCglobal standard based on the DNS protocol and infrastructure. It is used the in the EPC network to locate EPC Information Services (EPCIS)[1] [EPCIS]. The figure below depicts the overall service architecture.




*Source: Auto-ID Labs*

We will give a brief example to illustrate how the EPC of a given RFID tag-equipped object is resolved into a DNS Fully-Qualified Domain Name (FQDN), and of how that FQDN is used as a key to lookup information associated to the object.

When a tag-equipped product reaches a shop, an RFID reader located at the shop reads out the tag and receives an EPC identifier in binary form. Then it forwards the EPC identifier to a middleware or inventory system (for example), to retrieve information about the product from the manufacturers database on the Internet. The system

1 EPCIS's are distributed across the network, which are collections of available data about the particular object.

transmits the EPC identifier to a local ONS resolver, which converts the identifier into a DNS Fully-Qualified Domain Name (FQDN) as follows, according to current ONS specifications [ONS]:

Binary: "10 000 00000000000000 00000000000000011000 00000000000000000110010000"

→ a URI: urn:epc:id:sgtin:0614141.000024.400

→ an FQDN: 000024.0614141.sgtin.id.onsepc.com.

The resolver queries the local ONS server to get information corresponding to the domain name. In case the local ONS server does not have the information, it sends the query to the ONS root server. The latter typically responds with a referral to the corresponding local ONS server which has the authoritative data related to the manufacturer EPC-IS.

Note that such authoritative data are only related to the object class and not to the physical instance of object, as the serial-level information (the last part of the EPC) is not taken into account in the ONS query according to the current ONS specifications. Returned data will typically be a set of URLs which point to one or more services (for example, an EPCIS Server) and which are enclosed in a DNS NAPTR Resource Record set (RRset), in a similar way to ENUM technology.

**Example:**
000024.0614141.sgtin.id.onsepc.com. IN NAPTR 0 0 "u" "EPC+epcis" "!^.*$!http://example.com/epcis!"

The local resolver extracts the URL(s) from the DNS record and presents it/them back to the local server. The local server connects to the appropriate EPC-IS server according to the previous URL(s).

**2. ONS Perceived Limitations**

It is perceived that the current ONS specifications suffer from a set of limitations either at the technical or at the governance level. Here are some examples to illustrate the perceived limitations:

- The ONS is useful if all you need to find is the manufacturer and/or the class of the product, as the serial-level information within the EPC is currently ignored;
- Security is not fully taken into account (typical ONS users are more demanding than classical DNS users in terms of access control, privacy, confidentiality, etc.);
- A "Unique Root" does not meet geopolitical concerns even if a "Unique Root" is the most technically straightforward...

It is the last limitation above which has raised most concerns. As a matter of fact, according to the current ONS specifications by EPCglobal standardization body, there is a single ONS root zone,[2] onsepc.com (currently managed by EPCglobal inc and operated by Verisign Inc.), containing the whole ONS name space. Some industrial and political communities, notably in Europe, are not satisfied with the governance model and the architecture of a single root solution. They have expressed the need for a *Multi-Root ONS Architecture*, and have started working on this matter so that next revisions of the ONS standard will meet the new requirements.

On the other hand, it is expected that the ongoing efforts towards *Discovery Services* standardization will provide the RFID industry, and notably the supply-chain sector, with full track & trace functionality (in that context, physical instances of the products are dealt with instead of classes of products as it is currently the case in ONS). Such standardization efforts are carried out within EPCglobal [DiscServ] with the help of the IETF community [ESDS].

2 Note that in April 2008, a second root zone, onsepc.eu, was launched by GS1 France for the European Region [ONS-EU]. This second zone (onsepc.eu) is not presently connected to onsepc.com, mainly because the current standard specifications do not allow for multiple ONS roots co-existence.

### 3. What has been done? What is going on?

As a first step, GS1 France, assisted by Orange Business Services, launched in April 2008 an operational ONS root platform for the European region[3] [ONS-EU].

Besides, GS1 France has already asked a group of industrial and academic R&D teams to study the specific issue of Multi-Root ONS Architecture and to submit solutions in order to move the standards forward, based on concrete proposals. Within this context, AFNIC's R&D team has recently submitted its own proposal.

The ONS may be viewed as an RFID/DNS *Convergence Service*, in the same way as ENUM is viewed as a Telephony/DNS convergence service. Consequently, there is probably a real opportunity for collaborations between both the DNS and the RFID communities. That would take place in different ways, such as:

- Sharing knowledge and know-how in their respective business fields;
- Putting together efforts to get better and more stable solutions for new challenging issues (e.g.: Multiple-Root systems, Discovery Services, etc.)

To that end, AFNIC signed a partnership with GS1 in April 2008 [AFNIC-GS1]. Informal collaboration had been undertaken several months before.

3 This platform was originally designed to be a French ONS Root Server, but after discussion and consultation with European GS1 Member Organizations, the scope of the platform was extended.

### 4. References


- [ONS] http://www.epcglobalinc.org/standards/ons
- [EPCIS] http://www.epcglobalinc.org/standards/epcis
- [DiscServ] http://www.epcglobalinc.org/standards/discovery , see also *Bridge European Project* website : http://www.bridge-project.eu/index.php/description-and-outcomes/en/
- [ESDS] Extensible Supply-chain Discovery Services, IETF working group under formation: http://www.ietf.org/mail-archive/web/esds/current/maillist.html
- [ONS-EU] http://www.gs1.fr/gs1_fr/actualites__1/informations__1/communiques_de_presse/communiques_de_presse_2008/gs1_lance_le_premier_service_de_l_internet_des_objets_en_europe
- [AFNIC-GS1] http://www.afnic.fr/actu/nouvelles/general/CP20081002_en

# CZ.NIC Association Launches a Number of Internet Community Projects

*by Ondřej Filip, CZ.NIC CEO*

In the recent years, CZ.NIC Association, administrator of the Czech national domain and ENUM domain, has dedicated itself more to projects intended for the Internet community.

At the beginning of last year the representatives of the association announced a successful migration of CZ.NIC's data into a new registration system. And moreover, it was announced that CZ.NIC was resleasing its system called FRED (Free Registry for ENUM and Domains) as an open source to serve the needs of other users and other national registrars.

The FRED system is an internal project of the CZ.NIC Association. Since 2006 the system has been used to administer ENUM domains; since 1 October 2007 it has also been used to administer the Czech national domain .CZ. FRED has been released as open source software under GNU GPL (General Public Licence). Those interested have the possibility to obtain this system, including the source code, at http://fred.nic.cz. They are allowed to use the software as they wish, modify it, and spread it further under the conditions determined by the GPL. The functioning of the FRED system is also based on other purely open source applications, such as Apache or PostgreSQL. Access to the registry is provided by the EPP protocol via a secured connection (SSL); the entire system is IPv6 ready, internally and externally. A number of global domain registrars have shown interest in using the system and providing cooperation upon its further development; at the June 2008 meeting of the ICANN Association in Paris, the administrators of the Angolan national domain announced that they would be using this Czech registration system for registering domains with .CO.AO and .IT.AO suffixes. According to our information the system is being tested and, in the near future, it will be rolled out. Beside the western Africa's Angola we have recently noticed great interest in this system also in Tanzania.

The FRED system website offers the source code for free use as well as system installation packages. All functions of the system may simply be put on trial using a test registry, which may be run from the boot CD (Live CD) on any computer.

Another interesting project is the "V.I.P. contest – Vyvíjej, Inovuj, Programuj" ("D.I.P – Develop, Innovate, Program") launched by CZ.NIC at the beginning of this October. In this contest young talents can test their abilities in the area of ICT.

The projects eligible to participate in the contest are those focused on the development of new open-source software or software innovation in the area of Internet technologies, services and infrastructure. The contest consists of several stages. First the contenders submit their projects proposals. An expert board selects those fulfilling the prescribed criteria. Then the implementation of selected projects begins, followed by their evaluation and awarding the winners with incentive monetary prizes.

This project aims to support talented programmers and gives them a change to see their effort materialize in a specific goal. This means, beside the financial reward, also a real possibility to implement the project in practice.

The output of another CZ.NIC project will be a book on the IPv6 protocol. This is being created in a unique manner. We have placed the skeleton text of the book on http://knihy.nic.cz, written by a college teacher and respected specialist on this issue in the Czech Republic. For over a month since this October those interested in networks have had the opportunity to express their opinions with respect to the individual parts of the book at the Internet address concerned. All readers have been allowed to attach their comments under the individual chapters. The author of the original text will eventually implement the comments, and the final version of the book will be available for free download. Those interested will also be able to order hard copies of the book. The book on the IPv6 protocol is the first publication issued by the Association. Next year we are planning to bring other expert publications to the Internet community from the area of the Internet and Internet technologies.

The last of the series of projects to be mentioned is "@kademie CZ.NIC". It aims at bringing information to those interested in the Internet, Internet technologies and news from this area not offered by similar courses in the Czech Republic. The courses are intended, above all, for members of the association, for secondary and college students and for all those who are interested in Internet technologies and wish to be well-informed in this area. "@kademie CZ.NIC" also features a laboratory equipped with state-of-the-art hardware and software, used for classes within the individual courses. Expert courses are concluded with a test, and each participant in "@kademie CZ.NIC" receives a certificate.

# About CENTR

*Peter Van Roste, General Manager, CENTR*

CENTR is an association of Internet Country Code Top Level Domain Registries such as .uk in the United Kingdom and .es in Spain. Full Membership is open to organisations managing an ISO 3166-1 country code top-level domain (ccTLD) registry.
CENTR has over 50 members which account for over 85% of the country code domain registrations world wide.

**CENTR secretariat**

The CENTR secretariat is based in Brussels and consists of Eveline De Waele (Office Manager), Wim Degezelle (Communications Manager) and Peter Van Roste (General Manager). For further information on CENTR's mission or membership, you can contact us at secretariat@centr.org.

*Peter Van Roste (General Manager)*

*Eveline De Waele (Office Manager)*

*Wim Degezelle (Communications Manager)*

AGENDA

# Forthcoming Meetings

| | |
|---|---|
| 29-30 January 2009 | Internet Governance at the Crossroads, Oslo, Norway |
| **11 February 2009** | **28th CENTR Legal and Regulatory workshop, Dresden, Germany** |
| 12-13 February 2009 | Domain Pulse, Dresden, Germany |
| 1-6 March 2009 | ICANN Meeting 34, Mexico City, Mexico |
| **18 March 2009** | **15th CENTR Administrative workshop, Barcelona, Catalonia, Spain** |
| **19-20 March 2009** | **38th CENTR General Assembly, Barcelona, Catalonia, Spain** |
| 22-27 March 2009 | IETF 74, San Francisco, USA |
| **May 2009** | **29th CENTR Legal and Regulatory Workshop, Jersey (tbc)** |
| **May/June 2009** | **16th CENTR Administrative Workshop (tbc)** |
| **3 May 2009** | **20th CENTR Technical Workshop, Amsterdam, the Netherlands (tbc)** |
| 4-8 May 2009 | RIPE 58, Amsterdam, the Netherlands |
| **4-5 June 2009** | **39th CENTR General Assembly, Malta** |
| 21-26 June 2009 | ICANN meeting 35, Seoul, Korea |
| 26-31 July 2009 | IETF 75, Stockholm, Sweden |
| **September/October 2009** | **CENTR Open Day, Brussels, Belgium** |
| **30 September 2009** | **17th CENTR Administrative workshop, Vilnius, Lithuania** |
| **1-2 October 2009** | **40th CENTR General Assembly, Vilnius, Lithuania** |
| **4 October 2009** | **21st CENTR Technical Workshop, Lisbon, Portugal (tbc)** |
| 5-9 October | RIPE 59, Lisbon, Portugal |
| 25-30 October 2009 | ICANN meeting 36, Sidney, Australia |
| 8-13 November 2009 | IETF 76, Hiroshima, Japan |

visit our website at
www.centr.org

www.centr.org