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

# ccTLDs,
## Active Players in the Local Internet Community

INSIDE
*Whois,*
*IDNs,*
*IPv6 and IGF explained*

# Index

# Domain Wire Editorial

Welcome to this new edition of CENTR's Domain Wire!

Whilst 2009 marked CENTR's 10th anniversary and provided ample opportunity to reflect on the achievements and challenges faced by ccTLD managers; 2010 focussed on laying down the foundations ahead of the next decade. In keeping with CENTR's missions as a place for exchanges in best practices and for increasing awareness about trends in the domain name industry, this edition of Domain Wire includes examples of CENTR's proactive role on the international scene, and also information about its members' involvement in building a better Internet at national level.

In 2010, CENTR once again actively supported the IGF. The workshop organised in Vilnius about "resilience and contingency planning in the DNS" was highly praised for providing both a multi-stakeholder view of these issues, and additionally for providing concrete examples of how these concepts were applied in extreme cases such as the recent earthquakes which struck the countries of Haiti and Chile. As a decision is about to be taken on the future of the IGF, CENTR is continuing in providing support to the forum and the multi-stakeholder approach. More information can be found about the IGF in this edition.

DNS Security remained high on the international agenda in 2010, and CENTR further contributed towards increasing awareness among its members and European stakeholders about such initiatives as the DNS-CERT, and the concerns raised by some community members. A joint session with Government representatives on this issue was held at the Brussels General Assembly and demonstrated that such concerns were widespread, even outside the strict scope of ccTLD managers.

A further focus of our edition is aimed at highlighting how CENTR members invest in their Internet communities. Whilst the standard states that "[ccTLD managers] act as a Trustee for the local Internet community" each member of CENTR has its own way of implementing this principle according to their size, culture, and mission. Examples range from Russia to Canada, Latvia to Catalunya. This edition of Domain Wire aims at providing an overview of how diverse and fruitful such initiatives can be, and illustrating that ccTLD managers do indeed take this mission very seriously.

We hope this edition will provide you with some useful information and ideas. Enjoy the read!

*Mathieu Weill*

*Chairman of the Board, CENTR*

# What is WHOIS?

*by Patrick Myles, Information Manager, CENTR*

## Facts and Background

**In the CENTR 2010 A-Level Survey it was noted that 44 out of the 47 'country code Top Level Domains' (ccTLD's) offered a WHOIS tool as a fundamental part of their registry operations[1].**

The appropriately named WHOIS protocol is a query/response tool which allows a user to perform a query on any particular domain or IP address and retrieve information on its owner. Depending on the Top Level Domain one is searching under, details such as the domain owner's name, address, email address and often much more information can be readily found. The extent to which data can be extracted from the database is dependent on the local terms and conditions of the TLD registry, local laws and often bound by third parties such as ICANN (Internet Corporation for Assigned Names and Numbers).
The WHOIS protocol's original specifications can be found in the RFC 954 which was created in 1985 and an update to RFC 812. The more current RFC 3912 is essentially the accepted standard to how the protocol works now[2].
The users (or clients) of WHOIS can be grouped into three areas: command-line clients, web clients and automated client applications. Originally all clients used the text based command line (usually Unix operating system) however currently the web based service is the most common.

## Thin vs. Thick

There are two essential 'types' of lookups in the WHOIS; thin and thick. Thick is a WHOIS server which stores complete WHOIS information from all the registrars for the particular set of data (so that one WHOIS server can respond with WHOIS information on all .org domains, for example). Thin refers to a WHOIS server that stores only the name of the WHOIS server of the registrar of a domain, which in turn has the full details on the data being looked up[3]. Different registries will have differing approaches to this however there has been some debate and discussion on the differences stating that a thin WHOIS could increase the risk for a registrant should a registrar go out of business of fail on a technical level. Generally ccTLDs adopt the thick approach[4], however this is not a standardised rule.

## Applications of WHOIS

1. To determine availability of domain names or check registration status
2. For network administrators to locate and repair any system problems
3. To aid in legal trademark infringements or combat misuses of the internet (eg. Fraud, spam etc)
4. To enhance accountability of domain name holders

## Users of WHOIS[5]

- **Network Operators**: To identify appropriate contacts regarding network problems associated with the domain. In the traditional sense, this involves discussing technical DNS errors, routing, and other fundamental operations; or for more contemporary reasons such as identifying the source of spam and network attacks.
- **Registries and Registrars**: To determine the availability of a domain name, to identify the contacts of whether a domain name is available. It is worth noting, registries and registrars usually have more specialised protocols and procedures for these purposes, rather than using the anonymous WHOIS service.
- **Business users**: Domain names have become essential to businesses and their marketing strategies; therefore WHOIS can become a useful competitive tool.
- **Intellectual Property interests**: As it stores personal data on the registrant, WHOIS can be used to quickly identify a domain name holder using the Internet to infringe on an individual or company's intellectual property rights.
- **Consumers**: Domain names are the first identifier of an e-commerce site. WHOIS data can potentially be used by consumers to make sure the company behind the site is legitimate.
- **Registrants**: Registrant can use WHOIS to determine whether a Domain name is available or not. Additionally, WHOIS can inform the existing Registrant on the identity of another Registrant of a similar domain.
- **Law enforcement personnel**: When a Web site is the instrument of a fraud, law enforcement personnel can try and use WHOIS database to find more information about the fraudulent party.

## Example of WHOIS search and response

Note: With the rising usage of security extension DNSSEC, there is also a field displayed whether or not the domain has had DNSSEC signed to it. Please see DNSSEC Issue Paper from CENTR for more information.

Domain ID:D2063208-LROR
Domain Name:CENTR.ORG
Created On:29-Sep-1998 04:00:00 UTC
Last Updated On:12-Jul-2010 13:27:37 UTC
Expiration Date:28-Sep-2015 04:00:00 UTC
Sponsoring Registrar:Network Solutions LLC (R63-LROR)
Status:CLIENT TRANSFER PROHIBITED
Registrant ID:20486664-NSI
Registrant Name:Council of European Nat'l TLD Registries
Registrant Organization:Council of European Nat'l TLD Registries
Registrant Street1:Belliardstraat 20
Registrant Street2:6th floor
Registrant Street3:
Registrant City:Brussels
Registrant State/Province:
Registrant Postal Code:1040
Registrant Country:BE
Registrant Phone:+32.26275550
Registrant Phone Ext.:
Registrant FAX:+32.26275550
Registrant FAX Ext.:
Registrant Email:secretariat@centr.org
Admin ID:20486662-NSI
Admin Name:CENTR Secretariat
Admin Organization:CENTR
Admin Street1:Belliardstraat 20
Admin Street2:6th floor
Admin Street3:
Admin City:Brussels
Admin State/Province:
Admin Postal Code:1040
Admin Country:BE
Admin Phone:+32.26275550
Admin Phone Ext.:
Admin FAX:+32.26275559
Admin FAX Ext.:
Admin Email:secretariat@centr.org
Tech ID:20486664-NSI
Tech Name:Council of European Nat'l TLD Registries
Tech Organization:Council of European Nat'l TLD Registries
Tech Street1:Belliardstraat 20
Tech Street2:6th floor
Tech Street3:
Tech City:Brussels
Tech State/Province:
Tech Postal Code:1040
Tech Country:BE
Tech Phone:+32.26275550
Tech Phone Ext.:
Tech FAX:+32.26275550
Tech FAX Ext.:
Tech Email:secretariat@centr.org
Name Server:NS1.OPENMINDS.BE
Name Server:NS2.OPENMINDS.BE
Name Server:NS3.0M-POWERED.NET
DNSSEC:Unsigned

## PRIVACY (PROTECTION OF DATA)

*At the beginning of November 2011, the European Commission set out a strategy to 'strengthen EU data protection rules'[6]. The intention is to (with the use of public consultation) revise the EU's 1995 Directive on Data Protection.*

### The Concerns and discussions

While there are been no express mention to the WHOIS protocol within the Data Protection Directive nor within this review proposal, personal data is covered and protected by the 1995 Directive on Data Protection and therefore encompasses WHOIS. Generally discussions have focused around the protection of private individual data as opposed to commercial or legal persons. Discussions have also moved around the topic of freedom of speech and basic human rights to which are under threat when personal data is available publicly.
To address the key concerns and provide advice to the European Commission on data protection issues, Article 29 of the Directive expressly sets up the 'Article 29 Data Protection Working Party. The group is formed by member state representatives who bring expert opinion from their respective member state and promote uniform principles in the Directives.

A document produced in 2003 by the Article 29 Working Group made specific mention to the WHOIS protocol calling for a better definition of the purpose/s of WHOIS. It noted that, the original purpose (technical) of the WHOIS must not be expanded upon unnecessarily and must not compromise data privacy. The document also highlighted the distinction between data provided by private individuals and that of business or legal persons. It was mentioned that (in reference to private individuals); "*...while it is clear that the identity and contact information should be known to his/her service provider, there is no legal ground justifying the mandatory publication of personal data referring to this person..* "[7]

The theme was again raised at the Internet Governance Forum (IGF) in Greece in 2006 where it was mentioned by the Non-Commercial Users Constituency (NCUC) that (with reference to the Data Protection Directive 1995); *"Allowing access to personal contact information by people not substantively involved in resolution of technical problems with Internet domains violates these provisions..."*[8] (the provisions being those found in the 1995 Directive).

These concerns on data privacy for individuals are also clouded because of a conflict between ICANN policy and other local laws (in this case EU law). Within the ICANN Affirmation of Commitments, it states (in reference to the WHOIS data);
*"... existing policy requires that ICANN implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing, and administrative contact information."*
Within Europe, many of the ccTLD Registries provide their own Registrar agreements which dictate WHOIS policy, however the European Registrars are often in conflict with ICANN policy under their Registrar Accreditation Agreements (RAA).
One noted example of a registry in the midst of uncertainty in this area is PuntCat who manage the namespace for .cat (the Catalan speaking Community). In September 2005, Fundació puntCAT entered into a Sponsored TLD Registry Agreement with ICANN. Within their agreement it states; *'Registry will select among ICANN-accredited registrars wishing to register domain names in .cat Sponsored TLD..'*[9] Herein lies the conflict as both parties (registry and registrar) are bound by the ICANN policy obliging certain disclosure of WHOIS data whereas the Directive on Data Protection essentially stating the opposite.

### Addressing the Conflicts

ICANN produced in December 2006 a 'Procedure for Handling WHOIS Conflicts with Privacy Law'[10] with effective date in January 2008. The document spelled out a 6-step procedure to be followed in cases of conflicts between local privacy law and ICANN policy ranging from notification, consultation, analysis and recommendation, resolution, public notice and ongoing review. The Article 29 Working Group responded to the report (among others) in referring again to the Data Protection Directive and once again emphasising the importance of distinction between legal and natural persons. The Working group suggested introducing a distinction between publicly accessible and publicly inaccessible data to combat the problems of potential conflict.

### Privacy and ccTLDs

More specifically to ccTLDs, many of the European ccTLD registries employ a method whereby registrants are able to hide certain elements of data provided upon registration of a domain (24 out of the 45 ccTLDs survey by CENTR in 2010 have this feature[11]). In the case of Nominet (the registry for .uk) for example, they call it an 'Opt out' feature. In this case, a non-trading registrant has the ability inform the registry they do not wish their address details to be displayed publicly. At other ccTLDs the equivalent feature may mean data such as name, email, telephone, fax or even all details are not displayed publicly at the request of the registrant. In these cases, one could argue that the 1995 Directive on Data Protection is being adhered to. However the choice of hiding data is as it states; a choice. And in addition to that, it is not offered by all ccTLDs.
During the ICANN meeting in Seoul 2009 a list of recommendations supported by various international law enforcement bodies was given. Within the recommendations, it was stated in reference to WHOIS;
"Although LE does not support the use of proxy/privacy registrations, the LE agencies urge ICANN to exercise the following on proxy/privacy registrations:

a. *The proxy/privacy registrant is a private individual using the domain name for non-commercial purposes only, and;*
b. *The proxy/privacy registration service has been accredited by ICANN using the same due diligence process as a Registrar/Registry, and;*
c. *Information from the WHOIS database can be provided to law enforcement authorities when the information will assist in the prevention, detection, investigation prosecution or punishment of criminal offences or breaches of laws imposing penalties, or when authorised or required by law."*[12]

Although the above recommendation was made specifically with gTLDs as the focus, the principal is the same for ccTLDs and has even been expressly mentioned recently by the registry for .ru who intends to adopt the principals set out in Seoul. Also in the previous example of Nominet, one of the main criteria for 'opting out' is that the registrant must not be trading (commercial).

## Accuracy and Verification of Data

It is generally accepted that the data found in the WHOIS is not and should not be the responsibility of the registry running a ccTLD. The case is a little different for gTLDs to whom are again bound by ICANN policy which is uniformed and has specific provision for the attainment of accurate data in the WHOIS.

On the side of ccTLDs, various terms and conditions are used within registrar contracts to ensure the burden of responsibility of data accuracy is borne by the providers of WHOIS data. Having said this, a ccTLD registry does have a vested interest in ensuring accuracy of data due to the adverse outcomes inaccurate data could have. For example, if a registrant's contact details are missing or false when a phishing attack or site hijack has been detected, the registry may encounter problems when 'taking down' the site and potentially run into legal claims.

Several surveys and studies have been carried out on WHOIS accuracy and discussions are regularly held between ccTLD registries which highlight their own particular experiences, concerns and methods of combating potential issues. Generally the feeling is that there are indeed problems of data accuracy and that they do have a social responsibility to address them. In a survey conducted between April and May 2010 via CENTR and lead by the Co-ordination Centre for TLD RU (.ru) it was noted that out of 24 European ccTLDs only 6 perform verification checks (4 of those pass the information to the registrar). Of the 14 remaining TLDs who do not run a verification process, a majority do have in place a process of dealing with claims of false domain holder contact data.
On the side of gTLDs, a 2009 WHOIS accuracy study from NORC (National Opinion Resource Centre) and commissioned by ICANN showed that only 23% of the records in the sample were fully accurate (using a strict interpretation of criteria/ definition of accuracy)[13] however twice that number met a more relaxed version of accuracy. Overall around 70% of the sample had some form of contact.. Similar outcomes have been found on ccTLD surveys which suggests verification of data is not being achieved as well as it could be.

## DEVELOPMENTS IN WHOIS

### WHOIS searching

The PRPSS service (Public Registry Search Service) at Nominet is an innovative use of the WHOIS data which serves a more select group of users. The service allows for the search of the register of names registered to a particular legal entity and/ or of a similar name. Through this specialised service, users can (among other things) establish intellectual property rights, assist academic research or investigate criminal offences. The service does come at a cost of around 400 GBP which means it's found more in the use of for example large registrars, Intellectual Property companies and Law Enforcement agencies.

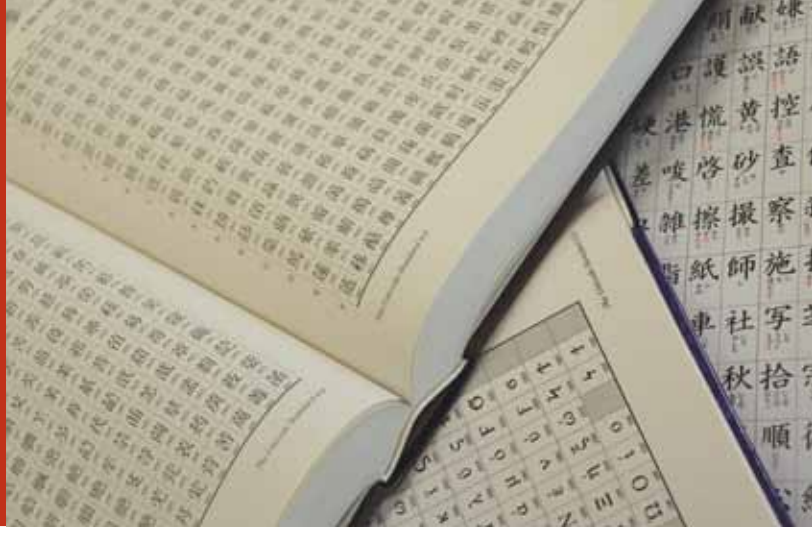
### 'CAPTCHA'

One of the threats to WHOIS is spamming via data harvesting. This is when plain text email addresses are 'harvested' from WHOIS databases and mass unsolicited emails are then sent out. To reduce this, the rate-limiting system, CAPTCHA is used frequently by TLDs. This tool is a challenge-response test to ensure that information provided is not given by a computer. See below screen shot for an example of CAPTCHA on a WHOIS search under the Eurid Registry (.eu) for www.eurid.eu. The graphical image is the CAPTCHA requesting the user to reproduce the text into the box.


1 Source: CENTR 2010 A-Level Survey (members only)
2 RFC 3912 (with links to obsolete RFC 954 and 812): http://tools.ietf.org/html/rfc3912
3 http://en.wikipedia.org/wiki/Whois
4 WHOIS – REGISTRY PERSPECTIVE VIEWS FROM AROUND EUROPE: https://www.centr.org/main/3401-CTR/version/6/part/12/data/Whois-RegistryPerspective.pdf?branch=main&language=default
5 CENTR WHOIS Paper with Article 29 comments 07/01/08 (members only)
6 WHOIS – REGISTRY PERSPECTIVE VIEWS FROM AROUND EUROPE: https://www.centr.org/main/3401-CTR/version/6/part/12/data/Whois-RegistryPerspective.pdf?branch=main&language=default
7 http://ec.europa.eu/justice/news/intro/news_intro_en.htm#20101104
8 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp76_en.pdf
9 Contribution Memorandum: Privacy Implications of WHOIS Database Policy (Non-Commercial Users Constituency (NCUC))
10 .cat TLD Sponsorship Agreement -Appendix S, Part V http://www.icann.org/en/tlds/agreements/cat/
11 http://www.icann.org/en/processes/icann-procedure-17jan08.htm
12 Source: CENTR 2010 A-Level Survey (members only)
13 Draft Report for the Study of the Accuracy of WHOIS Registrant Contact Information – pg 14 (http://www.icann.org/en/compliance/reports/whois-accuracy-study-17jan10-en.pdf) Full accuracy criteria: deliverable address, name linked to address, and registrant confirmed ownership and correctness of all details during interview

# IDN Top Level Domains

*by Peter Van Roste, General Manager, CENTR*




## Summary

**This paper aims at introducing the reader to Internationalized Domain Names (IDNs) and providing an overview of the reasons why the implementation of IDNs was necessary. It also explains the different processes that lead to their introduction in the Domain Name System (DNS) root zone and provides an overview of the current situation.**


## What are Internationalized Domain Names and why are they needed?

At the time of the introduction of the Domain Name System, designers of the DNS (and its predecessor, the "host.txt" file) wanted to allow for non-ASCII[1] characters to be used within the system, but the technology in use at that time was simply not powerful enough to accommodate this[2]. Additionally, the group of users was well defined and restricted: users of ARPANET and its successor were, well into the eighties, mainly US academics or research institutions. Even with the increasing internationalization of the web, those users had one thing in common: they used English to communicate and therefore had no other needs than the ASCII characters (Basic Latin script, Arabic numbers 0-9 and the hyphen) to create and use these humanly meaningful addresses (or domain names).

With the global deployment of the Internet and the exponentially increasing user base, English was still used as the Lingua Franca, but it became clear that the technical restriction which limited the characters that can be used in one script became a significant obstacle for large communities of users in e.g. the Arabic region, China, Indonesia or India. This limitation made it very difficult or even impossible for those users to connect with and interact over the web.

In response to such technical restrictions, these communities developed mechanisms that could partially overcome this hurdle by introducing hybrid domain names. While the root zone still only held ASCII-based top level domains, some of the registries operating those top level domains introduced the possibility of making use of different scripts in the second and third levels. Internationalized Domains Names are domain names that include or consist of different scripts such as Cyrillic, Hangul or Arabic.

This solution was however not regarded as satisfactory as it indeed led to a number of problems[3].

- Complexity of typing: Hybrid names still required the user to switch keyboards when typing in a domain name
- Confusion over label order: As some scripts are right-to-left, the direction could switch in a domain name.
- Ambiguity of visual appearance of different domain names: Different domain names could look identical depending on the input mechanisms of the application (e.g. browser).

The technical community – united within the framework of the Internet Engineering Task Force – initiated work on standards for Internationalized Domain Names in Applications (IDNA) in 2003. These standards[4] provide technical guidelines for the deployment of IDNs and describe a translation mechanism able to translate any standard script (or more precisely its Unicode equivalent) into a valid DNS character set. It should be noted that these technical guidelines are currently only applicable to the Domain Name System and do not provide a solution for other protocols[5]. With the additional introduction of ICANN's guidelines for IDN implementation[6] on the second level, the technical requirements were in place for the full introduction of non-ASCII characters in the DNS. In April 2007, the ICANN Board endorsed version 2.2 of the implementation guidelines which made these guidelines also applicable to the top level[7].

## The difficult road to IDNs in the Root

During initial discussions within the ICANN community, it became evident that full deployment of IDNs in the

root zone would take much too long to accommodate the immediate needs of the communities requiring these. While the technical standards were in place, the policy and political aspects of the introduction of IDNs were still quite complex and subject to long debates within the ICANN community. To name just a few:

- Which registries would be allowed to manage the new top level domains?
- Would the name of country X in a script that is not used in country X be assigned to country Y that is using that script? (E.g. would "Sweden" in Chinese be managed by a Swedish registry or by a Chinese registry?)
- How could political struggles between countries or territories be avoided for identical names?
- How could confusion be avoided between names that looked similar to the end-user even though they were written in different scripts[8]?
- How could could it be possible to avoid undermining accessibility of the Whois tool through the use of dozens of different scripts?

The final push for the introduction of IDNs came from the imminent threat that the Internet could break down in different zones, handling different scripts. It was expected that in particular the Russian Federation, the Arabic region and China would not continue to endlessly wait until their scripts were allowed in the DNS. This would have led to a scattered DNS and could have signaled the end of the Internet as we know it.

Answering calls from the Government Advisory Committee (GAC) and the country code Name Supporting Organisation (ccNSO), the ICANN Board agreed to split the introduction into two phases: a fast-track process with limited scope to fulfill the near-term demand and a regular Policy Development Process (PDP) that meet the long-term demand of those that did not qualify for the fast-track process[9]. In addition to the introduction of country names, the introduction of generic IDN names (such as .car or .com in non-latin scripts) will take place under the New gTLD Program.

1. IDN ccTLD Fast Track process
   The ICANN Board approved the implementation plan on October 30th 2009. The process was launched on November 16th 2009. The application was conditional upon fulfilling the following criteria:
   1. Access to the Fast Track process is restricted to countries or territories that appear in the ISO 3166-1 list[10].
   2. Every application needs to be accompanied by demonstrated community support
   3. Applied for strings need to be meaningful representations of the corresponding country or territory name
   4. Applied for strings should not be confusingly similar to existing strings[11]

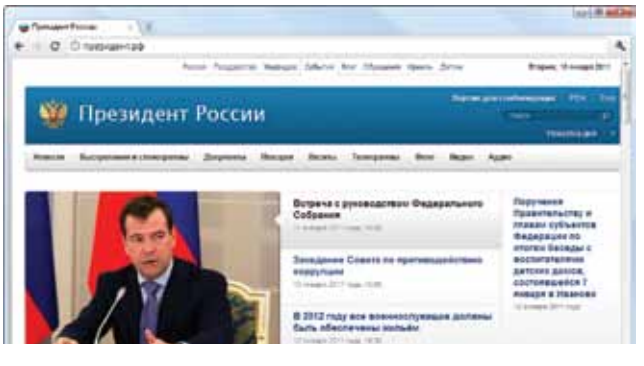
On 18 January 2011, 16 IDN ccTLDs have been inserted in the DNS root zone following a successful application under the Fast Track process:

- China (Simplified Chinese):.中国
- China (Traditional Chinese): .中國
- Egypt: .مصر
- Hong Kong: .香港
- Jordan: .الاردن
- Occupied Palestinian Territory: .فلسطين
- Russia: .рф
- Qatar: .قطر
- Saudi Arabia: .السعودية
- Sri Lanka (Sinhalese):. .ලංකා
- Sri Lanka (Tamil): .இலங்கை
- Taiwan, province of China (Traditional Chinese): .台灣
- Taiwan, province of China (Simplified Chinese): .台湾
- Thailand: .ไทย
- Tunisia: .تونس
- United Arab Emirates: .امارات

A striking example of the need for IDN ccTLD names is the very successful introduction of the Cyrillic equivalent to .RU - .рф. Since its launch on 11 November 2010, more than 700,000 domain names have been registered. Compared to the 3 million domains under .RU (operational since 1994) this demonstrates the significant potential to include users that have previously been left out.

Cyrillic Domain Name: президент.рф
ACE conversion: xn--d1abbgf6aiiy.xn--p1ai

This is the official website of Russian Presidential Executive Office (Administration)



## IDN ccTLD Policy Development Process

For those country code top level domains that do not meet those criteria, the country code name supporting organization (ccNSO) is developing a policy that will allow the introduction of all country names in all scripts. This program will take due account of the lessons learned from the Fast Track process. The new policy will also address some of the organizational questions that are raised with the introduction of IDN ccTLDs (e.g. what is their voting status in the ICANN multi-stakeholder model?).

## Generic IDNs and the New gTLD Program

For those TLDs which do not represent a country name, non-ASCII scripts will be introduced at the same time as the ASCII new generic domains (e.g. the equivalents of .com in simplified Chinese or .car in Kanji). This introduction will be subject to the New gTLD Program. The New gTLD Program focuses on offering a wider span of choice for generic top-level domains, or gTLDs. This expansion includes IDNs at the top level and is required so as to meet growing diversity and encourage competition for more innovation, choice and change to the Internet's addressing system. ICANN is developing both a process for registries to apply for new gTLDs and an Applicant Guidebook that takes applicants through the process and explains the implications of the many complicated issues surrounding these new top-level domains. The Internet community is currently working on resolving string contention, protecting intellectual property rights, handling internationally recognized issues of morality and public order, and the geographical naming process, inter alia. Following completion of several rounds of public comment, the process and the guidebook are expected to be fully approved and ready for implementation at the end of 2011. At the time of writing, only a couple of issues are still open for debate. Contentious issues such as the questions on protection of intellectual property rights have been closed for debate. The ICANN Board and the Government Advisory Committee are meeting in February 2011 to solve the remaining issues on geographic names (e.g. how to handle an application for .holland) and issues of morality and public order (e.g. how to handle an application for .god).

## The Future

While the exact date for the introduction of new gTLDs in unclear, it is expected that by mid-2012 the number of TLDs (currently standing at just over 300) will have increased significantly. An important part of that increase can be attributed to the introduction of IDN TLDs. At the time of writing 16 IDN TLDs have been added to the root zone, and more will be added soon (Oman, India - with 7 scripts, Morocco, Serbia, Islamic Republic of Iran, Syrian Arabic Republic and Algeria). As the introduction of the Cyrillic. рф has demonstrated, one can expect that a well managed IDN TLD will succeed in unleashing the enormous potential of those user communities that have so far been deprived of convenient access to the World Wide Web.

---

1 ASCII is a common numerical code for computers and other text handling devices. Computers can only understand numbers, so an ASCII code is the numerical representation of a character such as 'a' or '@'. When mentioned in relation to domain names or strings, ASCII refers to the fact that before internationalization only the letters a-z, digits 0-9, and the hyphen "-", were allowed in domain names.

2 Internationalization of Domain Names: a history of technology development.; Klensin, J. and Fälström, P.; http://www.isoc.org/internet/issues/docs/i18n-dns-chronology.pdf

3 A detailed overview of these difficulties can be found in "Internationalized Domain Names: The Long and Winding Road"; Benny Lipsicas, Doron Shikmoni; Domain Wire 2007; p7-11 https://www.centr.org/main/domainwire/3656-CTR.html

4 These are RFCs 3454, 3490, 3491, and 3492 - now obsolete by the introduction of RFCs 5890 and 5891

5 IDN usage in emails—or, more specifically, in the domain name part of the email address—is not yet fully available. The technical standard that will make this possible is being developed by the Internet Engineering Task Force.

6 These guidelines are applicable to second level domains. http://icann.org/topics/idn/implementation-guidelines.htm

7 Version 2.2 of the ICANN IDN implementation guidelines: http://www.icann.org/topics/idn/idn-guidelines-26apr07.pdf

8 The standard example is "www.paypal.рф" which is a full Cyrillic domain name but looks identical to the hybrid "www.paypal.рф". This would make the system vulnerable to fraud.

9 A full overview of the Fast Track process is available at: http://www.icann.org/en/topics/idn/idn-activities-seoul-28oct09-en.pdf

10 This list is maintained by the International Organization for Standardization, it can be consulted at: http://www.iso.org/iso/country_codes.htm

11 The notorious case (which was refused) is the application by Bulgaria for the Cyrillic version of .BG (.БГ) which was deemed to be confusingly similar to the Brazilian extension .BR (equivalent to .br or .Br)

# IPv6

*by Wim Degezelle,*
*Communications Manager, CENTR*

**News articles, presentations, and government documents, are all making an urgent appeal to adapt the Internet so as to cope with its growth. "The Internet is running out of IP addresses and if no immediate action is taken now, further growth will be impossible", they claim.**

This alarming message must be taken seriously. But, there is no need to panic, the Internet is not at risk and will not stop working. There is no bug or threat that has to be fixed; however, changes are needed to guarantee the continuous steep growth of the global network.

This article explains why the changeover from IPv4 to IPv6 is needed and outlines the primary difficulties in this changeover.

## Setting the scene – internet growth

The Internet has undergone exponential growth since it opened for commercial activities in 1992, and continues to grow relentlessly. By the end of 2010, almost 2 billion people already used the Internet, but it is still less than one third of the global population.[1] More and more users are going online, since efforts are being taken to connect developing countries and rural areas and much money is being invested in increasing the broadband penetration of fixed and mobile networks.

A further development lies in the fact that more and more devices are being connected to the network. Today, using your mobile phone to access the Internet is no longer exceptional. We're all familiar with sharing a printer on our home or office network but there are also many other devices, such as TV sets, games consoles, etc. that can be connected and used over the network. The next step is that devices will be able to communicate with each other without human intervention. This evolution goes further and some of the plans that are currently on the table of engineers, go beyond even the wildest of imaginations, for example an indigestible chip which is activated by stomach acid and communicates via a patch on the skin with your smart phone.[2]

## IP addresses ... the unique identifiers in the network

Any device which wants to communicate with other devices on a network requires a unique identifier. This identifier tells other devices how to find the device they want to communicate with. Hence, this identifier is the '*address*' of the device on the network. Without this address, it wouldn't be possible to communicate – send or/and receive information – with the device.

The IP allocation process

Initially all IP addresses are held in the so called Unallocated Address Number Pool, which is administered by the IANA (the Internet Assigned Numbers Authority).
Large blocks of addresses are then allocated to the five Regional Internet Registries (RIRs), AFRINIC, APNIC, ARIN, RIPENCC and LACNIC, each of them responsible for a geographical area.

The RIRs allocate the IP addresses in smaller blocks to those who need them, including Internet Service Providers (ISPs).

The allocation from IANA to RIR to ISP, is carried out on the basis of demonstrated need: there is no pre-allocation.
When the local pool reaches a low threshold size a further address block is allocated by IANA to the RIR.

On the Internet, the numerical string used to identify devices is called an IP address. You'll also say that the Internet is an IP-based network. IP stands for 'Internet Protocol'. A *protocol* is a set of rules that describe how to communicate on the network. Every device using the Internet has an IP address.

The information that is sent over the Internet is divided when it leaves the sender and is assembled again when it arrives at the destination. So if you receive an email or download a picture form a website, this information does not come to you as one email or a full picture, but as a number of small chunks called packages each containing a small portion of the entire email or picture.

Each package of information also contains a destination address and the address of the sender so that it finds its way over the network to its final destination.

## IPv4 and IPv4 exhaustion

The current and much widely used version of the Internet Protocol was developed in the mid 1970's and is called IPv4, which stands for Internet Protocol version 4. IP addresses in IPv4 are written as four decimal numbers separated by dots. These numbers can range from 0 to 255. For example 88.151.243.60 is a valid IPv4 address[3].

The popularity of the internet today, and as a result the high consumption of IP addresses, was certainly not foreseen in the 1970's. As explained above, an ever growing number of computers, laptops, mobile phones, etc all require IP addresses.

And the development continues further with televisions, network printers, games consoles, etc. all using the internet network.

It is much cheaper and easier to embed the IP protocol into new applications when they are being developed than inventing and implementing a new communications protocol.

It might come as a surprise, but as a result of all of the new applications available, major growth of the Internet happened AFTER the Internet "boom" between 1999 and 2001. For example, the world's IP address consumption peaked in 2010 at a new all-time high of an equivalent rate of 243 million addresses per year.[4] Since the total number of possible unique IP addresses in IPv4 is 4,294,967,296 it is quite obvious that at such a consumption rate, the IPv4 address space is at risk of being depleted.

## When will IPv4 run out?

In a recent article[5] Geoff Huston, Chief Scientist at APNIC predicted that 'As of September 2010 there are some 151 million addresses left in the general pool of unallocated addresses that are managed by the central pool administration, the Internet Assigned Numbers Authority (IANA).'

Based on this consumption rate, the IANA will exhaust its address pool in the first half of 2012. In fact there is an agreement between IANA and the five Regional Internet Registries (RIRs) that each of them will get one of the last five IPv4 address blocks.

At that time, the Regional Internet Registries (RIRs) will still have pools of addresses available, but IANA will be unable to provide any further addresses when their pools are empty. The pace of IP consumption differs between different continents (see box). As a result, a shortage of IPv4 addresses will fall sooner in some parts of the world.

In summary, IPv4 exhaustion will go through three different stages:

- **Stage 1**: The Internet Assigned Numbers Authority (IANA) will run out of unused IPv4 address space for allocation to the five RIRs

| IPv4 address consumption 2010 | |
|---|---|
| AfriNIC | 8.95 million |
| APNIC | 126.22 million |
| ARIN | 54.55 million |
| LACNIC | 17.29 million |
| RIPE NCC | 75.45 million |

- **Stage 2**: The RIRs will run out of unused IPv4 address space to allocate to their members
- **Stage 3**: Local Internet Registries (LIRs) that are using IPv4 space already allocated to them from the RIRs will run out of unused IPv4 address space to assign to their customers (End Users)[6]

Even when IPv4 addresses can no longer be allocated, this does not mean that the Internet will stop working. The addresses already assigned will be used and will continue to work. Yet, the growth and also capacity for innovation in IP-based networks would be hindered.

## After IPv4 comes IPv6

As early as the beginning of the 1990's, Internet engineers realised that at one point in the future the total number of available IP addresses would be depleted. In January 1995, after having examined different proposals the IETF settled on a successor to IPv4, the protocol called IPv6 (RFC1752)[7]. IPv6 addresses are longer so that more unique combinations can be made.
In theory[8] there are 340,282,366,920,938,463,463,374,607,431,768,211,456 unique addresses possible using IPv6.
An IPv6 address is represented by 8 groups of hexadecimal values separated by colons (:).
A typical example of an IPv6 address is 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

## Transition to IPv6

Unfortunately the transition to IPv6 requires that the entire network and all devices linked to it be adapted to the use of IPv6. There is no so-called 'backward compatibility' between IPv4 and IPv6.
Devices using IPv4 cannot communicate with devices using IPv6. In such a case, the IPv4 network could remain in place while all new devices are able to function using IPv6.

This creates major challenges because there is a transition phase during which both devices using IPv4 and devices using IPv6 will be operating simultaneously on the network. Without interim solutions it is not possible for these to communicate. It is even possible to say that there are two separate networks, one for IPv4 devices and one for IPv6 enabled ones.

Luckily, engineers have found ways to make it possible for IPv4 and IPv6 enabled devices to communicate over the Internet. There are different techniques. 'Dual-stack' techniques allow IPv4 and IPv6 to co-exist in the same devices and networks[9]; 'Tunnelling techniques' encapsulate IPv6 packets inside IPv4 packets[10]; 'Translation techniques' allow IPv6-only devices to communicate with IPv4 only devices.
However, such solutions all have their limitations; some techniques can only be used in very limited contexts. There seems, therefore, to be no other solution than to implement IPv6 across the entire network as soon as possible.

## Action needed!

The transition to IPv6 needs to be completed throughout the whole network. A billion end hosts, hundreds of millions of routers, firewalls and middleware units need to be verified and prepared. At this moment, most of the major servers software support IPv6 (Apache, LiteSpeed, BIND, etc) . But, for example, hosting a website via IPv6 also requires IPv6 support in the underlying software. Without patches and adjustments from vendors and software developers, supporting software such as the email server may not be able to provide IPv6 functionality.

According to NRO, the organisation of the RIRs, we are on track. 'Approximately 90% of end-users have computer operating systems that work seamlessly over IPv6. This means that many home and small business users are simply waiting for their service providers to offer IPv6 connections.'

### *Trading IPv4 addresses*

It is likely that when the IPv4 addresses become more scarce they will increase in value and a market to trade IPv4 addresses will arise. The higher the value of an IPv4 address, the higher the incentive to organisations to sell addresses they are not using. The RIRs, however, are rather sceptical about the emergence of such a secondary market.

A and AAAA records

The IPv4 address is stored in an "A" record while an IPv6 address is stored in an "AAAA" record. This name was chosen to clearly show that an IPv6 address is four times the length of an IPv4 address.
It is possible to publish both A and AAAA records. Systems with IPv6 connectivity will first check for an IPv6 AAAA record and try to connect and then fall back to an IPv4 record if IPv4 connectivity is available and IPv6 not.

Publishing an AAAA record is the last step once all other software is ready to serve content via IPv6. Otherwise the content will be inaccessible.

### *Recycling?*

The RIR or IANA could actively try to reclaim already allocated address blocks that are not fully used. However, there is no apparent mechanism for enforcing the return of unused addresses. It is possible that the cost of such an operation would far outweigh the additional lifetime it would bring to the pool of available addresses.

### *Or another solution?*

IPv6 transition technology is still a hot topic. 'There were 66 IPv6-related proposals tabled for the IETF in Beijing [November 2010] in various working groups, not only the classical IPv6 working groups but also those looking into transition technologies'[11]
Trading and recycling might extend the final deadline for the IPv4 exhaustion but will not alter the face of the problem. Adoption of IPv6 is not an 'if'-question but rather a question of when.

## Conclusion

The transition to IPv6 is necessary and inevitable because the exhaustion of IPv4 addresses puts a burden on the growth of the Internet.

Since IPv4 and IPv6 are not compatible, the transition has to be complete. During the transition period measures are taken to enable IPv4 and IPv6 devices to communicate with each other. However at one point in the future, when a critical mass has changed to IPv6, IPv4 will no longer be supported.
For the end user, the transition should be seamless and unnoticeable.

1 http://www.internetworldstats.com
2 Ipv6 inside everything and everybody, http://www.circleid.com/posts/20101115_ipv6_inside_everything_and_everybody/
3 88.151.243.60 is the IP address corresponding with www.centr.org
4 Geoff Huston
5 http://www.potaroo.net/ispcol/2010-09/exhaustguide.html
6 http://www.ripe.net/info/faq/IPv6-deployment.html#v6
7 Note: the reason for immediate transfer from IPv4 (Internet Protocol version 4) to version 6 is that the terminology IPv5 was already being used in the 1990's for an experimental version of the Internet Protocol (the Internet Stream Protocol, Version 2 (ST-II), RFC1190) intended to support sound, video and voice communication.
8 In practice the IPv6 address plan creates much less usable space . It is expected that the IPv6 space will encompass between 250 to 260 usable addresses which is still between 1 million and 1 billion times the size of the IPv4 address space.
9 In fact with dual stack, a system has both a public IPv4 and IPv6 address and connects through a provider that makes both protocols available from the system all the way to the internet
10 With tunnelling, a request is routed through a special server with access to both protocols. The server converts the request and also relies on the response back. Tunnelling is not an optimal solution because it adds a delay an overhead relying all communications trough a third party, put it permits connection between an IPv4 and IPv6 device.
11 CENTR Report on the IETF 79, https://www.centr.org/main/lib/g5/5991-CTR.html .

## FURTHER READING

IPv6 Deployment Monitoring website - daily updated overview of the IPv6 deployment in Europe: http://www.ipv6monitoring.eu/

NRO – the organisation of Regional Internet Registries: http://nro.net/

IPv6 Act Now: http://www.ipv6actnow.org/

IPv6 Tutorial: http://www.ripe.net/ripe/meetings/ripe-43/tutorials/ripe43-ipv6-tutorial.pdf

# An introduction to the Internet Governance Forum

*by Emily Taylor for CENTR*

**This CENTR issue paper aims to provide a clear explanation of the origins, the importance and relevance of the IGF to CENTR members. It tracks the different ways in which CENTR has supported and interacted with the IGF, and finally looks ahead at its likely future.**

## Origins of the Internet Governance Forum

The Internet Governance Forum was set up by the United Nations through its World Summit on the Information Society (WSIS) in 2005[1]. Originally, the WSIS had the goal of building "a people-centred, inclusive and development-oriented information society"[2]. In reality, the WSIS process was characterised by deep divisions over the management of the domain name system, particularly the US Government's contractual relationship with ICANN, and its role in authorizing changes to the domain name root database.

The issue proved so divisive that it threatened to derail the WSIS process. In this context, the Internet Governance Forum (IGF) was set up with a 5-year mandate in an attempt to diffuse tensions. The Internet Governance Forum has the following key features:

- Multistakeholder. Usually, UN processes are governments only. In the IGF, all stakeholders participate on an equal footing.
- Non-decision making. The IGF does not produce resolutions or declarations. Its role is to provide an "interactive, collaborative space where all stakeholders can air their views and exchange ideas".[3]

## Why is the IGF important?

The Internet has revolutionised the way people communicate with each other, particularly communication across national borders. In regulatory terms, the Internet differs from traditional communication systems, in that the Internet's governance *"has evolved as a network of institutions that brings experts, stakeholders and public interests together in a system that is controlled by no one but open to everyone. It's an innovative, although not necessarily perfect, new approach to global governance of vital assets"* (Carl Bildt, New York Times, 2005).

The Internet developed so fast that no global system to govern it could keep pace. Moreover, the nature of the Internet, with a diversely owned infrastructure, low barriers to creating/publishing content, or setting up as an Internet Service Provider, challenged traditional regulatory models based on a top-down license-and-control paradigm. For governments which favoured a free-market, light-touch regulatory approach, such as the US and some EU states, the disparate nature of the Internet was a key contributor to its innovation, and helped to underpin freedom of expression online. For others, including some totalitarian states, the openness of the Internet's governance, including its naming and addressing posed a potential threat to their regimes.

During the early part of the WSIS process, there was a wide spectrum of awareness amongst government negotiators about how the Internet works, and what regulatory interventions or structures would be feasible or desirable.

Whilst discourse within the WSIS tended to assume that there was a single model for domain name registries, in fact each ccTLD is each organised according to national laws, and there is a rich variety of models – including government run, private sector not-for-profits, and academic institutions. There was a risk that ccTLDs' local determination would be compromised through the absorption and centralisation of decision-making or regulation into the United Nations, or for greater intergovernmental oversight/regulation of ICANN.

One of the key aspects of the WSIS and IGF processes has been the rivalry between ICANN and the ITU. The ITU was rumoured to have ambitions take over the management of the domain name system, although this has been consistently denied by the UN Secretary General[5] and the ITU leadership[6]. Such a move would have transferred ICANN's coordination role into an intergovernmental structure. For some, this would be a more familiar, structured regime than ICANN, which was viewed as a chaotic environment in which governments' role was marginal and their advice sometimes disregarded. Opponents of change argued that non-governmental, key players in Internet Governance (eg many ccTLDs) would have no place at ITU as of right, and would lose the ability to influence issues relating to Internet infrastructure. The Internet Governance Forum's creation recognised that non-governmental actors had an important role in the Internet's development, and that there was a need for deeper understanding of the issues before creating or adapting institutional mechanisms to regulate it.

## What is the IGF's relevance for ccTLDs?

ccTLDs had an interest in making the IGF work. Throughout the WSIS, the contentious issue was the domain name system and its management. Therefore, for ccTLDs, part of the domain

## JARGON BUSTER

| | |
|---|---|
| **ccTLD** | country code Top Level Domain, eg .de, .es, .fr, .uk |
| **CENTR** | The Council for European National Top Level Domain Registries, the European regional ccTLD organisation www.centr.org |
| **ICANN** | Internet Corporation for Assigned Names and Numbers. ICANN is the global coordinator of the domain name system www.icann.org |
| **IGF** | The Internet Governance Forum, established by the United Nations 2005 www.intgovforum.org |
| **ITU** | International Telecommunications Union, the leading United Nations agency for information and communication technology issues, eg radio spectrum, telecommunication infrastructure, and interconnection standards www.itu.int |
| **MAG** | The Multistakeholder Advisory Group to the IGF, established by the UN Secretary-General. Its purpose is to assist the Secretary General in convening the Internet Governance Forums. It comprises 56 members from governments, private sector and civil society, including representatives from the academic and technical communities www.intgovforum.org/cms/magabout |
| **UN** | United Nations |
| **WSIS** | The United Nations' World Summit on the Information Society, 2003-2005 www.itu.int/wsis/index.html |

name ecosystem, unless the IGF was viewed as a success, there could be a fundamental change to the way that the domain name system was organised or regulated.

The Internet Governance Forum also provided an opportunity for ccTLDs to educate other stakeholders about the diversity of structures, and how effectively ccTLDs had developed to serve their local Internet communities. Whether government run, licensed or self-regulated, each ccTLD within the CENTR region was structured and defined its policies in a unique way according to the needs of its local community.There were numerous similarities between the CENTR community and the IGF. For example, like many Internet organisations, CENTR had always had a multi-stakeholder approach, reflecting that its member ccTLD managers came from both private and state sectors. There was also an emphasis on lightweight structures and information – best practice – sharing rather than negotiated decision-making.

## How is the IGF financed?

The IGF is not funded from the regular UN budget, but is funded through voluntary contributions by multistakeholders, from government, private sector and technical community actors. Throughout the IGF's initial 5 year term, the technical community has been generous in its support of the IGF, through donations in cash, in kind, and participation in meetings. Eight CENTR members are listed as IGF donors[7].

## How has CENTR interacted with the IGF?

Since the beginning of the IGF, CENTR has played a leading role in coordinating ccTLD involvement in the IGF in collaboration with other regional ccTLD organisations. It has organised ccTLD workshops at every IGF. The workshops provided a strong technical community contribution to best practice and information sharing within the IGF. The 2007 workshop "The Functioning of the Domain Name System" is included in the IGF's inventory of good practices[8]. Others were presented under the theme of Critical Internet Resources.
There is a CENTR IGF working group which has been active in developing workshop proposals, and identifying speakers, and coordinating with other regional ccTLD organisations.

## What will be the IGF's future?

The Internet Governance Forum's 5 year mandate expires at the end of 2010. During 2009, the United Nations organised a consultation with stakeholders on the continuation of the IGF.

87% of the stakeholders who responded to the consultation favoured continuation of the IGF in its current form, or with minor tweaks[9]. Many noted the IGF's flexibility, its responsiveness to change, which had enabled evolutionary improvements to be made throughout its lifespan without the need for external intervention. CENTR members supported the continuation of the IGF in its current format, with a lightweight, Geneva based independent secretariat, supported by the Multistakeholder Advisory Group, funded by voluntary contributions.

However, the UN Secretary General's note on continuation of the IGF indicated that the majority of contributors to the consultation called for "extension with improvements". It therefore recommended that "improvements to the format, functions and operations of the IGF be considered at its sixth meeting in 2011", and that other improvements, such as membership and rules of procedure of MAG...may be within the authority of the Secretary-General to address"[10]

The UN Secretary General's note reflects that some governments, including China and some developing countries, are uncomfortable with the IGF's multistakeholder environment and non-decision-making character, and express frustration at what they see as its failure to provide outcomes, results or tangible outputs. From their perspective, the IGF has failed to give sufficient attention to solving issues relating to control over the domain name root zone file "by one country" (ie the US).

By contrast, supporters of the IGF process point to its impact in bringing together stakeholders who would not normally meet under the same roof, its contribution to diffusing tensions (so visible during the WSIS) and improving the depth of understanding on key issues. Best practice sharing and influence on other Internet Governance processes (eg steps to internationalise ICANN) are also highlighted as positive impacts.

To reflect both these threads, it is anticipated that the United Nations General Assembly will decide to:
Renew the mandate of the IGF for a further five years.
Establish a working group to consider improvements to the IGF and make recommendations to the UN General Assembly in 2011.

## Conclusions

In regulatory terms, the Internet is still new, and its global governance remains in state of flux. The non-threatening, non-decision-making environment of the IGF has allowed multistakeholders to interact, improved the level of understanding on key issues, and helped to begin to diffuse tensions. However, the evolution of Internet Governance is not complete, and we can expect continuing change over the next 5 to 10 years.

Throughout the IGF's 5 year mandate, CENTR has proactively participated, sharing best practice, acting as an educator to the global community about ccTLD issues and governance. Its IGF working group has effectively coordinated with other regional ccTLD organisations, leading to the signing of a letter of intent for future collaboration.

## Further Reading

IGF Website: http://www.intgovforum.org/cms/

The Internet Governance Project:
http://www.internetgovernance.org/

World Summit on the Information Society:
http://www.itu.int/wsis/index.html

1 WSIS, the Tunis Agenda http://www.itu.int/wsis/docs2/tunis/off/6rev1.html, paragraphs 72-82
2 WSIS, Geneva Declaration of principles http://www.itu.int/wsis/docs2/tunis/off/6rev1.html, paragraph 1
3 http://www.intgovforum.org/cms/aboutigf
4 Keep the Internet free, Carl Bildt, New York Times, 11 October 2005
5 Kofi Annan, UN Secretary General "But let me be absolutely clear. The United Nations does not want to 'take over', police or otherwise control the Internet." WSIS Summit Highlights, November 2005, http://www.itu.int/wsis/tunis/newsroom/highlights/16nov.html
6 Dr Hamadoun Touré, October 2010 http://gibc.biz/2010/10/last-minute-diplomacy-secures-itu's-internet-future/
7 uk, .ch, .no, .at, .ru, .org, .info, .com www.intgovforum.org/cms/funding
8 http://www.intgovforum.org/cms/2010/good-practice.pdf
9 http://www.etlaw.co.uk/docs/Continuation%20of%20the%20Internet%20Governance%20Forum.pdf
10 http://unpan1.un.org/intradoc/groups/public/documents/un/unpan039400.pdf

# Celebrating .CA Websites that Make a Difference

*by David Fowler, Director Marketing and Communications, CIRA*

The Canadian Internet Registration Authority (CIRA) is the member driven organization that manages Canada's .CA domain name registry, develops and implements policies that support Canada's Internet community and represents the .CA registry internationally.

In 2006, CIRA updated its Letters Patent to expand its core mandate, allowing the flexibility to, "develop, carry out and/or support any other Internet-related activities in Canada".

As a first step in supporting the Canadian Internet community CIRA has recently developed and launched a Community Investment Program (CIP). This ongoing program provides a comprehensive framework for CIRA's community initiatives and encompasses the following areas: Internet governance, technology infrastructure, education and knowledge and .CA Excellence. Currently included within CIRA's CIP is the Canadian Internet Forum (CIF). The CIF will be the place where a diverse group of stakeholders discuss, debate and propose directions for the development, deployment and governance of the Internet in Canada. Through the month of November, CIRA hosted six consultations across the country focused on two thematic areas: the digital economy and digital literacy.

In addition, various sponsorship and partnership initiatives are also a key part of CIRA's CIP. Our latest program announcement is the .CA Impact Awards which was announced at CIRA's Annual General Meeting in September 2010 and formally launched at Toronto's mesh marketing digital conference in November 2010. The .CA Impact Awards celebrates people and organizations that use their .CA sites to truly make a difference in the lives of their users and those around them.

The .CA Impact Awards program is not intended to merely celebrate the technical wizardry of websites or the creative genius behind their design – plenty of programs

## *a celebration of the impact of .CA websites and technology*

do this already. Rather, as the name suggests, these awards are a celebration of the impact of .CA websites and technology. Impact is broadly defined and can be social, technological or economic.

The main objectives of the .CA Impact Awards are to celebrate excellence in .CA website development and foster innovation and the sharing of best practices across the .CA community.

There are four awards categories. The eLearning category recognizes youth and educators who are using their .CA domain to share knowledge with others and promote education in Canada and around the world. The Small Business category is open to small businesses with 50 or fewer employees whose website or application has fostered sales, helped create jobs or helped a business contribute to the community in which they operate. The Not-for-profit category is open to registered Canadian not-for-profit organizations making a difference in the lives of members, donors or the public. Finally, the Web Technology category celebrates innovative backbone technology or creative development and design of networks, security features, websites or mobile websites.

A panel of five to seven experts will judge the entries according to preset criteria and a $5,000 CAD prize will be awarded in each of the four categories. These expert judges will be recruited from a diverse array of fields to ensure a representative composition on the judging panel. Such fields include information technology, education, public policy, not-for-profit, the arts, academia, and business.

Entries will be accepted in January 2011, leading to an awards ceremony in May 2011. More information on the .CA Impact Awards is available at www.impactawards.ca.

# Safety does not happen by accident

*by Katrina Sataki, Manager of NIC.LV*

**Not so long ago, in the mid-1990s, when the Internet revolution had only just started, the first Internet pioneers did their best to attract more and more people to join the Internet user community. We advertised e-mail and the worldwide web, online banking and file downloads. We said how great it was to have your own domain name. Grab all those opportunities! Register your own address! Come and join us today!**

## Wait! Not so fast!

But at some point we realised that the Internet simply reflects society – there are plenty of good people out there, but also the full spectrum of bad ones. In real life we are more or less prepared to deal with bad things, but in cyberspace people are not yet ready to protect themselves adequately. There are different reasons for this, one of which is limited awareness of the issues of cyber threats and cyber security.

In most cases people believe that security is something they buy when they buy a computer, Internet subscription or a particular piece of software. For them, security is something they are entitled to. Unfortunately, this is not the case.

## Minors first, adults later

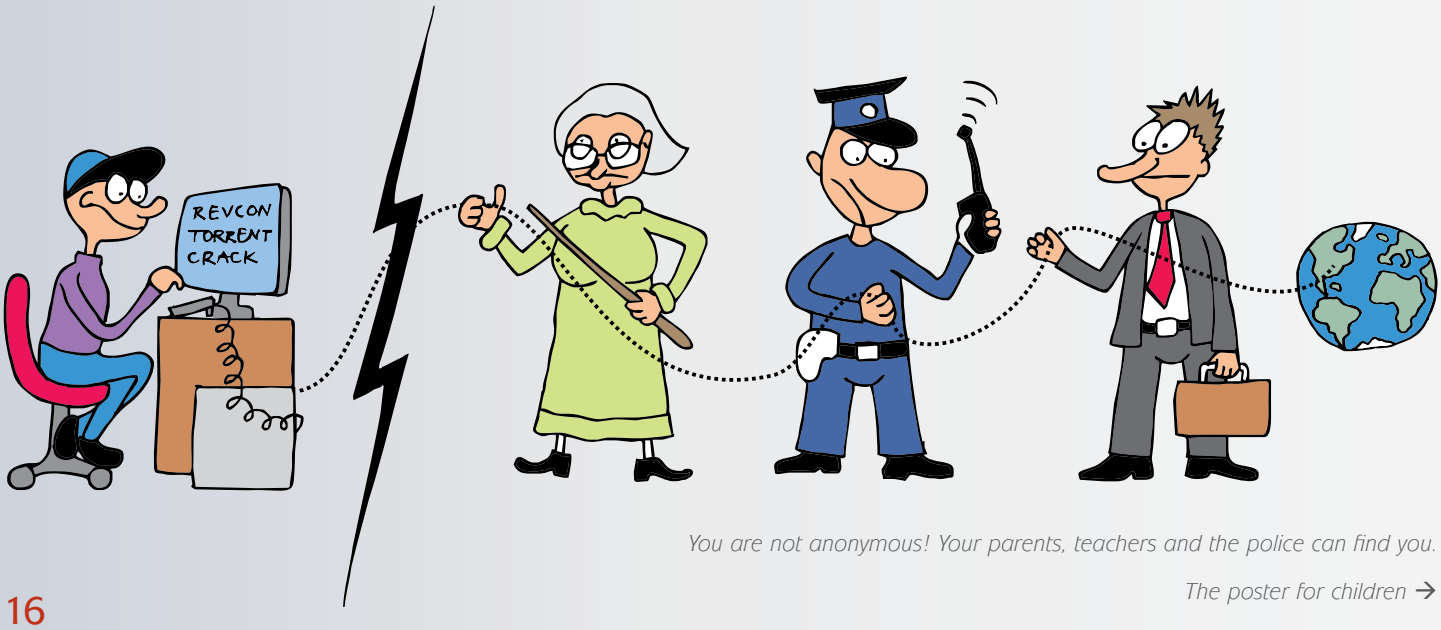
*One of the most vulnerable groups of Internet users is minors*

One of the most vulnerable groups of Internet users is minors. Their parents, who would normally protect them from harm, are very often significantly less technologically savvy than their offspring. And would children really listen to their elders, who can't tell a torrent from a gateway? Sure, adults have to be educated as well but we decided that that could wait. Minors first! For us, it was important to choose an attractive way of addressing some of the most important issues. Something that would attract interest and stick (literally and figuratively). A poster! A poster with funny cartoons. A poster that could be hung on the wall either at home or in a classroom. A poster that every child would be happy to own.

The first version of the poster was printed in 2005 and was a huge success. It was used by teachers and government officials to warn society and show that more a pro-active approach was required.
Earlier this year we decided to revive the idea and create a new version of the poster. Two versions, actually. We reworked the one for minors and developed a brand new one for adults (and older children).
When we were revising the old poster, we realised that some issues we had covered were no longer urgent and some new issues had emerged. For example, that children don't know what an e-mail is. Meanwhile, social networks have become more and more popular. So we tried to reflect some of the most pressing topics. This time we decided to create and distribute not only printed versions, but also electronic versions of the poster. We included a reference on the poster to the Net-Safe Latvia project website and hotline number for those who need help.

## We won't stop there

A poster for adults is still in preparation. In cooperation with the Ministry of Transport and security specialists from various organisations we have started work on a portal for Internet users: parents, government officials, home users, etc. The portal will contain simple yet important advice, security warnings, blog posts and other information to make our life safer and more secure.
NIC.LV – the Registry of the country code Top Level Domain .lv (Latvia) and its CSIRT team CERT NIC.LV has invited all security specialists to take part in these activities. It is not about competition. It is about cooperation. Cooperation between everyone who cares.




*You are not anonymous! Your parents, teachers and the police can find you.*

*The poster for children →*

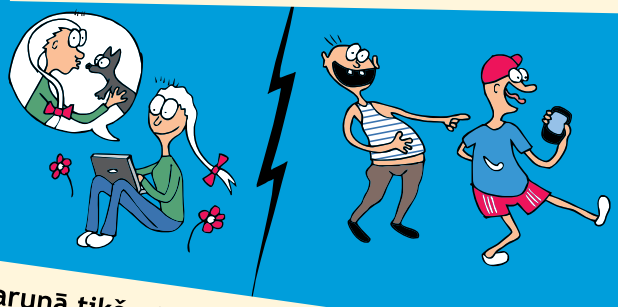
# Vai esi Interneta profiņš?

## Lieto drošas paroles!

Katram portālam izmanto savādāku paroli. Veido to pietiekami sarežģītu, lai to nevarētu uzminēt pat tie cilvēki, kas Tevi labi pazīst!

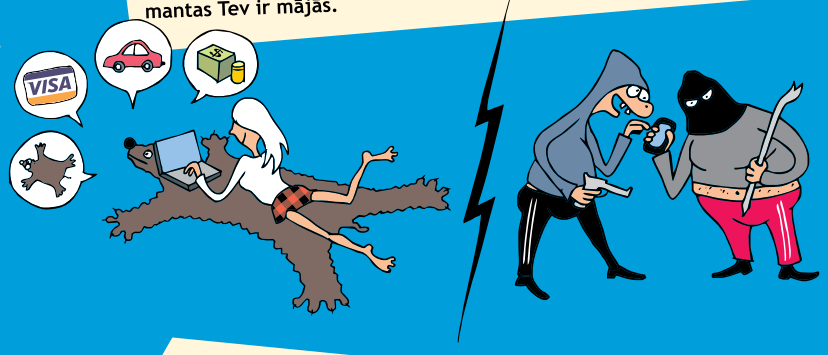
## Apdomā pirms publisko attēlus internetā!

Padomā, vai šie attēli neaizskar un nekaitē Tev, Taviem draugiem, klasesbiedriem, vecākiem vai jebkuram citam cilvēkam, kas attēlots fotogrāfijā. Pēc tam, kad attēls ir „ielikts" internetā, to vairs nevar iznīcināt vai padarīt par nebijušu.



## Neatklāj datus par sevi nepazīstamiem cilvēkiem!

Nebūt ne visi, ko Tu satiec virtuālajā vidē, ir tie, par ko uzdodas. Bieži vien ļaundari slēpj savu patieso seju, lai vieglāk piekļūtu Tev, Taviem radiem un draugiem. Jo vairāk Tu par sevi atklāsi, jo vieglāk viņi varēs nodarīt Tev pāri reālajā dzīvē. Neatklāj, kā Tevi sauc, kur Tu dzīvo, kas ir Tavi vecāki vai kādas mantas Tev ir mājās.



## Nesarunā tikšanās ar tīklā satiktajiem paziņām!

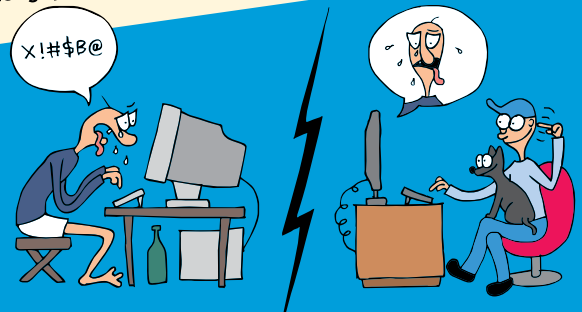
Atceries, ka tīklā satiktie cilvēki ne vienmēr ir tie, par ko izliekas! Sargā sevi, lai neviens nevar nodarīt Tev pāri! Nepiekrīti tikties ar nepazīstamiem cilvēkiem nomaļās vietās, kur nav neviena, kas nepieciešamības gadījumā varētu Tev palīdzēt.

## Darbības internetā nav anonīmas!

Tavas darbības internetā nav anonīmas! Vajadzības gadījumā tām var izsekot gan skolotāji, gan vecāki, gan likumu sargājošas iestādes.

## Neraksti aizskarošus komentārus!

Cilvēki, kas aizvaino citus, paši jūtas nelaimīgi. Taču, aizvainojot citus, neviens laimīgāks nekļūst. Nesāpini apkārtējos! Esi iecietīgs pret citu viedokli, dzīvesveidu, dzīves uzskatiem.



## Mēstules nav vēstules!

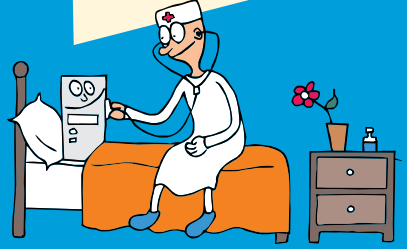
Ignorē mēstules, ko saņem nepazīstamiem cilvēkiem. Neatsaucies to „vilinošajiem" piedāvājumiem. Visbiežāk tie ir mēģinājumi izkrāpt Tavu naudu. Mēstules var izfiltrēt un par tām var sūdzēties.

## Neiepērcies internetā bez vecāku ziņas!

Nesniedz internetā savas vai vecāku kredītkartes datus, iepriekš neapspriežoties ar vecākiem. Atceries - izmantojot kredītkartes datus, var nozagt visu naudu, kas pieejama ar šo karti.

## Rūpējies par datora veselību!

Neinstalē nezināmas izcelsmes programmas uz datora, ko Tu lieto. Programma ļoti viegli var izlikties par spēli, bet patiesībā būt vīruss, kam Tu pats paver ceļu uz savu datoru.



**Ja Tu:**

- saņem nepatīkamas, aizvainojošas vēstules internetā,
- esi saskāries ar nepatīkamiem materiāliem internetā,
- esi pamanījis aizdomīgas darbības internetā,
- esi satraukts par savu drošību internetā,

pastāsti par to saviem vecākiem vai kādam citam no pieaugušajiem, kam uzticies! Vari zvanīt Bērnu un jauniešu bezmaksas uzticības tālrunim 116111 vai rakstīt uz: zinojumi@drossinternets.lv vai abuse@nic.lv



CERT NIC .LV

# To measure is to know

*by Anne-Marie Eklund-Löwinder, Quality & Security Manager, .SE*

**The words are those of Lord Kelvin, a 19th-century mathematician and physicist. Another of his quotations is: "If you cannot measure it, you cannot improve." .SE has taken this thinking to heart. Evaluation is critical to prove that something is successful (or not) in order to determine the level of quality, the effects and consequences of interventions and to be able to improve the tools used for measuring. In this article we describe three different areas where .SE is involved in measuring: Broadband Check, Internet statistics and .SE Health Check, and the driving force behind these activities.**

## Broadband Check (Bredbandskollen)

Broadband Check is Sweden's only independent consumer service to test broadband connections directly using a web browser. In three years, 11 million unique users have carried out 34 million individual tests, totalling an average of 40,000-50,000/day. 1.8 million of these tests have been initiated from 170,000 unique smart phones, totalling 7,000-8,000 tests/day. Broadband Check has been a great success, with millions of tests conducted by users of both mobile and landline broadband connections as well as iPhones, iPads and Androids.

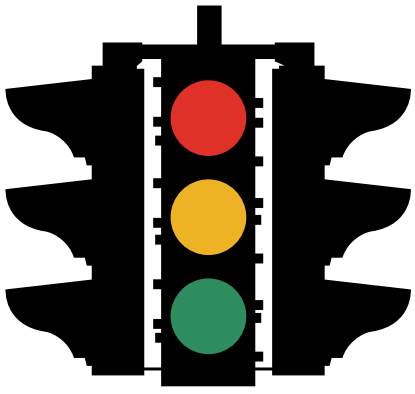
In 2009, Broadband Check was expanded to include a mapping service, which can be used to check average speeds for mobile broadband connections at various locations around Sweden, based on measurements that other users have made. The service provides not only the average speed for larger geographical areas but also individual measurements down to the level of a single street, and makes it possible to compare various operators within the same area.
With Broadband Check, we have helped contribute to a saner market. Not only do we make it possible for Swedish consumers to check their broadband connection, we have also forced Internet Service Providers to market Swedish broadband services more transparently, so that they now generally offer their customers a speed they can guarantee. In addition, we have developed a tool to help customers with troubleshooting.

## Internet statistics

The purpose of .SE's initiative on Internet statistics is to ensure the availability of up-to-date, reliable and relevant statistics for everyone who wants to monitor or analyse the development of the Internet in Sweden. A number of statistical reports have been published by .SE in this area.

We collaborate with four different independent analytical institutes and producers of Internet statistics: the Nordic Information Centre for Media and Communication Research (Nordicom), the Swedish Post and Telecom Agency, PTS, Statistics Sweden (SCB) and the World Internet Institute. Statistics and facts about the Internet and its use are published on www.internetstatistik.se.
.SE is running a project called The Swedish and the Internet in collaboration with the World Internet Institute. The project has been running since 2000 and collects data about how the Swedish population uses information and communications technologies as well as how this

affects individuals, families and society as a whole. The project is carried out through a panel study comprising approximately 2,000 yearly telephone interviews based on a random selection of the population, aged 16 and up. The telephone interviews are comprehensive and contain questions about the interviewees' background, access to technology, use of traditional media and, most of all, various forms of Internet usage.



The Swedish and the Internet is Sweden's contribution to the World Internet Project, an international research project monitoring the spread and use of the Internet around the globe. The number of participating countries increases every year and in 2010, the project had about 30 member countries. Every partner in a particular country finances its own activities in the project. The national selections are representative of the population. The questionnaires include just over 100 questions that are common to all countries, with identical wording in every country in order to produce comparable results. The World Internet Project was started in the USA in 1999 by Jeffery Cole at the UCLA Center for Communication Policy, and is now run by the Center for the Digital Future at the Annenberg School for Communication. The first panel studies were carried out in the US, Sweden, Italy and Singapore in 2000.

## .SE Health Status

.SE strives to ensure that the Internet infrastructure in Sweden functions well and offers a high degree of accessibility. We have created this area of focus in order to monitor the quality of Sweden's infrastructure – and when necessary, to draw attention to shortcomings and unsatisfactory conditions.

Over the course of 2010, we tested and evaluated .se domains for the fourth consecutive year regarding the quality of some specific parts of the Internet infrastructure in Sweden. The quality of society's most important domains was investigated using a mixture of different tools and software and the results issued in a special report, The Health Status of .se. Both the 2009 and 2010 studies included a control group of 10,000 randomly selected .se domains for comparison with the selected group of important social functions such as banks, government and media companies, among others.

Unfortunately, we have not been able to detect any positive trends or development over the years and many major quality problems still need to be dealt with. For the moment we are working on what will be our next step in order to raise the quality of .se domains.

## Why do we do this?

The foundation's charter states that .SE will promote the positive development of the Internet and stability in Internet infrastructure. In addition, .SE should promote research, development, training and education in data and telecommunications, with a specific focus on the Internet. The foundation's charter is implemented in practice through .SE's financing of projects that benefit Internet development in Sweden, using the surplus from domain sales.

## LINKS

Broadband Check http://www.bredbandskollen.se/ (only available in Swedish)
Internet statistics http://www.internetstatistik.se/ (only available in Swedish)
DNSCheck http://dnscheck.iis.se/
MailCheck http://mailcheck.iis.se/
The latest report from the Health Status Check of .se: http://www.iis.se/docs/Rapport-Halsolaget-2010-eng.pdf
The latest report on The Swedish and the Internet: http://www.iis.se/docs/SOI2010_web_v1.pdf (only available in Swedish)


# .eu goes ERASMUS, the first step for students in Europe

*by Giovanni Seppia,*
*External Relations manager, EURid*

**This autumn, EURid ran a marketing initiative aimed at promoting the European online identity and the .eu top-level domain to ERASMUS students.**

"ERASMUS is the EU's flagship education and training programme, enabling 200,000 students to study and work abroad each year. In addition, it funds co-operation between higher education institutions across Europe. The programme not only supports students, but also professors and business staff who want to teach abroad, as well as helping university staff to receive training." (http://ec.europa.eu/education/lifelong-learning-programme/doc80_en.htm)

*Erasmus students are well-suited as a .eu target group.*

Erasmus students are well-suited as a .eu target group. This was also the view expressed by Mrs Neelie Kroes, Vice-President of the European Commission and European Commissioner for the Digital Agenda, who said: "I very much welcome this initiative of EURid, the body behind the success of ".eu". Using a ".eu" website or email address is a strong sign of European identity: across the borders of our Continent, we, Europeans, share values and a community of destiny that has its place in the digital world too. I trust that this young and dynamic generation, represented by the ERASMUS programme, is best placed to convey this message".

The first ERASMUS campaign by EURid was produced in 2009, but did not prove to be a great success due to several factors, including a number of issues in terms of logistics and a lack of coordination within the chosen universities.

This year, the initiative consisted of a tour of three universities – Lessius Hogeschool in Antwerp (Belgium), the University of Pisa (Italy) and the Technical University of Liberec (Czech Republic) – during events taking place for outgoing and incoming ERASMUS students. Students were invited to register a complimentary .eu domain on site. The package included a one-year .eu domain registration, three 2 GB email addresses, antivirus/antispam, unlimited web space and a tool to create a website or blog in just a few quick steps.

The campaign was developed in partnership with one of the .eu accredited registrars. The basis of the initiative is the belief that the ERASMUS programme and .eu share some core values: both reflect the vision of a European identity, promote intra-European mobility and can help bridge the digital divide.

The initiative generated a lot of press coverage, mainly in the Czech Republic and in Italy. A special YouTube video with interviews with students was produced and is now available on the EURid YouTube channel (http://www.youtube.com/user/Europeanregistry).

Around 150 students out of 480 registered a .eu domain via the promotional campaign and are now in the process of creating their own website.

In the end, we may wonder whether it was worthwhile for EURid to run this initiative. The 2009 campaign can be seen as a pilot project that experienced a number of hiccups. The 2010 experience showed a lot of interest and enthusiasm among the universities and the students, but logistics are still a factor and need to be taken into account when weighing up the results against the cost and effort. However, we firmly believe that a customised domain where students can share experiences with friends and family provides added value for the ERASMUS experience itself and therefore, we are pleased to have given this opportunity to the young people who represent the next Internet generation and can further improve their knowledge via a complimentary .eu domain package.

# From cyber-bullying to medical research – the work of the Nominet Trust

*by Elaine Quinn, PR Manager, Nominet*

**After being bullied at school, 14-year-old Georgia Woods was driven to the point of almost taking her own life, but, like hundreds of thousands of other youngsters tormented by bullying, she was helped by cybermentors.org.uk and has turned her life around.**

CyberMentors is a safe, online social networking site for young people who are being bullied or cyber-bullied. It works by training 11 to 16 year-old mentors in schools to help and support other youngsters. The programme also ensures professional counsellors are on hand.

*I literally owe them my life*

"Beatbullying as an organisation is fantastic, a great help for people, and I don't know what I would have done without them. I literally owe them my life," says Georgia. Her mother adds: "This project helped Georgia so much with her self-esteem and her confidence has really, really grown. The way she's come through all this is purely down to the counsellors at school and Beatbullying. I could be sitting here telling you a completely different story, but thankfully I'm not." This month the CyberMentors programme, an initiative by the Beatbullying charity, will help its millionth youngster, and schools where the programme is running are reporting a 40% reduction in bullying.

CyberMentors was made possible with the support of the Nominet Trust, the charitable foundation set up in 2009 by .uk Internet registry Nominet. The Nominet Trust funds scalable, practical projects that help Internet users get better access, or stay safe, online, as well as research that uses the Internet to do things more effectively. Lesley Cowley, CEO of Nominet, comments "As a not-for-profit registry, we run .uk with a clear public purpose – it's in our 'DNA'. The work of the Nominet Trust is part of the organisation's commitment to making the Internet a force for good."

Since it was set up in 2009, Nominet has donated £13m to the Nominet Trust, which has invested in over 120 projects that contribute to creating a safer, more accessible Internet for all.

Annika Small, Director of the Nominet Trust, highlights the breadth of its operations. "The Internet offers tremendous opportunities for doing things differently and often more effectively. As well as projects that help Internet users directly, we are also investing in pioneering projects that only the Internet can make possible."
A case in point is The Alzheimer's Society, which is undertaking its first online clinical trial. This ground-breaking initiative allows a large-scale study to be undertaken for a fraction of the time and resources required for a traditional trial. The trial is designed to understand if an optimised Internet-based brain training package can successfully improve or sustain mental capacity. This important research will show whether brain training should be included in research into the prevention of dementia.


"This is hugely exciting", says Professor Ballard of The Alzheimer's Society, "as not only does this study have the potential to improve the lives of people with dementia, it has also gone some way to validating this new, innovative research methodology." Annika Small adds: "From Wikipedia to Kiva to TimeBank, we are witnessing communication and collaboration on an unprecedented scale with billions of people working together to create valued content, share ideas and develop new solutions to local and global challenges. As these examples show, the Internet has significant potential to improve lives and communities. The Nominet Trust is working to support initiatives that realise the Internet's potential as a tool for social improvement."

For more information on the Nominet Trust, visit www.nominettrust.org.uk

# Activities of the CZ.NIC Association for the Czech Internet community

*by Vilém Sládek, PR manager, CZ.NIC*

**The CZ.NIC Association has been responsible for the administration of the Czech national domain .CZ since 1998. The association has worked in a variety of areas in addition to maintaining the domain register from the outset. Equal amounts of effort have been put into various projects aimed at increasing awareness of Internet-related topics among both professionals and laypeople, as well as providing the Czech Internet community with useful services that enhance the security and ease of using the Internet.**

## mojeID

mojeID is CZ.NIC's largest ongoing project. Launched in October 2010, mojeID offers Czech Internet users the option to log into various online services, such as e-shops, news servers and discussion forums, using a single username and password combination. MojeID is based on OpenID technology, in which neither users nor service providers in the Czech Republic have expressed much interest to date. MojeID, however, offers one significant improvement – the centralisation and institutionalisation of the operation of the entire system. This guarantees the stability of the service and correct handling of service providers' business information and user data. MojeID also enables users to store all their contacts in one place, making them easier to manage.

## The CZ.NIC Academy

The CZ.NIC Academy is a training centre that provides further education in the area of the Internet and Internet technologies to anyone from the business community. Its courses are intended for anyone who would like to learn more about the theory and practice of current topics, such as key public infrastructure, IPv6 implementation, the BGP gateway protocol, or preventing SQL injection attacks. Participants are also entitled to use the Academy's modern laboratory, equipped with all the hardware and software required for testing and conducting experiments.

## The IT Conference (Internet and Technology)

Since 2008, CZ.NIC has organised an annual and now two-day professional conference called Internet and Technology. The meeting is aimed at both the general public and professionals from the Internet community, students, and journalists. The conference always focuses on current issues related to the Internet and Internet technologies – such as IDN, BGP, or spam. This year, most of the programme focused on the problem of running out of IPv4 addresses.

## Projects for Schools

CZ.NIC provides schools, teachers and students with informational materials free of charge. Where there is sufficient interest, CZ.NIC also organises educational events in schools. These are predominantly themed lectures for students in secondary schools and grammar schools with various levels of expertise, explaining the inner workings of the Internet, Internet security and copyright issues, and the benefits of owning an Internet domain. For teachers of ICT subjects, CZ.NIC offers a full-day lecture discussing these topics in more detail, including information about the IPv4 vs IPv6 issue, DNSSEC technology, or ENUM. All these events are provided to schools and their teachers free of charge.

## VIP Contest

The abbreviation in the contest name stands for three words in Czech – Vyvíjej, Inovuj, Programuj – or Develop, Innovate, Program. The contest is aimed primarily at young programmers. Anyone can enter the contest with a project that enhances or improves existing software in the fields of Internet technology, infrastructure or services. Young programmers have a chance to complete their projects and win substantial cash prizes. School projects and assignments can, of course, be entered into the contest as well.

## 6to4 Technology

In 2010, the CZ.NIC Association began operating the first public 6to4 relay router in the Czech Republic. 6to4 technology resolves one of the most significant problems related to the switch to the new IPv6 protocol, namely the incompatibility between IPv6 and the old IPv4 protocol, which makes computers connected via IPv4 unable to access Internet content using the IPv6 protocol and vice versa. The transitional 6to4 technology circumvents the problem by automatically "tunnelling" IPv6 traffic through the IPv4 network.

Thanks to this technology, which is widely supported and works automatically, for example, in the newer versions of the Windows operating system, computers connected using the old protocol can be given their own v6 address at the same time. Operating the 6to4 under the Czech backbone node of NIX.CZ brings Czech Internet users easier and faster use of this technology than if they were to use one of the foreign routers.

Overall, we work on many projects that can help the Czech Internet community raise awareness of the Internet technologies used today. We focus heavily on promoting IPv6 and boosting awareness of this up-and-coming Internet protocol. Our activities in this field include participation in public conferences (giving papers on these topics at events organised by ourselves or by our partners), the projects listed above, and numerous publishing activities in media outlets for various audiences. Our laboratories are also very active in promoting IPv6; their outputs include the world-renowned DNSSEC Validator and DNSSEC Tester projects.

# The IDN TLD for Russia: Lessons Learned

*by Leonid Todorov, Head of Government relations, Coordination Center for Top Level Domain .RU*

At 6.30pm on 11 November the time has come for champagne – after a six-hour long marathon, the number of domains registered on the first day of the open registration phase in the Cyrillic IDN TLD .RF has beaten even the most optimistic forecasts and hit a whopping 200,000-plus mark, the size of the whole .FI.
Now that the dust has settled a little, it is time to take a break and try to analyse what lies behind this success story, and see what can be learned from it.
In hindsight, the two-year journey seems a pretty simple exercise; a closer look, however, reveals a number of challenges the CCTLD .RU was facing over this period, the most serious of which are highlighted below.

## Multistakeholder-ism in Russia, or the Empire Revisited

It is common knowledge Russia has always developed in its own unique way, and the same applies to RUNET. It took policymakers a good decade to realise the potential of the web but they have now become staunch proponents of it, vigorously backing new initiatives to expand it, not least because, like many Russians, they feel nostalgic for their glorious imperial past when the country was a pioneer in the area of R&D.
So, they happily bought into the concept of launching the first Cyrillic IDN TLD, and we enjoyed their full support and active cooperation. IDN TLD .РФ has become, perhaps, the first public-private partnership in the history of modern Russia, with the Government readily teaming up with the wider community to achieve a common objective.

*the first public-private partnership in the history of modern Russia*

Users, too, had their say, by defining the name of the string, and academics proved it was a meaningful way to represent the country's abbreviated name.
OK, it may not be a proper multistakeholder-ism pattern, but so what? Russia has always developed in its own unique way, remember?

## It's Marketing, Stupid

Meanwhile, Internet users remained largely sceptical and suspected it was all about people making big money. Businesses, too, were sceptical about the idea of having another CCTLD for no obvious reason. The mass media, as usual, mostly failed to communicate the story adequately, even in the West, with tales of horror and gloomy prophecies about the collapse of RUNET and the Internet as a whole, due to the introduction of IDNs.
In the circumstances, the bulk of our efforts quite logically went into marketing, with a huge nationwide campaign running for a year and half and employing every possible marketing tool, including the grapevine. Though expensive, the campaign proved to be an indispensable lever to raise awareness and educate the audience, promote the benefits and values of the would-be .РФ, and spark general interest in the issue. In 2009, .РФ became the second most cited and talked-about subject in the country.

## Spine in Snipes

On a more serious note, the biggest challenge was to establish the rules of the game. To this end, the best legal experts were brought in to work out Registration Procedures for .РФ and draft other standards documents. The scale of the project was daunting, but international experience and the 15-year long record of CCTLD .RU were at hand, so the outputs were delivered on time and in line with best practices, and we were armed with well-defined and clear guidelines.

What's more, whenever a new problem arose, the experts were ready to respond promptly by modifying procedures accordingly. Although they attracted criticism from users and the media, such moves helped ensure effective protection from cybersquatters for the rights of trademark owners and government agencies to certain domain names as part of their overall portfolio of branding tools. We could cite numerous instances, some of which are hilarious, in this respect, but will save them for another publication.

## What's Up Next?

With .РФ up and running and a real boom in staking out new domains within it, it is now clear that IDN TLDs are not just a toy, nor are they an artificial, foreign body on the Internet. Users, businesses and governments are keen to secure their presence there – can there be any recognition higher than this for a humble TLD administrator? Today, the Coordination Centre's mission is to keep this source of national identification and tool to promote diversity intact and make sure it can expand and catch up with .RU – a serious challenge, indeed.

# Austrian "Netidee" celebrates its fifth anniversary

*by Monika Pink-Rank, PR & Marketing, NIC.AT*

Launched in 2006 by nic.at's owner, the non-profit Internet Foundation Austria, the country's largest call for Internet-related ideas, can look back on a very positive development: in five years, more than 320 projects have been submitted and over 80 of them awarded a grant ranging from €2,000 to €50,000 each. The last two calls, in 2008 and 2009, were dedicated to the theme "e-inclusion and e-literacy" to support projects aimed at bridging the digital divide.

## Bridging the digital divide – the Internet for all!

Although western countries show a high Internet penetration rate throughout the population, there are still groups that have no or only limited access to new technologies. "Offliners", one of the projects awarded a netidee grant, is a qualitative research project aimed at finding out why people do not use the Internet and designed to deliver empirical data about this situation for the first time. Based on these data, concrete recommendations can be put forward on how to make the Internet available for all. In addition, the study will raise awareness of the fact that a high online penetration rate in a particular country does not automatically mean that all sections of society have a chance to participate.

*How to make the internet available for all sections of society?*


## RoboBraille – supporting visually impaired people

Around 4% of Austria's population (approximately 318,000 people) suffer from a visual disorder and thus face difficulties in accessing electronic documents. The RoboBraille Project aims to abolish these barriers by translating files into Braille or converting them into an audio format for users. The principle is simple: users send their electronic documents (eg. in Word, .html or PDF format) by e-mail to a specific RoboBraille e-mail address. The text is then converted into Braille or an audio file and sent back to the user, who can either listen to it or read it with a Braille output device. Although this technique has been known about since the 1980s, it was only as a result of the netidee grant awarded in 2009 it could be developed and made available to the Austrian community for free. With the follow-up project "mathInBraille", awarded a grant in 2010, mathematical formulas can now also be converted.

## Digital city maps with AmauropMap+

Another project aimed at visually impaired people is Amauromap+, a digital city map that works with semantic descriptions. Created in 2008, it is now being developed further with extensive test data from various cities (such as Vienna) and evaluated with end users.

## MyTablet – the Internet opportunity for elderly people

One of the groups in society that is still under-represented in the Internet community is elderly people. The "MyTablet" project is working with a test population of people aged 60+ to determine if and how tablet PCs could be a gateway to the Internet for this target group. The hypothesis is that touch tablets, with their intuitive handling and no mouse, help to overcome inhibitions. In addition to usability studies and field research there will be training initiatives and personal coaching for senior citizens.

## Data Dealer: Raising awareness about data protection on the Internet

E-literacy is not only a catchword for "offliners" – even young people who are considered to be "digital natives" are often not aware of the risks and threats in the online world. The multiplayer online game "Data Dealer" has chosen to address this topic in an ironic way: operating within a pseudo-economic simulation, the user plays the role of a data dealer who tries to win a fortune by selling personal data – and not only with legal methods. The game shows, in a humorous way, what can happen if personal data are not protected. It is aimed at pupils aged from 12 to 16 and is a good way of illustrating that learning can be fun.

## Netidee - to be continued

More information (in German) about netidee can be found on www.netidee.at. The call will be repeated in 2011 and everyone is already curious to see which new ideas and projects will be entered in the next contest.

## Supporting the community in a variety of ways

The Internet Foundation Austria not only conducts its own annual call for projects but also participates in other initiatives where the innovate use of the Internet and web domains are rewarded: within the framework of Austria's largest business plan contest, "ideas2business", the foundation and nic.at have just sponsored a special award that was given to a young team developing new online tools for identifying, assessing, evaluating and forecasting the potential of talented upcoming athletes.

# Greater Internet security in Switzerland

*By Marco D'Alessandro, Media spokesman, SWITCH*

**SWITCH is stepping up the security measures for the Swiss Internet: Swiss websites that spread malicious software and infect the computers of Internet users with malware as they surf will be removed from the web.**

*We will only remove a website in an emergency*

Cybercrime attacks are becoming increasingly sophisticated. Frequently, just calling up a manipulated website is enough to infect a computer with viruses or Trojan horses. And this abuse goes unnoticed by the website operator and the visitor. "Each week we receive more than a hundred notifications of websites infecting other computers with malware," says Dr. Serge Droz, Head of the Security Division at SWITCH. This is why SWITCH introduced a new procedure to combat malware on 25 November 2010: SWITCH's security team checks the notifications it receives about websites spreading malware. If it finds malicious websites, SWITCH will contact the holder and the operator (provider) and ask them to resolve the problem. If no action is taken within one working day, SWITCH will block the Internet address. "We will only remove a website from the web in an emergency. The aim is for the malicious site to be cleaned up rapidly," explains Serge Droz. The foundations for these measures lie in the Swiss Ordinance on Addressing Resources in the Telecommunications Sector. This consistent approach will make a key contribution to maintaining a high security standard for Swiss Internet addresses. The feedback from our customers is extremely positive.

# .cat reinvests in the community

*by Jordi Iparraguirre, CEO, PuntCAT*

The .cat domain, a sponsored gTLD, is managed by a not-for-profit, self-funded, private foundation, "Fundació puntCAT", whose aims are to manage the TLD on behalf of the Catalan-speaking community and to participate in actions aimed at reducing the digital divide whilst promoting the presence of the Catalan language online.

Launched in February 2006, during its first four years of existence, .cat has reinvested its operating profits in consolidating its infrastructure, reducing domain registration and renewal fees as the number of registered domains grows, and two web-based Internet popularisation projects on safe browsing and basic DNS management

In 2010, .cat was ready to develop its not-for-profit and community reinvestment actions further. Last spring we issued a call to fund up to a maximum of €20,000 per project, for proposals put forward by the community addressing two main target areas. On the one hand, helping to reduce the digital divide, especially amongst groups of people at risk of social exclusion or those facing additional barriers to using the Internet or information and communications technologies (ICT); for instance, disabled people who, because of illness or an accident, face an extra burden in accessing the benefits of ICTs. On the other, projects aimed at increasing the quantity and quality of Catalan-based content online, or resources to increase and ease its use.

The call for projects was open to any not-for-profit associations or companies that wanted to address the strategic areas explained above whilst undertaking to run the projects on a not-for-profit basis and on the understanding that all the content developed would be under Creative Commons licences or, in the case of software, GPL. Our first call for projects closed in September 2010 and exceeded all our expectations, with 74 projects submitted.

An independent group of 20 well-established professionals, freelances and executives in the ICT area, as well as academics and ISOC-CAT representatives, had the responsibility of evaluating the projects, based on some basic guidelines set up by the puntCAT Foundation. We like this model of expert evaluation but for next time we are examining how to open the evaluation process to all .cat registrants as a way of offering them the possibility of being involved in the process, as all this is possible thanks to the contribution they have made through registering and renewing their .cat domains.

We offer to subsidise a maximum of €20,000 per project, which is not designed to cover running costs but only what is really needed to get the project up and running. The experience gained from this first call, analysing the 74 proposals we have received, demonstrates that there are lots of brilliant ideas as well as some unfulfilled needs in the not-for-profit world, which just need a small financial boost to come to fruition and add a lot of value to the community. On the other hand, certain initiatives need some more initial in-depth analysis to avoid reinventing the wheel, but this simply proves that not everybody is aware of the free tools the Internet is currently offering, nor that the solutions they want to implement are already being developed by other NGOs.

*here are lots of brilliant ideas as well as some unfulfilled needs*

The final number of winners depends on the total amount of money available and the sums required for the selected projects. For this first time, puntCAT will invest, or rather, reinvest, a little under €90,000 in the community. The grant allocated to each project is split into three parts and projects need to pass the checks at various control points to ensure the project is completed as planned. We have decided to monitor the projects to maximise the likelihood of their succeeding, so that the whole community benefits from the result and the resources invested are not wasted. We want .cat registrants to be able to say proudly that these initiatives were made possible thanks to their contribution.

Our conclusions from this first "Ajuts puntCAT" initiative are really positive. We are really excited about the projects selected and we firmly believe they will add a lot of value for us all. At the end of the day, puntCAT manages a common interest and as such we reinvest in the community so that we all benefit from .cat domain management and from the projects the community is willing to implement.

# About CENTR

CENTR VZW/ASBL
Belliardstraat 20
1040 Brussels
Belgium
Tel: + 32 2 627 55 50
Fax: + 32 2 627 55 59
Email: secretariat@centr.org
www.centr.org

**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 Peter Van Roste (General Manager), Wim Degezelle (Communications Manager), Patrick Myles (Information Manager) and Linda Verhaegen (Office Manager).
For further information you can visit our website www.centr.org or contact us at secretariat@centr.org


Peter Van Roste
(General Manager)


Wim Degezelle
(Communications Manager)


Patrick Myles
(Information Manager)


Linda Verhaegen
(Office Manager)

**CENTR members are the registries for**
.af (Afghanistan), .ac (Ascension Island), .ad (Andorra), .al (Albania), .am (Armenia), .at (Austria), .be (Belgium), .bg (Bulgaria), .ca (Canada), .ch (Switzerland), .cy (Cyprus), .cz (Czech Republic), .de (Germany), .dk (Denmark), .es (Spain), .eu (European Union), .fi (Finland), .fo (Faroe Islands), .fr (France), .gg (Guernsey), .gi (Gibraltar), .gr (Greece), .hr (Croatia), .hu (Hungary), .ie (Ireland), .il (Israel), .im (Isle of Man), .io (British Indian Ocean Territory), .ir (Iran), .is (Iceland), .it (Italy), .je (Jersey), .li (Lichtenstein), .lt (Lithuania), .lu (Luxemburg), .lv (Latvia), .me (Montenegro), .mt (Malta), .nl (Netherlands), .no (Norway), .pl (Poland), .ps (Palestinian Territories), .pt (Portugal), .re (Reunion Island), .ro (Romania), .rs (Serbia), .ru (Russian Federation), .se (Sweden), .si (Slovenia), .sk (Slovak Republic), .tr (Turkey), .uk (United Kingdom) and .va (The Holy See - Vatican City).
The registries for .cn, .jp, .mx, .nz, .us, .biz, .cat, .com, .info, .mobi and .org are Associated members.

# DATES OF UPCOMING MEETINGS 2011

| | |
|---|---|
| **2-3 February 2011** | **44th CENTR General Assembly/2011 Annual General Meeting, Tel Aviv, Israel** |
| **16 February 2011** | **34th CENTR Legal and Regulatory Workshop, Vienna, Austria** |
| **16 February 2011** | **22nd CENTR Administrative Workshop, Vienna, Austria** |
| 13-18 March 2011 | 40th ICANN Meeting, San Francisco, North America |
| 27 March -1 April 2011 | 80th IETF, Prague, Czech Republic |
| **28-29 April 2011** | **5th CENTR Marketing Workshop, Helsinki, Finland** |
| **2 May 2011** | **24th CENTR Technical Workshop, Amsterdam, Netherlands** |
| 2-8 May 2011 | RIPE 62, Amsterdam, Netherlands |
| **23 May 2011** | **3rd CENTR Joint R&D Workshop, Prague, Czech Republic** |
| **26 May 2011** | **35th CENTR Legal and Regulatory workshop, Prague, Czech Republic** |
| **7 June 2011** | **23rd CENTR Administrative workshop, Trondheim, Norway** |
| **8-9 June 2011** | **45th CENTR General Assembly, Trondheim, Norway** |
| 19-24 June 2011 | 41st ICANN Meeting, Amman, Jordan |
| 24-29 July 2011 | 81st IETF, Quebec City, Canada |
| September 2011 | IGF Meeting, Nairobi, Kenya (TBD) |
| **6-7 October 2011** | **46th CENTR General Assembly, Brussels, Belgium** |
| 23-28 October 2011 | 42nd ICANN Meeting, Africa |
| **30 October 2011** | **25th CENTR Technical Workshop, Vienna, Austria** |
| 31 October-4 November 2011 | RIPE 63, Vienna, Austria |
| 13-18 November 2011 | 82nd IETF, Tai Pei, Taiwan |
| **week 21 November 2011** | **23rd CENTR Administrative workshop (day tbc), Belgrade, Serbia** |

**DATE TO BE DECIDED FOR:**

| | |
|---|---|
| **Spring 2011** | **35th CENTR Legal and Regulatory workshop** |
| **Autumn 2011** | **6th CENTR Marketing workshop, Prague, Czech Republic** |
| **Autumn 2011** | **36th CENTR Legal and Regulatory workshop** |

**www.centr.org**