ccTLDs: autonomous but cooperative actors

Dr Farzaneh Badiei

ccTLDs: autonomous but cooperative actors

In this paper, I will trace Country Code Top Level Domain (ccTLD) operators' voluntary participation at ICANN and illustrate how they evolved and developed their policies and solutions without hierarchical control by ICANN (despite some early heavy-handed attempts to impose such policies on ccTLDs). ccTLD operators were also very much involved with the Internet Assigned Numbers Authority (IANA) transition and worked on enhancing ICANN's accountability and transparency. There are obvious incentives for ccTLDs to be involved with ICANN governance, and they have a vested interest in certain aspects of ICANN's governance. But the history of their involvement with the community and the driving force behind their voluntary cooperation can illustrate how and why internet actors participate in internet governance processes.

Tracing ccTLDs' voluntary cooperation with ICANN

Country Code Top Level Domains date back from before the Internet Corporation for Assigned Names and Numbers (ICANN) came into existence. The Domain Name System (DNS) was invented in 1982 and went into internet-wide deployment in 1984. In the same year, Postel and Reynolds issued RFC 920 (1984) which was about Domain Requirements. In that RFC, Postel and Reynolds included countries as top-level domains. To avoid politicizing the delegations, Postel used the 2-letter codes of the countries listed in ISO-3166-1 to define the labels of the ccTLDs.[1] IANA, in the person of Jon Postel, originally granted ccTLDs on a per-request basis, but he soon realized that a principle-based approach would be better. In 1994, Postel documented the process for the allocation of ccTLDs more formally through Request for Comment (RFC) 1591, "Domain Name System Structure and Delegation".

When ICANN was formed in 1998, the Generic Top-Level Domains (gTLDs) such as .ORG and .COM had to enter into a contract with ICANN and be quasi-regulated by ICANN. However, ccTLDs resisted such control[2] and therefore ICANN does not have the authority to take compliance action against ccTLD operators.[3]

The resistance to have a contractual relationship with ICANN did not mean that ccTLDs would also forgo cooperation though. ccTLDs in fact became one of the most active actors in ICANN. This paper questions why ccTLDs cooperate with ICANN despite having no contractual obligation to do so. From the interviews carried out with some ccTLD operators and by researching policy documents and mailing list archives, this paper concludes that ccTLD operators cooperated with ICANN for the following reasons: to preserve the IANA function, to respond to commercial incentives, to ensure collegiality and share best practices, and to get involved with policy development when it relates to their operations.

The early days of ICANN

When ICANN was established, ICANN staff provided a policy document that could apply to ccTLDs regarding the delegation and re-delegation (transfer of management of the TLD to another operator) of ccTLDs. The policy almost fully mirrored RFC 1591 but there were some crucial changes that were not acceptable to ccTLDs.[4] One of the most important additions to ICP-1 was granting ICANN the authority to revoke or re-delegate a ccTLD due to "misconduct", "violation of the policies set forth in ICP-1", or "persistent recurring problems with the proper operation of a domain". ICP-1 did not limit the revocation and redelegation to operational issues. It added the

1 Domain Requirements, https://tools.ietf.org/html/rfc920, J. Postel later on documented a more elaborate policy in RFC 1591, https://tools.ietf.org/html/rfc1591, 1994

2 Many ccTLDs resisted contractual obligations with ICANN. ICANN's authority over the root zone, however, gave it enough leverage to pressure some ccTLD managers into entering contractual relationships. See G. Christou & S. Simpson, Internet Policy Implementation and the Interplay Between Global and Regional Levels, in International Organizations and Implementation: Enforcers, Managers, Authorities?, 2006, p.75

3 ICANN, About ccTLD Compliance, https://www.icann.org/resources/pages/cctld-2012-02-25-en

4 ICANN, ICP-1: Internet Domain Name System Structure and Delegation http://archive.icann.org/en/policies/icp-1-archived.htm, 1999

ambiguous word "misconduct" (of the operator) to the text. In contrast, RFC 1591[5] did not explicitly reserve any right for IANA to redelegate or revoke; furthermore, it limited such inclinations to operational issues.

ICANN's early attempts to get involved with ccTLD affairs, combined with the governments' claim over their corresponding ccTLDs, made ccTLDs more attentive to ICANN and its decisions. ccTLD managers participated at ICANN frequently, and established the ccNSO to protect their interests and prevent ICANN from imposing rules on them. The risk of ICANN becoming the authority on who should be the manager of ccTLDs and when a ccTLD revocation should happen became more dire when ICANN, jointly with the respective governments, decided to re-delegate two ccTLDs: the ccTLD of Australia, .AU, and the ccTLD of Libya, .LY.

IANA's report on the re-delegation of .AU was quite alarming. In this case, ICANN had acted as the assessor of multistakeholder support within a local community and had made a non-technical, non-operational decision as to why the re-delegation should happen and who should run .AU. The report courageously mentioned that there was no technical or operational problem with the then operator of .AU, but the entities and individuals should be accountable to the internet community. It did not mention how the then .AU operator was not accountable and, as a rationale for its decision, referred to the government advisory committee principles which were issued in 2000, and which the ccTLDs opposed.[6]

A new beginning

Why do we not see re-delegation and delegation cases similar to .AU anymore? One reason is that ccTLDs participated in the processes and coordination at ICANN and among themselves. ccTLDs established regional domain name registry organisations and, to be more active at ICANN, in 2003 established the Country Code Name Supporting Organization (ccNSO). They successfully created and preserved their independence from ICANN, and in a way have turned ICANN into a rubber stamp on delegation and re-delegation decisions. In the framework of interpretation for the delegation and redelegation of ccTLDs, they have tried to limit IANA to a purely technical role.[7] Such independence is good for the internet from two angles: 1. ICANN's over-politicization would have led to an international crisis with the governments wanting to run ICANN. 2. ICANN and IANA exist primarily to ensure that the root zone works properly. Political decisions or even sometimes operational ones about removing TLDs from root zones because they are misbehaving or pose "security threats" was going to stop ICANN from following its mission of ensuring that the DNS remains globally connected.

It should be noted that ICANN (the organisation) has been trying to politicize its role and empower the governments over other actors.[8] The battle has not ended, but ccTLDs can bring more moderation to such imbalance.

The IANA function

One of the strongest incentives for ccTLD involvement with ICANN is the IANA function, which relates to maintaining the DNS root zone. The IANA function is partly the administration of TLD and ccTLD delegations in the root zone.[9] A single, global root zone by definition includes ccTLDs, and there is no viable alternative

5 J. Postel, RFC1591, https://tools.ietf.org/html/rfc1591, 1994, page 5. The paragraph ICANN tried to change, reads as: "In cases when there are persistent problems with the proper operation of a domain, the delegation may be revoked, and possibly delegated to another designated manager." http://archive.icann.org/en/policies/icp-1-archived.htm, 1999

6 IANA report on .AU redelegation, https://www.iana.org/reports/2001/au-report-31aug01.html, 2001

7 ccNSO, Framework of Interpretation of Current Policies and Guidelines Pertaining to the Delegation and Redelegation of Country-code Top Level Domain Names, https://ccnso.icann.org/sites/default/files/filefield_46435/foi-final-07oct14-en.pdf, 2014

8 This is evident from how ICANN drafted its contract with PTI, where ccTLDs had a role in fixing those problems. For more information refer to Stephen Deerhake, Presentation on PTI contract and how ICANN's contract was not optimal and invoked GAC principles. https://ccnso.icann.org/sites/default/files/file/field-file-attach/2016-12/presentation-iana-naming-function-agreement-06nov16-en.pdf, 2016

9 A list of IANA tasks, https://www.iana.org/performance

for ccTLDs if the root zone does not operate well or if they are removed from the root zone. Therefore, the maintenance of the root zone is very important for ccTLDs.

The root zone contains the delegations from the root to the nameservers of the TLD operators. The root zone database contains technical and administrative contact elements related to top-level domain names.[10] To keep the domain name system globally connected, certain coordination and upkeep must take place. It is important for IANA to perform that operation and implement the changes in a neutral and independent manner, in accordance with its mandate. IANA functions include maintaining the root zone and undertaking changes in accordance with ICANN's names community consensus policies. IANA functions are currently performed by Public Technical Identifiers (PTI), an organisation which was convened and incorporated in 2016.[11]

Because the IANA function concerns the root zone (where ccTLDs live with other TLDs), policies and governance changes that could affect the IANA function were of utmost importance to ccTLDs. On at least two occasions, ccTLDs were actively involved in internal policy making at ICANN that would affect IANA:

1. the IANA stewardship transition to the internet community;
2. ICANN's contractual arrangement with PTI.

1. ccTLDs' engagement with the IANA transition

Due to the importance of the IANA function for ccTLDs, ccTLDs engaged with the IANA stewardship transition, which started in 2014, to end ICANN's contract with the US government. This was an important issue for ccTLDs because of its consequences for the IANA function. They also engaged with the ICANN group mandated to work on accountability mechanisms for ICANN.

There were earlier attempts to rewrite ICANN's bylaws to make it a more powerful organisation. The IANA function transition required updating the bylaws with provisions related to IANA functions. Moreover, the US government approval for actions that would affect ccTLDs (either delegation or revocation) was always worrisome and undermined ICANN's legitimacy as a truly multistakeholder global organisation. Finally, the efficiency of the operation sometimes might have been affected because the US government was not as fast as non-governmental internet infrastructure actors in approving requests.[12]

2. ICANN's contractual arrangement with Post Transition IANA

ICANN (the organisation) was instructed by the ICANN community to transfer the operation of IANA to a not for profit organisation. In order to implement this recommendation, PTI was established, and ICANN drafted a contract that would govern the relationship between ICANN and PTI. The contract ICANN had drafted however had serious shortcomings that concerned ccTLDs. Some ccTLD representatives brought those issues forward to the ICANN IANA transition discussion platforms. The ccNSO, CENTR and other ccTLDs also filed public comments to address the shortcomings.[13]

The main points of concern were that the contract invoked the GAC principles of 2005 for the delegation and redelegation of ccTLDs and that it did not mention the framework of interpretation, which was the work of the ccNSO in collaboration with the GAC. In a way, it accepted that GAC principles were the policy for delegation and re-delegation. This worried the ccTLDs: in a discussion at the ccNSO, there was a call for collective action which successfully led to making the desired changes to the contract as requested by the ccNSO.[14]

---

10 IANA, The Root Zone Data Base, https://www.iana.org/domains/root/db

11 For more information about PTI refer to https://pti.icann.org/

12 A. Sullivan, US Congress Hearing on IANA Transition, https://www.iab.org/wp-content/IAB-uploads/2016/05/sullivan-to-senate-commerce-20160524.pdf, 2016, page 5

13 ICANN, Comments received by the community on the draft contract, https://forum.icann.org/lists/comments-iana-naming-10aug16/threads.html#00007, 2016

14 ccNSO, Teleconference meeting, https://ccnso.icann.org/sites/default/files/file/field-file-attach/2016-12/minutes-ccnso-council-meeting-01sep16-en.pdf, 2016

Security and stability of the domain name system

The overall security and stability of the DNS is also important to ccTLDs. Engaging with ICANN and its processes and being a part of the ccNSO signals their good intentions to contribute to the security and stability of the DNS by sharing best practices with their peers.

However, it is not all about voluntary cooperation. The security and stability of the domain name system is a purely technical matter. The DNS should respond to queries in a reliable and accurate manner. Since the DNS is a shared global pool of resources, security attacks on infrastructure can endanger all actors. Moreover, despite the fact that ccTLDs do not have a contract with ICANN, they are dependent on the operation of IANA. Furthermore, the contractual obligations that PTI (the operator of IANA) has with ICANN has some provisions regarding the suspension of ccTLDs due to security and stability issues. As a consequence, while ccTLDs do not have a contract with ICANN, they are incentivized to contribute to the security and stability of the DNS, because the IANA operator can take action against them if their infrastructure becomes a security threat to other infrastructures.

By participating at ICANN, ccTLDs have ensured that ICANN's mandate remains technical and limited. For example, in the Framework of Interpretation Working Group (FOIWG), "misbehaviour" of the operator is interpreted as a purely technical issue, stating that: "4.5. The FOIWG interprets RFC1591 to limit the IANA Operator's authority to step-in to situations where substantial misbehaviour by the ccTLD manager (a) poses a risk to the security and stability of the DNS or (b) involves the manager's failure, after notice and a reasonable opportunity to cure, to perform the objective requirements (i.e., to be on the Internet, maintain IP and email connectivity, identify a technical contact and to identify an in-country administrative contact)."[15]

Without the participation of ccTLDs, ICANN could have been empowered to remove ccTLDs from the root zone for bad behaviour that was not related to security and stability. Moreover, with the politicization of the internet and the geopolitical struggles this entailed, ccTLDs took a positive step in limiting ICANN's mission by taking over the policy-making related to the revocation of ccTLDs.

ICANN and ccTLDs: independent but interrelated policies

ccTLDs' internal policies, including how they manage the allocation of second-level domain names and facilitate domain name registration, are independent from ICANN policies and contracts. ccTLDs follow their own policies and applicable national laws. However, this independence is not absolute. Some ccTLDs involve themselves with ICANN regarding their own policies or when ICANN policies affect them. For example, they might invite ICANN to comment on their local policies so that they can follow their local laws whilst avoiding absolute conflict with ICANN policies. This happened in the case of CIRA (the operator of .CA for Canada). Canadian data protection law at the time required CIRA to publish personal information of domain name registrants in the WHOIS (the domain name registration directory). CIRA invited ICANN to contribute to its policy by submitting a public comment.[16]

If ICANN's policies could potentially affect ccTLDs, they get involved with the policy development process. As the next section will explain, ccTLDs' interest might justify such participation, but it can also be due to the fact that ccTLDs often adopt the same policies or refer the domain name registrants to an ICANN policy. ccTLD participation in policy processes that could affect their registrants and their local internet community is also of importance. For example, some ccTLDs, instead of having their own dispute resolution mechanism for resolving domain name disputes, refer the domain name registrants to ICANN's Uniform Dispute Resolution Policy (UDRP). It is therefore important for the ccTLDs to get involved with ICANN policies that they might adopt later on. In this example, the referral to UDRP has affected some ccTLDs' domain name registrants, as the language of the proceeding might not be the local language, or the UDRP panel might be biased and allow for trademark overreach. ccTLDs need to revisit their policies from time to time. Moreover, when ICANN is in

15 ccNSO, Framework of Interpretation Working Group (FOIWG), https://ccnso.icann.org/sites/default/files/filefield_46437/foi-revocation-07oct14-en.pdf, 2014, page 5

16 Canadian Internet Registration Authority and WHOIS, the then CEO invited ICANN to weigh in on CIRA's WHOIS policy: https://www.icann.org/en/correspondence/turcotte-to-twomey-25jul06.pdf, 2006

the process of revising policies that could affect domain name registrants, within ccTLDs, ccTLDs should get involved with those policy processes as well.

Commercial incentives

ccTLD cooperation with and their participation in ICANN policy development processes (such as policy processes regarding the allocation of new gTLDs) helps them gain legitimacy among their peers and also stops the development of policies that can damage the ccTLD commercial and non-commercial interests in general.

While ccTLD operators at an earlier stage had a conflict with the Government Advisory Committee to keep their independence, the GAC has served ccTLDs' interests in some instances. This is true for geographic domain names, which some governments believe belong to the nation-states and should not be allocated through the new gTLD program. The ccNSO agreed with that stance.[17] The GAC has also served the ccTLDs' interest with regards to reserving second level domain names that correspond to ccTLDs' labels.

In the case of two letter second-level domain names that correspond to ccTLDs, such as IT.SUCKS or IS.BABY, ICANN reserved two letter domains at the second level, preventing new gTLDs from registering them. Later on, the GAC advised ICANN to come up with a procedure for the allocation of such domain names. One of the voluntary solutions that ICANN came up with was: "Exclusive Availability Pre-Registration Period (voluntary): Registry Operators may implement an exclusive availability pre-registration for governments or ccTLD operators to register domain names corresponding to their country codes before the names are generally available".[18]

This meant that if registries allowed for pre-registration, ccTLDs had the opportunity to claim the second level domain names and then sell them off to interested registrars. This is only a hypothetical scenario and there is no evidence at the moment that ccTLDs have claimed these names. However, since they have the opportunity to do so, it could potentially be profitable for those ccTLDs that pre-register such names.

It is worth noting that support for reserving these names was not unanimous at the GAC; neither did all ccTLDs want such measures to be taken. Some ccTLDs have their rationale for supporting the pre-registration of two-letter domains that correspond to ccTLDs: to reserve them so that they do not cause confusion.[19]

In terms of geographic names, and as long as generic names are at stake, the ccNSO has showed its willingness to cooperate with the Generic Names Supporting Organization (GNSO) to come up with the right policy, which is specifically true for any new round of gTLDs. In the case of two-letter domains at the second level and geographic names, coordinated action with the GNSO where possible illustrates the cooperative nature of ccNSO.

Internationalized domain names (IDN) ccTLDs

Internationalized domain names are names made with a writing system that uses more than just ASCII characters. In the root zone, these are often known as IDN TLDs. The allocation of IDN ccTLDs that correspond to the country name of ccTLDs was one of the reasons some ccTLDs got more involved with ICANN, especially the ones that were managing ccTLDs in countries where a non-Latin alphabet was overwhelmingly used.

The allocation of IDN ccTLDs was not however a straightforward process. The early attempts to operationalize IDNs started in 1997 with a protocol suggested by Martin Dürst,[20] but the first successful protocol for IDNs did

17 Chair of ccNSO letter to ICANN then Board chair about disallowing geographic names that correspond to ccTLDs. https://ccnso.icann.org/sites/default/files/filefield_12869/disspain-to-dengate-thrush-21nov09-en.pdf, 2009

18 ICANN, Two-Character ASCII Labels Memo on Implementation, https://www.icann.org/en/system/files/files/implementation-memo-two-character-ascii-labels-22jan19-en.pdf, 2019

19 For example, LACTLD filed a public comment on two-character ASCII Labels consultation, explaining its concerns: https://forum.icann.org/lists/comments-proposed-measures-two-char-08jul16/msg00039.html, 2016

20 M. Dürst, Internationalization of Domain Names, https://tools.ietf.org/html/draft-duerst-dns-i18n-00, 1996

not come about until 2003.[21] There were many technical issues with the implementation of this RFC, which were gradually resolved by registries that used the RFC to register internationalized second level top level domains. Despite the persistence of the shortcomings, ICANN was under a lot of pressure to implement IDNs at least at country name level. The pressure led ICANN to allow the delegation of IDN ccTLDs in 2008. IDN ccTLDs have been delegated exclusively to the relevant ccTLD operators, in a fast track process started in 2009 in a multistakeholder fashion.[22] At the time this was a good solution as ccTLD operators had a lot of experience in how the local languages worked on the internet. However, there were shortcomings. For example, some IDN ccTLDs, despite having been delegated, have not yet been operationalized. Considering the current shortcomings, the IDN ccTLD delegation process should be improved and solidified.

The role of regional ccTLD organisations

The regional domain name associations and councils such as CENTR (members from Europe and some non-European countries), APTLD (members from Asia-Pacific), LACTLD (members from Latin America and the Caribbean region) and AFTLD (ccTLD members from Africa) also enhance the cooperation of ccTLDs with ICANN. Through memoranda of understanding with ICANN, filing public comments and holding regional capacity-building programs, they elevate the ability of ccTLDs to meaningfully participate at ICANN meetings and policy processes but also discuss the consequences of certain policies or best practices at regional level. ccTLD cooperation with ICANN was especially strengthened with the work of these regional ccTLD associations and council at ICANN in terms of the IDN fast track policy[23] as well as their involvement with the IANA transition and the Post Transition IANA contract.

The future of ICANN and ccTLDs

What is the future of ICANN and what are some interesting predictions about ccTLDs and their cooperation with ICANN?

Prediction number one, the DNS becomes irrelevant

One prediction could be that the DNS becomes irrelevant. There could be a superior protocol or a technology that overrules the DNS, revolutionizes the internet (or surpasses it) but keeps us in an interconnected global network. That technology would salvage us from the bureaucratic, politicized ICANN, but this seems to be far-fetched.

Prediction number two, ICANN becomes irrelevant (DoH takes over!)

Another possibility would be for ICANN to become irrelevant because of new protocols that empower browsers to add new names to their web servers. That protocol exists and is called DNS over HTTPS (DoH). A worry that is spreading is that, by using DoH, web servers such as Mozilla and content delivery networks such as Cloudflare could work together to serve name queries that are not in the DNS. For example, one could save on seven years of .Amazon's political conflicts over allocation by just adding .Amazon to the web server of Mozilla and by having Amazon and Cloudflare DoH servers respond appropriately. Geoff Houston from APNIC puts the problem across very clearly: "[with DoH] each web page is capable of constructing a local namespace that is

21 P. Faltstrom, P. Hoffman, A. Costello, RFC 3490, Internationalizing Domain Names in Applications, https://tools.ietf.org/html/rfc3490, 2003

22 IDNC Working Group, Final Interpretation Plan for IDN ccTLD Fast Track Process, https://www.icann.org/en/system/files/files/idn-cctld-implementation-plan-28mar19-en.pdf, 2019

23 On several occasions, these regional centers have communicated with ICANN with regards to the IDN ccTLDs Fast Track policy, for example APTLD wrote a letter to ICANN regarding the delegation of IDN ccTLDs, J. Shea, Chair of Asia Pacific Top Level Domain Association, https://www.aptld.org/documents/Others/201806/180.html, 2009; CENTR was particularly active in IANA transition discussions, providing informational material as well as contributing to public comments when it mattered. See CENTR's public comment on the proposed IANA naming functions agreement, https://forum.icann.org/lists/comments-iana-naming-10aug16/msg00001.html, 2016

essentially defined by that web page, and names can be 'bound' to that web context and may not be accessible via a general DNS query. For some, this may well look like a completely novel approach to naming, where names defined by DoH are tied into a referential context and do not necessarily exist outside that context. It challenges the characterisation of the DNS as a single unified and uniform namespace as it allows the creation of private branching within the namespace".[24]

But this threat is not novel at all. There have been many alternative root zone debates and fears of DNS fragmentation. Fragmentation of the DNS means not having a unified DNS. Will it happen? The answer to this question, as long as we are not technically and economically analysing the phenomenon, can vary depending on the respondent. Some ccTLDs believe that adopting DoH at the application layer and eliminating ISPs is a very bad idea. It might affect their business and surpass ICANN which provides the appropriate oversight for domain name allocation, so they believe it is a big risk to their existence and to keeping a distributed internet with accountable actors. Nevertheless, interoperability has historically been valuable to internet users, and having purely local namespaces that might give different answers from a different server do not seem likely to promote interoperation.

Another take on the current deployment of DoH is that DoH will not be used in the ways that have been predicted, because identifiers on the internet need to work. It might be a threat to filtering and blocking, but the DNS and ICANN are going to stay. The argument is that the unified root zone is only unified and authoritative because "networks have found it as a common path to collaborate together." They have granted ICANN the authority to operate the root zone by using its name servers and accepting the root zone as a shared namespace. To be able to take ICANN's authority away, all the networks would need to find another common path which is costly and perhaps impossible. The decision to replace the DNS with DoH will have to involve ccTLDs, TLDs and other actors, otherwise it cannot happen.

In its report on DoH, CENTR argues that the replacement of the DNS with DoH might in fact not require ccTLD and TLD involvement and cooperation. Since only a handful of powerful web servers handle most of the traffic on the internet, "should they (jointly or individually) decide not to respect the authority of the root zone, they could easily do so without repercussions".[25] It is argued that if the web servers do not respect the authority of the root zone, they can also surpass ICANN, ccTLDs and TLDs. Hence, CENTR has been raising awareness about this issue and companies such as Mozilla and Google which intend to use DoH are clarifying their modes of deployment. In a recent meeting at the Internet Engineering Task Force (IETF), Google and Mozilla explained that in deploying DoH they have adopted a set of criteria that could potentially alleviate some of the concerns. For example, Google explained that using DoH is voluntary and that Google will use more than one DoH resolver.[26]

There are many arguments and counter arguments regarding the deployment of DoH at this stage. The future of DoH and how its deployment could affect the ccTLDs, ICANN and the multistakeholder Internet community is yet to be seen.

Summary

The history of ccTLDs' cooperation with ICANN can illustrate what has been the cornerstone of internet operation for a long time: it is not the authority and contractual relationship that facilitate cooperation with regards to the governance of the root zone. Collaboration in the service of a common functional aim can also lead to optimal performance and good governance of the root zone.

---

24 G. Houston, DoH! DNS over HTTPS explained, https://labs.ripe.net/Members/gih/DoH-dns-over-https-explained, 2018

25 P. Van Roste and P. Malaja, CENTR Issue Paper on DNS over HTTPS, https://centr.org/library/library/policy-document/centr-issue-paper-on-dns-over-https.html, 2019, page 5

26 IETF 105, Montreal, notes of the meeting: https://etherpad.ietf.org/p/notes-ietf-105-add?useMonospaceFont=true,2019; a video with Google, Mozilla and others about DoH at IETF 105, https://www.youtube.com/watch?v=n5UjPQksHT8, 2019

Council of European National Top-Level Domain Registries

CENTR is the association of European country code top-level domain (ccTLD) registries, such as .de for Germany or .si for Slovenia. CENTR currently counts 54 full and 9 associate members – together, they are responsible for over 80% of all registered domain names worldwide. The objectives of CENTR are to promote and participate in the development of high standards and best practices among ccTLD registries. Full membership is open to organisations, corporate bodies or individuals that operate a country code top level domain registry.

This paper is part of a series of articles covering industry research, historical data analysis and the future of technologies such as digital IDs, published over the course of 2019 to mark CENTR's 20th Anniversary. These publications do not necessarily present the views of CENTR or of the CENTR community.

CENTR wishes to thank and acknowledge the organisations which have so generously contributed to the efforts of its 20th Anniversary:

Platinum sponsor

Gold sponsor

Silver sponsor

CENTR vzw/asbl
Belliardstraat 20 (6th floor)
1040 Brussels, Belgium
Tel: +32 2 627 5550
Fax: +32 2 627 5559
secretariat@centr.org
www.centr.org

To keep up-to-date with CENTR activities and reports, follow us on Twitter, Facebook or LinkedIn