Council of European National Top-Level Domain Registries

Report on RIPE78

Reykjavik
20-24 May 2019

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

Contents

Highlights

RIPE at 30, defending against becoming a "Routing Police"

The RIPE community celebrated its 30th anniversary at the meeting in Reykjavik, Iceland. Quite aptly, participants had fundamental discussions about the nature of RIPE's policy development work. They also discussed potential steps to rethink and rebuild one of its core infrastructures, the RIPE database, which holds information about all resources allocated to its members.

Three founders attend an evolved RIPE meeting

In May 1989, a group of 14 experts met to consult about connecting their various IP networks, support IP connectivity in Europe and consider how to coordinate IP networking activities and resources in the future. According to the minutes recorded from the meeting in Amsterdam, "it was agreed that all issues to be discussed are of a technical nature and do not constitute politics or policy in any way. As a working title for the activities the meeting adopted the name RIPE (Réseaux IP Européens)".

Three out of these 14 founders had travelled to the Reykjavik meeting, including Daniel Karrenberg (today Chief Scientist at RIPE NCC), Rüdiger Volk (today at DTAG) and Arnold Nipper (today at DECIX), but the community has changed considerably since their first encounter. With over 700 attendants, the 30th reiteration of the RIPE meeting was one of the largest ever. Meanwhile, the number of members climbed another 8% last year to a total of 22,500.

From technical coordination to control

The incredible growth – a result of the running-out of IPv4 address space and the promise to assign small blocks to every newcomer joining the club – plus the added attention IP resource management has received over the years has resulted in new considerations in the RIPE community over how to ensure accountability processes, how to best manage policy development processes and how to formalize some rather informal processes, such as the selection of a RIPE Chair (see below).

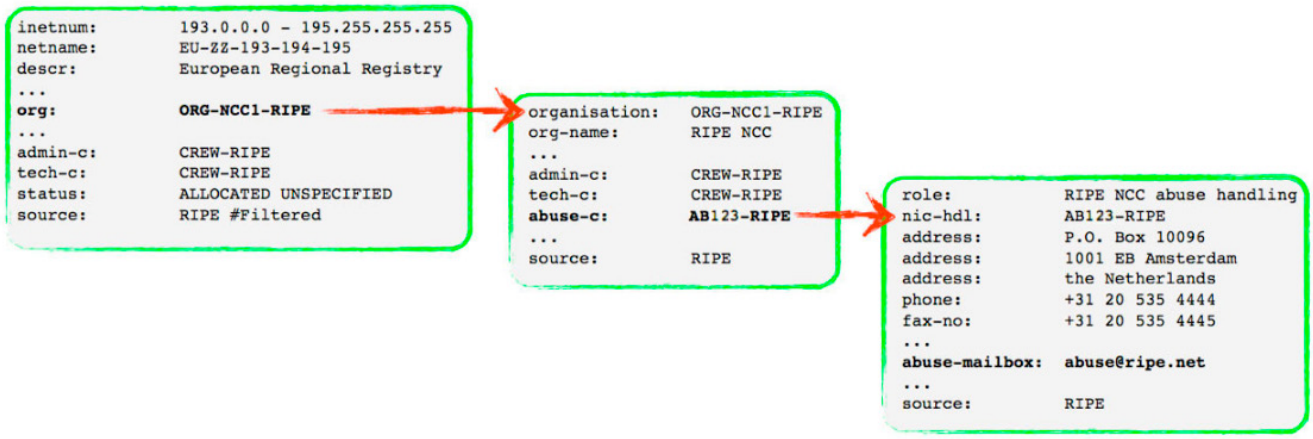
The current discussion on two new anti-abuse policies illustrates the dilemmas RIPE now faces. Jordi Palet Martinez, a well-known consultant on IPv6 inter alia for public authorities (including the European Commission), presented two documents aiming at tightening sanctions against resource holders who are unresponsive to complaints they receive via the anti-abuse contact email registered in the RIPE database or who are engaged in some sort of BGP hijacking.

The so called abuse-c record was introduced in 2013 after lengthy debates in the RIPE community. It was only last year that a follow-up policy ruled that the RIPE NCC had to check on an annual basis if the recorded abuse contact is still valid.

Angela Dall'Ara of RIPE NCC reported back to the community on the first ever round of re-validation of the abuse-c records. Dall'Ara reported that after checking 18,200 addresses of the 22,500 members, only 60 addresses were still waiting for validation. The check of the abuse-c of LIR resources was also finalized. The validation of abuse-c records of end-user resources is still to be concluded.

Palet's new policy proposal now wants to step up the game by stating that the purely automated handling of complaints is not good enough. In the future, RIPE NCC's validation process should include human intervention at some point in the process. After an initial phase of 15 days and additional escalation days, RIPE would be free to sanction the reluctant resource owner. Given that according to RIPE 78, the violation of RIPE's policies can result in the de-accreditation of resources or closure of membership, non-responsiveness or a single automated reaction can cost dearly.

Palet is hoping for a similar sanction system with an earlier policy proposal. While not spelled out in detail in the actual policy text, the title "BGP Hijacking is a RIPE policy violation" tells the tale. During the Abuse Policy WG session in Reykjavik, Palet underlined that only the deliberate use of third-party resources would fall under the new policy. He also said the title seemed a little misleading: "we do not want RIPE NCC to become the routing police", he said.



To decide whether a violation was done on purpose or by accident, a group of experts from a worldwide pool would review the complaints filed by the victims (including data points on networks affected, offender ASN, hijacked prefixes and timespan). RIPE NCC would provide a web-based form to make it easier to file a complaint. Appeals will be possible against the draft and the upcoming final report by the experts. A hijack would constitute a RIPE policy violation, Palet writes in the policy, even if both parties were located outside the RIPE region.

RIPE members: beware of becoming the routing police

Both policies were met with emotional objections, both in the run-up to the mailing list as well as during the meeting, mainly during the Abuse WG session.

Via the mailing list, Nick Hilliard of INEX warned against the weaponization of the registry data, turning the registry data "into a mechanism for punishing people when they do things that other people don't like". Given the span of the RIPE region, there was an "endless list of things

which are considered offensive or illegal in some or all jurisdictions in the RIPE NCC service area, for example spam, porn, offending political leaders, gambling, drugs, other religions, political dissent, blasphemy and so on".

Peter Koch of DENIC called Palet's proposals an "abuse of the identifier system for content control and punishment of misbehaviour" and rejected Palet's pointers to his efforts (and partly successes) to introduce similar policies in the other RIPE regions. Hopefully, he said, RIPE will resist these "abuse" efforts. Instead of adapting to calls from the increasingly involved law enforcement community, a number of members called for considerations on how best to reject non-technical requests.

Cost-benefit and next steps for abuse policies

Other RIPE members underlined the dubious cost-benefit calculation. The "human contact" obligation would cause considerable "organisational" headaches to third parties and the RIPE NCC. To do the first annual checks for the abuse-contact mailbox, the NCC had to hire 3 full-time persons for the project. At the same time, no additional benefit in better abuse handling would come from it, warned Michele Neylon, Blacknight Registrar. Industry experts like RIPE Chair Hans Petter Holen (Chief Information Security Officer at Visma) and Martin Levy (Network Strategist at Cloudflare) pointed out that network management automation was a trend, and that punishing network administrators for it without discrimination was contrary to that trend. Other arguments against the additional abuse-c policy were the lack of proportionality (which any court would therefore reject, Hilliard noted), and the sheer lack of clarity in how the policy was written.

For the "BGP hijacking is a policy violation"-proposal, a preliminary impact report of the NCC presented by Marco Schmidt stated that while such a policy was possible, the structure proposed to deal with the reporting and "judging" of hijacking events was tricky. Given that around 1-2 events per day could be reported, a large expert pool would be needed. Given the difficulties of attribution and distinction between deliberate and accidental, highly competent pool members would be needed. Furthermore, the policy could only be "enforced" against Local Internet Registries (LIRs, operators) in the RIPE region.

After the session, this reporter asked Palet about what next steps he considered for the proposals, given the lack of support during the meeting. Palet said that he intended to do new versions of the documents. At the same time, he noted that consensus would not be judged on the RIPE meeting discussions, but on the basis of the wider debates on the mailing list, where there was a balanced reaction with support expressed as well, he said. Brian Nisbet, Chair of the WG, underlined that the mailing list discussion was essential.

RIPE's Russian case

Discussions over the closure of two Russian RIPE members aptly illustrated how difficult it is to decide if a member's actions qualify as policy violations. Russian members LLC GCX and NetUP LLC were closed in February 2019 because they provided falsified information in their applications for resource assignments.

In the case of LLC GCX, RIPE NCC was told by the third party, for which LLC GCX had registered addresses, that they were not the holders of the respective resources. The information in the RIPE database was fraudulent. According to a report by the arbiters, GCX "stated that it is not commercially interesting for a sponsoring LIR to do extensive validation of their customers and sponsoring LIRs might not always have the legal resources to do so". In the case of NetUP, arbiters agreed with RIPE that the member acting as the sponsoring LIR had provided the RIPE NCC with a false end-user assignment agreement for the registration of independent resources. The end user had stated that the contract provided to RIPE NCC "had not been signed by them or by anyone authorised to sign on their behalf".

During the RIPE Services WG session, RIPE NCC Counsel Athina Fragkouli explained RIPE NCC's due diligence work in general, rejecting claims that the RIPE NCC would try to "punish" members for mere "mistakes". Contradicting the argument by Alexander Isavnin (Russian Internet Protection Society) that one of the closed members had merely made a mistake and was a respected provider, Fragkouli underlined that the RIPE NCC was looking for patterns. With 72 countries in the RIPE service region and considerable differences in legislation and provision of identification for persons and registered companies, due diligence and ID checks constituted difficult work.

At the same time, the RIPE NCC noted a growing number of fraudulent registrations. According to RIPE COO Felipe Victolla Silveira, investigations of possible falsified information have doubled in 2018 (240 instead of 120 in 2017).

RIPE Chair selection

One of the policy discussions which illustrates RIPE's maturity level at 30 is the chair selection process. Current Chair Hans Petter Holen (Visma) was still "crowned" by his predecessor, the late Rob Blokzijl. Blokzijl himself had been Chair for a quarter of a century before selecting Holen, while at the same time assigning him the task of creating a selection mechanism. In the future, the Chair and Vice-Chair will be selected according to a specific process. There will a maximum tenure of two 5-year terms (consecutively or not) and the possibility to recall a Chair. Interestingly, the community has opted against a voting system and in favour of using a nomination committee of people trusted by the community.

The necessary policy documents for the future RIPE Chair selection are ready for last call, as announced during the closing plenary by Holen. In Reykjavik, another BoF session was used to present documents on a nominating committee (NomCom) and on the RIPE Chair selection.

In January, a first document on the tasks of the RIPE Chair was published, which consists of a job description that mainly includes a moderating, steering function.

For the NomCom document, the task force adapted the Internet Engineering Task Force's BCP10. Cornerstones include that the Chair of the RIPE Nominating Committee will be appointed by the RIPE NCC Executive Board, then the NomCom members will randomly select from a pool of volunteers. The outgoing RIPE Chair (and potential additional experts) will act as advisors.

The process to nominate a NomCom Chair and transition from one chair to another will take place over three RIPE meetings: nomination, consultation and transition (see timeline below).

Holen announced last calls for the two documents and said that he had not yet decided if he would run for a second term.

Event	Time / Deadline	Nominal Month
NomCom chair appointed	15 days before nomination RIPE Meeting	April / 1
Nominations RIPE Meeting	two meetings before transition RIPE Meeting	May / 1
Call for nominations	during nomination RIPE Meeting	May / 1
Call for NomCom volunteers	during nomination RIPE Meeting	May / 1
NomCom volunteers announced	30 days after call for volunteers	June / 1
NomCom announced	45 days after call for volunteers	July / 1
Nominations close	60 days after call for nominations	August / 1
NomCom organised	60 days before consultation RIPE Meeting	August / 1
Nominees announced	15 days before consultation RIPE Meeting	Sept / 1
Consultation RIPE Meeting	one meeting before transition RIPE Meeting	Oct / 1
NomCom makes selection	90 days before transition RIPE Meeting	Feb / 2
Selection Confirmed	30 days after NomCom makes selection	March / 2
Selection Announced	15 days before transition RIPE Meeting	March / 2
Transition RIPE Meeting		May / 2
NomCom Report	during transition RIPE Meeting	May / 2
Transition	during transition RIPE Meeting	May / 2

Tabula rasa for the RIPE Database?

Despite all-clear signals from RIPE's legal department last spring regarding compliance to the EU General Data Protection Regulation (GDPR), it has become evident that more clean-up is necessary, said Dennis Walker, Co-Chair of the RIPE Database WG. During the session in Reykjavik, Walker asked the "Gretchenfrage": should the RIPE community take a shot at the outgrown RIPE Database and start a clean sheet approach? In Reykjavik, there was no opposition to creating a task force to first re-consider the purpose of a RIPE Database in the first place.

Walker said there were still around 2 million personal data points simmering in the RIPE databases, most of which could not easily be justified. What is more, while through its clean-up campaign the RIPE NCC had deleted about 130,000 personal data points since RIPE77, during the same period 105,000 had been added. During the Reykjavik meeting alone, he calculated another 2,500 were added. Walker called for a change in mindset in the RIPE membership. While 20 years ago nobody cared, nowadays the publication of personal data had to be either clearly justified by a purpose or the data should not be published.

Walker presented a list of questions to be considered regarding the purpose of a RIPE Database:

- What is a contact?
- What data is needed about a contact?
- Who needs to contact who and for what reason?
- Who needs to access contact data?
- Where should contact data be stored?
- How should contacts be referenced by operational and organisational data?
- Should all, part or none of the contact data be public?
- How to access contact data
- What are the RIPE Registry requirements for contact data?
- What are policy requirements for contact data?
- What are operators/resource holders requirements for contact data?
- Personal vs corporate contact data
- Organisations that are personal
- Is any personal data needed for any purpose?
- Mindset shift in resource holders about (not) entering personal data
- Clarity over who is responsible/liable for (personal) contact data entered into RIPE Database, against any new published guidelines
- Other interested parties (e.g. LEA, researchers) needs for/access to contact data
- Legacy personal data including data auto generated during the early registry transfer process
- How to transition from where we are now to where we want to be, over what timescale

While this could possibly be a clearing-kick amidst the GDPR issues and growing discontent with the quality of the often-outdated information (stale data) from law enforcement parties for example, a "clean sheet" approach could certainly end in a hot debate over purpose and uses of data – not very different from the Whois debate at ICANN.

Daniel Karrenberg (RIPE Co-Founder and Chief Scientist) and Nurani Nimpuno (Asteroid) spoke in favour of defining the purpose to restart the database. Both favoured the task force to either include or consult broadly with interested parties from different areas. Karrenberg called law enforcement the "elephant in the room". Peter Koch (Denic) recommended participants not to forget "the mouse" in the room – data protection experts. Without mentioning ICANN, he pointed to ICANN's failure to include data protection officials in the same way as law enforcement parties in the Whois debates at ICANN.

Other interesting news from the RIPE Database WG are the change from Google Analytics to an open source, self-hosted analytics system called Matomo (formerly Piwik). According to the RIPE NCC Database team, Matomo is "more anonymous" as "requests just go back to our own service. The client IP is anonymized on a /24 level. No other user data is stored, session data is only stored for 90 days and aggregated data across the whole service is stored for longer than that for historical analysis".

Another interesting fact is the attempt to use RPKI to perform some clean-up in RIPE's international routing registry. The policy proposal (2018-06) focuses on false data in the RIPE non-authoritative routing registry (IRR, RIPE Non-Auth) and reads: "If an object stored in the non-authoritative RIPE IRR ("RIPE-NONAUTH") conflicts with a RPKI ROA issued by one of the five RIRs,

then the IRR object must be deleted by the RIPE NCC".

According to RFC 6811, to determine whether IRR objects are in conflict with the RPKI route origin authorisations (ROAs), the origin validation procedure is applied using prefix and origin ASN instead of BGP updates. The most recent version of the policy which is currently under discussion eyes a notification window for the holder of the IRR object that is about to be deleted. A timeline for notification before deletion is still under discussion.

Recently, route origin validation has been taken up more and more by large providers. During the plenary, Alex Band (NLnet Labs) presented new software to set up one's own certification authority for users who want to sign their resources, as an alternative to the hosted versions RIPE NCC offers, for example. According to the experts, cleaning up the IRR still has to be done as a new RIPE database is years away.

Who are we?

With the ongoing disputes and upcoming discussions about a potential clean-slate database, an essential question is now taking centre stage: who is the RIPE community and what is the core task of its self-regulatory policy process?

The accountability task force has filed its recommendations, which will be taken up by the RIPE Chair to follow-up with next steps. The "who are we" question has become more critical with the number of members spiking and the growing interest from outside bodies.

In a dedicated BoF about the "Big Picture", the future of how to engage as a community was – beside the database question – the top issue. RIPE Chair Hans Petter Holen (Visma) asked if the organisation was adapting to the new members and new constituencies, including human rights organisations as well as law enforcement and regulatory representatives. Holen pointed to the 2 million personal data points LIRs have left in the database and recommended focussing on keeping the networks running, while keeping law enforcement happy.

RIPE NCC CEO Axel Pawlik said he felt as if he was sitting in the midst of a more fractured community, which showed off in the mailing list debates. While it was nice to say that the self-regulatory process worked and even the governments, like the German Ministry of Interior, attended the meetings and engaged in the discussion, many remote participants and mailing list commentators complained of their dissatisfaction. Pawlik said that he was afraid that "the people with the big stick might be going off doing the bad thing".

The rough tone on the mailing list where hundreds of mails were exchanged about the abuse proposals (see above) was criticized during the meeting and described as "uncivilized". Yet Peter Koch (DENIC) warned against accepting mere +1s in big numbers when consensus is "measured". Making RIPE decision-making vulnerable to outside campaigning, he spoke of "social media -style decision-making". Organizing self-regulatory decision-making with the many new RIPE members as well as the wider community was a challenge, BoF participants agreed.

Part of the membership clearly favours sticking to the technical coordination task, warning that RIPE should not become a "morality police" (Jim Reid). Other long-time members call for nuance, like Nurani Nimpuno: "while we are no political body, that does not mean that we cannot talk values". Organizing the joint deliberation and then judging consensus has become a difficult task, she said.

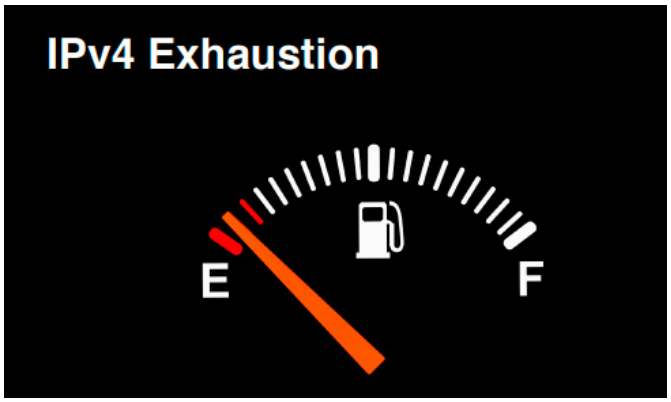
Niels Ten Oever, one of the human rights activists and a researcher at the University of Amsterdam, called on the community to take on responsibility for the trust and respect RIPE enjoyed. Ten Oever proposes to allow "value based routing" by introducing two new fields in the routing registry. With "AS-GDPR" set, the respective member declares that it is compliant with the GDPR. With AS-UNGP, the member declares itself compliant with the "United Nations Guiding Principles on Business and Human Rights". Other members could, if they wanted, set their filters for routing accordingly.

While the well-attended meeting was grappling with how to proceed, there was applause and at least some recommendations. Randy Bush (Internet Initiative Japan), a known figure in the RIR and standardization world applauded RIPE's style. Contrary to other RIRs, it was giving operators and researchers a home and slowly adapting to new developments including the implementation of a Chair selection mechanism (or onsite child care). Milton Mueller, Georgia Tech University and a former member of ARIN's Advisory Committe, reminded RIPE that it had a unique platform to organize self-regulation across borders in a democratic way. "Don't try to adapt your governance model to the rest of the world", he said.

Rüdiger Volk (DTAG), one of the founding members of

RIPE, underlined the need to bring much more debate back to the plenary, in an effort to organize the joint deliberation and decision making.

Scarcity: The (IPv4) end is near



It is unclear when the final IPv4 "crumbs" will be assigned to the still growing number of RIPE members. "We don't know if IPv4 will make it to Rotterdam (RIPE79)", Nikolas Pediaditis (RIPE NCC) said in Reykjavik. But the registry is nearly certain that there will be nothing left by RIPE80 in Berlin. Under its last mile regime, RIPE NCC has handed out 4,053 contiguous /22-packages of left-over IPv4 space. Another 3,088 /22-pieces are left. With an average consumption rate (last six months) of 475, it could take little more than half a year before RIPE NCC has to announce that everything is gone.

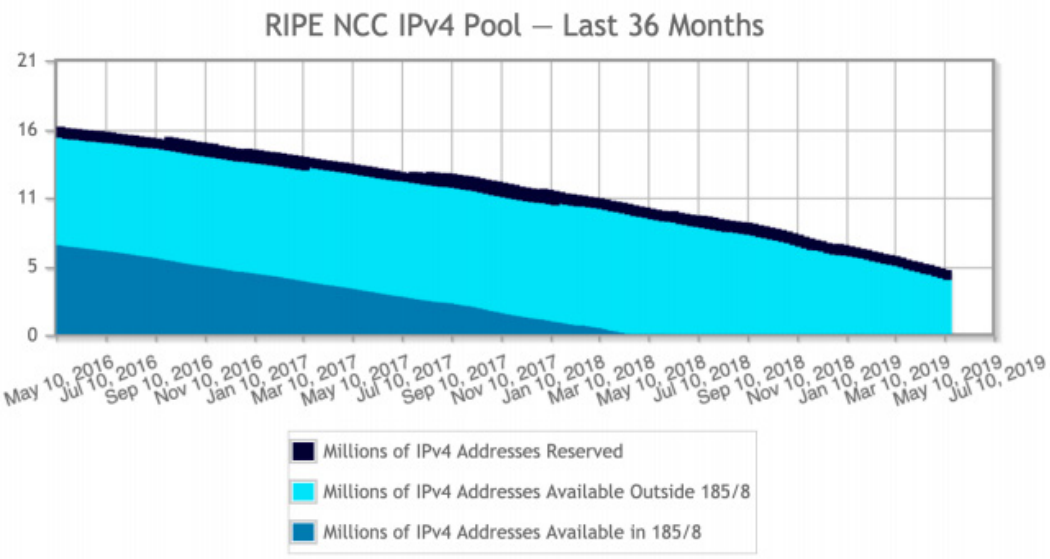
At the same time, Gert Döring, Address Policy WG Chair (SpaceNet) told this reporter that there are more members that have not yet fetched their last /22 block than there are /22s left. If everybody would call in the promised space, the pool would be empty. At the same time, RIPE membership continues to grow, and every new member receives their /22 alongside a package of IPv6.

When the pool is empty, addresses will have to be assigned based on a "first-come-first-served" waiting list. Preparations for a waiting-list policy are currently under way. For waiting list beneficiaries, the block to be assigned will be even smaller. A /24 (half the addresses as from a /22) has been proposed.

At the same time, a policy has been proposed to put more reserves into the pool dedicated to incoming Internet Exchange Points (IXP). Currently, a /16 has been reserved and half of the space has been allocated. The new policy wants to set aside a /15, sharpen the allocation criteria and possibly change the size of the one-time allocations.

As soon as the current IPv4 space for members has run dry, RIPE can only hand out space retrieved from various resources, for example when space is given back or found unused and recalled by the registries. As IPv4 is increasingly becoming a financial asset (see the meeting of brokers below), not much will be returned.

At the same time, RIPE will soon have to ask IANA for its second IPv6 allocation, as it has handed out around 80 percent of its first /12 block of IPv6 addresses. As the first RIR, it is eligible to ask for a second /12. The RIPE NCC closely followed a trend of members to collect large amounts of IPv6 addresses. For example, one RIPE member has 52 IPv6 allocations.



Interesting work on the IPv4 market was presented by members of the internet Governance Project (Milton Mueller and Brendon Kürbis, both Georgia Tech) during the plenary.

Number of allocations	Members	Total Allocations
1	13013	13013
2	681	1362
3	167	501
4	74	296
5	33	165
6	19	114
7	22	154
8	7	56
9	15	135
10	12	120
11	11	121
12	6	72
13	8	104
16	1	16
17	1	17
18	4	72
19	1	19
20	1	20
21	1	21
28	1	28
31	1	31

IP-Brokers – Code of Ethics?

For the first time, IPv4 brokers who are active in the RIPE and other RIR regions got together during RIPE78 in Reykjavik. According to Mike Burns (IPTrading) who chaired the Broker BoF, the goal was to share experiences, find potential partners and perhaps initiate work on a code of ethics.

About a dozen brokers took to the microphone, with many from the US, a few Western Europeans, two Russian address traders and one company headquartered in Asia. RIPE NCC got raging reviews for being very fast when it came to processing transfers, including inter-RIR transfers. Transfers could be processed in 48 hours while ARIN took around a week. Burns also noted the brokers loved RIPE addresses for coming without heavy rules attached to it. The list of brokers accredited by RIPE NCC is the longest of any RIR (around 70 compared to 30 at ARIN and 20 at APNIC).

One of the topics discussed by the participating brokers was the various business models in IP brokering. Some have contracts with either seller or buyer, some with both.

Paul Lam from the Hong Kong -based Larus Cloud Service Ltd explained that due to rising prices for IPv4 address space, his company was willing to lease address space and would be prepared to help other brokers with leasing contracts for a fee. Larus would also manage potential abuse problems and would fine leasing customers who violated the rules. The idea of leasing via Larus (plus abuse management) was received with great interest by other brokers. It was a good example of how competing brokers could cooperate, said Burns.

Another concept in the trading business were “flipping contracts”. Flipping means sellers will not know what buyers paid, and vice versa, allowing the broker to reap a potential difference. Eric Bais, address policy Co-Chair and owner of an IP-trading company himself, said the practice would violate RIPE policies. Burns underlined that while the practice was not banned in other LIR, his company, IP trading Ltd currently abstained from using that business model as it was frowned upon by some.

The brokers’ next step is to start working on an ethical code of conduct, which could include practices such as flipping. Brian Dickson (GoDaddy) asked participants to also consider the effects of routing table growth through splitting IP blocks during sales but Burns said that was too much to expect from brokers. “Every broker in this room will have split blocks”, he said. Eric Bais explained that routing table growth was not a broker problem, but a networking problem.

Work on the brokers’ ethical code of conduct will be initiated on a mailing list. In a quick show of hands, all brokers said they expected IP address brokering to keep them busy for at least the next 10 years.

Working Groups and RIPE Plenary Snippets

DNS Working Group – DoH and DoT in Software projects

It seems to be impossible to have a DNS meeting anywhere without looking into the DoH-DoT schism. The DNS WG meeting was presented with a different view of the development. Instead of reiterating the political debates spurred by the schism, Carsten Strotmann (Men &Mice) looked into the software developments spurred by the two competing protocols. The core recommendation from his study nevertheless touches policy: given that there is now a rich software environment to support DoH and DoT, ISPs should hurry to implement privacy-enhancing protocols, otherwise the traffic (and data) of their users will move to the cloud.

Strotmann briefly summarized the differences of both protocols (dedicated port 853 for DoT, making blocking easy, vs wrapping DNS queries into the HTTPS stream of DoH, implementation advantage for DoH via HTTPS libraries, making DNS an "app"). At the same time he found that the two protocols are highly similar. Both are currently implemented with outsourcing queries to third party resolvers outside the user's local network (see graph below). This is largely a result of the lack of local network implementations. In a side note Strotmann mentioned that the lack of DANE as an alternative to CA certificates for DoT was an issue.

The so-called TLS DNSSEC chain extension, introducing DANE as an alternative path for authorization, has been rejected by the IETF, due to opposition by browser companies, according to Geoff Huston. It could allow DNS privacy operators to get rid of known issues with the CA certificate system. During the meeting Huston bluntly said: "Infecting DoT with the CA mess is the first step to hell". Unbound (soon) as well as Knot (already) support DoH beside DoT. Petr Špaček (CZ. NIC) nevertheless qualified the DoH vs DoT efforts: "We hate DoH implementation, so please don't use it". As was illustrated by the efforts of the DNS open source software providers', DoH has been gaining on DoT when it comes to implementation. With regard to the software projects that have been counted, Strotmann listed 32 DoH and 23 DoT software projects on GitHub and Gitlab (see full list here). The list includes:

- *four applications (Firefox, Chrome curl, Tenta-Browser (Android), Bromite Browser (Android))*
- *three system resolvers (systemd-resolved/Systemd-based Linux, unwind/OpenBSD, resolver module for Linux glib/nsswitch.conf)*
- *eight client-proxies (SDNs, dnscrypt-proxy2, veild, Stubby, Unbound, Cloudflare, Dohnut, dns-over-https)*
- *four server proxies (rust-doh, dnsdist, dns-over-https, dnss)*
- *three DoH and or DoT servers (Unbound, Knot, SDNs)*

In a separate presentation Strotmann presented the OpenBSD system resolver Unwind, which can run on a laptop and offer the user with DoT and (opportunistic) DNSSEC validation. The resolver allows users to decide on their preferred resolving strategy, for example when captive portals come in between. The software, according to Strotmann, monitors DNS resolution and switches between the different resolving strategies (direct recursion, use of the DHCP supplied DNS resolver, use of configured DNS-over-UDP forwarder, use of configured DNS-over-TLS forwards), in an order that configurable by the user.

The fading of ENUM? - and other brief DNS news

For 15 years RIPE NCC has been acting as a registry for the global e164.arpa registry, under instructions by the internet Architecture Board (IAB) and in coordination with the International Telecommunication Standardization Bureau (ITU TSB).

Today at least 22 of the current 57 public delegations have developed some kind of technical issues. According to Marco Hogewoning (RIPE NCC) 16 had lame delegations and a lot of contact details are outdated and wrong (in what is erroneously a government-controlled space). Though they are all obliged to be DNSSEC-signed, not all ENUM zones are.

Since the summer of 2018, the RIPE NCC has been working to renew and clarify the original instructions for the delegation of ENUM zones. The respective document has been approved by both the IAB and the ITU. A zone deletion procedure was also added to the new document.

According to Hogewoning, now is the time to approach the various zone administrators / governments to fix issues and if necessary also to close zones.

ENUM (the use of phone numbers as domains) seems to have failed to take off, partly because those best situated to make services based on it – the telecom operators – chose to use it as private service (internally in their networks) while not offering it to their customers. Hogewoning said that ENUM was highly popular with mobile networks operators, but their use could not be documented as it was not visible in the public DNS.

The DNS WG also heard a presentation by Anand Buddhev (RIPE DNS Team) who briefly revisited the change from using Secure64 for DNSSEC signing to using Knot's embedded signing. He also pointed to an upcoming decision on whether to remain a customer of Neustar for DDoS protection – which has acquired this part of the business from Verisign (RIPE NCCs former supplier).

Roland van Rijswijk (NLnet Labs) gave a presentation on revisiting DNSSEC keytags, and Dave Knight merely pointed to a summary of the 30th DNS OARC meeting (with yet another half a dozen DoH presentations or more). DNS OARC has clearly become so successful that three meetings a year will now be planned going forward (one of which will be collocated with RIPE).

DNS Plenary Updates

Another DNS Flag Day

After a positive conclusion from the https://dnsflagday.net/ DNS flag day 2019, several of the flag day initiators want to continue to "clean up" the DNS. According to Petr Špaček (CZ.NIC) and Ondřej Surý (ISC), following discussions at the recent OARC meeting in Bangkok, operators and software vendors have set their eyes on IP fragmentation and blocking TCP transport for DNS.

During the first flag day which was focussed on EDNS workarounds, the breakage rate could be kept at relatively low rates, and an additional 5.6% of domains were picked up on. For Špaček, measurements showed that Chinese Provider HiChina had the bulk of broken domains (70%). A similar distribution is expected with regard to the chosen candidate for the 2020 flag day, including mandatory TCP support. One hypothesis is that a number of parked, unused domains could be behind the concentrated numbers.

TCP support has been made mandatory for DNS servers by RFC 7766. Growth in DNSSEC signing and validation plus the growth in IPv6 have added importance to TCP support by DNS Servers. The more light-weight and not session-based UDP has been optimized for 512 Bytes packets (and an 8 Bytes Header). Fragmentation does not work well with UDP. In addition, DNS experts see TCP as better protection against spoofing and DDoS attacks, and the protocol is necessary for adding encryption to sessions with TLS, and therefore a logical next step for DNS transport anyway.

Nevertheless there were servers blocking TCP on the resolver as well as on the authoritative side. Once more Špaček and Surý expect the problem will be heavily concentrated, with HiChina again talking the bulk. This concentration has been favourable in the announcement of a flag day for February 2020, since only a few parties still had to be convinced to adapt. In addition to obligatory TCP support, there will be a request for buffer sizes that are high enough for EDNS, with Surý suggesting that flag day organisers would recommend 1220 Bytes.

Geoff Huston added that the biggest problem was not vendor code, but firewalls as, according to his measurements, 17% of resolvers were behind firewalls blocking TCP sessions, with 6% of the internet's eyeballs affected. While most of the affected users would switch to other resolvers, 2% will not, so he expected the flag day to be about this 2%. There was nevertheless some criticism about the new flag day. Peter Koch said it was one issue to make changes in one's own software, but another to set standards like the buffer size and thereby telling others to organize their systems accordingly.

Rootzone Server System revisited

David Huberman (ICANN) recapped the history of the root server system which went from one (1984) and two root servers (1985), to seven in 1987, all still on US territory. It was only on 28 July 1991 that the first of today's three non-US locations was added, with NORDUnet (.se operator) taking on the eighth root server.

Root History

Label compression later allowed for additional root servers to be put in the priming query. The priming query is necessary to reach the root zone when a DNS resolver is booted, and it is hard-coded into

DNS resolvers. With label compression, in 1995 four additional root servers became possible.

Huberman told the story of how the additional four servers were assigned by the late Jon Postel and Mark Kosters (Network Solutions, later Verisign). Postel had L and M, and Kosters had J and K ready to be assigned to future root operators. The first request at that time came from RIPE and another one from the WIDE project in Japan. After RIPE was assigned K, Kosters did not want to give J to Japan, but instead requested Postel gave up one of his. So WIDE was assigned M (aptly for WIDE's Professor Murai). Network Solutions/ Verisign kept J, while L was later handed over to the NewCO – ICANN.

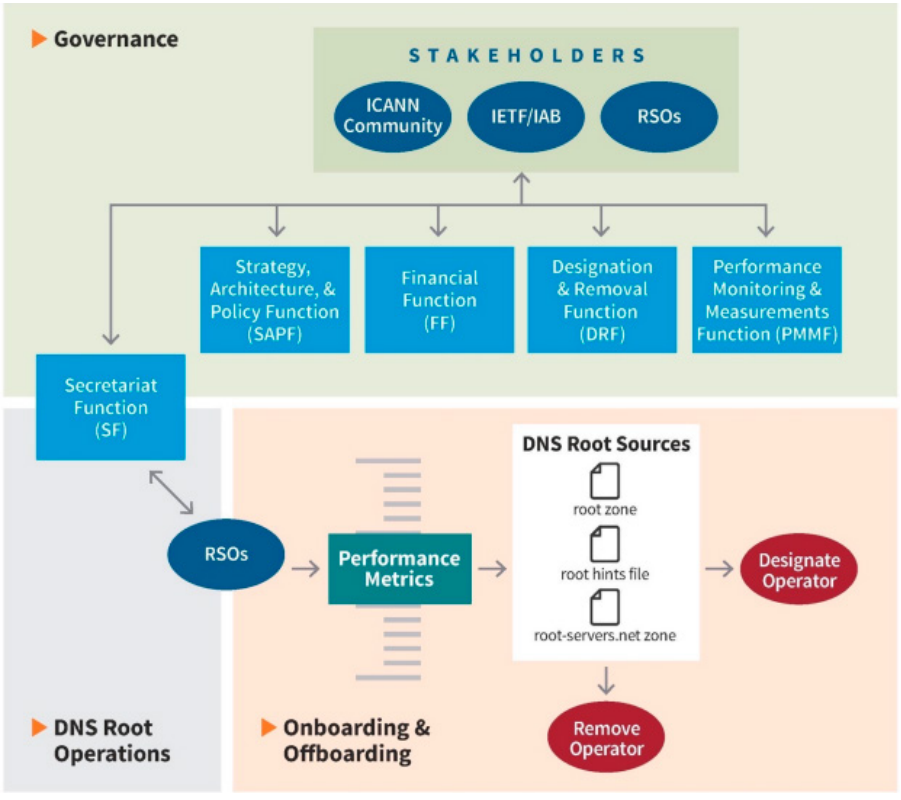
A: Verisign	G: U.S. DoD
B: USC ISI	H: U.S. Army Research Lab
C: Cogent	I: Netnod
D: University of Maryland	J: Verisign
E: NASA - AMES	K: RIPE NCC
F: ISC	L: ICANN
	M: WIDE

Huberman also delivered numbers about the distribution of the root, nowadays multiplied by anycast. All in all there are now 1120 instances of the root zone being distributed globally, with 340 in the RIPE region. 55 of the 75 economies that are in the RIPE region have a root instance, and according to Huberman five are in Reykjavik (E, F, I, J and K).

From informal to formal: ICANN still working on concept paper for RSSAC 037

Last summer, the Root Server System Advisory Committee (RSSAC) presented RSSAC 037 which proposes a secretariat function, a strategy, architecture and policy function, a designation and removal function, a performance and measurement function and a financial function. For the first time this could establish a formal procedure for adding (or removing) root servers, something that is handled very informally, as Huberman's anecdotes illustrated. Only when the designation and removal function decide that an additional root server was necessary, could a candidate from pool of proponents and vetted by the performance and measurement function be chosen.

With such a formalization the root server operators quite obviously want to answer to the pressure put on the operators and ICANN to add root servers, for example in China, India or Russia. Statements were made during the process to develop RSSAC 037 that the number 13 was not necessary, given distribution by anycast and manageable traffic numbers. Huberman pointed to a measurement from 1 December 2018 that saw 77.7 billion queries received by the root servers. At the same time he rejected the notion that there were



root server operators who wanted to stop providing the service for now. There are therefore more interesting political discussions still to come.

ICANN is currently preparing a "concept paper" on the future governance system, that would include the principles laid out in RSAC 037. Furthermore, according to Huberman it will outline "three phases of a community-driven process to finalize a new cooperation and governance model for the RSS". After this has been published, an ICANN public comment period will follow.

Distributed Denial of Service –a clearing house?

Rant about the KSK

Geoff Huston (APNIC) delivered an entertaining "rant" about the KSK roll, arguing that much has been left unclear about the effects of the KSK. For example it was clear that to this day "there remains some residual set of resolvers that are signalling that they have not yet learned to trust KSK-2017". However, Huston told RIPE attendees that it is unclear if this was an accurate signal about the state of the respective resolvers or about whether the respective resolver attempts DNSSEC validation. It was also unclear, how many users were affected, and if the respective users could make use of an alternative resolver. The example is indicative for a number of unknowns in the KSK through several phases, according to Huston's post-mortem diagnose. This includes the number of end users being affected by outages (like in the case of EIR) or by their operators turning off DNSSEC validation permanently.

It is also unclear why after the revocation of the key in January, Verisign looking at A and J root servers saw a jump in the number of queries until the point of removal. A part-explanation offered for the phenomenon is an old version of BIND.

Huston's recommends being rather cautious when proceeding with other KSK rolls, more so when done on a regular basis. According to him, knowledge of the effects is still limited.

Cooperation WG: COE, HR assessment and Christchurch

The Cooperation Working Group looked once more into internet policy developments at intergovernmental level and reflections of the grown attention for the operating and technical communities, without in the strong sense "cooperation" between state actors and the RIPE community.

Patrick Penninckx from the Secretariat of the Council of Europe presented the CoE's work on Internet Governance related topics, including the CoE Internet Governance strategy (2016 -2019). The Council is currently considering if there was a need, for example, to draft a convention on artificial intelligence, Penninckx said. The CoE is already preparing a recommendation on algorithms and their potential manipulative nature (a public consultation is planned for the summer). Other items of interest for the RIPE community and RIPE NCC with which the CoE hopes to cooperate are the responsibilities of internet intermediaries, the protection of journalists and internet freedom.

A part of the internet governance strategy was also to step up cooperation with industry. A partnership with tech companies started with an exchange of letters two years ago, and now has 14 business partners, Penninckx reported. He pointed to an interesting upcoming meeting, during which tech companies and ministers of the 47 CoE member states will discuss the role of algorithms in content moderation, including the identification of terrorist content, as well as disinformation during election campaigns and the question of facial recognition.

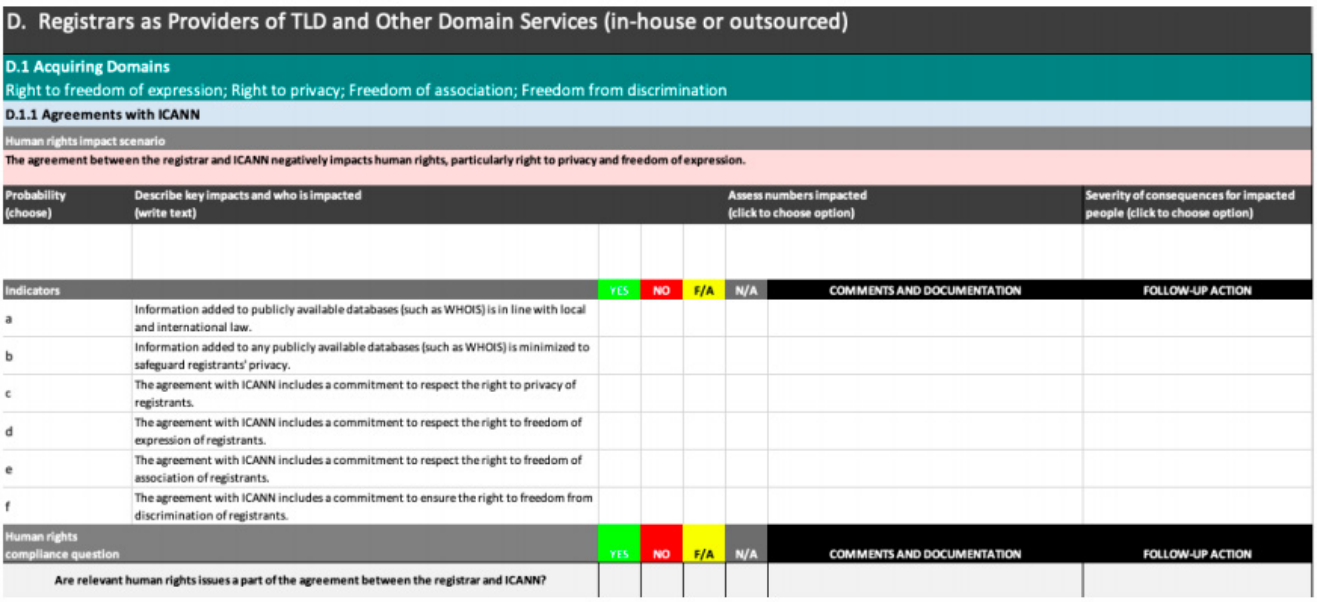
Human Rights Assessment for a registry

The registrar Blacknight underwent a human rights assessment of its business processes, assisted by the NGO Article19. Based on a tool first developed by the Danish Institute for Human Rights and refined for the Registrar Case by Article19, the parties engaged in what they call a multi-stakeholder HR assessment.

HR looked into several areas: the registrar as an employer, as a procurer of goods and services, as a self-regulatory member of professional bodies and local communities and as a provider of domain and web hosting to customers (see graph below). Due diligence was also considered as a dedicated area.

During the presentation, Neylon said that, whilst checking issues like privacy, security (or not employing five year olds) were rather quick checks, it was something different to consider a suppliers' code of conduct for example. Questions like 'have you considered how metals are mined?' and 'when one bought a new server' were part of the assessment. The larger a customer one is, the larger

Elements of the Tool



D. Registrars as Providers of TLD and Other Domain Services (in-house or outsourced)							
D.1 Acquiring Domains							
Right to freedom of expression; Right to privacy; Freedom of association; Freedom from discrimination							
D.1.1 Agreements with ICANN							
Human rights impact scenario							
The agreement between the registrar and ICANN negatively impacts human rights, particularly right to privacy and freedom of expression.							
Probability (choose)	Describe key impacts and who is impacted (write text)				Assess numbers impacted (click to choose option)		Severity of consequences for impacted people (click to choose option)
Indicators		YES	NO	F/A	N/A	COMMENTS AND DOCUMENTATION	FOLLOW-UP ACTION
a	Information added to publicly available databases (such as WHOIS) is in line with local and international law.						
b	Information added to any publicly available databases (such as WHOIS) is minimized to safeguard registrants' privacy.						
c	The agreement with ICANN includes a commitment to respect the right to privacy of registrants.						
d	The agreement with ICANN includes a commitment to respect the right to freedom of expression of registrants.						
e	The agreement with ICANN includes a commitment to respect the right to freedom of association of registrants.						
f	The agreement with ICANN includes a commitment to ensure the right to freedom from discrimination of registrants.						
Human rights compliance question		YES	NO	F/A	N/A	COMMENTS AND DOCUMENTATION	FOLLOW-UP ACTION
Are relevant human rights issues a part of the agreement between the registrar and ICANN?							

the leverage to also make an impact in procurement. Issues like a whistle-blower policy was discussed with the HR manager. All in all, he said it was an interesting process, which resulted in a review of internal and external policy, the creation of some additional policies for the company as well as added transparency reporting. It is still a work in progress.

Christchurch Call

Milton Mueller briefly talked about the Christchurch pledge, which was signed after a meeting in Paris by 17 countries and eight tech companies, who committed to eliminating terrorist and violent extremist content online. The pledge is a reaction to the attacks and murders in two Muslim Mosques in Christchurch, New Zealand on 15 March 2019. Mueller added that governments that have not signed include the US, China, Russia, South Korea and Finland. Civil society groups gathered a day before the government meeting and criticized the exclusive and government-led approach. They are concerned that the pledge will strengthen the ongoing push for new forms of content regulation, despite declarations by the respective governments that they are committed to freedom of expression. The terrorist content online regulation in the EU (or the German Netzwerkdurchsetzungsgesetz) are just two examples of this. According to Mueller it was important to distinguish between prevention of uploads (possibly filtered by algorithms, see the upcoming COE talks) or take-downs of reported content.

Closely watching the ITU: Cooperation WG, IPv6 WG, IoT WG

ITU presentations were scattered throughout the RIPE 78 agenda, each looking into work related to RIPE's mandate in one way or the other. Chris Buckridge, RIPE NCC's External Relations Manager (taking up the responsibilities also of Paul Rendek after the latter left RIPE NCC), gave an overview of liaison and sometimes watch-dog work performed for the Plenipotentiary Conference in 2018 and standardization efforts touching RIPE's remit, especially in IPv6, IoT and Internet Governance.

The Plenipot, held once every four years to set the course for the international organization, could not agree on any changes with regard to the existing set of internet resolutions, Buckridge reported. This meant that there will be no increased authority for the Council Working Group of the ITU on internet public policy making, and also no increased remit for the ITU with regard to cybersecurity. A resolution on AI was also rejected, a field where some countries would like to have an ITU mandate. From the perspective of

the I-Stars organisations a somewhat concerning new resolution on Over the Top Providers was adopted. Buckridge said that all in all, the RIPE NCC was looking forward to working with the ITU Development Sector and its newly-elected Head, Doreen Bogdan-Martin (US).

Cooperation efforts between both organizations have worked out well, Buckridge noted, in several aspects. On ENUM (see DNS WG above), there was a joint revisiting of the guidelines. On the issue of an IPv6 address plan dedicated to IoT, which was discussed in Study Group 20 and presented a year ago at the RIPE meeting in Marseille, the RIPE community won the argument. In April, after several rounds of discussions, the work item was abandoned by the study group, according to a detailed report by Marco Hogewoning (RIPE NCC) in the IPv6 WG.

Another IoT-related "battlefield" is a new standardization proposal in Study Group 20 presented by Patrik Fältström (Netnod) in the IoT WG. The recommendation (Y.4459) introduces the Digital Object Architecture (DOA) for IoT interoperability. The previously-discussed DOA defines a framework for information-oriented services. The proposed standard defines a framework for information management based on the use of digital objects, and a common set of secure services. It does so by using existing infrastructure, including internet infrastructure to enhance secure and managed information sharing over a distributed networking environment

The basic idea is to support registration, discovery, resolution, and dissemination of digital (IoT) objects above the existing naming, registration and resolution system. The DOA has caused some concerns earlier in the DNS community. Fältström explained that Sweden has rejected its approval because the draft has been put onto an alternative, faster approval track that would not allow for consultations. In Sweden's view not only was the draft not yet mature, but it also included regulatory and policy implications which called for the traditional standardization approach (instead of the alternative fast track). Countries who supported Sweden's objection were Canada, Finland, Australia, Czech Republic, New Zealand, Norway, the United Kingdom, the United States, Denmark. While the proposal currently seemed to be blocked, there was a new proposal from China on DOA and Blockchain for Smart Cities.

The next RIPE meeting will be in Rotterdam on 14-18 October 2019

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.

Rate this CENTR Report on RIPE78

(Thank you for your feedback!)

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