Council of European National
Top-Level Domain Registries

Report on
RIPE73

Madrid
24-28 October 2016

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 3

Plenary Bits, Working Groups 8

Highlights

WHOIS – Europol lobbying for accuracy

Law enforcement agencies (LEAs) have been pushing for WHOIS accuracy in the domain name area for years. They now want to reiterate the effort with the IP address registries, calling for much better accuracy in the IP address databases. At RIPE73, Gregory Mounier, Head of Outreach

European Cybercrime Centre (EC3) at EUROPOL, gave two talks to illustrate the problems law enforcement agencies face when using the RIPE IP address database, in essence calling for new global policies on WHOIS accuracy in all RIRs.

LEAs are requesting a policy to solve the "chain of custody inaccuracy"

In a plenary talk, Mounier presented an anonymized case to motivate further steps by the RIRs. According to Mounier, the British investigator tried to find an attacker that allegedly extracted 7.8 million customer details from a supermarket chain. But a check of the IP address found in the supermarkets log revealed a web of two person objects, two UK street addresses (presumably dropboxes), one street address in Serbia and one phone number in San Diego. Such a result made a court order to receive data on the users of the IP-address impossible.

Mounier underlined that there was no problem with RIPE members who were obliged by their contract with the RIPE NCC to keep the database accurate. The problem was a "chain of custody inaccuracy issue". Contrary to obligations for RIPE members, when their customers sub-allocated IP-space further down, the trail got lost. Therefore, the solution was to have sub-allocations documented as far as the last downstream provider. The problem faced would get worse for LEAs with the use of IP addresses in the IoT or potentially with new phone numbers in the net concept (Modern proposal at the IETF) and with IPv6.

To solve these issues, the LEAs are now lobbying for a new policy that would "require registration of all IP sub-allocations to downstream providers, so the entire chain of sub-allocations would be accurately reflected in WHOIS". To eliminate differences of policies for sub-allocation records, investigators (cooperating in ICANN's Public Safety Working Group) were currently lobbying for a new policy in all five regional IP address registries (RIRs). Costa Rican Police and US DEA had spoken at the LACNIC meeting in September, Sri Lankan Police had addressed the APNIC meeting in October and DEA, Canada's RCMP and FBI the ARIN. For AfriNIC, the Mauritius Police and/or African Union would follow-up in December.

More liability for ISPs, lack of data on the issue

There was considerable discussion on the LEAs' request. Concerns included the additional liabilities for RIPE members, and potential sanctions against them. Others noted that operators were not more apt to detect a web of drop companies than the police, in particular as the setting up of shell companies and use of dropbox addresses was not forbidden by law. Lack of evidence on the number of cases affected by the problem was also criticized during the plenary and the Anti-Abuse WG session.

One participant rejected the LEA push for the new policy pointing to the WHOIS obligation for new registry operators in the domain name space. That was a "clear attempt to push registries to be the network police" and the RIRs should not become part of a new "network police". Presentations of the sub-allocation policy in RIPE and APNIC had also not been consistent. Mounier rejected concerns over less rule-of-law-inclined police-systems in a number of countries: "The question is shall we not do anything because in some country that might be abused or the police don't have the same ethical practices than in others? I am law enforcement, don't ask me that, I will say no. We are going after the bad guys and I am sorry if it can be misused by others."

RIPE Chair Hans-Petter Holen noted in the end that the RIPE community could consider narrowing down personal information in the database. It had perhaps been overloaded over the years and an approach to limit the data to operator (ISP) data, and make sure that part was correct, could be considered. Mounier had said that personal data was not what law enforcement was after. On accuracy, the RIPE NCC is undergoing so-called Assisted Registry Checks, checking if the database entrances of LIR (RIPE members) are correct: so far, 3,900 ARCs have been completed, according to Andrew de la Haye, RIPE COO and 95% resulted in data updates (see page 12 of de la Haye's presentation in the NCC Service WG).

Work on a potential RIPE policy on documentation of sub-allocations will now start, with support from the Anti-Abuse WG Chair Brian Nisbett. The proposal will certainly receive a lot of attention.

The ITU, the WTSA and the Internet of Things turf race

The ITU has been the "bogeyman" of the RIPE (and also IETF) community for several years. The rivalry was revived once again with an invitation from ITU study group 20 to RIPE to cooperate on

a draft Recommendation for a "Reference Model of IPv6 Subnet Addressing Plan for Internet of Things Deployment". Study group 20 is the lead study group on IoT, on smart cities and smart services and on IoT identification. This is where one big turf race is ongoing between a number of standards bodies and industry associations.

With the IPv6 subnet addressing plan, the ITU, according to the RIPE NCC, has overstepped its borders. Before the Madrid meeting, RIPE has rejected the invitation, arguing the ITU was not the place to discuss IPv6 address planning. The clash motivated the RIPE NCC to put a brief discussion on the ITU World Telecommunication Standardization Assembly (WTSA) on the agenda of the Madrid meeting. WTSA met in parallel to the RIPE meeting (25 October - 3 November) in Hammamet, Tunisia to assign the work for its standardization WGs for the next four-year period. A short presentation by Chris Buckridge pointed to four different areas of concern for the RIPE: IPv6, IoT, the handle system (DOA) and domain names.

IPv6 address planning and the ITU

IPv6 has been on the agenda of the ITU for some time. The respective main resolution, "Resolution 64", was reviewed in Hammamet. Buckridge reminded the RIPE membership that for many years there has been an arm twisting between member states over a potential role of the ITU as an IPv6 registry. Buckridge said that observers expected this to "go nowhere" as the ITU member countries are split over this.

The recently published draft results from Hammamet mention the differences on the ITU-registry question, but in essence remain rather general. The main tasks agreed upon for ITU-T study groups 2 and 3 are "to continue to study the allocation of IP addresses, and to monitor and evaluate the allocation of IPv4 addresses which may be still available, returned or unused, in the interests of the developing countries" and "to analyse statistics for the purpose of assessing the pace and geography of IPv6 address allocation and registration for interested members and, especially, developing countries, in collaboration with all relevant stakeholders."

Study group 2 is (inter alia) the lead study group for numbering, naming, addressing, identification and Study group 3 (inter alia) is the lead study group for policy issues relating to international telecommunication/ICT.

The ITU Bureau on Development, ITU-D is mainly tasked to work on educational and training efforts for IPv6 in developing countries (in collaboration with the RIRs and other organisations). Member states are encouraged to promote migration to IPv6, for example by considering "the possibility of national programmes to encourage Internet service providers (ISPs) and other relevant organizations to transition to IPv6" and "using government procurement requirements to encourage deployment of IPv6 among ISPs and other relevant organizations, if appropriate."

ISOC, which has been monitoring the WTSA very closely, calls some of the IPv6 work duplicative, for example IPv6 measurements.

Protection of geographical names in gTLDs not adopted

While more in ICANN's area of interest, the RIPE NCC also follows the ITU's activities on domain names, for example in the Council Working Group on International Internet-related

Public Policy Issues (CWG-Internet). For Hammamet the main concern was that some member states would push for work on stricter protection of geographical top-level domain names via an ITU resolution through a list of names created by the ITU (Resolution 47). It was supported mainly by African states and resulted, at least in part, in complaints from the African Union over the handling of dot.africa.

Concerns about the "handle system"

Buckridge also noted concerns over the "digital object architecture", aka handle system, an alternative approach to current naming and addressing. Pushed by some countries as a potential tool in fighting counterfeiting, in the end the handle system was not included in the reviewed WTSA Cybersecurity Resolution (resolution 50), but was referenced in a brand new resolution on "ITU Telecommunication Standardization Sector studies for combating counterfeit telecommunication/information communication technology devices" as one potential "framework for discovery of identity management", based on ITU-T X.1255 (and resolution 188 from Busan 2014).

Further reading on DOA can be found here.

Internet of Things: New architectural, operational, administrative needs – or not?

Buckridge noted that very much in line with considerations about the DOA, discussions about the future of the IoT were how much it differed from the Internet and if there was in fact a need for additional architecture, administrative processes and/or bodies. "Where does the DOA fit into IoT? Can and should the ITU serve as a standardization hub?" asked Buckridge in Madrid. While DOA remained a side thought at the WTSA, IoT definitely received considerable attention, beside Cybersecurity, with one new Resolution "Enhancing the standardization of Internet of things and Smart Cities and Communities for global development" added to the body of ITU recommendations.

The role of the RIPE in IoT was therefore put on the agenda of a special Bird of Feather meeting. IETF, IEEE, ITU and additional new industry alliances (Buckridge noted, for e.g., the Alliance of Internet of Things Innovation, AIOTI, established by the European Commission) want to become focal points for IoT standards. All organisations have been discussing what their role is, more or less recently (see for the IETF, the IRTF, IEEE, the ITU with its new resolution and a dedicated IoT global standards initiative, AIOTI or even the more discreet ETSI).

While the RIPE was not a standards body, Buckridge and Marco Hogewoning called on the RIPE community in both the Cooperation WG and the BoF to consider what kind of role they thought the RIPE should play. Hogewoning underlined that in fact RIPE operators would, through the development of the IoT, become "a critical infrastructure" and therefore should participate in shaping the discussion.

Reactions by members varied considerably. Paul Wilson, CEO of APNIC, flatly rejected IoT as nothing more than a buzzword ("there is the Internet and there is a bunch of things connected to it"). Instead of jumping on the IoT bandwagon, which was out for new regulations, new infrastructures and new bodies/offices, the RIPE community, according to Wilson, should shed light on facts and also underlying interests driving the debate.

Others clearly see a role for the larger Internet community in "telling customers what a really smart architecture would look like" (Jari Arkko, IETF Chair). With having it made very easy to put things on the Internet, security was also a big operational and standardization concern for many BoF participants. "We do not want a door that everybody can open, and what if the cloud server for your home applications goes bust?" (Wolfgang Tremmel, Decix). Making the larger community, and also regulators, aware of the issues was said to be one potential task.

At the same time there was a question on how much influence standardizers still held in a "post-protocol world" (Peter Koch, DENIC). The leverage of protocol designers and operators might dwindle in the app-based world (and the networking being designed by electrical engineers in the first place), but the community as a whole could certainly offer help and hope that it would be accepted.

Guidelines for "what does it mean to be a good IoT device" could be necessary, for example, said a representative of Akamai, one that could perhaps be taken up by a body like the ITU. The RIPE will continue to discuss the issue, first on a dedicated mailing list. RIPE NCC will continue to monitor developments at the ITU as a sector member.

Documenting (and enhancing?) accountability in RIPE

The RIPE community will initiate a task force to document its existing accountability framework. Accountability of the RIPE NCC (the operational arm) to the RIPE community was well documented, according to Athina Fragkouli, RIPE NCC Legal Counsel, but additional documentation on accountability mechanisms of the RIPE community itself could be enhanced. Fragkouli said that based on the ICANN accountability work (accompanying the IANA transition) she and her colleagues sensed "that ICANN is just the beginning and other Internet organisations will be next, such as the RIPE NCC and the other RIRs".

RIR accountability has been described by the RIR representatives (and others) as exemplary, the respective matrix being quoted many times in the transition debate. However, Fragkouli said that now that the IANA transition was over and that the ICANN accountability work is getting into more detailed deliberations (including the one on the Address Supporting Organisations, ASO, the RIR body inside ICANN), questions would come up on "Where is this authority coming from? Who sets these guidelines for this discussions? What is the scope? Who is the RIPE community? Who are these participants? And who do they represent? What is this decision-making mechanism? How is it implemented and enforced?" Therefore, the community now has to proceed to a review of the RIPE community accountability processes.

On the particular question of ASO accountability, Fragkouli was supported by several participants in the discussion in the statement that RIR accountability was out of scope for the ICANN CWG follow-up discussion. Malcolm Hutty (Linx) said that it was "a matter for the RIRs to organise" and "we should do that here and ICANN should absolutely not be seeking to interfere nor supplant that." Hutty also pointed to one existing document on accountability in the RIPE community processes, RIPE-464, on enhanced cooperation (which also led to the establishment of the RIPE cooperation WG).

Filiz Yilmaz, former RIPE NCC employee and now Senior Manager Network Strategy at Akamai Technologies, called on participants to consider the enormous growth of the RIPE NCC membership and community. With that growth (RIPE NCC now has 13,500 members, compared to 12,000 a year ago, and the number of RIPE meeting attendees has also grown considerably - see graph) and the increased diversity in membership, there is a change in the nature of the community, which is also visible in the considerable fights over address policy at times.

One example: Chair Selection Process

A perfect example of how the community has outgrown itself is a current discussion on how to select/elect a RIPE Chairperson. It is quite notable that RIPE did not have a procedure for the selection/election. When RIPE's first Chair, the late Rob Blokzijl, stepped down, he just presented Hans Petter Holen as his successor. Blokzijl had served unchallenged between 1989 and 2014, and instead of starting the process to create a Chair selection mechanism, he simply handed this task over to Holen, together with the RIPE Chair "sceptre".

Holen now proposes to have a process with open calls for nominations and several steps to be made towards a final electronic vote overseen by an election committee of trusted individuals (support of five members of the community, presentation of candidates). However, there were some voices in Madrid that recommended to keep it the very old-fashioned way: the Chair nominating a Vice-Chair as a "crown prince" that would then follow after him when he steps down.

Some participants in Madrid warned that the very growth and diversification of the RIPE NCC membership (LIRs) combined with electronic voting would result in "failure to find the best person for the job." A process using a nomination committee (similar to the process in the IETF or, partly, ICANN) could be a better solution. Discussion on this issue will continue (here) for some time alongside the general accountability discussion.

Address Policy – Clash over IPv4, new policy for IPv6 follow-up allocation?

The RIPE community normally being a very friendly environment, "old" RIPE members were particularly shocked by personal attacks against Remco van Mook and one of the long-standing chairs of the Address Policy WG, Gert Döring, proponents of the policy proposal "Locking Down the Final /8 Policy" (2016-03). Attacks on Döring even included some distasteful nazi comparisons. The net effect of the discussion was that van Mook abandoned his policy proposal that aimed at preventing any transferring and trading of the last mile allocations for IPv4.

The "Locking-Down" policy proposal was yet another attempt to slow down the run on the last /8 resources by the RIPE, which first led to the opening of several accounts by a number of members and, when the RIPE Board stopped this temporarily, shifted towards the setting up of new companies to receive the /22 last mile allocation.

Van Mook's proposal would have disallowed for anybody to hold more than one /22 from the last RIPE IPv4-block (185/8) and would have obliged every member to hand back /22 resources from that block received through merger or acquisition. From the beginning, there was considerable discussion and the Chairs, Doering and Sander Steffann, have stated that it was difficult to come to a compromise on the proposal. While Steffann announced after the Madrid session of the WG that the proposal could still be taken up by somebody else, the appetite of reviving the discussion, which some called to be damaging to the RIPE community, should be limited. Yet discussions over how best (or the fairest way) to distribute what is left of IPv4 will go on.

The debate that followed was about a document integrating all transfer policies in the RIPE region (RIPE internal, inter-RIR transfers, IPv4, IPv6 and AS numbers). The draft policy disallows transfers of scarce resources (IPv4 addresses) for 24 months after they have been received, a rule that will again make quick acquisition and sale of IPv4 addresses more difficult.

Plenary Bits, Working Groups

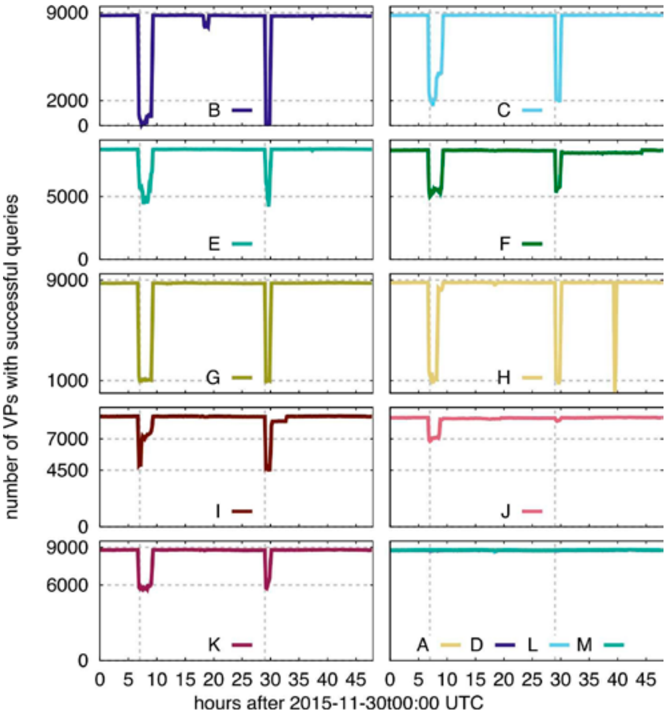
Anycast Root Servers: how many anycast sites are enough?

A few anycast sites can provide nearly as good performance as many, but what is even more important than the number of sites is the geographic location and good connectivity. This is one of the key results of an anycast study, presented at RIPE72 by Ricardo Schmidt (University of Twente). The researchers checked four different root servers for C (8 anycast sites), F (58 anycast sites), K (33 anycast sites) and L (144 anycast sites), measuring performance from more than 7,900 worldwide vantage points in 174 countries (VPs) in RIPE Atlas.

For C and K Roots, the researchers found that half of the VPs see a RTT of 32 ms or less, L's median RTT is 30 ms, and F's is 25 ms. It was obvious that median latency is not strictly following anycast size: while F and L have better latency than C and K, improvements were modest at best. C Root was optimal with 8 sites, according to the researchers, and L Root should do much better.

What matters a lot is location. An interesting result presented was that anycast sites in Asia are often unavailable to local users, obliterating positive effects from bringing anycast closer to the user and from routing policy. Local routing policy was not found to have an overly positive impact on latency. A potential impact from putting anycast servers for different services (letters) together in one data centre, on the other hand, yields bad effects in case of attacks.

Schmidt also presented a study on the effects of the big DDoS attack on the root server system in November 2015. His main findings there were that while several root servers were considerably affected (B, C, G, H) and others somewhat (E, F, I, J, K), all in all the system handled the 35 Gigabit/s attack well, thanks to redundancy (see graph from Schmidt's presentation on the right).



Schmidt nevertheless pointed to the constant rise of size and frequency of attacks: in 2012, the largest attack was 100 Gb/s; in 2016 1 Tb/s is possible; and DDoS as a service was offered for 5 Dollars for a few Gb/s. Several very large attacks had been launched since the end of 2015 (2015-11-30, 2015-12-01, 2016-06-25). The most recent one, which brought down some Dyn customers, was a topic of many hallway discussions at RIPE73.

Additional measurements using the RIPE Atlas network for other service types was also recommended by Schmidt. Another interesting measurement presented in Madrid was the setting up of an "Anycast on a shoestring"-service to allow routing measurements not afflicted by diverse routing policies and that the researcher cannot influence. For the experiment, Wouter de Vries (University of Twente) set up anycast sites distributed in the US, Australia, France, Japan, Brazil and in the Netherlands. Measuring the network "from the inside" by pinging and capturing ICMP echo replies coming back allows to get more insights on anycast catchment optimization.

The big attack and a call to strengthen the DNS

On the last day, Geoff Huston and Leslie Carr gave a presentation on the Dyn attack (see also article on RIPE Labs). Huston focused a lot on potential mitigations going forward. With more information being shared by Dyn, it is now accepted that a collection of compromised IoT devices were used as a botnet for the attack. The source code for the malware Mirai was even released, according to Brian Krebs (who was also recently hit by an unusually large attack). Krebs analyses the developments of IoT botnets.

Mechanisms described by Huston were a broken off TCP handshake, leaving only the final part of the three-way TCP handshake open. Systems were left in limbo. Contrary to other well-known attacks, it was not an amplification or reflection attack. Instead, the compromised devices were sending traffic towards the victim that looked like normal traffic, avoiding filtering as an option.

With regard to the attacks on the DNS, Huston said that the traffic was sent to authoritative nameservers. To get it down, the attack was sustained to live out the time-to-live (TTL) of the recursive servers, which in turn could not refresh from the attacked authoritative. "It's when the recursive servers lose that name that the name becomes, if you will, unavailable again", he said. The target were the authoritative DNS servers for the attacked domains.

On mitigation, Huston gave an overview of several options:

- "Building great walls" would be answered by "greater guns by the attackers" - "this is an endless loop. You lose."
- Longer TTLs to outlive the attacker, but longer TTLs would not be honoured by recursive servers regularly.
- Fixing it in the queries, setting up a front end query filter and block there – Huston called that "tail chasing"
- Filter IP addresses of devices, if possible.
- Filtering IP sources, as only 8,000 discrete addresses account for more than 90% of the users' DNS, other source IPs could be put on lower priority. Queries could be divided in friends and strangers for filtering.
- Getting recursive resolvers closer to the individual devices to answer the NXDomain query directly, using a combination of DNSSEC and NSEC signing. According to Huston, this would result in absorption of traffic by the recursive system.

In the long run, a more fundamental discussion would be needed on how to "leverage the existing DNS resolution infrastructure to be more resilient", using DNSSEC for one.

DNS WG: Benchmarking DNS Servers, new gTLD "noise"

Preparations for growing traffic, including for DDoS attacks, were also a topic in the DNS Working Group meeting in Madrid.

The RIPE DNS services have added Verisign as secondary DNS provider for ripe.net and related zones managed by the RIPE NCC after a request for proposal process this summer. The contract would be reviewed annually, according to the Head of DNS Services, Anand Buddhdev. With DDoS attacks getting bigger and bigger, RIPE NCC also did a DNS server benchmarking test. The test also serves to be prepared for a flexible upgrade path towards 10G connections.

For the test three runs of tcpreplay were staged, started at 100,000 q/s, ramped up by 100,000 each time until name server shows loss, in the end the maximum rate (-t option of tcpreplay) was used. Tested DNS software included: BIND 9.10, Knot DNS 1.6 and 2, NSD 4, Yadifa 2.2 and PowerDNS 4. Running TCP. The results are:

- NSD 4 performed best, under the condition that the "server-count" was increased from 1 to number of CPUs and reuseport is set to yes.
- CentOS 6 doesn't work (due to old kernel/drivers 85% of the packets lost, upgrade to CentOS 7 planned)

Buddhdev also reported about additions of anycast sites for K-Root (44 sites, 39 hosted single servers, 5 core sites), the migration of ccTLDs from the RIPE servers according to RIPE 663 (supposed to be finalized by mid-2017), the possibility to have ccTLDs monitored in the now RIPE-Atlas based DNS-monitoring system (eligibility according to RIPE 661), the migration of the RIPE DNS team from the abandoned DNSCheck to Zonemaster.

Johan Ihren, Netnod, reported in Madrid that in Sweden, following the Dyn attack, operators were talking about the need to add a second DNS provider. Other trends included the ubiquity of anycast services and a bigger concentration of professional DNS services with fewer providers, the latter not really pointing in the right direction for stable future as profit per zone got smaller and attack sizes increased.

Only a little noise

In a preview of the report on root stability amidst the introduction of new gTLDs, Jaap Akkerhuis, Nlnet Labs, summarised that traffic created by the new gTLDs had been growing, but was still negligible. In fact, compared with traffic from internal zones like .home arriving at the root, they were just "noise", despite the fact that now there are 1,800 gTLDs in the root. The Continuous Data-driven Analysis of Root Stability (CDAR) is currently in the public comment period at ICANN. Some interesting results are related to patterns on how the volume changes for a new gTLD before and immediately after its addition to the root: often, the volume of root traffic for a new gTLD decreases significantly in the days following its start in the root zone.

Other DNS-related bits: KSK roll, ECDSA

Roy Arends, ICANN, filled RIPE participants in on the timeline for the DNSSEC KSK roll. In parallel to the RIPE Madrid meeting, regular key signing ceremony (no 27) at ICANN's Key Management Facility in Culpepper, Virginia, produced the new DNSSEC KSK. The KSK will now sit in the safe (in four copies) until it will be transported by plane to the West Coast Key Management Facility, in Cupertino. Following the concept of basic "crypto hygiene", the roll will take place next year. Key algorithm and length remain unchanged.

With the export of the key to Cupertino, IANA will start publishing the new key. On 11 October, the Root Signing Key will be signed solely with the new KSK. Those validating and not preparing for the date could face considerable issues. With plenty of time being set aside for potential roll-back or adaptions, the old KSK (the first of its name) will finally be "securely destroyed" in January 2018.

ECDS advancing slowly

If people do not want to reform the DNS after all, now is the time to prepare for elliptic curve algorithms. Because the traditionally-used RSA keys have to get longer and longer, the switch to the more effective curve algorithms is becoming necessary to prevent the DNS from fragmenting packets. To compare: according to experts, a 3072 RSA key was just as secure as a much shorter ECDSA P-256.

Google ad powered stats wizard, Geoff Huston, Chief Scientist of APNIC, calculates that 10.75% of all resolvers globally are ECDSA enabled. The Scandinavian region is in the lead (Sweden at 74.02%; Norway at 70,46%; Latvia at 66%).

GM: Unchanged fee structure, more members, more staff

The General Meeting adopted the RIPE NCC charging scheme, a decision for redistribution of excess contribution paid in 2016 by redistributing the RIPE NCC 2016 surplus to the membership in 2017, amendments to the RIPE NCC Conflict Arbitration Procedure.

Fees unchanged

The fees for 2017 remain unchanged at 1,400 Euro per member. Net membership growth is expected to reach 2,000 and the number of independent resources charged is estimated at 22,500. For the supporting documents to all resolutions, see here.

"For the good of the Internet"

Executive Board members during the Services WG session presented parts of the 2017 activity plan, including the establishment of a Rob Blokzijl Foundation, in honour of the long-standing RIPE Chair who passed away 2015. The Foundation "will recognise people from our service region who have made a lasting contribution to the development of the Internet". Award recipients will be chosen by a nomination committee.

In 2017, the RIPE NCC will also apply to join the SEED Alliance, an organisation consisting of several RIRs and partner organisations funding "projects aimed at developing the Internet to support positive transformations in marginalized areas or communities".

RIPE NCC will contribute 100,000 Euro annually to the sustainability of the IETF following IETF presentations at RIPE71 and RIPE72, as well as subsequent discussions on the matter on the RIPE NCC Members Discuss Mailing List.

Finally, the “Community Projects Fund” activity will support specific projects that have been carefully vetted by the RIPE NCC and the Executive Board.

External Relations being bolstered up

With regard to expanding its service, RIPE NCC’s external relation team has been continuously expanded since 2012 to reach a total of 8 team members (2 in Amsterdam, 4 in Dubai, 2 in Russia). International meetings covered are the IGF, regional and national Internet governance events, ITU and regional coordination groups (CEPT Com-ITU, RCC, Arab Group), as well as the OECD and WSIS.

Altogether, RIPE NCC will add 7 staff members in 2017. Budgeted expenses for 2017 are 26.3M Euro, including 10.1M for staff. Expenditures will grow by 2,5M compared to 2016. The total income expected for 2017 is 29.9M Euro.

The next RIPE meeting will take place in Budapest on 8-12 May 2017

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 53 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.

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