Council of European National Top Level Domain Registries

Report on RIPE 70 Amsterdam

11 - 15 May 2015

Part II

Table of Contents

RIPE concerned over slipping time line / Termination an issue

Concerns over a slipping time line for the IANA transition came across in several discussions at RIPE 70. While the RIR management and leadership tried not to add fuel to the fire over differences with ICANN (the legal department, as sources say) with regard to potential termination clauses in a future Service Level Agreement (SLA) for the Regional Internet Registries (RIRs), RIPE NCC CEO Axel Pawlik clearly asked if the community backed such a clause.

The main I-ANA transition panel in Amsterdam provided an overview of the process so far. The mechanisms from the RIRs (filed in time in mid-January) include continued operation of the IANA function by ICANN under a new Service Level Agreement (SLA), signed jointly by all five RIRs. The new SLA would replace the ending contractual relation between NTIA and ICANN as IANA operator. The RIRs also envisage a review committee on the IANA number function. Just before the RIPE meeting in Amsterdam the legal team of the five RIRs published a draft text for the much debated SLA.

Dispute about Termination in SLAs

It was his understanding, Pawlik said during a plenary session devoted to the transition, that „this community, needs a termination clause at least for failure of operations in IANA." And he added: „I would appreciate any feedback from all of the RIRs communities on what we are supposed to do there".

A possibility to change to a new IANA operator receives very broad support in the technical community. An IANA SLA without such a clause looks like a showstopper for the RIPE (and other RIRs and the IETF). During the April ARIN meeting Bill Woodcock, (Packet Clearinghouse, ARIN Board of Trustees) had reported about disputes with ICANN staff representatives:

„The areas we're furthest apart on in negotiation are related: termination and separability of the three communities' IANA functions operators. ICANN has verbally represented that they will reject any proposed agreement in which ICANN is not deemed the sole source prime contractor for IANA functions in perpetuity. ICANN asserts that neither NTIA nor the US Congress will approve any transition plan which leaves open the possibility of a future non-US IANA Functions Operator."

What is not clear -with drafting of the final transition proposal still under way- is who is the right contractee at ICANN for now. While the RIRs had started to talk with ICANN's legal team, Academic Milton Mueller, ARIN Board of Trustees (and ICG), recommended the RIRs should contract with the Post-Transition IANA. The PTI, according to the CWG draft proposal on transition (consultation ending May, 20), shall be a fully owned subsidiary to ICANN.

ICG Co-Chair Patrik Fältström reported in Amsterdam that the ICG reacting to „these discussions and words about ICANN negotiating with various entities" had issued a recommendation to avoid such „side discussions in a non-transparent manner". ICANN Chair Crocker officially agreed in a written answer to ICG. At the same time, Fältström recommended not to „mix up negotiations on existing SLAs and agreements that might exist or have to exist until the transition happens to whatever the operational communities have defined. Those are two different things."

This might be slightly at odds with requests from the NTIA, just put forward in a May 6 letter by NTIA Ass. Sec. Lawrence Strickling. Strickling asked for expected time lines for finalizing not only the transition model, but also implementation of its main parts.

Pawlik explained during the transition panel that the answer to the stalled SLA talks was to present the SLA draft text developed by the RIR legal team to the community and the public at large and ask for comments. The Number Resource Organisation (NRO) Executive Council had withhold their decision on the SLA document. Pawlik called to the RIPE members to comment on the draft SLA text. CRISP Chair Izumi Okutani answering questions to this reporter said that a potential complete rejection of a termination clause would in the first place request clear rationales from the parties supporting it (ICANN or US administration).

Time Line and reluctance to talk about plan B quite yet

Lawrence Strickling's letter does also touch one or the top concern of many RIPE members: the slipping time line. While Strickling commits to transition when the community was ready, many experts consider the upcoming election and election campaigns an issue. The closer the evaluation of the transition plan gets toward the end of the legislature, the bigger the risk that key personnel was gone, Woodcock said, and lingering projects would be postponed. A new administration would take time to get back to the file, if there still was the political momentum.

Asked for what kind of plan B might exist, RIPE's Chair Hans Petter Holen underlined that it was too early to consider that. While it is very difficult to imagine that the man-years of work put into the transition process by the different communities, including the RIRs, will just end and IANA contracting will return to business as usual, RIRs and IETF in their recent meetings have been reluctant to already talk about the possibility of a plan B, not the least to not undermine the ongoing effort.

With regard to the time line, the Cross Community WG on Enhancing ICANN Accountability (CCWG), has a time line that extends into October. Athina Fragkouli, legal counsel of RIPE presented the main mechanisms proposed in the draft currently in the first of two planned public comment periods (ending June, 3). Mechanisms of the CCWG's proposal are to empower the community to take over the oversight role currently exercised by the NTIA, an elaborate appeal procedure and the inclusion of the affirmation of commitment reviews in the Bylaws.

The Community, represented according to the current proposal by the unincorporated Supporting Organizations and Advisory Councils, would be able to review and reject the budget, approve with high majority (75 percent) so called fundamental bylaws (core values in the ICANN Bylaws) and recall individual board members or the entire ICANN Board (again with a three quarter majority). A document intended to consider the effect of the mechanisms for the naming community (RIRs) was announced to be prepared right now.

There is always a question and concern how far the ICANN and PTI mechanisms proposed will extend to the RIR internal policy and operational processes. There are, as for example the IETF is acknowleging with regard to „special names“, at least some operational overlaps between the three basic IANA functions (names, numbers, protocols).

Even with the accountability work divided up into two work streams, with work stream 1 containing those items that could be resolved before the transition, „this seems to be snowballing“, said RIPE NCC's Head of Communications, Paul Rendek. He recommended to focus work stream 1 to a few essentials and postpone everything else to work stream 2. Chief Scientist Daniel Karrenberg said the community might consider, if there was not a real risk „that unless we assert ourselves a little bit more, we might be drawn into a negative attitude towards internet governance.“ Concerns were expressed by Rendek especially about the potential negative consequences of a failure of the transition process on the international arena, especially at the WSIS in December.

Working Groups

DNS WG

RIPE NCC is preparing for another expansion of its K-Root and will be starting to collect expressions of interest from operators to host a site (here). While the RIPE NCC DNS team did not want to see K-root expanded to „every broom closet or bedroom globally“ the setup was relatively easy („one Dell server“) and an IXP adapted set-up had been developed. Hosts are expected to pay for the necessary hardware and connectivity.

Another expansion considered by the RIPE NCC is a fourth site for the RIPE NCC authoritative DNS server (ripe.net, e164.arpa, in-addr.arpa and 76 ccTLDs), to be added to the instances in Amsterdam, Stockholm and London. A second provisioning server has already be added to the main provisioning server in Amsterdam.

Also an algorithm roll-over for RIPE'S DNSSEC signed domains is planned for November 2015, instead of SHA1, SHA256 will be used.

On the DNSMon service, RIPE NCC intends to pull the plug for the old DNSMON visualization, according to Romea Zwart from RIPE NCC. Raw data would still be available, also the historic data sets and could be visualized with the new DNSMON.

Knot DNS

Developers of Cznic Labs presented further steps with regard to their Knot DNS server. Jan Včelák explained new features of the 2.0 version (released February 2015) of the Knot authoritative server, Marek Vavrusa gave an update on work for the the Knot DNS resolver.
While version 1.6 of the authoritative resolver will be supported as the long-term version (bug fixes and security fixes will be provided), for version 2.0 two major features were added: one is flexibility for the configuration format, so smaller servers can use text format and larger binary format. The other is extended DNSSEC capability, namely including the possibility to automatize signing and roll-overs with what Včelák described as Key and Signature Policy (KASP) where the KASP database holds key material (according to Vclak it is similar to options provided by OpenDNSSEC). The Knot 2.0 series is using GNU TLS instead of OpenSSL, „not for security reasons“ Vclak underlined, but because GNU TLS was much better documented. The final release of Knot 2.0, he promised, would have a experimental possibility for DNSSEC online signing.

Knot has proved to be highly successful since its start, Včelák said customers included several ccTLD registries, Telefonica in the Czech Republic, Microsoft. ICANN was testing the server for L Root.

Another next step for the Knot developers is the development of the Knot DNS recursive server. Vavrusa explained that developers decided to provide it with a library of its own (to avoid dependency on a library built around some other technology that might become obsolete with the library not longer supported). The library currently provides two APIs for resolution, a system for extension, a cache and a reputation system (allowing to map Internet health and badly answering servers). The daemon is written in C and Lua. Lua according to Vavrusa could allow quick reactions to DDoS attacks through dynamic configuration. Vavrusa said that the current status of the resolver could be compared to a building with a roof, while there still was a lot to do to put in furniture. He gave a short demo and pointed participants to GitHub. The resolver was planned to be production ready by the end of the year.

Marco Prause explained in another presentation how DENIC experimented with path MTU discovery, chosen paths and congestion control algorithm (winning algorithm was TCP Hybla) to bring down transfer times for large zones (including 15 mio domains with 20.000 DNSSEC signed).

DLV Sunset

Jim Martin (ISC) announced the discontinuation of the DLV originally set up (2006) before the root zone was signed to fetch the public keys for DNSSEC signed zones. After the root was signed (2010) the need for the DLV was gone. With the DLV allowing children of unsigned parents to store their keys, there was even a potential problem, as the existence took away pressure from parents to go and sign. But as of now only 397 zones in the DLV (of around 4500) have unsigned parents and with ICANN obliging for DNSSEC signing and acceptance of signatures the problem is going away.
ISC is planning to accept no further DLV registrations as of early 2016 and start to remove records from early 2017 with the zone being depleted by 2017. DLV users and operators would be informed. Discussions on whether to remove DLV feature from BIND was still ongoing, according to Martin.

Anti-Abuse WG

The Anti-Abuse Group „re-elected" co-chair Brian Nisbet. Mainly there was no disagreement or alternative candidacy on the mailing list. Nisbet's continuing Co-Chair is Tobias Knecht. The group has no policy proposal it is working on; Nisbet said the „clean-up of the abuse contact" would be left to the Database WG. On another policy debate in the Address Policy WG policy about strengthening validation of ASN holders, Nisbet said that he would be following the debate closely. The idea is that RIPE NCC would send an email once a year to ask for confirmation from the ASN holders about their operation of the ASN.

The bulk time of the Anti-Abuse Group was spent on LEA cooperation. Marco Hogewoning, RIPE External Relations, reported about RIPE NCC activities with Law Enforcement Agencies, reports about it had been requested by RIPE members on several occasions.

He gave a short report about another full day meeting with law enforcement agencies from 25 countries (plus Europol) on March, 12. Outcomes, according to Hogewoning were a call that LEAs should get more involved with the Internet governance (and operational) fora and that operators should secure their servers and act swiftly to identify compromised systems. On the Global Conference on Cyberspace, Hogewoning noted that much attention was given to cybercrime and the need for public-private partnership to tackle it. Upcoming meetings include one with Interpol on Internet governance and dedicated training courses about the use of RIPE tools for LEAs (UK, Iran, Europol). Hogewoning said that RIPE NCC hoped the training would bring down requests to RIPE NCC, in fact requests according to the latest RIPE transparency report have been declining. From seven requests, five were asking for users of specific IP addresses, information that the RIPE NCC does not have. One request was for confirmation of the Whois data queried by the LEA.

John Flaherty (UK National Crime Agency) explained how his department was focused on protection and prevention instead of tradtional investigations. He described an exemplary operation which used RIPE data bases to map what Flaherty called a „bulletproof hoster" supposedly engaged in illegal activities. Tools used are RIPE Whois, Ripe Stats and also the databases of other RIRs (ARIN, APNIC). Flaherty said disruption of the illegal activities was the plan, but said he could not speak on successes as it was an ongoing investigation. Answering questions about how his agency dealt with anonymizing of traffic efforts he said additional tools the agencies needed was for example passive DNS and data sharing.

Bruce van Nice and Ralph Weber (Nominum) in the final presentation summarized trends of distributed denial of services attacks since 2014. Big spikes, they said, literally went away in 2015 after there had been large attacks during 2014, especially against the Apple Daily Newspaper in Hong Kong (Pingguo Ribao), which reported about the protests in Hong Kong. According to Nice and Weber, attacks were smarter and more targetted and had evolved from using open resolvers (there still were around 17 million, according to Weber) to using malware instead. Effective countermeasures were the filtering of outbound traffic to prevent putting additional stress on overloaded servers and the ingress filtering.

One year of DANE in the wild

Lack of DNSSEC deployment remains a big stumbling block for the use of DANE according to Patrick Ben Kötter and Carsten Strotmann. The two mail experts from Posteo, a German mail provider, underlined the potential of DANE to use the DNS as a policy channel. At RIPE 70 they reported about implementations at the German Government bund.de domain – which had both DNSSEC and DANE deployed. DANE allows to securely store either certificates or even PGP keys in the DNS and signal it via a new resource record. Certificates and keys can thus be verified. Compromises at CAs, man in the middle or downgrading attacks could be prevented. Encrypting email can be automated.

But DNSSEC deployment is a precondition to this, as it provides authentication for DNS answers. At the same time DNSSEC is difficult to implement (and a source of malfunctioning due to its cryptographic demands). Problems touched upon during presentation and discussion were the exchange of SHA1 and SHA2 certificates and key updates.
Posteo, which introduced DANE enabled services in winter 2013, sees especially customers that are interested in high security to show interest in DANE. DANE, they said, could still be viewed as the killer application for DNSSEC, as nobody would introduce DNSSEC just for the sake of DNSSEC (in Germany currently there are only around 20.000 delegations signed out of 15 Million registered domains). But for the promise of securing mail by DANE, people were all of a sudden prepared to bear cost and pain to introduce it.
The fact that DANE secured email can be offered by mail providers could be favorable for a much wider deployment of encryption, Strotmann and Kötter said. Mail providers were better in tacking the challenges of DNSSEC deployment.

RIPE BCOP series passes first document

The BCOP initiative at RIPE passed its No 1 Best Current Operational Practices document, „Troubleshotting IPv6 for residential ISP helpdesks“. The BCOP document series is intended to provide more practical guideline for implementing standards. It is still unclear what the home for the document series will be. The initiative has also been launched at ARIN which has passed several documents already.

At RIPE Amsterdam there were presentations on a document by Inria on DDoS mitigation. Olafur Gudmundsson (Cloudflare) called for a discussion on potential guidelines for TTLs: Gudmundsson's main point is that TTLs should be short. Two days as in .com was too long to keep parent and children in sync after changes. BCOP spiritus rector Jan Zorz (ISOC) asked if there might be a a need for a BCOP on TTLs. Mathijs Mekking questioned the possibility to give definite numbers. Longer TTLs were good for stability, Gudmundsson acknowledged, shorter were better for flexibility and faster updates.

Various

The Post-Snowden initiatve Cryptech is looking for sponsoring, according to a quick presentation of George Michaelson (APNIC). The initiative is working on trusted hardware development.

On WG Chair election, there was not much change so far with regard to WG Chairs after RIPE had decided that a process was needed for elections. Mostly the (re-)election was performed on the mailing lists. Brian Nisbet (anti-Abuse), Gerd Doering (Address Policy) were confirmed. There seemed also to be support for the DNS WG Chairs (Jim Reid, Jaap Akkerhuis and Peter Koch).