Council of European National
Top-Level Domain Registries

# Report on RIPE77

## Amsterdam

15-19 October 2018

# Contents

# Highlights

## An unexpected push for DNS 2.0

DNS Privacy expert Sara Dickinson (Sinodun) has beaten the drum for several months now to make DNS Operators, ISPs and network operators aware of the huge potential changes which the implementation of DNS over HTTPS (DoH) could bring. Dickinson spoke at both the DNSOARC/CENTR meeting and the RIPE meeting to alert the community to the choices between the two new privacy-friendly encrypted protocol variants of the DNS.

DNS over TLS (DoT) is slowly progressing with Android Pie and getdns/Stubby from the client's side, and 20 test servers, including Quad1 (Cloudflare) and Quad9 (PacketClearingHouse) from the resolver's side. At the same time all three large public resolvers are also experimenting with DNS over HTTPS, which receives DNS queries via HTTPS. According to Dickinson, Firefox is pushing ahead with Cloudflare as its "trusted resolver provider" and Google has not yet rolled out its implementation.

Only Cloudflare dared to present their implementation during the DNSOARC meeting, "taking all the flak" from angry operators, as presenter Olafur Gudmundson said. With the Mozilla-Cloudflare experiment to be continued and Google's stepping into the ring pending, a number of questions about what settings will be used remain open:

- Will there be an opt-in/opt-out for users on the client's side?
- Will the browsers use one or several resolvers, and will these be their own or partner resolvers?

### How DoH will change the DNS

Once Mozilla and Google attract DNS over HTTPS traffic via their browsers, DNS resolution will route around current DNS resolvers and, as the experts see it, go to only a limited number of "resolvers". This would concentrate DNS traffic in the hands of a few as a result and in some ways would simply intensify the already-ongoing trend toward Google's servers in particular.  Cloudflare's early start and joint project with Mozilla could be seen as an attempt to compete with Google. Cloudflare seems to be considering offering the DoH resolution as an additional service. A feature still to be designed is the discovery of the DoH server. In the case of Mozilla-Cloudflare or Cloudflare's enterprise solutions, a standard DoH server could be hard-coded. During the most recent IETF there was also a proposal to allow for the client to choose from a list of resolvers using so-called bloom filters. Another idea is that DNS answers should be added and pushed to a client system when sending the answer to one specific query (resolverless DNS).

For companies to buy into this new DoH, this offer could make sense as they will lose control of their DNS traffic, with browsers steering it away from the actual resolution monitored and policed by the company. An issue with regard to end user clients will be troubleshooting, as it will be highly unclear for the user which party will be resolving name queries.

### Privacy and neutrality issues

The added privacy for DNS users set in motion the development for DoT as well as DoH, as Browser vendors underline. Both protocols will encrypt the so far chatty DNS traffic. An advantage DoH has over DoT is that the latter uses port 853 and thereby can easily be singled out and blocked. To block the encrypted DoH traffic on the other hand would result in the blocking of all sorts of services, plus given a more concentrated market, large operators' web traffic would vanish, due to a rather crude and improbable filtering strategy.

User query information is ending up in large US-based providers, resulting in another set of privacy issues, even though browser vendors (mainly Cloudflare) are praising privacy gains. Cloudflare proactively tried to avoid the GDPR "trap" by announcing a strict data minimisation policy. Query data of the customers' users is thrown away after 24 hours, according to Gudmundsson. At Cloudflare, access to the data was highly limited to very few people. There have been no comparable announcements from Google so far.

However, transferring data to jurisdictions who lack adequate privacy regulations (according to GDPR) remains an issue (certainly not just limited to the DNS resolution). This is despite the fact that voluntary data-minimization policy platforms regularly have to submit to local policies (from FISA to filter policies in China).

Other questions of interest from a regulatory point of view are the obligations for non-discriminatory carriage, of neutrality and with regard to security-related regulation (such as the European NIS).

### What could influence the development of the DoH deployment?

Relying on users' decisions against using monopolistic services for DNS resolution by configuring DNS resolution providers of their choice would ask a lot from regular end-users.

A regulatory intervention could be triggered when concentration becomes too obvious or neutrality rules are undermined (using preferential treatment for one's own or partners' content via faster DNS resolution or blocking or re-directing some services altogether).

The implementation of the GDPR could be the first trigger of regulatory action once data protection authorities become/are made aware of potential privacy-related problems, at least in the case of European privacy. Observers have noted that expecting large platforms headquartered in the US to respect privacy seems nonsensical. Cloudflare's reiterated statement on a strict privacy policy for Mozilla DNS users, while trying to proactively answer potential GDPR questions, still might be caught in EU law violations, for example as their non-transparent transfer of data to places outside jurisdictions is considered "adequate".

### Reactions from operators

There have been rather harsh reactions from DNS operators, which Dickinson puts down to the fact that DNS administrators / operators only learned about the push for DoH very recently (with the large Mozilla-Cloudflare deployment underway, and Google obviously prepared to push the button) and that the browser community had not reached out earlier. The clash was noticeable during both the OARC and RIPE meetings. Ondrej Sury (BIND) said it would be difficult to bridge the gap after the clash. A number of people from the DNS community acknowledge that the lack of evolution with regard to answering requests to the DNS from the Web community was one root source for the current situation. Jan Zorz (ISOC) voiced strong opposition against the more centralized DNS 2.0/ DNSapp system at the RIPE meeting.

### Influence on ICANN

More discussion can certainly be expected at ICANN. According to experts with the potential to process DNS resolution over just a handful of large DoH providers – with one perhaps attracting 70% of the traffic via his browser – coordinating a hierarchical name space could become partly or fully obsolete.

Several bodies, including the Board, were highly interested in discussing the evolving situation around DoH and DoT at ICANN.

There have been explosive discussions in the German news portal heise.de, illustrating how passionate people can get when it comes to choosing between DoH and DoT. A first op-ed was published, which was clearly in favour of DoH as an innovative step away from the old DNS, and resulted in a flame war, as a second op-ed was published by an external DNS expert who called the heise editor's preference plainly wrong and dangerous.

## Abuse, Abuse

### Europol adds more to its wishlist for RIPE polices / Rise in fraud in address requests

Europol was back for RIPE77 with a new policy proposal on the WHOIS. While the first ever Europol-initiated RIPE policy – on the regular validation of the abuse contact field - was accepted in June and is now on its way to implementation, law enforcement actors have more policy suggestions. The new proposal (2018-5) concerns the publication of legal addresses for IP address owners in the RIPE WHOIS database.

Europol agent Sara Marcolla presented a toned-down proposal following harsh comments on the RIPE NCC mailing list. Instead of providing the company's full legal address, it might be sufficient to provide IDs that would allow law enforcement to reach out to the respective national databases. The policy was not meant to target the data of private persons in the first place. However, Marcolla argued that companies, including small companies, needed to register and therefore might be found much faster during investigations if they had company IDs. The idea to have include legal addresses for all sub-allocations of a local internet registry (LIR), which would force the LIRs (RIPE members) to list all their customers, had only been meant to be optional.

During the debate, RIPE members declared that listing customers with their addresses is firstly impractical and secondly, could possibly violate the GDPR. Several members warned that listing the addresses of resource owners could mean publishing personally-identifiable data. The problem with listing company IDs, while privacy-wise this is a better solution, is the non-existence of trade/commercial registers in some countries.

Opponents before and during the session had called on Europol to stick to due procedures and to get a warrant if they needed information on resource owners. Based on a warrant, data can be retrieved from the RIPE internal database (which according to the experts is rather accurate). Undeterred, Marcolla announced that she would file a new version of the proposal, regardless of the majority‘s opposition to the proposal. It will be interesting to see if this policy, like the earlier Europolicy, makes it through the RIPE policy process successfully. The regular validation of the abuse contact was pushed through despite considerable objections along the way. Law enforcement clearly views itself and acts as a RIPE community member.

RIPE Chair Hans Petter Holen called on the community to take a step back and use the proposal as an opportunity to make a decision. Since so much WHOIS data is out of date and incorrect, the community had to decide whether to clean it up or, as Holen confirmed to this author, suffer the consequences and get rid of the WHOIS altogether.

Jordi Palet requested further steps in validation and presented his ideas on potential policies in all the RIR regions, that would oblige RIR managers to perform validation more often and set deadlines for answering validating emails in a certain time. Palet said that he had considered 3 days to be a good measure but allowed stakeholders to be talked into a 15-week deadline. Participants in the RIPE NCC Anti-Abuse WG warned that the ideas, while still vague, would not address the increasing automation in answering queries to the abuse contact.

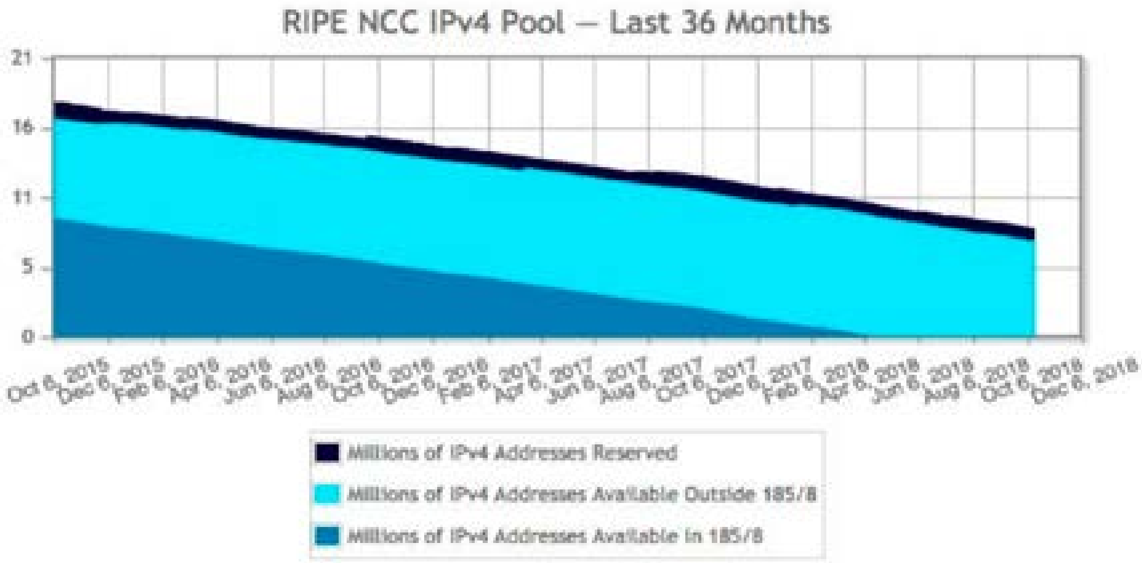
### Rise in fraud

Fraudulent activities in IP address requests have risen, RIPE NCC’s new COO Felipe Victolla Silveira, reported during the RIPE NCC Services Session. Compared to the 26 investigations performed in 2015, there have been 128 so far in 2018. Silveira said it was both “mice and elephants”, that is, there have been both smaller and larger cases involving fake passports, fake certificates and fake company registration papers when applying for resources. The shortage of IPv4 addresses and the high market prices for these are presumably the core reasons, according to Silveira.

Prices for IPv4 assets have risen to 18 US dollars per address, according to various broker companies. The number of RIPE NCC-recognized IPv4 broker companies currently stands at 56.

RIPE NCC is pushing for the automation of tasks for several reasons:

- There has been a continuing sharp growth of new members with 12,500 new members since the start of IPv4-last block allocations, an unprecedented growth in 2018 and the total



membership/LIR numbers expected to reach 24,000 soon (see RIPE NCC CEO Axel Pawlik's presentation);

- RIPE NCC has implemented additional checks on the quality of the RIPE NCC Registration Data (before and after registration);
- RIPE NCC has to verify legal authorization for address transfers and many other obligations.

Automation has currently been introduced in mergers, acquisitions and transfers with automated checks for authorisation, automated document management and automated updates of the RIPE NCC database once the procedure is completed.

### Last mile frenzy

The rapid, last-mile-induced growth which is keeping RIPE NCC very busy is expected to die down once the IPv4 addresses are all distributed. During the General Meeting there was a discussion about how RIPE NCC will prepare itself for the possible sharp decrease of resource allocation in businesses.

Currently only 5000 /22 blocks are left over from the last-mile /8 block at RIPE NCC, and another 1000 will be created from combining a /24 and a /23. After this, very little will be left (/25, /26). For addresses returned, a waiting list will be created for all those LIR that had not yet received their last-mile /22 block. Adaptions will be considered for the /16 unforeseen circumstances reserve. At the same time half of the reserve for new Internet Exchange Points (another /16) have already been distributed, resulting in a debate over whether additional addresses had to be added to this special pool.

## From DNSSEC KSK Roll to DNS Flag Day

In a very brief presentation on the KSK Rollover, Ed Lewis reiterated what had already been presented by Matt Larsen and representatives of Verisign during the OARC meeting. ICANN had received no direct complaints from parties during the KSK rollover on 11th October. After having been postponed last year, the rollover went through without any major issues, Lewis confirmed.

There were nevertheless some minor glitches. For example, one network-monitoring software, also used by ICANN, failed to update to the new key and showed a flat line. This event illustrates that the risk of failure was higher in software and applications, as keys once integrated were not dynamically managed.

A bigger issue was experienced by Irish provider eir (formerly Eircom) which, according to a BBC report, had a "DNS issue" after the KSK rollover and which lost internet services for at least 36 hours, according to angry users in a complaint forum (outside of eir). ICANN itself had reached out to Eircom after the first reports but did not receive any answers from the former Irish incumbent, which has travelled through rough seas since being deregulated. During the last decade it has changed owners many times.

A check on how DNS traffic on the RIPE Atlas probes flowed after the rollover showed the existence of failing validating resolvers in the eir Network according to Willem Toorop (NLnet Labs). Eir was due to become a victim of cache poisoning in 2009 and obviously decided to implement DNSSEC signing and validation. A presentation by Geoff Huston, Chief Scientist of APNIC, mentioned that a 2013 article had placed eir in the top 25 networks performing DNSSEC validation.

Toorop, who said that further analysis to check out what happened was necessary, found that at least one server switched to Google's public resolver and fell back to the original resolver. An expert of Cloudflare said to this reporter, his company had seen a drop in traffic from the Eircom Network by 60 percent.

Eir itself remained silent and has not answered inquiries sent by ICANN as of the time of this writing, nor did it react to press requests.

### Rolling every three years?

At the RIPE DNS Working Group meeting in Amsterdam, the discussion over the successful KSK rollover immediately turned into considerations about how often the KSK should be rolled in the future. Some DNS experts considered monthly rollovers to be good for crypto hygiene. Geoff Huston warned that given that data about what could break would remain blurred, making predictions highly vague, it would be better for the community to remain cautious and keep the currently foreseen five-year period.

In an interview with this reporter, ICANN CTO David Conrad revealed that his team had been preparing a strawman that would make the proposal to implement the rollover process every three years. KSK-rollover frequencies will certainly be discussed at the upcoming IETF in Bangkok. Paul Hofmann (ICANN) has announced a side meeting on the topic for Friday, which this time offers IETF participants to self-organize ad-hoc meetings on topics of their choice.

### Prepare for the DNS Flag Day!

Whilst the KSK rollover does not seem to have caused too much upheaval (besides the Eircom network), perhaps it will be different for the upcoming DNS Flag Day.

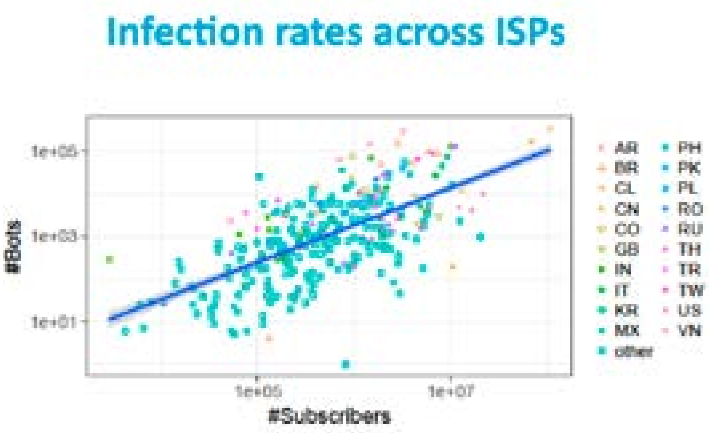
On Flag Day (1st February 2019) DNS servers which do not answer standard EDNS requests will be treated as "dead". Non-standard software, which has been hacked around by router vendors so far, will now become disabled. 20 years after the deployment of EDNS DNS software, vendors will stop providing workarounds for old software or non-standard behaviour. Instead those concerned will experience timeouts.

CZ.nic (Knot), NLnet Labs (unbound), ISC (Bind) and PowerDNS prepared jointly for the "clean up", with support from the public DNS recursive resolver operators (Cloudflare, Quad9). Beside old software implementations, some firewall software could also have issues with the change to standard EDNS only, explained Petr Špaček (CZ.nic) at the DNS WG meeting in Amsterdam. To be compliant, firewalls "must not drop DNS packets with EDNS extensions, including unknown extensions".

DNS Operators, software developers and users are invited to check their zones/software/domains via a test site, which also offers the source code for extended testing of zones instead of domains:

> *"Please test your implementations using the ednscomp tool to make sure that you handle EDNS properly. Source code of the tool is available as well.It is important to note that EDNS is still not mandatory. If you decide not to support EDNS it is okay as long as your software replies according to EDNS standard section 7."*

## IoT: ccTLD registries competing to offer tools for IoT security



After Dutch Registry SIDN announced last year that they would work on SPIN (Security and Privacy for In-home Network), a software handing back control over IoT devices in users' networks, SIDN's Canadian colleagues at CIRA presented their ideas for a Secure Home Gateway (SHG). According to Michael Richardson (CIRA), speaking at RIPE77, the reason that ccTLD registries like CIRA involve themselves in IoT security engineering is that large-scale attacks (Mirai-type attacks) are one of the biggest security issues for ccTLD registries.

In its first phase, SPIN focused on the easy monitoring of what IoT devices do in a home network (visualisation, blocking decisions). It is currently "implemented as a package that can be run on either a Linux system or an OpenWRT-based router; it can show network activity in a graphical interface and has the option to block traffic on top of existing firewall functionality".

### Secure Home Gateway (SHG) – first built for Turris Router & OpenWRT

The SHG aims to provide a secure home router – a home router software - which takes steps to secure IoT devices from the internet and the internet from leaky IoT devices. The base for SHG is a standard currently developed by the IETF, the Manufacture User Description (MUD). The declared goal of MUD is to provide a means for end devices to signal to the network what sort of access and network functionality they require to function properly. Based on MUD, IoT devices may send traffic or not at all. Machines that perform actions which are not in line with their MUD description or which are suspicious in any way can be quarantined.

CIRA hands out dedicated DNSSEC signed subdomains (domain.securehomegateway.ca) to manage the SHG-protected home network. If the SHG app is installed on a mobile phone, a new device can be QR code scanned and, after retrieval of the MUD profile, bestowed with the specific WIFI credentials it needs to do its work. According to Richardson, it will be possible for the SHG administrator – the user of a small home network – to remotely monitor when someone else wants to add a new device to the network and allow or disallow.

Proof of concept and prototype work is underway with the Turris Omnia Router and OpenWRT (for other routers). Android and iPhone clients are prepared. The idea is for other router vendors recognise the utility of the Secure Gateway and bundle it with their home routers in the future.

Jelte Jansen (SIDN) said the registries might contribute to the ongoing standardisation in IETF, namely on how to spread the MUD files, because many IoT manufacturers might not provide "decent MUD specifications" for their products. Jansen also announced that in its next phase, SPIN would also work on the inclusion of MUD for the management of the home network. There will therefore be some competition in the future.

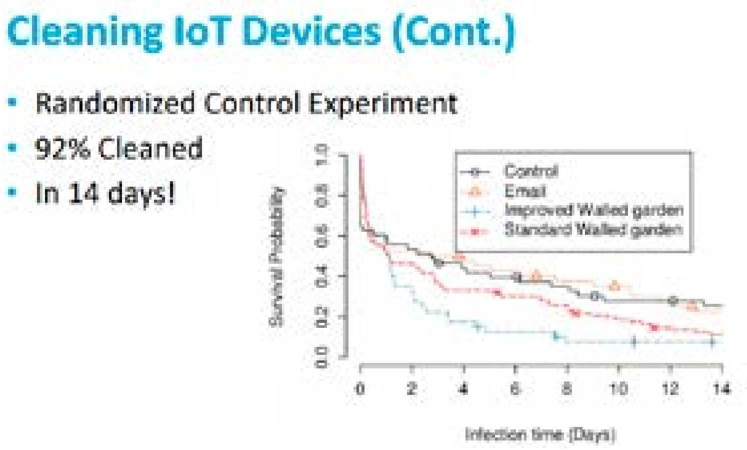
Richardson explained that CIRA developers had two different ways to retrieve MUD files in mind; one was from the manufacturer, the other was via a community. Both options would be included in a "curated database" and would be handed out with a secured DNSSEC trust anchor.

## They know not what they do – carrots and sticks for users, but more sticks?

Research on users' willingness to act when securing their networked devices from the Technical University of Delft suggests that it is mainly sticks that work. The researchers, represented by Arman Noroozian at RIPE77, found that a significant percentage of leaky devices sat behind home routers in Broadband ISP networks. They concluded that users, once their devices had been quarantined by the broadband ISP, reacted much more quickly.

*"We analysed 1,736 quarantining actions involving 1,208 retail customers of a medium-sized ISP in the period of April-October 2017. The first two times they are quarantined, users can easily release themselves from the walled garden and around two-thirds of them use this option. Notwithstanding this easy way out, we find that 71% of these users have actually cleaned up the infection during their first quarantine period and, of the recidivists, 48% are cleaned after their second quarantining. Users who do not self-release either contact customer support (30%) or are released automatically after 30 days (3%). They have even higher cleanup rates. Reinfection rates are quite low, and most users get quarantined only once" (see the research paper here).*

Interestingly, emailing people seems to have an even worse effect than just doing nothing (see graph).



Cleaning IoT Devices (Cont.)

- Randomized Control Experiment
- 92% Cleaned
- In 14 days!

## Smart regulation?

Marco Hogewoning, who has the lead on IoT at RIPE NCC, reported about several trends during the IoT session. One is the focus on security in IoT, not only in classical IoT surroundings, but also in other sectors which are switching on more and more networked devices, for example health or industrial manufacturing. With the rise in awareness of the risks, Hogewoning said there was also a call for regulation, with people saying they were not afraid of regulation. Instead they would prefer clarity, guidelines and a level playing field.

Hogewoning reported that potential regulatory "seeds" for handling IoT risks were already out there.

He pointed to talks between several EU Member States, including the Netherlands, France and Germany. These refer to the possibly of updating the EU Directive on the harmonisation of the laws of the Member States making radio equipment available on the market and repealing Directive 2914/53 to make it fit for IoT devices. Article 3 of the Radio Equipment Directive already has a number of provisions which could potentially tackle issues of wireless infrastructure.

The fact that Article 3 focuses on health issues with antennas and radio waves obliges manufacturers and operators that radio equipment must not "harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service" - The directive might lend itself to an interpretation which would cover for example DDoS attacks according to Hogewoning.

Other provisions include that:

- *"radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;*
- *radio equipment supports certain features ensuring protection from fraud;*
- *radio equipment supports certain features in order to ensure that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software has been demonstrated."*

As the European Commission is entitled to adopt delegated acts (in accordance with Article 44), fast updates which bypass the lengthy regulatory procedures would be an option, according to Hogewoning. Everything that has an antenna has already been covered, for instance a printer with USB Ethernet, Wifi or Bluetooth. Compliance checks have to be carried out on a self-assessment basis. These might be checked by third parties, consumer protection groups and the ultimate penalty in case of false labelling could be a forced recall of products.

Talks between Member States were underway, he said, with Germany having banned at least two devices so far: toys which listen to children to create targeted ads at their parents, and smartwatches (Destroy your kid's smart-watch!) which parents could use to not only track their children, but also to keep an audio tab on them.

According to the regular reporting procedure, an implementation report by the Commission to Parliament and Council is due in June 2019.

Peter Koch reminded participants in Amsterdam that regulatory obligations to allow only certified software to be distributed created a certain risk for open source software development.

## Dutch Police – data ownership in a hyper-connected environment

The Dutch police used the opportunity of RIPE NCC being in Amsterdam to make a joint presentation between an investigator (Jaap van Oss) and an officer working on the data protection side (Manon den Dunnen, Strategic Specialist on Digital Transformation). While von Oss reiterated the need for cooperation between the public and private sectors, to allow the tracking and attribution of attackers (mainly DDoS attackers), den Dunnen reported about the Dutch attempt to create a "trust framework" that would help citizens to be able to "govern" access to their data, while at the same time allowing for conditional access to data collected via applications of smart cities. Given that smart cities would be collecting data as people roam through the cities, from public utilities and more, there was a need for transparency and choice. Based on this transparency, citizens might decide which data to share, for which benefits and with whom.

Projects currently underway in the Netherlands are IoT registers in several Dutch cities as well as IRMA. IRMA currently allows authentication based on the Dutch civil registry and also data minimizing authorization (such as an over-18 service).

While projects are still in their infancy, den Dunnen said that public authorities in the Netherlands are recognizing that widespread data collection, storage and profiling can "create new forms of exclusion, reinforce and confirm existing biases and discrimination". This is therefore unconstitutional and "the police is here to investigate crime, but that's only a means to an end, the police is there to protect our constitutional values."

# Working Groups

## DNS Working Group: Gigabit K-Root, Managing Zones with Git and more

Beside talking about hot topics like the KSK rollover and DNS 2.0 (DoH vs DoT) in the plenary, the DNS Working Group was presented with the regular DNS Report by Anand Buddhev from the RIPE NCC DNS team. Buddhev gave updates on two major topics, the roll-out of 10- and 100 Gbit/s services for K-Root instances and how DNSSEC signing might not need hardware modules any more.

While the funding for another 100 Gigabit/s instance has been granted by the RIPE Executive Board, for now the roll-out will be mainly to bring the currently 1 Gbit/s instances up to 10 Gbit/s. The 100 Gbit/s instances will also only serve 10 for the time being, as transit costs remain high for small deployment. The switch would only make if there were more 100 Gbit/s servers, Buddhev explained. The other big project presented was the selection of a new solution for the DNSSEC signing. Since the existing Secure64 hardware module includes a signer that is running out of support and the acquisition of a new version product from Secure64 has been highly expensive, RIPE NCC selected the successor system from open source DNSSEC software which by now, Buddhev said, had become much better than when RIPE NCC started to sign its zones back in 2005. In 2010, when RIPE NCC changed from its own perl script version to a ready signer system, there was not a lot of choice.

They had the following list of criteria:

- Good and up to date documentation
- Bump-in-the-wire signing (XFR in, sign, XFR out)
- Support for modern algorithms and algorithm rollover
- Automated ZSK and KSK rollovers
- Safety during KSK rollovers
- Clear and verbose logging
- Import foreign ZSKs to allow for seamless migration

RIPE NCC used these criteria when considering the following options:

- BIND -good DNSSEC support, flexible (issues on dependency from Python module enabled, documentation poor)
- OpenDNSSEC - (dedicated signer, flexible, but Not packaged for CentOS 7 and poor documentation)
- PowerDNS - used by some large hosting companies for signing customer zones (no automatic key-rollover)
- Knot DNS - relatively new DNSSEC support
- Secure64 - new x86_64 signer based on Knot DNS (expensive and slower on Knot new versions than Knot itself)

In the end the decision was made to choose Knot. Instead of a secure hardware module for the keys, these will be stored on an encrypted partition of the disc. As Secure64 does not allow the export of keys for the change from one system to the other, the migration is combined with a key rollover.

Git was presented as a tool for zone managers by Ondřej Caletka from Czech ISP Cesne. The reasons for developing the tool was that zone updates, which are still performed manually by small and medium operators like his company, included many steps and were error-prone. OpenDNSSEC also occasionally deadlocked the SQLite database, and the switch to MySQL 1.4 was painful. Caletka's Git tool, dzonegit, used a "hidden master" which was controlled by a Git repository. DNSSEC signatures were independent components, allowing for the splitting of management to different teams. Caletka, who has implementations running, reported that broken zones would not be uploaded in the first place. Multiple repositories such as blacklists and whitelists can also be plugged in.

Another feature for the Knot Server was presented by Petr Špaček (cz.nic). Knot DNS 2.7 would offer GeoIP as a feature for better targeted local service (for those unable to do "real anycast", he said). With tailoring answers to subnets, in addition to the use of the MaxMind Database and EDNS client subnet, better-tailored responses would be available. In order to address potential DNSSEC issues, cz.nic proposes pre-signed DNSSEC answers since the other option of online signing would just be too slow.

The DNS WG also received a number of reports from other venues including the OARC meeting, which preceded the RIPE meeting in Amsterdam, the IETF DNSOP WG meeting and a report on DNS related IPv6 work.

### Plenary Bits on DDoS

Two presentations highlighted the growing problem of DDoS attacks, as well as potential though imperfect countermeasures.

Steinthor Bjarnason from Arbor Networks warned that the maximum attack sizes have increased by 174% (from 622 Gbps to 1.72 Tbps) and the average attack size has increased 24%. While frequencies have gone down somewhat, the overall attack volume is up 8% and attacks are "harder hitting" according to Bjarnason. In the first half of 2018, 47 attacks were greater than 300 Gbps compared to 7 in the first half of 2017 (571% increase). The Arbor expert illustrated several new trends like Memcached attacks and carpet floor bombing.

Carpet floor bombing attacks "instead of focusing on specific target IPs, attacked entire subnets or CIDR blocks", making it hard to detect attacks based on target IP monitoring. Due to rapid "weaponization" or commercialisation, this type of attack is now more prevalent. Memecache attacks use the fact that Memecache systems by default have no authentication features and listen on all interfaces on port 11211 (both UDP and TCP). Combined with spoofing, this resulted in the largest ever attack so far, a 1.7 Tbps DDoS reflection attack, experienced by Arbor. Mitigation is easier as port 11211 can be blocked or its rate limited. Filters are available, for example here.

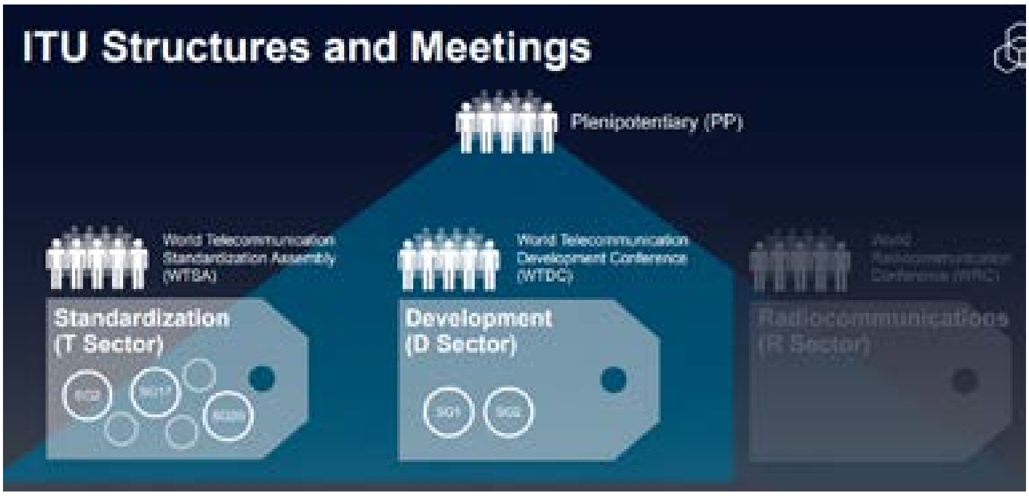
Longer caching times for CDNs might have helped against the Mirai attack, the first Terabyte DDoS attack. In a paper by Giovanne Moura, John Heidemann and others show that together, caching and retries by recursive resolvers improve the resilience of the DNS. "In fact, they can largely cover over partial DDoS attacks for many users," the authors write. Even with a DDoS resulting in a 90% packet loss and lasting longer than the cache timeout, more than half of the vantage points in the test got answers with 30-minute caches and about 40% get answers even with minimal duration caches.

## Cooperation Working Group: Plenipot, EPDP, EuroDIG 2019 and a legislative overview

The Cooperation Working Group meanwhile looked more like an Internet Governance Working Group, as they acted as an interface to other governance (and legislative) fora, and not so much as a space where governments and the community can meet.

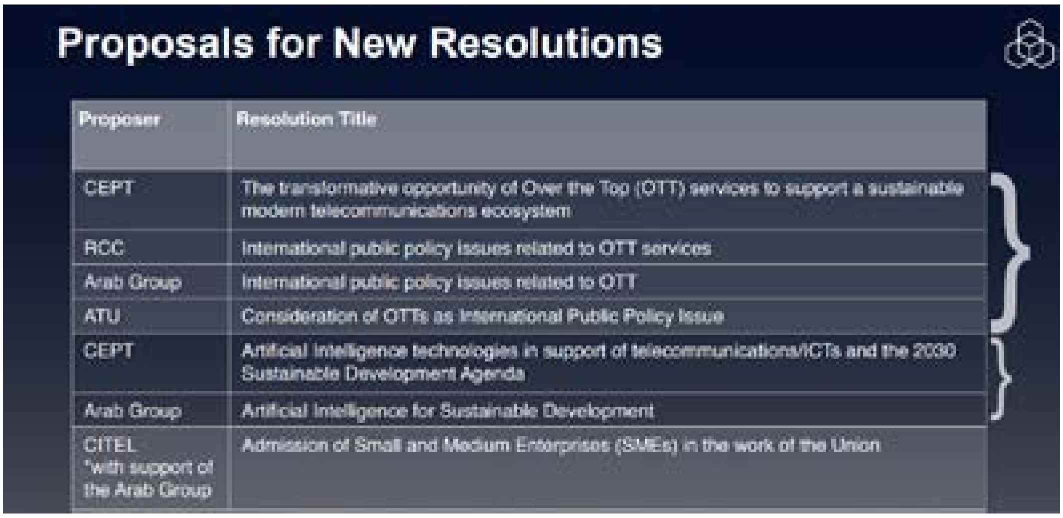
### ITU's Plenipot

For meeting governments right now, one just has to travel to Dubai, where the 2018Plenipotentiary meeting of the ITU is underway (until November 16!). The Plenipot, a kind of programmatic conference which decides on the mandate of the ITU for the next four years, will keep all I*-organisations, including RIPE NCC, busy for some time. The way the conference works is that Member States make proposals for updates on existing resolutions in the various areas of the ITU mandate, and also propose a couple of new resolutions. Chris Buckridge who is representing RIPE NCC in Dubai, explained that controversial proposals have to be taken as starting positions in an extended negotiation effort – after three weeks of meetings, maximalist requests often look quite different. Still the Internet community had to be there to be prepared to counsel government delegations. Furthermore, according to RIPE NCC, proposals for PP18 seem to be less specific when it comes to the remit of the RIRs.



ITU Structures and Meetings

Plenipotentiary (PP)
World Telecommunication Standardization Assembly (WTSA)
World Telecommunication Development Conference (WTDC)
World Radiocommunication Conference (WRC)
Standardization (T Sector)
Development (D Sector)
Radiocommunications (R Sector)



## Proposals for New Resolutions

| Proposer | Resolution Title |
|---|---|
| CEPT | The transformative opportunity of Over the Top (OTT) services to support a sustainable modern telecommunications ecosystem |
| RCC | International public policy issues related to OTT services |
| Arab Group | International public policy issues related to OTT |
| ATU | Consideration of OTTs as International Public Policy Issue |
| CEPT | Artificial Intelligence technologies in support of telecommunications/ICTs and the 2030 Sustainable Development Agenda |
| Arab Group | Artificial Intelligence for Sustainable Development |
| CITEL<br>*with support of the Arab Group | Admission of Small and Medium Enterprises (SMEs) in the work of the Union |

The relevant resolutions the RIPE NCC, ISOC, IETF and others will follow are listed here (see the RIPE LABs article on more details):

101: Internet Protocol-based networks

102: ITU's role with regard to international public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses

130: Strengthening the role of ITU in building confidence and security in the use of information and communication technologies

133: Role of administrations of Member States in the management of internationalized (multilingual) domain names

140: ITU's role in implementing the outcomes of the World Summit on the Information Society and in the overall review by United Nations General Assembly of their implementation

180: Facilitating the transition from IPv4 to IPv6

197: Facilitating the Internet of Things to prepare for a globally connected world

New proposals being followed more closely by I*organisations are over-the-top (OTT) services, artificial intelligence and what's to be done about the ITU's International Telecommunication Regulations. The negotiations to revise the ITR in 2012 led to a massive split between Member States.

One big topic from RIPE's point of view was a discussion of the future role of the ITU Council Working Group on International Internet-related Public Policy Issues (CWG-Internet). Some Member States propose to make this a multi-stakeholder venue, some want to allow the body to make recommendations to the ITU. Interestingly, neither idea sits well with RIPE NCC, as both might give the body and the ITU more weight in internet governance.

Dutch government representative Arnold van Rhijn, who presented the invitation to the EuroDig meeting in The Hague from 19-20 June 2019, said that the discussions over a more treaty-governed internet were still favoured by some Member States, and could come up at the ITU again.

### EPDP@RIPE77

A rather pessimistic look on the work of ICANN's Expedited PDP Working group on the WHOIS was presented by Julf Helsingius, the GNSO liaison to the GAC and Co-Chair of the Cooperation WG and a full member of the EPDP group. Helsingius is doubtful about whether the group could manage to get the controversial work done before the temporary specification that made the WHOIS GDPR compliant runs out. In the end, most of the discussions can be boiled down to access questions – questions pushed by IP and Business constituencies and governments alike. While ICANN's management tried to advance the Unified Access Model, the group itself has essentially agreed that the access questions could only come after the purpose for the data collection had been defined. Helsingius reminded the Cooperation Group that the WHOIS issue should have been completed years ago and was extremely disparaging about the challenging and intensive EPDP F2F work.

Meanwhile ICANN CEO Göran Marby said (during the ICANN meeting in Barcelona) that a "technical group should explore the technical and legal possibilities of a UAM", and Theresa Swinehart confirmed to this reporter that this group could be an extension of the RDAP working group.

## General trend: more regulation

While Dutch government representatives have underlined the need for multistakeholder and cooperative work on the challenges of new internet developments in various WGs, there is still a general trend of increased regulation. Regarding EU legislation under discussion, Suzanne Taylor from RIPE NCC external relations gave an overview of the draft EU legislation that relates to RIPE members and the RIPE community.

The list includes:

### Cybersecurity

EU Network Information Security (NIS, effective 9 May 2018): while some ccTLDs and Telecom/ISP providers fall under NIS, so far RIPE NCC has not been made a critical infrastructure provider.

**EU Cybersecurity Regulation** (presented in September): the main points are area certification framework for ICT products (voluntary or mandatory?), expanded ENISA mandate. EU cybersecurity industrial, technology and research competence centre and EU network of cybersecurity centres (both future proposals for 2021).

### Intermediary liability

**Copyright Directive:** the update of the 1995 Copyright Directive, which is currently in the trialogue has been heavily criticized because of upload filters and a new ancillary copyright (snippet law making platforms pay for publishers).

The intermediary liability for **terrorist content**, that is, obliging platforms and smaller content providers or hosters to remove content within 24 hours once notified by authorities has just been presented by the European Commission.

### Law enforcement cooperation

The **eEvidence Regulation** is currently under negotiation. While real-time interception has been ruled out, it will allow judicial authorities/police to request data directly from the provider in any EU country. A hearing will take place on 27 November.

### Data Ecomony, data protection

The **EU ePrivacy Directive** has been pushed by the European Parliament for some time, while Member States are in no hurry. Taylor said that the text in general was taking a restrictive approach toward meta data, and RIPE NCC thought it would have negative impacts on AI, IoT and big data. On AI the European Commission will publish a set of ethical guidelines by the end of the year, jointly working on this with the AI Alliance. The EU will also increase funding in AI by 1,5 billion euros.

### Dot.eu update

There is a proposal to update the .eu TLD legal framework.

**The next RIPE meeting will take place in Reykjavik, on 20-24 May 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 55 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 RIPE77**

(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*