Council of European National Top Level Domain Registries

Report on IETF 90 Toronto

21 - 25 July 2014

Table of Contents

Highlights 3

DNSOP: „Scaling the root“ or changing the root system architecture? 3

An IANA plan working group - a space for consensus 5

IETF will accept no more crypto standards from silver plates 6

Working Groups 8

DANE 8

Httpbis - Proxy Debate 9

Weirds 9

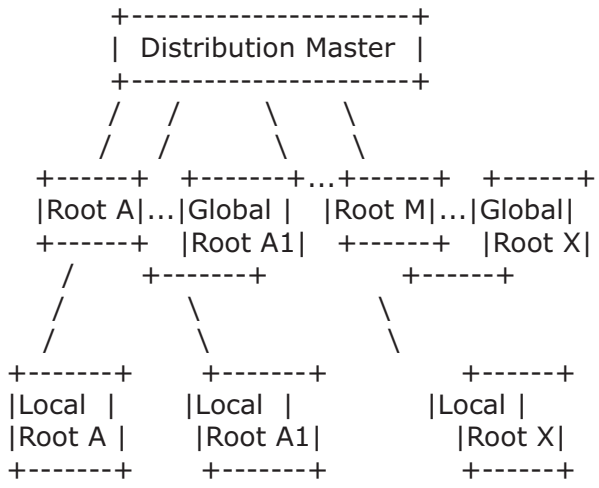
IETF News 10

DNSOP: „Scaling the root“ or changing the root server architecture?

The DNSOP WG does not seem to get over new political discussions. After staging a highly sensitive discussion during the last IETF meeting over the standards bodies' possibilities to allocate special TLDs – in parallel to the ongoing ICANN new TLD process – at Toronto it saw a discussion over potential changes of the core of the root server system. Triggered by a proposal from two CNNIC authors, the CEO of CNNIC, Lee Xiaodong and Yan Zhiwei, and BIND founder Paul Vixie, the WG had a short, but heated debate about the possibility to add new root servers. Interestingly Xiaodong Lee is also a member of the IANA Stewardship Transition Coordination Group (IGC).

The proposal by the title "scaling the root" calls it easily possible to add up to seven root servers to the existing 13 without even making EDNS0 or fall back TCP necessary (it is disputed if that is correct or not). Anyway the idea to keep all 13 servers in the 512 bytes prime request had to be given up with the advent of longer IPv6 addresses. The 512 byte boundary had for years been the argument against adding root servers.

Two models that would leave the current Root Server System intact are presented as alternatives: either IANA should create a signed copy of the root zone and allow it to be propagated by new parties (reachable via a new set of IP addresses under IN NS anycast-X1.iana-servers.net), or the new root provider should contract with any of the 13 root server operators. The related root server could be "globally anycasted or locally deployed and totally managed and controlled by a CDO." (CDO being Country, District, Organization)



The second model would be backward compatible, the authors write.
Vixie answering some questions via email compared the RSO contract model to a version of hierarchical anycast by Joe Abley.

Why not be satisfied with the current anycast when the root zone is already served at about 380 sites globally according to the draft (and an option to add anycast servers to locations that felt a need)? Points made in the draft are better geographical distribution and local control to avoid staleness following the outage of a parent root server. Anycasts were also not "open enough to

satisfy the special requirements of a country or district or organisation (CDO)". DNSSEC signatures would at the same time prevent changes to the original zone data, experts agree.

Reactions to the draft proposal were mixed, but most DNSOP participants question the technical need for adding root servers – even if it could be done. The issues of geographical distribution and locally serving answers are already addressed, according to them. The root zone was no longer really a simple hierarchical system, even if not a complete mesh net for now. Reasons for such an expansion from the point of view of most people therefore is purely political (to some only a question of Chinese "national pride").

Selecting locations for additional root servers is seen to result in a politicized discussion. Some argued in private discussions that instead of adding new root servers it might be better to relocate existing ones, (and one participant at the IETF a country like China certainly also could just think of "buying" a root server, was one opinion). Author Yan, while answering the question whether China wanted to be the host of one or more x-rootservers, said that the first aim was a better distributed system.

Despite much objections to the draft, there were at least some people who spoke out against ignoring potential issues. Former DNSEXT-Chair Andrew Sullivan, Director of Architecture at Dyn, said the IETF should not only take on the easy questions and avoid the hard ones.

More "scaling" ideas

Another idea for additional distribution of root zone information was put before the working group by Paul Hofman. While Yan/Lee/Vixie were looking at the authoritative servers, Hofman concluded, his proposal was pointing to recursive resolvers. With DNSSEC in place the root zone file could be copied to any recursive resolver who then could help to lighten the load of DNS servers. There was quite some opposition against it, with IETF participants asking the same question as in the authoritative server solution: what problem would be addressed? With zone file updates from the root servers once an hour resolvers could hammer the root servers for the updates.

More welcomed was the third presentation in the scaling discussion, again a paper from CNNIC-authors, including Ning Kong. It targets much more the general problem of how DNS servers can be positioned best with regard to geography and topology. Ning Kong gives an algorithm how to calculate where to place servers depending on what the factors are one is looking to optimize on (speed, budget, or others).

The formula in the draft would be suited to new gTLD in their efforts to bring their new TLDs to the market. The paper while applauded by some as positive for their work (Lars Liman, Netnod, btw. IGC member) was at the same time called still a little "too research-like" to become part of the WG process. It might on the other hand be further discussed at the OARC meeting later this fall.

Non-technical issues on the WG's table

How the WG will go on to discuss the root scaling issues remains to be seen. Given that the IETF is also in the midst of the IANA transition the start of the highly sensitive root server system topic might seem to some untimely. It also adds to the list of political issues the DNSOP WG has recently collected.

On the issue of special names – TLDs to be delegated by IETF outside of the ICANN process – discussed during IETF 89 there were no news in Toronto. Co-Chair Suzanne Woolf nevertheless mentioned that the just updated "Charter" now would allow the take on the issue of special domain delegation or/and the potential update of the respective RFC governing that process. Two applications have recently be sent to the IETF with requests for special use TLDs (one from engineers engaged in TOR, the other from the group dealing with name collisions).

The third rather political topic are documents that want to provide for more privacy in the DNS. The topic, according to DNSOP Co-Chair Tim Wicinski (Salesforce.com), was still "big on everybody's mind", but no slot was allocated to progress of the documents and some additional comments (see for example Vixie's post) to the issue.

The new Charter beside the classical "operational" issues of DNSOP now also includes work on protocols, somehow picking up pieces that had been left from the DNSEXT WG. If the WG tackles all the more political issues interesting times lie ahead for WG members.

An IANA plan working group - a space for consensus

The IETF got the first chance of the various IANA customers to ponder over the first meeting of the newly established IANA Stewardship Transition Coordination Group (ICG) on July 17-18. The 30 member ICG has worked on a Charter listing four tasks until September 15, 2015

- Liaison to all parties, including operational community and therefore collecting proposals from operational bodies and from the broader community,
- assessing proposals from the operational communities for compatibility and interoperability,
- assemble a complete proposal and
- share information on the process.

The IANAplan BoF meeting in Toronto established an IETF working group whose role has not become fully clear at the first meeting. While it was described as necessary space for consensus on the IETF submission to the ICG, there was an understanding that actual work would have to be done very much in the IAB give the ambitious time table presented by Alissa Cooper, IAB (and ICG member):

Combined the IETF community has four members (not counting ISOC or related technical community representatives like for example the Root Server Advisory Committee, RSSAC): IETF Chair Jari Arkko, IESG member Alissa Cooper, IAB Chair Russ Housley and Lynn St. Amour.

Arkko (IETF IGC delegate together with Alissa Cooper) did explain why there was a need to have broader participation from the IETF community, though. Presenting the final IETF proposal on how on IANA should be governed in the name of the IETF participants would put much more weight on them.

IETF's governance processes rock solid or lacking legitimacy?

On substance, the IETF Chair and many others pushed for a "ain't broken, don't fix it" or "no change" rationale. The proposal presented by Andrew Sullivan described the potential IETF contribution to the ICG process an inventory of what agreements, processes, including appeal processes, were in place at the IETF. The IETF's processes related to IANA had to be shown as "rock solid", several participants said.

The background of the rationale is not purely satisfaction with or trust in the running model. Instead attempts to make bigger changes from the standpoint of some long-time IETF participants bear some dangers: there was a chance that a change discussion could result in very hard and time consuming political fights – resulting in a necessary postponing of NTIA departure. Some even say if not achieved during this legislative term, there might be yet another mood swing in US politics.

Furthermore, as one participant put it: poking around long enough might unearth how "hand woven" some of the structures involving the IETF are for some aspects. Some aspects of the once rather informal system, now grown into a huge one might lack legitimacy, looked at from outside of the tightly knit technical community.

Against the calls that no change was necessary and ICANN therefore should keep the IANA function and deliver there were at least some stern warnings that while the IETF might not be interested in change, other communities very well might and the IETF should be prepared to answer these calls. Arkko agreed, saying that the IAB people involved had considered alternatives and were following the overall process closely.

A draft of the IETF submission can be expected to be discussed during the last IETF meeting this year, as it will mainly document the status quo. IGC member Russ Mundey (SSAC rep) in Toronto expressed his hope that the IETF could serve as a model for the community consultation processes, requesting the IETF to send its submission to the ICG early. At the same time, the ICG already has inherited several genes from technical organisations: adopting a charter, using "rough consensus" as the way to compromise in the group and the intensive remote cooperation (see the high traffic mailing list).

It will be interesting to see if the process, which is clearly driven by the technical community, is fast and smooth enough to avoid potential "side channel attacks".

IETF will accept no more crypto standards from silver plates

The Transport Layer Security Working Group (TLS WG) has decided to standardize new elliptic curves for the use in TLS (preferably to be also usable for PKIX) and has asked the Crypto Forum Research Group to select one or a few curves. At the IETF in Toronto crypto suddenly became an unusual hot topic. The IETF should no longer accept standards presented to them on a silver plate, which in turn had been presented by them on a silver plate, several speakers said in Toronto.

So far the IETF has very much relied on crypto standards published by National Institute on Standards and Technology (NIST). But after the Snowden revelations about the NSA bull run program and well planned attempts of the NSA to weaken crypto standards, not the least via its special relationship with NIST, there is considerable mistrust towards the NIST crypto standards. After the NIST finally withdrew its Dual Elliptic Curve Random Number Generator and started a review on potential weaknesses of its standardization process, changes to the "crypto-standard-taker role" of the IETF were considered.

The CFRG made one first step by devoting the big part of its session in Toronto to receive

presentations by Crypto experts, including University of Chicago/currently University of Eindhoven researcher Dan Bernstein, the German Crypto expert Tanja Lange (University of Eindhoven) and Brian La Macchia, Crypto and Security Director at Microsoft, und Microsoft crypto researcher Craig Costello. The two groups presented their respective proposals for new elliptic curves. Lange gave a very well received overview over elliptic curve cryptography.

New curve candidates

Bernstein in 2006 had offered the new curve 25519, which is in use at TOR, Apples IOS and more, and he is now proposing it as one option for TLS. Lange and Bernstein produced last year a brand new curve Curve 41417, following a request by PGP-founder Phil Zimmermann. The Microsoft researcher proposed their NUMS (nothing up my sleeves) curve.

Both groups seemed to favour to make a change in the functions used to compute the curves. While so far the Weierstrass function has been the preferred one in NIST curves, now the Edward's functions, and a variation called "twisted Edward" were proposed as being faster and more secure at the same time.

Other areas of emerging consensus were, according to a summary by new CFRG Co-Chair Kenny Paterson:

- Protection against side-channel attacks necessary
- Basic elements of curve selection defined over prime field; prime or near-prime order; twist security
- Existing algorithms have to be supported (ECDHE; EC, DSA and ECDH)
- Rigidity in curve generation

Paterson also presented a time table for the work, saying he hoped to reach consensus on the requirements in only two weeks and on the curves in four weeks. After that, final recommendations for the TLS WG would need additional two weeks. The TLS WG, according to Co-Chair Sean Turner, hopes to receive a recommendation for only one or few curves and would pick those recommended by the CFRG.

NIST reaction

NIST obviously seems to be a little concerned about losing its position as a more general (not only US-based) crypto standards maker. In Toronto, Tim Polk from NIST, who has been a Security Area Director in earlier years, announced that NIST, too, was considering to standardize new elliptic curves. Anyway he had not been in favour of the large set chosen that are standardized now.

Polk pointed to the recent report by an external expert group on weaknesses of individual standards and the NIST crypto selection and standardization process as a whole. From the Group Princeton University Professor Ed Felten, for example, strongly recommended that NIST should standardize new elliptic curves. Felten also was adamant that NIST should review the MoU it has with the NSA to regain and strengthen the independence of NIST in its work as a crypto standardization provider. Polk said, NIST was now in the process to consult on the final report of the expert group, and if stakeholders would recommend to have new curves the agency would go for it.

The new CFRG Co-Chair Paterson cut into Polks statement reminding him that the slot had been reserved to discuss the curves presented in Toronto instead. Certainly there is a hidden race now for who will make the crypto-standards provider for IETF standards, and while the FIPS-standards will remain binding for US providers in many instances, the IETF might emerge as a new provider for others. To push the development two new Co-Chairs have been selected for the CFRG, beside British academic Paterson (Royal Holloway), Alexey Melnikov (Isode). They will take over from the remaining Co-Chair Kevin Igoe (NSA) after he retires next year.

Working Groups

DANE

There is considerable progress in DANE that might very well become a killer-app for DNSSEC in the end, as DANE Co-Chair Olafur Gudmundsson tells us pointing especially to the potential for companies to use DANE for unified keying in the future and thereby saving money so far spent for certificates. Gudmundsson pointed to the importance of the "raw keys" draft discussed in Toronto. It will clarify that the DNSSEC secured domain can become the place for keying material of the mail user. So far the DANE specification is considered to favour (or even oblige the use) of certificates, even where no certificate provider is involved.

The Dane WG is about to finalize the DANE-SMTP and DANE-SRV documents and push it to the RFC publication process. Implementations of DANE secured email are already being reported for a growing list of email providers in Germany (see list). There are implementations for Postfix and Exim Mail Software.

Another draft document expected to proceed to the publication process is DANE OpenPGP. According to the author of the respective draft, Paul Wouters (Red Hat), only minor edits are left. The draft intends to use the DNSSEC protected DNS to become the central locus for retrieving the public key to encrypt mails with PGP. DANE OpenPGP as well as DANE SMIME, which still is under discussion in the WG, were mostly "about providing a standard location to check someone's key in a safe and authenticated location - inside the user's own controlled domain", Wouters explains. Keys would be stored in the DNS, under a special domain like XXXX._openpgpkey.mydomain.ca., with XXXX being the sha224 of the left hand side of the email address. An implementation allowing for automatic PGP key retrieval by MTA/MUA is here. It will, according to Wouters, look up openpgpkey records, and if found, encrypt the email and rewrite the subject: line to "[encrypted email]".

Wouters also presented the raw keys draft in Toronto, authored by John Gilmore, Electronic Frontier Foundation. The raw key draft wants to change the original DANE/TLSA RFC 6698 with regard to public keys. 6698 explicitly had specified that TLSA records could only store PKIX certificates. As the TLS WG had approved raw public keys (http://www.rfc-editor.org/rfc/pdfrfc/rfc7250.txt.pdf), the DANE specification should be updated accordingly, Gilmore wrote. It is the TLS-DANE raw public key update that will finally allow for what Gudmunsson called "unified public keying". Instead of using certificates for TLS and Keys for other applications, all keys can be stored and retrieved in the DNS. Gudmundsson called the technology "disruptive".

During the Toronto session it was considered to take the raw-key issues as yet another update point for a DANE update. After working on the operational guideline document, Viktor Dukhovni (also DANE SMTP author) has proposed to use the guideline document as a base to do a DANEBIS.

At the same time more use of the DNS stored, DNSSEC authenticated keying is considered for SIP (see SIPCORE WG) and NAT-Traversal (TRAM WG).

Httpbis - Proxy Debate

The httpbis WG has been crunching its issue list on the way to finalize the http update, while the renovation of http 1.1 is just about to be concluded with the approval of a set of documents (RFC 7230, 7231, 7232, 7233, 7234, 7235). Http 1.1 has modularized the original specification and is expected to make it easier to update in the future. Http 2 will only build on the 1.1 and change only some parts, namely the wire format, according to Julian Rescke, Greenbytes and 1.1 co-author.

One of the two httpbis Toronto sessions were devoted to discuss the potential standardization of an intercepting proxy, an issue discussed before. Concerns presented include issues like cost of end-to-end encrypted traffic for satellite connections in remote areas, especially in developing countries with lack of bandwidth and need to block access following obligations of regulators.

Given current developments with mandatory TLS for http 2.0 the web could be mostly https within the next few years, said Peter Lepeska, CTO of Acceleration Research Technologies at ViaSAT. He warned against negative effects for compression, caching and acceleration, providing the example of Opera Mini (which decrypts at the server level) as the preferred system in many low-bandwidth areas in Africa. Encrypting everything end-to-end according to his logic would be adding to the digital divide. Lepeska as well as Salvatore Loreto, Ericsson, urged the WG to define and standardize "an intermediary proxy" with the "consent of the user".

Adam Langley and almost all speakers in the debate warned to allow another break-in into end-to-end traffic. Despite the near-unanimous consensus that intercepting proxies should not be standardized for the next generation http and a request by security area director Stephen Farrell to document the WG consensus, WG Chair Mark Nottingham did not yet conclude the issue. Nottingham, who is working with Akamai, has written a draft on the proxy problem (and legitimate and not legitimate use cases for the proxy). In Toronto he summarized that publishing the proxy problem draft or standardizing **proxy.pac** (there is also an old IETF draft) would be one option – or think of other solutions for the underlying use cases.

The situation with the proxies could be compared with NAT. The latter was not standardized by the IETF because it was seen as a wrong technology solution. After the rejection NAT was deployed widely unstandardized – resulting in the need to patch things up, for example, for SIP. The NAT-trauma, as one participant called it, might cause the flinching for a final decision on the proxies.

Weirds

RDAP has to be said to be close to completion, and the WG Chairs have decided to set September deadlines for working group last call for all documents and IETF last call in October. On the bootstrapping document discussed in Toronto there were requests to address two issues, one related to queries for internationalizion (to be dealt with in an appendix).

The other issue was related to IANA's tasks in setting up new registries to allow to find RDAP servers (IPv4, IPv6, ASN, DNS). Peter Koch, DENIC, questioned the sentence that „registration policies for these new registries would be left to IANA".

A new proposal, which would open another round of discussions, was presented by Andy Newton concerning use of RDAP for Routing Policy.

There have been questions about the low activity in WEIRDS (nothing's happening there), now the hard timelines combined with the menace that WG would close down without producing a document, are intended to come to a close of the work. Jim Gavin (Afilias) in a personal conversation said that he could envisage ICANN mandating it to Domain Registries as soon as RFC is produced. Scott Hollenbeck (VeriSign) said that from VeriSign's point of view it would not make sense to introduce thick whois in parallel to RDAP, but the thick Whois deployment was still a request by ICANN at this point in time.

It will be interesting to follow how the introduction of RDAP will play out once it reaches the ICANN arena, especially given the just finalized report of the Expert Working Group on Future Registry Directory Services (EWG). The EWG report, which proposes a centralized data base and access to registration data was somehow coordinated with WEIRDS, according to Hollenbeck who has been active on both bodies.

IETF News

The IETF is in the process to update its systems. It has selected Cloudflare as a CDN service provider and at this time is reviewing proposals sent for a new meeting scheduling tool, a new website, an IMAP server and Email archiving.

Transparency and better behaviour

IESG telechats will be opened for observers until the IETF 91 as an experiment in order to allow authors and others to observe discussions.

The biggest discussion during the administrative plenary was concerned with future moderation of the IETF discuss list that had seen personal attacks. Moderation also became an issue with another experiment – an etherpad option to „queue" for the mic line at the plenary. When attendees started to make fun of the pad, the Chair „censored" the pad.

IETF-Chair Arkko finally also challenged IETF community to keep up to the pace of technology. Standardization organizations had to work fast to stay relevant.

Postel Award

The Jon Postel Award this year was awarded to Dr. Pun, founder of the Nepal Wireless network. Pun started in 2006 to hook up remote villages in the Himalaya to the net. Due to import restrictions for wireless equipments for some time, parts had to be „smuggled" across the border and Dr. Pun had taught villagers and students to put together and install the equipment in remote areas. A well-deserved price for a lot of work, it seems.

Next meeting will take place in Honolulu, Hawai, 9 - 14 November 2014