Council of European National
Top-Level Domain Registries

IETF 116

More than 153 working group sessions, a 2-day hackathon, a wide range of side events and considerable emphasis on '(post) quantum' issues.

MARCO DAVIDS AND CASPAR SCHUTIJSER, SIDN LABS

Table of contents

Introduction

The mission of the Internet Engineering Taskforce (IETF) is to make the internet better. And everyone is welcome to get involved. Most of the IETF's work is done online. However, the organisation also holds 3 meetings a year, at different venues all around the world. The 116th IETF meeting was held in Yokohama, Japan, from 25 to 31 March.

With 1,773 registered participants, IETF 116 was a well-attended meeting. There were 1,008 people present on site (just over 56 per cent), up again on the previous meeting. The remaining participants followed the meeting online.

The IETF Hackathon in the weekend prior to the meeting had 445 participants (363 on site, 82 remote). There was also a 'code sprint', at which a small group of volunteers worked at improving the tools made available by the IETF, such as the well-known Datatracker.

Special COVID safety measures were once again in force, in addition to the local regulations. Facemasks were mandatory in the meeting rooms, but merely recommended in the corridors and elsewhere. The aim is to dispense with special measures for the next meeting.

Every IETF meeting has a packed programme. The latest week-long gathering featured 100-plus working group (WG) sessions, a HotRFC, a plenary session and a wide variety of side meetings.

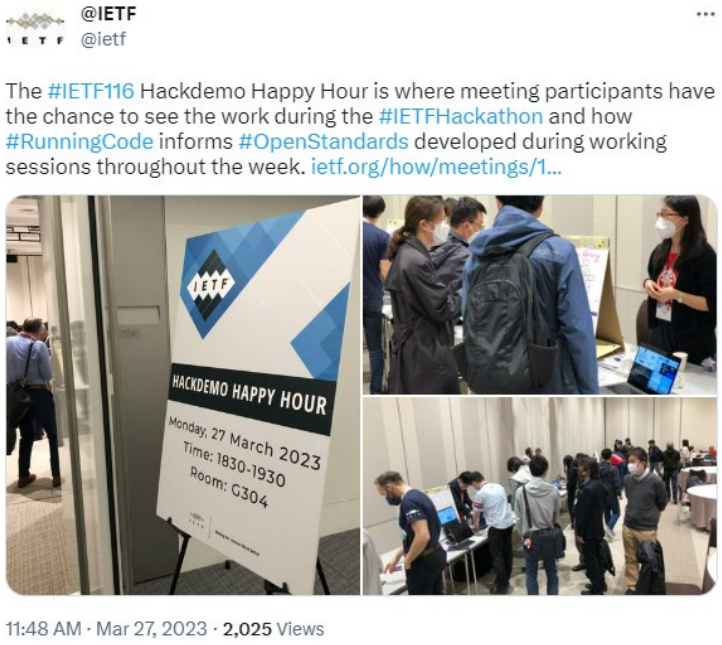
The meeting's host organisation also provided a special tour of their Quantum Internet Lab. Finally, there was a very well organised social event, at which a vat of sake was opened, according to Japanese custom.

Informal activities

During the weekend prior to the main proceedings, there were various informal activities: a Hackathon, the IEPG and the HotRFC Lightning Talks.

Hackathon

The Saturday kicked off with the now traditional hackathon, at which the applicability and interoperability of new concepts are tested. People from various organisations collaborate and get to know each other better. As usual, groups formed spontaneously. Various experiments were tackled, including interoperability experiments with 'Post-Quantum' X.509 certificates, the TEEP protocol, and exciting ideas such as satellite routing, to name just a few from a long list. One notable feature of the hackathon was the complexity of the work undertaken. A total of roughly 445 participants interacted and programmed together intensively throughout the weekend. The hackathon concluded with result presentations at the Hackdemo Happy Hour.



IEPG

The Sunday morning always begins with the IEPG, where attention focuses on topics with some form of operational significance. Nalini Elkins (Inside Products, Inc) gave an update regarding a metrics study of IPv6 extension headers.

In another presentation, the audience was told about a project aimed at measuring delay in the RPKI system. RPKI is used to protect the BGP protocol against erroneous route propagation. The researchers concluded that changes to RPKI announcements, known as Route Origin Authorisations or ROAs for short, are sometimes delayed by minutes or even an hour or more. Such delays can adversely affect the performance of BGP. That can be the case if, for example, an erroneous ROA requires prompt rectification, or if DDoS mitigation measures, such as the activation of a scrubbing service, are needed urgently (as they typically are during an attack).

Netnod's Christer Weinigel told the audience about an interesting phenomenon he had observed on the NTS servers operated by his organisation: inexplicably high system loads since November 2022. In the space of 3 months, traffic increased a thousand-fold, with queries ultimately coming from about 5 million unique IP addresses. This is quite abnormal for a new protocol such as NTS. Christer later repeated his presentation for the NTP WG.

HotRFC Lightning Talks

The Sunday ended with the HotRFC Lightning Talks, where speakers talk on a wide variety of topics and pitch ideas. In this context, 'RFC' does not stand for 'Request for Comments' (an important category of documents produced by the IETF), but for 'Request for Conversation'. The HotRFC session is a high-paced affair. Each presenter gets just 4 minutes, and no questions are allowed during the session. Any feedback has to be given later.

In Tokyo, there were 8 lightning talks in all, including one by SIDN Labs' Caspar Schutijser entitled 'Autonomous System Information Service (ASIS)'. In his talk, Caspar described his early-stage research into a self-hosted solution for sharing interoperability and policy information about a communication network. In light of the experience gained through Caspar, we can confirm that lightning talks do generate feedback. We would like to thank Stéphane Bortzmeyer and all the other contributors for their input.

Taekyoung Kwon of Seoul National University gave a talk with the title 'Using DNS resolvers as certificate validators'. The assumption behind this concept is that HTTPS/TLS will increasingly become the norm, driving certificate validation activity and increasing system loads. Assuming that end systems have secure DoT/DoH connections with their local DNS resolvers, the Seoul group's suggestion is that certificate validation could perhaps be delegated to those local resolvers. A bold idea, whose proponents themselves acknowledge that it involves various challenges and requires further study.

Finally, Marc Blanchet of Viagenie talked about 'Extending QUIC for large latency networks such as in space'.

QUIC is a fairly new protocol with great potential. Preliminary experiments suggest that QUIC is suitable for use over 'high-latency' connections, such as those established in space. Manned missions to the moon are planned before the end of the decade, and the intention is to use Wi-Fi and 5G communication, complete with IP connectivity. Marc told the audience about the research work conducted to date, involving PicoQUIC and the simulation of delay using Linux NetEm, for example.

Formal proceedings

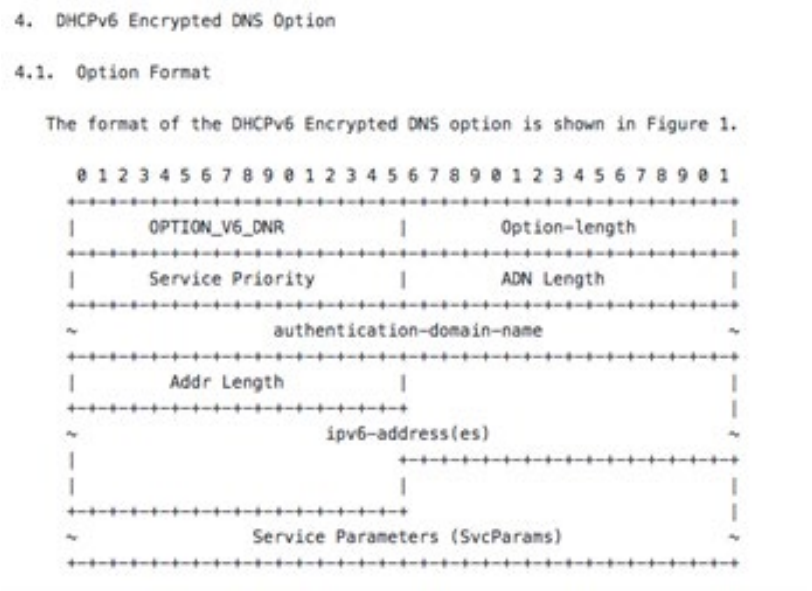
A few of the many working group sessions are outlined below.

ADD WG

The ADD Working Group operates in a highly dynamic field: automated mechanisms for informing clients where DoH/DoT/DoQ resolvers can be found. Central to such mechanisms are resolvers that support encrypted communication for extra security. Notably, this working group's ideas are being adopted very quickly, with several already implemented on Apple equipment and by public resolver service providers.

It was announced that 'draft-ietf-add-svcb-dns' and 'draft-ietf-add-dnr' had completed the Working Group Last Call phase and had been forwarded to the IESG in preparation for publication as RFCs.

The latter draft is called 'DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)'. As that title suggests, DHCP and IPv6 RA options are already in preparation, which clients will be able to use to obtain (encrypted) DNS resolvers. DHCPv6 is expected to become an official internet standard.



4. DHCPv6 Encrypted DNS Option

4.1. Option Format

The format of the DHCPv6 Encrypted DNS option is shown in Figure 1.

Figure 1: new DHCP option in draft-ietf-add-dnr

A draft by Quad9 and Microsoft, entitled 'Handling Encrypted DNS Server Redirection', or 'EDSR' for short, also warrants attention. The authors are proposing a mechanism for enabling a trusted, encrypted resolver to refer a client to another – more suitable – resolver, e.g. on the basis of geolocation. Clients are currently directed to the most suitable resolver instance by means of anycast. At first sight, the draft is not an easy read, but Sony's legal action against Quad9 may explain one of the possible fields of application envisaged by the authors. A resolver operator will sometimes choose (or be required) to direct clients to a particular resolver for legal reasons. Anycast is not always the best mechanism for doing that.

The most important takeaway from the activities of the ADD WG is that the disparity between the major public resolvers and the resolvers operated by most internet service providers (ISPs) is increasing rapidly. The ISPs are finding it harder and harder to keep up with developments. Hopefully, that is merely a temporary situation.

DNSOP WG

As always, the DNSOP Working Group, which is concerned with the evolution of (the operational aspects of) the DNS protocol, was very active and its sessions were well attended.

Since the previous IETF meeting, 'draft-ietf-dnsop-dnssec-bcp' has been ratified as RFC 9364: a BCP (Best Current Practice) document that brings together a group of DNSSEC-related RFCs and therefore serves as a useful reference work. Attendees were also given an update on the status of drafts currently under development.

There was a short session on the 'GNU Name System' (GNS), an alternative domain name system designed to be less susceptible to central control and filtering, and more privacy-friendly. Although GNS development does not fall within the DNSOP WG's remit, the project is relevant to the WG's activities. Coordination is therefore desirable, so that any future GNS implementation is not in conflict with the DNS.

DNS filtering is an increasingly common practice. With a view to providing users with clarity regarding the reasons for filtering, 'draft-ietf-dnsop-structured-dns-error' is being prepared to tie in with RFC 8914 (Extended DNS Errors). The draft's provisions include the use of codes that indicate whether traffic is filtered for spam, malware or in line with the resolver operator's policies. The document was briefly discussed at the meeting.

Another noteworthy draft on the agenda was 'draft-thomassen-generalised-dns-notify', which is relevant to registries that have implemented CDS/CDNSKEY (RFC8078) and/or CSYNC (RFC7477). Large-scale application of those protocols is problematic because it implies frequent scanning, which adversely affects efficiency. The draft proposes the reversal of the current arrangements. If a child zone publishes a CDS/CDNSKEY or CSYNC, it can send a notification to the parent.

PQUIP WG

The previous IETF report described moves to establish a working group on post-quantum cryptography. Since then, the Post-Quantum Use In Protocols (pquip) Working Group has come into being. It met for the first time at IETF 116, discussing topics such as the possible preparation of guidance for engineers on the implementation of post-quantum cryptography in their software. That proposal was well received and is being taken forward.

IRTF

Most IETF working groups are concerned with the production of internet standards. However, a number of them are engaged in more general research. Such WGs come under the umbrella of the Internet Research Task Force (IRTF). In recent years, IRTF sessions have accounted for a growing proportion of all sessions at IETF meetings. The sessions tend to be highly academic and now represent a substantial part of the agenda.

The IRTF working groups that held sessions at IETF 116 were:

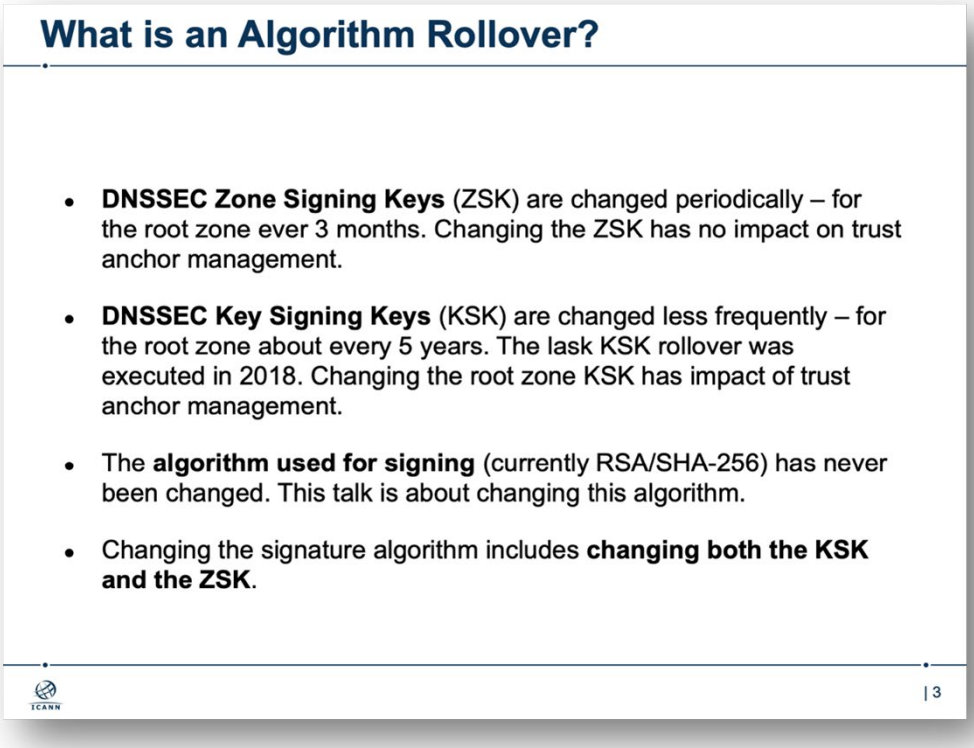
- Computing in the Network Research Group (coinrg)
- Quantum Internet Research Group (qirg)
- Information-Centric Networking (icnrg)
- Usable Formal Methods Proposed Research Group (ufmrg)
- Internet Congestion Control (iccrg)
- Privacy Enhancements and Assessments Research Group (pearg)
- Measurement and Analysis for Protocols (maprg)
- Network Management (nmrg)
- Decentralized Internet Infrastructure (dinrg)
- Global Access to the Internet for All (gaia)
- Research and Analysis of Standard-Setting Processes Proposed Research Group (rasprg)
- Crypto Forum (cfrg)
- Human Rights Protocol Considerations (hrpc)

Fascinating though the WG proceedings were, it obviously is not possible to describe them here in any detail. Nevertheless, the IRTF's discussions provide a useful picture of how the internet is developing. Topics covered range from the threats and opportunities associated with centralisation and quantum computing, to the promotion of human rights, privacy and sustainability, and the importance of performing complex network measurements.

By way of illustration, IETF 116 featured the first meeting of the Usable Formal Methods Proposed Research Group (ufmrg). One of the group's purposes is to investigate how 'formal methods' can be utilised in the IETF's work and its output, such as protocols. The value of formal methods in that context was illustrated by recounting how, during the development of TLS 1.3, the implementation of draft versions of the protocol was modelled, leading to the identification and removal of flaws. Without the modelling, the flaws might not have been noticed until after publication of the specification.

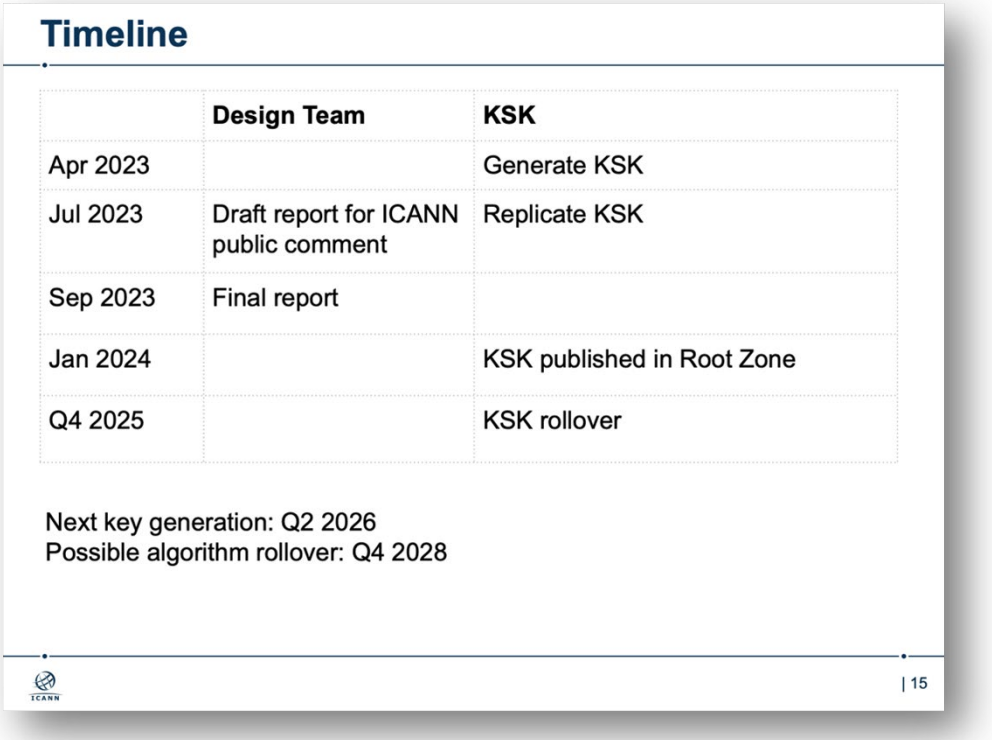
Side meetings

The side meetings, also known as BOFs, are gatherings that are not included in the formal programme. Their purpose is often to discuss the possibility of forming a new working group. A variety of side meetings took place on the fringes of IETF 116, one example being a meeting devoted to the Root Zone Algorithm Rollover study. ICANN flew in the design team for a closed session on the algorithm rollover and hosted a public session to explain the plans.



The rollover itself will be preceded by a study to clarify the possible impact on, for example, (stub) resolvers, root server operations (larger DNS responses), home devices and middleboxes. The study will also look closely at the algorithm selection criteria and the best way to perform the rollover.

The entire rollover process, including the study, will take several years.



IAB open meeting

The IAB open meeting provides an opportunity for direct interaction between the community and the IAB. The session involved the usual updates, plus 2 presentations on sustainability: one about WIDE and one about e-impact.

IRTF open meeting

The centrepiece of the IRTF Open Meeting is the presentation of Applied Networking Research Prizes (ANRP). The winners also present their research results to the audience. At IETF 116, for example, Arthur Selle Jacobs made a presentation entitled 'AI/ML for Network Security'.

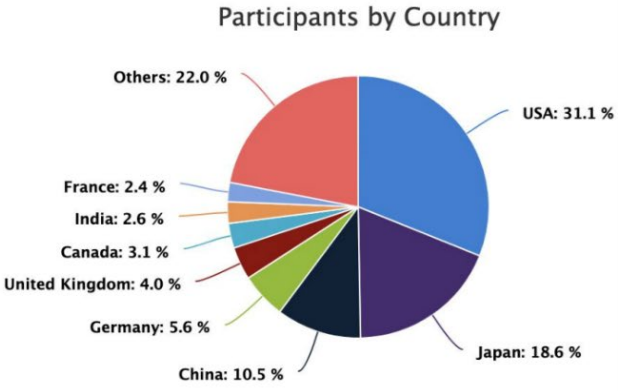
Epilogue

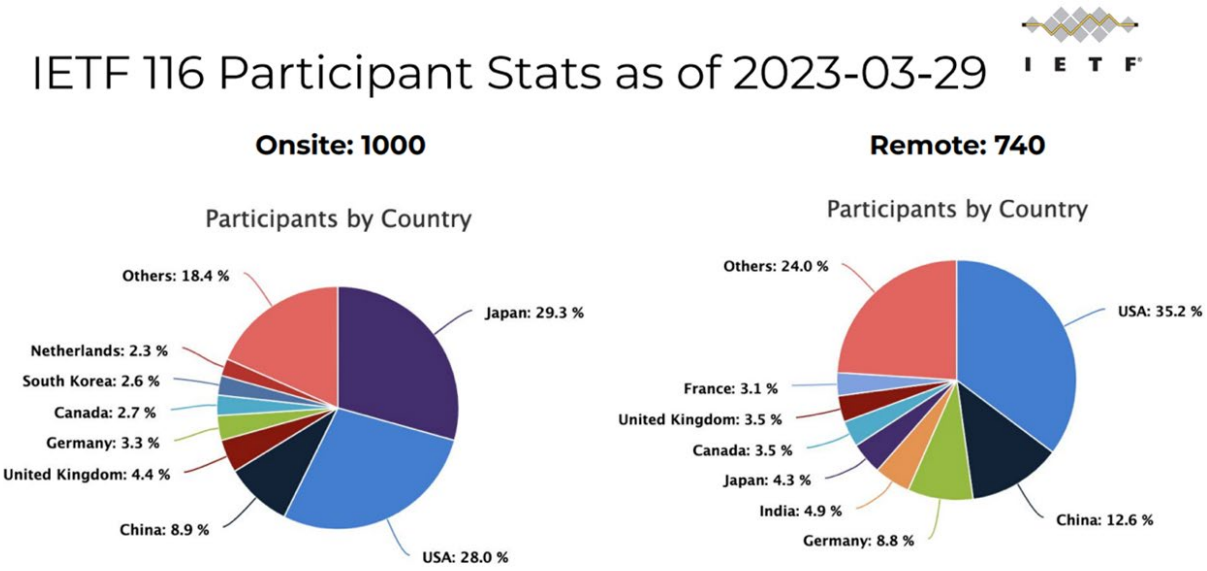
IETF 116 was a successful and very well-organised meeting, for which the host and sponsors deserve great credit. The agenda was once again extensive and substantive. One striking feature of the proceedings was that sessions are no longer confined to definition of the bits and bytes of protocols, but are increasingly complex. Not only are existing standards continually extended, as with DNS and IPv6, but a wide variety of novel initiatives are also being taken. What is more, the IETF is not afraid to tackle challenging topics. Along with human rights and threats to privacy and security, sustainability has an increasingly prominent place on the agenda. How can the emissions associated with fossil fuel combustion be minimised, for example? Every little contribution to emission reduction helps, including the modification of global standards. Future developments also command growing attention, both from the IETF and from the IRTF working groups. As a result, IETF meetings are always stimulating and relevant.

IETF 116 Participant Stats as of 2023-03-29

- **1740** registrations
  - **1000** on-site
  - **740** remote
- Fee waivers - Remote
  - **382** granted, **251** used
- Fee waivers - Onsite
  - IETF: **2** requests, **1** granted
  - IRTF: **7** requests, **6** granted
- **439** Hackathon registrations
  - **361** on-site, **78** remote
  - **72** Hackathon-only (**43** remote, **29** onsite)
  - **29** projects

Detailed attendance stats will be posted after the meeting





Source: https://datatracker.ietf.org/meeting/116/materials/slides-116-ietf-sessb-all-slides-ietf-116-plenary

The next IETF meeting is scheduled for 22 to 28 July 2023 in San Francisco.

Council of European National
Top-Level Domain Registries

About CENTR

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 52 full and 8 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.

Full membership is open to organisations, corporate bodies or individuals that operate a country code top level domain registry.

CONTACT

CENTR VZW/ASBL
Belliardstraat 20
1040 Brussels, Belgium
0885.419.166 | RPR Brussels

+32 2 627 5550

secretariat@centr.org

www.centr.org

FOLLOW US

To keep up-to-date with CENTR activities and reports, follow us on Twitter or LinkedIn