



Council of European National
Top-Level Domain Registries



IETF 117

More than 160 sessions, a 2-day IETF hackathon, and various side events

MARCO DAVIDS, SIDN LABS, AND PAWEL KOWALIK, DENIC





Table of contents

INTRODUCTION	3
INFORMAL ACTIVITIES	3
Hackathon	3
IEPG	4
HotRFC Lightning Talks	4
FORMAL PROCEEDINGS	5
DNSOP WG	5
REGEXT WG	5
OAuth WG	6
IRTF	7
BoF: Detecting Unwanted Location Trackers (DULT)	7
ACM/IRTF Applied Networking Research Workshop meeting	8
Decentralized Internet Infrastructure Research Group (DINRG)	8
IRTF open meeting	8
MAPRG (Measurement and Analysis for Protocols)	8
EPILOGUE	9

Introduction

The mission of the [Internet Engineering Taskforce \(IETF\)](#) is to make the internet better. Most of the IETF's work is done online, but the organisation also holds 3 [meetings](#) a year. The 117th IETF meeting was held in San Francisco, USA, from 22 to 28 July.

With [1,579 registered participants](#), the meeting was slightly less well-attended than the previous one. During the [plenary meeting](#), the IETF's Executive Director Jay Daley told the audience that the IETF Administration LLC was experiencing registration income fluctuations, which were making cost management difficult. Some 905 of the participants (just over 57%) were present on site. The remainder followed the meeting online. No special coronavirus-related measures were in place this time around.

The [IETF Hackathon](#) in the weekend prior to the meeting had 424 participants (362 on site, 62 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](#).

Every IETF meeting has a [packed programme](#). The latest week-long gathering featured 166 working group sessions, a HotRFC, a plenary session and a wide variety of [side meetings](#). Finally, there was a very well-organised social event.

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 now traditional Hackathon got under way on the Saturday prior to the main proceedings. At the Hackathon, the applicability and interoperability of new concepts were tested on a collaborative, non-competitive basis. [Groups](#) were formed spontaneously to work on a [range of experiments](#) from a [long list](#) of very complex challenges. A total of roughly 424 participants interacted and programmed together intensively throughout the weekend. The Hackathon concluded with result [presentations](#) at the Hackdemo Happy Hour.

The work done on the '[DNS table](#)' is worthy of a special mention. The topics tackled by the group included [DNS Out Of Protocol Signalling](#) (DNS-OOPS), a uniform method for signalling certain name server statuses, proposed in a recent draft. DNS-OOPS could, for example, be useful in connection with anycast, where BGP cannot be activated until the name server has signalled that a complete zone file has been loaded and that it's ready to start handling DNS queries. A D-Bus publication channel might be a suitable medium for signalling. Knot software [already uses a mechanism of that kind](#), and the proposal is that other name server implementations can adopt the same approach. However, the draft's authors are also looking at mechanisms such as DOTS (RFC9132) and MQTT.

Method	NOTIFY	D-Bus	DOTS	MQTT
Local to machine	+	++	+	+
inter-machine	+	-	+	+
inter-operator	+	-	++	-
Publish Subscribe	-	-	++	++
Authentication	+-	-	+	+
Client library availability	NA	++	?	++

Figure 1: draft-grubto-dnsop-dns-out-of-protocol-signalling par. 5.5

Another group at the Hackathon focused on the ever-topical subject of post-quantum cryptography (PQC). For a project called “[Adding PQ algorithm support into existing X.509 structures \(keys, signatures, certificates and protocols\)](#)”, they explored the possibility of using PQC in X.509 structures.

The Hackathon was used to test the interoperability of various algorithm implementations, to gain experience of using the new algorithms, and to generate feedback from real-world deployments, for use by the standardisation groups.

IEPG

The Sunday morning of an IETF meeting traditionally begins with the [IEPG](#), where attention is focused on [topics](#) with some form of operational significance.

Fastly’s [Job Snijders](#) made a presentation titled ‘[Roadmap for a More Secure Global Internet Routing System 2023-2028](#)’, arguing for increased BGP security. To illustrate the need for greater protection, he recounted an anecdote regarding an actual security incident. As well as wider use of RPKI, Snijders argued for – and updated the audience on the status of – the further development and adoption of BGPsec, ASPA (Autonomous System Provider Authorization) and [RFC9234](#).

HotRFC Lightning Talks

The Sunday ended with the [HotRFC Lightning Talks](#), where speakers talked on [a wide variety of topics](#) and pitch ideas. In this context, ‘RFC’ doesn’t stand for ‘Request for Comments’ (an important category of documents produced by the IETF), but for ‘Request for Conversation’. The HotRFC session is a fast-paced affair. Each presenter gets just 4 minutes, and no questions are allowed during the session; any feedback has to be given later.

The session featured a total of 9 talks on a [wide range of subjects](#).

Formal proceedings

A few of the many working group sessions are outlined below. Because many of the sessions take place in parallel, it can be difficult choosing which to attend. We are therefore grateful to [Pawel Kowalik](#) (DENIC), who at the meeting spontaneously offered to help by reporting on the [REGEXT](#) and [OAuth](#) IETF working groups, and on the [HRPC](#) IRTF working group.

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. A few highlights are presented below.

Since the previous IETF meeting, 'draft-ietf-dnsop-dns-catalog-zones' has been ratified as [RFC 9432](#). The RFC describes a straightforward, uniform method for providing secondary nameservers with a list of the zones that a primary name server is responsible for. No uniform approach previously existed.

Other drafts awaiting the RFC Editors' attention are 'draft-ietf-dnsop-alt-tld', 'draft-ietf-dnsop-svcb-https' and 'draft-ietf-dnsop-glue-is-not-optional'. However, 'draft-ietf-dnsop-dnssec-validator-requirements' has been parked until further notice. Although the latter concept was considered useful at the outset, DNSSEC has since matured, and its use has become more straightforward and widespread.

Two other drafts – 'draft-ietf-dnsop-zoneversion' and 'draft-ietf-dnsop-dns-error-reporting' – are now at the working-group-last-call stage, implying that they are one step from ratification. For a more detailed account of proceedings at the DNSOP-WG session, see the [APNIC report](#).

REGEXT WG

Despite being fairly small, the Registration Extensions Working Group is responsible for two protocols that are crucial for domain name registers: EPP and RDAP.

In connection with the latter, the WG has concluded two important initiatives. The first involved [enabling the integration of an RDAP server](#) with an OpenID identity provider to provide responses to authenticated users. The second was the definition of a mechanism for an RDAP server to tell clients [what data in a response has been redacted](#). The need for such a mechanism has arisen because, since the GDPR came in, many servers have started to shield certain data. The REGEXT WG has therefore developed a way for servers to tell their clients which fields contain real values, and which don't.

There was also an interesting discussion about the EPP protocol supporting the use of non-ASCII characters in the local part of an e-mail address (known as SMPTUTF8), for inclusion in the registration data. Because SMPTUTF8 isn't yet supported by all mail services, the WG considered whether the addition of an optional all-ASCII address might help during the transitional period.

However, the prevailing view was that it was better to retain the current single-address model for the time being.

The group also tackled the subject of **best practices for domain deletion**, which often leads to incorrect or even vulnerable delegations. That was in response to a study presented at IETF 115: “Risky BIZness - Risks Derived from Registrar Name Management”.

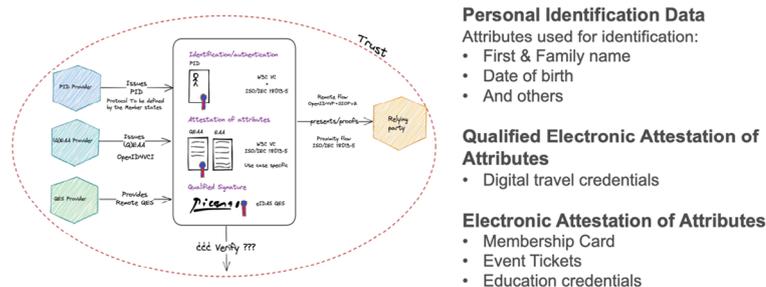
Finally, the WG started the process of looking at future data models that might ultimately replace **jCard** for the representation of contact data in RDAP responses. One option might be **to use JSContact**, a new specification currently under development at the IETF. Another possibility could be a simple JSON-based data model with only the required functionality. Key aspects of any successor to jCard will be the extensibility and internationalisation of address data.

OAuth WG

The Web Authorization Protocol WG is one of the most active working groups in the field of security, holding no fewer than 3 sessions at IETF 117. The last of them, on the Friday, was devoted entirely to ‘verifiable credentials’ and data models, and the associated challenges.

Paolo De Rosa from the European Commission made a **presentation** on the current status of the European Digital Identity Portfolio and the Commission’s plans for achieving the ambitious target of giving all EU citizens access to secure electronic identities (eIDs) recognised throughout the bloc by 2030.

The EUDI Wallet at glance



Personal Identification Data

Attributes used for identification:

- First & Family name
- Date of birth
- And others

Qualified Electronic Attestation of Attributes

- Digital travel credentials

Electronic Attestation of Attributes

- Membership Card
- Event Tickets
- Education credentials



The **Architecture and Reference Framework** describes the cornerstones of the technical solution that will underpin the initiative, ensuring the compatibility and interoperability of the various national systems.

Data formats such as **SD-JWT**, which the OAuth WG is currently working on, will be the ecosystem’s enabling technologies. SD-JWT extends the basic JWT formats by adding functions for privacy protection, such as selective disclosure, which will be a key aspect of the eWallet infrastructure.

IRTF

Most IETF working groups are concerned with the production of internet standards. However, a number of them are engaged in broader 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 are of a high academic standard, and now represent a substantial part of the agenda.

Fascinating though the WG proceedings were, it sadly isn't possible to describe them here in any detail. Nevertheless, the IRTF's discussions provide a useful picture of how the internet is developing.

The proceedings of the [Human Rights Protocol Considerations \(HRPC\)](#) WG are outlined below by way of example.

During the HRPC session, 2 important subjects were covered. First, Guillermo Baltra and John Heidemann made a presentation with the title '[Defining The Internet Core: Partial Connectivity and Internet Fragmentation](#)'. As well as asking how 'the internet' should be defined, and whether there is only one internet, Baltra and Heidemann talked the audience through some interesting measured data on 'islands' and 'peninsulas' – the parts of the network that are not freely accessible from the entire internet.

The [other presentation](#) described the progress that internet protocols have secured in the field of privacy and anti-surveillance protection since publication of the Snowden documents, as described in [RFC9446](#). The implementation of RDAP as a replacement for WHOIS was cited as a good example, with registries playing an important role. Other examples given were the widespread adoption of HTTPS and secure e-mail standards (STARTTLS).

The presentation ended by concluding that, although the Snowden revelations had been a big deal and had led to some vital improvements (thanks partly to [RFC7258](#)), much remained to be done. Indeed, in some fields, things had actually got worse for users, or were in danger of getting worse in the future.

BoF: Detecting Unwanted Location Trackers (DULT)

A [Birds of a Feather](#) session involves looking at a topic to decide whether it is something that the IETF should address. At IETF 117, there was a BoF session on location trackers: devices for tracking the whereabouts of somebody or something.

Location trackers have many legitimate uses, such as enabling people to find their lost keys. Nevertheless, they bring security and privacy concerns, because they can also be used to keep track of someone without their knowledge, for malicious purposes such as stalking.

Various manufacturers have therefore separately developed solutions with a view to protecting users against unwanted tracking. However, the value of such solutions depends on people being aware of the possibility of unwanted tracking, and taking the trouble to download multiple apps and regularly look at them to check whether they are being tracked.

A scalable solution for the detection of unwanted tracking requires that trackers support a universal protocol and behave consistently, so that unwanted tracking can be detected regardless of what make of tracker is involved.

The **DULT WG** has been set up to develop such a protocol. The purpose of the DULT BoF session was to define the problem and to establish whether there was interest in tackling it within the IETF. It was **agreed** that discussions would continue for the time being.

ACM/IRTF Applied Networking Research Workshop meeting

Swapneel Sheth of Verisign Labs made a **presentation** about how the DNS could be integrated with new systems, such as alternative naming systems based on Web3, e.g. Ethereum ENS. According to Sheth, that would boost interoperability and open the door to new applications.

Decentralized Internet Infrastructure Research Group (DINRG)

The **DINRG's purpose** is to act as an open forum for the discussion of phenomena linked to internet centralisation and the potential hazards associated with it. We see centralisation as a relevant field, and we are therefore monitoring this group. One of the **presentations** was on the topic of social networks. How would people reconnect with their contacts if, for example, Twitter were to fold? As a solution to that 'rendezvous problem', as the speaker dubbed it, an approach called **Minimal Global Broadcast (MGB)** was proposed.

IRTF open meeting

Siva Kakarla from UCLA made a presentation titled '**SCALE: Automatically Finding RFC Compliance Bugs in DNS Nameservers**' about a tool for identifying RFC compliance issues in DNS name server software, called **Ferret**. The aim being to automatically generate test cases for DNS name server implementations, covering as many DNS-related RFC specifications as possible. The project has already been reasonably successful, with Ferret picking up various previously unknown bugs.

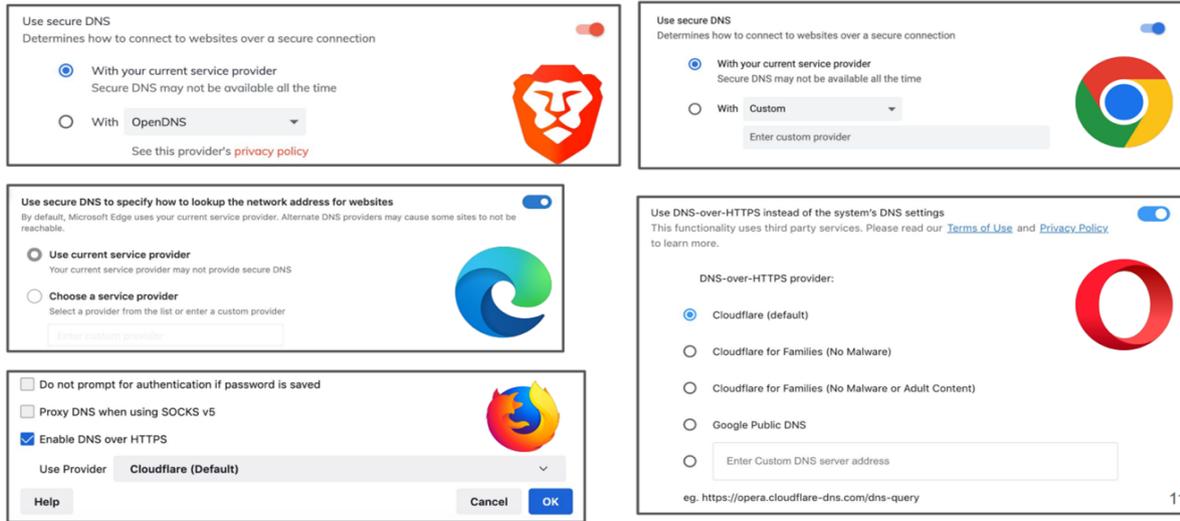
MAPRG (Measurement and Analysis for Protocols)

MAPRG **focuses on** measurements and analyses.

Jayasree Sengupta from the CISA Helmholtz Center for Information Security **presented** the results of a study into the performance of various DNS communication mechanisms (DNSo53, DoT, DoH and DNSoH3, which she confusingly referred to as DoQ on her slides). Her conclusion was that DoH3 performed best overall.

The University of Chicago's Ranya Sharma made a **presentation on Encrypted DNS** and how it could be implemented in various browsers, such as Chrome, Brave, Firefox, Edge and Opera.

Enabling DNS-over-HTTPS



Some of Sharma’s survey questions related to user behaviour in that context. For example, she found that 73 per cent of respondents had heard of the DNS. Of those, 59.9 per cent had heard of Encrypted DNS as well. Sharma’s research also showed that Comcast and Google Encrypted DNS were well-known, but NextDNS and Quad9 were not, while familiarity with Cloudflare was between those two groups’ familiarity. Where settings were concerned, 79.4 per cent of people stuck with the defaults.

Another interesting finding was that the different terms used by browsers (‘Secure DNS’ or ‘DNS over HTTPS’, see the illustration) elicited different perceptions.

Epilogue

IETF 117 was another successful gathering, for which the host and the sponsors deserve congratulations. There was once again a full and stimulating programme, and ample opportunity for participants to network and get to know each other. The focus is firmly on the future, within both the IETF working groups and the IRTF working groups. And, because the future is exciting, IETF meetings are consistently stimulating and relevant.

The 117th IETF meeting took place between 22 and 28 July 2023, in San Francisco, USA.

The next [IETF meeting](#) is scheduled for 4 to 10 November 2023 in Prague.



**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



© This publication has been authored by CENTR. Reproduction of the texts of this publication is authorised, provided the source is acknowledged.