# CENTR Tech Trends Watch

August 2020

The Tech Trends Watch is a new, regular part of CENTR's reporting on current affairs which takes into account ongoing trends in technology development from a range of standards development organisations and other technology forums. Its purpose is to trace out those trends that may have an impact on the addressing and numbering communities, and assess how those developments tie in with external stakeholders such as policy-makers and other industry sectors.

## Private address spaces in the DNS – the flight from ICANN?

**As the United States' isolationism casts ever larger shadows on the centralised but global internet governance mechanisms that have so far preserved the cross-border nature of the world wide web, voluntary technical specifications may be a route to creating both local adaptability and stronger regional autonomy.**

The IETF DNSOP Working Group, which covers DNS operational issues, has been considering a draft on private use top-level domains (TLDs) in the last quarter.[1] The drafters, who are both employed by ICANN, aim to bring structure to the use of top-level domains that are not ICANN-assigned and chart out which two-letter combinations and other special-use TLDs are already commonly in use for private, non-public internet oriented use-cases.

It is not clear that the IETF wants to be in a position where it is seen as making decisions on TLD allocations,[2] but CENTR community representatives have been broadly supportive of the endeavour.[3] Having generic TLDs that are disconnected from the global root is interesting for both internal use in organisations that want to use DNS technologies without being tied to the global internet, and for educational purposes.

Private-use TLDs and the issue of who should get to decide which TLDs are reserved for applications beyond the global root tie back into previous discussions at the IETF – notably in the discussions surrounding .onion and .gnu (see CENTR's IETF reporting from August 2020). The DNSOP drafters seek to contain some of the private-use TLDs to a somewhat fixed list of two-letter codes.

Pre-emptive standardisation is one way of ensuring that the global consensus that emerged from the 1990s DNS discussions, with ICANN managing the one root, is maintained. But for European entities this work also has other implications.

---

[1] https://datatracker.ietf.org/doc/draft-arends-private-use-tld/

[2] Suzanne Wolf at IETF DNSOP WG e-mail list: https://mailarchive.ietf.org/arch/msg/dnsop/3Tg-nO7bAZVkNPTLUNTxA6QuWP0/

[3] E-mail deliberations of IETF DNSOP WG in December 2019 and June 2020.

Tell us what you think!

Increasingly protectionist policies from the US administration create many difficulties for both European and American actors, but in particular they heighten awareness of the intrinsically jurisdictional aspects of DNS security and operations. The contractually binding policy development processes of ICANN, and especially their intrinsic connection to US and Californian jurisdictions (as exemplified by the California Attorney General's intervention in the recent discussions on .ORG), may raise warning flags with European actors and are quite difficult to work past. The voluntary nature of IETF specifications in this case is a shield for European countries increasingly seeking to safeguard their own sovereignties.

## Security in non-public mobile networks brings security to mobile networks – at last

**While mobile networks, owing to the legacy of telecommunications network management and vertically integrated service structure, have been restrained from implementing end-to-end security for communicating parties when facing a general public – not least to ensure opportunities for law enforcement to pursue both criminals and enemies of the state – new use-cases for mobile network technologies in factory environments and other private settings are creating a security revolution.**

A killer feature of the envisaged future 5G networks are the so-called non-public networks. These are mobile network infrastructures not intended for public use, but rather that target specialised environments such as smart cities, vertical factory settings and other services that end-consumers will not (or should not) have access to on their general-purpose rentals. The last quarter saw standardisation work picking up on security features for these non-public networks.[4]

Security in the non-public mobile network case is filled with interesting implications. On the one hand, the government security group known as SA3-Lawful intercept in the 3GPP standardisation community has less jurisdiction in a network that is not intended for regular citizen use. On the other hand, the applications foreseen by equipment and network vendors also require much more robust security features than are typically made available on general-purpose networks. For instance, end-to-end encryption for ensuring the authenticity, integrity and confidentiality of data streams – including much-needed and quick patching features – is within reach for mobile networks in the non-public domain, even as lawful intercept requirements have led to it being rejected for the public network case for over 20 years.

For the addressing community, mobile networks continue to be particularly interesting with respect to identity management and authentication novelties. Traditionally, mobile networks solve identification and authentication in much the same way as telephone networks do - by having nationally assigned number spaces that can be uniquely attributed to a customer in a particular territory for billing purposes. Up until now, mobile networks have not separated identity provisioning and connectivity provisioning at all. But things may be changing.

The new challenges that emerge in internet-of-things or factory settings may require more flexible approaches to identifying both devices and application programming interfaces. Both the assignment of identities and the revocation of identities may need to be done in bulk, at lightning speed, or in an ad hoc manner. The decentralised and adaptable registration features of DNS technology are, as demonstrated not

[4] 3GPP-SA3, Tdoc SP-200620 (FS_eNPN_SEC) Study on enhanced security support for non-public networks

least by CENTR members Afnic[5] and CIRA,[6] more than suitable for dealing with such rapidly changing requirements. Not only does the DNS provide adaptability, it can also be implemented independently by any actor in the networking technology stack and still federate, a feature notably missing from the SIM credential strategy so far deployed in mobile networks.

In fact, non-SIM credentials and authentication is exactly what the 3GPP security folks will be looking at in the upcoming year. While this is likely to create an upset with the established SIM credentials managers of the telecommunications industry, it is a change that has been in the making for some time.

## RDAP and EPP in the air? DNS-based drone identity management

**Airspace management presents new opportunities for internet-style identity management. On the one hand, the ease with which identities are added and removed from domain name system-based resource registries ensures a high degree of pseudonymity for both individual and commercial drone operators. On the other, there are already tried and trusted registries with experience in a robust, time-tested technology base in every country around the globe. As the European Union looks towards a digitally sovereign future, encouraging the participation of domestic internet infrastructure actors in traditionally state-owned database activities could be a way of creating the right conditions for cross-border innovation and regional autonomy.**

The domain name system is essentially a light-weight identity management system where human-language strings are matched to internet resources. The most well-known application is in the identification of resources available on the world wide web since the 1990s, but it is by far not the only type of resource that can be catalogued with DNS-like features.

Several CENTR members are already exploring the management of internet-of-things resource registration and traditional access control in web shops or administration.[7] A more novel application of the core technology of registries is, however, underway in the very recent field of unmanned aerial systems (UAS) identifiers. UAS are more popularly known as “drones”, and this technology field has seen a veritable explosion in the last few years, with device sizes becoming ever smaller and the number of non-professional (hobbyist) drone operators increasing manifold.

This development has raised regulatory concerns. Firstly, the risk that hobbyist drone operators will disrupt traditional airspace activities such as commercial flights by operating their UAS close to airports. Secondly, the risk that hobbyist or even professional drone operators will infringe on individuals’ privacy by flying UAS equipped with cameras close to household windows or over public spaces. Thirdly, a similar set of risks associated with unmanned, automated delivery systems operated by large online retailers, such as Amazon – or the protection of particular delivery operators from competitors, through enabling selective obfuscation of operator identifiers from unauthorized viewers.

While both China and the US are moving at lightning speed to identify technologies and regulatory frameworks for drone identifiers capable of satisfying these requirements, pushing at both domestic levels against manufacturers and internationally at the ICAO, the EU’s domestic civil aviation authorities in EASA

---

[5] https://www.afnic.fr/fr/expertises/labs/projets-en-cours/dins-nommage-et-services-dns-pour-iot-securise-et-sans-couture.html

[6] https://www.cira.ca/labs/projects/cira-secure-home-gateway

[7] See e.g. efforts by AFNIC and CIRA in managing home networks with IoT devices.

have been making more measured advances. As in many other data management fields, EU coordination relies on robust technical interoperability that ensures the autonomy not just of the EU as such, but also of each of its member states.

Starting from US public authorities NASA and FAA, a project is underway to standardise the use of DNS identifiers for UAS, to enable the real-time lookup of drones and their operators, and ensure accountability as well as privacy guarantees. This work is being carried out at the IETF through the DRIP Working Group, with participation of researchers from, among other places, the Linköping University in Sweden.

An advantage of the DNS identifier scheme is that cross-border interoperability is built into the technology as a foundational feature, rather than requiring additional interoperability layers on top of the actual technology. It is in fact an international technology that works the same way in all countries, while still allowing for local implementation and databases. As the diverse CENTR community is well-placed to demonstrate, the DNS can be adapted to local data management requirements and still function not just cross-border in the European space, but also beyond. The emphasis on identity management – keeping track of who is who – is an additional benefit beyond authentication-oriented solutions such as SAML or Oauth.

However, unlike in the world wide web or internet-of-things registration activities, drone operation is a highly regulated field where business models and technologies are ultimately pre-determined by the regulatory landscape. The technologies will be there for the European Union to use, and CENTR members of course demonstrate the feasibility of federated identifier management at European scale and beyond, but the choices may need to be made inside the European civil aviation community before European drone operators can benefit from flexible, modular and pseudonymous resource identifiers. As EASA and SESAR gear up to scrutinise specific technical solutions for a Common Service Management framework in the autumn of 2020, it will become clearer whether fixed, permanent pseudonyms as in a vehicle registry or dynamic, temporary pseudonyms, such as in DNS, will prevail.

## Every European country's right to be uniquely mediocre

**Can European cloud services harness and boost empowering enablement today? Gaia-X is certainly stepping up efforts in this direction. Leveraging experiences from telecommunications, it seeks to facilitate the federation of existing European cloud infrastructures through a JSON-schema for capability and policy communication, that will be interchanged between service providers and service users through open and secure APIs. But while these solutions may well ensure that existing cloud computing capacity in the European Union can scale in a way that respects the geographical sovereignty of each member state, it is less obvious that the nation-state infrastructure model is conducive to cutting-edge innovation and development.**

One of the primary purposes of technical standardisation is to ensure that different vendors in approximately the same sector can produce exchangeable equipment. Notable examples in the European Union are the usefulness of same-width railway tracks, same-voltage and same-number-of-holes electricity sockets or same-width steel pipes for e.g. ventilation or sewers. Ensuring that different equipment is "the same" gives scale advantages in both manufacturing (if a product provider can sell to a larger geographical area) and consumption (since consumers will not be tied to the only product provider that produces that-width pipes).

This principle generally works well for technologies that are established and that do not develop quickly. Pipes, railroads and electricity sockets are installed and stay unchanged – often for decades. And this is something that the European Union has worked on a lot: harmonised standards for the amount of cubic

cylinders in the engine of a light vehicle, harmonised standards for the amount of information that goes on a food label, harmonised standards for the proper way to write a date on a driver's license, and so forth.

It is also the way that telecommunications networks were traditionally built and managed: every European country first experimented with its own network, and at some point someone had the idea to attempt creating an interoperability layer that could compensate for differences in local network deployments. Analogous to how one might use electricity adapters when visiting jurisdictions (notably the UK) where the socket is still not European standard, but on the scale of national territories rather than a hotel bedroom.

European countries have tried this for a lot of things in information, communication and network technologies – and failed. Whether it be network infrastructure, domain name registries or operating systems, the standardisation cycles are longer than the product cycles, so European solutions end up falling behind international competitors. And Europeans that want to stay on the bleeding edge of technology have to purchase solutions in every area from network analytics to computational capacity from abroad or be content with slightly left-behind home-brews.

Understandably, but disappointingly, the latest attempt at European sovereignty in the cloud does not immediately look on track to remedy this short-coming of European technology policy. Unsurprisingly, the project does not aim to benefit from scale and adaptability but to enable everyone with their own national solution to share access to certain features of their infrastructure. Existing descriptions of technical architecture available from the project coordinators[8] appear to be closely modelled on the JSON-schemas already available through the Kubernetes project, which was developed by Google until 2014, at which point it was open sourced and placed into an independent foundation.[9]

That said, in sacrificing bleeding edge technology development the European Union is gaining something else: decentralised governance. With increasing national security tensions around data management and digital sovereignty, it is perhaps inevitable that technical developments are parked to make space for the institutional comfort required for acceptable security arrangements.



[8] https://www.bmwi.de/Redaktion/EN/Publikationen/gaia-x-technical-architecture.pdf?__blob=publicationFile&v=6

[9] https://www.theregister.com/2020/06/17/kubernetes_clayton_coleman_interview/