Digital Sovereignty and Public Key Infrastructure: A dynamic relationship

Victoria Baines
Wednesday 15th March 2026

Version 2

Introduction

The concept of digital sovereignty features prominently in cyberspace governance. By tracing its evolution and analysing publicly available data on digital Certification Authorities (CAs), this paper examines the role of Public Key Infrastructure (PKI) in the assertion of digital sovereignty at national, corporate, and individual levels. Analysis reveals that while the historical distribution of root CAs reflects the balance of power in cyberspace and the technology sector, it appears to be evolving in response to regulatory change, notably in the European Union. Potential future developments are also considered, all of which point to the greater importance of secure communication, authentication, and sovereignty in the sense of technological autonomy.

A Very Brief History of Digital Sovereignty

The concept of sovereignty is very often applied to nation states. In the context of political science national sovereignty may be traced back to the 1648 Peace of Westphalia, which carved up continental Europe between Catholic and Protestant powers. It is seen as a defining moment in Western politics, from which sprung the modern principle of state sovereignty, a national government's control and oversight of whatever happens on its territory.

Sovereignty underpins international law, which prescribes how nation states should behave towards one another. Article 2 of the United Nations charter declares, "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state." Sovereignty empowers states to govern as they see fit, provided they do not interfere in the governance of other states. This balancing rule is at the very heart of modern foreign policy and diplomacy.

The development of the Internet in the late 20th century has challenged established notions of national sovereignty. Perhaps the best known expression of this is found in A Declaration of the Independence of Cyberspace, published by Internet pioneer John Perry Barlow in 1996. Its now famous opening declares:

> *Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.*
>
> *We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.*

Always an ideological statement, it is now seen as somewhat idealistic in its aspiration for the Internet to be a global commons in which governments have no power. In the three decades since its publication, all governments without exception have understandably sought to apply Westphalian Order to the Internet, especially as regards public safety and national security.

Cyber attacks on nation states and their strategic interests have led to an increasing focus on cyberspace governance in international law. As cyberspace became a theatre of conflict and interference in critical infrastructure, there emerged different approaches to establishing rules and limits for the behaviour of states. Among these was the NATO-sponsored production of the Tallinn Manuals, in which a group of international scholars applied existing international laws including the law of armed conflict to cyber operations.[1] This approach was rejected by states such as Russia and China, who instead proposed a new, "comprehensive international convention on countering the use of information and communications technologies for criminal purposes" in the United Nations in 2011 (A/C.3/74/L.11/Rev.1). Almost a decade and a half later, and after multiple rounds of consultation and negotiation, The United Nations Convention against Cybercrime was adopted by the General Assembly in New York on 24th December 2024 (Resolution 79/243). Its provisions include measures for sharing digital evidence for the investigation of serious crimes. It also imposes requirements on states to strengthen their capacity to prevent and combat cybercrime, including through international capacity building and the sharing of technical expertise, all the while reconfirming that national sovereignty still applies (Article 5):

> *Protection of sovereignty*
>
> *1. States Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States.*
>
> *2. Nothing in this Convention shall entitle a State Party to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State by its domestic law.*

So much for hard law. Also in the last three decades we have seen the rise of large technology companies that have both driven and benefited from the Internet revolution. Fortune Global 500 data for 2024 reveals that of the top 20 tech companies (comprising both software and hardware manufacturers) with the largest revenues, 9 are based in the US, 3 each in China and Japan, and 2 each in Taiwan and the Republic of Korea.[2]

The Balance of Power

When we look at the rapidly evolving technology of Artificial Intelligence (AI), we see a different trend. Stanford University's AI Index reports that in 2023, 82.40% of patents granted for AI originated from East Asia and Pacific, with China accounting for 69.70% of the global total. While this cannot be said to be a predictor of the concentration of the tools and products that will dominate the market, it is certainly an indicator of investment in AI research and development.[3]

In the fields specifically of national and cybersecurity, in recent years we have seen numerous examples of nation states pushing back against what it sometimes framed as the 'technological hegemony' of the countries where the world's largest tech companies are based. In some cases this has manifested in threatened or outright bans of software that is identified as outside the effective technical control of the government. End-to-end encrypted apps such as WhatsApp and Signal are (officially if not practically) inaccessible from several countries for this reason.

1 https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9
2 https://fortune.com/ranking/global500/?sector=Technology
3 https://hai.stanford.edu/assets/files/hai_ai_index_report_2025.pdf

In others, the foreign ownership of and data processing by a service is assessed as a national security risk, as in the case of the TikTok, subject to ongoing pressure by the US government to acquisition by a US company, and whose use by government employees has been prohibited in various countries. We have also seen a raft of online safety legislation introduced in recent years, including the UK Online Safety Act and the EU's Digital Services Act, the aim of which is to formalise mechanisms and hold online platforms accountable for safe and secure use of their services, regardless of where in the world their operations are based. We have certainly also seen the exercise of national sovereignty as regards 5G infrastructure, with components manufactured by Huawei and ZTE explicitly prohibited or phased out from telecommunications infrastructure in the Five Eyes countries (UK, US, Canada, Australia, and New Zealand) and several states in the EU, including Germany, Romania, Estonia, and Sweden.

Balance of power is spread more evenly spread across countries, companies and NGOs when it comes to the operational governance and security of the global Internet. Here there is a greater tendency for 'bottom up', multistakeholder initiatives that anyone can join – whether governments, companies, civil society organisations, or individuals. Since 1986, the Internet Engineering Task Force (IETF) has been the world's leading organisation for the development and voluntary agreement of standards for the effective operation of the Internet. The management of the World Wide Web is similarly multinational and multistakeholder, marked in particular by the transition of the Internet Assigned Numbers Authority's top level domain assignment functions from US-led management in 2016. It is also worth noting in this context that the UN specialised agency for digital technologies, the International Telecommunication Union (ITU) boasts a membership of "more than 1000 companies, universities and international and regional organizations", in addition to 194 Member States.[4]

What, then of digital certification? Analysis of public data for the test websites of root certification authorities (CAs) enables us to test assumptions about the balance of power by mapping the owners of root certificates to their geographical locations. Data for all root certificates can also be compared to data for those returned as valid.

Mapping Root CA data – method and analysis

Among the tools linked to by the CA/Browser Forum is the cert.sh resource, created and maintained by Sectigo engineer Rob Stradling. For each of the test websites for root certificates, a result is returned regarding its validity at the time the cert.sh URL is visited, and specifically whether the certificate has expired or removed from trust stores. Data for all root CA owners and certificates was downloaded on 20th July 2025 at 14:52:20 UTC. This comprised 671 lines of data, for which the geographical location (city and country) of the owner company or other legal entity was added. Where this was not immediately obvious, this was obtained through open source research. While this data has been checked, the manual aspect of its collection means that errors cannot be ruled out. The hope is nevertheless that it provides helpful indicative insight. A total of 60 countries were identified as locations for root CAs as listed on the cert.sh website, as follows:

4 https://www.itu.int/en/about/Pages/default.aspx

Mapping Root CA data – method and analysis

Among the tools linked to by the CA/Browser Forum is the cert.sh resource, created and maintained by Sectigo engineer Rob Stradling. For each of the test websites for root certificates, a result is returned regarding its validity at the time the cert.sh URL is visited, and specifically whether the certificate has expired or removed from trust stores. Data for all root CA owners and certificates was downloaded on 20th July 2025 at 14:52:20 UTC. This comprised 671 lines of data, for which the geographical location (city and country) of the owner company or other legal entity was added. Where this was not immediately obvious, this was obtained through open source research. While this data has been checked, the manual aspect of its collection means that errors cannot be ruled out. The hope is nevertheless that it provides helpful indicative insight. A total of 60 countries were identified as locations for root CAs as listed on the cert.sh website, as follows:

Country	Root Certificates	Country	Root Certificates
USA	225	Tunisia	4
China	50	Cabo Verde	3
Spain	41	Norway	3
Switzerland	22	Slovak Republic	3
Japan	21	Slovenia	3
Belgium	19	Thailand	3
Germany	18	Turkey	3
India	18	Bangladesh	2
Hungary	17	Bulgaria	2
Poland	17	Denmark	2
France	15	Hong Kong	2
Bermuda	13	Pakistan	2
Finland	13	Romania	2
Greece	12	Saudi Arabia	2
Taiwan	12	Singapore	2
UAE	11	Uruguay	2
Curaçao	10	Venezuela	2
Malaysia	10	Australia	1
Brazil	8	Chile	1
South Africa	8	Croatia	1
Czechia	7	Estonia	1
Lithuania	7	Indonesia	1
South Korea	7	Italy	1
Austria	6	Latvia	1
Netherlands	6	Luxembourg	1
Canada	5	Macau	1
Israel	5	Serbia	1
Portugal	5	Sri Lanka	1
Colombia	4	Sudan	1
Sweden	4	UK	1

The top two countries in the table above may come as no surprise given their dominance of the global tech industry, also their prominence in the exercise of digital sovereignty as described above. Perhaps less expected is the offshore contingent, and the number of root certificates owned by some CAs based in the European Union (on which more below). This data has also been visualised as a treemap (See Annex, Figure 1) to aid comparison of countries' respective market shares.

When data only for valid root certificates is selected, this provides insight on current locations of digital trust. A total of 193 root certificates were identified as valid by cert.sh when the data was generated and downloaded. These are grouped by country as follows:

Country	Valid Root Certificates
USA	79
China	14
Germany	10
Spain	9
Bermuda	7
Belgium	6
Hungary	6
India	6
Switzerland	6
Taiwan	6
France	5
Japan	5
Poland	5
Finland	4
Greece	4
South Korea	4
Austria	2
Czechia	2
Norway	2
Romania	2
Slovenia	2
Croatia	1
Hong Kong	1
Italy	1
Slovak Republic	1
Tunisia	1
Turkey	1
UK	1

It is immediately evident that this is a much smaller list of countries that we can identify as locations for trusted root CAs. Here and in the associated treemap (See Annex, Figure 2), the concentration in the US is undeniable. Equally, it would appear that a sizeable number of countries in Latin America, Africa, the Middle East and the Asia Pacific region are no longer served by local or even regional root CAs with valid certificates. Recognising that the list published by cert.sh may not be complete, it nevertheless prompts the question why some government root CAs no longer have valid certificates, and to whom they have since turned for this service. Geographical mapping of geocoded data for locations of all root CAs tested and valid root certificates (See Annex, Figures 3 and 4) yields further insight on their concentration within individual countries.

There are also, of course, a number of countries that are notable by their absence from these lists. US-based CAs are prohibited from doing business with entities in countries on the sanctions list of the Department of Treasury's Office for Foreign Assets Control (OFAC), which includes Russia, Iran, North Korea, and Venezuela.[5] Russia announced the establishment of its own "Trusted Root CA" in March 2022.[6] This coincided with Ukraine's request that ICANN revoke Russia's top levels domains and that RIPE do the same for its IP address delegation – further demonstration, if it were needed, that geopolitics is more relevant than ever to the security of communications infrastructure.

EU countries are clearly more prominent in the active list than on the larger list of root CAs past and present, and it is reasonable to assert that to some degree this may reflect regulatory change in the region. The electronic Identification, Authentication and Trust Services (eIDAS) Regulation aims to improve assurance across the EU by introducing a common framework for electronic identification and trust services in the digital single market.[7] Included in the list of trust services are digital certificates, under the terminology of Qualified Website Authentication Certificates (QWACs), to be issued by Trusted Service Providers (TSPs). In the data generated by cert.sh, these appear to correspond to the root CAs in EU Member States. It is also worth noting that eIDAS has been adopted into UK law as The UK eIDAS Regulation.

5 https://www.wiyre.com/list-of-countries-banned-restricted-from-obtaining-ssl-certificates/#
6 https://www.eff.org/deeplinks/2022/03/you-should-not-trust-russias-new-trusted-root-ca

Microsoft's own announcement of its sovereign solutions heralds a move away from "sovereignty as niche requirements for a unique set of customers." New features available to all European cloud regions later this year will include: for the Sovereign Public Cloud offering Data Guardian, which ensures only Microsoft personnel residing in Europe control remote access to systems by Microsoft engineers; the ability for customers to connect to Azure using keys stored on their own Hardware Security Module (HSM); for the Sovereign Private Cloud offering Azure Local and Microsoft 365 Local, which will operate "in-country, on-premises or in partner-operated datacenters", "enabling organizations to meet specific data residency and sovereignty requirements." Delivery is envisaged through a partner program that gives customers the ability to choose suppliers who are headquartered in Europe – Leonardo, Vodafone, Orange, and Telefónica Tech among them.

The eIDAS Dashboard includes its own list of trusted services. On 24th July 2025, these numbered 248 active providers, of which 49 offer QWACs. These 49 TSPs are distributed by country as follows (See Annex, Figure 5 for corresponding tree map):[8]

Country	Active QWAC TSPs	Country	Active QWAC TSPs
Spain	12	Hungary	2
Bulgaria	4	Portugal	2
Slovak Republic	4	Slovenia	2
Germany	3	Belgium	1
Italy	3	Croatia	1
Poland	3	Finland	1
Austria	2	Netherlands	1
Czechia	2	Norway	1
France	2	Romania	1
Greece	2		

7 Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market, as amended by Directive (EU) 2022/2555 and Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.
8 Here, too, the caveat applies that the data has been subject to manual cleansing.

Once again, Spain appears to be leading the pack in terms of the European PKI trust market. As the framework and measures set out in eIDAS continue to be brought to bear, it is reasonable to expect that we will see a further proliferation in TSPs offering QWACs in EU Member States – perhaps even in the UK. **"Sovereign capability" is a concept traditionally associated with defence and kinetic security. The UK's National Security Strategy for 2025 pointedly includes cyber in its activities to improve sovereign capability, imposing requirements on businesses to enhance their cybersecurity, acknowledging that "reliance on data centres and other forms of digital infrastructure will also increase vulnerabilities to cyber-attack", and committing the government to "increase the cyber and economic security defences which are vital to our ability to achieve innovation and growth."**[9] Taking a longer range look at the future, several other developments are worthy of consideration.

The Future of Digital Trust

Thus far, this paper has considered digital trust in the here and now, in particular against the backdrops of regulation and geopolitics. Analysis has revealed that the exercise of sovereignty is increasingly evident in digital trust architecture, including data protection, supply chain assurance, use of AI, and certification. Public Key Infrastructure (PKI) both reflects and responds to global security developments.

When we scan the horizon, it is reasonable to assert that trustworthy authentication will be even more important in the future. If – and it is a big 'if' – developments in AI and quantum computing continue along their envisaged trajectories, the mid-term future will be one of superpowered automation on a grand scale. We also need to factor in the ongoing proliferation of objects requiring authentication, the Massive Internet of Things (MIoT), which is already transforming manufacturing, logistics, and critical infrastructure, is increasingly incorporated into smart city and consumer applications.

Market estimates inevitably vary. In 2023, Statista estimated that there were 15.14 billion IoT devices and that this would almost double by 2030, to 29.42 billion. Earlier this year, the forecast was extended to 40.6 billion by 2034.[10] In other words, the world is on a trajectory from a ratio of two connected objects to every human on the planet, to four to one in the next five years, to coincide with the ITU's projected standardisation of 6G communication.[11]

This future is one in which the speed and scale of authentication requirements are such that, while there will still need to be a human in the loop, certification, monitoring, and revocation will need to be automated. Meanwhile, developments in other technologies such as additive manufacturing (4D Printing), the continued proliferation of low earth orbit (LEO) satellites and picosatellites, and successful testing of a 'space internet' all indicate that there will be increasing demand for secure communication and authentication in space.[12] This brings additional geopolitical factors to bear, with connected devices subject to the UN Outer Space Treaty, and the market currently dominated by US companies such as SpaceX.

9 https://www.gov.uk/government/publications/national-securtty-strategy-2025-security-for-the-british-people-in-a-dangerous-world/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world-html
10 https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
11 https://www.6gworld.com/exclusives/itu-6g-standardisation-ready-no-later-than-2030/
12 https://spacesecurity.wse.jhu.edu/2022/11/16/south-koreas-danuri-orbiter-demonstrates-space-internet-en-route-to-moon/

Zooming in from outer space to the level of individual consumers, progress in medical IoT is expected to continue and its deployment to expand. Millions of people around the world already benefit from connected, implanted medical devices such as cardioverter defibrillators, insulin pumps, and continuous glucose monitors. Recent high profile advances in Brain Computer Interface technology build on the use of neural implants to alleviate the symptoms of medical conditions such as epilepsy and Parkinson's Disease. Many medical IoT devices currently use Bluetooth to communicate with a mobile app, which in turn relies on the patient's mobile or Broadband connectivity. Here, too, there will be greater need and increasing demand for secure communication and authentication. Our brains and bodies are arguably the most precious connected objects.

This future is also one in which there may be a compelling use case for much hyped blockchain technologies. Where scale and speed can challenge manual PKI and certificate management, a distributed ledger could provide an unalterable record of certificate issue and revocation, thereby enhancing security and strengthening trust. Several research institutions have been working on this in recent years, including Google and the China Mobile Research Institute.[13]

All these potential developments suggest that the line between cybersecurity operations and geopolitics will in the future be increasingly blurred. There is, perhaps, no better illustration of this than the fact that the owner of SpaceX and Neuralink was until May of this year a member of the US government. In this future, digital sovereignty becomes as much a matter of assuring technological autonomy as of exerting national jurisdiction. It is a world in which organisations in all sectors must continuously account for their supply chain decisions – our world, only more so.

Conclusion

This review of the past, present and future of digital sovereignty concludes that governments in Europe, including the UK, are taking steps towards digital autonomy in the interests of national defence and security, and not least their economies. In the context of the current geopolitical climate, they are moving to counteract the potential impacts of over-reliance on digital service providers in countries whose market dominance is increasingly intertwined with the complexities of foreign policy and cyber diplomacy. Global service providers appear to be responding to that need, and lawmakers are creating new regulatory frameworks, opportunities for businesses to exercise greater self-sufficiency, and markets for sovereign solutions. While the United States and China may maintain their leading positions in investment in tech development, the European Union is once again showing itself to be a leading global force in cybersecurity, triggering the emergence of a new ecosystem of trusted digital service providers in which certification and Public Key Infrastructure have central roles.

13 https://github.com/google/trillian/blob/master/docs/papers/VerifiableDataStructures.pdf; https://patents.google.com/patent/CN106384236A/en; https://ieeexplore.ieee.org/document/9343059

Fig. 1 Countries by number of Root Certificates (listed at https://crt.sh/test-websites, captured 20/07/2025)

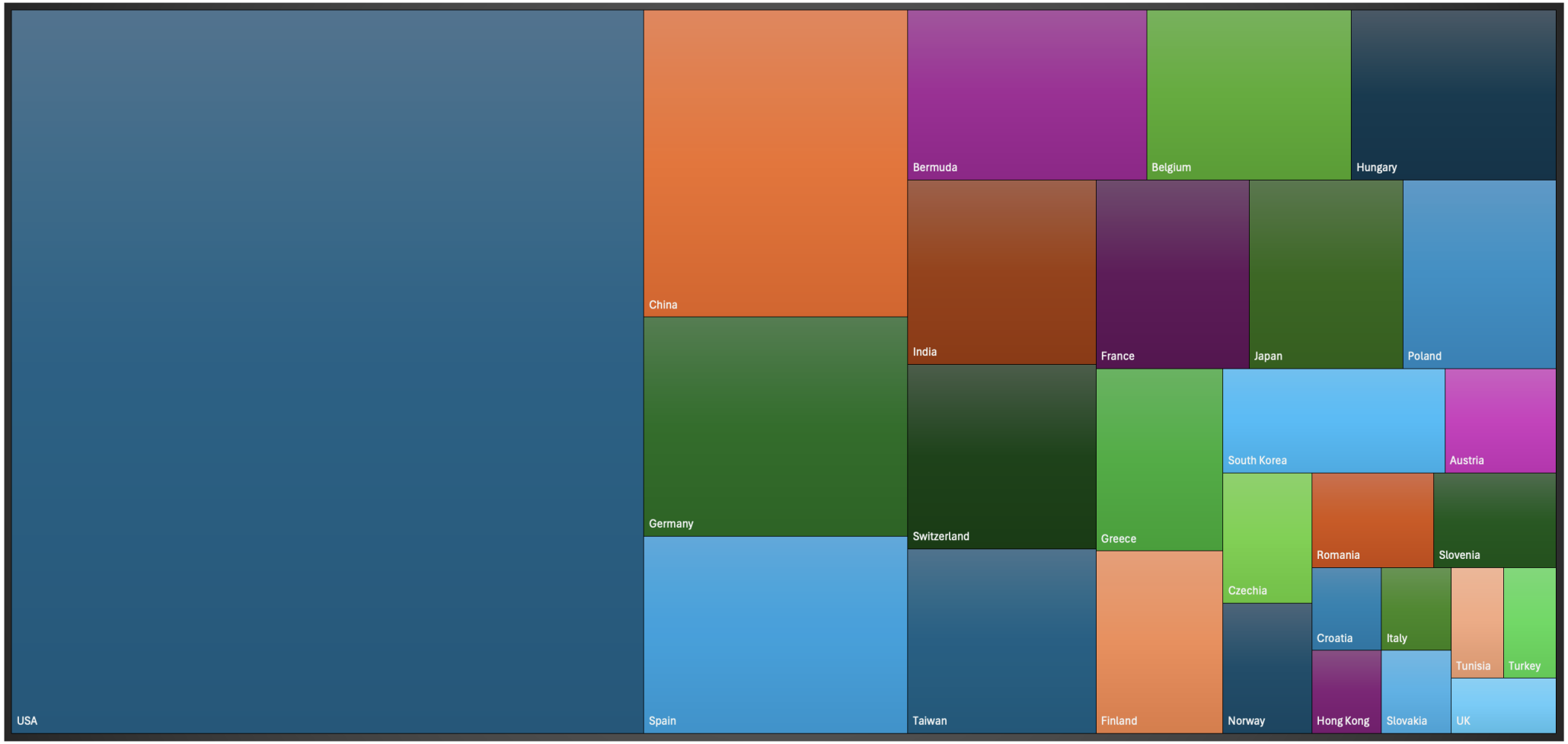

Fig. 2 Countries by number of Valid Root Certificates (listed at https://crt.sh/test-websites, captured 20/07/2025)

Fig. 3 Root Certificates past and present mapped by city and country (all test websites listed at https://crt.sh/test-websites, captured 20/07/2025)

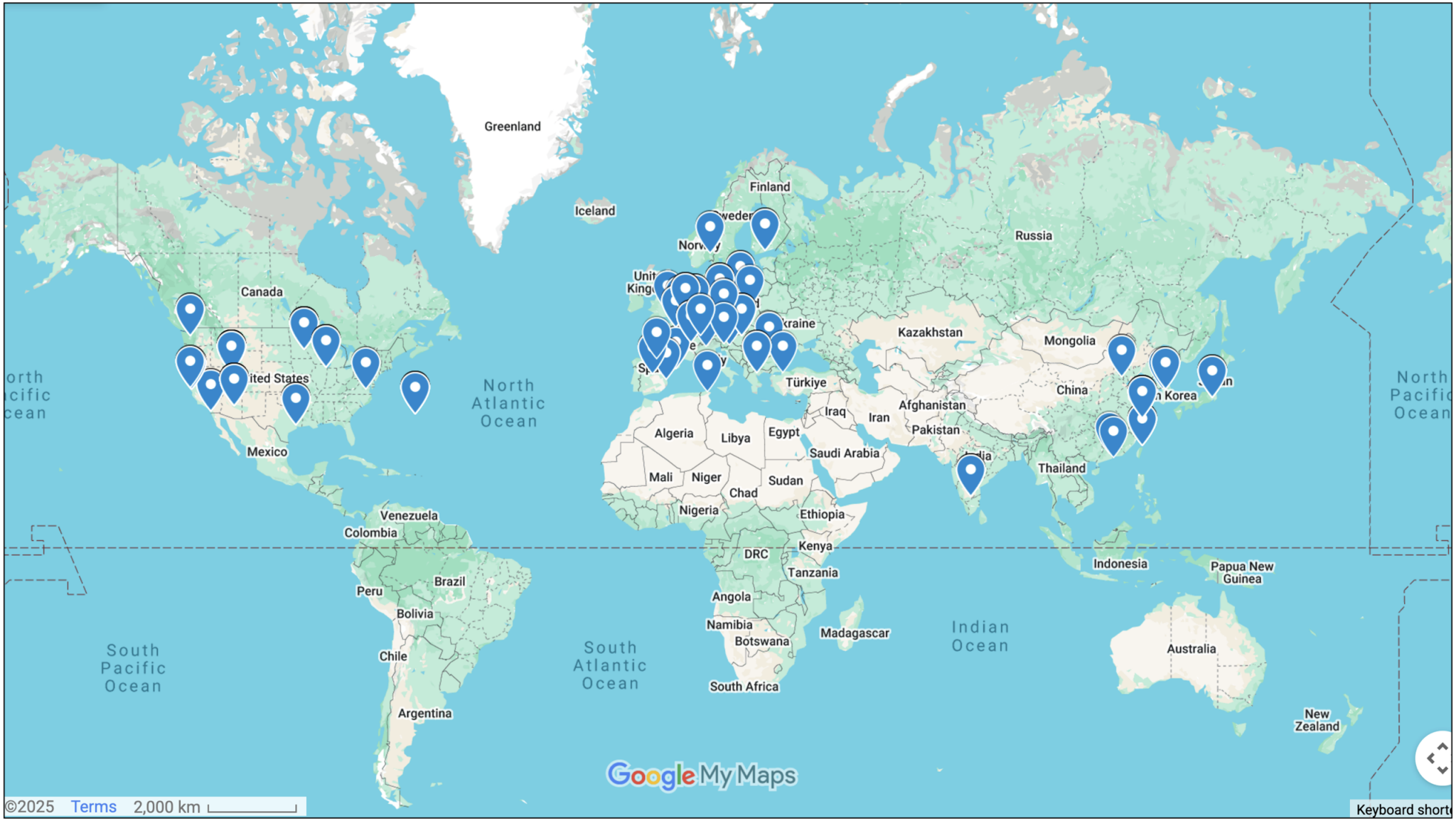

Fig. 4 Valid Root Certificates mapped by city and country (all test websites listed at https://crt.sh/test-websites, captured 20/07/2025)

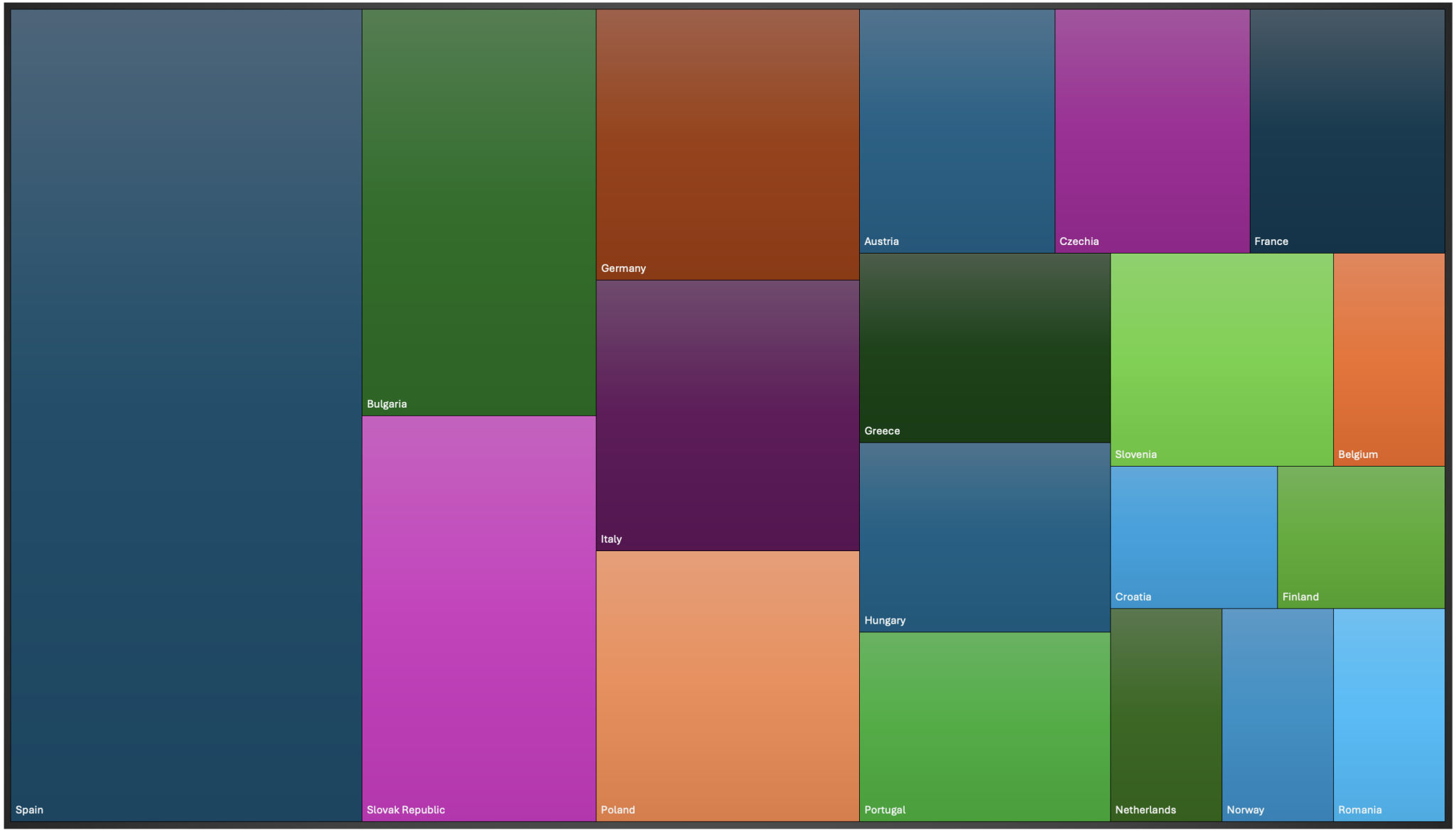

Fig. 5 Active eIDAS Trusted Service Providers offering QWACs, by country (listed at https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls/search , captured 24/07/2025)

Any further questions?
Contact our team

Email
info@aretiico.com

Telephone
+44 (0)20 8087 1000