

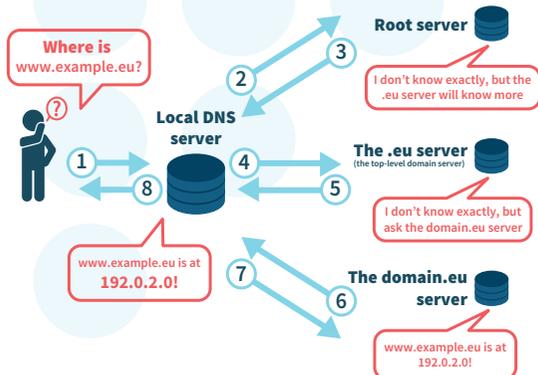
The DNS

The domain name system (DNS) associates domain names with IP addresses, as humans can more easily remember names than numbers.

 Think of it like the internet's address book.

The DNS is a hierarchically-organised database, which contains information on the 1500+ top-level domains (TLD) and their respective IP addresses. Each TLD registry manages the information and resolves DNS queries for their respective TLD.

In practice, for applications to work and/or communicate with each other via the internet, domain names need to be translated into machine-readable IP addresses. This is done through what is called a DNS query, which is launched every time a user wants to access a website or send an email.



Once you type a domain name into the browser, the computer will ask a DNS resolver (typically run by your ISP) for the domain name's IP address, e.g. www.example.eu. The resolver starts by asking "at the top", i.e. the root name server for the IP address of the DNS (registry) server (to find the TLD .eu). The DNS resolver then asks that DNS registry server for the IP address of the DNS server (to find the second-level domain, example.eu). With this information, the DNS resolver can finally ask the IP address for www.example.eu, and passes it back to the browser, which then contacts the website host using the IP address. HTTP traffic begins: you can see the webpages and their content.

It takes **less than 3 milliseconds** to resolve a DNS query (i.e. to find the website once you type it into a browser)

More information:

<https://www.centri.org/education/the-dns.html>

Key industry terminology explained

Registry vs. registrar vs. registrant:

A domain name registry is the technical operator and manager of a top-level domain (for example .de, .eu, .com). They almost exclusively work with registrars, which are the bodies that sell domain names to the public. The registrant is the person or company that purchases, i.e. registers, the domain name. If the registrant makes changes to the domain, the registrar will pass on that information to the registry, which then updates its database.

Domain name vs. website:

A domain name is not a website. The domain name is the address which helps your device find and access the online resources you are looking for. These can be websites, email servers or any other online resource. The website consists of webpages and content. Domains or domain names do not hold any content; they are the "address" of the website.

ccTLD vs. gTLD:

A top-level domain (TLD) is the right-most label of a domain name (www.example.eu). Two-letter TLDs are referred to as country codes, as defined in the ISO-3166-1 list, a standard developed by the International Organization for Standardization (ISO). TLDs with three or more characters are referred to as "generic" TLDs, or gTLDs (e.g., .org, .com, .name). ccTLDs are governed by national and international law, while gTLDs also need to comply with ICANN (www.icann.org) policies.

To view a full list of TLDs that are part of the internet, see IANA's Root Zone Database:

<https://www.iana.org/domains/root/db>



The association for exchange, dialogue and innovation of country code domain registries in Europe

www.centri.org



The Council of European National Top-Level Domain Registries

CENTR is the association for exchange, dialogue and innovation of country code top-level domain (ccTLD) registries in Europe, such as .ee for Estonia or .de for Germany.

It brings together the TLD registries of all country codes of the EU Member States (plus .eu), the European Free Trade Area (EFTA) countries and beyond in order to collaborate and share knowledge and expertise.

Fun fact: Together, its full members manage 50% of all country code domain name registrations worldwide, representing more than 75 million registrations.

CENTR acts as a channel of communication to internet governing bodies and other

organisations involved with the internet. It promotes the interests of ccTLDs and advocates on their behalf.

Together, its full members manage **50%** of all country code domain name registrations worldwide, representing more than **75 million** registrations.



ccTLD registries

A country code top-level domain (ccTLD) registry operator manages or administers a country-specific top-level domain, such as .si or .eu. It is like a database for all the domains in its TLD.

In short, this means that you are directed to the correct website when you type in a URL and that when you send an email, it goes to the right recipient.

Behind the scenes is more complex, as registries have to manage the registration of domains, including running the technical infrastructure of the DNS and managing the zone file (database) that includes all domain names registered under the specific top-level domain. Registries also invest a lot of time and effort into ensuring the security of the network and processes, including by following national and international standards for information security.

84% European registries are not for profit.

You can find more information at:

<https://www.centri.org/education/ccTLD-registry.html>

Not one ccTLD registry operator is like another!

They vary considerably in business models, ownership and size.

They can be foundations, cooperatives, universities, research institutes or part of their government. Many registries also invest considerably in education programmes for their local internet community and have strong links with their local governments.

84% European registries have formalised contact with their government.

Find out more with CENTR!

CENTR provides trainings to EU policy-makers and other stakeholders on how the internet and specifically the DNS works and how it interacts with other stakeholders in the internet ecosystem.

If you would like to learn more about CENTR, to meet with us or to request some training for yourself and/or your colleagues, you can reach us at:

CENTR vzw/asbl
20, Rue Belliard,
1040 Brussels, Belgium

+32 2 627 55 50
secretariat@centri.org
www.centri.org

ccTLDs and EU Policy

ccTLD registries are important because:

- They operate the technical layer of the internet's infrastructure that makes sure that applications and websites are accessible to citizens and businesses.
- They help users navigate the internet and find content online, but they do not host, nor pass any online content through their infrastructure.
- They are committed to a resilient, stable and secure internet as a key of their success.
- ccTLDs are rooted in their local jurisdictions and are closely linked to their local internet communities (including governments).

CENTR asks policy-makers to safeguard the stability and integrity of essential technical infrastructure: far-reaching actions and blanket definitions may risk or endanger the integrity and technical stability of the DNS.

ccTLD registries are mainly governed by national law. Yet, a number of EU policies impact their daily operations (e.g. cybersecurity, privacy and data protection, consumer protection). Other (non)legislative and standardisation initiatives, both at European and international levels, also play a role.

Cybersecurity

EU cybersecurity policies consider registries to be part of critical digital infrastructure: i.e. "operators of essential services".

Around 87% of European ccTLDs are either already certified or undergoing the process of cybersecurity certification under the International Information Security Management System (ISMS) standards, such as ISO/IEC 27001.

96% of European registries have been identified as being an "operator of essential services" by their government.

CENTR calls on policymakers to ensure that European cybersecurity policy or standardisation efforts do not duplicate or contradict efforts at international level.

Data Protection

ccTLD registries maintain a registration database that is used to collect and access the contact information of domain name holders (so-called WHOIS). This data contains personal information that is governed by EU data protection laws. Sometimes this personal data is used by law enforcement authorities to conduct their investigations.

CENTR asks policymakers to respect the principle of subsidiarity and proportionality when addressing the need for cross-border access to data held by registries. ccTLD operators have well-established information channels to their local law enforcement authorities, meaning that the mutual trust is established by a long-standing practice and network-building. Any cross-border data access request from a foreign law enforcement authority needs to respect local jurisdiction.

Consumer protection

Registries take great care to ensure that their domain zones are free from abuse. Consumer trust in online services is an important element for any business, including technical operators like ccTLDs.

Suspending or deleting a domain name and as such removing it from the DNS means that a user will no longer get a valid IP address when looking up the domain name. Deleting or suspending a domain name is a drastic intervention in the DNS, with the effect that the domain name can no longer be used to navigate to content that is published under the domain name and its different subdomains, and that all services linked to the domain name, such as email, stop working. Suspending or deleting domain name does not remove illegal content from the internet.

Forms of online filtering, such as DNS blocking, i.e. the mapping of a domain name to an IP address, does not remove illegal content from the internet either, and can be easily circumvented.

CENTR calls on policymakers to make informed decisions when addressing illegal content online and the role of ccTLD registries within the technical layer of internet infrastructure. DNS blocking measures are ineffective to protect consumers from online fraud and should be regarded as an interim measure to be used in the case of an emergency. Any decision to delete or suspend a domain name should take into consideration all the consequences and balance prudence with proportionality.