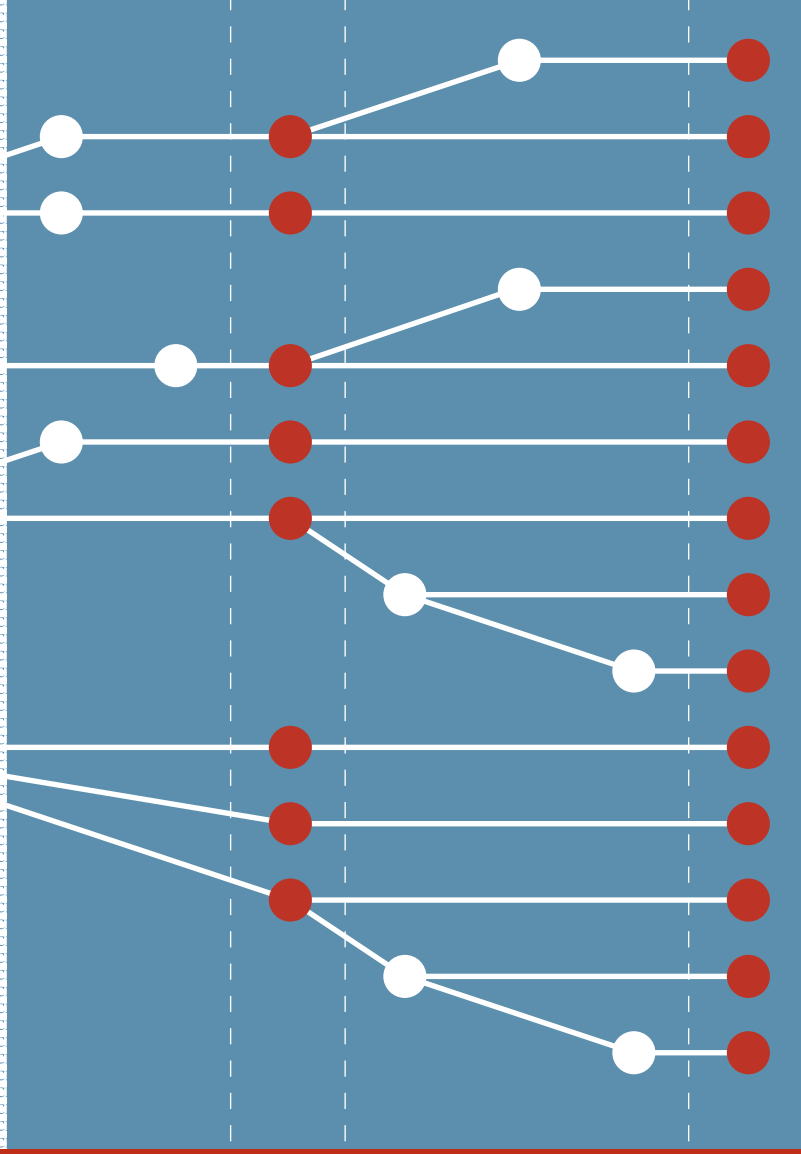
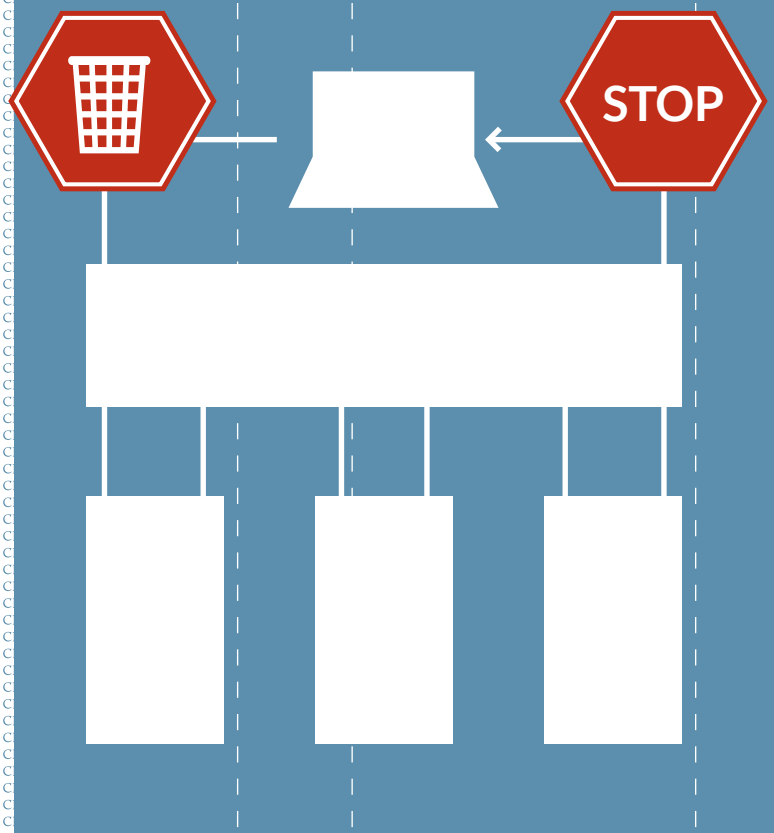


Domain conflicts and the legal system



FOREWORD

Today's live without the Internet is difficult to imagine. Many people are connected on a daily basis and use the Internet for much more than communication and entertainment. The Internet has become relevant also from a social, economic, political and legal perspective.

Not surprisingly, some of the conflicts that exist in the 'real world' pop up in the online world and the traditional law enforcement and legal actors are expected to deal with them. Some of those conflicts are linked to domain names, others arise because of services that are offered on the Internet or content that is published online.

The Internet and in particular domain names, are relatively new areas for the legal and law enforcement community. This guide wants to provide those involved such as legislators, judges, lawyers, prosecuting authorities and the police, with a level of knowledge of the technical and practical aspects of conflict resolution and the legal processes in this field.
This document is based on a brochure published by NORID, the registry for the Norwegian national domain name .no and was modified by CENTR to an international context.

We hope that this guide will be a useful tool, and we will be only too pleased to receive your suggestions or to respond to your questions.

CENTR, February 2012

01 INTRODUCTION

This guide explains what a domain name is and how the global domain name system (the DNS) is linked together. It describes the organizations involved, their roles and responsibilities, and explains the difference between a dispute involving the domain name itself, and a conflict about services or content found within a given domain.
Furthermore, the brochure also describes what happens when a domain name is deleted. It is important to be aware of the benefits achieved on deletion, but also to be fully aware of what we fail to resolve when we delete a domain, and the unintended consequences that can result from a deletion.
In conclusion, we provide an overview of the operations that can be carried out on a domain name, and how conflicts can be managed both within and outside the legal system.

About CENTR

CENTR is an association of Internet Country Code Top Level Domain Registries such as .uk in the United Kingdom and .es in Spain. Full Membership is open to organisations, corporate bodies or individuals that operate a country code top level domain registry. CENTR provides a forum to discuss matters of policy affecting ccTLD registries and acts as a channel of communication to Internet governing bodies and other organisations involved with the Internet. It promotes the interests of not-for-profit ccTLDs and lobbies on their behalf.

02 THE INTERNET ADDRESS SYSTEM

It are the services provided on the technical infrastructure that represent value to Internet users. The best-known services are websites and email, but it is also possible to use the net for activities such as connecting telephone conversations, downloading files and logging on to various databases.

So how do we get access to these services? All computers linked to the Internet have their own IP address, which consists of a long series of numbers. Using this address makes it possible to connect directly to a computer. However, to save users from having to remember long strings of numbers, the Domain Name System (DNS) attaches a unique domain name to the IP address in question.

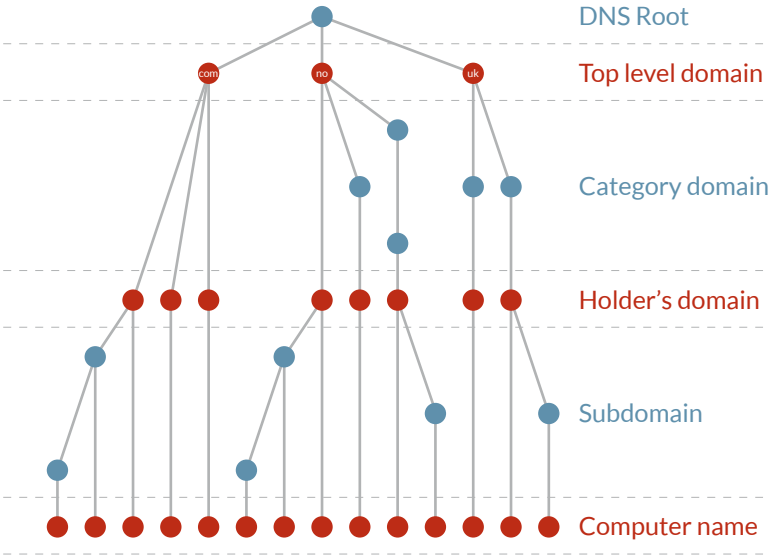
The terms domain name and domain are used interchangeably.

The domain name system represents the Internet's "telephone book". The domain name is used to look up addresses in the domain name system in the same way as you look up a name in a telephone book in order to find the right number. This lookup process sets in motion a search for an IP address which is then used to contact the computer offering the service you require access to. We all know that a telephone conversation is not conducted through the telephone book itself. In the same way, Internet traffic does not pass through the domain name system.

Domain names are commonly written in the form companyname.XY. If the domain name offers services such as websites and email, the web address may be www.companyname.XY, and a typical email address within the domain may be written in the form firstname.surname@companyname.XY. It is important to note that it is possible to register and hold a domain without it offering services to users.

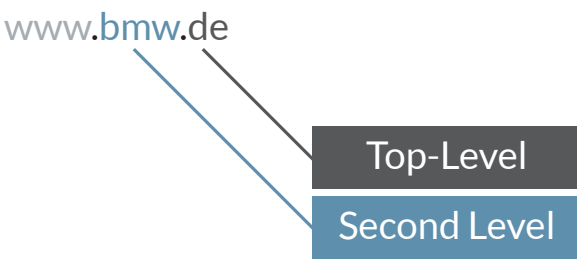
A domain name is always unique as the spelling is different. This rule applies even if the two names share the same meaning, the same domain holder and point to the same IP address.

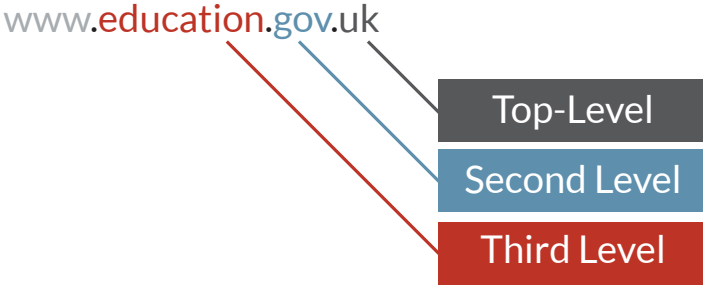
Organization of the domain name system



The domain name system is structured as a hierarchy and can be compared with a plant's root system. The uppermost level is often called the DNS root zone, or just the "root". The so-called "top level domains" represent the uppermost level immediately below the root. There are two types of top level domains. The first are the country codes, such as .no (representing Norway) or .fr (France), and regulations governing these are drawn up at the national level. The second are the generic top level domains such as .com, .org and .net. Regulations governing these domains are stipulated at the global level.

Below the top level domains we find what we most commonly associate with the term "domain names", (second-level domains) such as uio.no for the University of Oslo. Some top level domains also have their own so-called "second-level category domains" at this level. These domains are set up for specific groups, such as example.gov.uk – the "gov" refers to a category under the .uk top level domain specifically dedicated to government departments within the United Kingdom.



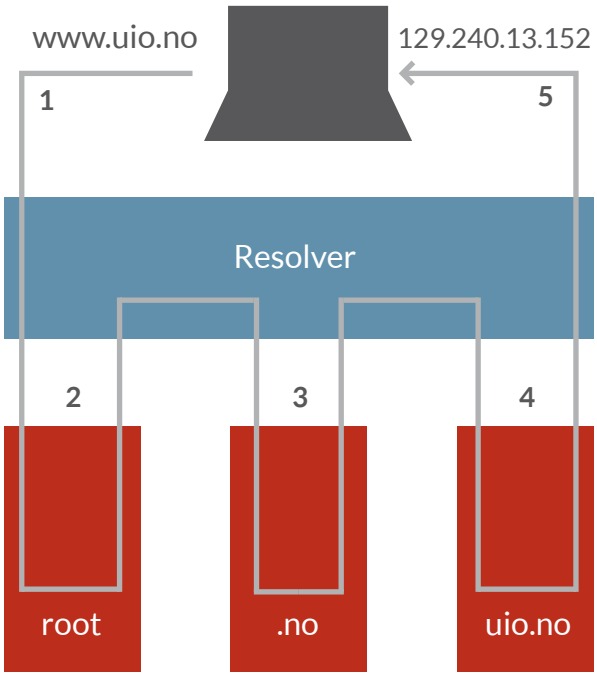


The root structure also reflects the levels of responsibility linked to the domain name system. Separate organizations have responsibility for the different levels. The Registry administers the regulations and operates the central database for each individual top level domain. Eg. the organization DENIC administer the German .de top level domain and NORID administers the Norwegian .no top level domain.

What happens when a domain name is looked up?

Name server: A computer which responds to enquiries regarding addresses registered within a domain name, such as "What is the IP address for www.uio.no?"

Each domain name is linked to a series of computers which respond to enquiries regarding addresses registered within the domain name. These computers are called name servers. For the most part, the user is unaware of communication with these computers.
An example of a typical enquiry: You want to look up a specific event posted on the University of Oslo's website. You know that the university's address is www.uio.no, so you enter this in your browser's address field.



1. A small software application in your computer contacts a separate computer – a so-called "recursive resolver" – which has been set up to process enquiries made to the domain name system. This computer is usually located on the premises of the Internet Service Provider (ISP).

2. The job of the recursive resolver is to find the IP address for www.uio.no. It sends the enquiry onwards to one of the name servers for the root in the domain name system. The root name servers recognize only the level below them in the hierarchy and so send back a list of the name servers for .no.

3. The resolver then re-sends the enquiry to one of the name servers for .no. These also recognize only the level immediately below them, and so send back a list of the name servers for uio.no.
4. The resolver repeats the enquiry to one of the name servers for uio.no, which responds with the IP address for www.uio.no.

5. The resolver then sends the IP address to your computer. When your browser receives the address, it can then contact the university's web server and download the website you want.

04 WHEN A CONFLICT ARISES

For services provided within domains and website content, national and European law applies in the normal way. The holder bears the full and sole liability for use of the domain. It is the holder who determines whether services shall be linked to the domain and which services he intends to offer. These may be services which he chooses to provide himself within his own organization and on his own computers, or he may purchase products offered by an ISP or other service providers. The services can vary in terms of content – from static websites to websites containing files for download, online games, portals, and a wide variety of other services. Two types of conflict involving domain names can arise: The first are those in which the domain name itself constitutes the focus of the dispute. The second are those in which the domain name is involved because it leads to content which becomes the subject of dispute. Under normal circumstances, a registry is not a party to these conflicts. Nor does it need to be in order to be able to take the necessary steps.

Conflicts regarding the domain name. For the most part, such conflicts concern civil law cases involving disputes over user rights to the domain in question. In theory it is also possible to imagine cases where one party argues that a domain name is in itself slanderous or illegal.

Conflicts regarding content and services. In the event of infringement of the law and unwanted activity on the Internet, it is usually the services and not the domain name which constitute the problem. Both websites and email may contain illegal content, or be used for illegal purposes such as attempts to commit fraud. Such conflicts often result in criminal proceedings in which the prosecuting authorities argue for the shutting down of a given content or service. It may also be the case that other parties, from either the private or public sector, may wish to shut down the content on a given website.

Domain name conflicts – measures

Disputes concerning rights to domain names can dealt with via an 'Alternative Dispute Resolution' process (ADR). ADR acts as a fast and economical alternative to the court system in cases of obvious conflict. Most Registries have some form of ADR procedure which can determine if a domain name should be transferred or if it should be deleted. If ADR is not sufficient, both parties are entitled to bring the dispute before the court at a later date.

Conflicts concerning content or services – measures

Removing the content or the service

The only effective means of making an illegal service entirely inaccessible without any negative impact on other parties, is to shut down the service. This can only be achieved locally on the computers on which the service is provided. This is the reason why the most effective approach in all cases is either to take steps focused directly against the domain holder or to contact the service provider.

Measures against the holder. The natural starting point in a conflict concerning content or services on the Internet is with the holder. Some conflicts are resolved by the holder voluntarily removing content or shutting down the disputed services.

If you are unsuccessful using this approach, legal proceedings represent an alternative means of instructing the holder to shut down the services in question.

Contact the service provider. If it is not possible to contact the holder, the next step is to contact the service provider. In many cases this will be the Internet Service Provider (ISP).

The majority of European ISPs have guidelines on how to prevent their clients from abusing the service provider's resources. Each individual provider makes an assessment on a case-by-case basis as to whether the contract with his client or specific legislation provide him with an opportunity to shut down a service himself, or if he requires a legal decision in order to sanction his client.

Deleting the domain name linked to the content or service

If approaches to the holder and service provider are unsuccessful, for instance if the service is operated by an overseas provider, deletion of the domain name may represent a last resort. The deletion of a domain name will not remove the service, but it may reduce the harmful effects it causes since the service will become less accessible.

In some instances it is not possible to contact either the holder or the service provider. In such cases, the registry for the top level domain in question can be contacted regarding deletion. The various top level domains operate with different requirements as to which criteria must be met in order to delete a domain name.

What happens when a domain name is deleted?

Deletion results in removal of the domain name from the domain name system. This means that you can no longer obtain the IP address for the service you have asked for when you look up the domain. Instead you receive an error notification telling you that the domain cannot be found. Deletion affects all services within the domain and all its sub-domains. However, this does not remove the content. The service is still available, but it will be considerably harder to access as the majority of Internet users are not aware of the IP address.

Let us look at an example. A student has published illegal content on a web page belonging to his university. The registry does not have access to delete the web page, the student's user space nor an individual sub-domain. The only option for the registry is to delete the domain name of the university, (eg university.XY). The consequences of a deletion of this kind will be as follows:

- All email addresses and web pages registered within the domain will cease to function. This will affect hundreds or thousands of email addresses and a large number of web pages.
- All name server computers within the domain will become inaccessible. This may affect other domains belonging to the other departments of the university. Furthermore, it may affect domains belonging to other organizations which use the university's name servers for their own domains. For example, a museum or library which is linked to the university but

has its own domain name, if this name relies on name servers within the domain of the university it will thus cease to function and as a result
- All other services within the domain will become inaccessible. This may have negative spin-offs for services provided outside the domain. For example external sites that rely on the domain for links or automated data harvesting tools.
- All sub-domains will become inaccessible. The University has several sub-domains, such as those linked to the various faculties,. All these, together with their email addresses, websites and other services, will cease to function.

The problem is that only the domain holder himself can know how many email addresses, web pages and other services are located within a domain. However, more detailed investigation of the holder's activities might let an investigator estimate the likelihood of innocent third parties also gaining access to services linked to the domain.

Furthermore, there are several ways of reaching a service via the IP address. A simple approach is to set up a link directly to an IP address without going via the domain name system. Methods such as this are used by those who send junk mail (spam). It is also possible to set up several domain names pointing to the same service – for example within various top level domains. If one domain name is deleted, the others can be utilized for lookups the normal way. This means that even if a particular domain name is deleted, the illegal content may still be accessible via alternative names a .com domain, for example.

05 SUSPENSION OR DELETION OF A DOMAIN NAME

Domain registries carry out a number of operations on domain names as part of their daily tasks. These include:
- Update of contact information
- Modification of name servers
- Domain transfer to a new registrar
- Suspension of a domain
- Domain transfer to a new holder
- Deletion of a domain

It is a precondition in the event of transfer that the new holder complies with the terms and conditions set out in the regulations.

It is important to understand the different between Suspension and Deletion of a domain name.

Suspension: The domain ceases to function, but remains registered by the holder.

Deletion: The domain is removed from the database. Normally it will immediately become available to other applicants.

Voluntary measures

A domain holder may request voluntarily that all of the aforementioned operations be implemented on his domain name. This provides a rapid and effective means of conflict resolution in cases where the parties are in agreement.

Mandatory measures

Mandatory measures that can be imposed on a holder may be either temporary or permanent. In the case of a temporary measure, the subscription will not be terminated, but the holder's user privileges to the domain will be strictly limited. The result of a permanent measure is that the holder loses his domain.

In most countries a written court order is required that enables the registry to implement mandatory measures on a holder.

Temporary measures:

- Suspend the domain until the conflict is resolved.
- Impose limits on the holder's rights to use the domain, for example by prohibiting deletion, transfer or other modifications before the conflict is resolved.
- Direct the subscriber to carry out operations on the domain, such as redirecting it to new name servers over which the opponent has control. Such actions may be relevant in criminal cases when the police may wish to assume charge of the technical function of the domain in order to conduct further investigations.

Note that an attempt to prohibit a change of registrar or name server will be more problematic. Both the registrar and the

provider of the name service may be third parties, not involved in the conflict, with legitimate reasons to terminate the holder's client accounts.
To hold a domain name is regarded as a subscription, and an annual renewal fee is charged. The majority of registries will automatically delete domain names if the renewal fee is not paid. When a domain is suspended or if deletion is prohibited, it must decided at the same time whether the holder or the opponent will be required to pay the renewal fee if payment is due during the conflict resolution process.

Permanent measures:

- Domain transfer to a new holder
- Deletion of a domain

It is important to note that the deletion of a domain does not prevent the holder from re-registering the same name. The automatic registration systems does not enable banning of individual applicants from registering specific domain names. A new deletion requires a new legal decision unless the first decision expressly deprives the holder of all rights to utilize the domain in the future. In such cases, the opponent may contact us and request a new deletion by making reference to the original decision.

Mandatory measures in civil cases

The court can process domain-related conflicts in the same way as other conflicts even if the case in question has previously been brought before an ADR process. Temporary measures will typically be in the form of temporary injunctions, while permanent measures will be handed down as part of a legal judgement.
In cases where a legally binding decision has been made, the domain name policy provides the authority to either transfer or delete a domain name, or to carry out other operations without the holder's consent.

Mandatory measures in criminal cases

In criminal cases and depending on the national law and practices a court can order to confiscate a domain name. Since the holder does not own the domain, but merely subscribes to it, withdrawal of a domain name will in practice function in a different way than if it had applied to property. The domain has been employed as a "telephone number" to gain access to an illegal service but is not in itself illegal. In the same way as for a telephone number it is thus the right to use the domain that is withdrawn, not the domain itself. The domain is deleted and remains part of domain resource administered by the registry.

This brochure is based on a concept created by UNINETT Norid AS, the .no registry

CENTR vzw/asbl
Belliardstraat 20
1040 Brussels
Belgium
Tel +32 2 627 5550
Fax +32 2 627 5559
secretariat@centr.org
http://www.centr.org