

DNS-News.fr

**Le Club Noms
de domaine**
<http://www.club-nd.fr>

Loïc Damilaville
loic@dns-news.fr

White paper on Domain names management

2007 Edition

CONTENTS

- 1) Why write a “white paper” on domain names management?
- 2) What is a domain name?

- 3) Defining a domain name strategy
- 4) Information to be provided when registering a domain name
- 5) Principles of management and usage

- 6) Participants
- 7) Principles of organising participants
- 8) The 10 duties of the “Domain names manager”

- 9) Legal aspects – prior rights and disputes

- 10) Major trends

CONCLUSION

ANNEX I: Glossary

ANNEX II: Organisations sponsoring the White Paper

ANNEX III: Introduction to the author

This White Paper has been translated from French by LINGUAFORCE (<http://www.LINGUAFORCE.com>)

1) Why write a “white paper” on domain name management?

The aim of this document is to introduce, as briefly and clearly as possible, the salient points of what needs to be known about managing domain names. It will help the reader to determine the main issues to consider, whether he or she is directly responsible for, or merely involved in, managing domain names for a company or other organisation.

Registering a domain name creates a legal responsibility and requires certain concepts to be fully understood in order to be used appropriately. Yet domain names are now found in every facet of the internet’s *modus operandi*. It has become impossible for any organisation that wishes to have web presence not to have domain names relating to its name, brands or trademarks.

Presence, identification, and existence are three strategic objectives that are met effectively by domain names, as long as the approach adopted forms part of a well thought out strategy and as long as some simple rules are observed. Managed somewhat haphazardly for a long time, domain names are now the focus of a rapidly growing professionalism in the field, both in terms of how they are viewed and in the skills of the individuals who have to manage them.

Published in 2002 in order to enable the individuals concerned to become initiated with or find out more about these issues, this report now aspires to support that professionalism without, however, giving up on its initial purpose.

This third edition is therefore significantly longer than previous editions, although concision and durability remain the intention. The additions complete and clarify what was already in the report, without undermining it. We have in particular expanded those sections dealing with domain name strategies, the questions to ask oneself when registering a name, the duties of domain name managers and the main current trends.

We have decided that this document should remain free of charge, sharing the philosophy of the internet itself, as a mechanism for mutual benefit and sharing of knowledge. We ask only that those wishing to use the content of this report do not “forget” to quote their source and the author’s contact details, which has unfortunately happened on several occasions since 2002. Although made freely available to all, the content remains protected by intellectual copyright and, of course, by “netiquette”.

If you have found this white paper helpful, you are requested to circulate it unaltered. Feel free to contact Loïc Damilaville (loic@dns-news.fr) with any questions regarding the distribution of this report or matters relating to domain name and web presence issues.

The following organisations have sponsored the production of this document and we would like to thank them warmly for their renewed trust:

*The French association of e-commerce and online services, **ACSEL** (Association pour le commerce et les services en ligne); the French domain names registry, **AFNIC** (Association Française pour le Nommage Internet en Coopération); the French business start-up agency, **APCE** (Agence Pour la Création d’Entreprise); the French association of practitioners of trademark and design law, **APRAM** (Association française des Praticiens du droit des Marques et des Modèles); the Paris chamber of commerce and industry, **CCIP** (Chambre de Commerce et d’Industrie de Paris); the French research and training centre for technical assistants working in retail, services and tourism, **CEFAC** (Centre d’Etudes et de Formation des Assistants techniques du Commerce, des services et du tourisme); the French association of major IT users, **CIGREF** (Club Informatique des Grandes Entreprises Françaises); the French digital economy club, **Club de l’économie numérique**; the French industrial property agency, **INPI** (Institut National de la Propriété industrielle); **ISOC France**; the French employers’ federation, **MEDEF** (Mouvement des Entreprises de France); the French **Ministry of Economy, Finance and Employment**, and the French anti-counterfeiting body, **Union des Fabricants**.*

Their details and logos are shown in Appendix II.

2) What is a domain name?

A domain name is a string of alphanumeric characters (A to Z, 0 to 9 and the hyphen) made up of the main body of the name plus a Top-level domain (TLD) separated by a dot. This string is the essential element of any internet address. The domain name is used not only to identify a web site and to route traffic to it, but also to provide “personalised” electronic mail addresses.

E.g.: “dns-news.fr” is the domain name element in the address <http://www.dns-news.fr>

E.g.: john.doe@dns-news.fr is the electronic mail address for John Doe, identifying him as a member of DNS News staff.

The benefit of these “personalised” email addresses will be noted, indicating as they do both the individual’s belonging to some organisation and, implicitly, the address of that organisation’s website.

Once registered, a domain name may or may not be used. If it is active, it will be linked to an “IP address”, which is a sequence of several series of figures (e.g. “123.250.45.76”) identifying the machine hosting the website on the internet. It is this technical link which enables access to web pages after a domain name is entered in a browser’s input field. A similar system makes electronic mail addressing work.

Top-level domains (“TLDs”)

To the right of the main body of the name and the “.” is found the Top-Level Domain, such as .com, .fr, .eu, etc.

TLDs are split into two main categories:

- **“generic” TLDs** (also known as gTLDs for generic Top-Level Domains), which are not associated with a particular territory, but rather a specific meaning or community. The com, net, org, info and biz are the best-known generic TLDs, but there is also .mobi (content adapted for mobile telephones), .museum (reserved for museums), .aero (reserved for the aeronautics community), etc. At this time, there are some fifteen generic TLDs and new ones appear almost every year.
- **“geographical” TLDs** (also known as ccTLDs for country code Top-Level Domains) which match up with a defined territory or country – fr for France, de for Germany, jp for Japan, and so on. There are some 250 of these TLDs.

Registries and internet name policies

Each TLD is managed by a “registry”. Registries usually have three key duties, namely to ensure the technical operation of the TLD, to manage the database of registered names and related data, and to lay down the rules for allocating and administrating domain names within the TLD.

These rules are usually referred to as the “internet name policy”. Policies vary widely from one TLD to another, depending on the registry’s philosophy, the maturity of the market and any restrictions that may be imposed by local legislation or the government.

Diversity of these policies is a complicating factor for applicants registering domain names in more than one TLD. However, some specialized service providers (the “registrars”) typically provide a one-stop service and fully understand all the terms and conditions to be complied with in order to obtain such-and-such a TLD.

3) Defining a domain name strategy

The term “domain name strategy” is used to describe the way a company ascribes itself a “common core” enabling it to assess the benefit to the company in registering a domain name and/or in retaining those it has already registered.

The methodology for drawing up a domain name strategy was discussed in an article published in collaboration with lawyer Etienne Wéry, and fairly completely in the book “*Stratégies de nommage*” (“Domain name strategies”) published in collaboration with Patrick Hauss. We give a brief summary here of the main points expounded in the first part of the book, the second part concentrating on surveillance policies for terms unprotected as domain names. Please feel free to contact Loïc Damilaville (loic@dns-news.fr) if you would like a copy of the book, subject to availability.

Identifying and evaluating the company's requirements

The basics of the methodology are straightforward. It firstly consists of identifying the requirements of the business to answer the question “What do we need to register or keep?” The following aspects in particular can form the basis of the identification phase:

- **Business lines and sectors:** make a list of the business lines and sectors in which the company and its subsidiaries are involved, and evaluate them to the extent this is possible with regard to their position in the lifecycle (emergence, maturity, decline) and the issues relating to the company's web presence.
- **Presence points:** list the countries or geographical areas, the type of presence, and strategic issues relating to that presence.
- **Trade names, brand names and registered trademarks:** list the trade names, brand names and registered trademarks, stating the geographical coverage, classes (for trademarks), the phase in the operational cycle, their renown, how and where they are used, the level of advertising investment extended towards them, and if possible, the share of revenue that each represents (overall and for each geographical area).

This comparison table naturally forms a very fine sieve, which few companies use in its entirety. At the end of this stage, the company must be able to determine which “markets” are the most important to it as regards internet domain names, a “market” being defined by the business line + country + trademark combination. The company has also managed to define a number of priorities and “markers” for the future scope of its domain names.

Defining the theoretical naming scope

Once the requirements have been identified and evaluated, listing the actual domain names themselves remains. This too involves a close look at three aspects:

- **the words** the company wants or needs to use when registering domain names, i.e. generic terms describing the company's businesses, in the various languages used in the countries where the company operates, key words or trademarks that usually form the basis of the company's promotion, variants of these words permitted by the naming system's syntax, and “obvious” variants resulting from spelling mistakes or typos.
- **the TLDs** under which these names are to be registered, be they strategic (corresponding to important “markets” for the company), well-known or highly intuitive (.com, a local TLD), “risky”, or “speculative”.
- **the character strings** to be used for registering the names – transcriptions into natural language, and the most obvious variants.

Defining the operational naming scope

The last step is to wrap up the exercise with a third stage, also broken down into three aspects:

- **list the domain names that are already, or will be, used in corporate communication of all kinds** (“Communication scope”). Such names are particularly strategic.
- **list the “markets” that need the most protection** (“Security scope”), i.e. key business activities in strategic countries focusing on current or future flagship trademarks.
- **cross-match the “desired” registrations with the constraints specific to each TLD** (local presence, administrative contact who can speak the language, etc.).

It may be helpful to point out that this exercise is iterative, the result of continuous adaptation of the name portfolio to fit requirements and a constantly changing environment. The most important aspect is probably less to “put the issue to bed” than to avail oneself of a means to evaluate what is right and what is not. This approach plays a key role in domain name-related risk management.

Manage risks that cannot be eliminated

Domain names are a constantly shifting world – rules become more flexible, new TLDs emerge every year, and with the introduction of IDNs (domain names in non-Latin character sets or accented Latin characters) a third dimension is added to the two that already needed to be considered (i.e. which names with which TLDs). In this situation, risk management in the elimination sense is a virtually unattainable objective, and out of most organisations’ reach for cost reasons.

If the risk cannot be eliminated, it therefore becomes important to learn how to manage it:

- **by determining what is, and what is not, important to the company**, following the exercise to identify communication and security requirements and scope. Within the scope, the company will not fail to register any “obvious” domain name.
- **by setting up automated surveillance** intended to warn the company whenever a third party registers a domain name identical or similar to the names being watched for. This system allows becoming ensnared in a spiral of pointless name registrations to be avoided, while affording protection against third party attacks. Such protection is imperfect, operating as it always does after the event, but the fact that this information is held when the nuisance arises allows a rapid response, and any counter-measures that may be needed to be taken within reasonable timeframes.

The instigation of counter-measures is always preceded by a damage assessment phase. Not all potentially contentious names harm the company’s image in the same way. Sometimes, they are too close to a trademark to be tolerated; sometimes they may only cause harm if they are actually used for certain purposes (to route to a competitor website, a fraudster or a harmful website).

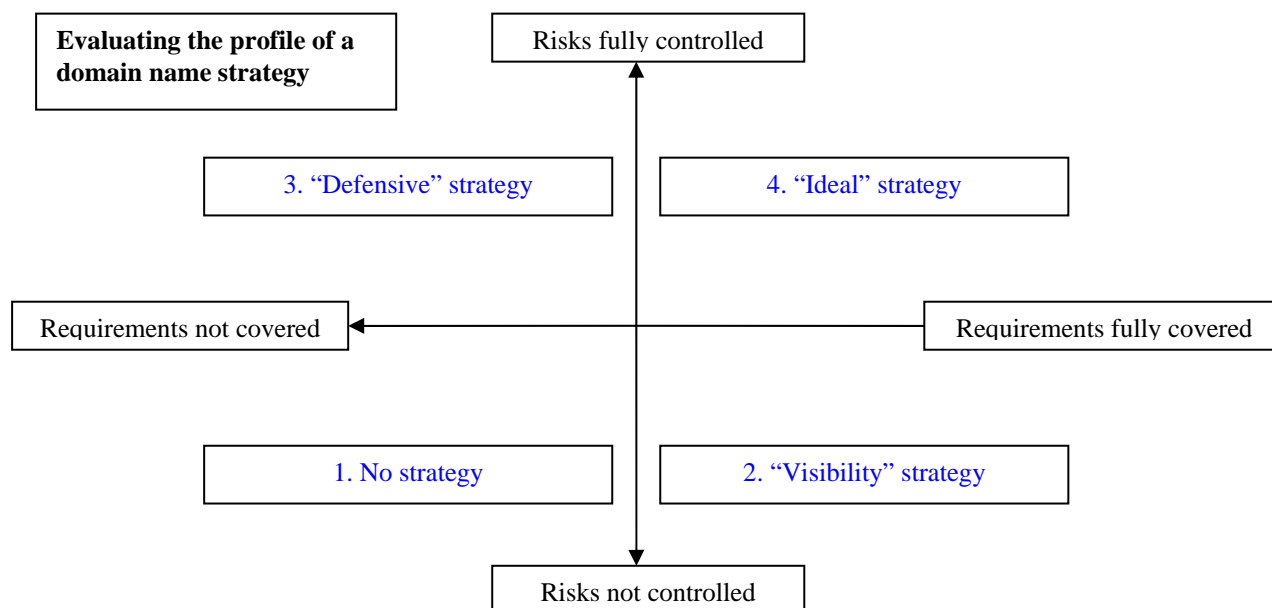
The degree of nuisance perceived by the company thus determines the amount that it is willing to pay to neutralise the contentious name. In 80% of cases, a company will let the name live on, but it may then be useful to check up regularly on the use to which the third party is putting it.

A full domain name strategy therefore usually includes the following two main aspects as regards domain names:

- **the quest for VISIBILITY**, finding an optimal fit between the company’s requirements and its domain name portfolio
- **the quest for PROTECTION**, this being broken down into defensive name registrations and name surveillance.

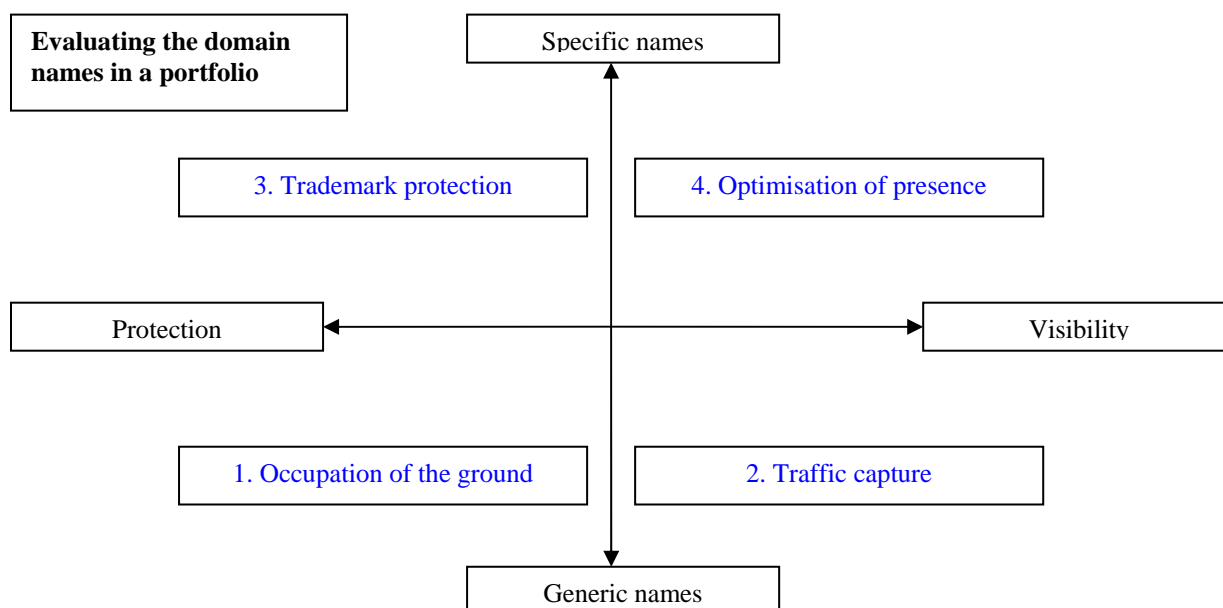
The diagram on the next page, used to evaluate the profile of a domain name strategy, is the outcome of such a philosophy.

Evaluating the profile of a domain name strategy



The second diagram is a domain name portfolio analysis chart, aimed at answering the question “Why have we registered this name and why are we retaining it?” As a general rule, companies register domain names in order to optimise their web presence (specific names / trademarks registered with a view to visibility) or to protect their trademarks against third parties (specific names / trademarks registered with a view to protection). The other two aspects, and particularly capturing traffic, still remain greatly underused.

Evaluating the composition of a domain name portfolio



It can be observed that defining a domain name strategy:

- **needs to be designed globally**, and based on thorough knowledge of the company's businesses, its plans, its brand portfolio, and so on
- **requires the involvement of various participants** who are organised to focus on a well-defined view of requirements, which can only be obtained through a degree of centralisation
- **is pointless unless it is designed from the outset as flexible, adaptable and to be carried over into the long term.** The requirements from 1998 are not necessarily those for 2007, and they will apply still less in 2016.

4) Information to be provided when registering a domain name

There are three major kinds of information to be supplied when registering a domain name, these applying, with some variation, to all TLDs.

The identity of the various contacts

These being:

- **the domain name holder, also known as the registrant.** This is the entity or individual legally holding the name, and therefore holding the highest level of authority over it. Depending on the country, the registrant is deemed to be the "owner" of the name (United States) or merely a holder who has simple usage rights over it (France). Under all jurisdictions, however, it is essential that the instructing party is itself the holder of the domain name it wished to register. Registrations carried out using the name of a service provider or a company employee as the holder, even in good faith, are to be avoided or rectified.
- **the administrative contact:** plays a key role, in particular by validating any changes made to the data concerning the domain names for which he or she is the contact, for example by approving a change to the service provider. For these reasons, it is important that this contact is under the management of the instructing party and not a service provider. It is however necessary for the contact's manager to be genuinely involved in domain name issues. An individual too highly placed in the hierarchy will know nothing about the issues and/or not be easy to "galvanise" if needed. Administrative contacts must nonetheless hold decision-making authority as regards managing the names under their responsibility.
- **the billing contact:** often the same individual as the administrative contact, which simplifies matters, but this role can also be delegated to some other unit in the company (accounts department) or to a service provider assigned with managing renewals on the company's behalf. This last solution is the simplest, but requires the use of a particularly reliable service provider.
- **the technical contact:** this contact should preferably be reserved for the service provider responsible for administration of the name servers on which the domain names are installed. Should the company have its own name servers, the technical contact is to be the individual or unit directly responsible for running the servers.

The contact details for the various contacts

The contact details must be useable and permanent.

- **Useable**, meaning functional. For example, there is little use in giving the address of the company's Paris head office if the administrative contact works in an office in Toulouse (there is every chance that mail will never be received unless the actual person name is on the envelope).

- **Permanent**, to avoid tedious updates. To give a practical example, if the administrative contact changes email address, all records will have to be updated (which is rarely done in a global and systematic way, with potentially serious consequences which could go so far as deletion of the domain name if a “sensitive” email goes astray).

The contact details requested are typically:

- the contact’s **name**: which by definition is not permanent, as people change jobs, but it is often required. Updating it must be envisaged if the individual changes, although this is not crucial if the electronic mail address aspect is handled correctly. When possible, encourage use of a “generic” name such as “DNS Admin” or “Domain Names Management”.
- **email address**: it is absolutely essential that this is “generic”, i.e. in the form “dns.admin@dns-news.fr” rather than personal such as “jean.dupont@dns-news.fr”. In this way, if the contact changes jobs or leaves the company, records will not need to be updated.

NOTE: email addresses recorded for contacts must work permanently, and the recipients of email sent to them must react promptly when messages are received regarding names under their responsibility. If one individual leaves, ensure that the email address used was not one of the recorded contact points before disabling it.

- **postal address**: the company’s registered office offers a guarantee of permanence, but it is preferable to use the premises where the contact (administrative, billing or technical) person works so that any mail sent has a reasonable chance of reaching the addressee internally. In the event of a move or a change, make plans to update all records concerned or, at least, to forward mail to the new recipient.
- **telephone number**: ideally, use the switchboard number of the company or the premises where the contact is based. This avoids contacts becoming the victim of marketing “harassment” on their direct lines, while keeping a degree of flexibility in the event of changes. Updates should be planned in the event of a change of number or a move.

Name servers

Name servers are machines on which data about the domain name will be held in order for it to work. Most registration offices offer their own name servers as a default option, which is the simplest solution. Conversely, if the name servers are managed directly by the company itself, the individual or the entity registering the name must know the server address before starting the registration procedure. These machines are generally identified by a name (e.g. “nsl.xxx.fr”) and an IP address (e.g. “145.214.12.33”).

In some countries, the servers must be configured before the name is registered, with the registry managing the local TLD undertaking some automatic technical checks before allocating the name requested. This is the case in France.

It is not essential that the DNS servers used for names pointing to a website are those of the hosting service provider for that site. This requirement, which is stipulated by some hosting service providers, is primarily intended to simplify technical management of the arrangement, by allowing them to alter hosting configurations without needing to involve another service provider or their client. This precaution can also avoid their “overlooking” a domain name of which they would be unaware and which would continue for example to point towards an obsolete IP address.

It is important to ensure that the two or three name servers on which a domain name is installed are not all located on the same network. If this is the case, a failure on this one network could prevent the domain name from working properly, whereas if the servers are located on different networks, the risk of total failure is clearly much lower.

5) Principles of management and usage

Management

Managing a domain name is straightforward as long as some basic rules are observed:

- **contacts and their contact details must be up-to-date, permanent and operational** (e-mail addresses are essential, and postal addresses are sometimes important in the event of a dispute, as is the identity of the “registrant”, the legal holder of the name). Keeping the administrative side up-to-date is generally neglected, which correspondingly undermines the portfolio by increasing the risk of procedural breakdown (lost or unread emails, etc.). It requires, in the event of subcontracting to a service provider, that they are kept reasonably informed of amendments to be made (moves, changes in contact details, etc.). However, where the portfolio is a large one, and in particular for local TLDs with little automation, these updates are often costly and relatively time-consuming.
- **the individuals recorded as administrative contacts must genuinely be responsible for the company’s domain names**, understand the issues and be able to respond to a given situation. Ideally, these individuals will be authorised to take decisions themselves.
- **financial management** is the most difficult area, especially where the portfolio includes dozens of names in various countries. In many cases, renewal procedures are decentralised and entrusted to subsidiaries (but here too, a minimum level of supervision on the part of the individual responsible for domain names is needed, since the risk attached to omissions and non-renewal of critical domain names is exponential). In other cases, a specialist service provider looks after all such procedures, which simplifies matters considerably but is also more expensive. Generally speaking, it is appropriate to avoid having renewal invoices (which are often dispatched automatically) sent directly to purchasing or accounts departments, the danger being that they will not know what the bill is for or that they will pay after the renewal deadline. When in-house management is the chosen solution, bills ideally should be sent to the administrative contact or to the individual coordinating domain name issues, for approval and subsequent forwarding to accounts departments.

The establishment of a schedule which can be used to anticipate and track renewal procedures over time and to determine the overall annual renewal budget is strongly advised. Domain names are typically renewed on an annual basis. In certain cases, they are initially registered for more than one year and may then be renewed for variable terms. Renewals for terms in excess of five years are not advisable, as the field of domain names and naming policies changes very quickly. Where the renewal term is longer than one year, it is advisable to check that the TLD registry allows this practice and that the official expiry date is in actual fact in X years’ time. The fact that a service provider has been paid for several years in advance without this being made official in the registry database could create subsequent problems, if the service provider folds or if the company wishes to switch provider.

- **technical management** is often outsourced to a service provider, except for those large companies having the skills available in-house. Continuous checking is needed that information is being properly passed on to the selected provider and within a reasonable time, taking account of constraints such as propagation (the time needed for the name servers across the network to take on the amended data). In cases where management is decentralised and outsourced to more than one service provider, the domain name manager needs to play a coordinating role and ensure that those involved are communicating with each other.

Usage

There are several types of domain name usage:

- **domain name reserved but not used:** the name is registered but is not installed on any DNS and is therefore not “used” for anything. It points to no website and “supports” no e-mail addresses. This is the case with many names that are registered “defensively”, to prevent a third party from acquiring them.

- **routing to a holding page:** the name is registered and installed on DNS servers. It is enabled and routes visitors to a holding page by default. A large number of names registered for strictly defensive purposes fall into this category.
- **name pointing to no site but used as support for e-mail addresses:** this case should notably be borne in mind by domain name managers at companies facing instances of cyber squatting. Just because a contentious name does not route to any site does not mean that a “fraudster” has not enabled e-mail addresses using the domain name, which would enable the hacker to capture e-mail, confidential or otherwise, sent to the company which should be the legitimate holder. This can be checked using the free technical tools made available to all by the registry for France, AFNIC, which work irrespective of the domain name TLD (see <http://www.nic.fr/zonecheck/>).
- **name pointing to a site but not used as support for e-mail addresses:** the majority of domain names actually used are in this category. Such names may point by default to the company’s main website, or websites for subsidiaries in the country matching the local TLD, or specific websites dedicated to a trademark or product.
- **name pointing to a site and used as support for e-mail addresses:** these names are of particular strategic interest and the company must handle them carefully, as they are a “bottleneck” in the company’s web presence arrangements. Any lengthy failure will make the site unavailable and will prevent those working in the company from communicating with the outside world. There is no “room for error” as regards these names.

“Optimum” usage of a name consists of making sure that it is profitable, both in terms of visibility and trademark protection. This is why “defensive” domain name activation must be recommended, insofar as such names may be viewed as intuitive by a proportion of Internet users (with a hyphen, without a hyphen, singular or plural, and some obvious variations in spelling, etc.). Should there be any doubts about the issue, these ought to be dispelled considering the prosperity of some “typo-squatters”, making money from domain names registered improperly by “parking”. Not all typo-squatter domain names are goldmines, but taken as a whole they undeniably divert traffic the value of which should not be disregarded.

Active names should preferably point towards sites to which they bring some meaning or value. Pointing an .it (Italian) domain name to the company’s corporate website instead of towards a website for the Italian subsidiary means potential loss of earnings for that subsidiary, with the risk of seeing Italian-speaking Internet users leaving the corporate website to look elsewhere. Having active names pointing to websites also improves positioning in search engines, although this is just one aspect out of many.

It is important to note that the use made of domain names can shift over time without the holders’ knowledge, for a wide variety of reasons. Names that are not renewed in time become disabled (“on hold” status); sometimes these alterations are due to the service providers hosting the DNS servers or website servers causing unexpected redirections, unless the DNS servers have been attacked by “hackers” who are then able to use the domain names as they see fit. Regular monitoring of the most strategic domain names is important in order to be able to attend to any eventuality.

Lastly, domain name usage needs to be organised as a flexible system operating over the long term. A name may be registered for a one-off event, and then abandoned. Conversely, names registered defensively and not used may suddenly become valuable in the event of a strategic reorientation or the launch of a new product. Domain names must be viewed as company assets, and be treated with the same care as its trademark portfolio. We will return to this point in the “Major trends” section.

6) Participants

By virtue of their nature, which combines technical, administrative, legal and marketing/communication aspects, domain name issues should, ideally, be handled by a steering committee bringing together these various skill sets, even if day-to-day management is dealt with by just one department or individual. Companies are increasingly adopting this approach, which provides a global view of the issues and the solutions that may be brought to bear.

Potential participants may be identified in three main ways:

- **by skill set:** administrative and accounting skills need to be galvanised for name management, and technical skills will be needed if the DNS servers belong to the company. But beforehand, individuals involved in strategy definition (anticipated mergers or acquisitions, penetration into new markets) and marketing policy (new product launches, etc.) also need to contribute. Communication department staff could advantageously help to determine which names are essential in order to support web aspects of the company's overall communication policy, and how to optimise its "presence" and Internet identity. Lastly, some input from lawyers specialising in intellectual property is inevitable, in particular during disputes with third parties, and also to maintain some consistency between developments in the trademark portfolio and changes to the domain name portfolio.
- **by subsidiaries, divisions, business lines:** the breakdown of participants will vary depending on the company and internal organisation. The overriding idea here is that "collective" management of domain names involves regular contributions from the various subsidiaries, divisions or business lines in the company in order to create and maintain a perpetual flow of information between them and the parent company, which is often the only entity to have an overall view of the issue, but which sometimes lacks information regarding the practical needs of company units.
- **by country or geographical area:** depending on the company's organisation, a foreign "subsidiary" could oversee all activity in a given country, or conversely focus on one precise product/market. The geographical aspect of domain name management must not therefore automatically be combined with the "market" aspect. It is important (in particular as regards management of domain names registered under local TLDs) that local participants are involved in managing the portfolio.

The domain name management arrangements could therefore form a matrix with three "inputs" - varying of course according to the size of the company and its actual needs. Although it may be complicated, in reality it proves fairly straightforward to implement and supervise as long as the participants have the same level of information and awareness. Work is therefore required on the organisation of the network and the flow of information, and this is where the individual and/or team responsible for naming issues has a particular role to play.

7) Principles of organising participants

Describing the various skill sets needed for optimum management of a domain name policy has highlighted several aspects:

- **many skills are required** and they intersect in a matrix-like manner
- **in small and medium-sized companies**, where the number of names to be registered and managed is not great, it is pointless to create a "permanent" network, it is however **advisable to identify the resources to be called upon when needed**
- **in larger organisations**, endowed with well-known trademarks, business units abroad, and working on several markets, the **network needs to operate on a regular basis** and must be able to be coordinated by a single individual (or if appropriate by a small team). The "representatives" are often the domain name administrative contacts, especially for local TLDs, even if the contact e-mail is still unique (and generic)
- **the authority invested in this "coordinator" varies depending on the company's internal policy.** In a highly centralised system, the coordinator has wider decision-making authority, and the participants are advisers or "executors", in a highly decentralised system, the coordinator is more of a "facilitator" enabling the various participants to work consistently with each other.

Besides these organisational aspects, it is advisable to think about the coordination between the various participants, which requires:

- **participants to be known**, in terms of their skill sets, the units to which they belong, their willingness and opportunities to devote time to domain name issues
- **participants to be trained**, both in the general aspects of domain name operations and surrounding issues, and in aspects connected to their skills (for example a lawyer will value training in the subtleties of the UDRP (Uniform Dispute Resolution Policy) as an alternative to the courts, etc.). Such training includes regular consultation of information on changes to local procedures and domain name policies, and domain name news (governance, new TLDs), etc. The company must also be alert to the appearance of new tools facilitating domain name management, as well as monitoring new registrations carried out by third parties, etc.
- **a definition of duties and tasks that are to be accomplished** by participants and representatives as regards name portfolio management.
- **operational procedures to be defined** (reporting lines, regular reviews, updates).

Ideally, it is advisable to train two individuals in each unit in domain name-related issues, in order to avoid any disruption in the event that the main representative leaves or is absent. These individuals must be properly identified and take their turn in playing the role of domain name “coordinator” within their units in order for information to circulate properly.

Irrespective of their authority levels, coordinators will always play a role of “input” relative to the representatives of the various units, who will often have a number of other questions to deal with. With the domain name policy’s general consistency with respect to corporate governance, the coordinator’s role is therefore of prime importance in monitoring and dealing with domain name issues in time, and mobilising the network. Domain names are typically not perceived as “strategic” until such time as a major problem arises reminding the company that its Internet presence is largely dependent on them...

8) The 10 duties of the “Domain names manager”

The domain names manager can sometimes turn into a one-man band, as is shown by the diversity of topics addressed in this white paper which is nonetheless intended to be brief.

The aim of this section is to introduce the potential range of activities related to domain name management. The degree to which the role defined by these 10 “duties” is multi-disciplinary will be noted, being in no way limited to technical, legal or administrative aspects. Quite the opposite. The domain name manager should ideally have reasonably thorough knowledge of the company and its development strategy, and be in a position to coordinate an entire network of representatives within the various units. It is therefore a position of some trust, involving a great deal of deliberation and human contact, a role which will gradually come to the fore as its added value is recognised.

- **Duty no. 1: ensure the company’s domain names are used appropriately:** bearing in mind that domain names cost money, it is important to ensure they are used to best meet the company’s needs. Failure in this respect, and non-optimal situations, are far from unusual.
- **Duty no. 2: ensure that the management principles defined in the policy are observed:** it is very important that the management principles laid down for the company’s domain names are observed throughout by everyone involved in domain name issues.
- **Duty no. 3: track alterations to the name portfolio:** a name portfolio is very changeable in nature; the domain name manager must keep it up-to-date in order to continue to remain the official “reference” and to retain a full and accurate picture of what is happening.
- **Duty no. 4: identify the internal participants and select external participants:** this of course involves building relationships with internal units in order to create a “network of representatives”, the corollary of this being the selection of one or more external service providers to which certain tasks will be outsourced.

- **Duty no. 5: approve suggestions made by company units and participants:** as the domain names manager is the “in-house reference”, it is his or her responsibility to ensure that requests from units are consistent with the company’s domain name policy and that there is no conflict between units as regards names which may be of interest to more than one of them. In some cases, approval may extend as far as budgetary control.
- **Duty no. 6: track and coordinate the implementation of measures planned, internally and externally:** as the domain names manager is often the coordinator between various participants, it is his or her responsibility to follow up changes in the portfolio and to ensure the measures taken are done so in an optimised way.
- **Duty no. 7: act as an operational interface between company departments:** the majority of the time, the domain names manager will be the most skilled in operational aspects of domain names. It is the manager’s responsibility to see the right people to push things forward, obtain vital information, or check that a particular measure truly meets a unit’s needs.
- **Duty no. 8: circulate information between all participants:** over and above operational aspects, the domain names manager fulfils a key role in terms of gathering and redistributing information, both internally (identification of requirements which might affect the name portfolio) and externally (surveillance of the environment).
- **Duty no. 9: involvement in drawing up and updating the domain name strategy:** the domain names manager does not always have the authority to change the strategy without endorsement from a cross-departmental steering committee intended to supervise the issue. On the other hand, he or she is naturally the primary recognized adviser as the in-house expert in such matters.
- **Duty no. 10: anticipate the company’s future Internet domain name requirements:** here too, the domain names manager is not necessarily a decision maker, but he or she is often the only individual with a vision based on in-depth knowledge of internal requirements and the external environment. He or she must therefore play the part of a “watchdog” in order to alert units as and when required.

9) Legal aspects – prior rights and disputes

Domain names are key allies in ensuring in a company’s Internet presence, and this strategic nature serves to intensify issues relating to the protection of the company’s identity and distinguishing marks, which are often the target of much nuisance instigated by third parties acting in either good or bad faith.

A new generation of improper practice

The oldest and best-known form of nuisance is cyber squatting, a practice which basically consists of registering a domain name matching a trademark. Until the UDRP was established in 1999 (see below), cyber squatting was generally followed by an attempt to resell the “hacked” domain name to the trademark’s owner for a sum well in excess of the registration cost.

The UDRP enabled an upper limit to be put on the costs of out-of-court settlements by giving legitimate trademark holders the possibility of recovering their domain names within a reasonable period (although there is a “tax” of 1,500 dollars minimum, which remains a significant sum). Squatters reacted accordingly, adopting evasive strategies which have undergone a rapid increase since 2005.

Typo-squatting and parking

Typo-squatting consists of registering names very similar to trademarks, differing by only one or two letters, or using the most intuitive spelling or phonetic variants. The purpose is no longer to sell the name back to the trademark holder but to capture traffic - searches by Internet users who make mistakes when typing the domain name into the browser.

The second step in the procedure is to generate money from this traffic, notably by the use of “parking” the squatted domains, which are then routed to pages of contextual links relating to some topic suggested by the domain name, the “squatter” benefiting from pay-by-click when the stray visitor clicks on one of the contextual links.

This practice became widespread as a result of a provision in the contract between the registrars and ICANN allowing registrars to obtain a full refund on the price of a domain name if they relinquished it within five days. As a result, mass registration of thousands of domain names relinquished within the deadline no longer costs anything, yet parking allows money to be made during the short period from the traffic generated by typo-squatted names, which are relinquished and then reregistered a few minutes later if they are really profitable.

Trademark owners are often powerless in the face of these practices, the simplest solution being of course to register the most obvious variants, to tolerate any nuisance where typo-squatted variants are not strategic, and to initiate the UDRP if they are. This demonstrates the benefit of having a fully-developed strategy beforehand, which can easily determine whether a name is strategic or not.

Slamming

Slamming consists of creating a situation where victims take decisions that they would not have taken had full information been available to them. It generally combines deception and psychological pressure. The three major categories of slamming are:

- **the fake renewal bill:** the domain name holder receives an “expiry notice” explaining that the name must be renewed if it is not to be lost. This is true... but the sender of this notice is neither the registry nor the registration office through which the name was registered. It is another registration office, trying to make its victims believe that they are going to lose their domain name if they do not subscribe to its services.
- **registration blackmail:** this tends to happen over the telephone and at off-peak times - a registration office contacts the holder saying that a third party is intending to use the office to register names similar to the holder’s trademarks. The registration office suggests registering the domains in question on behalf of the holder before the order from the third party can take effect; consent must therefore be given immediately and the prices are usually much higher than market rates.
- **confusion with the national TLD registry:** in this case, the scam is not strictly speaking about the domain name, but the creation of confusion between the third party, calling themselves the “internet registry” for a country, and the registry for the TLD for that country. The “service” on offer is a listing in a directory costing a great deal owing to the expected benefits, the implied message being that this subscription is essential to “be on the Internet”.

In addition to these new types of improper practice, mention could also be made of others, such as “phishing”, based on spoofing a company’s identity in order to capture its customers’ confidential data. “Hackers” have fertile imaginations and countermeasures are difficult to implement once the damage is done. The best protection remains a well-grounded strategy and organisation, enabling the most serious threats to be dealt with, and those people who may fall victim to this kind of attack to be made aware so they know how to respond. Putting monitoring tools in place is the indispensable corollary to such organisation.

Prior rights management

Registering a domain name, usually viewed as easy and “obvious”, can rapidly become a source of legal problems and risks. Taking prior rights into account is especially crucial for this reason.

There are several sorts of prior rights: prior rights of trademarks over domain names, of domain names over other domain names, and domain names over trademarks.

- **prior rights of trademarks over domain names:** in the event of a dispute between the holder of a domain name and the holder of an identical trademark, and if the trademark was registered before the

domain name, experts tend to find in favour of the trademark holder. In his or her defence, the domain name holder can claim ignorance of the existence of the registered trademark matching the domain name, especially if the trademark is not well known and if the holder is located in another country. He or she can also attempt to prove good faith by demonstrating no harm has been caused, and citing the “principle of speciality” - if the trademark was registered in a class entirely unrelated to the domain name holder’s business, the trademark holder’s claim will be weakened as a result.

- **prior rights of domain names over other domain names:** the number of disputes based on this type of prior right (for instance, the holder of a .fr name challenging the holder of a .com name registered afterwards) is still relatively low. However, such prior rights play an essential role in the early stages of a company’s plans. If the .com name for a future product is already registered, it would be better to change the name rather than hope to take over the .com. Here, the issue is more marketing-related than legal.
- **prior rights of domain names over trademarks:** in certain cases, attempts at “reverse cyber squatting” have occurred, with squatters registering a trademark matching a domain name that has become well-known in order to threaten the holder with taking it over. As a domain name is not always viewed as an intellectual property right, it is weaker than the trademark, although restitution will not of course be automatic, especially if the domain name is being used in good faith. Conversely, the holder of a well-known domain name may, if necessary, challenge the registrant of a trademark matching the domain name and registered after it. To avoid any concerns of this nature, a prior rights search on domain names already registered and active that match the future trademark is increasingly necessary.

In most disputes, a company of any size will need to avail itself of legal advisors specialising in this kind of issue, since these questions are quite evolutionary and the legal position changes frequently.

We cannot stress too strongly the need for prior rights searches (trademarks AND domain names) prior to any registration, as this meets two concerns:

- **it avoids disputes with third parties** already using these trademarks and/or domain names
- **it avoids seeing third parties already using these trademarks and/or domain names benefiting from the company’s own promotional efforts** employing very similar terms. That would be accidental “typo-squatting”, but it would work!

Very often, managers under time pressure do not take this stage into consideration, resulting in disputes, a by no means insignificant loss of traffic, and the purchase of domain names *in extremis* for sums which could have been spent elsewhere – on drawing up an official domain name strategy, for example...

Handling disputes

Disputes over domain names began to emerge in 1996-97, and the establishment of the UDRP in 1999 was a defining event. Since then, the nature of disputes has changed (see above) while local TLDs have striven to also set up dispute resolution procedures avoiding the need for rightful holders to have to use legal proceedings. Nowadays viewed as essential mechanisms, other DRPs, like the UDRP itself, have also demonstrated their limitations, having no deterrent effect and usually forced to restrict themselves to repairing damage, being powerless to prevent it.

No major company has been spared from attempted cyber squatting. For SMEs, which are often not the holders of well-known trademarks, cyber squatting is even more serious since the chances of recovering disputed domain names are low.

Distinction is made between three major methods of dispute resolution:

- **amicable (or out of court)**, whereby the name is purchased at a price agreed between the parties. This price typically does not exceed the cost of arbitration or legal proceedings, if the “victim’s” rights are obvious. If these rights cannot be incontestably established, there is no upper limit to the sums involved.

- **the administrative arbitration procedure, known as “UDRP”**. This consists of submitting the dispute to the assessment of experts in intellectual property. They will use three major criteria as the basis for restoring the disputed name to the plaintiff or otherwise:

- **the identity** between the disputed domain name and plaintiff’s name or one of the plaintiff’s trademarks
- **usage** of the domain name for purposes harmful to the plaintiff
- **bad faith** on the part of the current holder (a classic example of bad faith being proof that the holder is prepared to sell the name to the plaintiff).

The best known arbitration centre is in Europe, in Geneva. It was established by the World Intellectual Property Organisation (WIPO). Many local TLDs use the WIPO to handle their dispute resolution procedures, but not all. Hence, the procedure for the .eu TLD (European Union) is handled by a Czech body.

The cost of administrative procedures varies with the centre and the country. By way of a benchmark, a UDRP procedure with WIPO involving one expert costs 1,500 US dollars, to which will be added the fees of any advisor used to back up the plaintiff company’s case. One important point is that UDRP procedures and local variants thereof are not legal proceedings; the plaintiff cannot claim any compensation.

- **legal proceedings**. This consists of referring the matter to the courts, in the plaintiff’s country, in the domain holder’s country, or in the American courts for domain names ending in generic TLDs. However, legal proceedings are often long-winded, expensive and unpredictable. Even if the court to which the case is submitted, accepting jurisdiction, rules in favour of the plaintiff, that ruling will not automatically be enforced if the holder is located in another country, which runs the risk of resulting in new proceedings (exequatur). Legal action as the first resort is therefore recommended only when the plaintiff and the domain name holder are subject to the same territorial jurisdiction, or if the plaintiff wishes to make a point and obtain compensation and punitive (or exemplary) damages from the holder.

10) Major trends

The world of domain names is constantly changing, but these changes tend to follow major trends. The trends that appear to us to be the most important are listed below.

- **emergence of new TLDs**: new TLDs are created every year. This has been seen with the .eu, .mobi and .asia TLDs, and is being seen again with the many plans for regional TLDs or ones named after towns. In addition to the “generic” TLDs directed at specific uses or communities, new “geographical” TLDs result from geopolitical changes – for example the forthcoming creation of .me (Montenegro) and .rs (Serbia) to replace .yu (Yugoslavia). This is a defining trend as it obliges companies and other organisations to continuously evaluate any benefit there may be in registering names with these new TLDs, either to increase visibility or to protect flagship trademarks.
- **continuous changes to local policies**: this trend is similar to the previous one, at least in terms of impact. Not one month goes by without some registry somewhere in the world altering its policy, and from time to time these changes are significant, for example by allowing the registration of domain names that were previously blocked for whatever reason. The domain names manager must play the “watchdog” role and anticipate these changes in order to warn units and be able to calmly draw up a battle plan.
- **introduction and expansion of IDNs**: domain names using non-Latin and accented characters, or in character sets as diverse as Chinese, Arabic, Cyrillic, Hebrew, etc. are introducing a new dimension to domain name and web presence strategies. The possibility of “resolving” them and using them as supports for electronic mail addresses confirms their durability, even if their use remains very limited at this time. The general trend means however that users are inclined to use domain names in natural language, as testified by some advertising hoardings showing accented domain names in TLDs that do not yet offer them...

- **new appreciation of domain names as conveying a “message”:** TLDs are increasingly aware of the “message” that they can convey. Local TLDs quite logically base theirs on their outstanding link with a territory, language or culture, while new generic TLDs seek to unite communities (be they linguistic and cultural such as .cat for Catalan or “urban” such as .berlin) or to acquire a marketing “meaning”. The .mobi TLD, intended to show that a website has content optimised for mobile telephones, is a striking example of this trend.
- **valuing domain names as corporate assets:** the “second market” in domain names has experienced a meteoric rise since 2004, based on the principle that a domain name’s actual value may be much higher than the cost of registering it. The primary factor used in valuing a domain name is currently the traffic it captures – traffic which can then be made profitable by parking, an entirely legal practice as long as the domain name breaches no third party rights. This trend leads to domain names being viewed as assets by the companies registering them; in the same way that a trademark can create a competitive advantage, a domain name that generates a significant amount of traffic should be included as an intangible asset of the company.
- **new identification systems:** this trend still remains fairly theoretical and some time away, in terms of impacts on domain naming systems. Yet exist it does and it could, eventually, be a cause of changes in the way in which companies identify themselves on the web. The .mobi TLD is one example of the possible switch to a system where content will be accessible using “mobile” identifiers which work using a system other than DNS, even if such a system could retain similarities with DNS. As are RFID labels, the “root” system for which has been entrusted to Verisign, which already runs a few root servers in the current DNS. The emergence of these new identification systems of course raises some quite sensitive issues both in political terms (who supervises them, who runs them, how legitimately?) and also for users who will, in some cases, have to adapt their web presence strategies to include these new identifiers in line with new usages and new traffic generation channels.

Conclusion

The main purpose of this white paper is to provide a summary of the main points to consider when determining and operating an optimised and durable domain name policy.

As both budgets and issues become increasingly substantial, it is logical that the fair value of this aspect of corporate and other organisations’ web presence is increasingly acknowledged by those managing it. A “fair value” which strongly implies a need for optimisation and efficiency, i.e. identification of the requirements and risks, but also an increasingly professional approach by participants, evaluation of the benefits provided by the portfolio of names held and the tracking down of names swelling the budget to no useful purpose.

In a complex and shifting environment, a company must seek out and avail itself of tools enabling it to resolve its problems and to anticipate possible opportunities and possible threats alike. To achieve this, defining a domain name strategy combined with a policy, and organising the interaction between the various participants involved in the issue, along with the putting in place of effective monitoring tools, are essential assets for any organisation desirous of building itself a solid and effective web presence.

APPENDIX I

Glossary

ccTLDs (“Country-code Top-Level Domains”): top level TLDs corresponding to the ISO 3166-1 code allocated to countries and dependent territories: “.fr” for France, “.de” for Germany, etc. In some cases, the ccTLD does not equate to a sovereign state (“.re” for the island of Réunion, for instance). This is why we refer to “territories” rather than “countries”.

Domain name policy: the set of rules governing a top level TLD. Theoretically, it covers all administrative, financial and technical aspects of the domain names that can be registered under the TLD in question. The term also means, by association with the same idea, the set of rules that an organisation establishes to manage its domain name issues.

DNS (“Domain Name System”): the Domain Name System is the entire tree structure on which internet naming is based – the root, top level TLDs (TLD), second level TLDs and domain names. We sometimes use “DNS servers” to refer to machines dedicated to running the DNS.

Top-level domains (or TLDs): TLDs are directly located under the root in the DNS tree structure. There are ccTLDs (“Country-Code Top Level Domains”) and GTLDs (“Generic Top Level Domains”).

gTLDs (“Generic Top-level domains”) : generic TLDs are not bound to a specific territory, such as .com, .biz, .edu, and .int. In some cases, for historical reasons, some generic TLDs are reserved for the exclusive use of the United States, such as .gov (government), .mil (military), etc. Generic TLDs intended for specific user communities or particular usages have been created on a regular basis since 2000, such as .aero, .museum, .mobi, etc.

IDN (“Internationalized Domain Names”): domain names that use characters from non-Latin character sets (Chinese, Japanese, Cyrillic, etc.) or accented Latin characters (German, Spanish, French, etc.). Although still somewhat limited in terms of usage, the introduction of IDNs is a major development in the domain name system, which must be taken into consideration when drawing up domain name strategies.

Registrant: the “holder” of a domain name, possessing the exclusive right to use it. Given that a holder loses a name if it is not renewed, we cannot strictly speaking refer to “ownership” of a domain name. The holder is the ultimate authority in the event of conflict over a domain name. The holder also assumes the legal responsibility related to registration and use of the domain name, especially if the registration breaches third party rights.

Registry: entity providing TLD management functions, i.e. technical maintenance, management of the database of names and associated details (servers, holders, contacts, etc.) and which lays down the rules for allocating names (“domain name policy”).

Registrar (registration office): in addition to the registry, the registrar sells domain names. Registrars may also offer associated services such as technical, administrative and financial management of domain names registered through them.

Domain name strategy: the policy followed by an organisation with a view to optimising its domain name portfolio, typically in two key areas: firstly, the fit with its requirements in terms of web presence and visibility, and secondly, management of risk resulting from third party actions (improper registrations, cyber- and typo-squatting, etc.).

UDRP (“Uniform Dispute Resolution Policy”): administrative procedure for settling disputes set up in 1999 by the WIPO - World Intellectual Property Organisation. Many local DRPs, for specific TLDs, have emerged since.

APPENDIX II

Organisations sponsoring the white paper on domain name management

The following organisations are partners in this project (in alphabetical order):



ACSEL (*Association pour le Commerce et les services en ligne*)
(*Association of e-commerce and online services*)
<http://www.acsel.asso.fr>



AFNIC (*Association Française pour le Nommage Internet en Coopération*)
(*French domain names registry*)
<http://www.afnic.fr>



APCE

APCE (*Agence Pour la Création d'Entreprises*)
(*Business start-up agency*)
<http://www.apce.fr>



APRAM (*Association française des Praticiens du droit des Marques et des Modèles*)
(*Association of practitioners of trademark and design law*)
<http://www.apram.org>



CCIP (*Chambre de Commerce et d'Industrie de Paris*)
(*Paris chamber of commerce and industry*)
<http://www.ccip.fr>



CEFAC (*Centre d'Etudes et de Formation des Assistants techniques du Commerce, des services et du tourisme*)
 (Research and training centre for technical assistants working in retail, services and tourism)
<http://www.cefac.fr>



CIGREF (*Club Informatique des Grandes Entreprises Françaises*)
 (Association of major IT users)
<http://www.cigref.fr>



Le Club de l'économie numérique
 (Digital economy club)
<http://www.club-econumerique.org>



INPI (*Institut National de la Propriété Industrielle*)
 (Industrial property office)
<http://www.inpi.fr>



ISOC France
<http://www.isoc.fr>



Mouvement
 des Entreprises de France
MEDEF

MEDEF (*Mouvement des Entreprises de France*)
 (French employers' federation)
<http://www.medef.fr>



Ministère de l'Economie, des Finances et de l'Emploi
 (French Ministry of Economy, Finance and Employment)
<http://www.telecom.gouv.fr>



Union des Fabricants
(Anti-counterfeiting body)
<http://www.unifab.com>

APPENDIX III

Introduction to the author

A graduate of the EDHEC business school, Loïc Damilaville (loic@dns-news.fr) has been assisting companies with domain name issues since 1997, undertaking consultancy and support assignments. He is particularly involved in drawing up, implementing and monitoring company domain name and web presence strategies.

Since 1998, he had been publishing the monthly newsletter DNS News (<http://www.dns-news.fr>), and in 2005 founded France's domain names club (<http://www.club-nd.fr>) which currently has over one hundred members involved in managing this issue in major companies in France and elsewhere.

In 2002, he published the first version of this white paper, updated in 2004 and then again in 2007, more than 100,000 copies of which have been downloaded since publication.

Loïc Damilaville is an assistant to the CEO at AFNIC (the registry for the .fr and .re ccTLDs) where his duties include partnerships and marketing and communication aspects.

If you have found this white paper helpful, you are requested to circulate it unaltered. Feel free to contact Loïc Damilaville (loic@dns-news.fr) with any questions on a possible partnership regarding the distribution of this white paper or matters relating to domain name and web presence issues.