OPAALS PROJECT

Contract n° IST-034824

WP 12
Open Source Software Innovation and Socio-Economic Models for Digital Ecosystems

D12.12
Governance and Sustainability Strategies for DEs

Project funded by the European Community under the "Information Society Technology" Programme

Contract Number: IST-034824

Project Acronym: OPAALS

Deliverable N°: D12.12

Due date: M49

Delivery Date: M51

Short Description: In this deliverable, some key questions concerning DE regulation have been analysed, principally from the legal point of view. In relat¡on to DE regulation, basic elements for governance and sustainability strategies have been pointed out.

Authors: Pedro Bueso (UniZar), Daniel Oliver (UniZar), Tamara Martín (UniZar), Leda Gómez (UniZar), Diana Vollmer (UniZar)

Partners contributed: Universidad de Zaragoza (UniZar)

Made available to: Public

Versioning		
Version	**Date**	**Name, organization**
1.0	Jun 29, 2010	Pedro Bueso, Daniel Oliver (UniZar)
1.1	July 9, 2010	Pedro Bueso, Tamara Martín, Leda Gómez (UniZar)
1.2	July 26, 2010	Pedro Bueso, Daniel Oliver, Tamara Martín, Leda Gómez, Diana Vollmer (UniZar)

Quality check

Internal Reviewers: Anne English, Paolo Dini (LSE)

Dependencies:

Achievements*	First analyctical approach to the regulatory problematic of digital ecosystems as a part of a general theory on sustainability and governance of digital ecosystems; identification of the basic first steps in order to implement a sustainability and governance framework in the OPAALS Community.
Work Packages	WP0, WP6, WP10, WP11
Partners	ITA, LSE, T6 ECO
Domains	Social Science - Sustainability and Governance of DEs
Targets	PMB, ICT Members, OPAALS Community
Publications*	---
PhD Students*	No PhD students involved
Outstanding features*	Improvement of the state of the art: Theoretical construction for a general theory on Sustainability and Governance of Digital Ecosystems
Disciplinary domains of authors*	UniZar: P. Bueso (Law), D. Oliver (Law), T. Martín (Law, Business Administration), L. Gómez (Law), D. Vollmer (Law)

The information marked with an asterisk (*) is provided in order to address Recommendation n. 4 from the Year 2 review report

Table of Contents

EXECUTIVE SUMMARY

After making some introductory remarks, this deliverable aims, on the one hand, to establish the basic elements for the introduction of legal and regulatory issues into the Digital Ecosystem paradigm. This goal is pursued in a way that ensures workability of Digital Ecosystems in practice without damaging their architecture and design principles. For that, it focuses on business practices of Small and Medium Enterprises in a specific approach to Digital Ecosystems, i.e., the Digital Business Ecosystem.

In order to achieve this goal, after touching upon the Internet regulation debate, the deliverable identifies some basic key features of the Digital Business Ecosystem as regulation fields and maps the major regulatory issues connected to them, distinguishing between regulatory spheres and regulatory topics. The next step taken is to delimit the legal framework for the Digital Business Ecosystem under the consideration of the issues mapped, i.e., the regulatory constraints. Here, the deliverable pays special attention to the constraints resulting from the EU regulation on intellectual property rights, privacy and data protection, digital signatures, trademarks and domain names, companies and associations, information society services, and fair trade and competition. Regarding the regulatory issues and the related legal framework, the deliverable approaches some regulatory strategies which may suit the Digital Business Ecosystems: self- and co-regulation, alternative and on-line dispute resolution, *lex informatica*, and hinge or hybrid law. Finally, some concluding remarks are made and some implications from the regulatory strategy for the governance decisions are pointed out.

In addition, and considering the results of the Sustainability and Governance Workshop, held in SUAS Salzburg, in January, 2010, the deliverable summarises further basic elements for governance strategies of DEs, specially for a governance strategy of the OPAALS Community, together with the regulatory issues of the OPAALS Legal Entity, which is dealt with in detail.

1. INTRODUCTION

1.1. Document Scope

As a future vision of the Internet, the ***Digital Ecosystem*** (hereafter, **DE**) **paradigm** faces plenty of challenges, and not only those of a purely technical or computer sciencie-related nature. So, **sustainability** rises as a big, complex and interdiciplinary issue for the new environments for interaction between machines, applications, organisations and persons, such as the DE paradigm. The importance of sustainability has been pinpointed by the reviewers in their reports on the work done untill now in the OPAALS Network of Excellence.[1] In this context, **governance** is regarded as an asset for the success in sustainability; however, governance is qualified as a low-relevance asset. **Regulation** is a component of governance. So, reviewers referred to some topics which might be regarded as regulatory issues.[2]

As set out in the **DoW of Phase III** of OPAALS, UniZar has researched in Task 12.11 (Regulation and governance strategies for digital ecosystems) in the field of Regulation, regarded as a face of Governance, of DEs.

To be more precise, UniZar's research has aimed to establish the basic elements for the introduction of legal and regulatory issues into the DE paradigm, but to do it in a way that ensures DE workability in practice without damaging the architecture and design principles of DEs. For that, UniZar has focused on Small and Medium Enterprises (hereafter, SMEs) business practices in a specific approach to DEs, i.e., the **Digital Business Ecosystem** (hereafter, **DBE**), which mainly represents the case studies taken into account in WP11.

Therefore, UniZar has undertaken the following **steps**: (a) has focused on Regulation as a specific dimension of Governance; (b) has reviewed the relationship between Regulation and Governance in the context of DEs; (c) has built its work under strong consideration of D12.2, of the work done in WP11 and under a critical review of the building blocks for regulatory trust proposed in DBE's D32.2; (d) for that purpose, UniZar has developed and expanded an informal Governance research through collaboration with OPAALS researchers and integration of fieldwork results – this has been made easier because of the participation of UniZar in the ICT[3] working in this thematic area; (e) has identified Regulatory Spheres, Regulatory Topics or Issues and Regulatory Constraints of the Legal Framework for DEs; (f) has formulated a Regulation Strategy for DEs, especially exploring the consideration of DEs as providers of Information Society Services (ISS) and as markets for ISS; and (g) reports of UniZar's ICT work drawing the more relevant issues to DEs in general and to DBE for SMEs in particular.

Hence, the **aim of D12.12** is two-fold:

- On the one hand, the emergence of environments such as DEs poses a number of regulatory challenges, which the emerging theory of DEs has not yet addressed from a legal viewpoint. This deliverable aims to tackle the topic of **regulatory strategies** and, indirectly, governance strategies for DEs, mainly regarding SMEs as participants in DEs[4]. So, after mapping the DEs regulatory issues in M12.4, D12.12 goes deeper into the legal

[1] So, in Interim Review, p. 6: Actions; p. 11: WP inputs Phase III; however, there was no mention of governance; in 2nd Year Review, pp. 4 f.: main assets for sustainability: Regions, OKS.

[2] So, in 2nd Year Review, p. 4, R6: Legal Entity, IPRs Issues; p. 17: OSS greater uncertainty about governance, rules, licensing.

[3] Within the OPAALS organisational structure, "ICT" stands for Integration and Coordination Team, of which Prof. Pedro Bueso of UniZar is a member.

[4] This task began in Phase II of OPAALS, in WP6, Task 6.8, D6.9, under point 7, and culminates here in Phase III of OPAALS, in WP12, Task 12.11, after M12.4 "Mapping DEs Regulatory Issues".

framework of DBE and the regulatory strategies for DBE. Finally, a regulatory strategy is suggested.

- On the other hand, and considering the results of the **Sustainability and Governance Workshop** (hereafter, SuGo Workshop), held in SUAS Salzburg, in January 21 and 22, 2010[5], which includes the work done in WP11, further basic elements for governance strategies of DEs, especially for a governance strategy of the OPAALS Community, are summarised, together with the regulatory issue of the **OPAALS Legal Entity**, which is dealt with in detail.

1.2. Structure of the Document

Following the path drawn in D6.9[6], in Section 2 we first try to clarify what a DE is, whereby our attention will be largely focused on the *digital business ecosystem* [2.1]. After touching upon the Internet regulation debate [2.2], we shall confine ourselves to identify some basic key features of the digital business ecosystem as regulation fields and to map the major *regulatory issues* connected to them [2.3], and their *legal framework* [2.4]. We present then an approach to some *regulatory strategies* which may suit the digital business ecosystem [2.5]. Finally, some concluding remarks are made and some implications from the regulatory strategy for the governance decisions are pointed out [2.6].

Subsequently, in section 3, and as summary of UniZar's ICT work, the SuGo Workshop is reported on [3.1], and the study of the regulatory issue of the OPAALS Legal Entity is carried out [3.2].

1.3. Relation with other OPAALS' WPs

The following relationships with other OPAALS' WPs can be especially highlighted:

- Relation with WP0, more precisely with Task 0.6: Section 3 exposes a part of the efforts done by the Integration Coordination Team (ICT) targeted to advance in the area of Sustainability and Governance.
- Relation with WP6, precisely with D6.14: the legal background constitutes an example of second-order contractual regulatory issues in an activity sphere consisting of the provision of ICT services by means of Dynamic Service Composition (hereafter, DSC).
- Relation with WP10: the governance concepts discussed here are immediately relevant to Sustainable Community Building in the Open Knowledge Space, which is the focus of WP10.
- Relation with WP11: the experience and lessons coming from the case studies of this WP have been integrated in the identification of the basic elements for sustainability and governance strategies arrived at in the SuGo Workshop.

[5] See http://dbe.fh-salzburg.ac.at/index.php?id=salzburgworkshop2010
[6] See D6.9, p. 59 ff.

2. REGULATORY ISSUES, LEGAL FRAMEWORK, REGULATORY STRATEGIES AND DIGITAL ECOSYSTEMS

2.1. Digital Ecosystems

A DE can be defined as a combination of a specific technological infrastructure, the so-called "digital environment", and those entities or "digital components" (software, services, business processes or models, contractual frameworks, law, knowledge, etc.) which have been formalised, digitised and transported within the ecosystem and which can be further processed by humans or by computers.[7] Since there are always people –be they individual or collective players– involved in such an environment, it seems meaningful to complete this technical definition by adding a third aspect, namely the social community related to DEs.[8] This working definition could be surely refined, but these three **elements** –**digital environment**, **digital components** and **social community of players**– are inherent to all DEs.

A detailed classification of DE players is lacking,[9] but we can at least identify two types of actors involved: those actors that are responsible for the design and development of the technological infrastructure and those that use it for mutual interaction or transaction purposes. These two types may of course overlap, but whether this overlap exists and to what extent it does will depend on the specific organizational settings of each DE. Figure 1 illustrates this approach to **DEs as socio-technical environments**:

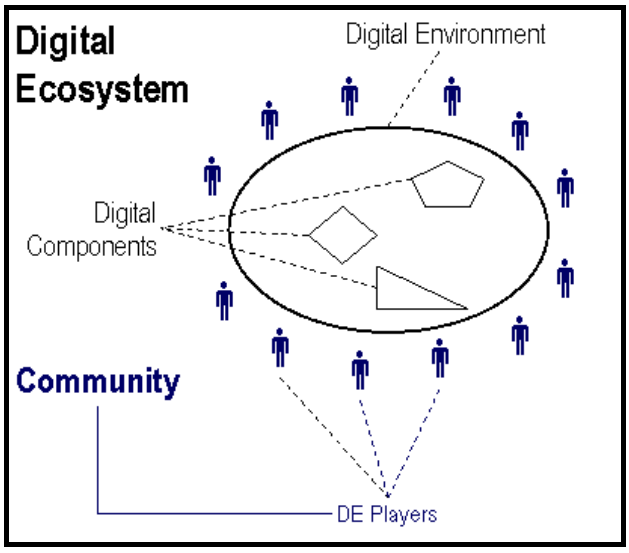

Figure 1: DE as socio-technical environment

[7] See www.digital-ecosystems.org; further approaches to the concept of DE may be found in Dini (2007: 25), who combines three definition frameworks based respectively on natural, social and computer sciences; or in Nachira, Dini & Nicolai (2007: 5), focusing on the concept of business digital ecosystem.

[8] «In a digital ecosystem the users can be considered to be the source of an 'external' selection pressure on the digital organisms» (OPAALS D1.2: p. 86). See further OPAALS D1.2: p. 87 ff.

[9] However, see DBE D32.2: p. 15-16.

Particular settings and structures of DEs may vary. As recently developed, however, the DE paradigm relies on certain normative assumptions associated with political, economic and social science arguments which determine DE design and architecture features.[10]

In this regard, a DE has been defined as «an open, loosely coupled, domain clustered, demand-driven, self-organising agent environment, where each agent of each species is proactive and responsive regarding its own benefit/profit (…) but is also responsible to its system» (Boley & Chang 2007: 2); or as «a self-organising digital infrastructure aimed at creating a digital environment for networked organisations that supports the cooperation, the knowledge sharing, the development of open and adaptive technologies and evolutionary business models».[11]

In the line of thinking of Boley & Chang[12], **the OPAALS Community** approaches **DEs as open, distributed and decentralised environments**, in which **local autonomy of DE players and Service Oriented Architecture** (SOA) **principles** are duly safeguarded thanks to the absence of a single point of control or failure (such as a central server).[13] These features respond to **normative decisions** on the side of DE proponents such as the OPAALS Community and have profound regulation and therefore governance implications; so, apart from its workability –we turn back to this point later on–, it seems that there is no permanent need for centralised control or for single-role behaviours, quite the opposite, a dynamic (environment-related and needs-oriented) leadership structure should be provided. In fact, the **main challenge** is how to achieve workability in real world without distorting the conception and principles of DEs.

As of the date of this report, practical applications of DEs are still few. Perhaps the most advanced implementation of the DE paradigm is the **DBE**, so that we shall focus on it.[14] On the one hand, DBE results from combining the DE infrastructure and a business orientation. To put it in terms of system theory, the combination of different aspects or subsistems enables a functional differentiation or specialisation of DEs. On the other hand, DBE shows a potential significance for SMEs trying to operate at a large scale. As stated in the seminal research works on DEs, these «will offer opportunities of participation in the global economy to SMEs and to less developed or remote areas» and «foster local economic growth», which will «preserve local knowledge, culture and identity and contribute to overcome the digital divide».[15] The challenge is how legal and

[10] See D3.6 for example.

[11] Boley & Chang (2007: 2) offer this negative definition: «A Digital Ecosystem is: unlike a client-server architecture, where the communication is centralised and which acts as a command and control environment; unlike a Peer-to-Peer architecture, where, at any time, each agent has a well defined role, i.e., can only be client or server, but not both; unlike a Grid architecture, which stitches partners together for resource sharing but cannot avoid counterfree riding; unlike a Web service network, where brokers are centralised and service requesters and providers are distributed in a hybrid architecture that does not guarantee trust and QoS. A Digital Ecosystem instead is an open community, and there is no permanent need for centralised or distributed control or for single-role behaviour. In a Digital Ecosystem, a leadership structure may be formed (and dissolved) in response to the dynamic needs of the environment».

[12] Boley & Chang 2007: 2.

[13] For a detailed description of the DE core architecture, see OPAALS D3.6. This, however, does not exclude other approaches to DEs which are based on different or even diverging assumptions. For a comparison between European and USA DEs, see Nachira 2005.

[14] Nevertheless, applications of the DE paradigm go beyond the business field: it could be applied to other areas such as eGovernment. In this respect, see: www.eisco2008.eu/declaration.php

[15] See www.digital-ecosystems.org. Dini et al. (2008) underline «the need for more sophisticated technology that can support the distributed coordination of loosely coupled B2B transactions in reconfigurable value networks, thereby preserving local autonomy and avoiding dependence on centralised transaction servers», and that «these aspects are centrally important in development contexts: (a) the local autonomy, because it is about social constructivist understandings of self-determination and (b) the independence, because, by empowering individual players, no matter how small, to play in the B2B market at the same level of multinational corporations, it achieves in the electronic B2B space a similar flattening and democratising effect the web has already reached in the content-sharing space».

regulatory issues can be introduced into the DE paradigm in a way that ensures DE workability in real business practices without damaging the architecture and design principles.[16]

2.2. Approaching DEs Regulation

Although the concept of regulation is difficult to grasp,[17] discussing regulatory issues posed by DEs at least requires a working **definition** of it. We shall adopt the notion developed by Black (2008: p. 139) over former definition attempts.[18] According to her, «by regulation is meant sustained and focused attempts to change the behaviour of others in order to address a collective problem or attain an identified end or ends, usually through a combination of rules or norms and some means for their implementation and enforcement, which can be legal or non-legal».

Some **complementary remarks** may be worth adding for the purpose of this paper:

- Regulation is **both a process and a product**.
- For it entails a ***set of practices*** **and procedures** leading either to the establishment or to formalisation of ***norms*** **or normative expectations** – which are binding at least in some respect.
- It thus necessarily implies a certain form of ***institutionalisation*** **or institutional framework**, be it formal or informal, state-based or not.
- Moreover, regulation attempts to steer or otherwise **organise a given *social context* or action sphere**.
- Therefore its outcome, the *norms*, is always **intended to affect human behaviour**, which can be pursued either directly (***social regulation***) **or** indirectly by addressing those technological means or infrastructure underlying human actions (***technical regulation***).

As binding decision-making, **regulation is** a legally and politically-laden phenomenon which remains tightly **linked to societal distribution and exercise of power**. In this way it merges into the manifold concept of ***governance***.

In fact, considering the variety of approaches to governance,[19] European governance,[20] Internet governance,[21] or electronic governance,[22] it might be said that this concept stresses political and

[16] «Legal requirements for underwriting contracts and guaranteeing operational aspects of the architecture can lead to an inflexible technology environment based on fixed legal entities»; «finding an organisational and decision-making framework that can mirror the de-centralised, distributed attributes of the technological architecture is a major challenge» (OPAALS D3.6 p. 82).

[17] See e.g. Baldwin and Cave (1999: p. 1 ff.). After reviewing recent literature on governance and regulation, Darking (2008: 17, 18) defines regulation as a «policy practice of placing restrictions (either legal or rule-based) on those aspects of social and economic behaviour considered potentially detrimental to the common good». A far broader notion of regulation as «any form of social control» is used in OPAALS (D3.6: p. 20).

[18] See in particular Selznick 1985: p. 363.

[19] «Governance in the public context is closely related to government and democracy, but has a different focus. (…) Government is the institutional view. (…) Democracy is the legitimacy view. (…) Finally, governance is the regulatory view. It is about how to best guide, steer or lead the society so as to identify and realize common interests» (Gordon 2004: p. 2-3); «"governance" emphasizes the regulatory, guiding or steering function of the state, i.e., the directing of society so to protect public interests and achieve, to the extent possible, the common good» (Gordon 2005: p. 3). See also Darking (2008: p. 17 ss.) and Rhodes (1997, 1996).

[20] The phrase "European Governance" refers to "rules, processes and behaviour that affect the way in which powers are exercised at European level, particularly as regards openness, participation, accountability, effectiveness and coherence", which are considered as "principles of good governance" in combination with the EU-legal principles of subsidiarity and proportionality (European Commission 2001: p. 10-11).

[21] Internet governance has been defined as, «the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision making procedures, and programmes that shape the evolution and use of the Internet» (WGIG 2005b: p. 4).

power-related dimensions involved in any regulatory process. Likewise, as far DEs are concerned, governance is about «community decision-making» (Darkin, Whitley & Dini 2008: p. 138), so that it inevitably emerges when dealing with regulation. We shall however **try to tackle governance and regulation as two separate issues** (Figure 2) –to the same extent as politics and law have been traditionally distinguished between.

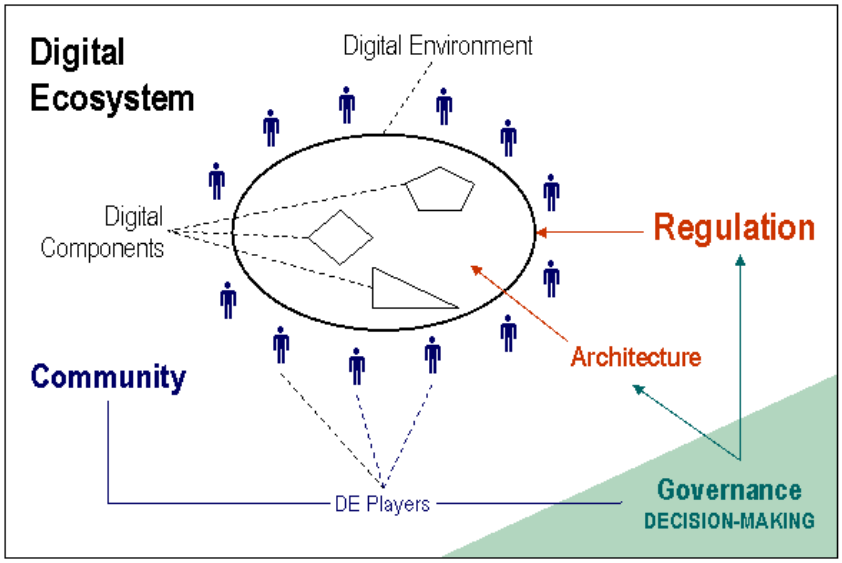

Figure 2: DE Regulation, as separated from governance

As mentioned, a **DE** may be conceived as a socio-technological environment, i.e a **social interaction field which is built upon and immediately determined by a specific technological infrastructure**. This applies in a sense to any social area, but *the intertwinement of the social and the technological* may be sometimes so relevant that it becomes a **distinctive feature**. The clearest instance for this is the **Internet**.

The phrase "**Internet regulation**" calls to mind a large variety of issues, but these boil down to three interwoven questions:

- Firstly, ***what regulation needs are to be considered?*** Emerging social environments such as the Internet always pose issues which need to be regulated, be it to avoid detrimental effects or to foster a certain development.[23]
- Secondly, ***do pre-existing legal or regulatory norms*** *(which were not set for the Internet)* ***apply on the Internet as well, and do they suffice for governing it, or is it rather necessary to establish specific norms*** **addressing Internet activities?**
- Thirdly, ***how could we manage to make*** *(both pre-existing and specific)* ***regulation certain and effective in online environments*****?**

Legitimacy and governance issues apart, the bulk of Internet regulation debates lay behind these questions, or at least could be traced back to them.

---

[22] «eGovernance is about the use of ICT to support the guiding or steering of an organization to achieve its goals. In the political context, as a special case, eGovernance is about the use of ICT to steer society and promote public interests» (Gordon 2004: p. 5); according to Finger & Pécoud (2003: 6), eGovernance «a dynamic concept, which implies the growing use of the NICTs for the three State's main functions (e.g. e-Government, e-regulation and e-democracy), increasingly involving non-state actors at levels other than the national one».

[23] Internet Regulation has been conceived of as involving three related *spheres*: «direct regulation of the Internet infrastructure itself; regulation of activities that can be conducted only over the Internet; and regulation of activities which can be, but need not be, conducted over the Internet» (Froomkin 2005: p. 1).

Regulatory debates on DEs show a similar structure.[24] So, we can transfer the above formulated questions to our concrete field of resarch in order to set out the structure for a "**DEs regulation debate**":

- The first question raises the point of indentifying the **regulatory issues** of DEs.
- The second question clearly asks to determine what parts of the preexisting **legal framework** are applicable to DEs, whose answer implies, on the one hand, to demarcate the margin or space left for regulatory activity; and, on the other hand, to provide concrete justification for the need for regulatory actions and their intensity: DEs are likely to pose particular problems which do not have a significant counterpart in previous legal framework, so that special regulatory measures must be taken.
- The third question looks for a distillation of the answers given to the questions above, in order to establish the best **regulatory strategies** for the DEs themselves and the role of **autopoiesis** in choosing such strategies, in combination with the goal of **workability**, i.e., certainty and effectiveness, of DE regulation. Thus it will be necessary to discuss regulatory strategies, but also implications regarding **governance** – i.e., legitimacy or regulatory processes.

In this context, **autopoiesis** shall be understood as a DE-autonomous regulation activity, as the use of a space for autonomous regulation in the context of the given legal framework; however, this shall not be understood as a reaction to an external causal deterministic stimulus to the legal framework, regarded as context or environment, but as the result of a decision-making process where relevant stakeholders participate as they establish the governance structure, that is going to be a part of the business model(s).

2.3. Mapping DBE Regulatory Issues

As explained in D6.9,[25] the classification of DBE-related regulatory issues could be only regarded as a starting point for the purpose of mapping DE regulatory issues: the identified wide categories of regulatory issues[26], their classification as "internal", "external" or both "internal-external"[27], and the actor-based classification suggested[28] provide limited guidance. The same happens with the classification of legal issues related to SME clusters and DBE as provided by the LEKTOR Project[29], because it remains little differentiated, i.e., too generic, and therefore does not fully capture those regulatory or legal complexities involved in DBE.

Therefore, we tried to refine these classifications in order to sketch a guide to DBE regulatory issues. To this end, it first makes sense to take a look at other socio-technological environments, such as SMEs IST-clusters, virtual professional communities (VPCs), e-marketplaces or B2B trading platforms, which offer a starting point for DBE regulation discussions. Taken as social communities and specialised business areas, DBE shows some similarities to those environments.[30] Of course

[24] Decision-makers must «be careful to avoid being blinded by the marvels of new technology in deciding law and technology cases», and must «look beyond the technology involved in a dispute to focus on the legal issues in question» (Mandel 2007: p. 552 and 560).

[25] See p. 61 ff.

[26] See DBE D32.1: p. 20 and D32.2: p. 11; OPAALS D3.6: p. 21; Elaluf-Calderwood & Tsatsou 2007: p. 100 ff.

[27] DBE D32.2: p. 14-15.

[28] DBE D32.2: p. 15.

[29] See the Lektor *eCatalogue on Legal Issues in eBusiness* (p. 8). Interestingly enough, the LEKTOR project links legal issues to business activities, and further includes a tentative priorisation: see both the Lektor *Analytical Study* (p. 33 ff.) and *Regulatory Roadmap* (p. 12 ff.) at www.ubique.org/lektor.

[30] So, B2B Internet trading platforms include «all Internet based technical solutions that aim at facilitating the establishment of new trading relationships between companies or at supporting existing relationships» (Expert Group on B2B Trading Platforms 2003: p. 3). A DBE can be conceived as a community of players or actors trying to do online business in a way that allows services as, for example, DSC.

there are significant differences between them, but an insight into DBE regulatory problems may be gained by approaching them comparatively.

In our view, regulatory issues posed by DBE may be mapped according to a scheme which consists of two interwoven parts

- First, two major **regulation spheres** covering both the DBE as a social *community* and the particular *activity* carried out within it, in our case B2B business transactions
- Second, two subsets of **regulatory topics** which may be typical for these spheres.

Hence, a tentative map of DBE-related regulatory issues can be introduced over this basic structure:

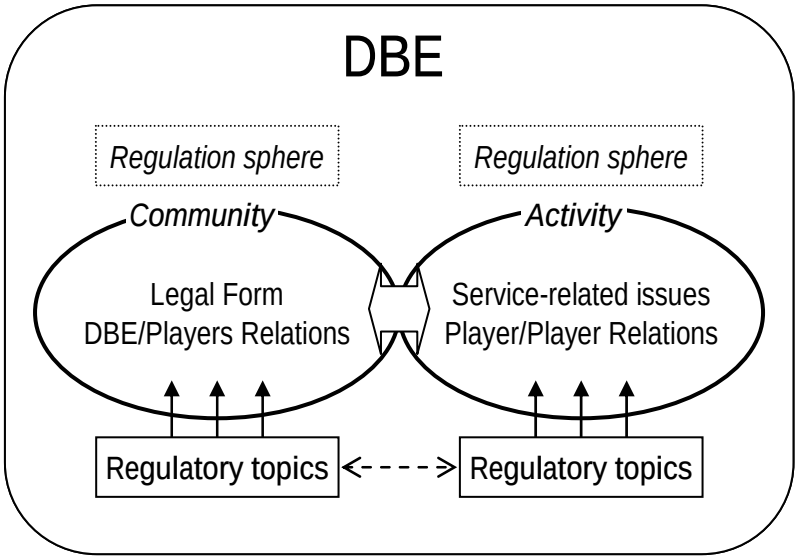

Figure 3: Basic structure of the Map of DBE Regulatory Issues

2.3.1. Regulation Spheres

When dealing with DBE-related regulatory problems, a starting distinction may be drawn between regulating the *DBE community* and regulating the *DBE activity.*

The regulation of the DBE **community** makes up, so to speak, the DBE 'constitution'*.* It may be taken to comprise two major issues:

- Firstly, it includes the **foundational settings** of the DBE, say, the legal form and structure of the community, which has to be seen as a take-off regulatory decision.
- Secondly, this sphere is about the **internal and organisational rules** of the DBE as such and, in particular, about those rules governing relationships between the DBE itself and the DBE players.

The sphere related to the DBE **activity** is concerned with the regulation of the relationships between DBE players themselves, i.e., with player-player transactions. There are at least two questions which must be answered in this sphere: what are the particular rules applicable to single business transactions between DBE players (*first-order contract rules*), and what are the rules applicable to the relationships within the DBE as a business environment (*second-order contract rules*):

- As for the **first-order contract rules**, a wide range of sector-specific issues may appear depending on concrete areas of DBE deployment, and even more specific issues may be raised by the parties entering contractual agreements within the DBE. Therefore, single transactions can be expected to be largely governed by contract agreements which are established between the DBE players.
- In their turn, **second-order contract rules** must be considered a regulatory issue for DBE. Services offered by the DBE platform need a regulatory framework. For example, DSC (Dynamic Service Composition) is not only the DBE most striking functionality, but also implies making complex contracts whose regulation poses a range of specific problems. For example, DSC leads to scenarios in which one client can simultaneously enter different contracts with different providers under potentially inconsistent conditions, so that second-order solutions must be reached to address this issue.

2.3.2. Regulatory Topics

DBE regulation may be also approached in terms of topics or issues. This can be done in various ways. For instance, a thematic list could be provided of those legal issues which are expected to be relevant for DBE, as is usual with regard to Internet-related environments,[31] and this list can eventually be refined and systematised by linking it to specific actors or to DBE lifecycles.[32] Previous attempts to list e-business legal topics show that a comprehensive classification is hardly achievable on an abstract level. Any legal issue may possibly arise, for it depends on the type of activity carried out within the DBE.

Anyway, we think that any list of relevant topics becomes more useful for players and regulators if it gets linked to the above regulation spheres.

Regarding the sphere of the DBE **community**:

- The **foundational settings** of the DBE include the decision on the **legal entity**, but also on **trade mark(s)** and **domain name(s)**. It can be assumed that potential players will be willing to enter a DBE if it has some legal entity rather than it has not, so that a given legal form must be chosen if a DBE is expected to work out as a business area. As discussed later, this choice does imply situating the DBE under a given (compulsory) legal framework.
- The **internal and organisational rules** of the DBE include **DBE identity**, a **general** framework for **privacy and confidentiality,** and community **currency**; *intellectual property rights* (IPRs)-related issues, such as the management of the **p2p architecture software** and of the **OKS** contents; i.e., ownership, licencing and liability rules; and, in order to solve the disputes which may arise regarding the issues identified above, a **general Alternative Dispute Resolution** (ADR) system.

Regarding the sphere of the DBE **activity**:

- In principle, the **first-order contract rules** do not need regulatory decisions, for they remain largely dependent on the players' will.

[31] For instance, legal issues raised by SME Clusters have been classified as follows (Seddon et al. 2006: p. 28 ff.): *choice of the legal structure* (for both clusters as such and specific co-operative networks); *relationship between cluster and cluster broker*; *know-how, IPR and confidentiality* issues; *legal barriers* (procurement and state aid) and 'other' issues such as *data protection and competition law* problems. In the same line, VPC legal issues have been classified into *IPR* issues (knowledge creation, ownership, protection and exploitation; infringement and liability; and confidentiality), *corporate law issues* (mainly related to the legal form), *labour law* issues and 'other' legal issues such as *international jurisdiction and arbitration* (Wallentin et al. 2005: p. 55 ff.).

[32] It appears that the aforementioned taxonomy of DBE regulatory issues (Figure 3) tried to follow this line. The same goes for VPCs or SME Clusters.

- The **second-order contract rules** include decisions on **trading and contracting rules**, where specific problems arise because of the particularity of DBE; for example, this is the case of contractual liability in DSC; this includes the setting of norms to protect users of the DBE, especially if they are regarded as consumers, and to ensure fair trade and accurate market competition[33]; **specific** frameworks for **privacy and confidentiality**; and **specific ADR** systems.

A tentative scheme could be as follows:

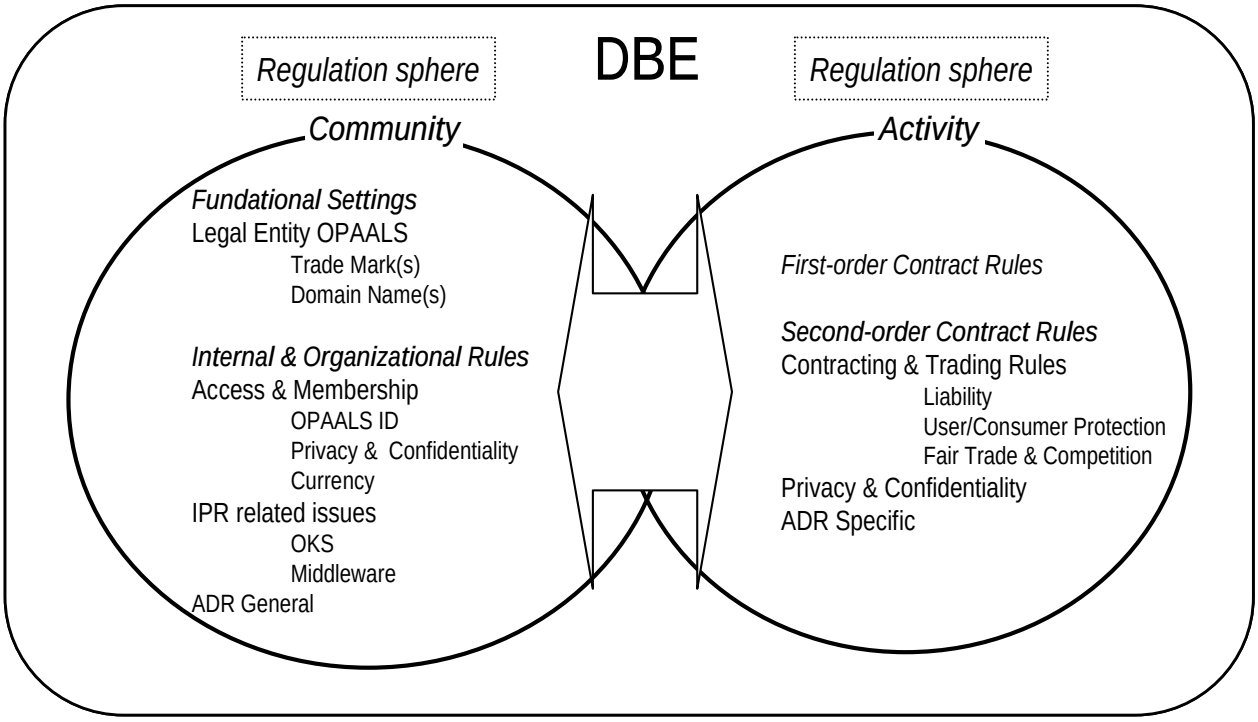

Figure 4: Tentative classification of Regulatory Topics

As an example, let us consider that possibly the most striking feature of the DBE is DSC. This is a rather complex functionality, but it could be seen as the autonomous discovery and creation of new services or processes by combining existing components at runtime upon a previous user request.[34] DSC shall allow users to create new Real World Business Offerings and Contracts from the ones that are provided by other parties or by the users themselves. Moreover, such a way of doing business, which is the common way to proceed in the human world, should be performed by a computer: the computer should provide the contract list which best fits the user demands, in an environment where the offers can be added and removed automatically and which can be expressed in different languages. From a legal point of view, the interaction of peers, i.e., SMEs, which offer services and products from different places with different currencies and regulatory frameworks, opens new issues to be solved: contractual gaps resulting from inconsistencies or contradictions and from insufficiencies of the general terms and conditions of the different SMEs taking part in a DSC must be filled in, in order to keep or increase legal certainty; which means, trust in the result of the DSC. All this inconsistencies, contradictions and insufficiencies are components of the subject-matter of second-order contract rules.[35]

[33] See below, 1.5.1.

[34] Further details about DSC can be found in Dustdar 2007.

[35] Extended, see D6.14, section 4.

2.4. Delimiting a Legal Framework for DBE

What has to be underlined now is that DBE regulatory decisions may be seen as an exercise of regulatory powers by a certain community of actors. However, this does not mean that these actors are totally free to take regulatory decisions. Quite the contrary, most of the regulatory options and decisions are predetermined or, at least, influenced by a variety of **regulatory constraints** which make up the **legal framework for DBE**. Hence, the basic structure of the tentative map of DBE-related regulatory issues can be completed as follows:

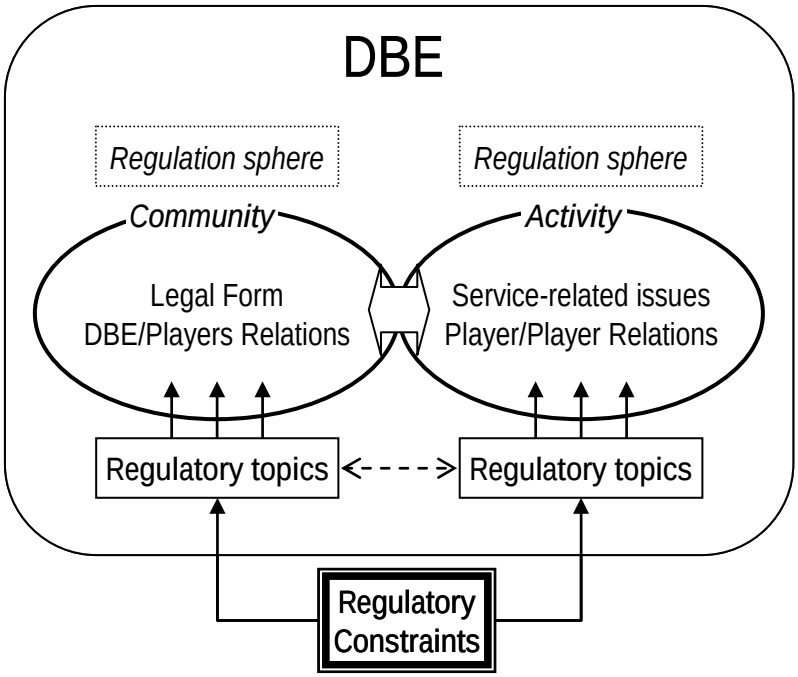

Figure 5: Completing the basic structure of the Map of DBE Regulatory Issues with Legal Framework

2.4.1. Regulatory Constraints

Despite of the fact that DBE is a new or emerging field, it cannot be contended that there are no rules or principles affecting it, i.e., that there are no limits to DBE regulation. On the contrary, there exists a **dense network of regulatory constraints** which will surround any DBE initiative. These must be taken seriously, for otherwise DBE will not work.

The **delimitation** of the such a legal framework is a very **complex task**, especially if it attempts to be exhaustive. Subjective, objective and geographical or territorial scopes of application of the regulatory constraints are very diverse, they all build a framework which is made up of both compulsory and non-compulsory (dispositive) elements, and only within the latter or in the absence of regulatory elements can DBE be said to be self-regulating. Here arises the question of **applicable Law** and, related to it, the question of **jurisdiction**. The determination of both axes should take into account a world-wide scenario as a goal. However, in order to simplify the model, we will focus on the European Union, i.e., on the Law promulgated in the European Union and its Member States and their jurisdiction as pattern to delimit a legal framework for DBE. Nevertheless, the resulting framework will be a basic one, open to be completed with other legal elements, for example, normative imputs coming from regional catalysts as community stakeholders searching for promoting DBE within their respective legislative and executive competences.

As mentioned above, one of the first questions to be solved by DBE, as a component of the **community** sphere, is the legal form or structure which the DBE will take. However, many legal

and statutory constraints do normally depend on the type of **activity** carried out by a legal actor, in our case the OPAALS Legal Entity and the single members of the DBE Community. For instance, whether the DBE is confined to B2B transactions or whether it envisages B2C relationships as well makes a big difference. In the latter case, a bulk of consumer protection legislation shall be applicable, thereby affecting many other aspects (e.g., promotion rules, contracting rules, information duties, jurisdictional issues). In this regard, the issues related to the formation of the OPAALS Legal Entity must be distinguished from the legal status which is applicable to this legal person, and which is normally determined by the kind of activities involved. So, regardless of its form, the OPAALS Legal Entity will, with high probability, fall into the concept of **Information Society Service Provider** in terms of the EU Directive on e-Commerce.[36] Likewise, if the DBE itself is devoted to commercial interchanges and therefore constitutes some sort of '**market'**, it will be subject to fair trade and competition law –so that some external regulation on unfair commercial practices ought to be respected, as well as antitrust provisions.

Again, it is difficult to agree on a general classification of regulatory constraints, for they are rather context-dependent. Nonetheless, because of the reasons explained above, an insight into the analysis of regulatory constraints may be gained trying to unfold the **EU regulatory framework on e-business** activities (i.e., following a directive-by-directive approach). Under EU law, there are legal provisions which must be considered at least in the following areas:

- e-commerce and information society services in general;[37]
- e-signatures and PKI infrastructures;[38]
- privacy and data protection rights in general;[39] privacy within the field of electronic communications;[40] and data retention by electronic communication providers;[41]
- copyright and related rights in the Information Society;[42]
- e-money;[43]
- competition and fair trade;[44]
- consumer protection (including unfair commercial practices, unfair contract terms, distance contracts and consumer financial services).[45]

[36] The establishment of any B2B e-Market is subject to EU law and particularly to the e-Commerce Directive: see in this respect EC COM 2004/479, p. 4.

[37] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[38] Directive 1999/93/EC on a Community framework for electronic signatures.

[39] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data.

[40] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector;Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.

[41] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

[42] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society; Directive 2004/48/EC on the enforcement of intellectual property rights; Directive 2009/24/EC of 23 April 2009 of the European Parliament and of the Council on the legal protection of computer programs

[43] Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions.

[44] Arts. 101 ff. of the TFEU.

[45] Directive 2005/29 of 11 May 2005 on unfair business-to-consumer commercial practices in the internal market; Directive 2005/29 of 11 May 2005 on unfair business-to-consumer commercial practices in the internal market; Directive 93/13/EC of 5 April 1993 on unfair terms in consumer contracts; Directive 2002/65/EC concerning the distance marketing of consumer financial services and amending council directive 90/619/EC and directives 97/7/EC and 98/27/EC.

A tentative scheme could be as follows:

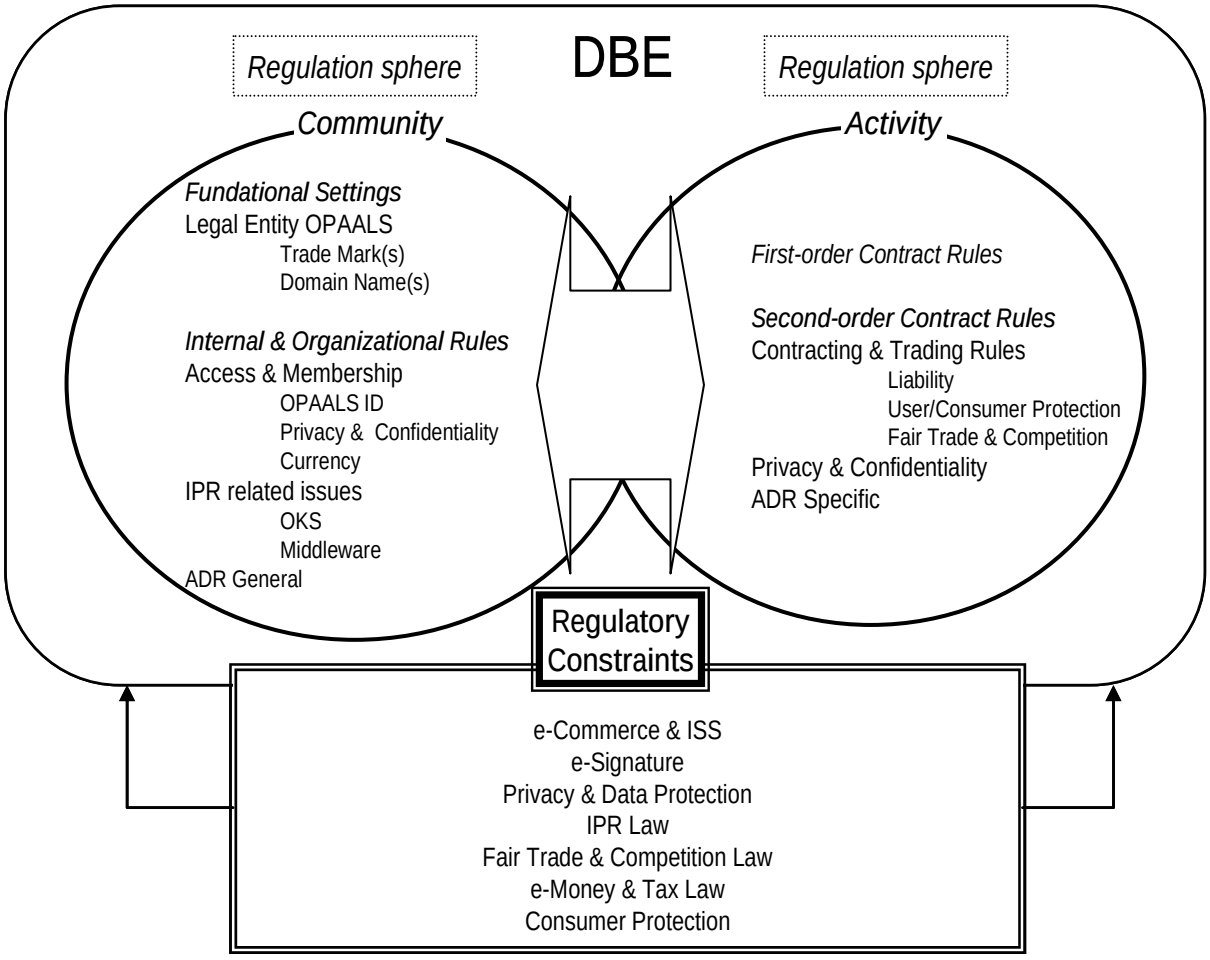

Figure 6: Tentative classification of Regulatory Topics and Regulatory Constraints

In view of this EU regulatory framework for e-business, it would be naive to think of a DBE as a community without regulatory constraints that could be completely self-regulating (or say fully **autopoietic**) –it could be at most, to borrow the term from Moore (1978), **a 'semi-autonomous' field (SAFS)**.[46] In each sphere of activity and for each legal topic related to DBE there may be compulsory, optional (or subsidiary) and regulation-free content. This content, mainly in form of legal rules, does exist independently of the DBE, and DBE actors cannot –at least not directly– influence its existence. Furthermore, the DBE environment has to facilitate compliance with compulsory rules: these are not only to be implemented by state organs, but the community bears a responsibility in implementing them.

However, this is not to say that there is no action margin for DBEs to regulate themselves. Section 2.5 deals with the question of what mechanisms and strategies are available to regulate DBEs. Before going into this point, the main features of the most relevant regulatory constraints are going to be presented below, in order to provide a more focussed approach to this complex task.

[46] The SAFS «can generate rules and customs and symbols internally, but (...) is also vulnerable to rules and decisions and other forces emanating from the larger world by which it is surrounded» (Moore 1978: 55).

2.4.2. Law on Intellectual Property Rights

As far as the OPAALS' OKS is concerned, it contains software and intellectual property objects other than software, this subsection deals, first, with options for the legal management of software and, second, with options for the legal management of intellectual property rights other than software.

2.4.2.1. EU Legal Framework on Computer Programs

The Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of **computer programs** does not contribute any definition of these; it considers the program like a literary work, implying that the authors of programs, on the basis of copyright, could arrange the measures that they consider appropriate for the protection of their creations, guaranteeing the rights of third legitimate buyers of such works. Thus, Article 1 of the Directive 2009/24/EC establishes that "[i]n accordance with the provisions of this Directive, Member States shall protect computer programs, by copyright, as literary works within the meaning of the Berne Convention for the Protection of Literary and Artistic Works", expressing Article 4.1 of Directive 2009/24/EC that exclusive rights of the author will include: the right to realize or to authorize the total or partial reproduction of a program of computer for any way and under any form, already it will be permanent or transitory; the translation, adjustment, arrangement and any other transformation of a program of computer and the reproduction of the results of such acts, without prejudice of the rights of the person who transforms the program of computer; any form of public distribution, included the rent, of the program of original computer or of his copies. In consequence, "[t]he [EU]'s legal framework on the protection of computer programs can accordingly in the first instance be limited to establishing that Member States should accord protection to computer programs under copyright law as literary works and, further, to establishing who and what should be protected, the exclusive rights on which protected persons should be able to rely in order to authorise or prohibit certain acts and for how long the protection should apply".

Therefore, the legal framework presented here does not prevent authors from managing software as **open source software** (hereafter, OSS).

2.4.2.2. Licensing Open Source Software

Currently, the license with which a program is distributed delimits exactly the rights that the users have over it. Normally, the conditions of the licenses of **OSS** are the result of an agreement between several aims:

- To guarantee some basic freedoms (of redistribution, of modification, of use) to the users.
- To assure some conditions imposed by the authors.
- To try to guarantee that the derivative works be also OSS.

The concept of OSS is concerned with the freedom of the users to execute, copy, distribute, study, change and improve the software. The users of OSS programs have four **essential freedoms or libertates**:

- Liberate 0: The freedom to execute the program for any intention.
- Liberate 1: The freedom to study how the program works, and to change it. The access to the source code is a necessary condition.
- Liberate 2: The freedom to redistribute copies.
- Liberate 3: The freedom to distribute to third parties copies of its modified versions. The access to the source code is a necessary condition.

A program is OSS if the users possess these four freedoms, being free to redistribute copies, with or without modifications, free of receiving a tariff for distribution, from anyone in any place:

- The freedom to execute the program means the freedom for any person or organisation to use it in any type of system of computation, for any type of work and intention, without obligation to communicate these uses to its programmer, or any other specific entity.
- The freedom to redistribute copies must include the binary or executable forms of the program and the source code, too.
- For these freedoms to be real, they must be irrevocable.

OSS does not mean that it is not commercial: it must be available for **commercial use**, commercial programming and commercial distribution.

The majority of the licenses of OSS are **based on copyright**, and limits exist in the types of requirements that can be based on copyright. Nevertheless, some licenses of OSS are **based on contracts**, and the contracts can impose a much bigger range of possible restrictions.

The more important OSS licenses are shown in the table below:

GNU GPL License	**BSD License**
- "Generic" license. - Holder of the text: Free Software Foundation. - Author preserves the copyright. - Modification and redistribution under the terms of the GNU GPL. - Parts: Headline, Prologue, Content, Application.	- Berkeley Software Distribution. - Author supports the copyright. - Users have unlimited freedom: free redistribution and modification. - Without copyleft. - Parts of the text: Legend Copyright, Content, Limitation responsibility. - It is possible to sublicense: free or exclusive Software.
MIT License	**QPL License**
- Massachusetts Institute of Technology. - Without copyright. - Condition: The note of copyright and rights are included in all the copies or essential parts of the Software. - Rights without restrictions. - It is possible to sublicense: free or exclusive Software.	- Q Public License. - Incompatible with the GNU GPL. - The modifications are distributed separated from the original Software.
MPL License	**Artistic License**
- Mozilla Public License. - It is possible to sublicense. - Incompatible with the GNU GPL. - Modifications must return to the original project. - Any subject that contributes to the source code of the project must resign to any patent right of the source code.	- OSI considers it to be a free Software, but the FSF does not.
APACHE License	**JAVA License**
- Descendant from the BSD. - The developer can do what he wishes with the source code. - The only restriction: Recognition of the developed.	- Special Protection of the language of programming SUN's JAVA Microsystems. - It prevents incompatible extensions from appearing with the language JAVA.
Common Development and Distribution License (CDDL)	**Creative Commons License**
- Published by SUN Microsystems. - Target: To liberate part of the software of JAVA to integrate it with other OSS's tools. - It allows to share the source code with other programs.	- Directed works multimedia. - It prohibits the alteration of the original product and its seller.

2.4.2.3. Protection of Software under the GNU GPL[47] License

Computer programs are considered from a legal point of view as an object of intellectual property, being able to take advantage of all the possible licenses in this matter for their protection.

One of the licenses adapted for the protection of software is the GNU GPL License. It is a license created by the Free Software Foundation, orientated principally to protecting the free distribution, modification and use of software, whose intention is to declare that the software covered by this license is a free software and to protect it from attempts of appropriation that restrict these freedoms for the users.

Developers that use the GNU GPL protect users' rights with two steps: (1) assert copyright on the software, and (2) offer users this license giving authors' legal permission to copy, distribute and/or modify it. For developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

All rights granted under this license are granted for the term of copyright on the program, and are irrevocable provided the stated conditions are met. This license explicitly affirms users' unlimited permission to run the unmodified program. The output from running a covered work is covered by this license only if the output, given its content, constitutes a covered work. This license acknowledges rights of fair use or other equivalent, as provided by copyright law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under Article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures. When authors convey a covered work, they waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this license with respect to the covered work, and authors disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, their or third parties' legal rights to forbid circumvention of technological measures.

Users may convey verbatim copies of the program's source code as users receive it, in any medium, provided that users conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this license and any non-permissive terms added in accordance with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this license along with the program. Authors may charge any price or no price for each copy that users convey, and may offer support or warranty protection for a fee.

The GNU General Public License is often called the GNU GPL for short; it is used by most GNU programs, and by more than half of all free software packages. The latest version is version 3. The GNU General Public License is available in these formats: HTML, plain text, ODF, Docbook, Texinfo, and LaTeX.

2.4.2.4. Other Licenses for Protecting Software

a) *BSD License*.[48] The license BSD is the original license of a distribution of software: Berkeley Software Distribution, who finished turning into a derivative of UNIX realised by the known University of California, Berkeley.

[47] http://www.gnu.org/licenses/gpl.html
[48] http://blackshell.usebox.net

The BSD License has had two forms principally: the classic one (with the clause of advertising), not in force and dissuaded for practical motives, and the current one (without this clause, from July, 1999).

The BSD License has effects very similar to those who are obtained by the MIT License, though the form is totally different. This way, the text differs: conditions, rights and disclaimer.

The part of the rights and the disclaimer must be included in all the redistributions of the source code, and, in case of binary redistribution, it is necessary to include a copy of the license in the distribution.

It is a license that allows the re-use of the software like that licensed as much to be free software as to be exclusive software, due to the fact that it is an allowed sublicense (though it does not say it explicitly, it does not say the opposite either).

The most common software that uses this license generally uses the *BSD variations: FreeBSD, OpenBSD and NetBSD; though there are many more projects.

b) *MIT License*.[49] It is a license from MIT (Massachusetts Institute of Technology).

No copyright is a license, which allows us to modify and adapt to our needs. However this may not be advisable, and even many voices within the Open Source community support this view.

License the text of the three-point difference: conditions, rights and limitation of liability.

The condition is that the copyright notice and the rights included in all copies or substantial portions of the Software. This is the condition that invalidates the license if not satisfied.

The rights are many: no restrictions, including use, copy, modify, integrate with other software, publish, sublicense and / or sell copies of the Software, and also allow people to whom the software is given to do the same.

Finally we have a disclaimer or notice of limitation of liability standard.

With regard to the rights granted, this license allows software to be reused and therefore be licensed as free software or proprietary software. This means that the fact can lead to sub-license to allow a derivative work that is closed, or even under the BSD license, GPL, or any other compatible with the MIT. This can be an advantage, when you make a product that at one point can make a profit by being closed (e.g., dual licensing schemes: we work with MIT for commercial use in exchange for monetary reward and sub GPL for community use), but also a drawback if we want our work to be used in a closed product.

Its application is very simple: you only need to add text to the source code for the license and the year that that code was released and the name of its author (and if possible a contact address or e-mail).

With this license we have Free Software. We may be interested if we have a business strategy based on, for example, dual licensing, if we want our development to become a standard and we want to facilitate its implementation, or just impose that our product be free without further consideration.

There are many examples of software that uses this license: X11, XFree86, Expat or PuTTY.

c) *MPL License*.[50] Mozilla Public License is open source and free software. It was developed originally by Netscape Communications Corporation, a division of America Online, the company, and later control was transferred to the Mozilla Foundation.

The MPL is fully compliant with the definition of OSS, the Open Source Initiative (OSI) and the four freedoms of free software listed by the Free Software Foundation (FSF). However, the MPL leaves

[49] http://www.gnu.org/licenses/gpl.html
[50] http://www.mozilla.org/MPL.

the door open to a possible free software re-use if the user so wishes, without restricting the reuse of code or relicensing under this license.

Although the primary purpose of the MPL license is to serve as control for the Mozilla browser and related software (Firefox or Mozilla Thunderbird mail client, for example), this agreement is widely used by developers and programmers who want to open its source.

It is a free software license, but not a strong copyleft. It has some complex restrictions that make it incompatible with the GNU GPL. In fact, it is not legally possible to bind a module covered by GPL with a module covered by MPL.

However, version 1.1 of MPL has a provision that allows a program (or parts of it) to offer the choice between MPL and other licenses. If part of a program allows GNU GPL or other compatible license as an alternative, that part of the program is compatible with GPL.

d) *Artistic License*.[51] Free Art License grants the right to freely copy, distribute, and transform creative works without infringing copyright, and recognises and protects these rights. Its application has been arranged in order to allow everyone to use the creations of the human mind in a creative manner, regardless of their types and forms of expression.

Public access to creations of the human mind is usually restricted by the application of copyright, which is favoured by the Free Art License. This license is intended to allow the use of the resources of a work, to enable new conditions for creation in order to increase opportunities for creation. The Free Art License grants the right to use a work, and recognises the right holder and user rights and responsibilities.

The main reason for the Free Art License is to promote and protect the creations of the human mind according to the principles of copyleft: freedom to use, copy, distribute, transform, and prohibition of exclusive appropriation.

The purpose of this License is to define the conditions under which one can use this work freely. Through this license the author specifies the extent to which you can copy, distribute, and modify it.

A license is compatible with the Free Art License provided that it grants the right to copy, distribute and modify the copies of the work, including for commercial purposes and with no limitations other than those required for the respect of the compatibility criteria. The compatibility criteria ensure proper attribution to the authors of the work and access to previous versions of the work. They also require that changes made to the work subject to this license or license also meet the criteria of compatibility.

This leave is not to deny the rights of the author in his speech or related rights. By choosing to contribute to the development of this common work, you only agree to grant to others the same rights with regard to their contribution as were granted by this license. Conferring these rights does not mean you have to give up their intellectual rights.

The freedom to run the job as defined by the Free Art License (right to copy, distribute, modify) implies that each individual is responsible for their own actions.

To take advantage of the Free Art License is sufficient to mention the following points in your work: Name of author, title, date of the work. Where appropriate, the names of the authors of the joint work, and, if possible, where to find the originals.

e) *Apache License*.[52] The Apache License is a descendant of the BSD license, allowing users to do whatever they want with the source code (including forks and proprietary products), provided that any changes are recognised.

[51] http://www.opensource.org/licenses/artistic-license-1.0.php.
[52] http://www.apache.org

The Apache Software Foundation uses various licenses to distribute software and documentation, to accept regular Contributions from Individuals and corporations, and to accept larger grants products of existing software.

These licenses help us achieve our goal of providing reliable and long-lived software products through open source collaborative software development. In all cases, contributors retain their full rights to use original contributions for any other purpose outside of Apache while providing the ASF and its projects the right to distribute and build upon their work within Apache.

The license is supposed to be compatible with other open source licenses, while remaining true to the original goals of the Apache group and development supportive of collaborative across both non-profit and commercial organisations. The Apache Software Foundation is still trying to determine if this version of the Apache License is compatible with the GPL.

f) *Common Development and Distribution License* (CDDL).[53] The Common Development and Distribution License, or CDDL is an open source license (OSI) and free, produced by Sun Microsystems, based on the Mozilla Public License or MPL, version 1.1. The CDDL was sent for approval to the Open Source Initiative on December 1, 2004, and was approved as an open source license in mid-January 2005. In the first draft of committee report OSI license, the CDDL is one of the nine popular licenses, widely used or with strong communities.

The previous license used by Sun for their open source projects was the Sun Public License (SPL), also derived from the MPL. The CDDL is considered by Sun to the SPL version 2.

As the CDDL was derived from the MPL, some people claim that the license is not compatible with the GNU General Public License (GPL.) The Free Software Foundation says that this is a free license but is incompatible with GNU GPL mainly due to some details.

2.4.2.5. Protection of the Content other than Software under Creative Commons Licenses

Creative Commons is a non-profit organisation devoted to expanding the range of creative works available for others to build upon legally and to share. The organisation has released several copyright-licenses known as Creative Commons licenses. These licenses allow creators to communicate which rights they reserve, and which rights they waive for the benefit of recipients or other creators[54]. Thus, Creative Commons puts at the disposal of the authors a series of licenses that allow them to authorise diverse uses of their works. The common link to all the Creative Commons' modalities is the respect of the paternity of the licensed work.

Basic licenses of the Organisation Creative Commons[55] are:

			**Attribution (cc by):** This license lets others distribute, remix, tweak, and build upon author's work, even commercially, as long as they credit for the original creation. This is the most accommodating of licenses offered, in terms of what others can do with the works licensed under Attribution.
			**Attribution No Derivatives (cc by-nd):** This license allows for redistribution, commercial and non-commercial, as long as it is passed along unchanged and in whole, with credit.
			**Attribution Non-Commercial No Derivatives (cc by-nc-nd):** This license is the most restrictive of our six main licenses, allowing redistribution. This license is often called the "free advertising" license because it allows others to download author´s works and share them with others as long as they mention the author and link back to him, but they can't change them in any way or use them commercially.

[53] http://www.sun.com/cddl.
[54] Definition of creativecommons.org.
[55] Creactivecommons.org.

			**Attribution Non-Commercial (cc by-nc):** This license lets others remix, tweak, and build upon your work non-commercially, and although their new works must also acknowledge and be non-commercial, they don't have to license their derivative works on the same terms.
			**Attribution Non-Commercial Share Alike (cc by-nc-sa):** This license lets others remix, tweak, and build upon author's work non-commercially, as long as they credit and license their new creations under the identical terms. Others can download and redistribute the work just like the by-nc-nd license, but they can also translate, make remixes, and produce new stories based on the work. All new work based on works will carry the same license, so any derivatives will also be non-commercial in nature.
			**Attribution Share Alike (cc by-sa):** This license lets others share, remix and build upon author's work, the work must be attributed in the manner specified by the author, and if user alters, transforms, or builds upon the work, he/she may distribute the resulting work only under the same or similar license to this one.

Obtaining the license: Once the choice of the type of license is made concrete, one obtains the license adapted for the software expressed in three forms:

1) *Commons Deed:* It is an easily understandable summary of the legal text with the relevant icons.
2) *Legal Code:* The legal complete code on which the chosen license is based.
3) *Digital Code:* The digital code, which is machine-readable and enables search engines and other applications to identify the software and its conditions of use.

Use of the license: Once chosen, the license has to include the button Creative Commons "Some rights reserved" near the work, connecting this button with the Commons Deed, so that all can be informed about the conditions of the license. If it is detected that the license has been violated, it will be possible to defend the rights of the author.

2.4.2.6. Record of the Content of OPAALS's OKS

Intellectual property rights come into effect from the moment of the creation of the intellectual property. For this reason, Records of Intellectual Property have been established that annotate the declaration of the registrant with respect to the authorship and the ownership of the rights related to the registered works, with the purpose of providing evidence against third parties of such a bill of rights.

In consequence, there are Records of Intellectual Property of diverse nature:

- *Public Records.* The inscriptions in these records constitute a proof that at a specific moment in time a certain person registered the work in this place and declared the concrete situation of the rights with respect to the same, having efficiency *"iuris tantum"*, i.e., their efficiency can be challenged by providing evidence that disproves such a presumption; in any case, the burden of the proof falls on the party who challenges the records.
- Private Records as, for example, *Safe Creative's Copyright Registry.*[56]

Safe Creative is a private Register of digital content where users can register their works, establishing a proof of their authorship and copyrights. In accordance with the service's terms and conditions, the user agrees to deposit their works and Safe Creative agrees to watch over the

[56] Safecreative.org

content and information according to the established conditions, publishing and allowing access to that information to any third person, but not allowing any exploitation of such in prejudice of user's rights and interests. Safe Creative becomes a third person that, through computing procedures, stores the content provided by users, allowing the registration of the mentioned information and the time at which it was stored.

The goal of this system is to have a valid evidence to prove plagiarism or an unlawful use of a work. Safe Creative's systems are based on strong technologies that encrypt contents uploaded by its users, adding some timestamps capable of proving the date of the registration, which form a solid structure that can be used in a court to prove the existence of a work before the work of a potential infringer.

In addition, this service has the advantage that it is free, accessible through the Internet, global and neutral, and it allows you to establish and record the right policy or licence of use defined previously by the user.

Safe Creative can issue digital certificates based on the register's data, providing the date of registration, the author or authors and exploitation rightsholders, as much as providing the content and pre-established use policy. These certificates are free and double-signed digitally by the issuer, that is, Safe Creative.

In conclusion, authors who register their work in Safe Creative's Registry have a valid way to prove that some content was created on a certain date, having a certificate issued by a company that has implemented in its systems technologies that are able to prove such statement.

2.4.3. Privacy and Data Protection Law

The functioning of the P2P network in Digital Ecosystems (DE), as well as the functioning of the different services which may be offered in a DE (i.e., Dynamic Service Composition), raises a complex set of questions related to data protection and privacy legislation. In order to address them, an overview of the applicable legal framework is first needed, followed by a specific consideration of the legal issues posed by a DE.

2.4.3.1. EU Legal Framework

Drawing on Article 8 of the European Convention on Human Rights and Fundamental Freedoms and Article 16 of the Treaty on the Functioning of the European Union, a regulatory framework has been established in the EU for the protection of personal information and privacy, as well as for the protection of the confidentiality of communications. A series of Directives have been passed on the basis of these texts which approach the regulation of the processing of personal data in the Information Society, and therefore they must be taken into account in any ICT environment. Although these directives have been largely implemented, further developed and specified at the national level (by internal legislative measures adopted by the different Members States), this document will solely focus on the EU regulatory framework.

The main Directives in this subject-matter are:

a) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
b) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications): It harmonises the necessary regulations of the Members States to guarantee an equivalent level of protection as to the citizen's fundamental rights and freedoms and, especially, privacy and confidentiality, regarding the treatment of personal data in the electronic communication sector, the free traffic of such information and services of electronic communications in the Community.

c) Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.
d) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC: The aim of this Directive is to harmonise the obligations of the suppliers to preserve certain information and to assure that these should be available for the purpose of criminal investigation, detection and prosecution (e.g. serious crimes as they are defined in the national regulation of every Member State, such as terrorism or organised delinquency).

2.4.3.2. Data Protection and Architecture and Services in Digital Ecosystems

The European legislation on data protection aims to protect the personal data[57] concerning users. In this context, the term "users" only applies to individuals or natural persons, whereas in some Member States the scope of national Law on data protection has been broadened to cover legal persons as well.

At this level we shall distinguish three major actors in the field of data protection:

- Data subject: Natural person to whom the data are related.
- Data controller: Responsible for the circulating personal data file of the affected data subject. So, Article 2 (d) of Directive 95/46/EC defines 'Controller' as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.
- Data processor: Actors who intervene when the data controller entrusts their management to a third party. So, Art. 2 (e) of Directive 95/46/EC defines 'Processor' as a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller[58].

After stating these concepts, we can move on to discuss the issue of protection of personal data within the OPAALS environment.

Thus, from the point of view of OPAALS's p2p architecture, the issue of treatment of the data does not give rise to any problem, because the data will simply be stored in a file according to statutory or legal requirements; therefore we must definitely establish and regulate the access to these data and make sure that this access complies with the requirements prescribed by Law.

However, from the point of view of the services that may be offered in the OPAALS environment, i.e., DSC, we must establish some common conditions that govern the traffic of personal data between recipients/users and providers/SMEs operating in the environment.

As has already been said, the object of protection of this legislation is personal data of natural persons or users. Under EU law, these data may be only processed in two cases: when the user has given his/her consent to the processing of data or when there is a statutory or legal authorisation which entitles a controller to process personal information without prior consent. Consequently, in the process of formalisation of the contracts which are entered by means of a DSC (these contracts being the result of business relationships between providers/SMEs and

[57] Definition of personal data in art. 2 Directive 95/46: (a) "'personal data' shall mean any information relating to an identified or identifiable natural person ('data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."
[58] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor".

recipients/users), a privacy policy must be established in order to fully inform users about the processing of their personal data, so that the users have to accept such processing as an essential requirement for the formalisation of the contractual relationship. The clause which etablishes the privacy policy has to provide the information required by Article 10 of the Directive 95/46.[59]

With regard to those data requested from users in the development of the relationship established by means of a DSC, on the one hand, it should be taken into account that only those data that are essential, necessary, relevant and not excessive for the formalisation of contracts entered in DE environment may be collected and processed; on the other hand, the (personal data) file shall be stored for a period which may not exceed the time necessary to fulfill the purposes for which the data were requested (except for Directive 2006/24/EC concerning data retention for the purposes of criminal prosecution and fight against terrorism, etc.).

In this context, the OPAALS Legal Entity (we assume e.g. that it will be an Association under Belgian Law) would take the position of a data processor (on behalf of each single provider or SME), whereas the position of data controllers is going to be taken by the providers/SMEs involved, since these ultimately determine the purpose, content and use of the personal data provided by users/recipients in operations entered by means of a DSC.

In any case, this organisation will have to be reflected in a contract or legal act between both parts, containing at least the requirements gathered in Article 17(3) of the Directive 95/46/EC ("*the processor shall act only on instructions from the controller and the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor*"); such an agreement must be established in writing or in an equivalent form (e.g. an electronic contract)[60]. More precisely, under this hypothesis, providers/SMEs acting in a DSC would have to develop and adhere to an agreement or convention in order to harmonise basic regulatory issues on data protection, i.e., a clause which establishes the common conditions in the processing of user data, regarding the existing regulation referred to above. So, the Convention regulating communications should include clauses referring to the following terms:

[59] Article 10 of Directive 95/46/EC establishes that "[i]nformation in cases of collection of data from the data subject Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:
(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing for which the data are intended;
(c) any further information such as
- the recipients or categories of recipients of the data,
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
- the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject."

[60] Article 17 of Directive 95/46/EC, establishes that "Security of processing:
1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures.
3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:- the processor shall act only on instructions from the controller,- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.
4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form."

- Procedure and conditions for access to data stored in the personal files and protected from users.
- Period of storage (how long will personal data be stored).
- Safety measures concerning the accessibility to personal data (setting password, Record as entrepreneurs or suppliers, etc.).
- Recognition of the responsible person and guarantor of security of the data (Belgian Association) by all adherents to the Convention.
- Other considerations that adherents themselves deem appropriate.

2.4.4. Law on Digital Signature

The Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a *Community framework for electronic signatures* had an essential aim of promoting e-commerce ensuring cross-border system interoperability, and guaranteeing security transactions. For that purpose, the Directive contributed to the regulation of the necessary requirements in order to attribute legal recognition of electronic signatures within the Community, that is, admissibility and effectiveness of the signature as if it had been handwritten. Moreover, the Directive created a European framework for several certification-service providers who must observe data protection legislation and individual privacy to increase the users' confidence in electronic communications and e-commerce.[61]

It should be stressed that the Directive does not address the conclusion and validity of contracts or other legal obligations prescribed by national or Community law regarding the form of contracts. Neither does it affect rules and limitations relating to the use of documents, provided in national or Community law. Consequently, the Directive does not affect national provisions requiring, for instance, the use of paper for certain types of contracts.[62]

The Directive, in Article 2(1), states the notion of electronic signature as data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. From this wide concept, it is possible to distinguish between three levels of electronic signature.

The first level of electronic signature is the simplest one, which is used to identify and authenticate data. It could consist on a password or a code with a personal name. The problem is that this kind of signature does not guarantee the signatory's identity and does not allow you to confirm the veracity of the data either, so its scope is limited.

The second level of signature is named “advanced electronic signature”. Although the Directive is technology-neutral, in practice this kind of signature refers normally to those that are based on a public key infrastructure (PKI) or asymmetric encryption system[63.] This technology uses encryption to sign data, which makes it necessary to have two keys: a public and a private one. The advanced signature is regarded as a “qualified signature” because a) it is uniquely linked to the signatory; b) it is capable of identifying the signatory; c) it is created using means that the signatory can maintain under their sole control; d) it is linked to the data to which it relates in such a manner that any subsequent change in the data is detectable.[64]

Finally, the third form of signature, mentioned in Article 5(1), is known as digital signature or “qualified advanced electronic signature”, in spite of not being mentioned by the Directive with this

[61] See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on tile protection of individuals with regard to the processing of personal data and on the free movement of such data.
[62] Extract from COM(2006) 120 final - Content of the Directive: Aim and scope.
[63] The asymmetric encryption system more common in practice is RSA, created in 1978 by Rivest, Shamir and Adelman.
[64] See Article 2(2) of the Directive.

name. It is an advanced signature based on a qualified certificate and created by a secure signature-creation device. Its effects are stated in Article 5(2) of the Directive, and are: a) the attribution of legal effects as if it were a handwritten signature, and b) the admission as evidence in legal proceedings. However, for doing so it is necessary that the signature fulfil the conditions stipulated in Annexes I, II and III of the Directive, that refer to requirements for qualified certificates, for certification-service-providers issuing qualified certificates, and for secure signature-creation devices, in order to produce these legal effects mentioned.[65]

The conditions enumerated in Annexes I, II and III manage the aim of creating a security architecture in order to protect the network users' communications. This security architecture must be provided with several security services which allow the digital signature to achieve:

- *Message integrity,* because the original data cannot be modified afterwards.
- *Authentication*, the possibility to identify the signatory.
- *Non-repudiation*. The signatory cannot deny to have sent the message, due to the fact that it was created by means which he maintains under his exclusive control.
- *Confidentiality.* The receiver is the only one who can access the message contents.

As was mentioned before, to achieve the above properties requires the adoption of a system of asymmetric encryption, based on a pair of keys (public and private). However, we should point out another problem regarding the existence of this pair of keys: it is necessary to guarantee that the signatory's public key is correlated with the private one. Thus, the technical solution established by the Directive is the participation of *trusted third parties* (TTP), who are considered as trusted entities for the parties involved in the transaction. The essential function of these third parties is the emission of certificates, which allows to connect a person's identity with a public key and, indirectly, with a private one. These certification service providers may incur liabilities if they do not guarantee the system's correct working, precisely because of their position as relaying parties. The Directive establishes in Article 2(9) the notion of certificate: "an electronic attestation which links signature-verification data to a person and confirms the identity of that person". Also, in Article 2(10) the concept of qualified certificate is defined as "certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II". In this case, the certification service providers must be accredited and obey several duties.[66] Indeed, through the qualified certificate issued by accredited certification service providers, it is possible to achieve the highest level of communications security.[67]

The main provision of the Directive states that an advanced electronic signature based on a qualified certificate created by a secure-signature-creation device satisfies the legal requirements

---

[65] See COM(2006) 120 final, 15 March; and see as well Information Processing Systems. OSI Reference model-part II: Security Architecture. ISO/IEC IS 7498-2, Jul. 1988. The security architecture promoted by ISO recommends to use asymmetric encryption system RSA to guarantee the integrity, authentication, non repudiation and confidentiality.

[66] See Annex II - Requirements for certification-service-providers issuing qualified certificates. Although the Directive establishes a wide enumeration of duties, we should emphasize the employing of personal, systems, proceedings, and products that guarantee technical security, confidentiality, invulnerability, and reliability.

[67] See Annex I - respect to the requirements of qualified certificate, they must in particular include:
- An indication that it is issued as a qualified certificate;
- the identification of the certification service provider;
- the name of the signatory;
- provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
- signature-verification data corresponding to signature-creation data under the control of the signatory;
- an indication of the beginning and end of the period of validity of the certificate;
- the identity code of the certificate;
- the advanced electronic signature of the issuing certification service provider.

The certificate must also be issued by a certification service provider which meeting specific requirements laid down in the Directive.

of a signature in relation to data in electronic form (integrity, authentication, non repudiation, and confidence) in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data. And it is also admissible as evidence in legal proceedings. Then, the conditions are:

- To be an advanced electronic signature.
- To be based on a qualified certificate.
- To be created by a secure-signature creation device.

It is certain that an advanced signature which fulfils these last conditions is safer than others, but also it is more expensive in terms of costs[68] and liability.[69]

2.4.5. Law on Trade Marks and Domain Names

2.4.5.1. EU Trade Mark

Apart from the national trade marks, there are two different ways to obtain protection for a trade mark in the EU:

a) *A Community trade* mark, an exclusive right that protects distinctive signs, valid across the EU, registered directly with Office for the Harmonisation of the Internal Market (OHIM) in Alicante, in accordance with the conditions specified in the Community Trade Mark (CMT) Regulations.

b) *An international trade mark designating the European Community*, likewise an exclusive right but administered by the International Bureau of the World Intellectual Property Organization (WIPO) in Geneva according to the Madrid Protocol. WIPO processes the application and then sends it to OHIM for examination according to the conditions specified in the CTM Regulations. This has the same effect as applying directly for a Community trade mark

c) *Community Trade Mark in detail*. The CTM system is based on a 'basic Regulation' of the Council of the European Union (Council Regulation (EC) No 207/2009 of 26 February 2009 on the Community trade mark) (the "CTMR")[70], and also on various Commission Regulations.

>> *Persons who can be proprietors of Community trade marks*: Any natural or legal person, including authorities established under public law, may be the proprietor of a Community trade mark (Article 5).

>> *Signs of which a Community trade mark may consist:* A Community trade mark may consist of any signs capable of being represented graphically, particularly words, including personal names, designs, letters, numerals, the shape of goods or of their packaging, provided that such signs are capable of distinguishing the goods or services of one undertaking from those of other undertakings (Article 4). Trade marks are words, logos, devices or other distinctive features which can be represented graphically. They can consist of, for example, the shape of goods, their packaging, sounds and smells

Only if a trade mark for goods or services is registered in accordance with the conditions contained in this Regulation and in the manner herein provided is it hereafter referred to as a Community trade mark (Article 1).

>> *Registration process:* A Community trade mark shall be obtained by registration. It is possible to follow different steps in order to obtain the registration:

---

[68] See Annex II, where it is stipulated the special duties of accredited certification service providers.

[69] Not only they could incur special liabilities stated in Electronic signatures Directive, but also liabilities established in Electronic Commerce Directive, because certification' services are considered as information service society.

[70] This is the last versión of the basic Regulation on CTMR. Before the CTM system was based on a basic Regulation' of the Council of the European Union (EC) No 40/94 of 20 December 1993 on the Community trade mark)

1- Filling a CTM application:

a. *Who is the person capable of filling a CTM application?* See Article 5 (above).

b. *Where?* Directly with the Office for Harmonization in the Internal Market (trade marks and designs), established in Alicante, or with the central office of a Member State or with the Benelux Trade Mark Office, with that office, subject to payment of the application fee within a period of one month of filing the abovementioned documents. After one month has lapsed and the fee is not satisfied, the Office will understand that the person withdraws the application.

c. *Minimum requirements:* Community trade mark applications may be filed online, by fax or by mail. A form is available for CTM applications made by fax or by mail.

There is a minimum set of requirements to register a trade mark (Article 26). These requirements are specified as a 'basic Regulation' of the Commission (CTMIR)[71].

- Name and address of the applicant (rule 1 CTMIR)
- Indication of the first and second language (rule 1 CTMIR)
- A representation of the trade mark (rules 1 and 3 CTMIR)
- A list of goods and services for which the mark is to be registered (rules 1 and 2 CTMIR which submit to "The Nice Agreement Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks")[72]
- Payment of the fees (rule 4 CTMIR which submits to Commission Regulation No 2869/95 of 13 December 1995 on the fees payable to the Office for Harmonization in the Internal Market)
- Signature

d. Which language must be used? (Article 115 CTM)

e. When is the application effective? Since the Office grants the filing date when the application meets the minimum requirements. Thus, the Office will conduct a formalities examination, which includes checking the signature, languages, owner and/or representative data, priority and/or seniority claims. If at any stage of the examination process a deficiency is detected, an objection letter will be sent to the applicant to remedy the application within two months. If the deficiency is not remedied, the application will be provisionally refused or, if the deficiency concerns a priority or seniority claim, the claim will be refused.

Also, the absolute grounds for refusal will be analysed (Article 7). In that case, the Office will refuse the trade mark as a sign because it understands that the sign does not satisfy one of the two essential conditions: it can not be represented graphically or it is not suitable for distinction. If the CTM application is refused, it will not be published.

2- Publication: Once the CTM application is accepted, it will be published in Part A of the Community Trade Marks Bulletin. Publication takes place as soon as the national office and OHIM search reports have been issued to the applicant.

[71] Commission Regulation (EC) No 2868/95 of 13 December 1995 implementing Council Regulation (EC) No 40/94 on the Community trade mark

[72] The Nice Classification is based on an agreement administered by the World Intellectual Property Organization namely, "The Nice Agreement Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks". It is intended to help with classifying each good or service for which protection is sought by the trade mark by clearly indicating its nature. The goods and services should, as far as possible, be grouped according to the classes of the Nice Classification. When required, the Office will propose an amended classification.

The publication of the application in Part A of the Bulletin opens the three month period for filing an opposition.

3- Searches: Following the examination of the Community trade mark application, a search report is produced by the OHIM and national offices which participate in the national search system (Article 38 CTM). The purpose is to find prior trade marks which could conflict with the new CTM application.

A Community search report is drawn up from the OHIM's database. Proprietors of the earlier CTM applications or registrations cited in this report are informed by letter about the new application after its publication. This is called a "surveillance letter". In parallel, the OHIM requests the production of national search reports from the relevant participating national offices.

The results of the search reports as well as the surveillance letters are "for information" only. The search reports are meant to give the applicants the possibility of withdrawing their applications after analysing the report's contents. The surveillance letters inform proprietors about new, similar trade marks and they can then decide whether or not to file an opposition.

4- Community search report: This report is drawn up from the OHIM's database of prior CTM applications and registrations taking into account the filing date and priority date, the trade mark name, the figurative elements of the mark and the classes of goods and services according to the Nice Classification.

5- Opposition: 'Opposition' is a procedure that takes place before OHIM when a third party requests the Office to reject a Community trade mark application. Once published there is a three-month opposition period. If no oppositions are filed during this period, the application proceeds to registration.

In general terms, an opponent must have rights in an earlier trade mark or other form of trade sign. The grounds on which an opposition may be made (called 'relative grounds for refusal') are indicated in Article 8 of the Regulation. For an opposition to be successful, the trade mark applied for must be found to be incompatible with such rights. Any proceedings start with a period during which parties can negotiate an agreement, the so-called "cooling-off" period. During this period the parties are given the possibility of terminating the proceedings without incurring additional costs.

The decision of the Opposition Division is subject to appeal by any of the parties. The appeal is decided by OHIM's Boards of Appeal. A further appeal can be made to the Court of First Instance of the European Communities (CFI) and ultimately to the Court of Justice of the European Communities (ECJ).

6- Registration: An application will be registered when the following conditions have been met:

- The examination of the trade mark has raised no objections or the objections raised have been waived; and
- Either no opposition has been filed, or any filled oppositions have been rejected.

7- Publication: The registered trade mark will be published in Part B of the Community Trade Marks Bulletin, and OHIM will then issue the registration certificate.

The rights conferred by a Community trade mark prevail against third parties from the date of publication of registration of the trade mark.

Once published, a CTM:

- Is valid in the European Union as a whole. It is not possible to limit the geographic scope of protection to certain Member States.
- Is valid for 10 years and can be renewed indefinitely for periods of ten years.

- Confers on its proprietor an exclusive right to use the trade mark and to prevent third parties to use, without consent, the same or a similar mark for identical or similar goods and/or services as those protected by the CTM.

>> *Fees:* Applications may be filed either directly with OHIM in Alicante or via national industrial property offices. The minimum cost of registering one Community trade mark is EUR 900 to file online (e-filing) or EUR 1050 if it is used the paper form.

Comparison: CTV vs International Mark[73]

Legal and practical differences between routes	**Direct CTM**	**IR designating the EC**
Persons who can be proprietors	Art. 5 CTMR Any natural or legal person	Art. 2 (1) (i) MP National of a Contracting State, or domiciled in a contracting State or having an effective industrial or commercial establishment in a Contracting State of the Protocol
Languages	Art. 119 CTMR - 1st from the official languages of the EC; - 2nd from the 5 of OHIM (and different from the 1st) *	Art. 145 CTMR, R 126 CTMIR, R. 9 (5)(g)(ii) CR - 1st language = language of the IA which is always a language of OHIM; - 2nd from the 4 remaining languages of OHIM
Translations of list of goods and services	Art. 120, 121 CTMR, R. 85 (5) CTMIR In all official languages of the EC	Art. 152 CTMR Re-publication in Part M1 limited to Class numbers, no multilingual elements re-published and no translations needed
Priority	Art. 29 CTMR, R. 6 CTMIR A priority claim can be made in the CTMA or within a two-month period of the filing date	Art. 4 (2) MP, R. 9(4)(a)(iv) CR A priority claim (normally of the basic application) can be made at the moment of filing an international application
Seniority	Art. 34, 35 CTMR, R. 9 CTMIR At the moment of filing or within 2 months thereof. Seniority can also be claimed after registration of the CTM	Art. 34, 35 CTMR, R. 9 CTMIR At the moment of filing or within 2 months thereof. Seniority can also be claimed after registration of the CTM
Fees	Art. 2 CTMFR Paid in Euros to OHIM, EUR 900 to file online (e-filing) or EUR 1050 if you use the paper form	Art. 8 MP, Art. 11, 13 CTMFR Paid in Swiss Francs to the IB (sometimes possible through the office of origin as well) of : - 1311 SFR the equivalent of EUR 870 -
Professional representation	Art. 92-93 CTM	R. 108(2), 112 (1), 114 (4) CTMIR Rules apply in case a direct communication with OHIM is needed or in case of provisional refusal
How to file?	R. 80, 82, 83 CTMIR - forms mailed, faxed, delivered in situ - e-filing	R. 9(2)(a) CR WIPO MM2 or MM3 Forms sent - through an office of origin for IAs; - through the office of the Contracting Party or directly to WIPO in case of subsequent designation under the Protocol Means (mail, fax) according to OHIM's rules

[73] Extract from www.oami.europa.eu

Where to file?	Art. 25 CTMR - at OHIM; - at a national offices of an EU Member State, including Benelux	Art. 2(2) MP, R. 1 (xvi) CR - through an Office of Origin
Time limits for examination	No time limit for AG and RG examination	R. 112 (5) CTMIR, Art. 5 (2) (b) MP - 6 months for AG; - 18 months maximum for issuing provisional refusal on any grounds
Classification	Art. 28 CTMR, R. 2 CTMIR Examined by OHIM	R. 9 (4) (a) (xiii), 12, 13 CR Examined by the Office of Origin and the IB, accepted by OHIM
Formalities	Art. 36 CTMR, R. 9 CTMIR Examined by OHIM	Art. 3 MP, R. 9 CR Examined by the Office of Origin (not necessarily same typology of marks for example)
Absolute grounds examination	Art. 37 CTMR, R.11 CTMIR Ends by the publication of the CTMA in Part A of the Bulletin for opposition purposes	Art. 154 CTMR, R. 112-113, 116 CTMIR 6-month period to examine AG starts by re-publication in Part M of the Bulletin of the IR designating the EC. Ends by the sending of a first Statement of Grant of Protection or a Provisional Refusal on AG
Relative grounds examination	Art. 41- 42 CTMR, R. 15- 22 CTMIR - 3-month opposition period only opens as from publication of the CTMA if and when it has been accepted on AG - Proof of use: 5 years counted back from the publication of the CTMA for opposition	Art. 156 CTMR, R. 114-115 CTMIR - Fixed period to oppose from month 6 until month 9 of the first republication. Provisional refusal sent to WIPO based on existence of admissible opposition. Then, no difference in opposition procedure compared to direct route (except withdrawal of the IR done before the IB). - Proof of use: 5 years counted back from the opening of the opposition period (6 months after the first re-publication of the IR designating the EC)
Publication	Art. 39 CTMR, R.12, 84 and 85 CTMIR CTM Bulletin: - Part A, CTMA (applications) - Part B, CTM (registrations)	R. 32 CR, Art. 152 CTMR - International Gazette (seniority details and refusals are only published there); - CTM Bulletin Part M at 2 different moments (second language only published there)
Rights conferred against third parties	Art. 9 (3) CTMR From the date of publication of the registration of the CTM - Reasonable compensation for matters arising after the publication of the CTMA in certain cases	Art. 151 (3) CTMR - From the date of the second re-publication of the IR designating the EC in the Bulletin - Reasonable compensation for matters arising after the first re-publication of the IR designating the EC in the Bulletin
Register, recordals and certificates of registration	Art. 120 CTMR, R. 24, 84 CTMIR CTM Register kept by OHIM	Art. 5 ter, 9 bis MP, R. 14 CR International Register kept by the IB
Inspection of files	R. 89 (2) CTMIR Inspection after publication of CTMA	R. 89 (2) CTMIR Inspection after re- publication of IR (before AG examination)
Use requirements	Art. 15, Art. 42 (2,), Art. 51 and Art. 57 (2) CTMR 5 years from Registration Date	Art. 160 CTMR 5 years from the date of the second re-publication

Dependence	N/A	Art. 6 (3) MP Dependence between the IR and the basic mark during 5 years from the date of the IR
Conversion	Art. 112 CTMR - conversion into national marks	Art. 159 CTMR, R 122, 123 CTMIR, Art. 2 (20) MP, R. 24 (2)(a)(ii), (6), (7) CR - conversion into national marks; - "opting back" into designations of Member States
Division	Art. 44, 49 CTMR, Rule 13a, 25a CTMIR Possibility of division of the CTMA or of the CTM	N/A

Abbreviations:
AG =Absolute grounds for refusal
Art. =Article
CR = Common Regulations
CTM = Community Trade Mark
CTMA = Community Trade Mark Application
CTMFR= Community Trade Mark Fee Regulation
CTMIR = Community Trade Mark Implementing Regulation
CTMR = Community Trade Mark Regulation
EC = European Community
EN = English
EU = European Union
FR = French
IA = International Application
IB = International Bureau
IR =International Registration
MP = Madrid Protocol
MS = Madrid System
NA = Non Applicable
OHIM = Office for Harmonization in the Internal Market
RG = Relative grounds for refusal
R. = Rule
SP = Spanish

Application of the Nice Agreement Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks to OPAALS Trade Mark. Regarding the kind of services which has been developed during the Project and the future perspectives, it shall be applied for Classes 42 and 35.

CLASS 42

- Scientific and technological services and research and design relating thereto;
- Industrial analysis and research services;
- Design and development of computer hardware and software.

Explanatory Note
Class 42 includes mainly services provided by persons, individually or collectively, in relation to the theoretical and practical aspects of complex fields of activities; such services are provided by members of professions such as chemists, physicists, engineers, computer programmers, etc.
This Class includes, in particular:
• the services of engineers who undertake evaluations, estimates, research and reports in the scientific and technological fields;
• scientific research services for medical purposes.
This Class does not include, in particular:
• business research and evaluations (Cl. 35);
• word processing and computer file management services (Cl. 35);

• financial and fiscal evaluations (Cl. 36);
• mining and oil extraction (Cl. 37);
• computer (hardware) installation and repair services (Cl. 37);
• services provided by the members of professions such as medical doctors, veterinary surgeons, psychoanalysts (Cl. 44);
• medical treatment services (Cl. 44);
• garden design (Cl. 44);
• legal services (Cl. 45).

CLASS 35

- Advertising;
- Business management;
- Business administration;
- Office functions.

Explanatory Note
Class 35 includes mainly services rendered by persons or organizations principally with the object of:
1. help in the working or management of a commercial undertaking, or
2. help in the management of the business affairs or commercial functions of an industrial or commercial enterprise, as well as services rendered by advertising establishments primarily undertakingcommunications to the public, declarations or announcements by all means of diffusion and concerning all kinds of goods or services.
This Class includes, in particular:
• the bringing together, for the benefit of others, of a variety of goods (excluding the transport thereof), enabling customers to conveniently view and purchase those goods; such services may be provided by retail stores, wholesale outlets, through mail order catalogues or by means of electronic media, for example, through web sites or television shopping programmes;
• services consisting of the registration, transcription, composition, compilation or systematisation of written communications and registrations, and also the compilation of mathematical or statistical data;
• services of advertising agencies and services such as the distribution of prospectuses, directly or through the post, or the distribution of samples. This Class may refer to advertising in connection with other services, such as those concerning bank loans or advertising by radio.
This Class does not include, in particular:
• services such as evaluations and reports of engineers which do not directly refer to the working or management of affairs in a commercial or industrial enterprise.

ONLINE www.oami.europa.eu we can access to EUROACE and EURONICE, two databases which includes the specific class for the products or services to register. In this way applicants can be sure that the Office will raise no objections on classification therefore greatly reducing the time required to process an application as there will be no need for correspondence. All terms in EUROACE correspond to the 9th edition of the international classification of goods and services established by the Nice Agreement

- Class 42 → *"Computer software design, computer software maintenance, updating of computer software."*
  Or
- Class 42 → : "*Construction of frameworks (computer software) and the creation of architectures for computer software systems*."

Even, it could be pointed out another class referred to e-commerce through DSC:

- Class 35 → "*e-commerce services*".

If it is filled an application for Community collective trade mark for the Association the cost will be 1.800 euros.

2.4.5.2. Transfer of Domain Names

During the Project, some of its members have registered on their own favour domain names related to the acronym "OPAALS". At the end of the Project, such domain names shall be transferred to the Legal Entity resulting from it.

The different regulation of the domain name establish rules which allow holders to pass on their domain names to other people or organisations. The transfer can be made by the current domain name holder or by an Internet Service Provider on behalf of the holder.

As mentioned above, currently there are several OPAALS domains registered under different authorities. These domain names will be transferred to the OPAALS Legal Entity, which will become their new holder, as a part of their contribution to the foundation of such a Legal Entity.

The foundation members of the Association have registered the followings domains:

Owner	Domain Name	Rules for Transfer
LSE	opaals.eu	http://www.eurid.eu/en/eu-domain-names/trades-transfers
	opaals-oks.eu	http://www.eurid.eu/en/eu-domain-names/trades-transfers
Techideas	opaals.org	http://www.icann.org/en/transfers/policy-12jul04.htm
Thomas Kurz	opaals.at	http://www.nic.at/en/service/modification/
Ossi Nykänen	opaals.fi	https://domain.ficora.fi/fidomain/aca.aspx
Anne English Consulting Ltd	opaals.ie	http://www.domainregistry.ie/TransferBillingContact.php
IPTI	opaals.org.br	http://www.icann.org/en/transfers/policy-12jul04.htm

2.4.6. Company and Association Law

As already pointed out, one of the questions to be solved by the OPAALS Community is the legal form or structure which it will take on. The choice of legal form, in turn, implies basing or locating the OPAALS Community, and as part of it, the DBE Community, as a **legal entity** in a certain territory, and therefore under a certain jurisdiction or legal order –for the sake of argument (but also for practical reasons), we assume that the DBE will be based in Europe and will act under EU Law.[74] Already this may constrain the regulatory freedom of the DBE Community –to give just an example: If it takes the legal form of a European Economic Interest Group (EEIG),[75] each member of the group could be held individually liable for the actions of the DBE. Just to name some other options, an OPAALS Legal Entity could take on the form of a civil or unincorporated association, a registered company, a partnership or even an association (or European association), as well as a number of (EC) corporate structures, too. This question is dealt with below, in subsections 3.1.6 and 3.2.

[74] Both national and international law (international treaties and bilateral agreements) will be left aside here.
[75] See European Council Regulation (EEC) No 2137/85.

2.4.7. e-Commerce and Information Society Services Law

Apart from the question regarding the choice and configuration of the legal entity for the OPAALS Community, a further important question that should be considered, when analysing the legal duties and liability issues on DE, is the European legal framework on e-commerce and information society services, as far as the OPAALS Legal Entity and the members of the OPAALS Community (and DBE Community) can be qualified as **Information Society Services Providers**. As already pointed out in Subsection 2.1, a DE is a specific technological infrastructure that combines a digital environment and several digital components (e.g. software, business models, contractual framework...).[76] Inside this infrastructure, it could be possible to add one of its most striking features, i.e., DSC.[77] The DSC needs to be based on a specific technical infrastructure for its functionality, and this kind of infrastructure is available in DE. In fact, DSC requires 1) the implementation of a *peer to peer platform* (P2P), for which each agent can be both provider or client; 2) an *interface* capable of transforming the contract language to XML language (legalXML e-contract); and 3) a *platform integrated finder* that enables a search for different information. Thus, addressing these requirements, it could be possible to apply specific European legislation, particularly, the Directive 2000/31/EC of the European Parliament and of the Council: the European Directive on Electronic Commerce ("e-Commerce Directive"). This question is dealt with below, in Subsection 3.2.8.

2.4.8. Fair Trade and Competition Law

Before dealing with regulation strategies, the treatment of DBE in the framework of Fair Trade and Competition Law deserves special consideration . As pinpointed above, and regardless of the existence of a legal entity, DEs – and especially DBE – can be considered as markets for Information Society Services. This facet of DBE raises the issue of its analysis from a Fair Trade and Competition (Antitrust) Law point of view[78]. Focusing on the last one, in an EU context, all regulatory and governance decisions shall comply with Art. 101 et seq. of the TFEU and the rest of primary and derivative EU provisions in this field of Law. Therefore, one of the first issues that shall be considered is, if DBE has to be regarded as a separate market in order to be assessed for Competition Law purposes; the consideration of DBE as an innovative market[79] could be relevant. This is a very important point to determine the effect, i.e., of the ***de minimis* rule** in such an assessment, specially relevant as far as SMEs are going to be the principal agents in DBE and this can represent a big advantage in order to work together in a business environment. But probably the most relevant aspect to be analysed is the impact of changing the pattern to a **collaborative competition approach**: potential competitors will collaborate in the development of their business; at least, they will exchange information, in order to provide services in a common frame. For the same purpose, they might achieve horizontal agreements establishing minimal standards for the services offered in the DBE, which can be necessary in order to enable their respective business. All of this can restrict competition. However, the question is, if, despite that, such agreements can be assessed positively ex Art. 101 (3) TFUE due to of the advantages of operating in the DBE for all agents concerned.

[76] See Deliverable 6.9: (7.1) Digital Ecosystems Regulation and IS Law, OPAALS.

[77] It could be defined as an electronic process of creating new services from a set of service component, supporting business agility, flexibility and availability", extract from "*Dynamic Service Composition and Its Applicability to E-Business Software Systems – The ICARIS Experience* (2000)". Vladimir Tosic, David Mennie, and Bernard Pagurek. Department of Systems and Computer Engineering, Carleton University.

[78] In this sense, Couto Calviño (2008: pp. 13-23), who pinpoints that Antitrust Law has just paid attention to basic Information Society Services as access to internet mainly linked to the regulation on telecommunications. However, new focussing is coming up; i.e., dealing with the questions which rise in the context of internet and selective distribution – as example, see Fuentes Naharro (2010).

[79] See Glader (2006).

2.5. Choosing Regulatory Strategies for DBE

Generally speaking, all approaches to Internet-related regulation share a common starting point: the **shortcomings of state and command-and-control regulation** when it comes to steer digital environments. In other words, the traditional states´ strategy of regulation comes to a head in these environments.

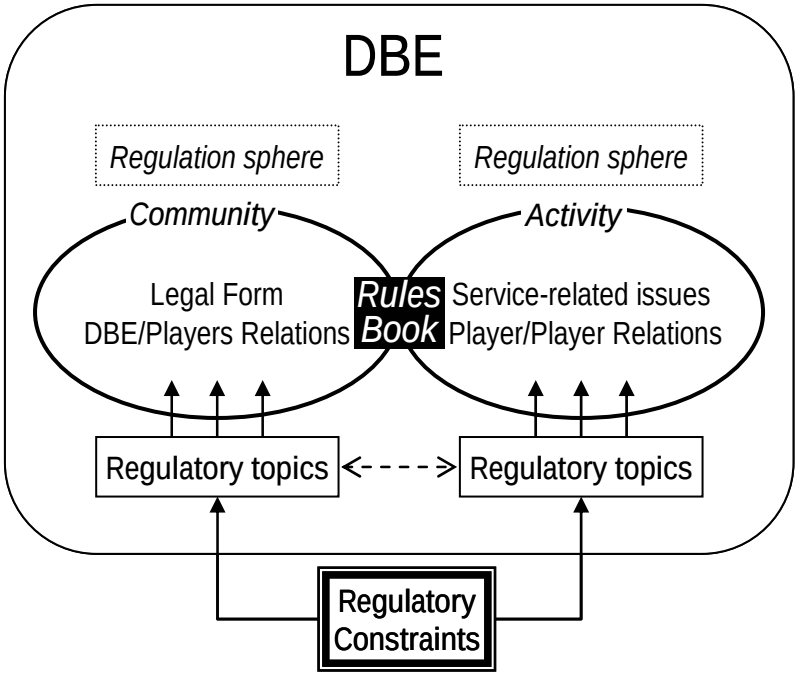

Figure 7: Completing the basic structure of the Map of DBE Regulatory Issues with Legal Framework and Regulatory Strategy

In an attempt to surmount these limits, **'new' regulation models** –which had been already applied to face regulatory crises in welfare states (e.g., responsive and reflexive regulation models)– have been adopted,[80] and specific regulatory tools have also been launched for the Internet and IST-related environments.[81] If states are not able to meet regulatory needs in digital environments, at least **a combination of state and non-state regulatory tools seems to be required**. This holds for our case: DBE can be regulated only on the basis of a complex regulatory strategy which integrates different instruments. Discussions on regulation are not only important to DBE participants (DBE-internal regulatory debates), but also to governments or political institutions involved in IST regulation (DBE external regulatory debates),[82] and any DBE regulatory scheme will have to rely on a combination of internal and external regulatory tools[83], which are

[80] See, among many others, Teubner 1986; Baldwin 1997; Black 1998, Griffiths 2003; Nonet & Selznick 1978; Ayres & Braithwaite 1992; Black & Baldwin 2008.

[81] See e.g. Holznagel & Werle 2002; Farrell 2002; Mifsud 2008; Koops et al 2006; Bennet & Raab 2003. As Reidenberg (1996) early observed, the Internet challenges classic patterns of regulation, not only as for who are the rule makers, but also as for the instruments used to set, implement and enforce rules.

[82] Koops et al. (2006) suggest the following starting points for regulating ICT-environments: technological neutrality of regulation, equivalence principle (*what holds off-line, should also hold on-line)*; active involvement of social and private actors (through *self-regulation* and *co-regulation*), regulation-by-technology, and regulative internationalisation and harmonisation.

[83] Alternative modes of governance such as co-regulation and self-regulation must be seen as a part of a new regulatory policy aiming to increase the transparency, effectiveness and legitimacy of EU action. See *EU White Paper on European Governance* COM (2001) 428 final.

going to integrate a **DBE Rules Book.** This kind of approach may be seen as an expression of **Legal Pluralism** or, to put it in other terms, as an instance of **Mesh regulation**.

In order to lay out such a Rules Book one should keep in mind that, although community and activity spheres can be separated for analytical purposes, they remain intertwined to some extent. This is the case here as the Rules Book must connect regulation in both spheres, and entail a systematic and coherent set of norms governing DBE. In other words, it shall operate as an interface between community and activity regulation and express the intertwinement of social and technological regulation; for it, the book will contain both rules related to social behaviour within the community and design or architecture features defining the very DBE technical infrastructure.

Regarding the community regulation sphere and regulatory topics, the key aspect is probably what can be called the *DBE access contract,*[84] which must cover admission, membership, participation and exclusion conditions.[85] It is plausible that one of the central conditions that players are expected to accept when accessing DBE is compliance with the rules governing the DBE internal interactions, which leads to the sphere of DBE activity regulation. As for the first set of rules governing DBE activities, second-order contract rules are to be laid down in the Rules Book.

It must be considered, too, that, in principle, DBE constitutional and organisational settings (*DBE community* regulation) are irrespective of the specific interactions carried out within it –be they contracts, information exchanges or any other type of interaction–, that seems to require a dedicated regulatory framework (*DBE activity* regulation). However, they will normally overlap to a certain degree. For instance, a general ADR model could be launched for solving any dispute arising within the DBE, be that related to the community itself or to an activity.

A tentative scheme could be as shown in Figure 8.

Here, we will analysed four regulatory instruments, which are at the forefront of both theory and practice, and have been successfully used to regulate digital and ICT-related environments similar to DBE (at least in certain aspects), such as virtual communities and social networks, e-business platforms and digital marketplaces:

- Self-regulation and Co-regulation.
- Alternative and On-line Dispute Resolution (ADR/ODR) Tools.
- Hinge-Law or Hybrid Law Solutions.
- *Lex informatica*, Regulation-by-Technology and “Code as Law”.

[84] The term is borrowed from Rodríguez de las Heras’ (2005: p. 231-32) study on e-Marketplaces.
[85] This is closely related to governance issues. See Wallentin et al. (2005: p. 24 ff.) on VPCs.

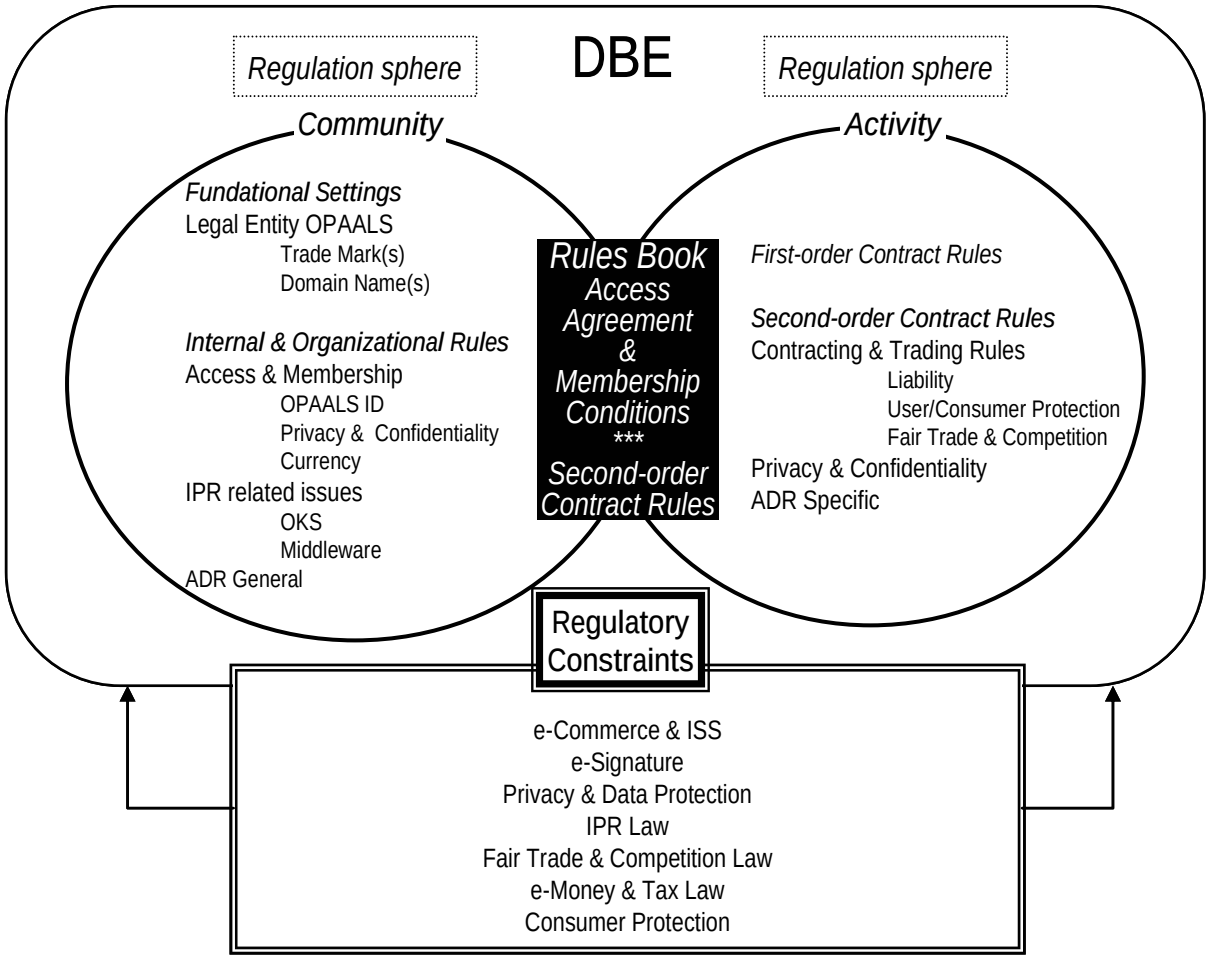

Figure 8: Tentative classification of Regulatory Topics, Regulatory Constrains and Rules Book

2.5.1. Self-regulation and Co-regulation

Self-regulation is deeply rooted in society (in a commercial context, see Uría/Menéndez 2006, p. 53-54). This is clearly shown by the so called **"Customary Law"** in the case of continental or civil Law systems (as opposed to Anglo-American or Common Law systems).

In this context, **"custom"** means a behaviour that is generalised, repeated and uniformly observed in a social community determined either geographically or by another relevant feature (as profession or activity). The members of such a community consider such conduct as juridically binding, i.e., its observance relies on being it of a legal nature (Lacruz 2002: p. 154). As the Spanish Supreme Court has said it is a rule that is established by the social consciousness by means of the repeation of the conduct performed with juridical purpose (Decision of April 18, 1951). Such a conduct is recognised by state institutional regulation (at the present time, only for ruling relations between persons acting as private parties; i.e., Art. 1 of the Spanish Civil Code and Art. 2 of the Spanish Commercial Code) as a source of Law. Nevertheless, the external and internal requirements needed to qualify a conduct as a piece of Customary Law (time and geographical requirements, uniformity, collective *opinio iuris*) make of Customary Law a very rare law today, because of the broad geographical dimension of communities and their quick evolution.

Thus, and as a contemporary adaptation of the fundamental idea of Customary Law, **Self-regulation** has evolved in recent decades as a legal and theoretical concept defining the capacity of a given social field, sector, area or community to establish its own rules. More accurately, self-regulation is a (process leading to establish) a set of norms voluntarily developed and accepted by those who take part in a certain social activity or interaction area (Trudel 2000: p. 204). In this

sense, it is an interesting means to govern social areas in which rules and practices can be well-established with little (or even without) state intervention, such as the Internet as a whole and, more concretely, the field of e-commerce.[86]

The key idea is that Law cannot be imposed from outside, but must be acknowledged by those agents operating in the social field which they are expected to regulate. Self-regulation, however, has many faces, and several types can be distinguished, e.g., according to rule-making procedures, degree of state intervention or enforcement tools.[87] Only two approaches to self-regulation will be touched upon here.

Following the first one, self-regulation is any (institutionalised) process by which a given social agent (or a group of them), normally a collective agent, establishes rules governing its own activity or parts of it without state intervention. Leaving aside Public Law (e.g., Criminal and Tax Law) constraints, the private ruling power is almost unrestricted.

This way of understanding self-regulation, which was in former years deemed typical for Anglo-American countries, is not fruitful for DBE regulation purposes. In our view, self-regulation does not equate to any social or private standard, but rather implies some sort of legal or state control. State Law provides the basis for social groups to create substantive rules and norms in a self-regulative process, that is, it regulates social self-regulation.

This approach is usually referred to as **co-regulation or regulated self-regulation**, and it exhibits almost a worldwide trend.[88] The aim is to structure social systems by providing procedures in which they can regulate themselves and on certain occasions by establishing minimum compulsory legal contents and requirements. In either case, private regulative schemes are supposed not to merely express the interests of single enterprises, associations or sectors –as it may happen if regulation is by and large left to the private sector, which is often defined as self-regulation– but to convey a certain social legitimacy and consensus. The EU directives have resorted to this strategy to facilitate regulation in many fields.

This is a regulatory strategy followed by State Members, too. Such is the case of **Spain**. As an example for such development we must point to Art. 18 of the Spanish Act No. 34/2002, on July 11, 2002, on Information Society Services and Electronic Commerce (LSSICE), which implements the e-Commerce Directive. Co-regulation is regarded as the better way to achieve a sectorial adaptation and application of the general rules on e-Commerce established in the Act. Art. 18 itself identifies as regulatory issues the detection and withdrawal of unlawful content, spam protection and ADR, and special consideration of the protection of human dignity and minors is requested. The legislator's vision is that such regulatory activity will be promoted by the Public Administrations, developed by the ISS provider associations with the participation of the ISS recipient associations, especially consumer associations.

The Spanish legislation gives a new and more general impetus to co-regulation in the new Arts. 37-30 of the Spanish Fair Trade Act (December 2009). Nevertheless, co-regulation is to a large extent an unknown regulation strategy in continental Law States, and the absence of such a tradition is a serious obstacle for a satisfactory function of co-regulation; this can be observed in the case of the Spain, as the *Public Trust Seal*[89] created by the Public Administration has shown little success. The legal culture factor must be regarded in deciding the use of this regulatory strategy.

[86] A detailed analysis of Internet-related self-regulation can be found in Mifsud 2008.

[87] See for instance Mifsud 2008; Darnaculleta 2005; Esteve 2002; Baldwin & Cave 1999.

[88] «As ICT law advances through the years, a gradual increase can be discerned in preference for co-regulation» (Koops et al 2006: p. 123).

[89] "*Distintivo Público de Confianza en los Servicios de la Sociedad de la Información y de Comercio Electrónico*", created in 2004 and regulated, at the present moment, by Royal Decree No. 1163/2005.

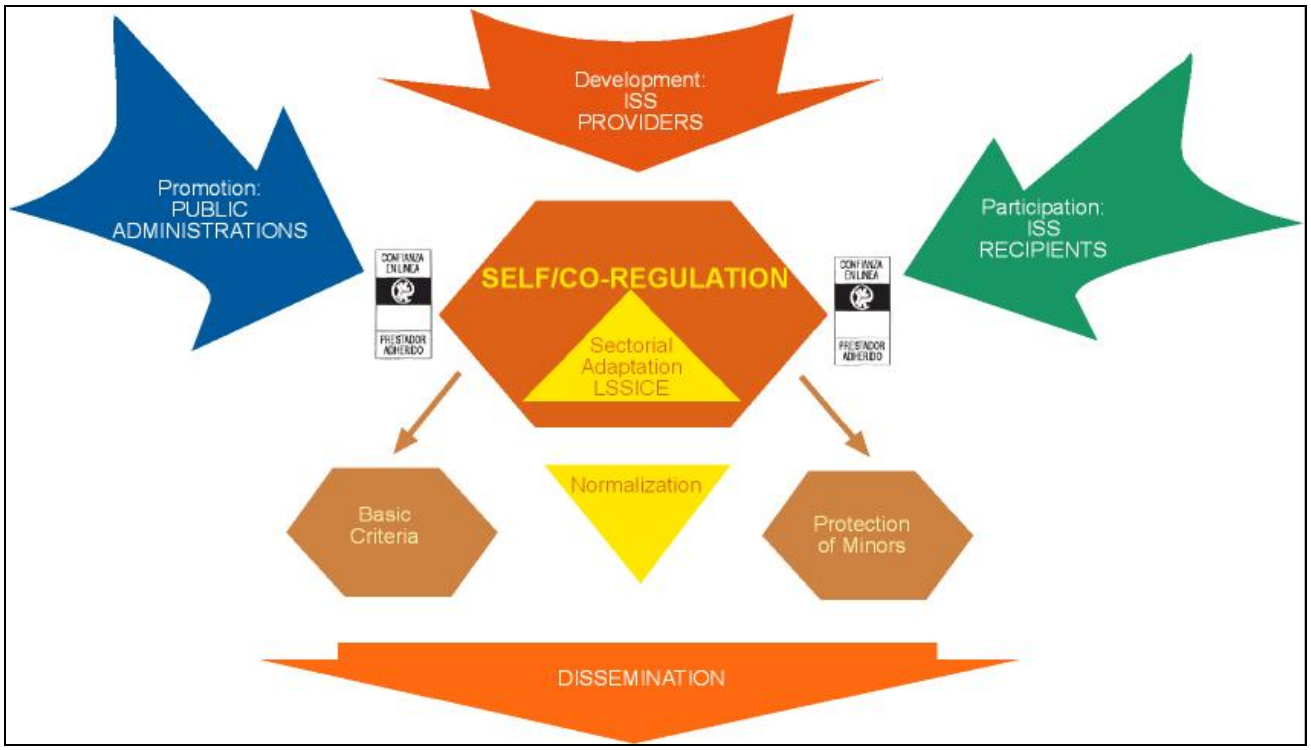

Figure 9: Self & Co-regulation in Art. 18 of the Spanish Act No. 34/2002 LSSICE

In any case, thanks to this openness of statutory legislation to private forms of regulation, State legislation can be combined with normative instruments generated and thus accepted by the social agents operating in a given social field. In the case of B2B e-commerce, self-regulation is the keyword, and it is assumed that it can play an important role in areas that are not covered by (mandatory) Law.[90] **Codes of Best Practices or Codes of Conduct** and other self-regulation tools, under certain circumstances, better meet regulation needs and reflect a consensus between all relevant stakeholders.[91] Its ability to catch up with technological advances and sector-specific problems of e-business makes co-regulation a proper solution to effectively regulate B2B trading platforms and DBE.

2.5.2. Alternative and On-line Dispute Resolution (ADR/ODR) Tools

Under a variety of names, **alternative dispute resolution** (ADR) has been for a long time competing with courts and official adjudication procedures. Yet it seems that it was the advent of the Internet that made ADR a trendy issue. Attempting to catch up with the ever-increasing complexity of the web society, official dispute resolution mechanisms have become too complicated and slow, and therefore inefficient in dealing with the wide range of conflicts raised by

[90] EC COM 2004/479: p. 7. See also Pullman et al 2006: p. 23 ss.

[91] See EC COM 2004/479: p. 8. A plea for a better self-regulation in B2B Internet trading platforms is to be found in Expert Group on B2B Trading Platforms (2003: p. 30), encouraging development of «Codes of Conduct aiming at enhancing transparency in the Internet platform and stronger commitment to respect fair trade principles. Such Codes of Conduct and participation terms should, wherever possible, be elaborated with the involvement of all relevant stakeholders, e.g. operators, buyers and suppliers, to ensure that all interests are duly taken into account. (…) Only under this condition can it be reasonably expected that Codes of Conduct are effectively followed and implemented. Codes of Conduct or participation terms should be fair and well balanced for all parties involved. (…). Self-regulation depends on the willingness to respect the agreed rules and principles in reality. The credibility of voluntarily agreed Codes of Conduct would certainly benefit from further enhancement by certification services and trust seals for B2B Internet trading platforms». One of the most interesting outcomes of this Expert Group Report was a checklist for the assessment of Codes of Conduct related to B2B Internet trading platforms (See Annex II).

digital media. Further, the international dimension of online interactions, either of commercial or merely informational character, points to the need for "deciders" beyond State Law. Resorting to courts in Internet-related disputes raises a number of complicated questions: which law applies, which authority has jurisdiction over the dispute, which forum is competent to hear the dispute, and whether the decision is enforceable across borders? Further, the cost of court proceedings may exceed the value of the goods or services in dispute, or their duration may be far slower than virtual time.

Alternative, **on-line dispute resolution** or just "out-of-court" systems have been set in motion worldwide to compensate for the failure of State Law to fulfil its adjudication functions. ADR refers to any unofficial means and processes designed to assist parties in resolving differences, supposedly in a speedy, cheap and easy way. Classic examples for ADR are facilitation or conciliation, mediation, and arbitration. More recently a wide range of new ADR procedures have been set down due to the so-called "de-judicalisation": settlement conference, early neutral mediation, hi/lo arbitration, baseball arbitration, mini-trial, summary jury trial, private jury trial, med-arb, arb-med, and mediation with arbitration on last offers. And things also get more sophisticated on the Internet, where on-line dispute resolution systems (ODR), i.e., online arbitration, mediation and automated negotiation, are increasingly gaining ground both for B2C and B2B interactions. The belief that ADR perfectly suits the Internet world is widely held.

In a national i.e. Spanish context, this is an approach followed by the legislation: Art. 32 of the Act. 34/2002 LSSICE promotes ADR/ODR in relation to ISS and linked the existence of ADR/ODR Codes of conduct as result of self/co-regulation; this is clearly shown by the conditioning of the authorisation of use of the Public Trust Seal to include in the code of conduct an ODR System; in the same way, Art. 37-39 of the Spanish Fair Trade Act.

2.5.3. Hinge-Law or Hybrid Law Solutions

Despite the fact that we have limited our legal framwork to an EU context, it is a matter of course that online regulation cannot be achieved without involvement of other States, especially the United States and several Asian countries.[92]

Take for instance the privacy issue –a similar development could be observed in other regulative areas. As the Internet evolved it was soon realised that an increasing number of privacy concerns should be accounted for. Both at national and international level, data protection or privacy laws were in force years before the advent of the Internet, such as the European Council 108 Convention (1981), or before the Internet extended to become a part of everyday life, e.g. the EU Data Protection Directive (1995).

At first, this *pre-existing regulation* was expected to solve those concerns: principle-based or analogical solutions were invoked for that purpose, and they could possibly have been sufficient to a certain extent.[93] But it was not long before the shortcomings of this approach became apparent:

[92] «As the Internet is neither an exclusively American nor an European phenomenon, a global regulatory framework is needed» (Holznagel and Werle 2002: p. 9).

[93] Earsterbrook's (1996) early "law of the horse"-thesis about Internet regulation is a striking instance for this. As Mandel (2007: p. 563-64) observes, «it is inevitable that legal disputes concerning the new technology will be handled under the pre-existing legal scheme in early stages (…); there often will not be enough information and knowledge about nascent technologies to develop or modify appropriate legal rules, or there may not have been enough time to establish new statutes, regulations, or common law for managing the technology. In addition, there often appears to be an inclination to handle new technology disputes under existing rules. This response is usually the easiest, both administratively and psychologically. Not surprisingly, however, the pre-existing legal structure may prove a poor match for new technology. Often there will be gaps or other problems with applying the existing legal system to a new technology issue».

- On the one hand, regulation-by-principles leaves too much room for uncertainty –it provides many so to say "doubtful" solutions– and regulators attempted to reduce this uncertainty by setting new norms.
- On the other hand, some online situations did not have an offline equivalent and could not be properly coped with by resorting to pre-existing law.

Special measures for the Internet, that is, *specific regulation*, were thus established, such as the norms included in the 1997 EU Directive on privacy in telecommunications. However, the regulatory strength of both previous and new provisions proved to be problematic, which led to the issue of effectiveness. This problem comprises several interrelated aspects.

- Activities conducted over the Internet may involve various geographical locations, so that diverse or even opposite regulatory frameworks can apply to them
- The number of such activities increases dramatically, and so does the number of related conflicts, but there is no set way to deal with them.
- Public authorities have no means to enforce or implement regulatory decisions beyond their territories or jurisdictions and even within them –tracking human actions is much more burdensome when they are carried out online than it is offline; and the same goes for courts or other official means to deal with Internet-related conflicts.

In view of that, regulatory tools and strategies were sought to overcome the obstacles to the effectiveness of online privacy regulation. Self-regulatory power was explicitly recognised for private actors and organisations, in an attempt to get Internet users and stakeholders involved in the making and application of regulatory decisions. However, in such a scenario, the overwhelming dominance of U.S.-based companies on the Internet makes it impossible to assure effectiveness of any regulatory attempt at a strong level of data protection in Europe, or elsewhere, unless certain privacy standards are assumed. As these, however, are still largely neglected within some legal cultures, the need arises to make two different cultural and legal traditions compatible with each other. This can be achieved through new forms of regulation –i.e., self-regulation– which can work in a global environment by merging contradicting legal frameworks.

Because of this, international legal frameworks were created to bridge diverging national laws on privacy issues, providing hybrid regulatory solutions. Such **hybrid institutions** are taken to be the seed of the forthcoming regulation models for the knowledge society, and are even considered as the only way in which state law can be able to cope with Internet-related regulation problems. Through this sort of **hinge-law** (in German: *Scharnierrecht*), legal interfaces are created that preserve the autonomy of national or regional regulation systems, making them at the same time compatible with the global and decentralized organization of the Internet.[94]

Therefore, with regard to the intersection between data protection and e-commerce, this role is to be played by the Safe Harbor Agreement,[95] which aims to reconcile two opposite approaches to privacy regulation, namely the European strong and state law model, on the one side, and the United States model, largely based on private norms and policies under little or no official control (inappropriately called self-regulation), on the other.[96] This is not a kind of surface opposition, but is firmly rooted in both legal cultures. Data protection is approached in Europe as a fundamental right prevailing, at least *prima facie*, over economic interests, whereas in the United States it is rather a mere commercial issue, so that the companies claim ownership over customer information and tend to deal with it just as they do with any other company asset. It belongs to the spirit of Safe Harbor to harmonise these approaches without outstanding damages in either model; i.e., respecting the basics of each model. European states attempt to provide their consumers with a pragmatic level of data protection, but not at any cost. In a non-traumatic way, i.e., through self-

[94] Farrel 2002: p. 27; Holznagel and Werle 2002: pp. 20-21.
[95] See http://www.export.gov/safeharbor, as well as Dhont, Pérez & Poullet 2004.
[96] Farell 2002: p. 37.

regulation, this agreement is ultimately expected to export strong data protection standards to the United States, where domestic law and weak self-regulation leave much to be desired as far as privacy protection is concerned.

2.5.4. Lex informatica, Regulation-by-Technology and "Code as Law"

Nevertheless, pieces of hinge-law such as the Safe Harbor Agreement mentioned above try to find common elements; therefore, a focus was put on the very technological infrastructure of the Internet, taking it as a "code" in which social and legal norms could be embedded.

The well-known significance of technical infrastructures for regulatory purposes has been successfully pointed out by Lessig (1999), who claims that the *code* of the cyberspace is built into its software and hardware.[97] More accurately, the concept of "code as law" refers to the process of setting legal norms through decisions on the contents and design of the technical infrastructure and applications; moreover, these decisions are dictated not only by purely functional issues, but also, and perhaps more importantly, by issues concerning the desired use of the technical infrastructure (van der Hof & Stuurman 2006: p. 206). The process of developing and setting technical standards and defining technical features of digital environments is a process of regulation (i.e., self-regulation). As it is a technical issue, the code may implement rules coming from both states and private groups, enabling them to waive territorial borders and legal frameworks and thus complementing state regulation. In many respects, regulation by technology is similar to self-regulation (be it based on contracts or codes of conduct). As Reidenberg (1998: 574) put it: «lex informatica allows customised rules to suit particular network situations and preserve choices for individual participants».[98]

2.6. Concluding Remarks and Implications for Governance of DEs

Sustainability is a "big issue" in the general theory of DEs, which shows a certain grade of maturity of this the vision about how DEs can become the Internet of the near future. Governance is a clear component of such sustainability, and regulation a part of governance. It is not the main issue, but the discussion about regulation cannot be postponed anymore. This highlights the **importance of Social Sciences** input in these environments. In any case, a decision on the basic elements for the introduction of legal and regulatory issues into the DE paradigm must be taken as a relevant part of a general theory on DEs.

We have seen that both DEs as such and DBE in particular seem to reproduce, albeit at a lesser scale, basic regulatory problems and issues which are typical of the Internet in general (virtualisation, technological turbulence, extraterritoriality, jurisdictional difficulties, multiple normative sources). How and to what extent these problems will affect DEs will depend on the features and particular settings of each DE, but, in any case, an **adequate balance between over-regulation and under-regulation** must be pursued –for otherwise regulatory attempts are likely to hamper DEs' developments.

Focusing on DBE regulation, as a special modality of ICT regulation, it requires the active involvement of the DBE actors and stakeholders, but it cannot be carried out apart from the State's legal constraints affecting most of the issues and topics raised by DBE activities. Therefore a **complex or combined regulatory strategy is suggested**: under the EU framework for e-

[97] See e.g. Reidenberg 1998; Lessig 2002; 2003 and 2004; Leene & Koops 2005; Klieve & de Mulder 2005; Bal 2005; Hosein et al 2002; Dommering & Asscher 2006.

[98] Many issues concerning regulation, especially regulatory implications of the architecture, have been already discussed in previous Deliverables of this Project: see e.g. OPAALS D3.6 (in special p. 18 ff., 49 ff., 65 ff. and 81 ff.) and D12.2; as well as DBE D32.2.

business, co-regulation and regulation-by-technology seem to be the most adequate basic combination. DBE regulatory needs (both community preferences or free decisions and decisions conditioned by external constraints) can be properly met by combining both strategies and their different instruments,[99] relying as much as possible in the strategy "Code as Law". Further, in order to avoid over-self-regulation, where no agreement between the stakeholders is possible, ADR/ODR mechanisms shall be relied on, which have a prospecting functionality, too. As long as we are considering a EU-based model, hinge or hybrid Law solutions are not going to be the main regulatory inputs, but we should not lose sight of such a strategy in favour of specific issues, and it can be used toegther with co-regulation, in order to generate broader territorial acceptance. In any case, no need for a specific regulatory activity of Public Authorities has been detected. Further, it can be argued that such an activity is not desirable, as long as DEs are environments that are still being configured.

Regarding the regulatory issues detected, IPR management can be solved by an agreement on the adoption of the licenses already existing: for software it is more accurate to choose one of the specific OSS licenses, because they are solutions designed specifically for it. Regarding information other than software of the OPAALS's OKS, Creative Commons Licenses might constitute the best option. The cc by-nc License might be the suitable one in case of a direct dissemination of its contents by the OPAALS Legal Entity, because it allows derivative works but prohibits the obtaining of a possible profit across a commercial use, which in this way respects the general non-profit ethos of the OPAALS Legal Entity. In other cases, the cc-by or the cc-by-nd may suit the needs of the OPAALS Community. The privacy and data protection issue has been addressed in Subsection 2.4.3, whereas the adoption of a data protection contract is needed as a second-order contract rule. The issues related to trade mark, domain names and digital signature can be solved by following the legal framework; the ones related to the OPAALS Legal Entity and the functioning of DBE as a market and its participants as market operators shall respect the legal framework on Company and Association Law and ISS Law, and Fair Trade and Competition Law, respectively.

Of course, the decision on the overall regulatory strategy has clear **implications for the governance of DEs**. As already pointed out, it necessarily implies a non-state based institutional framework and a set of practices and procedures leading either to formalise norms or normative expectations. Institutional and decision-making processes are basic elements of governance. From a regulatory point of view, the key concern is how to make regulation certain and effective. This shall be done in a way that ensures DE workability in real practice (specially regarding SME business practices) without damaging the architecture and design principles of DEs. The constitution of a non-profit Legal Entity which is able to coalesce the OPAALS Community, including the DBE Community as a part of it, and to fix the foundational settings in its Articles of Association, combined with a Rules Book, regarded as a Code of conduct, seems to constitute an acceptable institutional framework. Within such a framework, issues related to access and membership – as, for example, the requirements to become a Virtual Super Peer, can be solved by means of *Lex Informatica* established by a Hardware and Software Committee inside of the Legal Entity; IPR legal management can be entrusted to such Committee and to a OKS Committee, following the general guidelines given by the General Assembly of the Legal Entity; second-order contract rules, as a clear result of self- and co-regulation, can be included in the Rules Book by working groups integrated for the different community activities and supported by the Legal Entity.

[99] «Regulation in e-business follows the principle of requisite variety established in systems theory by W. Ross Ashby: 'the larger the variety of actions available to a control system, the larger the variety of perturbations it is able to compensate'. The ability to manage complexity in a self-organising and evolving system is in direct relation to the capability of the system to represent diversity through combinations of less complex regulations. Hence, in order to manage the complexity of the regulatory domain in digital ecosystems, it is helpful to build from general constraints towards the nuances of local and user-specific implementations (OPAALS D3.6: p. 21). See also DBE D32.1 on different regulatory layers.

3. BASIC ELEMENTS FOR SUSTAINABILITY AND GOVERNANCE STRATEGIES FOR DIGITAL ECOSYTEMS

As stated above, this section intends to summarise the basic elements for sustainability and governance strategies of DEs, especially for a governance strategy of the OPAALS Community. This is done considering the results of the above-mentioned SuGo Workshop[100] and the work done in WP11, in order to guide the contribution of UniZar in this section of the deliverable.

3.1. SuGo Workshop

On January 21 and 22, 2010, a workshop was held at SUAS (Salzburg), to catalyse plans for the sustainability and governance of OPAALS after the funded life-time of the project. The workshop was attended by a cross-section of representatives from OPAALS partners from both the Social Science and Computer Science domains. The following is a list of participants:

- CREATE-NET (Francesco Botto, Kiran Yedugundla)
- ITA (Javier Val)
- LSE (Paolo Dini, Anne English, Lorena Rivera Leon)
- NUR (Felix Akorli)
- SUAS (Raimund Eder, Thomas Heistracher, Thomas Kurz, Christoph Ruecker)
- T6 (Antonella Passani, Andrea Nicolai)
- UniKassel (Frauke Zeller)
- UniZar (Pedro Bueso)
- UL (Lorraine Morgan)
- WIT (Jason Finnegan)

[100] Summary Report done by Anne English, Thomas Kurz, Pedro Bueso, Andrea Nicolai, Lorraine Morgan and Paolo Dini.

3.1.1. Methodology

The workshop was moderated according to the Theme-Centered-Interaction (TCI) methodology, a simple strategy developed by Ruth Cohn for structuring workshops and maximising their outcomes.

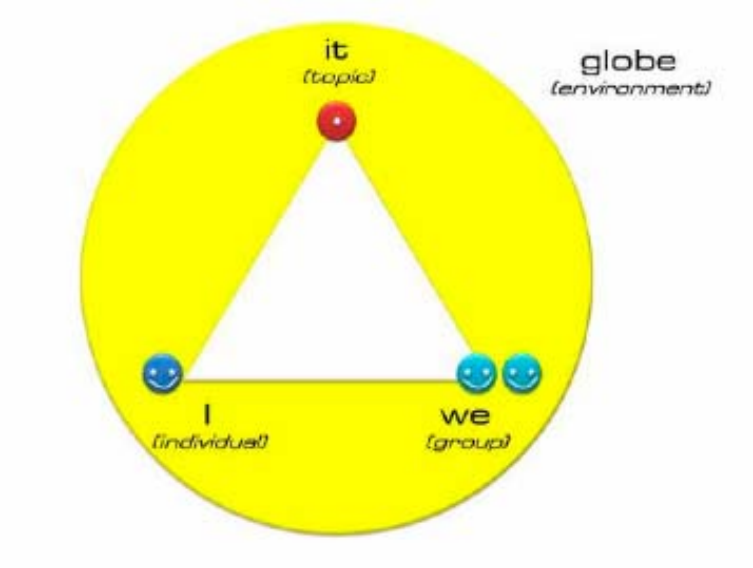

Figure 10: TCI Methodology

3.1.2. Agenda

- *Andrea, Pedro and all:* Distinguish between Governance and Sustainability
- *Jason: Update on Computer Science*
- *All:* Identify elements we need to sustain in e.g. OKS, software, research community, knowledge, collaboration approach, learnings
- *Antonella and Anne:* Report on learngings from relevant DBE deliverables
- *All:* Joint input on existing similar legal entities, foundations etc especially business models
- *All:* Identify sustainability model for OPAALS
- *All:* Identify governance model for OPAALS
- *All:* Concrete action plan, timelines and responsibilities
- *Andrea and Pedro:* Presentation of Follow-Up activities

The methodology and the agenda enabled a very constructive discussion on the topics of the workshop; however, there were two different levels of discussion, sometimes not clearly distinguished:

1. General Theory/Approach on Sustainability and Governance for DEs from the principles/foundations of the understanding of DEs of the OPAALS Community
2. Design of a Sustainability and Governance Strategy for the OPAALS Community regarded as an Academic DE

Nevertheless, it can be said that the second one was the main discussion level, with the first one a sort of background for the second one.

3.1.3. Discussion on Sustainability

The following guidelines for Sustainability can be drawn from the discussion:

- Open – Living Network
- Multi-layer – Social, Technical, Economic
- Demand-Oriented – "Bottom-up"

The discussion had as a result the conceptualisation of a "Virtuous Circle" for Sustainability:

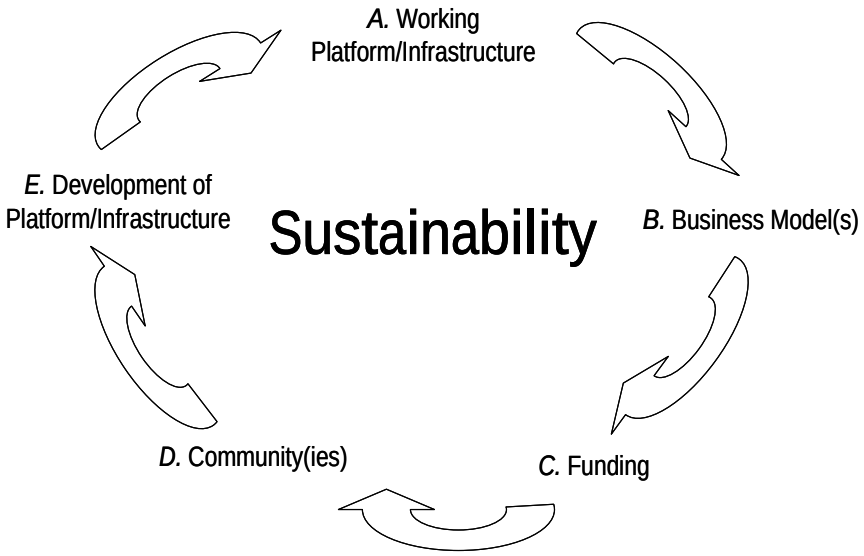

Figure 11: "Virtuous Circle" for Sustainability

Relating to the elements of the circle, the following attributes were identified:

A. Working Platform/Infrastructure
   a. OSS-based
   b. Reliability
   c. Usefulness
   d. Usability – user-friendly – easy adoption
      i. Tools
      ii. Example of services
      iii. Services for SMEs
   e. Standardisation
   f. Maintenance
      i. Seed Nodes
      ii. Multiple public Flypeer Nodes
   g. Advice/Support
B. Business Model(s)
   a. SW – OSS-based
   b. Multi-stakeholders oriented – synergies
      i. Multidisciplinary
      ii. Catalysts
   c. Revenue Model(s)
   d. Knowledge Management
   e. Social-Political Recognition, Credibility

   f. Governance
C. Funding
   a. Public
      i. Research Programs/Projects
   b. Private
   c. Money Flow
D. Community(ies) → Academic Community OPAALS
   a. Reinforce collaborative behaviour
   b. Identity: Value System
   c. Reputation
   d. Shared and Connected Knowledge
      i. OKS
      ii. Conference
      iii. Publication/Journal
      iv. Research Projects
   e. Enlargement – Critical Mass – International
E. (Future) Development of Platform/Infrastructure
   a. Technical Support
   b. Engine with
      i. Training
      ii. Education
   c. New Services

3.1.4. Discussion on Governance

The following Principles/Foundations for Governance can be drawn from the discussion:

- Democracy
  - Acceptability – Legitimacy
- Transparency – Accountability
- Flexibility – Scalability

The discussion had as a result a "Virtuous Circle" for Governance

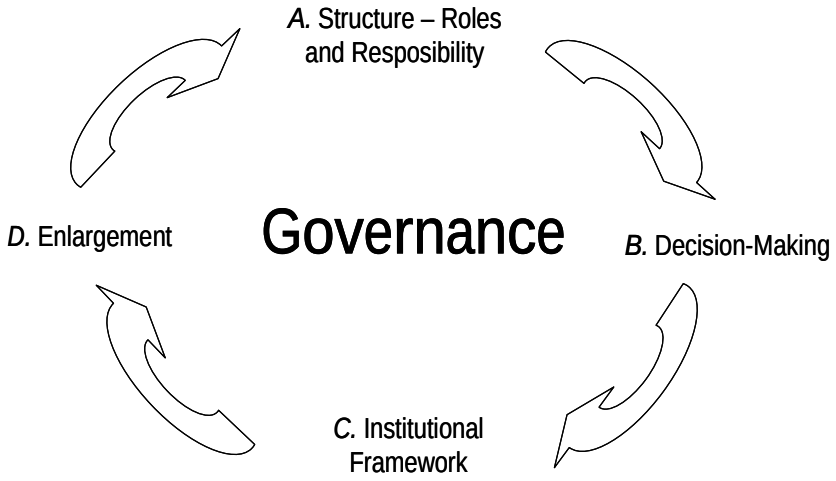

Figure 12: "Virtuous Circle" for Governance

Relating to the elements of the circle, the following attributes were identified:

A. Structure – Roles and Responsibility
    a. Membership
        i. Access - Requirements
        ii. Cancellation – Sanctions
    b. Assignment of Responsibilities
        i. SW Management and Maintenance
            1. Certification
        ii. OKS Management and Maintenance
        iii. Steering – Design of Policies
        iv. Advice
B. Decision-Making
    a. Process(es)
    b. Open – Democratic but Workable – Effective
    c. Rules – Norms
    d. Dispute Resolution
C. Institutional Framework
    a. Hard and Soft Framework
    b. Legal Entity
        i. Simplicity
        ii. Common Principles
D. Enlargement
    a. Independently reported show cases from the real world
    b. Ambassadors

3.1.5. Solutions/Outcomes

It was agreed that the following describes the facets of OPAALS requiring Sustainability and Governance frameworks and plans:

(1) Hard/software Infrastructure

Hardware - 4 rented and 4 academic nodes required with a network manager or coordinator who would monitor, maintain and report, starting October 2010 with a budget of €4K.

Software – platform required for whole stack from JXTA upward with goal of a stable, reliable, minimum data set of the beta version: end of May.

Release management for a stable/developed version is required together with relevant use cases, testing and usage. The access needs to be opened to developers and rights committed. Simultaneously documentation for each part of the stack needs to be created/finalised. Ownership of costs needs to be decided upon.

(2) Stakeholders: Communities (Academic, Regions, SMEs, SW Developers) and Enlargement

In the context of *Academics***,** the following were identified as contributing to the sustainability of OPAALS and to increasing academic recognition:

- Conferences (e.g. through the Springer LNICST proceedings of OPAALS '10)
- Publications – journals/books
- OKS knowledge repository

Regions would require:

- How-to guides and Information pack
- Ambassadors & mediators
- Public funds (EU, national, regional…)

- Links with Non-Regions

SMEs would require:

- To provide low-cost software
- Helpdesk
- Knowledge repository
- Social networks (contacts with academia)
- Engagement with clusters or intermediate actors

Software developers would require:

- Social networks (contacts with academia)
- Reputation
- Organise a showcase, marketing event etc (e.g. the workshop for regions and SMEs that ITA will host in June if the software works)
- Maintenance of s/w platform
- Offer support information

(3) Business models and funding

In terms of business models, the OPAALS community needs to establish a Bootstrap plan that will cover the initial community after the funded lifetime of OPAALS is over and segue into a long-term business model. The governance framework is an integral part of the Business Plan. Identification of funding mechanisms is central to the sustainability of the business model.

The Business Model needs to detail the value of engagement with OPAALS for the various actor types (SME, academic, S/W engineer etc). It was noted the value proposition for private vs. public organisations would be different and thus a series of value dials needs to be established.

The need to establish relationships/synergies with suitable target audiences was highlighted. This needs to begin now within the consortium and before the end of the project. Our sustainability plans should also be validated by external experts.

3.1.6. Suggested Legal Entity

Further, Pedro Bueso suggested the Belgian AISBL (*Association Internationale Sans But Lucratif* - a member-based international non-profit association) as a suitable legal entity for the OPAALS community. This entity would own the IPRs on software and other knowledge than software produced by the OPAALS community. He pointed out that member classes or categories would need to be identified. Such classes or categories could include super-members, full members, public/private partnerships, companies, researchers.

There would also need to be an OKS board or committee.

The concept of 'Ambassador' or 'Champion' was suggested to promote OPAALS.

Working groups could be used to focus on various aspects of the OPAALS community needs; such groups can be integrated in the structure of the entity or exist outside of the entity but supported by it.

A board or committee could be set up to govern the software and hardware going forward: this committee shall include computer experts and experts on social sciences, too, in order to help orient the requirements of the software development.

3.2. OPAALS Legal Entity

3.2.1. Requirements for the AISBL from SuGo Workshop

As a main component of the Institutional Framework of the Governance of OPAALS as a Digital Ecosystem, a need for a legal entity was identified. This need is related to the necessity to assume some functions as:

- Ownership of the IPRs on software and other knowledge than software produced by the OPAALS Community.
- Management of the OKS and the linked IPRs
- Management of the hardware and software and the linked IPRs.
- Common house of the different stakeholders in the OPAALS Community.
- Support of the OPAALS's Working Groups.

After considering different options, the suggestion in favour of the Belgian AISBL (*Association Internationale Sans But Lucratif* - a member-based international non-profit association) as a suitable legal entity for the OPAALS Community had a broad acceptance. Hence, a draft of its articles of association is going to be developed as a part of the work of Prof. Bueso as a member of the ICT, linked to the task to be done in D12.12.

In the drafting of such articles of association, the following points have to be developed:

- Member classes or categories will need to be identified. Such classes or categories could include super-members, full members, public/private partnerships, companies, researchers, institutional members (i.e. universities).
- The concept of 'Ambassador' or 'Champion' has to be made concrete, as an instrument for the promotion of the OPAALS Community.
- A Hardware & Software Board or Committee shall be set up to govern the software and hardware going forward: this committee shall include computer experts but also experts in social sciences, in order to help oriente the requirements of the software development.
- There is also need for an OKS Board or Committee.
- The interaction with Working Groups who will focus on various aspects of the OPAALS Community needs shall be established; such Groups can be integrated in the structure of the entity or exist outside of the entity but be supported by it.

3.2.2. What is an AISBL?

An International Non-Profit Association is a legal entity regulated by the Belgium Law of 25th October 1919 on International non-profit association, which was significantly amended in 2000 under the Law of Non-profit association, including both Belgium non-profit association (ASBL) and International non-profit association (AISBL) regulation (last amendment in December 2009).

The AISBL is a legal entity established for religious, charitable, scientific, cultural or educational purposes; however, it cannot be used to carry out any industrial or commercial activities.

After the Judgement of the European Court of Justice of 29 June 1999 (Case C-172/98 Commission of the European Communities vs. Kingdom of Belgium), there is no need to have a Belgian member in the administration of an AISBL or a minimum, and majority, presence of members of Belgian nationality in order for the legal personality of the AISBL to be recognised.

However, ASIBL must have their place of management in Belgium and, consequently, they are generally subject to the income tax for legal entities in Belgium.

An AISBL is different from a foreign ASBL. The AISBL is an open legal entity whether its members are Belgian or not. It is an association regulated by Belgium Law and its headquarters must be placed in Belgium. It is possible to point out one character that enables to distinguish it from a simple ASBL: its purposes must pursue an international utility. A foreign ASBL is constituted abroad in accordance with the established foreign Law, but its headquarters must be located in Belgium as well.

In general, the regulation for both ASBL and AISBL is similar, but it is even more flexible for the AISBL. The essential point is the principle of freedom of contract, therefore there is a wide space for the adaptation of the AISBL to the organisational needs of the founders.

3.2.3. Constitution of an AISBL

The constitution of AISBL requires the fulfilment of more formalities than ASBL:

- First, it is necessary that the articles of association be recorded in an authenticated document: an authentic and private deed (Article 48).
- Second, the articles of associations must be communicated to the Minister who is competent for Justice with the request to grant legal personality and approve the articles of association (Article 50(1)).
- Third, the AISBL will acquire a legal personality on the date of the royal decree pursuant to which it is recognized (Article 50(2)). In order to obtain the royal decree, the information must be submitted to the following address:

  Service Public Fédéral Justice, Direction Générale de la Législation et des Libertés et Droits Fondamentaux.

  No 115, Boulevard de Waterloo - 1000 Bruxelles

The following should be submitted to the above address:

(1) the authentic and private deed, which includes the articles of association and its annexes;

(2) one request for the Minister to obtain legal personality; and

(3) a list of the members who take part in the Board of Directors or Governors.

3.2.4. Mentions of Articles of Association

Article 48 establishes a minimum set of data that articles of association shall mention:

(1) the name of the international non-profit association and the address of its seat;

(2) the precise description of the purpose or purposes for which it was created, as well as the activities it envisages to attain this purpose or these purposes;

(3) the conditions and formalities regarding the admission and resignation of the members and, if applicable, of the members of different categories;

(4) the rights and obligations of the members and, if applicable, of the members of different categories;

(5) the powers, the convocation modalities and the decision-making modalities of the general directional body of the international non-profit association, as well as the conditions pursuant to which its decisions are communicated to the members;

(6) the powers, the convocation modalities and the decision-making modalities of the governing body of the international non-profit association, the modalities regarding the nomination, termination and revocation of the Governors, their minimum number, their term of office, the extent of their powers and the modalities to exercise them, as well as the modalities to designate the persons who shall have the power to bind the association towards third parties and to represent it in actions and in legal proceedings;

(7) the conditions to modify the articles of association, to dissolve and liquidate the association, and the destination of the assets of the international non-profit association. In case of dissolution these assets shall be used to promote a disinterested purpose.

It should be remarked that any modification in the data mentioned in Article 48, paragraph 2, shall be approved by the King. Other modifications to the articles of association shall be communicated to the Minister who is competent for Justice or to his representative and shall be accepted by either one under the conditions and within the limits of the Law.

3.2.5. *Publicity requirements*

All deeds, invoices, announcements, publications and other documents emanating from an international non-profit association which has been granted legal personality shall mention its name, preceded or followed immediately by the words “internationale vereniging zonder winstoogmerk” / “association internationale sans but lucratif” or by the abbreviation “IVZW” / “AISBL”, as well as the address of its seat (Article 47).

Also it is necessary that AISBL makes a request for a file from the Ministry of Justice which must be kept for each international non-profit association. The following shall be deposited in this file:

(1) the articles of association and their modifications;

(2) the coordinated text of the articles of association following their modification;

(3) the deeds regarding the nomination, the revocation and the termination of office of the Governors and, if applicable, of the persons empowered to represent the international non-profit association; these deeds contain the name, first names and domicile, or, when a legal entity is concerned, the name, the legal form and the seat, and mention the extent of the powers of these persons as well as the way to exercise them;

(4) the decisions recording the dissolution and liquidation of the international non-profit association;

(5) the annual accounts of the international non-profit association prepared in accordance with Article 53.

3.2.6. Liability of AISBL, its Members and Governors

3.2.6.1. Liability against third parties

The governing body that manages and represents the international non-profit association through the court and out-of-court are the Governors. They are involved in managing tasks and also in the fulfilment of obligations whose inobservance is legally penalised.

Therefore, **Members** are not considered to be personally liable towards third parties for the debts of the association.

Regarding the Directors or **Governors**, they are not considered to be liable for the obligations entered into by the association, that is, those that were entered into by the Governors on behalf of the association in the context and in the framework of the representative powers of the

Governors. The Law establishes that Governors' and persons entrusted with the daily management are not personally bound by the obligations of the international non-profit association (Article 49). The association contracts obligations through its appointees, therefore it holds the benefits and also is responsible for the faults attributable to its appointees or to the bodies through which it acts. Thus, a third party whose interest is frustrated by breach of contract will able to require to AISBL the fulfilment of the contract terms or compensation.

The are some exceptions to the last rule. One of them refers to the importance of inserting a *contemplatio domini* which mentions the name of the Association, preceded or followed by the words "international non-profit association" or by the abbreviation AISBL, as well as the address of its seat. This information must be included in all deeds, invoices, announcements, publications and other documents emanating from the association which grant its legal personality. In case of not inserting that *contemplatio domini,* the appointees which take part in these external acts could be personally bound by the obligations of the international non-profit association.

On the other hand, Governors may commit a tort, i.e., if they commit a *culpa in contrahendo* during and as a result of a contract negotiation. A Governor will always be held personally liable for torts that he/she committed. Indeed, under Belgium general civil law, the legal person is personally responsible for committed tortuous acts by its organs. Therefore, the person who suffered damage may take action against both the association and the Governor(s) committing the tort.

On the contrary, torts committed by Governors in the execution of a contract to which the association is a party will not lead to their liability. Either the Governor would have acted as the organ of the company: in this case the contractual error can only be attributed to him/her personally if at the same time this error would be considered to be negligence. Under Belgium law, however, it is very unlikely that a default under an agreement also constitutes a tort given the legal doctrine honoured in Belgium by the Supreme Court regarding coexistence of contractual and tort liability.

Governors may also be held personally and severally liable for damage suffered by third parties as a result of infringements of the Law or the Articles of Association. Even, Governor(s) may be liable for damage suffered by third parties when not acting with prudence or diligence required.

Further, infractions committed by Governors could generate both civil and penal liability under certain conditions. We could point out some of the most common infractions committed by Governors in practice:

- To resign from daily management.
- To acquire obligations when Governors know or must know that association can not satisfy them.
- Not to give enough information to General Directional body.
- To incur serious faults.
- Serious inobservance of legal, accountant and financial formalities, or serious non-fulfilment of obligations.
- Not to pay employees wages.
- To be negligent when making applications or formalities in order to receive grants for the association.
- Abuse of trust or power.
- To do commercial activities through AISBL.
- Not to attend regularly meetings of governing body (Board of Governors).
- Not to monitor the persons entrusted with the daily management.

- Not to pay invoices reasonably.
- To make public confidential information.
- Not convening the general directional body when dissolution cases need to be addressed.
- Not to keep legally required documents.
- To allow depreciation of assets.

The liability of Governors is limited to the execution of their assigned task and the faults committed in their management. However, the provisions of Article 1382 of the Civil Code, which establish the tort liability (extracontractual or non-contractual liability), are not excluded.

Governors are personally liable for committed defaults, except for those torts committed by all together. In this case, they are jointly and severally liable and the association may take action for torts against anyone.

3.2.6.2. Liability against the Association

Different from Law of business corporations, Governors do not incur any personal liability by breaching Law, or articles of association. Their liability *vis-à-vis* the company is judged as if Governors were agents of the association. Governors shall be responsible in accordance with civil Law for the duties entrusted to them. This applies equally to the day-to-day Governor. The liability on account of the day-to-day management shall be determined in accordance with the general statutory Law of mandate.

An important consideration is that Governors are only responsible for tort but not for bad management. Governors are not responsible if decisions are reasonable but they reduce the assets, the equity or the incomes of association.

As the Governors are contractually liable *vis-à-vis* the association, it is obvious that the authority to decide whether or not to start proceedings against the Governors (the so-called *actio mandati*) rests with the General Assembly If the General Assembly decides to institute a claim against the Governors on behalf of the association, it may appoint one o more agents to implement such decision and to institute a suit. In this case, the Association must prove the damage suffered and the causal connection between the damage and the default committed.

Also, Governors incur liability when executing their assigned tasks with abuse of power. AISBL may take action against Governors if the General Assembly had limited in the Articles of Association the powers attributed to Board of Governors and they acted without considering those restrictions.

3.2.7. Dissolution cases

At the request of the public prosecutor or of any interested party, the dissolution can be pronounced in the following cases (Article 50):

- Utilisation of assets or revenue of non-profit association for purposes other than the purposes for which it was constituted.
- Insolvency.
- Absence of management.
- Serious violation of the articles of association, or violation of the Law or public policy.
- Other dissolution cases established on articles of association.

3.2.8. OPAALS AISBL as Intermediation Information Society Service Provider: Concept and Liability

3.2.8.1. Information Society Law Framework and AISBL

As introduced in section 2.4.7, we should answer two basic questions in order to give an explanation about the consequences of being considered an Information Society Service (ISS) Provider (ISSP). First of all, we should analyse the agents who could be considered ISSP in the DE field. Secondly, It should be taken into account if the OPAALS AISBL, with its own constitution and nature, could be under the notion of Intermediary ISS Provider (InterISSP). This second point is of great interest as it will allow us to determine if the application of specific duties or liabilities, that e-Commerce Directive states in Article 9 and following, respectively, is possible.

Before differentiating between ISSP and InterISSP, we should point out a first aspect of the related issues. The European Legislator defines Information Society Service in Article 1(2) of Directive 98/34/EC (as amended by Directive 98/48/EC) as "any service *normally* provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." According to this notion, any non-remunerated service which is considered as an economic activity for its providers could be considered as an ISS as well. This conclusion can be drawn from the literal definition of ISS, which refers to the expression "*normally* provided for remuneration", and the concept of "established service provider" as any natural or legal person who effectively pursues an *economic activity* using a fixed establishment for an indefinite period"[101]. Therefore, there is no doubt about the possibility of offering non-remunerated services when they can be regarded as an economical activity, *e.g.* those rendered with promotional purposes. In other words, the scope of e-Commerce Directive only refers to Service Providers who offer ISS, which means that such services represent an economic activity for the provider, whether it is remunerated or not by the recipients.

3.2.8.2. Agents that could be regarded as ISSPs and InterISSPs

There is no doubt that the professional providers who take part in the DE, offering their services through DSC, as ISSPs, because they access this environment to follow a wide range of business purposes, *e.g.* for promotion, data exchange among companies, obtaining competitive advantages, market share improvement, signing strategic agreements, or executing electronic commerce through DSC. Therefore, it can be easily understood that all these diverse services represent economic activities for these agents according to the e-Commerce Directive, which stipulates some information requirements that ISSPs must fulfil when offering their services. Those requirements are compulsory in case of online contracts concluded with consumers.[102]

With regard to the responsibility that must be assumed by the ISSPs in this context, the Directive does not state a set of rules on the attribution of liabilities. Instead, it refers to the general rules of Law in order to determine that responsibility, that is, the ISSP's liability will be defined according to the civil, criminal or administrative current Law in each country's Legal System.[103] Indeed, the e-Commerce Directive does not declare a special distribution of liability for ISSPs when executing e-commerce or other information society services, except for the InterISSPs, whose liabilities are specifically regulated. What the Directive states is spheres of non-liability or exemptions for these InterISSPs under the observance of several conditions. The aim of these exemptions is to remove barriers to the development of cross-border services within the Community, guaranteeing the intermediaries' interests in order to allow them to provide an efficient and effective service. For that purpose, a non-general obligation has been established in order to monitor the third parties'

[101] See Article 2(b) and (c) of Electronic Commerce Directive.
[102] See Articles 10 and 11 of Electronic Commerce Directive, where it is said that *at least* some information must be given by the service provider clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service, *ad ex.* the steps to follow to conclude the contract, languages offered for the conclusion of the contract, the code of conducts, the contract terms and general conditions...
[103] As it will be analysed subsequently, the Directive only stipulates a specific responsibility for Inter ISSPs.

behaviours. However, to take advantage of these exemptions, which basically allow the providers not to incur any liabilities from users' conduct, InterISSP must obey several conditions or requirements.[104]

It is more complex to consider the DE as an ISSP in the terms used by the Directive, whether it carries out an intermediary activity or not. Firstly, because of the ecosystem's own nature, which could not properly be conceived as an association that promotes a common interest, but as an environment that allows its users to interact among them and with the applications and tools implemented on a network infrastructure. Secondly, in relation to the last point, if DE is conceived as a simple environment whose main function is to allow interaction among different agents – who will individually look for their own private interests – , it is not possible to attribute to this environment the achievement of an economic activity. Consequently, it will be an agent out of the Directive's scope.

However, we should take into account if in the future OPAALS Legal Entity – as an association or mediator agent behind the good working of the environment – could be conceptualised as ISSP. So far the question is not well defined, because it is necessary to clarify some controversial aspects like the Legal Entity's form. In spite of that, we could point out a final consideration. In case OPAALS was considered as an entity with its own legal personality, capable of executing an economic activity, it could certainly be considered to fit under the notion of ISSP, but it is not clear if it could be considered as intermediary service provider. Due to its position as a mediator agent, we could understand that OPAALS would be included in the InterISSP category. However, the e-Commerce Directive only attributes this qualification to several *numerus clausus* intermediary services. Consequently, if its activity is not one of the mentioned by the Directive, its conceptualisation as an InterISSP will have no further consequences. According to the e-Commerce Directive, only *network operators and Internet access providers, data transmission providers, and hosting and date storage providers* can be considered InterISSP.

3.2.8.3. Implications of considering OPAALS AISBL as an InterISSP

As it was pointed out before, the Directive regulates a specific liability to apply to InterISSPs. The technique used by the Directive consists of defining spheres of non-liability or exemptions when a InterISSP executes activities as mediator. Thus, InterISSPs will not be responsible for infractions committed by third parties under the observance of several conditions. The aim of this regulation is to remove barriers of Internal Market ensuring free movements of goods, services and the freedom of establishment (Article 26(2) TFEU). Existing and emerging disparities in Member States' legislation and case-law concerning liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition.

This Directive strikes a balance between the different interests at stake and establishes principles upon which industry agreements and standards can be based. Also, it excludes that Member States can impose a monitoring obligation on service providers with respect to obligations of a general nature. This does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation. Otherwise, the exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient. This activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.

[104] See Articles 12, 13 and 14 of Electronic Commerce Directive.

Thus, according to the Directive, in order to benefit from a limitation of liability, the InterISSP, where its service consists of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level (Article 14).

3.2.8.4. Liability of P2P Developer

Finally, we should take in consideration another important question: whether it is possible to attribute any liability to P2P developers for illegal acts committed by users? The majority of legal doctrine understands that in this case it not possible to apply the exemptions regarded to InterISSP. Then, a software developer is not protected by these spheres of non-liability, and therefore he/she must assume the responsibility that each Legal System has established for that type of acts.

However, although the InterISSP which allows the downloading of P2P software, through hosting activity, or promotes access or data transmission services for the good working of the P2P platform, could be considered responsible for the infractions committed by third parties, the spheres of non-liability should be applied as well.

3.2.9. Articles of Association Draft for "Open Knowledge Space/Online Knowledge Society – OKS", A.I.S.B.L. (v. 1.4)

N. B. This is a tentative version of the Articles of Association of the OPAALS Legal Entity, called "Open Knowledge Space/Online Knowledge Society – OKS", A.I.S.B.L. There are some data or passages which are marked with red/yellow, since they are more specific open questions; however, the whole drafting is a proposal with the aim to serve as basis for further discussion.

Section 1. Designation, Registered Office, Duration and Mission

Article 1. Designation

The International Association is designated by the name "OKS" and the qualification "Open Knowledge Space/Online Knowledge Society". Either the full name or the acronym may be used.

OKS is a Not-for-profit International Association constituted and governed by the provisions of Title III of the Belgian Law of 27 June 1921 on non-profit associations, non-profit international associations and foundations, and its subsequent amendments.

All legal instruments, invoices, announcements and other documents issued by the non-profit association to which legal personality has been granted must mention its name, immediately preceded or followed by the words *"Association internationale sans but lucratif"* (International Non-Profit Association) or the acronym "AISBL", together with the address of its registered office.

Article 2. Registered Office

The Association's registered office shall be situated at [address in Belgium, i.e., in Brussels], Belgium, in the judicial district of Brussels.

It may be transferred to any other location in the judicial district of Brussels, Belgium, by decision of the Board of Governors, which shall be published the month subsequent to this decision in the annexes to the Belgian Official Journal: *Moniteur Belge* (Belgian State Gazette).

Article 3. Duration

OKS has been established for an unlimited duration. It can be dissolved by the General Assembly in accordance with the conditions foreseen by these Statutes.

Article 4. Mission

OKS is a global network of excellence formed around multi-disciplinary research into digital ecosystems. OKS research covers social science, linguistics, computer science, business and innovation, software engineering, mathematics, and biology.

The main claim that OKS makes is that in order to achieve sustainable digital business ecosystems of small and medium enterprises and software components it is necessary to understand in depth the collaborative processes and ICTs that underpin the continuous creation, formalisation and sharing of knowledge in the form of business models, software infrastructure for e-business transactions, and new formal and semi-formal languages.

The association will open its output to the public during its lifespan. Output and research results will be published in the Open Knowledge Space (OKS). These pages reflect work in progress as well as historical output from work activities that will be completed or subsumed by other activities.

Article 5. Objectives

The Association is not pursuing profit. Its objectives shall be:

- Ownership of the Intellectual Property Rights (hereafter, IPRs) on software and other knowledge than software produced by the OKS Community.
- Management of the OKS and the linked IPRs.
- Management of the hardware and software and the linked IPRs.
- Common house of the different stakeholders in the OKS Community.
- Support of the OKS's Working Groups.

Article 6. Actions

The association will perform the following activities in order to fulfil its objectives:

1. Initiate, perform or coordinate basic and applied scientific studies in computer science, natural science and social science issues relevant to the mission above.
2. Collaborate with the relevant European and International institutions on the development of digital ecosystems which represent the next generation of Internet usage.
3. Interact with public institutions at local, regional, national, European and international level that are involved in the promotion of digital ecosystems.
4. Publish and circulate printed or electronic information in line with the objectives above.
5. Organise meetings, workshops, conferences and other events in line with the objectives above.

6. Perform any other activity, in accordance with Belgian law, that can support the objectives above.

Section 2. Membership Criteria, Subscriptions, Admission, Withdrawal, and Expulsion

Article 7. Membership Criteria (*tentative*)

Membership of OKS is open to both individuals and political, territorial, public or private organisations which undertake the development of digital ecosystems. Such organisations shall be legal entities, fully able to participate in the purposes and activities of OKS, and to assume the responsibilities of membership. Such organisations may operate at the local, regional, national or international level.

OKS has established two categories of effective (or active) members and other one of non-effective (or non-active) members, together with an special category of members called "Ambassadors".

A. EFFECTIVE or ACTIVE MEMBERS

1. FULL- or NON-PROFIT MEMBERS

a) INDIVIDUAL MEMBERS: Academics, researchers, and managers, acting on their own personal behalf, who are linked to the development of digital ecosystems.

b) NON-PROFIT INSTITUTIONAL MEMBERS:

RESEARCH INSTITUTIONS: Universities, research centres, and other non-profit institutions involved in the development or distribution of software, hardware and other technical and social components for digital ecosystems.

NON-RESEARCH INSTITUTIONS: Associations, foundations, public 'regional catalyst' institutions, active at international, national, regional or local level in the development of digital ecosystems.

[Current Members of the OPAALS Project are listed in Appendix of these Statutes. The number of Members has no upper limit.]

2. SUPPORTERS or FOR-PROFIT MEMBERS:

Any other organisation, company or individual willing to support the work of OKS. Supporters are not full members. They are regarded as associated members which shall fulfil the requirements and conditions established in Statutes and Internal rules. They shall have no voting rights in General Assembly, and they shall have other rights established by internal rules. Otherwise, they shall take part into the collaborative network activity.

B. NON-EFFECTIVE or NON-ACTIVE MEMBERS

3. OBSERVERS

Individuals, academic institutions, learned societies, professional associations, commercial organisations, other European or International Networks, and any other organisation that fails to

qualify for membership of OKS under the above criteria may apply for acceptance as Observers. These observers, by reason of their activities, work or expert knowledge, are able to assist OKS in carrying out its purpose. They shall have no voting rights or decision-making power and may not sit on the Board of Governors.

Observers will be determined by the Board of Governors and set out in Internal Regulations. As well as full members, organisations applying for observer status in the association must show proof that neither they nor the organisations to which they report are profit-making organisations.

C. AMBASSADORS

Individuals, members or non-members of OKS, may be appointed as Ambassadors of OKS. These ambassadors, by reason of their goodwill, are able to assist the association in extending the OKS Community. Because of being Ambassadors, they shall have no voting rights or decision-making power and may not sit on the Board of Governors. Ambassadors will be determined by the General Assembly under proposal of the Board of Governors and set out in Internal Regulations.

Article 8. Subscriptions (*tentative*)

All Members of OKS shall pay an annual subscription to support the purposes and activities of the Association. The amount of such annual subscription, the dates of the year to which it applies, and the required date of payment shall be determined by the Board of Governors and set out in Internal Regulations.

The annual subscription may be varied for certain categories of Member as determined by the Board of Governors. All OKS Observers shall pay whatever amount is required by the Board of Governors to participate in the activities of the Association. The amount, the required date of payment, and the rights and benefits offered in return will be determined by Board of Governors and set out in Internal Regulations.

Article 9. Admission

The admission of any new member is decided by the Board of Governors. This decision must be ratified by the General Assembly, at its next session. Any decision refusing an application for membership shall contain the grounds upon which the decision is made. Where admission is refused or where no decision is made within a reasonable time frame, the applicant may refer the relevant decision or lack thereof to the courts of Brussels.

Article 10. Withdrawal and Expulsion

Any Member may withdraw from OKS by giving twelve months notice, from the next 1 January, of this intention. Notice of intention to withdraw from membership shall be made in writing, by recorded delivery, to the Secretary General. It will then be presented to the next Meeting of Board of Governors for acceptance.

The expulsion of a member who fails to abide by the Statutes (including failing to abide by the conditions for membership) or by the Internal Rules, is decided by the Board of Governors. To take effect, this decision must be ratified by the General Assembly at its next session. The member in question shall always be entitled to present its defence before such decision is made by the Board of Governors and by the General Assembly. Any expulsion shall contain the grounds upon

which the decision is made. The expelled member may refer the relevant decision to the courts of Brussels.

Any member ceasing to take part in OKS as a result of resignation, expulsion or for any other reason shall have no claim upon OKS patrimony. The member shall remain under the obligation to pay its subscription as laid down in Article 8 and any financial commitments decided by the General Assembly to which it has committed itself.

Article 11. Decision-making bodies

The Association's two decision-making bodies shall be the General Assembly and the Board of Governors.

Section 3. The General Assembly

Article 12. Composition of and Representation at the General Assembly

The General Assembly is composed of all of the Members of OKS. Each Member shall appoint a formal representative to attend the General Assembly, and to validly exercise the rights of the Member without the Association having to verify his credentials.

The General Assembly shall meet at least once every year. It shall be presided over by the President, assisted by the Vice-Presidents, elected as set out in Article 13.

Article 13. Powers of the General Assembly

The General Assembly is the supreme power of the Association. It holds all the powers that are expressly reserved by law, and that are not devolved to the Board of Governors by the current Statutes, except for powers of representation.

The powers of the General Assembly are:

1. to appoint and to revoke the members of the Board of Governors;
2. to elect the President. Apart from exceptional circumstances, the President shall be elected from members of the Board of Governors. In any case, the President must be an Association Member or belong to an Institutional Association Member;
3. to elect one Vice-President, selected by and from the members of Board of Governors;
4. to elect the Treasurer, who will be selected from the members of Board of Governors apart from exceptional circumstances, where the Treasurer will be elected among members of the General Assembly;
5. to elect or dismiss the auditor(s);
6. to ratify the budget approved by the Board of Governors, approve the annual accounts.
7. to fix the financial contribution for the various members and the annual subscriptions, in accordance with the rules laid down in the Internal Rules;
8. to ratify the decisions of the Board of Governors on admissions or expulsions of members;
9. to approve a Board of Governors programme of activities and initiatives for the forthcoming year;
10. to modify the Statutes;
11. to modify the Internal Rules;
12. to pronounce the dissolution of OKS in accordance with the legal provisions in this respect.

Article 14. Meetings of the General Assembly

The General Assembly shall meet in ordinary session at least once a year, under the chairmanship of the President of the Board of Governors, who shall convene the General Assembly with a six-week notice. The notice indicates the place, date, hour and agenda of the General Assembly and is sent by letter, facsimile, or any other written means (including electronic format). As the case may be, working documents will be attached to the notice.

Members shall be notified of a General Assembly one month in advance, in writing or electronically, by the Board of Governors, normally through the Secretary General. Notifications shall inform Members of the date, venue, time and agenda. The Board of Governors shall determine the agenda for meetings of the General Assembly, but all proposals, in writing through the Secretary General, signed by at least two Members shall also be placed on the agenda.

The President of the Board of Governors must convene an extraordinary session of the General Assembly if at least a fifth of the Members entitled to vote so request, with a four-week notice period being given to the members of OKS.

Proceedings and decisions of the General Assembly will be recorded in minutes which shall be signed by the President or Vice-president and the Secretary General.

The minutes are kept in a register, accessible to the members, at the registered office of OKS. A copy of the minutes will also be sent out to the Members.

Article 15. Voting rights

Members may vote by letter or fax, and it will also be possible to vote electronically.

OPEN QUESTION: It is possible to attribute different voting rights in the General Assembly depending on the member categories. Even it is possible that member of a particular category does not have voting rights but may participate in the General Assembly meeting. In our case, full member would have voting rights, but not supporters, observers and ambassadors.

Members can delegate their voting rights at the General Assembly to another member, who will have the same rights, provided that the Secretary General has been informed in written form before the General Assembly. In addition to its own voting rights, a Member may represent the voting rights of only one other member. Only Members whose membership fees and payments are not overdue have the right to vote.

Article 16. Quorum and decisions (*tentative*)

Option 1: The ordinary General Assembly is validly constituted in the first convocation if the majority of the voting rights of the members are present or represented by a delegate. In the second convocation, one hour later, the General Assembly is validly constituted regardless of the number of the voting rights presents or represents. Decisions are taken by a simple majority of the present or represented voting rights.

Option 2: The extraordinary General Assembly is validly constituted in the first convocation if 75% of the members are attending or are validly represented. In the second convocation, one hour later, the General Assembly is validly constituted if at least one third of the voting rights are

presented or represented. If the quorum is not reached in the second convocation, a third convocation can be called, at least two weeks later. In this case, the General Assembly is constituted regardless of the number of the voting rights presents or represents. Valid decisions need to be taken a 75% majority in extraordinary Assembly, except for insolvency. In last case, it shall be sufficient 25% for a valid decision of voluntary bankruptcy petition.

Article 17. Presidency

The General Assembly shall be chaired by the President of the Association's Board of Governors or, in the absence thereof, by the Vice President.

Article 18. Internal Finance Committee/Audit

The General Assembly shall establish an Internal Finance Committee which shall be charged with auditing the accounts of the Association and presenting an annual report to the General Assembly.

However, the General Assembly may decide to entrust the audit of the Association's accounts to an external auditor, who must in such event be a chartered accountant (*réviseur d'entreprises* or *expert comptable*).

Article 19. Liability

Members are not considered to be personally liable towards third parties for the debts of the association.

Section 4. The Board of Governors

Article 20. The Board of Governors

The Association shall be governed by Board of Governors.

The Board of Governors shall consist of [odd number] persons elected for a maximum renewable term of three years by the General Assembly from among the members' representatives. The mandate of the members of Board of Governors, not re-elected and leaving the Board of Governors, ends immediately following the ordinary General Assembly. The mandates of the members of Board of Governors can be withdrawn at any time by a decision of the General Assembly taken by simple majority. The mandate is not remunerated.

Board Members and their representatives shall formally accept their election. Board Members may resign at any time following which the Board of Governors may consider whether to nominate a replacement to serve until the next General Assembly. Individual representatives on the Board of Governors may be replaced at any time.

Article 21. Meetings of the Board of Governors

The Board shall meet at least three times a year, at least once in person, with two weeks' notice. An extraordinary session must be convened if at least three members of Board of Governors call for such a meeting in which case a two week notice period has to be respected and the agenda

must contain at least the issues raised by the members of Board of Governors who asked for this meeting.

Convocation is issued by the President and indicates the place, date, hour and agenda of the meeting. It is sent by letter, facsimile, or any other written means (including electronic format). As the case may be, the working documents are attached to the notice.

Article 22. Decisions

The deliberations of the Board of Governors can only be valid if more than half of its members are present or represented.

The decisions of the Board of Governors are taken by simple majority. Each member of Board of Governors has only one vote.

Proceedings and decisions of the Board of Governors shall be recorded in minutes which shall be signed by the President and Secretary General.

The minutes are kept in a register, at the disposal of the Board of Governors, at the registered office of OKS. A copy of the minutes will also be sent out to all members of Board of Governors.

Article 23. Powers of Board of Governors

The Board of Governors shall have all powers except those reserved to the General Assembly.

Article 24. Special operations

Acts binding OKS to third parties and which are not part of the daily management operations, shall, except where special authorisation is given, be signed by the President or by the Vice-President, who shall not have to justify their powers to third parties.

Article 25. Delegated Committees

The Board of Governors has the right to set up an Delegated Committees in order to govern specific areas of OKS. The composition of the committees and its particular roles shall be determined by the Board of Governors, according to the Internal Rules.

Article 26. Hardware and Software Committee

Specifically, the Board of Governors has the right to set up a Hardware and Software Committee. It shall be set up to govern the software and hardware going forward. This programme committee shall include computer experts but experts on social sciences, too, so as to oriente the requirements of the software development.

The Board of Governors shall determine the composition and role of the Hardware and Software Committee, in accordance with the rules laid down in the Internal Rules.

Article 27. Chairmanship of programme committees

The Chairpersons of each Delegated Committee are invited to the meetings of the Board of Governors, but they have only a consultative voice.

Article 28. Working Groups

The Board of Governors shall be empowered to set up and disband Working Groups, to either advise the Board of Governors or to develop and implement plans in line with guidance provided by the Board of Governors.

The Board of Governors may set up as many Working Groups as it deems to be advisable to establish, in order to help OKS in achieving its mission in accordance with the present Articles of Association.

The Board of Governors shall determine the composition, the duration and the terms of reference of the Working Groups, nominating the Chairpersons and the members thereof, in accordance with the rules laid down in the Internal Rules.

Article 29. Accounts

Each year, the Board of Governors shall submit for approval by the General Assembly the accounts for the year ended and shall submit for ratification the budget for the year to come.

Article 30. Liability of members of Board of Governors

Members of the Board of Governors, being the persons entrusted with the daily management, shall assume no personal liability by reason of their office and shall be responsible solely for the performance of their duties.

As the liability of Members is limited to the execution of their assigned tasks and the faults committed in their management, they are not considered to be liable for the obligations entered into by the association in the context and in the framework of the representative powers. In these cases, the Association is the only responsible.

However, the provisions of Article 1382 of the Civil Code, which establish the tort liability (extracontractual or non-contractual liability), are not excluded for members of Board of Governors committing tortuous acts by its organs.

Section 5. Fiscal year and Financial Management

Article 31. Financial Year

The financial year shall begin on 1 January and end on 31 December of each year. As necessary and whenever required by law, the Association shall entrust the auditing of the Association's financial position.

Fees paid to the auditor or auditors shall be determined by the General Assembly at the time of appointment. Auditors may be reappointed for additional terms.

Article 32. Resources

The Association shall be funded by:

- the fees of members
- aid, notably financial, given to the Association by natural or juridical persons;
- asset income, such as dividends from a small participation (no more than 15%) in a profit-making company allied with OKS;
- subsidies from the European Union, its Member States and other International Organisations;
- income generated by its work, studies or actions;
- and any other sources authorised by law.

Section 6. Dissolution and Liquidation

Article 33. Dissolution cases

In the event of dissolution of the Association, the General Assembly shall appoint one or more liquidators.

Decisions concerning the dissolution of OKS must be taken according to the voting procedure foreseen for the extraordinary Assembly.

In the event that OKS is to be dissolved, the General Assembly shall decide by a simple majority of the votes cast on (i) the appointment, powers and remuneration of the liquidators, (ii) the methods and procedures for the liquidation of OKS and (iii) the destination to be given to the net assets of OKS for altruistic purposes.

Section 7. Amendments of Statutes

Article 34. Alteration of Articles of Association

When proposals are made to modify the Articles of Association, the texts thereof shall be appended to convocations to the General Assembly which shall deliberate upon them.

In this specific case, the convocations shall be sent at least two months before the meeting. Decisions concerning alterations to the Articles of Association must be taken according to the voting procedure foreseen for the extraordinary Assembly.

Any decision related to the amendments of the Articles of Association shall be published in the Annexes to the Belgian Official Journal, "*Moniteur Belge*".

Section 8. Final Provisions

Article 35. Provision I

The General Assembly may approve Internal Rules compatible with the provisions of the present Articles of Association, so as to ensure the correct functioning of OKS and its administration.

Article 36. Provision II

All cases not provided for in the present Articles of Association and, in particular, the question of publications to be made in the Annexes to the Belgian Official Journal, "*Moniteur Belge*", shall be dealt with in accordance with the provisions of the Belgian Law.

APPENDIX: CURRENT MEMBERS OF OPAALS

Participant organisation name:	**Short name**	**Country**
London School of Economics and Political Science	LSE	UK
T6 Ecosystems srl	T6 ECO	IT
Fachhochschule Salzburg GmbH (Salzburg University of Applied Sciences)	SUAS	AT
The University of Surrey	SURREY	UK
Waterford Institute of Technology	WIT	IE
Tampereen Teknillinen Yliopisto (Tampere University of Technology) Foundation	TUT Foundation	FI
TechIDEAS Asesores Tecnológicos	TI	ES
The University of Dundee	UNIVDUN	UK
University of Limerick	UL	IE
Create-Net (Center for Research and Telecommunication Experimentation)	CN	IT
Universität Kassel	UniKassel	DE
Indian Institute of Technology Kanpur	IITK	IN
Instituto de Pesquisas em Tecnologia da Informaçao	IPTI	BR
National University of Rwanda	NUR	RW
Instituto Tecnológico de Aragón	ITA	ES
Universidad de Zaragoza	UNIZAR	ES
University of Cambridge and Lucy Cavendish College	CAM	UK
National University of Ireland - Maynooth	NUIM	IE
University of Hertfordshire	UH	UK

REFERENCES

- Ayres, I. y J. Braithwaite (1992): *Responsive Regulation,* Oxford: OUP.
- Baldwin, R. y M. Cave (1999), *Understanding Regulation*, Oxford: Oxford UP.
- Baldwin, R. (1997), «Regulation: After Command and Control», en: K. Hawkins (ed.), *The Human Face of Law: Essays in Honour of Donald Harris*, Oxford: OUP.
- Baldwin, R. y J. Black (2008), «Really Responsive Regulation», *The Modern Law Review* 71/1, pp. 59-94.
- Benkler, Y. (2006): *The Wealth of Networks. How social production transforms markets and freedom*, Yale UP: New Haven.
- Berkey, J. (2002): «Outline of International e-commerce regulatory issues». Intel/Unitar Campus, New York www.un.int/unitar/intel_nct_campus/2002/conference_presentation.htm
- Black, J., Lodge, M. y Thatcher, M. (2005): *Regulatory innovation: a comparative analysis*, North Hampton, Ma: Edward Elgar.
- Black, J. (1998), «Regulation as Facilitation», *The Modern Law Review* 61/5, pp. 621-660.
- Black, J. (1996), «Constitutionalizing Self-Regulation», *MLA* 59/1, pp. 24-55.
- Boeraeve, C; Dasnois, R, y Mélotte, V., *Responsabilité des administraeurs*, Guide ASBL, Edipro, pp. 155 ff.
- Bullock, G. (2006), *Governance, Accountability, and Legitimacy*, WP Series, Univ. of California, Berkeley: http://nature.berkeley.edu/infolab/files/u3/InfoLab_WP06-01_Governance.pdf.
- Couto Calviño, R. (2008), *Servicios de certificación de firma electrónica y libre competencia*, Col. Derecho de la sociedad de la información, vol. 17, Granada: Comares.
- Darking, M, Whitley, E.A. y P. Dini (2008): «Governing diversity in the digital business ecosystem», *Communications of the ACM* 51/10, pp. 137-140.
- Dhont, J., M.V. Pérez Asinari & Y. Poullet (2004), *Safe Harbour Decision Implementation Study*, Namur, at: http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/safe-harbour-2004_en.pdf.
- Dini, P. et al. (2008), «Beyond interoperability to digital ecosystems: regional innovation and socio-economic development led by SMEs», *Int. J. Technological Learning, Innovation and Development, Vol. 1, No.3,* pp. 410 – 426.
- Dommering, E.J. & L.F. Asscher (2006), *Coding regulation - Essays on the Normative Role of Information Technology*, The Hage: T.M.C. Asser Press.
- Easterbrook, F.H. (1996), «Internet and the Law of the Horse», *Univ. of Chicago Legal Forum* 207.
- Elaluf-Calderwood, S. & P. Tsatsou (2007), «Trust among SMEs in DBE: Theoretical and Methodological Foundations for Establishing Trust through a Knowledge Base of Regulatory Issues», in: F. Nachira et al. (eds.), *Digital Business Ecosystems*, Luxembourg: EC, pp. 98-105.
- European Commission (2007), *What is e-Business?*, e-Business Watch, Luxembourg.
- European Commission (2005), The Commission's contribution to the period of reflection and beyond: Plan-D for Democracy, Dialogue and Debate, COM (2005) 494 final.
- European Commission (2001), *European Governance. A White Paper*, COM (2001) 428.
- Farell, H. (2002): «Hybrid Institutions and the Law: Outlaw Arrangements or Interface Solutions», *Zeitschrift für Rechtsoziologie* 23, pp. 25-40.
- Fernández Rozas, José Carlos (2004), *Ius mercatorun: autorregulación y unificación del derecho de los negocios transnacionales*, Madrid, Consejo General de los Notarios.
- Froomkin, M. (2005), «International and National Regulation of the Internet», in: E.J. Dommering & N.A.N.M. van Eijk (eds.), *The Round Table Expert Group on Telecommunications Laws: Conference Papers.*
- Glader, M. (2006), *Innovation Markets and Competition Análisis. EU Competition Law and US Antitrust Law*, Col. New Horizonts in Competition Law and Economics, Edward Elgar, Cheltenham, UK/Northampton, MA, USA.
- Goddard, M. y R. Mannion (1998): «From competition to co-operation», *Health Economics* 7, pp. 105-119.
- Gow, G., Elaluf-Calderwood, S. y Tsatsou, P. (2005): "DBE Regulatory Framework: Task B11: Knowledge Base of Regulatory Issues" WP 32, M32.2, prepared by the London School of Economics, November.

- Holznagel B., Werle, R. (2002): «Sectors and Strategies of Global Communication Regulation», *Zeitschrift für Rechtsoziologie* 23, pp. 3-24.
- Hosein, I., Tsiavos, P. y Whitley, E.A. (2002): «Regulating Architecture and Architectures of Regulation: Contributions from Information Systems», *Int. Review of Law Computers & Technology*, Vol. 17/1, pp. 85-97.
- Bocken, H., y De Bondt, W., *Introduction to Belgian Law*, Kluwer Law International, 2001, pp. 328 ff.
- Kleve, Pieter y Richard De Mulder (2005), **«**Code is Murphy's law», *International Review of Law Computers & Technology*, Volume 17, 3, pp. 317-328.
- Koops, B.J. et al. (eds.) (2006), *Starting Points for ICT Regulation,* The Hage: T.M.C. Asser Press.
- Lacruz Berdejo, J.-L., *et al*. (2002), *Elementos de Derecho Civil, I, Parte General,* Vol. 1,, 3.º ed., revisada y puesta al día por Delgado Echevarría, J., Dykinson, Madrid, 2002.
- Leenes, Roland y Bert-Jaap Koops (2005), **«**'Code': Privacy's death or saviour?», *International Review of Law Computers & Technology*, Volume 17, 3, pp. 329-340.
- Lessig, L. (2006), *Code 2.0*, NY: Basic Books.
- Lessig, L. (2003), «Law Regulating Code Regulating» *Loyola Univ Chicago Law Journal* Vol. 35, pp. 1-14.
- Lessig, L. (2002), *El código y otras leyes del ciberespacio*, Madrid: Taurus.
- Macaulay, S. (2000) «Relational Contracts Floating on a Sea of Custom? Thoughts About the Ideas of Ian MacNeil and Lisa Bernstein», *Northwestern University Law Review* 94, pp. 775–804
- Mandel, G.N. (2007): «History Lessons for a General Theory of Law and Technology», *Minnesota Journal of Law, Science & Technology* 8/2, pp. 551-570.
- Mifsud Bonnici, J.P. (2008), *Self-Regulation in Cyberspace*, The Hage: T.M.C. Asser Press.
- F. Nachira, A. Nicolai & P. Dini (eds.) (2007), *Digital Business Ecosystems*, Luxembourg.
- Fuentes Naharro, M. (2010), «Distribución selectiva e internet: análisis de la problemática concurrencial del fenómeno desde las restrcciones verticales a la libre competencia», *Revista de Derecho de la Comptencia y la Distribución* 6, pp. 117-141.
- Nonet, Ph. y Ph. Selznick (1978), *Law and Society in Transition*, New York: Octagon.
- Pérez, J. et al. (2008), *La gobernanza de internet*, Ariel, Barcelona.
- Polanski, PP. (2007), *Customary Law of the Internet*, The Hage: T.M.C. Asser Press.
- Reidenberg, J. (1998), «Lex informatica», *Texas Law Review* 76, p. 553 ff.
- Reidenberg, J. (1996), «Governing Networks and Cyberspace Rule-Making», Emory Law Review, 45, 1996.
- Rhodes, R.A.W. (1997): *Understanding Governance*, Open University Press.
- Rhodes, R.A.W. (1996): «The new governance: Governing without government», *Political Studies* 44 (4), pp. 652-667.
- Rodriguez de las Heras, T. (2006), *El Régimen Jurídico de los mercados electrónicos cerrados (e-Marketplaces),* Madrid, Marcial Pons**.**
- Schoubroeck Van, C., H. Cousy et al. (2001a) *Virtual Enterprise Legal Issue Taxonomy*. K.U Leuven University ALIVE Project, at: www.vive-ig.net/projects/alive.
- Selznick, R. (1985), «Focusing Organizational Research on Regulation», in: R. Noll (ed.), *Regulatory Policy and the Social Sciences*, Berkeley.
- Solum, L.B. & M. Chung (2004), «The Layers Principle: Internet Arquitechture and the Law», *Notre Dame Law Review* 79/3, p. 815-948.
- Teubner, G. (1986), «After Legal Instrumentalism? Strategic Models of Post-Regulatory Law», en: G. Teubner (ed.), *Dilemmas of Law in the Welfare State*, Berlin: W. de Gruyter, p. 229-325.
- Uría, R. & Menéndez, A., et al. (2006), *Curso de Derecho Mercantil*, t. I, 2.ª ed., Thomson-Civitas, Madrid.
- WGIG (2005a), *Reforming Internet Governance*, at: http://www.wgig.org/index.html.
- WGIG (2005b), *Internet Governance*, at: http://www.wgig.org/index.html.