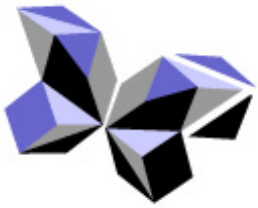

Digital Business Ecosystem

Contract n° 507953

Workpackage 32

Regulatory Framework

Task B11: Knowledge Base of Regulatory Issues

Deliverable 32.1

Literature Review

Information Society Technologies

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

Contract Number: 507953

Project Acronym: DBE

Title: Digital Business Ecosystem

Deliverable N°: 32.1

Due date: 30/04/2005

Delivery Date : 30/04/2005

Short Description:

This report presents a review of fundamental regulatory issues that have been identified as most significant during the initial adoption of e-business services among European small and medium-sized enterprises (SMEs), and to building and maintaining trust in digital ecosystems more generally.

Partners owning: LSE, Department of Media and Communications
(Gordon Gow, Kristina Glushkova, Silvia Elaluf-Calderwood)
Partners contributed:
Made available to: All project partners and the EC

VERSIONING		
VERSION	**DATE**	**AUTHOR, ORGANISATION**
1	30/04/05	Gow, Glushkova, Elaluf-Calderwood, LSE
2		
3		
4		

Quality check
1st Internal Reviewer: Neil Rathbone (IBM)
2nd Internal Reviewer: Tim Romberg (FZI)

Table of Contents

Executive summary

The aim of the literature review presented in this deliverable has been to report on key regulatory issues identified as most significant during the initial adoption of e-business services among European SMEs, and to building and maintaining trust in digital ecosystems more generally. The literature review provides a necessary pre-requisite for subsequent activities in task B11 and takes the first step towards establishing a knowledge base of regulatory issues relevant to the DBE vision. The need for such a knowledge base has been suggested by Nachira (2002) as a way of tackling the complexity of regulations applicable to e-business and the lack of knowledge and resources on the SME side to address this complexity, which currently constitutes one of the major barriers to SME e-business adoption.

The literature review adopted the thematic notion of trust as the initial point of focus inasmuch as academic commentators and practitioners have increasingly recognized it as a key enabler of e-business. The regulatory domain is central to building trust relationships in services and technological solutions, business activities and in access to information. However, an obstacle to assessing the role of trust in the DBE vision is that much of the current research has focused on B2C settings rather than B2B settings. Nonetheless, it is possible to model regulatory trust using types X, Y and Z, which describe various interaction scenarios between SMEs in the DBE vision.

Taking up the theme of trust the literature review identifies the three building blocks of regulatory trust: privacy and consumer protection, e-signatures and security, jurisdiction and consumer protection. Each of these building blocks provides the foundation for developing a more complex investigation and analysis of regulatory issues relevant to sector-specific and local implementations of the DBE. The literature review sets out the generic layer regulatory issues in each of the building blocks and highlights the areas to be considered in the context of the DBE vision.

Privacy and consumer protection refers to the regulatory issues arising in the processing, control and distribution of personal and consumer data over electronic formats, taking into account the individual rights and freedoms of the e-business users. The

challenges for the DBE vision in this area include defining the level of data sharing in line with existing data protection regulations, limiting data sharing with third parties external to the agreements, and providing a means of generating traceable records to deal with any breaches of the data sharing agreements

E-signatures and security refers to the issues arising when sharing information over digital media, where regulatory considerations are especially important in the areas of authentication, digital signatures, electronic invoicing and payments. In the context of the DBE, relationships between partners will always lead to transactions and payments of some type, and the issues related to e-signatures and authentication will be important for establishing and sustaining trust between partners. In addition, considerations of interoperability of electronic invoicing systems and the traceability of processes within these systems may be a significant factor in ensuring successful collaboration between partners.

Jurisdiction and consumer protection refers to the issues resulting from the cross-border nature of many e-business services, and the associated challenges in contractual relationships between goods or service providers and customers, such as jurisdictional issues and means for resolving cross-border disputes. The challenges in this building block include the lack of knowledge and legal expertise on the side of the SMEs of the rules applicable to e-business in the jurisdictions of their potential business partners, compliance with information requirements in relation to contracting process, the effects of the liabilities risk exposure on SME willingness to join the DBE and availability of cost- and time-efficient mechanisms for resolving e-business disputes.

The implications of the literature review suggest that regulatory considerations identified are an important, if not crucial, part of ensuring the realisation of the DBE vision in the long run. The issues identified in the document are used as a basis for determining the particular areas of the regulatory environment to be investigated in relation to sector-specific and local implementations. The document concludes by setting out the questions to be approached at the next stages of the task and suggesting the relevance of other EU funded research in the area of e-business regulation as an additional source of guidance.

Introduction

The vision of the Digital Business Ecosystem is "to create an integrated, distributed pervasive network of local digital ecosystems for small business organizations and for local e-governance which cooperates exchanging dynamically resources, applications, services and knowledge." (Nachira 2002:18). In order to realise this vision, it is necessary in the first instance to promote trust relationships among DBE participants and potential participants by enabling and supporting the creation of services and transactions that will be compliant with EU, sector specific, and local regulatory requirements. While regulatory requirements aim at establishing certainty in commercial exchanges, it is often the lack of awareness and expertise about regulatory issues that creates uncertainty and reluctance in e-business adoption among small business organizations. Therefore, the DBE vision, if it is to be viable in the long term must take into account the regulatory environment and related concerns relevant to those organizations for which it purports to offer the greatest benefits.

This deliverable presents a review of fundamental regulatory issues relevant to the DBE at the generic layer that will support basic components and services (Nachira 2002:13). The term 'fundamental' in this context refers to those areas of policy and regulation that have been identified in published reports and sources as most crucial to overcoming trust barriers in e-business adoption. This report refers to these areas as *building blocks of trust* that include matters such as privacy and data protection, security and authentication of digital documents, electronic invoicing and payments, online contracts, jurisdiction and dispute resolution — issues that make up a significant part of the regulatory domain within which the DBE will come to exist. The literature review, however, is not intended to identify every potential regulatory issue that might enter into play—this would be neither feasible nor helpful in a practical sense—but is intended as a basic methodological step necessary in preparing and undertaking the successive stages of research for task B11. These stages will involve the development of a sector-specific knowledge base (Activity B-11.2) and a localized knowledge base (Activity B-11.3), each intended to parallel the conceptual development of the DBE vision and its implementation

(Nachira 2002:13). Findings from this literature review are also intended to support a transfer of knowledge to other tasks within Work Package 32. More specifically, these are task C-46 Knowledge Base Model of the Regulatory Framework (ISUFI) and task C-52 Contracts and Agreements (WIT).

The decision to limit the focus of this literature review to fundamental regulatory issues is both practical and methodological. A comprehensive review is neither feasible, given time and resource constraints, nor is it appropriate at this stage of research. Moreover, the literature review identified a number of EU-funded projects that have been involved with very similar concerns and it was determined to assess these for their potential contribution to DBE-specific research (see Appendix 2 for a summary). For instance, in February 2005, a meeting was arranged with TrustCoM IP to discuss possible linkages with the DBE and with Task B11. While the outcome of the meeting was helpful, it primarily highlighted a number of complicating factors and underscored the need for a systematic, step-wise engagement with the regulatory domain as it pertains to the DBE vision. In many cases, the EU-funded initiatives are also well resourced and have taken the lead on researching many questions that are relevant to the DBE vision.

Given this early experience, it was determined that the initial stage of research—and a necessary prerequisite for the subsequent activities in task B11—should be to establish an baseline understanding of the policy and regulatory domain within which the DBE is being conceptualized, created, and implemented. This foundation is herein referred to as the "Generic Knowledge Base" (Activity B11.1), and is intended to provide fundamental perspectives on a range of issues that have been identified in the literature as essential factors for establishing trust relationships in e-business settings, and specifically for small and medium-sized enterprises (SMEs) in the European Union.

This report also recognizes that the DBE vision is ambitious and clearly seeks to move beyond "e-business" and toward a "digital business ecosystem"—a vision portrayed by Nachira (2002) as a ladder of adoption for Internet technologies. This model of adoption suggests, at least methodologically, that certain fundamental regulatory concerns affecting implementation of the DBE vision must be addressed before turning attention toward the more complex dynamics of a self-organizing, evolutionary network. As such, in addition to providing a Generic knowledge base, this review will also serve to support the

identification and research design of case study activities in the more complex undertakings represented by sector specific and local implementations of the DBE (these will be taken up under Activities B11.2 and B11.3).

The structure of the document is as follows. Following this introduction, section 1 is devoted to the background for this report, outlining the need for the knowledge base of regulatory issues. Section 2 examines the role of trust in e-business and regulatory trust in the context of digital business ecosystems. Section 3 identifies and conceptualises "the building blocks of trust" model that has been adopted as the framework for the literature review. Section 3 identifies and discusses a set of regulatory issues most significant during the initial adoption of e-business services among European SMEs. Section 4 concludes with a summary of key findings and an assessment of their implications for the DBE vision and for subsequent stages of Task B11. The report also includes a set of appendices intended to provide an overview of sources on the EU legal framework for e-business and sources of related research activities (completed and ongoing) within the EU.

1. The Need for a Knowledge Base of Regulatory Issues

The adoption of new forms of e-commerce and e-business in the European small and medium enterprise (SME) sector has been identified by policy makers as a key priority for fostering innovation and competitiveness of the European SMEs in global markets (EU Commission 2005). The aim of the Digital Business Ecosystem (DBE) is to overcome existing barriers and to promote innovative forms of software creation, knowledge sharing and community building, thereby enabling long-term growth and competitiveness of the European SME sector. As envisioned by Nachira (2002), the DBE is intended to foster new and flexible modes of co-operation and networking through a dynamic aggregation and self-organizing evolution of services and organisations by means of open-source methods of software and service creation.

This vision contrasts radically with business ecosystem concepts based on proprietary methods of software and service creation, where control over infrastructure, services, and knowledge can be tightly managed; for example the DBE vision does not include hierarchical service and application frameworks such as those characterized by firms such as SAP, Novell or Microsoft .NET in which a main controller or owner of the software code rights is clearly in control of development. Within a proprietary model, these elements are produced, transferred, and implemented in a managed process, usually with important checks and balances in place to ensure quality of service and compliance with policy and regulatory environments within which the systems will operate.

The DBE vision, however, does present some unique and very difficult challenges insofar as it has chosen to adopt an open source model. An open source model suggests a decentralized undertaking, open to a diverse range of participants across many locations, making quality control difficult to achieve. Issues such as favouritism in the hierarchy creation, risk of exclusion or flaming, peer review mechanisms, problems in measuring team performance, effective correction of software errors, management of human resources have all been highlighted in the literature as often creating difficulties in open source

environments (Raymond 1999; Bezroukov 1999). The aim of achieving self-organization in the DBE suggests a higher order capability to reproduce components with minimum intervention of human agents, thereby raising the stakes again for quality control.

The complexity of regulations applicable to e-commerce and e-business transactions and the lack of knowledge and resources on the SME side to address this complexity are identified as one of the barriers that need to be overcome in order to realise the digital business ecosystem vision. Nachira, for instance, has stated that, 'unlike larger companies, with their teams of lawyers and consultants, SMEs tend to avoid the legal risks of engaging in cross-border commerce.' (Nachira 2002:6). This claim is validated by results of a recent consultation on the nature of legal barriers in e-business, where over 75 % of companies did not consider the regulatory framework for e-business to be satisfactory, while 46 % admitted having insufficient information about applicable legislation (EU Commission 2004). The consultation, in which a large majority of participants were SMEs, also suggests that the complexity of regulatory requirements, differences between legislation on national level, and late implementation of EU Directives relating to e-commerce are also behind the slow adoption of e-business. In response to this situation, Nachira's vision for the DBE identifies an adoption strategy comprised of three action points:

- The creation a knowledge base of norms and laws to support service creation;
- The identification of alternative methods for dispute resolution;
- The development of training and learning modules for SMEs.

The aim of the literature review reported in this document is to take an initial step toward the fulfilment of the first requirement through the creation of a knowledge base of regulatory issues relevant to the generic layer of a digital business ecosystem. Nachira describes this layer as 'a common support environment and a *generic* basic infrastructure which includes basic service components, generic integrated solutions and infrastructure components' [emphasis in original] (Nachira 2002: 13, 15).

However, the requirement to create a knowledge base of norms and laws to support basic e-services faces a number of significant obstacles if the DBE vision for self-organisation or an "evolutionary systemic process" (Nachira 2002: 13) is to be achieved. Foremost among these is the range and complexity of norms and laws that will apply to any number of business organisations operating in different sectors and across jurisdictional

domains. This is of course not to mention the immense challenges associated with organisational and cultural differences that affect the activities of small and medium sized enterprises (Burn 2000; Hornby et al, 2004). The DBE vision, for instance, encompasses at least 25 countries of the European Union, and with some 20 languages officially distributing guidelines about e-businesses practices (EbuinessLex 2005). Moreover, there is a pronounced gap in the adoption and use of information and communication technologies (ICTs) among EU member states, and part of the rationale behind the DBE vision is to address the 'regional digital divide arising from the different rates of progress within e-business development within the EU', and with particular reference to the countries of Southern Europe (Nachira 2002:3)

The formidable challenges to the creation of a knowledge base of norms and laws for the DBE may not be insurmountable, but the task must be approached systematically and in a step-wise fashion if the complexity of such an undertaking is to be effectively managed. Furthermore, if the full DBE vision is to be achieved then this knowledge base of norms and laws must lend itself to the dynamics of self-organisation and open source principles of development. This suggests that research and development activities behind the creation of such a knowledge base should *not* be directed at identifying specific "norms and laws" but, rather, that research and development should be aimed at developing a methodology and model that will facilitate specific knowledge transfer autonomously through the interactions of a "virtual learning community" (Nachira 2002:14). It is not clear by any means, however, if such a methodology and model are achievable in practice, given the current state of knowledge about self-organising systems and studies of social practice (Mingers 1997a and 1997b).

The intent of this literature review is to take the first step toward the systematic development of the methodology mentioned in the previous paragraph. The report therefore presents the findings from a review of issues identified as salient features of the regulatory domain within which the DBE vision is being proposed. The outcome of the review is intended to initiate the development of a generic knowledge base that will then provide the foundation for refining the methodology as it is applied to subsequent stages of task B-11 in the sector specific and local implementation cases. In addition, the findings from this review will be formalised into a taxonomy intended to support work being

undertaken by task C-46 Knowledge Base Model of the Regulatory Framework (ISUFI) and task C-52 Contracts and Agreements (WIT).

2. Regulatory Trust and the DBE Vision

2.1. Trust and e-Business

In attempting to identify and assess the regulatory domain of the DBE vision, the literature review adopts the thematic notion of *trust* as the initial point of focus. Both academic commentators and practitioners increasingly recognize trust as a critical enabler of e-business (Yovovich 1996; Sultan et al 2002; Swan & Rosenbaum 2004; Ruppel et al 2003; Keen 2000; Clarke 2002a). During the early phases of online commercial activity the notion of trust was mainly regarded as an issue related to security and privacy for commercial websites. Today, however, it has taken on more complex and pervasive attributes and some see it as the foundation of the digital economy (Shankar et al 2002; Pavlou 2002a) – an economy that involves new organizational forms, collaborative activities and complex partnerships that rely on trust relationships for their success. Trust therefore provided the thematic backdrop to the research question that guided the overall literature review process:

> What are the key regulatory issues that have been identified as most significant during the initial adoption of e-business services among European small and medium-sized enterprises (SMEs), and to building and maintaining trust in digital ecosystems more generally?

Trust relationships are central to e-business activities simply because any kind of economic transactions requires a level of confidence. Mechanisms for minimizing risk have therefore existed for a long time, credit bureaus and insurance companies being two longstanding institutions that have arisen out of this need. In the context of online commerce, however, trust relationships may be more difficult to establish and sustain: not only are there difficult challenges in establishing the trustworthiness of parties in the online environment but electronic networks also provide increased possibilities for opportunistic behaviour compared to other settings (Mansell and Collins 2004; Pavlou 2002a; Jarvenpaa and Tractinsky 1999, Clarke 2002b). Recent research on barriers to e-business indicates that the difficulty in establishing trust relationships has been the main deterrent for companies globally to engage in e-business activities (Shankar et al 2002). More specifically to the EU context, considerations of trust have been identified as one of the

most important obstacles to e-business adoption in different sectors of the economy (EbusinessWatch 2004).

The regulatory domain is central to building trust relationships, and this is evident in the common characterization of 'trust' as a measure of confidence required by two or more parties to enter into economic exchange. A trust relationship might be described in the following manner:

> The willingness of a party to be vulnerable to the actions of another party based on the expectations that the other party will perform a particular action important to the trustee, irrespective of the ability to monitor or control that other party. (Mayer, Davis and Schoorman 1995)

In other words, trust enables action by establishing confidence among interested parties in the expected outcomes of current or future transactions (Clarke 2002a; Dutton and Sheppard 2004). One important prerequisite to confidence is 'certainty', which is a core issue for SMEs operating in a complex regulatory environment. In the e-business context envisioned by the DBE, certainty is related to trust in each of the three facets that Nachira (2002: 14) has identified as necessary to a digital ecosystem:

- Trust in services and technological solutions
- Trust in business activities
- Trust in knowledge

Trust in services and in technological solutions is a measure of confidence expressed in terms of security and reliability. This facet of trust comes close to the notion of 'technological trust' (Rosenbaum 2003) or 'belief that technologies will perform reliably and will not be used for untoward purposes'. For trust relationships to develop within the DBE, developers and users need to have a confidence that both the basic layer and supported applications provide a necessary degree of security and that risks to the services provided using the DBE platform are minimised;

Trust in business activities is a measure of confidence expressed in terms of the mutual recognition of accepted practices and procedures for specific sectors and local contexts. This facet of trust is related to the notion of 'institutional trust' or a collective expectation that the procedures needed for carrying out transactions successfully will be facilitated and followed (Pavlou 2002). For companies to successfully adopt and continue using DBE services, there will need to be trust relationships established in relation to the

expected patterns of behaviour and organisational practices adhered to within the digital business ecosystem environment – without such shared understanding and existence of supporting structures to facilitate the creation of such trust relationships, cultural and organisational differences are likely to inhibit the formation of business relationships within in the DBE vision;

Trust in knowledge is a measure of confidence expressed in terms of symmetric access to information. Because knowledge is a critical asset in e-business activities (Fahey et al, 2001), differences in access to knowledge and information relevant for e-business activities can lead to unequal advantage within the a business ecosystem environment. Hence facilitation of symmetric knowledge sharing and equal access to information is important for establishing trust relationships between companies participating in the DBE vision.

Addressing each of these facets of trust in a digital business ecosystem depends on a variety of factors, such as organisational arrangements, technological solutions, cultural norms, economic and competition considerations, and crucially, regulatory and legal environment within which the DBE will operate. The next section turns to examination of the role of regulatory issues in establishing and sustaining trust relationships between e-business parties and outlines a proposed model for approaching regulatory trust in a digital business ecosystem environment.

2.2. Regulatory trust in a digital business ecosystem

An obstacle to assessing the role of trust in the DBE vision is that much of the current research in the field has largely focused on business-to-consumer (B2C) settings rather than business-to-business (B2B) settings. Unfortunately much of the B2C-oriented research is not directly applicable to B2B concerns and more specifically to e-business B2B concerns because of several important differences. First, the results of a consultation on trust barriers in B2B e-business activities in the EU (2002) indicates that B2B relationships are usually characterized by a high level of familiarity between parties and are often based on long-standing cooperation between firms. In order to exploit the advantages of e-business practices, SMEs may need to interact with unfamiliar parties and to put new

procedures into place, thereby creating a need to establish new and unfamiliar trust relationships in each of the three facets listed above (technology, business activities, and knowledge).

Second, in e-business B2B settings trust relationships may be spread across multiple parties and the B2C model of a simple buyer/seller relationship may not adequately describe many B2B transactions (Meents et al 2003). Finally, e-business B2B interactions may be structured by organizational and institutional arrangements that employ formal control mechanisms (e.g., certification), thereby establishing a confidence mechanism for a specific sector or local setting rather than between individual sellers and buyers (Pavlou, 2002).

There is a large body of literature on interorganisational and B2B trust which distinguishes several types of factors that influence levels of confidence, such as monitoring (Zucker 1986), accreditation (Pavlou 2002), reputation of parties (Meents et al 2003), and feedback mechanisms (Ba & Pavlou 2002). Despite this material, the importance of the regulatory domain generally, and especially in the context of e-business activities, does not appear to be well covered so far. Nevertheless, the role of regulatory domain in establishing and sustaining trust relationships in a B2B setting is vital. As Mann (2000) points out, regulatory and legal considerations are part of the necessary 'infrastructure' that makes possible the conduct of e-business: the 'infrastructure of protocols, laws and regulations' which 'affects the conduct of those business engaging in and impacted by electronic commerce, as well as the relationships between businesses, consumers, and government' (2000:3). Regulations such as those relating to technical standards, certification procedures, privacy, content requirements all affect the conduct of e-business activities, and the regulatory domain is central influence in shaping trust relationships in online settings generally (Mansell and Collins 2004). Hence, what might be called 'regulatory trust' is likely to be an important consideration for SMEs seeking to adopt e-business practices.

Regulatory trust in a digital business ecosystem can be modelled using categories proposed by Meents, Tan and Verhagen (2003) and developed for B2B virtual marketplaces. These authors suggest a three-dimensional model based on the basic types of trust relationships that one might expect to develop out of the DBE vision. First,

participants joining a virtual marketplace must have confidence that it will provide secure services over proven technology, and that it is capable of facilitating trust relationships in business activities. This is referred to as Trust X. Second, there must be a level of confidence that other participants joining a virtual marketplace are not behaving opportunistically, perhaps through asymmetrical access to information. This suggests a need to ensure that opportunistically behaving companies are denied access or, alternatively, that symmetric access to information in certain areas is given high priority in order to deter unwanted opportunistic behaviour. This dimension is referred to as Trust Y. Finally, a virtual marketplace must ensure trust relationships can be established between participants themselves; that is, it must engender confidence that bi-lateral transactions will be honoured. This dimension is referred to as Trust Z.

This basic model of trust relationships can be applied to the DBE vision, and is depicted in Figure 2.2. Using this framework, a number of specific factors influencing regulatory trust can be distinguished.

Trust type X in this model refers to trust (perceived or actual) on the side of joining companies towards the DBE.

- From regulatory perspective, the expectation is that technical architecture and basic services incorporate the existing e-business regulations, and provide facilities for carrying out transactions in a way that will ensure compliance with established laws and norms.

Trust type Y in this model refers to the expectation from established DBE participants towards joining companies.

- In order to establish good trust relationships, companies are expected to comply with established laws and norms, and to avoid creating unnecessary risks for their counterparts within the DBE.

Trust type Z in this model refers to the trust relationships between DBE participants themselves.

- This type of trust is supported by confidence in the ability of norms and laws to govern the interactions resulting in part from the self-organisation and evolution of the DBE implementation.

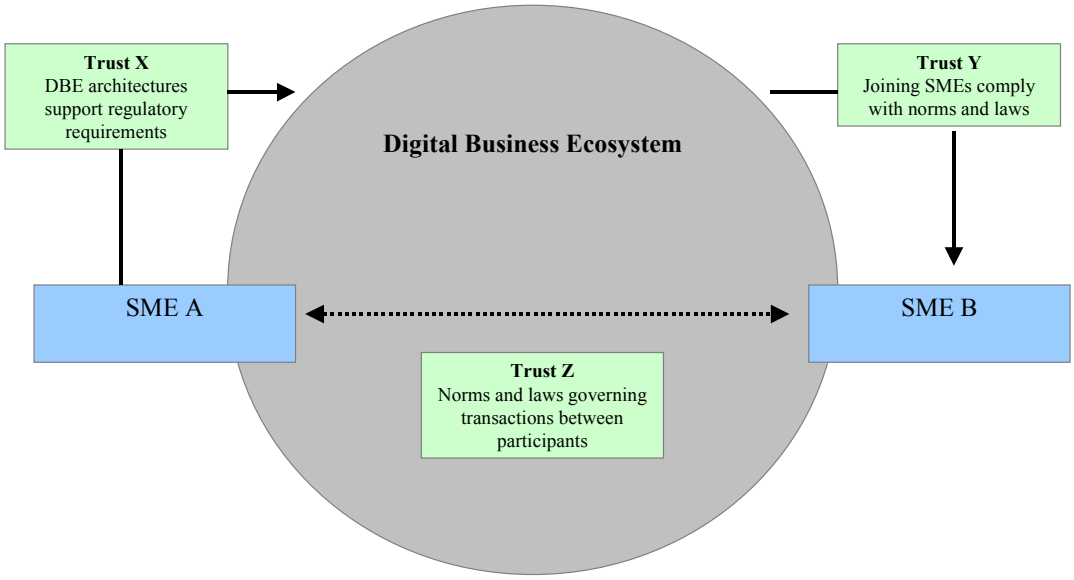

Figure 2.2 Types of regulatory trust in a digital business ecosystem

All three dimensions of regulatory trust are interrelated and all are necessary to support confidence of developers and users sharing the DBE vision. For example, in case of rules related to protection of personal data, the software architectures should at least not infringe, and preferably facilitate, the proper handling of data (trust X); joining SMEs should comply with applicable regulations and not misuse the personal data they acquire as a result of transactions within DBE (trust Y); and finally in case of such misuse, the mechanisms for identifying the misuse and legal instruments for dealing with such misuse should be in place (trust Z). On each of these dimensions, however, different considerations apply:

- Trust type X is of concern with respect to the design of system architecture and supported services;
- Trust type Y is a concern of institutional and governance arrangements of the DBE vision;
- Trust type Z is established on the ongoing co-operation and contractual obligations between companies and is dependent on both the conduct of the SMEs and the existence of legal remedies to provide adequate solutions in the event breaches occur.

In order to facilitate these three dimensions of regulatory trust, it is first necessary to identify the regulatory issues to support the DBE developers, governing bodies and users at

the different stages of software lifecycle. As outlined in section 1 of the document, the work of task B11 is directed towards developing such a knowledge base, departing from the analysis of the features of regulatory environment that are most relevant for overcoming trust barriers to e-business and taking into account the different dimensions of trust in the digital business ecosystem context. In the following sections the domains of the regulatory environment that have been identified as critical for considerations of trust are introduced, followed by an outline of the methodology adopted in task B11 to examining these areas.

2.3 The building blocks of regulatory trust

The areas of the regulatory domain that are most significant for initial adoption of e-business in the EU have been identified based on the empirical work on the topic. These include a report published by the European Commission (2004b) on the ICT usage by companies, the results of the open consultation on legal barriers in e-business (EU Commission 2004a), proceedings of the European E-business Legal Conference (2004) and the research carried on legal issues in e-business out within FP5 and FP6 funding. Relevant research projects within FP5 include ECLIP (Electronic Commerce Legal Issues Platform), ELEGAL (Specifying Legal Terms of Contract in ICT Environment), ALIVE (Advanced Legal Issues in Virtual Enterprises) and currently ongoing TrustCoM (Trust, Security and Contract Management for Virtual Organisations) and Legal-IST (Legal Issues for the Advancement of Information Society Technologies)[1].

The 1997 *European Initiative on e-Commerce* identified the following areas as relevant to e-business activities: Jurisdiction, liability, taxation, copyright, authentication, encryption, data protection, content, and consumer protection (Berkey 2002). In terms of high-level regulatory considerations, there are four EU Directives directly relevant to e-commerce: Legal aspects of E-Commerce; Electronic Signatures; Data Privacy; E-Money. A number of other EU measures also have a bearing on e-commerce, such as directives on Distance Selling of Goods; Unfair Terms in Consumer Contracts; Distance Marketing of

[1] A summary of these research activities is included in the appendix to this report.

Financial Services; Copyright and Related Rights as well as regulations on Jurisdiction and Enforcement of Judgments; Dual Use Export Control Regime.

A number of regulatory domains most immediately relevant to establishing trust relationships in e-business activities have been identified for the purposes of our task. Following an extensive review of literature from US, EU, and international organizations, Berkey (2002) has identified three main categories of international regulatory issues related to e-business:

- **Privacy and consumer protection** refers to the processing, control and distribution of personal and consumer data over electronic formats, taking into account the individual rights and freedoms of the e-business users;
- **E-signatures and security** refers to the issues created with the sharing of information over digital media. It is a concern to ensure autonomy and cross-border interoperability through authentication, integrity and non-repudiation;
- **Jurisdiction and consumer protection** refers to the issues resulting from the cross-border nature of many e-business services, and the associated challenges in contractual relationships between goods or service providers and customers, such as jurisdictional issues and means for resolving cross-border disputes.

These categories of regulatory issues represent the building blocks of regulatory trust, meaning that they are priority concerns when developing e-business initiatives. In other words, these are generic layer building blocks, which also means that they tend to identify a broad set of concerns without specifying how those concerns are relevant to any specific set of circumstances. It is necessary from a methodological standpoint to first establish these generic layer building blocks in order to move toward higher order specifications in sector and local implementations (see Figure 2.3.).

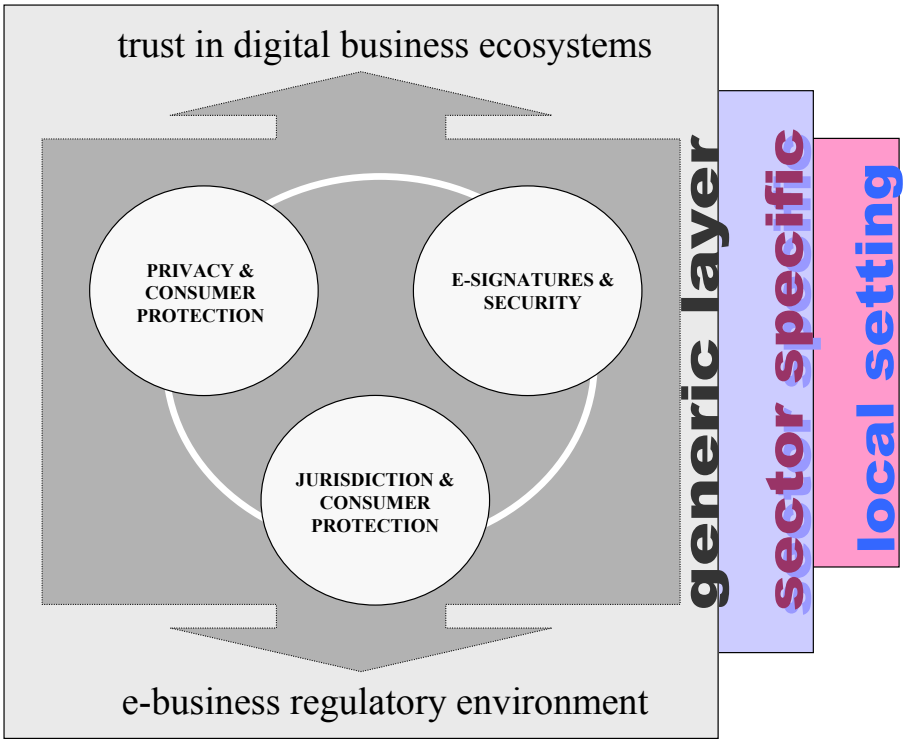

Figure 2.3. The three-stage research design for Task B11

In the initial stage, the building blocks of regulatory trust are approached at a generic level. This report identifies the key regulatory domains, describes key issues and relevant EU level policy and regulations. After the identification of the generic blocks, the methodology will be continuously refined and populated with information on regulatory requirements relevant to sector-specific and local implementation cases.[2] In these subsequent a research design that combines *bottom-up and top-down approaches* will be adopted. The issues identified at the generic level will form a basis for further investigation of sector-specific and local regulatory constraints based on the empirical cases from the field.

The research design follows the principle of requisite variety established in systems theory by W. Ross Ashby, which states 'The larger the variety of actions available to a control system, the larger the variety of perturbations it is able to compensate' (Ashby 1956). The principle of requisite of variety is relevant when working from a body of

[2] The specific sector and local content is to be defined based on the selected pilot cases.

general constraints toward complex instantiations, as can be expected of the DBE vision when it is implemented in successive layers proposed by Nachira (2002). 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 building blocks. By analogy, in order to manage the complexity of the regulatory domain it is helpful to build from general constraints towards the nuances of local implementations.

The logic of this approach can be illustrated with a hypothetical example from the travel industry. In this case, the issue of regulatory trust might concern the records of passenger information for flights to the United States (which requires this information for all inward flights). Figure 2.4. depicts a set of laws and norms established in a dependent hierarchy that follows the principle of requisite diversity.

Fig. 2.4. Layers of regulatory complexity in a hypothetical travel industry case

At the most basic (generic) level, the retention and access to the information on passenger records might be regulated at the EU level, through a specific Directive or other statutory instrument. This provides the baseline of regulatory trust on this matter, yet the International Air Transport Association (IATA) might apply sector-specific guidelines for companies that have additional considerations or other complicating factors. Finally, at the local implementation level, travel firms may apply specific bilateral or multilateral contractual terms and conditions for handling customer data. Whereas the EU regulatory domain provides a general set of constraints, both the sector specific and local

implementations build on and may extend those generic requirements. The methodology adopted is aimed at capturing the regulatory issues at all the three levels effectively.

The next section turns to identifying and assessing the specific building blocks of regulatory trust, outlining the importance and parameters of the areas identified as most relevant for the DBE vision.

3. Literature Review

3.1. The EU regulatory environment for e-business

The need for an accelerated development of a coherent regulatory agenda in order to maximise the benefits of 'information society technologies' was spelled out in the 1994 Bangemann report (Bangemann 1994), and a further call for establishing a coherent legal and regulatory environment to enable a 'vigorous growth in e-commerce' was raised by the 1998 Committee communication (European Parliament 1998). Since then the EU regulatory framework has evolved considerably and a number of directives[3] have been introduced to address the challenges raised by online business activities. These include the following:

- Electronic Commerce Directive (EU directive 2000/31/EC)
- Electronic Signatures Directive (EU Directive 1999/93/EC)
- Copyright Directive (EU Directive 2001/29/EC)
- Data Protection Directive (EU Directive 2002/58/EC)
- Distance Selling Directive (EU Directive 97/7/EC)

It has been suggested that with the adoption of the e-commerce regulatory framework a comprehensive legal basis for encouraging online commercial activity and reducing associated risks in the EU has been achieved – however, many challenges still remain (Jahankhani 2002; Pearce and Platten 2000).

As reflected by the Legal Barriers in e-Business (EU Commission 2004) consultation results, there are a number of obstacles that hamper the effectiveness of these regulatory measures. First, the transposition of the EU directives to national regulatory frameworks has neither been uniform nor quick, and the differences in legislation applicable at the national level increase legal uncertainty and raise the cost of regulatory compliance. Second, while issues related to B2C e-commerce are rather comprehensively covered by the existing legislation, problems arise in B2B transactions in general and in

[3] Directives are the most common form of EU level legislation, other forms such as proposals and recommendations represent more 'light-touch' forms of regulation.

relation to the evolving organizational forms in B2B e-business, such as virtual enterprises and digital marketplaces. Moreover, there are still major knowledge gaps and barriers caused by the complexity of the regulatory framework that need to be addressed in order for companies to be able to enter and operate in the e-business environment. All of these problems apply to a greater or lesser extent to all of the regulatory issues reviewed in this document.

The remaining sections review these regulatory issues as building blocks of trust relationships, outline the current regulatory measures in these areas at the EU level and suggest the relevance of these for the DBE vision.

3.2 Privacy and Consumer Protection

Defining the building block

Privacy is defined as the non-disclosure of stored or transmitted information relating to a uniquely identifiable entity, be it a company or an individual. Similarly, data protection is the prevention of unauthorised access to this information. An important question that remains unresolved is whether data protection principles should apply to aggregate information that does not refer to individual entities, such as profiles derived from databases (Berkey 2002). In the EU, data privacy has historically been viewed as a human rights issue applicable to individuals and EU privacy legislation has continued to develop along these lines with the growth of e-commerce. For instance, the European Directive on Privacy and Electronic Communications—E-Communications Directive (EU Directive 2002/EC/58)—bans placement of data-gathering cookies on users' computers or direct marketing by SMS messages to mobile phones without the individuals' prior consent.

In the sphere of industry, privacy is closely linked also to consumer rights and therefore forms part of most business-to-consumer (B2C) legal contracts, which are heavily regulated under EU law. The EU consumer of a product is the final link in a long chain of commercial transactions and, it might be argued, makes an informed choice regarding the country from which he or she purchases goods and, by implication, whether or not his or her consumer rights are to be governed by EU law.

EU legislation governing business-to-business (B2B) contracts is less stringent because many production processes will inevitably involve the transfer of company data to third-party countries outside the EU, which may not have an adequate level of data protection, but which is necessary as part of a chain of contracts. For example, the privacy legislation covering data in this case depends on the countries supplying the components required in the assembly of a consumer product. A complicating factor in determining the right to privacy and data protection is that security technology remains governed by national law. In the UK, for instance, an individual or company may be compelled to reveal an encryption key should the authorities demand it, whereas in Ireland there is no such legal provision. Given these difficulties in implementing B2B privacy legislation, EU-wide regulation in this area is unlikely to converge into a coherent body of rules in the near future.

Area of influence

Traditionally, the jurisdiction of courts has been defined in geographical terms but with the advent of e-commerce, these boundaries are no longer as relevant as they once were. This is as true of the EU borders as it is of national boundaries within the EU. The Internet has posed new challenges because it is no longer clear where transactions occur. If a wholesaler in Germany imports toys from China, the transaction might be regarded as if the seller went to Germany, or as if the buyer went to China. There may be areas in which different laws apply in the respective countries and different interpretations of existing laws. With regard to the privacy of the data exchanged during such transactions, the governing jurisdiction is even less clear. In some cases, neither country may be able to enforce legislation over data protection unless a bi-lateral agreement between trading partners is in place.

Legal mechanisms governing privacy in international transactions depend heavily on the geographical location of the industries involved and the extent to which the Internet is used as the medium of commerce. The Hague Convention on Jurisdiction and Foreign Judgements in Civil and Commercial Matters (1971) has been widely accepted as the standard covering conventional commercial transactions, but when applied to e-commerce its interpretation is necessarily different as legislation in one country may protect the right to private transactions and the associated exchange of private data, whilst another country's

laws might regard what is represented by the data as illegal. For instance, the French courts ruled in 2000 that Yahoo! Inc. was required to introduce technology blocking access to U.S.-based auction sites selling Nazi memorabilia as they contravened national law. Yahoo! then appealed to the U.S. courts to overturn the order on the grounds that the French government had no jurisdiction over what was effectively a voluntarily exchange of private data between French citizens and a company in the U.S. (It should be noted that shortly afterwards Yahoo! itself voluntarily banned the auctions from all its sites). This case shows how one country's laws regarding the privacy of electronic data transactions may conflict with another country's laws concerning what is represented by that data.

Despite these challenges, projects run under EU Fifth Framework Programme (such as ECLIP, ELEGAL, ALIVE, Octane) and Sixth Framework Programme (Legal-IST, TrustCoM) have attempted to identify the way EU legislation may be applied in individual countries to protect the rights of individuals or businesses regarding data privacy (see Annex 2). In the EU there have also been attempts (e.g. ECLIP—see Annex 2) to unify national data privacy legislation, some of which ultimately aim to provide a model of co-operation that could in future be extended beyond EU borders.

Addressing the issues at the EU level

Within the EU borders, important data privacy standard is established in the Regulatory Framework for Data Protection as per Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data. It is focused on individual and consumer rights, with European and national data supervisors overseeing the implementation and enforcement of the directive. In the field of B2B commerce, the Directive on Privacy and Electronic Communications 2002/58/EC offers detailed guidelines relevant to business, such as provisions for anonymity in billing, the protection of the right to withhold calling line identification, and providing emails that can be read without downloading additional information from the Internet.

Given the lack of international consensus regarding data privacy legislation, some non-EU bodies have proposed their own governing standards. These standards, which include guidelines and best practices, propose a means for building trust relationships but do not themselves guarantee that these relationships will be established and are not easily

enforced since they require widespread acceptance; if there are too many competing standards, none may be adopted. The International Chamber of Commerce Task Force on Jurisdiction, for example, emphasises self-regulation and on-line dispute resolution mechanisms based on voluntary industry codes of conduct. The intent of this approach is to avoid expensive arbitration. The OECD, ICC and Transatlantic Consumer Dialogue have also proposed their own sets of standards.

A high proportion of B2B transactions will necessarily involve the transfer of data to third party countries, for which the EU is unable to legislate directly. Protecting data privacy for such transactions is a more complex issue involving bi-lateral agreements and coherent international standards. Current legislation regarding the free movement of data is set out in Regulation (EC) 45/2001 of the European Parliament and of the Council of 18, but this applies only to personal, not business data. Guidelines for e-commerce involving third-party countries are still under development, overseen by the EU Advisory Body of Data Protection and Privacy and independent committees established by Articles 29 and 30 from the 95/46/EC Directive.

The existence of regulation, standards, guidelines and best practices, however, provide a necessary but not sufficient backdrop for the business environment. Such mechanisms do not by themselves create trust between individual parties involved in a transaction, since it is still the duty of each party to establish a reputation for reliability over time. This is particularly true for the privacy of business data, where failures in trust will not be detected immediately, if at all, and where there are few instruments for compensating a business for breach of trust. The consequence for a digital business ecosystem is that current legislation is only one factor in building confidence in data protection and privacy.

Relevance

In the context of the DBE, we encounter a particular issue relating to the management of databases to be shared between its members. These databases may contain data that can identify an individual as such or create sensitive data patterns. The Data Protection Working Party (2005) report highlights a number of issues concerning legal compliance in the use of the data (articles 6 and 7 from directive 95/46/EC). These issues

become more acute where sensitive business data is involved (article 8 of the same directive). In such cases, it states the following (Mahler and Olsen 2004):

- There shall be a level of anonymity when handling data;
- The purpose of the use of the data shall be clear and specific;
- Information and transparency in the handling of and access to the database must be clear;
- There shall be a clear relevance and proportionality in the access to the database, accuracy in its use, and ideally a non-automatic decision making process that can be stopped at any time;
- There shall be an evaluation of the data sensitivity;
- There shall be a clear policy concerning the rights of individuals to prevent or allow onward transfer of personal data;
- When issues arise from data disclosure and assessment of the level of information security, the level of sensitivity of the data should be stated.

While the DBE does not have a clear definition as a legal entity, there nevertheless remains a need to comply with a body of regulation that points to responsibilities and obligations, which in the case of the DBE vision can rarely be performed by a unique designated partner. Leadership roles might need to be rotational or shared by partners, where the DBE could act as a dynamic digital broker (see, for instance, Shankar 2002).

Considerations in the context of the DBE vision

The DBE applies the concept of privacy to two types of transactions: B2B and B2C. The advantage of the knowledge base of regulatory issues in terms of B2C is that law and governance at national or EU level already covers individual rights to privacy for consumers. With B2B it is slightly different, since there is a greater need for flexibility with sensitive data in order to produce a valuable exchange between trading companies.

In the digital business ecosystem risks associated with privacy are derived from the accessibility granted to raw data. For example, a manufacturer of shoes in Italy gets an order from a retail company in the UK to produce a model of shoes in a certain size. The company in Italy will have access to locations where the product will be delivered in the UK. It could be the case that the Italian company might find a different retailer in the UK to sell the shoes produced for the first retailer.

The challenges for the DBE vision are:

- To define the level of data sharing that does not violate current data protection regulation;
- To establish confidence between partners that data will not be shared with third parties external to the agreement and;
- To establish a means of generating traceable records to deal with breaches to the agreed data sharing agreements.

3.3. E-Signatures and Authentication

Defining the building block

In this section of the document we will present the building block of e-signatures and authentication. The areas of electronic invoicing and payment are also included as part of the e-signatures domain.

In order to understand this building block, the concept of security is important. Security, in this context, is a technical term relating to computer and information security, and often encompasses other concepts such as privacy, data integrity, accessibility and authentication. We do not intend to explore the technical issues relating to security since they are not often a matter for policy or legislation, especially given that the technology guaranteeing confidentiality, such as encryption algorithms, checksums and the associated software, is freely available. Similarly, accessibility is also a technical issue. For example, while unauthorized obstructing of a service, such as a website, may be against national law in most countries, the onus is almost always on the organization to install the technology to protect itself. Authentication, however, involves a number of policy issues such as membership, access rights and their revocation, and public certification of identity.

Authentication is the process whereby an entity (person, computer or organization) establishes that another entity is who it claims to be. It is closely associated with access control –granting or denying access to different resources based on identity–and with authorization, which includes both authentication and access control. Accurate authentication is one of the building blocks of trust since it provides the means for identifying any malpractice such as non-payment and prevents repudiation of a transaction

(i.e. denying that it ever took place), which without authentication may require only the deletion of, say, a file containing an invoice.

Electronic invoicing and payments are the processes related to the completion of online transactions for the purchase or exchange of goods and services. Secure payment and accurate monitoring of electronic payments are also building blocks of trust since they provide the means to oversee the processes involved in e-business transactions.

Digital signatures are one of the most widespread methods of proving identity. Using techniques borrowed from the field of cryptography, a digital certificate showing the details of identity can be electronically signed by a trusted party with a uniquely identifiable "signature". It is possible to establish a hierarchy of authority by chaining certificates, as in the following (hypothetical) example:

Customer A in Spain wants small accountancy company S in Amsterdam to prove its identity. S shows A its digital certificate, which has been signed by the local branch of the Association of Small Accounting Firms. The national office of the same association, whose own certificate has been signed by the Dutch Companies House and granted the authority to sign other certificates, in turn, has signed company's A certificate. Since the Dutch Companies House is the highest authority for identifying companies in the country, its own certificate may be "self-signed" and it is responsible for establishing the credentials of any organization to which it delegates powers. Such a body is known as a Certification Authority and its own certificate is known as a qualified certificate.

This example shows the importance of establishing a hierarchy of trust when authenticating companies. The European Union has implemented legislation granting electronic signatures, provided they are chained to qualified certificates and created by a secure signature creation device, giving them the same status as hand-written signatures. The legislation also states that the electronic signature should be unalterable (which can be guaranteed by the security technology). However, they have left it up to each member state to decide which body is responsible for certification, and each member state may also contract the function out to private service providers who will be liable for the validity of the signature.

Authentication may cover not only identification of the parties involved in an online B2B transaction, but may also provide an audit trail of activities during the transaction allowing any disputes about fact to be resolved efficiently. The Electronic Commerce Directive stipulates that all service providers must clearly identify themselves as party to the transaction in a manner that is easily, directly and permanently accessible to the intended customer and to the relevant authorities. In some industries such as business banking, networks include only a limited number of participants who join the network under its own terms and conditions. Trust is established through membership, there is no central authority, and electronic signatures may not be considered necessary. The directive cited allows for a degree of autonomy in such cases.

EU Invoicing directive (EU Directive (2001/1154/EC)–Updated 2004) contains the main body of legislation in this field. The directive provides recommendations in the following areas:

Encryption and Electronic Signatures: It is advised that all e-invoices should be transmitted in a secure environment using industry-accepted encryption technologies or other means, such as electronic signatures (also known as digital signatures), chained certificates and data digests. The purpose of an electronic signature is to state the identity or origin (who the sender claims to be). Certificates are chained ultimately to a recognized certification authority (to establish the authenticity of the sender). Data digests guarantee the integrity of the e-invoice data (to ensure that it has not been tampered with while in transit).

Electronic Storage: Electronic document storage is also accepted under this new legislation. Data can be stored in electronic format in any place provided invoices can be made available without undue delay. Some Member States may require notification of duration of storage, which can vary from State to State. Where digital signatures are used they should stay attached to each e-invoice during the storage period to guarantee authenticity throughout.

Notification for using E-invoices*:* EU businesses will now have the right to send invoices electronically without seeking approval from their national Customs Offices, providing prior notification is given. Third parties such as accountants can supply the

required security technology and expertise that might otherwise prove to be costly to develop in-house.

Considerations in the context of the DBE vision

In the context of a digital business ecosystem, relationships between partners will lead to payments or transactions of some type. On a general view they could be B2B or B2C oriented. In any case the mode of payment is a reflection of the actual trade of goods and services against the level of trust and security established between the partners (Abrazhevich 2001).

This level of trust and security is applicable to the way payments are made; either by account systems (generic systems, specialized systems, credit and debit systems) or by token-based systems (smart card systems, online cash systems). The unsatisfactory level of those means of payments might be resolved by dealing with mediating systems to reduce the limitation of the methods used to make payments (Bargh and Jassen 2002). The literature also highlights the limitations due to scalability, convertibility and interoperability of such systems (Buck 1997; Mazzeo 2004).

In regard to digital business ecosystems it is possible to identify that as well as the issues of security and privacy, a major concern for DBE partners may be

a) Incompatibility of electronic invoicing systems (different amounts of VAT, or taxation to be added to bills, territoriality of tax if invoicing is between different countries or economics zones)

b) Accountability and integration of those systems.

As the DBE vision develops into a functioning business ecosystem the issues described above will become critical in the development of successful relationships between partners. In the long run, the DBE initiative might even lead to proposed changes to the current directives to get a working framework in this area.

3.4. Jurisdiction and Consumer Protection

Defining the building block

The domain of jurisdiction and consumer protection as outlined by Berkey (2002) represents a broad category of regulatory issues stemming from the cross-border nature of many e-business transactions. While traditionally commercial activities took place within clear geographical boundaries, in e-business settings communication can take place from any location, raising new challenges related to the jurisdiction governing the transactions, choice of consumer protection law as well as resolution of cross-border disputes.

From the perspective of the DBE vision the main concerns in this domain centre around the regulatory issues related to cross-border online contracting. This section aims to identify and discuss the regulatory aspects of online contracting practices that are relevant to the generic layer of the DBE vision: the uncertainties related to validity of e-contracts, governing jurisdiction, information requirements, liabilities and the means for resolving cross-border disputes. In addition, the issues discussed in Section 3.3 in relation to digital signatures also apply to considerations of authenticity of contracts as to other documents signed by digital means.

While this report aims to identify the regulatory issues related to online contracting on a generic level, a number of EU funded projects have addressed different aspects of online contracting in more specific terms and may be relevant to the DBE vision: ECLIP examined legal issues in designing a web-contracting process; ELEGAL developed a library of model contracts with a focus on the construction sector; ALIVE carried out work on model contracts for Virtual Enterprises; TrustCoM project is running currently and aims to develop a contracting framework for Virtual Organisations.

Contracts in e-business

Contracts provide a means for formalising commercial relationships through mutual agreement that defines the obligations between two or more parties in a legally binding way. Generally defined as a *legally enforceable agreement in which two or more parties commit to certain obligations in return for certain rights* (Reinecke et al 1989), a contract is an essential foundation of any kind of economic interactions, serving as an instrument to

organise the exchange relationships and to reduce the vulnerability of transacting partners by putting legal obligations in place (Wigand et al, 1997; Blois, 1999).[4]

Online contracts are at the heart of the development of e-business, providing the very possibility to enter into business relationships online (Murray, 2005), are often seen as a positive development in contracting practices overall. As Angelov and Grefen suggest, electronic contracts serve to 'improve the efficiency and effectiveness of paper contracting and to extend the opportunities of the contracting parties' (2003:79). The fast pace of development since the advent of e-commerce has led to a high level of sophistication of online contracting practices, posing a variety of regulatory difficulties arising from new technological solutions (e.g. contracts concluded by software agents), as well as new organizational forms to be facilitated by electronic contracts (e.g. virtual enterprises).

On the other end of the spectrum are the very basic problems that companies encounter when entering e-business and initiating relationships with previously unfamiliar partners. The legal complexity involved in online contracting, and especially in cross-border settings, is one of the main sources of uncertainty for companies entering e-business. In fact, this is the most common legal issue encountered by EU companies as revealed by the consultation on legal barriers in e-business (EU Commission, 2004) with 39% of companies reporting problems related to online contracts, while in the consultation on trust barriers to e-business (EU Commission, 2002) 56% identified a lack of information on the terms and conditions of contracts as a major barrier to participating in digital marketplaces. It is hence an important set of regulatory concerns that need to be taken into account for the DBE vision. The following section describes the main regulatory issues related to cross-border online contracting and the relevant EU level regulatory measures.

[4] It has to be noted, however, that although in the literature contracts are often seen as either 'guarantors' of trust or substitutes for trust, the role that contracts play is more complex than these positions imply, and may vary depending on the context and features of the business relationship itself as well as change over time (Woolthuis, Hillebrand & Nooteboom 2002). While contracts are the basis for formalising relationships and do provide a degree of reliability, these are only one, albeit an important one, element of building trust relationships in e-business.

Validity and jurisdiction

The Electronic Commerce Directive is the basis for the recognition of validity of electronically concluded contracts across the EU[5] where rules relating to contracts are functionally similar to the international UNCITRAL model laws.[6] Article 9 (1) of the Directive requires Member States to 'ensure that their legal system allows contracts to be concluded by electronic means'. In principle, this implies that contracts entered into by electronic means should not be denied validity on these grounds. In practice, however, according to the review of the implementation across the EU, the directive has not yet been applied uniformly by the member states and in some sectors, such as financial services, there are practical barriers or conflicts with other regulatory requirements for recognising the validity of contracts concluded electronically (EU Commission 2003a).

While the process for conclusion of online B2C contracts is specified in detail by the Directive, in the case of B2B contracts the Directive is only concerned with non-discrimination between on- and off-line settings and does not specify what constitutes the rules for contracts to be legally binding, such as conditions of offer and acceptance. The questions of legal validity of B2B contracts in practice are decided by the contract law of the member state under which jurisdiction the contract is governed, where rules are likely to vary depending on the country and legislative system. These differences in legislation relating to contractual issues create problems for companies entering e-business, as there is no certainty about conditions applicable to contracts. Work at the EU level is ongoing with the aim at creating coherence in contract law provisions among the member states (EU Commission 2003b); however, this is a major undertaking that is not likely in the near future to resolve the difficulties.

---

[5]There are four exclusions: contracts that create and transfer rights in real estate, contracts that require involvement of courts, public authorities or professions exercising public authority, contracts of suretyship granted or collateral security contracts furnished by consumers, and contracts governed by family law or law of succession.

[6] UNCITRAL Model Law on Electronic Commerce has its origin in a UN initiative aimed at providing certainty in electronic data transactions (originally for the purposes of EDI) and has been transposed or adapted in the national legislation of a number of countries, including US, Australia, France, Singapore, Canada, Ecuador. A further initiative by UNCITRAL currently under development is a convention on electronic contracting (UN, 2004).

Issues related to *jurisdiction* are among the most significant challenges for companies engaging in e-business, as companies might face litigation in any of the countries where e-business services are offered (Berkey 2002; Brightbill 2002). Ultimately, jurisdiction determines the terms under which the consumers and companies can be protected against opportunistic behaviour and to what extent and with what difficulties the obligations of agreed contracts can be enforced. This is currently one of the most problematic areas in e-business regulation: not only the approaches to deciding the governing jurisdiction vary between countries (e.g. in the EU the rules for determining jurisdiction is defined by existing regulation, in the US case law approach several methods co-exist and there is less certainty as to applicable jurisdiction), but also rules applicable to e-business services differ significantly between jurisdictions (e.g. certain services may be considered illegal in the EU while protected under regulations in other countries).

In the EU, the rules for determining jurisdiction and choice of law are set out by two main regulatory acts: the so-called Brussels 1 regulation (Council Regulation (EC) No 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of judgments in civil and commercial matters) and the Rome Convention (EC Convention on the law applicable to contractual obligations (Rome 1980)).

As in the case with validity, the rules for defining the jurisdiction differ for B2C and B2B contracts. Consumers are provided a degree of protection under the regulations and in B2C cases the jurisdiction of the contract is defined based on the country of consumer residence. While this is a crucial condition for ensuring online consumer protection, it may cause companies to abstain from offering services and products in other countries, as this requires knowledge of and compliance with regulations applicable to e-business services in other jurisdictions.

In the case of B2B transactions companies are free to specify the governing jurisdiction as part of the contract. Regulation provides that in cases where such agreement was not part of the contract, the governing jurisdiction is derived based on the so-called country of origin principle. In other words, legal action is to be taken in the country of the supplier of goods or services. In reality, however, the supplier's domicile state can be very difficult to establish: the place of provision of services may differ from the place where the internet servers of the provider are located and yet be different from a country of

registration of the seller/provider. Thus, although some suggest jurisdictional issues in e-business are less problematic for B2B transactions (Berkey 2002) others argue instead that current regulations do not resolve but rather complicate matters relating to jurisdiction in business contracts (Stone, 2002; Rosner, 2002; Weitzenböck 2002).

Considerations in the context of the DBE vision

While the E-Commerce Directive lays down the basic requirements for online contacts, challenges in cross-border transactions arise because in practice validity and the binding power of contracts is determined based on the governing jurisdiction. This requires an understanding and knowledge on the side of SMEs of the applicable regulation in the countries where rules can differ significantly, especially in the case of B2C contracts where jurisdiction is defined based on a consumer's residence. SMEs adopting e-business in a digital business ecosystem may have difficulties conducting transactions with customers from other countries due to the lack of legal expertise and will need support in this area. Challenges are likely also in relation to B2B contracts, where the jurisdiction is determined based on supplier's location, which is not always clear in e-business transactions. A possible approach for SMEs to reduce the risks in this area is to always negotiate and agree the governing jurisdiction prior to entering into the contract relationship, and the governing jurisdiction clause could be included as part of the contracts framework of the DBE.

Information requirements for online contracts

Another critical issue for fostering trust in e-business concerns information requirements for online contracts. A EU Council communication states that this issue represents a major concern for the confidence in products and services offered online, especially when it comes to small enterprises whose presence online is often 'quite basic or poor in nature' (EU Presidency, 2004:11).

At the EU level, the Electronic Commerce Directive is aimed at addressing this issue by setting out the basic requirements on information to be made 'easily, directly and permanently accessible' in relation to an e-business service provider, including the provider's name, geographical location, means of contact, registry information as well as relevant authorisation and professional associations. More specifically in relation to the contracting process, the Directive requires the basic information to be provided prior to the

placing of the order by electronic means, except if concluded solely by email or though other individual communication. These include:

- A description of technical steps needed to conclude a contract;
- Information on filing and later availability of the concluded contract;
- Technical means for identifying and correcting the errors prior to placing the order;
- The languages in which the contract is available and information on the codes of conduct the provider subscribes to and information on how to access these codes.

The directive further requires that service providers make available a means of identifying and correcting input errors prior to order placement. After an order has been placed, the provider is required to send an acknowledgement of the receipt to the buyer 'without undue delay'. Finally, the directive requires the terms and conditions of the contract to be made available to the buyer for filing.

Considerations in the context of the DBE vision

Two main issues in this area are relevant to the DBE context. First, SMEs are generally not well aware of the requirements, and, while consumer knowledge of their rights to information has been improving, businesses that are not compliant have been suffering a loss of consumer confidence (EU Presidency 2004). The SMEs thus need to be made aware of the existing requirements, and information provision has to be fostered within the applications through which service or goods orders can be placed.

Second, the information rules for the contracting process laid down by the E-commerce Directive, with the exception of terms and conditions requirement are necessary only in the of B2C transactions. The directive may not apply to in B2B transactions as it allows the requirements to be overruled by parties who are not consumers agreeing otherwise prior to concluding the contract. This may be part of the reason why the uncertainties related to the online contracting process are the most important concerns for online B2B purchasing transactions as reflected in the results of a recent EU consultation (2002) on trust barriers in e-business. It may be advisable to accommodate these requirements in the contracts framework of the DBE vision with exemptions for certain instances.

Dispute resolution

The difficulties associated with enforcing of contractual obligations and resolving disputes in cases when disagreements arise are especially critical in e-business transactions. In online environments, where new models for conducting business are being established, often involving cross-border transactions, the risk of litigation is potentially increased and disputes are difficult to avoid. Therefore, any uncertainty about potential liabilities and existing dispute resolution mechanisms is an important factor that can discourage companies from entering e-business (Schulze and Baumgartner 2001; OECD 2004a). This observation is confirmed by empirical studies, including a recent global survey of 277 companies by ABA (2004) where the risk of litigation was mentioned as the biggest fear of companies engaging in e-business and an EU consultation on trust barriers to participation in B2B marketplaces (EU Commission 2002), with 50% of respondents reporting uncertainty about dispute settlement as a major issue.

There are two main interconnected considerations in this area. First, the exposure to the risk of litigation in cross-border settings may deter companies from engaging in certain e-business activities all together. The risks of litigation associated with product and service liabilities become more severe in a cross-border e-business environment due to inconsistencies in applicable regulations in different jurisdictions; this particularly may be an issue for SMEs which do not have the resources and legal teams on their side for considering appropriate risk exposure and evaluating potential consequences of engagement in cross-border activities. Secondly, companies that do adopt e-business may face severe challenges in resolving disputes regarding product or service liabilities when these arise, which may especially negatively effect SMEs due to high cost and time-consuming nature of traditional litigation (OECD 2004a and 2004b).

In order to improve the effectiveness of resolving cross-border commercial disputes, policy makers at the EU level have promoted alternative dispute resolution mechanisms. Commission Recommendation 98/257/EC sets out the principles applicable to the bodies responsible for out-of-court consumer disputes, while the Electronic Commerce Directive requires Member States not to hinder the use of alternative dispute resolution (ADR) and to allow the use of online dispute resolution (ODR) mechanisms. Further to this, a European Code of Conduct for Mediators has been developed by a group of stakeholders

with the assistance of the European Commission and a draft Directive on Mediation published in 2004. Alternative dispute resolution provides a means for settling disagreements without litigation in the court, through the use of such mechanisms as mediation, negotiation, conciliation and arbitration in order to reduce the time, cost and complexity involved in settling commercial disputes.[7]

Online dispute resolution mechanisms represent an evolution in dispute resolution, employing technological means to facilitate faster and efficient settlement of disputes, and is especially well suited for disputes arising in e-business as it is able to adapt more flexibly to the evolving technology and business practices (Wahab 2004). There are several types of online dispute resolution schemes depending on the mechanisms used and employing a variety of technical solutions, from simple email interfaces to negotiation software and online settlement.[8] Work is currently ongoing at the EU level to promote online dispute resolution mechanisms. Relevant EU funded initiatives include projects such as E-dispute (electronic dispute settlement for SMEs), OnlineConfidence (dispute resolution process for smaller claims and online confidence network development) and E-Arbitration-T (open-source solution for ODR and information portal on ODR issues for EU companies).

Considerations in the DBE context

A major issue that SMEs face in the regulatory domain of jurisdiction and consumer protection is a potential exposure to litigation based on product or service liabilities. In the context of the DBE this is one of the areas to be considered as not only litigation risks may deter SMEs from engaging in e-business, but in case of such engagement, arising disputes might be very difficult to resolve. Clarity of legal rules applicable in the jurisdictions in which SMEs offer products and services and availability of simple and efficient redress mechanisms are critical areas for the realisation of the full DBE vision. Challenges that

[7] For a detailed description of the types of online dispute resolution mechanisms, see Wahab (2004), Hornle (2004)

[8] These mechanisms employed include negotiation (online spaces provided for negotiating between companies), mediation (a neutral third party is involved using online facilities to assist resolving of a contract dispute), arbitration (a neutral third party – the arbitrator – delivers an award after evaluating the facts of the case), ombudsmen proceedings (mediation services offered by consumer organisations) and cybercourts (resolving of conflict using online juries).

SMEs face in this area will be included for further investigation in the next stages of the research.

Online dispute resolution (ODR) mechanisms potentially provide an effective means for settling cross-border e-business disputes and may be especially attractive for SMEs because of lower cost and higher efficiency (OECD 2004a); however, there are currently two obstacles to the use of ODR mechanisms by SMEs in the B2B e-business settings. First, the existing ODR solutions have been developed for and most widely used in C2C and B2C contexts, and their applicability to B2B context and multi-player disputes is not yet certain. Second, one of the barriers to the use of ODR currently is a lack of awareness in the business sector of the availability of such mechanisms generally (Wahab 2004), and particularly in the SME sector there is little experience using ODR (OECD 2004b). While activities aimed at overcoming the barriers to the use of ODR are ongoing in the EU, it is possible that SMEs joining the DBE in the future will need support and information on access and applicability of such mechanisms in specific sectors and to different types of transactions. In the long-term, possibilities for facilitating dispute resolution mechanisms within the DBE itself may be considered, as this could provide an important resource for the SMEs and increase incentive for participating in the DBE vision.

4. Summary and Conclusion

The aim of this literature review has been to report on key regulatory issues identified as most significant during the initial adoption of e-business services among European SMEs, and to building and maintaining trust in digital business ecosystems more generally. In this report we refer to these issues as *building blocks of trust* that constitute the regulatory domain within which the DBE vision will come to exist. The literature review provides a necessary pre-requisite for subsequent activities in task B11 and establishes a knowledge base of regulatory issues for other tasks in Work Package 32.

The literature review adopted the thematic notion of trust as the initial point of focus inasmuch as academic commentators and practitioners have increasingly recognised it as a key enabler of e-business. The regulatory domain is central to building trust relationships in services and technological solutions, business activities and in access to information. However, an obstacle to assessing the role of trust in the DBE vision is that much of the current research has focused on B2C settings rather than B2B settings. Nonetheless, it is possible to model regulatory trust using types X, Y and Z, which describe various interaction scenarios between SMEs in the DBE vision.

Taking up the theme of trust the literature review identified three building blocks of regulatory trust. These are privacy and consumer protection, e-signature and security, jurisdiction and consumer protection. Each of these building blocks provides the foundation for developing a more complex investigation and analysis of regulatory issues relevant to sector-specific and local implementations of the DBE vision.

The review defines each of the building blocks as a set of related regulatory issues, describes current concerns and areas of relevance as well as considerations in the context of a digital business ecosystem. Subsection 4.1 summarises key observations from this review. Subsection 4.2 considers the implications of these observations for the DBE vision and provides guidance for research activities B11.2 and B11.3.

4.1. Summary of findings

There has been a considerable effort at the EU level aimed at accommodating and encouraging e-business activities through a unified regulatory framework, however, there are still many challenges in the area of B2B transactions and new organisational forms facilitated by digital technologies, in addition to the major gaps in knowledge and awareness on applicable regulation among European SMEs. This is directly relevant for the DBE vision as it aims to be a B2B pan-European space for SMEs, based on an yet untested concept of a digital business ecosystem, representing the so far most advanced organisational and technological set up in e-business. These challenges are evident in all regulatory domains reviewed in this document. The following main issues relevant for the DBE vision have been identified:

Privacy and consumer protection

Privacy refers to the non-disclosure of stored or transmitted information relating to a uniquely identifiable entity, while data protection is the prevention of unauthorized access to this information. These issues are closely linked to consumer rights and existing legislation comprehensively covers B2C transactions, while for B2B contracts the rules are less stringent. Due to a lack of international consensus and coherent regulatory approach to privacy and data protection issues, differences between the rules applicable in non-EU countries and between the EU states are likely to create obstacles for companies seeking to adopt e-business practices.

In the context of the DBE vision, issues related to the management of databases shared between members of the ecosystem are critical, as these databases are likely to contain information to which privacy controls are applicable as well as create sensitive commercial data patterns. In such cases it is important to ensure compliance when handling data, as well as taking into account the clarity of the purpose of data use and transparency in handling of data and accessing databases. Other concerns include relevance and proportionality in the access to the database and accuracy in the use of data, an evaluation of data sensitivity, and, finally, a need for a policy on the rights of companies to prevent or allow transfer of sensitive data.

Although the DBE vision as of yet has no clear definition as a legal entity, there remains a need to comply with the body of regulation in this area if trust is to be established among potential participants. The literature review has identified three main challenges in this area for the DBE vision:

- To define the level of data sharing that does not violate data protection regulations;
- To establish terms and conditions between partners to ensure data will not be shared with third parties external to agreements;
- To establish a means of generating traceable records to deal with any breaches of the data sharing agreements.

E-signatures and Authentication

The building block of e-signatures and authentication is closely related to security issues in e-business. While in many cases these issues are of technical nature, regulatory considerations are especially important in the areas of authentication, digital signatures, electronic invoicing and payments. Concerns related to this building block are crucial for trust relationships in e-business, since authentication supports both access (or denial of access) to different resources as well as the means for identifying malpractice and may provide an audit trail of transactions necessary for resolving disputes.

EU level legislation provides basic framework for the use of electronic signatures for authentication; however, the process and the bodies responsible for certification are decided by each member state. Current regulations also address issues related to encryption, electronic storage and the use of e-payments and e-invoices.

In the DBE vision, relationships between partners will lead to payments or transactions of some type, and the issues related to e-signatures and authentication will be important for establishing and sustaining trust between partners. In addition, considerations of interoperability of electronic invoicing systems and the traceability of processes within these systems may be significant factor in ensuring successful collaboration between partners.

Jurisdiction and Consumer Protection

The building block of jurisdiction and consumer protection refers to the broad category of regulatory issues stemming from the cross-border nature of many e-business transactions. From the perspective of the DBE vision, the main concerns in this building block centre on regulatory issues related to cross-border online contracting.

Validity of electronically concluded contracts may be a concern for two reasons. First, while the EU Directive requiring non-discrimination between on- and off-line contracts, it has not yet been implemented uniformly by all member states and electronic form may not be valid in some cases due to specific sector or local requirements. Second, while B2C online contracting process is covered by existing legislation, difficulties with determining legal validity or the binding power of a contract may arise in B2B transactions as it is determined based on the contract law of the governing jurisdiction. This may turn out to be a barrier to successful electronic contracting between SMEs joining the DBE vision.

Issues related to *jurisdiction* are crucial in cross-border e-business setting: not only approaches to determining the governing jurisdiction vary between countries but also there are significant differences in regulations applicable to e-business in different jurisdictions. In the EU, the B2C contract jurisdiction for consumer protection reasons is based on consumer domicile–hence companies engaging in cross-border activities risk litigation in different jurisdictions, and this may deter SMEs from offering goods and services online. The jurisdiction for B2B contracts may be agreed between contracting parties, but in cases where there is no such agreement, jurisdiction is based on the supplier domicile. This may create risks for SMEs when jurisdiction is not agreed prior to contract, and there are further uncertainties caused by the fact that jurisdiction is not always easy to determine in e-business settings; where jurisdiction is agreed by the parties, SMEs may lack negotiation power and legal expertise to agree favourable jurisdiction when dealing with bigger companies. SMEs joining the DBE environment may need information on the rules for determining jurisdiction and requirements applicable to e-business in other jurisdictions. It may also be necessary to accommodate for the negotiation of jurisdiction prior to the conclusion of the contract in the DBE contracts framework.

Requirements of *information provision* related to the contract (provider details and contracting process) set out in the EU regulatory framework are currently a challenge for SMEs. First, there is little awareness of these requirements leading to non-compliance on the SME side, and second, insufficient information provision to potential customers is often a reason for lack of trust towards the provider. Goods and services offered within the envisioned DBE environment may need to accommodate information provision requirements, and the means for complying with these requirements will need to be considered.

Challenges related to potential product and service *liabilities* and resolving *cross-border disputes*, which are difficult to avoid in an e-business setting, may be especially relevant for the SMEs who have little resources to spare for costly and lengthy processes involved. This issue is a major barrier to e-business uptake by the SMEs, who may abstain from e-business activities associated with risk of litigation in different countries under inconsistent laws. Online dispute resolution (ODR) mechanisms, which represent an alternative to litigation in court that is cost-efficient and time saving, may be particularly suited for the SMEs. However, most of the ODR schemes so far have been designed for C2C or B2C disputes and it is yet unclear how well these are suited for B2B environment characterized by the DBE vision. Moreover, there appears to be low awareness in the SME sector about the existing ODR schemes and expertise in using these schemes. It may be important to consider alternative ways of resolving disputes through ODR mechanisms and, in the long run, look for possibilities for establishing such schemes within the DBE system to ensure efficient and fast resolution of disputes.

4.2. Implications for the DBE vision and Activities B11.2 and B11.3

Regulatory trust and the DBE vision

The implications of the literature review suggest that regulatory considerations are an important, if not crucial, part of ensuring the realisation of the DBE vision in the long run. The challenges currently faced by the SMEs in regulatory domain are an important barrier that will need to be overcome in order to both encourage SMEs to take up e-

business opportunities offered by the DBE and establish trust relationships within the ecosystem as well as between its participants.

Out of the three types of trust (X, Y, Z) identified in this review, the development activities within the DBE are likely to me most efficient in facilitating the Trust type X (trust of the participating SMEs that the DBE architectures support regulatory requirements) and Trust type Y (facilitating governance and/or technical mechanisms to ensure that joining SMEs are compliant with norms and laws). Trust type Z (trust relationships between SMEs supported by the power of norms and laws to govern transactions between participants) may be outside the scope of DBE development activities; nonetheless, it is an important factor to be considered as knowledge of the applicable regulation on the side of SMEs is an important part of facilitating this facet of trust.

These findings are important for guiding further work of task B11, particularly the next stage of formalising the findings into a taxonomy (D32.2) that is intended as an input for other tasks in Work Package 32. The literature review and the taxonomy together form the first stage of Task B11. Both the review and taxonomy should be regarded as *a dynamic knowledge base* inasmuch as findings from activities B11.2 and B11.3 will be incorporated into this foundation. For instance, activity B11.2 is intended expand the knowledge base for a set of sector specific regulatory issues, while B11.3 will identify and further formalise regulatory issues relevant to selected local implementation cases.

Areas to be further explored

The literature review suggests a number of areas that should be explored in the subsequent activities of Task B11.

Privacy and consumer protection

In the area of privacy and consumer protection, the following questions need to be further examined as aspects of regulatory trust within the DBE vision:

- To what extent are privacy and data protection requirements likely to be relevant for the practical implementation of the DBE vision?
- What types of data will companies deposit and exchange within the DBE environment and what kinds of regulatory controls are likely to apply?

- What are the critical issues in ensuring that management of the databases within the DBE environment complies with regulatory requirements and commercial needs for protecting sensitive data?
- What are the means for determining the level of data sharing between DBE members and with third parties external to the agreement?
- What are the requirements for generating traceable records for dealing with breaches to the data sharing rules?
- In what ways could compliance with applicable regulation be fostered within the DBE? (e.g., could this be performed by a designated partner, rotational or shared responsibility?)

E-signatures and Authentication

In the domain of e-signatures and authentication, the literature review suggests a number of questions:

- What are the specific issues in the area of e-signatures and authentication that are relevant for the SMEs joining the DBE vision?
- What is the level of security requirements in these areas applicable to the transactions carried out by the SMEs in selected implementation cases?
- To what extent are the issues related to invoicing system interoperability and traceability of invoice and payment information relevant for the SMEs joining the DBE vision? In what particular areas/sectors do these issues arise?
- What are the models for establishing the hierarchy of authentication relevant to the selected sector and local implementations?
- What are the requirements for generating traceable records within the selected implementation cases and in what ways can this effect the transactions carried out in the DBE environment?
- To what extent are the requirements for electronic storage of documents relevant for the SMEs joining the DBE? In what ways may the differences in regulations between member states effect the transactions? Should these differences be accommodated within the DBE environment? If so, how can this be done?
- In what potential ways could the critical security requirements identified in the next stages of research be accommodated within the DBE vision – through technological mechanisms, based on third-party security services, organisational compliance mechanisms and governance framework?

Jurisdiction and Consumer Protection –Online contracting

The following questions arise in the area of cross-border online contracting within the DBE vision:

- In what cases may there be barriers to recognition of electronically concluded contracts in the selected implementation cases? What are the implications of this for the DBE contracts framework?
- To what extent are the issues of jurisdiction relevant for the joining SMEs? In which selected implementation cases is this most critical and what are the implications for SME participation in the DBE vision?
- What can be done to decrease the risks of litigation that may deter the SMEs of engaging in certain e-business activities? Can SMEs be supported in negotiating a favourable jurisdiction in B2B contracts? Should the jurisdiction clause be implemented in the DBE contracts framework?
- To what extent should the information provision requirements be embedded in the DBE generic layer and services? How critical is this issue for SMEs in selected implementation cases? Are the SMEs aware of the existing requirements and the effect this may have on their activities?
- What is the perceived significance of the risks related to product and service liabilities on the side of the SMEs joining the DBE and is this seen as a major barrier to engaging in e-business activities? What are the possible ways for reducing these risks in the DBE context?
- What are the challenges in the area of dispute resolution joining SMEs are likely to face? To what extent is this seen as a barrier by the joining SMEs in the selected implementation cases?
- What are the online dispute resolution schemes (ODR) available for the SMEs in the sector and local implementation cases? Are they aware of the existence of these schemes? How can awareness of the existing ODR mechanisms be best facilitated within the DBE vision?
- Should the possibilities for including ODR schemes directly in the DBE system be considered? If so, how can this be done and what could be the main requirements for such ODR schemes? In what ways the functioning of ODR mechanisms within the DBE system can be organised and managed in the long-term?

Relevance of EU funded research projects on regulatory and legal issues in e-business

In addition to the generic level of regulatory issues identified in this review, a number of projects funded under Fifth and Sixth Framework Programmes (summarised in Appendix 2) have carried out research into specific regulatory issues in e-business, which may be relevant for the DBE vision and future stages of task B11. Initial steps have been taken to identify the relevant research within these projects, and contacts made with FP6 funded TrustCoM IP and Legal-IST.

The outcome of a meeting arranged with TrustCoM indicated a willingness to provide input to the DBE on best practices and key findings, but that its work is not directly relevant to the unique parameters established in the DBE vision due to several differences such as ownership of licensing (TrustCoM being proprietary, and DBE Open Source orientated), software and ecosystem membership (TrustCoM has well-defined rules for working partnerships, the DBE is still in a process of defining the rules for attracting membership to the project) and overall scope (TrustCoM is aimed mainly at virtual enterprise type of formations, whereas DBE vision is to facilitate all kinds of collaboration modes between SMEs from simplest to most complex models).

Contacts with Legal-IST legal experts have also been established, with willingness on the Legal-IST side to conduct research into specific legal issues relevant for the DBE vision and the results of subsequent stages of task B11 may provide input for Legal-IST research activities.

Projects under FP5 that have already been finalised may also be relevant for further activities in Task B11, but this will likely depend on the selected implementation cases which will inform further stages of the task. It is intended that these sources of information work will help to inform consultations with SMEs and other DBE partners during subsequent activities in Task B11.

Bibliography

ABA (2004) Global Internet Jurisdiction: The ABA/ICC Survey. American Bar Association. http://www.mgblog.com/resc/Global%20Internet%20Survey.pdf (last accessed 15.02.05).

Abrazhevich, D. (2001) *Classification and Characteristics of Electronic Payment Systems*. Lecture Notes in Computer Science 2115(2115/2001): 81.

Angelov, S. and P. Grefen (2003) *The 4W framework for B2B e-contracting.* Int. J. Networking and Virtual Organisations. 2(1), pp. 78-97.

Ashby, W. R. (1956) *Introduction to Cybernetics*. London: Chapman and Hall http://pespmc1.vub.ac.be/ASHBBOOK.html. (last accessed 15.02.05).

Ba, S., Pavlou, P.A. (2002) *Evidence of the effect of trust building technology in electronic markets: price premiums and buyer behavior*. MIS Quarterly 26 (3), pp. 243–268.

Bangemann, M. (1994) *Recommendations to the European Council: Europe and the global information society.* Brussels, 26.05.1994. http://europa.eu.int/ISPO/infosoc/backg/bangeman.html (last accessed 15.02.05).

Bargh, M., W. Janssen, et al. (2002) *Trust and Security in E-Business Transactions*. Enschede, The Netherlands, Telematica Institute.

Berkey, J. (2002) *Outline of International e-commerce regulatory issues*. Intel/Unitar Campus of New Information and Communication Technologies and Diplomacy, New York, US. at http://www.un.int/unitar/intel_nct_campus/2002/conference_presentation.htm (last accessed 15.02.05).

Bezroukov (1999) *Open Source Software Development as a Special Type of Academic Research (Critique of Vulgar Raymondism*). First Monday 4(10). Available at http://firstmonday.org/issues/issue4_10/bezroukov/

Blois, K. J. (1999)*Trust In Business To Business Relationships: An Evaluation of Its Status*. Journal of Management Studies (36:2), pp. 197-215.

Brightbill, T.C. (2002) *Barriers to International Electronic Commerce: Recent Issues and Developments*, Wiley Rein & Fielding LPP discussion paper. Available http://www.wrf.com/publication.cfm?publication_id=11623(last accessed 15.02.05).

Buck, S. P. (1997). *From electronic money to electronic cash : payment on the Net*. Journal of Enterprise Information Management 10(6): 289-199(11).

Burgwinkel, D. (2003) *Electronic Contracting in cross-media environments. Discussion Paper.*, University of St. Gallen. Available: http://VirtualGoods.tu-ilmenau.de/2003/econtractingmedia.pdf (last accessed 15.02.05).

Burn, J. (2000) *Editorial.* Journal of Global Information Technology Management. 3(1): p. 3-7.

Clarke, R. (2002a) *Trust in the context of e-Business.* Internet Law Bulletin. 4(5): p. 56-59.

Clarke, R. (2002b) *e-Consent: A Critical Element of Trust in e-Business.* Proc. Of 15th Bled Electronic Commerce Conference. Bled, Slovenia. Available at http://www.anu.edu.au/people/Roger.Clarke/EC/eConsent.html

Data Protection Working Party (2005) *Guidelines for Terminated Merchants Databases* (pp. 22). Brussels: EU. http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/others/2005-01-11-fraudprevention_en.pdf (last accessed 15.02.05).

Dutton, W.H. and A. Shepherd (2004) *Confidence and Risk on the Internet. Foresight Cyber Trust & Crime Prevention Project.* Available at http://www.foresight.gov.uk/Cyber_Trust_and_Crime_Prevention/Reports_and_Publications/Cyber_Trust__Crime_Prevention__Confidence_and_Risk_on_the_Internet.html

E-businessWatch (2004) *The European e-Business Report: A portrait of e-business in 10 sectors of the EU economy*. 2004 edition. Available (last accessed 15.02.05).

Ebusinesslex (2005) The E-business Legal Portal . Available at http://www.ebusinesslex.net/front/ele_paesi_leggi.asp (last accessed 17.03.05)

Endeshaw, A (2003) *Web Services and the Law: A Sketch of the Potential Issues.* International Journal of Law and IT, vol. 11 (3), pp. 251 – 273.

European Parliament (1998) Opinion of the Committee of the Regions on the 'Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on "A European initiative in electronic commerce"' (98/C 180/03) http://europa.eu.int/ISPO/ecommerce/oj/1998/1998C180/cdr350_97_en.doc (last accessed 15.02.05).

EU Commission (2002) *Open consultation on "Trust barriers for B2B e-marketplaces". Presentation of the main results*. Summary report. http://europa.eu.int/comm/enterprise/ict/policy/b2b-consultation/b2b-trust-cons-sum.pdf (last accessed 15.02.05).

EU Commission (2003a) *Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.* COM (2003) 702(01. http://europa.eu.int/eur-lex/en/com/rpt/2003/com2003_0702en01.pdf (last accessed 15.02.05)

EU Commission (2003b) *Communication from the Commission to the European Parliament and the Council–A more coherent European contract law–An action plan.* Official Journal C 063 , 15/03/2003 P. 0001 – 0044. http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=C2003/063/01&model=guichett

EU Commission (2004a) *Legal barriers in e-business: The results of an open consultation of enterprises.* Commission Staff Working Paper. Brussels, 26.4.2004 SEC(2004) 498. http://europa.eu.int/comm/enterprise/ict/policy/doc/legal_barriers_sec_2004_498.pdf (last accessed 15.02.05).

EU Commission (2004b) *Report on the results of the "ICT usage of enterprises 2002" – survey. February 2004*. http://europa.eu.int/comm/enterprise/ict/studies/entr-ict-2002.pdf (last accessed 15.02.05).

EU Commission (2004c) *The European e-Business Legal Conference.* Dublin, Ireland, 27-28th April 2004. Proceedings at http://europa.eu.int/comm/enterprise/ict/policy/legal/dublin/ (last accessed 15.02.05).

EU Commission (2005) *The activities of the European Union for small and medium-sized enterprises (SMEs)–SME Envoy Report*. Brussels, Belgium http://europa.eu.int/comm/enterprise/entrepreneurship/sme_envoy/index.htm

EU Presidency (2004) *Building Consumer Confidence in the European Online Marketplace*. Information by the Presidency to the EU Council, 9466/04. Brussels, 12th May 2004 http://www.eu2004.ie/templates/document_file.asp?id=17903 (last accessed 01.02.05).

Expert Group (2003) *Final report of the Expert Group on B2B Internet trading platforms*. http://europa.eu.int/comm/enterprise/ict/policy/b2b/wshop/fin-report.pdf (last accessed 15.02.05).

Fahey, L., et al. (2001) *Linking e-business and operating processes: The role of knowledge management*. IBM Systems Journal. 40(4): p. 889-907.

Ganesan, S. (1994) *Determinants of Long-Term Orientation in Buyer-Seller Relationships.* Journal of Marketing 58(2): 1-19.

Hornby, G., P. Goulding, and S. Poon (2004) *Perceptions of Export Barriers and Cultural Issues: The SME e-Commerce Experience.* Journal of Electronic Commerce Research. 3(4), pp. 213 – 226.

Hörnle, J. (2004) *Online Dispute Resolution (ODR)–JISC Legal Briefing Paper*, JISC Legal Information Service. http://www.jisclegal.ac.uk/pdfs/HornleODR.doc (accessed 01.02.05).

Hwang, P. and W. Burgers (1997) *Properties of trust: an analytical view*. Organizational Behavior and Human Decision Processes, vol. 69 (1), pp. 67–73.

Jahankhani, H. (2002) *The impact of law on e-business practices in the EU*. In proceedings of *INET 2002*- Internet crossroads: where technology and policy intersect. Internet Society: Washington DC, USA. http://inet2002.org/CD-ROM/lu65rw2n/papers/g11-b.pdf (last accessed 15.02.05).

Jarvenpaa, S. L. and N. Tractinsky (1999). *Consumer Trust in an Internet Store: A Cross-Cultural Validation*. Journal of Computer Mediated Communication, vol. 5(2): 45-71.

Keen, P.G.W. (2000) *Ensuring E-trust.* Computerworld, vol. 34 (11), p. 46.

Knights, D., F. Noble, T. Vurdubakis and H. Willmott (2001) *Chasing shadows: control, virtuality and the production of trust*. Organization Studies, vol. 22 (2), pp 311-336.

Lodder, A. and H. Kaspersen (2002) *eDirectives: Guide to European Union Law on E-commerce*. Hague: Kluwer Law Int.

Mahler, T. and T. Olsen (2004). *Reputation Systems and Data Protection Law*. Oslo, TrustCoM.

Mansell, R. and B. Collins (2004) *Cyber Trust and Crime Prevention: A Synthesis of the State-of-the-Art Science Reviews*. Foresight Cyber Trust & Crime Prevention Project. http://www.foresight.gov.uk/Cyber_Trust_and_Crime_Prevention/Reports_and_Publications/Cyber_Trust__Crime_Prevention__Synthesis_of_the_Science_Reviews.html (last accessed 15.02.05).

Mansell, R. and W.E. Steinmueller (2000) *Mobilizing the Information Society: Strategies for Growth and Opportunity*. Oxford & NY: OUP.

Mayer, R.C., Davis, J.H., Schoorman, F.D., 1995. *An integrative model of organizational trust*. Academy of Management Review, vol. 20, pp. 709–734.

Mazzeo, M. (2004) *Digital Signatures and European law*. Security Focus. http://www.securityfocus.com/infocus/1756 (last accessed 17.03. 05).

Meents, S., Tan Y-H. and Verhagen. T. (2003) *Distinguishing different types of trust online B2B marketplaces.* Proceedings of the Tenth Research Symposium on Emerging Electronic Markets 2003, pp. 53 – 65.

Mingers, J. (1997a) *Systems Typology views in the Light of Autopoiesis: A reconceptualisation for Boulding's Hierarchy, and a Typology of Self-Referential Systems*. Systems Research and Behavioral Science 14: 303-313.

Mingers, J. (1997b) *Self-Producing Systems–Implications and Applications of Autopoiesis*. Journal of the Operational Research Society 48(11): 1149-1149 (1).

Murray, A. (forthcoming 2005) *Contracting Electronically in the Shadow of the E-Commerce Directive*, in Edwards L. (ed), The New Legal Framework for E-Commerce in Europe, Hart Publishing, Oxford.

http://www.100megsfree4.com/andrewmurray/EContracting.pdf (last accessed 15.02.05).

Nachira, F. (2002) *Towards a Network of Digital Business Ecosystems Fostering the Local Development*. Discussion Paper. http://www.digital-ecosystems.org/ (last accessed 15.02.05).

OECD (2004a) *ICT, E-business and SMEs*. Report by the Working Party on the Information Economy. Paris. http://www.oecd.org/dataoecd/32/28/34228733.pdf

OECD (2004b) *Alternative Dispute Resolution (ADR) Online Mechanisms for SME Cross-Border Dispute*, *Promoting Entrepreneurship and Innovative SMEs in a Global Economy: Towards a More Responsible and Inclusive Globalization Conference.* Istanbul: OECD. http://www.oecd-istanbul.sme2004.org/documents/07%2BAlternative%2BDispute%2BResolution.pdf (last accessed 15.03.05)

Pavlou, P. A. (2002) *Institution-Based Trust in Interorganizational Exchange Relationships: The Role of Online B2B Marketplaces on Trust Formation*. The Journal of Strategic Infor-mation Systems 11(3-4): 215-243.

Pearce, G. and N. Platten (2000) *Promoting the Information Society: The EU Directive on Electronic Commerce.* European Law Journal, vol. 6(4), pp. 363-378.

Pearce, J.L., Branyiczki, I., Bigley, G.A., 2000. *Insufficient bureaucracy: trust and commitment in particularistic organizations*. Organization Science, vol. 11 (2), pp. 148–162.

Raymond, E. S. (2001) *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Revised Edition. Sebastopol, CA, USA, O'Reilly and Associates, Inc.

Regev, G. and A. Wegman (2002) *UML for Early Requirements Elicitation: A regulation based Approach.* Lausanne, Switzerland, EPFL-IC Technical Report no IC/2002-13.

Reinecke, J., Dessler, G. and Schoell, W. (1989*) Introduction to Business–A Contemporary View*. Boston: Allyn and Bacon.

Rosenbaum, H. and E. Davenport (2003) *Situational Trust in Digital Markets: a socio-technical exploration. Ninth Americas Conference on Information Systems–Proceedings*. Available http://www.maggieswan.com/papers/situational_trust.pdf (last accessed 15.02.05).

Rosenbaum, H. (2004) *The importance of trust in the digital networked economy*. Workshop "Creating partnership online" Concept and Tools, Darmstadt, Germany.

Rosner, N. (2002) *International Jurisdiction in European Union E-Commerce Contracts*. LLRX discussion paper. http://www.llrx.com/features/eu_ecom.htm (last accessed 15.02.05).

Ruppel, C., L. Underwood-Queen, and S.J. Harrington (2003) *E-commerce: The Roles of Trust, Security, and Type of Ecommerce nvolvement*. e-Service, vol. 2(2), pp. 25-45.

Schulze, C. and J. Baumgartner (2001) *Don't Panic! Do E-commerce.* Report by the EU Commission Electronic Commerce Team (Information Society Directorate General). http://europa.eu.int/ISPO/ecommerce/books/dont_panic.pdf (last accessed 15.02.05).

Shankar, V., G.L. Urban, and F. Sultan (2002) *Online trust: a stakeholder perspective, concepts, implications, and future directions.* Journal of Strategic Information Systems, vol. 11(2002), pp. 325-344.

Shelbourn, M., T. Hassan, et al. (2003) *Identification of the potential Legal and Contractual gaps and problems within the cluster projects*. Loughborough, Loughborough University–ICCI.

Spindler, G., C. Carter, et al. (2004) *State of the Art of Research on Legal Issues Related to the Information Society Technologies*. Dublin, Legal IST.

Stone, P. (2002) *The Treatment of Electronic Contracts and Torts in Private International Law under European Community Legislation.* Information and communication Technology Law, 11(2), pp. 121 – 139.

Sultan, F., Urban, G et al (2002) *Determinants and Role of Trust in E-business: A Large Scale Empirical Study.* MIT Sloan Working Paper Series. Available http://e-commerce.mit.edu/cgi-bin/viewpaper?id=231 (last accessed 15.02.05).

Swan, M. and H. Rosenbaum (2004) *The social construction of trust in e-business: An empirical investigation*. Americas Conference on Information Systems. Available http://aisel.isworld.org/pdf.asp?Vpath=AMCIS/2004&PDFpath=SIGEBZ01-1766.pdf (last accessed 15.02.05).

Wahab, M. (2004) *The Global Information Society and Online Dispute Resolution: A New Dawn for Dispute Resolution.* Journal of International Arbitration, 21(2): p. 143-168.

Weitzenböck, E. M. (2002) *Determining Applicable Law and Jurisdiction in contractual disputes regarding virtual enterprises* in Pawar, K. S.; Weber, F.; Thoben, K.-D. (Eds.): ICE 2002. Proceedings of the 8th Int. Conf. on Concurrent Enterprising: *Ubiquitous Engineering in the Collaborative Economy*. Rome, Italy, 17-19 June 2000, pp.27-34.

Wigand, R., Picot, A. and Reichwald, R. (1997) *Information, Organization and Management in Expanding Markets and Corporate Boundaries*. John Wiley and Sons Ltd.

Woolthuis, R.K., B. Hillebrand, and B. Nooteboom (2002) *Trust and Formal Control in Interorganizational Relationships.* Research report. Erasmus Research Institute of Management.

Yovovich, B. G. (1996) *Trust Among Partners Foundation of Success.* Advertising Age's Business Marketing. Vol. 81. Issue 6, July/August. pp. 12–15.

UN (2004) *Legal aspects of electronic commerce. Electronic contracting: provisions for a draft convention.* United Nations Commission on International Trade Law (UNCITRAL). Note by the Secretariat. http://daccessdds.un.org/doc/UNDOC/LTD/V04/541/06/PDF/V0454106.pdf?OpenElement (last accessed 15.02.05).

UN (1998) *United Nations Commission on International Trade Law, Model Law on Electronic Commerce of 1996, with additional Article 5 bis, 1998*. http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm (last accessed 15.02.05).

Zucker, L. (1986) *Production of trust: institutional sources of economic structure 1840–1920*. Research in Organization Behavior 8 (1), pp. 53–111.

Annex 1: Summary of relevant EU level regulatory measures

- 1980 Rome Convention on the law applicable to contractual obligations (consolidated version)

http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:41998A0126(02):EN:HTML

- Green Paper on Alternative Dispute Resolution in Civil and Commercial Law, Brussels, Com(2002)0196 final.

http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=COM:2002:0196:FIN:EN:PDF

- Directive 98/34/EC of the European Parliament and of the Council Laying Down a Procedure for the Provision of Information in the Field of Technical Standards and Regulation and of Rules on Information Society Services.

http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31998L0048:EN:HTML

- Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 Adopting a Multiannual Community Action Plan on Promoting Safer Use of the Internet by Combating Illegal and Harmful Content on Global Networks.

http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32004D0787:EN:HTML

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures.

http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

- Directive 2000/31/EC on Certain Legal Aspects of IS Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce).

http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=COM:1999:0427:FIN:EN:PDF

- Directive 2001/29/EC of the European Parliament and of the Council of 22nd May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society.

http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_167/l_16720010622en00100019.pdf

- 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).

http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF

- European Code of Conduct for Mediators. Voluntary code developed by a group of stakeholders with the assistance from the European Commission 2004.

http://europa.eu.int/comm/justice_home/ejn/adr/adr_ec_code_conduct_en.pdf

- Proposal for a Directive of the European Parliament and of the Council on certain aspects of mediation in civil and commercial matters {SEC(2004) 1314}

http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2004/com2004_0718en01.pdf

- 98/257/EC: Commission Recommendation of 30 March 1998 on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes

http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31998H0257:EN:HTML

- Council Regulation (EC) No 44/2001, of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_012/l_01220010116en00010023.pdf

- Council Regulation (EC) No 1504/2004 of 19 July 2004 amending and updating Regulation (EC) No 1334/2000 setting up a Community regime for the control of exports of dual-use items and technology

http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32004R1504:EN:HTML

- 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

http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32000L0046:EN:HTML

Annex 2: Summary of research within FP5 and FP6

Completed and ongoing projects examining legal and/or regulatory issues relevant to e-business and e-commerce environments:

FP5 projects

ECLIP: Electronic Commerce Legal Issues Platform (2000 – 2002)

Project home:

http://www.jura.uni-muenster.de/eclip/

Research on a number of areas in e-business regulation. The aims of the project were to develop awareness of legal issues, provide information and support, a teaching programme for legal issues in e-commerce, support to other FP5 programs with legal background, studies on policy issues integrating analysis with consideration of technological solutions, support and influence EC policy in this area.

Regulatory issues studied in depth: Contracts, Consumer Protection, Jurisdiction, Privacy, Data Protection, IPR. Looked at use and deployment of Electronic Agents, Smart Cards, M-commerce.

ELEGAL: Specifying Legal Terms of Contract in ICT Environment (2000 – 2002)

Project home

http://cic.vtt.fi/projects/elegal/public.html

Objectives: to define a framework for legal conditions and contracts regarding the use of ICT in project business–specify user requirements, implement legal support tools & promote an enhanced business practice in which the use of ICT in inter-enterprise information exchange is contractually stipulated. Main focus was on Contract Law, IPR, Liabilities. The project developed a definition of the user requirements for legal support of ICT in project-based businesses (focused on construction) and a library of model contracts and recommendations to standardisation.

ALIVE: Advanced Legal Issues in Virtual Enterprises (2001 – 2003)

Project home:

http://www.vive-ig.net/projects/alive/

Focus on virtual enterprises. The project analysed virtual enterprise life-cycles, created a taxonomy for analysing related legal issues, studied in depth 9 selected areas, and provided recommendations for further policy work in the area. The issues studied in detail included nature and legal identity of Virtual Enterprises (VEs), contract law (developed model contracts to be used by VEs, also issues relating to IPR, data protection, liability and insurance, Alternative Dispute Resolution, Consumer protection, competition, Tax matters.

E-COMMLEX (2001-2002)

E-lex portal home

http://www.elexportal.com/

Aimed at providing comprehensive information to European enterprises on regulatory issues and requirements in e-commerce. Main result of this project was the E-Lex portal which provides comprehensive information on different areas of e-business and e-commerce law, as well as enquiry service to find out about national differences in requirements. The focus is mostly on B2C transactions

Other projects that covered regulatory/legal issues within their scope on a smaller scale include:

- E-Arbitration T (regulatory framework and infrastructure for electronic dispute settlement; relevant issues in Procedural Law, Dispute Resolution, tools to settle disputes electronically)
- CCForm (looked at establishing multilingual complaint forms, covered issues in Concillation – Procedural Law and Alternative Dispute Resolution)
- Virtual Winery (web-based winery to promote European Wines, looked at issues arising in Contract and Liability law, Consumer Protection, Data Protection, Jurisdiction, Arbitration).
- Octane (trial project on secure business applications; focused on electronic contracts and developed a process for electronic contracts called ‘Open Contracting Service)

FP6 Projects

Legal-IST: Legal Issues for the Advancement of Information Society Technologies).

(04/2004 – 03/2004)

Project home

http://www.ve-forum.org/apps/comm.asp?$1=369

The objectives of legal IST include consolidation of the results of the research into legal issues undertaken in previous projects, support to research activities within IST projects by conducting legal studies and providing assistance to ongoing projects, contribution to the policy work on the EU regulatory framework validated though a campaign involving governments, policy-makers and public institutions and to deliver an on-line community for SMEs delivering legal advice to support their e-business and e-commerce activities.

TrustCom: Trust, Security and Contract Management for Virtual Organisations

Project home :

http://www.eu-trustcom.com/index.php?page=Home

The project objective is to develop a framework for trust, security and contract management in dynamically-evolving virtual organizations. The framework will enable secure collaborative business process management and sharing in an on-demand, self-managed, dynamic value-chains of businesses and governments. The framework will leverage and extend the emerging convergence of open-standards such as Web Services, Grid technologies and protocols for inter-enterprise interactions (using open agent protocols).

PRIME (04/2004 – 02/2008)

Project Home

http://www.prime-project.eu.org/

Prime is a multidisciplinary project aimed at developing solutions for digital identity management and privacy, the main focus on devising an identity management architecture supporting privacy of ICT users and enterprise data processing.