European Commission, Directorate-General for Enterprise and Industry

Benchmarking of existing national legal e-business practices, from the point of view of enterprises (e-signature, e-invoicing and e-contracts)

Draft Final Report

November 2006

RAMBØLL management

European Commission
Directorate-General for Enterprise and Industry

Benchmarking of existing national legal e-business practices, from the point of view of enterprises (e-signature, e-invoicing and e-contracts)

Draft Final Report

November 2006

Ref	
Edition	4
Date	1 November 2006
Appd.	
Checked	
Prepd.	JSY/CASS/ANCB

Rambøll Management
Nørregade 7A
DK-1165 København K
Denmark

Phone: +45 3397 8200
www.ramboll-management.dk

RAMBØLL management

Table of contents

Executive Summary

Introduction

This is the Draft Final Report for the study 'Benchmarking of the existing national legal e-business practices, from the point of view of enterprises, with particular emphasis in the fields of e-signature, e-invoicing as well as contract conclusion and implementation'. The study was commissioned by the European Commission, Directorate-General for Enterprise and Industry, and carried out by Rambøll Management during 2006.

The study is based on in-depth reports for each of the 25 Member States, prepared by local legal experts and covering national legal e-business practices (published separately); comprehensive desk research of legal documents, reports and other documents; and a survey among the Member States on the current status for administrative and business practices within the areas of electronic signatures and electronic invoicing.

The aims of the study are:

- to collect information in order to identify the various national legal and administrative e-business practices in the field of e-signatures, contract conclusion and implementation, and e-invoicing
- to describe the different national e-business practices in the fields mentioned above;
- to benchmark them with a view to distinguish best practice among them; and
- to present relevant conclusions and recommendations.

Status and conclusions in the three main fields covered by the study

E-signatures

All Member States have implemented the e-Signatures Directive and the basic features of electronic signatures are well transposed into national legislation. Qualified electronic signatures are accepted by all Member States as legally equivalent to handwritten signatures and electronic signatures are admissible as evidence in legal proceedings. The basic legal foundation for use of electronic signatures by businesses is therefore present. For businesses to increase their use of electronic signatures it is, however, important that Member States remove formal hindrances in national legislation in relation to use of electronic means, such as, e.g. requirements for a written signature in two copies on a specific form.

In addition, there is some uncertainty in the interpretation of the Directive. This uncertainty encompasses both the legislative level in the Member States and the users of electronic signatures.

E-government services appear to be the main driver for electronic signatures, making the public sector a key player in facilitating and encouraging the use of electronic signatures. Interaction in the private sector, i.e. business and citizens, still provides for very little use of electronic signatures. It seems that the private sector, especially SMEs, has still not experienced sufficient need or external demand for adopting electronic signatures when communicating electronically.

Overall, the use of electronic signatures in the Member States is still very limited. This applies especially to the use by enterprises and consumers of electronic signatures based on qualified certificates. Seen from a business perspective, the important issue is to make rational use of new technologies when this supports the activities of the enterprise. The currently demanded services in the business world do not depend on the use of electronic signatures. The incentive for investing in and adopting electronic signature technology has to be present.

The court cases illustrate that the use of electronic communication, including electronic signatures, are accepted by courts as evidence and can constitute the basis of binding contracts. The court cases do, however, also show the challenges for the legal systems in addressing the technically difficult issues connected to the use of electronic communication.

Cross-border use of electronic signatures depends on the possibility of a party to technically receive, read and control the other party's electronic signature. Establishment of a well-functioning PKI infrastructure that provides for technical interoperability between various certification service providers is the first condition for cross-border use. Technical interoperability is, however, not sufficient *per se* to support cross-border use. Commercial interoperability must also be present when establishing a PKI infrastructure with involvement of Certification Service Providers with different business models. An enterprise in one country is not necessarily able to accept an electronic signature from a customer in another country using a certificate from its domestic Certification Service Provider if a clearance agreement has not been agreed between the enterprise and the foreign Certification Service Provider.

The advantage of using electronic signatures based on qualified certificates is the support from the legal framework created by the e-signatures Directive. This advantage depends, however, on a well-functioning Internal Market as underpinned in Article 4. From a legal point of view, the introduction of accreditation schemes pursuant to Article 3 (1) and the possibility of establishing additional requirements in the public sector pursuant to Article 3 (7) seem to be the most critical when using electronic signatures in communication with the public sector. It must be emphasized that such additional requirements in the public sector for receiving electronic signatures must be kept at a minimum to reduce the risk of limiting the free flow and use of electronic signatures.

Contract conclusion

Despite the overall approximation of regulation in the Member States and a series of initiatives aimed at increasing the overall coherence of European contract law, there are still dissimilarities in how legal principles are understood and practiced by the Member States. Ongoing European legal initiatives and international initiatives i.a. in the form of model laws and conventions do, however, function as building blocks for a uniform framework for enterprises doing online business.

There is no uniform definition of whether or not the presentation of goods or services on a website ('display of goods or services in a web shop') is an offer to the customer or only an invitation to the customers to make an offer. In several Member States, online advertising on a website can under certain conditions be regarded as a binding offer.

A correct implementation by the online vendor of the requirements stated in Article 10 (1) (a) of the e-Commerce Directive (information on the different technical steps to follow to conclude the contract) will clarify this issue when the possibility of online conclusion of contracts are provided by the vendor.

The uncertainty and lack of transparency in the national legislation may, however, lower the incentive for SMEs and consumers to enter into cross-border trade. Uncertainty concerning cross-border regulation is considered a specific and significant hindrance especially for SMEs and consumers.

The proposal from the Commission for a Regulation of the European Parliament and the Council on the law applicable to contractual obligations (Rome I) will clarify the present situation with regard to verifying the applicable law to the contract. But this clarity might be viewed as an administrative burden since distance selling will encompass the task of drafting contracts targeted individually to all European Member States. This might, again, be especially burdensome for SMEs.

e-Invoicing, payment, and other matters related to the execution of electronic contracts

Despite the quite significant savings attached to the use of electronic invoices, usage levels remain low meaning that businesses do not reap the full economic benefits of electronic invoices. Clearly, government strategies in this area and, in particular, general government acceptance of electronic invoices are useful tools to increase the general usage of electronic invoices.

On a more practical level, the main problems seem to be the different standards for security of the electronic invoice and different underlying technologies, making the use of electronic signatures difficult for SMEs, particularly in cross-border trade.

The use of credit payment cards is a vital factor for e-commerce, and in particular for web-shops selling to consumers. Despite the significant protection offered to consumers using credit cards under the Directive 97/7/EC, trust remains low.

Another significant problem seems to be the lack of a more clear framework governing payments made by businesses, in particular SMEs acting as consumers outside their regular business field (for instance in the acquisition of office supplies etc.)

The contract execution rules vary quite significantly from Member State to Member State. Significant differences seem to exist even in areas were the European Union has introduced minimum requirements, for instance in relation to the withdrawal period in distance sale contracts. However, the difference seems to be even more significant outside areas influenced by Community legislation.

Main legal and administrative barriers to e-business in the European Union

Member States have, on an overall level, implemented the relevant Directives and thus have a robust legal framework to support online business. However, in practice, the legal framework and the legal practices do meet challenges when businesses and consumers do e-business.

Legal uncertainty
More than half of the Member States report that there is uncertainty as regards the legal binding effect and recognition of electronic documents in national trade relations due to the lack of court decisions. The lack of court cases and legal precedent is significant in the fields of e-signature, e-invoicing and e-contract conclusion, as there has been no court case from a Supreme Court or High Court on these issues across the Member States. This uncertainty may influence on the interest and willingness of commercial entities to make investments in technology to promote new business models and services to customers and business partners. A few countries also report inconsistencies between different regulations, and even insufficient legislation on e-business.

Lack of international standards and interoperability
There is a lack of international standards for electronic signatures. There are, however, widely adopted standards that most certificates to electronic signatures are based on. The real issue is the lack of 'filled-in' standards, i.e. standards on how to fill in the different fields in a certificate, as there is no generally adopted standard on how to provide this information in the certificates. Administrative practices are also a significant barrier to cross-border use of electronic signatures, since a number of Member States only provide access to the national electronic signature(s) to citizens and/or companies registered in the country. The lack of common and freely usable implementation of existing standards also applies to cross-border use of electronic invoices, where there is a similar need for adoption of filled-in standards and cross-border interoperability.

Lack of trust
Generally, lack of trust in electronic transactions is reported by many countries. Electronic commerce in B2C relations is very much dependent on the use of credit cards. From a legal point of view, the widespread lack of trust is largely unfounded since Directive 97/7/EC provides consumers with a fundamental legal protection from the fraudulent use of payment cards. However, there is a widespread lack of compliance with legislation among a large share of online shops, and this contributes to uncertainty among consumers. This is widely regarded to be caused mainly by a *lack of awareness* on the part of the businesses about their obligations as regards e.g. protection of personal data, information to customers on withdrawal rights from distance contracts etc. Related to this, consumers are often not aware of their rights and, feeling unprotected, this adds to their mistrust.

Limited protection of SMEs
Consumers generally enjoy a high degree of protection when doing business online. The same degree of protection does not apply to smaller enterprises. The low level of protection for SMEs is reported as a problem. The general rationale is that B2B transactions are regarded as business between two equal partners. With regard to doing business online, small businesses do feel a legal uncertainty and lack of knowledge that constitutes a barrier.

Interpretation of the country of origin principle
The country of origin principle as such has a very positive impact on the opportunity and incentive to provide cross-border e-business. However, the interpretation of the country of origin principle in the e-commerce Directive is reported as a problem by several respondents. The delimitation between regulation included in the country of origin principle and regulation outside the scope is reported as not clearly identifiable.

Awareness among businesses about national authorities in charge of solving legal problems in e-business

Alternative Dispute Resolution (ADR) schemes or out-of-court mechanisms have been developed across Europe to help citizens who have a consumer dispute, but have been unable to reach an agreement directly with the trader. However, these out-of-court mechanisms have been developed differently across the European Union. The ADR initiatives are supplemented by the European Consumer Centres Network that consists of Consumer Centres in all Member States. The existing lack of awareness among businesses in relation to the general legislation is explicitly reported in several country reports. This could also imply a lack of knowledge about national authorities in charge of solving legal problems in e-business.

Legal and administrative good practices in e-business

The country reports show that Member States have taken a wide range of initiatives to promote the use of e-business, and electronic communication in general. The reported best practices can be divided in four overall categories: legal initiatives, information campaigns, administrative initiatives and infrastructure projects.

Legal Initiatives

The Netherlands has implemented the e-commerce Directive and the Distance Selling Directive directly into the Civil Code. By implementing the Directives into the Civil Code, electronic contracts are directly integrated with the general legal system of the Civil Code. This is reported to have increased the awareness of the validity of electronic contracts in the Netherlands.

In *Ireland*, Directive 1999/93/EC on a community framework for electronic signatures was quickly implemented into the Irish Electronic Commerce Act from 2000. The act on electronic commerce gave same status to electronic signatures, electronic contracts and electronic writing as the paper-based equivalents. The early implementation is reported to have helped to create legal certainty for enterprises, and hence promote e-commerce activity.

In *Belgium*, the Government has established an office for administrative simplification. Many of the initiatives have related to the introduction of paperless transactions by making minor changes to old laws. As a result, it is now possible to make electronic storage of evidence documents in hospitals, electronic registration of vehicles, and electronic annual corporation tax returns. More than 150 laws have been abolished or simplified as a result of the initiative since 2003.

In *Denmark*, a similar initiative, focusing on the barriers to digital communication, has been taken. This initiative has also functioned as the official follow-up on the requirement in Article 9 of the e-commerce Directive to remove obstacles for electronic conclusion of contracts. It was decided by the Government that every ministry was to review its legislation for references to such formalities that may constitute barriers to the efficient use of information technologies. Each ministry was to develop a prioritised plan of action to be implemented, and set forward the specific proposals for changes. The plans were presented in 2003, and implemented in subsequent years. The initiative has now been replaced by a continuous monitoring of new legislation by the Danish Ministry of Justice to ensure continued focus on digital communication and consistency of measures.

Administrative initiatives
On a European scale, the *Euro-label initiative* is a trustmark to be used by websites that comply with the European Code of Conduct. It is promoted by 8 national institutions, acting as national Euro-Label certification bodies. The Code was drafted to reflect current and anticipated future European legislation. It draws on the EU Directives on Electronic Commerce, Distance Selling and Data Protection.

The *Luxembourg certification initiative* is an example of an interesting initiative taken at national level. It is managed by the Luxembourg Chamber of Commerce with the support of the Ministry of Economy and External Commerce. The initiative consists of three distinct certificates (or trust marks) that are to promote secure e-commerce sites: the *e-privacy certificate,* the *e-commerce certificate,* and the *e-commerce certified partner*.

At European level, the *Trusted Shops* initiative, involving a number of commercial partners including a major insurance group, and with a market focus on the United Kingdom, Germany, France, Belgium, the Netherlands and Scandinavia. There are currently about 1600 internet retailers operating under the Trusted Shops standard.

Also in the field of alternative settlement of disputes in e-commerce, self-regulation initiatives have been taken. The *Global Business Dialogue on Electronic Commerce,* a forum of dialogue between the private sector and governments to discuss e-commerce issues, has been instrumental in the establishing of a number of e-commerce initiatives, including standards of alternative dispute resolution.

Information Campaigns and Initiatives
Econsumer.gov is a resource website for consumers who buy products and services online from sellers in other countries. Launched in 2001, the aim of econsumer.gov was to enhance consumer protection and consumer confidence in e-commerce. It is a cooperation of consumer agencies in 20 countries. The initiative has two components: a multilingual public Web site, and a government, password-protected Web site.

The International Chamber of Commerce, ICC, is another example of a comprehensive web-source of information, in this case concerning ADR providers. The ICC website provides an inventory with contact information for firms and organizations around the world that can help resolving online disputes.

In *Finland*, the Government has established an Information Society Program to promote and develop governmental initiatives on advancement of the information society. The programme maintains a web-site containing guidelines, news and a collection of best practice examples.

In *Austria*, an Internet ombudsman was established already in 1999 in a cooperation between the Austrian Institute for Applied Telecommunication (ÖIAT) and the consumer information organisation (VKI). A dedicated site provides advice on safe on-line shopping and information on standards in e-commerce.

In the *UK*, the Government asked the Alliance for Electronic Business and the Consumers' Association to work together and set up a self-regulatory scheme to address the needs of consumers transacting on-line. The approach is that accredited websites will display the TrustUK Hallmark either on its own, or together with the logo of the code owner they subscribe to.

In *France*, the Ministry of Finance is behind an information website with the title 'E-commerce and you' that includes advice on how to buy on the internet, describes the rights of the consumer, guides the consumer in case of complaints and presents and explains the recent EU directives.

In *Spain*, the Ministry for Industry, Tourism and Commerce has included a list on its web site of systems of self-regulation. On the same website, there is a list of Frequently Asked Questions that help explain and interpret the requirements established by e-commerce rules. The questions provided are a mix of questions of interest to e-commerce shops and to consumers.

Finally, in *Belgium*, the Ministry of Economic Affairs has set up the so-called 'Internet Rights Observatory'. The main tasks of this Observatory is to submit opinions on the economic problems brought about by the use of new information and communication technologies; to organize consultations among the economic actors concerned; and to inform the public on these aspects. The Internet Rights Observatory is composed of persons with experience in the new technologies but also of representatives of economic actors and of ICT users.

Infrastructure initiatives

In *Denmark*, the executive order on electronic settlement and the executive order on information in OIOXML require all public institutions to be able to receive electronic invoices in the OIOXML format. Further, the requirement included in the invoicing legislation to make use of electronic invoice mandatory, when providing services to public authorities, is generally regarded as an initiative that will accelerate further the private use of electronic invoices in B2B relations.

Estonia has implemented an Identity Card as the primary document to identifying all its citizens and alien residents living within the country. The card, besides being a physical identification document, has advanced electronic functions that facilitate secure authentication and a legally binding digital signature. The initiative is supplemented with nationwide online services.

In *Spain*, the Government launched in March 2006 a similar initiative: a new Identity Card with a chip containing certificates to allow for authentication and signing with digital signature.

In *France*, the Government has officially approved plans for a new electronic ID card in 2005, and the plans are to commence distribution of the e-ID Card in 2007. The new Digital ID card will be obligatory, and every resident is supposed have the Card by 2011.

In 2004, *Belgium* adopted plans to provide all citizens with an electronic identity card. The card contains an embedded microchip storing the holder's personal data. The electronic ID card is planned to be distributed to all citizens until the end of 2009 when the transition to the new card is expected to be complete.

Recommendations

- *It is recommended that Member States take initiatives to review their national legislation for references to such formalities that may constitute barriers to the efficient use of information technologies.*

- *It is recommended that a concerted effort is undertaken at international level to improve the use of e-signature and e-invoicing by creating a common and freely usable implementation of the e-signature and e-invoicing standards at least between the countries parties to the European Economic Area Agreement*

- *It is recommended that an effort is made at international level to establish cross border trust models among e-signature Certification Service Providers at least between the countries parties to the EEA Agreement.*

- *It is recommended that national Governments take the lead in promoting the use of e-signatures, e-invoices etc. through their provision of online (e-government) services.*

- *It is recommended to launch a multi-annual action for making available multilingual information aimed at SMEs and consumers in all countries parties to the EEA Agreement about their rights and obligations regarding Internet transactions, in particular cross-border transactions (both intra-community, export and import).*

- *It is recommended that an initiative is taken at European level to include in the principles of good marketing practice that debit of the buyer's account can only be made once the good has been shipped or the service delivered.*

- *It is recommended to enlarge the scope of* Regulation (EC) 2560/2001 *in order to equal all the charges for payments done between Member States in euros or in the national currency to those made for domestic payments.*

- *It is recommended to carry out initiatives to raise awareness among SMEs of the advantages provided by Regulation 2560/2001.*

- *It is recommended that initiatives are taken to promote a more uniform contractual regulation within the European Economic Area.*

1. Introduction

This is the Draft Final Report for the study 'Benchmarking of the existing national legal e-business practices, from the point of view of enterprises, with particular emphasis in the fields of e-signature, e-invoicing as well as contract conclusion and implementation'. The study was commissioned by the European Commission, Directorate-General for Enterprise and Industry, and carried out by Rambøll Management during 2006.

The study is based on in-depth reports for each of the 25 Member States, prepared by local legal experts and covering national legal e-business practices; comprehensive desk research of legal documents, reports and other documents; and a survey among the Member States on the current status for administrative and business practices within the areas of electronic signatures and electronic invoicing.

The above-mentioned 25 Country Reports, published separately, constitute the main volume of reporting of the results of this study, and the present report brings together the overall framework, key conclusions and good practices seen across the 25 Member States.

Chapter 2 provides an introduction to the background, scope and purpose of the study as well as the applied methodology. In chapter 3, the framework for analysis of national legal e-business practices is presented. This is followed by three chapters on the legal and administrative practices in the three key areas: electronic signature (chapter 4), electronic contract conclusion (chapter 5), and electronic invoicing, payment and other matters related to the execution of electronic contracts (chapter 6). Chapter 7 provides a general assessment, cross-cutting analysis of the national legal and administrative e-business practices, including identification of best practices. Finally, chapter 8 will present the recommendations which can be made on the basis of the findings and conclusions of the study.

2. Background, scope and methodology of the study

2.1 Background

The background of the study is as follows:

- More enterprises than ever are interested in and engaged in e-business
- The technical development has enabled opportunities for cutting costs and expanding opportunities in new areas
- Increased investments in ICTs, especially a more efficient use of them, would allow for substantial productivity gains

The existence of different rules in each of the EU Member States can represent a significant barrier for the electronic conduct of key business processes between the EU Member States and, from a wider geographic perspective, between the parties to the EEA Agreement. Therefore, the harmonisation of certain elements of national legislation could mean increased economic efficiency for conducting electronic trade in the European Internal Market.

The differences between the Member States' regulation present challenges to the use of cross-border electronic business as enterprises and consumers will need to understand and comply with specific national rules and requirements when engaging in cross-border commerce and exchange of information electronically[1]. It is also important for the efficiency and cost-effectiveness of the use of electronic communication that the systems and standards that are used are interoperable[2].

To stimulate e-business, the EU has set out a legal framework in key areas and supporting key business processes such as:

1) Electronic signatures (Directive 1999/93/EC on a Community framework for electronic signatures),

2) Information society services including electronic commerce (Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market (the "e-commerce directive")),

3) Consumer protection when doing business-to-consumer transactions notably by electronic means (Directive 1993/13/EC on unfair terms in consumer contracts; Directive 1997/7/EC on the protection of consumers in respect of distance contracts; Directive 1998/6/EC on consumer protection in the indication of the prices of products offered to consumers; Directive 1999/44/EC on certain aspects of the sale of consumer goods and associated guarantees; Directive 2002/65/EC concerning the distance marketing of consumer financial services and amending Directive 90/619/EEC, 97/7/EC and 98/27/EC; Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market and amending Directives 84/450/EEC, 97/7/EC, 98/27/EC and 2002/65/EC), and

4) Electronic invoicing (Directive 2001/115/EC amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the

[1] European Commission, Internal Market Directorate-General, 2004: Impact Assessment: Action Plan on e-Public Procurement, Part 1: Baseline Analysis

[2] Ibid

conditions laid down for invoicing in respect of value added tax (the "e-invoicing directive))[3].

Most of these Directives have been implemented[4], and national practices have been developed in the respective fields. Thus, it is now possible to assess these practices and the progress in the different fields of e-business.

2.2 Purpose of the study

The purpose of the study is to identify the most appropriate national legal practices in the relevant fields of e-business from the point of view of enterprises. Reaching this objective could contribute to the simplification and improvement of the administrative and regulatory framework for enterprises engaged in e-business.

The study shall provide a description and a benchmarking of the legal and administrative practices in the fields of *e-signature*, *contract conclusion and implementation* and *e-invoicing* within the 25 EU Member States.

The specific aims of the study are:

- Firstly, to collect information in order to identify the various national legal and administrative e-business practices in the field of
    - e-signatures: focusing on the legal and administrative practices emanating notably from the application of the e-signatures directive;
    - contract conclusion and implementation: focusing on the legal and administrative practices emanating notably from the implementation of the following directives: Directive 1999/13/EC, 1997/7/EC, 1998/6/EC and 1999/44/EC;
    - e-invoicing: focusing on the legal and administrative practices emanating notably from the application of the e-invoicing directive;
- Secondly, to describe the different national e-business practices in the fields mentioned above;
- Thirdly, to benchmark them with a view to distinguish best practice among them;
- Fourthly, to present relevant conclusions and recommendations.

2.3 Scope of the study

The scope of the study is to cover legal and administrative practices in e-business from the *viewpoint of enterprises*. In principle, this would include the commercial relations of enterprises with both other enterprises (business-to-business, B2B), consumers (business-to-consumer, B2C) and public institutions (business-to-government, B2G). However, as explained below, the focus of the study is especially on legal and administrative practices relevant for business-to-business and business-to-consumer relations.

[3] See e.g. Kroes, Quinten R., 2003: E-Business Law of the European Union. The Hague. Kluwer Law.

[4] Member States shall adopt and publish the laws, regulations and administrative provisions necessary to comply with this Directive by 12 June 2007.

These different types of commercial relations are governed to various degrees by specific legislation as briefly summarized below:

1. **Business-to-consumer**
   The 25 Member States have specific legislation regulating business-to-consumer transactions. This is laid down in various types of legislation such as national consumer protection laws, contract law etc. Furthermore, there is an EU consumer policy and an EU legal framework responsible for harmonising rules in order to promote the Internal Market and ensure that all 460 million citizens of the EU Member States benefit from a high minimum level of consumer protection[5].

2. **Business-to-business**
   Generally, business-to-business relations are less regulated in formal law and primarily governed by contracts between the parties. However taking into account that, on an average, 91.5% of enterprises in the EU are micro-enterprises with less than 10 employees[6] and that many micro-enterprises have only 1 employee, certain Member States have extended to SMEs the protection granted by their national legislation to consumers in electronic transactions.

3. **Business-to-government**
   The 25 Member States have specific legislation regulating business-to-government commercial relations. This is laid down in national public procurement legislation which implements the European Union Directives for public procurement[7].

Since other past and ongoing[8] studies for the European Commission address the legislation in the field of e-government best practices, the main focus of the current study is on the business processes involved in business-to-business and business-to-consumer relations. Business-to-government relations are dealt with to the extent that it is important for the general uptake of e-business, such as initiatives to set up a Public Key Infrastructure (PKI) for e-signature.

Legislation relevant for e-business originates from both EU and Member State level. The current study will focus on the applicable legislation in this area independently of whether it has an EU origin (when it is national legislation implementing an EU Directive), or it has a purely national origin, such as contract law, which mostly originates from the national level.

2.4 E-business dynamics – a model

In this section, we present a model for understanding the dynamics and driving forces in the field of e-business (fig. 1, below). The methodology for the study takes this model as its point of departure and will be presented in the following section.

---

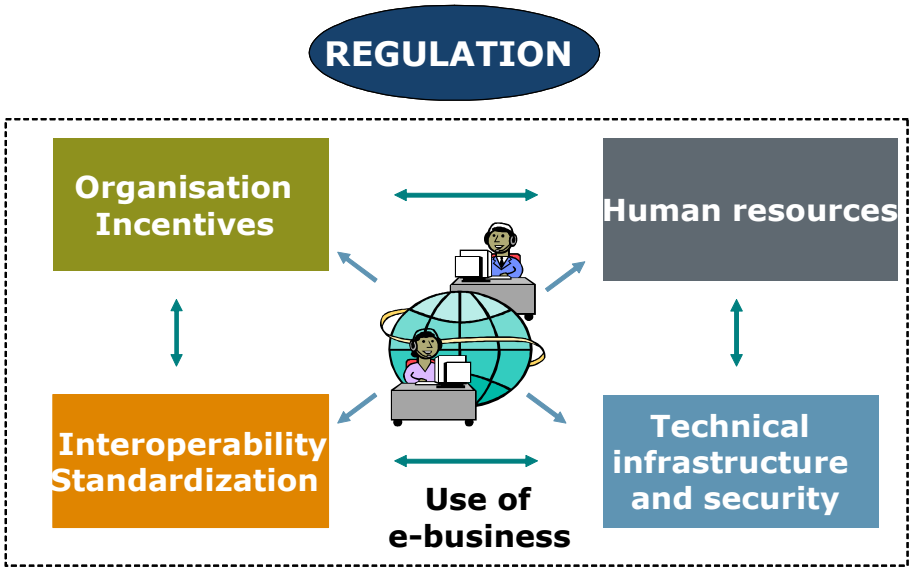
[5] http://www.eubusiness.com/guides/consumer.
http://ec.europa.eu/consumers/overview/index_en.htm

[6] http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-NP-06-024/EN/KS-NP-06-024-EN.PDF

[7] See description on the webpage of Directorate-General Internal Market:
http://ec.europa.eu/internal_market/publicprocurement/index_en.htm

[8] Most notably under IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens), http://ec.europa.eu/idabc/en/home

Figure 1: The key drivers for e-business



While there are natural variations between the EU Member States and differences between the strengths and importance of the drivers, our research findings in other studies indicate that this conceptual model is generic and may be applied as a framework for interpreting the processes and experiences in all countries as regards the development of e-business.

As the figure illustrates, regulation is the framework within which all economic operators must work. The next level of drivers directly influences the e-business activities and will thus also influence uptake of e-business.

The elements of the model are briefly commented upon in the following:

Regulation
Regulation is an important element of the macro-environment for e-business. It provides the basic framework for the evolution of e-business. The fundamental role of the regulatory framework is shown in the figure above as the basic driver that influences all other factors in the model.

Administrative practices will often be intertwined in the area of regulation, as the administrative practices might be derived directly from law or other regulation. However, some public authorities also develop administrative practices that are not directly mandated by a given law or regulation. These administrative practices can for instance be endorsement of technical standards.

Regulation and standardization can, obviously, cause or remove barriers for e-business. A widespread interoperability of different business processes will naturally increase the use of e-business, whereas lack of interoperability will constitute a barrier.

Organisation, stakeholders and incentives
The group of drivers labelled organisation, stakeholders and incentives refers to the (macro level) institutional model in the field of e-business, including which public institutions and companies are involved, how their respective

roles and responsibilities are defined, and how the interaction between the involved businesses and institutions takes place.

The main stakeholders in the field include the enterprises (large enterprises as well as SMEs) and their customers, but public organisations are also relevant players. The organisational set-up and stakeholders are closely linked to the third element – incentives. The organisational set-up influences the configuration of the incentives and vice versa. In this context, incentives are to be understood as the set of motivational factors which make the various stakeholders act as they do within the defined organisational structure and processes.

Interoperability, standardization and security

The level of interoperability and standardization of the available solutions is cited by most data sources as a main driving force in the development of e-business. Interoperability, as described in the European Interoperability Framework for Pan-European e-Government services[9] concerns technical (including data formats and communication protocols), organisational and semantic interoperability.

To ensure that e-business does not create new barriers in the Internal Market, interoperability is important in a number of areas, notably in cross-border transactions and in business-to-business and business-to-government e-business transactions.

Regulation and standardization in the field are naturally determining for the level of interoperability. A widespread interoperability will increase e-business, whereas lack of interoperability will constitute a barrier.

Security is also an important issue, as lack of trust and security can represent a barrier to suppliers and buyers. Some suppliers and buyers are concerned about using the Internet to transmit confidential information. Possible security flaws in transactions over the open Internet will decrease confidence in e-business.

Human resources and knowledge

Moving from organisation and incentives at macro level (above) to micro level, the human resources and knowledge factor refers to the availability of strategic and organisational capacity as well as technical ICT skills at micro level (contracting authorities and companies).

This constitutes an important driving force in the diffusion of e-business. Organisational capacity is in many cases a question of organisational change readiness (i.e. the readiness of employees to employ new working processes, levels of experience and trust in using electronic tools).

Organisational capacity is also a question of having the knowledge and skills to re-engineer internal or external work-flows to reap the full benefits from e-business. Technical ICT skills at micro level are often dependent on the level of experience and trust in use of electronic tools.

While most e-business processes are actually fairly simple to use, some are more advanced (for instance the use of electronic auctions). Thus, ICT skills in general as well as specific skills of key employees related to specific advanced e-business processes can be an essential factor to benefit from the advances of e-business.

[9] http://ec.europa.eu/idabc/servlets/Doc?id=19528

The issue can be problematic for many SMEs because they may not have the skills and the staff required, e.g. in the latter stages of an electronic procurement phase, where system integration internally and externally requires a high level of technical skills as well as redesign of internal business processes.

The area of human resources and knowledge is, however, not dealt with in any detail in this study. Firstly, the human resource and knowledge area has been benchmarked on a general level in other benchmarking studies[10], and secondly it would be difficult to distinguish between the level of human resources and knowledge in the individual areas that should be benchmarked under this study. We refer instead to already documented benchmarks that can shed general light on the human resource and knowledge issues in relation to e-business.

2.5 Methodology

The study provides a benchmark of the national legal practices in the fields of e-signature, contract conclusion and implementation, and e-invoicing within the 25 EU Member States, based on three main sources of data:

- 25 in-depth Country Reports on national legal status and practices in each Member State, prepared by national experts (published as a separate volume)
- Comprehensive desk research of legal documents, reports and other relevant material on legal and other aspects of e-business, mainly at European level
- A survey among Member States on national administrative and business practices within the fields of electronic signatures and electronic invoicing.

In this section, we describe the overall benchmarking approach, as well as the different methods of data collection and their contribution to the study.

2.5.1 Benchmarking Methodology

A definition of benchmarking was proposed by USAID in 1999:

> *"A process of measuring another organization's product or service according to specified standards in order to compare it with and improve one's own product or service. (…) Benchmarks may be established within the same organisation (internal benchmarking), outside of the organisation with another organisation that produces the same product or service (external benchmarking), or with reference to a similar function or process in another industry (functional benchmarking)"*

There are a number of benchmarking typologies in use, of which we find the distinction between *process benchmarking* and *results benchmarking* (Trosa and Williams 1996) one of the most important ones.

Results benchmarking can be used to create *rankings* of the benchmarked entities based on quantitative scores. This can be an effective way to create attention – and thereby help spread good practices. However, such an approach requires availability of (mainly quantitative) high quality data – e.g.

[10] Forinstance in the eEurope 2002 benchmarking report

recent, valid, and covering all 25 Member States - in order to be able to assess the performance of each Member State in relation to specific, objective benchmarks. Some European data are available – e.g. from the European e-business Readiness Index[11] which has data from 2004 on adoption and use of ICT by businesses. However, as stated in the most recent report, the index is partial and seriously constrained by data gaps and conceptual limitations[12].

Further, and more importantly, such an 'objective' assessment would require that direct causality exists between the legal and administrative practices and the performance of each Member State in relation to enterprises' e-business uptake. This is not necessarily the case, as other factors such as business culture and organisation, level and distribution of ICT skills, and general technical preconditions such as the availability and cost of e.g. broadband internet connections, will also influence heavily on the overall e-business uptake of each Member State (cf. also the e-business dynamics model described above). Thus, at best, the quantitative data from sources such as the European e-business Readiness Index[13] would only qualify as 'proxy' or indirect indicators.

Thus, instead of a quantitative benchmarking exercise aimed at developing scoreboards that compare country performance and identifies more or less successful countries, a more qualitative approach has been selected for this study. The aim of the benchmark approach applied is to illustrate similarities and differences between the national legal approaches and ways in which Directives of relevance to the various processes of e-business and applications such as electronic signatures and electronic invoices are implemented.

In this way, the study identifies successful practices in the Member States which can be disseminated and thus inspire other actors. It also identifies barriers to e-business at EU, Member State or institutional level - particularly in terms of implementation of the Directives, standardization, interoperability and cross-border issues.

When benchmarking different legal and administrative practices, the national practices will be assessed in order to identify, describe and explain good practices. This is the essence of the qualitative approach to benchmarking. However, we find it important to distinguish between "best practices", "ideal practices" and "good practices":

From an international perspective, "best practice" cases are very helpful to point out different solutions to the same or similar problem. But the question for decision-makers is: which of the identified solutions work best at home? From a scientific point of view, the question can be raised whether the known solutions are really the relatively best ones. There may be other approaches – "ideal practices" - that yield better results, but we may not know about them. Even in a world of perfect information, the absolute "best practice" may not be the theoretically best one (the ideal practice).

The consideration of ideal practices is, however, more a theoretical point than a practical one for the present study. The concept of "good practices" is more in tune with how the study can help creating a framework for facilitating e-business uptake by inspiring Member States to adopt practices that have proved to yield good results in other countries. The concept of "good

[11] http://www.e-thematic.org/download/The%20European%20e-business%20readiness%20index%202004.pdf

[12] Ibid, p. 4.

[13] http://ec.europa.eu/enterprise/ict/policy/ebi/index_en.htm

practices" in the context of benchmarking stems from the realization that there is not a 'single best way' of developing processes or structuring organisations. This approach to benchmarking has been influenced by contingency theory (se for example Waterhouse and Tiessen (1981), Zeithaml et al. (1988) and Sitkin et al. (1994)[14]). We see a contingency, context-oriented approach as providing improved explanations and understanding of structures and – more importantly here – processes.

In view of these considerations, the practical approach which has been applied in this study is summarised in the table below.

Table 2.1 Benchmarking approach

Approach	Methodology	Outcome
Process benchmarking	Describe e-business legislation in 25 Member States Examine similarities and differences in legal approach Examine outcome/practices in areas such as e-signature, contract conclusion and e-invoicing Analyse reasons for variations in legal and administrative practices (to the extent possible)	Identify obstacles in Member States Identify best practices Identify areas of improvement of legal and administrative practices (recommendations)

2.5.2 Data collection

The benchmarking analysis is based on three main data sources which are briefly described below.

Desk research
Comprehensive desk research has been carried out throughout the study with a view to describing and analysing the relevant Directives[15] and their overall implementation as well as obtaining more general and comparative (cross-European) information on legal and administrative e-business practices. Thus, legal documents, reports and other relevant material on legal and other aspects of e-business, mainly at European level, have been studied in order to establish a common background against which to analyse the country-specific data supplied via the country reports and the Member State survey.

[14] Waterhouse, J. and Tiessen, P. (1981) 'A contingency framework for management accounting systems research'. In: Chenhall, R., Harrison, G. and Watson, D. (eds.) *The Organizational Context of Management Accounting*, pp. 100–114, Boston: Pitman.
Zeithaml, V.A., Varadarajan, P.R. and Zeithaml, C.P., (1988) 'The contingency approach: its foundations and relevance to theory building and research in marketing'. *European Journal of Marketing*, Vol. 22, No. 7, pp. 37-64.
Sitkin, S.B., Sutcliffe, K.M. and Schroeder, R.G., (1994) 'Distinguishing control from learning in total quality management: a contingency perspective'. *Academy of Management Review*, Vol. 19, No. 3, pp. 537-564.

[15] Cf. the list of directives in chapter 3 of this report.

Country reports
At the core of the benchmarking exercise are the country reports – one for each of the 25 EU Member States. The country reports have been prepared by local legal experts with thorough knowledge about their national legislation. The focus of the reports is the national legislation and administrative practices. The reports are qualitative and descriptive and have an average length of 20-30 pages.

The reports have been prepared following a common structure, thus allowing for comparison across countries. The structure and contents of the country reports are shown in the table below.

Table 2.2: Structure of the country reports

I -General information on the national legal system
The aim of this section is to provide a general understanding of the national legal system.

II – Electronic signatures
The aim of this section is to provide a description of the various national legal and administrative e-business practices in the field of electronic signatures, including practices emanating from the application of the electronic signatures Directive.

III – Electronic contract conclusion
The aim of this section is to provide a description of the various national legal and administrative e-business practices in the field of electronic contract conclusion, focusing on the legal and administrative practices emanating from the national legal framework.

IV - Electronic invoicing, payment and delivery
The aim of this section is to provide a description of the various national legal and administrative e-business practices focusing on electronic invoicing, electronic payment and delivery.

V - General assessment
The aim of this section is to conclude on the most interesting findings related to the country's legal and administrative practices in the fields of electronic signature, electronic contract conclusion and electronic invoicing, electronic payment and delivery.

The country report format has been developed in close co-operation and dialogue with the Commission and the Steering Group for the study through an iterative process over several months:

- A first draft structure was discussed with the Commission and subsequently elaborated in a pilot country report (Denmark).
- The pilot report was revised in several steps, until a final format and structure was arrived at and approved. Subsequently, a second pilot report (Germany) was prepared
- Draft versions of the remaining 23 reports were submitted to the Commission and the Steering Group (which includes representatives of all Member States) for comments – both general and country-specific.
- Following revision of the draft reports, a second draft was forwarded for comments and a third and final draft subsequently prepared.

Member State survey
The Member State (country) survey is designed to supplement the country reports. Whereas the country reports focus on the legal aspects, the survey covers other important aspects of e-business practices such as government strategy, administration, standards, technology and uptake. The survey focuses on the fields of electronic signatures and electronic invoicing.

The methodology for the country survey was different from that of the Country Reports, as the survey was carried out via a questionnaire sent to the Member State representatives of the Steering Group[16]. The survey contains both quantitative and qualitative questions, with focus on quantitative (closed-end) questions in order to facilitate cross-country comparisons. To assist in the completion of the questionnaire by the Member States, preliminary answers from Denmark were included in the questionnaire for reference. The survey questionnaire is included in Annex II.

In total, full or partial responses were received from 18 Member States: Austria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Hungary, Ireland, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Slovak Republic, Slovenia, Spain, and Sweden.

No replies were received from Belgium, Germany, Greece, Italy, Latvia, Portugal, and the UK.

Survey data have been included in the analysis of the state of play in the fields of electronic signatures and electronic invoicing. Selected data has been presented in the report in tables providing an overview of the status in the different Member States. Furthermore, a full version of the survey data for all Member States contributing to the survey has been included in Appendix III to this report.

[16] The Member State representatives in the Steering Group have co-ordinated the completion of the questionnaire in their own countries, often in co-operation with officials in the responsible government institutions.

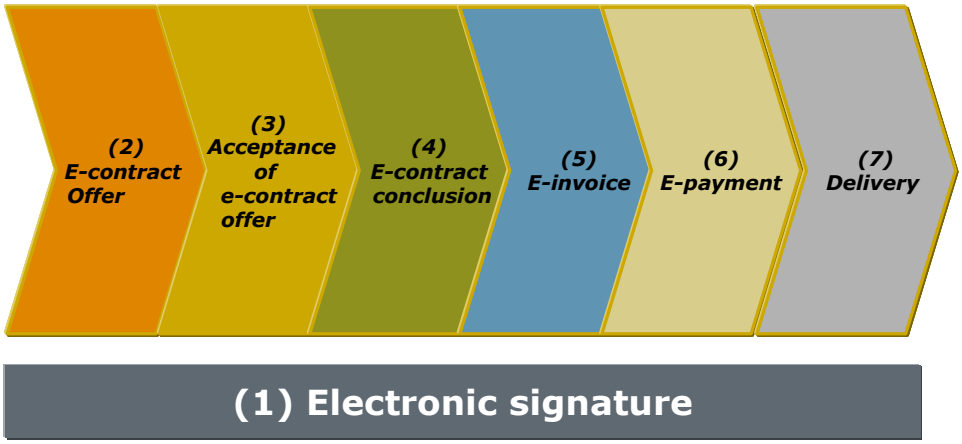
3. Framework for analysis of national legal e-business practices

The main application areas of e-business selected for this study are:

1. Electronic signatures, which is an underlying technology potentially supporting the key e-business transactions
2. Electronic contract conclusion, consisting of the sub-phases submission and acceptance of an electronic offer and conclusion of a contract.
3. Execution of a contract concluded electronically, consisting of the sub-phases electronic invoicing, payment and delivery of the product (including the right of return)

Often, there will be more steps involved in e-business, as each of the main activities can be further broken down into subsets of activities. This is shown in the figure below.

Figure 2: key e-business processes



The figure represents a stylised model of key activities involved in e-business, where electronic signature is an underlying technology supporting secure transactions in most of the other business processes.

The most important Directives regulating e-business have, for the purposes of this study, been identified as:

- Directive 1999/93/EC on a Community framework for electronic signatures
- Commission Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council[17].
- Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market ("e-commerce directive");

[17] OJEC L 175 , 15/07/2003 P. 45-46, Eur-Lex: 32003D0511 : http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l_175/l_17520030715en00450046.pdf

- Directive 2001/115/EC amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax ("e-invoicing directive").

Other important directives are dedicated to consumer protection when making notably electronic transactions:

- Directive 1993/13/EC on unfair terms in consumer contracts;
- Directive 1997/7/EC on the protection of consumers in respect of distance contracts;
- Directive 1998/6/EC on consumer protection in the indication of the prices of products offered to consumers; Directive 1999/44/EC on certain aspects of the sale of consumer goods and associated guarantees;
- Directive 1999/44/EC on certain aspects of the sale of consumer goods and associated guarantees
- Directive 2002/65/EC concerning the distance marketing of consumer financial services and amending Directive 90/619/EEC, 97/7/EC and 98/27/EC;
- Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market and amending Directives 84/450/EEC, 97/7/EC, 98/27/EC and 2002/65/EC).

EC regulation is, however, not the only regulation applicable to e-business. The question of contract practices – including e-business practices – differs from Member State to Member State, as each country has its own contract law and supporting regulation. Thus, the study to a high degree also addresses the relevant national legislation within the fields subject to the above-mentioned Directives.

In this context it should also be mentioned that the study does not address sector-specific regulation (i.e. regulation specifically addressing single sectors/types of business such as, e.g., telecommunications or package holidays), as this would far exceed the volume of regulation which can be considered within the remit of this study. Furthermore, as a general rule, these sector-specific regulations contain specific provisions on e-business, as opposed to other kinds of business relations.

4. Legal and administrative practices in the field of electronic signature in the 25 European Union Member States

This chapter describes the findings in the field of electronic signatures with particular focus on the national and administrative practices concerning electronic signatures issued under the national rules implementing Directive 1999/93/EC.

Focus is on the following key issues:

- Directive 1999/93/EC on a community framework for electronic signatures
- Basic features of electronic signatures
- Use of electronic signatures
- Reported problems in the field of electronic signatures
- Cross border issues concerning electronic signatures

4.1 Electronic signatures

According to Article 2 (1) of the Directive, an electronic signature is data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. An electronic signature can merely be the name typed in an e-mail or a copy of a scanned signature inserted into an electronic document.

If users of electronic communication want to obtain further certainty for the validity of their communication, they need to use a more sophisticated technology; the advanced electronic signature (also known as a digital signature).

An advanced signature is generally taken to be a subset of the electronic signature and is defined in Article 2 (2) of the Directive as *an electronic signature which meets the following requirements:*
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

Like a written signature, the purpose of an advanced electronic signature is, inter alia, to guarantee that the individual sending the message really is the person that he or she claims to be (i.e. authentication).

The functionalities of a an advanced electronic signature are, however, broader than a physical signature, since the advanced e-signature can also be used as a tool for identity verification when using electronic applications, for example online electronic services, and can be used as a means for secrecy due to the built-in option of encrypting content. The identification of the signer can be read in a so-called “certificate”, which is traditionally attached to the electronic signature. A certificate can be compared to a passport, since it contains valid information about its holder. For a more comprehensive introduction to electronic signature technology, please refer to section 4.3.

4.2 Directive 1999/93/EC on a Community framework for electronic signatures

The main objective of Directive 1999/93/EC is to create a Community framework for the use of electronic signatures, allowing the free flow of electronic signature products and services across borders, and ensuring a basic legal recognition of electronic signatures.

The Directive does not address the conclusion and validity of contracts or other legal obligations prescribed by national or Community law regarding the form of contracts. Neither does it affect rules and limitations relating to the use of documents, provided in national or Community law[18].

The overall objective of creating a Community framework for the use of electronic signatures contains two main objectives: 1) Establishing a legal framework for electronic signatures and certification services and 2) Facilitating the use of electronic signatures.

Consequently, the Directive does not affect national provisions requiring for instance the use of paper for certain types of contracts. Furthermore, the Directive does not exclude the possibility for parties in a closed system (e.g. corporate intranet or between a service provider and its customers) to negotiate specific terms for the use of electronic signatures within this system.

The legal sphere in which electronic documents and electronic signatures may be used is not regulated by the Directive, cf. recital 21, where it is stated that this is governed by national law.

The Directive addresses electronic signatures in general, facilitates their use and contributes to their legal regulation, cf. Article 1:

The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market.

It is, however, important to stress that even though the Directive addresses electronic signatures in general, the central regulations in the Directive only refer to electronic signatures based on qualified certificates. The specific provisions regarding qualified certificates include inter alia supervision (Article 3 (3)), legal effect (Article 5 (1)), and liability concerning issuance (Article 6).

Facilitation of qualified certificates can be described as the key element of the Directive.

According to the definitions in Art 2 a 'qualified certificate' is a certificate which meets the requirements laid down in the Directive's Annex I and is provided by a certification-service provider, which fulfils the requirements laid down in the Directive's Annex II.

For an electronic certificate to be encompassed by the specific provisions under the Directive, Annex I letter (a) stipulates that the certificate must contain an indication stipulating that the certificate is issued as a qualified certificate. If an electronic certificate does not include this stipulation, it is only encompassed by the general provisions of the Directive.

[18] This is regulated by Article (9) of Directive 2000/31/EC (The e-Commerce Directive).

It should also be noted that the Directive only addresses advanced and qualified signatures that are generated or signed by natural persons.

According to Article 2 (3) a 'signatory' is a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents. Although the Directive does not state that the electronic signature has to refer to a *natural* person, the signatory of a qualified electronic signature (article 5 (1) of the Directive) can only be a natural person, as this form of signature is considered as the equivalent of the handwritten signature.

This matter has been debated since it was argued by the Parliament in the preparatory work that the Directive should reflect that a signatory could be only a natural person, but this approach was not followed in the final text. The above conclusion is, however, confirmed by the Commission in the Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures (The Operation Report)[19].

4.2.1 UNCITRAL Model law on Electronic Signatures[20]

On a global scale, the EU Directive on Electronic Signatures is supplemented by the UNCITRAL Model Law on Electronic Signatures. The Model Law was adopted by UNCITRAL on 5 July 2001 and aims at bringing legal certainty to the use of electronic signatures.

The Model Law provides a very general framework that is designed to assist States in establishing a harmonized and legislative framework to address the issues of electronic signatures. It is intended to foster the understanding of electronic signatures and the confidence that certain electronic signature techniques can be relied upon in legally significant transactions.

The Model Law follows a technology-neutral approach, which avoids favouring the use of any specific technical product. The Model Law further establishes basic rules of conduct that may serve as guidelines for assessing possible responsibilities and liabilities for the signatory, the relying party and trusted third parties intervening in the signature process.

Article 6 of the UNCITRAL Model Law on Electronic Signature provides that "where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement."

Building on the flexible definition of a signature contained in Article 7 of the UNCITRAL Model Law on Electronic Commerce, The Model Law on Electronic signatures establishes criteria of technical reliability for the equivalence between electronic and hand-written signatures.

---

[19] Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures. Report from the Commission to the European Parliament and the Council, COM (2006) 120 final of 15.3.2006, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0120:EN:NOT

[20] http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html

The similarities and dissimilarities between the Model Law on Electronic Signatures and the EU Directive shall not be analyzed in this report. It is merely to be concluded that both legal frameworks support the same fundamental principles, even if the approach may vary. It must be emphasized that a Model Law, in contrast to a Directive, has a non-binding character for national lawmakers and therefore has a different function and structure.

4.2.2 Implementation of Directive 1999/93/EC on a community framework for electronic signatures

The Directive was adopted on 13 December 1999 and the deadline for national implementation was 19 July 2001.

Prior to the adoption of the Directive in 1999, a few Member States (Portugal, Italy, France, Germany and Belgium) had existing national legislation concerning electronic signatures and a few other Member States had initiated preparatory work in the field.

An example of pre-Directive legislation is the German Digital Signature Act that came into force on August 1, 1997, where it became the first digital signature law in the world to govern the entire area of a state[21]. The German law outlined conditions under which digital signatures were considered secure and regulated a voluntary accreditation scheme of service providers. The law was also used as the basis for a series of national projects on electronic signatures. The 1997 law was replaced by a new national law implementing the Directive on 22 May 2001.

The Member States with active initiatives, in the period before the Directive entered into force, seemed to focus on the same issues in their national legislation, in particular the requirements on service providers and products, the conditions under which electronic signatures would have legal effect, and the structure of accreditation schemes. Despite a general trend of a uniform regulation of factual themes in national law, it was apparent that the relevant regulations, or the lack of them, in the Member States would be different to the extent that the functioning of the Internal Market in the field of electronic signatures would be endangered. The Directive therefore has specific focus on these issues, for instance Article 5 on legal effects of electronic signatures.

The functioning of the Internal Market is inter alia addressed in Recital 7, where it is stated that the Internal Market ensures the free movement of persons, since citizens and residents of the European Union increasingly need to deal with authorities in Member States other than the one in which they reside; the availability of electronic communication could be of great service in this respect.

All Member States have implemented the Directive on Electronic Signatures.

The majority of the Member States have made a horizontal implementation of the Directive into new national legislation (implementation by creating a new law parallel to the Directive).

[21] Alexander Rossnagel: Digital signature regulation and European trends, http://www.emr-sb.de/news/DSregulation.PDF

Only a very small number of countries have been delayed in their transposition. In these cases, the delay may be due to the very complex technical character of the Directive, which is very unlike traditional legislation.

The research conducted in connection with this study has only found very few examples of legal problems (refer to section 4.2.1.1 below) in the implementation of the Directive.

However, the horizontal implementation of a Directive into national law in a technically complicated area might constitute the risk of creating a legal 'island'. The true interaction of Community provisions (including the underlying purposes) with current legislation may not be totally evident if the provisions and wording of the Directive is more or less copied into a new national law. Furthermore, due to the relatively low uptake and use of electronic signatures in some Member States (and especially the very low use between Member States), the legislative frameworks have not yet been challenged to reveal any possible lack of conformity and legal problems.

4.2.2.1 Specific issues concerning implementation of the Directive

Our findings show that specific conditions concerning the implementation of the Directive exist in Austria and Estonia.

Austria
The Austrian Federal Act on Electronic Signatures defines two types of electronic signatures: 1) an electronic signature and 2) a secure electronic signature. The latter is based on a qualified certificate.

The Austrian Federal Act defines an electronic signature as electronic data attached to or logically associated with other electronic data serving as a method of authentication, i.e., identification of the signatory's identity. The amendment of the Austrian definition concerning the authentication of the signatory's identity varies from the definition of an advanced signature in the directive (which forms the basis for a qualified electronic signature).

The definition of an advanced electronic signature in the Directive (Article 2 (2)) also requires that the signature is linked to the data to which it relates in such a manner that any subsequent change of data is detectable. The Austrian definition of an electronic signature only provides for identification of natural persons and *not* for the integrity of contents.

The lack of a definition of an advanced (non-qualified) signature in the Austrian Federal Act might create a legal gap for this category of signatures, which may result in only the secure electronic signature (based on a qualified certificate)[22] obtaining sufficient legal recognition to be used for e-business and e-government, where security for the integrity of contents also is a key element in communications.

Estonia
The Estonian Digital signature Act only regulates 'Electronic signatures'. The electronic signature covered by the act is, by definition, technically equivalent to an advanced electronic signature as defined in Article 2 (2) of the Directive. The Estonian legislation does not define a qualified certificate.

[22] In this report a signature in accordance with Article 5.1 will be termed "a qualified electronic signature" .

As a result of this, it is not possible to issue qualified certificates pursuant to the Estonian Digital Signature Act. This omission seems to be an essential error in the implementation of the Directive, since the Internal Market provisions in Articles 3 and 4 of the Directive are based on the issuing of qualified certificates. In addition, one of the advantages of the legal framework established by the Directive is the mutual recognition of qualified signatures by the Member States. Such a legal mutual recognition does not necessarily exist for other types of electronic signatures.

The Estonian Digital Signatures Act limits the group of entities that can act as certification service providers (regulated in § 18). Only the following entities and persons which are entered in the Estonian State register of certificates as service providers and registered in the corresponding register in Estonia can be certification service providers:

- public limited companies;
- private limited companies the share capital of which exceeds 400.000 Estonian Kroons (approximately 25 000 EUR);
- legal persons in public law if this is prescribed in an Act concerning the legal person in public law and
- State agencies determined by the Government of the Republic.

The provision does not seem to be in compliance with Article 3.1 of the Directive which stipulates that Member States shall not make the provision of certification services subject to prior authorisation.

Conclusion
The lack of a definition of a qualified signature as seen in Estonia could affect the practical use of certificates between Member States by causing trust-related challenges, since the receiving party does not necessarily have sufficient information about the certificate to determine its security level. Refer to an analysis of this issue in section 4.6.1.

In this context, it is also relevant to mention that positive knowledge regarding the security level of a certificate (i.e. strength of encryption, organisational framework etc.) is necessary before using a certificate to support transfer of personal data. The Directive 95/46/EC on the protection of personal data[23] mandates that the processing of sensitive personal data is carried out with appropriate security in order to protect the rights and privacy of targeted persons. Not all certificates provide for such appropriate security. Refer to section 4.4.2 for a further review of the handling of problems concerning personal data.

4.2.3 Legal equivalence to written signatures

A central point when dealing with electronic signatures is the legal equivalence compared to traditionally written signatures. If an electronic signature cannot be upheld as effective evidence of the signatory's will to be bound in court by the accompanying statement, the use of such signatures will naturally be limited in professional relationships.

[23] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, of 23/11/1995, p. 31-50, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

According to Article 5 (1) of the Directive, Member States shall ensure that advanced electronic signatures, which are based on a qualified certificate and created by a secure-signature-creation device:

(a) Satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and

(b) Are admissible as evidence in legal proceedings.

The benchmarking analysis demonstrates that the legislation in all Member States accepts qualified electronic signatures as legally equivalent to handwritten signatures.

It is important to note that Article 5 (1) (a) does not require a qualified electronic signature to be legally equivalent to a written signature as such. The equivalence is tied to the digital context. To use an electronic signature in the same manner and with the same legal effect as a handwritten signature, the relevant legislation must accept this use by elimination of formal requirements that presume a written signature as one being made traditionally with pen and paper. Refer to further review of this question below in this section.

Article 5 (1) (b) requires Member States to ensure that qualified electronic signatures are admissible as evidence in legal proceedings. This Article gives special status to qualified electronic signatures. The provision is, however, supplemented by Article 5 (2) that establishes a general principle of legal recognition of all kinds of electronic signatures.

According to Article 5 (2), Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

- in electronic form, or
- not based upon a qualified certificate, or
- not based upon a qualified certificate issued by an accredited certification-service provider, or
- not created by a secure signature-creation device.

It can be argued that Article 5 gives preferential treatment to qualified electronic signatures and thereby imposes this as a standard for electronic signatures. The legal equality to handwritten signatures is for example only given to qualified certificates in Article 5 (1) and not to the electronic signatures generally addressed in Article 5 (2).

The study shows that in all 25 Member States, electronic signatures are admissible as evidence in legal proceedings. This seems to be based on the general principles of free admission of evidence in courts.

It should be noted that some Member States (including the Czech Republic, Denmark, and Sweden) have implemented Articles 5 (1) (b) and 5 (2) merely by reference to the general principle of free admission of evidence. The special status given to qualified signatures in Article 5 (1) (b) of the Directive, as stated above, has thereby not been transferred into national legislation in these countries.

4.2.3.1 Formal requirements for the use of electronic signatures

A matter of relevance to the subject of legal recognition of an electronic signature is the Member States' legislation and legal tradition concerning the formal requirements regarding use of electronic communication as a means to enter into binding agreements. See also section 5.1.

In recital 21, it is stated that *'national law governs the legal spheres in which electronic documents and electronic signatures may be used; this Directive is without prejudice to the power of a national court to make a ruling regarding conformity with the requirements of this Directive and does not affect national rules regarding the unfettered judicial consideration of evidence*'.

The elimination of legal obstacles for the conclusion of contracts by electronic means is regulated by Article 9 of the Electronic Commerce Directive that places an obligation on Member States to carry out a screening of their national legislation to enable use of electronic communication and electronic contract conclusion.

The national screening of formal requirements is of the utmost importance to establish a basis for practical use of electronic signatures within the Member States. The principle of the legal recognition of electronic signatures is in practice dependent on the removal of hindrances in general legislation[24].

Our findings show that the principle of functional equivalence between a handwritten signature and an electronic signature is well established in the Member States.

It can be concluded that electronic signatures are admissible as evidence in legal proceedings in all Member States and where electronic communication and electronic contract conclusion is permitted in national law, qualified electronic signatures are equivalent to written signatures.

4.2.4 Main issues and recommendations

All Member States have implemented the Directive and the basic features of electronic signatures are well transposed into national legislation. Qualified electronic signatures are accepted by all Member States as legally equivalent to handwritten signatures, and electronic signatures are admissible as evidence in legal proceedings. The basic legal foundation for use of electronic signatures by businesses is therefore present. For businesses to use electronic signatures as part of electronic communication it is, however, important that Member States remove formal hindrances in national legislation in relation to the use of electronic means.

The findings show that there is some uncertainty in the interpretation of the Directive. This uncertainty encompasses both the legislative level in the Member States and the users of electronic signatures. It is our opinion that initiatives aimed at creating a consistent interpretation of the Directive on a Community level would be useful to support the overall use of electronic signatures.

[24] A review of national legal practices is not included in this report.

4.3 Basic features of electronic signatures

Advanced electronic signatures (also known as digital signatures) are based on Public Key Infrastructure (PKI) technology. A PKI infrastructure enables users of an insecure public network such as the Internet to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

When the proposal for the Directive was being examined, the Commission was very much aware that, given the pace of technological development, it was necessary to be open to the fact that a variety of technologies and services are capable of authenticating data electronically. The Directive is, however, not completely technologically neutral, since the basis for the regulation is the advanced electronic signature (digital signature) that is a technology-specific type of electronic signature, which involves the use of public key cryptography to sign a message. In this sense, the Directive can be described as a two-tier regulation. It seeks legal neutrality by granting minimum recognition to most authentication technologies, while at the same time it incorporates provisions for a specific authentication technology.

Advanced electronic signatures provide for three basic features:

- **Integrity:** ensures that data is unchanged from its source and has not been accidentally or maliciously altered
- **Authenticity:** authentication ensures that messages are what they purport to be and message originators are whom they purport to be, and that the intended recipients receive the messages.
- **Non-repudiation:** ensures that a receiver of a message has strong and substantial evidence that the sender has indeed sent the message. This includes the ability of a third party to verify the integrity and origin of the message.

4.4 Use of electronic signatures

Many non-electronic transactions between government and enterprises/citizens are concluded with a signature, such as the authorizing of a tax return or filing of a form with a local public institution. Depending on the importance of the transfer, the government institution may also require the use of an official ID card to achieve a high degree of certainty regarding the identity of the citizen or a business representative.

When services are moved to the electronic world, the need emerges for equivalent electronic means to ensure: 1) the authenticity of each party within the electronic communication; 2) the integrity of the contents of the communication; and 3) that the electronic communication can be confirmed if there is a dispute (i.e. the non-repudiation). When information is being sent via the Internet, confidentiality of the information also has to be secured[25].

[25] Directive 95/46/EC on the protection of personal data mandates that the processing of sensitive personal data is carried out with appropriate security in the interests of protecting the rights and privacy of targeted persons. As a consequence, personal and sensitive data transferred via an open network (e.g. the Internet) must be encrypted.

The country reports show that electronic signatures are first and foremost used in e-government services. Used in these services, advanced electronic signatures provide for an effective and cost-saving tool that can replace the need for the enterprise or citizen to physically appear at a government office to carry through transactions that need signing a document or showing an ID.

The use of electronic communications that advanced electronic signatures support, offers to a public authority the possibility of acquiring the relevant information in a structured form that can be put directly into the IT systems of the authority without the involvement of a person.

This is not only an advantage for enterprises and citizens that can communicate with public authorities 24 hours a day without physical attendance, but it is also an advantage for the public authorities that can provide a better service to enterprises and citizens at a (potentially) lower cost.

The key to such e-government services is the use of electronic signatures that provides all the necessary features required to exchange valid data in a secure manner.

In e-business relations, the central benefits that electronic signatures provide can also be used. When two parties enter into a business relationship via the Internet, security of the other party's identity (authenticity), certainty that the other party does not reject that the communication has taken place (non-repudiation) and security for the integrity of information can also be a clear benefit that can improve business. But in contrast to the public authorities, the e-business vendor can obtain a certain degree of security to the deal entered online by other means than electronic signatures:

The use of SSL[26] cryptography provides for security that information transferred between the vendor and the customer is not being eavesdropped on. Combined with the use of payment cards that provide a high degree of security for the identity of the consumer, the vendor and the customer create a framework that in most cases provides for sufficient security for the parties to accept business.

For public authorities, the *identity* of the citizen is crucial when providing online services. This is especially important when e-government services include the exchange of personal, sensitive data. Such data must under no circumstances fall into the wrong hands. Therefore, securing correct identification of the citizen is important. However, for many types of businesses, in particular those that limit their activities to online trade of goods and basic services, the identity of the customer is not the most crucial element. More important is the ability to pay for the services that are ordered online – and, of course, to create sufficient security for the validity of the transfer.

A wide range of private services do, however, also need correct identification of customers, for example a business that provides consumer financial services online pursuant to Directive 2002/65/EC.

[26] Secure Socket Layer. This technology is built into most standard web-browsers (e.g. MS Internet Explorer, Firefox and Netscape) and is a method for hiding the information a web browser and a web server send to each other, cf. the Internet Engineering Task Force, www.ietf.org; in the present state of technology, SSL version 2.0 is not secure anymore and SSL version 3.0 should be used, http://httpd.apache.org/docs/2.0/ssl/ssl_intro.html.

The conclusion must be that the more advanced and individually targeted the online services are, the larger the need for correct and non-disputable identification. The fact that e-government services are per se individually corrected is the reason for the growing use of electronic signatures in these services. In the business sector, it is to be expected that advanced services in, inter alia, online financial services will grow in the coming years, which will result in a growing demand for digital signatures[27].

4.4.1 Status of Government initiatives in the field of electronic signatures

The survey of the current status in Member States in the area of electronic signatures carried out for this study[28] shows that most countries have a strategy in place for the introduction of electronic signatures. Among the 18 Member States responding to the survey, 7 have an official government strategy specifically for electronic signatures, while 9 do not have an individual strategy, but have included the issue in an overall national e-government strategy, as shown in the table below.

Table 4.1: Existence of an official government strategy (in writing) for introduction of electronic signatures?

Yes	No	No individual strategy but part of national e-government strategy	No answer
Ireland	Cyprus	Austria	Slovenia
Luxembourg		Czech Republic	
Malta		Denmark	
The Netherlands		Estonia	
Slovak Republic		Finland	
Spain		France	
Sweden		Hungary	
		Lithuania	
		Poland	

Source: Member State survey, 18 Member States participating

A third of the participating Member States have formulated official, quantitative government objectives for the introduction of electronic signatures as shown in table 4.2.

[27] The development of digital services in Europe is described in the Capgemini report "Online availability of Public Services: How is Europe Progressing", June 2006.

[28] The questionnaire and overview of key results of the survey can be found in Annexes II and III to this report.

Table 4.2: Existence of an official quantitative government objective for introduction of electronic signatures?

Yes	If yes: Target	No
Austria	8 million eCards distributed by end of 2005	Czech Republic
Denmark	A total of at least 1.1 million digital signature certificates fulfilling the Danish OCES standard issued to citizens, workers and businesses by the end of year 2006.	Cyprus
Estonia	All public sector institutions have to accept digitally signed documents (from 2002)	Finland
Lithuania	25.000 civil servants (government and local authorities) by the end of year 2007	France
Malta	Rollout in 2007 of smart e-ID Card capable of signing. Penetration: 100% since this will replace the mandatory national ID card.	Hungary
Spain	The full extension of the eID card issuance service is to be completed in two years time, and the total holder count is expected to eventually reach 35 million (most of the Spanish over-18 population) in a few years.	Ireland
		Luxembourg
		The Netherlands
		Poland
		Slovak Republic
		Slovenia (no answer)
		Sweden

Source: Member State survey, 18 Member States participating

The majority of Member States also have more qualitative objectives in place for the introduction of electronic signatures, most of them formulated fairly broadly in terms of more secure and efficient electronic communication.

Table 4.3: Existence of an official qualitative government objective for electronic signatures?

Yes	No
Austria	Cyprus
Czech Republic	France
Denmark	Hungary
Estonia	Ireland
Finland	Malta
Luxembourg	Slovenia
The Netherlands	Spain
Poland	
Slovak Republic	
Luthuania	
Sweden	

Source: Member State survey, 18 Member States participating

Almost all Member States have Government initiatives in place for building a Public Key Infrastructure, as shown in the table below. The two exceptions are Austria and Cyprus. Austria states that PKI in the country is largely market-driven, and that the social insurance institution is the only public body issuing certificates to citizens. In Cyprus, a project regarding PKI has been carried out, for academic use, by the Cyprus Research & Academic Network

Table 4.4: Existence of a government initiative concerning building a Public Key Infrastructure (PKI) and Internet link?

Yes	No
Czech Republic	Austria
Denmark	Cyprus
Estonia	
Finland	
France	
Hungary	
Ireland	
Lithuania	
Luxembourg	
Malta	
The Netherlands	
Poland	
Slovak Republic	
Slovenia	
Spain	
Sweden	

Source: Member State survey, 18 Member States participating

Further results from the survey regarding the adoption of a common standard for electronic signatures and regarding cross-border access to national electronic signatures will be presented in the following sections.

4.4.2 Safeguarding personal data

Directive 95/46/EC on the protection of personal data mandates that the processing of sensitive personal data is carried out with appropriate security in the interests of protecting the rights and privacy of targeted persons[29].

Article 17 of Directive 95/46/EC requires data controllers[30] and processors of personal data to take measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. These provisions have implications for the security requirements of networks and information systems used for e-government and e-commerce services.

[29] Se also Andreas Mitrakas, Information Security and Law in Europe: Risks Checked?, Information & Communications Technology Law, Volume 15, March 2006

[30] Any person or body (private or public) that individually or jointly determines the purposes and means of processing (Article 2(d)). A data controller could for example be a government entity processsing personal data.

According to Article 17 (1), Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

As a consequence of Article 17, it is incumbent on the Member States to ensure an appropriate level of security when personal data is transferred on an open network. As mentioned above, the implemented measures shall ensure "a level of security appropriate to the risks represented by the processing and the nature of the data to be protected." Therefore, higher security standards apply where either so-called 'sensitive data'[31] or personal data that by their nature imply specific higher risks (including but not limited to financial data or data that are subject to professional confidentiality obligations) are processed.

In response to this, personal and sensitive data must be encrypted[32] when transferred on the internet. As described above in section 4.3, digital signature technology can provide for confidentiality of a message and ensures that information can be read only by authorized entities.

This functionality is very important when two parties, e.g. a citizen and a public institution, exchange sensitive personal data in an e-mail correspondence. Such information must, according to Article 17 in the Data Protection Directive, be protected against unauthorized access.

Finally, it should be emphasised that the obligation to take appropriate measures requires anyone who processes personal data to control how such personal data are used, disclosed and protected.

The increasing focus on security is also expected to result in an increasing use of digital signatures to enable secure e-mail for transfer of legal and financial information between businesses.

4.4.3 Summary of main issues

E-government services seem to be the main driver for electronic signatures, making the public sector a key player in facilitating the use of electronic signatures. Transactions in the private sector, i.e. B2B and B2C, provide for very little use of electronic signatures. It is our impression that the private sector, especially as regards SMEs, has still not experienced sufficient need or external demand for adopting electronic signatures when communicating electronically. Refer to section 4.5 below for a review of potential issues in the field of electronic signatures that might constitute a partial cause for not adopting electronic signatures.

Viewed in the light of the public sectors' central role in the use of electronic signatures, it is important that government institutions, when providing online services or taking legislative initiatives, recognize and support the use of electronic communication in general and electronic signatures in particular as a tool to provide effective and secure communication, not only in busi-

[31] Sensitive data are defined by Article 8 in the Data Protection Directive as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or data about health or sex life.

[32] When transmitting sensitive information normally with the use of strong encryption.

ness-to-government situations but also when providing the framework for B2B and B2C relations.

4.5 Reported problems in the field of electronic signatures

The recent implementation of the Directive in Member States means that legal issues arising from the practical use of electronic signatures are only just beginning to emerge in the Courts.

Furthermore, the modest use of electronic signatures means that potential problems in the present national legal framework concerning electronic signatures have not arisen yet. It can be expected that the use of electronic signatures will increase in the following years which will naturally challenge the current regulation and practice concerning electronic signatures and electronic communication as such.

The general picture drawn by the country reports shows that the use of electronic signatures in the Member States is still very limited. In particular, the use by enterprises and consumers of electronic signatures based on qualified certificates is even more limited.

As described earlier, electronic signatures are based on the Public Key Infrastructure technology that uses the system of a 'trusted third party', which allows parties that have never met to trust each other even though they communicate at a distance, for example via the Internet. Such an infrastructure is not established on a day-to-day basis by small service providers. In addition to the cost of a complex technical infrastructure, there is also a substantial cost associated with setting up a secure and trustworthy human organisation to run the technical infrastructure.

The condition for success of such an infrastructure is the existence of a demand from the users of electronic communications. Until now, the vast majority of enterprises have chosen alternative (simpler and cheaper) technologies to meet the demands of the market.

As previously described, e-commerce transactions are most commonly based on SSL technology, which ensures the integrity of the electronic transfer. Combined with the use of payment cards that gives the consumer a high degree of security in connection with payment (cf. section 6.2.2), e-commerce transactions are carried through in a manner that, from the point of view of security, satisfies the market without using advanced electronic signatures.

It is indicated in several country reports[33] that since the traditional methods of concluding contracts are well developed and functioning, the requirement for electronic signatures in business are not considerable.

The country reports leave an impression of the existence of a chicken-and-egg problem. A key condition for investing in electronic signature solutions and establishing electronic services is that there is a certain number of users holding an electronic certificate. But the number of holders of electronic certificates is low exactly because of the low number of services available[34].

[33] Inter alia Denmark, France and Hungary

[34] An example of this definition of problems is the country report from Poland where it is reported that the public authorities are not ready to receive electronic signatures which reduces the penetration in the market.

Examples of four countries who have tried to address this problem with national initiatives are Denmark, Estonia, Austria and Spain.

In **Denmark**, the Government offers free software-based (advanced) signatures to all citizens. The government has, at the same time, established a high number of e-government services that support the use of signatures[35].

In **Estonia**, the government issues ID cards including electronic signatures (based on qualified certificates) to all citizens. Concurrently, there has been a huge focus on establishing supportive e-government and private services.

In **Austria**, the Citizen Card (Bürgerkarte) is a fundamental part of the e-government strategy. The Citizen Card is a smartcard embedded with an electronic signature and a digital certificate which enable citizens to securely access electronic public services and complete administrative procedures electronically. The novelty of the Austrian e-ID concept is that there is not just one single type of Citizen Card. In principle, any card which makes it possible to sign electronically in a secure form and to store personal data is suitable for use as a Citizen Card[36].

In **Spain**, the Government has begun in 2006 to distribute a new version of the ID Card (DNIe) that includes 2 certificates, one for secure identification in an electronic transaction (notably with the public authorities, like filing a tax declaration), and the other for the e-signature of e-documents. The card is offered freely to all citizens[37].

Based on the country reports, it seems that the use of electronic signatures in Member States is most prevalent in the public sector[38]. It is also in the public sector that the call for electronic signatures is mostly present because of the need for secure identification and exchange of information with citizens and business (as described above in section 4.4.1). The central role of the public sector in society also makes it a driver for distribution and penetration of signatures.

In view of this, it is no surprise that in a number of Member States, it is described as a practical problem that e-government solutions are not fully developed for the use of electronic signatures.

In relation to this, it would also seem to be a barrier to further use of electronic signatures that a number of countries have not adopted a common standard for electronic signatures, as the results of the country survey indicate. The table below shows the status for the Member States participating in the survey.

---

[35] Denmark has chosen to interpret the Annex II section d. concerning requirements for verification of identity, based on the principle of direct face-to-face identification. This strict requirement is considered to be one of the main reasons for the very limited numbers of issued qualified certificates after the Digital Signature Act became effective and may also be part of the why the Government promoted the issuing of advanced electronic signatures instead of qualified electronic signatures.

[36] For further information, refer to the Bundeskanzleramt Österreich, http://www.cio.gv.at, and the main page on the Austrian Citizen card project, http://www.buergerkarte.at/index_en.html

[37] For further information, refer to the Spanish Interior Ministry, www.mir.es or DNIE Electronico, http://www.dnielectronico.es/

38 This is for example reported in the Danish, Polish, and French country reports

Table 4.5: Has a common standard for electronic signatures been adopted?

Yes	No
Austria	Czech Republic
Denmark	Cyprus
Estonia	Malta
Finland	Poland
France	Slovenia
Hungary	Sweden
Ireland	
Lithuania	
Luxembourg	
The Netherlands	
Slovak Republic	
Spain	

Source: Member State survey, 18 Member States participating

4.5.1 Court cases

The legal consequences of interaction (or confrontation) of electronic signatures with traditional technologies and practices in business and communications is to a high extent left to court practice.

Court cases in the field of electronic signatures (in a broad sense) have been identified in Greece, Lithuania, Estonia, Italy and Finland.

4.5.1.1 Greece: Case 1327/2001 Court of first Instance of Athens

The court was asked to decide whether a statement of recognition of a debt contained in an e-mail could generate legal effects (A service agreement concluded by a Czech agent with a Greek travel agency).

The judge recognised the validity and the binding effect of the legal acts that were exchanged through the e-mail communications.

The judge pointed out that an e-mail address can be considered as an electronic equivalent of a handwritten signature since it is linked to a specific individual (the sender of the e-mail) and identifies this sender in a unique manner towards the e-mail recipient.

In order to promote the use of electronic communication, the evident force of the e-mail exchange was correctly accepted by the judge. But the comparison of the functionalities of a handwritten signature and an e-mail address must rely on a misunderstanding or be very concretely reasoned.

The unique link between electronic content, e.g. an e-mail, to a specific individual is the core functional essence of an advanced signature, e.g. Article 2.2 of the Directive. This functionality is not created by an e-mail client per se.

4.5.1.2 Lithuania: Židrūnas Šapalas v. AB Lietuvos taupomasis bankas, of 20 February 2002

The Lithuanian Supreme Court ruled that the usage of a payment card with a PIN code is usage of an electronic signature, which is equivalent to a hand-made signature under Lithuanian contract law. In its ruling, the Lithuanian Supreme Court emphasized that the burden to ensure reliability and security of an electronic signature system used for payment orders lies on the bank, rather than on the user of the payment instrument (the payment card).

This ruling seems to be in accordance with the principles laid down in Article 6 of Directive 1999/93/EC concerning the responsibilities for activities performed by certification service providers. But using a payment card with a PIN code does not per se constitute the use of an electronic signature if the card is only used for enabling the transaction of money and an electronic signature (if implemented on the card) was not used for the transaction.

4.5.1.3 Estonia: Tallinn Administrative District Court of June 12, 2003

The Tallinn Administrative District Court ruled that digitally signed documents must be considered equivalent with handwritten ones in court proceedings.

The district court declared that documents may be sent to court by e-mail if they have a digital signature according to laws.

A lawyer representing a client in a dispute sent a digitally signed document to court by e-mail. Tallinn administrative city court claimed that they were not able to read the document and thus rejected it.

The case was taken to district court, where it was ruled that digital signatures are equivalent to handwritten ones in Estonia and therefore the court should not have claimed that they can not use it.

The district court ruling claims: "The reception of a digitally signed document was not obstructed by the lack of appropriate software - it was and still is possible to immediately install such software at courts when necessary."

4.5.1.4 Italy: The Court of Cuneo, December 15, 2003[39]

The Court of Cuneo ordered a company to fulfil its obligations to another company on the basis of a claim proven with e-mail communications.

The Judge of Cuneo held that the use of authentication credentials such as a user ID and password to access the e-mail account represents a valid means of adducing evidence on the origin of the message. Therefore, the Judge held that the e-mails had the same validity as written documents and admitted them as trial evidence.

Simple identification of a person with a user ID and a password does not create the same level of security concerning authentication as identification based on an advanced electronic signature. But the decision is consistent with the E-signature Directive because it provides that a document with a mere 'e-signature' is not denied legal effectiveness or admissibility just because it is in electronic form.

[39] Tribunale Di Cuneo Ricorso Per Decreto Ingiuntivo, December 15, 2003

4.5.1.5 Finland: The Supreme Administrative Court December 23, 2005[40]

The Finnish Supreme Administrative Court found in its judgment on December 23, 2005 that a county government could not require that conclusion of an electronic service contract used by a real estate broker with its customers was secured with qualified certificate or other similar means under best practices requirements, since the requirement of using a qualified certificate or other such advanced verification mechanisms were not required under the letter of the law.

The position of the Supreme Administrative Court was that the county government had no right to impose additional form requirements such as a qualified certificate to the real estate broker, as the law does not mention the form of such contracts. The law does require that the terms of the broker's assignment are provided in a manner that cannot be changed unilaterally. The current generally accepted practice is that the brokers may conclude such service contracts either in writing or by electronic means without necessarily using qualified certificates to secure the electronic transaction.

4.5.2 Summary of main issues

The general conclusion of the benchmarking analysis is that the use of electronic signatures in the Member States is still very limited. In particular, the use by enterprises and consumers of electronic signatures based on qualified certificates is even more limited.

Seen from a business perspective, the important issue is to make rational use of new technologies when this supports the activities of the enterprise. The key issue is not whether to use a specific technology, e.g. electronic signatures.

The current demand for services in the business world does not depend on the use of electronic signatures. This is not to say that electronic signatures will not play a role in business relations, but the incentive for investing in and adopting electronic signature technology has to be present. As described in section 4.4, the public sector plays an important role in facilitating the spreading and use of electronic signatures. As stated, this may be done by central government initiatives.

The court cases illustrate that use of electronic communication, including the use of electronic signatures, are accepted by courts as evidence and can constitute the basis of binding contracts. In this context it is interesting to note that the wide acceptance by the courts of 'ordinary' electronic communication as binding evidence to a certain extent minimizes the need for advanced electronic signatures as tools to provide a high degree of security of evidence. The court cases do, however, also show the challenges for the legal systems in addressing the technically difficult issues connected to the use of electronic communication.

[40] The Supreme Administrative Court, December 23, 2005, case 2722/2/03

4.6 Cross-border issues concerning electronic signatures

A central element of the Directive is the Internal Market principle concerning mutual recognition of qualified certificates issued in other Member States (Article 4).

According to Article 4 (1), each Member State shall apply the national provisions which it adopts pursuant to this Directive to certification service providers established on its territory and to the services which they provide. Member States may not restrict the provision of certification services originating in another Member State in the fields covered by this Directive.

According to Article 4 (2), Member States shall ensure that electronic signature products which comply with this Directive are permitted to circulate freely within the Internal Market.

The principles of freedom of establishment in the European Union arise from Article 43 of the European Community Treaty that prohibits restrictions on the freedom of establishment throughout the Union and Article 49 that prohibits restrictions on the freedom to provide services.

Article 4 is central to the main objective of the Directive: To create a Community framework for the use of electronic signatures, allowing the free flow of electronic signature products and services across borders, and ensuring a basic legal recognition of electronic signatures.

This objective is also apparent in recital no. 10 that reads as follows:

The internal market enables certification-service providers to develop their cross-border activities with a view to increasing their competitiveness, and thus to offer consumers and businesses new opportunities to exchange information and trade electronically in a secure way, regardless of frontiers; in order to stimulate the Community-wide provision of certification services over open networks, certification-service-providers should be free to provide their services without prior authorisation; prior authorisation means not only any permission whereby the certification-service-provider concerned has to obtain a decision by national authorities before being allowed to provide its certification services, but also any other measures having the same effect;

In reality, however, specific national requirements will constitute obstacles to cross-border services if they are specific for the country in question.

Three Member States (Czech Republic, Estonia, and Slovak Republic) seem to be in conflict with the free market principle in Article 4.

The Czech Republic has some exceptions to the main rule of mutual recognition: For example, electronic tax returns may only be signed by the recognized electronic signature issued by a Czech service provider.

In Estonia, in order to be recognized as being equivalent to certificates issued by an Estonian certification service provider, certificates from a foreign certification service provider must either be confirmed by a registered certification service provider, be explicitly compliant with the Digital Signatures Act requirements or covered by an international agreement. These requirements restrict the provision of certification services originating in other Member States.

In the Slovak Republic, qualified certificates have the same validity and legal recognition, regardless of their country of origin, but it is reported that a verification process must be accomplished before a non-national qualified certificate is fully accepted.

With the exception of the abovementioned countries, no specific *legal* obstacles for the cross-border use of electronic signatures have been found.

However, the *administrative* practices for access to the electronic signature(s) in use in individual Member States for enterprises and citizens from other Member States constitute a significant barrier, since a fair number of Member States do not issue electronic signatures to citizens and/or enterprises which are not registered in the country, as can be seen from the Member State survey. This is shown in the table below.

Table 4.6: If electronic signature is introduced, do enterprises and citizens from other EU Member States have access to the electronic signature?

Yes	No	Don't know/ No answer
Austria	Czech Republic	Cyprus
Estonia	Denmark	
France	Finland	
Hungary	Ireland	
Lithuania	Malta	
Luxembourg	Slovenia	
The Netherlands	Sweden	
Poland		
Slovak Republic		
Spain		

Source: Member State survey, 18 Member States participating

4.6.1 Key elements of a qualified certificate

One of the most significant strengths of the Directive on Electronic Signatures is the definition of a qualified certificate. A qualified certificate is by the force of the Directive a high-quality certificate with a transparent security level which provides for legal recognition in all Member States. This overall quality does not exist for any other type of certificates (irrespective of their factual qualities) that can be acquired in the Member States.

The Member State survey shows that two thirds of the Member States participating in the survey issue qualified certificates as defined in the Directive, as shown in the table on the next page.

Table 4.7: Are qualified certificates as defined in the e-signature Directive issued in your country?

Yes	No
Austria	Cyprus
Czech Republic	Denmark
Estonia	France
Finland	Luxembourg
Hungary	Malta
Ireland	Sweden
Lithuania	
Netherland	
Poland	
Slovak Republic	
Slovenia	
Spain	

Source: Member State survey, 18 Member States participating

The lack of a definition of a qualified signature in national law (as seen in Estonia) or the use of other types of electronic signatures could affect the practical use of certificates by causing trust-related challenges as the receiver of the certificate (the Relying Party) does not necessarily have sufficient information about the certificate to determine its level of security (organisational and technically)[41].

This positive knowledge of security and legal recognition as laid down in the Directive is one of the core essences of the qualified signature framework.

When receiving a certificate marked as a qualified certificate, users in the Member States are able to rely on the Community legal framework and should therefore, as a starting point, be confident refraining from further investigation of the certificate and the underlying legal and organisational framework.

This security and trustworthiness based on a common legal framework does not reach the same level when a user receives an 'un-qualified' signature. Even though this 'un-qualified' signature is based on a certificate with a high technical security level and is backed by a well–known, trustworthy organisation, the user does not know for a fact if the certificate provides a sufficient level of security for the intended use.

In principle, to get sufficient knowledge of the certificate and the related infrastructure including the issuing organisation, the user has to make a further study of the organisation's published certificate documentation.

When setting up a Public Key Infrastructure with the issuing of certificates, the certification service provider (Certification Authority) is expected to publish at least two documents: A Certificate Policy (CP) and a Certification Practices Statement (CPS). The CP describes the requirements for operation of the PKI and for granting certificates as well as lifetime management of those certificates. The CPS describes the actual steps that the Certification

[41] Annex I (a) in the E-signature Directive requires that a qualified certificate contains an indication that the certificate is issued as a qualified certificate.

Authority takes in implementing the CP. These two statements taken together are designed so that a Relying Party can look at them and obtain an understanding of the trustworthiness of the certification offered by the certificate issuing Certificate Authority. For most business and personal users, the (very technical) documents will not be of any help in evaluating if a specific certificate provides sufficient trust.

The built-in legal and technical certainty of a qualified certificate provides a significant reduction in administrative burdens when using certificates both inside and between Member States.

In this context, it is also relevant to mention that positive knowledge regarding the security level of a certificate (i.e. the strength of encryption, the organisational framework behind it, etc.) is necessary before using a certificate to support transfer of personal data. Directive 95/46/EC on the protection of personal data mandates that the processing of sensitive personal data is carried out with appropriate security in the interests of protecting the rights and privacy of targeted persons. Not all certificates provide for such appropriate security. Refer to section 4.4.1 for a further review of this issue.

4.6.2 Potential challenges for cross-border use

In the following subsections, examples of potential challenges to cross-border use will be analysed further. Finally a short review of the regulation concerning electronic communication in the procurement Directives can be found in section 4.6.3. A well-functioning Internal Market for certificate services is a condition for the success of the initiatives concerning use of electronic communication in public procurement.

4.6.2.1 Additional requirements in the public sector

A cross-border issue may emerge due to Article 3 (7) that opens up for additional requirements for use in the Public Sector.

Article 3 (7) reads as follows:

Member States may make the use of electronic signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens.

It can very well be argued that any additional requirements, regardless of the reason, may constitute an obstacle to cross-border services for citizens. But the possibility for the public sector to operate with additional requirements is well founded i.e. to establish effective e-government solutions. An example of an additional requirement subject to Article 3 (7) could be a requirement concerning the content of certificates to be accepted by Public Authorities. If Public Authorities e.g. use social security numbers to register and file communication with citizens, the existence of a social security number (or a substitute for this) in certificates could constitute such an additional requirement.

Since certificates are not produced or issued piecemeal on a practical level, it should be noted that such additional requirements specified by national Public Authorities will, however, unavoidably constitute an obstacle to cross-border services. With the current technology on the market today, Certifica-

tion Authorities will not be able to issue customized certificates to facilitate e.g. cross-border use.

4.6.2.2 Accreditation Schemes

According to Article 3 (1) Member States may not make the provision of certification services subject to prior authorisation.

Without prejudice to this provision it is possible for Member States to introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision, Article 3 (2). All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory.

Voluntary accreditation is defined in Article 2, (13) as *any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.*

In other words, an accreditation scheme sets out specific requirements that certification service providers must conform to if they want to mark their certificates as accredited. The purpose of voluntary accreditation schemes is to encourage the development of best practices among certification-service providers by creating a framework that supports services towards the levels of trust, security and quality demanded by the evolving market (recital 13).

There is no doubt that voluntary accreditation schemes could be beneficial for the development of a competitive market for the issuance of electronic signatures, since it can give certification-service providers the possibility of demonstrating their level of security and trustworthiness. Accreditation schemes could for example be used to certify a specific sufficiency of a particular service for the health care sector, where sensitive personal data is handled and extra high security is required for certain operations.

Despite the positive aspects of voluntary accreditation schemes, there is a risk that accredited certificates will constitute a higher level of electronic signatures that is given a special position that supersede the qualified certificate described in Article 5 (1) as the most secure and flexible signature which is also legally recognized among the Member States. Such a situation would be in conflict with the overall purpose of the Directive.

Even though accreditation schemes on the formal side are voluntary, they may constitute a hindrance to the free provision of certification services as stated in Article 3 (1) and especially for the provision of certificates from other Member States (in accordance with Article 4 (1)) and certificates issued by a service provider in a third country (in accordance with Article 7 (1)).

A hindrance is created if the actual use of certificates in a country presumes that the issuing of certificates is included in an accreditation scheme. Such a situation exists if accredited certificates are given a legal status that is superior to 'ordinary' qualified certificates or if e.g. use of the certificate in transactions with public institutions requires that the certificates are accredited.

CASE: Accreditation of Service Providers in Germany

Accreditation of service providers plays a central role in the German legislation on electronic signatures.

Accreditation was introduced in the first German Digital Signature Act of 1997, where notification of the national accreditation scheme was a precondition for providing signatures that could ease the burden of proof in court proceedings on the basis of their assumed security. The 1997 Digital Signature Act prescribed a two-stage certification structure. The Regulation Authority is the only root certification authority. It certifies all licensed certification authorities and they certify the users.

The law currently in force, The Law Governing Framework Conditions for Electronic Signatures (Signatures Law)[42] Section 2 (15), defines 'Voluntary accreditation' as a procedure to issue a permit that authorizes the operation of a certification service and confers specific rights and obligations.

According to Section 15 of the Signatures law, Certification-service providers may be accredited by the competent authority[43] upon application.

Accreditation shall be given if the certification-service provider can show that the requirements under the Law and the accompanying statutory ordinance are fulfilled. The security of electronic signatures, provided by voluntarily accredited certification authorities, is assured by close vetting of all trust centre equipment, software and even personnel. The equipment and software provided to holders of cards used for generating digital signatures must likewise satisfy the stringent requirements of the Act.

Accredited certification service providers will be given a quality sign by the competent authority. This quality sign will function as proof that the accredited qualified electronic signatures offer security that has been comprehensively tested technically and administratively. The service providers shall be allowed to call themselves accredited certification-service providers and refer to the proven security in legal and business transactions.

To fulfil the requirements described above, the general security requirements for issuing certificates as described in the law shall be comprehensively tested for their suitability and practical implementation and approved by an official office appointed by the competent authority. The testing and approval of the certification service provider shall be repeated following any changes that greatly affect security, and at regular intervals of time.

If an accreditation is revoked or withdrawn, or if an accredited certification-service provider ceases to operate, the competent authority shall ensure that his operations are taken over by another accredited certification-service provider or that the contracts with the signature-code owners can be handled.

The top-level node in the accredited infrastructure is the competent authority, which acts as a 'root' certification authority. The competent authority generates public and private keys for lower-level certification authorities (the accredited service providers) and issues certificates affirming the authorities' ownership of public keys, just as the accredited service providers issue certificates for its customers.

[42] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, May 16 2001.

[43] According to Section 3 the task of the competent authority shall be performed by the Regulatory Authority for Telecommunications and Posts. According to section 15 the competent authority may make use of private offices for the accreditation.

Comments:
It could be argued that the mandatory transfer of operations (e.g. certificate holders) if an accreditation is revoked or withdrawn, is in conflict with the principle of voluntariness that is imposed by the Directive, since the certification-service provider has not necessarily ended his operations as a 'regular' issuer of non-accredited qualified certificates. The provision links together the right to operate as a service provider with a portfolio of certificates to a requirement of being encompassed by the accreditation scheme. The implication is that, if the service provider no longer has an accreditation, operation as a Certification Authority is no longer possible[44].

As described above, it may be problematic if Member States in general create a new category of electronic signatures, with a security level that supersedes qualified signatures and therefore provides more flexible use and better legal recognition than qualified signatures.

Such a situation would force Certification Authorities to apply for accreditation in each Member State where the Certification Authority wishes to provide services. This would potentially impose a huge financial and organisational burden on the Certification Authority, since the accreditation schemes are not necessarily identical in the Member States. A consequence of this would be that cross-border services would be limited. As stated in the KU LEUVEN report[45], accreditation schemes should focus on the assessment of best practices and appropriate security and not be considered as instruments to control the compliance with the Directive or with national legal provisions.

4.6.2.3 Commercial relations

Unless Certification-Service Providers are part of a public authority, they issue certificates on the basis of a business model that requires turnover and profit[46].

There are two basic services offered by a Certification Service provider: One is issuance of certificates; and the other is the setting-up and operation of a certificate revocation list.

In addition to these two services, the Certification Service Provider can also offer other services, for example archiving and time stamping services.

To keep the business running, the Certification Service Provider must generate an income. This income may either flow from the issuing of certificates and/or from providing access to the revocation list, which is a precondition for establishing trust in the user's certificate.

Pricing of certificates does not as such constitute a cross-border concern, since an enterprise or a citizen may just choose to require a certificate from another, more competitive Certification Service Provider. The concern lies in the pricing of access to the revocation list. A Certification Service Provider may choose to operate with a business model that consists of very low fees

[44] Survey of International Electronic and Digital Signature Initiatives, The Internet Law & Policy Forum.

[45] KU LEUVEN, legal and Market aspects of Electronic Signatures, 2003. Study for the European Commission – DG Information Society

[46] Public initiatives may of course also be based on a business model, but the focus on profit and turnover is for obvious reasons not as significant as for private business.

(if any) for issuing certificates but a very high fee for access to the revocation list for professional users, e.g. enterprises and public institutions.

A public authority that has a high incentive for using certificates may accept paying a considerable subscription fee for using certificates from its own domestic Certification Authority because it has a high number of registered users that demand the electronic services of the authority. But if a foreign enterprise seeks to use his national (foreign) certificate as an identification mechanism or if a national enterprise has acquired a certificate from a foreign Certification Authority, the public authority may not necessarily accept the certificate from the enterprise, if it doesn't have an agreement with the foreign Certification Authority (on the assumption that the foreign Certification Authority requires such an agreement to provide access)[47].

The problem of cross-border use as described seems only possible to solve by establishing an international Certification Authority validation network, that provides not only for technical interoperability, but also for commercial clearance among participating Certification Authorities.

The establishment of a cross-border validation network that sets up a relationship between end users (certificate holders), relying parties (e.g. government institutions) and Certification Authorities can be constructed through various models which all have their specific strengths and weaknesses.

The different models will not be examined in this study, but it should be emphasized that without establishment of cross-border trust models among Certification Service Providers in the Member States, there will be no wide use of electronic signatures between Member States.

4.6.3 Initiatives concerning public procurement

The EU wants to see the role of e-signatures continuing to grow. This was i.a. demonstrated in Directive 2001/115/EC on e-invoicing[48] (refer to section 6.1.1). One of the latest legislative initiatives that support electronic signatures concerns the procurement area.

With the introduction of the Procurement Directives, 2004/18/EC and 2004/17/EC, the rules are established for tendering electronically and conditions put in place for modern purchasing techniques based on electronic means of communication.

According to the Communication from the Commission on an Action plan for the implementation of the legal framework for electronic public procurement[49], this initiative makes e-procurement the first sector in which busi-

[47] The described business model is used in Denmark where the official Certification Service Provider TDC requires a fee from enterprises that wants to use certificates from TDC in their online services.

[48] Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernizing and harmonizing the conditions laid down for invoicing in respect of value added tax

[49] Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions Action plan for the implementation of the legal framework for electronic public procurement {SEC(2004)1639} /* COM/2004/0841 final */

nesses use qualified signatures in transactions with public authorities in a Member State other than their home country.

The regulation concerning public procurement is set out in article 42 and Annex 10 of the Procurement Directives.

In Annex 10 it is inter alia stated that devices for the electronic receipt of tenders, requests for participation, and plans and projects in contests must at least guarantee, through technical means and appropriate procedures, that electronic signatures relating to tenders, requests to participate and the forwarding of plans and projects comply with national provisions adopted pursuant to Directive 1999/93/EC.

The provisions (Article 42(5) (b) of Directive 2004/18/EC, and Article 48(5)(b)of Directive 2004/17/EC) do not define which type of e-signature should be used in electronic tendering. Thus, Member States - who have different legal signature concepts – may choose the level they require in conformity with the e-signatures Directive 1999/93/EC.

However, a consequence of the abovementioned articles in the Procurement Directives is that any public purchaser in the EU must receive and process tenders submitted, if required, with a qualified signature and their accompanying certificates, regardless of their origin within the EU or their technical characteristics, and even when they contain documents of different origin (i.e., from a consortium of suppliers) and possibly bear signatures of different levels from different sources (i.e., from different national authorities).

This provision places a nearly impossible burden on public purchasers that offer the possibility of delivering electronic offers, since it is in practice not possible to receive and handle certificates from unknown certification service providers. This brings into sharper focus the interoperability problems on all levels or, as phrased in the Action plan for the implementation of the legal framework for electronic public procurement: *The interoperability problems detected despite the existence of standards, and the absence of a mature European market for this type of signatures pose a real and possibly persistent obstacle to cross-border e-procurement.*

The existing differences between qualified signatures as required by some Member States should therefore be reason for great concern since they, on both a practical and legal/organisational level, will obstruct the use of electronic signatures as it was intended in the procurement Directives.

A further description of the introduction of electronic means in public procurement can be found in the Commission Staff Working Document “Requirements for conducting public procurement using electronic means under the new public procurement Directives 2004/18/EC and 2004/17/EC.”[50].

4.6.4 Summary of main issues

Cross-border use of electronic signatures depends on the possibility of a party to technically receive, read and control the other party’s electronic signature. Establishment of a well-functioning PKI infrastructure that provides for technical interoperability between various certification-service pro-

[50] SEC(2005) 959 Commission Staff Working Document: Requirements for conducting public procurement using electronic means under the new public procurement Directives 2004/18/EC and 2004/17/EC.

viders is the first condition for cross-border use. Technical interoperability is, however, not sufficient per se to support cross-border use (or use between certificate users connected to various certification service providers). Commercial interoperability must also be provided when establishing a PKI infrastructure with involvement of Certification Service Providers with different business models. An enterprise in one country is not necessarily able to accept an electronic signature from a customer in another country using a certificate from its domestic certification service provider, if a clearance agreement has not been established between the enterprise and the foreign Certification Service Provider.

The advantage of using electronic signatures based on qualified certificates is the support from the legal framework created by the Directive. This advantage depends, however, on a well-functioning Internal Market as underpinned in Article 4. From a legal point of view, the introduction of accreditation schemes pursuant to Article 3 (1) and the possibility of establishing additional requirements in the public sector pursuant to Article 3 (7) seem to be the most critical when using electronic signatures in communication with the public sector. It must be emphasized that such additional requirements in the public sector for receiving electronic signatures must be kept at a minimum to reduce the risk of limiting the free flow and use of electronic signatures.

Community legislative initiatives that support the use of electronic signatures in electronic communication i.a. as seen in the Procurement Directives and the Invoicing Directive[51] will not only increase the use of electronic signatures in the Member States but will also contribute to the advancement of cross-border use.

[51] Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax. Refer to section 6 for a further review of this Directive .

5. Legal and administrative practices in the field of electronic contract conclusion in the 25 European Union Member States

This chapter describes the findings in the field of contract conclusion with particular focus on the national and administrative practices concerning the national contract laws and rules implementing the following Directives:

- Directive 93/13/EC on unfair terms in consumer contracts;
- Directive 1997/7/EC on the protection of consumers in respect of distance contracts;
- Directive 1998/6/EC on consumer protection in the indication of the prices of products offered to consumers;
- Directive 1999/44/EC on certain aspects of the sale of consumer goods and associated guarantees;
- Directive 2000/31/EC on information society services (The e-Commerce Directive)
- Directive 2002/65/EC concerning the distance marketing of consumer financial services and amending Directive 90/619/EEC, 97/7/EC and 98/27/EC;
- Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the Internal Market and amending Directives 84/450/EEC, 97/7/EC, 98/27/EC and 2002/65/EC.

The analysis in this chapter addresses the following key issues:
- Contract conclusion: European legal traditions and possible convergence
- Implementation of the Directives most relevant to contract conclusion
- Binding or not binding nature of the electronic invitation to make an offer, submission of and acceptance of an offer
- Information requirements in the Directives
- Reported problems in the field of contract conclusion
- Court cases
- Cross-border issues

5.1 Contract conclusion: European legal traditions and possible convergence

The European Union has brought together many legal systems under a single legislator, which in turn has adopted laws and Directives taking precedence over national laws. In effect, the European Union could be called a mixed jurisdiction, there being a growing convergence within the Union between Europe's two major legal traditions, the Civil law of the continental countries and the Common law of England, Wales and Ireland.

Civil law may be defined as the legal tradition which has its origin in Roman law, as codified in the Corpus Juris Civilis of Justinian and as subsequently developed in Continental Europe and around the world. Civil law is highly systematized and structured and relies on declarations of broad and general principles, often ignoring the details.

Common law is the legal tradition which evolved in England from the 11th century onwards. Its principles appear for the most part in reported judgments, usually of the higher courts, in relation to specific fact situations aris-

ing in disputes which courts have adjudicated. The common law is usually much more detailed in its prescriptions than the civil law[52].

The substantive differences between the European systems of private law are considerable, especially between the Common law of England and Ireland and the Civil law of the other countries. But there are also wide divergences between the Civil-law systems of continental Europe.

These differences between the legal systems have influenced how basic legal principles are understood and practiced by the Member States.

The European Commission has, for a number of years, addressed problems of contracting in the Internal Market by adopting measures relating to specific contracts or sectors. As a supplement to this, the European Commission has undertaken a series of initiatives aimed at increasing the overall coherence of European contract law[53].

In particular, the focus of the ongoing work is to examine whether the proper functioning of the Internal Market may be hindered by problems in relation to the conclusion, interpretation and application of cross-border contracts.

The Commission's Action Plan on a more coherent European contract law[54] presents the conclusions drawn from the first round of consultation on European contract law.

The Action Plan suggested, as a first measure, the improvement of the existing and future Community Acquis in the field of contract law. This could be achieved by means of a so called Frame of Reference, which contains rules on the conclusion, validity and interpretation of contracts as well as performance, non performance and remedies, rules on credit securities and movable goods and on the law of unjust enrichment. This would fill in the many lacunae which the Acquis leaves open.

The Action Plan seeks to launch a second round of discussion by proposing three measures. The measures suggested include both regulatory and non-regulatory actions. This action would be taken in concert with the current sector-specific approach and intends:

- to increase the quality and the coherence of the EC Acquis in the area of contract law;
- to promote the elaboration of EU-wide general contract terms;
- to examine further the opportunities of non-sector-specific solutions such as an optional instrument in the area of European contract law.

The Commission has collected all the responses to the Action Plan including contributions to the ongoing work on a more coherent European contract

---

[52] A more thorough review can be found in the article Mixed jurisdictions : common law vs civil law (codified and uncodified) by William Tetley on the Unidroit homepage http://www.unidroit.org/english/publications/review/articles/1999-3.htm

[53] Communication from the Commission to the Council and the European Parliament on European Contract Law, of June 11, 2001 COM(2001) 398. http://ec.europa.eu/consumers/cons_int/safe_shop/fair_bus_pract/cont_law/cont_law_02_en.pdf

[54] Communication from the Commission to the European Parliament and the Council - A more coherent European contract law - An action plan; COM (2003) 68 final, of of 12 February 2003; OJ C*63, of 15.3.2003, p. 1-44.* http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0068:EN:HTML

law. The responses to the three measures submitted in the Action Plan have generally been positive, but also shows that Member States and stakeholders do have different understandings concerning needed initiatives[55].

A concrete initiative to promote a more uniform framework for e-Commerce was stated in a Communication of 2001 on European Contract Law, where the Commission agreed to examine whether it could promote the development by private parties of EU-wide Standard Terms and Conditions, in particular by hosting a website where market participants could exchange relevant information[56].

After careful examination, the Commission has chosen not to host a webpage i.a. because if an EU-wide Standard Terms and Conditions were to be enforceable in all EEA legal systems, it would need to comply with the most restrictive national law. The Commission believes that parties that do not operate in all EU jurisdictions, in particular not in those with the most restrictive national regimes, might be tempted to not use such a standard. This would greatly reduce the circle of economic actors that would benefit from such an exercise.

The reason given by the Commission shows that there are differences in the Member States of such a character that a joint initiative such as a Standard Terms and Conditions is not possible.

In the First Annual Progress Report on European Contract Law and the Acquis Review[57], the Commission sets out the latest status of the European initiatives on contract law. The report is the first of a series of yearly reports that will be presented in order to fulfil the Commission's commitment to the Council and the European Parliament in the 2004 Communication[58].

5.1.1 International initiatives

The European initiative concerning a more uniform contract Law is supplemented by a number of international initiatives. The four most important of these initiatives are the Commission of Contract Law, The UNIDROT Principles of Commercial Contracts, the UNCITRAL Model law on Electronic Commerce and the United Nations Convention on Contracts for the International Sale of Goods (CISG).

The Commission of Contract Law has focused on a uniform legal framework in Europe for the contractual relationships of parties doing business. It provides for a set of rules detached from national legal systems and thus facilitating cross-border trade within Europe

The UNIDROT Principles of Commercial Contracts sets forth general rules for such contracts and can also be used as a supplement to domestic law and a model for national and international legislators.

The UNCITRAL Model law on Electronic Commerce has a more strict focus on e-commerce and aims at enhancing legislation governing the use of alterna-

---

[55] http://ec.europa.eu/consumers/cons_int/safe_shop/fair_bus_pract/cont_law/analyticaldoc_en.pdf

[56] Section 4.1 COM(2001) 398

[57] http://ec.europa.eu/consumers/cons_int/safe_shop/fair_bus_pract/cont_law/index_en.htm

[58] COM(2005) 456, First Annual Progress Report on European Contract Law and the Acquis Review

tives to paper-based methods of communication and storage of information and in formulating such legislation where none currently exists.

The CISG provides a uniform text of law for international sales of goods. The convention applies to contracts for the sale of goods between enterprises having their places of business in different countries

All four initiatives will be introduced below in section 5.1.1.1 – 5.1.1.4.

To the above must be added that UNCITRAL on 23 November 2005 adopted the United Nations Convention on the Use of Electronic Communications in International Contracts. The convention has so far only been signed by 6 countries, but has the potential to be of significant importance in the coming years in international e-Commerce and will therefore have an indirect impact on European e-business practices. The Convention will be briefly examined in section 5.1.1.5

5.1.1.1 The Commission of Contract Law

The official initiatives on European contract law in the European Commission are supplemented by a number of private initiatives. One of the most noted non-governmental unification projects is the Commission of Contract Law[59] that began its operations in 1980[60].

The prevailing idea was that a Common Market requires a uniform legal infrastructure, especially of contract law, as the existing plurality of national contract laws might be an obstacle to the Internal Market. As a solution to this obstacle and to harmonize the various contractual regimes, legal academics from all the Member States of the European Community have formulated a set of common European principles of contract law: “The Principles of European Contract Law” (PECL)[61]. PECL aims to be a Community-wide, uniform 'infrastructure' for the contractual relationships of parties doing business. It provides for a set of rules detached from national legal systems and thus facilitating cross-border trade within Europe.

The aim of the Commission has not been to develop revolutionary new provisions but to formulate appropriate modern uniform European principles by seeking the best and most expedient principle in each case[62].

Part 1 of the Principles, dealing with performance, non-performance and remedies, was published in 1995. PECL Parts I and II were published in 1999 and Part III in 2003[63].

The Principles of European Contract Law Parts I and II cover the core rules of contract, formation, authorities of agents, validity, interpretation, contents, performance, non-performance (breach) and remedies. The Principles previously published in Part I are included in a revised and re-ordered form. Part III covers plurality of parties, assignment of claims, substitution of new debt, transfer of contract, set-off, prescription, illegality, conditions and capitalization of interest.

---

[59] Also known as the Lando Commission, named for its chairman Law Professor Ole Lando

[60] http://www.cisg.law.pace.edu/cisg/text/peclintro.html

[61] http://frontpage.cbs.dk/law/commission_on_european_contract_law/pecl_full_text.htm

[62] The rules of European Contract Law, Ole Lando,
http://www.cisg.law.pace.edu/cisg/biblio/lando2.html

[63] http://frontpage.cbs.dk/law/commission_on_european_contract_law/survey_pecl.htm

The commission has now ended its work, but it is widely recognized to have created a very important contribution to European contract law[64].

In the following analysis of the European e-commerce regulation, parallels will be drawn to the work of the Commission.

5.1.1.2 UNIDROIT Principles of International Commercial Contracts 2004

The International Institute for the Unification of Private Law (UNIDROIT) is an independent intergovernmental organisation with its seat in Rome. The purpose of UNIDROIT is to study needs and methods for modernizing, harmonizing and co-coordinating private and, in particular, commercial law between States and groups of States[65]

The UNIDROIT Principles of international Commercial Contracts were first published in 1994[66]. The Governing Council of UNIDROIT stressed the need to monitor their use "with a view to a possible reconsideration of them at some time in the future." In 1997, UNIDROIT resumed its work with a view to the publication of an enlarged second edition. This edition was published in 2004.

There are provisions which are very concise and formulated in general terms (i.a. provisions concerning the principle of freedom of contract and the formation of the contract), while others are much more detailed (i.a. provision on the currency of payment and the right to cure). In general, the UNIDROIT Principles are drafted more in the style of the European codes than in the more elaborate fashion typical of common law statutes.

Each article in the principles is accompanied by comments and, where appropriate, by factual illustrations intended to explain the reasons for the black letter rule and the different ways in which it may operate in practice.

The UNIDROIT Principles deliberately seek to avoid the use of terminology peculiar to any given legal system. The international character of the Principles can also be noted by the fact that the comments to the black letter rules systematically refrain from referring to national laws in order to explain the origin and rationale of the solution retained. Only where the rule has been taken over more or less literally from the world-wide accepted CISG, an explicit reference is made to its source.[67]

A number of national legislators have chosen the UNIDROIT Principles as one of the sources of inspiration for the reform of their domestic contract laws. More recently, the UNIDROIT Principles have been chosen as a model for inter alia the new Civil Codes of Estonia and of Lithuania, both of which entered into force in 2001[68].

---

[64] When the work of the Lando Commission ended, the so-called "Study Group on a European Civil Code" (SGECC") has followed as a successor under its chairman Professor Christian von Bar from Osnabrück, http://www.uni-graz.at/bre1www/tom/page16/page16.html

[65] www.unidroit.org

[66] http://www.cisg.law.pace.edu/cisg/biblio/bonell96.html

[67] http://www.cisg.law.pace.edu/cisg/biblio/bonell96.html

[68] Michael Joachim Bonell, UNIDROIT Principles 2004 – The New Edition of the Principles of International Commercial Contracts adopted by the International Institute for the Unification of Private Law

5.1.1.3 UNCITRAL Model law on Electronic Commerce

On a global level, the need to provide harmonized rules to facilitate electronic commerce have been recognized, among others, by UNCITRAL[69].

The UNCITRAL Model Law on Electronic Commerce was adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 1996 in execution of its mandate to promote the harmonization and unification of international trade law, so as to remove unnecessary obstacles to international trade caused by inadequacies and divergences in the law affecting trade.

The Model Law is intended to facilitate the use of modern means of communications and storage of information. It is based on the establishment of a functional equivalent in electronic media for paper-based concepts such as 'writing', 'signature' and 'original'. By providing standards by which the legal value of electronic messages can be assessed, the Model Law aims to play a significant role in enhancing the use of paperless communication. The Model Law also contains rules for electronic commerce in specific areas, such as carriage of goods.[70]

The Model Law was prepared in response to a major change in the means by which communications are made between parties using computerized or other modern techniques in doing business. The Model Law is intended to serve as a model to countries for the evaluation and modernization of certain aspects of their laws and practices in the field of commercial relationships involving the use of computerized or other modern communication techniques, and for the establishment of relevant legislation where none presently exists.[71]

5.1.1.4 The United Nations Convention on Contracts for the International Sale of Goods (CISG)[72]

The United Nations Convention on Contracts for the International Sale of Goods (CISG) provides a uniform text of law for international sales of goods. The Convention was prepared by the United Nations Commission on International Trade Law (UNCITRAL) and adopted by a diplomatic conference on 11 April 1980.

The convention applies to contracts for the sale of goods between enterprises whose places of business are in different states when the states are Contracting States or when the rules of private international law, i.e., choice of law rules, lead to the application of a Contracting State's law. Freedom of contract, however, is a fundamental principle of the Convention, and the parties may opt out or modify the effects of its provisions.

The Convention aims at simplifying contract negotiation and dispute resolution. The Convention does not cover all contracts since it is only applicable to sale of goods and to business-to-business transactions. The convention is therefore not applicable to business-to-consumer transactions and to the provision of services.

---

[69] http://www.uncitral.org/

70 www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html

71 www.jus.uio.no/lm/un.electronic.commerce.model.law.1996/history.background.html

[72] http://www.uncitral.org/uncitral/en/uncitral_texts/sale_goods.html

5.1.1.5 Convention on the Use of Electronic Communications in International Contracts[73]

The United Nations Convention on the Use of Electronic Communications in International Contracts was adopted in November 23, 2005 and is open for signature until 18 January 2008.

The Convention complements and builds upon earlier instruments prepared by UNCITRAL, including the UNCITRAL Model Law on Electronic Commerce.

The aim is to enhance legal certainty and commercial predictability where electronic communications are used in relation to international business-to-business contracts. It addresses the determination of a party's location in an electronic environment; the time and place of dispatch and receipt of electronic communications; the use of automated message systems for contract formation; and the criteria to be used for establishing functional equivalence between electronic communications and paper documents (including 'original' paper documents) as well as between electronic authentication methods and hand-written signatures.

The Convention is designed to remove barriers and provide legal certainty to those engaged in international electronic transactions, in much the same way that the EU Directives on electronic commerce and on e-signatures do.

5.1.2 Summary of main issues

Despite the overall approximation of laws in the Member States due to general Community Law and a series of initiatives aimed at increasing the overall coherence of European contract law, there are still dissimilarities in how legal principles are understood and practiced by the Member States. Ongoing European legal initiatives and international initiatives i.a. in the form of model laws and conventions do, however, function as building blocks for a uniform framework for enterprises entering into online business.

5.2 Implementation of the Directives most relevant to contract conclusion

5.2.1 Outline of the Directives

A number of Community rules have reference to and influences on e-commerce and contract conclusion.

Some of these Directives grant minimum rights (mainly to consumers) that must be offered by national law. The main Directives with relevance to e-commerce and contract conclusion will be outlined in the following subsections.

5.2.1.1 Directive 93/13/EC on unfair terms in consumer contracts[74]

The purpose of the Directive on unfair terms in consumer contracts is to approximate the laws, regulations and administrative provisions of the Member

[73] http://www.uncitral.org/pdf/english/texts/electcom/2005Convention.pdf

[74] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31993L0013:EN:HTML

States relating to unfair terms in contracts concluded between a seller or supplier and a consumer (Article 1 (1)).

Member States must ensure that unfair terms used in a contract concluded with a consumer by a seller or supplier shall not be binding on the consumer and that the contract shall continue to bind the parties upon those terms if it is capable of continuing in existence without the unfair terms.

The Directive also requires contract terms to be drafted in plain and intelligible language and states that ambiguities will be interpreted in favour of consumers.

Member States must make sure that effective means exist under national law to enforce these rights and that unfair terms are no longer used by businesses.

The Unfair Contract Terms Directive introduces a notion of 'good faith' in order to prevent significant imbalances in the rights and obligations of consumers on the one hand and sellers and suppliers on the other. This general requirement is supplemented by a list of examples of terms that may be regarded as unfair.

Member States were required to implement the Directive into their national law by 31 December 1994.

5.2.1.2 Directive 1997/7/EC on the Protection of Consumers in Respect of Distance Contracts[75]

The objective of this Directive is to approximate the laws, regulations and administrative provisions of the Member States concerning distance contracts between consumers and suppliers (Article 1).

The aim is to ensure a high level of consumer protection and put consumers who purchase goods or services through distance communication means in a similar position to consumers who buy goods or services in shops.

The Directive applies to most contracts where a consumer and a supplier, running an organised distance-selling scheme do not meet face-to-face at any stage until after the contract has been concluded.

The central elements of the Directive encompass requirements for Information to the customer before and after the purchase supplemented with a minimum 7 days cancellation right awarded to the consumer.

The Directive also protects the consumer from unsolicited selling and fraudulent use of payment cards (right to cancellation of a payment).

Member States were required to implement the Directive into their national law by 4 June 2000.

[75] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0514:EN:HTML

5.2.1.3 Directive 1998/6/EC on consumer protection in the indication of the prices of products offered to consumers[76]

The main purpose of the Directive is to ensure that the selling price and the price per unit of measurement (unit price) are indicated for all products offered by traders to consumers, in order to improve consumer information and to facilitate comparison of prices. The selling price must be unambiguous, easily identifiable and clearly legible (Article 4).

The scope of application of the Directive is limited to products and does not apply to services. The obligation to indicate the selling price and the unit price for all products offered by traders to consumers is of general application. However, Article 3 (2) of the Directive allows Member States to derogate from this general obligation for products supplied in the course of the provision of a service, for sales by auction and for sales of works of art and antiques. When making use of this derogation, Member States can therefore decide that neither the selling price nor the unit price should be indicated[77].

A minimum harmonisation clause is contained in Article 10 of the Directive, whereby Member States are not prevented from adopting or maintaining provisions which are more favourable as regards consumer information and comparison of prices, if compatible with the Treaty.

Member States were required to implement the Directive into their national law by 18 March 2000.

5.2.1.4 Directive 1999/44/EC on certain aspects of the sale of consumer goods and associated guarantees[78]

The purpose of this Directive is the approximation of the laws, regulations and administrative provisions of the Member States on certain aspects of the sale of consumer goods and associated guarantees in order to ensure a uniform minimum level of consumer protection in the context of the Internal Market (Article 1).

The Directive gives the consumer a right to have goods repaired or replaced or a price reduction given.

According to the Directive, the seller is liable to the consumer for any lack of conformity that exists when the goods are delivered to the consumer and the lack of conformity become apparent within a period of two years.

In the first six months of ownership it will be assumed that faulty goods have been sold with the fault unless disputed and proven otherwise by the manufacturer. Any guarantees offered by the manufacturer or retailer will become legally binding and will have to be given with details of how to make a claim.

Member States were required to implement the Directive into their national law by 1 January 2002.

---

[76] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0325:EN:HTML

[77] Communication from the Commission to the Council and the European Parliament on the implementation of Directive 1998/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of prices of products offered to consumers.

[78] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0044:EN:HTML

5.2.1.5 Directive 2000/31/ECon certain legal aspects of information society services in the Internal Market (The e-Commerce Directive) [79]

The e-Commerce Directive seeks to contribute to the proper functioning of the Internal Market by ensuring the free movement of information society services (including e-commerce) between Member States (Article 1 (1)).

According to Recital 18, Information society services span a wide range of economic activities which take place online. They can, in particular, consist of selling goods online (traditionally e-commerce). Activities such as the delivery of goods as such or the provision of services off-line are not covered.

Member States may not, for reasons falling within the coordinated field defined in the Directive, restrict the freedom to provide information society services. The coordinated field covers all requirements in national legislation that could be applied to an Information Society service (e.g. conditions on the establishment and access to the activity; legislation on content such as illicit content, defamation, language requirements; legislation on consumer protection etc.).

The effect of the Internal Market principle in the Directive is that Member States cannot restrict information society services provided from another Member State.

According to Article 9.1 of the Directive, Member States shall ensure that their legal systems allow contracts to be concluded by electronic means.

Member States were required to implement the Directive into their national law by 17 January 2002.

5.2.1.6 Directive 2002/65/EC concerning the distance marketing of consumer financial services and amending Directive 90/619/EEC, 97/7/EC and 98/27/EC[80]

The objective of the Directive is to establish a harmonised and appropriate legal framework for distance contracts concerning financial services while ensuring an appropriate level of consumer protection.

The Directive supplements Directive 97/7/EC, which ensures appropriate consumer protection in respect of most products and services other than financial. The Directive establishes common rules to govern the conditions under which distance contracts for financial services are concluded.

The Directive covers contracts for retail financial services that are negotiated at a distance (e.g. by telephone, fax or over the Internet), i.e. by any means which do not require the simultaneous physical presence of the parties to the contract. The Directive gives the consumer the right to reflect before concluding a contract with a supplier and gives a certain right to withdraw from the contract.

Member States were required to implement the Directive into their national law by 9 October 2004.

[79] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML

[80] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0065:EN:HTML

5.2.1.7 Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market and amending Directives 84/450/EEC, 97/7/EC, 98/27/EC and 2002/65/EC[81]

The purpose of this Directive is to contribute to the proper functioning of the Internal Market and achieve a high level of consumer protection by approximating the laws, regulations and administrative provisions of the Member States on unfair commercial practices harming consumers' economic interests.

The new legislation outlines 'sharp practices' which will be prohibited throughout the EU, such as pressure selling, misleading marketing and unfair advertising. Certain rules on advertising to children are also set out. Through this legislation, EU consumers will be given the same protection against aggressive or misleading marketing whether they buy locally or from other Member States' markets. Businesses will benefit from having a clear set of common EU rules to follow, rather than a myriad of divergent national laws and court case rulings, as is currently the case[82].

Member States are required to implement the Directive into their national law by 12 June 2007[83].

5.2.2 Implementation of the Directives

The Directives create a legal framework that is important when performing electronic commerce in the Member States both between an enterprise and consumer (or business-to-consumer, B2C) and between enterprises (or business-to-business, B2B).

The Directives relevant to online contract conclusion seem to have been implemented correctly in national law by the Member States and only few deficiencies have been found.

The lack of reported problems may be due to a number of reasons: first and foremost the majority of the Member States have had a number of years to implement the Directives. In addition to this the legal adequacy of the national implementation will be first tested when an increase in the use of electronic trade, especially cross-border trade, will challenge and reveal any dissimilarity between Member States that may exist[84].

Even though the Directives might have been implemented more or less faithfully, compliance with some of the national rules emanating from the Directives remains a major challenge to businesses that carry out distance selling. This will be analyzed further in section 5.4.

---

[81] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0022:01:EN:HTML

[82] http://ec.europa.eu/consumers/cons_int/safe_shop/fair_bus_pract/index_en.htm

[83] According to Article 3 (5) Member States are until at 12 June 2013, able to continue to apply national provisions within the field approximated by the Directive which are more restrictive or prescriptive than this Directive and which implement directives containing minimum harmonisation clauses.

[84] It is reported from Cyprus that even though the Directives have been implemented into national legislation, the adoption of the regulation at an administrative level is far from complete since the use of new technology is still fairly new in Cyprus and are not used widely by business.

For a review of Directive 1997/7/EC and Directive 2002/65/EC with respect to contract execution refer to section 6.3.

5.3 Binding or not binding nature of the electronic invitation to make an offer, submission of and acceptance of an offer

The activity of selling goods and services is governed by contract law, which as a main rule is a matter of national competence[85]. Seen from an overall perspective, Member States use the same main legal principles for the conclusion of contracts.

All the legal systems in the Member States uphold the principle of the binding character of contracts: A party to a contract must be able to rely on the other party keeping his part of the bargain.

These basic principles of contract conclusion can be expressed in the following three elements that must all be present:

- A meeting of the minds between the parties demonstrating that they both understand and agree to the essential elements of the deal
- Consideration – the exchange of something of value, typically a payment in return for goods or a service.
- An agreement to enter into the contract.

The last element - an agreement to enter into the contract - is the core essence of the conclusion of contracts. It consists of an offer from one party and requires the other party to respond with an acceptance.

The general principles of contract law in the Member States do not require a contract in any particular form to be legally binding and can, as a rule, be formed without any written formalities. This principle is in compliance with Article 9.1 of Directive 2001/31/EC concerning treatment of contracts that requires the Member States to ensure that their legal systems allow contracts to be concluded by electronic means[86]. In particular, the legal requirements applicable to the contractual process must neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness or validity on account of their having been made by electronic means.

Article 9 (1) reads as follows:

Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts be-

85 Refer to the current initiatives on contract law at the DG Health & Consumer Protection http://ec.europa.eu/consumers/cons_int/safe_shop/fair_bus_pract/cont_law/index_en.htm

86 with the possible exception of the following categories (Article 9.2):
- contract creating or transferring rights in real estate (except for rental rights)
- contracts requiring by the law the involvement of courts, public authorities or profes-sions exercising a public authority
- contracts of suretyship granted and on collateral securities furnished by persons acting for purposes outside their trade business or professions,
- contracts governed by family law or by the law of sucession

ing deprived of legal effectiveness and validity on account of their having been made by electronic means.

To enforce a contract it is, however, important that it has been agreed in a manner that can be used to provide sufficient proof of the meeting of the minds between the parties involved. This is why written contracts in business relations are usually preferred to oral contracts when the subject of the contract concerns more essential business relations.

To provide sufficient proof of the meeting of minds, an electronic contract may therefore advantageously, like a traditional contract, be signed by the parties involved. The e-Commerce Directive does not explicitly refer to the signing of contracts and does not prevent Member States from imposing requirements of particular techniques to be used in order for a formal requirement of a signature to be satisfied.

According to recital 34 of the Directive the legal effect of electronic signatures is dealt with by the e-Signature Directive (1999/93/EC). Recital 35 ascertains that the e-Commerce Directive does not affect Member States' possibility of maintaining or establishing general or specific legal requirements for contracts which can be fulfilled by electronic means, in particular requirements concerning secure electronic signatures.

The e-commerce regulation therefore recognizes electronic contracts, but does not create a uniform transparent level of recognized signatures. Refer to section 4.1 for a review of Article 5 in the e-Signature Directive.

5.3.1 Distinction between the offer and the invitation to make an offer

From a legal perspective, it is important to distinguish between an offer and an invitation to make an offer (invitation to treat).

An offer is, generally, defined as a clear and unambiguous statement of the terms upon which the first party is willing to contract, should the person or persons to whom the offer is addressed decide to accept.

An invitation to make an offer is generally defined as a statement made under circumstances where it is not intended that it will result in a contract if the person or persons to whom the statement is made indicates his assent to its terms.

When selling goods or services online it is important to determine whether or not the presentation of goods or services on a website (‘display of goods or services in a web shop’) is an offer to the customer or only an invitation to the customers to make an offer.

On a fundamental level, the discussion basically concerns who – the seller or the buyer – carries the risk if the seller has posted an item with a wrong price or if seller runs out of stock of goods which he has displayed at an attractive price online. In other words, must the buyer accept that what seemed to be an attractive offer was not so or must the seller compensate the buyer for the bargain he thought was real?

The country reports show that there is no uniform, and much less clear, definition of this question across the Member States.

In the majority of the Member States (16), advertising on a website for goods and services is, as a main rule, merely considered as being an invitation to make an offer.

However, in the report from 4 countries (France, Italy, Portugal and Spain) it is explicitly stated that as long as all the relevant information is made available to the other party, clicking on an 'I Agree' button on a webpage will be sufficient to conclude a contract. In particular, a French judgment from as early as 1999 recognized that an offer of products for sale on a webpage could constitute an actual offer[87].

In several Member States online advertising on a website under certain conditions can be regarded as a binding offer. When determining this, a number of conditions must be considered:

- Is the website intended for a limited number of persons, e.g. a group of regular customers, or is the website open for an unlimited number of customers?
- Does the website have an online form that can be filled by the customer?
- Does the website have an automatic sales function?
- Is online payment possible?
- The presence of a statement from the vendor that explicitly clears the matter.

The national regulation of this question in traditional commerce relations, e.g. in regular shops, seems to be transferred to the online world. This applies, for instance, to Germany, where offers in a shop window do not constitute a legal offer. The same principle therefore also applies to shops that sell goods online.

A German court case from 2002 concerning an online internet auction shows that the specific circumstances are important for the judgement. On the auction site the seller had indicated a minimum price for the presented items that he was willing to sell at. The court ruled that a winning bid that exceeded the minimum price on such an auction was not considered an invitation but rather a valid binding offer[88].

In Denmark, displaying of goods in a shop window is considered a binding offer, whereas the display of goods online is still debated. The Danish Consumer Ombudsman claims that advertising on the internet constitutes a binding offer, and that this is – at least – clearly the case for businesses that have a 'sales function' on their web-page.

Generally, it seems correct to conclude that the more advanced a given sales function is, e.g. if the online shop has an integrated sales and inventory function, the more likely it will be that goods and services advertised online constitute binding offers.

To the above must be added that a correct implementation by the online vendor of the requirements stated in Article 10 (1) (a) of the e-Commerce Directive (information on the different technical steps to follow to conclude

[87] CA Paris December 3, 1999 Fragrance Counter v. Estee Lauder, No. 1999/12186

88 OLG Hamm, decision December 14, 2002, U 58/00.

the contract) will clarify this issue when the possibility of online concluding of contracts are provided by the vendor[89].

Ultimately, it is up to the national courts to conduct the final interpretation of this issue. The overall lack of court cases does, however, result in some uncertainty. Refer to section 5.6.1 for a review of court cases concerning the distinction of between an offer and the invitation to make an offer.

5.3.1.1 The Principles of European Contract Law (PECL)

The national legal practice of the invitation to treat compared to an offer might be inspired by the regulation in the PECL. The PECL recognize that the offer can be communicated not only to one or more specific persons but also to the public in general.

Article 2:201 (ex Article5.201) - Offer
(1) A proposal amounts to an offer if:
(a) it is intended to result in a contract if the other party accepts it, and
(b) it contains sufficiently definite terms to form a contract.

(2) An offer may be made to one or more specific persons or to the public.

(3) A proposal to supply goods or services at stated prices made by a professional supplier in a public advertisement or a catalogue, or by a display of goods, is presumed to be an offer to sell or supply at that price until the stock of goods, or the supplier's capacity to supply the service, is exhausted.

Seen from an e-business perspective, the provision is interesting. Unless otherwise stated by the enterprise, the offering of services constitutes a binding offer even if it is made to the public, which is the case for enterprises that offer goods and services via the internet to an unlimited base of customers.

By accepting the offer from the vendor, the buyer can enter into a binding agreement. At the same time, the rule protects the supplier since he cannot be bound beyond his capacity to provide, if for example his stock of goods is exhausted[90].

The PECL are applicable to both consumer and business transactions but does not include specific provisions for the protection of consumers.

Even though the above provision provides for some certainty - the buyer decides through his acceptance of the offer if a contract shall be concluded - the provision also opens a certain degree of uncertainty seen from a buyer perspective, since the vendor is not obliged to sell if he runs out of stock or if he accepts offers beyond his capacity. On a practical level, the provision therefore may not create the needed clarity since the buyer never knows if such a situation exists when he makes his acceptance.

One of the advantages of PECL is that it is technology-neutral but the above provision may have its weaknesses in a modern e-business environment, where the operation of e-business with online inventory solutions gets more

[89] Refer to section 5.4 for a review of the information requirements in the E-commerce Directive.
[90] For a further review of PECL and electronic contracts, refer to Katarzyna Kryczka, Principles of European Contract Law and the formation of Contracts in the Information Society. Published in EU Electronic Commerce Law, DJØF Publishing 2004.

common. Using such advanced online services, customers become accustomed to the fact that goods displayed online for sale are available and a contract is concluded unless otherwise explicitly stated by the vendor. Consumers might therefore experience the PECL solution as confusing and non-transparent.

5.3.2 Summary of main issues

There is no uniform definition of whether or not the presentation of goods or services on a website ('display of goods or services in a web shop') is an offer to the customer or only an invitation to the customers to make an offer.

In several Member States, online advertising on a website under certain conditions can be regarded as a binding offer.

A correct implementation by the online vendor of the requirements stated in Article 10 (1) (a) of the e-Commerce Directive (information on the different technical steps to follow to conclude the contract) will clarify this issue when the possibility of online conclusion of contracts are provided by the vendor[91].

The uncertainty and lack of transparency in the national legislation may, however, lower the incentive for SMEs and consumers to enter into cross-border trade.

5.4 Information requirements in the Directives

According to the country reports, a large number of Member States have experienced problems with the lack of compliance of enterprises with the requirements for information to be provided to the consumers by suppliers and online service providers. Some of the court cases resulting from the lack of compliance with the information requirements in the Member States are described under section 5.6 below.

Directive 1999/7/EC and Directive 2001/31/EC both contain obligations concerning information on the main characteristics of the goods or services sold online. This information is to be provided to the consumer by the supplier prior to and after an order is placed when committing business online. The requirements are primarily laid down in Arts. 4 and 5 of the Distance Selling Directive and Arts. 5 and 10 of the e-Commerce Directive.

Directive 2000/31/EC lays down obligations concerning the identification of the service provider (Article 5 (1) and 6(b)), the proper reference to prices (Article 5 (2)), obligations concerning commercial communications as such (identification, description of participations' conditions - Article 6 (a), (c), (d)), as well as information relating to the actual process of contract conclusion by electronic means (in particular, information about the different technical steps leading to contract conclusion and about the technical means for identification and correction of input errors - Article 10).

The information in Article 10 is generally applicable to business-to-consumer as well as business-to-business transactions; although in business-to-business transactions the parties can agree to exclude all or certain information obligations.

[91] Refer to section 5.4 for a review of the information requirements in the E-commerce Directive.

The information required in Article 10 does not apply to contracts concluded exclusively by exchange of e-mail or by equivalent individual communication[92], since such individual communication is viewed as equivalent to individual negotiations in the offline world.

To illustrate the amount of information that is required to be provided by online service providers, the transparency obligations in the e-Commerce Directive and the Distance Selling Directive are summarized below:

Article 5 (1) of the e-Commerce Directive requires the following information to be permanently rendered by the service provider to recipients of the services:

a. the name of the service provider;
b. the geographic address at which the service provider is established;
c. the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner;
d. where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register;
e. where the activity is subject to an authorization scheme, the particulars of the relevant supervisory authority;
f. as concerns the regulated professions:
    - any professional body or similar institution with which the service provider is registered,
    - the professional title and the Member State where it has been granted,
    - a reference to the applicable professional rules in the Member State of establishment and the means to access them;

g. where the service provider undertakes an activity that is subject to VAT, the identification number referred to in Article 22(1) of the sixth Council Directive 77/388/EEC of 17 May 1977 on the harmonization of the laws of Member States relating to turnover taxes — Common system of value added tax: uniform basis of assessment.

Article 5 (2) of the Directive 2000/31/EC requires Member States to ensure that service providers, when they refer to prices, these are to be indicated clearly and unambiguously and, in particular, must indicate whether they are inclusive of tax and delivery costs.

Article 6 of the Directive 2000/31/EC sets out supplementary minimum conditions to ensure a general transparency in relation to commercial communication and specifically in relation to promotional measures when these are permitted in a Member State.

Commercial communication must be in compliance with the following requirements:

(a) the commercial communication shall be clearly identifiable as such;

(b) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable;

[92] Article 10 (5)

(c) promotional offers, such as discounts, premiums and gifts, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously;

(d) promotional competitions or games, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions for participation shall be easily accessible and be presented clearly and unambiguously.

Article 10 of the e-Commerce Directive requires the following information to be provided by the service provider clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service:

a. a description of the different technical steps the customer must follow to conclude the contract.
b. confirmation of whether or not any contract concluded between the service provider and the customer will be filed by the service provider and, if so, whether it will be accessible by the customer.
c. a description of the technical means by which the customer can identify and correct input errors prior to placing of the order.
d. the language(s) offered for the conclusion of the online contract.

According to Article 4 of the Distance Selling Directive, the consumer must receive the following information in a clear and comprehensible manner in good time prior to concluding a distance selling contract:

a. the identity of the supplier and, in the case of contracts requiring payment in advance, his address;
b. the main characteristics of the goods or services;
c. the price of the goods or services including all taxes;
d. delivery costs, where appropriate;
e. the arrangements for payment, delivery or performance;
f. the existence of a right of withdrawal (with a few exceptions stated in Article 6.3);
g. the cost of using the means of distance communication, where it is calculated other than at the basic rate;
h. the period for which the offer or the price remains valid;
i. where appropriate, the minimum duration of the contract in the case of contracts for the supply of products or services to be performed permanently or recurrently.

Article 5 describes the requirements for written confirmation of information. The consumer must receive such written confirmation or confirmation in another durable medium available and accessible to him of the information referred to in Article 4 (1) (a) to (f), in good time during the performance of the contract, and at the latest at the time of delivery where goods not for delivery to third parties are concerned, unless the information has already been given to the consumer prior to conclusion of the contract in writing or on another durable medium available and accessible to him.

In any event the following must be provided:

- written information on the conditions and procedures for exercising the right of withdrawal, within the meaning of Article 6, including the cases referred to in the first indent of Article 6 (3),

- the geographical address of the place of business of the supplier to which the consumer may address any complaints,
- information on after-sales services and guarantees which exist,
- the conclusion for cancelling the contract, where it is of unspecified duration or a duration exceeding one year.

According to Article 6 in the same Directive, the consumer has a cooling-off period of at least 7 days. If the supplier has failed to fulfil the obligations laid down in Article 5, the period shall be three months. In the case of sold goods the period begins from the day of receipt by the consumer. When services are sold the period begins from the day of the conclusion of the contract.

It could be argued that the very thorough description of information to be provided constitutes a detailed requirement specification that could be used constructively by enterprises to provide services in compliance with European regulations. This is of course the case for serious enterprises with expertise in the legislative field but, as stated in the beginning of this section, the requirements also seem to be treated negligently by a significant percentage of the enterprises carrying business online in the Member States.

5.5 Reported problems in the field of contract conclusion

With a few exceptions no specific problems are reported in the Country Reports in relation to the conclusion of electronic contracts as such.

The correspondent from Cyprus reports that the main problem for parties entering into online business is the complete lack of case law. It is not known how courts will interpret in practice the provisions of the relevant legal instruments. This condition has not been reported as a specific problem by the other Member States, but it is the assessment that legal uncertainty based on the absence of court practice is of some concern when entering into online trade.

The country report from Finland mentions that the majority of problems occurring in Finland with regard to the use of electronic contracts relates to frauds perpetrated through electronic means. Since the amounts involved are often small and finding the perpetrators is quite difficult, many fraud cases are left unresolved.

Even though it is indisputable that online fraud also exists in the other Member States, this is not reported as being a specific problem vis-à-vis online contract conclusion by the country reports.

5.6 Court cases

The following court cases have been listed in the country reports.

5.6.1 Court cases concerning the invitation to make an offer

5.6.1.1 Sweden: The Swedish Market Court, case no. 2004:18, July 2004

In a case brought before the Swedish National Board for Consumer Complaints[93], the board stated that an offer which has been addressed by a supplier to the public on a web page did not constitute a binding and valid offer.

Such an offer of supplied goods or services should be regarded as an invitation to anyone who could be interested in the goods or services to leave an offer. For the conclusion of contract the supplier has to accept or verify the consumer's offer in some way.

The board's opinion was confirmed in a case brought before the Swedish Market Court in 2004 by the Swedish Consumer Ombudsman. In this case, a number of persons had been invoiced by a telecommunications company for certain services provided on a number of websites. The persons had connected to the websites in question and had been invoiced for services which they had not explicitly ordered.

The persons had not confirmed any order by stating their names or by leaving any other personal information. In spite hereof, the company sent out invoices and claimed payment for the services provided on the websites. The court came to the same conclusion as the board in that sense that a contract, regardless of its conclusion on the internet or not, can only be valid and binding if there is proof supporting that the parties in any way accepted the agreement by manifesting their will to be bound.

It is interesting to notice that The Market Court established that three clicks are required in order for an Internet order to be valid: (1) to mark the interest of buying, (2) to confirm that you have read the details of the order and the contractual conditions, and (3) to confirm the order itself and accept the contractual conditions. According to the Market Court, the web pages of the telecommunications company did not fulfil these requirements, and was thus in breach of the Swedish Market Practices Act.

5.6.1.2 Germany: OLG Hamm, Higher Regional Court Hamm, 14 December 2000 – 2 U 58/00

A German court case from 2000, concerning an online internet auction, shows that specific circumstances are important for deciding whether a regular offer, or only an invitation to make an offer, has been made.

On an auction site the seller had indicated a fixed starting price for the presented item (a car). The court ruled that a winning bid that exceeded the price on such an auction was not considered an invitation but rather a valid binding offer[94].

The Court held that in the context of an auction, the seller had wide discretion to influence the auction's process by setting a starting, minimum price

[93] Decision of the Swedish National Board for Consumer Complaints no. 2001-4889, May 22, 2002

[94] The court reversed a lower court's decision

for the car, and by determining the bidding steps as well as the auction's fixed time frame. The Court accepted that the seller, in choosing the auction as a means of promoting or actually selling its product, runs the risk of selling at less than what he/she might have hoped for. This fact, the Court concluded, cannot be understood as a problem of fair pricing. The Court held that such a view ignores the particular quality of the auction mechanism as a market too.

The Court explained that an auction holds such risks for the seller (sale at a less than desirable price) but presents a number of opportunities for the seller as well.

The Court reasoned that an auction's process results in the strong likelihood that a price is achieved that is not a reasonable assessment of what might be fair and adequate price but, rather, reflective of the energy associated with the bidding activity that so often attends auctions. With regard to this bidding process and its possibly special dynamic in the internet, where bidders simultaneously learn about other bids and make new bids through the internet itself, the advantages to the seller might even be greater. Certainly, the seller has the advantage of a much larger possible market at an internet auction than at a traditional auction. The Court concluded that this speculation is the seller's responsibility when put before the alternative of advertising or auctioning[95].

5.6.1.3 Denmark: The High Court of Jutland, 2003, U2003.907V

The High Court was presented with the question of whether advertising a used car from a second-hand car dealer on a web page should be considered a legally binding offer or non-binding invitation to make an offer.

The used car dealer had mistakenly advertised a used Audi for sale at a price of DKK 119,900[96]. The correct price was DKK 349,900. A consumer contacted the used car dealer on the phone and declared that he wanted to buy the car for 119,900. He was informed during the telephone conversation that the price of 119,900 was incorrect and that the correct price was much higher. Later the same day, the consumer sent a confirmation of the agreement to the used car dealer by e-mail.

During the proceedings it was maintained by the consumer that the car had been advertised and that the lack of any reservations for mistakes on the web-page of the used car dealer meant that the car was legally offered at DKK 119,900 and that he thus could accept that offer.

The High Court of Jutland resolved the matter ruling in favour of the used car dealer. It is expressly stated in the grounds for the result (the *ratio decidendi*) that advertising on the internet under the present circumstances was to be considered an invitation to submit an offer.

[95] Peer Zumbansen: German Contract Law and Internet Auctions, German Law Review Vol. 2 No. 7 - 15 April 2001

[96] Approx 15.900 Euro

5.6.2 Court cases concerning information requirements

5.6.2.1 The Netherlands: District Court Rotterdam, 19 January 2006, LJN AU9939

Two similar court cases concerning cancellation of a contract in view of a breach of the information requirements in the e-Commerce Directive have been reported from the Netherlands[97].

An internet company sued consumers for failing to pay subscription fees. The consumers had applied for a temporary subscription (trial membership) of erotic content and disputed that an agreement for a long term subscription had been concluded. In both cases, the internet company had failed to prove that it had confirmed the long-term agreement as a consequence of which the consumer was entitled to cancel the agreement.

The decision shows the importance of being in compliance with the requirements for providing the necessary information to the consumer concerning the contract concluded.

In the decision, the Rotterdam Court referred to Article 6:227b of the Civil Code which implements all five requirements listed in Article 10 (1) and (2) of the e-Commerce Directive, and determined that none of those requirements had been complied with. In particular, the Court considered that the internet company did not send any confirmation of the agreement pursuant to which the trial membership had been 'automatically' converted into a permanent membership, nor did it inform as to where the (archived) contract had been filed for later reference, and it remained unclear at which point in time the permanent membership had started.

5.7 Cross-border issues related to the conclusion of electronic contracts in the European Union

5.7.1 The Internal Market clause

Directive 2001/31/EC introduces in Art 3 (1) an Internal Market clause in relation to e-commerce.

According to article 3 (1): *Each Member State shall ensure that the information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field*.

This Article provides that information society services provided to a person in a Member State by a service provider from an establishment in the same or another Member State must comply with the national legal requirements that fall within the coordinated field (se section 5.7.1.1 below). The national enforcement authorities are responsible for ensuring compliance.

The effect of this is to shift the responsibility for enforcement of national legislation (including that implementing EC Directives) to the authorities of the Member State where the provider of information society services is established. National enforcement authorities will regulate information society

[97] District Court Haarlem (cantonal sector) 6 October 2005, LJN AV2652; District Court Rotterdam (cantonal sector) 19 January 2006, LJN AU9939.

services provided from their own country, regardless of where they are delivered inside the Community. Similarly, information society services provided from elsewhere in the Community will be regulated by the enforcement authorities of those Member States.

The principle gives the suppliers the possibility to provide their services all over Europe on the basis of one coordinated legal system, i.e. the rules in the country where the supplier is established.

Where Article 3 (1) regulates how Member States must monitor the performance of services from service providers on its own territory, Article 3.2 provides that any national requirement may not be applied to an information society service provided by a service provider established elsewhere in the Community for reasons that fall within the coordinated field, if this would restrict the freedom to provide that service in the Member State concerned[98].

Together Article 3 (1) and Article 3 (2), establish what is called the *country of origin principle*, which consists of two elements: 1) a principle of home country control and 2) a principle of mutual recognition.

Article 3 (3) provides for derogations from the country of origin principle (listed in the Annex to the Directive) in the following areas relevant for contract law:

- freedom of the parties to choose the law applicable to their contract (5th indent of the Annex),
- contractual obligations concerning consumer contract (6th indent of the Annex),
- formal validity of contracts creating or transferring rights in real estate where such contracts are subject to mandatory formal requirements of the law of the Member State where the real estate is situated (7th indent of the Annex).

Consequently, online advertising, as well as the actual conclusion of a contract by electronic means, are governed by the country of origin principle

5.7.1.1 Coordinated field

Key to the country of origin principle in Article 3 is the coordinated field. The coordinated field is defined in Article 2 (h) as;

the requirements laid down in Member States' legal systems applicable to information society service providers or information society services, regardless of whether they are of a general nature or specifically designed for them.

The 'coordinated field', cf. Article 2 (i) covers requirements with which the service provider has to comply in order to provide information society services (e.g. for qualifications, authorisation or notification), requirements regarding his behaviour, requirements regarding the quality or content of the service (including those applicable to advertising and contracts) and requirements affecting his liability.

[98] Article 3 (2) reads as follows: *Member States may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State.*

In other words, the coordinated field, in principle, is very broad and consists of all the obligations that the information society service provider comes across when initiating and carrying out the activity of an information society service[99].

The definition of the coordinated field does not, cf. Article 2 (ii), include requirements applying to goods as such, to the delivery of goods or to services not provided by electronic means. It also does not cover the exercise of rights of pre-emption by public authorities concerning certain goods such as works of art.

The legal principles related to conclusion of a contract do not fall within the coordinated field and are not harmonized by EU legislation. Nevertheless, as examined above, the principles related to conclusion of contracts are on a general level based on the same principles as in the other Member States.

5.7.2 Applicable law and jurisdiction

There a two central issues for all those who take part in cross-border e-commerce. The question of which national law is applicable to concluded contracts and which is the competent jurisdiction if a dispute is brought to trial. In this section, the fundamental regulations will be examined.

5.7.2.1 Applicable law

In the areas excluded from the scope of application of the country of origin principle referred to above, it is necessary to determine the applicable law. This section will shortly examine the rules and principles that determine which law is applicable in a certain contractual interaction between two parties in the EU.

The question of the applicable law to contractual obligations is the subject of the Rome convention on the law applicable to contractual obligations (1980)[100]. The 15 Member States were already parties to this convention[101]. When in May 2004 the 10 new Member States acceded to the EU, a convention, which is presently under ratification, was concluded in order to allow their accession to the Rome Convention.

It should be noted that present or future provisions of Community law that lay down the choice of law rules in relation to particular matters concerning contractual obligations will take precedence over the terms of the Rome convention.

The Rome Convention allows parties to choose the law applicable to their contract (Article 3).

The material validity of such a contractual choice is, in general, determined by the law which would govern the contract if the choice of law were valid (Article 8). For example, if a supplier offers terms and conditions on his website which provide that any purchase is governed by the laws of Greece, then the question whether the terms and conditions (including the choice of law) are validly applied, must be determined under Greek law. The freedom of

[99] Cf. Recital 21.

[100] "Convention on the law applicable to contractual obligations 1980; OJ C 27, of 26/1/1998, p.34–46; Eur-Lex: 41998A0126(02); http://www.rome-convention.org/

[101] http://europa.eu/scadplus/leg/en/lvb/l33109.htm

parties to choose the applicable law is not unlimited. Firstly, a choice of law does not prejudice the application of mandatory rules of the country to which all elements relevant to the situation are connected.

Other limitations relate to the protection of weaker parties (Article 5 and Article 6). For instance, in the absence of a choice of law, contracts for the supply of goods and services concluded with consumers are governed by the law of the country in which the consumer has his habitual residence where, inter alia, the contract was preceded by a specific invitation or advertisement in the consumer's country and he took all the necessary steps on his part for the conclusion of the contract (e.g. payment) in that country. However, even a choice of law may not deprive a consumer of the protection afforded to him by the mandatory rules of law of his country of residence, if the contract was entered into in the circumstances described above.

If no choice of law is made by the parties (not consumers) to a contract, it is governed by the law of the country with which it is most closely connected. This is presumed to be the country of the habitual residence of the party which is obliged to effect the performance characteristic of the contract. Thus, under normal customer-supplier relationships where the customer orders goods or services from the supplier, the laws of the country of the habitual residence of the supplier will apply[102][103].

5.7.3 Competent Jurisdiction

This section will briefly examine the regulations on jurisdiction within the European Union.

On 27 September 1968, Member States, acting under Article 293, fourth indent, of the EC Treaty, concluded the Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, that was amended by four Conventions on the Accession of the new Member States to that Convention (the consolidated text, hereinafter referred to as the 'Brussels Convention')[104].

On 16 September 1988, Member States and EFTA States concluded the Lugano Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, which is a parallel Convention to the 1968 Brussels Convention.

On 1st March 2002, Council Regulation (EC) No 44/2001 of 22 December on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters ('Brussels I') entered into force. This Regulation replaces for all EU Member States, except Denmark, the Brussels Convention. In this respect, the relationships of Denmark with other Member States will soon be governed by the Agreement between the European Community and the

[102] Quienten R. Kroes (Ed.)., E-business Law of the European Union, Allen & Overy, Legal Practice, Kluver Law International 2003.

[103] In 2005 the Commission has presented a proposal for a Regulation of the European Parliament and the Council on the law applicable to contractual obligations (Rome I)- COM(2005) 650 final that is presently under negotiation.

[104] OJ L 299, 31.12.1972, p. 32-42; Eur-Lex: 498Y0126(01); OJ L 304, 30.10.1978, p. 1; OJ L 388, 31.12.1982, p. 1.; OJ L 285, 3.10.1989, p. 1; OJ C 15, 15.1.1997, p. 1; for a consolidated text, see OJ C 27, 26.1.1998, p. 1.

Kingdom of Denmark on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters[105].

Article 23 of the Council regulation allows parties to a contract to choose a forum in any Member State, whose Jurisdiction shall be exclusive unless agreed otherwise, and stipulates certain formal requirements necessary to give effect to such a choice. According to Article 23 (2), the agreement may be entered into electronically if evidenced by an electronic communication providing a durable record.

There are some limitations to this choice that relates to the protection of the weaker party. As regards contracts concluded by consumers, the choice of court agreement should be entered into after the dispute has arisen or satisfy the conditions under Article 17 (2) or (3).

According to Article 16 (1) of the Regulation, the general rule is that a "*consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or in the courts of the place where the consumer is domiciled*". The consumer thus has the choice, while proceedings *against* the consumer may only be brought to the courts of the Member State in which the consumer is domiciled. As a result of this, consumers can bring disputes before their home jurisdiction.

According to Article 15 (1) (c) of the Regulation, this jurisdictional rule applies if "(…) *the contract has been concluded with a person who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State or to several States including the Member State, and the contract falls within the scope of such activities*".

The definition of 'consumer contracts' therefore includes all contracts where an enterprise pursues commercial or professional activities in the Member State of the consumer's domicile or directs activities to that Member State[106].

When the Regulation was passed, a joint declaration was issued by the European Parliament and Commission which stated that:

'…*the mere fact that an Internet site is accessible is not sufficient for Article 15 to be applicable, although a factor will be that this Internet site solicits the conclusion of distance contracts and that a contract has actually been concluded at a distance, by whatever means. In this respect, the language or currency used by a web site does not constitute a relevant factor*.'

Guidance to the understanding of these rules might also be found in competition law, especially Paragraph 51 in The Commission's guidelines on Vertical Restraints, May 2002[107] The guidelines clearly distinguish between active and passive sales and specify that "general advertising or promotion in media or on the Internet that reaches customers in other (…) territories (…) are passive sales. (…) Insofar as a web site is not specifically targeted at [a group of] customers [from another territory], (…) for instance with the use of banners or links (…) specifically available to these exclusively allocated

[105] OJ L 299, 16.11.2005, p. 62–70; Eur-Lex: 22005A1116(01).

[106] Please note that these rules do not apply to contracts of transport other than contracts which, for an inclusive price, provide for a combination of travel and ac-commodation, according to Art 15 (3).

[107] OJ C122 of 23.5.2002

customers, the web site is not considered a way of active selling". It is added in the guidelines that "if a customer [without being previously actively targeted by the company] visits the website of a distributor and if such contact leads to a sale, including delivery, then that is considered passive selling".

It is, however, important to notice that competition law is concerned with the effects of the market, and thus operates on a more abstract level not taking into account the single contract as such, which is the focus of consumer contract law. The legal value of the guidelines on Vertical Restraints as a guidance to understanding Article 15 (1) on the Brussels I regulation is therefore limited[108].

5.7.3.1 Proposal for a Regulation of the European Parliament and the Council on the law applicable to contractual obligations (Rome I)

In 2005, the Commission presented a proposal for a Regulation of the European Parliament and the Council on the law applicable to contractual obligations (Rome I[109]) that is presently (September 2006) under negotiation. The proposal involves changes to the current regulation in the Rome Convention.

The current legal framework for consumer contracts in cross-border cases, set up by the Rome Convention, establishes, as described above, the general principle of the freedom of choice of the parties with regard to the applicable law to the contract. Nevertheless, in the case of consumer contracts the convention departs from this general principle if the contract has been preceded by 'a specific invitation' addressed to the consumer in another country. In this case the law of the country of the consumer would be applicable.

The proposal introduces in Article 5 (1) what is described as a new, simple and foreseeable conflict rule consisting of applying only the law of the place of the consumer's habitual residence, without affecting the substance of the professional's room for manoeuvre in drawing up his contracts.

As a background for the new regulation, the proposal states that the solution adopted in the Rome Convention has been widely criticised as it often produced hybrid solutions in which the law applicable to the professional and the mandatory provisions of the law applicable to the consumer were applied in parallel. To this is added that, in the event of a dispute, this complex solution entails additional procedural costs that are all the less justified as the consumer's claim will tend to be quite small.

There are two possible solutions to prevent this hybrid situation – full application of the law applicable to the professional or the law applicable to the consumer – only the latter would be truly compatible with the high level of protection for the consumer demanded by the Treaty.

This also – as further stated in the proposal - seems fair in economic terms, since a consumer only makes cross-border purchases occasionally whereas most traders operating across borders will be able to spread the cost of learning about one or more legal systems over a large range of transactions.

According to the proposal, this new solution to the problem of applying the applicable law does in practise substantially modify the situation of the pro-

[108] Jurisdiction and Enforcement in the Information Society, Article by Peter Mankowski, in EU Electronic Commerce Law, DJØF Publishing 2004.

[109] COM (2005) 650 final

fessional, for whom the initial difficulty in drafting standard contracts is to comply with the mandatory provisions of the law in the country of consumption, since under the Convention, the mandatory provisions are already those of the country of the consumer's habitual residence. Regarding other clauses, which the parties are free to draft as they wish, the freedom of the parties to draft their own contract is the rule that continues to prevail; it therefore matters little whether they are governed by the law of one or other party.

The proposed regulation will clarify the present situation, where it is necessary to consider if the contract was preceded by a specific invitation to the consumer in another country, before relevant law can be determined. Seen from a business perspective this clarity might be viewed as an administrative burden since distance selling now encompass the task of drafting contracts targeted individually to all European Member States. This might be especially burdensome for small and medium sized companies.

5.7.4 Reported cross-border related issues

It is the assessment in a majority of the country reports that many SMEs are experiencing difficulties with cross-border trade.

Problems in understanding the provision of e-commerce contract law in force in other Member States and the lack of certainty of the legal status of electronic contacts agreed with trade partners from other Member States are seen as obstacles for SMEs.

However, the study has not identified any national legislative initiatives that establish specific protection of SMEs that enter into online trade parallel with the legislation applied for consumer protection.

None of the country correspondents are aware of any court rulings on the use of electronic contracts in cross-border trade between legal persons or between consumers and businesses.

In addition to the abovementioned general issues, some of the respondents have reported the following specific issues with regard to cross-border trade:

In the Hungarian Country Report, consumers' lack of understanding of their legal rights in connection with cross-border contracts are mentioned as a reason for not concluding contracts with service providers in other Member States.

The correspondent from Ireland indicates that the main cross-border regulatory issue concerning the conclusion of an electronic contract is the lack of clarity concerning the interaction of the principle of the country of origin with the Rome Convention on applicable law and the Brussels I Regulation on competent jurisdiction. Also, the uncertainty concerning the exact time at which a contract is formed operates as a barrier to clear regulation and certainty.

In the German Country Report it is stated that the different extent of the cooling-off period within the Member States poses a difficulty to enterprises that sell to consumers across borders. A pragmatic solution used is to allow the longest cooling of period (14 days) for consumers in order to save the expense of providing different contracts for different countries. This is, however, not considered the best possible solution.

5.7.5 Summary of main issues

Regulation concerning applicable law and jurisdiction seems to be a legal area difficult to understand for non-experts in this field. This is of course not a surprise, as the regulation in this area for good reasons is fairly complicated. But as stated above, uncertainty concerning cross-border regulation is considered a specific and significant hindrance especially for SMEs and consumers.

The proposal from the Commission for a Regulation of the European Parliament and the Council on the law applicable to contractual obligations (Rome I[110]) as examined in section 5.7.3.1 will clarify the present situation with regard to verifying the applicable law to the contract. But as noted in section 5.7.3.1, this clarity might be viewed as an administrative burden since distance selling will encompass the task of drafting contracts targeted individually to all European Member States. This might be especially burdensome for SMEs.

[110] COM (2005) 650 final

6. Legal and administrative practices in the field of electronic invoicing, payment and other matters related to the execution of electronic contracts in the 25 European Union Member States

6.1 Electronic invoicing

Electronic invoicing brings substantial savings to all enterprises independently of their size. It facilitates migration to paperless trade, improves the quality of invoice data and streamlines business processes for both seller and buyer. Examples of the gains in efficiency can be the improved responsiveness, the reduction of paper trails involved in the transactions, and the omission of otherwise necessary tasks including the retyping of data into the invoice[111].

Additionally, over time, the invoice data creates a mass of business intelligence about the business history of and between enterprises, and informs how enterprises may choose to engage in business with other trading partners in the future. Moreover, the technology has the capacity to increase trade and thus tax revenue, enhance regulatory monitoring and oversight capabilities, decrease regulatory costs, and improve official enforcement options and opportunities.

Even with the obvious benefits to be gained from electronic invoicing, one of the key obstacles to broad-based adoption of the technology emanates from diverse legal and regulatory requirements. These obstacles have been created by diverse national legislation, which prevents businesses and administrations from consolidating the electronic commerce environment.

The diversity and complexity of the regulatory environment has until recently created a climate of uncertainty that negatively affects investment by businesses in electronic invoicing solutions.

6.1.1 Directive 2001/115/EC amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax (Directive 2001/115/EC)

Directive 77/388/EEC, the so-called 6th VAT Directive, aimed at bringing greater VAT harmonisation between Member States. The Directive has, partly due to the complexity of its subject matter, been amended a number of times since.

The rules on invoicing were, however, not harmonised and thus left open for separate regulation by each of the Member States. As a consequence, different national rules emerged.

In 1999, the European Commission recognised the need for a standardization of VAT rules governing invoicing including the cross-border transmission of electronic invoices within the EU. As a result, Directive 2001/115/EC amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax

[111] An Italian study conducted by Bruno Dei – Pier Roberto Sorignani, *Fatturazione e archiviazione elettronica* ("*Invoicing and electronic storage*") IPSOA 2004 (p. 20) on the benefits of electronic invoicing demonstrates that savings using electronic invoices is an average of 27.00 € per invoice.

('the e-Invoicing Directive') was adopted. This Directive simplifies the required content of a tax invoice and removes barriers for electronic transmission and electronic storage of invoices across the EU. Member States were required to implement the Directive by 1 January 2004. From this date onwards, invoices sent by electronic means shall be accepted as legal VAT documents by all EU Member States, provided that the authenticity of the origin and integrity of the contents are guaranteed by means of an advanced electronic signature or electronic data interchange (EDI). Member States can also accept other electronic means.

6.1.2 Implementation of Directive 2001/115/EC

Directive 2001/115/EC has been implemented by all 25 Member States.

Various types of legislation have been used by the Member States but the majority have implemented the Directive by amendments to their existing value added tax (VAT) legislation or by issuing new secondary legislation (regulations/administrative orders) authorised by the national VAT legislation. A few Member States have, however, implemented the Directive in several different laws[112].

However, the implementation by Member States through national legislation has, to some extent, not been consistent with the Directive, and the Commission has started infringement proceedings against several Member States. This primarily concerns the contents of the VAT invoice. An example could be the case[113] of the United Kingdom failure to fulfil its obligations under the Directive. It was held that according to the VAT (Input Tax) (Person Supplied) Order 1991 ('the Order'), a taxable person is granted the right to deduct VAT in respect of supplies of road fuel to a non-taxable person, where the taxable person reimburses to the latter the cost of the fuel. Although the language of the Order is general, it appears that the right of deduction is granted to employers in respect of purchases of road fuel by their employees.[114]

The Commission observed that the provisions of the Order are incompatible with Art. 17(2)(a) of the Sixth VAT Directive in as much as they enabled a taxable person (the employer) to deduct VAT in respect of fuel supplied to non-taxable persons (employees) in conditions that did not guarantee that the VAT deducted related solely to fuel used for business purposes. Finally, the deduction is granted in the absence of any VAT invoice, contrary to Art. 18(1)(a) of the Sixth VAT Directive.[115]

Another point of interest in relation to the implementation of the Directive is the fact that a national system on electronic invoicing was already in place in the Netherlands prior to the implementation of the Directive. The requirement of a prior permit, which was laid down in a national regulation of 1997, had already been abolished in that Member State.

---

[112] Sweden has, for instance, implemented the Directive in the national laws on Value Added tax (SFS 1994:200), the Tax Paying Act (1997:483) and the Accounting Act (1997:483).

[113] The Commission of the European Communities v. United Kingdom (Case C-33/03), OJ C115,14.05.2005, p.2

[114] http://www.lawreports.co.uk/WLRD/2005/ECJ/ecjmarf0.2.htm

[115] Ibid.

6.1.3 *Legal equivalence to written signature, authenticity and prior acceptance*

The harmonisation of the use of electronic invoices rests on a number of different key provisions, one of the most central being the obligation for the Member States to accept invoices sent by electronic means provided that the authenticity of the origin and integrity of the contents are guaranteed[116]. This key provision has been chosen for the initial assessments of national e-business practices concerning electronic invoicing.

Concerning the legal status of electronic invoicing, the benchmark shows that all Member States have adopted rules granting electronic invoices the same legal status as paper invoices.

The Directive explicitly states that the authenticity of the origin and integrity of the contents shall be considered guaranteed by: 1) an electronic signature within the meaning of Article 2(2) of Directive 1999/93/EC or 2) by means of electronic data interchange (EDI) as defined in Article 2 of Commission Recommendation 1994/820/EC[117]. Member States may, however, ask for the advanced electronic signature to be based on a qualified certificate and created by a secure signature creation device.

The benchmark analysis demonstrates that all Member States accept electronic signatures as proof of origin and authenticity. A number of Member States have, however, required advanced digital signatures to be used including for instance, Italy, Lithuania and Latvia.

Another prerequisite for the use of electronic invoicing is, however, that the invoice is VAT compliant. This means, in practice, that the customer must have accepted the use of the electronic invoice either implicitly or explicitly.

The requirement for an acceptance means that the use of electronic invoices will, normally, be limited to situations where the issuer of the electronic invoice has a longer contractual relationship with the receiver of the electronic invoice (typically B2B relationships) or where the issuer of the electronic invoice knows that the electronic invoice will be accepted by the recipient despite the lack of a longer contractual relationship (typically B2G business, where businesses know that the Government will accept electronic invoices). Similarly, electronic invoices will seldom be used in B2C relationships, as these will typically not be of a long-lasting nature, and will not lead to significant savings for the consumer.

6.1.4 *Reported problems in the field of electronic invoicing including court decisions*

A central problem reported in most Member States is the relatively low up-take of electronic invoices despite the obvious gains in effectiveness and costs.

A key reason behind the low up-take might be the fact that the use of the electronic invoice must be accepted by the recipient. Approximately half of Member States require that the acceptance of the invoice is explicit, whereas the other half only require implicit acceptance.

---

[116] Article 2 (d2) of the Directive

[117] 94/820/EC: Commission Recommendation of 19 October 1994 relating to the legal aspects of electronic data interchange Eur-Lex: 31994H0820

It is clear that the requirement for an acceptance in itself might limit the use of electronic invoices to long-lasting B2B contractual relationships, where both parties gain efficiency from using electronic invoices, and B2G business, where the Government has made a general declaration of its acceptance of electronic invoices. If the seller does not know or trust that the invoice will be accepted, he will probably not risk sending a request for an acceptance of the electronic invoice that is denied and then having to send the paper invoice, making the procedure more burdensome than just sending the paper invoice.

In this sense, the very requirement for acceptance becomes a hindrance for the more widespread use of electronic invoices, as they will typically only be used in situations where both parties have an interest in using the electronic signature.

Some countries have taken various initiatives to boost the use of electronic invoices, the most significant initiative being taken in Denmark, where an executive order has been issued obliging national Danish enterprises[118] which provide services to public institutions to send invoices electronically in OIOXML format.

The mandatory use of electronic invoices in Denmark[119] will, naturally, result in a huge increase in the number of SMEs that use electronic invoices in their transactions with the Government and thereby uses the Government standard for electronic invoices. The fact that the SMEs will become used to dealing with electronic invoices in their commerce with the Government and that they will be used to the Government standard may obviously have the derived effect that the likelihood of a positive accept to a request for use of electronic invoices in the business environment increases, leading again to a more widespread use of electronic invoices in B2B relations.

As such, a strong government support for electronic invoices may kick-start the use of electronic invoices also in B2B relations.

The tables below provide an overview of the various Member State strategies to increase uptake of electronic invoices and common standards for invoices to public institutions.

[118] Foreign enterprises may still send regular paper invoices.

[119] A test panel under the Danish Ministry of Economic and Business Affairs have calculated that the introduction of electronic invoices in B2G commerce in Denmark will result in reduced administrative burdens for SMEs equalling about 97 million DKK (about 13 million EUR) and about 119 million DKK (about 16 million EUR) yearly in postal costs. Further information available at: http://www.virk.dk/virkportal/site/videnogvaerktoej/oekonomi/temaelektroniskfakturering/omefakturering.aspx#ID9 (in Danish)

Table 6.1: Existence of an official government strategy (in writing) for introduction of electronic invoices?

Yes	No	No individual strategy but part of national e-government strategy
Finland	Estonia	Austria
Slovak Republic	Hungary	Czech Republic
	Malta	Cyprus
	Poland	Denmark
		France
		Ireland
		Lithuania
		Luxembourg
		Netherland
		Slovenia
		Spain
		Sweden

Source: Member State survey, 18 Member States participating

The table above demonstrates that most of the Member States have either included the use of electronic invoices as an objective in a national government strategy, but only two Member States have concluded a strategy specifically aiming at electronic invoices.

Table 6.2: Existence of an official, quantitative government objective for introduction of electronic invoices?

Yes	If yes: Target	No	Don't know/ No answer
Denmark	By the end of 2006, at least 40% of all public authorities undertake purchasing in digital form with digital invoicing (2003: 15 percent)	Austria	The Netherlands
Finland	Electronic invoicing should be more than 50 % of all invoicing by 2005.	Czech Republic	Slovenia
France	Locally, in the public sector, within the framework of semi-annual performances, the objective is to make 33 % of the invoices electronically at the end of 2010.	Cyprus	
Ireland	-	Estonia	
		Hungary	
		Lithuania	
		Luxembourg	
		Malta	
		Poland	
		Slovak Republic	
		Spain	
		Sweden	

Source: Member State survey, 18 Member States participating

Some problems have been reported in relation to the text of the Directive itself, namely that because of the lack of clarity in the Directive concerning checking the validity of advanced signatures, there are problems with the execution of electronic invoices. This problem can only be solved at a European level.

The link between the e-signature legislation and the e-invoicing legislation has also given rise to the question of whether the use of electronic signatures for verification and authenticity purposes in electronic invoices means that an electronic invoice may only be signed by a natural person using an electronic signature. This would, of course, be a change to the normal business practices relating to electronic invoices, where invoices are rarely signed by natural persons.

In the Slovak Republic it has, for instance, been reported that it is not entirely clear from the Act on Value Added in conjunction with the Accountancy Act whether the invoice shall be signed or not. In practice, it is very frequent and usual that the invoice is requested by its addressee to be signed. Because of the fact that prior approval of the addressee of the invoice is required if it is to be issued electronically, the practice of electronic invoicing is facing difficulties.

In Sweden, it has been debated whether the Public Procurement Act (SFS 1992:1528) might be considered as preventing the government sector from requiring that suppliers use electronic invoices. Since it is not allowed to discriminate certain suppliers. the question has arisen whether or not suppliers unable to produce electronic invoices should be considered discriminated. However, it has been suggested that since software for electronic invoicing has become affordable and electronic invoicing has become common in certain lines of business, a requirement of electronic invoicing should not be considered as discrimination, not even in relation to smaller enterprises.[120]

6.1.4.1 Specific cross-border issues

The Directive affects all enterprises engaging in cross-border transactions. The harmonisation of VAT rules across the EU will make trading with other Member States much easier from a legal and practical perspective. Enterprises will no longer need to deal with outdated VAT invoice rules, and cross-border exchange of electronic invoices will provide them with significantly more flexibility than previously. Using an electronic system will save time, reduce costs and improve the speed of payment across the EU Member States. Also, if an enterprise chooses an e-invoicing service provider that utilises encryption and digital signatures to protect the transmission and storage of all e-invoice data, its e-invoices will automatically comply with the strictest security regulations.

However, a number of more specific cross-border issues give rise to practical problems for SMEs using electronic invoices across borders.

Firstly, the Directive allows the Member States to use varying degrees of security for electronic invoices[121]. The security requirements range from just guaranteeing the integrity of the invoice (Sweden, Finland) to requirements of qualified electronic signatures (e.g. Germany, Slovakia, Spain). This

[120] The National Post and Telecom Agency's report nr. PTS-ER-2002:3, E-handel och statens instrument för att utveckla förutsättningarna, dated 22 February 2002, p. 27.

[121] As explained above under section 6.1.3

means that cross-border use of electronic invoices might be hindered by different requirements for security in the Member States. This would, of course, be especially true for cross-border use of electronic signatures going from a Member State with a low security level to a Member State with a high security level.

However, also the different underlying technologies for electronic signatures may cause a hindrance for cross-border use of electronic invoices[122]. Indeed, the establishment of any *national* common standard may in some cases limit cross-border trade as a consequence of the different standards and technical solutions in the Member States.

Secondly, the problem of the likelihood of an acceptance of electronic signature seems to be a very genuine problem in relation to cross-border use of electronic invoices, as it seems reasonable to assume that foreign consumers or SMEs will be (even more) hesitant to accept a cross-border electronic invoice than a regular national electronic invoice.

6.1.4.2 Summary of main issues

Despite the quite significant savings attached to the use of electronic invoices, usage levels remain low meaning that SMEs do not reap the full economic benefits of electronic invoices. Clearly, government strategies and, in particular, general government acceptance of electronic invoices are useful tools to increase the general usage of electronic invoices.

On the more practical level, the main problems seem to be the different standards for security of the electronic invoice and different underlying technologies making the use of electronic signatures difficult for SMEs in particular in cross-border trade.

6.2 Payment[123]

Payment is an essential element of commerce, as the vendors' delivery of the purchased service or good to the buyer is made on the condition that the agreed sales sum is paid, and the payment is, in turn, a precondition for the delivery of the purchased good or service.

Payments in on-line transactions are often (practically always) made through electronic means (various payment systems), as the very purpose of the on-line transaction typically is to allow the vendor and the purchaser to form (electronic) agreements without the need for a physical presence of the parties.

The most important method of online payment in the EU are credit cards. A 2003 study of European websites found that 78% of websites in the sample studied accept classic credit cards, 51% direct debit and 9% e-banking.[124]

---

[122] The particular issues concerning cross-border use of electronic signatures are examined under section 4.6 above.

[123] The Institute for Prospective Technological Studies (part of the European Commission's Directorate General Joint Research Centre) has set up an Electronic Payment Systems Observatory (ePSO) http://epso.jrc.es/.

[124] OECD, Directorate for Science, Technology and Industry 18 April 2006 (DSTI/ICCP/IE(2004)18/FINAL) with further references

However, other payment methods are also in use such as mediating services, mobile payment systems and electronic currency which may be appropriate for different transactions. However, with the exception of the mediating service PayPal[125], the majority of alternative online payment means have not yet gained the necessary wide user base of both merchants and consumers[126].

The focus of the benchmark of payment is, similarly, focused on payment by credit card.

There is a significant difference between the characteristics and problems concerning payment with credit cards in B2B and B2C transactions. In B2B transactions, the main issue is how to optimize procurement practices and, especially, catalogue management, but little focus is typically given to the actual payment.

Electronic commerce in B2C relations is very much dependent on the use of payment cards (credit cards). This is true both for national B2C commerce and for cross-border commerce. Naturally, consumers' trust in the online payment systems using or relying on payment cards is of paramount importance for the consumers' trust in the online transaction and thereby for the development of B2C electronic commerce.

The aim of EU legislation in the field of distance selling is to put consumers who purchase goods or services through distance communication means in a similar position to consumers who buy goods or services in shops. A first step in the area of payment was the Commission Recommendation of 17 November 1988 concerning payment systems, and in particular the relationship between cardholder and card issuer (88/590/EEC)[127].

Directive 97/7/EC marked a significant step forward in the protection of consumers, as it provides the consumers with a fundamental legal protection from fraudulent use of payment cards.

Some types of contracts are excluded from all the provisions of the Directive. The exemptions include contracts for financial services and contracts concluded through an auction. Contracts for financial services are covered by the Directive 2002/65/EC on Distance Marketing of Financial Services.

6.2.1 Implementation of Directives 97/7/EC and 2002/65/EC

Directives 97/7/EC and 2002/65/EC (The Distance Selling Directives) have been implemented by all Member States.

The preferred method of implementing the Directives by Member States varies for each of the two Directives.

Directive 97/7/EC has mainly been implemented in the national laws of the Member States by means of amendments in the existing consumer legisla-

[125] http://www.paypal.com/, a subsidiary of eBay.

[126] OECD, Directorate for Science, Technology and Industry 18 April 2006 (DSTI/ICCP/IE(2004)18/FINAL) p. 12

[127] The legal framework on payment is in a rapid development. Currently, a possible new legal framework for the single payment area in the Internal Market is being considered (MARKT/208/2001 - Rev. 1)

tion, whereas Directive 2002/65/EC on the other hand has been implemented mainly through the introduction of new legislation.

6.2.1.1 Problems in the implementation of Directives 97/7/EC and 2002/65/EC

Most Member States seem to have implemented the Directives correctly, and only a few problems have been reported concerning the implementation.

Some problems have, however, been reported in some Member States:

Luxembourg has, as yet, not implemented Directive 2002/65/EC. Also, minor deficiencies in the implementation of the Directives may be found in the national legislation of some Member States.[128]

6.2.2 Consumer protection in case of fraudulent use of payment cards

Many of the consumer rights granted by the Directive are of instrumental importance for the consumers' trust in electronic commerce. The question of whether national law allows the consumer to request cancellation of payments and reimbursement of amounts paid in the event of misuse of the payment card, has, however, been chosen for the initial assessments of national e-business practices as being a key safeguard for consumer trust in on-ine purchases.

All Member States have legislation granting the consumer a right to be refunded sums paid or have them returned in the event of fraudulent use of the payment card of the consumer. However, the legislation issued in some Member States seems to differ from Art. 8 of Directive 1997/7/EC, as only the damage occurring after the moment the consumer gives notification of the fraudulent use is borne by the credit institution.

A key problem of interest is the question of whether the protection offered to consumers against fraudulent use of credit cards may be extended to SMEs, in particular when they are acting outside the scope of their normal business (the small real estate agent buying office supplies, for instance).

In most Member States, the protection against fraudulent use of credit cards seems limited to consumers, but some Member States have extended the protection to cover both B2B and B2C transactions. In Denmark, for instance, all card users are covered by the same rules as 'users' of credit cards. In Austria, the protection against fraudulent use applies to B2B contracts, but on a non-mandatory basis.

Differences in the rules concerning the scope of the protection against fraudulent use of credit cards might have rather severe effects on cross-border electronic commerce. As described in section 6.1 above, much of the electronic commerce in the European Union relies on the use of credit cards meaning in turn that fear of liability for misuse of credit cards might cause SMEs to abstain from purchasing goods or services through electronic commerce.

[128] An example being Article 8 of Directive 97/7/EC that seems incorrectly implemented in Estonia.

6.2.3 *Regulation (EC) 2560/2001 of the European Parliament and of the Council of 19.12.2001 on cross-border payments in euro*

Regulation (EC) 2560/2001 of the European Parliament and of the Council of 19.12.2001 on cross-border payments in Euro essentially obliges banks and other electronic payment service providers to align fees for cross-border electronic transactions in euro to the levels of national fees within a Member State, provided the IBAN and BIC codes are used when ordering the payment.

This obligation affects cross-border cash withdrawals, card payments and other electronic payment transactions and cross-border credit transfers, up to a maximum amount of €50,000. It also applies to innovative e-payment services facilitating cross-border funds transfers in euro within the EU.

Further, the Regulation sets out a redress mechanism for those with a complaint against a payment service provider.

Regulation (EC) 2560/2001 is currently applicable not only in the 12 Member States having the euro as currency, but also in Sweden[129] following the decision of the Swedish Authorities to extend the Regulation's application to the Swedish krona[130].

The awareness of the Regulation among businesses is very much affected by whether the business operates in a Member State where the Regulation is applicable or not. In the UK, for instance, it is considered "unlikely that a significant number of enterprises are aware of the provisions of this Regulation"[131].

In the Eurozone, awareness of the Regulation seems to be higher, and particular information campaigns have been initiated in for instance Greece, where the the Greek banks that are active in electronic payments have published a number of guidelines and information brochures with the aim to make Greek businesses aware of the advantages in cross-border electronic payments brought by Regulation 2560/2001. For instance, the Association of Hellenic Banks has recently published a guide on the advantages of the IBAN and BIC codes[132]. Austria, Belgium, Italy and Netherlands are other Member States where it appears that enterprises are aware of and find useful the possibility to effect cross-border payments with the same charges as domestic payments.

---

129 http://ec.europa.eu/internal_market/payments/docs/reg-2001-2560/reg-2001-2560-article9_en.pdf

130 Communication from the Commission pursuant to Article 9 of Regulation (EC) No 2560/2001 of the European Parliament and of the Council, OJEC C 165, of 11/07/2002, p.36–36; Eur-Lex: 52002XC0711(03) http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:52002XC0711(03):EN:HTML

131 Cf. the UK Country Report prepared for this study.

132 The document can be downloaded in Greek (only) from the website of the Association at: http://www.hba.gr/iban.pdf.

6.2.4 *Commission Decisions relating to proceedings under Article 81 concerning VISA*[133]

As explained under section 6.2 above, the majority of cross-border payments relating to electronic commerce are done by the payment cards, the bulk of which are payments in the VISA system.

The Commission has examined the compatibility of the VISA rules with Article 81 of the Treaty. After long discussions with Visa and consultation of interested parties, a package of reforms was submitted by Visa to the Commission, which enables it to grant an exemption under Article 81(3) of the EU treaty[134]. The package consists of the following:

First, Visa will reduce the level of its multilateral interchange fee (MIF) for the different types of consumer cards. As concerns Visa's deferred debit card and credit card payments, the weighted average MIF rate will be brought down in stages, to a level of 0.7% in 2007. For debit card transactions Visa will introduce immediately a flat-rate MIF of €0.28.

Secondly, the MIF will be capped at the level of costs for certain specific services provided by issuing banks, which in the Commission's view correspond to services provided by cardholders' banks which benefit those retailers who ultimately pay the cross-border MIF. These services are: transaction processing, payment guarantee and free funding period(3). These will be determined by a cost study, to be carried out by Visa and audited by an independent accountant. This ceiling will apply regardless of the reductions in the level of the MIF offered by Visa (that is, if the cost cap is below 0.7%, then the MIF will have to be below 0.7%).

Furthermore, Visa will allow member banks to reveal information about the MIF levels and the relative percentage of the three cost categories (currently considered business secrets) to retailers at their request. Retailers are to be informed of this possibility.

The exemption decision only applies to cross-border payment transactions with Visa consumer cards (credit cards, deferred debit cards and debit cards) at retailer outlets within the European Economic Area, which represent about 10% of all Visa card transactions in the EEA.

The decision does not apply to MIFs for domestic Visa payments within Member States, nor to MIFs for corporate Visa cards (that is, cards used by employees for business expenditure). An assessment of MIFs for domestic payments, or in different payment systems than Visa, would have to be made in the light of the different market conditions applicable to such cases. In particular, the question of what constitutes a reasonable and equitable MIF might be answered differently in different circumstances.

---

133 http://ec.europa.eu/comm/competition/antitrust/cases/index/by_nr_58.html
http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/02/1138&format=HTML&aged=1&language=EN&guiLanguage=en
http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/04/616&format=HTML&aged=0&language=EN&guiLanguage=fr
http://www.mastercard.com/us/company/en/corporate/mif_information.html

134 http://europa.eu/rapid/pressReleasesAction.do?reference=IP/02/1138&format=HTML&aged=0&language=EN&guiLanguage=en

Some national competition authorities have reviewed the VISA rules for domestic transactions that are exempted from the Commission Decision. Spain can be mentioned as an example.[135]

6.2.5 *Reported problems in the field of payment including court decisions*

In relation to the rules in focus of this study[136], it might be noted that cases concerning fraud with credit cards, codes, etc. are rather abundant: however, due to the clear compensation rules contained in Directive 97/7/EC, the compensations are normally done outside the court system.

A number of special cases concerning more specific issues relating to Directive 97/7/EC are listed below:

In Austria, the Supreme Court has ruled in a question of whether the risk of fraudulent use of a payment card may be transferred by the standard terms of the financial institution. The Supreme Court held that a clause in standard terms transferring the risk of fraudulent use of a credit card to the card holder enterprise is not *per se contra bonos mores*. In particular, if the card holder enterprise may choose between different options regarding liability for fraudulent use (and chooses a cheaper option where the card issuer's liability for fraudulent use is excluded), no excessive misbalance of contractual obligation rules the contract[137].

Despite the insertion of these provisions in the Austrian Act on Consumer Protection, they also apply to B2B contracts. However, the provision is only mandatory for B2C contracts and, hence, may be amended in B2B contracts. Despite the possibility to amend the application of sec. 31a of the Austrian Act on Consumer Protection, clauses in B2B contracts transferring the risk of fraudulent use to the cardholder may still be null and void as provisions *contra bonos mores*.

Even though a great number of Member States (such as Denmark, Finland and France) give cardholders full compensation for their loss caused by fraudulent use, some countries have different requirements in order to give their consumers the same kind of treatment. Some examples are inserted below:

In Hungary, the holder of the electronic payment instrument is obliged to notify the issuer of the electronic payment instrument after becoming aware i) of the loss or theft of the electronic payment instrument ii) of the loss or theft of his/her personal identification number or access code iii) of the recording of any unauthorized transactions. The holder is responsible for all the damage that has occurred before this notification. This is unfavourable to the consumer who may not be aware of the fraudulent use immediately, and therefore may suffer a heavy loss.

In Slovenia, the consumer has the right to cancel a fraudulent payment if the payment transaction has not yet been performed. The cancellation of payment should be requested from the company/subject registered for performance of such transaction. In case the payment transaction has already

135 http://www.tdcompetencia.es/html/memorias/38der.htm (Expte. A 291/01, Tasas Intercambio VISA) de 11 de abril de 2002

136 As described under section 6.4 above, a new framework for the single payment market is being developed.

137 CASE Ob54/04W

been performed and the payment or credit card was fraudulently used, the consumer has the right to demand the company/subject to which the payment was transferred, to return the paid amounts.

This approach complicates consumers' opportunity to receive their loss back, since they have to demand it from a third party who is not interested in losing money.

In Spain, the rules of refund and cancellation demand that the cardholder acts immediately. These provisions are aimed at combating fraud and so if it later transpires that the cardholder did indeed make the payment and that cancellation had been improperly requested, the customer will be liable to cover any loss to the vendor arising as a result.

The main problems in the area of payment are, however

- the types of payments that are not covered by the compensation rules of Directive 97/7/EC[138], for instance payments by PC banking or credit card payments in B2B relationships.
- The scepticism of consumers towards Internet payments

It seems very clear that differences in the rules concerning the scope of the protection against fraudulent use of credit cards might have rather severe effects on cross-border electronic commerce. As described in section 6.1 above, much of the electronic commerce in the European Union relies on the use of credit cards meaning in turn that fear of liability for misuse of credit cards might cause enterprises to abstain from purchasing goods or services through electronic commerce.

6.2.6 Specific cross-border problems

The general cross-border problems seem to be the costs of payments in transactions in other currencies and the trust the consumers put in vendors of other countries. Trustmark schemes etc. are more or less national and allow the consumer to distinguish whether the vendors meet the national requirements, but only in the jurisdiction of the consumer.

In addition, a number of national schemes grant the consumer a protection going further than the protection offered by the EC legislation when buying in their own jurisdiction. Here, the joint opinion of the Nordic Consumer Ombudsmen might be mentioned. The opinion expressly states that vendors should only debit an account (credit card) once the good is actually shipped for the consumer and that debit of the account of the consumer prior to the shipment of the good is in contradiction of good market practice. This grants the consumer a high degree of safety in relation to the bankruptcy or other non-performance of the vendor (as well as the possibility of retaining interest rate for the purchase sum until the delivery). When the consumers buys in other jurisdictions, they risk a lower degree of protection and, more disturbingly, that the credit card is debited without the shipment of the good meaning that the consumer will have to start proceedings against the vendor of another country.

[138] See for instance ECB ISSUES PAPER FOR THE ECB CONFERENCE ON 10 NOVEMBER 2004 http://www.ecb.int/pub/pdf/other/epaymentsconference-issues2004en.pdf

To illustrate this point, it could be mentioned that a Dutch study[139] showed that no major practical problems in relation to online payment have been reported. In spite of clear legislative protection, some consumers, however, still feel reluctant to use their payment card online due to fear of misuse. A survey of 381 internet consumers indicated that 25% of those consumers prefer Dutch web stores over foreign web stores.

In Austria, the BIC/IBAN system is well established and is used for private as well as business matters. However, the BIC/IBAN system has still caused significant loss of revenue for cross-border transactions for Austrian banks. Some banks, according to information provided by the Austrian Consumer Protection Association VKI, appear to have used unclear standard forms in the past, and charged cross-border transaction rates for transactions between clients in different Member states as clients used the wrong form.

Another issue relates to currency. Regulation 2560/2001 guaranties equal charging for domestic transfers in euros, but this regulation does not cover transfers made in for example Danish currency. This means that a money transfer in Danish kroner from a Danish bank account to a bank account in another Member State does not benefit from the principle of equal charges for a cross-border transaction and a strictly domestic transaction within the European Union.

In order to avoid these cross-border problems is important that the banks respect certain provisions of the Regulation. For example, it is reported in Luxemburg that a bank publishes on its website costs for cross-border cheques stating that a cheque in EUR issued in Luxembourg is free of charge but that as regards cheques issued abroad, the cost depends on the amount of the transaction. Such a provision infringes on the non-discrimination principle of the Regulation.

6.2.7 Summary of main issues

The use of credit payment cards is a vital factor for e-commerce, and in particular for web-shops selling to consumers. Despite the significant protection offered to consumers using credit cards under the Directive 97/7/EC, trust remains low.

Another significant problem seems to be the lack of a more clear framework governing payments made by business, and in particular SMEs acting as consumers outside their regular business field (for instance in the acquisition of office supplies etc.) The lack of clarity in relation to SME purchases might cause SMEs to abstain from acting as consumers in e-commerce.

6.3 Contract execution

The execution of the contract covers the phase spanning from the actual conclusion of the contract to the proper performance of the contractual duties of the seller in form of the delivery of the purchased good or service and the remedies available to the purchaser in the event of the seller's breach of contractual obligations.

The actual execution of the contract in form of the delivery of the purchased good or service is the key reason for the purchaser to enter into the contract and to pay the purchase price.

[139] www.webwereld.nl/articles/31348.

As described above under section 6.2, the seller and the buyer very rarely meet in electronic transactions, as the transaction will normally be initiated by the buyer through a computer located outside the office of the seller (typically at the home or office of the buyer). The fact that the buyer does not meet the seller (and sees the service or good to be sold) means that the buyer needs to trust the seller to deliver the purchased good or service, or to trust the remedies offered to the buyer for non-performance or non-delivery. In that sense, the trust of the buyer in the delivery of the seller and the available remedies becomes a precondition for e-commerce.

The rules concerning the execution of contracts are largely based on the various national legislations in the field of sale-of-goods with widespread variations in the legislation from Member State to Member State. Furthermore, the exact content of the legislation concerning contract execution typically depends on the legal status of the buyer as either consumer or enterprise. The actual content of the national rules varies quite significantly, meaning in turn that the actual national e-business practices must primarily be found the individual country profiles.

The EU legislation in the field of contract execution is, generally, aimed at the B2C relation giving obligations to the enterprises and minimum rights to the consumers in particular in distance selling contacts, whereas the B2B relation on the other hand is primarily regulated by the contract of the parties and the national sale-of-good Acts[140]

The significant differences between the national sale-of-good Acts give rise to some difficulties in relation to the choice of valid indicators for the benchmark. Obviously, the part of the distance selling rules originating from the Distance selling Directives are and therefore form a valid basis for a benchmark.

The comparisons of the remedies offered to the buyer[141] are, however, often difficult, as specific conditions must usually be met under national law in order to exercise the right. For example, while it would be possible to examine what remedies are available for delivery of faulty or deficient goods, it would still be difficult to compare results, as the assessment of whether the good is faulty or deficient depends on national law and court practice going clearly beyond what can be benchmarked. As the remedies are to some extent comparable, it has, nevertheless, been chosen to compare the available remedies to consumers in relation to late delivery and delivery of goods not in conformity with the contract.

6.3.1 Distance selling contracts

The aim of EU legislation[142] in the field of distance selling is to put consumers who purchase goods or services through distance communication means in a similar position to consumers who buy goods or services in shops, but the rules concerning consumer protection in relation to the contract execution are in essence based on the national sale-of-goods Acts. The Community legislation in the contract execution phase is primarily founded on the so-called Distance selling Directives (Directive Directives 97/7/EC and

[140] In cross-border commerce the relevant sale-of-good Act (or similar national provisions) will be chosen under the choice-of-law rules examined above under section 5.7.2

[141] The choice of law rules will often imply that consumers are entitled to using the remedies offered under the national law, see section 5.7.2 above

[142] Other international Organisation

2002/65/EC). The Distance selling Directives are in most areas a welcome supplement introducing minimum standards and rights for the consumers, but many Member States have introduced rights going beyond those of the Community Legislation (examples can be found in table 6.4 below covering the Withdrawal period under article 6 of Directive 1997/7).

6.3.1.1 Implementation of Directives 97/7/EC and 2002/65/EC[143]

Most Member States seem to have implemented the Directives correctly, and only a few problems have been reported concerning the implementation.

Some problems have, however, been reported in some Member States:

Luxembourg has, as yet, not implemented Directive 2002/65/EC. Also, minor deficiencies in the implementation of the Directives may be found in the national legislation by some Member States.

6.3.1.2 Consumer withdrawal rights under Directive 97/7/EC and 2002/65/EC[144]

Even the rules implementing the withdrawal rights under Article 7 of Directive 97/7/EC (the Distance Selling Directive) vary quite significantly.

The Member States may roughly be divided into two different groups; one increasing the withdrawal period to 14 days and the other applying the 7 days of the Directive, but with an increase in the withdrawal period if the seller has failed to provide the consumer with the relevant information[145]. Some Member States distinguish between calendar days and working days. A few Member States use 8-10 days withdrawal periods.

The tables on the following pages demonstrate the various withdrawal principles offered in the Member States under the Distance Selling Directives.

[143] See also section 6.4.1 above.
[144] See also MEMO/06/339 from http://ec.europa.eu/consumers/cons_int/safe_shop/dist_sell/index_en.htm
[145] See section 5.4 above

Table 6.3 Withdrawal periods (cooling-off-periods) under Directive 97/7/EC

Member State	Withdrawal period under article 6 of Directive 1997/7/EC
Austria	7 working days. Extended to 30 days if service provider fails to fulfil his information obligations
Belgium	7 working days. In case the consumer was not properly informed about his right of withdrawal, this term is extended to three months
Cyprus	14 days
Czech Republic	14 days, and 3 months if seller has not performed his information obligations.
Denmark	14 days
Estonia	14 days
Finland	14 days, and 3 months if seller has not performed his information obligations.
France	7 working days
Germany	14 days
Greece	10 working days
Hungary	8 working days, and 3 months if seller has not performed his information obligations.
Ireland	7 working days and 3 months if seller has not performed his information obligations.
Italy	10 days, and 90 days if seller has not performed his information obligations.
Latvia	14 calendar days
Lithuania	14 calendar days
Luxembourg	7 working days and 3 months if seller has not performed his information obligations.
Malta	
Netherlands	7 working days
Poland	10 days, and 3 months if seller has not performed his information obligations.
Portugal	14 days
Slovak Republic	7 Working days as of delivery of a product or conclusion on condition that the seller fulfilled its information obligations according to this act. In case that the information obligations of the seller were fulfilled later on, right to withdraw may be exercised within seven business days as of fulfilment of these obligations. In any case, the consumer shall have a right to withdraw only within three months as of the delivery of goods or services at the latest.
Slovenia	15 days
Spain	Seven working days
Sweden	14 days
United Kingdom	7 working days, and 7 working days plus 3 months if seller has not performed his information duties.

Table 6.4 Withdrawal periods (cooling-off-periods) under Directive 2002/65/EC

Member State	Withdrawal period under article 6 of Directive 2002/65/EC
Austria	14 days starting from the time of contract conclusion or (if later) the day of reception of contractual terms nad conditions or any information that has to be provided prior to the conclusion of a distance contract.
Belgium	14 days running from the signature date
Cyprus	14 days
Czech Republic	14 days, except life insurance which is 30 days
Denmark	14 days
Estonia	15 days, and 30 days regarding life- and pension insurances
Finland	14 days
France	(?)
Germany	15 days, and 30 days regarding pension funds for single persons
Greece	14 Days
Hungary	14 days, and 30 days in case of insurance
Ireland	14 days, and 30 days in case of pensions plans or life insurance
Italy	14 days, and 30 days in case of pensions plans or life insurance
Latvia	14 calendar days
Lithuania	14 days, and 30 days in case of pensions plans or life insurance
Luxembourg*	The Directive is not yet implemented, but never the less a 30 day period is offered in case of pensions plans or life insurance
Malta	
Netherlands	14 calendar days
Poland	14 days, and 30 days in case of pensions plans or life insurance
Portugal	14 days, and 30 days in case of pensions plans or life insurance
Slovak Republic	14 days, and 30 days in case of pensions plans or life insurance
Slovenia	7 days, and 30 days in case of pensions plans or life insurance
Spain	7 working days
Sweden	14 days, and 30 days in case of pensions plans or life insurance
United Kingdom	14 days, and 30 days in case of pensions plans or life insurance

The tables above demonstrate the quite significant differences between the Member States as to the conditions under which given consumer rights may be used. These inherent differences are, naturally, more significant in relation to the conditions under which other consumer rights may be exercised under national law.

6.3.2 Remedies available to the consumers in national law

It clear that the rights offered to the consumers vary from Member State to Member State, and that it would be a huge task for a consumer to understand more than their own legal system. This means, in turn, that if the consumer buys services or goods from other Member States the question of the consumers' subjective trust in the rules of the legal system of the other Member State becomes relevant[146].

[146] These questions are naturally linked to the choice-of-law and forum selection issues described above.

According to the empirical evidence, in very general terms the consumers of the Internal Market indeed seem to believe that their own protection systems are better than those of their neighbours. Of the respondents in the Consumers Survey 31.5% thought that their consumer rights would be well or very well protected in a dispute with a seller or manufacturer in another Member State, whilst 55.6% thought the same about a dispute in their own country.[147]

6.3.2.1 Delivery of a good not in conformity with the contract

The rules governing the actual assessment of the conformity of the delivered good with the contract vary from Member State to Member State. Generally however, goods are not in conformity with the contract inter alia if they do not comply with the description and possess the qualities; if they do not show the quality and performance which are normal in goods of the same type; if they are not fit for any particular purpose for which the consumer requires them and which he made known to the seller at the time of conclusion of the contract; or if they are not fit for the purposes for which goods of the same type are normally used.

Typical remedies offered for lack of conformity are the right to timely and proper reparation for free, that the seller shall be obliged to eliminate the defect without undue delay, or that the consumer may request its exchange for a new one unless the producer will incur unreasonable costs compared to the price of the product or seriousness of the defect. The consumer is also entitled to ask for a reduction of the price due from the defect as to claim damages and compensation for his/her loss.

In addition to that, the consumer can rescind the contract or withdraw from the purchase contract (in such a case, the purchase contract is deemed to never have existed).

The differences between the national rules might be seen in the different deadlines for consumers notification of the lack of conformity used in each Member State.

For example, Denmark and Finland maintain the 2 year deadline for consumer rights, whereas in Italy, Spain and Sweden, the deadlines may be extended to 26 months and 3 years respectively in specific circumstances (for instance hidden faults).

[147] *The Rise of European Consumer Law — Whither National Consume Law? http://www.austlii.edu.au/au/journals/SydLRev/2006/4.html#fn38*

Table 6.5 Delivery of a good not in conformity with the contract, remedies to consumers

	Repair or replace the defective good	Reduction of the purchase price	Compensation	Withdraw from the contract	Limitation period
Austria	Yes	Yes	-	Yes*	-
Belgium	Yes	Yes	-	Yes**	2 years
Cyprus	Yes	-	Yes	-	-
Czech Republic	Yes	Yes	-	Yes	-
Denmark	Yes	Yes		Yes	2 years
Estonia	Yes	Yes	-	Yes	2 years
Finland	Yes	Yes	-	Yes	-
France	Yes	Yes	-	Yes	2 years
Germany	Yes	Yes	Yes	Yes***	-
Greece	-	-	-	-	-
Hungary	Yes	Yes	Yes	Yes	2-3 years
Ireland	Yes	Yes	-	Yes*	6 months
Italy	Yes	Yes	-	Yes	26 months
Latvia	Yes	Yes	-	Yes	2 years
Lithuania	Yes	Yes	Yes	Yes	2 months
Luxembourg	Yes	-	-	-	-
Malta	Yes	Yes	-	Yes	2 years
Netherland	Yes	Yes	-	Yes	2 years
Poland	Yes	-	-	****	6 months
Portugal	Yes	Yes	-	Yes	2-5 years
Slovak Republic	Yes	Yes	-	Yes	-
Slovenia	Yes	Yes	Yes	Yes ***	2 years **** 6 months/contract terms ** (for hidden defects)
Spain	Yes	Yes	Yes	Yes	3 years
Sweden	Yes	Yes	Yes	Yes***	36 months
United Kingdom	Yes	Yes	-	Yes	2 years

* The right to rescind the contract, however, does not exist in case of minor lacks of conformity.
** Claims based on hidden defects should be made within a short timeframe.
*** The right to refrain from the contract demands that the buyer has given the seller the possibility to correct his mistake within a certain amount of time.
**** The consumer can not withdraw if he did not notify the seller about stating non-compliance with the contract within 2 months.

6.3.2.2 Late delivery

The available remedies for non-performance in B2C relationships are, in essence, based on the same principles in all the Member States.

The consumer can, as a general principle, demand specific performance, which requires that the buyer receives the product exactly as specified in the contract.

The table below provides an overview of how the question of significant (qualified) late delivery is handled in the Member States. In essence, the use of the specific rights of the consumer is, normally, attached to a number of specific conditions going beyond what can be coverd by the table. The table should therefore only be seen as an indicative overview of consumer rights in the case of significant (qualified) late delivery.

Table 6.6: Significant late delivery (or non-performance) remedies to consumers

	Reduction of the purchase price	Claim money back	Compensa-tion	Delay payment	Withdraw from the contract
Austria	-	Yes	-	-	-
Belgium	-	-	Yes	Yes	Yes
Cyprus	-	Yes	-	-	-
Czech Republic	-	-	-	-	Yes
Denmark	-	-	Yes	-	Yes
Estonia	Yes	Yes	Yes	Yes	Yes
Finland	-	-	Yes	Yes	Yes
France	-	Yes	Yes	-	Yes
Germany	-	-	Yes	-	Yes
Greece	Yes	-	-	-	-
Hungary	-	Yes	Yes	-	Yes
Ireland	-	Yes	-	-	Yes
Italy	Yes	-	Yes	-	Yes
Latvia	-	Yes	-	-	Yes
Lithuania	-	Yes	-	-	Yes
Luxembourg	-	Yes	-	-	Yes
Malta	-	-	-	-	Yes
Netherlands	-	Yes	-	-	Yes
Poland	-	-	Yes	Yes	Yes
Portugal	-	-	-	-	Yes
Slovak Republic	-	-	Yes	-	Yes
Slovenia	Yes	Yes*	Yes	-	Yes
Spain	-	Yes	Yes	-	Yes
Sweden	No	No	Yes	Yes	Yes
United Kingdom	-	Yes	Yes	-	Yes

An example of the quite significant differences in the national conditions to exercise the right to termination may be seen when comparing the rules of termination of Denmark and Hungary with those of Sweden. In Denmark and Hungary, the consumer may only terminate the contract if the breach is material, whereas the Swedish consumer may terminate the contract in the case of delay, even if the delay is not material.

On a more detailed level some Member States offer the consumer rights of a more specialised nature. This is the case, for instance, in Estonia, Greece

and Italy, were the consumers are granted a price reduction if the seller does not deliver on time[148].

Several countries such as Estonia, Hungary, Ireland and Luxemburg maintain that consumers should get their payment back after 30 days from the contract, if they have not received their products.

6.3.3 Reported problems in the field of contract execution

The main problem in the field of contract execution is the lack of trust consumers put in the various legislative systems, as the payment rules described above under section 6.4 often grants the consumer quite good fundamental rights.

This is especially true in the Nordic Countries, where the joint opinion of the Nordic Consumer Ombudsmen might be mentioned. The opinion expressly states that vendors should only debit an account (credit card) once the good is actually shipped to the consumer and that debit of the account of the consumer prior to the shipment of the good is in contradiction of good market practice. This grants the consumer a high degree of safety in relation to the bankruptcy or other non-performance of the vendor.

6.3.4 Specific cross-border problems

It may be concluded from the above that on a general level, the basic (core) of the contract execution legislation in the Member States rest on the same common principles (for instance the right to termination in case of non-performance). However, a more thorough comparison of the legislation of the Member States demonstrates clearly that there are many important and significant differences in the legislations of the Member States. These differences are to some extent demonstrated rather clearly by the fact that significant differences may be seen in areas harmonised under Community Directives.

On the practical level, some of the problems relating to the differences between the contract execution rules of the Member States may be solved under the choice-of-law and forum rules described above under section 5.7.2, but the barrier of different legislation in the field of contract execution is still very significant.

It might be noted that consumers can approach the contact points of the consumer Europe[149] network in their countries, but these are to some extent inadequate and ineffective, as consumer awareness is low or lacking.

6.3.5 Summary of main issues

The contract execution rules vary quite significantly from Member State to Member State. Significant differences seem to exist even in areas were the European Union has introduced minimum requirements, for instance in relation to the withdrawal period in distance sale contracts. However, the differ-

[148] As an example of a consumer right of a more special nature, it might be mentioned that non-delivery might result in fines in Estonia

149 The European Consumer Centres Network (ECC-Net)
ec.europa.eu/consumers/redress/ecc_network/index_en.htm

ences seem to be even more significant outside areas influenced by Community legislation.

Surprisingly, a study has shown that consumers are well aware that the barriers relating to different legislation might in some cases widen the rights of the consumers and that consumers of some Member States actually tend to trust the legislation of other Member States over that of their own Member State. Still, the majority of consumers in the Community seem to trust the legislation of their own Member State over that of other Member States.

7. General assessment of the national legal and administrative e-business practices

This chapter presents the main conclusions of the study. First, we summarize the conclusions of the preceding chapters regarding the current status of legal and administrative practices in the three main fields of e-signatures, electronic contract conclusion and e-invoicing.

This is followed by a discussion of a number of themes cutting across these three areas, namely the main legal and administrative barriers to e-business in the European Union, and the issue of awareness about national authorities in charge of solving legal problems in e-business. Finally, a number of national and European good practices (legal, administrative, information, and infrastructure initiatives) are presented.

7.1 The current status – conclusions

As mentioned above, this section summarizes the conclusions of the three preceding chapters on e-signatures, electronic contract conclusions, and e-invoicing, respectively.

7.1.1 E-signatures

All Member States have implemented the e-Signatures Directive and the basic features of electronic signatures are well transposed into national legislation. Qualified electronic signatures are accepted by all Member States as legally equivalent to handwritten signatures and electronic signatures are admissible as evidence in legal proceedings. The basic legal foundation for use of electronic signatures by businesses is therefore present. For businesses to increase their use of electronic signatures it is, however, important that Member States remove formal hindrances in national legislation in relation to use of electronic means, such as, e.g. requirements for a written signature in two copies on a specific form.

In addition, there is some uncertainty in the interpretation of the Directive. This uncertainty encompasses both the legislative level in the Member States and the users of electronic signatures. Thus, initiatives aimed at creating a consistent interpretation of the Directive on a community level would be useful to support the overall use of electronic signatures.

E-government services appear to be the main driver for electronic signatures, making the public sector a key player in facilitating and encouraging the use of electronic signatures. Interaction in the private sector, i.e. business and citizens, still provides for very little use of electronic signatures. It is our impression that the private sector, especially SMEs, has still not experienced sufficient need or external demand for adopting electronic signatures when communicating electronically.

In the light of the public sectors' central role in promoting the use of electronic signatures, it is important that government institutions, when providing online services, take initiatives to recognize and support the use of electronic communication in general, and electronic signatures in particular, as a tool to provide effective and secure communication not only in business-to-

government situations but also when providing the framework for business-to-business and business-to-consumer relations.

Overall, the use of electronic signatures in the Member States is still very limited. This applies especially to the use by enterprises and consumers of electronic signatures based on qualified certificates, which is even more limited. Seen from a business perspective, the important issue is to make rational use of new technologies when this supports the activities of the enterprise. The currently demanded services in the business world do not depend on the use of electronic signatures. This is not to say that electronic signatures will not play a role in business relations, but the incentive for investing in and adopting electronic signature technology has to be present.

The court cases illustrate that the use of electronic communication, including electronic signatures, are accepted by courts as evidence and can constitute the basis of binding contracts. In this context, it is interesting to note that the wide acceptance by the courts of 'ordinary' electronic communication as binding evidence to a certain extent minimizes the need for advanced electronic signatures as tools to provide a high degree of security of evidence. The court cases do, however, also show the challenges for the legal systems in addressing the technically difficult issues connected to the use of electronic communication.

Cross-border use of electronic signatures depends on the possibility of a party to technically receive, read and control the other party's electronic signature. Establishment of a well-functioning PKI infrastructure that provides for technical interoperability between various certification service providers is the first condition for cross-border use. Technical interoperability is, however, not sufficient *per se* to support cross-border use (or use between certificate users connected to different certification service providers as such). Commercial interoperability must also be present when establishing a PKI infrastructure with involvement of Certification Service Providers with different business models. An enterprise in one country is not necessarily able to accept an electronic signature from a customer in another country using a certificate from its domestic Certification Service Provider if a clearance agreement has not been agreed between the enterprise and the foreign Certification Service Provider.

The advantage of using electronic signatures based on qualified certificates is the support from the legal framework created by the e-signatures Directive. This advantage depends, however, on a well-functioning Internal Market as underpinned in Article 4. From a legal point of view, the introduction of accreditation schemes pursuant to Article 3 (1) and the possibility of establishing additional requirements in the public sector pursuant to Article 3 (7) seem to be the most critical when using electronic signatures in communication with the public sector. It must be emphasized that such additional requirements in the public sector for receiving electronic signatures must be kept at a minimum to reduce the risk of limiting the free flow and use of electronic signatures.

Community legislative initiatives that support the use of electronic signatures in electronic communication i.a. as seen in the Procurement Directives and the Invoicing Directive[150] will not only increase the use of electronic signa-

[150] Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax. Refer to section 6 for a further review of this Directive .

tures in the Member States but will also contribute to the advancement of cross-border use.

7.1.2 Contract conclusion

Despite the overall approximation of regulation in the Member States due to general Community Law and a series of initiatives aimed at increasing the overall coherence of European contract law, there are still dissimilarities in how legal principles are understood and practiced by the Member States. Ongoing European legal initiatives and international initiatives i.a. in the form of model laws and conventions do, however, function as building blocks for a uniform framework for enterprises doing online business.

There is no uniform definition of whether or not the presentation of goods or services on a website ('display of goods or services in a web shop') is an offer to the customer or only an invitation to the customers to make an offer. In several Member States, online advertising on a website can under certain conditions be regarded as a binding offer.

A correct implementation by the online vendor of the requirements stated in Article 10 (1) (a) of the e-Commerce Directive (information on the different technical steps to follow to conclude the contract) will clarify this issue when the possibility of online conclusion of contracts are provided by the vendor[151].

The uncertainty and lack of transparency in the national legislation may, however, lower the incentive for SMEs and consumers to enter into cross-border trade.

Regulation concerning applicable law and jurisdiction seems to be a legal area difficult to understand for non-experts in this field. This is of course not a surprise, as the regulation in this area for good reasons is fairly complicated. Uncertainty concerning cross-border regulation is considered a specific and significant hindrance especially for SMEs and consumers.

The proposal from the Commission for a Regulation of the European Parliament and the Council on the law applicable to contractual obligations (Rome I) will clarify the present situation with regard to verifying the applicable law to the contract. But this clarity might be viewed as an administrative burden since distance selling will encompass the task of drafting contracts targeted individually to all European Member States. This might, again, be especially burdensome for SMEs.

7.1.3 e-Invoicing, payment, and other matters related to the execution of electronic contracts

Despite the quite significant savings attached to the use of electronic invoices, usage levels remain low meaning that businesses do not reap the full economic benefits of electronic invoices. Clearly, government strategies in this area and, in particular, general government acceptance of electronic invoices are useful tools to increase the general usage of electronic invoices.

On a more practical level, the main problems seem to be the different standards for security of the electronic invoice and different underlying technolo-

[151] Refer to section 5.4 for a review of the information requirements in the e-commerce Directive.

gies, making the use of electronic signatures difficult for SMEs, particularly in cross-border trade.

The use of credit payment cards is a vital factor for e-commerce, and in particular for web-shops selling to consumers. Despite the significant protection offered to consumers using credit cards under the Directive 97/7/EC, trust remains low.

Another significant problem seems to be the lack of a more clear framework governing payments made by businesses, in particular SMEs acting as consumers outside their regular business field (for instance in the acquisition of office supplies etc.) The lack of clarity in relation to SME purchases might cause some SMEs to abstain from acting as consumers in e-commerce.

The contract execution rules vary quite significantly from Member State to Member State. Significant differences seem to exist even in areas were the European Union has introduced minimum requirements, for instance in relation to the withdrawal period in distance sale contracts. However, the difference seems to be even more significant outside areas influenced by Community legislation.

Surprisingly, a study has shown that the consumers are well aware that the barriers relating to different legislation might in some cases widen the rights of the consumers and that consumers of some Member States actually tend to trust the legislation of other Member States over that of their own Member State. Still, the majority of consumers in the Community seem to trust the legislation of their own Member State over that of other Member States.

7.2 Main legal and administrative barriers to e-business in the European Union

As discussed in the previous chapters and summarized above, Member States have on an overall level implemented the relevant Directives and thus have a robust legal framework to support online business. However, in practice, the legal framework and the legal practices do meet challenges when businesses and consumers do e-business.

The country reports show that there is a wide consensus in Member States regarding the existence of legal and administrative barriers. In the following, some of the most important of these barriers are summarised and discussed.

7.2.1 Legal uncertainty

More than half of the Member States report that there is uncertainty as regards the legal binding effect and recognition of electronic documents in national trade relations due to the lack of court decisions.

As stated above, electronic signatures are admissible as evidence in legal proceedings in all 25 Member States. This seems to be based on the general principles on free admission of evidence in courts. However, the general lack of court cases creates uncertainty regarding both the strength of evidence presented in electronic form and among enterprises and administrative bodies on how courts will address these issues.

The lack of court cases and legal precedent is significant in the fields of e-signature, e-invoicing and e-contract conclusion, as there has been no court case from a Supreme Court or High Court on these issues across the Member States. This uncertainty may influence on the interest and willingness of

commercial entities to make investments in technology to promote new business models and services to customers and business partners.

A few countries also report inconsistencies between different regulations, and even insufficient legislation on e-business. For example, the Czech correspondent points to inconsistencies between the Act on Electronic Signature, the Civil Procedure Act, and the Administrative Procedure Act regarding what type of electronic signature shall be used when communicating with public authorities.

7.2.2 Lack of international standards and interoperability

More than half of the country reports point to various barriers to cross-border exchange of electronic signatures, electronic contracts and electronic invoices.

Eight country reports indicate that there is a lack of international standards for electronic signatures. There are, however, widely adopted standards that most certificates to electronic signatures are based on, like ITU-T X.509[152]. The real issue is the lack of 'filled-in' standards, i.e. standards on how to fill in the different fields in a certificate. An example of this is the requirements for qualified certificates stated in Annex I in the e-signature Directive. Litre (i) requires the certificate to contain information about limitations on the scope of use of the certificate, if applicable; and litre (j) provides for information concerning the limits on the value of transactions for which the certificate can be used, if applicable.

There is no generally adopted standard on how to provide this information in the certificates. Should limitations concerning the scope of use be written in prose that could be read and understood by humans (even though the different possibilities of interpretation of the text would be endless[153]) or should it be written in structural text that could be read and interpreted by automatic systems? There is no simple answer to this. But before a uniform standard for this is accepted, there will not be a widespread use of such features in the certificates.

Seen from a cross-border perspective, interoperability between the different electronic signature infrastructures of the Member States also requires a common implementation of standards.

However, technical standards are not the only barrier. Administrative practices are also a significant barrier to cross-border use of electronic signatures, since a number of Member States only provide access to the national electronic signature(s) to citizens and/or companies registered in the country. Of the 18 Member States participating in the survey carried out in connection with this study, 7 do not give access to the electronic signature to enterprises and citizens from other Member States.

The described difficulties of a lack of common and freely usable implementation of existing standards for e-signatures also apply to cross-border use of electronic invoices, where there is a similar need for adoption of filled-in standards and cross-border interoperability.

7.2.3 Lack of trust

Generally, lack of trust in electronic transactions is reported by nine countries. As an example, the Finnish Country Report mentions this as the princi-

[152] http://www.ietf.org/html.charters/pkix-charter.html ; http://en.wikipedia.org/wiki/X.509

[153] The legal interpretation and value of such limitations on use in certificates is moreover unclear.

pal barrier to e-business in Finland. A number of fraud cases have featured prominently in the Finnish media, in particular attempts at 'phishing' internet-banking access codes, and this has made parts of the population, especially more senior people, hesitant towards electronic transactions[154]. Several other countries also report on consumers being reluctant as regards payment via the internet.

Although this issue to some extent falls outside the scope of the country reports, it is well known that the need for effective information security continues to rise. A precondition for a well-functioning market for e-commerce is that business can be done in a safe environment. There are several examples of attempts on fraud that make use of the vulnerabilities of electronic communication via the internet. Well-known fraud techniques are Phishing and Pharming[155].

A phishing attack typically consists of a fraudster using a false (spoofed) e-mail address to request e.g. sensitive information (user name, password, credit card number, etc.) from an unsuspecting recipient who believes that the request comes from e.g. his bank. A phishing attack can be combined with a pharming attack, where the unsuspecting recipient is lead to a counterfeit website that e.g. appears to be the website of the recipient's bank. Through the counterfeit website, the fraudster can eavesdrop on sensitive information such as e-banking passwords.

In order to counter the technical attacks, the Commission has set up the European Network and Information Security Agency (ENISA)[156].

As discussed in section 6.4, electronic commerce in B2C relations is very much dependent on the use of credit cards. This is true both for national B2C commerce and for cross-border commerce. Naturally, consumers' trust in the on-line payment systems using or relying on credit cards is of paramount importance for the consumers' trust in the on-line transaction and thereby for the development of B2C electronic commerce. From a legal point of view, the lack of trust is largely unfounded since Directive 97/7/EC provides consumers with a fundamental legal protection from the fraudulent use of payment cards.

However, the legislative protection of consumers is not always capable of handling online enterprises that do not comply with traditional business norms and regulation. As discussed in Section 5.4, there is a general lack of compliance with legislation among a large share of online shops, and this contributes to uncertainty among consumers.

One of the reasons for the lack of compliance with regulation may be the very low entry level for online business. Compared to opening a traditional brick and mortar business, the barriers for opening an online business providing goods or services online are almost nonexistent. With a very small investment, anyone with a minimum of technical expertise can establish an online business and present themselves to a huge market. Seen exclusively from a free competition and open market point of view, this broad possibility for opening a shop and competing in the market is very positive.

---

[154] It should be noted, however, that e-commerce in Finland, according to the Country Report, is growing steadily.

[155] www.antiphishing.org

[156] http://www.enisa.eu.int/

There is, however, a clear downside, since it also gives a wide opportunity for enterprises lacking in seriousness to enter into business. When a traditional shop in a local community disappoints its customers, this will normally have a direct consequence for the shop's economic performance because customers will tend to spread the message of the business' untrustworthiness by word-of-mouth. Although there are online forums where users can communicate their experiences with on-line shops, the risk is considerably smaller for an online shop that has a huge market with a lot of potential customers that are easy to lure with for example low prices and huge discounts.

However, the widespread lack of compliance among online shops and online auctions is widely regarded to be caused mainly by a *lack of awareness* on the part of the businesses about their obligations as regards e.g. protection of personal data, information to customers on withdrawal rights from distance contracts etc.

Related to this, consumers are often not aware of their rights and, feeling unprotected, this adds to their mistrust. They are also not generally aware of where to turn for help when they experience problems. As is pointed out in the Netherlands Country Report, the European Consumer Centres Network (ECC-Net) is practically unknown among consumers (cf. also section 7.3, below).

7.2.4 Limited protection of SMEs

Notwithstanding a fairly widespread lack of trust among many consumers in electronic transactions, consumers generally enjoy a high degree of protection when doing business online. The same degree of protection does not apply to smaller enterprises. The low level of protection for SMEs is reported in 12 country reports as a problem. In Member States, the general rationale is that B2B transactions are regarded as business between two equal partners. With regard to doing business online, small businesses do feel a legal uncertainty and lack of knowledge that constitutes a barrier.

The UK Country Report refers to a survey carried out by the e-commerce Innovation Centre (eCIC) at Cardiff University that investigated e-commerce adoption and use by Welsh SMEs[157]

The survey shows that small firms benefit less from e-commerce compared to larger firms that can benefit more effectively from the improved communications that e-commerce can provide inside the company. The survey also showed that distinguishing between B2B SMEs and B2C SMEs is relevant and that B2B SMEs have a higher level of benefits achieved than B2C SMEs.

7.2.5 Interpretation of the country of origin principle

Finally, there is no doubt that the country of origin principle as such has a very positive impact on the opportunity and incentive to provide cross-border e-business. It should, however, be noted that the interpretation of the country of origin principle in the e-commerce Directive is reported as a problem by several respondents.

The delimitation between regulation included in the country of origin principle and regulation outside the scope is reported as not clearly identifiable. The lack of understanding of the precise scope of the 'coordinated field' de-

[157] eCIC website: http://www.ecommerce.ac.uk/. The cited report is 'eCommerce in Welsh SMEs: The State of the Nation Report 2002-2003', pp. 45-46, http://www.ecommerce.ac.uk/pdf/StateoftheNation20022003.pdf

fined in Articles 2 (h) and 3 (1) and (2) of the e-commerce Directive seems to create uncertainty among enterprises entering into e-business.

7.3 Awareness among businesses about national authorities in charge of solving legal problems in e-business

Alternative Dispute Resolution (ADR) schemes or out-of-court mechanisms as they are also known have been developed across Europe to help citizens who have a consumer dispute, but have been unable to reach an agreement directly with the trader[158]. ADR schemes usually use a third party such as an arbitrator, mediator or an ombudsman to help the consumer and the trader, reach a solution[159].

The advantage of ADR is that it offers more flexibility than going to court and often the needs of both consumers and professionals are better met by the ADR. Compared to going to court these schemes are cheaper, quicker and more informal, which means they are an attractive means for consumers seeking redress.

However, these out-of-court mechanisms have been developed differently across the European Union. Some are the fruit of public initiatives both at central level (such as the consumer complaints boards in the Scandinavian countries) and at local level (such as the arbitration courts in Spain), or they may spring from private initiatives (such as the mediators/ombudsmen of the banks or insurance companies). Precisely because of this diversity, the status of the decisions adopted by these bodies differs greatly. Some are mere recommendations (such as in the case of the Scandinavian consumer complaints boards and most of the private ombudsmen[160]), others are binding only on the professional (as in the case of most of the bank ombudsmen) and others are binding on both parties (arbitration).

The ADR initiatives are supplemented by the European Consumer Centres Network[161] that consists of Consumer centres in all the Member States. The Consumer Centres give advice and information on consumer rights and help consumers solve problems with goods and services purchased within the EU.

It should be noted that 13 country reports state that the question on awareness about national authorities in charge of solving legal problems in e-business has not been the subject of a particular study. However, the country reports do leave the impression that, in spite of the European and national initiatives on different types of ADR, there are still challenges to be met when communicating the message of different forums for solving legal problems related to e-business.

The existing lack of awareness among businesses in relation to the general legislation is explicitly reported in several country reports. This could also imply a lack of knowledge about national authorities in charge of solving legal problems in e-business.

[158] http://ec.europa.eu/consumers/redress/out_of_court/index_en.htm

[159] COM(2002) 196 The Commission green paper on alternative dispute resolution in civil and commercial law

[160] Information about the Swedish ombudsman: http://www.konsumentverket.se/

[161] http://ec.europa.eu/consumers/redress/ecc_network/index_en.htm

7.4 Legal and administrative good practices in e-business

The country reports show that Member States have taken a wide range of initiatives to promote the use of e-business, and electronic communication in general.

The reported best practices can be divided in four overall categories: legal initiatives, information campaigns, administrative initiatives and infrastructure projects.

7.4.1 Legal Initiatives

The *Netherlands* is a particular example of implementation approach. While most Member States have made a horizontal implementation of the E-commerce Directive into national law, the Netherlands has implemented the e-commerce Directive and the Distance Selling Directive directly into the Civil Code.[162]

By implementing the Directives into the Civil Code, electronic contracts are directly integrated with the general legal system of the Civil Code. Although there was no need for major amendments to the Civil Code to ensure the validity of contracting online, the transposition of the Directive into the code is reported to have increased the awareness of the validity of electronic contracts in the Netherlands. The adoption of the new Civil Code in the Netherlands is also mentioned in the report from the Committee on the Internal Market and Consumer Protection as an example that could serve as a model for other Member States when drafting new legislation[163].

In *Ireland*, Directive 1999/93/EC on a community framework for electronic signatures was quickly implemented into the Irish Electronic Commerce Act from 2000. The act on electronic commerce gave same status to electronic signatures, electronic contracts and electronic writing as the paper-based equivalents. The early implementation is reported to have helped to create legal certainty for enterprises, and hence promote e-commerce activity[164].

As noted back in 1999 by Forfás, the Irish national policy and advisory board for enterprise, trade, science, technology and innovation, when urging in a detailed report the government to swiftly implement e-commerce initiatives: "*In e-commerce, trust is particularly important as the parties to the transaction may never meet - the identity of partners is therefore a serious issue. The buyer wants assurance that the seller (a) exists, and (b) is worth doing business with. The seller likewise wants to know that the buyers are who they say they are, and that the payment is secure*"[165]

---

[162] www.bakernet.com/ecommerce/netherlands-t.htm and "Harmonisation of EU marketing law", Anne-Dorte Bruun Nielsen, Associate Professor, Aarhus University, pp.73-75 http://www.norden.org/pub/velfaerd/konsument/sk/TN2002509.pdf#search=%22Burgerlijk%20Wetboek%20%20%22e%20commerce%22%22

[163] The report of the Committee on Legal Affairs and the opinion of the Committee on the Internal Market and Consumer Protection (A6-0055/2006) (Page 3)

[164] Please note that also other Member States have made swift implementation of the Directives of relevance to E-business.

[165] Report on e-Commerce – The Policy Requirements, cfr. http://www.forfas.ie/publications/ecommerce/business.htm

There is no doubt that a swift implementation of the Directives into national law helps enterprises and consumers that seek a clear and transparent framework for e-business, especially when engaging in cross-border trade.

In *Belgium*, the Government has established an office for administrative simplification[166]. One of the main tasks of the office has been to take legal and practical initiatives to abolish burdensome administrative rules. Many of the initiatives have related to the introduction of paperless transactions by making minor changes to old laws. As a result, it is now possible to make electronic storage of evidence documents in hospitals, electronic registration of vehicles, and electronic annual corporation tax returns. More than 150 laws have been abolished or simplified as a result of the initiative since 2003.

According to the Belgian office for administrative simplification, a World Bank study suggests that the cost of establishing an enterprise in Belgium has been halved during 2005[167]. According to the same office, the Belgium Kafka-initiative has been drawing significant attention also from newspapers abroad, showing interest in the Belgian approach to legal simplification.

In *Denmark*, a similar initiative, focusing on the barriers to digital communication, has been taken.[168] This initiative has also functioned as the official follow-up on the requirement in Article 9 of the e-commerce Directive to remove obstacles for electronic conclusion of contracts.

It was noted by the Danish Government that requirements of formality which was found in older legislation, such as the mentioning of the need for signature and requirements for written communication etc. could pose unnecessary barriers to the effective use of digital communication. While it was considered possible to interpret most legislation in the light of the possibilities of new technology, it was noted that the very interpretation would carry the risk with it that enterprises and citizens would refrain from using digital solutions due to the potential doubt that may prevail in relation to any interpretation of law. Therefore, it was decided by the Government that every ministry was to review its legislation for references to such formalities that may constitute barriers to the efficient use of information technologies. Each ministry was required to go through its own legislation because knowledge of the material content would be essential for the reporting to be presented within 12 months. In the reports, each ministry was required to pinpoint all examples of such requirements of formality, and in those cases where the ministry would not suggest abolishing the formal requirements the ministry was to give a detailed explanation of the reasons making it impossible to propose a change. Having pinpointed the areas where barriers exists, each ministry was to develop a prioritised plan of action to be implemented, and set forward the specific proposals for changes as well as a timetable for their implementation. The plans were presented in 2003, and implemented in subsequent years.

---

[166] www.kafka.be

[167] World Bank Report "Doing Business 2007", quoted in De Tijd, 6 September 2006, and reproduced at the site www.kafka.be

[168] Plan of action for the modernisation of legislative demands of formality that may constitute unnecessary hindrances to digital communication. Issued in 2002 by the Ministry of Science, Technology and Development together with the Ministry of Justice.
http://e.gov.dk/fileadmin/Filer/Dokumenter/Resultater/2002/handling.doc

The Danish initiative mentioned above has now been replaced by a continuous monitoring of new legislation by the Danish Ministry of Justice to ensure continued focus on digital communication and consistency of measures.

Legal initiatives such as those described above are helping companies and consumers through the development of trustworthy framework conditions around e-commerce, being based on visible consumer safeguards and unambiguous legal regulation.

7.4.2 Administrative initiatives

On a European scale, the ***Euro-label*** *initiative* is a significant example of an initiative to increase confidence in e-commerce[169]. The Euro-Label is a trust mark to be used by websites that comply with the European Code of Conduct. It is promoted by 8 national institutions, acting as national Euro-Label certification bodies. The Code was drafted to reflect current and anticipated future European legislation. It draws on the EU Directives on Electronic Commerce, Distance Selling and Data Protection.

The Euro-label site also includes a portal of certified shops, thus bringing business and consumers together. It further provides guidance on how to resolve disputes with shops in case of breach of the code of conduct.

Euro-Label's central objective is to foster the growth of e-transactions within Europe, by ensuring that there is a common basis for on-line trading that is trustworthy and fair.

The Euro-label organisation is at the same time acting as a central point for complaints, particularly for cross-border purchases, and it also provides links to international Alternative Dispute Resolution providers. Consumers can thus submit a complaint against a trader who does not respect the European Code of Conduct. This complaint will be handled by the system until its satisfactory resolution, either through the appropriate national certification body, or through an ADR.

The ***Luxembourg certification*** *initiative* is an example of an interesting initiative taken at national level. It is managed by the Luxembourg Chamber of Commerce with the support of the Ministry of Economy and External Commerce[170].

The initiative consists of no less than three distinct certificates (or trust marks) that are to promote secure e-commerce sites.

The first, the Luxembourg *e-privacy certificate,* is a guarantee to the user that personal data are treated in accordance with EU requirements. It is proposed to websites that do not include commercial ties or financial transactions, but which for any given purpose may collect and deal with the personal data provided. This could be to subscribe to a free newsletter or when filling in an electronic template for a given purpose.

The Luxembourg *e-commerce certificate* is intended for internet relations which include an offer to enter into a trade relation. The intention is to cover in particular two situations:

[169] www.euro-label.com

[170] www.e-certification.lu

- Commercial transaction sites which propose the conclusion of a deal to obtain a product or service entailing on-line payment or bank transfer;
- Commercial sites without economic transaction such as on-line reservation sites

Sites having received the Luxembourg e-commerce certificate are subject to a thorough audit, covering compliance with all requirements linked to the certificate, which in the case of commercial transaction sites also includes requirements to the ways of concluding contracts and conditions to ensure safe payments.

Finally, the Luxembourg *e-commerce certified partner certificate* targets service providers that for instance are hosting IT-platforms for other companies, or are operating platforms for electronic payments.

The Luxembourg Chamber of Commerce site also includes a guide to information system safety and a description of the requirements that a site must comply with in order to qualify for a certificate.

The basis for the Luxembourg certification initiative was a benchmarking study of certification systems around the world, commissioned by the Ministry of Economics, which was published in March 2002. In an initial phase, the Ministry of Economics tested the certification procedure, but once the certificate was well established, the Ministry has limited its own role to mainly providing assistance to the Chamber of Commerce in creating publicity around the certification of companies.

Another initiative with a similar aim but developed in a commercial context and **at European scale**, is the ***Trusted Shops*** initiative, which was created in early 2000. The primary objective, in the words of the website of Trusted Shops: "*was to meet the demands made by leading politicians for better security in the internet – and to confirm to the consumer that this security is here to stay*[171]."

This initiative is a private venture, involving a number of commercial partners including a major insurance group, and with a market focus on the United Kingdom, Germany, France, Belgium, the Netherlands and Scandinavia. There are currently about 1600 internet retailers operating under the Trusted Shops standard.

The idea is to give the label of Trusted Shops to reliable e-commerce operators and collect premiums as a percentage of purchase from customers preferring to buy from such shops. Given the problems of reliability and security of B2C e-commerce and e-payments, the project started successfully and by the end of 2004 it had handled risks totalling 250 million euros, covering an increasing number of consumers[172].

The Trusted Shop label offers a guarantee of safe shopping for their customers, including a money back guarantee. To the interested company the Trusted Shops initiative promises the dual advantage of customer confidence flowing from the guarantees linked to the label, and the potential of more trade due to some promised large-scale PR and marketing campaigns.

[171] http://www.trustedshops.com/

[172] Quoted from UNCTAD Information Economy report 2005, chapter 3, page 131 http://www.unctad.org/en/docs/sdteecb20051ch3_en.pdf

Also it offers a free insurance coverage and a multi-lingual on-line dispute service. The label is obtained by the online shop after Trusted Shops conducts a financial assessment, a privacy and reliability check, and a technical check of the website[173].

Also in the field of alternative settlement of disputes in e-commerce, self-regulation initiatives have been taken. The *Global Business Dialogue on Electronic Commerce*[174], being a forum of dialogue between the private sector and governments to discuss e-commerce issues, has been instrumental in the establishing of a number of e-commerce initiatives, including standards of alternative dispute resolution.

Together with Consumers International, a set of ADR Guidelines have been negotiated, which providers of ADR can subscribe to, and thus give the consumer, interested in settling an e-commerce complaint through alternative means, a guarantee that the ADR provider is trustworthy[175].

The above initiatives are successful examples of initiatives taken in the public or in the private sphere with a view to diminish risk for the consumer and increase the visibility and attractiveness of the company, and thus reduce the transaction costs in e-commerce.

7.4.3 Information Campaigns and Initiatives

Across Europe, governments and private organisations have established information websites that provide practical and legal advice to consumers and businesses on e-commerce. These sites supplement the **Consumer Europe** websites that have been established on the initiative of the European Commission[176].

Below is a description of some good practice examples of information sites and campaigns.

Econsumer.gov is a resource website for consumers who buy products and services online from sellers in other countries. Launched in 2001, the aim of econsumer.gov was to enhance consumer protection and consumer confidence in e-commerce. It is a cooperation of consumer agencies in 20 countries. The initiative has two components: a multilingual public Web site, and a government, password-protected Web site.

The public site provides general information about consumer protection in all countries that belong to the ICPEN (International Consumer Protection Enforcement Network), contact information for consumer protection authorities in those countries, and an online complaint form. All incoming complaints are shared through the government Web site with participating consumer protection law enforcers with a view to develop effective enforcement of e-commerce legislation and help prevent fraud.

The econsumer.gov site does not, however, take up individual complaints automatically, but seeks to gather information to prevent systematic fraud and act at a structural level to promote safe cross-border on-line commerce.

---

[173] http://www.ombuds.org/center/ODR%20Europe_Muenster%20Report1.htm

174 www.gbde.org

175 www.gbde.org/agreements/adragreement03.pdf

176 The European Consumer Centres Network (ECC-Net)
ec.europa.eu/consumers/redress/ecc_network/index_en.htm

Further, the econsumer.org provides amongst other advice to consumers wishing to engage in the settling of a dispute through ADR providers, and it provides access to a list of ADR-providers.

The International Chamber of Commerce, ICC, is another good example of a comprehensive web-source of information, in this case concerning ADR providers. The ICC website provides an inventory with contact information for firms and organizations around the world that can help resolving online disputes[177].

At the national level, there is a number of government information initiatives, of which a few are mentioned in the following.

In *Finland*, the Government has established an Information Society Program to promote and develop governmental initiatives on advancement of the information society[178]. The programme maintains a web-site containing guidelines, news and a collection of best practice examples. Further, the Finnish Information Society Development Centre (TIEKE), a non-profit organisation of a large number of private companies and public bodies, has been developing information campaigns and educational activities amongst other together with the Finnish Ombudsman on e-commerce[179].

In *Austria*, an Internet ombudsman was established already in 1999 in a cooperation between the Austrian Institute for Applied Telecommunication (ÖIAT) and the consumer information organisation (VKI).

The overall aim is to contribute to the development of better consumer protection in e-commerce as a means of increasing e-commerce activity overall.

A dedicated site[180] provides advice on safe on-line shopping and information on standards in e-commerce.

The Internet Ombudsman provides expert assistance to consumers free of charge to resolve disputes with e-commerce companies. Since 1999, more than 3000 disputes have been settled and the ombudsman has answered more than 12.000 questions concerning use of the internet. The Internet Ombudsman also participated in developing the official e-commerce trustmark in Austria, which is an active part of the Euro-label cooperation.

The Austrian Internet Ombudsman is partly based on private contributions and voluntary work, and partly financed by the Ministry of Social Security and Consumer Protection.

In the *UK*, the Government was behind the initiative to establish a common trustmark in the UK, named TrustUK. The Government asked the Alliance for Electronic Business and the Consumers' Association to work together and set up a self-regulatory scheme to address the needs of consumers transacting on-line.

The main concern was that a large number of schemes were being developed world-wide which allowed individual web-traders to use a symbol or hallmark on their websites. The Government was also concerned that consumers would become confused by a proliferation of symbols. It believed

177 www.iccwbo.org/home/ADR/inventoryhome.asp

178 www.tietoyhteiskuntaohjelma.fi

179 www.tieke.fi

180 www.ombudsmann.at/ombudsmann.php

there was a possibility consumers might make false assumptions about the value of a particular symbol and the trustworthiness of the trader using it.

The role of TrustUK was to remove potential confusion. The approach is that accredited websites will display the TrustUK Hallmark either on it's own, or together with the logo of the code owner they subscribe to - so that one can see at a glance whether the website meets the minimum standards set in TrustUK's Accreditation Criteria.

A separate, independent Approvals Committee decides whether a code of practice meets the minimum standards of the TrustUK. The TrustUK Approvals Committee also consider any appeals from consumers who feel a code owner has not handled their complaint according to the proper, approved procedure.

In *France*, the Ministry of Finance is behind an information website with the telling title 'E-commerce and you'[181] that includes advice on how to buy on the internet, describes the rights of the consumer, guides the consumer in case of complaints and presents and explains the recent EU directives.

The website is short and concise, and provides detailed explications of a practical nature to the internet consumer, and refers the reader to possible further information elsewhere, through links.

In *Spain*, the Ministry for Industry, Tourism and Commerce has included a list on its web site of systems of self-regulation[182]. The Ministry notes that this is an area where there is a significant value in self-regulation given the constant changes of possibilities in technology and given the interest of the industry in providing itself with a model that reflects a positive image to the consumer. The Ministry does at the same time make it clear that presenting such a list of self-regulation systems does not imply that these systems are endorsed by the Ministry, nor is it a guarantee that they are in conformity with existing laws.

On the same website, there is a list of Frequently Asked Questions that help explain and interpret the requirements established by e-commerce rules[183]. The questions provided are a mix of questions of interest to e-commerce shops and to consumers.

Finally, **in *Belgium***, the Ministry of Economic Affairs has set up the so-called 'Internet Rights Observatory'[184]. The main tasks of this Observatory is to submit opinions on the economic problems brought about by the use of new information and communication technologies; to organize consultations among the economic actors concerned; and to inform the public on these aspects. The Internet Rights Observatory is composed of persons with experience in the new technologies but also of representatives of economic actors and of ICT users.

7.4.4 Infrastructure initiatives

A number of significant infrastructure initiatives have been taken that merit further mention.

181 "Le Commerce Electronique et Vous", www.finances.gouv.fr/cybercommerce

182 www.lssi.es/Secciones/Autorregulacion

183 www.lssi.es/Secciones/Preguntas

184 http://www.internet-observatory.be/

In *Denmark*, the executive order on electronic settlement and the executive order on information in OIOXML require all public institutions to be able to receive electronic invoices in the OIOXML format[185]. Further, the requirement included in the invoicing legislation to make use of electronic invoice mandatory, when providing services to public authorities, is generally regarded as an initiative that will accelerate further the private use of electronic invoices in B2B relations.

A number of Member States have started the development and implementation of *national electronic ID cards*.

Estonia has implemented an Identity Card[186] as the primary document to identifying all its citizens and alien residents living within the country. The card, besides being a physical identification document, has advanced electronic functions that facilitate secure authentication and a legally binding digital signature. The initiative is supplemented with nationwide online services.

Each Identity Card contains various personal data, Certificates (two certificates, one for authentication and one for digital signing) and an e-mail address assigned to the card holder by the government.

In *Spain*, the Government launched in March 2006 a similar initiative: a new Identity Card with a chip containing certificates to allow for authentication and signing with digital signature[187]. This application complies with the International standards created by the IETF[188] as well as European standards[189].

The new ID card can thus document to third parties the identity of the cardholder, and the electronic signature of the new ID card will have full legal force. It is expected that the new ID card will be distributed progressively to all residents in Spain until April 2008.

In *France*, the Government has officially approved plans for a new electronic ID card in 2005, and the plans are to commence distribution of the e-ID Card in 2007. The new Digital ID card will be obligatory, and every resident is supposed have the Card by 2011[190].

The plan is to develop e-ID cards and biometric passports in tandem.

Providing the citizens with an electronic signature is expected to foster the take-up of e-government and e-commerce services, and the future e-ID card and new passport will both contain the holder's personal information and biometric identifiers.

Finally, it should be mentioned that ***Belgium*** in 2004 adopted plans to provide all citizens with an electronic identity card[191].

---

[185] www.oes.dk

[186] http://www.id.ee/

[187] www.dnielectronico.es

[188] Internet Engineering Task Force, PKIX, reference document RFC 3647 (of November 2003): "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"

[189] ETSI TS 101 456: Policy Requirements for certification authorities issuing qualified certificates; ETSI TS 101 862: Qualified Certificate Profile and ETSI TS 102 042: Policy Requirements for certification authorities issuing public key certificates.

[190] http://europa.eu.int/idabc/en/document/4100

[191] http://eid.belgium.be/en/navigation/12000/index.html

The card contains an embedded microchip storing the holder's personal data. This personal information, linked to databases in the country's central population register, will be updated using the most stringent PKI (Public Key Infrastructure) standards.

The chip will also contain a digital certificate enabling remote authentication of the holder, making it possible for users to securely access e-government applications and affixing a digital signature to certify the authenticity of data transmitted when needed. All documents signed electronically using the card will have the same legal value as those signed by hand[192].

The electronic ID card is planned to be distributed to all citizens until the end of 2009 when the transition to the new card is expected to be complete[193].

[192] *Belgian e-ID card enters deployment phase* - eGovernment News – 24 September 2004 – Belgium – Identification & Authentication

[193] http://www.ibz.fgov.be/download/eid/CIE_en_20_questionsjuin05.pdf

8. Recommendations

Based on the findings and conclusions of this study, in particular the identification of barriers to e-business in the European Union, a number of recommendations can be made for European and national initiatives with the objective to reduce some of these barriers. Below, the recommendations are listed along with some background observations and considerations.

1. The basic legal foundation for use of electronic signatures by businesses is present in all Member States. In many Member States there are, however, still **formal hindrances** in national legislation in relation to use of electronic means, such as, e.g. requirements for a written signature in two copies on a specific form.

    - *It is recommended that Member States take initiatives to review their national legislation for references to such formalities that may constitute barriers to the efficient use of information technologies.*

2. Improved **cross-border interoperability** is of key importance to reducing the barriers to cross-border e-business and create equal opportunities for all citizens and businesses.

    - *It is recommended that a concerted effort is undertaken at international level to improve the use of e-signature and e-invoicing by creating a common and freely usable implementation of the e-signature and e-invoicing standards at least between the countries parties to the European Economic Area Agreement*

3. Establishment of a well-functioning PKI infrastructure that provides for technical interoperability between various certification service providers is the first condition for cross-border use. Technical interoperability is, however, not sufficient *per se*. Commercial interoperability must also be present when establishing a PKI infrastructure with involvement of Certification Service Providers with different business models.

    - *It is recommended that an effort is made at international level to establish cross border trust models among e-signature Certification Service Providers at least between the countries parties to the EEA Agreement.*

4. It is clear from this study that **e-government services** are the main driver for the uptake of electronic signatures, making the public sector a key player in facilitating and encouraging the use of electronic signatures. Furthermore, usage of electronic invoices remains low despite significant efficiency gains to be reaped. Also in this area, Government acceptance – or even requirement - of e-invoices can be an important element in creating the incentive for businesses to take up e-invoicing. It is important that government institutions, when providing online services, take initiatives to recognize and support the use of electronic communication in general, and electronic signatures and e-invoicing in particular, as a tool to provide effective and secure communication, not only in business-to-government situations but also when providing the framework for business-to-business and business-to-consumer relations. A number of countries have taken important initiatives, but in many Member States, there is a need for increased e-government implementation.

- *It is recommended that national Governments take the lead in promoting the use of e-signatures, e-invoices etc. through their provision of online (e-government) services.*

5. A widespread **lack of trus**t in electronic transactions among many citizens and enterprises is a key barrier for the increased uptake of e-business. This is, in particular, related to the fact that enterprises, in particular SMEs, as well as consumers, are not sufficiently aware of their rights and obligations when, respectively, selling or buying online, and about national authorities in charge of solving legal problems in e-business. Consequently, there is a widespread lack of compliance by enterprises selling online with their information and other obligations.

    - *It is recommended to launch a multi-annual action for making available multilingual information aimed at SMEs and consumers in all countries parties to the EEA Agreement about their rights and obligations regarding Internet transactions, in particular cross-border transactions (both intra-community, export and import). This could include information about e-signature and e-invoicing standards, as well as on their implementations. This could, e.g., be done by means of a European e-Business Portal, similar to the one funded by DG Enterprise and Industry 2003 and 2004 (ebusinesslex.net [194]), that would also include links to similar national portals.*

6. The lack of trust is also related to the experiences of consumers and businesses in connection with bankruptcy or other non-performance of the vendor, where payment has been made but the goods or services not delivered.

    This issue has been addressed in the Nordic Countries, where a joint opinion of the Nordic Consumer Ombudsmen expressly states that vendors should only debit an account (credit card) once the good is actually shipped to the consumer and that debit of the account of the consumer prior to the shipment of the good is in contradiction of good marketing practice. This grants the consumer/buyer a high degree of safety and thus increases trust in economic transactions over the Internet.

    - *It is recommended that a similar initiative is taken at European level to include in the principles of good marketing practice that debit of the buyer's account can only be made once the good has been shipped or the service delivered.*

7. Cross-border payments between the 13 Member States where Regulation 2560/2001 is applicable, are charged the same as domestic payments. Cross-border payments when one of the parties is located in one of the 12 Member States where Regulation 2560/2001 is not applicable may be (and usually are) subject to higher charges than domestic payments. This is a disincentive to cross-border transactions in the Internal Market, including e-commerce.

    In addition, in certain Member States where Regulation 2560/2001 is applicable, it seems that enterprises are not fully aware of the advantages provided by it.

[194] Online from April 2003 till December 2005.

The extension of the scope of this regulation also to transactions made in all EU national currencies, and awareness-raising actions of the advantages provided by Regulation 2560/2001, could increase the volume of transactions and of payments in the Internal Market, including electronic transactions.

- *It is recommended to enlarge the scope of* Regulation (EC) 2560/2001 *in order to equal all the charges for payments done between Member States in euros or in the national currency to those made for domestic payments.*

- *It is recommended to carry out initiatives to raise awareness among SMEs of the advantages provided by Regulation 2560/2001.*

8. The functioning of the Internal Market would gain from a **legal unification of contract law** since enterprises and especially SMEs would obtain a more simple and foreseeable regulation of their contracts. A legal transparency of contractual regulation seems especially valuable for e-business where a key element is safe and simple cross-border trade.

    - *It is recommended that initiatives are taken to promote a more uniform contractual regulation within the European Economic Area.*

Annex I: List of references

EU Directives

Commission of the European Communities - Directive 1994/820/EC, Legal aspects of electronic data interchange, http://www.it-retten.dk/bog/bilag/19/Recommendation%20EDI.pdf

Commission of the European Communities - Implementation of Directive 1998/6/EC on consumer protection in the indication of prices of products offered to consumers;
http://ec.europa.eu/consumers/cons_int/safe_shop/price_ind/comm_21062006_en.pdf

Commission of the European Communities - Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures;
http://europa.eu.int/information_society/eeurope/i2010/docs/single_info_space/com_electronic_signatures_report_en.pdf

Commission of the European Communities - Requirements for conducting public procurement using electronic means under the new public procurement Directives 2004/18/EC and 2004/17/EC;
http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/sec2005-959_en.pdf

Directive 1997/7/EC, Article 8 - The protection of consumers in respect of distance contracts;
http://ec.europa.eu/consumers/policy/developments/dist_sell/dist01_en.pdf

Directive 2000/31/EC – on certain legal aspects of information society services, in particular electronic commerce, in the Internal Marked;
http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML

European Parliament – Directive on access to, and interconnection of, electronic communications networks and associated facilities (10418/1/2001-C5-0416/2001- 2000/0186 (COD))
http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/documents/112-12_access_e.pdf

Other legislation

Real Decreto 1553/2005 – Regulation of the Spanish national identification card and electronic signature;
http://www.boe.es/boe/dias/2005/12/24/pdfs/A42090-42093.pdf , and
http://www.belt.es/legislacion/reciente/pdf/RD_24_dic_05.pdf

Convention on the International Sales of Goods- Introduction to the Principles of European Contract Law (PECL);
http://www.cisg.law.pace.edu/cisg/text/peclintro.html

Convention on the International Sales of Goods - The rules of European Contract Law; http://www.cisg.law.pace.edu/cisg/biblio/lando2.html

Convention on the International Sales of Goods- The UNIDROIT Principles of International Commercial Contracts and the Principles of European Contract Law: Similar Rules for the Same Purposes?
http://www.cisg.law.pace.edu/cisg/biblio/bonell96.html

European Commission- Consumer affairs - European contract law,
http://ec.europa.eu/consumers/cons_int/safe_shop/fair_bus_pract/cont_law/index_en.htm

European Commission - Convention on the law applicable to contractual obligations (Rome Convention),
http://europa.eu/scadplus/leg/en/lvb/l33109.htm

Jus - Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996),
www.jus.uio.no/lm/un.electronic.commerce.model.law.1996/history.background.html

International Institute for the Unification of Private Law- Common law vs. civil law (codified and uncodified), William Tetley;
http://www.unidroit.org/english/publications/review/articles/1999-3.htm

Ley de Servicios de la Sociedad de la Información, Spanish Law;
http://www.lssi.es/

Peer Zumbansen - German Contract Law and Internet Auctions, German Law Review Vol. 2 No. 7 - 15 April 2001,
http://www.germanlawjournal.com/past_issues.php?id=65

Regulation (EC) No 2560/2001 of the European Paliament and og the Council on cross-border payments in Euro,
http://eur-lex.europa.eu/LexUriServ/site/en/oj/2001/l_344/l_34420011228en00130016.pdf

Scint - Tribunale Di Cuneo Ricorso Per Decreto Ingiuntivo, December 15, 2003, Italian law: http://www.scint.it/news_new.php?id=407

Tribunal de defensa de la competencia – Memoria 2005, Spanish law;
http://www.tdcompetencia.es/html/memorias/38der.htm

United Nations Commission on International Trade Law - Model Law on Electronic Commerce with Guide to Enactment,
www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html

Court cases

Estee Lauder v. Fragrance Counter, Inc., 1999 U.S. Dist. LEXIS 14825 (S.D.N.Y. 1999).
http://www.perkinscoie.com/casedigest/icd_results.cfm?keyword1=advertising&topic=Advertising

District Court Haarlem (cantonal sector) 6 October 2005, LJN AV2652,
http://zoeken.rechtspraak.nl/resultpage.aspx?snelzoeken=true&searchtype=ljn&ljn=AV2652&u_ljn=AV2652

District Court Rotterdam (cantonal sector) 19 January 2006, LJN AU9939, http://zoeken.rechtspraak.nl/resultpage.aspx?snelzoeken=true&searchtype=ljn&ljn=AU9939&u_ljn=AU9939

European Commission - Antitrust cases, http://ec.europa.eu/comm/competition/antitrust/cases/index/by_nr_58.html

OLG Hamm, decision December 14, 2002, U 58/00, http://www.olg-hamm.nrw.de/

Swedish National Board for Consumer Complaints no. 2001-4889, May 22, 2002, http://www.arn.se/

The Supreme Administrative Court, December 23, 2005, case 2722/2/03, http://www.kho.fi/en/paatokset/34165.htm

Reports

Alexander Rossnagel- Digital signature regulation and European trends, http://www.emr-sb.de/news/DSregulation.PDF

Andreas Mitrakas- Information Security and Law in Europe: Risks Checked?, Information & Communications Technology Law, Volume 15, March 2006 http://www.enisa.europa.eu/doc/pdf/LR_33-54.pdf

Capgemini, "Online availability of Public Services: How is Europe Progressing", June 2006, http://ec.europa.eu/information_society/soccul/egov/egov_benchmarking_2005.pdf

Commission of the European Communities- Action plan for the implementation of the legal framework for electronic public procurement, http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/actionplan/actionplan_en.pdf

Commission of the European Communities - European Contract Law, http://ec.europa.eu/consumers/cons_int/safe_shop/fair_bus_pract/cont_law/cont_law_02_en.pdf

European Commission, Internal Market Directorate-General, 2004: Impact Assessment: Action Plan on e-Public Procurement, Part 1: Baseline Analysis, http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/2004-12-impact-external-vol1_en.pdf

European Commission - Green paper on alternative dispute resolution in civil and commercial law, http://europa.eu/eur-lex/en/com/gpr/2002/com2002_0196en01.pdf

European Commission - Reaction to the Action Plan: A more coherent European Contract Law; http://ec.europa.eu/consumers/cons_int/safe_shop/fair_bus_pract/cont_law/analyticaldoc_en.pdf

Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, May 16 2001, http://www.bundesnetzagentur.de/media/archive/2596.pdf

Infraestructura de Clave Pública: DNI Electrónico
http://www.dnielectronico.es/PDFs/politicas_de_certificacion.pdf

KU LEUVEN- Legal and Market aspects of Electronic Signatures, 2003 Study for the European Commission – DG Information Society;
http://europa.eu.int/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

Michael Joachim Bonell- UNIDROIT Principles 2004: The New Edition of the Principles of International Commercial Contracts adopted by the International Institute for the Unification of Private Law,
http://www.unidroit.org/english/publications/review/articles/2004-1-bonell.pdf

Summers, CJ and Black, D.- eCommerce in Welsh SMEs: The State of the Nation Report 2002/2003, eCommerce Innovation Centre, Cardiff University 2003, http://www.ecommerce.ac.uk/pdf/StateoftheNation20022003.pdf

The National Post and Telecom Agency's report, Sweeden- E-handel och statens instrument för att utveckla förutsättningarna, 2002,
http://www.pts.se/Archive/Documents/SE/E-handel%20och%20statens%20instrument%20for%20att%20utveckla%20forutsattningarna%20-%20PTS-ER-2002_3.pdf

The report of the Committee on Legal Affairs and the opinion of the Committee on the Internal Market and Consumer Protection (A6-0055/2006),
http://www.europarl.europa.eu/omk/sipade3?PUBREF=-//EP//NONSGML+REPORT+A6-2006-0055+0+DOC+PDF+V0//EN&L=EN&LEVEL=2&NAV=S&LSTDOC=Y

Websites

Bundeskanzleramt Österreich, http://www.cio.gv.at

Danish Agency for Governmental Management, http://www.oes.dk

E-certification, Luxembourg; http://www.e-certification.lu/

European Law website- EUR-Lex, Official Journals
http://europa.eu.int/eur-lex/lex/en/index.htm

European Commission - Commission exempts multilateral interchange fees for cross-border Visa card payments,
http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/02/1138&format=HTML&aged=1&language=EN&guiLanguage=en

European Commission - Commission welcomes increased transparency in VISA and MasterCard cross-border fees,
http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/04/616&format=HTML&aged=0&language=EN&guiLanguage=fr

European Commission – Overview of consumer policy,
http://ec.europa.eu/consumers/overview/index_en.htm

European Commission – Public Procurement
http://ec.europa.eu/internal_market/publicprocurement/index_en.htm

European Commission- Helping consumers seek redress: Alternative Dispute Resolution (ADR), http://ec.europa.eu/consumers/redress/out_of_court/index_en.htm

European Consumer Centres Network (ECC-NET), http://ec.europa.eu/consumers/redress/ecc_network/index_en.htm

European Union Business Guides - Consumer Policy in the European Union, http://www.eubusiness.com/guides/consumer.

International Institute for the Unification of Private Law, www.unidroit.org

Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens, http://ec.europa.eu/idabc/en/home

ID, http://www.id.ee/

The Internet Engineering Task Force, http://www.ietf.org

The Internet Engineering Task Force,- Public-Key Infrastructure, http://www.ietf.org/html.charters/pkix-charter.html

The Internet Observatory, http://www.internet-observatory.be/

Kafka, www.kafka.be

Konsumentverket, http://www.konsumentverket.se/

Mastercard, http://www.mastercard.com/us/company/en/corporate/mif_information.html

Oficina de Atención al Usuario de Telecomunicaciones – Presentación Reclamaciones, Spanish Consumers Complaints Office; http://www.usuariosteleco.es/comoreclamar/PresentacionReclamaciones/

Programa ARTE/PYME, http://www.mityc.es/Artepyme/

Quienten R. Kroes (Ed.)., E-business Law of the European Union, Allen & Overy, Legal Practice, Kluver Law International 2003

Sociedad de la Información – Firma Electrónica, Spanish information about electronic signature; http://www.mityc.es/DGDSI/Servicios/FirmaElectronica/

The Spanish National Identification Electronic Card, http://www.dnielectronico.es/

Tietoyhteiskuntaohjelma website, http://www.tietoyhteiskuntaohjelma.fi/

Trustedshops, http://www.trustedshops.com/

United Nations Commission on International Trade Law - International Sale of Goods (CISG) and Related Transactions http://www.uncitral.org/uncitral/en/uncitral_texts/sale_goods.html

United Nations Commission on International Trade Law, http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html

Uni-graz – The SGECC and its Working Groups
http://www.uni-graz.at/bre1www/tom/page16/page16.html

Webwereld, www.webwereld.nl/articles/31348

Wikipedia, http://en.wikipedia.org/wiki/X.509

Annex II: Questionnaire for the Member State survey

Questionnaire for European Commission study on e-Business - electronic signatures and electronic invoicing

A short introduction
This questionnaire is part of the study "Legal and administrative practices in e-business". The aim of the study is to:

- support better regulation through removal of barriers for e-business
- improve the functioning of the Internal Market
- improve the framework conditions for European business.

The questionnaire is a supplement to the description in the country reports of national legal and administrative e-business practices that you have already received in June 2006.

About the survey
This questionnaire contains questions on the current status in your country in the areas of electronic signatures and electronic invoicing. The topics of the questionnaire are: government strategies and objectives, standards, technology, costs and use.

The survey is quantitative in nature and contains mainly closed-end questions with a possibility to elaborate on specific subjects.

The questionnaire is designed to be easy to fill out, and to be completed in less than 15 minutes once you have the relevant knowledge to answer the questions. The contact point for this questionnaire is members of the steering group, mainly officials in the responsible government institutions.

What if I have questions?
If you have any questions concerning the questionnaire, please do not hesitate to contact:

- Anne Svaneborg Vesterstroem, Anne.Svaneborg.Vesterstrom@r-m.com, +45 33 97 82 00

- Kasper Ovesen, kasper.ovesen@r-m.com, +45 33 97 82 00

Thank you for your time and cooperation!

Electronic signature in your country

Question	Answers for your country	Answers for Denmark
Existence of an official government strategy (in writing) for introduction of electronic signatures?		No individual strategy, but e-signature is part of the national e-government strategy
If yes, please provide document reference and/or Internet link (if possible in English)		http://e.gov.dk/uploads/media/strategy_2004_06_en1_01.pdf (page 7 and 29) http://www.e.gov.dk/english/results/2003/digital_signature/index.html
Existence of an official quantitative government objective for introduction of electronic signatures		Yes
If yes, please indicate year and target		A total of at least 1.1 m. digital signature certificates fulfilling the OCES standard have been issued to citizens, workers and businesses by the end of year 2006.
If yes, please provide document reference and/or Internet link		http://e.gov.dk/uploads/media/strategy_2004_06_en1_01.pdf (page 7 and 29)
Existence of an official qualitative government objective for electronic signatures		Yes, for OCES e-signature
If yes, please describe the objective		Secure communication, more efficiency with electronic communication
If yes, please provide document reference and Internet link		http://www.e.gov.dk/english/results/2003/digital_signature/index.html http://www.tst.dk/image.asp?page=image&objno=118385867#276,10,OCES-digital signatur – Målsætning
Existence of a government initiative concerning building a Public Key Infrastructure (PKI) and Internet link?		Yes
If yes, has the government provided economic support to the establishment of a Public Key Infrastructure (PKI)?		Yes, around EUR 7 million
If yes, please describe initiative and provide Internet link		The responsible Ministry initiated the selection of a Certification Authority, TDC A/S http://www.digitalsignatur.dk/visArtikel.asp?artikelID=615 http://www.digitalsignatur.dk/visArtikel.asp?artikelID=618
Has a common standard for electronic signatures been adopted?		Yes. It OCES is based on an early version of UBL 0.7. Currently, UBL 2.0 is being adopted. http://www.oio.dk/?o=a54bd5e3b9e3e94209f94882ac0c9301
If introduced, do enterprises and citizens from other EU Member States have access to the electronic signature?		No, only companies registered in Denmark and citizens with a Danish CPR-number
No. of certification service providers		1
If any CSPs, please list names and Internet link (only most important if many)		TDC A/S http://privat.tdc.dk/digital/

Question	Answers for your country	Answers for Denmark
Type of electronic signatures issued by certification providers in country.		Advanced electronic signature
Are qualified certificates as defined in the e-signature Directive issued in your country?		No
Technology available for electronic signatures		Software is the most widespread. Other applications are available, including USB key and ID card
Services available		Yes, at the end of 2005, private citizens could use more than 80 e-services with e-signature. 400 public authorities can receive secure e-mail with digital signatures. e-Services include: Tax, health, education, pension, insurance, telecommunication, e-mails to public authorities http://videnskabsministeriet.dk/site/forside/publikationer/2006/it-and-telecommunication-policy-report-2006/Policy_report.pdf
(Example of) Costs of a certificate for enterprises (Registration fees, annual fees, signature cards etc., in national currency and its equivalence in Euro)		3.200 DKK in registration for first e-signature excl. LRA 2.500 for second to tenth e-signature excl. LRA 500 from eleven and upwards e-signature excl. LRA http://erhverv.tdc.dk/artikel.php?dogtag=tdc_e_digi_sig_virk_pr
(Example of) Costs of a certificate for employees (Registration fees, annual fees, signature cards etc.)		10-100 DKK in registration fee (depending on security level) 0-40 DKK per year (depending on security level) http://erhverv.tdc.dk/artikel.php?dogtag=tdc_e_digi_pris_eks
Costs of a certificate for citizens (Registration fees, annual fees, signature cards etc.)		Software bases certificates are free for citizens
No. of certificates issued (total and in the last year)		More than 650.000 advanced e-signatures issued (summer 2006) http://www.digitalsignatur.dk/visForside.asp?artikelID=588
No. of certificates issued (employees)		Around 50.000 (to be confirmed)
No. of certificates issued (citizens)		Around 600.000 (to be confirmed)
No. of transactions with digital signature		No data
Please provide any other data on e-signature you find relevant		Users are generally satisfied with e-signatures. More than 55% use their signature at least once a month http://videnskabsministeriet.dk/site/forside/publikationer/2006/it-and-telecommunication-policy-report-2006/Policy_report.pdf

Electronic invoicing in your country

Indicative questions	Answers for your Member State	Answers for Denmark
Existence of an official government strategy (in writing) for introduction of electronic in-voices		No individual strategy, but e-invoicing is part of the national e-government strat-egy
If yes: please provide document reference and Internet link		http://e.gov.dk/uploads/media/strategy_2004_06_en1_01.pdf (page 6)
Existence of an official, quantitative govern-ment objective for introduction of electronic invoices		Yes
If yes, please describe objective (year and target)		By the end of 2006, at least 40 per cent of all public authorities undertake pur-chasing in digital form with digital invoic-ing (2003: 15 percent)
If yes, please provide document reference and Internet link		http://e.gov.dk/uploads/media/strategy_2004_06_en1_01.pdf (page 6)
Existence of an official, qualitative govern-ment objective for electronic invoices		Yes
If yes, please describe objective		Enhance efficiency of the public sector, avoid manual entry and data input, save time in approval of invoices
If yes, please provide document reference and Internet link		http://www.oes.dk/sw1903.asp http://www.fm.dk/1024/visArtikel.asp?artikelId=7148
Introduction of a common standard for elec-tronic invoices from enterprises to public cus-tomers		Yes, OIOXML based on OASIS / UBL http://www.oio.dk/?o=a54bd5e3b9e3e94209f94882ac0c9301
Which is, in your knowledge, the most widely used standard(s) for electronic in-voices sent to private companies in your country?		ebXML, UN/EDIFACT
Number of invoices sent electronically per year by private enterprises to public institu-tions (estimate) Latest year available, link if possible		14 million invoices sent electronically of the total 15 million invoices (ultimo 2005). Sent via either VANS or via estab-lished read-in service centres. http://videnskabsministeriet.dk/site/forside/publikationer/2006/it-and-telecommunication-policy-report-2006/Policy_report.pdf (page 23)
Percentage of invoices sent electronically by private enterprises to public institutions com-pared to the total number of invoices Latest year available, link if possible		Estimated > 90% of total are sent elec-tronically (ultimo 2005) http://videnskabsministeriet.dk/site/forside/publikationer/2006/it-and-telecommunication-policy-report-2006/Policy_report.pdf (page 23)
Number of invoices sent electronically per year by private enterprises to private enter-prises (estimate) Latest year available, link if possible		Awaiting updated data
Percentage of invoices sent electronically by private enterprises to private enterprises compared to the total number of invoices Latest year available, link if possible		Awaiting updated data
Please provide any other data on use of e-invoices you find relevant		

Annex III: Key results of the Member State survey

Table 1: National strategies on electronic signatures

	Existence of an official government strategy (in writing) for introduction of electronic signatures?	Existence of an official quantitative government objective for introduction of electronic signatures	Existence of an official qualitative government objective for electronic signatures	Has a common standard for electronic signatures been adopted?	If introduced, do enterprises and citizens from other EU Member States have access to the electronic signature?	Existence of a government initiative concerning building a Public Key Infrastructure (PKI) and Internet link?	Are qualified certificates as defined in the e-signature Directive issued in your country?
Austria	No individual strategy, but e-signature is part of the national e-government strategy, i.e. part of the concept Citizen Card	Yes	Yes	The Citizen Card concept has adopted the major signature standards, i.e. W3C XMLDSig, CMS/PKCS#7, some EESSI amendments of these standards (CAdES, XAdES), respectively.	Yes	No, PKI is largely market driven. The social insurance institution is the only public body issuing certificates to citizens.	Yes
Czech Republic	Yes, but no individual strategy	No	Yes	No	No	Y(only machine readable passport, no PKI for e-gov services or for qualified CSP's)	Yes
Cypress	No	No	No	No	Info unavailable	No, but a project regarding the PKI has been carried out, for academic use, by the Cyprus Research & Academic Network	No

	Existence of an official government strategy (in writing) for introduction of electronic signatures?	Existence of an official quantitative government objective for introduction of electronic signatures	Existence of an official qualitative government objective for electronic signatures	Has a common standard for electronic signatures been adopted?	If introduced, do enterprises and citizens from other EU Member States have access to the electronic signature?	Existence of a government initiative concerning building a Public Key Infrastructure (PKI) and Internet link?	Are qualified certificates as defined in the e-signature Directive issued in your country?
Denmark	No individual strategy, but e-signature is part of the national e-government strategy	Yes	Yes, for OCES e-signature	Yes. OCES is based on international standards like i.e.: X.509.v3 and ETSI TS 102 042 v 1.2.1 see reference in the OCES CP: https://www.signatursekretariatet.dk/certifikatpolitikker.html	No, only companies registered in Denmark and citizens with a Danish personal registration number (CPR-number)	Yes, the OCES standard constitutes a PKI which has now been established	No
Estonia	No individual strategy, but e-signature is part of the national e-government strategy, i.e. part of the concept Citizen Card	Yes	Yes	Yes, based on ETSI 101903 (XML Advanced Electronic Signatures, aka XAdES) Implementation is publicly available from www.openxades.com, see also http://www.sk.ee/pages.php/020305010101	All certificate holders can use technology available from www.openxades.com	Yes PKI is running from 2002	Yes

	Existence of an official government strategy (in writing) for introduction of electronic signatures?	Existence of an official quantitative government objective for introduction of electronic signatures	Existence of an official qualitative government objective for electronic signatures	Has a common standard for electronic signatures been adopted?	If introduced, do enterprises and citizens from other EU Member States have access to the electronic signature?	Existence of a government initiative concerning building a Public Key Infrastructure (PKI) and Internet link?	Are qualified certificates as defined in the e-signature Directive issued in your country?
Finland	No individual strategy, but e-signature is a part of the national e-government strategy. The legislation of e-signatures is in force.	No	1. In authenticating citizens in e-services qualitative objective is: - qualified certificates (EU directive and national legislation) - national TUPAS –standard, created by Finnish Bankers' Association for Internet-banking 2. For civil servants the use of qualified certificates for authentication and secure communications is recommended and a frame contract that covers the whole of government has been negotiated.	Yes. A list of standards used is at the end of this questionnaire.	Citizens from other member states that live permanently in Finland are able to get the Finnish electronic –ID. There is no national electronic signature scheme for companies.	The Public Key Infrastructure was built in 1999.	Yes.
France	No	No	Not for the moment but it's under definition in the Security General Framework used for govern-	It's part of the Interoperability General Framework under definition used for governmental e-services.	Yes	Yes	No

	Existence of an official government strategy (in writing) for introduction of electronic signatures?	Existence of an official quantitative government objective for introduction of electronic signatures	Existence of an official qualitative government objective for electronic signatures	Has a common standard for electronic signatures been adopted?	If introduced, do enterprises and citizens from other EU Member States have access to the electronic signature?	Existence of a government initiative concerning building a Public Key Infrastructure (PKI) and Internet link?	Are qualified certificates as defined in the e-signature Directive issued in your country?
			mental e-services. The private sector seems to be keen on following the same requirements.	The private sector seems to be keen on following the same requirements. We foresee to define a Xades subset as the standard signature format.			
Hungary	No individual strategy (a working paper exists), but e-signature is part of the Hungarian Information Society Strategy and E-government 2005 strategy	No direct objectives	Technology neutral legislation	Yes, there is a ministerial recommendation for the format of electronic signatures. This is a narrowed version of ETSI TS 101 903 (XAdES). http://www.itktb.hu/resource.aspx?ResourceID=A_kozig_form_V68_e1_V1_1	Yes, any natural, legal persons and corporations without legal entity.	Yes http://www.kgyhsz.gov.hu/	Yes
Ireland	Ireland has enacted law in this area called the Electronic Commerce Act 2000.	No	No	Yes for Revenue – not used anywhere else.	Enterprises registered with the Irish Revenue Commissioners may. It is not applicable for citizens.	Yes	Yes
Lithuania	No individual strategy, but e-signature is part of the national Information Society and public administration development strategies	Yes	Yes	Yes. ETSI TS 101 733 adopted, PKCS#7 and XAdES are in	Yes	Yes	Yes

	Existence of an official government strategy (in writing) for introduction of electronic signatures?	Existence of an official quantitative government objective for introduction of electronic signatures	Existence of an official qualitative government objective for electronic signatures	Has a common standard for electronic signatures been adopted?	If introduced, do enterprises and citizens from other EU Member States have access to the electronic signature?	Existence of a government initiative concerning building a Public Key Infrastructure (PKI) and Internet link?	Are qualified certificates as defined in the e-signature Directive issued in your country?
				use			
Luxembourg	Yes (cf. chapter 2.5 (Security and privacy) of the Egovernance master plan)	No	Yes	Yes	Yes	No answer	No
Malta	No	Yes	No	Ministry of Investments, Industry and IT (MIIIT) is responsible for the setup of a Government CA which is wholly managed by the Government ICT agency MITTS Ltd. The registration process for applicants (all Citizens) is conducted by an independent RA.	All Maltese residents	Yes. This is in finalisation stages.	They will be as From 2007
Netherland	TTP (trusted third party) strategy formulated in 1999, evaluated in 2003. E-signature strategy is also part of the larger e-government strategy	No	Yes	Yes, based on the standards created by ETSI ESI working group. Within the government PKI these standards have been expanded, to create a Program of Requirements (Programme van Eisen)	Yes, theoretically anyone can purchase certificates from PKI overhead CSPs. However, the signatures are intended for communication with or within the Netherlands.	Yes	Yes
Poland	No individual strategy. Government is a central root provider and Ministry of Economy is currently responsible for e-	No such objective	The Act of 18 September, 2001 on Electronic	The Regulation of 7 August 2002 by Cabinet regarding	Qualified certificate is available for citizens from other EU Mem-	Yes. State founded and state owned	Yes

	Existence of an official government strategy (in writing) for introduction of electronic signatures?	Existence of an official quantitative government objective for introduction of electronic signatures	Existence of an official qualitative government objective for electronic signatures	Has a common standard for electronic signatures been adopted?	If introduced, do enterprises and citizens from other EU Member States have access to the electronic signature?	Existence of a government initiative concerning building a Public Key Infrastructure (PKI) and Internet link?	Are qualified certificates as defined in the e-signature Directive issued in your country?
	signature certification services supervision.		Signature (Journal of Laws of 15 November, 2001) and secondary legislation to this act.	Electronic Signature (Journal of Laws of 12 August 2002). As a result we have common qualified certificate profile but no common e-signature file standard.	ber States. As for now foreign enterprises seem to be interested in time stamping services only.	central root in National Bank of Poland.	
Slovak Republic	Introduction of ES is a part of the national strategy for informatization of a society. Proposal was adopted by the government in January 2004.	Information unavailable	Yes, for :"ZEP" - qualified electronic signature defined in the Slovak legislation.	Yes, ZEP can be CAdES (ETSI TS 101 733) type or XAdES (ETSI TS 101 903) type. It is defined in decrees of the NSA no. 537 - 542. http://www.nbusr.sk/sep/en-default.html	Yes	Yes	Information unavailable
Slovenia	No	http://www.mju.gov.si/index.php?id=30&L=1	No. (Governmental CPS issues qualified certificates.)	No.	No, only companies registered in Slovenia and citizens with a Slovenian Personal Identification Number.	PKI is established within the government.	Yes
Spain	The Spanish eGovernment most recent strategy related to electronic signature is the "Plan Conecta". A key compo-	Yes	Yes, for eGovernment services using the national	At the moment, the Spanish Electronic Signature Law (Ley	As long as they fulfil with the Spanish legislation on the	Existence of a Public multiPKI Valida-	Yes

	Existence of an official government strategy (in writing) for introduction of electronic signatures?	Existence of an official quantitative government objective for introduction of electronic signatures	Existence of an official qualitative government objective for electronic signatures	Has a common standard for electronic signatures been adopted?	If introduced, do enterprises and citizens from other EU Member States have access to the electronic signature?	Existence of a government initiative concerning building a Public Key Infrastructure (PKI) and Internet link?	Are qualified certificates as defined in the e-signature Directive issued in your country?
	nent of this plan is the introduction of an electronic national identity card by the name of DNI Electrónico, which will gradually replace the traditional Spanish Identity card. Roll out of the new card has started in march 2006. The card incorporates integrated eSignature and eAuthentication capabilities. The Ministry of Interior acts as a certification service provider issuing qualified certificates for eDNI. Furthermore, the launch of the electronic national identity card has been complemented by the creation of a multiPKI validation platform supported by the Spanish Ministry of Public Administrations that validates electronic certificates and signatures for eGovernment services (currently around 262 available services)		eID card	59/2003) is based on the functional equivalence of the qualified (recognised) signature and the written signature, which both have the same legal value. On the other hand, various working groups have been set up in the Spanish Public Administration in order to analyse the convenience of adopting eSignature standards aimed to be used for the Public Administration	matter	tion Platform supported by the Spanish Ministry of Public Administrations. The multiPKI Validation Platform (VA) provides Electronic Identity Services to eGoverment applications, such as electronic certificate validation, eSignature validation, time stamping service… all of this within the new Electronic Citizen´s Identity Card framework.	
Sweden	No individual strategy, but e-signature is part of the national e-government strategy	No, not a quantitative. The object is to (during a limited time) procure e-identity-services	Yes	No, not appointed by national government. Banks and certain public sector actors is developing coordi-	No, banks and other CAs act as third party Guarantees based on the Swedish Population Register, distributed via the Tax	Yes (not specifically PKI, though)	No (but Advanced signatures are, among others). No supplier has reg-

	Existence of an official government strategy (in writing) for introduction of electronic signatures?	Existence of an official quantitative government objective for introduction of electronic signatures	Existence of an official qualitative government objective for electronic signatures	Has a common standard for electronic signatures been adopted?	If introduced, do enterprises and citizens from other EU Member States have access to the electronic signature?	Existence of a government initiative concerning building a Public Key Infrastructure (PKI) and Internet link?	Are qualified certificates as defined in the e-signature Directive issued in your country?
		to all public agencies in Sweden which intend to develop eGov-services (but which also hesitate because of the cost of e-identity services). The objective is in other words to contribute to the establishment of a working market for e-identity-services.		nation, best illustrated at http://www.e-legitimation.se/). This coordination might develop into a de-facto-standard eventually. A cooperation called SAMSET between public sector actors has been vital for the development of e-signatures in Sweden (http://www.skatteverket.se/samset.418e1b10334ebe8bc800046.html) On the following site you'll find current eID suppliers: http://www.e-legitimation.se/Elegitimation/Templates/LogolistPageTypeB.aspx?id=86. A major supplier on the Swedish e-ID market is BankID (www.bankid.com).	Agency. To get an electronic signature device it is thus necessary to be registered citizen of Sweden and to have a Civic Registration Number.		istered at the supervisory authority (Post och telestyrelsen [PTS.se]).

Table 2: National strategies on electronic invoices

	Existence of an official government strategy (in writing) for introduction of electronic invoices	Existence of an official, quantitative government objective for introduction of electronic invoices	Existence of an official, qualitative government objective for electronic invoices	Introduction of a common standard for electronic invoices from enterprises to public customers
Austria	No individual strategy, but legislation was recently changed to allow electronic invoicing. Additionally there is a government funded initiative to introduce XML based standards for e-invoicing. There is also a pilot project to introduce e-invoicing for the federal government has been initiated by the CIO and the Ministry of Finance.	No official objective	Yes (for the government funded standardization initiative)	Yes: ebInterface, an XML-based standard http://www.ebinterface.at/
Czech Republic	No individual strategy, but there is White paper on eCommerce	No	Yes	Information unavailable
Cypress	No individual strategy, but e-invoicing is included in one of the strategic options of the e-procurement strategy study	No	No	No
Denmark	No individual strategy, but e-invoicing is part of the national e-government strategy	Yes	Yes	Yes, OIOXML based on OASIS / UBL http://www.oio.dk/?o=a54bd5e3b9e3e94209f94882ac0c9301
Estonia	There is no any specific strategy from the public authorities in order to promote e-invoicing. Presumed reference as general eBusiness development	No	No	Estonian e-invoice standard available at http://www.pangaliit.ee/arveldused/e-arve/
Finland	Public Administration Recommendation No 155 (year 2003) on use of electronic invoices in Public Administration	Yes	Yes	Yes eInvoice: http://www.einvoiceconsortium.com/en/standardit.html Finvoice:

	Existence of an official government strategy (in writing) for introduction of electronic invoices	Existence of an official, quantitative government objective for introduction of electronic invoices	Existence of an official, qualitative government objective for electronic invoices	Introduction of a common standard for electronic invoices from enterprises to public customers
				http://www.fba.fi/finvoice/
France	On a central (government) level, only one project has thus far used electronic invoicing. : Edi Rafale, the maintenance part of the combat fighter Rafale (Ministry of Defense). Moreover, in terms of public sector no other electronic invoicing projects are for the time being taken place. However, in terms of digitization and electronic filing of justification cases some developments have started in order to automate public procurement procedures as well as reaching the goals of the action plan « e-2010).Locally, in the public sector (117 000 public offices), a simple XML invoice has been introduced for the purpose of exchanges between local offices and the state.	Locally, in the public sector, within the framework of semi-annual performances, the objective is to make 33 % of the invoices electronically at the end of 2010.	The objective is to favorites and advocate for the XML formats.	Consult the work of EDI-France / Direction Générale de la Modernisation de l'etat. (The directorate general for the modernization of the state.)
Hungary	There is no government strategy, but the e-Invoicing directive (2001/115/EC) has been transposed, and there is the 20/2004. (IV. 21.) Decree of Finance Minister on electronic invoices http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0400020.PM	No	No	There is a recommendation issued by MELASZ, the Hungarian Electronic Signature Association (www.melasz.hu) It is based on Oasis e-invoice format
Ireland	No individual strategy for electronic invoices but material relating to e-procurement and e-payments.	Yes, www.finance.gov.ie/documents/publications/other/eprocurefinal.pdf and ePayments material available at http://193.178.1.225/epaymentsthetour/	Yes, www.finance.gov.ie/documents/publications/other/eprocurefinal.pdf and ePayments material available at http://193.178.1.225/epaymentsthetour/	No

	Existence of an official government strategy (in writing) for introduction of electronic invoices	Existence of an official, quantitative government objective for introduction of electronic invoices	Existence of an official, qualitative government objective for electronic invoices	Introduction of a common standard for electronic invoices from enterprises to public customers
Luxembourg	No, but the availability of electronic signatures in 2007, will allow to launch new G2B projects related to electronic invoices.	No	No	No
Lithuania	No individual strategy, but e-invoicing is part of the national e-government strategy	Law on Value Added Tax (No IX-751 as of 5 March 2002) http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=216030 Regulations on the Use of Value Added Tax Invoices Issued and/or Received by the Electronic Means http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=232733	No	No
Malta	None to date	None to date	None to date	None to date
Netherland	Information unavailable	Information unavailable	Information unavailable	Information unavailable
Poland	No such objective		No such objective	Yes. We have recently introduced proposal for common standard developed by all qualified certification providers (EDI-XML GS1) http://www.e-gospodarka.net.pl/crwde/efaktura.htm
Slovak Republic	Introduction of e-invoicing is part of national strategy for information of society.	No such objective	No	Information unavailable
Slovenia	Information unavailable	No	Information unavailable	Information unavailable
Spain	-	-	-	-
Sweden	No individual strategy, but e-invoicing is part of the national e-government strategy	Yes	Yes	Not appointed by central national government. But, a few frontrunners (among a few are public agencies) are currently discussing a-de-facto-standard for invoicing. This cooperation is Scandinavian with focus on Swedish and Danish ac-

	Existence of an official government strategy (in writing) for introduction of electronic invoices	Existence of an official, quantitative government objective for introduction of electronic invoices	Existence of an official, qualitative government objective for electronic invoices	Introduction of a common standard for electronic invoices from enterprises to public customers
				tors. (This Scandinavian cooperation is partly organized by Helle Dam Sörensen at VTU in Denmark)