Study for the European Commission - DG Information Society

Service Contract Nr. C 28.400

THE LEGAL AND MARKET ASPECTS OF ELECTRONIC SIGNATURES

Legal and market aspects of the application of Directive 1999/93/EC and practical applications of electronic signatures in the Member States, the EEA, the Candidate and the Accession countries

Jos Dumortier

Stefan Kelm

Hans Nilsson

Georgia Skouma

Patrick Van Eecke

Interdisciplinary centre for Law & Information Technology

KATHOLIEKE UNIVERSITEIT LEUVEN

Management Summary

1.1 Assignment and Methodology

The European Commission requested a study on the legal and practical issues concerning the implementation of EU Directive 1999/93 of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (the "Directive") and on the practical usage of electronic signatures and related services on the European market.

The study was performed by a team under the supervision of **Jos Dumortier**, Professor at the Faculty of Law and Director of the Interdisciplinary Centre for Law and Information Technology (ICRI) at the K.U.Leuven (Katholieke Universiteit Leuven). For legal aspects professor Dumortier worked together with his research fellow **Patrick Van Eecke** and with **Georgia Skouma** of the IT Law Unit of the law firm Landwell (Bogaert & Vandemeulebroeke, Brussels). For market and technical issues Professor Dumortier was assisted by **Hans Nilsson** (HN Consulting) and **Stefan Kelm** (Secorvo)*.*

The project's first objective was to provide an analysis of national legislation implementing the Directive in the EU Member States and to provide an analysis of the legal situation on electronic signatures in the EEA countries and the candidate countries, including relevant case law on the subject matter.

The project's second objective was to analyse the main practical and commercial usage of electronic signatures in the countries concerned, with a special focus on the technologies used, interoperability issues between products and services and the use of common standards in this field.

Based on information collected and an analysis of both the legal and practical issues relating to electronic signatures, recommendations were drafted for a possible modification of the Directive's scope in light of technological, market and legal developments.

The study resulted in different deliverables all of which are contained in this final report. They are:

1) a report on the implementation of Directive 1999/93 in the Member States and the legal status of electronic signatures and related services in the EEA countries and candidate countries, including conclusions and recommendations
2) the replies to the questionnaires from the national correspondents
3) a set of documents including all relevant national legislation and case law

4) a scorecard of national electronic signature applications, outlining their commercial and technical profile and their conformity with Directive 1999/93

5) a set of index cards ("fiches") outlining the legal status and practical applications of electronic signatures in all of the counties surveyed.

A quality review team assessed each deliverable on its legal and technical qualities before it was submitted to the European Commission.

In order to fulfil its tasks the research team worked together with a network of national correspondents based in the EU Member States, the EEA Countries, the Candidate and the Accession Countries. The correspondents were mostly lawyers with a sound knowledge of technical matters. They were chosen for their practical knowledge and for their understanding of electronic signature applications on use in their home market.

The correspondents were asked to respond to a questionnaire containing more than 200 questions relating to both the legal and the practical implementation of the electronic signatures Directive in their country. They were also asked to collect and send all relevant national legislation, case law and documentation on significant practical applications of electronic signatures to the research team. The correspondents consulted other related persons or organisations and administrations in their respective countries in order to ensure a comprehensive collection of the relevant data.

Having received the national feedback, the research team began its analysis of the legal and practical consequences of the implementation of the Directive. The team focussed on possible gaps in national legislation and on possible difficulties of implementation. The team also examined issues that are typical for more countries and which could hinder the practical implementation of electronic signatures and related services on both a national and on a pan-European level.

Furthermore, the team analysed the practical and commercial usage of electronic signatures in the different countries involved. The practical applications were assessed with an emphasis on commerce, technology, and related standards currently in use. Practical applications were also assessed based on their 'European directive-conformity'. This means that the researchers examined whether practical applications were in line with the legal requirements and recommendations of the Directive, such as conformity with the Annexes (type of certificate, type of CSP, type of signature creation and verification device).

An interim report was presented to the European Commission containing the first results of the study. The correspondents were invited to Brussels for a two-day workshop in order to present and discuss the preliminary results. The national correspondents were able to add their own remarks and to point out subtle nuances existing in their national legal and practical framework. Based on the correspondent's feedback and feedback from the Commission, the

research team updated and refined the deliverables and began to reflect on what conclusions and recommendations needed to be made.

When working on the conclusions, the research team paid particular attention to the technologies being used for generating electronic signatures, those markets most reliant on electronic signatures, the level of e-signatures cross-border use and the fine line drawn between licensing a certification service (forbidden by the Directive) and accrediting this service (allowed).

The analysis of current national legislation, best practices, case law and market efforts, lead to practical recommendations on how to adapt the current European legal framework on electronic signatures.

The final report was presented to the European Commission in Brussels by the research team in October 2003.

1.2 Findings and Recommendations

1.2.1 Findings

The study team discovered that most of the EU Member States have, more or less **faithfully, transposed** the Directive into national legislation. In addition, many of the non-EU countries surveyed have based their own electronic signatures and delivery of signature related services legislation on that of the EU Directive. From a technical point of view the Directive has even influenced international standardization initiatives, such as the IETF standardization work on Qualified Certificates. It is clear that the **Directive has influenced** legal and technical activities outside of the European Union boundaries. Remarkably, new terminology introduced by the Directive (especially Qualified Certificate, Advanced Electronic Signature, Certification Service Provider) has been taken on board by the EEA countries, Switzerland, the Accession and the Candidate countries.

Although the broad lines of the Directive have been respected by the Member States when transposing the Directive, a number of issues have nevertheless been identified as problematic. These problems can mainly be attributed to a misinterpretation of the Directive's wording, which in turn leads to divergences in national laws and/or divergences in the practical application of the rules.

Regarding the market access rules as stipulated by Article 3 of the Directive, the following remarks need to be made. The good news is that for the moment, none of the Member States surveyed submit the provision of certification services by providers established in another Member State to **prior authorization**, thus formally respecting Article 3.1 on market access. It is, indeed, perfectly possible for a CSP established in one Member State to provide

certification services in another Member States, without having to ask the prior permission of a national authority. This was not possible everywhere in Europe before the Directive was issued and transposed.

On the other hand, various Member States have established **supervision schemes** that are very close to prior authorization, and are possibly infringing Article 3.1 provisions. Given that CSPs have been established in all but a few of the countries surveyed and given that the majority of supervision schemes are still in the very early stages of development, it is impossible to compare yet the practical implications of the supervision systems. Nevertheless, it has become obvious that there are very important divergences between the various supervision schemes in the Member States. Although the effect of these divergences remains limited, since most of the CSPs still operate exclusively in their home country, the divergences will begin to show a negative impact once European or non-European providers start to launch more cross-border certification services across the EU.

Also, the Directive's rules on **voluntary accreditation** seem to be misunderstood by national governments. Many European countries wrongfully consider voluntary accreditation schemes as a means of controlling whether or not a Certification Service Provider operates in compliance with the provisions of the Directive. Another alarming observation is that the voluntary accreditation schemes, in many European countries, are in practice, not really voluntary. A typical example being that many national e-government programmes only accept accredited CSPs to participate in the programme, and thus indirectly oblige a CSP to get an accreditation. This evolution is certainly not in line with the Directive's vision.

Concerning the so-called "**public sector exception**" of Article 3.7, which allows Member States to make use of electronic signatures in the public sector subject to possible additional requirements, we have seen divergences in both the interpretation and implementation of this provision. It seems clear that in many countries the use of electronic signatures in the public sector is subject to additional (security) requirements. Communicating electronically with public authorities is in many European countries possible only through the use of signatures based on Qualified Certificates issued by an accredited CSP. Member States need to be reminded that applying additional conditions can only be justified by objective reasons and should only relate to the specific characteristics of the application concerned. Also, Member States need to ensure that basic competition rules are not being infringed by their initiatives.

As to the **conformity assessment of secure signature-creation devices** many countries seem quite reluctant to designate their own designated bodies for SSCD assessment. This may be due to the very high SSCD security requirements and the lack of active vendors in most countries. Another reason is the very large resources needed for operating an assessment body. The process of assessing a product is usually extremely expensive as well as time-consuming. Two further reasons why vendors are sometimes reluctant to have their products assessed is that an assessment is usually only valid for a fairly short amount of time

(the product needs to be re-assessed), and a conformity assessment "freezes" a product so that it cannot be changed (e.g., in order to apply a security patch) without making invalid the assessment. Consequently, although there already are a small number of SSCDs which have been assessed; all of these have been assessed by a relatively small number of designated bodies. Only in Austria, Germany and the Czech Republic has the number of products assessed been higher than two. In some countries (Austria, Germany) signature products other than SSCDs have been assessed as well.

The **non-discrimination principle of electronic signatures**, as regulated by Article 5.2 of the Directive, has been taken over by most of the national legislators. However, the transposition of Article 5.2 has not always been explicitly done and in those countries with an explicit transposition the scope of Article 5.2 has not always been covered in its entirety. It is not yet clear whether this rather vague transposition in some countries will have a practical impact on the legal use of electronic signatures. Thus, how electronic signatures will be treated in future national legislation and case law requires close monitoring.

It would be too premature to jump to early conclusions on judges' position vis-à-vis electronic signature given that to date there are but a few legal cases on this subject. Indeed, until recently, the sample of **case law** tackling directly or simply evoking electronic signatures issues is still too small and fragmented to be considered as representative enough of the judge's mind in this area.

As to the **legal effect of Qualified Electronic Signatures** (the ones regulated by Article 5.1 of the Directive), there has been a general tendency in the majority of European countries to explicitly recognise the equivalence between a handwritten signature and a specific "type" of signature by imposing the same or slightly different conditions than the ones stipulated in Article 5.1. It is, however, important to know that the Directive obliges Member States only to make sure that a Qualified Electronic Signature is legally speaking treated in the same way as a handwitten signature, but that it does not regulate the legal use and consequences of a handwritten signature itself, and thus not the legal consequences of the Qualified Electronic Signature either. The legal use and consequences (which transactions need a signature, which evidential value is given to a signature, etc) remains a nationally regulated matter.

Qualified electronic signatures need to be in compliance with the requirements as stated by the first three **Annexes** of the Directive. It is, therefore, important that the Annexes are correctly transposed into national legislation. The implementation of **Annex I** is very similar in most of those countries surveyed. The only risk is related to interoperability problems which might occur if technical implementations of Annex I diverge by, for example, not using ETSI TS 101 862, or any other common format for encoding the requirements of Annex I. The Commission should therefore promote the use of interoperability standards for the technical implementations of Annex I. For the implementation of **Annex II**, implementation levels are sometimes quite varying, meaning that the establishment and running of a CSP will differ

considerably. Any organization wishing to establish a CSP business in several countries must therefore adapt itself to different requirements and procedures. Product vendors will also have difficulties building products for this very fragmented market. In addition, several countries put additional detailed and unnecessary requirements on the CSP, thus creating barriers for the establishment of a CSP. The Commission should therefore point out any unnecessary and excessive requirements for CSPs, which might be perceived as market obstacles. For the implementation of **Annex III**, there is also evidence of fragmentation. The requirements for SSCDs are, for example, much higher in Austria and Poland than in some other European countries. As far as **Annex IV** is concerned, Article 3.6 is very clear. The list contains only recommendations, which have to be taken into account by the Member States and the European Commission when they work together in order to promote the development and the use of signature-verification devices. They can certainly not be changed into obligatory requirements at a national level, as some Member States have done.

With very few exceptions, all European countries have provided for a special **liability** provision transposing Article 6 of the Directive into national legislation. Within the European Union, the respective liability clauses of the EU Member States have followed the wording and rationale of Article 6. In cases where transposition was not explicit, the general tendency has been to provide stricter liability clauses, by broadening the scope of application of the Article, notably, by extending the list of liability causes as laid down in the Directive.

All countries under examination have prescribed in their national laws rules on the legal recognition of **foreign Qualified Certificates** in their territory. Only Ireland, the UK and Malta, do not distinguish between domestic and foreign Qualified Certificates. Most of the EU and EEA countries have faithfully transposed the conditions of Article 7 into their national legislation. In the Accession and Candidate countries the situation appears to be somewhat more complicated.

The implementation of the **data protection** rules of Article 8 into national legislation apparently did not pose any real difficulties. Some countries, though, did not correctly implement article 8.2 of the Directive. In those countries, a CSP is not obliged to follow the stricter data protection rules, whereas a CSP established in another Member State must adhere to its national rules. This may give rise to complaints of unfair competition in that it could act as an obstacle trade within the internal market. Further discussion also needs to centre on whether the stringent rules of Article 8.2 for CPS issued certificates to the public, (such as obligation to for direct personal data collection), are realistic, given that most CSP data is obtained from third parties such as a local registration authority. The use of a **pseudonym** in a certificate is allowed in all but two of the countries surveyed. Only Estonian and Bulgarian electronic signature legislation forbids the use of pseudonyms in their national rules on Qualified Certificates. Many countries explicitly require the disclosure of real names to the public authorities upon request and under strict conditions.

An important question, which needs to be posed, is what the **use of electronic signatures in Europe** really is? The number of supervised and accredited CSPs issuing Qualified Certificates in the European countries varies considerably from country to country, with many countries having either no or only one CSP. In the few countries where any larger numbers of Qualified Certificates have been issued, this is almost exclusively due to some form or another of government promotion. There is currently no natural market demand for Qualified Certificates and related services. The largest application area in Europe for electronic signatures is generally linked to e-banking applications in a closed user environment, and thus outside the scope of the Directive. Within the scope of the Directive, very few applications are in use today and they are almost completely limited to e-government.

It is interesting to note that many application service providers currently on the market falsely believe that their applications require Qualified Electronic Signatures as a minimum in order to be legally compliant, leading to **unnecessary costs and complexity** on planning and designing for the use of Qualified Electronic Signatures.

Technology evolves rapidly and in the near future many electronic signature technical solutions will be based on **new technological developments**, such as new secure PC environments, mobile signatures and signature servers. Consequently, supervision bodies, designated bodies and others involved in the regulation of Qualified Electronic Signatures should look at these technologies with an open mind and not restrict security assessments to what is known and available today.

The lack of **interoperability**, both at national and cross-border level, is a big obstacle for market acceptance and the proliferation of electronic signatures. It has resulted in many isolated “islands” of electronic signature applications, where certificates from only one CA can be used for one application. In a few cases only can certificates from multiple CAs be used for multiple applications. Much more should therefore have been done earlier at a European level to promote interoperability.

The EESSI (European Electronic Signature Standardisation Initiative) programme has developed some **standards** that are Directive compliant. However, the delay in developing the standards and having their references published in the Official Journal, has led to a situation whereby several countries have either developed their own technical interpretations of the Directive, (leading to varying requirements in different countries), or else have waited for standards to be developed, leading to a vacuum for product and service vendors on the market. Not until the publication of references to standards in the Official Journal in July 2003 has there been any clarity on the standards acceptable to all Member States. Another risk relating to interoperability is that currently only one set of standards related to Qualified Electronic Signatures (based on PKI) currently exists, which may hinder further technologies being used for Qualified Electronic Signatures.

1.2.2 Recommendations

1.2.2.1 Introduction

Our first recommendation is not to amend the Directive. Such amendments would have to be considered as an ultimate solution, only to be used when all other measures are deemed to be insufficient. Amending the Directive is a long and cumbersome operation that should be avoided if at all possible. As with all EU Directives, the Electronic Signature Directive is by no means a perfect legal text. It is a compromise which has been reached after long and difficult negotiations between 15 Member States all of whom have very divergent views on these issues. Our main conclusion is that the text of the Directive is adequate enough to serve its purpose in the near future but that it needs re-interpretation and clarification.

1.2.2.2 General recommendation

- The primary aim of the Directive was to create a Community framework for the use of electronic signatures, allowing for the free cross-border flow of products and provision of services, together with a basic legal recognition of electronic signatures throughout the EU. This objective has clearly not entirely been met. However, this negative situation is not necessarily the fault of the Directive but rather due to the way in which it has been implemented by the Member States. Some of the Directive's provisions seem to have been, in part, misunderstood and the Member States, when transposing the Directive into national legislation, have not always taken the European perspective of the new regulatory framework into account. It is therefore our impression that, at this moment, there is a primary need for a consistent, clear and workable re-interpretation of the provisions of the Directive.
- In our view the Commission needs to first and foremost examine how a more "Community-focused" interpretation of the Directive could be supported. Of course the ultimate judge on the correct interpretation of European law provisions rests with the European Court of Justice. At the same time, however, the Commission is in a position to issue a non-binding document, which could considerably influence the electronic signatures scene in Europe. Such an instrument could be combined with realistic accompanying measures capable of being implemented in the short term.

1.2.2.3 Supervision of CSPs

- The European countries surveyed for this study appear to have difficulties in striking a balance between "appropriate supervision" of Certification Service Providers and the prohibition to submit their activities to prior authorization. It would therefore be useful to

publish guidelines on how the supervision can be organized in order to make it conform to the Directive's provisions.

- The European Commission can take action against Member States that have established a scheme for the supervision of CSPs leading to measures that have the equivalent effect as a prior authorization.
- The guidelines to be published by the European Commission can also be used to clarify a number of currently unresolved legal issues in this area. One of the most difficult questions is to know what the notion of "establishment on the territory" in practice means for a Certification Service Provider (for example, certificate issuer established in one Member State but collaborating with registration authorities, directory service providers, etc. in other Member States: who is in charge of the supervision?).
- Not all the Member States have established a scheme for the appropriate supervision of CSPs issuing Qualified Certificates to the public. The Commission can take action against these Member States, because this situation creates the possibility for CSPs established in those Member States to issue Qualified Certificates to the public in other Member States without being submitted to appropriate supervision.
- Ideally the supervision schemes in the Member States should be harmonized, at least to a certain degree. We think that efforts in this direction should be supported. The Commission should, in our view, discourage supervision of CSPs other than those issuing Qualified Certificates to the public.
- Since EESSI already has published a number of valuable documents in this area it is recommended that supervisory authorities be encouraged to make use of these specifications. In our view, however, the use of such specifications by supervisory authorities has to be closely monitored. The standardization documents describe possible paths to fulfil the requirements of the Directive, but should never be considered obligatory for CSPs wishing to issue Qualified Certificates to the public. If a CSP believes that he fulfils the requirements of the Annexes he should be free to issue Qualified Certificates to the public without asking authorization.

1.2.2.4 Voluntary accreditation

- Measures should be taken in order to clarify the vision of the European legislator with regard to voluntary accreditation schemes for Certification Service Providers. In our view, cross-border accreditation and diversification of the schemes should be encouraged. The Commission should, on the other hand, discourage as much as possible the establishment of *national* accreditation schemes for Certification Service Providers issuing Qualified Certificates to the public. 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.

- Given the scarcity of top experts in the area of information security and given the relatively small amount of CSPs, the Commission should stimulate the clustering of efforts on a Community level. The objective should be to establish a limited number of high quality European accreditation schemes, preferably focusing on or specialising in specific categories of certification services for application domains.

1.2.2.5 Secure signature-creation devices.

- Partly because the Directive currently sets very high requirements on SSCDs, such devices still rarely find their way to the market. In order to stimulate the production of secure signature-creation devices, the requirements for formal assessment need to be more flexible in the future. The procedures for obtaining a conformity declaration should be shorter and less costly. The European Commission should support every effort in this direction.
- As to the rules to be followed by the designated conformity assessment bodies, the Commission should provide coordination and guidance. The Commission Decision of 2000 on the minimum criteria when designating conformity assessment bodies is a valuable first step but needs to be pursued. The independent, transparent and non-discriminatory character of the assessment procedure should ideally be monitored.
- In the view of the authors of this study it is absolutely necessary to discourage the perception that it is an obligation to submit every SSCD to a lengthy Common Criteria influenced assessment performed by a designated body. Instead, limited evaluations, based on 50-100 pages of documentation and requiring 10-20 days of checking, need to be promoted. In not allowing self-assessment, an independent party should be able to assess the security claims (with respect to Annex III) as made by the vendor and check to some extent whether or not this is state of the art. The Commission should examine how it can tackle the obligation to submit an SSCD to a designated body for conformity assessment, currently existing in many Member States. Discouraging the too strict conformity assessment would allow for a larger variety of products while at the same time protecting the consumers.

1.2.2.6 Public sector exception

- The Commission should emphasize the conditions that are needed before the Member States can use the “public sector exception” of Art. 3.7 of the Directive. Member States should be made aware that the non-discrimination rule of Art.5.2 of the Directive applies not only to the private but also to the public sector.

- The Commission should examine in more detail the compliance of certain e-government initiatives not only in relation to the Electronic Signatures Directive's provisions but also in relation to general EU competition rules, particularly with a view on Art. 86 of the EC Treaty.
- More generally, it is necessary to perform a more detailed study on the Internal Market consequences of the e-government programmes of the Member States. There is a clear danger that these programmes will result in national barriers, fragmentation and interoperability.
- Efforts towards improvement of interoperability between e-government programmes and particularly between their electronic signature applications should be supported or initialised at a European level.

1.2.2.7 Qualified Electronic Signatures

- With regard to Art. 5.1 there is primarily a need for clarification about the scope of this provision. It should be made clear to all interested parties that 1) "Qualified Electronic Signature" is not a synonym of "legally valid electronic signature" and 2) fulfilling the requirements of a Qualified Electronic Signature is one – but by no means the only - way to get the rules on handwritten signatures applied.
- From a European perspective the success of Art. 5.1 depends entirely on the availability of a very well standardized and easily recognisable European "Qualified Electronic Signature, including not only criteria for creation devices and certificates but specifying the complete signature and verification chain.
- A standardized "Qualified Electronic Signature" should merely give users a presumption that a signature complying with this standard will be presumed equivalent to handwritten signatures throughout Europe.
- Member States should be discouraged from inserting references to "Qualified Electronic Signatures" in new legal texts. The concept of the "Qualified Electronic Signature" should be used mainly for its original purpose, namely to obtain automatic acceptance of electronic signatures and that the same provisions governing handwritten signatures apply to electronic ones.
- Member States should be made aware that the concept of the Qualified Electronic Signature" is mainly useful for cross-border transactions in Europe. It serves as a "passport" that guarantees in every Member State the application of the rules applicable to handwritten signatures.
- The Annexes have been more or less literally transposed into national legislation by virtually all the countries surveyed. The remaining task is to make sure that the

implementation gets streamlined throughout Europe. Every effort in this direction should be supported. National implementations of the Annexes have, on the other hand, to be firmly discouraged.

- The Commission may consider taking actions against those Member States who have not correctly transposed the Annexes by, for example, translating the recommendations of Annex IV into requirements for Qualified Electronic Signatures at a national level.

1.2.2.8 Non-discrimination rule

- With regard to the application of Art. 5.2 there is a primary need for clarification. All interested parties should be better informed about the objective and the scope of this provision.
- The Commission should systematically examine if the Member States have issued legislation referring to Qualified or Accredited Electronic Signatures and detect where such references don't comply with the rule of Art. 5.2.

1.2.2.9 Standardization

- The Commission and Member States must ensure that all Member States correctly implement presumption of conformity with standards referenced in the Official Journal. This is currently not the case everywhere.
- The Commission and Member States should encourage further work on standards related to Annex II (f) and Annex III, in order to promote the use of alternative technologies for Qualified Electronic Signatures. Although the present standards are mostly technology neutral (within the framework of PKI), they still favour the use of smart cards as SSCDs for example.
- The long-term maintenance of the standards referenced in the Official Journal must be ensured, either by transferring the current CWAs to a more permanent body, for example ETSI, or promote the CWAs to European Norms.
- The Commission must urgently ensure the acceptance of a common specification for algorithms and parameters, as well as a common maintenance procedure for that specification.
- The complex areas of archiving and long-term validation of electronically signed documents are often perceived as obstacles for the use of electronic signatures. The Commission should promote work on guidelines and standards in these areas.
- The Commission and the Member States should find mechanisms to promote/recommend the standards for interoperability already developed by ETSI within the framework of EESSI.

- The Commission should support the work being done in EUCLID and CEN Workshop on e-authentication, steering them towards developing appropriate European standards, taking into account the results from EESSI, pki Challenge and other projects.
- The Commission should promote or arrange a European forum for electronic signatures, directed towards CSPs, product vendors and application providers in order to stimulate development and use of standards, possibly also initiating the setting up of interoperability testing facilities.
- It is probably useful to systematically *scan* the existing standardization documents from a user's perspective. With regard to Qualified Electronic Signatures the aim of the standardization activities should be to develop the specifications of a solution that gives the user the possibility to use electronic signatures on a European-wide scale. Such a solution has to take into account *all* the aspects of an electronic signature, not only covering the whole signature chain but also taking care of typical users' concerns such as ease of use, language obstacles, cost considerations, etc.

1.2.2.10 Trust service providers

- The Directive is very strongly focused on one business model, which was the centre of the attention from 1998 and 2000 but which has progressively been replaced by a much more heterogeneous and complex market situation. The regulatory framework thus includes , for example, quite detailed rules for certificates providers but does not deal with other categories of certification providers. The regulatory needs relating to other categories of trust service providers are nevertheless at least as urgent as those with regard to certification service providers. There is, for example, a clear need for regulation dealing with archival service providers, or with registered mail services. From a users' perspective it is difficult to understand why such services remain completely unregulated, while at the same such a complex regulatory framework has been established for issuers of certificates. We, therefore, recommend undertaking studies about the need for regulation with regard to other categories of trust services.

1.2.2.11 Data protection

- Last but not least it is necessary to combine electronic authentication with personal data protection. The current European regulatory framework is very much focused on the use of identity certificates. In recent years, attention has shifted towards better privacy protection in the online environment. Research has been done on various possibilities combining electronic authentication with the needs for anonymity or the use of multiple virtual identities. The efforts of the European Union to promote advanced personal data protection for its citizens should not be contradicted by its regulatory framework for electronic authentication. Closer examination is needed on

the possibilities to combine anonymity and pseudonymity with the provisions of the electronic signatures Directive

Table of contents

MANAGEMENT SUMMARY

1.1 ASSIGNMENT AND METHODOLOGY 2
1.2 FINDINGS AND RECOMMENDATIONS 4
1.2.1 Findings 4
1.2.2 Recommendations 9
1.2.2.1 Introduction 9
1.2.2.2 General recommendation 9
1.2.2.3 Supervision of CSPs 9
1.2.2.4 Voluntary accreditation 10
1.2.2.5 Secure signature-creation devices. 11
1.2.2.6 Public sector exception 11
1.2.2.7 Qualified Electronic Signatures 12
1.2.2.8 Non-discrimination rule 13
1.2.2.9 Standardization 13
1.2.2.10 Trust service providers 14
1.2.2.11 Data protection 14

TABLE OF CONTENTS 16

TERMINOLOGY AND ABBREVIATIONS 23

INTRODUCTION 25

CHAPTER 1 THE EUROPEAN ELECTRONIC SIGNATURE DIRECTIVE 27

1.1 SCOPE OF THE DIRECTIVE (ARTICLE 1) 27
1.2 DEFINITIONS (ARTICLE 2) 29
1.2.1 (Advanced) electronic signature 29
1.2.2 Certificates and certification services 31
1.3 THE CERTIFICATION SERVICES MARKET (ARTICLES 3.1, 3.2, 3.3 AND 4.1) 36
1.3.1 Free circulation of certification services 36
1.3.2 No prior authorisation 37
1.3.3 Voluntary accreditation 38

1.3.4 Supervision 39
1.3.5 Public sector exception 40
1.4 ELECTRONIC SIGNATURE PRODUCTS (ARTICLES 3.4, 3.5, 3.6 AND 4.2) 41
1.4.1 Free circulation of electronic signature products 41
1.4.2 Secure signature-creation devices 45
1.4.3 Secure signature-verification devices 48
1.5 LEGAL EFFECTS OF ELECTRONIC SIGNATURES (ARTICLE 5) 48
1.5.1 Article 5.1 49
1.5.2 Article 5.2 50
1.6 LIABILITY (ARTICLE 6) 51
1.6.1 Qualified certificate 52
1.6.2 Issued to the public 52
1.6.3 "Guaranteed to the public" 53
1.6.4 Liability causes 53
1.6.5 Reasonable reliance 53
1.6.6 Absence of negligence 55
1.6.7 Limitation of liability 55
1.6.7.1 Limitation provisions of the EU-Directive 55
1.6.7.2 Liability limitation outside the Directive 56
1.6.7.3 Liability limitation statements 56
1.6.8 Business model behind Article 6 57
1.7 OTHER PROVISIONS 57
1.7.1 International aspects (Article 7) 57
1.7.2 Data protection (Article 8) 59
1.7.3 Committee (Article 9-10) 60
1.7.4 Notification (Article 11) 62
1.7.5 Review (Article 12) 62
1.7.6 Implementation (Article 13) 62

CHAPTER 2 THE TRANSPOSITION OF THE DIRECTIVE 63

2.1 DEFINITIONS (ARTICLE 2) 63
2.1.1 Electronic signature 63
2.1.2 Signatory 65
2.1.3 Certification service provider 66
2.1.4 Other definitions 67
2.2 LEGAL EFFECT OF E-SIGNATURES (ARTICLE 5) 68
2.2.1 Legally relevant electronic signatures 68

2.2.1.1 State of implementation in Europe 68
2.2.1.2 Conclusion 69
2.2.2 Electronic signatures equivalent to handwritten signatures (Article 5.1) 69
2.2.2.1 Reminder 69
2.2.2.2 State of implementation in Europe 70
2.2.2.3 Conclusion 76
2.2.3 Non-discrimination rule (Article 5.2) 77
2.2.3.1 State of implementation in Europe 77
2.2.3.2 Conclusion 79
2.2.4 Progress monitoring of relevant case law 80
2.2.4.1 Status of case law development 80
2.2.4.2 Description of developments on a country level 80
2.2.4.3 Conclusions 82
2.3 LIABILITY ISSUES (ARTICLE 6) 83
2.3.1 Transposition of the special liability clause 83
2.3.1.1 Reminder 83
2.3.1.2 State of implementation 83
2.3.2 Scope of implementing provisions 84
2.3.2.1 Description 84
2.3.2.2 Conclusion 86
2.3.3 List of liability causes 86
2.3.3.1 Description 86
2.3.3.2 Conclusion 89
2.3.4 Burden of proof 90
2.3.4.1 Description 90
2.3.4.2 State of implementation 90
2.3.5 Limitations of liability 91
2.3.5.1 Description 91
2.3.6 General Conclusion 91
2.4 INTERNATIONAL ASPECTS (ARTICLE 7) 92
2.4.1 Overview of the transposition into national law 92
2.4.2 Conclusions 94
2.5 DATA PROTECTION (ARTICLE 8) 95
2.5.1 Basic data protection rules (Article 8.1) 95
2.5.2 Specific data protection rules (Article 8.2) 96
2.5.3 Use of pseudonyms (Article 8.3) 97
2.5.4 Other national data protection rules 98
2.6 PUBLIC SECTOR (ARTICLE 3.7) 99

2.7 CONTROLLING MECHANISMS (ARTICLE 3) 99
2.7.1 Prior authorisation (Article 3.1) 99
2.7.2 Notification of CSPs 100
2.7.3 Supervision (Article 3.3) 101
2.7.4 Voluntary accreditation (Article 3.2) 104
2.7.5 Conformity assessment of SSCDs (Article 3.4) 106
2.7.6 Summarizing table 108
2.8 TRANSPOSITION OF THE ANNEXES 110
2.8.1 Annex I: Qualified Certificates 110
2.8.2 Annex II: CSPs issuing Qualified Certificates 110
2.8.3 Annex III: Secure Signature-Creation Devices 111
2.8.4 Annex IV: Secure Signature Verification 112
2.8.5 Products for signature creation and verification 113
2.9 NOTIFICATION TO THE COMMISSION (ARTICLE 11) 114

CHAPTER 3 STANDARDIZATION ASPECTS OF ELECTRONIC SIGNATURES 116

3.1 THE EESSI FRAMEWORK 116
3.1.1 Background 116
3.1.2 Impact of EESSI standardization 118
3.2 THE NEED FOR STANDARDS 118
3.2.1 The need for security standards related to Qualified Electronic Signatures 119
3.2.2 The need for interoperability standards 119
3.3 PRESUMPTION OF CONFORMITY FOR QUALIFIED ELECTRONIC SIGNATURE STANDARDS 120
3.4 PROMOTION OF INTEROPERABILITY THROUGH STANDARDS 121
3.4.1 Promotion by the Commission 121
3.4.2 National promotion of interoperability 122
3.5 ALGORITHMS AND PARAMETERS FOR ELECTRONIC SIGNATURES 123
3.6 TERMINATION OF CSP OPERATION 123
3.7 CERTIFICATE DIRECTORIES 124
3.8 ROOT CAS AND BRIDGE CAS 124
3.9 CONCLUSIONS 125

CHAPTER 4 ELECTRONIC SIGNATURES IN PRACTICE 127

4.1 THE MARKET FOR ELECTRONIC SIGNATURE PRODUCTS AND SERVICES 127
4.1.1 Products in use 127
4.1.2 Number of CSPs and certificate volumes 128

4.1.3 Volumes of issued certificates *129*
4.1.3.1 Certificates issued by accredited and supervised CSPs 129
4.1.3.2 Other certificates issued to the public 130
4.1.3.3 Other certificates issued under contractual agreement 130
4.1.3.4 Revocation of certificates 130
4.1.4 Use of smart cards *130*
4.1.5 Other CSP services *130*
4.1.6 Archiving of electronically signed documents *130*
4.1.7 Security problems *131*
4.2 APPLICATIONS IN USE 131
4.2.1 Types of applications *131*
4.2.2 Types of certificates and signatures *132*
4.2.3 Use of CSPs *132*
4.2.4 Costs *133*
4.2.5 User identities *133*
4.2.6 User software and hardware *133*
4.3 PROBLEMS IDENTIFIED WITH PKI 134
4.4 ALTERNATIVES TO PKI FOR ELECTRONIC SIGNATURES 135
4.5 NEW TECHNOLOGICAL DEVELOPMENTS 135
4.6 CONCLUSIONS 137

CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS 139

5.1 INTRODUCTION 139
5.2 THE OBJECTIVES OF THE DIRECTIVE 140
5.3 STIMULATING THE INTERNAL MARKET 141
5.3.1 Certification services *141*
5.3.2 Supervision of CSPs *142*
5.3.3 Voluntary accreditation *144*
5.3.4 Conformity assessment of SSCDs *146*
5.3.5 E-government *148*
5.4 PROMOTING LEGAL ACCEPTANCE OF ELECTRONIC SIGNATURES 150
5.4.1 Qualified electronic signatures *150*
5.4.2 Implementation of the Annexes *154*
5.4.3 Non-discrimination (Article 5.2) *156*
5.5 CREATING A FAVOURABLE CLIMATE 158
5.5.1 Effect on the market *158*
5.5.2 Standardisation *158*

5.5.3 Taking a user's perspective *160*

APPENDIX 1: NATIONAL QUESTIONNAIRES **162**

APPENDIX 2: COLLECTION OF RELEVANT LEGISLATION AND CASE LAW **163**

APPENDIX 3: SCORECARDS OF APPLICATIONS FOR ELECTRONIC SIGNATURES **164**

APPENDIX 4: COUNTRY INDEX CARDS **172**

COLLECTION OF WEB LINKS 173
AUSTRIA 174
BELGIUM 177
DENMARK 179
FINLAND 182
FRANCE 186
GERMANY 189
GREECE 192
IRELAND 195
ITALY 198
LUXEMBOURG 201
NETHERLANDS 204
PORTUGAL 207
SPAIN 209
SWEDEN 212
UNITED KINGDOM 215
CYPRUS 218
CZECH REPUBLIC 220
ESTONIA 223
HUNGARY 226
LATVIA 229
LITHUANIA 231
MALTA 233
POLAND 236
SLOVAKIA 239
SLOVENIA 241
BULGARIA 243
ROMANIA 246
ICELAND 248
LIECHTENSTEIN 250
NORWAY 253

SWITZERLAND 256

APPENDIX 5: PRESENTATION OF THE RESEARCHERS 259

PRESENTATION OF THE RESEARCH TEAM 259
PRESENTATION OF THE QUALITY CONTROL TEAM 260
PRESENTATION OF THE CORRESPONDENTS 261
EU countries 261
EEA countries & Candidate countries 262

Terminology and Abbreviations

Terminology

EU Member States	Current 15 Member States
Accession countries	The 10 countries set to join the EU in 2004
Candidate countries	Bulgaria and Romania
EEA countries	Iceland, Liechtenstein, Norway
Qualified Electronic Signature	Signature according to Article 5.1 of the Directive

Abbreviations

AES	Advanced Electronic Signature
CA	Certification Authority
CC	Common Criteria
CEN	Comité Européen de Normalisation
CRL	Certificate Revocation List
CSP	Certification Service Provider
CWA	CEN Workshop Agreement
EEA	European Economic Area
EESSI	European Electronic Signature Standardization Initiative
ETSI	European Telecommunication Standards Institute
EU	European Union
ICTSB	ICT Standards Board
IETF	Internet Engineering Task Force
ISO	International Standards Organisation

OCSP	Online Certificate Status Protocol
OJ	Official Journal of the European Communities
PDA	Personal Digital Assistant
QC	Qualified Certificate
QES	Qualified Electronic Signature
QCP	Qualified Certificate Policy (ETSI TS 101 456)
RA	Registration Authority
SIM	Security Identity Module
SSCD	Secure Signature-Creation Device

Introduction

This study has been structured on three core components. These components analyse the opinions and findings of the research team and relate to the following issues:

- Content description and basic interpretation of the Directive's articles [Chapter 1]
- An overview of the Directive's implementation into national legislation in those European countries here surveyed [Chapters 2, 3 and 4]
- Reflections on the objectives of the Directive and the achieved results, taking into account the way in which such objectives have been translated in national legal systems and in market practices [Chapter 5].

Background material and explanatory tables illustrating the findings are contained in the accompanying Appendices (see description below).

Chapter 1 discusses the main goals and content of the Directive article-by-article. The aim of such an analysis is to help the reader understand, through an objective description of the Directive's content, the *raison d'être* of the Directive and the main challenges the national legislator has been confronted with when interpreting or transposing the Directive. The analysis devoted to each article is as objective and neutral as possible. This Chapter gives a brief but essential overview of all thirteen of the Directive's Articles, including Annexes, and serves as a reference point for the following Chapters.

Chapter 2 looks into the implementation of the Directive in thirty-one European countries (EU Member States, EEA, Accession and Candidate Countries and Switzerland). It depicts article by article the way in which these countries have conceived and interpreted the Directive's provisions, as well as the solutions that they have elaborated. This Chapter does not seek to be an exhaustive and overly detailed description of the laws of each country relevant to electronic signatures. The focus was primarily to highlight the differences from the common interpretation of the Directive and striking elements that have been found in the national laws under examination. On many occasions, the objective description of the transposition of a given article in national legal systems is followed by a brief set of conclusions.

This information is complemented by a list of country "fiches" in Appendix 4. The "fiches" are a kind of summary of the implementation of the Directive in each of the countries surveyed and tackle the core provisions of the Directive. The findings described in Chapter 2, as well as the country fiches, have been collected with the help of a detailed questionnaire and accompanying literature sent to us by national correspondents.

Chapter 3 outlines the role of standardization in the implementation of the Directive. It starts with a brief description and evaluation to the first Europe-wide initiative in standards setting in the area of electronic signatures (EESSI). It then goes on to discuss the need for

interoperability as laid down in the Directive and the way in which interoperability requirements may be (have been) satisfied by standards. Further, it refers to the efforts made by the EU Commission or at a national level to promote the deployment of interoperable electronic signatures solutions.

Chapter 4 gives an overview of the practical and commercial usage of electronic signatures in the countries under examination. First, it identifies the most significant electronic signature applications that are currently deployed in each country, with an emphasis on PKI technology. Second, it provides preliminary reflections on the difficulties felt by the market to support full implementation of PKI solutions compared to other technology alternatives.

This Chapter is accompanied by a set of "scoreboards" in Appendix 3, illustrating the commercial and technical features of the electronic signature applications that have been identified on a country basis.

The core conclusions in the light of the analysis of the preceding Chapters are discussed in Chapter 5. It is a synthesis of constructive remarks and recommendations taking into account the Directive's rationale and objectives and the legal/market progress that has been scrutinised in the previous parts.

Chapter 1 The European Electronic Signature Directive

This study begins with an analysis, "article by article", of EU Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Where appropriate, the analysis of the Directive also refers to standardization documents developed in the context of the EESSI.

1.1 Scope of the Directive (Article 1)

According to Article 1 the purpose of the Directive is 1) to facilitate the use of electronic signatures and to contribute to their legal recognition and 2) to establish a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market. The Directive has, in other words, a dual objective.

As far as the first objective is concerned, Article 1 is formulated in a prudent manner. The Directive does not contain an overall regulation of electronic signatures. Rather it aims to merely "facilitate their use. Nor does the Directive intend to cover entirely the question of legal recognition of electronic signatures. It only seeks to "contribute".

The second objective is to create a common European legal framework in order to avoid divergent national laws in this domain. During our analysis of the provisions of the Directive we will discover what is meant by the term "legal framework" in this respect. The framework does not cover all kinds of certification services but only "certain" of these services. We will see that the framework is in the first place more concerned with certificate *issuers* and much less with other categories of Certification Service Providers.

Article 1 specifies further that the Directive "does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Community law". Recital (17) specifies that the Directive "does not seek to harmonise national rules concerning contract law, particularly the formation and performance of contracts, or other formalities of a non-contractual nature concerning signatures. For this reason the provisions concerning the legal effect of electronic signatures should be without prejudice to requirements regarding form laid down in national law with regard to the conclusion of contracts or the rules determining where a contract is concluded". The Directive does consequently not affect national provisions requiring, for instance, the use of paper for certain types of contracts.[1]

[1] The elimination of legal obstacles for the conclusion of contracts by electronic means is the subject of Article 9 of the "Electronic Commerce Directive".

Article 1 further provides that the Directive does not affect rules and limits, contained in national or Community law, governing the use of documents. Many provisions in the law of the Member States impose the use of particular forms, for instance for tax declarations, building permits, etc. Sometimes the law requires that documents be archived for a certain period of time. As long as these laws do not permit the use of electronic forms or electronic document archiving, electronic signatures cannot be used in these domains.

In Recital (16) we can read that the Directive "contributes to the use and legal recognition of electronic signatures within the Community; a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law between a specified number of participants; the freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data should be respected to the extent allowed by national law; the legal effectiveness of electronic signatures used in such systems and their admissibility as evidence in legal proceedings should be recognised." In the explanatory memorandum of the draft Directive, the Commission justifies this as follows: "There are obvious applications of electronic signature technology in closed environments, e.g. a company's local area network, or a bank system. Certificates and electronic signatures are also used for authorization purposes, e.g. to access a private account. Within the constraints of national law, the principle of contractual freedom enables contracting parties to agree among themselves the terms and conditions under which they do business, e.g. accept electronic signatures. In these areas, there is no evident need for regulation".[2]

One of the primary aims is to guarantee the interoperability of electronic signature products. Essential requirements specific to electronic-signature products must be met in order to ensure free movement within the internal market and to build trust in electronic signatures, but Recital (5) stresses this has to be done without prejudice to Council Regulation 3381/94/EC of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods and Council Decision 94/ 942/CFSP of 19 December 1994 on the joint action adopted by the Council concerning the control of exports of dual-use goods. Moreover the Electronic Signature Directive does not harmonise the provision of services with respect to the confidentiality of information where national provisions concerned with public policy or public security cover them.[3]

[2] Proposal for a European Parliament and Council Directive on a common framework for electronic signatures, COM(98)297final, p. 6.

[3] See Recital (6).

1.2 Definitions (Article 2)

1.2.1 (Advanced) electronic signature

Before the Commission issued its first version of the draft Directive in May 1998, all the European documents regarding this subject, used the term “digital signature”. In the original draft Directive of May 1998, the European Commission started to use “electronic” signature. The definition of “electronic signature” in the first draft was however still more or less identical with the present definition of an “advanced” electronic signature.

In the final text the term “electronic signature” has been given an extremely wide sense: “data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication”. Recital (8) justifies this approach, stating that “rapid technological development and the global character of the Internet necessitate an approach which is open to various technologies and services capable of authenticating data electronically”. The same recital makes it also clear that the term “electronic signature” relates to “data authentication” and does not cover methods and technologies for “entity authentication”. For example, entering a PIN-code to get access to an electronic bank account will not fall within the scope of the “electronic signature” definition. Entering the same code in order to confirm a financial transaction, on the contrary, is an example of data authentication and is therefore considered as an electronic signature.

Notwithstanding the very wide definition it has to be kept in mind that the notion of “signature” as it is used in the Directive, refers to a legal and not to a technical concept. The objective of the definition is to cover not only all current and future technologies that can be used for electronic signatures, but also to include all possible meanings of the term “signature” in the law of the Member States. It is well known that the term “signature” has not the same legal meaning in every Member State of the Union. For example, a printed name or even a company stamp on a document, will be considered as a valid legal signature in the U.K. whereas the notion of “signature” in France, Belgium or Germany – until recently at least – only included handwritten signatures. One could say that the “electronic signature” definition adopted in the Directive is the greatest common denominator of all “signature” concepts that are used in the laws of the Member States.

It is very probable that the legal concept of the “signature” will evolve and broaden with the increasing use of electronic signatures, but it remains nevertheless important to clearly distinguish it from the technical concept of a (digital) signature. Many applications that make use of digital signature technology will not be considered as electronic signatures by the law in the Member States. The distinction between the two concepts is particularly important in

applications making use of digital signature technology for both entity authentication (for example, to control access to a web portal) and for the creation of electronic signatures.[4]

Fortunately, the very wide definition of the term "electronic signature" does not have many legal consequences because, except in Article 5.2, all the provisions of the Directive are dealing with "advanced" or with so-called "qualified" electronic signatures. And it is precisely the aim of Article 5.2 – as we will see later on in this report – to prohibit "a priori" rejection of any kind of electronic signature anyway. In all cases where an electronic signature – in the widest sense – is presented to a court or a public administration, its meaning and its scope will have to be examined on a case-by-case basis.

An "Advanced Electronic Signature" is an electronic signature meeting the following four requirements:

1. uniquely linked to the signatory;
2. capable of identifying the signatory;
3. created using means that the signatory can maintain under his sole control; and
4. linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Everybody will notice that these requirements are formulated in a very general and technology-neutral manner. In practice however, the definition refers mainly to electronic signatures based on digital signature technology or, in other words, making use of public key cryptography. In the framework of EESSI, a format for Advanced Electronic Signatures has been described in the ETSI Technical Specification (TS 101 733). It is based on the existing standard format that dominates the e-mail and document security market (i.e. Internet specification RFC 2630). It also specifies how time-stamping or trusted archiving services may be used to ensure that the electronic signature remains valid for long periods so that it can be later presented as evidence in the case of a dispute. The document defines how the Internet specification RFC 2630 cryptographic message syntax should be used for Advanced Electronic Signatures and defines additional fields and procedures, which are compatible with this syntax, to support long term validity. The evidence provided through use of the ETSI format protects against the signatory later attempting to deny (repudiating) having signed a document, and can be verified even after the validity of the supporting certificate expires.[5]

A "signatory" is defined as "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". The

[4] Examples can be found in the "electronic identity card" projects, for instance in Finland or Belgium. The card contains two keypairs: one for access control (entity authentication) and one for electronic signatures (data authentication).

[5] ETSI TS 101 733 "Electronic Signature Formats", V.1.4.0 is available at http://portal.etsi.org/esi/el-sign.asp

European Parliament suggested here to specify that a signatory could only be a "natural" person but this amendment was not integrated in the final text. The probable reason for this is that in some Member States, such as the United Kingdom, a document is not only considered to be "signed" if it contains a handwritten signature by a natural person but also when it bears a company's seal, a stamp or simply a name, as long as the authentication is sufficiently clear.[6] Nevertheless it seems to us that, although it is true that an electronic signature does not necessarily need to be attributed to a natural person – other entities can also "sign" -, the "signatory" will always be the (natural) person who "holds" the signature-creation device. Even in countries where, for example, signatures can be directly attributed to legal persons, it remains necessary, from a legal point of view, to identify the natural person(s) who actually activated the device in order to generate the signature.

Contrary to the original draft the signatory is no longer "the person who creates an electronic signature": It is the person who holds the signature-creation device. Such a device is defined in Article 2.5 as: "configured software or hardware used to implement the signature-creation data". A common example of a signature-creation device is a *smart card* but there are many other possible devices such as a *smart pen*, a mobile phone, a PDA or a computer hard disk. The signatory is the person who holds this device and who acts in order to generate a signature. The signature can be either on behalf of the signatory himself or on behalf of a natural or legal person or entity he represents.

Signature-creation data are "'unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature". The term "signature-creation data" consequently refers to the private key, whereas "signature-verification data" – defined as "data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature" – is used as a technology-neutral synonym for the public key. The software or hardware used to verify the public key is called "signature-verification device".

Signature-creation devices and signature-verification devices are both part of the more general category of "electronic signature products". These are defined in Article 2.12 as "hardware or software, or relevant components thereof, which are intended to be used by a Certification Service Provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures".

1.2.2 Certificates and certification services

Article 2.9 defines a "certificate" as "an electronic attestation which links signature-verification data to a person and confirms the identity of that person". A "Qualified Certificate" is "a certificate which meets the requirements laid down in Annex I and is provided by a

[6] Chris Reed, "What is a signature?", JILT 3000/3, available at http://elj.warwick.ac.uk/jilt/00-3/reed.html

Certification Service Provider (CSP) who fulfils the requirements laid down in Annex II of the Directive.

Annex I lists ten requirements for Qualified Certificates. They must contain:

(a) an indication that the certificate is issued as a Qualified Certificate;

(b) the identification of the Certification Service Provider and the State in which it is established;

(c) the name of the signatory or a pseudonym, which shall be identified as such;

(d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;

(e) signature-verification data which correspond to signature-creation data under the control of the signatory;

(f) an indication of the beginning and end of the period of validity of the certificate;

(g) the identity code of the certificate;

(h) the Advanced Electronic Signature of the Certification Service Provider issuing it;

(i) limitations on the scope of use of the certificate, if applicable; and

(j) limits on the value of transactions for which the certificate can be used, if applicable.

The ETSI Technical Specification (TS 101 862) defines how the X.509 public key certificate format, which dominates the public key infrastructure market, may be used to meet the requirements of Annex I of the Directive. In addition, where there is currently no defined mechanism for meeting a requirement (e.g. limits on the value of the transaction) the specification builds on the existing extension capabilities of X.509 to define the necessary optional data structures.[7]

Certification-service-providers issuing Qualified Certificates must, following Annex II:

(a) demonstrate the reliability necessary for providing certification services;

(b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;

(c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;

[7] ETSI TS 101 862 V.1.2.1 (2001-06) is available at http://webapp.etsi.org/exchangefolder/ts_101862v010201p.pdf

(d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a Qualified Certificate is issued;

(e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;

(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;[8]

(g) take measures against forgery of certificates, and, in cases where the Certification Service Provider generates signature-creation data, guarantee confidentiality during the process of generating such data;

(h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;

(i) record all relevant information concerning a Qualified Certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

(j) not store or copy signature-creation data of the person to whom the Certification Service Provider provided key management services;

(k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily

[8] The security requirements for trustworthy systems managing certificates for electronic signatures have been specified in two related CEN Workshop Agreements (CWAs). The first, CWA 14167 Part 1, specifies overall security requirements on trustworthy system components, used by Certification Service Providers (CSPs), to create standard Qualified Certificates. The second, CWA 14167 Part 2, defines specific requirements on the CSP's cryptographic modules. By conforming to these specifications, a CSP's systems and its cryptographic devices fulfil the requirements for trustworthy systems stated in point f) of the Annex II of the Directive. The Workshop Agreements relating to electronic signatures are available at http://www.cenorm.be/cenorm/businessdomains/businessdomains/informationsocietystandardizationsystem/published+cwas/cwa+download+area.asp

understandable language. Relevant parts of this information must also be made available on request to third parties relying on the certificate;

(l) use trustworthy systems to store certificates in a verifiable form so that:

- only authorised persons can make entries and changes,
- information can be checked for authenticity,
- certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
- any technical changes compromising these security requirements are apparent to the operator.

ETSI Technical Specification (TS 101 456) defines security management and policy requirements for Certification Service Providers issuing Qualified Certificates. It defines two specific policies for: 1) CSPs issuing Qualified Certificates to the public, and 2) CSPs issuing Qualified Certificates to the public requiring use of a secure signature-creation device. In addition, it defines a general framework for other policies for CSPs issuing Qualified Certificates including those applicable to closed communities.[9]

Article 2.9 of the Directive contains a very broad definition of the concept of "Certification Service Provider": "an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures". Recital (9) justifies this by stating that "electronic signatures will be used in a large variety of circumstances and applications, resulting in a wide range of new services and products related to or using electronic signatures; the definition of such products and services should not be limited to the issuance and management of certificates, but should also encompass any other service and product using, or ancillary to, electronic signatures, such as registration services, time stamping services, directory services, computing services or consultancy services related to electronic signatures."

According to Recital (12) the CSP has to be established in accordance with national law. Member states are free to establish a state-controlled entity as a CSP. A state-controlled CSP can be created in different forms depending on the administrative law of the respective member state. In most cases of public entities, there is a choice between establishing the CSP as part of the administration, as a state-controlled legal person or as a private legal person that is mainly owned by the government. The suitable form for creating this type of certification service provider will depend on the extent of state control to be exercised over it.

[9] ETSI TS 101 456, V 1.2.1 (2002-04) is available at http://webapp.etsi.org/exchangefolder/ts_101456v010201p.pdf

Of course, in case a member state sets up a state-controlled CSP, it will have to take into account the application of European and national competition rules.[10]

Although it is theoretically possible for a natural person to offer certification services, the organizational and administrative efforts to be made will usually require the set up of a corporation. However, it might be possible for a natural person to act as sub-entity of another CSP, for example as a registration authority. In most cases where natural persons assume the role of a trusted third party they do not act for themselves but as representatives of another entity. For example, if a CEO of a certain company issues certificates to the employees of that company, he acts on behalf of the company and not for himself as a natural person. In the few cases in which a natural person might actually become a CSP no act of incorporation is necessary.

The most common form of providing certification services is through a private legal person. Regarding their organisation, CSPs can also be a sub-entity of another corporation or an association consisting of other sub-entities. The available and suitable forms of corporations depend on the law of the country in which the certification service provider will be established. As is the case for all businesses, the most suitable form of corporation to conduct the business has to be decided by taking into consideration a number of factors. The main factors include the applicable tax regulations and liability limitations, the size of the corporation, the available capital etc.

Although the Directive does not explicitly prescribe the relationship between a CA (Certification Authority) and a RA (Registration Authority), there is an underlying assumption in the Directive that the CSP covers both of these functions or, more precisely, that both functions are accomplished under the responsibility of the CSP issuing the certificates.

[10] Article 86 of the EC Treaty is of particular importance In this context. The first two paragraphs of this Article are as follows:

"1. In the case of public undertakings and undertakings to which Member States grant special or exclusive rights, Member States shall neither enact nor maintain in force any measure contrary to the rules contained in this Treaty, in particular to those rules provided for in Article 12 and Articles 81 to 89.

2. Undertakings entrusted with the operation of services of general economic interest or having the character of a revenue-producing monopoly shall be subject to the rules contained in this Treaty, in particular to the rules on competition, in so far as the application of such rules does not obstruct the performance, in law or in fact, of the particular tasks assigned to them. The development of trade must not be affected to such an extent as would be contrary to the interests of the Community."

1.3 The certification services market (Articles 3.1, 3.2, 3.3 and 4.1)

1.3.1 Free circulation of certification services

The central provision concerning certification services – in its widest sense – is Article 4.1 of the Directive. It provides that each Member State shall apply the national provisions, which it adopts pursuant to the Directive, to Certification Service Providers established on its territory and to the services they provide. Member States may not restrict the provision of certification services originating in another Member State in the fields covered by this Directive.

Article 4 introduces, in other words, the "country of origin" principle for certification services. Certification service providers are submitted to rules of the country in which they are established (their "country of origin"). They do not have to take into account the rules of all the European countries in which they provide their services. Once they respect the rules of the country in which they are established, their services have to be considered in line with the rules of all the Member States in which they operate. In every Member State, providers originating in other Member States should have the same chances for providing their services as the providers established in the Member State, particularly in the fields covered by the Directive. Especially supervision or accreditation schemes should never lead to legal or practical restrictions for the provision of certification services by providers established in other Member States.

The notion of establishment has been developed by the European Court of Justice in the context of the freedom and the right of establishment, as guaranteed in Article 43 of the European Community Treaty. In the *Gebhard* case, the Court states that "the concept of establishment within the meaning of the Treaty is a very broad one, allowing a Community national to participate, on a stable and continuous basis, in the economic life of a Member State other than his state of origin and to profit there from, so contributing to economic and social interpenetration within the Community in the sphere of activities as self-employed persons".[11]

The essential requirements for an establishment seem to be (i) a fixed, i.e. a stable and permanent establishment[12], (ii) for an indefinite period, (iii) in another Member State than the state of origin, and (iv), the actual pursuit of an economic activity.[13]

---

[11] *Gebhard v Consiglio dell' Ordine degli Avvocati e Procuratori di Milano* (Case C-55/94)[1995] ECR I-4165, para. 25;

[12] *INASTI v Kemmler* (Case C-53/95) [1996] ECR I-704, para 8.

[13] *R.v Secretary of State for Transport, ex p. Factortame* (Case C-221/89) [1991] ECR-I-3905, para 20;

The meaning of 'establishment' has to be seen in contrast with the notion of 'provision of services' of Article 49 of the European Community Treaty.[14] In essence, the difference concerns the temporary nature of the provision of services in another Member State than the state of origin. The temporary nature of the activities has to be determined in the light, not only of the duration of the provision of the service, but also of its regularity, periodicity and also its continuity.[15] The fact that the provider is equipped with some form of infrastructure does not necessarily mean that the temporary aspect of the services is lost.

If a Certification Service Provider is only established in one Member State, he will be submitted to the legal provisions enacted in that Member State in the field of the Directive. The law of that Member State will also be applicable to services provided in other Member States. A CSP established in Belgium, for example, will remain under the supervision of the Belgian laws even if he provides the majority of his services in other Member States. The other Member States are not allowed to restrict the provision of the services of the Belgian provider, even if the Belgian legal rules in the field of the Directive are less strict. If the CSP is established in more than one Member State, he will be submitted to the laws of all these Member States.[16]

1.3.2 No prior authorisation

Article 3.1 prohibits Member States to make the provision of certification services subject to prior authorisation. Recital (10) specifies that "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."

The consequence is that any Certification Service Provider will have to be allowed to provide his services without prior authorisation. At the same time the Directive requires the EU-

[14] P. Craig, G. De Burca, *EU Law, Text, Cases and Materials*, 1998,Oxford University Press, 728;

[15] *Gebhard v Consiglio dell' Ordine degli Avvocati e Procuratori di Milano* (Case C-55/94)[1995] ECR I-4165, para. 26;

[16] In case the CSP qualifies as an 'Information Society Service Provider', the rules determined by the Directive on electronic commerce need to be taken into account. See Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ 2000, L178/1.

Member States to make sure that the provisions of the European Directive are adhered to by the Certification Service Providers.[17] As a result, Member States have to ensure that Certification Service Providers operating on their territory offer their services in compliance with the EC-Directive, but may not exercise supervision by requiring prior authorization. Thus, national legislators have to find a way to exercise supervision without setting up a system of mandatory examination prior to the commencement of services.

1.3.3 Voluntary accreditation

Article 3.2 states that, without prejudice to the prohibition formulated in Article 3.1, "Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification service provision". Article 2.13 defines voluntary accreditation 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".

Further, according to Article 3.2 of the Directive, "all conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited Certification Service Providers for reasons which fall within the scope of this Directive." Recital (11) explains that "voluntary accreditation schemes aiming at an enhanced level of service-provision may offer Certification Service Providers the appropriate framework for developing further their services towards the levels of trust, security and quality demanded by the evolving market; such schemes should encourage the development of best practice among Certification Service Providers; Certification Service Providers should be left free to adhere to and benefit from such accreditation schemes". In Recital (12) it is stated that "Member States should not prohibit Certification Service Providers from operating outside voluntary accreditation schemes" and that "it should be ensured that such accreditation schemes do not reduce competition for certification services".

The idea behind a voluntary accreditation scheme is that it offers an incentive for service providers to offer high quality services to meet the requirements of the accreditation scheme. The certified proof of compliance will help to attract potential clients. In contrast to mandatory surveillance, voluntary accreditation schemes are supposed to have the advantage of being able to adapt more easily to developments in a quickly changing technical environment. Since accreditation schemes are regulated by market forces - i.e. the market players have to gauge if the expected rise in revenue generated by the anticipated increase of consumer trust is

[17] See Recital (13).

worth the necessary investment for complying with the security requirements of an accreditation scheme - they are assumed to be able to adapt to business needs more quickly.

The establishment of different accreditation schemes that are open to Certification Service Providers of all countries should ideally lead to an increased competition among these schemes. According to the Directive, accreditation schemes may not be based on discriminatory requirements. Thus, the restriction of such a scheme to service providers established in one particular Member State as opposed to providers established in other Member States would violate the provisions of the Directive. Thus, national accreditation schemes will potentially be open to any Certification Service Provider based in Europe or not.

1.3.4 Supervision

Article 3.3 provides that national law has to establish appropriate systems to allow *supervision* of Certification Service Providers established on its territory and issuing *Qualified Certificates to the public*. National law thus has to establish supervisory bodies, which see to it that providers issuing Qualified Certificates comply with the requirements laid down in the Directive, particularly in Annex II.

Member States are only required to establish a system allowing supervision for Certification Service Providers issuing Qualified Certificates to the public. The term "public" is not defined in the Directive and consequently has to be interpreted in its common sense: a service for the public is a service available to all members of the public on the same basis. Particular examples of services that should not be considered "to the public" are those provided over corporate networks and/or to closed user groups.[18] The Directive does not *explicitly* forbid Member States from extending the scope of their supervisory systems to all CSPs, irrespective of the fact whether they issue their certificates to the public or not. But it is certainly not the European legislator's intention to have supervision introduced for all CSPs either. If Member States extend the scope of the supervision beyond what is required by the Directive, they need to be very careful and avoid that supervision results in an infringement against basic Internal Market rules, particularly against the rules regarding freedom of establishment.

Article 3.3 is one of the most problematic provisions of the Directive, because it simultaneously prohibits the provision of certification services subject to prior authorisation. This prohibition not only extends to authorisations given by national bodies prior to the actual provision of certification services by a provider, but also includes all measures with a similar effect. Supervisory systems can very easily include measures that have similar effects as prior

[18] This was the viewpoint of the European Commission in its Communication of 4 April 1995 on the status and implementation of Directive 1990/388/EEC on competition in the markets for telecommunications services, OJ C 275, 20.10.1995, p. 2, [http://europa.eu.int/comm/competition/liberalization/legislation/95c275_en.html]

authorizations. The Directive explicitly prohibits the inclusion of such measures into supervisory systems.

Besides this restriction, Member States may freely decide how to ensure the said supervision. The Directive does not preclude the establishment of private-sector-based supervision systems (Recital 13).

While interpreting the obligation to ensure the supervision of CSPs, the Member States have to proceed cautiously. It is important to strike a balance between consumer and business needs (Recital 14). The consumer and the public in general must have the possibility to recognise Qualified Certificates and must be protected against the illegal use of the designation 'qualified'. At the same time companies must be able to offer their certification-services to the public freely and without obstacles.

Several Member States will perhaps solve this problem by requiring the Certification Service Provider established on their territory to give notification to the appropriate public authority before starting the provision of services. Such a notification is perfectly in line with the Directive as long as it remains a purely administrative obligation and the service provider does not have to wait for a positive or negative answer before starting operations.

The scope of the supervisory systems set up by the Member States is limited to Certification Service Providers *established* on their territory. Every Member States supervises, in other words, "its own CSPs". If a provider is established in more than one Member State, all these Member States will supervise its activities. The notion of "establishment" has been explained earlier in this report.

Regarding the fact that Member States may not restrict the provision of certification services originating in another Member State in the fields covered by this Directive (Article 4.1 of the Directive) and that Qualified Certificates that are issued by a CA situated in any EU-Member State will have to be given equal legal effect in any other EU-Member State, Certification Service Providers might consider establishing their business in one of the states with less strict requirements.

1.3.5 Public sector exception

Following Article 3.7 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. The additional requirements may not constitute an obstacle to cross-border services for citizens. It is not yet very clear how the last part of this provision has to be interpreted. The possibility granted to public administrations to specify more in detail the characteristics of their public key infrastructure seems self-evident and necessary to achieve a sufficient degree of interoperability. It is also understandable that the

additional requirements have to be objective, transparent, proportionate and non-discriminatory. Perhaps less clear however is the provision that the additional requirements "shall relate only to the specific characteristics of the application concerned" because the public authorities will in most cases not formulate requirements for public key infrastructures at the level of one specific application but at a more general level. One infrastructure – products and services – set up by a particular public administration will generally be used to secure all kinds of applications being used by that administration. It is therefore evident that the specific characteristics justifying the additional requirements can relate to several applications at the same time.

What is meant by "additional" requirements? The term refers mainly, but not only, to the lists of requirements contained in the Annexes. Very often a public administration will not be able to set up its own public key infrastructure without formulating technical requirements that are much more precise and detailed than those of the Directive. Within the limits of the rules on public procurement, public administrations will conclude detailed contracts with particular service providers and/or product vendors.

If national governments formulate additional requirements on a general level for all kinds of e-government applications, competition on the market for electronic signature-related products and services can be seriously affected. The Commission has however sufficient possibilities to intervene in such cases, not only on the basis of the Electronic Signatures Directive but also in the context of the application of European competition law, more particularly of Article 86 of the EC Treaty.

1.4 Electronic signature products (Articles 3.4, 3.5, 3.6 and 4.2)

1.4.1 Free circulation of electronic signature products

Article 4.2 of the Directive urges the Member States to ensure that electronic signature products complying with the Directive are permitted to circulate freely in the internal market. Recital (5) specifies, "The interoperability of electronic signature products should be promoted. In accordance with Article 14 of the Treaty, the internal market comprises an area without internal frontiers in which the free movement of goods is ensured. Essential requirements specific to electronic-signature products must be met in order to ensure free movement within the internal market and to build trust in electronic signatures, without prejudice to the regulation regarding dual-use goods".[19]

[19] Council Regulation (EC)No 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods and Council Decision 94/ 942/CFSP of 19 December 1994 on the joint action adopted by

Article 3.5 provides that the Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognised standards for electronic signature products in the Official Journal of the European Communities.[20] Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those standards.

Article 3.5 does not contain an obligation for the European Commission. It only mentions a possibility and it is up to the Commission whether or not it will make use of this possibility. If the Commission uses this possibility it has to follow the procedure laid down in Article 9 of the Directive. In practice this means that the Commission needs the advice of the "Article 9 Committee" before it can publish reference numbers of standards.

According to Article 3.5, the European Commission can only establish and publish reference numbers of standards that are "generally recognized". The qualification "generally recognized" in the context of Article 3.5 should be given the usual interpretation that these wordings receive in the context of standardization.[21] "Generally recognized" refers to the degree of acceptance by knowledgeable people. A generally recognized standard reflects the "state of the art".

It is not easy to determine what the precise criteria for "generally recognized" or "state of the art" should be. This difficulty has however never been an obstacle for European and national legislators to use such qualification as a reference.

An example can be found in the General Product Safety Directive, in which the codes of good practice in respect of health and safety in the sector concerned, the state of the art and technology and the safety that consumers may reasonably expect, are referred to in order to determine the safety of a product.[22]

Article 7 of the Product Liability Directive[23] provides another example. It defines a defective product as one "that does not provide the safety which a person is entitled to expect". In the

---

the Council concerning the control of exports of dual-use goods. Regulation 3381/94/EC has been amended by Regulation 1334/2000 (as last modified by Regulation 149/2003).

[20] A first set of references have been published by 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 (Text with EEA relevance), http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_175/l_17520030715en00450046.pdf

[21] See for example Judgment of the Court (First Chamber) of 2 December 1982. Société RU-MI v Fonds d'orientation et de régularisation des marchés agricoles (FORMA), Case 272/8, *European Court reports*, 1982, page 04167.

[22] Council Directive 92/59/EEC on general product safety, OJ 1992, L228/24.

[23] Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ 1985, L210/29.

Medical Devices Directive[24], the "generally acknowledged state of the art" is used to define an essential requirement. In the Pressure Equipment Directive one can read: "the essential requirements laid down in this Directive are to be interpreted and applied in such a way as to take account of the state of the art and current practice at the time of design and manufacture as well as to technical and economic recitals which are consistent with a high degree of health and safety protection".[25]

The Kalkar Decision[26] of the German Constitutional Court has made clear that "state of the art" can have several meanings. It can refer to "what is technically feasible". In this sense the qualification points at the borders of science and technology at a given moment. But the term can also refer to "the dominant views among technical practitioners". Used in this sense, compliance with the "state of the art" has to be examined differently. The German Court has very well explained that, even if a technical solution does not reflect the latest development of science, it can still be considered as the most acceptable solution by the majority of the experts in the domain. Ideally both criteria should be combined. "Generally recognized" should, in other words, refer to scientific and technological updates but at the same time to what is widely used in practice by a majority of representative practitioners.

EN 45020 defines therefore properly "state of the art" as "developed stage of technical capability at a given time as regards products, processes and services, based on the relevant consolidated findings of science, technology *and experience*.

Does this mean that a standard can never be called "generally recognized" before it has received wide application? In our view this is not a necessary pre-condition. In the legal discussion concerning DIN 32615 the German jurisprudence has correctly estimated that the criterion of "fitting for the purpose" has ideally to be measured by looking at the widespread application of the standard. But when this is not possible, for instance in the case of recently developed technology that is only at the start of receiving practical application, the acceptance by representative practitioners can also be demonstrated by the fact that these practitioners have participated in the development of the standard. In other words: the evaluation of the standardization process can, in particular with regard to recently developed technical solutions, provide one of the elements for demonstrating that a standard can be qualified as "generally recognized". Two requirements, to be fulfilled by the standardization process, are particularly relevant in this respect:

---

[24] Council Directive 90/385/EEC on the approximation of laws of the Member States relating to active implantable medical devices, OJ 1990, L189/17

[25] European Parliament and Council Directive 97/23/EC on the approximation of laws of the Member States concerning pressure equipment, OJ 1997, L181/1, Annex I , 4th preliminary remark.

[26] Judgment of 8 August 1978, BverfGE 49, 80 (p. 135 et seq.)

- Inclusiveness: the process must be open to the participation of all interested parties under non-discriminatory and fair conditions at technical and policy level, and
- Transparency: clear and publicly known procedures, wide access from the earliest moment to appropriate documents and public access to the outcome.

In all cases where the general recognition of a standard is not demonstrated by its wide application, other criteria such as "inclusiveness" and "transparency", applied to the development process of the standard, will become relevant. To qualify a standard as "generally accepted" the evaluation of the standardization process will have to be combined by a technical evaluation of the standard itself, in order to examine whether it is technically up to date.

Because the effect of the publication of the reference numbers by the European Commission is a presumption that a product meeting those standards, complies with the requirements laid down in Annex II, point (f), and Annex III, the scope of Article 3.5 is limited to electronic signature products that have to meet requirements specified in these Annexes. This means that the publication of reference numbers is only relevant for 1) trustworthy systems used by "qualified" Certification Service Providers (Annex II, point (f)) and 2) secure signature-creation devices addressed in Annex III.

Although the Directive allows the European Commission to establish and publish reference numbers of standards for particular categories of electronic signature products only, it does not exclude the establishment and the publication of standards for *other* electronic signature products or for electronic signature related services.

Article 211 of the EC Treaty gives the European Commission, in order to ensure the proper functioning and development of the common market, the power to "formulate recommendations or deliver opinions on matters dealt with in this Treaty, if it expressly so provides or if the Commission considers it necessary".

It is consequently perfectly possible for the European Commission to formulate recommendations or to deliver opinions on the application of standards beyond the limits of Article 3.5.

In a recommendation or an opinion, the Commission could, for instance, publish reference numbers of standards for electronic signature services or for other electronic signature products other than those addressed in Article 3.5. In such recommendations or opinions, the standards of which the reference numbers would be published, don't necessarily have to be "generally recognized standards". On the other hand, the publication of such reference numbers to standards in a recommendation or an opinion will not lead to a presumption that the services or products meeting those standards are compliant with the requirements of the Directive.

1.4.2 Secure signature-creation devices

According to Annex III of the Directive, secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:

(a) The signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;

(b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;

(c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.

Annex III further requires that secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

These requirements for secure signature-creation devices ensure the functionality of Advanced Electronic Signatures. They do not cover the entire system environment in which such devices operate. There are no formal requirements in the Directive regarding the signature creation process and environment. However, a CEN Workshop Agreement (CWA 14170) supports the objectives of the Directive by specifying "voluntary" security requirements for the signature creation systems which create Advanced Electronic Signatures with the help of secure signature-creation devices and Qualified Certificates by means of 1) a model of a "signature-creation environment" and a functional model of "signature- creation systems", 2) overall requirements that apply across all of the functions identified in the functional model, and 3) security requirements for each of the functions identified in the signature-creation system, excluding the secure signature-creation device. The CWA thus gives guidance to implementers to ensure that application and computer system environments incorporating signature creation are implemented in a way and provide functionality necessary for signature creation that is of sufficient quality to minimize chance of dispute.

Two CEN Workshop Agreements (CWAs 14168 and 14169) define more specifically the security requirements for secure signature-creation devices. The security requirements are formulated in a Protection Profile following the rules and formats specified in the international standard ISO 15408.

Article 3.4 of the Directive provides that the conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by *appropriate* public or private bodies designated by Member States. In a Decision of 6 November 2000 the Commission, pursuant to the procedure laid down in Article 9, established criteria for Member

States to determine whether a body should be designated.[27] Article 2 of this Decision states that, "where a designated body is part of an organisation involved in activities other than conformance assessment of secure signature-creation-devices with the requirements laid down in Annex III to Directive 1999/93/EC it must be identifiable within that organisation" and that "different activities must be clearly distinguished".

Following Article 3 "the body and its staff must not engage in any activities that may conflict with their independence of judgement and integrity in relation to their task. In particular, the body must be independent of the parties involved. Therefore, the body, its executive officer and the staff responsible for carrying out the conformance assessment tasks must not be a designer, manufacturer, supplier or installer of secure signature-creation-devices, or a Certification Service Provider issuing certificates to the public, nor the authorised representative of any of such parties. In addition, they must be financially independent and not become directly involved in the design, construction, marketing or maintenance of secure signature-creation-devices, nor represent the parties engaged in these activities. This does not preclude the possibility of exchange of technical information between the manufacturer and the designated body.

Article 4 of the Decision provides that the accreditation body and its personnel must be able to determine the conformity of secure signature-creation-devices with the requirements laid down in Annex III to Directive 1999/93/EC with a high degree of professional integrity, reliability and sufficient technical competence.

Following Article 5, the body has to be "transparent in its conformity assessment practices and shall record all relevant information concerning these practices. All interested parties must have access to the services of the body. The procedures under which the body operates must be administered in a non-discriminatory manner. Article 6 states that the body must have at its disposal the necessary staff and facilities to enable it to perform properly and swiftly the technical and administrative work associated with the task for which it has been designated. In Article 7, the Decision specifies that the personnel responsible for conformity assessment must have: 1) sound technical and vocational training, particularly in the field of electronic signature technologies and the related IT security aspects, and 2) satisfactory knowledge of the requirements of the conformity assessments they carry out and adequate experience to carry out such assessments.

Article 8 of the Decision of 6 November 2000 states that the impartiality of staff shall be guaranteed. Their remuneration shall not depend on the number of conformity assessments carried out nor on the results of such conformity assessments. Following Article 9 the body

[27] Commission Decision 2000/709/EC of 6 November 2000 on the minimum criteria to be taken into account by Member States when designating bodies in accordance with Article 3.4 of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures, OJ L289 of 16/11/2000, p. 42.

must have adequate arrangements to cover liabilities arising from its activities, for example, by obtaining appropriate insurance. Article 10 provides that the body must have adequate arrangements to ensure the confidentiality of the information obtained in carrying out its tasks under Directive 1999/93/EC or any provision of national law giving effect thereto, except vis-à-vis the competent authorities of the designating Member State. Finally, following Article 11, where a designated body arranges for the carrying out of a part of the conformity assessments by another party, it must ensure and be able to demonstrate that this party is competent to perform the service in question. The designated body must take full responsibility for the work carried out under those arrangements. The final decision remains with the designated body.

A determination of conformity with the requirements laid down in Annex III made by the bodies designated by a Member State has to be recognised by all other Member States. As far as the conformity of secure signature-creation devices is concerned, a conformity declaration in one Member State is, in other words, sufficient for the distribution of the device in all the other Member States.

Article 3.4 of the Directive does not explicitly state that it is obligatory to submit an SSCD to a conformity assessment by a designated body. It can be read in different ways and the interpretation depends very much on what chooses to emphasis or not. The most important objective of the provision, in our view, is to guarantee that, *if* the devices are submitted to conformity assessment bodies, these bodies have to be really "appropriate". Therefore the second sentence to the provision immediately adds that the Commission will determine what is meant by "appropriate" and these criteria have been established in the Commission Decision of November 2000. The European legislator wanted to avoid that conformity assessment bodies would be manipulated by interest groups or misused by Member States as instruments of economic policy. Only if the assessment body fulfils all the criteria of expertise, independence and professionalism foreseen in the Commission Decision, will the Member States automatically recognize the conformity declaration issued by these bodies. This doesn't mean, however, that Member States can't recognize other SSCDs fulfilling the requirements of Annex III. Following Art. 3.5 they *should* even presume compliance to these requirements in all cases where the SSCD meets the standards referenced by the Commission in the Official Journal.[28]

[28] Currently a device that meets the standard described in CWA 14169 "Secure Signature Creation Devices EAL 4+" (March 2002) *has* to recognized as an SSCD by all the Member States (but be aware: this standard is not obligatory for such recognition). The standard is available from the download area of the CEN/ISSS website: http://www.cenorm.be/cenorm/businessdomains/businessdomains/informationsocietystandardizationsystem/published+cwas/cwa14169.pdf

1.4.3 Secure signature-verification devices

According to Article 3.6 Member States and the Commission shall work together to promote the development and use of signature-verification devices in the light of the recommendations for secure signature-verification laid down in Annex IV and in the interests of the consumer. Annex IV recommends that, during the signature-verification process, it should be ensured with reasonable certainty that:

(a) the data used for verifying the signature correspond to the data displayed to the verifier;

(b) the signature is reliably verified and the result of that verification is correctly displayed;

(c) the verifier can, as necessary, reliably establish the contents of the signed data;

(d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;

(e) the result of verification and the signatory's identity are correctly displayed;

(f) the use of a pseudonym is clearly indicated; and

(g) any security-relevant changes can be detected.

In order to fulfil this goal, a CEN Workshop Agreement (CWA 14171) contains a specification for the signature verification procedure, including both the products used for verification, and their management. The standard identifies the security requirements for the various elements of a signature verification system. Beyond the verification process itself, the standard identifies the various interfaces, i.e. Application Programme Interfaces (APIs) or Man-Machine Interfaces (MMIs) that are needed, in particular, to select the signer's document and the electronic signature to be verified, to present the signer's document with the right format, to get the signer information and the output status after signature verification, to get additional data for long term verification and to fetch information from various CSPs. The CWA identifies the data that needs to be captured and archived so that it can be later used for arbitration, should a dispute occur between the signer and verifier. The document uses an optional concept of a signature policy as the basis to verify an electronic signature.[29]

1.5 Legal effects of electronic signatures (Article 5)

Article 5 is without any doubt the most controversial provision of the Directive. It states in its first paragraph that "Member States shall ensure that Advanced Electronic Signatures which

[29] In ETSI TS 201 733 a "signature policy" is defined as "a set of rules for the creation and validation of an electronic signature, under which the signature can be determined to be valid". See further the IETF Internet-Draft "Electronic Signature Policies", < http://ftp.ietf.org/internet-drafts/draft-ietf-smime-espolicies-01.txt >.

are based on a Qualified Certificate and which are 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 hand-written signature satisfies those requirements in relation to paper-based data; and (b) are admissible as evidence in legal proceedings.

Following 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.

Recital (20) explains: "Advanced Electronic Signatures which are based on a Qualified Certificate and which are created by a secure-signature-creation device can be regarded as legally equivalent to hand-written signatures only if the requirements for hand-written signatures are fulfilled". Recital (21) further specifies that "in order to contribute to the general acceptance of electronic authentication methods it has to be ensured that electronic signatures can be used as evidence in legal proceedings in all Member States" and "the legal recognition of electronic signatures should be based upon objective criteria and not be linked to authorisation of the Certification Service Provider involved".

In the same Recital one can also read: "national law governs the legal spheres in which electronic documents and electronic signatures may be used" and "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 recital of evidence".

1.5.1 Article 5.1

Article 5.1 thus deals with "Advanced Electronic Signatures which are based on a Qualified Certificate and which are created by a secure-signature-creation device". They are commonly called "Qualified Electronic Signatures". The Directive attributes to this category of electronic signatures, in relation to electronic data, the same status as hand-written signatures have in relation to paper documents. Article 5.1 contains, in other words, not an obligation to use electronic data processing. Legal rules enforcing the use of paper documents can consequently continue to exist and they don't have to be abrogated, at least not according to

this Directive.[30] But where the use of electronic data processing is legally permitted, the Qualified Electronic Signature should, in relation to these data, receive a status that is equivalent to the legal status that hand-written signatures normally have in relation to paper documents.

It is of course not contrary to Article 5.1 to replace current legislation requiring hand-written signatures by new legislation in which the use of electronic data is permitted without the use of Qualified Electronic Signatures. It is not the objective of the Directive to require the use of Qualified Electronic Signatures in every situation in which, up to now, the use of hand-written signatures was obligatory. On the other hand, Member States can also continue to introduce new legislation requiring additional security guarantees, above the level of Qualified Electronic Signatures. In relation to paper documents, hand-written signatures aren't the exclusive security measure either. In all cases, however, where in relation to paper documents a hand-written signature would have been sufficient, Member States have to give an equivalent status to Qualified Electronic Signatures when they start to allow the use of electronic data processing as a substitute for the paper documents. The status of the hand-written signature in its relation to paper documents determines, in other words, the status of the Qualified Electronic Signature in relation to electronic data. In the longer run, this solution may loose its efficiency because the hand-written signature will not forever be present as a reference point.

The second rule of Article 5.1, stating that Qualified Electronic Signatures should be admissible as legal evidence in legal proceedings, seems superfluous. Digital data, including electronic signatures, is accepted as evidence in legal proceedings in all Member States. Only the value of such evidence varies between the Member States. Moreover the question of the acceptability of electronic signatures as evidence in legal proceedings is, in most of the Member States, dealt with on a case-by-case basis and decided on by the judge in each specific case. Recital (21) explicitly mentions that the Directive does not affect the role of the judge in this context.

1.5.2 Article 5.2

As a general principle the Directive states in Article 5.2 that Member States may not deny the legal effect of an electronic signature or the admissibility as evidence in legal proceedings only because of the electronic form of the signature or because the requirements of the Annexes 1 to 3 are not being fulfilled.

Article 5.2 essentially states, in other words, that electronic signatures may not be denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form or that the signature in question is not a qualified signature. The effect of

[30] The progressive abrogation of such rules is, as far as electronic contracts are concerned, one of the objectives of the Electronic Commerce Directive.

Article 5.2 is that Member States may not draft or maintain regulation, or endorse or authorize private rules with a view to condemn the use of an electronic authentication tool solely by virtue of its electronic format or non-qualified nature.

It is fair to infer from the plain language that a denial of legal effect requires something more than a reference to its electronic format. This seems to translate into a requirement that a substantive disapproval must be involved, such that any objection must be "on the merits" of the particular technology involved. It is required, in other words, that any denial of an electronic signature's legal effect or admissibility be based on an affirmative finding of, e.g., a lack of technological reliability, circumstantial impropriety, or accountability. A denial of legal effect must be fully supported by a sufficiently reasoned and rationally based evaluation, one that is individual in nature, rather than being general in design.

As to the interaction with Article 5.1, the rule in Article 5.2 puts a limit on the use of the label of “Qualified Electronic Signature”. Article 5.2 states that Member States have to ensure that an electronic signature is not denied legal effectiveness, solely on the grounds that it is not based upon a Qualified Certificate and/or not created by a secure signature-creation device. This is, for example, relevant in a court proceeding: a judge could not refuse an electronic signature on the sole ground that it is not a “Qualified Electronic Signature”. He is, however, not obliged to give that signature the same legal effect, as a hand-written signature would receive. Suffice it to say that the provision of Article 5.2 touches Member States’ legislators as well. Laws denying legal effectiveness of electronic signatures solely on the grounds that they are not “Qualified Electronic Signatures” would not be in line with Article 5.2. The label of “Qualified Electronic Signature” is only meant to be used to test the equivalency of an electronic authentication method with the handwritten signature in the paper-based environment. Using the label for other purposes is in principle not allowed.

1.6 Liability (Article 6)

In its Article 6, the Directive contains liability provisions for issuers of Qualified Certificates. According to Article 6.1 and 6.2, a Certification Service Provider issuing a certificate as a Qualified Certificate to the public or guaranteeing such a certificate to the public, is liable for (a) the accuracy and the completeness of the content of the Qualified Certificate and of the revocation lists, (b) the assurance about the possession of the private key by the certified signatory at the time of issuance and (c) the correspondence between the private and the public key in cases where the Certification Service Provider generates both of these keys.

Article 6 provides for a minimum liability for CSPs. This means that the Member States can go beyond the requirements of Article 6 in their implementation of the Directive, but they are not allowed to introduce a lesser extent of liability on CSPs.

For example, Member States are allowed to introduce strict liability for CSPs or to introduce liability provisions that also cover CSPs issuing non-Qualified Certificates. In this respect the effect of Article 6 of the Directive is to enforce user protection.

On the other hand, Article 6.3 and 6.4 foresees certain liability limitations that the Member States have to recognize. This part of Article 6 can be considered as "CSP friendly".

For the liability provisions of Article 6 of the Directive on electronic signatures to be applicable, a number of conditions have to be fulfilled:

1.6.1 Qualified certificate

Firstly, the minimum liability provisions of the Directive only apply if a certificate has been *issued as a Qualified Certificate*. Thus, whether the defective certificate is actually qualified or unqualified is irrelevant. What is decisive is its designation (as "qualified") by the CSP. The reasoning behind this condition becomes obvious when considering that the requirements that have to be fulfilled by a certificate to be qualified and by a Certification Service Provider to fall under the definition of Annex II, are mostly set up to guarantee the security of the certification service. In the majority of cases, the signatory and the relying party do not have the means to control if a certificate is actually qualified in the terms of the Directive. They rely on the designation of the certificate by the CSP as qualified as it is required for Qualified Certificates in Annex I (a).

1.6.2 Issued to the public

Secondly, the certificate has to be "issued to the public" or "guaranteed to the public" (Article 6.1 and 6.2). The meaning of this term is open to interpretation. According to Recital (16), "a regulatory framework is not needed for electronic signatures that are exclusively used within systems, which are "based on voluntary agreements under private law between a specified number of participants". The provisions of the Directive do not apply to such closed systems because "the freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data should be respected to the extent allowed by national law". Since the Directive on electronic signatures expressly refrains from regulating the rights and obligations of parties in a closed system, it seems plausible that Certification Service Providers operating in a closed system are also excluded from the liability provisions of the Directive since their mutual relationships enable them to set up their own contractual liability provisions.

While in an open system, the relying party typically does not have any contractual relationship with the Certification Service Provider and is therefore dependent on the law to introduce an appropriate liability system, the relying party in a closed system can rely on the contractual liability of the CSP.

The expression " issuing to the public" can be interpreted as referring to certification services that are open to verifiers that do not have a prior relationship with the CSP.

1.6.3 "Guaranteed to the public"

As an alternative to having issued a Qualified Certificate to the public, a CSP can also be held liable for having "guaranteed" a Qualified Certificate "to the public". It is not clear in which way this kind of guarantee should be provided. Certainly, the guarantee required will have to go beyond a simple recognition of the other CSP´s public key, as it is the case in cross-certification. In most cases the guarantee will be provided in a contract between CSPs and subsequently be communicated to the public through the certification practice statement (CPS) of the issuing provider of the Qualified Certificate. The guarantee should cover at least the items mentioned in paragraphs (1) and (2) of Article 6. One case of guaranteeing a certificate is mentioned in Article 7.1(b) of the Directive (see further).

1.6.4 Liability causes

According to Article 6.1 of the Directive, the CSPs operating within the scope of this provision, are liable for the accuracy and completeness of all the information in the certificate, the identity of the signatory holding the signature creation data corresponding to the signature-verification data given or identified in the certificate and the complementary usage of signature creation data and signature-verification data if the CSP has created them both.

Consequently the CSP has to control whether or not the signatory to whom the certificate is being issued, is also the holder of the private key corresponding to the public key mentioned in the certificate. This can be done, for example, by inviting the signatory to use his/her private key for a sample Qualified Electronic Signature that is subsequently verified by the CSP.

According to Article 6.2 the CSP is liable for failure to register the revocation of the certificate. In some cases the CSP will delegate the revocation task to a specialized provider of revocation services. This delegation will not exempt the CSP from the minimum liability provided by Article 6.2.

1.6.5 Reasonable reliance

Liability of CSPs according to Article 6.1 and 6.2 of the Directive requires "reasonable reliance" by the party who suffered the damages.

The recipient of an electronic signature, who relies on one or more certificates when verifying that signature, is undoubtedly a „relying party" in the meaning of this provision. As far as the signatory is concerned, however, the situation appears more ambiguous. It is not quite clear from the wording of the Article if the signatory is included.

The signatory enters into a contract with the CSP regarding the issuance of the certificate. Therefore, it could be argued that liability of the CSP to the signatory is governed by the terms of that contract or national contract law only and that the liability provisions of the Directive thus do not apply to the signatory. Considering the fact, that the liability rules of the Directive do not apply to closed systems because the parties of such a system should be free to "agree among themselves the terms and conditions" for their communication (see Recital 16, hs.3), it could be argued that in the relationship between signatory and CSP, questions of mutual liability will be governed by contractual stipulations, valid insofar as they don't affect the minimum liability of the CSP vis-à-vis third relying parties.

Regarding liability for defective certificates, the requirement of reasonable reliance could be of specific relevance within Article 6.1 (a) var.2 of the Directive, which constitutes liability for the completeness of information contained in a certificate. It might be questionable, if the recipient of a Qualified Electronic Signature can be said to have reasonably relied on the respective certificate if the information specified in Annex I of the Directive is missing in that certificate. It might be possible that the technical expertise of the consumer will be taken into consideration to interpret the term reasonableness on an individual basis.

Another question of relevance is, to what extent a CSP can exclude reasonable reliance by limiting his liability in his terms and conditions. Since the introduction of valid liability limitation clauses in relation to the relying party is legally doubtful due to the absence of a contractual relationship, the reasonableness requirement might open a door for CSPs to limit their liability in a tort relationship. It will be up to the courts to decide whether a relying party can be said to have reasonably relied on a certificate if that certificate excludes liability of the issuer in a respect that is not covered by Article 6.3 and 6.4 and to what extent these kinds of liability limitations will be considered valid in a tortuous relationship. Possibly, the rules and provisions governing contractual liability limitations will be taken into consideration when answering that question.

Possibly, a disclaimer (which could e.g. appear to the relying party when he/she receives an electronically signed message) in which the CSP states that its liability is limited could be used to prevent reasonable reliance. The advantage of that method would be that the relying party is confronted with the disclaimer 'up-front' - the disclaimer could e.g. state that by relying on the certificate the relying party agrees to the limitation of liability clause or to the terms and conditions of the CSP in which a limitation of liability clause inserted.

1.6.6 Absence of negligence

Strict liability - as it exists in product liability law[31] - is not demanded by the Directive. Instead, negligence of the provider is a precondition for a title to compensation for damages. This precondition is based on the typical situation of the relying party. The recipient of a signature that turns out to be invalid will often not be in a position to analyse the technical background of that failure, whereas the CSP itself has much better insight into its own organizational and technical proceedings. Accordingly, the Directive imposes the burden of proof for negligence on the CSP, who has the necessary technical know-how to investigate the matter.

1.6.7 Limitation of liability

To reduce the financial risk associated with liability, Certification Service Providers will look for methods to limit their liability. The Directive provides for a number of liability limitations. These limitations have to be recognized by the Member States on condition that they are included in the certificate itself and in a form that is recognizable to third parties. To be considered valid, all liability limitation clauses generally have to be made available to the CSP´s contract partner or the relying party in clear and readable form.

1.6.7.1 Limitation provisions of the EU-Directive

The Directive in Article 6.3 and 6.4 explicitly provides for certain liability limitations. E.g. a CSP can include a value limit for commercial transactions. If that limit is transgressed, the CSP „shall not be liable for damage resulting from this maximum limit being exceeded“. If the wording of the Directive is taken literally, this does not offer a very extensive limitation option. If the CSP has to be at fault for liability to arise, the damage in a successful case will most likely be the result of a negligent act of the CSP rather than being caused by the excess of the maximum transaction limit. Thus, an interpretation of Article 6 that allows a CSP to limit his liability by referring to a maximum transaction value clause in the certificate should be followed[32]. The majority of legal literature that has been published on this topic so far interprets Article 6.4 to allow a relative liability limitation only, meaning that only the maximum value *per transaction* can be limited, but not the absolute liability for the certificate regardless of the number of transactions. This interpretation seems reasonable, since it is not possible for the relying party to see the number of previous transactions that have been conducted by the

[31] Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 141, 04/06/1999 p. 0020 – 0021.

[32] The recognition of a per-incident and aggregate cap on a CSP's liability is also recommended by the ABA Science & Technology Information Security Committee, available at: http://www.abanet.org/scitech/ec/isc/ukkeyr1.html

signatory or the extent to which the liability for the certificate has already been "consumed" by these previous transactions.

The provisions of the Directive also provide the possibility to indicate a limitation of use of a certificate, for example that the certificate may only be used for a certain type of transaction or that it may only be used within a particular company, a specified country or within the EC. If the signatory then transgresses these limitations by using the certificate for purposes outside the limitation, the Certification Service Provider will not be held liable for resulting damages.

Depending on the law of the Member States, liability limitations can be included in the certificate itself – such limitations have to be accepted by all the Member States - but national law can also provide the limitations to be mentioned in a Certificate Practice Statement or in a separate statement under the condition that it has been brought effectively to the attention of the relying party and the signatory.

1.6.7.2 Liability limitation outside the Directive

Outside the scope of the Directive, national laws govern the liability of Certification Service Providers. The extent, to which liability limitations will be allowed under these provisions, may depend on a number of factors, such as for example the "class" of the certificate.

1.6.7.3 Liability limitation statements

Considering the liability limitations already included in the Directive, it is a frequent practice of CSPs to establish a maximum cap for liability for Qualified Certificates. The maximum cap often includes liability for all ancillary services that the certificaction service provider may be held liable for. The maximum cap can, for example, vary depending on the quality of the certificate issued. CSPs issuing cross-certificates to other CSPs sometimes clearly state the limitation of usage of these certificates to avoid liability to relying third parties other than CSPs. In addition to that, a certificate may include a limitation that allows its use for a certain type of transaction only, e.g. a contract for the sale of movables.

While liability limitations that go beyond the ones foreseen in the Directive are only valid outside the scope of this Directive, a CSP might seek to prevent potential liability by explicitly stating that no liability will be assumed for any statements by the signatory that are not verified by the certificate.

Moreover, to clearly avoid liability for potential conflicts regarding the legal validity of a digital signature in a certain context, the CSP may wish to make clear that he does not guarantee the legal effect of an electronic signature that bears his certificate. Since there exists no jurisprudence regarding the interpretation of the liability provisions of the European Directive, yet, CSPs often include liability limitations that are based on the narrowest possible interpretation of these provisions. For example, it is not clear at the moment to what extent

courts will hold CSPs liable for indirect damages arising from a defect certificate. Thus, exclusion of any form of liability for indirect damages incurred by either signatory or relying party is often foreseen in the Certification Practice Statements of many CSPs.

To increase the probability that liability limitations in relation to relying third parties will be enforceable in court, it is common practice to require a relying party to agree on the terms and conditions for usage of the certificate revocation list before enabling him to access the list or before giving him access to an OCSP service. The statement that a relying party will be deemed to have agreed to the terms and conditions if he relies on the certificates issued by the Certification Service Provider may be considered insufficient for that purpose if it cannot be established that the relying party had to take notice of the conditions prior to using the CSP´s certificate for verification.

1.6.8 Business model behind Article 6

Article 6 of the Directive puts the liability for damages resulting from negligence during the registration process on the shoulders of the provider issuing the Qualified Certificate. The same is true for the liability related to the revocation services. This means that the (only) business model supported by Article 6 is the one whereby the issuer of the certificates is liable for the whole of the certification chain.

The issuer of the certificate is the provider whose name appears in the certificate and who signs the certificate. Even if another provider performs the registration activities or if the revocation services are provided by another CSP, the CSP whose name appears in the certificate will be liable according to Article 6. By simply looking at the certificate, the relying party will not be aware of the task division between different providers that are involved in the certification chain. By adopting a business model that puts the whole liability on one of these providers, Article 6 aims at protecting the relying party. In practice the contract between the CSPs participating in the certification chain generally provides that the issuer of the certificate will be exonerated for liability related to all the services in the certification chain that are performed by other providers. This is of course perfectly compliant with the provisions of the Directive.

1.7 Other provisions

1.7.1 International aspects (Article 7)

The recitals of the Directive emphasize that the development of international electronic commerce requires cross-border arrangements involving third countries. In order to ensure

interoperability at a global level, agreements on multilateral rules with third countries on mutual recognition of certification services could be beneficial.[33]

Article 7 of the Directive requires the Member States to ensure that certificates which are issued as Qualified Certificates to the public by a Certification Service Provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service- provider established within the Community, providing one of the following three conditions are met:

(a) the Certification Service Provider fulfils the requirements laid down in the Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or

(b) a Certification Service Provider established within the Community which fulfils the requirements laid down in the Directive guarantees the certificate; or

(c) the certificate or the Certification Service Provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.

The first possibility for CSPs established in a third country to obtain legal equivalence for their certificates is not very clearly formulated. Of course it is absolutely understandable that these CSPs have to fulfil "the requirements laid down in the Directive". The problem is that, contrary to their EU-based competitors, CSPs established in third countries will not be under the scope of one of the national supervisory systems established in the Member States. Therefore the provision contains "accreditation" as an *additional* requirement. The point is that voluntary accreditation schemes don't necessarily control the compliance of the CSP with the requirements of the Directive. On the contrary, Art. 3.2 explicitly promotes all kinds of voluntary accreditation schemes, for example aiming at enhanced levels of certification-service provision. For the purpose of Art. 7.1(a), however, the voluntary accreditation scheme, used by the third country-based CSP, should, albeit for this particular task, control whether or not this CSP meets the requirements of the Directive.

According to Article 7.2, in order to facilitate cross-border certification services with third countries and legal recognition of Advanced Electronic Signatures originating in third countries, "the Commission will make proposals, where appropriate, to achieve the effective implementation of standards and international agreements applicable to certification services. In particular, and where necessary, it shall submit proposals to the Council for appropriate mandates for the negotiation of bilateral and multilateral agreements with third countries and international organisations. The Council shall decide by qualified majority".

Article 7.3 provides that "whenever the Commission is informed of any difficulties encountered by Community undertakings with respect to market access in third countries, it may, if

[33] Recital (23).

necessary, submit proposals to the Council for an appropriate mandate for the negotiation of comparable rights for Community undertakings in these third countries. The Council shall decide by qualified majority. Measures taken pursuant to this paragraph shall be without prejudice to the obligations of the Community and of the Member States under relevant international agreements."

1.7.2 Data protection (Article 8)

Member States have to ensure that Certification Service Providers and national bodies responsible for accreditation or supervision comply with the requirements laid down in 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.[34]

According to Article 8.2 a Certification Service Provider issuing certificates to the public may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject.

Without prejudice to the legal effect given to pseudonyms under national law, Member States may not prevent Certification Service Providers from indicating in the certificate a pseudonym instead of the signatory's name. Recital (25) specifies: "provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Community or national law".

In its Working Document on on-line authentication services, adopted on 29 January 2003[35], the Article 29 Working Party, established in the framework of the European Data Protection Directive 95/46/EC, underlined that both those who design and those who actually implement on-line authentication systems (authentication providers) bear responsibility for the data protection aspects. Whilst PKI applications can enhance privacy[36], there are serious privacy risks linked with the use of PKI.[37]

---

[34] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on tile protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p 31.

[35] http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp68_en.pdf

[36] e.g. the use of digital certificates reduces the ever-recurring need to provide basic evidence of identity (date of birth, address, etc.) and guarantees confidentiality of communications through encryption of messages.

[37] The privacy issues listed below are extensively discussed in: The Office of the Federal Privacy Commissioner, Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals, http://www.privacy.gov.au/government/guidelines; International Working Group on Data Protection in

Currently PKI is still very often entirely based on the use of identity certificates. In order to improve privacy protection, researchers have proposed to make more use of attribute certificates or, more generally, certificates which certify a credential, rather than an identity. Such certificates function in much the same way as cinema tickets or subway tokens: anyone can establish their validity and the data they specify, but no more than that. Furthermore, different actions by the same person cannot be linked. Certificate holders have control over what information is disclosed, and to whom. Potential applications include electronic cash, electronic postage, digital rights management, pseudonyms for online chat rooms, health care information storage, electronic voting, and even electronic gambling. [38]

1.7.3 Committee (Article 9-10)

In the framework of the Electronic Signature Directive the Commission has received a number of implementing powers, e.g. in Article 3.4 (criteria for the designation of accreditation bodies) or Article 3.5 (publication of reference numbers of generally recognized standards). In the exercise of these implementing powers an "Electronic Signature Committee" assists the Commission with representatives of the Member States.

Articles 4 and 7 of Decision 1999/468/EC[39] are applicable to this Committee. Article 4 describes the management procedure of the Committee:

1. The Commission shall be assisted by a management committee composed of the representatives of the Member States and chaired by the representative of the Commission.
2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit, which the chairman may lay down according to the urgency of the matter. The opinion shall be delivered by the majority laid down in Article 205(2) of the Treaty, in the case of decisions, which the Council is required to adopt on a proposal from the Commission. The votes of the representatives of the Member States within the

---

Telecommunications, Working Paper on data protection aspects of digital certificates and public-key infrastructures, 28 August 2001, Berlin, http://www.datenschutz-berlin.de/doc/int/iwgdpt/pubkey_e.htm; see also: CLARKE, R., Privacy requirements of PKI, paper presented at the IIR IT Security Conference, Canberra, 14 March 2000, http://www.anu.edu.au/people/Roger.Clarke/DV/PKI2000.html and CLARKE, R., PKI position statement, 6 May 1998, http://www.anu.edu.au/people/Roger.Clarke/DV/PKIPosn.html.

[38] See further on this topic: CHAUM, D., Achieving Electronic Privacy; Scientific American, August 1992, 96-101 and BRANDS, S., Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy, MIT Press, 2000, 356 p.

[39] Council Decision of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission, OJ L 184 , 17/07/1999 p. 0023 – 0026.

committee shall be weighted in the manner set out in that Article. The chairman shall not vote.

3. The Commission shall, without prejudice to Article 8, adopt measures, which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. In that event, the Commission may defer application of the measures which it has decided on for a period to be laid down in each basic instrument but which shall in no case exceed three months from the date of such communication.
4. The Council, acting by qualified majority, may take a different decision within the period provided for by paragraph 3.

According to Article 7:

1. Each committee shall adopt its own rules of procedure on the proposal of its chairman, on the basis of standard rules of procedure which shall be published in the Official Journal of the European Communities. Insofar as necessary existing committees shall adapt their rules of procedure to the standard rules of procedure.
2. The principles and conditions on public access to documents applicable to the Commission shall apply to the committees.
3. The European Parliament shall be informed by the Commission of committee proceedings on a regular basis. To that end, it shall receive agendas for committee meetings, draft measures submitted to the committees for the implementation of instruments adopted by the procedure provided for by Article 251 of the Treaty, and the results of voting and summary records of the meetings and lists of the authorities and organisations to which the persons designated by the Member States to represent them belong. The European Parliament shall also be kept informed whenever the Commission transmits to the Council measures or proposals for measures to be taken.
4. The Commission shall, within six months of the date on which this Decision takes effect, publish in the Official Journal of the European Communities, a list of all committees which assist the Commission in the exercise of implementing powers. This list shall specify, in relation to each committee, the basic instrument(s) under which the committee is established. From 2000 onwards, the Commission shall also publish an annual report on the working of committees.
5. The references of all documents sent to the European Parliament pursuant to paragraph 3 shall be made public in a register to be set up by the Commission in 2001.

The main tasks of the Committee are to clarify the requirements laid down in the Annexes of the Directive, the criteria referred to in Article 3.4 and the generally recognised standards for electronic signature products established and published pursuant to Article 3.5.

1.7.4 Notification (Article 11)

Member States have to notify to the Commission and the other Member States the following:

1. information on national voluntary accreditation schemes, including any additional requirements pursuant to Article 3.7;
2. the names and addresses of the national bodies responsible for accreditation and supervision as well as of the bodies referred to in Article 3.4;
3. the names and addresses of all accredited national Certification Service Providers.

The information supplied and changes in respect of that information have to be notified by the Member States as soon as possible.

1.7.5 Review (Article 12)

Two years after its implementation the Commission will carry out a review of the Directive so as, inter alia, to ensure that the advance of technology or changes in the legal environment have not created barriers to achieving the aims stated in the Directive. It will examine the implications of associated technical areas and submit a report to the European Parliament and the Council on this subject. The report will in particular include an assessment, on the basis of experience gained, of aspects of harmonization. The report shall be accompanied, where appropriate, by legislative proposals.

1.7.6 Implementation (Article 13)

The Member States have to transpose the Electronic Signature Directive before 19 July 2001 and forthwith inform the Commission thereof. When Member States adopt these measures, they have to contain a reference to the Directive or be accompanied by such a reference on the occasion of their official publication. The Member States themselves can lay down the methods of making such reference.

Member States are required to communicate to the Commission the text of the main provisions of domestic law which they adopt in the field governed by this Directive.

Chapter 2 The transposition of the Directive

The research team analysed the laws, practices and existing case law in all EU Member States, the EEA Countries, the Candidate Countries and the Accession Countries. Switzerland was also analysed. The team focussed on possible gaps in national legislation and on possible difficulties of implementation. The team also looked for issues that are typical for more countries and which could hinder the practical implementation of electronic signatures and related services on a national and on a pan-European basis.

Since European directives are not directly applicable to private entities such as CSPs, signatories and relying parties, they have to be implemented into national law to be fully effective. As a result, the rights and obligations of CAs are technically not directly governed by the Directive itself, but by the national laws that have been enacted in accordance with the Directive. Since only the objectives of a European directive are binding and not the way these objectives are achieved by the national legislators, is the implementation of the Directive is not identical in every Member State.

As with Chapter I, the structure of the Directive has been followed and its implementation followed on an article-by-article basis.

2.1 Definitions (Article 2)

It is always dangerous to compare definitions from different legal frameworks since a definition should at all times be regarded in its own legal context. An “electronic signature” as defined by one national law could indeed be subject to other legal conditions and have other legal consequences than an “electronic signature” as defined by the laws of another country. The following chapter provides but an overview of definitions without referring to their specific context.

2.1.1 Electronic signature

The Directive defines “electronic signature” as data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication (Article 2.1).

Most Member States (e.g. Belgium, Germany, Greece, Netherlands, Spain, United Kingdom) literally transposed this definition into their national legislation. Also some candidate countries and EEA countries closely stick to the Directives definition (e.g. Czech Republic, Lithuania, Norway).

Some countries, however, narrow down the broad EU definition of an electronic signature:

- Some countries do this by specifying the specific purposes of authentication (Austria, Italy) or by defining the term "authentication" (Finland, Hungary, Poland and Romania, Iceland). It is interesting to see that, although no definition of "authentication" has been given by the Directive quite a few countries define authentication as establishing the identity of the signatory (Austria, Finland, Portugal, Poland, Romania, Iceland) or replace the term "authentication" by its functions (Sweden: "used to verify that the content originates from the alleged issuer, and has not been altered."). Other countries restrict the purpose of electronic signatures to "a method of computer authentication" (Italy).
- Other countries narrow the scope of the definition down to the use of the signature by a person (and not a machine) (Denmark) and/or technologies (Ireland). Ireland indeed states that an electronic signature should include an "Advanced Electronic Signature".[40]
- Interestingly, Hungary defines "electronic signature" as "data in electronic form or electronic record which are logically associated with and inseparably attached to other electronic record, with the purpose of authentication", thus requiring the fulfilment of both logical association and attachment.
- Luxembourg did not include the Directive's definition of an "electronic signature" in its law, but states than an electronic signature consists of a data string linked in an indivisible way to a document guaranteeing the integrity, identifying the signatory and expressing signatory's commitment to the content of the act. The Belgian law on electronic signatures contains a similar clause, apart from the Directive's definition.

A few non-EU countries define electronic signature in a non-"technology neutral" way. This is the case for Estonia ("Digital signature" making use of public key pair) and Bulgaria ("information […] secure enough based on the market demands").

In summary, the national laws of most countries define an "electronic signature" in exactly the same wordings as the Directive. Some countries did not literally take over the definition of the Directive, but specified the term "authentication" or specified the functions of an electronic signature.

[40] Our Irish correspondent informs us that the definition of an electronic signature in the Electronic Commerce Act 2000 is closely based on the definition in the Directive with two additions which are intended to clarify the definition and not to limit it: 1) the Irish definition of electronic signature expressly includes an Advanced Electronic Signature and 2) definition of "electronic".

2.1.2 Signatory

The Directive defines a "signatory" as 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.

Some countries transposed this definition of the Directive in a literal (France, Luxembourg, Spain, United Kingdom, Romania, Iceland) or similar way (Greece, Ireland, Netherlands, Portugal, Norway).

- Ireland, for example, defines a signatory as a person who, or public body which, holds a signature creation device and acts in the application of a signature by use of the device either on his, her or its own behalf or on behalf of a person or public body he, she or it represents.

Other countries filled in the definition of signatory differently.

- Italy for example defines a signatory as the natural person to whom the electronic signature is attributed and who has access to the device for a creation of the electronic signature.
- Sweden for example defines a signatory as "a natural person who is authorised to control a signature creation device."
- Hungary defines a signatory as "a natural person to whom the signature verification data is connected according to the list of signature verification data published by the electronic signature Certification Service Provider".
- The Slovenian law provides a simple definition: "a person by whom, or on whose behalf, an electronic signature is created."

Some countries do not have the term "signatory" defined but use other terminology.

- For example, Belgian law talks about the "certificate holder" as the natural or legal person to whom a certificate has been issued;
- German law talks about "Signature-code owners', which are natural persons who own signature codes and to whom the appropriate signature test code have been assigned in Qualified Certificates.

Other countries do not provide for a definition at all for the user of the signature application (Estonia, Switzerland).

It is noteworthy that Bulgarian law provides two definitions relevant to electronic signatures, namely the "signature-owner" and the "signatory". The owner of the electronic signature is the natural or legal person on whose behalf the electronic statement is performed. The signatory is the natural person who is authorized to make electronic statements on behalf of the owner of the electronic signature.

In several Member States there has been a discussion about whether or not a signatory has necessarily to be a natural person and this discussion is sometimes reflected in the legal provisions adopted by some of the Member States. From the perspective of the European Directive, it is clear that an electronic signature can refer not only to natural persons but also to all kinds of other entities. An electronic signature can, for example, be the electronic substitute for a stamp belonging to a particular administration within the government or to a specific department of a university. This is the logical consequence of the very broad definition of the term "electronic signature" in the Directive. On the other hand, it is also clear that a Qualified Electronic Signature in the meaning of Article 5.1 of the Directive can only be the signature of a human being, for the very simple reason that it has to be legally considered as the (electronic) equivalent of the handwritten signature.

For the same reasons a legal person can never be considered as the signatory. The concept of the "signatory", being the person who "holds" the signature-creation device, is useful in cases where it is not clear which individual is actually at the origin of the signature. Even though it is theoretically acceptable to defend the argument that a signature can be attributed directly to a legal person, it remains in most cases very important for legal reasons to identify the individual who acted on behalf of this legal person. The definition of the "signatory" in the Directive is aimed at solving this problem.[41]

Notwithstanding the sometimes very obscure and complicated provisions on "electronic signatures of legal persons" in some Member States, the discussion remains mainly theoretical and fortunately its practical consequences are negligible.

2.1.3 Certification service provider

The Directive defines a "Certification Service Provider" (CSP) as an entity or legal or natural person who issues certificates or who provides other services related to electronic signatures.

Most countries have transposed this definition of the Directive in a literal sense (Greece, Ireland, Luxembourg, Netherlands, Spain, Slovenia, Romania) or else have adopted a similar approach (Austria, Belgium, France, Italy, Portugal, United Kingdom, Czech Republic, Lithuania, Iceland, Norway) way.

- Belgium, for example, defines a CSP as every natural person or legal entity issuing and administering certificates or providing other electronic signature related services.

[41] The theoretical and sometimes emotional discussions about the "signature of legal persons" can lead to quite aberrant legal provisions. In Belgium, for instance, Article 8, § 3 of the law of 9 July 2001 introduces an obligation for Certification Service Providers established in Belgium to hold, for every legal person to whom they issue a Qualified Certificate, a register with the identification and the function of all the natural persons "who are using the signature of the legal person"!

- Italy for example, only refers to an entity (and not a person) as CSP; the United Kingdom and the Czech Republic only refer to a person.

Some countries restrict the definition of a CSP to the issuing of certificates (Denmark, Finland, Switzerland, Sweden).

- Denmark uses the term Certification Authority instead of Certification Service Provider.
- Germany defines the activities of a CSP operating under the scope of the law, to issuing Qualified Certificates or qualified time stamps.

In Bulgaria, Hungary and Poland the specific activities of a service provider that would make it a CSP are explicitly summed up (e.g. certificate issuance, time stamping). Our national correspondents informed us that this enumeration should not be regarded as a limited one but as an exemplary one. It is noteworthy that in Estonia, only registered agencies and persons are regarded as Certification Service Provider.

In summary, the definition of CSP is in the national laws of most countries in line with the EU definition. Only a few countries deviate from the EU definition, mostly by restricting the activities of a CSP to the issuance of certificates only.

2.1.4 Other definitions

Some countries' national legislation include definitions that cannot be traced back to the wordings of the Directive.

- Ireland for example, defines the term 'electronic' as electrical, digital, magnetic, optical, electro-magnetic, biometric, photonic and any other form of related technology.
- Austria includes a definition of "secure electronic signature". This definition is closely related to the description of an electronic signature in the sense of Article 5.1 of the Directive. However, this secure electronic signature needs to be created using technical components and procedures which comply with the security requirements of the Austrian federal law and the orders issued on the basis thereof. Also Poland introduces a "secure electronic signature" based on the same principles as the Austrian one.
- Germany, Italy, Portugal, Hungary, Iceland and Norway provide for a definition of a 'Qualified Electronic Signature'. The definition reflects the contents of Article 5.1 of the Directive.
- Bulgaria introduces a new kind of signature, the "universal signature". This signature is similar to an Article Qualified Electronic Signature under the Directive but the relating certificate is issued by an accredited Certification Service Provider.

Some countries provide for definitions for time stamps (Germany, Hungary, Poland).

- Poland for example, defines a time stamp as the attachment to data in electronic form, logically associated with the data certified with electronic signature or authentication, of specification of time and electronic authentication (confirmation) of the data generated in such way by the provider of the service.

2.2 Legal Effect of E-Signatures (Article 5)

2.2.1 Legally relevant electronic signatures

2.2.1.1 State of implementation in Europe

All European countries under examination, with the exception of Cyprus which has not yet transposed the Directive, recognise that electronic signatures can have a legal relevance. It is, however, not always clear to what extent electronic signatures are legally acceptable. The common denominator of the classification under this question is whether a signature fulfilling the requirements of the definition of "electronic signature" under national legislation is recognised by law as capable of producing legal effects.

In some countries the legislator confirms explicitly the more or less evident principle that electronic signatures are not yet acceptable in all circumstances and that some procedures remain – perhaps for the time being – based on the use of paper documents and handwritten signatures.

- In Sweden, for instance, the legal effects of the handwritten signature cannot be satisfied by electronic means in all circumstances.
- Similarly in Norway, electronic signatures may have a legal relevance if electronic communication is allowed in the area the act is referring to.

In a few countries, the legal relevance of the electronic signature is expressed in generic terms:

- The Italian law expressly states that an electronic document with an electronic signature satisfies the legal requirement of writing. It is inferred from this rule that the electronic document on which the electronic signature is apposed can in principle be related to any legal consequences that derive from the written form.
- In Portugal, an electronic signature purported to be equivalent to a handwritten one is presumed to confirm: i) the identity of the signatory, ii) the intention of signing and iii) the integrity of the signed document.

- Similarly, in Belgium, an electronic signature can serve as evidence so long as long as one can derive with certainty: i) the identity of the author and ii) the integrity of the contents to be signed.

In those Common law countries surveyed (the UK and Ireland), the form of signature does not matter. In the same way that a sign or symbol carries with it a certain legal authority , an electronic signature has a legal significance once it satisfies the functions of a signature.

In the Czech Republic, the term "handwritten signature" has no particular legal significance; consequently, electronic signatures have inherently a legal effect unless the given law or act requires "official attested signature" (being a signature done by a notary).

In a few countries, the legal effect of a signature can also be derived from the functions of a signature. These functions (in addition to, or other than the authentication function) are explicitly stated in the definition of the electronic signature in the given country.

- In Sweden and Denmark, an electronic signature has to ensure both data origin authentication and data integrity.
- In Portugal, the electronic signature must reveal who is the author of the electronic document in question.
- In Luxembourg, apart from data origin authentication (identification) and data integrity, an electronic signature should also serve to expres a signatory's commitment to the content of the act.

2.2.1.2 Conclusion

All European countries having transposed the Directive recognise its relevance either: i) with restrictions ii) in general terms or iii) by associating the electronic signature with explicit functions, that are for the most part laid down in the definition of the signature in the national law (e.g. Sweden, Portugal). In a few cases, this legal significance may also derive from the law itself (e.g., Belgium) or from jurisprudence (e.g. UK).

2.2.2 Electronic signatures equivalent to handwritten signatures (Article 5.1)

2.2.2.1 Reminder

According to Article 5.1 of the Directive an electronic signature shall be considered equivalent to a handwritten signature in all of the Member States so long as it it fulfils the following requirements:

1. it meets the four functional requirements of the Advanced Electronic Signature;

2. it is based on a Qualified Certificate (QC);
3. it is created by a Secure Signature Creation Device (SSCD).

This provision thus establishes the (refutable) presumption that any electronic signature fulfilling these requirements is considered as satisfying the legal requirements of a signature in relation to electronic data in the same way as a handwritten signature does in relation to paper-based data.

Article 5.1 does not expressly name the electronic signature that responds to the above-mentioned conditions. Nevertheless, for the sake of distinguishing between such a signature and other forms of signature, which do not meet the same level of functional security, the legal doctrine and practice generally refer to the electronic equivalent of the handwritten signature with the term “Qualified Electronic Signature”.

Further to the recognition of the legal equivalence, the same Article reaffirms in a second paragraph [point (b)] that the Qualified Electronic Signature is admissible as evidence in court proceedings.

2.2.2.2 State of implementation in Europe

When examining the implementation of Article 5.1, from a horizontal point of view, countries can be categorised into those that:

- have transposed in more or less literal terms the provision in question (literal transposition);
- have adopted their legislation to the purpose of the provision (transposition *in fine*), whilst they impose other conditions than the ones set out in the Directive;
- have not recognised the legal equivalence in all circumstances;
- have not implemented this provision explicitly (no explicit transposition).

i. Literal transposition

EU Member States, Belgium, Greece, Finland, Portugal and Spain have introduced in their legislation an explicit provision that basically reiterates the wording of Article 5.1.

- Two countries in this group, Portugal and Spain, even have even explicitly named and defined the “Qualified Electronic Signature” in their national laws.
- It is noteworthy that in Belgium the law establishes an even stronger wording than Article 5.1 since it expressly *assimilates* the Qualified Electronic Signature to the handwritten one.

- The Greek electronic signatures law transposes expressly both Article 5.1 (a) and (b) by stating that the Qualified Electronic Signature is equivalent in to the handwritten one both in substantial law and in procedural law.
- Finally, Portuguese legislation derives three presumptions from the apposition of the Qualified Electronic Signature on a document: i) the person who placed the electronic signature is presumed to be the holder thereof, ii) the electronic signature was placed with the intention of signing and iii) the electronic document has not been altered.

From the Accession and Candidate countries, Malta, Lithuania, Latvia, Poland (but, see also categorisation below) and Romania have transposed Article 5.1 by an explicit provision in their electronic signature laws.

- In addition, the Lithuanian law reiterates expressly the basic rule that signatories can by agreement determine the legal validity of the signature used (thus, that they can recognise the legal validity of the handwritten signature to other electronic signatures than the qualified ones).
- The Latvian provision of the law on electronic documents reaffirms this equivalence although the terms used are slightly different from the terminology of Article 5.1 (the Qualified Electronic Signature is called *Secure electronic signature*, SSCD is any *Secure Tools for Creating electronic signatures* and the QC is the *Certified* Certificate.
- The Polish electronic signatures law also stipulates explicitly that electronic documents signed with *Secure* electronic signatures (being equivalent to Advanced Electronic Signatures created by SSCD) verified with the use of a valid QC have legal effects equivalent to documents signed with handwritten signatures.

The Romanian Act assimilates electronic documents incorporating a signature based on a QC and generated using an SSCD to documents under private signature. Further, the law specifies that if the written form is required as proof or validity condition of a legal document in such cases as the law may provide, a document in electronic form shall satisfy to this condition if a Qualified Electronic Signature is used. The draft Electronic Signature Act of Liechtenstein provides explicitly for equivalence along similar lines.

In terms of the EEA countries, Iceland explicitly defines the Qualified Electronic Signature and stipulates in stronger words than the Directive the rule of Article 5.1, namely that Qualified Electronic Signatures shall always be considered as meeting the requirement of a signature under Icelandic law.

ii. Transposition *in fine*

It is noteworthy that the legislation of a number of countries recognises the effect of Article 5.1 (that certain electronic signatures should be considered as legally equivalent to handwritten ones) but they do so by: i) translating such a rule in a direct or indirect way in basic generic

laws (Civil Code, Code of Civil Procedure, etc.), ii) imposing conditions other than those stipulated in Article 5.1 for the recognition of the legal equivalence, or iii) associating the presumption of the legal equivalence with signatures other than qualified ones.

In the first category (i) fall the legislation of France, Germany, Luxembourg, Poland and Hungary.

- The French Civil Code has been amended to introduce the legal equivalence of the electronic signature to the handwritten one if certain conditions are fulfilled: reliability of the identification process, and link between signature and signed data. An electronic signature that follows the requirements of the Qualified Electronic Signature as prescribed in the French legislation is presumed to fulfil the reliability requirement of the signature creation process. As in the Directive, the French Qualified Electronic Signature is an Advanced Electronic Signature based on a QC and created by an SSCD. A slight difference from the Directive is that the French law does not provide for a presumption of "equivalence" but for a presumption of "reliability": once a Qualified Electronic Signature has been used, the signature creation process followed is presumed to have been adequately reliable to relate the electronic signature with the effects of the handwritten signature.
- As far as Germany is concerned, although the electronic signatures law defines the Qualified Electronic Signature, it does not provide explicitly for the legal validity of this signature. Such a validity shall be adduced by reference to five basic laws: (1) the German Civil Code being amended to introduce the legal validity of electronic documents (that the electronic form can in general be used as substitute of the written form) and (2) also, a new provision of the Civil Code states that "qualified" electronic signatures based on Qualified certificates and created by SSCD that meet the requirement of the German electronic signatures law are purported to be equivalent to handwritten signatures. Moreover, the Code of Civil Procedure establishes a presumption for the "qualified" electronic signature used for evidential purposes: According to this law, the "qualified" electronic signature constitutes a *prima facie* evidence that it ensuring the "authenticity" of a declaration of intention which is signed by a qualified electronic signature. Besides of the Civil Code (only for the private sector) and the Civil Procedure Act there are three basic codes for the public sector, that regulate the electronic form as equivalent to the handwritten form: the administrative procedure law, the general tax law and the general social law.
- In Luxembourg, the enactment of the Electronic Commerce Act (law incorporating also provisions on the legal validity of electronic signatures) has put handwritten and electronic signatures on an equal footing. The Luxembourg Civil Code has been amended to confirm that a private act with legal effect (*acte sous seing privé*) may be signed by a handwritten or electronic signature. Furthermore, it is also clearly stated in

the Civil Code that the *act sous seing privé* equals to the original act, as long as one can adduce reliable guarantees that content integrity has been maintained as from the first day of its creaction on a stable form.

- The Polish Civil Code sets out that a declaration of intent signed with a Qualified Electronic Signature is equivalent to the written form.
- Similar amendments have been introduced in the Civil Code and Act on Civil Procedures in Hungary. It should be noted that Hungarian legislation does not recognise the concept of a "handwritten" signature. Therefore, the equivalence between handwritten/other kind of signature applies at the level of document/electronic document-electronic deed. On the one hand, the Hungarian Civil Code introduces the rule that electronic deeds signed with Advanced Electronic Signatures is considered as contract made in written form. On the other hand, the Act on Civil Procedures pronounces that private deeds have full probative force if a Qualified Electronic Signature is placed on the electronic deed.

In the second category (ii) fall the legislation of Austria, the Netherlands, the Czech Republic, Poland [in addition to case (i)], Slovenia, Bulgaria.

Some of the above mentioned countries associate the Qualified Electronic Signature with security requirements phrased in terms wider than that used by SSCD.

- In this sense, the Austrian law states that Secure signatures must meet the requirements of the written form as defined in the Austrian Civil Code. However, an Austrian Secure signature can be created by using "technical components and procedures which comply with the security requirements as stipulated in the Austrian regulation". This phrase may be understood to mean not only the device used to create the signature strictly speaking (SSCD), but also the overall signing procedure and components of the signature creation application.
- Similalry, Dutch law speaks about "the reliability of the authentication method used". Consequently, any electronic signature which is based on a reliable authentication method has the same legal effect as a handwritten signature. However, the law establishes a presumption in favour of the Qualified Electronic Signature. Thus, a method shall only be deemed "sufficiently reliable" if the signature responds to the functional requirements of the qualified one (same conditions as in the Directive). We note that Dutch legislation is similar to French legislation.

In other countries, the requirements are higher at the level of the definition of the "Advanced" electronic signature.

- This is the case in Polish law which involves the use of an SSCD already at the level of "Advanced" electronic signature (referred to as *Secure* electronic signatures).

- The same approach is followed in the electronic signature acts of Slovenia and the Czech Republic.

Within the third category (iii), two countries can be identified (Italy and Estonia). These two countries refer to one specific technology, namely the "digital signature"-technology.

- Under Italian legislation, digital signatures appear to be on an equal footing with Qualified Electronic Signatures (Qualified Electronic Signatures are explicitly defined, same requirements as in the Directive). Accordingly, an electronic document has full effect as evidence if it is signed with a digital signature or a Qualified Electronic Signature.
- The Estonian digital signatures Act regulates only one type of signature, namely the digital one. This signature is equivalent to the Advanced Electronic Signature of the Directive, with the additional requirement that the digital signature has to determine the time of signing. The Digital Signature of the Estonian law is automatically awarded the legal value of the handwritten signature in any private, business or administrative relations unless a special law prohibits *expressis verbis* such equivalence. Further, the Estonian law provides accordingly a presumption in favour of this signature: thus, any signature fulfilling the requirements of the digital one is deemed to generate the legal consequences of a handwritten signature.

A country actually falling into both categories ii) and iii) is Bulgaria.

- Bulgarian electronic signatures legislation makes a distinction between three levels of signatures - the electronic signature (*de facto* equivalent to the Advanced Electronic Signature of the Directive), the qualified one (similar to the "qualified" electronic signature of the Directive) and the "Universal" electronic signature (a "qualified" electronic signature based on a certificate that is issued by a CSP registered under a special procedure). The Bulgarian law explicitly states that Advanced and "qualified" electronic signatures are equivalent to handwritten signatures mainly between private parties. On the contrary, a Universal signature has the effect of the handwritten one even in relations with and between state and local authorities (unless the Council of Ministers decide for another type of electronic signature to be used in a particular context). It appears, therefore, that according to the Bulgarian law:i) Advanced and "qualified" electronic signatures are on an equal footing but have a limited scope of use, whereas Universal signatures (entailing extra procedural requirements for CSPs issuing Qualified Certificates) have the legal value of handwritten signatures in all circumstances.

iii. Only equivalency if electronic communication is admitted

In Scandinavian countries the legislator likes to confirm the more or less evident principle that a Qualified Electronic Signature will only be considered as equivalent to a handwritten signature in those cases where the law admits the use of electronic means. This is the case in Denmark, Sweden and Norway.

- Under Swedish legislation, a prerequisite of accepting the equivalence between the Qualified and handwritten signature is that the legal requirement for a handwritten signature can be satisfied by electronic means. Accordingly, a "qualified" electronic signature does not automatically meet the requirement of "affixing a (handwritten) signature", but only in the cases in which, the law allows for the form requirement to be met by electronic means.
- Danish legislation lays down the same conditions. Further, it stipulates that, once the conditions are met, this rule applies equally to the exchange of documents to or from the public authorities, unless special legislation provides otherwise.
- Norwegian legislation has adopted a similar approach. The equivalence between handwritten and Qualified Electronic Signatures is not founded on absolute terms, but only if two conditions are met: i) the law requires a signature for an act to produce its legal effects and ii) electronic communication is allowed in the area the act is referring to.

iv. No explicit transposition

In a few countries, Article 5.1 of the Directive has not explicitly been transposed. This is the case in the UK, Ireland, the Czech Republic and Switzerland.

- As far as the UK and Ireland are concerned, the non-transposition of Article 5.1 as such does not mean that an electronic signature is not recognised as able to produce the legal effects of the handwritten signatures. On the contrary, in both legal systems any electronic signature can be considered as the equivalent of the handwritten one, insofar as they can ensure fulfilment of the functional requirements of a signature.
- Since UK law does not recognise the concept of a "handwritten signature", there has been no need to explicitly recognise by law that an electronic signature could act as an equivalent or indeed alternative. However, various legislative acts have generally recognised that an electronic signature is a valid form of signature in the legal area in question.
- Irish legislation stipulates that any electronic signature can be used in place of, and with the effects, of the handwritten one provided that: i) the recipient consents to the use of an electronic signature and ii) in cases where the recipient is a public body or authority, any information technology or procedural requirements imposed by that body are respected. On the contrary, Irish law lays down specific (and rather stringent)

functional requirements if electronic signatures are to be witnessed electronically and for the electronic sealing of documents (e.g. the signature to be witnessed has to be an advanced one).

- On the other hand, the electronic signatures Act of the Czech Republic has adopted a rather narrow approach when determining the legal effect of the Guaranteed electronic signature (being the equivalent of Advanced Electronic Signatures under Czech law). Accordingly, the law states that the application of a guaranteed electronic signature based on a Qualified certificate and secured signature creation enables the recipient to verify whether a data statement has been signed by a person specified in the Qualified Certificate. It seems that, given that "handwritten signatures" are not known in the Law of the Czech Republic, it would be superfluous to provide for (automatic or not) equivalence between handwritten and electronic signatures.
- Finally, in Switzerland, the Ordinance regulating the provision of electronic certification services - currently, the only law relating to electronic signatures - does not refer at all to any "equivalence" between handwritten and electronic signatures. It is noteworthy, however that the draft law on electronic signature under preparation seems to introduce the legal equivalence in so far as a Qualified Electronic Signature (named expressly as such) is based on a Qualified Certificate of a recognised (accredited) Certification Authority.

2.2.2.3 Conclusion

There has been a general tendency in the majority of European countries to explicitly recognise the equivalence between a handwritten signature and a specific "type" of signature (by imposing the sameor slightly different conditions than those stipulated in Article 5.1).

Various means have been chosen for this transposition. An implementation *in verbatim* of Article 5.1 has been followed in a number of states. Other countries have begun to amend their generic laws (notably, Civil Code and Code of Civil Procedure) in order to: i) introduce the legal equivalence of a certain level of electronic signatures to the handwritten ones and/or ii) to establish the general principle of admissibility and legal effect of electronic documents.

Concerning the recognition of equivalence as such, in a number of countries the probative value recognised to qualified or "digital" signatures is even stronger than the one inherent to handwritten signatures (e.g. Italy). In some countries the equivalence is expressly stated in law to apply in both the procedural and substantial law (e.g. France, Germany, Greece, Malta), whilst in other cases the question is left open to interpretation under national law (Poland, Czech Republic, Switzerland).

It has already been noted that most European countries already recognise those electronic forms of signature meeting the functional requirements of the Directive. In a number of

countries, however, the types of the electronic signatures as recognised in national legislation, and in some cases the inherent security characteristics of these types, differ from those of the Directive (e.g. the "Secure" electronic signature verified by a QC in Poland). In many cases, only the terminology used is different (e.g speaking about "extensive" or "secure" electronic signatures rather than "Advanced" in some countries), while the functional characteristics to be met remain in substance the same as in the Directive. In a few cases, nevertheless, national electronic signatures laws have translated in somewhat stricter terms the functional requirements that lead to the assumption of the legal equivalence. In isolated cases, extra conditions have directly or indirectly been stipulated (e.g., "Recognition" of CSPs through a specific procedure for "Universal" electronic signatures in Bulgaria, accreditation of CSPs in the draft Swiss law). Given these divergencies, the question of whether Article 5.1 has been faithfully transposed in the given legal system, has to be examined in the light of the overall legal principles and rules governing the probative force of the handwritten signatures in the country concerned.

In a few countries, the equivalence is granted to "lower" or "higher" levels of signatures than the Qualified Electronic Signature of the Directive. Accordingly, the "Advanced" electronic signature (Bulgaria) or the digital signature (Italy, Estonia) are automatically be awarded the effect of the handwritten signature. On the other hand, "Universal" electronic signatures in Bulgaria require extra requirements.

2.2.3 Non-discrimination rule (Article 5.2)

2.2.3.1 State of implementation in Europe

i. Explicit transposition of Article 5.2

The majority of the EU Member States (Austria, Belgium, France, Greece, Luxembourg, the Netherlands, Ireland and Italy) have provided for an explicit provision translating the rule of Article 5.2.

- It is noteworthy that two countries (Belgium and France) expressly confirm that an electronic signature is a valid form of signature for evidential purposes so long as it can ensure certain functions (being that the author can be identified as well as the integrity of the data to be signed). In addition, Belgium reiterates the wording of Article 5.2 in an explicit provision.
- Under Irish law, the effect of Article 5.2 has been implemented by various provisions but there is also an explicit confirmation in law recognising the legal effect, validity and enforceability of information being in electronic form.

Almost half of the accession countries (Latvia, Lithuania, Poland, Slovenia, Malta, Liechtenstein - draft law -) have also transposed Article 5.2. without any significant variations from the Directive.

- A comment can be made with regard to Malta. The Maltese law on electronic signatures recognises the legal effect of the electronic signature in general whilst it does not state anything with regard to the admissibility of such a signature. However, it shall be inferred that the term "legal effect" of the electronic signature is meant in this case in its broadest sense and, consequently, it covers admissibility.

ii. Non-explicit transposition of Article 5.2

Some EU countries (Denmark, Germany, Portugal, Spain, Finland and Sweden) have not expressly implemented Article 5.2. However, it seems that this is a deliberate omission on behalf of the national legislator, since these national legal systems have already recognised prior to the enactment of the Directive the legal effect of electronically signed documents, in some cases even without restrictions.

- In Germany, for instance, the probative value of documents bearing any kind of electronic signature is determined by the effective security that the given signature can ensure. The "adequate" or not security can be proved on a case-by-case basis.
- It is to be noted that under Portuguese law, the evidential value of electronic documents that do not bear a Qualified Electronic Signature certified by an accredited CSP shall be assessed under the general terms of law. However, it is not clear from the law what would be the evidential and legal value of an electronic document that bears an electronic signature and is certified by an accredited CSP.

As far as the EEA countries are concerned, Switzerland and Norway have not implemented Article 5.2. Similarly as far as the EU Member States mentioned above are concerned, it seems that the basic reason for this failure is once again that these countries recognise the system of free evaluation of evidence by the judge.

As for the Accession countries, the Czech Republic has not implemented the rule, whilst Hungary has partially done so. Estonia is a rather particular case:

- Under Czech legislation, the use of electronic signatures as a means of evidence is unlimited (also, in criminal proceedings). The only restriction to this use are the legal acts that require an "official attested signature" in order to be legally binding - in other words a signature done by a notary.
- On the other hand, the Hungarian law stipulates that an electronic signature shall not be denied legal effect, admissibility or suitability for making a legal statement solely on the grounds that it exists in electronic form.

- The Estonian Digital Signatures Act recognises only digital signatures, which means that any other kind of electronic signatures not complying with the Act have no explicit legal value and their use is unregulated. However, in the light of the principle of the free form and consideration of evidence that governs the Estonian legal system, any piece of information (signed or not) may have a legal value that will be assessed on an *ad-hoc* basis.

As far as Candidate countries are concerned, Bulgaria did not need to transpose Article 5.2 since any electronic signature falling within the definition of "electronic signature" of the Bulgarian law is not deprived of legal effects.

- However, it is noteworthy that in this respect that the Bulgarian electronic signatures Act already relates its "basic" electronic signature with specific functional requirements (being *de facto* equal to the Advanced Electronic Signature of the Directive). Consequently, electronic data signed with a non-secure electronic signature will be considered "unsigned" under the Bulgarian law. However, the authorship of such "unsigned" data can be proved by all means provided for in the Bulgarian legal system in the same terms as a party is asked to prove the probative force of any electronic signature under Article 5.2 of the Directive.
- Finally, Romania narrows down the scope of Article 5.2 by recognising documents bearing an electronic signature (signature that does not necessarily respond to the functional requirements of Article 5.1) the effects of an authentic document between those who signed it or those who represent their rights (relative probative effect).

iii. Partial transposition of Article 5.2

UK regulations on electronic signatures address the admissibility of electronic signatures but not the legal effectiveness thereof. As has already been mentioned above, any signature (including any electronic signature) under the UK legal system is admissible as evidence. However, the legal effectiveness of electronic signatures is addressed through specific Orders. In the absence of specific legislation, the probative value of the electronic signature shall be decided by court on an *ad-hoc* basis.

2.2.3.2 Conclusion

Only eight countries have correctly transposed Article 5.2 of the Directive. The rest only took the prohibition of discrimination of electronic signatures as such into account or else state in their national laws that all kinds of electronic signatures, other than the Qualified Electronic Signatures, will be examined by the courts on a case-by-case basis.

The fact remains, however, that Article 5.2 contains much more. It also prohibits the rejection of electronic signatures on the sole ground that they are not based upon a Qualified

Certificate, or that the certificate has not been issued by an accredited Certification Service Provider. Moreover it prohibits not only discrimination of electronic signatures as evidence in court proceedings but also the adoption of legal instruments denying legal effectiveness thereof. For instance, non-Qualified Electronic Signatures.

2.2.4 Progress monitoring of relevant case law

2.2.4.1 Status of case law development

Given that the Directive is still in the early phase of implementation, and given the limited use of electronic signatures (see chapter "electronic signatures in practice"), it is still too premature to talk about a solid jurisprudence at national or EU level addressing the legal effect of electronic signatures. Few are the countries in which this issue has ever been tackled before the national courts. Even more than that, in cases where the legal validity of the electronic signature has been brought to judgement, it is difficult to yet anticipate : i) whether these rulings reflect the beginning of the formation of a new jurisprudence regarding (electronic) signatures law or ii) whether they are *ad-hoc* reflections that the court made in consideration of the facts and specific circumstances of the case at hand.

2.2.4.2 Description of developments on a country level

In only a few countries has the meaning and validity of an electronic signature been tackled directly in court.

- In Germany, a judge was asked to consider the evidential value of unsigned e-mails.[42] The German courts decided not to award unsigned e-mails any probative force. To come to this conclusion, the German judge looked ultimately at the knowledge and intention of the defendant and found that these elements were indeed the decisive ones to conclude whether the functions of the signature were fulfilled even without a signature being physically attached to the document.
- In a similar vein, the Italian Supreme Court[43] ruled that an unsigned electronic document constitutes full evidence of the represented facts, unless proof to the contrary exists.
- In Greece, the Court of First Instance in Athens[44] admitted that recognition of a debt submitted to the other contractual party in the form of an electronic message (e-mail) is a legal act binding the debtor. In this ruling, the Greek judge accepted that an e-mail

[42] AG Bonn, Decision of 25 October 2001.

[43] Supreme Court Decision, n°. 11445 of 6 September 2001.

[44] Decision 1327/2001.

address satisfies the legal functions of a signature (unique identification of the signer, unique link between the signatory and his e-mail address) and, thus, can be considered as the electronic equivalent of the handwritten signature. According to the Greek judge, the inherent security problems (e.g. risks of third party intrusions to the computer and e-mail system) that could possibly constitute a hindrance to the recognition of such equivalence should not be considered as a "weakness" of the e-mail (electronic signature) *per se* but rather as a risk that should normally be borne by the message recipient.

- On the contrary, confronted with the same question the Dutch judge ruled that the e-mail message could not be granted any legal value because of the evident security risks of the e-mail communication (especially, within open systems).
- Similarly, a Greek and Lithuanian judge, were asked to pronounce on the legal effect of a PIN code when it is used together with a payment card; in this case, he accepted that the PIN code used in electronic payments can be regarded as an equivalent to the electronic signature.
- In Finland, disputes submitted thus far to national judges concern the admissibility and legal enforceability of documents (signed or not) transmitted through electronic means, mainly facsimiles. Another question tackled by the Finnish courts was whether specific types of documents (e.g. petitions of appeal or other documents exchanged in judicial procedures) can be delivered by electronic means.
- Concerning the value of documents used in or exchanged through court proceedings, there has also been a decision of the Tallinn Administrative District Court in Estonia ruling that digitally signed documents must be considered equivalent to handwritten ones in court proceedings.
- In the same context, a UK Court confirmed by a ruling in *obiter dictum* that an electronic signature in a computer generated facsimile would have satisfied the requirements of the Insolvency Act in terms of signing a proxy voting form. Further, it has also been made clear in a recent ruling of the UK Appeals Court[45] that the conclusion of whether or not a contract is binding does not only relate to the use of a (handwritten or electronic) signature but should primarily depend on the intention of the parties. In other words, all elements necessary to make a contract may well exist within e-mail exchanges, as may not, depending on what the real intention of the parties was.

[45] Case Pretty Pictures Sarl v. Quixote Films Ltd [2003], EWHC 311 (QB).

- The legal value of the electronic signature was explicitly pronounced in Spain, where the Court of First Instance of Madrid ruled that an electronic contract between private parties was null and void on the grounds that it did not bear an electronic signature.
- In Sweden, the Administrative Supreme Court ruled that an electronic signature does not suffice for an administrative legal act to be valid, insofar as the administrative law requires a handwritten signature. In other words, the Court affirmed the general rule of the Swedish electronic signatures law that an electronic signature can be regarded as the equivalent of a handwritten one, on condition that the legal requirement satisfied by the handwritten signature can also be satisfied by electronic means. By ruling thus, the Court did not go any further in determining what functional requirements the electronic signature should fulfil in order to have probative value.

2.2.4.3 Conclusions

So soon after the implementation of the Directive into national legislation, national courts are yet to be seriously confronted with issues regarding the legal value of electronic signatures or electronic documents in general. It would therefore be premature to jump to early conclusions on the position of national judges on the four critical issues outlined below:

- the admissibility and probative value of electronic documents;
- the admissibility and probative value of electronic documents signed with an electronic signature;
- the meaning and legal effects of an electronic signature in general;
- the (added or not) legal value of an Advanced or Qualified electronic signature.

Until now, the sample of case law tackling directly or simply evoking electronic signatures issues is still too small and fragmented to be considered as representative enough of the judge's mind in this area.

Ultimately, by adopting a functional approach, the Directive leaves open the ground to varying, if not diametrically opposed, interpretations of national jurisprudence. It has been shown for instance that according to one national judge an e-mail address was found to satisfy adequately the signature functions. According to another national judge it is deprived of any legal value. It is, however, striking that although both opinions emphasise the notion of "security" and whether or not an e-mail may satisfy this requirement they, nevertheless, end up with contradictory conclusions. Since, in the absence of a common harmonised interpretation, they define separate (based on their own experience and jurisdictional culture) interpretations of what "security" may or may not mean.

It would appear that based on the Directive's current text, these varying approaches seem unavoidable. However, it is difficult to prejudge at this stage whether such variations should be

considered as the fruit of chance, due mostly to the judge's inexperience before this kind of question, or whether they actually reflect more profound divergences between the countries' legal traditions difficult to streamline at a European level.

2.3 Liability issues (Article 6)

2.3.1 Transposition of the special liability clause

2.3.1.1 Reminder

The Directive provides for a specific liability rule concerning the supply of certification services of CSPs which issue Qualified Certificates to the public (Article 6). No other market category (e.g. manufacturers or suppliers of signature creation devices or other products) fall within the ambit of this Article or by any of the other special clauses.

Specific and minimum grounds for liability are stated in Article 6 which is related to a "reversed burden of proof" to the detriment of negligent CSPs. Any third party having reasonably relied on a certificate issued by the negligent CSP may benefit from this provision.

The Article sets out specific CSP liability limitations to be transposed by the Member States into national law. These limitations concern the scope of use of the certificate and the value of transactions for which the certificate can be used.

2.3.1.2 State of implementation

With but a few exceptions (France and Portugal), all EU Member States include explicit liability clauses implementing Article 6 of the Directive in their electronic signatures laws and regulations *per se*.

- In France, a new Bill on "Confidence in the digital economy" is currently under discussion and provides for an explicit provision that will transpose Article 6 of the Directive literally into national legislation.
- In Spain, although the current electronic signatures law includes a liability clause, this addresses liability to all CSPs (issuing QC or not) through a general liability clause (the scope of the provision covers any injury or loss caused to certificate holders and third parties). However, the Spanish liability provision lays down the reversed burden of proof (CSPs are held liable unless they prove their non-negligence). It can therefore be concluded that Spanish legislation has provided for an express liability clause for CSPs but based on a much wider basis than that of the Directive.

A similar approach is followed in the large majority of Accession and Candidate countries, with the exception of Cyprus which has yet to transpose the Directive and Poland and Estonia.

Switzerland is another country, which, as with Spain, has followed a wider approach in the transposition of the article in the draft electronic signatures law (the Swiss provision in question covers all CSPs and establishes a "reversed burden of proof" against them for any infringement of this law).

Other than those cases which have already been outlined above the liability clauses laid out in national legislation, by and large, incorporate the essence of the Directive's Article 6.

2.3.2 Scope of implementing provisions

2.3.2.1 Description

Article 6 of the Directive covers CSPs who issue Qualified Certificates to the public or which guarantee such certificates. The injured party to benefit from the reversed burden of proof laid down in this Article may be any entity, legal or natural person who reasonably relies on the certificate. The Directive does not clarify further: i) whether signatories shall be considered as covered in the notion of "relying party", ii) the actual evidential impact of "reasonable reliance", leaving to the national legal systems the interpretation of such conditions (if implemented as such in national laws) in the light of the national legal principles and/or jurisprudence. We examine hereunder one by one the transposition of all elements of Article 6 that condition the applicability of this provision:

i. CSPs issuing Qualified Certificates to the public or guaranteeing such certificates

Concerning those categories of CSPs caught by the special national liability clauses, most of the EU Member States[46] restrict the applicability of these provisions to CSPs issuing/guaranteeing Qualified Certificates to the public.

The Accession countries, Lithuania, the Czech Republic, Slovenia and Malta make a distinction between liability of CSPs in general and special liability of CSPs issuing QC in terms of the Directive.

- It is noteworthy that those countries who are still to transpose Article 6 *per se*, have opted for general liability rules (e.g. Poland: "any failure to comply with CSPs' obligations" or "any performance of CSPs' obligations with negligence") or enlarged lists of liability clauses including, most of the time, the liability clauses spelled out in Article 6 of the Directive.

[46] The only exception seems to be Spain, where the legislation contains a special liability provision for all CSPs.

- In Lithuania (being considered as country having implemented Article 6), the situation inclines more than in the rest of countries having adopted generic liability rules towards the spirit of the Directive: Although the corresponding section of the electronic signatures law about liability covers all CSPs, the list of liability clauses established in the section applies only to CSPs issuing Qualified Certificates.
- Another particular case is Latvia where they have established a liability clause for CSPs that only issue and not guarantee QC.

From the Candidate countries, Romania adopted the scope of Article 6 (CSPs issuing/guaranteeing Qualified Certificates), but without specifying explicitly whether the presumption of "causality" should also apply in the case of Qualified CSPs that supply certificates to specific user communities ("closed user groups") on the basis of contractual relationships and not to the public. On the other hand, the liability provisions of the Bulgarian electronic signatures legislation applies to CSPs issuing both Qualified and Universal certificates (Qualified certificates issued by a CSP registered through a special procedure before a special authority).

From the EEA countries, the Norwegian liability clause applies to CSPs issuing Qualified Certificates both to the public and within a restricted users' group.

ii. Any entity, legal or natural person reasonably relying on the certificate

The rule of "reasonable reliance" (any person reasonably relying on the certificate may benefit from the reversed burden of proof established by the liability clause) has been explicitly transposed in the liability provisions of most of the EU Member States.

In a few cases, the rule of "reasonable reliance" has been transposed either through a similar phrase (e.g. in Austrian electronic signatures law: *bona fide* trust in the certificate) or it is considered inherent to the general principles of evidence in a few countries (e.g. Sweden and Finland).

- No indication of the "reasonableness condition" can be found in the Hungarian law.
- Norwegian law assumes a similar approach and uses the word "normal" instead of "reasonable" (reliance) that may result in a narrower application of the liability clause (the expectations of a third party relying on the normal use of the certificate are probably different from what a user may reasonably expect from a certificate, but of course it shall be examined if such an assumption is confirmed by the Norwegian legal doctrine or jurisprudence).

In a few countries, it is either explicitly stated or can be implicitly inferred that signatories can also benefit from this provision against negligent CSPs.

- This is the case under Danish and Hungarian law.

- Estonia transposed the rule even more amply, since CSPs can be held liable for any patrimonial damage caused as a result of violation of the obligations of the service provider.

2.3.2.2 Conclusion

It is noteworthy that most of those countries here examined have, by and large, transposed Article 6 of the Directive following its strict applicability and scope. In other words the provision of services by CSPs supplying or guaranteeing Qualified Certificates to the public. Even in those countries where any category of CSPs may be considered subject to explicit liability clauses, this has been done in line with a general duty of compliance including obligations specified in the (electronic signatures or other) national legislation, not with respect to the transposition of Art cle 6 of the Directive *stricto sensu.*

Bar a few exceptions, the national clauses transposing Article 6 address the liability of CSPs issuing Qualified Certificates to the public, not to specific user groups but rather through contract relationships. In some isolated cases (Norway, Romania…), the presumption of "causality" can be used against CSPs offering certificates to the public or through contract with specific user groups. Further research is needed as to whether broadening the ambit of the "presumption of causality" clause to the last category may be deemed to be in conformity or not with the Directive.

2.3.3 List of liability causes

2.3.3.1 Description

Below, three transposition streams have been distinguished

(i) Countries which have transposed the list of liability grounds of Article 6.1 in an identical or similar way as the Directive

(ii) Countries which have amplified the list by including the scope of Article 6.2 (omission to register revocation of QC).

(iii) Countries which have extended the scope of the list (by adding other liability clauses as specific failures or "omissions to act".

i. Countries having transposed the list of liability grounds of Article 6.1 in an identical or similar way as the Directive

Most of the EU Member States provide for specific liability clauses and most of them follow the Directive's exact wording (Belgium, Greece, Ireland, Italy, the Netherlands, United Kingdom). The same is also true for the transposition of liability clauses in Ireland, with the sole

difference that wherever Article 6.1 refers to Signature Creation/Verification Data, the Irish provision refers to Signature Creation/Verification Device.

On the contrary, the laws of most Accession, Candidate countries and EEA countries (with the exception of Iceland transposing literally the list of liability causes) fall under one or all the two of the categories referred to below.

ii. Countries having amplified the list by including the scope of Article 6.2 (omission to register revocation of QC).

In a number of countries the omission to register revocation of the certificate is included in the list of liability causes either in the form of an "omission to act" or as an infringement of a positive duty.

In the EU Member States, this is the case in Austria, Denmark, Luxembourg, Finland and Sweden.

- Under the Danish electronic signatures law, the failure to revoke the expired or invalid certificate is spelled out as a separate case, in addition to the causes listed in Article 6.1.
- The obligation of immediate revocation of the certificate (at the request of signatory or for other reasons) and of mentioning the exact date and time of issue and/or revocation are spelled out in the Swedish liability clause, which, for the rest, reflects by and large the Directive's causes.

From the Accession countries, inclusion of the omission to register revocation can also be found in the Slovenian and Lithuanian law and from the EEA countries, in Norway and in the draft regulation of Liechtenstein. The practical legal consequence of such a transposition is that it may lead to an extension of CSPs' liability guaranteeing or issuing QC. This implies that a CSP which guarantees the certificate of another CSP may even be held liable for the first CSP's failure to register a certificate in the revocation list.

iii. Countries having extended the scope of the list (by adding other liability causes as specific failures or "omissions to act").

In a few EU Member States and in most of the Accession and Candidate countries, the list for ground of liability is larger than that of the Directive.

- Accordingly, CSPs in Denmark are held liable on the grounds of the special liability clause if they communicate wrong information on 1) whether the certificate has been revoked and when (expiry date) or 2) whether the certificate includes limitations on the scope of use or the value of transactions for which the certificate can be used.

- On the contrary, German electronic signature law does not provide any list. Rather it establishes liability in cases of "infringement of the requirements as spelled out in the electronic signatures regulation and failure of the CSPs' products for Qualified Electronic Signatures or other technical security facilities". It can be inferred from this that the Directive's grounds for liability are actually included in the scope of the German general provision. Accordingly, the omission is worded in more generic terms, as CSP failure to supply a correct directory or revocation service.

In the case of the Accession Countries where liability clauses are also laid down according to a list (Czech Republic, Estonia, Hungary, Lithuania, Slovenia, Latvia and Malta), one can note that:

- Czech law includes a list of liability clauses as stipulated in Article 6 of the Directive, as well as in Annex II (requirements for CSPs issuing Qualified Certificates).
- Hungarian electronic signatures legislation stipulates expressly under the terms of liability that a CSP has a duty to: i) inform users about the terms and conditions of the certification service and on the publication, revocation, suspension of certificates, ii) keep records related to certificates, iii) maintain a continuous service and iv) use of SSCD in the framework of provision of advanced services. For the rest, Hungarian law adopts the Directive's liability causes
- Latvian special liability provision sanctions, other than the causes stipulated in Article 6.1 say that , i) any infringement of non-compliance with laws and regulations and conditions of certificates' delivery as provided in the register and ii) any undue use of the signature creation and control data.

The list of liability grounds has also been lengthened in two of the Candidate Countries:

- Bulgarian law provides for CSPs to be, in all cases, responsible for the correspondence between the signature creation data and the signature verification data, irrespective of whether they have generated them or not (condition laid down in Article 6). Furthermore, the special liability grounds encompass all cases of non-performance of the statutory duties (sufficient financial resources, usage of trustworthy systems, etc.) that the Bulgarian law defines for CSPs.
- Romanian law broadens the scope of Article 6 further, since it adds to the special liability clause several duties and obligations that CSPs must fulfil when operating their services, including the requirements of Annex II.

Additional omissions or failure to register revocation of certificate are stipulated in a few laws, for instance in:

- Swedish law - failure to ensure precise date/time of certificate's issuance/revocation
- Hungarian law - failure to inform the users about terms and conditions of service

- Bulgarian law - omission to perform some obligations spelled out in law requiring CSPs' action, - e.g. obligation to issue a certificate if all requirements are met and verified, obligation to register certificate under directory.
- Austrian law - failure of a CSP to comply with specific duties regarding the reliable provision of certification services and/or of the signature creation components and procedures. Such transgressions are caught by the liability clause transposing Article 6.1.

The most important implications of these additions is the presumption of causality being extended to cover many more cases of liability "due to failure or omission" than that spelled out in Article 6.2.

2.3.3.2 Conclusion

It is noteworthy that all countries have been diligent when including the liability grounds as defined in Article 6. They have chosen from three different streams:

i) To provide a list of the Directive's liability grounds associated with a reversed burden of proof. This is the case in the majority of European countries surveyed.

ii) To add additional duties and obligations to the list of Article 6. Generally speaking, this is the case in most of the Accession and Candidates countries, but also in a few EU Member States (Denmark, Sweden). In some countries, the liability clause is far too broad (the Czech Republic, Romania) since the presumption of causality can actually be used on the occasion of any failure of CSP to comply with its duties/obligations as provider of Qualified Certificates (Annex II of Directive).

iii) To use general liability clauses (e.g. Germany) without laying down a list of liability grounds but implying, in this way, that the Directive's minimum liability rules are included in the sense of these generic provisions.

As to the content of the liability grounds, it is striking that many countries have added as supplementary cause CSPs' obligations with respect to the revocation/suspension of certificates (e.g., obligation to communicate related info, etc.). Other countries sanction under this more severe liability clause any omission or infringement of CSPs relating to the issuance of Qualified Certificates (Annex II) or to the provision of reliable certification services in general.

Broadening the list of liability grounds is authorised by the Directive (see Article 6 and Recital 22). Nevertheless, heavier liability regimes may act as a deterrent to the establishment of CSPs in the countries where stricter rules apply. On the other hand, linking generic liability rules with the presumption of causality as established in Article 6 may result in a considerable fragmentation of the internal market since: i) CSPs will have to take the rules of evidence into

account depending on which country they or their subcontractors are established in ii) the presumption of "causality" will turn out to become the rule rather than the exception (which seems to be the intention of the Directive) in the cases in which any infringement or damage can be considered as falling within the general liability clause as is currently the case in certain countries.

2.3.4 Burden of proof

2.3.4.1 Description

With respect to the liability grounds and omissions addressed in Article 6, the Directive introduces a reversed burden of proof in favour of the injured party: Any party who relied on the certificate and suffered damages because of this does not need to demonstrate the cause of the damage if the latter arise from the list of liability causes set out in Article 6. The CSP will be considered *de facto* liable in relation to these liability causes ("presumption of causality"), unless he is able to demonstrate that he has not acted negligently ("refutable presumption").

2.3.4.2 State of implementation

Most of the countries examined have included the reversed burden of proof liability in their legislation as provided for by the Directive. It is noteworthy that those countries which have transposed this rule have also interpreted it in a correct manner. In other words - it is up to the plaintiff to prove the exact nature and extent of the damage done. Once the exact cause of the damage has been established, the CSP will automatically be held liable for having caused the said damage. All countries have established this presumption as refutable, meaning that the CSP is entitled to counter-prove that he has not acted carelessly [the meaning and degree of care that a CSP shall display is defined in national laws and jurisprudence].

- Estonia is one of the countries that regulate the liability of CSPs through a general clause ("Service providers are liable for patrimonial damage which is caused as a result of violation of the obligations of the service provider"). Compared to the Directive, no presumption of causality is explicitly established against negligent CSPs and the national rules of evidence apply.
- Maltese liability clauses provide expressly for a presumption of liability only in connection with failure to register or publish revocation or suspension of the certificate. The "reversed burden of proof" relates to a CSPs' failure to comply with the other liability duties as laid down in the Article and is founded not in the liability clause itself but in the general principles governing Maltese law.

- On the other hand, Hungarian legislation (see section above) establishes a reversed burden of proof also in relation to additional liability causes provided for in Hungarian legislation

2.3.5 Limitations of liability

2.3.5.1 Description

The Directive provides two limits beyond which the CSP issuing Qualified Certificates cannot be held liable: the first refers to the limitations of use of the certificate and the second to the value of transactions for which the certificate can be used.

The same limitations are recognised in the national legislation in most of the countries examined.

- The United Kingdom on the one hand, and Switzerland and Estonia on the other hand (considered herein as countries that have not literally implemented Article 6, but that provide for CSPs liability in their laws) do not provide explicitly for such exceptions. Estonian legislation stipulates that, CSPs cannot be held liable for damages resulting from the certificate's use or misuse, since certificate holders are presumed to bear such a risk.

In a few countries, further limitations have been inserted.

- For example, Hungarian electronic signatures legislation states that, in addition to the limitations of the Directive, CSPs shall not be held liable for use of the Qualified Certificate outside of the geographical area for which they have been issued.
- Similarly in Poland, CSPs can not be held liable for damages resulting from data contained in the certificate that have been put at the request of the signatory.

2.3.6 General Conclusion

With a very few exceptions, all European countries have provided for a special liability provision transposing Article 6 of the Directive into national legislation. Within the European Union, the respective liability clauses of the EU Member States follows the wording and rationale of Article 6. In cases in which the transposition was not explicit, the general tendency was to provide for stricter liability clauses, by broadening the scope of application of the Article (notably, by extending the list of liability causes as laid down in the Directive).

The option to provide for higher levels of liability higher even than the minimum provisions laid down in the Directive has been followed in the large majority of Accession, Candidate, EEA countries and Switzerland. It is noteworthy that in many cases, the list of liability grounds is much broader than foreseen in the Directive. In a few cases, the list also includes a liability

ground in general terms, sanctioning any CSPs' non-compliance with the rules and regulations regarding the provision of certification services or the electronic signatures law in general.

The result being that the reversed burden of proof, as established in almost all countries under examination, relates in these cases to an "extended" list of liability clauses. Another issue is that European countries appear to have adopted diverging approaches as to whether signatories may also benefit from this special liability clause.

2.4 International aspects (Article 7)

2.4.1 Overview of the transposition into national law

Most of the EU and EEA countries (Belgium, Denmark, Finland, France, Germany, Iceland, Italy, Norway, Spain and Portugal) have transposed Article 7.1 of the Directive almost literally without further precisions and following the alternative conditions of equivalency as spelled out above.

A number of variations have been identified in the following cases:

- Under Austrian electronic signatures legislation, all certificates, including foreign issued ones, have to be verifiable in Austria. As for the rest, it is recognised that all certificates issued within the EU are automatically equivalent to Austrian certificates (provided that their validity can be checked from Austria). On the other hand, QCs of third countries are equivalent to EU/Austrian ones if the same conditions as stipulated in Article 7 of the Directive are fulfilled (provided that the validity of these certificates can also be checked from Austria).
- Swedish electronic signatures legislation reiterates conditions a) and b) of Article 7, but it does not recognise condition c), namely the existence of international agreements mandating equivalency. Another remarkable difference is that the law regulates the "recognition of certificates issued outside Sweden", not outside the Community. However, the Swedish provision transposing Article 7 remedies this restriction by stating as condition that any QC issued by a CSP established within the EEA who is permitted to issue QC are deemed equivalent to QC issued by CSPs established in Sweden.
- The UK and Ireland have not transposed Article 7. According to our correspondent in Ireland, it could be inferred that Irish QCs issued by all CSPs (within the EU, EEA or third countries) that meet the requirements of Annexes I and II of the Directive have equal validity to certificates issued in Ireland.
- The draft bill on electronic signatures of Liechtenstein provides that (as is the case in Austrian legislation) all certificates (issued within the EEA or in another third country) have to be verifiable from Liechtenstein. As for the rest, the draft bill stipulates the same

conditions as article 7 of the Directive. Apart from the recognition of "foreign" certificates, the Liechtenstein act provides an explicit provision on the recognition of "foreign" electronic signatures. The latter is accepted as a secure electronic signature (equal to the QES of the Directive) if it is based on a recognised QC and is created with an SSCD, for which a home or a recognised foreign confirmation assessment exists (issued by a domestic or foreign designated confirmation body).

- In Luxembourg, the recognition of a foreign QC is subject to the same conditions as those outlined in Article 7. The difference is that the voluntary accreditation scheme of the foreign country according to which the foreign CSP has been accredited has to be analysed in Luxembourg before any formal decision is taken on the recognition of equivalency.
- In Switzerland, the current certification services law does not explicitly resolve the issue of recognition of foreign QCs; it only states that this matter is subject to specific international conventions. On the contrary, the new electronic signatures law, currently under preparation, provide explicitly for the recognition of foreign CSPs with some simplifications if the given CSP has already been recognised abroad. CSPs wishing to be recognised as a CA in Switzerland need to be registered in the Registry of Commerce, meaning that they need to have at least a secondary residence in Switzerland. International conventions may provide different alternatives (as provided in Article 7.1 c)). Another difference is that the condition b) (warranty of certificate by an EU CSP) has not been overtaken in the Swiss law: Either the foreign CSP requests that it be recognised (following the same procedure as a Swiss CSP as and when it wants to be recognised) or it acts as an "assistant" to the recognised Swiss CSP (and, consequently, it is not put on an equal footing with Swiss CSPs).

As far as Accession Countries are concerned, it is noteworthy that with the exceptions of three countries (Malta, Hungary and Slovenia), all the other countries have inserted several "variations" on the alternatives put forward by Article 7.1 of the Directive.

- The current Maltese electronic commerce act does not make an explicit distinction between domestic and foreign QCs. Thus, all QCs are recognised as equivalent to Maltese ones, so long as they meet the requirements of the Maltese law.
- On the other hand, Hungary and Slovenia have transposed the conditions of Article 7.1 almost literally as far as non-EU CSPs are concerned. As for QCs issued by CSPs established within the EU, the Hungarian and Slovenian electronic signatures acts recognise the equivalence automatically.
- In the Czech Republic, foreign certificates can be recognised as QCs by a decision of the Ministry of Informatics or if they are "honoured" by a Czech CSP issuing QC [conditions b) and c) of Article 7.1 are also applicable].

- Under the Estonian digital signatures Act, the equivalence between foreign and Czech QC is also recognised by a decision of the Chief processor of the register [condition b) and c) of Article 7.1 are also applicable].
- Under Latvian electronic documents legislation, a third QC is recognised as equivalent to a Latvian one if it has been issued or guaranteed by a CSP accredited according to a voluntary accreditation scheme in Latvia or in an EU Member State.
- Similar provisions to Latvian law are stipulated in the Lithuanian law on electronic signatures.
- Under the Polish electronic signatures Act, no mention is made about obtaining/recognising equivalency through voluntary accreditation. However, the recognition of equivalence is taken upon decision of the Minister of Economy and costs 10.000 EUR.

Concerning the Candidate Countries, it is noteworthy that:

- According to Bulgarian legislation, a foreign CSP issuing QCs shall be "recognised" in the country of its establishment. Alternatively, a Bulgarian CSP must accept liability for actions/omissions of the foreign CSP (being a kind of "warranty", as stipulated under condition b) of Article 7.1). [Condition c) is also covered].
- Romanian legislation expressly specifies that EU QCs are to be recognised automatically. It is, however, remarkable that certificates of non-EU countries are recognised only if the foreign CSP has been accredited according to Romanian law (not of an EU country) or if a CSP established in Romania (not in an EU country) guarantees the certificate. [Condition c) is covered].

2.4.2 Conclusions

With the exception of Ireland, the UK and Malta, (which have not drawn a distinction between domestic and foreign QC), all of the other countries surveyed have prescribed in their electronic signatures or related provisions, specific rules regulating the legal recognition of foreign QC in their territory.

Most of the EU and EEA countries have faithfully transposed the conditions of Article 7.1 establishing equivalency. In only three states (Austria, Luxembourg and Liechtenstein) do the provisions imply extra requirements (possibility to verify the validity of the foreign QC in the territory of Austria or Liechtenstein/ procedure of verification in Luxembourg of the foreign voluntary accreditation scheme to which the foreign CSP has adhered).

In the Accession and Candidate countries the situation appears to be somewhat more complicated.

It is noteworthy that in a number of states under these categories (Hungary, Slovenia, Romania), QCs issued in one EU Member State are automatically recognised as equivalent to domestic ones. In these cases, foreign certificates are thus deemed non-domestic and categorised as certificates issued outside of the EU. In other cases (Latvia, Lithuania), voluntary accreditation [seen as a condition for recognition of QC equivalence] granted from an EU Member State equates automatically to domestic voluntary accreditation.

In the other Accession and Candidate countries, no distinction has been made between EU QCs and QCs issued in a third country. In most of these countries, the tendency has been to impose conditions reflecting the rationale of Article 7.1 only sometimes varying from the conditions of this provision. It is noteworthy, for instance, that in certain cases (Czech Republic, Estonia), the recognition of foreign QCs can also be achieved by the intervention of an authority. Also, in other countries such as Bulgaria, they pay particular attention as to whether the foreign CSP is “recognised” (accredited) or not, whilst other do not include in the conditions granting equivalence voluntary accreditation (Poland).

2.5 Data protection (Article 8)

The Directive seeks to increase user confidence in electronic communication and electronic commerce, by requiring Certification Service Providers to observe data protection legislation and individuals privacy (Recital 24 of the Directive). Article 8 of the Directive reiterates the principle that personal data processing should be performed in line with the European data protection Directive (Article 8.1), which strengthens the data protection rules for CSPs issuing certificates to the public (Article 8.2) and allows for the use of certificates containing a pseudonym instead of the signatory’s real name (Article 8.3).

2.5.1 Basic data protection rules (Article 8.1)

The Directive requires Member States to ensure that Certification Service Providers and national bodies responsible for accreditation or supervision comply with the requirements laid down in the European data protection Directive (Directive 95/46/EC 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).

Most countries have not explicitly transposed this Article 8.1 in to their national electronic signature legislation (e.g. Austria, France, Germany, Sweden, United Kingdom, Norway, Poland, Slovenia, Switzerland). This is not surprising given that the data protection principle has already been implemented by national data protection acts implying that CSPs, accreditation and supervisory bodies are all subject to the general data protection rules. No explicit reference to the European Directive 95/46/EC is necessary as long as this directive has been implemented in the respective countries.

It is nevertheless interesting that in those countries where reference has been made to the compliance obligation in line with European Directive 95/46/EC or its national equivalent (e.g. Belgium, Denmark, Greece, Luxembourg, Portugal, Spain, Switzerland), some countries have limited this obligation to Certification Service Providers whilst forgetting to include the national bodies responsible for accreditation or supervision (Belgium, Denmark, Spain). Although not a complete transposition of Article 8.1, this should not pose too many problems since the data protection rules, if implemented correctly, need to be respected by all players.

2.5.2 Specific data protection rules (Article 8.2)

In Article 8.2, the Directive tightens its basic data protection principles for Certification Service Providers issuing certificates to the public. Indeed, Member States are obliged to ensure that this type of service provider collects personal data only directly from the data subject him or herself or after their explicit consent has been granted and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. Furthermore, the data may not be collected or processed for any other purposes without the explicit consent of the data subject. Since these data protection requirements are stricter than the national general data protection rules (based on the European data protection Directive), these requirements need to be explicitly transposed.

Most countries transpose more or less literally Article 8.2 (e.g. Austria, Belgium, Finland, Germany, Italy, Luxembourg, Hungary, Iceland, Norway, Portugal, Sweden, The Netherlands).

- However, some countries only refer to their general data protection legislation (Czech Republic, Estonia, Lithuania), or even do not refer at all to the general data protection rules (France, Ireland, Poland, Romania, Slovenia).
- In countries, in which no specific electronic signature related legislation exists, data protection is still guaranteed by general data protection legislation (Cyprus). In these countries, the more stringent rules on data protection for CSPs issuing certificates to the public, may not be respected, causing a problem of improper transposition of the Directive, and causing an internal market obstacle.

As a rule, explicit consent should be given by the certificate holder for the CSP to provide third parties with the personal data of the data subject (Article 8.2, last sentence). In some countries, though, the electronic signature law allows legal authorities to require from the CSP the personal details of certificate holders for crime detection or prevention (e.g. Hungary), or in the framework of a civil law action or a non-civil law action (e.g. Poland).

- Further, in the Netherlands, the goal-binding principle does not hold if the processing of the personal data is necessary for fraud detection or if the processing is otherwise required by or through law.

- Although the other countries do not explicitly refer in their national electronic signature legislation to an information duty towards legal authorities, the national criminal procedure laws would impose this kind of general co-operation duty (e.g. Belgium, France). These exceptions on the consent principle are in line with the Directive on data protection and the electronic signature Directive and are indirectly confirmed by Recital (25) of the electronic signature Directive.

2.5.3 Use of pseudonyms (Article 8.3)

Member States are not allowed to prevent Certification Service Providers from using a pseudonym in place of the signatory's name when issuing certificates. This obligation has no impact on the legal effect that would, or would not be given to pseudonyms, within the terms of national legislation. Member States are also still permitted access to identification data relating to the signatories using a pseudonym (Recital 25). As to Qualified Certificates, the Directive states in its Annex I that Qualified Certificates containing a pseudonym, should be identified as such.

- Some countries explicitly allow Certification Service Providers to include a pseudonym (Austria, Germany, Greece) or give users permission to request (Hungary) a pseudonym instead of the real name of the signatory, or simply allow for actual identification data to replaced pseudonym (Italy).
- In most of these countries though, an explicit reference to the use of pseudonyms is only made in the transposition of Annex I, stating that a Qualified Certificate should mention that it contains a pseudonym instead of the real name (Belgium, Czech Republic, Denmark, Finland, Iceland, Lithuania, Ireland, Norway, Poland, Portugal, Romania, Slovenia, Sweden, The Netherlands, United Kingdom).
- Only Estonian and Bulgarian electronic signature legislation forbids the use of pseudonyms in their national rules on Qualified Certificates (or its national equivalent). These laws state that these types of certificates may only be issued to physical persons and must contain the real name of certificate holder.

Most countries require the CSP to mention in the Qualified Certificate that a pseudonym is being used (which is a transposition of Annex I, c of the Directive). Some countries go further and regulate the use of a pseudonym in a more stringent way.

- For example, in Austria the pseudonym shall not be offensive and shall not be open for confusion with other names.
- In Hungary and Germany, the pseudonym may only be used with the consent of the represented person, of the signatory uses an attribute in the certificate stating that he acts on behalf on the represented person. This last approach is interesting, because it clearly shows that the national law-maker intends the use of pseudonyms in

certificates for signing on behalf of another person or an entity, especially for representing legal entities. Originally the introduction of the right to use a pseudonym was meant to be used for performing anonymous transactionsthe pseudonym may only be used with the consent of the represented person. This last approach is interesting, because it clearly shows that the national law-maker also intends the use of pseudonyms in certificates for signing on behalf of another person or an entity, especially for representing legal entities. Originally the introduction of the right to use a pseudonym was meant to be used for performing anonymous transactions.

Many countries explicitly require in their electronic signature legislation the disclosure of real names to the public authorities upon request and under strict conditions (e.g. Austria, Belgium, Czech Republic, France, Germany, Luxembourg, Spain, Hungary, Romania, Slovenia). Indeed, the Directive in Recital (25) permits Member States to request identification of persons pursuant to Community or national law.

In Italy the CSP has to maintain registries with real names for at least 10 years after the certificate's expiry. In any case most countries require CSPs to record all relevant information regarding Qualified Certificates for a minimum time period (Annex II,i of the Directive), this will probably include a requirement to record information about the pseudonym and its "owner" for the same period as well.

2.5.4 Other national data protection rules

Some countries provide for more detailed data protection obligations.

- For example, in Greece the Signature Regulation stipulates that the annual reports submitted by CSPs issuing Qualified Certificates to EETT (in the framework of the supervisory duties exercised by the latter) shall make explicit reference to the measures that CSPs have taken to protect archives and data. In addition, the Regulation states that CSPs issuing Qualified Certificates should describe the procedures they follow to protect confidential information and to process personal data.
- The Italian law also provides explicitly that the CSP has to respect the security measures provided by the Italian personal data protection Act.

Some laws explicitly provide involvement of the national data protection authority in the supervision of CSPs.

- In Finland for example, the Data Protection Ombudsman supervises the compliance with the data protection provisions of the Act on Electronic Signature, and has the right to obtain information and to perform inspections referred to in the Personal Data Act.

Some countries also explicitly mention some confidentiality-professional secrecy obligations (e.g. Romania, Poland,) for the CSP employees, including criminal liability consequences.

2.6 Public sector (Article 3.7)

Article 3.7 of the Directive specifies: "Member States may make the use of electronic signatures in the public sector subject to additional requirements. Such requirements shall be objective, transparent, proportionate, and non-discriminatory and shall relate only to the specific characteristics of the application concerned."

Many countries do allow for specific requirements when it comes to using signatures in the public sector.

- In most cases technological as well as procedural requirements are additionally imposed. In several countries there are application-specific laws and/or regulations concerning the signatures to be used. Mostly they impose the use of electronic signatures based on Qualified Certificates issued by accredited CSPs.
- In Germany long-term provable signatures are mandatory for public entities for a few public administration applications;
- Spanish and Latvian legislation requires that certain electronic documents in the public sector shall be signed using a Qualified Certificate and that they be time-stamped.
- In some Member States (e.g., Ireland, Italy, Portugal, Czech Republic) public authorities restrict applications to Advanced Electronic Signatures based on a Qualified Certificate issued by an accredited CSP or created by a secure signature-creation device.

There is also a risk that public agencies will restrict their application services to specific national CSPs. Such requirements could, therefore, be in possibly breach of Article 3.7 in that they do indeed "constitute an obstacle to cross-border services for citizens."

2.7 Controlling mechanisms (Article 3)

A table summarizing the status of implementation can be found at the end of this chapter.

2.7.1 Prior authorisation (Article 3.1)

Article 3.1 of the Directive states that Member States shall not make the provision of certification services subject to prior authorisation. About half of all the European countries surveyed apply Article 3.1 of the Directive such that prior authorisation of certification services in these countries is explicitly prohibited by law. All other countries fail to have corresponding

regulations in their national legislation. However, the practice of common certification in those countries is still in line with Article 3.1 of the Directive.

2.7.2 Notification of CSPs

Although neither regulated nor mandated by the Directive, most countries (except Ireland, Malta, Latvia, Switzerland, and the UK) generally require CSPs issuing Qualified Certificates to notify their services to some kind of supervisory authority. The notification is usually supposed to happen a few weeks (e.g. 30 days) at the latest before starting to operate or prior to establishing their activities . In most cases the CSP has to submit several documents to the authority, e.g. security concepts, policies, internal documents, and contracts (see summarizing table below).

It is crucial to look very closely at how the notification process is being implemented in each country. The question to ask is whether or not the submission of documents by the CSP is sufficient for starting services or whether a decision by the relevant body is actually necessary. In the latter case, notification would resemble prior or "hidden" authorisation.

As to what kind of CSPs are supposed to notify, the different laws do vary throughout Europe.

- Whereas in many countries (Belgium, Denmark, Finland, Germany, Italy, Luxembourg, Netherlands, Portugal, Sweden, Czech Rep., Estonia, Lithuania, Poland, Iceland, Bulgaria, Norway) only CSPs issuing Qualified Certificates to the public are supposed to inform the supervisory body, there are also a few countries (Austria, Greece, Spain, Slovenia, Hungary, Romania, Liechtenstein) that do require *all* CSPs to notify, regardless of the issuance of Qualified Certificates. Although not conflicting with the Directive's provisions, it can still be regarded as an overzealous implementation of the Directive.
- In Switzerland, the UK, Malta, Latvia, and Ireland CSPs do not need to notify at all although Irish CSPs tend to consult with the relevant bodies as a form of common practice.
- It is interesting to note that, in contrast to all the other European countries, Estonia has established a *mandatory registration* scheme for CSPs issuing Qualified Certificates. CSPs issuing other types of certificates are free to operate in Estonia without any limitation or supervision.

The authority responsible for notification in almost every country is an independent public agency (e.g. ministry or regulatory authority) under the auspices of the government. Only a few countries (Austria, Belgium, Finland, Netherlands, Hungary, Lithuania, Poland, Slovenia) actually require the authority to take any decision after having received a CSP's notification, sometimes even within a fixed amount of time. With respect to the Directive this would be a violation of Article 3.1 if the CSP would have to wait for the decision to be made:

- in Finland, for example, the provision of Qualified Certificates cannot start before the notification is submitted by the CSP to FICORA;
- in Hungary CSPs need to undergo a "qualification procedure" before being allowed to issue Qualified Certificates – this is clearly a de-facto authorisation.

The cost of the notification procedure varies largely throughout Europe: in some countries (Belgium, Spain, Luxembourg, Czech Rep, Romania) notification is free of charge to CSPs whereas in most countries CSPs have to pay an amount of approx. 5 to 15,000 €. Some countries require the fee to be paid on an annual basis. Moreover, in Germany and Austria CSPs have to pay a fee per issued certificate.

With a few exceptions all countries require CSPs to notify the supervisory body about any major changes (e.g. in procedures or security components) in due time. The same is true for a CSP planning to cease operations.

To summarise, notification procedures vary throughout Europe, especially in terms of what kind of CSPs are obliged to notify their services to an authority. Common practice seems to show that some countries (e.g. Austria, Belgium, Romania, Poland, Slovenia) are using the response to notification as some kind of "hidden licensing" or "hidden registration" scheme, thus in reality introducing prior authorisation of CSP services without actually using that term.

Similarly, the documentation to be submitted by CSPs upon notification differs widely in both quantity and detail. Again, there is a risk that Member States may misuse the notification process through requiring detailed documentation to be submitted by the CSP: what happens if the CSP fails to fulfil any or all requirements with respect to the document submission?

2.7.3 Supervision (Article 3.3)

According to Article 3.3 of the Directive, Member States are required to establish "an appropriate system that allows for supervision" of CSPs issuing Qualified Certificates to the public. With respect to the definition of CSPs in Article 2 this means that the supervision covers not only the issuance of certificates but also 'other services related to electronic signatures'.

Every European country (with the exception of Cyprus, which has no electronic signature legislation yet) has already implemented or plans to implement such a supervisory system. The responsible body inside the single countries is identical to the one being notified by CSPs (see previous chapter).

- In some countries (e.g. Switzerland) the supervisory body is a company which needs to be accredited (not to be confused with 'voluntary accreditation') by an independent public authority in order to supervise CSPs.

- In the UK, on the other hand, there is a general provision for "regulation" (as specified in Part 1 of the Electronic Communications Act 2000) which has not been implemented yet. Because of the absence of CSPs issuing Qualified Certificates, a system of supervision according to Article 3.3 has also yet to be implemented.

Similar to the notification process, there is a difference in terms of what kind of CSPs are being supervised (see summarizing table below):

- Many countries strictly follow Article 3.3 in that only CSPs issuing Qualified Certificates to the public are subject to supervision whereas in other countries *all* CSPs are being controlled.
- In Iceland, even CSPs issuing certificates to closed user groups fall under the supervision. Although this is perfectly permissible, it was clearly not the intention of the Directive to have all CSPs supervised.

Large differences are visible with respect to how supervision is actually being carried out. In many countries supervision is based on regular audit controls being done by the supervisory authority and/or external experts on behalf of the authority. However, the details of the audit controls often are unknown as of yet. This is mainly due to the fact that in most countries only very few CSPs have actually started operating. Therefore, the supervisory system has not been established thoroughly.

- In those countries that already have been able to establish supervision (e.g. Austria, Belgium, Denmark, Estonia, Romania), audit controls are being carried out regularly, e.g. annually. Germany, on the other hand, carries out audit controls, if any, only at the initial review process.
- There are a few countries (Greece, Lithuania, Bulgaria) in which supervision is not being realized through audit controls but through investigative measures (either due to an external complaint or on the initiative of the supervisory authority).

Once audit controls are in place the cost of these controls varies too.

- In some cases the CSP has to pay a comparably low fee amounting to a few thousand Euro (e.g. Austria, Liechtenstein), sometimes the fee is based on the hours worked by the supervisory body (e.g. Germany), and in some countries the fee can be as high as 100,000 Euro (e.g. Denmark).
- In a few countries the fee is borne by the supervisory body or related federal authorities; the CSPs thus are not subject to any supervision related fees. This, again, leads to the question of whether or not the payment of the fee actually can be misused to introduce some form of prior authorisation: what happens if the CSP declines to pay the supervision fee? Is the CSP then not allowed to issue certificates?

As to corresponding compliance criteria there are major differences too.

- Some countries (e.g. Iceland, Malta, Norway) did not specify any compliance criteria for supervision at all.
- Others (Austria, Spain, Poland, Slovenia, Switzerland) do measure a CSP's compliance against requirements as laid down in their respective laws and/or decrees. For instance, Slovenia requires a CSP to use products evaluated according to the American standard FIPS 140-1 or according to "recommendable EAL5 or at least EAL3" – this being an over-specified requirement in the legislation, especially since the question of which products need to be evaluated has been left unanswered.
- Finally, a few countries (Denmark, Luxembourg, Estonia and Bulgaria) have published detailed documents containing several criteria which need to be followed.

Most countries use investigative measures as a means of exercising compliance control. These investigations usually carried out following complaints or else are initiated on demand by the supervisory authority. In all countries the authority is subject to data protection laws and general provisions during its supervisory tasks.

Another area of differences throughout Europe is the use of standards by the authority in the supervision process.

- Many of the EU Member States have not specified which standards have been followed. It seems likely that the Member States did not want to wait for other standards to be finalised; they thus used their own ones instead.
- On the other hand most of the non-EU countries have relied heavily on standards which have been published by several organisations, such as EESSI, ETSI, CEN, ISO, and IETF.

In most countries the supervisory system does not differentiate between accredited and non-accredited CSPs (see next section). Only in a few cases (e.g. Germany, Czech Republic) will the initial review be slightly more demanding before CSPs can be accredited. Moreover, there are no major differences when it comes to consequences of non-compliance: most countries do impose injunctions and prohibitions on CSPs who violate any regulations. In addition, most CSPs are subject to fines and similar penalties. The CSP, however, almost always has the possibility to challenge any decision before court. A noteworthy exception seems to be Portugal where legislation does not foresee any consequences.

To conclude, in most countries either only a few (if any) CSPs have been established and actually started issuing certificates - or else supervision is still very much in the early stages of development - or both. Therefore, it is impossible to compare the practical implications of supervision systems. Yet, it already seems obvious that CSPs based in more than one country will be subject to very different supervision rules. Any CSP who wants to establish its company in more than one country will have to adapt to different requirements and procedures.

2.7.4 Voluntary accreditation (Article 3.2)

The Directive allows Member States in Article 3.2 to "introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision."

Many countries indeed explicitly define an accreditation system in their legislation whereas some countries (Denmark, Finland, Hungary, Poland, Iceland, Norway) do not recognise any such concept at all (see summarizing table below).

- With the exception of the Netherlands and the UK the accreditation roles in the European countries are being fulfilled by public bodies such as ministries or other federal agencies (e.g. regulatory authorities for telecommunications as already established in many countries).
- The Netherlands and the UK, on the other hand, have implemented private, self-regulated accreditation schemes named TTP.NL and tScheme, respectively. Whereas TTP.NL has been driven by both public and private organisations, tScheme was created by UK industry. Within those schemes the responsible bodies perform "monitoring" for adherence to the relevant applicable criteria.
- Most voluntary accreditation schemes use accreditation as an enhanced assurance level of supervision, i.e. fulfilling the requirements for issuing Qualified Certificates. This clearly never was the intention when mentioning voluntary accreditation in the Directive.

In practice, voluntary accreditation suffers from problems similar to those faced by supervisory systems, i.e. the small number of CSPs in most countries (except Austria, Germany, Italy) did not lead to many well-established accreditation schemes. Moreover, the process of achieving an accreditation usually takes many months for a CSP. Countries like France, Greece, Ireland, Portugal, Spain, Malta, Latvia, Liechtenstein, and Romania have yet to implement an accreditation scheme in practice. One other reason for the relatively slow deployment of such schemes seems to be the imprecise definition of "voluntary accreditation" in Article 2 of the Directive.

A few side notes:

- In Bulgaria CSPs do have to register with the relevant authority if they want to issue certificates for so-called "universal" electronic signatures (mainly to be used in the public sector).
- In Switzerland CSPs may notify to Certification Bodies which, in turn, are accredited by an Accreditation Organ.
- According to preparatory legislation documents in Norway, it is up to the market to decide whether or not a voluntary accreditation scheme should be implemented. Currently, there seems to be not enough demand for such a scheme in Norway.

- CSPs in Sweden may voluntarily be evaluated/tested against certain standards by a "certification body", accredited by SWEDAC (national accreditation body).
- The Belgian law does not define what accreditation is but refers to accreditation in Articles 17 and 18. Article 17 states "a CSP fulfilling the requirements of Annex II, issuing Qualified Certificates following the specifications of Annex I, and using a secure signature-creation device can ask to be accredited by the Administration."
- In the UK, the term "accreditation" is used in the sense of the assessment of independent bodies ("assessors") which perform certification of services. With UKAS being the accreditation body, schemes like tScheme (which is a voluntary trust-service "approval" scheme) are being accredited in order to perform evaluations/assessments of CSPs. tScheme is essentially co-regulatory by nature in that it is a private sector-led organisation meeting public policy objectives set out in legislation.
- In Italy all the current CSPs have been accredited under the pre-Directive Italian digital signature act. A "new" accreditation scheme, based on the new electronic signature law has not been implemented yet.
- In Luxembourg, the 'Office Luxembourgeois d'accréditation et de surveillance' (OLAS) has published a number of detailed documentation surrounding accreditation of CSPs, requirements for components, qualification of IT auditors and supervision of CSPs issuing QCs. These documents are based on the standards as published within the EESSI framework.
- In the Netherlands, a voluntary accreditation scheme, named TTP.NL, has been established which assesses a CSP's compliance with ETSI TS 101 456. TTP.NL is a self-regulation initiative.
- Slovakia has implemented a *mandatory accreditation* scheme for CSPs issuing QCs.

Once again, the use of accreditation criteria as well as standards differs widely throughout Europe: some schemes seem to be following the more general requirements as laid down in legislation whereas other schemes make use of international standards, e.g. ISO 17799 and EN 45012. In turn, other than in the Netherlands, the EESSI deliverables played a major role in non-EU countries only.

Only in very few countries (e.g. the Netherlands and Malta) is the accreditation body different from the supervisory body, usually both tasks being fulfilled by the same authorities.

As to the validity of an accreditation, in most schemes the accreditation is valid for 3 years, with few systems requiring regular controls during the validity period. Some schemes (e.g. Austria, Italy, Czech Rep., Slovenia, Switzerland) do not impose a limit on the accreditation at all. This means that in some countries CSPs need to get a renewal of their accreditation every few years whereas in other countries the accreditation is not limited at all.

The only explicit right of a CSP after having been accredited is the right to make use of the status "accredited CSP" in most countries. Similarly, there is no explicit evidential value for an accredited CSP in many countries. On the contrary, many CSPs are subject to additional obligations (e.g. extended archival periods) once they have been accredited.

Implicitly, however, many systems definitely encourage their accreditation systems since (qualified) certificates issued by accredited CSPs are being favoured or even required in some areas, e.g. in the public sector.

Within the framework of ViTAS[47] members of several European and non-European schemes are currently discussing a possible Mutual Recognition Agreement, based on common Codes of Practice. However, it is far too early to say what the possible result of this could be.

To summarize, many voluntary accreditation schemes currently are either already in place or in preparation. Some countries expressed their objections to the very term "accreditation" because this term is being used and well established in another context; thus the procedure is named differently (e.g. "approval", "registration", "recognition", or even "certification") in some countries. Comparable to the supervision of CSPs there is no real common accreditation practice established as of yet (except in Austria, Germany, Italy), especially with respect to the European perspective. Moreover, the value of accreditation is being judged very differently: whereas some countries are clearly in favour of voluntary accreditation ("must be regulated") other countries seem to be much more reluctant ("is it really needed?").

Whether or not the existence of different accreditation schemes is an advantage or a disadvantage remains to be seen because of the lack of experiences in most countries. Some countries place very high requirements on their accreditation procedures whereas in other countries accreditation is based on much more general rules to be followed by a CSP. The varying requirements and characteristics of voluntary accreditation schemes in practice means that the effort to set up and operate a CSP under one accreditation scheme will be significantly different to the efforts of other accreditation scheme.

2.7.5 Conformity assessment of SSCDs (Article 3.4)

The Directive specifies in Article 3.4 that the conformity of secure signature-creation devices (SSCDs) with Annex III "shall be determined by appropriate public or private bodies designated by Member States." Moreover, a product assessment "shall be recognised by all Member States."

Article 3.4 does not strictly mandate vendors to undergo a product assessment; it merely states that once an assessment shall be done, it has to be performed by designated bodies, Recital (15) is more clear in requiring "the Commission and the Member States to act swiftly to

[47] Voluntary Trust-service Approval Schemes common interest group, http://www.vitas-cig.org/

enable the bodies charged with the conformity assessment [...] to be designated; in order to meet market needs conformity assessment must be timely and efficient."

- Most countries did interpret the Directive in a sense, requiring an explicit mandatory conformity assessment for signature-creation devices in order to be recognized as SSCDs. The assessment normally is based on the very strict methodology of Common Criteria (CC).
- Noteworthy exceptions to this situation are Spain (with conformity assessment explicitly being of a voluntary nature), the Netherlands and the United Kingdom (which does not know the concept of an SSCD at all, because it does not know the concept of a Qualified Electronic Signature).
- On the other hand, only in a few countries does the legislation explicitly assign an evidential value to SSCDs whose conformity has been assessed. However, an evidential value is frequently present implicit by, for example, relevant statements in civil law.

As to the establishment of conformity assessment bodies, only very few countries (Austria, France, Germany, Czech Rep., Hungary, Lithuania, Poland) have actually designated this task to a relevant authority with a few more countries already planning to do the same. This is mostly due to the fact that the amount of time and money necessary for establishing such an assessment body would be too high an effort for most organisations. All countries, therefore, do (either explicitly or implicitly) recognize those assessments that have been performed by a designated body in another EU Member State, thus following Article 3.4.

- In most countries there is a national accreditation body responsible for appointing other persons or bodies that in turn perform product assessments.
- Interestingly, in Italy there currently exists an assessment scheme for military purposes only. A commercial scheme is under preparation. Therefore, assessment bodies established in other countries are currently performing product assessment in Italy.

The process of assessing a product is usually both extremely expensive (it might cost up to a few hundred thousand Euros for the vendor) as well as time-consuming. In reality conformity assessment is far from being "timely and efficient" as hoped for by Recital (15). Two other reasons why vendors sometimes are reluctant to have their products assessed are the facts that an assessment is usually only valid for a fairly limited amount of time (the product needs to be re-assessed afterwards), and a conformity assessment "freezes" a product such that it cannot be changed (e.g., in order to apply a security patch) without making invalid the assessment. Moreover, due to the time delays during the assessment process the evaluation may not even be performed according to the state of the art with respect to new attacks and countermeasures.

Consequently, although there already are a small number of SSCDs which have been assessed, all of these have been assessed by a relatively small number of designated bodies only. Only in Austria, Germany and the Czech Republic is the number of products assessed more than two. In some countries (Austria, Germany) signature products other than SSCDs have been assessed as well.

To conclude, although not strictly mandated by the Directive, an SSCD assessment is in practice mandatory in most, but not all, European countries (see table below). Closely related to this issue is the question of whether or not an assessment of SSCDs is actually needed in order to declare a product as being an SSCD. Again, the Directive does not mandate this in legal terms but common practice seems to indicate that there will be no SSCDs without formal assessment by recognized bodies. Furthermore, in countries like the United Kingdom SSCDs are not specified in the legislation at all.

2.7.6 Summarizing table

	Notification	**Supervision**	**Accreditation**	**SSCD assessment**
AUSTRIA	all CSPs	all CSPs	yes	yes
BELGIUM	CSPs issuing QCs	CSPs issuing QCs	yes	yes
DENMARK	CSPs issuing QCs	CSPs issuing QCs	no	yes
FINLAND	CSPs issuing QCs	all CSPs (CSPs issuing QCs in practice)	no	optional
FRANCE	CSPs issuing QCs ("crypt. services")	CSPs issuing QCs	yes	yes
GERMANY	CSPs issuing QCs	CSPs issuing QCs	yes	yes
GREECE	all CSPs	all CSPs	yes	yes
IRELAND	No	CSPs issuing QCs (not yet in place)	yes	not yet
ITALY	CSPs issuing QCs	all CSPs	yes	yes
LUXEMB.	CSPs issuing QCs	CSPs issuing QCs	yes	no
NETHERL.	CSPs issuing QCs	CSPs issuing QCs	yes (industry scheme)	optional

	Notification	Supervision	Accreditation	SSCD assessment
PORTUGAL	CSPs issuing QCs	all CSPs	yes	yes
SPAIN	all CSPs	all CSPs	yes	no
SWEDEN	CSPs issuing QCs	CSPs issuing QCs	yes	yes
UK	No	CSPs issuing QCs	yes (industry scheme)	no
CYPRUS	N/A	N/A	N/A	N/A
CZECH R.	CSPs issuing QCs	CSPs issuing QCs	yes	yes
ESTONIA	CSPs issuing QCs (mandatory registration)	CSPs issuing QCs	no	no
HUNGARY	all CSPs	All CSPs issuing certificates to the public	no	yes
LATVIA	No	CSPs issuing QCs	yes	no
LITHUANIA	CSPs issuing QCs	CSPs issuing QCs	yes	yes
MALTA	No	CSPs issuing QCs	yes	no
POLAND	CSPs issuing QCs	all CSPs	no	yes
SLOVAKIA			mandatory for CSPs issuing QCs	yes
SLOVENIA	all CSPs	all CSPs	yes	"not officially"
BULGARIA	CSPs issuing QCs	CSPs issuing QCs	yes	yes
ROMANIA	all CSPs	all CSPs	yes	yes
ICELAND	CSPs issuing QCs	CSPs issuing QCs (incl. closed user groups)	no	yes
LIECHT.	all CSPs	all CSPs	yes	yes
NORWAY	CSPs issuing QCs	CSPs issuing QCs	no	no
SWITZERL.	No	CSPs issuing QCs (voluntary)	yes	no

2.8 Transposition of the Annexes

2.8.1 Annex I: Qualified Certificates

Annex I contains requirements for Qualified Certificates. Most countries have literally copied the requirements of Annex I or specified similar requirements. A few things may be noted:

- In Germany and Switzerland, the certificate shall be signed with a **Qualified Electronic Signature**, not just an Advanced Electronic Signature as specified in the Directive. This means that the CSP must be a natural person, holding a Qualified Certificate and using an SSCD. This has led to the somewhat strange situation whereby the issuer name in a certificate (for example X-Trust) is actually a pseudonym for a person within the CSP organisation.
- In Italy, the regulation instead explicitly refers to “Annex I of the Directive 1999/93/EC”, which means that anyone wanting to find out the requirements has to find a copy of the text of the Directive.
- In Luxembourg, the certificate validity period is limited to 3 years.
- In Spain, the Qualified Certificate is mandated to contain the national identity number.
- In Estonia, the term “Qualified Certificate” is not used, but "certificate" is defined similarly.
- In the Czech Republic, other personal data may only be present with the consent of the signer.
- In Bulgaria only is the use of a pseudonym not permitted and there is no requirement for QC indication. The Bulgarian regulation contains many more detailed requirements of certificate content.
- Only the Netherlands, Lithuania and Bulgaria have explicitly specified ETSI TS 101 862 for the fulfilment of these conditions.

In summary, no serious differences can be found with respect to the transposition of Annex I. However, there is a risk of interoperability problems if technical implementations of Annex I begin to diverge, if ETSI TS 101 862 is not used, or if any other common format for encoding the requirements of Annex I is not met.

2.8.2 Annex II: CSPs issuing Qualified Certificates

Annex II specifies requirements for CSPs issuing Qualified Certificates. Most countries have literally copied the requirements of Annex II. A few things may be noted:

- In Austria and Germany, the regulations contain additional detailed requirements, such as:
    - The CSP is obliged to forward information on products which comply with the requirements for generation and verification of Qualified Electronic Signatures.
    - The CSP may not use a cryptographic module which allows backup of the certificate signing key.
- In Denmark, the regulation contains additional detailed requirements. In the Netherlands, Annex II has been extended with additional requirements. In Greece, there is an additional requirement for a 30 years retention period of records. In Estonia, the regulation contains a detailed but different list of requirements.
- In Spain, there are some additional specific requirements on the CSP for the insurance amount, archiving period (15 years) and information to be given to the certificate holder.
- In Latvia and Bulgaria, the CSP is also required to offer time-stamping services.
- In the case of Slovenia, a detailed regulation is also in force in addition to the copy of Annex II. The detailed regulation includes requirements for a crypto module evaluated according to the American standard FIPS 140-1, and software evaluated according to Common Criteria.
- Finally, in Switzerland similar requirements to Annex II are specified, with additional details, spread out over different regulations.

Only a few countries (the Netherlands, Lithuania, Slovenia, Bulgaria) refer to EESSI and other standards for the fulfilment of the requirements relating to Annex II.

To conclude, the varying requirements for CSPs mean that the effort needed to establish and run a CSP differs considerably from one European country to another. Any organisation wishing to establish a CSP business in several countries must adapt to different requirements and procedures for each respective country. Product vendors may also have difficulties building products for this very fragmented market. In addition, several countries put additional detailed and unnecessary requirements on the CSP, thus creating barriers for the establishment of a CSP.

2.8.3 Annex III: Secure Signature-Creation Devices

Annex III specifies requirements for secure signature-creation devices (SSCD). Most countries have literally copied the requirements of Annex III. A few things may be noted:

- In Germany, it is explicitly required “that it is not possible to duplicate the signature keys”.
- In Austria, there are additional specific requirements regarding the regulation of SSCDs. On the other extreme, in the United Kingdom, there is no transposition of Annex III at all. In Estonia, the regulation contains no legal requirements at all for SSCD, i.e. protection of "private key", although in practice, electronic ID cards are currently being deployed as signature creation devices.
- In Hungary, the regulation contains the same requirements as in Annex III, but part of it has been mistranslated. The SSCD “must present data to be signed”, instead of “must not prevent from being presented”. This in fact means that the SSCD should actually contain a display device.
- In Poland, the requirements are formulated in such a way that the SSCD "should" actually encompass parts of the Signature Creation Application, which means that it can then not be implemented as, for example, a smart card could be.
- A few countries (the Netherlands, Lithuania, Bulgaria) refer explicitly to CWA 14169 for the fulfilment of these conditions, even before a reference to this standard was published by the Commission in the Official Journal.

In summary, the requirements for SSCDs are higher in Austria and Poland, leading to barriers for vendors established in those countries. On the other hand, the lack of requirements for SSCDs in the United Kingdom and Estonia might lead to uncertainties in recognition of Qualified Electronic Signatures from those countries. For example, a UK resident would probably need to obtain an SSCD from another Member State in order to be sure that his Qualified Electronic Signature is recognised for example in France or Germany.

2.8.4 Annex IV: Secure Signature Verification

Annex IV contains recommendations for secure signature verification. Most countries have not transposed Annex IV at all, while some have transposed it as recommendations, just as in the Directive. A few things may be noted:

In Austria, Spain, the Czech Republic, Lithuania, Poland and Slovenia, the regulation contains a copy of almost all the same items as Annex IV, but specifies them as **requirements** instead of recommendations.

- In Austria, certified products (see next section) **must** be used for secure creation and verification of Qualified Electronic Signatures.
- In Germany, the signatory "**should**" use products recommended by the CSP, "or take other suitable steps to secure Qualified Electronic Signatures".

- In Spain, the new legislation contains requirements on products for signature verification, but there is no mandatory requirement to use such products. In the Czech Republic, the legislation only defines "secure verification" without specifying its use. "However, if the signature proves that the damaged party failed to perform all the procedures necessary to verify the validity of the guaranteed electronic signature, the liability shall be waived."
- In Slovenia, only an Advanced Electronic Signature verified according to the specified requirements is regarded as being equal to a handwritten signature.
- In Poland, the mandatory compliance requirements of the "secure verification device" shall be "set in separate provisions."
- Only Bulgaria and Lithuania refer to CWA 14171 for signature verification.

In conclusion, it is very unclear what these **requirements** mean from a legal point of view, and what the consequences are if the requirements for "secure verification" are not followed (see also next section). In the Czech Republic, for example, it seems to mean that "due care" has not been exercised, and that the signatory can not be held liable for damages. In both Austria and Slovenia, following the verification requirements is a prerequisite for equivalence with handwritten signatures.

2.8.5 Products for signature creation and verification

According to Recital (15) of the Directive, "Annex III covers requirements for secure signature-creation devices to ensure the functionality of Advanced Electronic Signatures; it does not cover the entire system environment in which such devices operate."

However, in both Austria and Germany, the CSP is obliged to inform the signatories about products which comply with the requirements for creation and verification of Qualified Electronic Signatures.

- In Austria such products need to be certified by a confirmation body, A-SIT. In Germany, a Manufacturer's Declaration is sufficient for products recommended by a supervised CSP whereas formal conformity assessment is required for products recommended by an accredited CSP.
- In Austria, such certified products **must** be used for secure creation and verification of Qualified Electronic Signatures. In Germany, the signatory "**should**" use such products, "or take other suitable steps to secure Qualified Electronic Signatures".

To conclude, it is a widespread perception that in Austria and Germany, a Qualified Electronic Signature according to their legislation can only be created using a product which has been certified.

2.9 Notification to the Commission (Article 11)

Article 11 of the Directive requires Member States to "notify to the Commission and the other Member States" information on each of the following issues:

- national voluntary accreditation schemes;
- national accreditation and supervision bodies;
- accredited CSPs.

At the time of writing only Austria, Denmark, France, Germany, the Netherlands, and the United Kingdom have notified information on any or all of the issues listed above to the Commission. Whether or not the information has also been submitted to the other Member States cannot be answered at this time but it seems unlikely. All the other EU Member States have failed to notify as of yet. Since the notification process itself does not follow any difficult rules (it is sufficient to send an informal e-mail to the Commission only) this is not really understandable.

	Article 11: Notification to Commission
AUSTRIA	yes
BELGIUM	yes
DENMARK	yes
FINLAND	no
FRANCE	yes
GERMANY	yes
GREECE	no
IRELAND	no
ITALY	no
LUXEMB.	no
NETHERL.	yes
PORTUGAL	no
SPAIN	no
SWEDEN	no

	Article 11: Notification to Commission
UK	yes

Chapter 3 Standardization aspects of electronic signatures

The study of the European regulatory framework for electronic signatures would not be complete without taking a look at the standardization process in this area. Simultaneous to presenting the first draft proposal for a Directive, the European Commission also issued a mandate to the European standardization bodies. This mandate has led to the establishment of the European Electronic Signatures Standardization Initiative (EESSI). Furthermore the Directive also refers to "generally recognized standards" for electronic signature products, giving the European Commission the possibility to publish references to such standards in the Official Journal.

The European Commission has also taken various initiatives to stimulate further standardization and interoperability in the area of electronic signatures. Efforts have also been done at the level of the Member States.

In this third chapter of our study, the research team analyses these standardization initiatives and evaluates their effect on the market.

3.1 The EESSI framework

3.1.1 Background

The Directive identifies requirements for Qualified Certificates, qualified Certification Service Providers and secure signature-creation devices. The Directive also allows the Commission to establish and publish references of generally recognized standards for electronic signature products under the scope of these requirements. As a consequence, Member State's laws needs to presume compliance with the requirements laid down in the Directive when one of those products meets the referenced standards.

In order to provide timely standards permitting full and efficient implementation of a common framework, industry and European standardization bodies, within the frame of the European ICT Standards Board (ICTSB), have been requested by the European Commission to analyse, in a coherent manner, the needs for standardization activities in support of essential legal requirements as stated in the Directive in relation to electronic signatures products and services to be made available to the market.

A first assessment was made of available standards and current initiatives at global and regional level, both in formal standardization bodies and industry consortia. The assessment has identified gaps and the need for any additional standardization initiatives in all relevant

forms, such as standards, specifications, agreements, workshops or any other form of consensus building. On the basis of this analysis, a work programme has been defined.

To initiate and coordinate the necessary standardization, the ICTSB, with the support of the European Commission, launched an open initiative bringing together industry, market players, public authorities, and legal and technical experts: the European Electronic Signature Standardization Initiative (EESSI).

As a result, EESSI delivered its initial recommendations (July 1999) in a report that contained an overview of the requirements for standards-related activities, as well as a detailed work programme to meet these requirements. Three key areas were identified as crucial in the work programme:

- Quality and functional standards for Certification Service Providers (CSPs);
- Quality and functional standards for Signature Creation and Verification Products;
- Interoperable standardization requirements for Electronic Signatures.

The standards-related work required at European level was to be carried out by the European Standards Organizations CEN/ISSS and ETSI, in collaboration with other organizations as required.

The work started in 2000, and a number of standards have been developed and approved by the two organisations. Detailed information on the work and the deliverables can be found at:

- http://www.ict.etsi.fr/eessi/EESSIIntro.htm
- http://portal.etsi.org/esi/el-sign.asp
- http://www.cenorm.be/isss/Workshop/e-sign/Default.htm

The current EESSI deliverables are now published as CEN Workshop Agreements (CWA) and ETSI Technical Specifications (TS). For the work items related directly to the Annexes of the Directive, the following standards have been developed:

For the requirements of Annex II f):

- CWA 14167-1 (June 2003): Security requirements for trustworthy systems managing certificates for electronic signatures - Part 1: System Security Requirements
- CWA 14167-2 (March 2002): Security requirements for trustworthy systems managing certificates for electronic signatures - Part 2: cryptographic module for CSP signing operations - Protection Profile (MCSO-PP)

For the requirements of Annex III:

- CWA 14169 (March 2002): Secure Signature-Creation Devices

The development of these standards has unfortunately taken much longer than anticipated. For CWA 14167-1, the work was prolonged through a lengthy discussion and disagreement regarding the referencing of FIPS 140-1 as a possible standard to be used for Cryptographic modules. For CWA 14169, work has been held up for a long time because of disagreement over which Common Criteria Evaluation Level is required for the Protection Profile. As a result, two standards were submitted by the Commission to the Article 9 Committee, which opted for CWA 14179 using EAL4+.

The references to the above standards have been published by Decision 2003/511/EC of 14 July 2003.[48]

3.1.2 Impact of EESSI standardization

At the start of the EESSI standardization work, intense discussion took place between the different parties on the scope of the EESSI activity. Some parties wanted EESSI to restrict its work on standards related to the Annexes of the Directive. This was clearly the focus of the initial EESSI work programme but the EESSI programme also contained a number of work items related to interoperability, something that later has shown to be highly appreciated. If anything, EESSI can now be criticized for not having done enough to promote interoperability, the result of which has been that several countries have developed their own national interoperability standards.

Many countries are now promoting, using, or planning to use several of the EESSI deliverables. The publication of references to the CWAs related to the Directive, as stated above, has clarified the situation regarding which security standards to follow in order to implement the requirements of the Directive. The interoperability standards developed by ETSI have also been accepted as de-facto standards by many market actors, although much more work is still needed, mainly to promote the actual use of the currently available interoperability standards.

3.2 The need for standards

In relation to the Directive on electronic signatures, there are actually two areas where standards are needed: security standards related to Qualified Electronic Signatures, and interoperability standards.

[48] 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 (Text with EEA relevance), http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_175/l_17520030715en00450046.pdf

3.2.1 The need for security standards related to Qualified Electronic Signatures

As described earlier, Article 3.5 specifies that the Commission may establish and publish reference numbers of generally recognized standards for electronic signature products in its Official Journal (OJ). Member States shall then presume that there is compliance with the requirements as laid down in Annex II (f) and Annex III when an electronic signature product meets those standards. The next section will describe how presumption of conformity with such standards has been implemented in European countries.

However, several things need to be pointed out:

- OJ-referenced standards currently in existence relate to CSPs issuing Qualified Certificates and to SSCDs only. They are thus restricted to the requirements related to the creation of Qualified Electronic Signatures.
- OJ-referenced standards currently in existence represent just one way of complying with the requirements. Hopefully, other standards will also be developed and accepted by the Commission.
- OJ-referenced standards currently in existence should not be regarded as a minimum obligation for fulfilling the requirements, but rather as *one* way of fulfilling all requirements securely.

Those standards published in the OJ and developed by EESSI are in the form of CEN Workshop Agreements (CWA). However, a CEN Workshop is a time-limited effort, and the current CEN E-SIGN Workshop is due to close at the beginning of 2004. This means that after it ceases to exist, the workshop will be unable to maintain the standards already agreed and which are subject to technological and market developments. EESSI is fully aware of this fact, and is looking for solutions, for example transferring the current CWAs to a more permanent body or promoting the CWAs to European Norms, in which case the standards will be maintained through regular standardization procedures.

3.2.2 The need for interoperability standards

Recital (5) states that “the interoperability of electronic-signature products should be promoted”. Although it has not been specified who exactly should do this promotion, one can assume that the intention is for interoperability to be promoted both by the Commission, Member States and industry. In order to achieve interoperability, standards are required. In the area of electronic signatures, a number of basic standards exist, based on PKI technology:

- ISO/ITU X.509: Contains the basic format of the certificate
- IETF PKIX RFC 2459/3280: X.509 Certificate and CRL profiles

- IETF PKIX RFC 3039: Qualified Certificate Profile

The two first basic interoperability standards are presently used by almost all current market players for electronic signatures based on PKI. The third standard is presently being accepted as a standard for issuing Qualified Certificates. However, both the X.509 and PKIX standards are very open and can be interpreted very differently, so there is a need for further detailing these standards in the form of profiles. Such work has also been carried out within the EESSI framework, resulting in several standards related to electronic signatures being based on PKI technology. The promotion of interoperability and use of standards for that purpose in the European countries is further described in the later sections of this chapter.

3.3 Presumption of conformity for Qualified Electronic Signature standards

A majority of EU Member States (Austria, Belgium, Denmark, Finland, Germany, Greece, Portugal, Spain and Sweden) explicitly state that conformance to electronic signature standards, for which references are published in the Official Journal, implies a presumption of conformity with the corresponding requirements in national law/regulation. Further, some non-member states (Latvia, Poland, Slovenia, Iceland and Norway) specify more or less the same recognition of standards referenced by the European Commission in the OJ as the EU Member States.

Instead of stating presumption of conformity for OJ-referenced standards, some countries (France, Italy, the Netherlands, Lithuania, Bulgaria, Romania, Switzerland) either refer explicitly to specific EESSI standards or other international standards, or even publish EESSI standards as national standards. In Spain, CWA 14169 is being translated into a national standard.

Ireland and the United Kingdom do not specify any presumption of conformity for OJ-referenced standards and do not specify any other standards.

Some countries mandate adoption of specific standards:

- The Netherlands specifies presumption of compliance with requirements through the use of a number of EESSI standards. A guide for the use of TS 101 456 has been published.
- France specifies CWA 14169 for SSCDs and a French version of ETSI TS 101 456 for CSPs in its accreditation scheme.
- Denmark mandates the use of certain parts of the ETSI TS 101 456 standard.
- Lithuania has adapted a number of EESSI and ISO standards as national standards to be followed.

- Slovenia has mandated an American standard for cryptographic modules used worldwide (FIPS 140-1), and evaluation of CSP software according to Common Criteria.
- Poland has adopted an additional standard to follow for Certificate Policies with respect to security requirements.

In a few cases, countries also specify EESSI standards as voluntary.

Ireland and the UK do not state any presumption for standards referenced in the OJ, and do not specify any other standards.

3.4 Promotion of interoperability through standards

Recital (5) of the Directive states: "the interoperability of electronic-signature products should be promoted", since interoperability is necessary in order to achieve wide-spread use of electronic signatures and related services. Article 4.2 of the Directive also obliges Member States to ensure that electronic-signature products complying with this Directive are permitted to circulate freely in the internal market. One way to put this obligation into practice is through standardization.

3.4.1 Promotion by the Commission

The European Commission has sponsored several activities and projects related to electronic signatures and PKI standardization, such as ICE-TEL and ICE-CAR, PKICUG, the pki Challenge, ESTIO, TIE and EESSI.

From 1999 to 2000 the **TIE** project (Trust Infrastructure for Europe)[49] sought to bring together the main PKI developers and service providers active on the European market and to build a secure e-commerce infrastructure based on open standards. The business objective of the project was to provide an infrastructure to support secure electronic commerce in Europe by developing interoperable certification authorities that supply digital signature and time stamping services within a clearly defined legal framework.

ICE-TEL (http://www.darmstadt.gmd.de/ice-tel/) and its successor **ICE-CAR** (http://ice-car.darmstadt.gmd.de/) has as its objective to provide all the technology components to support the secure use of the Internet for commercial and administrative applications in Europe. The project seeks to improve and deploy the existing security tool sets from the perspective of usability and interoperability.

[49] Funding Programme: ESPRIT 4 - Project Reference Number: EP 26763

The goal of the **Public Key Infrastructure for Closed User Groups (PKICUG)** project was to experiment with the implementation of PKI techniques, and draw from those experiences common procedures and organisational practices that could be extended to all IDA networks.

The pki Challenge (http://www.eema.org/pki-challenge/), a two-year project which started in January 2001 under the auspices of EEMA, has sought to provide a solution to interoperability between PKI related products, and to develop specifications and best practice in the PKI standards area. Two very important deliverables from the project are

- **Recommendations for vendors (D8.3):** This document considers the implications of the pki Challenge conclusions and its effect on the vendor community. It makes recommendations about the features and levels of support for standards that PKI products should exhibit to encourage interoperability between users of different vendors' products.
- **Challenges for the PKI Industry (D8.4):** This is directed at standardisation bodies, the European Commission, other groups with an interest in this area and other participants. The paper outlines some of the technical challenges still facing the industry.

The ESTIO project (http://research.ac.upc.es/ESTIO/) has specified and developed a set of tools to perform the required interoperability tests of the electronic signature related products and services in Europe.

Finally, **EESSI** (European Electronic Signatures Standardization Initiative (http://www.ict.etsi.fr/eessi/EESSI-homepage.htm), has developed several standards related to interoperability of electronic signatures based on PKI:

- ETSI TS 101 456: Policy Requirements for Certification Authorities issuing Qualified Certificates
- ETSI TS 101 733: Electronic Signature Formats
- ETSI TS 101 862: Qualified Certificate Profile

3.4.2 National promotion of interoperability

In most EU Member States and some non-EU countries general measures have been taken to a varying degree for promoting interoperability between different CSPs and vendors of signature-creation products, either through government or private sector initiatives. In some of those cases, the ETSI signature format standard has been used, either directly or as a basis for national specifications. One example of this is Estonia and its Electronic ID card project.

Most countries have also specified or promoted standards for certificates and CRLs to a varying degree in order to promote interoperability. However, most of them have only specified

the use of X.509v3, and some have specified the use of ETSI 101 862, the Qualified Certificate Profile for fulfilling the requirements of Annex III. A few countries have made detailed national specifications. The best example of this is the ISIS-MTT specifications in Germany (which, however, not all CSPs adhere to), but also in Sweden, Italy and Poland where national specifications exist to a varying degree.

In a further example, six years after having enacted the first electronic signature law in Germany ("Signaturgesetz"), both the government as well as industry (service providers and vendors) founded the German Signature Alliance ("Signaturbündnis") in order to foster the use of (qualified) electronic signatures.

It should also be noted that there is an ongoing European project EUCLID (European initiative for a Citizen digital ID solution, http://www.electronic-identity.org/) initiated by the Population Register Centre of Finland to support the eEurope Smart Card Trailblazer 1 "Public Identity", partly through the establishment of standards in the area of electronic ID cards.

3.5 Algorithms and parameters for electronic signatures

Security standards are not really useful without accompanying specifications of algorithms and parameters (for example length of cryptographic keys) to be used. In addition, use of the same algorithms is of course a pre-requisite for interoperability.

Within the framework of EESSI, ETSI has published a Special Report, ETSI SR 002 176, containing a specification of algorithms and parameters for electronic signatures.

Most countries have not yet made any requirements or recommendations regarding algorithms and parameters. Only some countries (Austria, Germany, Italy, Spain, Czech Republic, Poland, Bulgaria, Romania, Switzerland) have published a national list of approved or recommended algorithms and parameters for electronic signatures.

France and Switzerland refer to the report published by EESSI on algorithms and parameters for electronic signatures. Only Germany has specified a process and a one-year cycle for review of the algorithms.

3.6 Termination of CSP operation

For the sake of Qualified Certificate market acceptance it is important that a well-defined procedure is followed when a CSP terminates its operation. This would prevent all previously issued certificates from becoming null and void.

About half of those countries surveyed have published procedures outlining what must happen if and when a CSP terminates its operation. In practice, at least 7 CSPs are known to have terminated operations or merged with other organizations. However, it is unclear to what

extent the specified procedures have been followed and in the absence of prescribed procedures what course of action was taken.

One conclusion to be drawn from this is that such a requirement should have been incorporated into Annex II to ensure that all countries incorporate it into national provisions. Fortunately, however, requirements for CSP termination procedures have been specified in ETSI TS 101 456. This has been adopted in several countries.

3.7 Certificate directories

Annex II (b) requires a CSP to "ensure the operation of a prompt and secure directory and a secure and immediate revocation service".

All countries are therefore requiring CSPs to operate such directory and revocation services. In all countries, revocation procedures seem to have been properly established. All CSPs provide CRL services, most also provide OCSP. There is no central directory of issued certificates in any country.

3.8 Root CAs and Bridge CAs

One problem for any entity wanting to validate a certificate used for an electronic signature is to find out if the issuing CA is trustworthy or not. For example, when receiving a signature based on what is claimed to be a Qualified Certificate, how can the recipient validate that the CA is supervised or accredited according to national regulation, and that they have neither shut down their services nor been ordered to withdraw from the market? There are several solutions to this problem: The Root CA, the Bridge CA and the Trust Status List.

A Root CA is a CA that issues certificates to subordinate CAs, and is directly trusted by an end entity. This means that by using a common Root CA certificate, all underlying user certificates can be verified. The concept of a Root CA does not imply that a Root CA is necessarily at the top of any hierarchy, simply that the Root CA is trusted directly, usually using a self-signed "root certificate".

In a few countries, a common Root CA has been established:

- Germany, by RegTP, for accredited CSPs only
- The Netherlands, for government use only
- Poland
- Belgium

Many experts are now of the opinion that the value of using a Root CA has been overestimated. It is a very crude instrument for determining the reliability and status of a CA issuing certificates. For business applications, parties relying on a certificate most often

therefore prefer to specify directly the CAs that are to be trusted, instead of relying on an automated chain of certificates.

An issue related to this is the very politically sensitive question of who would be responsible for operating such a Root CA, and would the Root CA itself be following any standards? That this is an issue can be seen in Germany where RegTP (as supervisory and accreditation body) is also responsible for running the Root CA. Unfortunately, the Root CA is not following common PKI standards down to the last detail, resulting in a situation in which interoperability cannot be ensured among all CSPs issuing QCs.

An alternative, but very similar, technology for providing trust through a single trust point is the concept of a Bridge CA. The main difference compared to a Root CA is that the user uses his own CA (and its self-signed certificate) as a trust anchor instead of the lesser known Root CA. Every participating CA is then cross-certified by the Bridge CA, and a trusted chain of certificates can thus be built from the own CA, through the Bridge CA, to any end entity certificate.

There are currently several Bridge CA projects in Europe. A Bridge CA is currently being planned by the European Commission within the framework of IDA for use between public administrations in Europe. The “European Bridge-CA” project was initiated by Deutsche Bank and Deutsche Telekom and is supported by TeleTrusT (http://www.bridge-ca.org/). Although a Bridge CA may seem more attractive, it does not really solve the need for more detailed information on the status of a CA, and for that reason, the “IDA Bridge CA” project is currently planning for a modified Bridge CA, also containing Trust Lists.

A Trust List is a signed list of information regarding CAs and their status. In Italy, the government (*i.c.* AIPA) developed such technology quite early on in order to distribute information about accreditation status of CAs, and several other countries have been contemplating doing the same. For that reason, ETSI is currently developing a standard ETSI TS 102 231 for provision of harmonized status information of CAs, which may be used by the IDA Bridge CA.

3.9 Conclusions

Currently, not all Member States have specifically stated presumption of conformity for standards referenced in the Official Journal.

Regarding security standards related to the Qualified Electronic Signatures of the Directive, there currently only one set of standards exists, developed by EESSI and based on PKI technology, since the requirements of Article 5.1 presume certificate-based solutions. This may hinder other technologies to be used for Qualified Electronic Signatures, and prejudice the use of PKI for other electronic signatures.

The EESSI standards also took much longer than expected to be developed and have their references published in the Official Journal. This has led to a situation where several countries have either developed their own technical interpretations of the Directive, leading to varying requirements in different countries, or waited for the standards, leading to a vacuum in the market place for product and service vendors. Not until the publication of references to standards in the Official Journal in July 2003 has there been any clarity on what standards can be used.

The development of a common specification for algorithms and parameters used for electronic signatures should have been done much earlier on at a European level, for example through EESSI. The present lack of commonly recognised specifications will lead to interoperability problems and lack of cross-border acceptance. The current situation with several national specifications, most often published only in a national language can also be perceived as a market barrier.

Regarding interoperability standards, the lack of technical interoperability, both at national and cross-border level, is a big obstacle for the market acceptance and proliferation of electronic signatures. It has resulted in many isolated “islands” of electronic signature applications, where certificates from only one CA can be used for one application. In a very few cases only can certificates from multiple CAs be used for multiple applications. Much more should therefore have been done earlier at a European level to promote interoperability:

- Although EESSI has worked on interoperability standards, this was reluctantly accepted by several Member States and therefore failed to get the necessary attention needed at an early stage.
- Although the Commission has sponsored several R&D projects related to interoperability (pki Challenge, ESTIO, TIE), the results of these projects have not been visible in the market, and certainly not in the application of electronic signatures.

The development, promotion and use of interoperability standards must now be done at a European level. If left to the nation state the result will be a plethora of different European standards. This would not only prevent cross-border use but also expect national vendors to apply different requirements. Such a scenario would probably diminish vendors adherence to EU standards. We can only hope for interoperability in standard products if European-wide requirements can be put to the vendors.

Chapter 4 Electronic signatures in practice

The purpose of Chapter 4 is to analyse information on the practical and commercial usage of electronic signatures in the different countries involved. The researchers have tried to identify three relevant electronic signature applications in each country. The practical applications were assessed with an emphasis on commerce, technology, and related standards.

The practical applications were also assessed according to their 'European directive-conformity status'. The researchers examined whether practical applications are in line with the legal requirements and recommendations of the Directive, such as conformity with the Annexes (type of certificate, type of CSP, type of signature-creation and signature-verification device). Also under investigation was the type of legal signature likely to be produced in the future when using the signature application (electronic signature, Advanced Electronic Signature, Qualified Electronic Signature).

The result is a detailed report on the practical implementation of Directive 1999/93 in the Member States, and the legal status of electronic signatures and related services in the EEA countries and candidate countries as well as a set of "scorecards" in an Appendix outlining the commercial and technical situation of national electronic signature applications and their conformity with Directive 1999/93.

The focus of this study has been on electronic signatures based on certificates and PKI technology, since this is a requirement for Qualified Electronic Signatures. One section below does go on to discuss alternative technologies for electronic signatures and authentication.

4.1 The market for electronic signature products and services

4.1.1 Products in use

A wide variety of products from different vendors are in use in Europe today. For CSP operation, CA products from Baltimore, Entrust, IBM, SmartTrust, RSA and Verisign are in use. For client and server products, either Microsoft standard products or dedicated (often nationally developed) products are used. Nationally developed products are almost exclusively used for Qualified Electronic Signature applications, where there are always special national requirements to be taken into account.

4.1.2 Number of CSPs and certificate volumes

The following table describes the number of Certification Service Providers in the countries as well as roughly estimating the number of certificates issued.

	Number of accredited CSPs	**Number of supervised CSPs**	**Volume of QCs by accredited CSPs**	**Volume of QCs by supervised CSPs**	**Volume of other certificates to the public**
AUSTRIA	2	6 (2QC)	10,000	-	5,000
BELGIUM	0	2	-	-	> 250.000
DENMARK	N/A	3	-	Ca 2,000	25,000
FINLAND	N/A	1			
FRANCE	0	0	-	-	800,000
GERMANY	23	23	25.000	-	20,000 est.
GREECE	0	5 (2 QC)	1,000	-	50,000
IRELAND	0 (1)	0	< 100	-	1000s
ITALY	14	14	Ca 1M	-	250,000
LUXEMBOURG	0	0	-	-	-
NETHERLANDS	1	1	< 50	-	Numerous
Portugal	0	0			
SPAIN	0	0	-	2,000,000	1,500,000
SWEDEN	0	0	-	-	Ca 100,000
UK	3	0 (3)	-	-	-
CYPRUS	N/A	N/A	-	-	-
CZECH REP	1	1			
ESTONIA	1	1	200,000	-	-
HUNGARY	N/A	6 (2 QC)	-	< 10	Ca 1,000
LATVIA	0	0	-	-	-
LITHUANIA	0	0	-	-	-
MALTA	0	0	-	-	
POLAND	N/A	4	-	-	-
SLOVAKIA	4				
SLOVENIA	0	4	-	85,000 +	-
BULGARIA	0 (1UC)	1	-	-	-
ROMANIA	0	1	-	Ca 20,000	-
ICELAND	N/A	1			
LIECHTENST.	0	0	-	-	-
NORWAY	N/A	1	-	Ca 60,000	Limited
SWITZERLAND	0	0 (1 temp.)	-	-	> 10,000

The following observations can be made:

- Germany and Italy have exceptionally many accredited and supervised CSPs. All of the Italian ones and several of the German were actually operating already under the previous "pre-Directive" legislation which required measures comparable to mandatory accreditation. To be more precise, 7 (3 physical and 4 virtual trustcenters) were accredited before the new German Signature Law entered into force and 15 were accredited after that. In Germany, many of the CSPs are "virtual", basing their service on one of the eight "physical" CSPs in operation.
- Only Austria (6), Belgium (2), Denmark (3), Greece (2), the United Kingdom (3), Hungary (4), Poland (4) and Slovenia (4) have more than one supervised and/or accredited CA.
- Only Portugal, Lithuania and Sweden have no supervised and/or accredited CSPs at all.
- Although in the United Kingdom three CSPs have been accredited under the industry not-for-profit tScheme system, no CSPs has issued QCs as of yet.
- In Switzerland the government has authorised a German CSP to provide certificates as a temporary measure as long as no Swiss CSPs starts operations.
- In Ireland one CSP has been accredited although officially no accreditation scheme has been implemented so far.
- In Bulgaria one CSP has been “registered” by the corresponding authority; this can be seen as a process similar to accreditation.

4.1.3 Volumes of issued certificates

4.1.3.1 Certificates issued by accredited and supervised CSPs

The table above shows estimates of certificates volumes in the different countries. The following observations can be made:

- A very large number of Qualified Certificates have been issued by accredited CSPs in Italy. The main application area for these certificates is for access to company registration information (InfoCamera).
- In Estonia, the large volume is a result of large-scale deployment of electronic ID cards.
- In Germany, quite a large number of Qualified Certificates have been issued and are regularly used in various e-government applications.

- In Slovenia, a substantial number of Qualified Certificates have been issued, mainly for corporate e-banking purposes and for e-government.
- The differences in certificates from accredited versus supervised CSPs are mainly a reflection of the different governments promoting/mandating accredited CSPs.

4.1.3.2 Other certificates issued to the public

As can be seen from the table, quite large numbers of other certificates have been issued to the public in several countries, primarily for e-government, with tax filing as the most widely used application. However, many of these are probably used also for authentication/authorization purposes, and not only for electronic signatures.

4.1.3.3 Other certificates issued under contractual agreement

Large numbers of certificates have been issued under contractual agreement in almost all EU Member States, mostly for e-banking, but also for internal corporate use. Figures reported from countries vary from between 100,000 to 2,000,000. Moreover, many of these have also been used for authentication/authorization purposes, and not only for electronic signatures.

4.1.3.4 Revocation of certificates

In those countries where certificates are issued, the percentage of certificates revoked is usually in the order of 1 %.

4.1.4 Use of smart cards

The degree of smart cards usage varies, even for Qualified Certificates, from 100% (Germany, Estonia, Norway) to 50% (Ireland, Slovenia). For non-Qualified Certificates, the usage of smart cards varies from 80% (estimate for Germany) to < 5% (Denmark, Ireland).

4.1.5 Other CSP services

In several countries (Denmark, Germany, the Netherlands, Estonia, Hungary, Bulgaria), time stamping is offered as an additional CSP service. In Latvia and Bulgaria, CSPs are actually mandated to offer time-stamping services. Other services being offered in some countries are notary, validation and archiving services.

4.1.6 Archiving of electronically signed documents

One reason for the reluctance of using electronic signatures today is that the actual archiving of electronically signed documents is considered too complex and uncertain. With the common legal requirements of 30 year archiving period or more for government documents,

many organizations feel uncertain if and how this can be achieved with electronic documents and electronic signatures. It certainly requires additional technology and procedures for migrating electronic documents and signatures and keeping them readable and verifiable over such a long time.[50]

4.1.7 Security problems

In several countries, some forms of security-related problems have been reported. In Germany only have details been released to the public regarding problems with secure viewers.

4.2 Applications in Use

Appendix 3 contains "scorecards" for a number of certificate-based electronic signature applications being used in Europe today. This section will summarize the findings of studying these applications.

4.2.1 Types of applications

There are two dominating applications for electronic signatures in Europe: e-banking and e-government.

Personal e-banking (“consumer banking”) has been used for several years now by all of the Member States and by most other European countries. Traditionally, personal e-banking has to a large extent been relying on and still is relying on, one-time passwords and tokens. Nevertheless certificate are gradually increasing in use. Although many e-banking applications are only using these technologies for authentication purposes (secure login), electronic signing of transactions is also increasing in use. At the same time, very few personal e-banking applications are using smart cards. On the other hand, **corporate e-banking** ("business-to-business") and inter-bank clearing require higher security, and is therefore using smart cards to a much larger extent.

E-government is the rapidly rising application for electronic signatures in Europe. Many EU Member States and several other European countries either have launched applications

[50] Further reading on this issue: DUMORTIER, J., *Réflexions juridiques relatives à l'archivage numérique. Rapport Numérisation de l'information et des archives parlementaires,* Centre Européen de Recherche et de Documentation Parlementaires, p.20-31, Tome Ier. (Bruxelles-La Haye); DUMORTIER, J., "E-Government and Digital Preservation", *E-Government: Legal, Technical and Pedagogical Aspects, Publicaciones del Seminario de Informatica y Derecho*, Universidad de Zaragoza, 2003, p. 93-104, ISBN 84-95480-96-4; DUMORTIER, J. & VAN DEN EYNDE, S., 'Electronic signatures and trusted archival services', in *Proceedings of the DLMForum 2002*, Barcelona 6-8 May 2002, Luxembourg, Office for Official Publications of the European Communities, 2002, p. 520-524.

(Austria, Denmark, Finland, Germany, Ireland, Italy, Sweden, the United Kingdom, Estonia, Slovenia, Czech Republic, Poland, Romania) or are planning to do so (Belgium, the Netherlands, Hungary). Most often, the e-government applications are based on the use of Electronic ID cards.

4.2.2 Types of certificates and signatures

E-banking relies almost exclusively on non-Qualified Certificates. The only exception being corporate e-banking in Slovenia, which uses Qualified Certificates.

For e-government, the following table summarizes the types of certificates and signatures being used or planned in some European countries:

Country	**Certificate**	**SSCD**	**Legal basis**
AUSTRIA	Non-QC	Yes	5.2
BELGIUM	QC	Yes	5.1
DENMARK	Non-QC	No	Adapted laws, 5.2
FINLAND	QC	Yes	5.1
GERMANY	QC from accr.CSP	Yes	5.1
IRELAND	Non-QC	No	5.2
ITALY	QC from accr.CSP	Yes	5.1
NETHERLANDS	QC from accr.CSP	Yes	5.1
SWEDEN	Non-QC	No	Adapted laws, 5.2
UK	QC from accr.CSP	No	5.2
CZECH REP	QC from accr.CSP	Yes	5.1
ESTONIA	QC from accr.CSP	Yes	5.1
POLAND	Non-QC	No	Special law
SLOVENIA	QC	Yes	5.1
ROMANIA	QC	Yes	5.1

4.2.3 Use of CSPs

In all cases where e-banking is being used and in e-government cases, there is a one-to-one relationship between the CSP and the application. This means that a certificate issued by one CSP can only be used for one specific application. However, for e-government in Denmark, Germany, Italy, Sweden and Slovenia, several CSPs issue certificates and sometimes also

SSCDs according to country-wide standards, thus, in theory, enabling interoperability. In other countries, for example Estonia, certificates for a national electronic ID card create a de-facto standard, and can be used for a multitude of applications, both for e-government and other applications.

4.2.4 Costs

User costs vary heavily in Europe, from "almost free" for non-Qualified Certificates for e-banking, to 60 € per year for Qualified Certificates based on smart cards for e-government.

In most countries, there seems to be no costs involved for the receivers of electronic signatures (Relying Parties), i.e. application providers or others relying on the certificates. The only known exceptions are the following:

- In Sweden, the CSPs used for e-Government certificates charge for access to CRLs, either per transaction or as a yearly fee.
- In Denmark, Relying Parties of the OCES certificates pay 0,5 - 1 € per "active user" per year independent of how frequently the certificate is used by the receiver.

4.2.5 User identities

For both e-banking and e-government, full name and/or pseudonym are used together with some form of unique identifier. Some countries include an official personal identity number in the certificate (Italy, Sweden, Estonia). Others have opted for a different unique number, which can be translated into a real identity by the CSP (Finland). Austria is now introducing a kind of "attribute certificate" containing the official identity number, for which the certificate holder can decide when he wants it disclosed.

4.2.6 User software and hardware

Almost all electronic signature applications (except for secure e-mail) require some form of application software to create signatures, since this is not a standard software feature today. The signature application software is most often provided by the CSP or the application service provider.

When a smart card/SSCD is used, a card reader is also needed combined with driver software for a card and card reader. This is either supplied by the CSP delivering the SSCD, or available on the market.

4.3 Problems identified with PKI

Given the slow market uptake of electronic signatures in Europe, it may be worthwhile reflecting on whether this has something specific to do with electronic signatures per se or rather whether this has something to do with the use of PKI. Over the last few years, several articles have been written, describing the risks and problems identified with PKI. They have sought to explain why the use of PKI has not taken off.

In July 2003, an article was published in Le Monde, stating that the introduction of electronic signatures is being delayed, because industry is put off by complex PKI requirements. The technology will have to rely on a general distribution of certificates based on electronic identity cards.

In 2000, Carl Ellison and Bruce Schneier wrote an article entitled "Ten risks of PKI".[51] The following risks described below apply to electronic signatures:

- Who do we trust and for what?
- Who is using my key?
- How secure is the verifying computer?
- Which John Robinson is he?
- Is the CA an authority?
- How did the CA identify the certificate holder?

All of these issues are addressed in one way or another by the very strict requirements for Qualified Certificates and secure signature-creation devices. However, the complexity needed to cover all these issues is starting to become incomprehensible for the ordinary user.

Peter Gutmann, in his article "PKI: It's is not dead, just resting", gives several following reasons, amongst which the following relate to electronic signatures:[52]

- The naming issue (also mentioned in the article above): Although a certificate contains a name, it is in reality impossible for anyone except the issuer to know who is behind that name. This means that in most cases, certificates can only be used by the same organizations that issue them (example: E-banking using a customer number; E-government using a citizen identity number, which for privacy reason should not generally be used).
- The revocation issue: Although revocation and revocation lists constitute a nice theoretical model, in reality there are problems. Users will forget or have difficulties in

[51] http://www.counterpane.com/pki-risks.pdf

[52] http://www.cs.auckland.ac.nz/~pgut001/pubs/notdead.pdf

revoking their certificates, and relying parties will have difficulties accessing CRLs. All this will contribute to uncertainties regarding the possibility of the user later denying his signature. Another issue related to revocation is that in fact time-stamping should always be required in order to safely accept an electronic signature. But time-stamping just adds another complexity level to the use of electronic signatures.

Two related issues which have led to both implementation and usage problems in past PKI projects has been the lack of some kind of "secure display component" which would be able to show to the user with high certainty the data to be signed as well as the data to be verified (as opposed to the standard PC environment), and the complexity of designing and operating certificate repositories (e.g. directories) within large infrastructures consisting of huge numbers of users.

4.4 Alternatives to PKI for electronic signatures

It is very interesting to note that in all countries, other technologies are also used for authentication and electronic signatures, and most often to a larger degree than PKI. The alternative technologies are password/PINs and different kinds of one-time password (OTP) generators, such as "scratch-pads" and password tokens. Of course, these technologies can not be used for Qualified Electronic Signatures (5.1), since such signatures require certificate-based technology, but they can certainly be used for general electronic signatures (5.2) having legal effect as well as for access authentication. These technologies are mostly used in e-banking, but there are also actual examples of one-time passwords being used for e-government, for example in Belgium and Sweden.

One of the main reasons why these technologies are so wide-spread is that the "electronic signature device" is often provided for by the service provider, who has no direct interest in that his customer can apply the same device towards other services. Therefore, the use of different OTP technologies is still dominating the market and is likely to do so in the foreseeable future.

However, one major drawback of these technologies is that each password generator is limited in its use to one service provider. A user accessing different services will need one OTP generator for each service, compared to PKI where he can use one certificate/private key for creating electronic signatures for multiple service providers. Thus, most experts agree that over the long-term , there is no realistic PKI alternative.

4.5 New technological developments

Are there new technological developments that will change the present "standard model" of electronic signatures, based on smart cards, X.509 certificates and PKI? In order to formulate

an appropriate European regulatory strategy in this field, it is absolutely necessary to take these new developments into account.

If we first restrict the discussion to PKI, the smart card is today seen by many as the most obvious "signature creation device", especially for Qualified Electronic Signatures, where the smart card is the SSCD. However, there are technological developments which will in all likelihood make the credit card sized smart card just one of several possibilities for storing a private key securely:

- Mobile phone incorporate a smart card (SIM), capable of holding a private key and performing secure electronic signatures. Several industry alliances are working to promote this area (Radicchio, Open Mobile Alliance etc) and pilot projects are being run by mobile operators in almost every country.
- With handheld devices (PDAs) are getting more and more common in both private and business use. These too might be used as signature creation devices. Rather like smart cards, PDAs could allow the secure storage of cryptographic keys. Furthermore, the user would be able to maintain the PDA "under his sole control". Some promising research has been done in this area only recently (e.g. "Hand held computers can be better Smart Cards"[53]).
- For the "standard PC platform", several vendors are cooperating to provide a more secure environment for applications through the Trusted Computing Group (TCG).[54] As an example, Microsoft's Next-Generation Secure Computing Base (NGSCB) is a new security technology which will be integrated into a future version of the Microsoft Windows operating system using a secure hardware device as a security component. Although details of the architecture have not yet been released to the public, the system will most likely be able to securely protect a private key and its cryptographic operations on the user's PC.[55]
- The concept of a centralized "signing server" is used by several product vendors in developing easy-to-use electronic signature solutions.[56]

---

[53] http://www.cs.princeton.edu/sip/pub/pilotkey.php3

[54] http://www.trustedcomputing.org/home; these initiatives are also heavily criticized, see e.g.: http://www.againsttcpa.com/

[55] Further reading on NGSCB: http://www.microsoft.com/resources/ngscb/default.mspx ; For critical comments on this and other similar initiatives: http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html

[56] Just one example is "Cryptomathic Signer" (http://www.cryptomatic.com/products/signer_index.html). This solution has enabled the Danish Savings Banks Data Center (SDC) to offer their customers a mobile home banking solution based on mobile digital signatures.

All of these developments are still related to certificate-based PKI for the creation of electronic signatures. It is therefore safe to say that in the near future we will see many other “signature creation devices” other than the smart card.

The X.509 certificate in itself is a cornerstone of today’s PKI-based electronic signature solutions, where it is being used to distribute public key information. However, there are also alternatives to the X.509 certificate. One of the most well-known is PGP (Pretty Good Privacy) which is used extensively in closed user groups. Another important technology for the future is the XML Key Management Specification (XKMS) proposed by Microsoft and Verisign.[57]

Regarding alternative technologies to PKI, (i.e. public/private key technology), as a whole, the situation is more uncertain. Although several vendors are advocating the use of electronic signatures based on “handwriting dynamics”, this area is still very much in its infancy and based on vendor-specific technology, with no industry-wide standards.

4.6 Conclusions

Although not regulated by the Directive, e-banking (corporate and personal) is the dominating application for PKI and electronic signatures in Europe today.

E-government will in the short-term (3-5 years) dominate application for electronic signatures as regulated by the Directive. Regarding e-government, the following conclusions can be made:

- A majority of countries use, or plan to use, Qualified Electronic Signatures.
- Some countries are using other types of electronic signatures, for instance based on passwords or tokens (Austria, Belgium, Denmark, Sweden, Ireland, United Kingdom).
- Some countries have application-specific laws for or regulation for the legal basis of the signatures.

There is still a long way to go before the vision of a "many CSPs - many application services” for electronic signatures can be realised. Most application services are based on certificates from one specific CSP. The certificates are then procured by the application service provider for that specific purpose only, even in e-government.

However, one should not underestimate the role that could be played by building an infrastructure starting from a small group of realistic applications (e.g., e-government), and allowing other parties to rely on that infrastructure. By taking competition rules into account the investment being made at such an initial stage could become beneficiary to all players.

[57] http://www.xmltrustcenter.org/xkms/index.htm

Many application service providers also prefer to deploy one-time password technology for electronic signatures to their customers instead of PKI, since they do not want the customers to use their electronic signature device towards other application service providers.

Besides the inherent complexity of PKI, the current business model may be one important reason why PKI, in general, and electronic signatures in particular have not taken off. Users do not see much benefit in obtaining a certificate. On the other hand, the application service providers, (for which the use of certificates and electronic signatures offer new business opportunities and/or rationalization savings), are frequently not being asked to pay anything for the reliance on certificates for authentication purposes.

The lack of common "electronic signature software" also leads to a slow market uptake and user acceptance of electronic signatures. Also, SSCDs being deployed today are not compatible: every type of SSCD requires card-specific software to being installed. For those who have little user knowledge this can act as an obstacle.

With the advent of electronic identity cards in many countries, there is a common need for being able to identify citizen electronically, while at the same time fulfilling data protection needs. Different solutions in different countries for solving this common problem will certainly lead to interoperability problems for the cross-border use of e-government applications.

In the area of PKI-based electronic signatures, we will in the near future see many new products based on technological developments, such as mobile signatures, Microsoft's NGSCB and signature servers. It is of great importance, therefore, that supervision bodies, designated bodies and others involved in the regulation of Qualified Electronic Signatures look at these technologies with an open mind, not restricting security assessment to what is known and available today.

Chapter 5 Conclusions and recommendations

The analysis of current national legislation, best practices, case law and market efforts in the preceding chapters now lead us to some general conclusions and recommendations. Our initial recommendation is not to amend the Directive. Such amendments would have to be considered only as a last resort to be used when all other measures are deemed insufficient. Amending the Directive is a long and cumbersome procedure which should be avoided if at all possible. As with all European Directives, the Electronic Signature Directive is by no means a perfectly drafted legal text. It is a compromise reached after long and difficult negotiations between 15 Member States with very divergent views on important topics covered by the Directive. The question is whether the text of the Directive is adequate enough to serve its purpose in the foreseeable future.

5.1 Introduction

The EU Directive has led to the adoption of national regulatory frameworks for electronic signatures in all but one of the European countries surveyed. The divergences between these regulatory frameworks are noteworthy and the resulting picture very complex.

The main aim of the Directive has been to create a Community framework for the use of electronic signatures, allowing for the free cross-border flow of products and service provisions, together with a basic legal recognition of electronic signatures throughout the EU. This objective has clearly not completely been reached. This, however, may not necessarily be the fault of the Directive itself. To the largest extent, this is due to the low market uptake of the PK technology itsef. However, the diverge of the implementations of the Directive in the Member States have in addition created uncertainties about the use of electronic signatures. Some of the Directive's provisions seem to have been misunderstood in part and the Member States, while transposing the Directive into national law, have sometimes failed to focus on the European dimension of the new regulatory framework. We are therefore under the impression that there is a primary need for a consistent, clear and workable **re-interpretation** of the Directive's provisions.

In our view the Commission should begin by examining in which way a more "Community-focused" interpretation of the Directive could be supported. Of course the ultimate judge on the correct interpretation of EU law rests with the European Court of Justice. Nevertheless the Commission is in a position to issue a non-binding document that can influence considerably the electronic signatures debate in Europe. Such an instrument could be combined with realistic accompanying measures that can be implemented on a short term. Such measures can focus on the improvement of interoperability between solutions, procedures, schemes and applications, the streamlining of national solutions for supervision of certification service

providers, co-ordination of voluntary accreditation schemes and of conformity assessment schemes for secure signature-creation devices, interchange between electronic signature-related applications and schemes in the public sector, etc.

Although this study does not cover the legal landscape of the US, Canada, Japan and Australia it is still wise to consider what is happening in other parts of the world before formulating European recommendations. The major market players global strategies vis-à-vis electronic signatures and internet standardization will also have to be considered in order to get a clear forecast for the future situation in Europe in this field.

5.2 The objectives of the Directive

By issuing EU Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures, the European Parliament and the Council aimed to achieve a series of objectives. These objectives are explicitly mentioned in the recitals of the Directive:

- To establish a clear Community framework regarding the conditions applying to electronic signatures, thus strengthening confidence in, and general acceptance of, electronic signatures (Recital 4);
- To prevent divergent provisions with respect to legal recognition of electronic signatures and the conditions for the provision of certification services (Recital 4);
- To prevent Member States' legislation from hindering the free movement of goods and services in the internal market (Recital 4);
- To promote the interoperability of electronic-signature products and ensure that essential requirements specific to electronic-signature products are met in order to guarantee free movement within the internal market and to build trust in electronic signatures (Recital 5);
- To adopt an open approach to various technologies and services capable of authenticating data electronically (Recital 8);
- To strike a balance between consumer and business needs (Recital 14);
- To increase user confidence in electronic communication and electronic commerce (Recital 24).

We can classify the objectives into three parts: 1) stimulating the internal market, 2) promoting legal acceptance of electronic signatures and 3) creating a favourable climate in this area for business and consumers. On the basis of the results of the foregoing chapters of this study we will now draw general conclusions for each of these levels and formulate concrete recommendations for the near future.

5.3 Stimulating the internal market

As far as the internal market is concerned, the objective of European legislation is contained in Recitals (5) and (10) of the Directive. Recital (5) deals with electronic signature products and Recital (10) relates to (certification) services.

5.3.1 Certification services

In terms of services, Recital (10) is illustrative of the vision forming the core of the Directive's provisions:

"*The internal market enables certification-service-providers to develop their cross-border activities with a view to increase their competitiveness, and thus to offer consumers and business 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 authorization; prior authorization 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*."

The Recital refers explicitly to the provision of cross-border certification services. This is not suprprising given that when the Directive was agreed, certain Member States had already introduced legislation submitting the provision of certification services to prior authorization by national authorities. It is certainly true that the legislation of these Member States did not exclude services provided by CSPs established in other Member States. On the other hand, these CSPs needed a license from a EU or EEA State and the conditions for obtaining such a license had to be equivalent.[58]

Prohibiting a Member State from establishing or maintaining licensing schemes or other similar barriers for service providers in this area is therefore directly linked to the internal market objectives of the Directive. If every Member State were to submit the provision of certification services to a prior authorization by authorities of that Member State, it would evidently be impossible - or at least very cumbersome - for a service provider to develop European-wide certification services.

[58] § 15 of the former German Signaturgesetz of 01 Aug. 1997 stated: "Digital signatures capable of being verified by a public signature key in another Member State of the European Union or in another State party to the Agreement on the European Economic Area shall be deemed equivalent to digital signatures under this Act *insofar as they show the same level of security*"; Article 8 of the Italian Presidential Decree n. 513 of 10 Nov. 1997 was formulated as follows: "The certification process referred to in Article 1 may also be carried out by a certifying authority, whose license or authorization was issued, *subject to equivalent requirements*, by another Member State of the European

In our overview of European legislation, we have seen that presently none of the Member States[59] submits the provision of certification services by providers established in another Member State, to any form of prior authorization. Theoretically, it is perfectly possible for a CSP established in one Member State to provide certification services in another Member State, without having to ask the permission of the national authorities of these other Member States.[60] This was not possible everywhere in Europe prior to the Directive being issued and transposed. It has often been over looked that this is one very positive outcome stemming directly from the Directive. One of the most important internal market objectives of the Directive has, in this respect, been achieved.

5.3.2 Supervision of CSPs

It has often been written and indeed confirmed by our study that various Member States have established supervision schemes which are very close to prior authorization. Article 3.1 is however very clear. Making the provision of certification services – qualified, accredited, or other – subject to prior authorization or taking other measures that have the same effect, are strictly prohibited by the Directive. Wherever the notification or registration procedures established in the Member States leads to effects that are similar to a prior authorization needed by a CSP before being able to start the provision of services, the European Commission has the possibility of acting against a Member State for not having respected the provisions of the Directive.

Fortunately the supervision of certification services by the Member States' authorities only affects providers established on their own national territory. One could have expected that Member States would keep the supervision regime for the providers established on their own territory as limited and as flexible as possible in order not to affect negatively the competitive position of their "own" service providers in comparison with providers established elsewhere.

However, bar a few exceptions the Member States and the other countries covered by this study have followed a completely different strategy. We have seen in our overview how some of the national supervision schemes sometimes put heavy burdens on the local Certification Service Providers before these can begin to provide qualified services. Apparently Member States are still convinced that most of the Qualified Certificates issued to the public on their

---

Union or the European Economic Area".

[59] The situation is different for the accession and the candidate countries. But, for example, Section 17.2 of the Slovakian Electronic Signature Act of March 2002 (see: http://www.e-podpis.sk/laws_en.html) is formulated as follows: "On the day of Slovakia's entry into the European Union, any certificate, issued by a to whose principal place of business is in a Member State of the Community, whose validity is verifiable in Slovakia, shall be an equivalent of a certificate issued in Slovakia".

[60] With the exception of the public authorities of the Member State where the CSP is established; see infra our comments on the supervision schemes in the Member States.

own territory will be provided by CSPs established on that territory. Another reason could be that some Member States use the supervision schemes to raise the security level of the CSPs established on their territory in order to improve their quality and hence their competitiveness on the European and international market. Last but not least Article 3.3 of the Directive explicitly requires the establishment of an appropriate system allowing for the supervision of Certification Service Providers. Recital (13) makes clear that the objective of supervision is to control whether or not an established CSP issuing Qualified Certificates to the public, provides this service in compliance with the requirements of the Directive. The requirements are listed in Annex II. Member States have, very understandably, thought that supervising the compliance with these complex technical requirements necessarily includes a close and detailed control of the CSPs and the way they operate.

In any case and as long as they avoid prior authorization, according to the Directive, Member States are largely free to organize the supervision of the CSPs established on their territory themselves. Recital (13) states "Member States may decide how they ensure the supervision of compliance with the provisions laid down in this Directive". It was clearly not the objective of the Directive to have similar or harmonized supervision schemes in every Member State.

The same Recital also states: "this Directive does not preclude the establishment of private-sector-based supervision systems". Most supervision schemes have been implemented under the auspices of public authorities but in some countries the supervisory is body actually a private company, which needs to be accredited by an independent public authority in order to supervise CSPs. It is still much too early to attempt an evaluation of these private-sector-based supervision schemes.

Our study has shown that, in most countries, only a few (if any) CSPs have been established and are actually issuing certificates. The majority of the supervision schemes are still at a very early stage of development. It is therefore impossible to compare the practical implications of supervision systems. Nevertheless, it remains obvious that very important divergences between the supervision schemes in the Member States exists. Conditions on how to enter the market for qualified certification services vary considerably from Member State to Member State. For the time being the effect of these divergences remains limited because most of the CSPs continue to operate exclusively from their home country. This is expected to change once European or non-European providers begin to launch more cross-border certification services in the EU.

Recommendations:

- The European countries surveyed appear to have difficulties striking the right balance between "appropriate supervision" of Certification Service Providers and the prohibition to submit their activities to prior authorization. Publish guidelines as to how

supervision can be organized in order to be compliant with the Directive's provisions would, therefore, be useful.

- The European Commission may consider taking actions against Member States that have established a scheme for supervision of CSPs leading to measures that have the same effect as a prior authorization.
- Guidelines published by the European Commission could also help clarify a number of currently unresolved legal issues in this area. One of the most difficult questions is knowing what the notion of "establishment on the territory" in practice actually means for a Certification Service Provider (for example, certificate issuer established in one Member State but collaborating with registration authorities, directory service providers, etc. in other Member States - who then is in charge of the supervision?).
- Not all Member States have established a scheme for appropriate supervision of CSPs issuing Qualified Certificates to the public. The Commission may consider taking actoins against these Member States, because this situation creates the possibility of CSPs established in one Member States being able to issue Qualified Certificates to the public in another Member States without being submitted to appropriate supervision.
- Ideally the supervision schemes in the Member States should be harmonized, at least to a certain degree. We think that efforts in this direction should be supported. The Commission should, in our view, discourage supervision of CSPs other than those issuing Qualified Certificates to the public.
- Since EESSI has already published a number of valuable documents in this area we recommended that supervisory authorities are encouraged to make use of these specifications. In our view, however, the use of such specifications by supervisory authorities has to be closely monitored. The standardization documents describe possible ways in which the requirements of the Directive could be fulfilled but should not be considered obligatory for CSPs wishing to issue Qualified Certificates to the public. If a CSP believes that he fulfils the requirements of the Annexes he should be free to issue Qualified Certificates to the public without asking authorization.

5.3.3 Voluntary accreditation

Recital (11) of the Directive states: "Voluntary accreditation schemes aiming at an enhanced level of service provision may offer certification-service-providers the appropriate framework for developing further their services towards the levels of trust, security and quality demanded by the evolving market; such schemes should encourage the development of best practices among certification-service-providers; certification-service-providers should be free to adhere to and benefit from such accreditation schemes." Therefore Article 3.2 of the Directive

stipulates that Member States can maintain or even introduce voluntary accreditation schemes aiming at enhanced levels of certification-service provision.

The European legislator has estimated, very rightly, that voluntary accreditation schemes could be beneficial for the development of the market. It can give Certification Service Providers operating in Europe the possibility of demonstrating their level of security and trustworthiness. Accreditation schemes could certify the adequacy of the security level of a particular certification service for being used in particular contexts or applications. For instance, specialized accreditation schemes could certify the adequacy of particular certification service for the health care sector.

Recital (11) also refers to the evolving market in this area. When new solutions are discovered and introduced into the market, accreditation schemes can help providers gain user trust. The accreditation schemes should mainly be created or maintained for the benefit of the providers themselves. They should encourage the development of best practices and remain up-to-date with state-of-the-art technology in the sector. They are a form of common quality control, organized at the level of a particular sector. Of course, setting up such accreditation schemes requires considerable resources, mainly in terms of expertise.

Consequently the aim of the Directive has never been to have a national accreditation scheme in every Member State. It is also fully incorrect to consider voluntary accreditation schemes as a means to control whether or not a Certification Service Provider operates in compliance with the provisions of the Directive. Our study has shown that, unfortunately, many European countries are merging the supervision of CSPs which issue Qualified Certificates to the public with the voluntary accreditation. We have also seen that in the majority of European countries accreditation is, in practice, not really voluntary, for example because it is a necessary condition to participate in the national e-government programmes.

Such a development is certainly not in line with the Directive's vision. The provision concerning voluntary accreditation schemes was intended mainly to prevent Member States from misinterpreting the prohibition of prior authorization. This prohibition should not be understood as incompatible with existing or future voluntary accreditation schemes. On the contrary, the Directive encourages the creation of such schemes, as long as the conditions related to those schemes are objective, transparent, proportionate and non-discriminatory. Moreover, as is stated in Recital (12): "Member States should not prohibit certification-service-providers from operating outside voluntary accreditation schemes; it should be ensured that such accreditation schemes do not reduce competition for certification services".

Recommendations:

- Measures should be taken in order to clarify the vision of the European legislator with regard to voluntary accreditation schemes for Certification Service Providers. In our

view, cross-border accreditation and diversification of the schemes should be encouraged.

- The Commission should, on the other hand, discourage as much as possible the establishment of *national* accreditation schemes for Certification Service Providers issuing Qualified Certificates to the public. Accreditation schemes should focus on the assessment of best practices and appropriate security and not be as deemed instruments needed to control compliance with the Directive or with national legal provisions.
- Given the scarcity of top experts in the field of information security and given the relatively small amount of CSPs, the Commission could stimulate the clustering of efforts at a Community level. The objective would be to establish a limited number of high quality European accreditation schemes, preferably focusing on or specialising in specific categories of certification services or application domains.

5.3.4 Conformity assessment of SSCDs

Recital (5) of the Directive states: "essential requirements specific to electronic-signature-products must be met in order to ensure free movement within the internal market and to build trust in electronic signatures". Notwithstanding the general character of this phrase, the Directive only contains requirements for secure signature-creation devices, which are needed to produce Qualified Electronic Signatures in the meaning of Article 5.1. Recital (15) confirms that "Annex III covers requirements for secure signature-creation devices to ensure the functionality of Advanced Electronic Signatures": it does not cover the entire system environment in which such devices operate". The same Recital again refers to the internal market objectives of the Directive: "the functioning of the internal market requires the Commission and the Member States to act swiftly to enable the bodies charged with the conformity assessment of secure signature-creation devices with Annex III to be designated; in order to meet market needs conformity assessment must be timely and efficient".

It is worth noting that the Directive does not contain requirements for electronic-signature products as such. The requirements of Annex III are only applicable to secure signature-creation devices or, in other words, for devices to be used for the creation of Qualified Electronic Signatures. One of the objectives being that secure signature-creation devices have to be easily recognized by the users. When using a secure signature-creation device, users should feel confident that the security of this device is legally recognized, not only in their own country but also in the other Member States. If a user creates an Advanced Electronic Signature based upon a Qualified Certificate and using a device labelled as an SSCD, he should be certain that this signature will be considered as the legal equivalent of a handwritten

signature everywhere in the European Union. It is our understanding that, from the perspective of the Directive, either the producer, under his own responsibility, may put the SSCD-label on the device, or the label can be the result of a conformity assessment by a designated body. In the latter case, the designated body should fulfil the criteria of independence and professionalism determined by the European Commission.

In order to avoid divergences in the conformity determination of signature-creation devices by designated bodies or to guide the manufacturers wishing to introduce SSCDs in the market, the Directive has explicitly emphasized the need to have legally recognized standards. It is for this reason that Article 3.5 gave the European Commission the possibility to establish and publish reference numbers of generally recognized standards. Manufacturers of signature-creation devices can be certain that their devices will be considered as SSCDs by all the EU Member States, assuming that their products "meet those standards".

Of course this whole construction had to be put in practice very swiftly. Therefore the European Commission published already in November 2000 its Decision 2000/709/EC on the minimum criteria to be taken into account for the designation of the conformity assessment bodies. Designated bodies were very rapidly operational in Germany and in Austria. Of course it was never the intention of the European legislator to have conformity assessment bodies in every Member State.

Many countries appeared to be quite reluctant to designate their own designated bodies for SSCD assessment. This may be due to the very high SSCD security requirements and the subsequent lack of active vendors in most countries. Another reason being the very large resources needed for operating an assessment body. Therefore all countries seem either explicitly or implicitly – but very rightly - to accept assessments made by bodies based in other Member States.

The level of competence and running cost of the assessment laboratories are such that not every country will be able to afford such services at a national level. This would not be a real constraint if a network of laboratories would provide these services at European level based on mutual recognition of methodology and criteria. Furthermore, such a network could include international laboratories as well, with all agreeing on a mutual recognition protocol.

Currently the main problem in this area appears to be the lengthy and costly character of the conformity assessment procedures. Even for an experienced SSCD vendor the process of having a relevant product evaluated and assessed by designated bodies might take up to one year. The most time-consuming tasks include the vendors' preparation of documents describing the product to be assessed in great detail. Thereafter, the assessment body has to both evaluate those documents as well as test the product against the documentation as provided by the vendor. It is likely that this process requires multiple changes before the vendor can fix any problems that might have been found during the evaluation. Since all these tasks involve a large amount of time at both the vendor level and the assessment body level,

the overall process becomes costly.[61] The process itself may be only slightly reduced by using previously assessed components, e.g., crypto processors.

Recommendations:

- Partly because the Directive currently sets very high requirements on SSCDs, such devices still rarely find their way on to the market. In order to stimulate the production of secure signature-creation devices in the future, requirements for formal assessment need to be more flexible in the future. The procedures for obtaining a conformity declaration should be shorter and less costly. The European Commission should support every effort in this direction.
- As to the rules to be followed by the designated conformity assessment bodies, the Commission should provide coordination and guidance. The Commission Decision of 2000 on the minimum criteria when designating conformity assessment bodies is a valuable first step but needs to be pursued. The independent, transparent and non-discriminatory character of the assessment procedure should ideally be monitored.
- The researchers involved in this study are of the view that it is absolutely necessary to discourage the perception that it is an obligation to submit every SSCD to a lengthy Common Criteria assessment performed by a designated body. Instead, limited evaluations, based on 50-100 pages of documentation and requiring 10-20 days of checking, need to be promoted. In not allowing self-assessment, an independent party should be able to assess the security claims (with respect to Annex III) as made by the vendor and check to some extent whether or not this is state of the art. The Commission should examine how it can tackle the obligation to submit an SSCD to a designated body for conformity assessment, currently existing in many Member States. Discouraging the too strict conformity assessment would allow for a larger variety of products while at the same time protecting the consumers.

5.3.5 E-government

Article 3.7 of the Directive contains the so-called “public sector exception”. Member States may make the use of electronic signatures in the public sector subject to possible additional requirements. However these requirements should be objective, transparent, proportionate and non-discriminatory and relate only to the specific characteristics of the application concerned.

[61] As an example we were provided with a cost range from 50.000€ to 200.000€ for a single assessment.

There are divergences in both interpretation and implementation of this provision. It seems clear that in many countries the use of electronic signatures in the public sector is subject to additional (security) requirements. Communicating electronically with public authorities is in many European countries only possible when using signatures based on Qualified Certificates issued by an accredited CSP.

The Directive does not strictly forbid this if the requirement is justified by objective reasons and relates only to the specific characteristics of the application concerned. Moreover a measure introducing such a requirement should be proportionate, transparent and non-discriminatory. Consequently, it would be prohibited, for example, to issue legislation imposing the use of Qualified Electronic Signatures for *all* electronic relations between citizens and the government. Such a rule is in contradiction with Article 5.2 of the Directive because it denies the legal effectiveness of electronic signatures solely on the grounds that these are not qualified.

Even imposing the use of Qualified Electronic Signatures for a single e-government application, for example, introducing electronic communication for a tax declaration, without justifying objectively the necessity of such a measure, is clearly in contradiction with the Directive.

When introducing the use of electronic signatures for public sector applications, Member States should also be aware of other rules. For example, imposing the obligation to obtain an accreditation for Certification Service Providers as a condition to participate in e-government programmes, is also in contradiction with Recital (11) of the Directive because the consequence of such a measure would be that the CSPs are no longer free to adhere to an accreditation scheme. The measure would also reduce in a disproportional way the competition for certification services.

Member States should also be careful not to intervene directly in the market for certification services if this contradicts the EU's competition rules. For example, a government is perfectly allowed to set up a public key infrastructure in order to support the use of electronic signatures for its own e-government applications. Setting up a public key infrastructure, whether or not in a partnership with one or more private companies, in order to support the use of electronic signatures outside the public sector would however not be admissible. Such an initiative, even if the private partner has been chosen in compliance with European and national public procurement rules, clearly reduces competition in the market for certification services and can constitute a barrier for the internal market in this area.

Recommendations:

- The Commission should emphasize the conditions that are needed before the Member States can use the "public sector exception" of Art. 3.7 of the Directive.

Member States should be aware that the non-discrimination rule of Art.5.2 of the Directive is not only valid in the private but also in the public sector.

- The Commission should examine in more detail the compliance of certain e-government initiatives not only with the provisions of the Electronic Signatures Directive but also with general European competition rules, particularly with a view on Art. 86 of the EC Treaty.
- More generally, it is necessary to perform a more detailed study on the Internal Market consequences of the e-government programmes of the Member States. There is a clear danger that these programmes will result in national barriers, fragmentation and interoperability problems.
- Efforts towards improvement of interoperability between e-government programmes and particularly between their electronic signature applications and services should be supported or initialised at a European level.

5.4 Promoting legal acceptance of electronic signatures

Recital (20) of the Directive predicts how "harmonized criteria relating to the legal effects of electronic signatures will preserve a coherent legal framework across the Community". The new European legal framework in this respect contains two main rules:

1. Advanced Electronic Signatures should be considered in all Member States as the equivalent of handwritten signatures if they are based upon a Qualified Certificate and created by means of a secure signature-creation device;
2. Electronic signatures should never be denied legal effectiveness or admissibility in legal proceedings solely on the grounds that they are in electronic form, not based on Qualified Certificates, not based on certificates issued by accredited providers or not created by a secure signature-creation device.

5.4.1 Qualified electronic signatures

For the European legislator, it was clear that "national law lays down different requirements for the legal validity of handwritten signatures". The objective was clearly not to harmonize the requirements for the legal validity of electronic signatures but instead to establish in every Member State an equivalency between the legal status of handwritten signatures in the paper-based environment and the legal status of electronic signatures in the electronic environment. In other words, the European legislator tried to determine a type of electronic signature, which should consequently be considered by every Member State as the equivalent of a handwritten signature. The type of electronic signature being chosen by the European legislator is the so-

called Qualified Electronic Signature, described in Article 5.1 of the Directive: an Advanced Electronic Signature based on a Qualified Certificate and created by a secure signature-creation device. The Member States were required to attribute to this type of electronic signature the same legal status as the one attributed by their national law to the handwritten signature.

It should be very clear that, as a consequence of this choice, the legal status of Qualified Electronic Signatures has not been harmonized between the Member States. The legal requirements for handwritten signatures differ from Member State to Member State. Qualified electronic signatures have the same status as handwritten signatures. Therefore the legal requirements for Qualified Electronic Signatures remain also different in each of the Member States. This principle is expressed at the end of Recital (20)[62] and it is very important for understanding many of the discussions about the transposition of Article 5.1 in the Member States.

Further, it should be made clear that European legislation has opted for a solution in which the legal regime for Qualified Electronic Signatures "follows" the national legal regime for handwritten signatures. If a Member State has, for example, very strict rules for the legal validity of a handwritten signature on a certain type of contract, this Member State will then adopt the same strict rules to Qualified Electronic Signatures for this same type of contract. If another Member State has very flexible rules for handwritten signatures for that type of contract, the rules for the use of Qualified Electronic Signatures on that same type of contract will also be very flexible. The legal regime for handwritten signatures is, in other words, the *reference point*, the principle being to award Qualified Electronic Signatures in the electronic environment the same legal status as handwritten signatures in a paper-based context.

During the transposition of the Directive, some Member States, such as the UK, discovered that their legal system has no legal provisions for handwritten signatures. In the absence of national legislation for the use of handwritten signatures, it follows that there can be no legal status for the use of Qualified Electronic Signatures either. Even more - if a legal system does not legally recognise the concept of a "handwritten signature", it is impossible to adopt provisions introducing a legal equivalency between a handwritten signature and something else. It is difficult to use something as a reference point if this "something" does not exist.

A further consequence of the approach adopted by EU law has been to make the legal status of the Qualified Electronic Signature dependent on the legal status of handwritten signatures. Implicitly this approach is based on the presumption that there is – but not necessarily always will be – a choice between two alternatives. In other words either to sign by hand or to sign

[62] "(...); Advanced Electronic Signatures which are based on a Qualified Certificate and which are created by a secure signature-creation device can be regarded as legally equivalent to handwritten signatures only if the requirements for handwritten signatures are fulfilled;"

electronically. Nevertheless more and more, specific rules are being addressed to the electronic environment, with the paper-based context no longer being referred to. It is not hard to imagine that, ten or twenty years from now, many applications will only use communications in an electronic form and that the rules applicable to those applications will no longer refer to handwritten signatures. In other words, the handwritten signature will, bit by bit, loose its value as a reference point. It is therefore doubtful whether the concept of the Qualified Electronic Signature as an "electronic equivalent" to the handwritten signature will survive over a long period of time. Nevertheless, for the time being, and for most of the Member States' legal systems, the linkage of the Qualified Electronic Signature to a handwritten signature can perhaps be useful. Whether or not this will actually be the case, largely depends on how clear the concept of a" Qualified Electronic Signature" actually is. It does not make much sense to require a Member State to award electronic signatures the same legal status as a handwritten signature on condition that it is a "Qualified Electronic Signature", especially if this concept is not uniformly understood across the EU. A Belgian citizen, for example, wishing to make an electronic commercial transaction with a Greek company by using Qualified Electronic Signature should be certain that his/her signature will have, under Greek law, the same legal status as a handwritten signature. What I, as a Belgian, consider a "Qualified Electronic Signature" should be equally recognised as such by Greek authorities. The whole system adopted by European legislation is only useful on condition that there is one common European concept of "Qualified Electronic Signature".

The most delicate problem of the European electronic signatures Directive is precisely the difficulty of defining exactly what a "Qualified Electronic Signature" means. Of course, Article 5.1 contains a definition. For example, a "qualified" certificate is necessary and must make mention of the certificate itself. Supervisory bodies, instruments and/or procedures ensure that CSPs are forbidden from making untruthful claims regarding their qualified status . Secure signature-creation devices can be submitted to conformity assessment bodies which in turn can receive a conformity label. In the foregoing chapters we have amply demonstrated the difficulties that have to be solved before Qualified Certificates and secure signature-creation devices will be widely distributed in Europe. However these problems are not the result of the Directive's text rather to the way in which the text has been interpreted and subsequently transposed by some of the Member States.

One should also not forget that a Qualified Electronic Signature must fulfil the four requirements of the Advanced Electronic Signature as well. Is the signature uniquely linked to the signatory? Is it capable of identifying the signatory, even if the name of the signatory is "Jean Dupont"? Has the signature been created using means that the signatory can maintain under its sole control? Is it linked to the data to which it relates in such a manner that any subsequent change of the data is detectable?

It has often been stated that the Directive only focuses on the security of the signature-creation device and of the certificate, in order to determine whether or not an electronic signature fulfils the requirements of Art. 5.1. This is not entirely correct. One could say that a Qualified Electronic Signature has to fulfil **six** requirements: the four requirements of the Advanced Electronic Signature and the two additional requirements that are expressly mentioned in Art. 5.1 itself. It is true that the four requirements of the Advanced Electronic Signature have not been given more provisions in the Annexes, unlike the approach adopted for Qualified Certificates and SSCDs. However, from a legal point of view, the absence of further provisions is not totally relevant. The lack of greater provisions on how to fill in the criteria of the Advanced Electronic Signature is in the first place a practical problem, which can be solved by further standardization. We will come back to this standardization issue later in the Chapter.

Recommendations

- With regard to Art. 5.1 there is a primary need for clarification about the scope of this provision. It should be made clear to all interested parties that 1) "Qualified Electronic Signature" is not a synonym of "legally valid electronic signature" and 2) fulfilling the requirements of a Qualified Electronic Signature is one – but not the only - way to get the rules on the handwritten signature applied.
- From a European perspective the success of Art. 5.1 depends entirely on the availability of a very well standardized and easily recognisable European "Qualified Electronic Signature, including not only criteria for creation devices and certificates but specifying the complete signature and verification chain.
- A standardized "Qualified Electronic Signature" should merely give users a presumption that a signature complying with this standard will be presumed equivalent to handwritten signatures throughout Europe.
- Member States should be discouraged from inserting references to "Qualified Electronic Signatures" in new legal texts. The concept of the "Qualified Electronic Signature" should mainly be used for its original purpose: to obtain "automatically" for electronic signatures the application of the rules applicable to handwritten signatures.
- Member States should be made aware that the concept of the "Qualified Electronic Signature" is useful mainly for cross-border transactions in Europe. It serves as a "passport" that guarantees the application of uniform regulations applicable to handwritten signatures across Europe.

5.4.2 Implementation of the Annexes

In the preceding paragraph we have explained that the success of the strategy adopted in Article 5.1 of the Directive largely depends on the question of how, in practice, one can recognise a Qualified Electronic Signature. The rule of Article 5.1 – "if it is a Qualified Electronic Signature, deal with it as if it would be a handwritten signature" - is simple. Only, however, on condition that everyone can easily discern one Qualified Electronic Signature from another. Ideally a Qualified Electronic Signature should be as easy to recognize as a handwritten signature.

In order to guarantee this as much as possible, European legislation chooses not only to list in detail the requirements to be fulfilled by certificates, Certification Service Providers and signature-creation devices but also to make sure that a Qualified Certificate can be recognized easily: 1) does the certificate contain the mention "qualified" or not? and 2) did the signature-creation device receive a conformity declaration by a designated body?

It is evident that these very simple means of control can hide a world of differences. The requirements that need to be fulfilled in order to qualify as a Certification Service Provider or to obtain a conformity declaration for a secure signature-creation device can vary considerably from one country to another. It should be clear, however, that these divergences are deliberately not taken into account by the European legislator. If a Certification Service Provider operates as a "qualified" CSP in one Member State, under the supervision of the authorities of that Member State, he has to be a recognised CSP in every other Member State. If a signature-creation device is confirmed to be a secure signature-creation device by a designated conformity assessment body in one Member State or if it meets the standard referenced by the European Commission in the Official Journal, every other Member State will have to accept this device as an SSCD.

Notwithstanding these very simple principles, it is interesting to note how the requirement for Qualified Certificates, Qualified Certification Service Providers and Secure Signature-Creation Devices, listed in Annex I to III of the Directive, have been transposed by the European countries surveyed for this study. Even if divergences in the implementation of these Annexes might not have important legal consequences, the fact remains that a more or less uniform implementation of these technical requirements is necessary to guarantee that a Qualified Electronic Signature created in one country, remains technically verifiable in another country. This is the whole problem of interoperability. To realize the vision of the European legislator – a "European" Qualified Electronic Signature that can be used for cross-border electronic communications in the Union and beyond – the "Qualified Electronic Signature" should be something more or less identical throughout the EU. One additional problem, evidently, is the language barrier. Certificates contain text and refer to other documents such as practice statements or policies, and these texts are all written in one or another language. For a user in Ireland, it might not be evident to read and understand the messages accompanying

certificates that have been issued in Greece, or vice versa. Standardizing the most important fields and messages as much as possible or to use one common language for these purposes appear to be the only way to solve this problem.

Our study shows that the implementation of Annex I has, fortunately, shown close convergence in the different countries. The only risk is related to interoperability problems which might occur if technical implementations of Annex I diverge, not using ETSI TS 101 862, or any other common format for encoding the requirements of Annex I. The Commission should therefore promote the use of interoperable standards for the technical implementations of Annex I.

Regarding Annex II, implementation does sometimes vary meaning that the effort needed to establish and run a CSP will differ considerably amongst the countries. Any organization that wants to establish a CSP business in several countries must therefore adapt to different requirements and procedures. Product vendors will also have difficulties building products for this very fragmented market. In addition, several countries put additional detailed and unnecessary requirements on the CSP, thus creating barriers for the establishment of CSP. The Commission should therefore point out any unnecessary and excessive requirements for CSPs, which might be perceived as market obstacles.

For the implementation of Annex III, there is also a fragmented situation. The requirements for SSCDs are for example much higher in Austria and Poland than in some other European countries.

As far as Annex IV is concerned, Article 3.6 is very clear. The list contains only recommendations that have to be taken into account by the Member States and the European Commission when they work together in order to promote the development and the use of signature-verification devices. And although more guidelines on the security and the functionality of such devices would benfit the users, the recommendation as of Annex IV can certainly not be changed into obligatory requirements at the national level, as some Member States have done.

Recommendations:

- The Annexes have been more or less literally transposed into national law by practically all the countries under the scope of this study: the remaining task is to make sure that the implementation gets streamlined throughout Europe. Every effort in this direction should be supported. National implementations of the Annexes have, on the other hand, to be firmly discouraged.

- The Commission can take measures against Member States who fail to transpose the Annexes correctly. For example by translating the recommendations of Annex IV into requirements for Qualified Electronic Signatures at a national level.

5.4.3 Non-discrimination (Article 5.2)

One of the most fundamental principles of Directive 1999/93/EC is outlined in Recital (21): "the legal recognition of electronic signatures should be based upon objective criteria and not be linked to authorization of the certification-service-provider involved". Consequently, Article 5.2 of the Directive stipulates that an electronic signature should not be denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is, for instance, not based upon a Qualified Certificate or not created by a secure-signature-creation device. All kinds of electronic signatures should be taken into consideration and their legal effectiveness should only depend on an objective examination of the given signature.

Unfortunately the principle as laid down in Article 5.2 did not receive very much attention. It has also become clear that there is some confusion in the Member States as to how Article 5.2 should be interpreted. What is actually meant by "not to deny legal effectiveness of an electronic signature solely on the grounds that it is not based upon a Qualified Certificate or not created by a secure signature-creation device"? Is it forbidden for the Member States to introduce legislation in which they require a Qualified Electronic Signature for certain types of documents? By issuing such a provision, don't they deny legal effectiveness of electronic signatures that are not qualified in the sense of Article 5.1?

Article 5.1 of the Directive states that Member States have to ensure that "Qualified Electronic Signatures" satisfies 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. Therefore Member States can, for example, issue legislation stipulating that a Qualified Electronic Signature on an electronic document will have the same legal effect as a handwritten signature on a paper document. The denial of the legal effectiveness of other electronic signatures in such a provision is, in other words, not solely based on the grounds that they are not "qualified" but on the ground that the electronic document needs an electronic signature that is the equivalent of the handwritten signature on the paper document.

This is exactly what we have called "taking the paper-based environment as the reference point". What Article 5.2 prohibits, is to attribute to the "qualified" or "accredited" electronic signature a legal value beyond this equivalency. The Member States should, in other words, never introduce legislation requiring the use of "Qualified Electronic Signatures" except in a context where there is a need to have an electronic substitute for a handwritten signature. As an example, legislation referring to "Qualified Electronic Signatures" in a context where paper-based procedures have completely disappeared would be in contradiction with Article 5.2.

The objective of Art. 5.1 has certainly never been to introduce, neither now nor in the future, a more or less unique European standardized secure electronic signature that can be used for various legal transactions. That would be a very dangerous strategy, of a sort constantly avoided by legislators. In order to remain stable and to avoid constant changes and updates, laws formulate only rules but rarely describe *how* people have to implement the rules. The "how" is the object of standards, which have, by definition a voluntary character. As long as people comply with the rule, they are free to decide how they do this. Sometimes legislation refers explicitly to standards, but only insofar that this is strictly necessary and the reference to a particular standard is mostly interpreted in a restrictive manner.

These elementary principles should be borne in mind when interpreting Art. 5.1 of the Directive and having regard to these principles, the reference to the (standardized) "Qualified Electronic Signature", should not be extended. Meeting the requirements of a QES only results in a presumption of equivalency with the handwritten signature. Art. 5.2 explicitly forbids to go beyond this restriction and to use the QES-concept for other purposes.

It should also be made clear that Article 5.2 does not deal uniquely with the legal admissibility of electronic signatures as evidence in legal proceedings. The provision is not only meant to guide judges in the Member States but also legislators. Article 5.2 mentions also the denial of legal effectiveness.

One could call Article 5.2 for this reason a "long-term" provision. European legislation has not sought to use the concept of "Qualified Electronic Signature" beyond the context of Article 5.1. As soon as it is no longer necessary to search an "automatic" electronic substitute for the handwritten signature, the concept should be abandoned. Every kind of electronic signature should, from that moment onwards, be judged only with regard to its objective adequacy in the specific context.

How should one then look upon the numerous provisions issued in the Member States and requiring explicitly the use of electronic signatures based on a Qualified Certificate issued by an *accredited* certification-service-provider? Are these provisions not in contradiction with Article 5.2? The answer is that most of these national provisions are probably based on the public sector exception of Article 3.7 of the Directive but one should evidently bear in mind the restrictions and limits on the use of the public sector exception that have been explained earlier in this report.

Recommendations:

- With regard to the application of Art. 5.2 is a primary need for clarification. All interested parties should become better informed about the objective and the scope of this provision.

- The Commission should systematically examine if the Member States have issued legislation referring to Qualified or Accredited Electronic Signatures and detect where such references don't comply with the rule of Art. 5.2

5.5 Creating a favourable climate

Besides the internal market objectives and the promotion of a European-wide legal acceptance of electronic signatures, the European Directive also seeks to create a favourable electronic communications and e-commerce climate in the EU. This objective has often been misunderstood. The European Directive has frequently been criticized because it was not able to generate a large-scale use of (PKI-based) electronic signatures in Europe.

5.5.1 Effect on the market

It has become quite apparent that the introduction of a Community legal framework for electronic signatures could never lead to a massive introduction of PKI. This has never been the intention of European legislation. The Directive certainly aims to promote the use of electronic signatures and also to encourage secure electronic commerce - but only by removing some of the possible legal obstacles.

From the Directive's perspective, it primary objective was to protect the Internal Market in order to create a geographically larger market for European product vendors and service providers. In the second place it promotes the general legal acceptance of electronic signatures, thus removing legal obstacles for cross-border electronic transactions in Europe. It is clear that the Directive's objectives have not entirely been realised. The Directive has resulted in a whole series of national regulatory frameworks which have not lead to a European-wide environment for the use of electronic signatures. In previous paragraphs we have seen what can be done in order to remedy this situation.

It has never been the Directive's intention to facilitate the launching of PKI for electronic signatures in Europe. Whether or not there is a demand for this kind of option is not dependant on a comprehensive legal framework. Nevertheless it may be worth examining what can be done to stimulate the use of electronic signatures and secure electronic communications in general. In our view specific efforts are needed in the area of standardization. Moreover, initiatives can be taken in order to increase general trust in electronic signatures by, for example, taking the user more into account.

5.5.2 Standardisation

Regarding the security standards related to the Qualified Electronic Signatures of the Directive, currently only one set of standards exists. These have been developed by EESSI and based on PKI technology, since the requirements of Article 5.1 presumes certificate-

based solutions. This may hinder other technologies from being used for Qualified Electronic Signatures, and prejudice the use of PKI for other electronic signatures.

The Commission and Member States should encourage further work on standards related to Annex II (f) and Annex III, in order to promote the use of alternative technologies for Qualified Electronic Signatures. Although the present standards are mostly technology neutral (within the framework of PKI), they still favour the use of smart cards as SSCDs for example.

At the same time it is vital to ensure the long-term maintenance of the standards referenced in the Official Journal, either by transferring current CWAs to a more permanent body, for example ETSI, or to promote the CWAs to European Norms.

The development of a common specification for algorithms and parameters used for electronic signatures should have been done much earlier at a European level, for example through EESSI. The present lack of commonly recognised specifications will lead to interoperability problems and lack of cross-border acceptance. The current situation being that several national specifications are more often than not published in a national language only. This can potentially act as a market barrier.

The lack of interoperability, both at a national and cross-border level, is a big obstacle for market acceptance and proliferation of electronic signatures. It has resulted in many isolated "islands" of electronic signature applications, where certificates from only one CA can be used for one application. In a few cases only can certificates from multiple CAs be used for multiple applications. Much more should therefore have been done earlier at a European level to promote interoperability:

- Although EESSI has worked on interoperability standards, this was reluctantly accepted by several Member States, and therefore did not receive the appropriate attention at an early stage.
- Although the Commission has sponsored several R&D projects related to interoperability (pki Challenge, ESTIO, TIE), the results of these projects have not been visible in the market, and certainly not in the application of electronic signatures.

The development, promotion and use of interoperability standards must now be done at a European level. If done only at the level of the nation state the result will be varying standards, which in turn hinders cross-border use whilst at the same time putting different requirements to product vendors from every national market, thus diminishing the probability that vendors will adopt their products to the standards. We can only hope for interoperability in standard products if European-wide requirements can be put to the vendors.

Recommendations:

- The Commission and Member States must ensure that all Member States correctly implement presumption of conformity with standards referenced in the Official Journal. This is currently not the case in all European countries.
- The Commission and Member States should encourage further work on standards related to Annex II (f) and Annex III, in order to promote the use of alternative technologies for Qualified Electronic Signatures. Although the present standards are mostly technology neutral (within the framework of PKI), they still favour the use of smart cards as SSCDs for example.
- The long-term maintenance of the standards referenced in the Official Journal must be ensured, either by transferring the current CWAs to a more permanent body, for example ETSI, or promote the CWAs to European Norms.
- The Commission must urgently ensure the acceptance of a common specification for algorithms and parameters, as well as a common maintenance procedure for that specification. It must also ensure that the related procedures are sufficiently open.
- The complex areas of archiving and long-term validation of electronically signed documents are often perceived as obstacles for the use of electronic signatures. The Commission should promote work on guidelines and standards in these areas.
- The Commission and the Member States should find mechanisms to promote/recommend the standards for interoperability already developed by ETSI within the framework of EESSI.
- The Commission should support the work being done in EUCLID and CEN Workshop on e-authentication, steering them towards developing appropriate European standards, taking into account the results from EESSI, pki Challenge and other projects.
- The Commission could promote or arrange a European forum for electronic signatures, directed towards CSPs, product vendors and application providers in order to stimulate development and use of interoperability standards, possibly also initiating the setting up of interoperability testing facilities.

5.5.3 Taking a user's perspective

Our final reflections in the framework of this study focus on the user. In our view it is absolutely necessary to put more emphasis on the user's perspective in all discussions regarding the European electronic signatures regulatory framework. The absence of this perspective has been a more or less constant theme not only in the legal discussion but also in the standardization activities around the Directive. Business and/or technical considerations prevailed strongly in every debate in this area. This has resulted in a set of legal and technical solutions that are often far removed from the daily needs of the common user.

As far as standardization is concerned, it is probably useful to systematically *scan* the existing standardization documents from a user's perspective. With regard to Qualified Electronic Signatures the aim of the standardization activities should be to develop the specifications of a solution that gives the user the possibility to use electronic signatures on a European-wide scale. Such a solution has to take into account *all* aspects of electronic signatures, not only covering the whole signature chain but also taking account of typical users' concerns such as ease of use, language obstacles, cost considerations, etc.

With regard to the legal framework it may become necessary to take a more practical approach. The Directive focuses very strongly on one business model, which took centre stage from 1998 to 2000 but which has since been replaced by a much more heterogeneous and complex market. As a result of this, the current regulatory framework includes detailed rules for issuers of certificates but fails to consider other types of certification providers. Services like time-stamping, revocation, repository, and archival can be offered by third parties which are contracted by the authority issuing certificates. And yet regulatory needs relating to other categories of trust service providers are at least as important as those relating to the certificaction service providers. There is, for example, a clear need for regulation dealing with archival service providers, or with registered mail services. From a users' point of view it is difficult to understand why such services remain completely unregulated, while complex regulatory frameworks have been well established for those issuing certificates. We therefore recommend that further studies be carried out dealing with other categories of trust services.

Last but not least it is necessary to combine electronic authentication with personal data protection. The current European regulatory framework is very much focused on the use of identity certificates. In recent years, attention has shifted towards better privacy protection in the online environment. Research has been focused on the possibility of combining electronic authentication with the needs for anonymity or the use of multiple virtual identities. The efforts of the European Union to promote advanced personal data protection for its citizens should not be contradicted by its regulatory framework for electronic authentication. Further research is needed into the possibility of combining anonymity and pseudonymity with the provisions of the electronic signatures Directive.

The Research Team is aware of the fact that its conclusions and recommendations can only be considered as a first step in the review of the European regulatory framework for electronic signatures. It hopes that the study will provide interesting material for launching a European-wide discussion on this subject.

September 2003

Appendix 1: National questionnaires

See separate binder comprising national questionnaires.

Appendix 2: Collection of relevant legislation and case law

See separate binder comprising collection of relevant legislation and case law.

Appendix 3: Scorecards of applications for electronic signatures

This chapter describes a number of applications for electronic signatures in actual use in Europe today. It contains typical examples and is by no means complete and exhaustive. Pure authentication applications (secure login) and simple pilot applications or trials are not included.

Austria: Foreign account management

Application	Registration procedure of the Austrian National Bank for foreign bank accounts, using electronic form processing
Certificates	Non-Qualified Certificates issued by an accredited Austrian CSP
Costs	Registration fee 12 €, annual fee 12 €, signature card 25 €
CSPs	A-Trust
Users	Foreign account owners
User identity	pseudonym and CIN (Cardholder Identification Number)
Requirements	SSCD and software recommended by A-Trust
Legal basis	5.2

Austria: Notary certificate archive

Application	Notary certificate archive (CyberDoc): Scanning, signing and archiving of certificates. Application Provider: Siemens
Certificates	Non-Qualified Certificates issued by an accredited Austrian CSP
Costs	Registration fee 12 €, annual fee 12 €, signature card 25 €
CSPs	A-Trust
Users	Notaries and their staff
User identity	pseudonym and CIN (Cardholder Identification Number)
Requirements	SSCD and software recommended by A-Trust
Legal basis	5.2

Belgium: E-government

Application	Planned E-government using Electronic ID-card
Certificates	Qualified certificates issued by government as accredited CSP
Costs	About 10 €
CSPs	Belgian government
Users	All citizens above 18 years during 5 years
User identity	Official personal ID number from National Register
Requirements	SSCD
Legal basis	Contract

Belgium: E-tax for citizens

Application	Electronic tax declaration (tax-on-web)
Certificates	None (typical access authentication with userID & passwords on scratch card)
Costs	Free
CSPs	Belgian government
Users	Limited to natural taxable persons in employee status (currently 75.000

	users registered)
User identity	Official personal ID number from National Register or social security nr.
Requirements	Token (scratch card)
Legal basis	Contract

Denmark: E-banking

Application	Private e-banking
Certificates	Non-Qualified Certificates issued by all major banks
Costs	Free
CSPs	Banks
Users	1.9 million bank customers
User identity	Customer number
Requirements	No smart card required
Legal basis	Contract

Denmark: E-government

Application	Planned e-government services by public authorities, using ETSI signature format standards
Certificates	OCES-certificates (simplified certificates for electronic services)
Costs	Free
CSPs	CSPs entitled to issue OCES-certificates (at the time being TDC and Eurotrust).
Users	Public authorities and citizens. Today ca. 40.000 OCES-certificates are issued. It is expected that the number will be +350.000 within a year.
User identity	Name or pseudonym (upon choice by the signatory). Official personal IĐ numbers are replaced with special new numbers for which the CSP holds the keys for conversion.
Requirements	No smart card required
Legal basis	OCES-signatures (5.2)

Finland: E-government

Application	Several e-government services using Electronic ID card, issued by Population Register Centre (PRC)
Certificates	Qualified Certificates
Costs	EID-card, card reader
CSPs	PRC
Users	Ca 2,000 citizens
User identity	Full name and the special electronic transaction identifier given to every citizen and stored into the population information system
Requirements	Card reader and software
Legal basis	Can be used for handwritten equivalence (5.1)

France: E-tax for citizens

Application	E-declaration of gross income
Certificates	Non-Qualified Certificates
Costs	Free
CSPs	Ministry of Finance (operated by Certplus)
Users	Citizens
User identity	
Requirements	
Legal basis	

France: E-tax for companies

Application	E-declaration of VAT
Certificates	Non-Qualified Certificates
Costs	Free
CSPs	Banks (mostly operated by Certplus) and other CSPs
Users	Companies
User identity	
Requirements	
Legal basis	5.2 and special legislation

Germany: E-government for citizens

Application	About 200 applications for e-government in cities for citizens
Certificates	Qualified certificates from accredited CSPs
Costs	Typically 60 €/yr
CSPs	Telekom Telesec, Datev, Deutsche Post SignTrust
Users	Ca 5.000 civil servants
User identity	Name (Pseudonym)
Requirements	SSCD, evaluated software provided by CSP. Software for verification.
Legal basis	Can be used for handwritten equivalence (5.1)

Germany: E-government for professionals

Application	10 applications for e-government in states for professionals, for instance for communication between lawyers and courts
Certificates	Qualified certificates from accredited CSPs
Costs	Typically 60 €/yr
CSPs	Telekom Telesec
Users	Ca 1.000 civil servants and professionals
User identity	Name (Pseudonym)
Requirements	SSCD, evaluated software provided by CSP. Software for verification.
Legal basis	Can be used for handwritten equivalence (5.1)

Germany: Internal E-government

Application	Internal e-government in states for instance in the administration of the State Niedersachsen
Certificates	Qualified certificates from accredited CSPs
Costs	Typically 60 €/yr
CSPs	Telekom Telesec
Users	Ca 15.000 civil servants
User identity	Name (Pseudonym)
Requirements	SSCD, evaluated software provided by CSP. Software for verification.
Legal basis	Can be used for handwritten equivalence (5.1)

Greece: Stock exchange

Application	Submission of company information to stock exchange
Certificates	Qualified certificates and Non-Qualified Certificates
Costs	Paid by Stock Exchange
CSPs	ASYK (subsidiary of Athens Stock Exchange)
Users	Ca 1,000 authorised company employees
User identity	Full name + registered identification number
Requirements	Smart card
Legal basis	Handwritten equivalence (5.1)

Ireland: Secure e-mail

Application	Secure e-mail
Certificates	Non-Qualified Certificates
Costs	"Almost free"
CSPs	PostTrust
Users	Professionals, like solicitors and accountants
User identity	E-mail address
Requirements	Secure e-mail plugin, provided by PostTrust
Legal basis	Can be used for handwritten equivalence in Ireland

Ireland: E-banking

Application	E-banking, offered by all major Irish banks
Certificates	Non-Qualified Certificates
Costs	"Almost free"
CSPs	Unknown
Users	Private and corporate banking customers
User identity	Customer identity
Requirements	
Legal basis	Contracts

Ireland: E-tax

Application	Tax submission, offered by Revenue Online Services (ROS)
Certificates	Non-Qualified Certificates
Costs	"Almost free"
CSPs	ROS
Users	Business users
User identity	Special identity number established for the service
Requirements	
Legal basis	Handwritten equivalence

Italy: E-government

Application	Different services offered by public administrations
Certificates	Qualified certificates from accredited CSPs
Costs	Typically 150 €
CSPs	Accredited CSPs
Users	Citizens and companies
User identity	Name, surname, fiscal code
Requirements	SSCD, software
Legal basis	Handwritten equivalence

Netherlands: DigiNotar

Application	Certification services by notaries. Envisaged applications comprise government, financial, industry, logistics, healthcare, commerce and independent professionals.
Certificates	Four types: a personal company certificate, an envelop certificate (identifying a company or a department within a company), a server certificate and a certificate for the independent professional.
Costs	
CSPs	76 notary-offices will function as Registration Authorities to the CSP Diginotar BV (planning to be accredited during 2003)
Users	Government and company employees, professionals
User identity	In case of an envelop certificate, the company name and a unique number (issued by Diginotar) are contained in the certificate
Requirements	For some applications, smart cards are required
Legal basis	Adapted legislation, 5.2

Netherlands: E-government

Application	PKI Overheid: Planned e-government
Certificates	Qualified certificates with accredited CSPs
Costs	
CSPs	None yet
Users	government institutions, employees, companies, citizens
User identity	Name, possibly also pseudonym, employee functions, employee authorisations or professions
Requirements	SSCD,
Legal basis	Handwritten equivalence (5.1)

Portugal: Bank transaction security

Application	Signing of transactions between banks (used by several banks)
Certificates	Non-Qualified Certificates with Extended Key Usage
Costs	Signer: Certificate, card and reader: 95 € Verifier: CRL free, OCSP 0.09 €/transaction
CSPs	MULTICERT
Users	About 100 clients, creating on average 2 signatures/day
User identity	Pseudonym and full name (can include customer and/or internal number)
Requirements	Software provided by MULTICERT
Legal basis	Can be used for handwritten equivalence

Spain: E-government

Application	Central and local e-government applications, mainly in the fields of taxes and social security
Certificates	Qualified certificate based on smart card
Costs	Certificates for tax filing are free
CSPs	FNMT (Spanish Mint)
Users	Citizens
User identity	Name and NIF (tax identity number)
Requirements	Use of smart card for Qualified Electronic Signatures
Legal basis	5.1 and 5.2 signatures

Sweden: E-banking

Application	e-Banking is provided by all Swedish banks, with about 3 million users

Certificates	Some banks use certificates, others using tokens and one-time passwords for electronic signatures
Costs	0 – 20 €
CSPs	Each bank
Users	3 million private and corporate customers
User identity	Name, personal ID number
Requirements	None
Legal basis	Contract

Sweden: E-government

Application	Ca 10 applications: Tax returns, parental leave compensation, energy registration, company registration, health care,
Certificates	Non-Qualified Certificates, using government defined standard
Costs	Users: 0 – 50 € Relying parties: 0.4 €/transaction
CSPs	Appointed via government procurement process: Several banks, Sweden Post, Telia
Users	Citizens, companies
User identity	Name, personal ID number
Requirements	Software provided by CSPs
Legal basis	Adapted laws, 5.2

Sweden: Secure e-mail

Application	Secure e-mail
Certificates	S/MIME
Costs	Mostly free
CSPs	Sweden Post, Telia, Verisign
Users	Citizens companies
User identity	e-mail address
Requirements	
Legal basis	5.2

Czech Republic: E-customs

Application	Electronic custom clearance
Certificates	Qualified certificates from accredited CSP
Costs	12-67 €
CSPs	První certifikační autorita
Users	
User identity	Name, pseudonym
Requirements	SSCD
Legal basis	Law, 5.1

Estonia: eID-card

Application	An Electronic ID card is being deployed which can be used for several different electronic signature applications: • exchange of signed documents between individuals, • communication between bank and real estate brokers and loan customers for exchanging real estate evaluation acts. • submission of applications to local government for changing their place of living in the population register. • companies can use electronic signatures to coordinate their

	internal work regulations with the Labour Inspection
Certificates	Qualified certificate
Costs	10 € /card. Associated software (Digidoc) free
CSPs	AS Sertifitseerimiskeskus issues certificates for the eID cards
Users	Potential uses are all ID card holders (more than 200 000 in May 2003)
User identity	Name, user ID, email address
Requirements	eID card and OpenXAdES/DigiDoc software
Legal basis	5.1

Poland: E-government

Application	Płatnik (by Prokom Software)- an application used for the transmission of social insurance data between ZUS (Polish Social Insurance Institution) and entities employing more than 5 employees
Certificates	Non-Qualified Certificates
Costs	60 €/yr
CSPs	The service has been provided by Unizeto for ZUS
Users	Users acting on behalf entities employing more than 5 employees
User identity	
Requirements	Special software, free of charge
Legal basis	Special law

Poland: Interbank clearing

Application	ELIXIR - “the Electronic Clearing System - is a system for clearing interbank transactions
Certificates	Non-Qualified Certificates
Costs	60 €/yr
CSPs	KIR - provides the service and issues certificates
Users	38,000 users in banks
User identity	
Requirements	Smart cards
Legal basis	Contract

Slovenia: Corporate e-banking

Application	Corporate and private e-banking
Certificates	Qualified certificates
Costs	Corporate: 100 €; private 25 €
CSPs	Halcom CA, AC NLB
Users	Persons authorised by their companies to sign the documents; citizens
User identity	Full name, VAT number
Requirements	70 % use of smart cards for corporate e-banking
Legal basis	Handwritten equivalence (5.1)

Slovenia: E-government

Application	Internal and public e-government applications (G2G, G2B, G2C)
Certificates	Qualified certificates
Costs	Ca 100 € for G2G, G2B; < 10 € for G2C
CSPs	Sigen-CA, Sigov-CA
Users	Employees, citizens
User identity	Full name, VAT number
Requirements	Smart cards required for internal e-government (G2G)
Legal basis	Handwritten equivalence (5.1)

Romania: E-tax

Application	e-government: payment of local taxes
Certificates	Qualified certificates
Costs	40 € for certificate, 50 € for hardware
CSPs	E-SIGN ROMANIA S.A
Users	Company employees
User identity	Full name, e-mail address
Requirements	Smart card
Legal basis	Handwritten equivalence (5.1)

Norway: Betting

Application	On-line gaming/betting at National Lottery
Certificates	Qualified certificate
Costs	9 €/yr incl smartcard, reader
CSPs	ZebSign
Users	Citizens
User identity	Full name and unique Id which may be 'translated' to national personal IÐ number if necessary
Requirements	Software provide by service provider
Legal basis	5.2

Norway: M-commerce

Application	Mobile e-commerce at Telenor Mobile
Certificates	Qualified certificates
Costs	0.1-0.3 €/transaction
CSPs	ZebSign
Users	Citizens
User identity	Full name and unique Id which may be 'translated' to national personal IÐ number if necessary
Requirements	Mobile phone
Legal basis	5.2

Appendix 4: Country index cards

COLLECTION OF WEB LINKS 173
AUSTRIA 174
BELGIUM 177
DENMARK 179
FINLAND 182
FRANCE 186
GERMANY 189
GREECE 192
IRELAND 195
ITALY 198
LUXEMBOURG 201
NETHERLANDS 204
PORTUGAL 207
SPAIN 209
SWEDEN 212
UNITED KINGDOM 215
CYPRUS 218
CZECH REPUBLIC 220
ESTONIA 223
HUNGARY 226
LATVIA 229
LITHUANIA 231
MALTA 233
POLAND 236
SLOVAKIA 239
SLOVENIA 241
BULGARIA 243
ROMANIA 246
ICELAND 248
LIECHTENSTEIN 250
NORWAY 253
SWITZERLAND 256

Collection of web links

The web links contained in the subsequent country index cards are also available on the following web page:

http://www.pki-page.info/eu/

This web page is regularly updated.

Austria

Transposition of the Directive	Federal Law n°. 190/99 on electronic signatures as last amended in 2001, entered into force January 1, 2000. Federal Ordinance n°. 30/2000 on Electronic Signature, entered into force February 3, 2000.
Definitions (art. 2)	Signatory can only be a natural person. In the definition of signatory fall also CSPs who issue certificates to provide certification services. CSPs acting as signatories can also be legal persons.
Types of signatures	Two types are defined: "Basic" and "Secure" electronic signatures. Secure electronic signatures are AES which in addition: i) are based on a QC, ii) are created using technical components and procedures which comply with the security requirements as stipulated in the Austrian regulation.
Legal equivalence to handwritten signatures (art. 5.1)	Secure electronic signatures meet the requirements of handwritten signatures, especially the requirements of written form as defined in Austrian Civil Code. A special law or agreement between the parties may provide otherwise. Presumption of authenticity of private deeds signed with a secure electronic signature. Secure electronic signatures do not have the legal effects of handwritten signatures for: i) legal transactions in family and inheritance law requiring a written or other special form, ii) declarations of intent or legal transactions requiring formal certification (incl., notary's form), iii) acts requiring official certification in order to be put on a register, iv) declarations of guarantee.
Legal effect of e-signature (art. 5.2)	Explicit transposition: general non-discrimination clause for all forms of signatures. Under the Austrian Civil law system there is no restriction for the use of electronic signatures.
Relevant case law	No ruling yet addressing the use/legal effect of electronic signatures.
Liability (art. 6)	Explicit transposition. CSPs issuing QC are liable vis-à-vis persons who rely on certificates. CSPs which supply secure electronic procedures are liable for the legal conformity and suitability of the signature creation products they supply or recommend. Two additional liability clauses to the Directive's ones: i) failure to immediate revoke a certificate, ii) failure to comply with the requirements of Annex II of Directive, incl. failure to supply secure technical components and procedures. Reversed burden of proof: CSP has to prove that it or its personnel did not act negligently. Limits of liability are the same as in the Directive (limits of use of certificate, value of transactions).
International Aspects (art. 7)	Validity of all foreign certificates (issued by CSPs established within the EU or not) shall be verifiable. EU QCs are tantamount to Austrian ones, provided that their validity can be checked. For non-EU certificates: common certificates

	are recognised without conditions if their validity can be verified. Non-EU QCs: same conditions as in art. 7 but, in addition, the validity of QC must be verifiable from Austria. Explicit obligation on supervisory body to operate a directory of Third-State-CSPs who have a liability contract with an Austrian CSP.
Data Protection (art. 8)	Austrian Law states specific data protection obligations: i) Limitation of collection to data being necessary to perform the service. Also, direct collection by the person concerned or an authorised third party; ii) Disclosure of real personal data (if pseudonyms are used) only for an overriding legitimate interest, iii) Communication of data to assist courts and other authorities. No explicit reference to the Austrian Data Protection Act, but implicitly, this Act remains applicable. Use of pseudonyms is permitted if: i) it is indicated as such, ii) pseudonyms are not offensive or obviously open to confusion with real names or signs.
Implementation of the Annexes	All Annexes are copied. However, the Annex II requirements are augmented with requirements for "secure time" and additional security measures. The CSP is also obliged to inform the signatories about products which they must use, complying with the requirements for secure creation and verification of QES. Such products need to be certified by a confirmation body, A-SIT. Annex IV has been transposed as requirements.
Provision of certification services	The legislation explicitly prohibits prior authorization of CSPs. Notification is mandatory for all CSPs, the responsible body is TKK (Telecom Control Commission). The cost of notification is in the range of €100 to €6,000. All CSPs established in Austria are subject to supervision, this process is carried out through regular audit controls. Compliance criteria have been specified. The legislation specifies voluntary accreditation; a scheme has already been implemented. Evaluation rules and accreditation criteria have been established. The Austrian system does not encourage accreditation.
Number of CSPs	6 CSPs issue Qualified Certificates, 2 of which have been accredited.
Use of e-signatures in the public sector	The legislation does not provide any special requirements for the public sector. E-identity applications are being introduced.
Conformity assessment of SSCDs	There is a mandatory assessment of SSCDs, the designated assessment body of which is A-SIT. SSCD products have already been assessed. There are some requirements on the client software, e.g. for presenting the document to be signed.
Use of standards (Article 3.5)	Presumption of conformity to requirements for standards referenced in OJ. No other standards are mandated. However, SigV is being revised at the moment and will include such requirements. SigV also specifies algorithms to be used

	as well as a number of additional standards to follow voluntarily.
Promotion of interoperability	In addition to the voluntary standards mentioned above, the Bürgerkarte project also promotes interoperability through open specifications.
Market for electronic signature products and services	About 10,000 Qualified Certificates have been issued, all based on the use of SSCDs. About 5,000 other certificates have been issued. The most widely used applications are in corporate e-banking and notary archiving. The applications are based on non-Qualified Certificates and smart cards (although not SSCDs), thus rendering 5.2 signatures. The first Austrian electronic ID cards have now been issued. The cost per card is approximately EUR 100 (including card reader and registration fee), and the validity of a Qualified Certificate amounts to three years. A "simplified" Citizen Card is also being introduced, without requirements for evaluated SSCD, and which will be used for a number of e-government applications where there are no strict form requirements for handwritten signature.
Web links	http://www.ris.bka.gv.at/bundesrecht/ http://mailbox.univie.ac.at/thomas.menzel/docs/Signature_Law_E.pdf http://mailbox.univie.ac.at/thomas.menzel/docs/Signature_Order_E.pdf http://www.buergerkarte.at/ http://www.signatur.rtr.at/en/index.html http://www.cio.gv.at/identity/ http://www.a-sit.at/signatur/bestaetigungsstelle/bestaetigungsstelle.htm http://mailbox.univie.ac.at/thomas.menzel/pubs/ifip99_paper.pdf http://www.bka.gv.at/datenschutz/indexe.htm http://www.signatur.rtr.at/repository/rtr-csp-notification-10-20010601-de.zip http://www.signatur.rtr.at/ http://www.signatur.rtr.at/en/repository/tkk-accreditation-atrust-20020311.html http://www.a-sit.at/signatur/bestaetigungsstelle/bescheinigung/veroeffentlichung_18_5_/veroeffentlichung_18_5_.html http://www.a-sit.at/signatur/bestaetigungsstelle/bescheinigung/veroeffentlichung_andere/veroeffentlichung_andere.html http://www.a-sit.at/

Belgium

Transposition of the Directive	i) Act of 20 October 2000 "introducing the use of telecommunications tools and electronic signatures in the judicial and extra-judicial procedure", entered partially into force 1 January 2001 (ES-Act). ii) Act of 9 July 2001 "introducing a legal framework for electronic signatures and certification services" entered into force 9 October 2001 (CSP Act). iii) Royal Decree of 6 December 2002 "organising the supervision and accreditation of CSPs issuing QC", entered into force 27 January 2003.
Definitions (art. 2)	No definition of signatory: Instead, reference to "certificate holder", being a physical or legal person whom has been issued a certificate by a CSP.
Types of signatures	Three types are defined: "Basic" as in the Directive and Advanced Electronic Signature (responding to the same requirements as in the Directive). Implicit recognition of a higher level of signature (being the "qualified" one: AES based on a QC and created by an SSCD).
Legal equivalence to handwritten signatures (art. 5.1)	For all legal purposes: AES based on a QC and created by an SSCD are assimilated with handwritten signatures, irrespective of the fact that the signature has been put by a legal or natural person.
Legal effect of e-signature (art. 5.2)	Explicit transposition: No electronic signature can be denied legal effectiveness and admissibility as evidence in legal proceedings. For evidential purposes, an e-signature can be used as an alternative of the handwritten one, if: i) one can derive with certainty the identity of the author; ii) one can derive with certainty the integrity of the contents to be signed.
Relevant case law	No ruling yet addressing the use/legal effect of e-signatures.
Liability (art. 6)	Literal transposition.
International Aspects (art. 7)	Same Article as in the Directive.
Data Protection (art. 8)	Explicit transposition. CSPs need to observe general data protection legislation and obligations described in the data protection clause of the CSP Act (following verbatim art. 8 of the Directive). Use of pseudonyms is authorised. Such pseudonyms shall be disclosed to public authorities under the conditions stipulated in the Code of Criminal Procedure.
Implementation of the Annexes	The Annexes are literally copied.
Provision of certification	The legislation does not prohibit prior authorisation of CSPs. Notification is mandatory for CSPs issuing QCs, the responsible body is the ministry of economic affairs. There is no cost of notification.

services	economic affairs. There is no cost of notification. CSPs issuing QCs to the public and established in Belgium are subject to supervision, this process is carried out through audit controls at any time. Compliance criteria have been specified but not published yet. The legislation does not explicitly define accreditation but refers to accreditation in Art 17 and 18; a voluntary scheme has already been implemented. Evaluation rules have been established, accreditation criteria are being drafted but have not been published as of yet. The Belgian system does not encourage accreditation.
Number of CSPs	2 CSPs issue QCs, there is no accredited CSP yet.
Use of e-signatures in the public sector	The legislation defines specific requirements for the use of electronic signatures in the public sector. On-going projects include e-identity, e-VAT, and e-social security projects.
Conformity assessment of SSCDs	There is a mandatory assessment of SSCDs, the designated assessment body of which has not been appointed yet.
Use of standards (Article 3.5)	Presumption of conformity to requirements for standards referenced in OJ. No other standards are mandated or recommended. No algorithms have been specified.
Promotion of interoperability	Different working groups exist in which the market players interchange information (e.g. ADM, L-SEC, BELCLIV).
Market for electronic signature products and services	The most widely used applications are e-banking (using contractual agreement and/or 5.2 signatures). The Belgian electronic ID card was officially launched in March 2003. It will progressively replace, over a period of five years, the current paper ID cards that are mandatory for all citizens and residents in the country. Belgium will then become the first European state to issue electronic ID cards to its entire population. The project costs are estimated to amount to EUR 10m for the pilot phase and EUR 100m for the whole project. Each resident will have to pay around EUR 10 to get his/her electronic ID card, which will then be used as a proof of identity for accessing services in the real as well as the virtual world. It will contain the same data currently featured on the paper ID cards, plus two electronic signatures (one serving for identifying the holder and the second for signing electronic documents). The card will therefore be the main identification and authentication instrument for accessing e-government services.
Web links	http://www.icri.be/ http://www.mineco.fgov.be/ http://www.digitalsignature.be/

Denmark

Transposition of the Directive	Act n°. 417/2000 on Electronic Signatures entered into force on 1 October 2000. Content of Act very similar to the content of Directive. Executive Order n°. 923/2000 on "Security Requirements etc. for Certification Authorities", entered into force on 16 October 2000. Executive Order n°. 922/2000 on "Reporting of Information to the National Telecom Agency by CAs and system Auditors" entered into force on 16 October 2000.
Definitions (art. 2)	E-signature defined as any data that ensure data origin and data integrity. Signatories can only be natural persons. Law defines Certification Authorities, not CSPs. Narrow definition of CAs: natural or legal persons who issue certificates. Other definitions same as in the Directive.
Types of signatures	3 types: "Basic" - AES (defined as in the Directive). The law implicitly recognises a "higher level" of signature, the qualified e-signature: AES based on a QC and created by an SSCD.
Legal equivalence to handwritten signatures (art. 5.1)	If law stipulates that electronic messages/documents shall be provided with a signature this requirement is met as long as a qualified e-signature is used. In the case of electronic messages/documents to or from public authorities, this rule applies unless special legislation provides otherwise.
Legal effect of e-signature (art. 5.2)	No transposition. The effect of art. 5.2 has already been applying as a general rule. Specific provisions in law may preclude the use of e-signatures (work in ministries is underway to identify cases for amendment of current regulation).
Relevant case law	No ruling yet addressing the use/legal effect of e-signatures.
Liability (art. 6)	Explicit transposition. Clause addresses liability of CAs issuing QC to the public for damages caused to any party (including signatories) reasonably relying on certificate. Liability clauses the same as in art. 6 and, in addition: i) failure to revoke, ii) lack or erroneous information on revocation of certificate, expiry date or on whether certificate includes limitations. Reverse burden of proof. Limitations of liability same as in the Directive (limits of certificate uses and value of transactions). CAs cannot waive their liability by prior agreement or limit it to other cases than the pre-stated ones.
International Aspects (art. 7)	Explicit transposition of art. 7. Conditions of recognition identical to the Directive's ones.
Data Protection (art. 8)	Act stipulates data protection obligations for CAs only. These obligations reiterate art. 8 §2 of Directive. Use of pseudonyms is authorised, provided that they are identified as such.
Implementation of	Annex I, II and III are copied. The CSP requirements in Annex II are

the Annexes	augmented with a number of detailed requirements. Annex IV is not transposed.
Provision of certification services	The legislation does not prohibit prior authorisation of CSPs. Notification is mandatory for CSPs issuing QCs, the responsible body is ITST (National IT and Telecom Agency). There is no cost of notification but an annual audit has to be paid by the CSPs. CSPs issuing QCs to the public and established in Denmark are subject to supervision, this process is carried out through annual audit controls. Several documents have been published as the basis of compliance criteria. The legislation does not mention voluntary accreditation; a scheme thus has not been implemented.
Number of CSPs	3 CSPs issue QCs.
Use of e-signatures in the public sector	The legislation does not provide any special requirements for the public sector.
Conformity assessment of SSCDs	There is a mandatory assessment of SSCDs, no assessment body has been designated though.
Use of standards (Article 3.5)	Presumption of conformity to requirements for standards for SSCDs referenced in OJ. Some requirements from ETSI TS 101456 (QCP) are mandated in the Order. No other standards are mandated or recommended. No algorithms have been specified.
Promotion of interoperability	The Forum for Digital Signatures within Danish Standard Association has issued a profile for Qualified Certificates in Denmark. This includes a recommended sequence for verifying a digital signature. A lightweight certificate, OCES, has also been specified for e-government use.
Market for electronic signature products and services	Ca 2,000 Qualified Certificates have been issued, 90 % of which are based on SSCDs. In addition, ca 25,000 non-Qualified Certificates have been issued, mainly for e-banking under contractual agreement. For e-government, 350.000 OCES-certificates are expected to be issued by May 2004 and 1.300.000 by May 2007. The certificates will initially mainly be used for tax filing under adapted laws using 5.2 signatures.
Web links	http://www.videnskabsministeriet.dk/cgi-bin/doc-show.cgi?doc_id=41719&leftmenu=LOVSTOF http://www.itst.dk/wimpdoc.asp?page=tema&objno=95024223 http://www.itst.dk/wimpdoc.asp?page=tema&objno=95024224 https://www.signatursekretariatet.dk/ http://www.e.gov.dk/

	http://www.certifikat.dk/ http://www.kmd-ca.dk/ http://www.eurotrust.dk/ http://www.videnskabsministeriet.dk/cgi-bin/news-archive-list.cgi http://www.jm.dk/wimpdoc.asp?page=dept&objno=59213 http://www.itst.dk/mainpage.asp

Finland

Transposition of the Directive	i) Act on Electronic Signatures n°14/2003 being the main implementation law, entered into force on 1 February 2003. ii) Act n°. 15/2003 amending the Act regulating the Finnish Communications Regulatory Authority (FICORA), entered into force on 1 February 2003. iii) Regulation of FICORA on CAs' notification obligations. iv) Regulation of FICORA on the reliability and security of CAs providing QC.
Definitions (art. 2)	Signature: defined as in the Directive. Signatory: can only be a natural person holding lawfully the signature creation data. CSP: natural or legal person who provides certificates. Despite the apparent narrow meaning of the term CSP, the scope of Act actually addresses all "certification-related" services.
Types of signatures	"Basic" - AES (same requirement as Directive). The Act implicitly provides for a "higher level" of signature, being the qualified one: AES based on a QC and created by an SSCD.
Legal equivalence to handwritten signatures (art. 5.1)	Explicit transposition. The requirement of a signature is fulfilled at least by an AES based on a QC and created by an SSCD.
Legal effect of e-signature (art. 5.2)	No explicit transposition. Finnish law is based on principles of contractual freedom, incl. the form of legal acts, and of free consideration of evidence by courts. Consequently, any e-signature than the qualified one can have a legal value. There may be cases in which e-signatures could not be used in a particular legal context.
Relevant case law	Existing case law up to now does not address directly admissibility/legal value of e-signatures, but other issues related to admissibility of e-documents: Petition of appeal can be delivered by facsimile. Time of document's arrival onto the fax machine is crucial, not the time of actual printing.
Liability (art. 6)	Direct transposition. Applicability to CSPs issuing QC to the public for third parties relying on certificate (not just reasonably). All liability grounds of art. 6 are covered and, in addition: failure to revoke a certificate (so applicable also to CSP that guarantee certificates of another CSP). Reverse burden of proof. Limitations of liability (the certificate specific usage restrictions).
International Aspects (art. 7)	Explicit transposition - similar conditions to the ones stipulated in the Directive.

Data Protection (art. 8)	Explicit transposition in the Act but addressing only data protection obligations for CSPs. Finnish Data Protection Act applies to infringements committed by any party. The special data protection provision in the Act: i) follows the main rules of the Data Protection Act, ii) reiterates some obligations in relation to CSPs (e.g. namely specifying rules of data transmission through the Population Information System, prohibition to indicate personal identity numbers on certificates, etc.). Data Protection Ombudsman supervises compliance with data protection obligations. Pseudonyms on certificates shall be identified as such.
Implementation of the Annexes	Annex I and III copied, Annex II implemented with similar requirements. Annex IV is not transposed.
Provision of certification services	The legislation does not prohibit prior authorisation of CSPs. Notification is mandatory for CSPs issuing QCs, the responsible body is FICORA (Communication Regulatory Authority). The cost of notification is €3,000. All CSPs established in Finland are subject to supervision, this process is carried out through annual audit controls. In practice, only CSPs issuing QCs seem to be actually supervised. Compliance criteria have been specified both in the e-sign act as well as in regulations. The legislation does not mention voluntary accreditation; a scheme thus has not been implemented.
Number of CSPs	1 CSP issues QCs.
Use of e-signatures in the public sector	The legislation defines specific requirements for the use of electronic signatures in the public sector. On-going projects include e-identity, Internet banking, and social and health care projects.
Conformity assessment of SSCDs	There is an optional assessment of SSCDs, a designated assessment body of which has not been appointed.
Use of standards (Article 3.5)	Presumption of conformity to requirements for standards for SSCDs referenced in OJ. The Finnish Communication Regulatory Authority (FICORA) may issue additional technical orders and recommendations on the requirements of reliability and data security of the operations of CSPs providing Qualified Certificates relating to electronic signatures.
Promotion of interoperability	Population Register Centre (PRC) test card readers and software for their interoperability with the systems of the Centre. In addition the Population Register Centre provides card reader software freely via Internet and has published an open source code for service providers to build electronic services based on certificates. The HST-group has been established consisting of telecommunications operators, banks, a credit card service company and the

	PRC. These parties are issuing smart cards that enhance the use of Qualified Certificates, especially the one given by PRC. In addition, PRC has initiated and is heavily involved in EUCLID (European initiative for a Citizen digital ID solution) to support interoperable electronic identities.
Market for electronic signature products and services	Three types of applications: e-banking (mostly for authentication), e-government (based Electronic ID card) and mobile e-commerce (by mobile operators). Several e-government services are using the EID card, issued by Population Register Centre (PRC), which has been issued to about 2,000 citizens and contains Qualified Certificates. The signatures have handwritten equivalence. The Cooperative Banks Group will introduce the electronic ID by the Population Registration Centre in autumn 2003 in all its smart cards. The operator TeliaSonera will start test use of the electronic ID in its SIM cards in autumn 2003. Moreover, the electronic ID card and the social security card will be combined in June 2004.
Web links	http://www.mintc.fi/www/sivut/suomi/tele/saadokset/telecom/norms/14-2003en.htm http://www.finlex.fi/linkit/sd/20030015 http://www.ficora.fi/englanti/document/FICORA072003M.pdf http://www.ficora.fi/englanti/document/FICORA082003M.pdf http://www.finlex.fi/linkit/ajansd/20030013 http://www.finlex.fi/linkit/sd/20030299 http://www.finlex.fi/linkit/ajansd/19930507 http://www.finlex.fi/linkit/sd/20030300 http://www.finlex.fi/linkit/ajansd/19990829 http://www.finlex.fi/linkit/ajansd/20020458 http://www.finlex.fi/pdf/saadkaan/E9990523.PDF http://www.tietosuoja.fi/uploads/p9qzq7zr3xxmm9j.rtf http://www.mintc.fi/www/sivut/suomi/tele/saadokset/telecom/norms/1999_565.htm http://www.ficora.fi/englanti/tietoturva/index.htm http://www.ficora.fi/englanti/tietoturva/allekirjoitus.htm http://www.mintc.fi/www/index.html http://www.ficora.fi/englanti/index.html http://www.om.fi/333.htm http://www.ficora.fi/suomi/lomake/Laatuvarmennetoiminnan_aloitusilmoituslomake.pdf http://www.ficora.fi/ruotsi/document/Anmalan_om_inledande.DOC http://www.makropilotti.fi/english/ http://www.intermin.fi/intermin/home.nsf/pages/

	25B44413D2D0CA91C2256BC30038F079?opendocument http://www.sahkoinenhenkilokortti.fi/certsearch.asp http://www.openmobilealliance.org/ http://www.pankkiyhdistys.fi/sisalto_eng/upload/pdf/tupasV2eng.pdf

France

Transposition of the Directive	i) Act n°. 2000-230 on "Adaptation of the Law of Evidence on Information Technology and Relevant to e-signatures" entered into force on 14 March 2000 (introducing amendment to Civil Code). ii) Decree n°. 2001-272 "Implementing the new Modification of the Civil Code and relating to e-signatures" entered into force on 1 April 2000. iii) Decree n°. 2002-535 on the "Evaluation and Certification of the Security ensured by e-signatures Products and Systems" entered into force on 20 April 2002. iv) Departmental Order on "the Qualification of CSPs and the Accreditation of the Evaluation Bodies" entered into force on 1 June 2002.
Definitions (art. 2)	E-signature is defined as: data resulting of use of a reliable process of identification guaranteeing the link between the e-data attached to the e-signature and the e-signature". Signatory: Same definition as in Directive but limited to natural persons. CSPs: called "Providers of Electronic Certification Services". Law speaks about "qualification of CSPs" not "accreditation". The latter term is used in relation to the designation of bodies that will audit CSPs for "qualification".
Types of signatures	Three types of signatures: "Basic" - Secure (being the AES of Directive) – a higher level of signature (qualified e-signatures)
Legal equivalence to handwritten signatures (art. 5.1)	Explicit transposition. Act assimilates the e-signature to handwritten signature if certain reliability conditions are fulfilled (identification, link between signature and contents). No explicit mention to other legal effect/validity. The reliability of the e-signature process is presumed when the signature has been created, the identity of the signatory assured and the integrity guaranteed following the conditions of the Decree 2001-272 (i.e. Secure e-signatures based on a QC and created by an SSCD).
Legal effect of e-signature (art. 5.2)	Explicit transposition. Equivalence between the e-signature and a handwritten signature is recognized even if the e-signature does not fulfil the conditions of a QES, unless special legislation prohibits it. French law does not set out cases in which e-signature cannot be used. Decision to be taken on an ad-hoc basis, probably prohibition of e-signature use in relation to acts on consumer protection.
Relevant case law	No ruling yet addressing the legal effect/validity of e-signatures.
Liability (art. 6)	Implementation of this provision in the draft Bill on "Confidence in numeric economy" (Bill is still under discussion). Current law provides for liability rules with larger scope: no list of liability causes. Applicability to all CSPs (issuing QC or not).

International Aspects (art. 7)	Transposition in verbatim of art. 7.
Data Protection (art. 8)	No transposition. General Act on Data Protection applies. Pseudonyms can be used on certificates and shall be indicated as such.
Implementation of the Annexes	All Annexes (I - IV) copied.
Provision of certification services	There is no prior authorization of CSPs in France. CSPs have to notify their activity to DCSSI, they have to inform whether or not they intend to issue QCs. This notification applies to all CSPs. CSPs issuing QCs established in France are subject to supervision, this process is carried out through audit controls. Compliance criteria are currently being specified. The legislation specifies voluntary accreditation (named "qualification" in France), a scheme has already been implemented but "needs to be completed" (e.g. there is no accreditation body yet). Evaluation rules and accreditation criteria are currently being drafted. The French system does not encourage accreditation.
Number of CSPs	No CSPs issuing QCs yet.
Use of e-signatures in the public sector	The legislation does not provide any special requirements for the public sector. Several applications have been introduced, e.g. VAT and gross incomes.
Conformity assessment of SSCDs	There is a mandatory assessment of SSCD, DCSSI being the only designated assessment body. One SSCD product has already been assessed until now.
Use of standards (Article 3.5)	No automatic recognition of standards referenced in OJ, but recognition of conformity certificates from EU Member States. Instead, specific standards are referenced: CWA 14169 for SSCD, CWA 14167-2 for cryptographic modules and a French version of TS 101 456 for CSPs in the voluntary accreditation scheme. General recommendations for algorithms and parameters have been published by DCSSI.
Promotion of interoperability	A certificate profile has been developed for the VAT declaration project.
Market for electronic signature products and services	No supervised or accredited CSPs. E-declaration services have been established based on NQC both for citizens (gross income) and companies (VAT), with Certplus as dominating certification operator on behalf of CAs (Ministry of Finance and banks).

Web links	http://www.legifrance.gouv.fr/ http://www.telecom.gouv.fr/ http://www.internet.gouv.fr/ http://www.ssi.gouv.fr/ http://www.premier-ministre.gouv.fr/ http://www.minefi.gouv.fr/ http://www.droit-technologie.org/ http://www.ssi.gouv.fr/fr/confiance/documents/SIG-P-01.pdf

Germany

Transposition of the Directive	Act on "Framework Conditions for E-signatures and Amending Other Regulations" (SigG Act) entered into force on 22 May 2001 with the exception of certain provisions. Ordinance on E-signatures (SigV) entered into force on […]
Definitions (art. 2)	E-signature: as in the Directive. Signatory: can only be natural person who owns signature codes. Legal persons cannot be signatories. Narrow definition of CSP: being a natural/legal person issuing Qualified Certificates or qualified time-stamps. In addition, following terms are defined: Qualified e-signature / Signature application components / Technical components for certification services / Qualified time-stamps. Terms similar in meaning to Directive's ones: Signature codes, being equivalent to signature creation data and Signature test codes, being equivalent to signature verification data.
Types of signatures	Three types of signatures: "Basic" - AES (same requirements as in Directive) and Qualified (AES based on a QC and created by an SSCD).
Legal equivalence to handwritten signatures (art. 5.1)	Explicit transposition. Amendment of the Civil Code to confirm that the "electronic form" can be used as substitute of the written form. Code of Civil Procedure establishes a presumption of prima facie evidence for qualified e-signatures as ensuring effective security provided that they meet the requirements of their definition. All other codes of procedure refer to this provision. Also equivalency by the administrative procedure law, the general tax law and the general social law.
Legal effect of e-signature (art. 5.2)	No explicit transposition. Electronically signed documents are admissible and have legal effectiveness as evidence in legal proceedings without restrictions. Their probative value is determined by their effective security that can be proven. There may be a few cases in which e-signature cannot be used in a particular legal context.
Relevant case law	A few court cases denying the proof value of unsigned e-mail. On the contrary, a ruling accepted computer generated fax without electronic signature.
Liability (art. 6)	Transposition in broader terms than in art. 6. Clause addresses liability of CSPs issuing QC. Ambit of clause larger than art. 6: Liability for: i) infringements of the requirements of German e-signatures law, ii) failure of e-signature products or of other technical security facilities used by CSPs. Reverse burden of proof. Same liability limitations as in the Directive (certificate uses and value of transactions).
International	Only signatures with a certificate from an EU/EEA country which meets the

Aspects (art. 7)	requirements of art. 5.1 of Directive can be recognised as a qualified e-signature. Signatures with a certificate from a non-EU/EEA country have the same effect as qualified ones if specific conditions are met. These conditions are the same as in art. 7.
Data Protection (art. 8)	Specific provision on data protection obligations for all CSPs. Reiteration of basic data protection principles and restriction of data usage to the purposes of certificate issuance. Use of pseudonyms on certificates is authorised. Public authorities and courts are empowered to take knowledge of real names under conditions.
Implementation of the Annexes	Annex I has been copied, with the difference that the signature of the certificate must be a QES, not just AES. Annex II has been transposed as very detailed requirements for CSPs in SigG and SigV. Annex IV has been transposed as recommendation. The CSP is obliged to inform the signatories about products which comply with the requirements for creation and verification of QES. Certification is required for products recommended by an accredited CSP whereas a supervised CSP can substitute a Manufacturer's Declaration for the certification. The signatory "should" use such products, "or take other suitable steps to secure QES".
Provision of certification services	The legislation explicitly prohibits prior authorisation of CSPs. Notification is mandatory for CSPs issuing QCs, the responsible body is RegTP (Regulatory Authority for Telecommunications and Posts). The cost of notification is based on hours worked. CSPs issuing QCs and established in Germany are subject to supervision, this process is carried out at the initial notification review. In terms of data protection laws all CSPs are subject to supervision. Compliance criteria have been specified. The legislation specifies voluntary accreditation; a scheme has already been implemented. Detailed evaluation rules and accreditation criteria have been established in both law and ordinance. The German system implicitly does encourage accreditation for few applications in the public sector and only for public entities but not for citizens.
Number of CSPs	23 CSPs issue QCs, they are all accredited.
Use of e-signatures in the public sector	The legislation defines specific requirements for the use of electronic signatures in the public sector. On-going projects include several e-government (e-identity, e-VAT and e-social security) projects.
Conformity assessment of SSCDs	There is a mandatory assessment of SSCDs, several designated assessment bodies have been appointed. SSCD products have already been assessed.

SSCDs	
Use of standards (Article 3.5)	The functional requirements for signature components are stipulated without the adoption of specific standards. Standards referenced in OJ are also considered as filling the requirements of the Act, except for products used under voluntary accreditation. No other standards are mandated or recommended. Algorithms and parameters have been published by RegTP after a proposal by BSI and are reviewed yearly together with industry.
Promotion of interoperability	Over the years, several bodies have been established to promote interoperability (TeleTrust, ISIS-MTT, Alliance for Electronic Signatures). ISIS-MTT has published detailed profiles for interoperability, based on international standards. A root-CA has been set up by RegTP for accredited CSPs.
Market for electronic signature products and services	About 25,000 Qualified Certificates, all based on SSCDs, have been issued by accredited CSPs. Many applications are in use based on Qualified Electronic Signatures, mainly in e-government in cities and states for civil servants and professionals. Problems have been reported with insecure viewer. An estimated 300,000 other certificates have been issued mainly for internal PKIs.
Web links	http://www.regtp.de/ http://www.isis-mtt.de/ http://www.mediakomm.net/ http://www.telesec.de/ http://www.signtrust.de/ http://www.datevstadt.de/ http://www.authentidate.de/ http://www.tctrustcenter.de/ http://www.d-trust.de/

Greece

Transposition of the Directive	Presidential decree n°. 150/2001 on the "Implementation of the electronic signatures Directive" (ES-Act) entered in force on 25 June 2001. Regulation n°. 248/71 of the National Telecommunications and Post Commission (EETT) entered in force on 16 June 2002. The Act transposes the Directive. The Regulation regulates in detail the provision of certification services.
Definitions (art. 2)	Same definitions of terms as in the Directive. Only difference: Law assimilates the AES with the digital signature.
Types of signatures	3 types: "Basic" as in the Directive and advanced or digital e-signature (responding to the same requirements as in the Directive). Also, implicit recognition of a higher level of signature, the "qualified" one (not named expressly as such in the Act).
Legal equivalence to handwritten signatures (art. 5.1)	Explicit transposition. Advanced e-signatures based on a QC and created by an SSCD are equivalent to handwritten signatures in both the substantial law and law of procedure.
Legal effect of e-signature (art. 5.2)	Explicit transposition. Any electronic signature can have legal effects. Use of e-signatures is however excluded in relation to certain legal acts (e.g., establishment of a handwritten will, acts on real estate involving notary's intervention, other acts requiring notary's form etc.).
Relevant case law	An e-mail message stating/confirming the recognition of a debt can be regarded as equivalent to a handwritten signature.
Liability (art. 6)	Explicit transposition. Clause applies only to CSPs issuing QC being accredited or not. Same list of causes as in the Directive. Same provision on omission to register revocation of certificates. Reversed burden of proof recognised (CSPs is presumed liable unless it proves that it was not at fault: the notion of fault includes all cases of negligence that could be avoided by the average professional).
International Aspects (art. 7)	Explicit transposition. Identical content as of art. 7. (N.B.: omission to mention expressly that conditions are laid down as alternative conditions).
Data Protection (art. 8)	Explicit transposition (same wording as in the Directive). Regulation provides in addition some special rules (namely: i) obligation of CSPs issuing QC to mention in their annual reports to EETT measures taken to protect archives and stored data, ii) obligation of CSPs issuing QC to describe data protection policies and procedures in the Certificate Practice Statement, iii) obligation to provide access to stored data if data subject requires so, iv) explicit penalties for breaches of the secrecy and confidentiality duty).

Implementation of the Annexes	All Annexes are literally copied. For Annex II, a 30-year period for retention of records is specified in addition.
Provision of certification services	The legislation explicitly prohibits prior authorisation of CSPs. Notification is mandatory for all CSPs, the responsible body is EETT (National Telecommunications and Post Commission). The cost of notification is in the range of €100 to €300. All CSPs established in Greece are subject to supervision, this process is not carried out through audit controls. There are no compliance criteria; compliance controls merely regulate a CSP's alignment with the e-sign act. The legislation specifies voluntary accreditation; a scheme has not been implemented yet. Evaluation rules and accreditation criteria are currently being prepared. The Greek system does not encourage accreditation.
Number of CSPs	5 supervised, 2 notified for issuing Qualified Certificates
Use of e-signatures in the public sector	The legislation defines specific requirements for the use of electronic signatures in the public sector.
Conformity assessment of SSCDs	There is a mandatory assessment of SSCDs, the designated assessment body of which has not been designated yet.
Use of standards (Article 3.5)	Presumption of conformity to requirements for standards referenced in OJ. In the absence of such standards, relevant national standards or standards developed by European Standards Organizations are also valid.
Promotion of interoperability	The eBusiness forum has established a working group on electronic signatures.
Market for electronic signature products and services	ASYK has issued about 1,000 QCs for transmission of company information to Athens stock-exchange, based on smart cards, giving Qualified Electronic Signatures. There is also corporate and private e-banking based on NQC.
Web links	http://www.eett.gr/gr_pages/index2.htm http://www.ebea.gr/ecomm/legal/index.htm http://www.ebusinessforum.gr/ http://www.ypan.gr/ http://www.yme.gov.gr/ http://www.dpa.gr/ http://www.taxisnet.gr/ http://www.e-oikonomia.gr/ http://www.syzefxis.gov.gr/

	http://www.ase.gr/ http://www.ebusinessforum.gr/index.php?op=modload&modname=Downloads&pageid=583 http://www.asyk.gr/repository/

Ireland

Transposition of the Directive	Electronic Commerce Act 2000 entered into force on 19 September 2000. Act structured in four Parts: - Part 1: Preliminary and General matters, - Part 2: Non-discrimination and Legal Recognition of e-signatures, - Part 3: Certification Services, Part 4: Domain Name Registration). - Schedule of the Act contains the first three Annexes of Directive.
Definitions (art. 2)	Although not taken verbatim from the Directive, definitions of e-signature, signatory, CSP and AES appear to follow the meaning of the Directive.
Types of signatures	"Basic" as in the Directive and advanced e-signature (responding to the same requirements as in the Directive). No other "higher level" of signature recognised expressly or implicitly.
Legal equivalence to handwritten signatures (art. 5.1)	All electronic signatures may be functional equivalents of handwritten signatures. Where the use of a signature is required, an e-signature may be used provided that: i) the recipient consents to the use of the e-signature, ii) if recipient is a public body, any information technology or procedural requirements imposed by that body are respected. Additional requirements for: i) a signature to be witnessed electronically (among the four conditions laid down in law: the signature to be witnessed shall be an AES based on a QC); ii) the sealing of documents electronically (among the four conditions laid down in law: document must include an AES based on a QC of the person/public body by whom the document is required to be sealed).
Legal effect of e-signature (art. 5.2)	Implementation by various provisions but also more expressly as such: "Any information cannot be denied legal effect, validity or enforceability solely on the grounds that it is in electronic form". E-signatures cannot be used for: wills, trusts and powers of attorney, interests in real property, affidavits and declarations, rules/practices/ procedures of a court or tribunal, unless otherwise provided by special regulation.
Relevant case law	No ruling yet addressing the use/legal effect of e-signatures.
Liability (art. 6)	Explicit transposition. Clause applies only to CSPs issuing QC to the public for any damage caused to a person who or public body which reasonably relies on certificate. Same list of causes as in the Directive, with one difference: While the Directive refers to "signature creation data" and "signature verification data", the Act uses the terms "signature creation device" and "signature verification device". Same provision on omission to register revocation of certificates. Reversed burden of proof recognised. Same limitations as in the Directive

	(certificate usage/value of transactions).
International Aspects (art. 7)	The Act is silent on the issue of territoriality. It would appear that QC issued by all CSPs which meet the legal requirements of Directive's Annexes I and II have equal validity.
Data Protection (art. 8)	No explicit data protection rules. No reference to pseudonyms.
Implementation of the Annexes	Annexes I, II and III are literally copied. Annex IV is not transposed.
Provision of certification services	The legislation explicitly prohibits prior authorisation of CSPs. Notification of CSPs is not mandatory; however, CSPs tend to consult with the 'relevant bodies' anyway. There is enabling legislation to establish a supervision scheme for CSPs issuing QC to the public. A supervisory system has not been put in place yet ("there is nothing there to supervise because the market is so underdeveloped"). There is enabling legislation establishing voluntary accreditation in Ireland; the legislation has been drafted but is not yet enacted. A scheme thus has not been implemented yet. Evaluation rules and accreditation criteria have not been established yet, however, the draft regulation contains a scheme based on EN45012 and EA-7/03. The Irish system does not encourage accreditation. The legislation specifies voluntary accreditation; a scheme has not been implemented yet. Evaluation rules and accreditation criteria thus have not been established yet. The Irish system does not encourage accreditation.
Number of CSPs	No CSPs issue QCs yet; however, 1 CSP has been accredited by NAB (National Accreditation Board).
Use of e-signatures in the public sector	The legislation defines specific requirements for the use of electronic signatures in the public sector.
Conformity assessment of SSCDs	There is enabling legislation to designate persons or bodies to determine conformity of SSCD with Annex III. NO such designation has been made to date.
Use of standards (Article 3.5)	No presumption of conformity to requirements for standards referenced in OJ. No other standards are mandated or recommended. No algorithms are specified.
Promotion of interoperability	Department of Communications has stated that the Government is not interested in pursuing the issue of interoperability at a national level. Instead, it is felt that this matter should be dealt with at European level.
Market for electronic	A few hundred QCs have been issued by the one accredited CSP. Several thousand NQCs have been issued by Revenue On-line Service for electronic tax submission, with equivalence of handwritten signatures.

signature products and services	tax submission, with equivalence of handwritten signatures. E-banking is the dominating application, using NQC under contract.
Web links	http://www.ucc.ie/ucc/depts/law/irlii/statutes/2000_27.htm http://www.ucc.ie/law/irlii/statutes/1999_2.htm http://www.bailii.org/ie/legis/num_act/cea1992151/s1.html http://www.bailii.org/ie/legis/num_act/ca1990107/s1.html http://www.marine.gov.ie/ http://www.entemp.ie/ecd/ebusinfo.htm http://www.nab.ie/ http://www.marine.gov.ie/display.asp/pg=455 http://www.entemp.ie/ecd/ebusdel.htm http://www.isc.ie/index.html http://www.privacy.gov.au/publications/pki.doc

Italy

Transposition of the Directive	i) Legislative decree n° 10 of 23 January 2002 transposed the Directive. A number of acts were in force before the enactment of Directive. Certain of these laws remain still applicable: ii) Law n° 59 of 1997: general principle of validity of e-docs, iii) Presidential Decree n° 445 of 2000: Digital signatures & CSPs, iv) Decree of the President and Council of Ministers of 1999 providing technical rules, v) Presidential Decree of January 2003: co-ordination of rules on digital signatures and electronic signatures (law published on 17 June 2003).
Definitions (art. 2)	Signatory: Natural person to whom the e-signature is attributed and who has access to the device for a creation of the e-signature. According to general principles, signatory cannot be a legal person. No other fundamental differences.
Types of signatures	4 types: "Basic" as in the Directive, digital and advanced e-signature (responding to the same requirements as in the Directive). Implicit recognition of a higher level of signature (being the "qualified" one: AES based on a QC and created by an SSCD).
Legal equivalence to handwritten signatures (art. 5.1)	Electronic document with digital signature or AES based on a QC and created through an SSCD has full effect as evidence.
Legal effect of e-signature (art. 5.2)	Almost literal transposition. An electronic document signed with an electronic signature is not denied legal effectiveness and admissibility as evidence for the same reasons as stated in art. 5.2 of Directive. Also: "electronic document with electronic signature satisfies the legal requirement of writing". Not any e-signature but only digital one can be used in presenting instances and declarations to public administration. Electronic or digital signatures do not provide the legal equivalent of the "atto pubblico" (deed).
Relevant case law	Supreme Court: Electronic document without a signature can be admitted as evidence of representation of facts (rebuttable presumption).
Liability (art. 6)	Explicit transposition. Liability for CSPs issuing QC for damages caused to any party reasonably relying on QC. Same liability causes as in the Directive. Reverse burden of proof. Same liability limits as in the Directive (uses of QC and value of transactions).
International Aspects (art. 7)	Literal transposition.
Data Protection (art. 8)	No explicit provision in the decree 10/02 transposing the Directive. Presidential Decree 445/00: i) reference to the Personal Data Protection Act, ii) Obligation of CSPs to respect the security measures provided by the

	Personal Data Protection Act. Use of pseudonyms is recognised. CSPs obligated to maintain registries with real names for at least 10 years after expiration of certificate.
Implementation of the Annexes	Instead of copying the Annex I, the Italian regulation explicitly refers to the Annex of the Directive. For SSCDs, ITSEC E3 High or CC EAL 4 evaluation is required.
Provision of certification services	The legislation explicitly prohibits prior authorisation of CSPs. Notification is mandatory for CSPs issuing QCs, the responsible body is the department for innovation and technology. There is no cost for notification. All CSPs established in Italy are subject to supervision, the supervisory process has not been implemented, though. Compliance criteria have not been established. The legislation specifies voluntary accreditation; a scheme has not been implemented yet. CSPs have to simply submit a request for evaluation, accreditation criteria have not been established as of yet. The Italian system does not encourage accreditation; however, QCs issued by accredited CSPs are required for some applications in the public sector.
Number of CSPs	14 CSPs issue QCs, all of which have been accredited.
Use of e-signatures in the public sector	The legislation defines specific requirements for the use of electronic signatures in the public sector. On-going projects include public administration projects.
Conformity assessment of SSCDs	The legislation specifies a mandatory assessment of SSCD, a commercial scheme, however, assessing products has not been established yet, thus the designated assessment body has not yet been appointed (currently there is a “national” scheme for military purposes only). SSCD products have been assessed (only in other Member States?).
Use of standards (Article 3.5)	No presumption of conformity to requirements for standards referenced in OJ. However, it is expected that those standards will be adopted specifically after publication. Algorithms and parameters are specified by AIPA in Technical Rules.
Promotion of interoperability	UNINFO STT commission on Security in Electronic Transactions, established within Uninfo (Standards for the Information Technology) is working for acknowledging EESSI standards as Italian Standards. The members of the commission are representatives of the market (C.A., software houses), of the Public Administration (AIPA) and experts in the field of electronic signatures.
Market for electronic signature products and services	About 1 million QCs have been issued by accredited CSPs. About 2 million QCs have been issued by supervised CSPs. The main applications are services for public administrations using Qualified Electronic Signatures and access to company register information at the Chamber of Commerce (InfoCamera).

	Nine smart card providers will adopt a new unique standard ensuring interoperability of the cards distributed across the whole Italian territory. This protocol applies to the two types of smart cards issued by public authorities in Italy: the Electronic Identity Card (Carta d'Identità Elettronica, CIE) and the National Services Card (Carta Nazionale dei Servizi, CNS).The Italian CIE and CNS will be used for accessing a number of electronic services, such as health, tax or even voting.
Web links	http://www.innovazione.gov.it/ita/intervento/normativa/normativa_firmadigitale.shtml http://www.aipa.it/

Luxembourg

Transposition of the Directive	i) Law of 14 August 2000 on electronic commerce entered into force on 12 September 2000, herein EC-Act, ii) Law of 22 March 2000 relating to the creation of a National Accreditation Register, a National Council for Accreditation and a standardization body. iii) Regulation of 1 June 2001 relating to electronic signatures, electronic payment and implementation of the e-commerce Directive. iv) Regulation of 28 December 2001 on the creation, inter alia, of the *Office Luxembourgeois d'Accreditation et de Surveillance (OLAS)*.
Definitions (art. 2)	Electronic signature: a string of data linked in an indivisible way to a document guaranteeing data integrity, identifies the signatory and expresses signatory's commitment to the content of the act. Signatory and CSP: same definitions as in the Directive. EC-Act gives additional definitions of Accreditation ("Voluntary accreditation defined as in the Directive) and Accreditation System.
Types of signatures	Basic – "Electronic Signature of a CSP delivering Qualified Certificates (being AES). Implicit recognition of a "qualified" level of signatures: signature based on a QC and created by an SSCD that the signatory can maintain under its sole control.
Legal equivalence to handwritten signatures (art. 5.1)	No explicit transposition. However, Civil Code was modified to state that an "acte sous seing privé" may be a handwritten or electronic signature. Also, the electronic "acte sous seing privé" equals to the original act, as long as one can adduce reliable guarantees that content integrity has been maintained as from the first day of its creation on a stable form (CC 1322-2).
Legal effect of e-signature (art. 5.2)	Literal transposition. EC-Act does not apply to taxation and cartels cases or to the cases of representation and defence of a client before the courts.
Relevant case law	No ruling yet addressing the use/legal effect of e-signatures.
Liability (art. 6)	Almost literal transposition. Covered CSPs issuing or guaranteeing QC to the public. Same list of liability causes. Omission to register revocation of certificates stands as a liability ground not only of CSPs not only issuing, but also guaranteeing QC. Reversed burden of proof. Same liability limits as in the Directive (limits of certificate's use and value of transactions).
International Aspects (art. 7)	Same rules as in the Directive. The accreditation scheme of a CSP is evaluated before any recognition.
Data Protection (art. 8)	Almost literal transposition. All market categories (esp. CSPs and the National Accreditation and Supervision Authority) shall comply with almost same obligations as in the Directive. Also, rules of professional secrecy

	apply: infringements of these rules are sanctioned as criminal offences. Use of pseudonyms is authorized, as long as they are identified as such on the certificate.
Implementation of the Annexes	Copy of Annex I, with a limitation of 3-year validity period. Annex II is copied, with the additional requirement that CSPs shall retain records for at least 10 years. Annex III is literally copied. Annex IV is not transposed.
Provision of certification services	The legislation does not prohibit prior authorisation of CSPs. Notification is mandatory for CSPs issuing QCs, the responsible body is OLAS (National Accreditation and Supervision Authority). There is no cost of notification. All CSPs issuing QCs established in Luxembourg are subject to supervision and this process is carried out through audit controls being performed by external security auditors. Compliance criteria have been specified in a detailed set of documents (national supervision and accreditation scheme). The legislation specifies voluntary accreditation and a scheme has already been implemented. Accreditation criteria have been specified in a detailed set of documents (national supervision and accreditation scheme). The system does not encourage accreditation.
Number of CSPs	No CSPs issuing QCs yet.
Use of e-signatures in the public sector	The legislation does not provide any special requirements for the public sector. However, additional requirements are likely to be laid down in future laws. An e-government project is under preparation.
Conformity assessment of SSCDs	There is no mandatory assessment.
Use of standards (Article 3.5)	No explicit presumption of conformity to requirements for standards referenced in OJ. The Minister may publish references to suitable technical norms, except those that are already published in OJ, thus assuming that those are already suitable. Planned for extensive use of EESSI standards in supervision and accreditation.
Promotion of interoperability	No specific promotional activities.
Market for electronic signature products and services	Mainly e-banking
Web links	http://www.etat.lu/OLAS/

	http://www.eluxembourg.lu/

Netherlands

Transposition of the Directive	i) Act on Electronic Signatures of 8 May 2003 entered in force on 21 May 2003. Act adapts Civil Code, Telecommunications Act and Economic Offences Act. ii) Decree and Regulation on e-signatures entered in force on 21 May 2003. iii) Policy rule on designation of certification bodies (still draft).
Definitions (art. 2)	Definitions virtually the same as in the Directive. Signatories can also be legal entities. Signatory is the person using (not holding) signature creation device. Lack of the word "entity" in the definition of CSP.
Types of signatures	"Basic" e-signature
Legal equivalence to handwritten signatures (art. 5.1)	An electronic signature has the same legal consequences as a hand-written signature if the authentication method used is sufficiently reliable. A method is presumed to be sufficiently reliable if the e-signature meets the following conditions: requirements of AES + QC + SSCD.
Legal effect of e-signature (art. 5.2)	Explicit transposition. A method cannot be deemed insufficiently reliable on the sole grounds that: i) certificate is not QC, ii) certificate not issued by an accredited CSP, iii) signature not created by an SSCD. First condition of 5.2 not relevant, since evidence under Dutch law is form-free. There may be cases in administrative law in which e-signatures cannot be used. Property law may be another exception.
Relevant case law	Legal value of an e-mail message was considered to be null, given the openness (manipulability) of the e-mail system.
Liability (art. 6)	Literal transposition of provision in the Civil Code. Liability for CSPs issuing QC and applies vis-à-vis parties reasonably relying on a certificate. The liability clauses are the same as in the Directive. Reverse burden of proof. Limits of liability are the same as in the Directive (uses of certificate and value of transactions).
International Aspects (art. 7)	Explicit transposition. Conditions of certificate equivalence are the same as in the Directive, with reference to EEA countries where art. 7 refers to "EU Member State".
Data Protection (art. 8)	Dutch Data Protection Act applies. Art. 8 §2 of Directive is implemented through a specific Article in Telecommunications Act (literal transposition of art. 8.2). Exception laid down in law: disclosure of personal data is permitted if necessary for fraud detection or if the processing is otherwise required by or through law.
Implementation of the Annexes	Same requirements as Annex I and III, more extensive requirements than Annex II. Annex IV has not been transposed.

the Annexes	
Provision of certification services	The legislation does not prohibit prior authorisation of CSPs. Notification is mandatory for CSPs issuing QCs to the public and established in the Netherlands, the responsible body is OPTA (Independent Post and Telecommunications Authority). The cost of notification is unknown. All CSPs issuing QCs to the public and established in the Netherlands are subject to supervision, this process is not carried out through audit controls. The legislation specifies voluntary accreditation, a self-regulated scheme (TTP.NL) has already been implemented. The ministry will designate accreditation bodies. Evaluation rules and accreditation criteria have been established within the TTP.NL scheme. The Dutch system implicitly does encourage accreditation through simplified registration procedures.
Number of CSPs	1 CSP issues QCs which has been accredited
Use of e-signatures in the public sector	The legislation does not provide any special requirements for the public sector. However, additional requirements are likely to be laid down in future laws. A government PKI (PKI-Overheid) is being set up.
Conformity assessment of SSCDs	There is a mandatory assessment of SSCDs, a designated assessment body has not been assigned though.
Use of standards (Article 3.5)	No presumption of conformity to requirements for standards referenced in OJ. Instead, there is presumption of conformity for specific standards, mainly TS 101 456 (QCP), TS 101 862 (QC) and CWA 14169 (SSCD). A guidance for the use of TS 101 456 has been published. No algorithms have been specified.
Promotion of interoperability	No specific promotion, except through the cooperation established through TTP.NL.
Market for electronic signature products and services	Only a few dozen QCs have been issued so far. Numerous NQCs have been issued to specific user groups, e.g. hospitals. A root certificate for the government (PKI-Overheid) has been generated, with QCs and Qualified Electronic Signatures planned for e-government applications.
Web links	http://www.overheid.nl/op/ http://www.ecp.nl/ http://www.ecp.nl/dossieritem.php?dossier_id=7 http://rechten.uvt.nl/simone/ds-lawsu.htm http://www.opta.nl/ http://www.ecp.nl/publicatieitem.php?id=17

	http://www.ecp.nl/publications/TTP-NL_Scheme_version_5_final.pdf http://www.pkioverheid.nl/contents/pages/00000239/cps_pa_pkioverheid_v1_0.pdf http://www.pkioverheid.nl/contents/pages/00000110/Toegestane_algoritmes_binnen_de_PKI_voor_de_overheid_v1_0.pdf http://www.pkioverheid.nl/asp/get.asp?xdl=../views/pki/xdl/Page&VarIdt=00000001&SitIdt=00000002&ItmIdt=00000369 http://www.ecp.nl/deelnemers.php https://service.diginotar.nl/cert_zoeken.html https://service.diginotar.nl/cert_verifieren.html http://rechten.kub.nl/simone/Ds-art.htm

Portugal

Transposition of the Directive	Decree-law 290-D on Digital Signatures, entered into force on 3 August 1999 (existing before the Directive's publication). Decree-law n° 62/2003 being the basic law implementing the Directive, that entered into force on 4 April 2003. There is also a draft Regulation on technical issues relating to e-signatures (enactment expected in the end of 2003).
Definitions (art. 2)	E-signature: "Result of electronic data processing likely to be subject to an exclusive and individual right used to make known the author of an electronic document" (literal translation). Signatory: similar as Directive; can also be a legal person. However, stricter corporate rules may limit the applicability of this provision. CSP: similar to Directive's definition. In addition, definitions of: Qualified e-signatures / Certification body / chronological validation / e-mail address.
Types of signatures	3 types: "Basic" / AES (same requirements as Directive. Digital signature is expressly named as one type of AES) / Qualified e-signature: a digital or other type of AES based on a QC and created by an SSCD.
Legal equivalence to handwritten signatures (art. 5.1)	Explicit transposition. Qualified e-signature on an e-document is equivalent to handwritten signature on a printed document. Specific presumptions are laid down in law: i) Person who placed the e-signature is presumed to be the holder thereof, ii) e-signature was placed with the intention of signing, iii) e-document has not been altered.
Legal effect of e-signature (art. 5.2)	No explicit transposition. There is however a provision that: "the evidential value of e-documents that do not bear a qualified e-signature certified by an accredited CSP shall be assessed under the general terms of law". Consequently, judge will decide on the specific legal value of an e-signature on an ad-hoc basis.
Relevant case law	No ruling yet addressing the admissibility/legal effect of e-signature.
Liability (art. 6)	Transposition in broader terms than art. 6. All CSPs (issuing QC or not) are subject to general liability for injury or loss caused to certificate holders and third parties resulting from infringements of the e-signatures legislation. Liability clause wider than art. 6. Reverse burden of proof applies. No possibility to waive or limit liability resulting from clause (art. 6 §3 of Directive has not been transposed).
International Aspects (art. 7)	Mere copying of Directive.
Data Protection (art. 8)	Direct transposition. Provision binds CSPs and accreditation body. General data protection clause referring to general Data Protection Act and a specific clause reiterating some data protection obligations. Use of pseudonyms is

	authorised under condition that the latter are clearly identified on certificates.
Implementation of the Annexes	Annexes I, II and III are copied or very similar to the Directive. Annex IV is not transposed.
Provision of certification services	The legislation explicitly prohibits prior authorisation of CSPs. Notification is mandatory for CSPs issuing QCs through a 'registration procedure", the responsible body is ITIJ (accreditation authority). The cost of notification is not yet known. All CSPs established in Portugal are subject to supervision, this process is carried out through regular audit controls. The legislation specifies voluntary accreditation; a scheme has not been implemented yet. Detailed evaluation rules and accreditation criteria have been established in law. The Portuguese system does not encourage accreditation
Number of CSPs	No CSPs issuing QCs yet.
Use of e-signatures in the public sector	The legislation defines specific requirements for the use of electronic signatures in the public sector. On-going projects include e-identity projects.
Conformity assessment of SSCDs	There is a mandatory assessment of SSCDs, the designated assessment body of which has not been appointed yet.
Use of standards (Article 3.5)	Presumption of conformity to requirements for standards referenced in OJ.
Promotion of interoperability	MULTICERT has studied different standards and has adopted the ones that were being used by most of the players in this market, for example Electronic Signature formats TS 101 733 v 1.4.0 and XML Advanced Electronic Signatures (XAdES) - TS 101 903.
Market for electronic signature products and services	Certificates from MULTICERT are mainly used for secure e-mail and e-banking. Companies in Portugal with annual sales figures of over 500,000 euros will be required to file their VAT declarations online to the State from September.
Web links	http://www.citiap.gov.pt/documentos/290.pdf http://www.oa.pt/direitonarede/detalhe.asp?idc=11741&scid=11762&idr=11895#a1 http://www.itij.mj.pt/ http://www.oa.pt/direitonarede/detalhe.asp?idc=11741&scid=11762&idr=11761&ida=12748

Spain

Transposition of the Directive	i) Draft Bill on electronic signatures (being still under discussion at the time of publication of the present report), ii) Royal Decree-Law on electronic signatures 14/1999 of 17 September 1999, iii) Order on the accreditation of CSPs and certain electronic signature products of 21 February 2000.
Definitions (art. 2)	Electronic Signature: as Directive. Signatory: any person who holds a signature creation device and who acts on his own name or in the name of the legal entity, which it represents. Thus, signatory can also be a legal person. CSP: as Directive.
Types of signatures	"Basic" – AES and QES (explicitly named as such).
Legal equivalence to handwritten signatures (art. 5.1)	Explicit transposition. QES are equivalent to handwritten signatures. Same presumption as in art. 5.1.
Legal effect of e-signature (art. 5.2)	No explicit transposition. Under Spanish law, this rule is obvious since any document (electronic or not, signed electronically or not) is admissible as evidence in legal proceedings. Admissibility and legal validity of any electronic signature will be decided on an ad-hoc basis by the judge. Some types of contracts (under family or succession law) are excluded from the principle of freedom of form and require a handwritten signature.
Relevant case law	Yes, there have been a number of cases. The first court of instance of Madrid denied recognising the existence and legal validity of a private contract on the grounds that it did not bear an electronic signature.
Liability (art. 6)	The draft bill implements explicitly art. 6. All categories of CSPs issuing or guaranteeing e-signatures certificates (including other than QCs) are covered. Liability grounds are formulated in a broader way than in art. 6: CSP is liable for violation of obligations stated in different Articles of the Bill, among which figure the liability cases of art. 6.1. Reversed burden of proof. Limitation or exoneration of liability for specific faults or omissions of the certificate holder or certificate recipient (namely, communication of wrong information as to the holder's identity or qualities, failure to notify need of certificate's revocation, use of certificate after expiration of the indicated date of use, etc.). No respect of the limits of certificate's use or value of transactions is also included.
International Aspects (art. 7)	Explicit transposition. Recognition of foreign certificates under the same conditions as in the Directive.
Data Protection (art. 8)	Explicit implementation of this provision: reference to the Spanish general data protection Act and confirmation of some special rules as in the Directive.

(art. 8)	Use of pseudonyms in certificates is authorized. CSPs are obliged to provide the real names to public authorities pursuant to a court order.
Implementation of the Annexes	For Annex I, there is an additional requirement for the inclusion of the national identity number in the certificate. For Annex II there are some additional specific requirements on the CSP for the insurance amount, archiving period (15 years) and information to the signer. Annex III is literally copied. The implementation of Annex IV in Article 25 contains requirement on products for signature verification, but there is no mandatory requirement to use such products.
Provision of certification services	The legislation explicitly prohibits prior authorisation of CSPs. Notification is mandatory for all CSPs, the responsible body is the Ministry of Science and Technology. There seems to be no cost of notification. All CSPs established in Spain are subject to supervision, this process is not being carried out through audit controls. Compliance criteria have been specified within the e-signature bill. The legislation specifies voluntary accreditation; a scheme has not been implemented yet. Evaluation rules and accreditation criteria have not been specified yet. The Spanish system does not encourage accreditation.
Number of CSPs	No CSPs issuing QCs yet.
Use of e-signatures in the public sector	The legislation defines specific requirements for the use of electronic signatures in the public sector. On-going projects include e-identity and taxation projects.
Conformity assessment of SSCDs	There is no mandatory assessment. The signature bill mentions a voluntary scheme aiming at compliance of signature creation devices with requirements set forth by the bill. No corresponding bodies have been designated as yet.
Use of standards (Article 3.5)	Presumption of conformity to requirements for standards referenced in OJ. If EU standards do not exist, widely used international standards or national standards will be recognized. A list of permitted algorithms has been published by the Ministry of Finance.
Promotion of interoperability	No specific promotional activities or standards, although the planned electronic identity card will establish a de-facto standard.
Market for electronic signature products and services	Ca 1.5 million certificates have been issued to the public for electronic tax declarations. A number of banks are providing e-banking based on certificates.

Web links	http://www.congreso.es/ http://www.setsi.mcyt.es/ http://www.mineco.es/oficvirtual/OfiVirtual_marcos.htm http://www.mcyt.es/ http://www.enac.es/html/enac.html https://www.feste.com/ http://www.ace.es/ http://www.mju.es/guia_f_elect.htm http://delitosinformaticos.com/firmaelectronica http://www.cert.fnmt.es/clase2/

Sweden

Transposition of the Directive	Act on "Qualified Electronic Signatures" (2000:832), basic law transposing the Directive. Entry in force on 1 January 2001. Act applicable to CSPs established in Sweden who issue QC to the public. A number of Government Ordinances on Qualified e-signatures: i) Financing of the operations of National Post and Telecom Agency. ii) One regulation on determination of fees according to the Act on Qualified e-signatures, iii) the Technical Conformity Assessment Act providing a voluntary accreditation scheme.
Definitions (art. 2)	E-signature: has to ensure both data origin authentication and data integrity. Signatory: natural person authorised to control a signature creation device (legal persons cannot be signatories). Narrow definition of CSP: services restricted to issuance of certificates or guaranteeing certificates of others.
Types of signatures	3 types: "Basic" – AES and Qualified e-signature (expressly stated as such): AES based on a QC and created by an SSCD.
Legal equivalence to handwritten signatures (art. 5.1)	Qualified e-signatures do not automatically meet the requirements of handwritten ones. The law states that: if the legal requirement for a handwritten signature may be satisfied by electronic means, a Qualified e-signature is deemed to fulfil this requirement.
Legal effect of e-signature (art. 5.2)	No transposition. E-signatures were permissible as evidence and could not be denied legal effectiveness even before the enactment of the Directive.
Relevant case law	Decision of Administrative Supreme Court: an e-signature is not sufficient when administrative law requires a handwritten signature.
Liability (art. 6)	Explicit transposition. The provision addresses liability of CSPs issuing QC to the public if damages are caused to anyone relying on certificate. List of liability causes largely reflects the Directive and, in addition: obligation to ensure that date and time of issuance and revocation are determined precisely. Liability cannot be waived. Reverse burden of proof. Same limitations as in the Directive (uses of certificates and value of transactions).
International Aspects (art. 7)	Explicit transposition. Equivalence of QC issued by a CSP established outside Sweden with QC issued in Sweden if: i) CSP is established in another EEA country and is authorised to issue QC in that country, (or) ii) CSP satisfies the legal requirements of Swedish law and is accredited in another EEA state, (or) iii) CSP compliant with Swedish legal requirement guarantees the certificates as qualified. No transposition of Directive's requirement on the existence of

	bilateral/multilateral agreement.
Data Protection (art. 8)	Transposition of paragraph 2 of art. 8 (thus, no reference to general applicability of Swedish law on data protection). Subject to this provision are CSPs (as defined in the Act). Pseudonyms on certificates can be used provided that they are identified as such.
Implementation of the Annexes	Annexes I, II and III are copied or very similar to the Directive. Annex IV is not transposed.
Provision of certification services	The legislation does not prohibit prior authorisation of CSPs. Notification is mandatory for CSPs established in Sweden that issue QCs to the public, the responsible body is PTS (National Post and Telecom Agency). The cost of notification is approx. €10,000 but may be significantly reduced in the future. All CSPs issuing QCs to the public and established in Sweden are subject to supervision, this process may be carried out through audit controls. No compliance criteria have been specified. The legislation does not mention voluntary accreditation. However, CSPs may voluntarily be evaluated/tested against certain standards by a certification body, accredited by SWEDAC (national accreditation body).
Number of CSPs	No CSPs issuing QCs yet.
Use of e-signatures in the public sector	The legislation does not provide any special requirements for the public sector.
Conformity assessment of SSCDs	There is a mandatory assessment of SSCDs, a designated assessment body of which has not been appointed yet.
Use of standards (Article 3.5)	Presumption of conformity to requirements for standards referenced in OJ. No other standards are mandated or recommended. No algorithms are specified.
Promotion of interoperability	Swedish standards for certificate profile have been established. A testing tool for interoperability has been developed by SWEDAC.
Market for electronic signature products and services	About 100,000 NQCs have been issued by banks, Sweden Post and Telia. They are used for e-government, including electronic tax declaration, based on 5.2 signatures. About 1 million NQCs have been issued for e-banking. 30% are estimated to be based on smart cards.
Web links	http://www.pts.se/Archive/Documents/SE/engelsk%20oversattning%20av%20lag%20elektroniska%20signaturer.pdf http://www.pts.se/Archive/Documents/SE/

	PTS%20foreskrifter%20om%20avgifter%20enligt%20lagen%20om%20kvalificerade%20elektroniska%20signaturer.pdf http://www.pts.se/Archive/Documents/SE/Anmalan_kval_certifikat.pdf http://www.riksdagen.se/ http://www.lagrummet.gov.se/ http://www.pts.se/ http://www.regeringen.se/ http://www.naring.regeringen.se/ http://www.swedac.se/ http://www.statskontoret.se/ http://www.rsv.se/

United Kingdom

Transposition of the Directive	i) Electronic Signatures Regulations 2002 entered into force on 8 March 2002 (implementing certain provisions of Directive notably in relation to CSPs, incl. liability and data protection. ii) Electronic Communications Act 2000 entered into force on […] addresses the admissibility aspects of e-signatures.
Definitions (art. 2)	Definitions of e-signature / signatory and CSP are identical to the Directive's ones. Legal persons can be signatories. No definition of the term SSCD.
Types of signatures	Two types: "Basic" and AES (same definition as in the Directive).
Legal equivalence to handwritten signatures (art. 5.1)	No transposition. English law does not distinguish the concept of "handwritten" signature. Therefore, no requirement to recognise an "e-signature" as an alternative. Various legislative acts have generally recognised that an e-signature is a valid form of signature in the specific context concerned.
Legal effect of e-signature (art. 5.2)	Partial transposition: Electronic Communications Act addresses the admissibility but not the legal effectiveness. The latter is generally addressed through specific Orders. E-signatures are generally valid in the absence of specific legislation. They are admissible as evidence, although their probative value is to be decided by court on an ad-hoc basis. Use of e-signatures may be prohibited in a particular legal context.
Relevant case law	Decision in obiter dictum: An e-signature in the form of a computer-generated facsimile would have satisfied the requirements of the Insolvency Act in terms of signing a proxy voting form.
Liability (art. 6)	Explicit transposition. Clause addresses liability of CSPs issuing QC to the public. All grounds of liability stipulated in the Directive are included. Reverse burden of proof. No express liability limitations as in the Directive. Therefore, standard rule on tort liability applies - damage must be sufficiently proximate.
International Aspects (art. 7)	No transposition.
Data Protection (art. 8)	E-Sign Regulations provide for data protection obligations of CSP only. Provisions provide enforceability clauses and determine the scope of their application. Further, they impose specific restrictions with no direct reference to the UK Data Protection Act. Use of pseudonyms on QC is authorized provided they are identified as such.
Implementation of the Annexes	Annex I and II are copied. Annex III and IV are not transposed.

Provision of certification services	The legislation does not prohibit prior authorisation of CSPs. There is no notification for CSPs. All CSPs issuing QCs to the public and established in the UK are subject to supervision, this process is not carried out through audit controls. No compliance criteria have been specified. Relevant general "regulations" (Part 1 of ECA 2000) have not been implemented as yet, however, CSPs that have been "approved" by tScheme are being monitored for adherence to the Code of Conduct. The legislation does not mention voluntary accreditation; however, an industry, not-for-profit, voluntary self-regulated scheme (tScheme) has already been implemented. The accreditation process is carried out by assessor organizations which in turn are accredited by UKAS (UK Accreditation Service). Other accreditation schemes would be possible. The system implicitly does encourage accreditation (in the "government gateway").
Number of CSPs	There are 3 accredited CSPs. However, neither is issuing QCs.
Use of e-signatures in the public sector	The legislation defines specific requirements for the use of electronic signatures in the public sector. A 'government gateway' has been established to provide a centralized registration service for e-government services.
Conformity assessment of SSCDs	There is no mandatory assessment. (However, "the Directive is felt to have direct effect in respect of the validity of non-UK SSCDs.")
Use of standards (Article 3.5)	No presumption of conformity to requirements for standards referenced in OJ. No other standards are mandated or recommended. No algorithms have been specified.
Promotion of interoperability	None (tScheme is only concerned with security requirements).
Market for electronic signature products and services	No information
Web links	http://www.hmso.gov.uk/si/si2002/20020318.htm http://www.legislation.hmso.gov.uk/acts/acts2000/20000007.htm http://www.dti.gov.uk/ http://www.dti.gov.uk/industries/ecommunications/ http://www.tscheme.org/ http://www.tscheme.org/process/index.html https://www.tscheme.org/directory/index.html

	http://www.tscheme.org/library/tSd0244_1-00%20Required%20Assessment%20Procedures.pdf http://www.btignite.com/uk/products/trustservices/products/idcerts.html http://www.hmso.gov.uk/legis.htm http://www.gateway.gov.uk/ http://www.equifaxsecure.co.uk/ebusinessid/ http://www.ukas.com/ https://www.tscheme.org/process/index_fees.html

Cyprus

Transposition of the Directive	No law on electronic signatures yet. The preparation of a study looking into the preparation of a Bill on e-commerce and electronic signatures is now underway. No formal decision on the necessity to draft such a Bill will be taken before the end of this year (2003).
Definitions (art. 2)	-
Types of signatures	-
Legal equivalence to handwritten signatures (art. 5.1)	-
Legal effect of e-signature (art. 5.2)	-
Relevant case law	No ruling yet on the use/legal effect of an e-signature.
Liability (art. 6)	No transposition. General contractual and tort law applicable. Also, the regulation on the sale of defective products.
International Aspects (art. 7)	No transposition.
Data Protection (art. 8)	No transposition. General Data Protection Law could apply.
Implementation of the Annexes	N/A
Provision of certification services	N/A
Number of CSPs	N/A
Use of e-signatures in the public sector	N/A
Conformity assessment of SSCDs	N/A
Use of standards (Article 3.5)	N/A

Promotion of interoperability	None
Market for electronic signature products and services	Some use of corporate e-banking only.
Web links	http://www.thunderworx.com/ http://www.cyprus-eu.org.cy/ http://www.planning.gov.cy/

Czech Republic

Transposition of the Directive	i) Act n° 227/2000 on "electronic signatures and on amendments to some related acts"; ii) Government Decree n°. 304/2001 implementing the Act n° 227/2000; iii) Regulation of the Office for the Protection of Personal Data n°. 366/2001 on "specification of some terms and conditions of the ES-Act and of the requirements for e-signature devices", iv) Act n° 368/92 on administrative fees, as amended, v) Government Decree n° 140/2000 on the list of free trade licences.
Definitions (art. 2)	Signatory is defined as a natural person who has the means to create an e-signature and who acts on its own behalf or on behalf of another natural or legal person. Legal persons cannot be signatories. Additional definition of accredited CSP. No definition of "e-signature product". Accreditation is meant differently than in the Directive: Accredited CSP is the provider who meets the requirements of the e-signatures law.
Types of signatures	"Basic" and "Guaranteed" e-signature (equivalent to AES). Implicit recognition of a "higher level" of signature: Guaranteed e-signature based on a Qualified Certificate and secured signature creation.
Legal equivalence to handwritten signatures (art. 5.1)	No explicit transposition. No recognition of the term "handwritten signature". Czech law merely uses the term "signature" and "official attested signature". The Act only states that: "The application of a guaranteed e-signature based on a QC and secured signature creation enables the recipient to verify whether a data statement has been signed by a person specified in the QC".
Legal effect of e-signature (art. 5.2)	No explicit transposition. Czech law does not restrict forms or means of evidence. Use of e-signatures as means of evidence unlimited. An e-signature cannot however replace the "official attested signature (signature done by a notary).
Relevant case law	No ruling yet addressing the use/legal effect of e-signatures.
Liability (art. 6)	Transposition in more generic terms than in the Directive. CSPs issuing QC are liable for violations of their obligations stipulated by the Act, to the extent of special legislation. List of liability causes more extensive than art. 6, (incl. requirements of Annex II). Reverse burden of proof. Liability limit: the specific certificate use.
International Aspects (art. 7)	Specific conditions of equivalence are stipulated. i) Foreign QC are honoured as such by a CSPs issuing QC in accordance with the Act, ii) the compliant CSP guarantees the accuracy and validity of the foreign certificates, iii) recognition by decision of the Ministry of Informatics or by

	another bilateral/international agreement.
Data Protection (art. 8)	Protection of personal data is subject to special legal provisions, being the Personal Data Protection Act. No specific data protection rules in the Act, mere reference to the Data Protection Act. Use of pseudonyms is authorised, provided that they are identified as such. CSP shall keep documentation related to their operations, incl. copies of personal data submitted by signatories.
Implementation of the Annexes	Annex I is copied from the Directive, with the addition that other personal data may only be included with the consent of the signer. Annex II and III are copied, and Annex IV is copied but as requirements instead of recommendations.
Provision of certification services	The legislation does not prohibit prior authorisation of CSPs. Notification is mandatory for CSPs issuing QCs, the responsible body is the Ministry of Informatics. There is no cost for notification. CSPs issuing QCs and established in the Czech Rep. are subject to supervision, this process is carried out through regular audit controls. Compliance criteria consist of several documents including security concepts. The legislation specifies voluntary accreditation; a scheme has already been implemented. Evaluation rules and accreditation criteria have been established through the e-signature act. The Czech system implicitly does encourage accreditation (in the public sector).
Number of CSPs	1 CSP has been accredited.
Use of e-signatures in the public sector	The legislation defines specific requirements for the use of electronic signatures in the public sector. E-identity cards are being introduced within several projects.
Conformity assessment of SSCDs	There is a mandatory assessment of SSCDs, the designated assessment body of which is the Ministry of Informatics. SSCD products have already been assessed.
Use of standards (Article 3.5)	No presumption of conformity to requirements for standards referenced in OJ, but presumption of product compliance to requirements through CC-evaluation. No other standards are mandated or recommended. Algorithms published by Ministry of Informatics.
Promotion of interoperability	None
Market for electronic signature products and services	About 10,000 QCs issued by accredited CSP for electronic custom clearance based on adapted laws and Qualified Electronic Signatures. About 400,000 NQCs have been issued for health insurance, e-government applications and stock exchange using 5.2 signatures.

services	
Web links	http://www.micr.cz/ http://www.cryptosavvy.com/ http://www.ica.cz/ http://www.caczechia.cz/ http://www.ca.cz/

Estonia

Transposition of the Directive	Digital Signatures Act of 8 March 2000 (consolidated law). Entry in force on 15 December 2000. The last law having amended this act entered in force on 01.08.2002.
Definitions (art. 2)	Recognition of digital signature only: a data unit, created using a system of technical and organisational means, which a signatory uses to indicate his/her connection to a document. No explicit definition of the signatory. The latter can be only a natural person (certificates suitable for creating digital signatures are issued exclusively to natural persons). Narrower definition of CSPs than in the Directive: agencies and persons categorised in the Act that entered in the state register of certificates as service providers and are registered in the corresponding register in Estonia.
Types of signatures	Only one type: digital signature. This signature is equivalent to the AES of the Directive with one additional requirement: determination of the time at which the signature is given.
Legal equivalence to handwritten signatures (art. 5.1)	Same legal consequences as a handwritten signature if: i) these consequences are not restricted by law, ii) it is proved that the signature in question fulfils the requirements of a digital signature (unique identification, determination of time of signing, preservation of data integrity). It is considered as a general rule in the Estonian legal system that any digital signature compliant with the Act is equivalent to the handwritten one in any private, business or administrative relation, unless a specific law stipulate *expressis verbis* otherwise.
Legal effect of e-signature (art. 5.2)	No explicit transposition. E-signatures not compliant with the Act have no explicit legal value and their use is unregulated. Any piece of information and document (signed or not) may have a legal value recognised on an ad-hoc basis. Use of electronic signatures may be restricted/forbidden in certain circumstances (as defined by special law or acts requiring intervention of notary).
Relevant case law	Tallinn Administrative District Court ruled that digitally signed documents must be considered equivalent with handwritten ones in court proceedings.
Liability (art. 6)	No transposition. A general liability clause holding CSPs liable for any patrimonial damage resulting from violation of obligations. All liability causes stipulated in the Directive may be considered falling into the general liability provision of the Act. No “reversed burden of proof” recognised. No CSP liability for certificate use or misuse; the certificate holder is in principle liable in this case.
International Aspects (art. 7)	Foreign certificates are equivalent to Estonian ones, if at least one of the following conditions is met: i) upon decision of the Chief processor of the

Aspects (art. 7)	register, foreign CSP complies with requirements of the Act, ii) guarantee of certificates by CSP acting on the basis of the Act, iii) recognition of equivalence pursuant international agreement.
Data Protection (art. 8)	No explicit transposition. Personal Data Protection Act applies (Digital signature Act merely refers to the Personal Data Protection Act). National Data Protection Authority supervises maintenance of the national registry of CSPs. Use of pseudonyms is not authorised.
Implementation of the Annexes	The term QC is not used, but the requirements for "certificates" are similar to Annex I. Requirements for CSPs are similar to Annex II. There are no specific requirements for SSCDs (Annex III) or private key protection. Annex IV has not been transposed.
Provision of certification services	The legislation does not prohibit prior authorisation of CSPs. On the contrary: registration of CSPs issuing QC in the 'national register of CSPs' is mandatory. All CSPs issuing QC established in Estonia are subject to supervision, this process is carried out through annual audit controls. Several compliance criteria have been specified. A voluntary accreditation scheme in the sense of Art. 3.2 is not in place.
Number of CSPs	1 CSP has been accredited.
Use of e-signatures in the public sector	The legislation defines specific requirements for the use of electronic signatures in the public sector. On-going projects include e-identity and 'e-citizen portal' projects.
Conformity assessment of SSCDs	There is no mandatory assessment.
Use of standards (Article 3.5)	No presumption of conformity to requirements for standards referenced in OJ. No other standards are mandated or recommended.
Promotion of interoperability	The OpenXAdES standard, based on ETSI TS 101 9039, is used as de-facto signature format standard.
Market for electronic signature products and services	More than 200,000 EID cards have been issued, containing QCs from the accredited CSP, to be used as a general tool replacing handwritten signatures in e-government and other applications. Banks have been issuing proprietary certificates to their corporate e-banking customers and merchants for authentication and automatic transaction processing purposes.
Web links	http://www.id.ee/file.php?id=122 http://www.eik.ee/english/2002/p23_t.htm http://www.legaltext.ee/text/en/X30081K3.htm

	http://www.legaltext.ee/text/en/X30085.htm http://www.legaltext.ee/text/en/X60032.htm http://www.legaltext.ee/text/en/X50058K1.htm http://www.legaltext.ee/text/en/X1032K4.htm http://www.legaltext.ee/text/en/X1060K4.htm https://www.riigiteataja.ee/ert/act.jsp?id=26553 http://www.id.ee/ http://www.legaltext.ee/ http://www.riigiteataja.ee/ http://www.riso.ee/ http://www.sk.ee/ http://www.mkm.ee/ http://www.sa.ee/ http://www.fin.ee/ http://www.just.ee/ http://www.eesti.ee/ http://www.openxades.org/ http://www.evs.ee/

Hungary

Transposition of the Directive	Act XXXV of 2001 of e-signatures. This Act is implemented by: i) Government decision 1075/2000 on "the necessary measures related to the act", ii) A number of decrees regulating: a) duties & competence of Regulatory Authority, b) designation of conformity assessment bodies, c) detailed requirements for services related to e-signatures, d) administrative fees, e) registration of experts in the field of services for e-signatures, f) security requirements for the services related to qualified e-sign.
Definitions (art. 2)	Signature: "data in electronic form or electronic record which are logically associated with and inseparably attached to other electronic record, whit the purpose of authentication" Signatory: the natural person to whom signature verification data is connected. CSPs: a person (organisation) performing activities identified in law. Law stipulates expressly the certification services to be performed by CSPs (exhaustive list). No definition for voluntary accreditation and signature verification device. A list of additional definitions is provided: verification of e-signature / use of e-signature / signing by e-means / e-records / e-document / e-deed / time stamp / qualified e-sign / qualified CSPs / service regulations.
Types of signatures	"Basic" – AES (same requirements as in the Directive) – Qualified e-signature (AES based on a QC and created by an SSCD).
Legal equivalence to handwritten signatures (art. 5.1)	No explicit transposition. The most relevant amendments of Civil Code & Act on Civil Procedures are: i) When the written form is a prerequisite for the legal validity of a contract, an electronic deed signed with AES is considered as contract made in written form. ii) Private deeds have full probative force - until otherwise proven – if the author placed his qualified e-signature on the electronic deed.
Legal effect of e-signature (art. 5.2)	No explicit transposition. However, all Hungarian codes of procedure (penal, etc.) are based on the principle of free evidence. Act stipulates that: "acceptance of e-signatures or e-documents or e-records may not be denied, including their application as evidence, and their suitability for making a legal statement or having a legal effect may not be questioned, solely on the grounds that they exist in electronic form". E-signatures may not be used to attest certain legal relationships as specified in law (e.g. marriage, family and guardianship).
Relevant case law	No ruling yet addressing the legal effect/validity of e-signatures.
Liability (art. 6)	Transposition in broader terms. General clause on liability for all CSPs to any third person for damages arising from infringements of specific

	provisions. Several liability causes are listed, incl. all liability causes of art. 6 and others (failure to provide information or to ensure continuous operation, etc.). Burden of proof on CSP. Limits of liability: geographical and usage scope of certificate, value of transactions.
International Aspects (art. 7)	Distinction between QC issued within EU – other. Automatic equivalence for EU QC. Under conditions for non-EU: i) CSPs established within EU assumes liability, ii) foreign CSP meets the Directive's requirements and accredited in an EU M-S, iii) existence of international agreement.
Data Protection (art. 8)	Law reiterates the principles of the Hungarian DP Act in a special clause. Pseudonyms on the QC shall be identified as such. Disclosure to investigative/other authorities possible.
Implementation of the Annexes	Annex I, II, III and IV are copied, with some small modifications.
Provision of certification services	The legislation does not prohibit prior authorisation of CSPs. Notification is mandatory for all CSPs, the responsible body is HIF (Communications Authority of Hungary). The cost of notification is in the range of approx. €1,000 to €6,000. All CSPs issuing QCs as well as all other CSPs issuing certificates to the public and established in Hungary are subject to supervision, this process may be carried out through audit controls. Several documents have been established as compliance criteria. The legislation does not mention voluntary accreditation; a scheme thus has not been implemented.
Number of CSPs	2 CSPs issue QCs.
Use of e-signatures in the public sector	The legislation does not provide any special requirements for the public sector. On-going project include electronic tax declaration and credit institution applications.
Conformity assessment of SSCDs	There is a mandatory assessment of SSCDs.
Use of standards (Article 3.5)	No presumption of conformity to requirements for standards referenced in OJ. No other standards are mandated or recommended.
Promotion of interoperability	None
Market for electronic signature products and services	No QCs issued so far. About 100,000 test certificates and some thousand NQCs issued by registered CSPs. One of the service providers has experienced several security related

and services	problems both in hardware and software products.
Web links	http://www.hif.hu/english/menu4/m4_8/es.pdf http://www.netlock.net/ http://index.hu/tech/jog/digitala http://sansserif.hu/ealairas/index.htm http://www.crysys.hu/ http://www.hif.hu/ http://e-alairas.lap.hu/ http://www.hif.hu:7777/pls/portal30/ESIGN_PORTAL.menu.show http://www.hif.hu:7777/pls/portal30/ESIGN_PORTAL.DYN_TERMEK_ALL.SHOW

Latvia

Transposition of the Directive	Law on Electronic Documents in force from 1 January 2003. Five (5) Regulations of the Cabinet of Ministers will be elaborated on: i) use of e-documents in public administration and e-archiving, iii) description of security of information systems, iv) facilities & procedures for delivery of certification services, v) procedures of control of security of information systems, vi) establishment of insurance premium and mode of calculation for CSPs.
Definitions (art. 2)	Same definition of e-signature (purposes: authenticity and signatory's identity). Signatory: can be only natural person; the definition speaks about a person who "*has tools for creating of electronic signature*". CSP: Provider of certification services. Certification services are enumerated in law. Signature verification device is not defined. Additional definitions: *Secure tools for creating of e-signatures*: same requirements of SSCD of Directive. Definition of e-document. Definition of time-stamp.
Types of signatures	"Basic e-signature" and "Secure e-signature": being AES created by Secure tools for creating e-signatures (SSCD) and based on a *Certified Certificate* (QC) – Same definition as QES of Directive.
Legal equivalence to handwritten signatures (art. 5.1)	Same conditions as in art. 5.1. Same presumption as Directive: "E-documents shall be deemed signed in person if it contains secure e-signature".
Legal effect of e-signature (art. 5.2)	Explicit transposition in the following wording: E-signature is a legal proof and delivery of e-document as evidence to the competent authorities shall not be limited on the basis that: i) document is in electronic format, ii) it has not secure e-signature. No use of e-signatures in contracts of: i) real estate property, ii) subject to formal procedure, iii) guarantees, iv) of family & inheritance law.
Relevant case law	No ruling yet addressing the use/legal effect of e-signatures.
Liability (art. 6)	Explicit transposition with following differences: Not covered in scope: CSPs guaranteeing QC. Liability clauses: 6.1 (a) and (b) implemented. 6.1(c) not implemented. In addition: i) general infringement of non-compliance with laws and regulations and conditions of certificates' delivery as provided in register, ii) due use of creation and control data of e-signatures.
International Aspects (art. 7)	Explicit provision. Only difference: recognition in case that a CSP accredited within the EU guarantees or issues the QC.
Data Protection (art. 8)	There is a data protection clause but it differs from art. 8. The rules stipulated in the provision are: i) direct collection of data from data subject or after its consent, ii) exclusive processing of data for certificate issuance/maintenance.

Implementation of the Annexes	Annex I and III copied. Annex II worded differently, with additional requirement to provide time-stamping services. Annex IV not implemented.
Provision of certification services	The legislation explicitly prohibits prior authorisation of CSPs. There is no notification at all for CSPs. All CSPs issuing QCs are subject to supervision, this process is carried out through audit controls. Compliance is measured against the law. The legislation specifies voluntary accreditation; a scheme has not been implemented as yet.
Number of CSPs	No CSPs issuing QCs yet.
Use of e-signatures in the public sector	The legislation does provide for special requirements within the public sector. An e-ID card project has been started.
Conformity assessment of SSCDs	There is no mandatory assessment.
Use of standards (Article 3.5)	No presumption of conformity to requirements for standards referenced in OJ. No other standards are mandated or recommended. No algorithms are specified.
Promotion of interoperability	None
Market for electronic signature products and services	There is only one serious PKI application in Latvia – Information System of the Bank of Latvia.
Web links	http://www.likumi.lv/ http://www.komersants.lv/ http://www.dvi.gov.lv/ http://www.bank.lv/

Lithuania

Transposition of the Directive	Law on Electronic Signature of 11 July 2000. Amended in 6 June 2002. Five (5) decrees and one (1) resolution regulating aspects of certification services provision.
Definitions (art. 2)	Similar definition of e-signature to the Directive's one. Signatories can only be natural persons. Signatures of legal persons recognised as equivalent to the signature of the representative of the legal person seconded by a stamp.
Types of signatures	3 types: "Basic" and Secure e-signature: same as the AES. Recognition of a higher level of signature, equivalent to the "qualified" e-signature.
Legal equivalence to handwritten signatures (art. 5.1)	As in the Directive: Secure e-signatures based on a QC and created by an SSCD is equivalent to handwritten signature. Explicit reference that signatories can agree on the legal validity of signature used.
Legal effect of e-signature (art. 5.2)	Explicit transposition: same circumstances as in the Directive. No explicit mention in the Law of cases prohibiting use of e-signatures in general.
Relevant case law	Yes. A PIN code in relation to the use of a payment card is an e-signature.
Liability (art. 6)	Provision similar to art. 6 of Directive. Same Article provides for liability of all CSPs, whilst one paragraph stipulates expressly the liability of CSPs issuing QC (= art. 6). Liability towards any party reasonably relying on certificate. One more liability cause compared to Directive: omission to revoke/suspend certificate. Liability limits as in the Directive (certificate usage/value of transactions exceeding clear limitations on the QC).
International Aspects (art. 7)	Equivalence between QC issued by foreign CSPs and QC issued in Lithuania, if: i) issued by a CSP accredited in Lithuania, or, ii) issued by a CSP accredited in EU, or, iii) CSP in Lithuania compliant with legal requirements guarantees the certificate, or, iv) CSP of an EU member-state compliant with legal requirements that correspond to Lithuanian law guarantees the certificate, or, v) recognition of CSPs or certificates on the basis of international agreement.
Data Protection (art. 8)	Only reference to Law on Legal Protection of Personal Data. Mandatory registration of CSPs acting as data controllers to the State Data Protection Inspectorate. Pseudonyms can be used.
Implementation of the Annexes	Annex I, II (subset) and III are copied. Annex IV copied as requirements.
Provision of certification services	The legislation does not prohibit prior authorisation of CSPs. Notification is mandatory for CSPs issuing QCs, the responsible body is IVPK (Information Society Development Committee). The cost of notification is unknown. CSPs issuing QCs and established in Lithuania are subject to supervision,

	this process is not carried out through audit controls. The legislation specifies voluntary accreditation; a scheme has already been implemented. The establishment of evaluation rules or accreditation criteria is unknown. The Lithuanian system does not encourage accreditation.
Number of CSPs	No CSPs issuing QCs yet.
Use of e-signatures in the public sector	The legislation does not provide any special requirements for the public sector. Future projects might include electronic tax declaration.
Conformity assessment of SSCDs	There is a mandatory assessment of SSCDs.
Use of standards (Article 3.5)	No presumption of conformity to requirements for standards referenced in OJ. Instead, several standards have been re-issued as national standards to be used (ETSI TS 101 456, CWA 14167, CWA 14171, ISO/IEC 15408 and ISO 9001:2001). No algorithms have been specified.
Promotion of interoperability	National standards
Market for electronic signature products and services	No CSPs issuing Qualified Certificates. Only very small use of PKI for e-banking.
Web links	http://www3.lrs.lt/cgi-bin/preps2?Condition1=204802&Condition2= http://www3.lrs.lt/cgi-bin/preps2?Condition1=204710&Condition2= http://www3.lrs.lt/cgi-bin/preps2?Condition1=204713&Condition2= http://www3.lrs.lt/cgi-bin/preps2?Condition1=208073&Condition2= http://www3.lrs.lt/cgi-bin/preps2?Condition1=198003&Condition2= http://www3.lrs.lt/cgi-bin/preps2?Condition1=204712&Condition2= http://www3.lrs.lt/cgi-bin/preps2?Condition1=204711&Condition2= http://www3.lrs.lt/cgi-bin/preps2?Condition1=208886&Condition2= http://www3.lrs.lt/cgi-bin/preps2?Condition1=104555&Condition2= http://www.ivpk.lt/ http://www.lrs.lt/ http://www3.lrs.lt/pls/inter/w3_viewer.ViewTheme?p_int_tv_id=1012&p_kalb_id=2&p_org=0 http://www.infobalt.lt/

Malta

Transposition of the Directive	Electronic Commerce Act (Act III of 2001) that entered into force on 10 May 2002. Act deals with e-signatures, as well as with other matters relating to e-commerce. Legal notice 110/2002 designating Maltese Communications Authority as competent authority for supervision of CSPs in Malta.
Definitions (art. 2)	E-signature: same definition as in Directive. Signatory is not defined. According to normal interpretation rules signatory must be any person (natural or legal) who signs. Definition of CSP: identical to Directive's one. No definitions for: Signature Creation Data / Signature Creation Device / Signatory / Electronic Signature Product.
Types of signatures	3 types: "Basic" / AES (meaning identical to Directive's one) / provision of a "higher level" of signature (being the "qualified" signature): AES based on a QC and created by a Secure Creation Device (N.B.: the law does not expressly refers to a Secure Signature Creation Device).
Legal equivalence to handwritten signatures (art. 5.1)	Advanced e-signature based on a QC and created by a Secure Signature Device shall be presumed to be the signature of the signatory for all intents and purposes of law.
Legal effect of e-signature (art. 5.2)	Explicit transposition. If under any law in Malta the signature of a person is required, such requirement is deemed to have been satisfied by an electronic signature. Legal effectiveness of a signature cannot be denied because: I) signature in electronic form, ii) not based on QC, iii) not based on a QC issued by an accredited CSP, iv) not created by an SSCD (same hypotheses as Directive). The only difference is that the Law does not expressly state that all signatures are admissible in legal proceedings (however, this may be inferred from the confirmation of legal effectiveness). Law provides cases in which e-signatures cannot be used (e.g., creation of wills, rights on immovable property, provision of evidence in criminal proceedings, etc.). [Question to correspondent: what is difference between the 5.1 and 5.2 if also 5.2 signature is deemed to satisfy signature requirements?]
Relevant case law	No ruling yet on the admissibility/legal effect of e-signatures.
Liability (art. 6)	Liability for CSPs issuing QC to the public for damages caused to any person reasonably relying on QC. Same grounds of liability but expressed as duties of CSPs. Also, the same Article includes a general liability clause for any damage caused to any person who reasonably relies on QC. So, ambit of liability clause wider than in Directive. Reverse burden expressly stated for failure to register or publish revocation or

	suspension of QC. Same for breach of CSPs' duties (but arising from general principle of Maltese law. No reverse liability for any other cause. Limitation of liability: limits of QC's use.
International Aspects (art. 7)	No distinction between QC issued by a CSP located in Malta or in other country. Thus, only requirement for equivalence: compliance with the requirements of Maltese law.
Data Protection (art. 8)	No transposition. However, all entities referred to in Law fall under the scope of applicability of the general Data Protection Act. Use of pseudonyms on certificates is authorised, provided that they are identified as such.
Implementation of the Annexes	Annexes I, II and III are copied. Annex IV is not transposed.
Provision of certification services	The legislation explicitly prohibits prior authorisation of CSPs. Notification is neither defined in the legislation nor implemented in practice. However, it is likely that a notification scheme will be set up in the future. CSPs issuing QCs to the public are subject to supervision. Since the supervisory system itself has not been put into place compliance criteria have yet to be established. The legislation specifies voluntary accreditation; a scheme has not been implemented yet. Therefore, neither evaluation rules nor accreditation criteria have been established. It is assumed that accreditation will be encouraged once the system has been implemented.
Number of CSPs	No CSPs issuing QCs yet.
Use of e-signatures in the public sector	The legislation does not provide any special requirements for the public sector. E-government services are in the process of being established.
Conformity assessment of SSCDs	There is no mandatory assessment.
Use of standards (Article 3.5)	Recognition of European Standards, no specific recognition of standards referenced in OJ.
Promotion of interoperability	None
Market for electronic signature products and	No e-signature applications yet. E-banking based on tokens and passwords.

services	
Web links	http://www.mca.org.mt/ http://www.msa.org.mt/ http://www.cimu.gov.mt/ http://www.mitts.gov.mt/ http://docs.justice.gov.mt/lom/legislation/english/leg/vol_13/chapt426.pdf http://www.mca.org.mt/images/library/LN%20110%20of%202002.pdf http://www.gov.mt/ http://justice.gov.mt/ http://www.gov.mt/egovernment.asp?p=105&l=2

Poland

Transposition of the Directive	"Electronic Signature" Act of 18 September 2001 that entered into force on 18 June 2002. Eight (8) decrees regulate various aspects of certification services, incl. technical specifications applying to CSPs issuing QC.
Definitions (art. 2)	The e-signature definition does not link to authentication but to identification. Signatories can only be natural persons. The definition of CSPs explicitly addresses entrepreneurs or public authorities offering certification services and the National Bank of Poland. Four definitions are provided in addition to the Directive's ones: certification attestation, time-stamping, electronic authentication and verification of secure e-signature.
Types of signatures	Three types: Basic and secure e-signatures (all requirements of the AES are transposed, except the unique identification of the signatory). In addition, both signature creation data and SSCD shall be held under the sole control of the signatory. Also, implicit recognition of a higher level of signature equivalent to the "qualified" one of the Directive (being the secure e-signature verified with a valid QC).
Legal equivalence to handwritten signatures (art. 5.1)	Modification of the Polish Civil Code: Declaration of intent signed with a "qualified" e-signature is equivalent to the written form.
Legal effect of e-signature (art. 5.2)	Explicit transposition. Any data that meet the requirements of the definition of the (basic) e-signature is an e-signature and can generate legal effects.
Relevant case law	No ruling yet addressing the use/legal effect of e-signatures.
Liability (art. 6)	No transposition. Regulation of the civil liability of all CSPs (of both QC and non-QC) in a more generic way than in the Directive. The liability causes are stated at large: CSPs' failure to comply or negligent fulfilment of its obligations. Exhaustive list of cases in which a CSP cannot be held liable: i) damages arising from false data that have been put on the certificate at the request of the signatory and ii) certificate usage/value of transactions exceeding clear limitations on the certificate. In general, CSP cannot be liable if damages are caused by circumstances for which CSP is not responsible or for damages it could not foresee (e.g. force majeure).
International Aspects (art. 7)	Certificates issued by CSPs not established or operating in Poland are legally equivalent to QC issued by CSPs established or operating in Poland under certain conditions (fulfilment of one of these conditions suffices). These conditions are: i) accreditation of the CSP, ii) recognition on the basis an international agreement, iii) registration to the registry of qualified CSPs, iv) CSP being established within EU guarantees the certificate, v) recognition of

	CSP or of the QC on the basis of an international agreement between EU and third country/organisation.
Data Protection (art. 8)	No explicit transposition. Recognition of a general duty of secrecy on all CSPs (issuing QC or not) and their employees/subcontractors, esp. in relation to data which serve to make certification authentications. Provision of exceptions to this rule (obligation to disclose information in certain circumstances). The duty to keep secret data serving to certification authentications is for perpetuity. Use of pseudonyms is recognised provided that they are indicated as such. Explicit obligation on CSPs to destroy data serving for authentication certification as soon as the certification attestation is annulled.
Implementation of the Annexes	Annex I and II have been transposed almost literally. Annex III has been transposed in such a way that the SSCD actually also encompasses parts of the Signature Creation Application, and can for example not be implemented in a smart card. Annex IV has been transposed as requirements, with mandatory product conformity assessment for "verification devices".
Provision of certification services	The legislation explicitly prohibits prior authorisation of CSPs. Notification (called 'registration') is mandatory for CSPs issuing QCs, the responsible body is Centrast SA on behalf of the Ministry of Economic Affairs. The cost of notification is €10,000. All CSPs established in Poland are subject to supervision, this process is carried out through regular audit controls. Compliance is measured against the law. The legislation does not mention voluntary accreditation; a scheme thus has not been implemented.
Number of CSPs	4 CSPs issue QCs.
Use of e-signatures in the public sector	The legislation does not provide any special requirements for the public sector. Upcoming projects include e-identity as well as electronic promulgation of legal acts.
Conformity assessment of SSCDs	There is a mandatory assessment of SSCD. There is a national accreditation body (PCA), which is responsible for appointing other bodies that in turn perform product assessments. No assessment bodies have been established yet.
Use of standards (Article 3.5)	No specific presumption of conformity to requirements for standards referenced in OJ. Instead, the Decree lists several specific EESSI standards implying presumption of conformity. The decree also specifies algorithms and parameters. A standard is mandated for the certificate policy of CSPs.
Promotion of interoperability	The government distributes a booklet on e-signatures. A certificate profile has been established. Also the following standards are promoted: ETSI TS 101 733 -Electronic Signature Format, ETSI TS 101 903 - XML Advanced

	Electronic Signatures (XAdES), and ETSI TS 101 861 - Time Stamping Profile.
Market for electronic signature products and services	Very few QCs have been issued. A Root CA, Centrast, has been set up on the demand of the National Bank of Poland. The major applications for certificates are e-government (transmission of social insurance data), regulated by law, and clearing of interbank transactions, regulated by contracts.
Web links	http://www.geocities.com/wi-ko/st/law/epustawaen.html http://www.unizeto.pl/ http://www.signet.pl/ http://www.mg.gov.pl/ http://www.kir.com.pl/ http://www.polcert.pl/ http://www.sigillum.com.pl/ http://www.cryptotech.com.pl/ http://www.piit.org.pl/ http://www.bsb.com.pl/ http://www.centrast.pl/?i=6 http://www.zus.pl/ http://www.vagla.pl/podpis http://www.informatyzacja.gov.pl/scripts/detail.asp?id=78 http://www.pca.gov.pl/ http://www.edukacjait.pl/ http://bap-psp.lex.pl/cgi-bin/demo.cgi?id=&comm=jednostka&akt=nr17017653&ver=-1&jedn=-1

Slovakia

Transposition of the directive	Law n. 215/2002 on e-signatures entered into force May 1, 2002 and decrees n. 537-542 entered into force October 1, 2002
Definitions (art. 2)	Signatory can only be a natural person. In the definition of signatory fall also CSPs who issue certificates to provide certification services.
Types of signatures	Digital signature
Legal equivalence to handwritten signatures (art. 5.1)	Secure signatures meet the requirements of handwritten signatures but only with qualified certificates issued by an accredited certificate authority.
Legal effect of e-signature (art. 5.2)	The electronic signature has legal effect but only when it is created by a secure signature creation device.
Relevant case-law	No ruling yet addressing the use/legal effect of e-signatures.
Liability (art. 6)	Explicit transposition. CSPs which supply secure electronic procedures are liable for the legal conformity and suitability of the signature creation products they supply or recommend. Limits of liability are the same as in the directive (limits of use of certificate, value of transactions).
International Aspects (art. 7)	The certificates of foreign certificate authorities can be validated by cross certificate or by signed international agreements.
Data Protection (art. 8)	CSPs which issue certificate to the public may collect personal data only directly from the data subject and the date can be collected or processed in conformity with law for protection of personal data.
Implementation of the Annexes	Annexes from EC 1999/93 are implemented to our law 215 and to decrees 537-542/2002.
Provision of certification services	There is the Root Certificated Authority in the National Security Authority. A CA who wants to issue qualified certificates must be accredited by NSA.
Number of CSPs	There are five CAs in Slovakia. There is no accredited CA.
Use of e-signatures in the public sector	Qualified certificates issued by accredited CA must be used.
Conformity assessment of SSCDs	There is a mandatory assessment of SSCDs. There are some requirements on the client software, e.g. for presenting the document to be signed.

Use of standards (Article 3.5)	These standards are published in the decree 537/2002.
Promotion of interoperability	We are looking for new possibilities for interoperability support.
Market for electronic signature products and services	No qualified certificates have been issued. Five CAs issue certificates.
Web links	http://www.nbusr.sk/indexb.php

Slovenia

Transposition of the Directive	Electronic Commerce and Electronic Signature Act adopted by the Parliament in June 2000 (entry in force 2 months after its publication in the Official Journal). More detailed and technical issues addressed in the Decree "on Conditions for Electronic Commerce and Electronic Signing", adopted in August 2000. Additional rules on registration of CSPs passed by ministerial decree in 2001.
Definitions (art. 2)	E-signature & CSP defined as in the Directive. Signatory being a person by whom, or on whose behalf, an e-signature is created. Additional definition of time-stamp. No other significant differences from Directive.
Types of signatures	3 types: "Basic" and AES (following the Directive's definition of the advanced, incl. additional requirement: signature created by an SSCD that is maintained under signatory's sole control). Implicit recognition of a higher level of signature, the "qualified" one.
Legal equivalence to handwritten signatures (art. 5.1)	Advanced e-signatures verified with QC are equal to handwritten signatures as for legal effectiveness and admissibility.
Legal effect of e-signature (art. 5.2)	Explicit transposition. All e-signatures are widely recognised in all official proceedings. No use of e-signatures in contracts of real property, donations, acts requiring notary's form, etc.
Relevant case law	A few cases recognising that e-mails and electronic documents are admissible as written and signed complaints against the other party if signed with a "qualified" e-signature.
Liability (art. 6)	Explicit transposition. Rule applicable only to CSPs issuing QC for any person who reasonably relies on QC. All liability cases of the Directive transposed and, additionally: i) duty of immediate revocation of certificate and ii) failure to adhere to the legal requirements regarding AES and QC. Reversed burden of proof applies (CSP is presumed liable unless proof that damage occurred without its fault).
International Aspects (art. 7)	Automatic equivalence for QC issued by CSPs established within the EU. QC of CSPs established in a non-EU country are equivalent if: i) voluntary accreditation granted in Slovenia or an EU-country, ii) domestic CSP guarantees foreign certificates, iii) equivalence granted on the basis of bilateral or multilateral agreement.
Data Protection (art. 8)	No explicit transposition - Personal Data Protection Act applies. Use of pseudonyms in certificates is authorised provided that pseudonyms are identified as such. Other obligations related to confidentiality duty and data protection may derive from general rules governing CSPs issuing QC.

Implementation of the Annexes	Annex I and III copied. Annex II copied with additional detailed regulation and evaluation requirements. Annex IV copied as requirements.
Provision of certification services	The legislation explicitly prohibits prior authorisation of CSPs. Notification is mandatory for all CSPs, the responsible body is MID (Ministry of Information Society). The cost of notification is approx. €20,000. All CSPs established in Slovenia are subject to supervision, this process is carried out through audit controls, either regularly or on demand. As to compliance criteria a CSP has to use products evaluated according to FIPS 140-1 and the Common Criteria (CC). The legislation specifies voluntary accreditation; a scheme has already been implemented. Evaluation rules and accreditation criteria are not yet known. The Slovenian system does not encourage accreditation.
Number of CSPs	4 CSPs issue QCs, there is no accredited CSP yet.
Use of e-signatures in the public sector	The legislation defines specific requirements for the use of electronic signatures in the public sector. Future projects may include e-identity cards.
Conformity assessment of SSCDs	There is no mandatory assessment.
Use of standards (Article 3.5)	Presumption of conformity to requirements for standards referenced in OJ. In addition, CSPs must use products evaluated according to FIPS 140-1 and Common Criteria. No algorithms have been specified.
Promotion of interoperability	None
Market for electronic signature products and services	About 90,000 QCs have been issued, with 50 % based on smart cards, for use with Qualified Electronic Signatures in e-government. Another 20,000 have been issued under contractual agreement, mostly for corporate and private e-banking.
Web links	http://www.atrp.si/ http://www.gov.si/mid/ http://www.perenic.com/ http://www.skb.si/ http://www.perenic.com/e-commerce http://www.halcom.si/

Bulgaria

Transposition of the Directive	i) "Electronic Document and Electronic Signature Act" (EDESA) last amended in 2002 and entered into force on 7 October 2001. ii) Ordinance of 2002 on "the Activities of CSPs, the Terms and Procedures of Termination thereof, and the Requirements for Provision of Certification Services". iii) Ordinance on "the Requirements to the Algorithms for QES" of 2002 entered. iv) Ordinance on "the Procedure for Registration of CSPs" of 2002 entered into force. All three Ordinances entered into force on 12 February 2002.
Definitions (art. 2)	E-signature: The purposes that should be served by the signature are laid down (identification of signatory / manifestation of signatory's consent / data integrity). Not all signatures as defined in the Directive shall be considered as e-signatures under Bulgarian law. Distinction between "Owner" and "Signatory": - Owner: natural or legal person on behalf of whom the e-statement is performed. - "Signatory": Only natural persons who create electronic statements (only signatories have access to signature creation data). CSP: Person issuing QC, keeps directory & provides a third person with access to published certificates, provides service for the creation of key pair.
Types of signatures	i) "Basic" e-signature: similar to the AES of Directive. ii) qualified e-signature (expressly stated as Advanced): Similar to "qualified" e-signature under the Directive – Universal e-signature (expressly stated as such): qualified e-signature based on a certificate issued by a CSP that is registered under a special procedure.
Legal equivalence to handwritten signatures (art. 5.1)	No explicit transposition. All types of e-signatures have same legal effect as handwritten signatures. N.B.: AES and qualified e-signature are equivalent to handwritten signatures only between private parties. A Universal e-signature has the effect of a handwritten one towards any party, incl. state/local authorities.
Legal effect of e-signature (art. 5.2)	No explicit transposition. Any signature falling within the definition of e-signature under Bulgarian law can have legal effects. E-signatures cannot be used for acts requiring qualified written form or when storage of documents have a specific legal meaning (securities, bills of lading, etc.). Use of e-signatures in judicial system or by certain state authorities (e.g. Bulgarian National Bank, National Assembly, etc.) shall be recognised by special laws.
Relevant case law	No ruling yet addressing the use/legal effect of e-signatures.

Liability (art. 6)	Explicit transposition. Liability of CSPs issuing Qualified and Universal certificates for damages occurred to owners and third parties. List of liability causes broader than in the Directive. All liability causes listed in the Directive are transposed, and, in addition: i) failure to register revocation of certificates, ii) CSPs liable for correspondence between signature creation and signature verification data in all cases (even if it does not generate such data), iii) The special liability clause encompasses all cases of non-performance of CSPs' statutory duties as defined in law. Reverse burden of proof. No possibility to waive liability. Limits of liability same as Directive (use of certificate and value of transactions).
International Aspects (art. 7)	Recognition of foreign certificates as issued by CSPs established in Bulgaria if: i) CSP or certificate recognised by international agreement, (or) ii) CSP compliant to requirements that correspond to the ones under Bulgarian law and is recognised in the country of establishment, (or) iii) a Bulgarian CSP undertakes liability for actions/omissions of foreign CSP.
Data Protection (art. 8)	Specific data protection obligations upon CSPs and supervisory authority with respect to collection of data and maintenance of registries. For other data processors, the general Data Protection Act applies. Use of pseudonyms in certificates is not recognised.
Implementation of the Annexes	The implementation of Annex I is similar, but no QC indicator is required, and full name is always required, not just a pseudonym. More details are also specified. Annex II is copied with the additional requirement for liability insurance and provision of time-stamping services. Annex III is copied and Annex IV is partly implemented, recommending CWA 14171 to be used.
Provision of certification services	The legislation does not prohibit prior authorisation of CSPs. Notification is mandatory for CSPs issuing QCs, the responsible body is CRC (Communications Regulation Commission). The cost of notification is in the range of €5,000 to €10,000. Several compliance criteria have been specified. The legislation specifies two schemes: one scheme describing voluntary accreditation which has not been implemented yet, another scheme for voluntary "registration" which is applicable to CSPs issuing QCs for "universal" e-signatures (to be mainly used in the public sector) and which has already been established. The Bulgarian system implicitly does encourage accreditation through favouring QCs for "universal" signatures.
Number of CSPs	1 CSP issues QCs, it is also 'registered' to issue QCs for 'universal' signatures.
Use of e-signatures in the public sector	The legislation defines specific requirements for the use of electronic signatures in the public sector.
Conformity assessment of SSCD	There is a mandatory assessment of SSCDs, until now only foreign assessment bodies are being recognized.

Use of standards (Article 3.5)	No specific presumption of conformity to requirements for standards referenced in OJ. Instead, the Communications Regulation Commission maintains and publishes lists with recognized international standards. A special ordinance has been published on Algorithms for Qualified Electronic Signatures. It is mandatory for CSPs to offer time-stamping services.
Promotion of interoperability	Only through publication of algorithms.
Market for electronic signature products and services	Only very few QCs have been issued so far. Ca 5,000 certificates have been issued under contract for e-banking.
Web links	http://www.orac.bg/en/resources-links http://www.crc.bg/v2/files/bg/629.pdf http://www.crc.bg/ http://www.is-bg.net/ http://www.bia-bg.com/ http://www.csd.bg/ http://www.lex.bg/ http://www.stampit.org/

Romania

Transposition of the Directive	Law n°. 455 on the Electronic Signature entered into force on 31 July 2001 (except from a number of Articles specified in Law). Government Decision n°. 1259 of 2001 "regarding the Approval of the Technical and Application Rules of the Law".
Definitions (art. 2)	E-signature: similar definition to Directive's one. Signatory: not expressly specified in Law if it can be only natural person. It appears that legal persons can be signatories. Express definition of "Qualified CSP": CSP issuing QC.
Types of signatures	Three types: "Basic" / Extended e-signature (being equivalent to the AES of the Directive) / Also, provision for a higher level of signature ("Qualified): Extended e-sign based on QC and created by an SSCD.
Legal equivalence to handwritten signatures (art. 5.1)	Yes. When the written form is required as proof or validity condition of a legal document in cases stipulated by law then: a document in electronic form shall satisfy to this condition provided that there is an extended e-signature attached to it which is based on a QC and created by an SSCD.
Legal effect of e-signature (art. 5.2)	No explicit transposition. The law makes a distinction between "document under private signature" and "authentic document". i) The e-signature which is based on a QC and which is created by an SSCD is assimilated, in as much as its requirements and effects are concerned, to a written document under private signature. N.B.: this signature need not be an extended e-signature. ii) A document including an e-signature acknowledged by the party the respective document is opposed to has the effects of an authentic document. Consequently, any signature may constitute "proof of authenticity" if it is acknowledged.
Relevant case law	No ruling yet addressing the admissibility/legal effect of e-signature.
Liability (art. 6)	Direct transposition. Liability of CSPs issuing QC (not only to the public) for damages caused to any person the behaviour of which is based on the legal effects of certificate. All liability grounds of Directive included, and in addition: i) failure to suspend/revoke certificate, ii) failure to fulfil to certain obligations specified in Law (inter alia, with respect to notification or data protection obligations). Accordingly, scope of provision wider than Directive's one. Reverse burden of proof. Limitations of liability same as in Directive (limits of certificate's use and value of transactions).
International Aspects (art. 7)	QC issued in EU have the same value as Romanian QC. Certificates of non-EU countries are recognised under conditions: i) foreign CSP accredited according to Romanian law, ii) CSP established in Romania guarantees QC, iii) bilateral/multilateral agreement acknowledges equivalence.

Data Protection (art. 8)	No explicit transposition. Law stipulates the obligation to keep secret and confidential personal data that become known to CSPs, the Controlling and Homologation Authorities. Breaches of this duty amounts to criminal liability.
Implementation of the Annexes	Annex I, II and III have been copied. Annex IV has not been transposed.
Provision of certification services	The legislation explicitly prohibits prior authorisation of CSPs. Notification is mandatory for all CSPs, the responsible body is the Authority for Coordination and Supervision. There is no cost for notification. All CSPs established in Romania are subject to supervision, this process is carried out through bi-annual audit controls. Compliance criteria have been specified. The legislation specifies voluntary accreditation; a scheme has not been implemented yet. Evaluation rules and accreditation criteria have been established. The Romanian system does implicitly encourage accreditation.
Number of CSPs	1 CSP issues QCs, there is no accredited CSP yet.
Use of e-signatures in the public sector	The legislation does not provide any special requirements for the public sector.
Conformity assessment of SSCDs	There is a mandatory assessment of SSCDs, the designated assessment body of which has not been appointed yet. SSCD products have already been assessed.
Use of standards (Article 3.5)	The Application Rules states that a list of European standards to be followed will be established. It also specifies some technical details regarding the algorithms to be used.
Promotion of interoperability	None besides the Application Rules
Market for electronic signature products and services	About 20,000 QCs have been issued for payment of local taxes and e-government using Qualified Electronic Signatures.
Web links	http://www.mcti.ro/ http://www.e-sign.ro/

Iceland

Transposition of the Directive	Electronic Signatures Act n°. 28/2001. Act basically adopts the text of the Directive, without significant changes.
Definitions (art. 2)	Definitions of signature/signatory and CSP as in the Directive. Act does not specify whether legal persons can be signatories (issue subject to judicial interpretation). Explicit definition of Qualified e-signature.
Types of signatures	Idem as Directive: "Basic" – AES (same requirements as in the Directive) and Qualified (AES connected to a QC and made with an SSCD).
Legal equivalence to handwritten signatures (art. 5.1)	If there is a requirement for a signature deriving from law or otherwise, Qualified e-signatures shall always be considered to meet such a requirement.
Legal effect of e-signature (art. 5.2)	Explicit transposition. Notwithstanding the legal status of qualified e-signatures, all other signatures can meet the requirements of a valid signature. The judge will decide on the validity of the signature on an ad hoc basis. The e-commerce Act precludes conclusion of contracts by electronic means relating to: transfer in real estate (except rental rights), family law or inheritance conventions, acts subject to notarisation or other form requirements (e.g. stamps).
Relevant case law	No ruling yet addressing the use/legal effect of e-signatures.
Liability (art. 6)	Explicit transposition. Clause addresses CSPs' liability issuing QC to the public vis-à-vis damages arising from the normal use of certificates. List of liability causes are same as in the Directive. Reverse burden of proof applies. Same liability limits (use of certificate and value of transactions).
International Aspects (art. 7)	Provision of Directive is copied verbatim in Icelandic Act.
Data Protection (art. 8)	Explicit transposition. Provision of a special data protection clause in the Act (similar to art. 7.2 of Directive) and reference to the Act on the Protection of Privacy. Obligation of CSP to notify its operation in accordance with the latter Act. Pseudonyms can be used provided that they are clearly identified on the certificate.
Implementation	Annex I, II and III have been copied. Annex IV has not been transposed.

of the Annexes	
Provision of certification services	The legislation explicitly prohibits prior authorisation of CSPs. Notification is mandatory for CSPs issuing QCs, the responsible body is Löggildingarstofa (Accreditation Agency). The cost of notification is approx. €11,700 annually. CSPs issuing QCs (even to *closed user groups*!) established in Iceland are subject to supervision, this process is carried out through audit controls. Compliance criteria have not been specified. The legislation does not mention voluntary accreditation; a scheme thus has not been implemented.
Number of CSPs	1 CSP issues QCs.
Use of e-signatures in the public sector	The legislation defines specific requirements for the use of electronic signatures in the public sector. On-going projects include e-tax and e-government projects.
Conformity assessment of SSCDs	There is a mandatory assessment of SSCDs, the designated assessment body of which has not been appointed yet.
Use of standards (Article 3.5)	No statement of presumption, only that EU published standards on SSCD and trustworthy systems shall be recognized. Conformity with BS 7799 (ISO 17788) is by the supervisor considered an important criteria in determining compliance with Annex II.
Promotion of interoperability	No statement of presumption, only that EU published standards on SSCD and trustworthy systems shall be recognized. Conformity with BS 7799 (ISO 17788) is by the supervisor considered an important criteria in determining compliance with Annex II.
Market for electronic signature products and services	Only very few QCs have been issued so far by supervised CSP. Verisign is issuing what they call "Qualified Certificates" (Class 3) based on soft keys for e-government using 5.2 signatures. Around 2000 other certificates have been issued for e-government and e-banking (based on smart cards).
Web links	http://www.althingi.is/lagas/128a/2001028.html http://www.althingi.is/lagas/128a/2002030.html http://www.althingi.is/altext/128/s/1158.html http://forsaetisraduneyti.is/interpro/for/for.nsf/pages/it.html http://fjarmalaraduneyti.is/interpro/fjr/fjr.nsf/0/61229A4CE8658A6500256B1A003BE03A?OpenDocument&Highlight=0,kpmg

Liechtenstein

* (Responses are given on the basis of the draft Bill and Ordinance)

Transposition of the Directive	Legal framework has not been enacted formally yet. i) Draft Electronic Signature Act, to be adopted in September 2003. ii) Draft Electronic Signature Ordinance, to be adopted until Dec. 2003, iii) Draft Ordinance on the minimum criteria for confirmation bodies, to be adopted until end of 2003.
Definitions (art. 2)	"E-signature": as Directive. Signatory: a natural person to whom the signature creation & verification data are allocated", or a CSP issuing certificates. Thus, the definition of signatory includes CSPs. Broader definition than in the Directive: Natural or legal person or any other legally capable institution which issues certificates or provides other signature and certification services. Additional definitions: "Secure" e-signature: being the QES of the Directive, time stamping service, Compromise: breach of security measures or security technique so that the level of security set up by the CSP no longer applies.
Types of signatures	"Basic" e-sign, AES and "Secure" e-signature: equal to QES.
Legal equivalence to handwritten signatures (art. 5.1)	Explicit transposition: "A secure electronic signature meets the legal requirement of a handwritten signature especially the requirement for the written form as defined in §886 of the CC unless a different definition is laid down by law or by an agreement between the parties".
Legal effect of e-signature (art. 5.2)	Explicit transposition. In addition, a provision that "Signature procedures with different levels of security and different classes of certificates can be used for legal or commercial transactions". E-signatures cannot be used for: i) contracts under family and inheritance law, ii) acts subject to formal requirements or official certification, iii) guarantees.
Relevant case law	No ruling yet addressing the use/legal effect of e-signatures.
Liability (art. 6)	Explicit transposition. Liability clauses as in the Directive, and in addition: i) failure to register revocation is spelled out in the list of liability causes, ii) failure to use trustworthy products & procedures for the generation/storage of signature creation data, iii) responsibility for signature creation products and procedures used. Reversed burden of proof. Liability may not be limited or excluded in advance.
International Aspects (art. 7)	Explicit transposition. EEA countries are not considered as third countries. Both domestic, EEA and foreign certificates shall be verifiable from Liechtenstein. Same conditions as art. 7.1, with the difference that whenever Directive refers to "Community" or "EU Member State", the law refers to "the

	EEA" or "EEA Member State" accordingly. Noteworthy: specific provision on the recognition of "foreign" electronic signatures as equivalent to "Secure" electronic signatures (QES) of Liechtenstein.
Data Protection (art. 8)	Explicit transposition. Reference to the general legislation on data protection and, in addition, specific provisions on use of pseudonyms and CSPs' obligations for disclosure/transmission of data to certain authorities. The specific data protection rule applies only to CSPs, not other bodies or authorities. Use of pseudonyms is authorised if they are indicated as such. Pseudonyms shall not be offensive or obviously open to confusion with names or signs. Disclosure of real names is possible for specific reasons and provided that the transmission is recorded.
Implementation of the Annexes	Annex I, II, III and IV are more or less copied.
Provision of certification services	The legislation explicitly prohibits prior authorisation of CSPs. Notification is mandatory for all CSPs, the responsible body is the "Amt für Telekommunikation". The cost of notification is approx. CHF 5,000. All CSPs established in Liechtenstein are subject to supervision, this process is carried out through bi-annual audit controls. Compliance criteria have been specified. The legislation specifies voluntary accreditation; a scheme has not been implemented yet, though. No accreditation criteria, but evaluation rules have been established. The Liechtenstein system does not encourage accreditation.
Number of CSPs	No CSPs issuing QCs yet.
Use of e-signatures in the public sector	The legislation does not provide any special requirements for the public sector.
Conformity assessment of SSCDs	There is a mandatory assessment of SSCDs, the designated assessment body of which has not been appointed yet.
Use of standards (Article 3.5)	Presumption of conformity to requirements for standards referenced in OJ. No other standards are mandated or recommended. The ETSI SR 002176 is specified in the order.
Promotion of interoperability	Recommended use of EESSI standards.
Market for electronic signature products and services	The most interesting are E-Mail; E-Banking; E-Government; E-Billing; E-Procurement; social- and medical applications.
Web links	http://www.gesetze.li/

	http://www.sewr.llv.li/

Norway

Transposition of the Directive	"Electronic Signature" Act No 81 2001 (consolidated version) and Regulation "on Requirements for Issuers of Qualified Certificates". Both acts entered into force on July 1, 2001 (consolidated version on January 1, 2003). The Act implements all the provisions of the Directive except Annex IV. The Regulation contains more detailed provisions in relation to the provision of Qualified Certificates.
Definitions (art. 2)	Electronic signature: same as in the Directive. Signatory: A person holding a signature creation device who acts on his own behalf or on behalf of another natural or legal person. Explicit definition of QES.
Types of signatures	3 types: Distinction between basic, advanced and qualified e-signatures as in the Directive. Qualified e-signatures are AES based on a QC and created by an SSCD.
Legal equivalence to handwritten signatures (art. 5.1)	No general equal status between handwritten signatures and qualified e-signatures. However, qualified e-signature fulfils the requirements of a signature if: i) the law requires a signature for an act to produce its legal effects and ii) electronic communication is allowed in the area the act is referring to. "qualified" electronic signatures can be created only by natural persons.
Legal effect of e-signature (art. 5.2)	Any e-signature (also non-qualified) may comply with the requirements of a signature. This signature will be evaluated on an ad-hoc basis by the judge. However, the Norwegian law precludes the use of e-signatures in certain cases (e.g. wills, certain acts under labour law, etc.).
Relevant case law	No ruling yet addressing the use/legal effect of e-signatures.
Liability (art. 6)	Explicit transposition of art. 6 in Norwegian Act. The latter provides for the liability of CSPs issuing QC (incl., ALL certificates, issued to the public and on a contractual basis). Same liability causes as art. 6. The omission to register revocation of a QC is included in the list of liability clauses. The CSP bears the burden of proving that it has not acted negligently (although this appears to be contrary to the Norwegian tort law). The liability limits are the same as in Directive (certificate usage/value of transactions exceeding clear limitations on the QC).
International Aspects (art. 7)	QC issued by CSPs established in a third country are equivalent to QC issued within the EEA if certain conditions are met. These conditions are the same as in the Directive (art. 7). [N.B.: certificates issued "in a Member State" is replaced by certificates issued "within the EEA-area"].
Data Protection (art. 8)	The Norwegian Data Protection Act applies. The Electronic Signature Act implements only art. 8 (2) of Directive. The "data protection" clause of the Act covers activities of all CSPs, issuing QC or not. Use of pseudonyms on certificates is recognised, provided that pseudonyms are identified as such.

	Information related to QC shall be stored for a minimum period of 10 years. The activities of CSPs shall be notified to the Data Inspectorate (Norwegian Data Protection Authority) prior to any process of personal data.
Implementation of the Annexes	Annex I, II and III are copied. Annex IV not transposed, but similar requirements specified for communication with and within public administrations.
Provision of certification services	The legislation does not prohibit prior authorisation of CSPs. Notification is mandatory for CSPs issuing QCs to the public; the responsible body is NPT (Post and Telecommunications Authority). The cost of notification is approx. €12,500 annually. CSPs issuing QCs established in Norway are subject to supervision, this process is carried out through an audit at notification time. Compliance criteria have not been specified. The legislation does not mention voluntary accreditation; a scheme thus has not been implemented. According to preparatory documents "it is up to the market to decide on whether a voluntary accreditation scheme should be established".
Number of CSPs	1 CSP issues QCs.
Use of e-signatures in the public sector	The legislation does not yet provide any special requirements for the public sector.
Conformity assessment of SSCDs	There is no mandatory assessment.
Use of standards (Article 3.5)	Presumption of conformity to requirements for standards referenced in OJ. Only publication of recommended algorithms and parameters for use in e-government.
Promotion of interoperability	A co-ordinating body for the use of PKI in the public sector is expected to be established during the autumn 2003. PKI-forum's working group on interoperability is preparing a report on the issue.
Market for electronic signature products and services	About 60,000 QCs have been issued based on standard smart cards and SIM-cards. Main applications are online betting and mobile e-commerce (5.2 signatures) and e-banking (using NQC under contract).
Web links	http://www.npt.no/ http://odin.dep.no/nhd/ http://www.statskonsult.no/ http://www.pki.no/ http://www.zebsign.no/

	http://www.lovdata.no/all/hl-20010615-081.html http://www.lovdata.no/for/sf/nh/nh-20010615-0611.html http://www.lovdata.no/for/sf/aa/aa-20020628-0656.html http://www.handel.no/pkiforum/ http://handel.no/ http://www.enorge.org/ http://odin.dep.no/aad

Switzerland

Transposition of the Directive	Ordinance of 12 April 2000 on "Services related to Electronic Certification" entered into force on 1 May 2000. Based on this Ordinance: Ordinance of the Federal Office for Communications (BAKOM) of 15 August 2000 on "Technical and Administrative Regulations on Services related to Electronic Certification" which entered into force on 1 September 2001. Imminent discussion of the Draft Bill on "Services Related to Electronic Signatures" in the Parliament in summer 2003.
Definitions (art. 2)	Same definition of e-signature as Directive (draft law). No explicit definition of signatory. Signatories can be natural and legal persons. Narrow definition of CSP: services limited to issuance of certificates (draft law).
Types of signatures	Only "basic" in the current Ordinance. * Draft Bill: Distinction between "basic, "improved" and "qualified" e-signatures.
Legal equivalence to handwritten signatures (art. 5.1)	No transposition in the existing Ordinance, which expressly reserves the legislation on private law in this regard. No express presumption exists in favour of any e-signature. * Draft Bill: equivalence between handwritten and qualified e-signatures based on a QC of a recognised (accredited) CA if the electronic signature originates from a natural person.
Legal effect of e-signature (art. 5.2)	No explicit transposition. The judge is in principle free to consider any evidence submitted by the parties. In practice, Swiss Authority for Accreditation may be asked to provide confirmations about the security of a signature (correspondence of private/public keys, certificate issued by a recognised CSP, certificate valid at a particular point of time). E-signatures cannot be used for acts that need to be notarised.
Relevant case law	No ruling yet addressing the use/legal effect of e-signatures.
Liability (art. 6)	No transposition of this clause (a special "liability" clause transposing art. 6 is included in the Draft Bill under discussion). A general provision in the current Ordinance stipulating CSPs' liability for damages incurred to third parties resulting from: i) defective electronic certificates, ii) lack of adherence to obligations pertaining to publication, provided that the CSP cannot prove that the damage occurred without his fault. No express limitations of liability.
International Aspects (art. 7)	No express provision in the current Ordinance. Only mention that this matter is subject to specific international conventions. * Draft Bill: makes possible recognition of foreign CSPs, with some simplification if CSP has already been recognised abroad.
Data Protection	No explicit transposition. Reference to the legislation on data protection and, in

(art. 8)	addition, stipulation of one obligation: CSP shall only treat the personal data which is necessary for the fulfilment of its tasks. Use of pseudonyms recognised (obligation of express mention of use of a pseudonym). The real identity must be verified as in the normal cases.
Implementation of the Annexes	Parts of Annex I have been copied, with the additional requirement of QES for the signature of the QC. Some of the requirements of Annex II can also be found, but with more detailed requirement distributed over different regulations. Annex III is literally copied, as well as most of Annex IV.
Provision of certification services	The legislation does not prohibit prior authorisation of CSPs. There is no notification of CSPs. However, CSPs voluntarily may register with a 'certification body', accredited by SAS (Swiss Accreditation Service). CSPs issuing QCs which have been recognized by a 'certification body' and are established in Switzerland are subject to supervision, this process is carried out through audit controls, either regularly or on demand. Compliance criteria have been specified in the e-sign ordinance. The legislation specifies voluntary accreditation (so-called 'recognition'), a scheme has already been implemented. The Swiss system implicitly does encourage accreditation through favouring recognition.
Number of CSPs	No CSPs issuing QCs yet (however, the government has temporarily authorised a German CSP to provide certificates); no accredited CSP yet.
Use of e-signatures in the public sector	The legislation defines specific requirements for the use of electronic signatures in the public sector. On-going projects include e-identity, e-tax, e-voting, and e-government projects.
Conformity assessment of SSCDs	There is no mandatory assessment.
Use of standards (Article 3.5)	No mentioning of standards referenced in OJ. Instead, several international standards are referenced: BS7799, ITU-T X.509, FIPS, ISO 15408. For algorithms and parameters, the EESSI ALGO paper is referenced. Furthermore, a recognised CSP's cryptographic keys must be generated by a device that is compliant with FIPS140-1 Level 3 (at a minimum) and is certified EAL4 (at a minimum).
Promotion of interoperability	The BAKOM regulation. The PKI Forum.
Market for e-signature products and services	No QCs have been issued. More than 10,000 certificates have been issued for e-government and more several 100,000 certificates have been issued, mostly for access control. Many security problems have been seen.

Web links	http://www.admin.ch/ch/d/sr/7/784.103.de.pdf http://www.admin.ch/ch/d/ff/2001/5716.pdf http://www.admin.ch/ch/d/sr/7/784.103.1.de.pdf http://www.bakom.ch/imperia/md/content/deutsch/telecomdienste/internet/digitalesignatur/digsig_prescriptions_oscert_v4_150801_de.pdf http://www.ofj.admin.ch/d/index.html http://www.admin.ch/ch/d/sr/6/641.201.1.de.pdf http://internet.estv.admin.ch/data/mwst/d/egv/pdf/fs_digsig_d.pdf http://www.bakom.ch/de/telekommunikation/internet/digsig/ http://www.pki-forum.ch/ http://www.ech.ch/ http://www.isps.ch/site/default.asp?dossiers=1 http://www.bakom.ch/ http://www.sas.ch/en/index.html http://www.sas.ch/fr/pki_isms/index.html http://www.admin.ch/ch/f/egov/index.fr.html

Appendix 5: Presentation of the researchers

Presentation of the Research Team

Jos DUMORTIER	Interdisciplinary Centre for Law and Information Technology Faculty of Law University of Leuven, Tiensestraat 41, 3000 Leuven Belgium E-mail: jos.dumortier@law.kuleuven.ac.be
Patrick VAN EECKE	Interdisciplinary Centre for Law and Information Technology Faculty of Law University of Leuven, Tiensestraat 41, 3000 Leuven Belgium E-mail: patrick.vaneecke@law.kuleuven.ac.be
Georgia SKOUMA	IT Law Unit Bogaert & Vandemeulebroeke E-mail: georgia.skouma@bvlaw.be
Hans NILSSON	Hans Nilsson Consulting Fredriksstrand 5 S-185 35 Vaxholm SWEDEN e-mail: hans@hansnilsson.se
Stefan KELM	Secorvo Security Consulting GmbH Albert-Nestler-Strasse 9, D-76131 Karlsruhe E-Mail kelm@secorvo.de

Presentation of the quality control team

Bart Preneel	K.U.Leuven ESAT/COSIC
Claude Boulle	Consultant Orsay, France

Presentation of the Correspondents

EU countries

Austria	Dr. Thomas MENZEL IKT-Stabsstelle, BMöLS
Denmark	Dr. Henrik UDSEN Bech-Bruun Dragsted Law Firm
Finland	Prof. Dr. Ahti SAARENPÄÄ University of Lapland
France	Muriel QUADERNO CERTPLUS
Germany	Prof. Dr. Alexander ROSSNAGEL Universitaet Kassel
Netherlands	Prof. dr. Bert-Jaap KOOPS Tilburg University
Greece	Georgia SKOUMA Attorney at law, Brussels
Ireland	Prof. Dr. Maeve MCDONAGH & Dr. Fidelma WHITE University College Cork,
Italy	Prof. Avv. Giusella FINOCCHIARO Studio legale Finocchiaro, Bologna

Portugal	Pedro DIAS Ferreira Pinto & Associados - Sociedade de Advogados
Spain	Professor Dr. Rosa BARCELO Attorney at Law
Sweden	Anna NORDÉN Tekki AB
United Kingdom	Dr Ian WALDEN Centre for Commercial Law Studies, Queen Mary, University of London

EEA countries & Candidate countries

Bulgaria	George G. DIMITROV O.R.A.C. Dimitrov, Petrov & Co.
Czech Republic	Vladimír SMEJKAL Court Expert
Cyprus	Olga GEORGIADES VAN DER POL Lawyer
Hungary	Dr. Balázs RÁTAI Legal advisor at the Communications Authority of Hungary
Iceland	Birgir Már RAGNARSSON, Attorney at law Managing Director, Audkenni Inc.

Baltic States: *Estonia* *Lithuania* *Latvia*	 Mr Ain JÄRV AS Sertifitseerimiskeskus (Certification Centre Ltd) Prof. Dr. Rimantas PETRAUSKAS Law University of Lithuania, Vilnius Ints Zitars JSC Hansabanka, Riga
Malta	Dr Olga CARUANA-FINKEL Gatt Frendo Tufigno Advocates
Norway	Rolf RIISNAES Norwegian Research Center for Computers and Law, Oslo
Poland	Marcin BUTKIEWICZ University of Poznan
Romania	Paula-Adriana ACSINTE Attorney-at-Law
Slovakia	Mr. PILAT National Security Bureau, Bratislava
Slovenia	Matjaz CADEZ, univ.dipl.ing. Halcom informatika d.o.o.
Switzerland (not EEA)	Dr. Thomas LEGLER Attorney-at-law