Another step towards an european framework for electronic signatures

Vinje, Thomas; Julia Barcelo, Rosa

Published in:
Computer Law and Security Report

Publication date:
1998

Document Version
Publisher's PDF, also known as Version of record

ELECTRONIC SIGNATURES

ANOTHER STEP TOWARDS A EUROPEAN FRAMEWORK FOR ELECTRONIC SIGNATURES: THE COMMISSION'S DIRECTIVE PROPOSAL

Rosa Julià-Barceló and Thomas C. Vinje[1]

Parties involved in electronic commerce in open networks such as the Internet are faced with the problem of *authentication* of the communicating parties, i.e. knowing that the sender of an electronic message is actually the person he purports to be. In addition, communicating parties also need to ensure that the electronic message received is the one that actually was sent, i.e. the *integrity* of the message.

These goals can be achieved through the use of electronic signatures, including digital signatures created through public key cryptography. However, for electronic signatures to accomplish such objectives in open networks, they need to be used together with certificates issued by certification service providers that certify the link between the electronic signature and the identity of the electronic signature holder. Therefore, for electronic commerce to flourish, electronic signatures must be legally recognized as equivalent to their hand-written counterparts. In addition, a legal regime must be created for the establishment and operation of certification service providers that will generate trust among trading parties in certification authorities, and thereby in electronic signatures.

In May 1998, the Commission presented a Proposal for a Directive aimed at establishing a legal framework for electronic signatures and certification service providers in Europe. The Proposal addresses, inter alia, the liability of certificate service providers towards third parties and the legal recognition of electronic signatures, both within Europe and internationally. The proposal provides that certification service providers need not obtain authorization to act as such, although Member States are free to introduce a system of voluntary accreditation for service providers. The Proposal has adopted a technologically neutral approach — governing electronic signatures generally rather than only digital signatures — in an effort to ensure that the Directive will not be made obsolete as technology progresses.

Despite lacking clarity in certain important respects, the Proposal is to be welcomed and the Commission congratulated in taking a key step forward in promoting electronic commerce in Europe.

On 13 May 1998, the Commission presented a proposal for a directive aimed at establishing a legal framework for electronic signatures and certification service providers in Europe ('the Proposal').[2] This article will provide a brief description and analysis of the main issues addressed in the Proposal.

ANTECEDENTS OF THE PROPOSAL

Most European Union Member States have laws requiring written documents and hand-written signatures for purposes such as validity and enforceability of contracts and admissibility and valuation of evidence. Electronic documents and electronic signatures are not always regarded as fulfilling these requirements. Until recently, however, the failure to give legal recognition to electronic documents and signatures presented little obstacle to commerce. Before the recent dramatic expansion of the Internet, electronic documents and signatures were used only in the context of closed networks. In particular, they were used between individual businesses trading with one another through electronic data interchange (EDI),[3] and these trading parties would agree amongst themselves on the legal value of electronic documents and signatures as well as procedures providing security to EDI transactions. Thus, little need was perceived for a legal regime governing electronic signatures.

However, starting with the TEDIS project[4] in the early 1990s, the European Commission perceived that EDI would expand from closed groups to open groups, and that a need would arise for legislation ensuring security of electronic transactions in this context. In particular, it was foreseen that there would be a need for a legal regime recognizing electronic signatures and governing the establishment and operation of certification service providers (then called 'trusted third parties' or 'electronic notaries').[5]

In the end it was not the expansion of EDI to open groups, which has occurred only to a rather limited extent, but the expanded penetration of the Internet that led to demands for the regulation of electronic signatures and certification service providers. With the Internet's ability to connect — at low cost — vast numbers of trading parties having no pre-existing relationship, enabling electronic transactions on a large scale, came a dramatically increased need for authenticity and integrity in such transactions. Contrary to business conducted in closed environments, where the contracting parties know and trust one another, parties conducting business in an open Internet environment who do not

know one another need special mechanisms to ensure that the person with whom one believes one is doing business is actually the person he purports to be (authenticity), and that the messages exchanged between contracting parties have not been altered (integrity). At least with respect to authenticity, such mechanisms are offered by certification service providers, who issue certificates guaranteeing the identity of the holder of a particular electronic signature and who maintain databases ensuring the continued validity of such certificates.

Even if the ultimate driving force behind the need for greater security in electronic commerce became the immense growth of the Internet rather than the expansion of EDI to open networks, the Commission's efforts in the EDI area proved valuable. In particular, beginning in 1992 the Commission funded numerous useful projects on both the technical and legal aspects of digital signatures.[6]

For several years, however, the Commission took no legislative steps in this area, perhaps, among other reasons, because cryptography issues appeared to many to fall within the competency of the Member States. Meanwhile, in the United States and at international organization level, the legal debate became very heated and many legislative initiatives were launched.

In the United States, since 1994 almost all the 50 states have either passed or initiated legislation on electronic or digital signatures.[7] With respect to Federal legislation, Article 2B of the Uniform Commercial Code (UUC), which will cover, *inter alia*, legal recognition of electronic records and signatures, is currently being drafted by the National Conference of Commissioners on Uniform State Law (NCCUSL).[8] Moreover, the American Bar Association has published Digital Signature Guidelines.[9]

With regard to international organizations, in 1996 United Nations Commission on International Trade Law (UNCITRAL) began working on a Proposal for Uniform Rules on Electronic Signatures, which will complement the Model Law on Electronic Commerce.[10] In 1997, the Organization for Economic Cooperation and Development (OECD) adopted Guidelines for Cryptography Policy to guide countries when drafting cryptography regulations. In the same year the International Chamber of Commerce published guidelines entitled "*General Usage for International Digitally Ensured Commerce*" with the objective of promoting the understanding of technical issues within the business community.[11]

Finally, in April 1997, the European Commission issued a Communication entitled "*A European Initiative on Electronic Commerce*",[12] which, for the first time, officially recognized the need for building trust and confidence in electronic transactions and announced, inter alia, an initiative to establish an EU regulatory framework for digital signatures. A Bonn Ministerial Declaration also endorsed the need for a legal and technical framework at European level in digital signatures.[13]

In October 1997, a second Communication entitled "*Ensuring Security and Trust in Electronic Communication — Towards a European Framework for Digital Signatures and Encryption*" was issued jointly by the Directorate Generals for Industry (DG XIII) and Internal Market (DG XV).[14] This Communication identified potential divergences among Member State laws as a basis for an EU initiative and enumerated the basic principles of the regulatory framework envisioned by the Commission for digital signatures and certification service providers.[15] Immediately after issuance of this Communication, the European Commission initiated an intense activity resulting in the recent Proposal.

One of the reasons for this haste after several years of quiescence is that between the two Commission Communications various EU Member States had adopted laws or had proposed legislation on digital signatures.[16] Of those Member States already to have adopted laws, Germany was the first, in August 1997, to enact a Digital Signature law,[17] followed by Italy in November 1997.[18]

The Communication received a positive reaction from industry and Member States. Indeed, in December 1997 the Council of Ministers endorsed the Communication, inviting the Commission to submit a proposal in the second quarter of 1998.[19]

LEGAL BASIS FOR THE PROPOSAL

For some time, a key issue in the debate on electronic signatures was whether the regulation of electronic signatures and certification service providers should be done at the European or at national level. Now this question seems to have been resolved by the above-mentioned Communications and Council Resolution.

As noted, from 1997 most Member States were considering legislative actions in the field of electronic and digital signatures. Diverging approaches were emerging among the Member States. The Proposal's Explanatory Memorandum notes several possible discrepancies among legislative initiatives of Member States, including the rules concerning the legal effect attributed to electronic signatures, liability rules applicable to certification service providers, and technical conditions under which electronic signatures would be presumed secure.[20]

As the Proposal's Explanatory Memorandum correctly recognizes, the increasing number of divergent legislative initiatives in the Member States would lead to adoption of an unharmonized legal framework within the European Union. This would create barriers to the growth of electronic commerce and, therefore, endanger the functioning of the Internal Market. For example, if a company in Belgium sold goods to another company in Spain over the Internet, using digital signature technology, and the Belgian courts refused to give legal recognition to the digital signature certified according to Spanish law in an action for payment brought by the Belgian seller against the Spanish buyer, this would hinder both the development of electronic commerce and trade between Member States.

Therefore, the Proposal has as its objective the elimination of these obstacles, "in particular differences concerning the legal recognition of electronic signatures and restriction on the free movement of certification services and products between the Member States". In short, it seems that the Commission has properly identified a threat to the functioning of the Internal Market in an area of vital importance to Europe's economic future, and that the Commission therefore has appropriately employed Articles 57(2), 66 and 100A of the EC Treaty as the legal basis for the Proposal. Moreover, the Commission has respected the principle of subsidiarity by

carefully limiting its Proposal only to those issues that must be harmonized in order to avoid distortions of the Single Market.

BASIC SCOPE AND APPROACH OF THE PROPOSAL

The two main objectives of the Proposal are to establish the legal recognition of electronic signatures and the creation of a legal framework for the establishment and operation of certification service providers.

Legal recognition of electronic signatures

Most European Union Member States have laws requiring written documents and hand-written signatures for purposes such as validity and enforceability of contracts and admissibility and valuation of evidence.[21] Electronic documents and electronic signatures will not always be regarded as fulfilling these requirements, and this lack of legal recognition presents a barrier to the spread of electronic commerce.

Article 1 of the Proposal addresses this issue, noting that the Proposal "aims at facilitating the use of electronic signatures as well as providing for their legal recognition". However, as Article 1 recognizes, the Proposal does not cover aspects related to the conclusion and validity of contracts or other, non-contractual, acts (such as the filing of tax returns). Therefore, Member States are not required to eliminate such formal requirements (including signatures) but to recognize that paper requirements can be fulfilled by electronic means.

This approach seems appropriate because, in order to eliminate obstacles to electronic commerce, it does not appear necessary to eliminate or harmonize formality requirements imposed by Member States as a basis for the validity of contracts or other acts. Moreover, it is important to keep in mind that such matters (e.g. the formalities required for the validity of contracts) generally do not fall within the Commission's competence. Furthermore, formality requirements find their roots in internal legal principles of Member States, and proposing the elimination or modification of such requirements would significantly increase the political difficulties likely to be faced by the Commission in obtaining adoption of its Proposal.

Indeed, proposals requiring changes to Member State formality requirements have been poorly received in the past. For example, in 1981, a Recommendation of the Council of Europe (N° R (81) 20) recommended such changes, as did, in 1985, the Recommendation of the United Nations Commission on International Trade Law.[22] Both recommendations advised countries to eliminate legal requirements of paper documents and hand-written signatures for evidentiary purposes as well as to decrease the value of the contracts requiring formalities. European Union Member States implemented none of these suggestions, on the grounds that the proposed modifications would distort traditional national contract and evidentiary rules, thus having a negative effect in other areas of law. By simply requiring Member States to provide that, under certain circumstances, electronic signatures shall be deemed to satisfy existing requirements for hand-written signatures, the Proposal avoids this legal and political quagmire.

Another wise choice made by the Commission was to adopt a technologically neutral approach to the legal recognition of electronic signatures. The Proposal does not limit the recognition of signatures to those created using a specific type of technology. Indeed, it uses the general expression 'electronic signatures' as opposed to special types of electronic signatures such as digital signatures.

This approach is reflected in Article 2, which contains, inter alia, a definition of 'signature' adopting a *functional approach*, establishing several requirements that must be fulfilled for any signature to qualify as a signature for the purposes of the Proposal. Specifically, the Proposal's definition of an 'electronic signature' is a "signature in digital form in, or attached to, or logically associated with, data and used by a signatory to indicate the signatory's approval of the content of that data". Additionally, to qualify as an electronic signature, any signature must:

- be uniquely linked to the signatory
- be capable of identifying the signatory
- be created using means that the signatory can maintain under his control
- be linked to the data to which it relates in such a manner that it is revealed if the data is subsequently altered

It can be seen that the criteria set forth by Article 2 relate to the traditional functions of hand-written signatures: first, the ability to identify the signatory is reflected in the first two requirements. Second, the capacity of revealing alteration (or integrity) which is attributed (not always rightly) to written documents with a hand-written signature is reflected in the final requirement. However, the above criteria go further than the requirements met by a hand-written signature. Indeed, for example, a hand-written signature can be forged and thus will not necessarily stay within one's control.

The technologically neutral approach allows room for future developments, thus encouraging the growth of new electronic signature techniques and provision of new business opportunities. Moreover, had the Proposal confined the legal recognition of signatures to the current digital signature technology, and one day this technology no longer provided adequate security (for example, because computer capacity rose to the point where it was possible rapidly to discover a private key from the public key), the law would become obsolete.

Contrary to this approach, the Italian legislation on Electronic Documents and Digital Signatures and the German Digital Signature Act are limited to public-key cryptography, i.e. digital signatures. Moreover, the German law requires the satisfaction of very specific standards. This may mean that if the Proposal is adopted in its current form, the German and Italian legislation will need to be adapted to the Proposal. On the other hand, perhaps these laws could remain in place on the following theory: as long as Member States implement laws recognizing all electronic signatures that meet the general requirements set forth by the Directive, they may still enact *specific* rules for digital signatures establishing the criteria such signatures must fulfil to be deemed to meet the Directive's general criteria.

Although the Commission's initiative to ensure the legal recognition of electronic signatures should be welcomed,

one might question whether the Commission should have extended its initiative to electronic *documents* as well. As noted above, most Member States have laws requiring not only hand-written signatures but also 'written documents' as conditions for the validity and enforceability of contracts and admissibility and valuation of evidence. Because there is uncertainty about whether electronic documents will meet these requirements, it might have been wise for the Commission to address this issue as well. This would ensure that electronic documents are given the same recognition as electronic signatures.

Legal framework for certification service providers

The trustworthiness of electronic signatures, and especially digital signatures, depends on the use of third parties, namely so-called certification service providers who provide the necessary assurances of the *identity* of the key holder by issuing certificates binding the public key of the key holder to his identity.[23] Because of the importance of certification service providers to secure electronic commerce and because of the lack of harmonized rules governing certification service providers, it is to be welcomed that the other main area addressed in the Commission's Proposal is the creation of a legal framework for the establishment and operation of certification service providers.

The legal framework for certification service providers established by the Proposal covers two aspects: first, the *establishment* of certification service providers, providing certain basic requirements for those who wish to act as certification service providers; and, second, the *operation* of certification service providers, i.e. the legal and technical requirements that must be fulfilled by the certification service provider when issuing certificates. However, the Proposal's legal framework for the establishment and operation of certification service providers is limited, excluding certain areas from its application.

First, Article 1 of the Proposal is limited to the establishment of a legal framework for certification services made available *to the public*. Moreover, the Proposal's Explanatory Memorandum explicitly indicates that no regulation is needed for closed *environments* such as banking systems and corporate intranets. Instead, certification carried out in closed groups will be based on the principle of contractual freedom, thus enabling parties to agree on the terms and conditions under which they do business.

The significance of this carve-out becomes clear when one considers the size and importance of closed electronic environments that will fall outside the ambit of the Directive, such as those operated between certain large trading parties, between banks (for example, for credit card systems) and by professional organizations (e.g. chambers of lawyers and physicians). However, although the deference given by the Proposal to the principle of contractual freedom in the context of closed systems seems appropriate, one might wonder whether those operating closed systems, while not required to do so, might have incentives to comply with the rules established by the Directive. In particular, those groups (especially within the banking sector) may have an interest in complying with the legal requirements laid down by the Proposal in order to benefit from the recognition accorded to electronic signatures under it.

The availability of the legal recognition provided by the Proposal to electronic signatures based upon qualified certificates (see below) would appear to be especially important insofar as courts may not allow contracting parties to decide for themselves on the admissibility and weight of evidence. Indeed, some courts might well say that this falls within their exclusive competence,[24] and deny the effectiveness of agreements between electronic trading parties providing that electronic signatures shall have the same force of evidence as hand-written ones.

Of course, this raises the question whether parties employing electronic signatures in closed networks would be *entitled* to rely on the regime established by the Proposal. Unless they can do so, they might be left 'out in the cold' — without the benefit either of contractual solutions or of the Proposal. Insofar as the Proposal is limited, in Article 1, to establishing a legal regime for certification services 'made available to the public',[25] it might be argued that trading parties operating in closed environments may not rely on the benefits of the regime to be established by the directive. However, this would be an unfortunate result; while it is appropriate to provide contractual freedom to those operating in closed networks, it would seem wise to allow them to take advantage of the directive's regime if they see fit. Perhaps the Proposal should, as it makes its way through the legislative process, be clarified in this regard. Alternatively, the Directive might provide that courts must accept agreements between parties operating in closed environments about the admissibility and weight of electronic documents and signatures.

The second main way in which the Proposal's legal framework for the establishment and operation of certification service providers is limited is that it is intended to cover only one type of certificate, namely a digital attestation that links a signature verification device to a person, confirming the *identity* of that person. Indeed, the Explanatory Memorandum explicitly recognizes that the Proposal focuses uniquely on the function of a certificate as a linkage to the civil identity or the role of a person: "[T]he legal framework is needed for certificates to enable the authentication of the electronic signature of a signing individual."

However, as Article 2 of the Proposal points out, "certification services provide other services related to electronic signatures to the public". For instance, in addition to certifying the link between a particular signature and the identity of its holder, some certification service providers certify *qualities* of the signature holder (e.g. membership of a bar specialized in a particular legal area or compliance of a Web site operator with privacy laws).[26] The option taken by the Commission means that such certification services will fall outside the scope of the Directive.[27] This seems appropriate, and the Proposal's failure to address the legal effect of non-identity certificates would not seem to present any significant barrier to electronic commerce.

We now proceed to a more detailed analysis of the Proposal. Because the rules on the legal effects of electronic signatures follow largely from the regime governing the establishment and operation of certification service providers, we turn first to a discussion of that regime.

ANALYSIS OF THE PROPOSAL

The Regime Governing the Establishment and Operation of Certification Service Providers

The Licensing Debate

One of the key questions when drafting the Proposal was whether certification authorities would have to be licensed to be permitted to act as such. Article 3 of the Proposal answers this question by providing that "Member States shall not make the provision of certification services subject to prior authorization." However, Article 3.2 permits Member States to "introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification service provision".[28]

From the formulation of Article 3, the following can be deduced:

- First, certification services may be offered without prior authorization, i.e., anyone is free to offer certification services.
- Second, EU Member States would keep the *option* of setting up voluntary accreditation schemes for service providers for enhanced levels of security. (Such schemes could require the fulfilment of certain conditions in order to achieve high levels of security.The basis for maintaining voluntary accreditation schemes may be found in the need for high level services among very specific groups such as notaries and physicians and the need even among the general public for high level services in certain circumstances.)
- Third, with respect to such voluntary accreditation schemes, Member States must ensure that all conditions related to such schemes are "objective, transparent, proportionate and non-discriminatory". (This is the standard commonly imposed by EU legislation to ensure the proper functioning of the Internal Market.)
- Fourth, in operating voluntary accreditation schemes, Member States may not limit the number of certification service providers.

In opting for the 'voluntary' approach, the Commission appears to have followed the path employed in the German Digital Signature Law, although the German law's actual wording leaves some doubt about whether it establishes a mandatory licensing scheme. The Italian law is also somewhat unclear on this point: although an aspiring certification service provider must apply to the Autorita'per l'informatica nella Pubblica Amministrazione (AIPA) before beginning operations and prove that it fulfils the requirements defined by the law, the AIPA appears to have no ability to prevent the applicant from beginning operations and no licence is issued by the AIPA. Finally, the UK Government, in its "Secure Electronic Statement" issued in May 1998, abandoned the suggestion for a mandatory licensing system made earlier in its *Public Consultation Paper on Proposal for Legislation on Trusted Third Parties*[29] and now proposes a voluntary licensing scheme.[30]

Although conditions established by Member State accreditation schemes must be "objective, transparent, proportionate and non-discriminatory", the Proposal does not specify the requirements that may be employed as the basis for accreditation. However, as discussed further below, the Proposal does contain an annex (Annex II) that sets forth conditions that must be met by certification service providers in order for electronic signatures based on their certificates to be accorded certain legal benefits.[31] The availability of these legal benefits will give certification service providers an incentive to comply with Annex II, and it seems likely that the criteria contained in Annex II will be employed by Member States in their voluntary accreditation schemes.[32]

Presumably in order to permit the Commission to monitor whether Member State accreditation schemes meet the requirements established by Article 3 (and in particular the objectivity, transparency, proportionality and non-discriminatory conditions), Article 10 of the Proposal requires Member States regularly to provide information to the Commission about their accreditation schemes.

The 'voluntary' approach is a good one: permitting companies to provide certification services without authorization, and allowing accreditation schemes for those entities providing high standards of security, will permit desirable flexibility and limit the costs of certification services not requiring high levels of security. In addition, the absence of strict technical requirements and licensing obligations applicable to all certification service providers will allow smaller actors with limited resources to provide certification services.

Overall, this approach should encourage the development and competitiveness of the certification services market, benefiting both consumers and certification providers. Consumers will also benefit from the fact that in operating voluntary accreditation schemes, Member States may not limit competition by restricting the number of certification service providers.

The Issuance of Certificates

Qualified versus non-qualified certificates

The Proposal differentiates between two types of certificates: *qualified* certificates and *non-qualified* certificates. Article 2.5 defines the former as follows: "a digital attestation which links a signature verification device to a person, confirms the identity of that person and meets the requirements laid down in Annex I". In other words, a qualified certificate is an *identity certificate* that fulfils the requirements of Annex I.

Annex I provides that a qualified certificate must contain, inter alia:

- the identifier of the certification service provider issuing it
- the 'unmistakable' name of the holder of the certificate or an 'unmistakable' pseudonym that shall be identified as such
- a specific attribute of the certificate holder such as his address, authority to act on behalf of a company, credit worthiness, VAT or other tax registration numbers
- a signature verification device corresponding to a signature creation device under the control of the holder
- the operational period of the certificate
- any limitations on the scope of use of the certificate
- any limitations on the service provider's liability or on the value of transactions for which the certificate is valid

Non-qualified certificates are not defined. Presumably, they include all certificates that do not fulfil the conditions to be a qualified certificate. In other words, non-qualified certificates include (1) all *non-identity* certificates and (2) identity certificates *not meeting the requirements of Annex I.*

The capability to issue qualified certificates does not depend on whether the certification service provider is accredited, or whether it meets the requirements in *Annex II.* On the contrary, it follows from the Proposal that *any* certification service provider can issue qualified certificates.

However, as discussed further below, a qualified certificate will enjoy certain legal benefits, including automatic evidentiary admissibility and treatment equivalent to hand-written signatures, *only* if it is issued by a certification service provider meeting the requirements of Annex II. Because these legal benefits are of considerable importance (indeed they are central to the legal recognition accorded to electronic signatures by the Proposal), users will have a powerful incentive, in many cases, to obtain qualified certificates from service providers meeting the requirements of Annex II — and certification service providers therefore will have a strong incentive to comply with Annex II.

Of course, certification service providers, even those meeting the requirements of Annex II, will surely continue to offer a range of certification products; they will issue not only qualified certificates, but also often non-qualified certificates. Among these non-qualified certificates will be not only *non-identity* certificates (which by their nature will be non-qualified certificates), but also *identity* certificates that provide less security (e.g. so-called level 0 certificates) and that do not constitute qualified certificates because they do not meet the requirements of Annex I. For example, to obtain such low-security certificates one need not provide any document demonstrating one's identity. Such certificates are satisfactory for use in connection with relatively unimportant transactions, for example, where it is not cost-effective to invest in a high degree of security.

The question of legal persons

One issue that has generated surprising controversy in some countries has been whether certificates granted to legal persons should enjoy the same legal benefits as certificates issued to natural persons. Insofar as Article 2.5 of the Proposal defines 'qualified certificates' as those verifying the identity of 'a person', without making any distinction between physical and legal persons, one might conclude that not only certificates issued to physical persons but to legal persons will be eligible for the legal recognition guaranteed by the Proposal. Although Annex I(c) includes among attributes that *may* be contained in a certificate "the authority to act on behalf of a company", the Annex does not *require* such an attribute to be contained in any certificate. Therefore, it would seem wrong to infer that Annex I(c) somehow excludes certificates issued to legal persons from the Proposal's coverage.

In our view, certificates should be allowed to link signatures not only to the identity of physical persons but also to that of legal persons, and certificates issued to legal persons should be entitled to the same legal benefits as those issued to physical persons. It should be left to companies to decide whether to use one or the other: we can see no way in which the availability of corporate identity certificates could disadvantage any third party, and companies therefore should be left to themselves to decide whether they wish to accept the risk of being bound by non-identified persons.

If, for example, a corporation chooses to obtain a certificate in the name of the corporation, and it then permits corporate personnel to employ this certificate and to issue digital signatures directly on behalf of the corporation, the law should fully recognize the validity of such signatures. The corporation should be allowed to decide for itself whether it wishes to run the risk that it will become liable for use of the corporation's certified signature by employees for unauthorized purposes — and that the corporation will not be able to identify the physical person (whether an unauthorized employee or a thief) because the certificate identifies only the corporation. Perhaps the corporation's choice would be based on the technology used; for example, in the context of EDI, where contracting occurs between computers rather than actual persons, it would seem rather anomalous for signatures to identify physical rather than legal persons.

Moreover, it should be taken into account that if qualified certificates may not identify legal persons, companies that wish to use this type of certificate will need to use non-qualified certificates, with resulting disadvantages for public confidence.

Division of service provider roles

Service providers must fill various roles. For example, service provider functions include the technical functions of generating key-sets, maintaining a certificate revocation database, and issuing certificates. In addition, service providers must fulfil a registration function — before issuing certificates, certification service providers must obtain and verify certain information. For instance, the certification service provider may need to ascertain and verify the name of the holder and attributes such as address, authority to act on behalf of a company, and tax registration numbers.

So far, companies offering certification services have tended to be companies with technical expertise, and it may be more efficient and effective for them to contract out to others non-technical tasks such as registration. In our view, it should be permissible for different actors to share the different roles service providers must fulfil. Allowing such a division of roles may be the only way to enable small certification service providers, who for example may not have sufficient resources to maintain a 24-hour database of revoked certificates, to be in the market and compete with larger companies.

The Proposal does not address the legality of such division of roles. In principle, nothing would seem to prevent such arrangements, although questions might arise about who bears liability among the different actors. Presumably, the actual issuer of the certificate will be liable under the rules established by the Proposal, although a party to whom the registration function has been assigned might ultimately be held liable for failure properly to carry out the registration function.

Liability of certification service providers

One of the main areas of discussion with respect to the legal regime governing certification service providers is the

scope of service provider liability. To take just one example, should service providers be strictly liable for issuing certificates containing inaccurate information about the identity of the certificate holder, or should some other liability standard apply?

The Proposal addresses this issue in Article 6, but it establishes a set of rules on liability that apply only when the service provider (whether accredited or not) issues *qualified* certificates. Thus, when a certification service provider issues *non-qualified* certificates, it presumably will be subject to general liability rules under national law. Thus, the issuance, for example, of non-identity certificates would not be subject to the Proposal's liability regime.

For qualified certificates, the Proposal establishes the following liability regime: first, it seems that the regime governs liability only between certification service providers and third parties. This conclusion appears to follow from the introductory sentence to Article 6 of the Proposal, which addresses only a service provider's liability to "any person who reasonably *relies* on the certificate". Moreover, the items identified in Article 6 with respect to which certification service providers may incur liability appear to apply only to third parties who rely upon certificates, and not to *certificate holders*. Therefore, it seems that the Proposal does not address the scope of service provider liability to certificate holders. Moreover, it would seem to follow that service providers may contractually exclude any liability to certificate holders, except to the extent this ability is limited by other laws such as consumer protection laws.

Second, vis-à-vis third parties who 'reasonably rely' on a qualified certificate, service providers are liable for the following:

a) the accuracy of all information in the certificate as of the date it was issued, unless the certification service provider has stated otherwise in the certificate[33]
b) compliance with all requirements of the Directive in issuing the certificate
c) assurance that the holder identified in the qualified certificate held, at the time of the issuance of the certificate, the signature creation device corresponding to the signature verification device given or identified in the certificate
d) assurance that the signature creation device and the signature verification device function together in a complementary manner, in the cases where the certification service provider generates the devices[34]

Third, although Article 6 requires Member States to ensure that a service provider 'is liable' to reasonably relying third parties for the items listed above, it is not very clear what standard should apply to imposing such liability. In particular, is this article intended to impose a strict liability standard? Only by reading Article 6.1 in conjunction with Article 6.2 might one conclude that a strict liability standard seems to be intended.

Specifically, in Article 6.2, the Proposal provides that a service provider shall *not* be liable "for errors in the information in the qualified certificate that has been provided by the person to whom the certificate is issued, *if it can demonstrate that it has taken all reasonably practicable measures to verify that information* [emphasis added]". Insofar as the service provider could avoid liability only by making this demonstration, it would appear that the *general* liability standard is not one of a duty of care, but rather one of strict liability. Moreover, insofar as Article 6 provides for the possibility to avoid liability essentially by demonstrating compliance with a duty of reasonable care *only* with respect to errors resulting from information provided by certificate holders — and not with respect to the other items for which liability might be imposed under Articles 6.1 (b), (c), and (d) — it would seem that the liability regime applicable to these latter items is one of strict liability.

Thus, in effect the Proposal seems to establish a two-tiered set of liability criteria. Even if the Proposal seeks to establish a strict liability standard for the items listed in Article 6.1 (b), (c), and (d), this standard is tempered with respect to Article 6.1 (a). For the accuracy of information contained in a qualified certificate (at least to the extent that information has been provided by the certificate holder), the Proposal establishes essentially a with-fault liability regime.

Assuming the above interpretation of Article 6 is correct, and in general a strict liability regime is intended, it would have been preferable for the Proposal to have expressed this point more clearly.

Apart from establishing the above-described general liability scheme, Article 6 sets forth two ways in which a certification service provider may limit its liability to third parties. First, it may indicate in the certificate certain limits on its use. If the certificate is used 'contrary' to these limits, the service provider shall not be liable. Second, the service provider may indicate in the certificate a limit on the value of transactions for which the certificate is valid, and it will not be liable for damages to third parties beyond that limit.

With respect to such limitations, the Proposal answers one of the questions with respect to which controversy has existed, namely whether such limitations (1) must be contained in the certificate or (2) may be contained in separate document and addressed only by reference in the certificate itself. In a move that is favourable to consumer protection, the Proposal requires limitations to be contained in the certificate itself.

In addition, Article 6.5 recognizes the continued applicability of the Directive 93/13/EC on unfair terms in consumer contracts. This would seem to mean, for instance, that certain limits will exist upon certification service providers' ability to include liability exclusions in their contracts with certificate holders — at least where the certificate holders are consumers.

Finally, one highly important issue related to the liability of certification service providers that is not addressed by the Proposal is the question of liability for failure to maintain an accurate database of revoked certificates. As noted above, in order to establish a trustworthy framework for digital signatures, it is necessary to establish a trustworthy database maintaining an up-to-date list of valid certificates (so that trading parties can have the requisite confidence that the certificate holder's private key has not been compromised during the time between the certificate was issued and the moment it is actually used).[35] Because severe damage can be caused to third parties who rely on an inaccurate database for the conclusion that a certificate remains valid when in fact it is not, it is surprising that the Proposal fails to address this issue.

Legal Effects of Electronic Signatures

Electronic signatures cannot play their proper role in facilitating electronic commerce unless they are legally recognized. Article 5 of the Proposal aims to provide legal recognition to electronic signatures in the same way as their paper counterparts.

Article 5 is divided into two parts. First, Article 5.1 relates to electronic signatures *generally*, and Article 5.2 accords special benefits only to *qualified* certificates *issued by service providers complying with Annex II.*

With respect to electronic signatures generally, Article 5.1 provides that electronic signatures shall not be denied legal effect, validity and enforceability *solely* on the following three grounds:

- the fact that the signature is in electronic form
- the fact that the signature is not based on a qualified certificate
- the fact that the signature is not based upon a certificate issued by an accredited service provider

The formulation of Article 5.1 is significant not only for what it does say, but also for what it does not. Article 5.1 does provide that an electronic signature *shall not be denied* legal effect, validity or enforceability on the above grounds. But Article 5.1 does *not* say that *any* electronic signature automatically will be accorded such benefits. Presumably, then, it would remain up to the person who seeks to rely upon a particular signature not qualifying for special benefits under Article 5.2 to demonstrate that it meets some general requirements of reliability in order to qualify for legal recognition. In addition, Member States presumably remain free to establish certain criteria that will be employed by the courts to determine whether electronic signatures not qualifying for special treatment under Article 5.2 will be accorded legal recognition.

Unlike Article 5.1, which merely provides that electronic signatures shall not be denied legal effect, validity or enforceability on certain grounds, Article 5.2 affirmatively requires Member States to accord certain legal recognition to electronic signatures if they: (1) are based on a qualified certificate and (2) the certificate has been issued by a service provider meeting the requirements of Annex II.

Compliance with Annex II is of course intended to ensure the reliability of the certification service provider. To comply with Annex II, service providers must, inter alia, operate a prompt and secure revocation service; employ personnel possessing certain expert knowledge, experience, and qualifications; use certain trustworthy systems and products; and maintain sufficient financial resources.

Electronic signatures meeting the requirements of Article 5.2 must be accorded two legal benefits:

- assurance that they satisfy the legal requirement of a hand-written signature
- admissibility as evidence in legal proceedings in the same manner as hand-written signatures

The formulation of Article 5 gives rise to several questions. First, why is there a difference between the legal benefits that may not be denied on the grounds specified in Article 5.1 and the legal benefits that must be accorded to certain signatures under Article 5.2?

Article 5.1 provides that an electronic signature may not be denied *'legal effect, validity and enforceability'*, whereas Article 5.2 requires certain electronic signatures to be deemed (1) to satisfy the legal requirement of a hand-written signature and (2) to be admissible as evidence to the same extent as a hand-written signature. Apart from the fact that it is rather unusual to speak of the 'enforceability' of a *signature* (whether hand-written or electronic), do the two legal benefits that must be accorded under Article 5.2 fall within the terms 'legal effect and validity'? For example, would denial of the *admissibility* of an electronic signature as evidence constitute a denial of the signature's *legal effect, validity or enforceability*? The answer to this question does not seem clear. If the answer is "no", then apparently courts may deny that electronic signatures satisfy the legal requirement of a hand-written signature and deny their admissibility as evidence based solely on the fact that they are in electronic form or that they are not based on a qualified certificate issued by an accredited service provider. In any event, it would be helpful for this issue to be clarified.

Second, how will a person seeking to rely upon an electronic signature demonstrate in a given case that the issuing certification service provider fulfils the requirements of Annex II? If such a person must submit substantial evidence about the certification service provider to make this demonstration, the benefits of Article 5.2 are likely in practice to be rather ephemeral.

In light of the difficulties individual certificate holders would appear to face in demonstrating on their own in individual lawsuits that the service provider that issued a particular certificate met the requirements of Annex II, perhaps the most likely result is the following: Member States will develop voluntary accreditation schemes linked to the requirements of Annex II, and courts will rely on accreditations issued under such schemes to conclude that the requirements of Annex II are met for purposes of Article 5.2 of the Proposal.

Insofar as users would thus have a great incentive to obtain qualified certificates only from accredited service providers, one could legitimately ask how 'voluntary' such an accreditation scheme would be in practice. In the end, it seems likely that nearly all service providers issuing qualified certificates will effectively be forced to become accredited, and that accreditation schemes will be linked to Annex II.

Third, what is the regime applicable to the legal recognition of electronic signatures in public documents? When the law requires a hand-written signature before a notary, would an electronic signature fulfilling all the requirements established by the Proposal be valid? Insofar as Article 5.2 of the Proposal says generally that "electronic signatures ... based on a qualified certificate issued by a certification service provider ... fulfilling the requirements set out in Annex II ... satisfy the legal requirement of a hand-written signatures", a literal interpretation would seem to include all types of signatures, both ones contained in private documents and those done before a notary.

International Recognition

Given the global nature of electronic commerce, the cross-border recognition of electronic certificates and signatures is a key issue. Article 4 of the Proposal addresses this question among the EU Member States, and Article 7 deals with the issue of EU recognition of electronic certificates and

signatures issued by certification service providers established in third countries.

Article 4 of the Proposal guarantees the free circulation and non-discriminatory treatment of electronic signature services and products within the European Union. In particular, "Member States may not restrict the provision of certification services that originate in another Member State in the fields covered by [the] Directive" and they are obligated to ensure that "electronic signature products which comply with [the] Directive are permitted to circulate freely in the Internal Market". Thus, for example, a German court must accord the benefits guaranteed by Article 5.2 to an electronic signature based on a qualified certificate issued by a service provider in Spain that fulfils the requirements of Annex II. (Presumably the German court would also have to accord equal weight to a voluntary accreditation issued in Spain confirming compliance with Annex II.)

Concerning certificates issued in third countries, Article 7 of the Proposal requires Member States to treat such certificates as legally equivalent to those issued by an EU-based service provider under the following three circumstances:

- if the certification service provider fulfils the requirements laid down in the Directive and has been accredited in the context of a voluntary accreditation scheme established by a Member State of the European Community
- if a certification service provider established within the European Community that fulfils the requirements laid down in Annex II guarantees the certificate, to the same extent as for its own certificates
- if the certificate or the certification service provider is recognized under the regime of a bilateral or multilateral agreement between the European Community and third countries or international organizations

As one respected commentator has noted, the second method of recognizing non-EU certificates provided for in Article 7 is especially interesting, "as it provides another method of international recognition in addition to the more conventional methods of accreditation in the forum or by international treaty .... In practice, this option will most likely be used not so much by foreign certification authorities contracting with an EU [service provider], but by the subsidiaries of multinational companies already active in the EU themselves becoming accredited and then guaranteeing the certificates of their non-EU associated entities."[36]

CONCLUSION

Despite a lack of clarity in several significant respects, the Proposal is to be welcomed. The existing uncertainty in the European Union regarding the legal recognition of electronic signatures and the rules governing the establishment and operation of certification service providers is a significant obstacle to the development of electronic commerce, and the Proposal goes a long way towards eliminating this uncertainty and creating a level playing field throughout the European Union and beyond.

The Commission should be congratulated, among other things, for adopting a consumer-friendly yet flexible, technologically neutral approach, emphasizing a voluntary regime for certification service provider accreditation, and acknowledging the need for smooth cross-border recognition of electronic signatures not only within the European Union but with third countries as well.

As the Council of Ministers and the European Parliament now address the Proposal, they should consider adopting amendments to address the issues raised above, in particular with respect to the formulation of the liability regime and the rules governing the legal recognition of electronic signatures. With some clarifications on these and a few other points, the ultimate Directive could become one of the key paving stones on the way towards a thriving electronic commerce in Europe.

Footnotes

[1]**Rosa Juliá-Barceló** is researcher at the Centre de Recherches Informatique et Droit, 59 Rempart de la Vierge, Namur, Belgium, E-mail: rosa.julia@fundp.ac.be **Thomas Vinje,** Report Correspondent is managing partner of the Morrison & Foerster LLP Brussels office and a Report correspondent. Morrison & Foerster LLP, Avenue Molière 262, B-1180 Brussels, Belgium.

[2]"Proposal for a European Parliament and Council Directive on a common framework for electronic signatures". COM (1998) 297 final.

[3]The EDI Model Agreement approved by the Commission in December 1994 defines EDI as follows: "the electronic transfer from computer to computer of commercial or administrative transactions using an agreed standard to structure the transaction or message data".

[4]The TEDIS Programme was launched in two phases. The initial one started in 1988 and finished in 1989. The second phase started in 1991 and lasted until the end of 1994. The general objective of the programme was promoting the use of EDI in Europe. Among the relevant legal aspects, from the beginning it became clear that the existing legal requirements for paper documents and hand-written signed documents as well as the legal constraints on evidence constituted a real challenge for EDI. For a survey of the legal issues of EDI considered in the TEDIS programme see: Troye, A., The development of legal issues of EDI under the European Union-TEDIS programme, *The EDI Law Review*, Vol. 1, No. 3, 1994, pp. 195-222.

[5]See for instance: TEDIS- EDI Trusted Third Parties Workshop, Barcelona, 8-10 February 1995; TEDIS II- Service Infrastructure for EDI Security, 1993; TEDIS II- Security in Open Environments, 1992; The TEDIS-EDI security workshop, Security in a multi-owner system, Brussels, 20-21 June, 1989. See also the Green paper entitled "*Green Paper on the Security of Information Systems*" prepared by DG XIII but never published.

[6]The following programmes contained several projects in the field of electronic and digital signatures: Information Technology Program; Standardization and the Information Society; Acts Program, Projects on Security of Security of Telecommunications and Information Systems, Projects in the European Trusted Services Programs.

[7]For several overviews of State Government Electronic and Digital Signatures Legislation see: http://www.magnet.state.ma.us/itd/legal/pollaw/htm. See also MacBride Baker

Coles site at http://www.mbc.com/ds_sum.html.

[8]In addition, note other federal legislative initiatives such as the Baker Bill, the so-called Eshoo Bill (for transactions involving federal government entities) and the Banking Initiative (for digital authentication within the banking industry). Finally, concerning standards, the National Institute of Standards and Technology (NIST) has published its Draft Certificate Policy imposing certain technical, operational and liability requirements on certification service providers whose certificates will be relied upon by Federal Government entities.

[9]The report was prepared by the Information Security Committee of the Electronic Commerce Division.

[10]See the following reports of the Working Group on Electronic Commerce A/CN.9/WP.IV/WP.71, A/CN.9/WP.IV/WP.73, A/CN.9/WP.IV/WP.76, A/CN.9/WP.IV/WP.77. See also A/CN.9/437, A/CN.9/446.

[11]See General Usage for International Digitally Ensured Commerce, at p. 4.

[12]COM (97) 157 final, (16.4.97).

[13]Ministerial Declaration "Global Information Network: Realising the Potential", Bonn, 6-8 July 1997.

[14]COM (97) 503.

[15]For an analysis of this Communication see Julia-Barcelo, R.; Vinje, T., "Towards a European Framework for Digital Signatures and Encryption. The European Commission Takes a Step Forward for Confidential and Secure Electronic Transactions", [1998] 14 *Computer Law & Security Report*, pp. 79-85.

[16]See Explanatory Memorandum, which contains, at pages 4-5, a useful summary of Member State initiatives in this area.

[17]The Digital Signature Law (DSA) is part of the "Federal Act Establishing the General Conditions for Information and Communication Services". An Ordinance containing the legal provisions for the implementation of DSA articles was adopted on 1 November 1997. For a comment on the German Digital Signature Law, see: Julia Barcelo, R., The German Legal Situation after the "Digital Signature Law", *Droit de l'Informatique et des Télécoms*, 1, 1998, pp. 77-79.

[18]The Law No. 59 of 15 March 1997 entitled "Delegation to the Government for the transfer of tasks and functions to Regions and local authorities, for the reform of the Public administration, and to simplify administrative procedures" published in *Supplemento Ordinario to Gazetta Ufficiale*, No. 63, 17 March 1997 contains a delegation of power to reform public administration. This law was followed by the Presidential Decree of 10 November 1997, No. 513 "Regulation on criteria and methods of application Article 15 (2) of Law No. 59 of 15 March 1997 concerning the creation, storage and transmission of documents by means of computer-based or telematic systems, published in *Gazette Ufficiale* 13.3.1998, No. 60.

[19]The Council Resolution was issued on 1December 1997.

[20]See Explanatory Memorandum at 5 (need for harmonization).

[21]For example, Article 1341 of both Belgian Civil Code and French Civil Code require written evidence when the value of the contract (for example, a sales contract) is beyond a certain limit. Furthermore, certain copyright laws require copyright licences to be entered in a written form with hand-written signatures. For further details on formal requirements within the EU Member States see: Lamberterie, I., La valeur probatoire des documents informatiques dans les pays de la CEE, Revue *Internationale de Droit Comparé*, No. 3, 1992, pp. 641-685.

[22](A/40/17), Supp. 17.

[23]For a description of digital signatures and public key cryptography, see Julia-Barcelo/Vinje, supra No. 15, pp. 2-3.

[24]This is especially true in Germany. See Blechschmidt, R., The German Basic Electronic Data Interchange Agreement Versus the European Model EDI Agreement: Some Reflections on German Law, *The EDI Law Review*, No. 3, 1996, pp. 107-124 and Hoeren, T., An Assessment of Long-Term Solutions for Copyright and Multimedia products, European Commission, DG XIII, EUR 16069, 1995. See as well Van Esch, R., Statute of Frauds and EDI, *The EDI Law Review*, No. 3, 1996, pp. 81-84. On the contrary, contracting out of the requirement for hand-written signatures and documents has been regarded as valid in France and Belgium. For further considerations on this issue, see Bensoussan, A., La convention sur la preuve dans les accords d'interchange, *Cahiers Lamy droit de l'informatique*, Supplement au No. 50, 1993, pp. 2-6; Boizard, M., Preuve des payements par cartes bancaires et signature informatique, Cahiers *Lamy Droit de l'Informatique*, N I, 1988, Paris, pp. 7-12.

[25]See also Recital 10 of the Proposal and paragraph 3 of the Explanatory Memorandum, which say, perhaps misleadingly, that a regulatory framework is not needed for electronic signatures exclusively used within closed systems.

[26]We can find in the market several initiatives such as Webtrust or the initiative of the International Chamber of Commerce that provide a certification mark that ensures the Web site meets certain legal requirements (e.g. business practice disclosures, integrity of transactions).

[27]Of course, if a certification service provider provides both services, as will often be the case, the service provider itself will not fall outside the Directive, but rather only the service of certifying qualities.

[28]Article 3.4 permits Member States to "make the use of electronic signatures in [the] public sector subject to *additional* requirements", although such requirements shall themselves also be "objective, transparent, proportionate, and non-discriminatory, and shall only relate to the specific characteristics of the application concerned (emphasis added)". This provision is difficult to comprehend. Does it mean, for example, that Member States may require the use of electronic signatures that have been certified by *accredited* service providers in the public sector (e.g. in connection with the filing of tax returns)? Or does it mean that in the public sector Member States may require the use of electronic signatures that have been certified by service providers meeting a standard higher than that established by Annex II? The latter interpretation might meet the concerns of the German government, which has been planning large-scale programmes requiring compliance with the strict standards adopted in the German Digital Signature Law. See C. Kuner, "The Emerging European Framework for Digital Signatures", *BNA Electronic Commerce and Law Report*, 27 May 1998. In any event, it would seem appropriate for Article 3.4 of the proposal to be reformulated so its meaning is clear.

[29]Department of Trade and Industry, Public Consultation

Paper on Detailed Proposals for Legislation "Licensing of Trusted Third Parties for the Provision of Encryption Services, March 1997.

[30]Department of Trade and Industry, *Secure Electronic Commerce Statement*, 27 April 1998. Available at http://www.dti.gov.uk/CII/ana27p.html.

[31]For example, Annex II requires certification service providers to operate a prompt and secure certificate revocation service, to employ personnel with particular expertise, and to maintain sufficient financial resources.

[32]Article 9 of the Proposal provides for a consultative committee composed of Member State representatives that will advise the Commission on, *inter alia*, the requirements laid down in Annex II. It can be hoped that the operation of this committee will, at least informally, lead to a high level of consistency in the application of Annex II and the criteria employed by Member States in their voluntary accreditation schemes.

[33]This formulation of Article 6.1 (a) is unsatisfactory. Specifically, it is not at all clear precisely what the service provider might 'state otherwise' in the certificate, and thus for *what* the service provider might escape liability by so stating. Does this phrase in Article 6.1 (a) mean that a service provider may exculpate itself from liability vis-à-vis third parties for inaccuracies in the information contained in the certificate if it states in the certificate that it shall not have such liability? If this is not what this provision means, it is unclear what else it might mean.

[34]Proposal, Article 6.1.

[35]In this context, it should be noted that point (b) of Annex II explicitly requires a "prompt and secure revocation service".

[36]Kuner, supra note 28, p. 715.

Book Review

Multimedia

Adapting the EU Regulatory Framework to the Developing Multimedia Environment — A Study for the European Commission (DGXIII), three volumes plus summary report, 1998, soft-cover, Squire, Sanders & Dempsey

This study, which does not have an ISBN reference, was prepared for the DGXIII of the European Commission by Squire, Sanders & Dempsey LLP and Analysis Ltd in fulfilment of a Commission contract. The work is divided into four volumes — a summary report, a main report, and two annexes. These documents present an analysis of the legal and regulatory issues surrounding the development of a multimedia market in the European Union. The context is the Internet, which has enhanced the visibility of the multimedia market within the European Union and the United States. Estimates of the number of Internet users worldwide vary from 35-60 million, and the Internet market, including networks and services, may be worth 10 billion ECU by the year 2000. Digital broadcasting has also been launched, with many players now exploring the delivery of multimedia services over digital broadcast networks. Chapter 1 of the study provides an overview of the current market sectors that will comprise the future multimedia market. Chapter 2 builds on the information presented in the earlier sections, providing additional supporting evidence. In particular, it examines the key medium term developments in market structure, pricing and standardization. This discussion also addresses regulatory problems that could arise as players seek to build market share in the new markets. The third section reviews the evolution of multimedia markets in terms of a series of key regulatory themes, ranging from pricing practices to public service goals. It also reviews an alternative regulatory model, which reflects the market realities of convergence in the light of the distinctive regulatory traditions of the Member States. Section four seeks to synthesise the previous discussion into a set of options and recommendations for adapting the telecoms regulatory framework within the European Union to a future multimedia market. The fifth section, which is Annex 1 of the study, offers a comparative overview of the current legal framework governing key regulatory issues affecting multimedia in each of the Member States (current to 1 October 1997). It examines how barriers are breaking down between the hitherto separate sectors of telecoms and broadcasting and identifies variations in achievement of multimedia companies across the European Union in terms of market entry and operation. The final part, which is Annex 2 of the study, offers a detailed review of the Member States' laws relevant to convergence issues and regulatory governance in a multimedia environment.

Further information from: Squires, Sanders and Dempsey LLP, Brussels Office, Avenue Louise 165, B-1050, Brussels, Belguim; tel: +32 2 627 11 11 or fax: +32 2 627 11 00; Internet: www.ssd.com.