Proposal for a directive establishing a common framework for electronic signatures

Julia, Rosa

Published in:
Electronic commerce : opening up new opportunities for business

Publication date:
1998

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

Electronic Commerce: Opening Up New Opportunities for Business
Paul Timmers, Brian Stanford-Smith & Paul T. Kidd (Eds.), 1998

Proposal for a Directive Establishing a Common Framework for Electronic Signatures: An Overview

Rosa JULIA-BARCELO
Centre de Recherches Informatique et Droit
Rempart de la Vierge, 5, 5000-Namur, Belgium
Tel: + 3281725205; Fax: + 3281725202;
E-mail: rosa.julia@fundp.ac.be

Abstract. The growth of electronic commerce, and opportunities for SMEs to play a role in electronic commerce, depends on the ability of electronic messages to be secure. The need for security exists in a great variety of electronic communications, including in particular electronic contracts (both business-to-business and business-to-consumer). The main technological tools for ensuring confidentiality and security of electronic communications are digital signature methods. This paper analyses the European Commission's Proposal for electronic signatures issued on 13 May 1998, including critical questions concerning the legal recognition of electronic signatures, the regime governing the establishment and operation of certification authorities, and the liability rules governing the activities of certification authorities.

1. Introduction

The use of an open network such as the Internet reduces costs and increases the playing field for small and medium sized businesses, allowing them to reach a broader number of consumers and business partners. However, these opportunities for SMEs depend on the ability of electronic contracting parties to identify themselves to one another (this is often referred to as *authentication*). Moreover, when a consumer orders a product from a website, both the consumer and the company which owns the web site should be able to sign the contract electronically so they have certainty that the agreed content of the messages is the same that actually was sent (this is referred to as *integrity* of the data).

At the moment, several methods are available to fulfil authentication and integrity needs. Nevertheless, one type of electronic signature, the so-called digital signature technology based on public key cryptography, is regarded as the most reliable technique. For digital signatures to achieve authenticity functions, it is necessary to use a third party who will provide information concerning the identity and qualities of the parties (referred to as a certification authority).

On 13 May 1998, the Commission presented a Proposal for a directive aimed at establishing a legal framework for electronic signatures and certification authorities in Europe[1] (hereinafter "the Proposal")[2]. This article will provide a brief description and analysis of the main issues of the Proposal.

2. Scope of the Proposal

The two main objectives of the Proposal are the legal recognition of electronic signatures and the creation of a legal framework for the creation and functioning of certification authorities.

2.1. Legal Recognition of Electronic Signatures

Most European Union States have laws which require written documents and hand-written signatures for different purposes such as validity and enforceability of contracts and evidence[3]. Since electronic documents and electronic signatures will not always be regarded as fulfilling these requirements, their existence risks inhibiting the spread of electronic commerce.

Article 1 of the Proposal intends to solve this problem by establishing that it "[....] aims at facilitating the use of electronic signatures as well as providing for their legal recognition". Therefore, the Proposal intends to achieve the legal recognition of electronic signatures.

However, as Article 1 explicitly recognises, the Proposal does not cover aspects related to the conclusion and validity of contracts or other non-contractual formalities requiring signatures. Therefore, Member States are not required to eliminate formal requirements but to recognise that paper requirements can be fulfilled by electronic means.

The legal recognition of signatures as stated in the Article 1 is technologically neutral, i.e., it does not limit the recognition of signatures to a specific type of technology. This approach seems to be a wise one because it allows room for technological developments, thus encouraging the outgrowth of new techniques and providing new business opportunities. Moreover, if the Proposal had confined the legal recognition of signatures to the current digital signature technology, it could happen that one day this technology would no longer provide adequate security (for example, because computer capacity rises to the point where it is possible rapidly to discover a private key from the public key) and thus, rendering the law obsolete. Article 2 contains, inter alia, a definition of "signature" setting out a *functional approach*. Indeed, the Article calls for several requirements which need to be fulfilled for a signature to qualify as a signature for the purpose of the Proposal, and which therefore will benefiting from the legal recognition of electronic signatures.

Article 2 says: "1. <<electronic signature>> means 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 and which meets the following requirements: (a) is uniquely linked to the signatory; (b) is capable of identifying the signatory; (c) is created using means that the signatory can maintain under his control; and (d) is linked to the data to which it relates in such a manner that it is revealed if the data is subsequently altered".

The criteria laid down by Article 2 define the traditional functions of the hand-written signatures: the ability to identify the signatory are enclosed in requirements (a) and (b). The capacity of revealing alteration (or integrity) is attributed (not always rightly) to written documents with a hand-written signature at the bottom of the paper sheet. 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 always stay within one's control.

2.2. Legal Framework for Certification Authorities

The trustworthiness of electronic signatures, and especially digital signatures depends on the use of third parties, so-called certification authorities 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.

The legal framework for certification authorities is only intended to cover this type of certificate which is defined by Article 2.5 as "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" and is referred to as a "qualified certificate". Thus, qualified certificates will be "identity certificates".

The requirements listed in Annex I are, inter alia, the following ones:

- the identifier of the certification service provider issuing it;
- the unmistakable name of the holder or an unmistakable pseudonym which shall be identified as such;
- a specific attribute for the holder such as the address, the authority to act on behalf of a company;
- the credit worthiness, VAT or other tax registration numbers;
- the existence of payment guarantees or specific permits or licenses;
- a signature verification device;
- operational period of the certificate;
- limitation on the scope of use of the certificate, etc.

It should be noticed that from the wording of Article 2.5 the identity of a physical person would be included as well as a legal person.

The legal framework for certification authorities is limited to certain types of activities and subjects, therefore excluding from its application the following hypothesis:

First, 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 certification of the identity, certification authorities could certify *qualities* of the subscriber of a certificate. However, as the explanatory memorandum explicitly recognises, 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".

To the extent that in reality there seems to exist a real need for certification of qualities (for instance, consumers might want to have a certificate ensuring that the web site meets privacy laws[4]), the option taken by the Commission means that many businesses consisting in certifying qualities will fall outside the scope of the Directive.

Second, Article 1 of the Proposal limits the establishment of a legal framework to certification services made available to the public. Moreover, the explanatory memorandum of the Proposal explicitly excludes closed environments such as company's local area network or bank systems from its application. Therefore, for those closed groups, the regulation of the Proposal will not apply. On the contrary, the 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 which they do their business.

3. Certification Authorities - Establisment

3.1. Voluntary Accreditation Schemes

One of the key questions when drafting the Proposal was whether certification authorities would have to be licensed, and whether a Member State requiring licensing would have to accept certificates issued by a non-licensed authority in a Member State having no licensing obligation.

Article 3 of the Proposals gives an answer to the first question, establishing the following: "1.- Member States shall not make the provision of certification services subject to prior authorisation". Article 3, second paragraph, adds "Member States may not limit the number of certification service providers for reasons which fall under the scope of this Directive".

Therefore, from these paragraphs we can infer that a voluntary accreditation schemes or non-licensing system are permissible.

However, paragraph 2 of Article 3 adds the following precision: "Without prejudice to the provisions of paragraph 1, Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification service provision".

From the combination of both paragraphs, it seems clear that certification services could be offered without prior authorisation, but EU Member States would keep the option of setting up voluntary accreditation schemes for service providers.

The basis for maintaining this option is found in the need for public service providing high level services. In addition, the relationships with the public sector (e.g., with the tax Authorities) could be subject to the use of accredited certification authorities and qualified certificates.

As a result of being qualified as a accredited certification authority, probably it will issue certificates which will meet the requirements of Annex I, the so-called "qualified certificates" as they are described in Article 2, although it could provide as well certificates which fall outside of the scope of the Proposal. And if it issues qualified certificates it will benefit automatically from the legal validity of the associated electronic signatures (see below).

The voluntary scheme approach is a positive one because it enhances business development and mostly competitiveness from which both consumer and certification providers will benefit.

3.2 Common Requirements for Certification Service Providers

To the question of how these conditions should be met in a voluntary accreditation schemes, the Proposal provides with the following answer: "All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory".

Article 3 does not refer to the list of what could be the content of these conditions. However, Article 5, which deals with legal effects of electronic signatures, attaches some benefits from the use of certificates issued by a certification service provider which fulfils the requirements set out in Annexe II. Moreover, Article 9 sets down a Consultative Committee to assist the Commission on the requirements for certification service providers laid down in Annex II.

In relation to the content of the requirements listed in Annex II, they seem to be appropriate ones. We should highlight, inter alia, the following ones:

- demonstrate the necessary reliability for offering the services;
- operate a prompt and secure revocation service;
- verify by appropriate means the identity and capacity to act of the person to which a qualified certificate is issued;
- employ personnel which possesses the expert knowledge, experience and qualifications necessary for the offered services;
- use trustworthy systems, and electronic signature products that ensure protection against modification of the products so that they cannot be used to perform functions other that those for which they have been designed;
- take measures against forgery of certificates, and in cases where the certification service provider generates private cryptographic keys, guarantee the confidentiality during the process of generating those keys; and
- maintaining of financial resources to operate in conformity with the requirements laid down in this Directive.

It is important that in the framework of digital signatures, in order to achieve the requisite confidence that the key has not been compromised during the time between the certificate was being issued and the moment that it is really used, it is necessary to establish a trustworthy database maintaining an up-to-date list of valid keys. It should be noticed that point b of Annex II explicitly requires a "prompt and secure revocation service". However, as we will see below, it does not address liability questions derived from a failure to publish the revocation, probably because the need of databases is linked to a specific technology, i.e., digital signatures. Therefore, the lack of regulation of databases containing certificates perhaps is due to the technology neutral approach taken by the Proposal.

3.3. Consultative Committee

Member States shall inform the Commission, inter alia, of the establishment of national accreditation regimes and additional requirements.

A Committee, called the "Electronic Signature Committee" will be created to assist the Commission on its examination of the requirements whenever necessary in order to achieve a harmonised and proportionate application of the requirements enclosed in Annex II.

4. Certification Authorities - Functioning

4.1. Issuing Certificates

Once the certification authority has been created, whether it is an accredited or non-accredited certification authority, and whether it follows the requirements set down in Annexe II or not, it follows from the Proposal that it can issue qualied certificates. To do so, the certification authority when issues qualified certificates needs to comply with the requirements described in Annex I.

However, in order to benefit from the legal validity of the associated electronic signatures, the certification authorities need to comply with Annex II, and probably in order to make sure of this compliance they will need to be accredited certification authorities.

It is also possible that an accredited certification authority issues qualified certificates in addition to non-qualified certificates, perhaps certificates of qualities which will not be covered by the Proposal.

4.2. Liability of Certification Authorities

The Proposal establishes a set of rules on liability that will apply when the certification authority issues qualified certificates and besides its accreditation.

The liability rules are contained in Article 6 of the Proposal. This Article provides the following: "1. Member States shall ensure that by issuing a qualified certificate, a certification service provider is liable to a person who reasonably relies on the certificate for: (a) accuracy of all information in the qualified certificate as of the date it was issued, unless the certification service provider has stated otherwise in the certificate; (b) compliance with all requirement of this Directive in issuing the qualified 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) in the cases where the certification service provider generates the signature creation device and the signature verification device, assurance that the two devices function together in a complementary manner". "2. Member States shall ensure that a certification service provider is not 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".

The two above paragraphs contain two different liability criteria: the first one sets down an objective liability criteria applicable when the obligations (b), (c) and (d) are not fulfilled. Therefore, the subscriber of a certificate or the relying party who uses a certificate will have to prove a failure to fulfil these obligations and the certification authority will be liable. The second paragraph establishes a with-fault liability criteria in relation to the accuracy of the information in the qualified certificate with a presumption of liability which can be rebutted if the certification authority shows that it has taken all reasonable measures to verify the information. However, the certificate might state that the information has not been checked.

The Proposal allows for certain limitations: as stated in Article 6.3, the certification service provider may indicate in the qualified certificate limits on the uses of a certain certificate. Article 6.3 provides that the service provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate is valid. Both rules set down the controversy of whether limitations should be contained in the certificate or a reference would be necessary, by requiring it to be in the certificate. This is a positive measure specially for consumer protection.

As noted above, the Proposal does not address the question of liability for failure to publish a revocation of certificates. Therefore, when a subscriber applies for a certificate, the conditions of availability of the database and liabilities will be regulated by contract. This means that a certification authority could exclude liability when it fails to publish the revocation of a certificate after proper notice by the certification holder of the theft of his certificate.

5. Legal Effects of Electronic Signatures

Electronic signatures cannot play their proper role in facilitating electronic commerce unless they are legally recognised. In other words, electronic signatures must be legally equivalent to hand-written signatures before they can become an effective business tool.

As noted above, EU member State laws currently impose requirements of hand-written signatures and written documents with various purposes. Article 5 of the directive aims to provide legal effects to electronic signatures.

Article 5.2 contains a rebuttable presumption which provides that electronic signatures based on a qualified certificate issued by a service provider which fulfils the requirements set out in Annex II satisfy the legal requirement of hand-written signatures and are admissible as evidence in legal proceedings in the same manner as hand-written signatures. Therefore, two conditions need to be fulfilled to enjoy the presumption: a qualified certificate and a service provider satisfying the requirements, which presumably will be a accredited certification provider.

Article 5.2 provides that "Member States shall ensure that an electronic signature is not denied legal effect, validity and enforceability solely on the grounds that the signature is in electronic form, or not based upon a qualified certificate, or not based upon a certificate issue by an accredited certification service provider". On the bases of this article, uses of non qualified certificates and non-accredited certification providers will be able to prove their validity by establishing the security and reliability of the systems and signature in question.

Of course, for a user of a qualifed certificate, it will easier to have a certificate issued by a certification service provider accredited or otherwise fullfilling the requirements set out in Annex II, since it will not need to prove the security of the system it has used.

6. International Aspects

One of the most important questions when drafting the Proposal was the cross border recognition of electronic certificates and signatures within the European Community as a key element for the development of electronic commerce.

Article 7 of the Proposal addresses the question of EU recognition of electronic certificates and signatures issued by certification authorities established in third countries in the following way: (a) if the certification service provider fulfils the requirements laid down in this Directive and has been accredited in the context of a voluntary accreditation scheme established by a Member State of the European Community; or (b) if a certification service provider established within the European Community, which fulfils the requirements laid down in Annex II, guarantees for the certificate, to the same extent as for its own certificates; or (c) if the certificate or the certification service provider is recognised under the regime of a bilateral or multilateral agreement between the European Community and third countries or international organisations".

Therefore, the certification authority wishing to have its certificates recognised in EU Member States needs to be accredited in one Member State. Alternatively, it can use a certification authority which fulfils the requirements laid down in Annex II to guarantee its certificates. Finally, it could benefit from agreements on multilateral rules on mutual recognition at a global level.

7. Conclusions

An overview of the Proposal leads to a positive impression for various reasons:

First, the Proposal's recognition for electronic signatures is to be welcomed by those who want electronic commerce to be successful. Moreover, its technology-neutral approach is a wise one because it does not hinder the use or development of new authentication technologies. Moreover, given the infany state of this area of business, flexibility should be provided for experimentation.

Second, by excluding closed groups and certificates of qualities from the Proposal 's

sphere of application, the Proposal leaves room for party autonomy and for business opportunities.

Third, the voluntary accreditation scheme is an appropriate non-discriminatory approach which will encourage companies to undertake this business activity, increasing their competitiveness.

Finally, strict liability rules for certain obligations concerning issuing the certificates, combined with the possibility of limiting responsibilities on the use of the certificates and on the value of the transactions for which the certificate is valid, offers an adequate balance between consumers and certification service providers.

---

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

[2] This Proposal was preceded by two previous Communications issued in 1997. The first one entitled " A European Initiative on Electronic Commerce", COM (97) 157 final, (16.4.97) recognised the need of building trust and confidence in electronic transactions and in the planning for new actions there is a prevision of creating a regulatory framework for digital signatures. The second proposal entitled "Ensuring Security and Trust in Electronic Communication- Towards a European Framework for Digital Signatures and Encryption" which sets up the basic principles of the regulatory framework. For a comment on 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", Computer Law & Security Report, 14 (1998) 79-85.

[3] 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.

[4] We can find in the market several initiatives such as Webtrust which provide with a certification mark which ensures that the web side meets the law (business practices disclosures, integrity of the transactions and privacy laws).