COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 13.05.1998
COM(1998) 297 final

98/0191 (COD)

Proposal for a

EUROPEAN PARLIAMENT AND COUNCIL DIRECTIVE

on a common framework for electronic signatures

(presented by the Commission)

EXPLANATORY MEMORANDUM

I. BACKGROUND

Open networks such as the Internet are of increasing importance for world-wide communication. They offer the possibility of interactive communication between parties who may not have pre-established relationships. They offer new business opportunities by creating tools to strengthen productivity and reduce costs, as well as new methods of reaching customers. Networks are being exploited by companies that wish to take advantage of new ways of doing business and new means of working, such as telework and shared virtual environments. Government departments are also using these networks in their interactions with companies and with citizens. Electronic commerce presents the European Union with an excellent opportunity to advance its economic integration.

In order to make best use of these opportunities, a secure environment with respect to electronic authentication is needed. Several different methods exist to sign documents electronically varying from very simple methods (e.g. inserting a scanned image of a hand-written signature in a word processing document) to very advanced methods (e.g. digital signatures using "public key cryptography"). Electronic signatures allow the recipient of electronically sent data to verify the origin of the data (*authentication of data source*) and to check that the data are complete and unchanged and thereby safeguard their integrity (*integrity of data*).

Verification of the authenticity and integrity of data does not necessarily prove the identity of the signatory who creates the electronic signatures. For instance, how does the recipient of a message know that the sender is really the one he claims to be? The recipient may therefore wish to obtain more reliable information on the identity of the signatory. Such information can be given by the signatory himself, issuing the recipient with satisfactory proof. Another way is to have it confirmed by a third party (e.g. a person or institution mutually trusted by both parties). In the context of this Directive, these third parties are called *certification service providers.*

In its Communication on "A European Initiative in Electronic Commerce[1]" of 16 April 1997 directed to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, the Commission recognized digital signatures as an essential tool for providing security and developing trust on open networks. The Bonn Ministerial Declaration[2] also identified the need for digital signatures as a key issue for electronic commerce.

As a first step, the Commission presented a Communication on "Ensuring Security and Trust in Electronic Communication - Towards a European framework for Digital Signatures and Encryption"[3], to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, which outlined the need for a coherent approach in this field. On 1 December 1997, the Council welcomed the Communication and invited the Commission to submit a proposal for a European Parliament and Council Directive on digital signatures as soon as possible.

---

1 COM(97) 157 final, 16.4.1997.

2 European Ministerial Conference "Global Information Networks: Realizing the Potential", Bonn, 6-8 July 1997.

3 COM(97) 503 final, 8.10.1997.

Following the publication of the Communication and as a result of meetings with Member States, with representatives of the private sector, notably the European cryptography industry, and of the Copenhagen international expert hearing[4], the Commission received input from the various parties involved. The following conclusions can be drawn from the information collected:

1. The increasing legislative activity in this area in several Member States emphasize the urgent need for a harmonized legal framework at the European level so as to avoid the development of serious obstacles to the functioning of the Internal Market.

2. While there is much discussion and work on digital signature technologies which employ public-key cryptography, a Directive at the European level should be technology-neutral and should not focus only on these kinds of signatures. Since a variety of authentication mechanisms is expected to develop, the scope of this Directive should be broad enough to cover a spectrum of "electronic signatures", which would include digital signatures based on public-key cryptography as well as other means of authenticating data.

3. In order to ensure the functioning of the Internal Market and to support the rapid development of the market in terms of user demand and technological innovation, prior authorization has to be avoided. As a means to gain the confidence of consumers, voluntary accreditation schemes for certification service provider aiming at providing enhanced levels of security is considered to be useful. As far as such measures are required by the market, they could give a clearer or more predictable level of legal security for both the certification service provider and the consumer.

4. Electronic signatures used within closed groups, for example, where contractual relationships already exist, should not automatically fall within the scope of this Directive. Contractual freedom should prevail in such a context.

5. Ensuring legal recognition - in particular across borders - of electronic signatures and of certification services is regarded as the most important issue in this area. This involves clarifying the essential requirements for certification service providers, including their liability.

6. Industry is supposed to take the lead with standardization bodies in developing internationally agreed standards for electronic signatures. These standards should focus on establishing an open environment for interoperable products and services. The role of the Commission will be to support this process.

7. At the international level, many activities and discussions are underway. The United Nations Commission on International Trade Law (UNCITRAL) has adopted a Model Law on Electronic Commerce and has initiated subsequent work aimed at the preparation of uniform rules on digital signatures. The Organization for Economic Cooperation and Development (OECD) also has work underway in this area, following upon its 1997 Guidelines for Cryptography Policy. Other international organizations, including the World Trade Organization (WTO), have also become involved in related issues. These ongoing

---

4 International Hearing, Copenhagen, 23-24 April 1998.

developments should be taken into account in the implementation of a legal framework at the European level.

II. NEED FOR HARMONIZATION

Several Member States have already started detailed legislative initiatives related to electronic signatures:

Member State	Status of legislative initiatives
Austria	Preparatory work
Belgium	• Telecommunications law: voluntary prior declaration scheme for service providers; • Drafting of law on certification services related to digital signatures; • Drafting of law amending the Civil Code with regard to electronic evidence; • Drafting of law on the use of digital signatures in social security and public health.
Denmark	Drafting of law on the secure and efficient use of digital communications.
France	• Telecommunication Law (Authorization and Exemption Decrees): ⇒ supply of electronic signature products and services subject to information procedure; ⇒ use, import and export of electronic signature products and services free. • Legislation concerning the use of digital signatures in social security and public health.
Finland	• Drafting of law on the electronic exchange of information in administration and administrative judicial procedures; • Drafting of law on the status of the Population Register Centre as provider of certification services.
Germany	• Digital signature law and ordinance in place: conditions under which digital signatures are deemed secure; voluntary accreditation of service providers; • Drafting of catalogue of suitable security measures; • Public consultation on legal aspects of digital signatures and digitally signed electronic documents currently ongoing.
Italy	• General law on the reform of the public service and administrative simplification in place: principle of legal recognition of electronic documents; • Decree on creation, archiving and transmission of electronic documents and contracts; • Decree on requirements on products and services under preparation; • Decree on the fiscal obligations arising from electronic documents under preparation.

Netherlands	• Voluntary accreditation scheme for service providers in preparation; • Taxation law providing for the electronic filing of income statements; • Draft law amending the Civil Code under preparation.
Spain	• Circulars of the customs department on the use of electronic signatures; • Resolution in the field of social security regulating the use of electronic means; • Laws and circulars in the field of mortgages, taxation, financial services and registration of enterprises allowing the use of electronic procedures; • Budget Law 1998 mandating the Mint to act as a certification service provider.
Sweden	Preparatory work.
United Kingdom	• Drafting of legislation concerning the voluntary licensing of certification service providers and the legal recognition of electronic signatures.

The overview shows that the different initiatives in the Member States lead to a divergent legal situation. Although Member States seem to focus on the same issues, in particular the requirements on service providers and products, the condition under which electronic signatures will have legal effect, and the structure of accreditation schemes, it becomes apparent that the relevant regulations, or the lack of them, will be different to the extent that the functioning of the Internal Market in the field of electronic signatures is going to be endangered. Divergent rules concerning the legal effect attributed to electronic signature are particularly detrimental to the further development of electronic commerce and, for this reason, to economic growth and employment in the Community. Further uncertainty results from different liability rules and the risk of uncertain jurisdiction concerning liability where services are provided among different Member States. It also seems likely that Member States will set up different technical conditions under which electronic signatures will be presumed secure.

This diverging situation could create a serious barrier to communication and business via open networks throughout the European Community, by inhibiting the free use and supply of electronic signature-related services, as well as limiting the development of new economic activities linked to electronic commerce. The objective pursued by the attached proposal for a Directive is to remove obstacles, in particular differences concerning the legal recognition of electronic signatures and restrictions on the free movement of certification services and products between the Member States. Given the objectives pursued, the responsibility for the planned measure falls under the exclusive competence of the Community. The proposal for a Directive aims at "enabling" the use of electronic signatures within an area without internal frontiers by focusing on the essential requirements for certification services and leaves detailed implementation provisions to the Member States. It is consistent with the Commission's legislative policy with regard to subsidiarity, proportionality and legislative simplification necessary.

Therefore, the Commission proposes Articles 57(2), 66 and 100A as the legal basis for the present proposal. For reasons of proportionality, the Commission considers a Directive to be the appropriate form of a legal instrument.

III. AIM AND SCOPE OF THE DIRECTIVE

1. This Directive aims at ensuring the proper functioning of the Internal Market in the field of electronic signatures by creating a harmonized and appropriate legal framework for the use of electronic signatures within the Community and establishing a set of criteria which form the basis for legal recognition of electronic signatures.

2. Global electronic communication and commerce are dependent upon the progressive adaptation of international and domestic laws to the rapidly evolving technological infrastructure. Although in many situations analogies to existing rules could provide satisfactory solutions, certain adaptations to these existing laws in the light of new technologies may be required in order to avoid inappropriate and undesirable effects. Although digital signatures produced using cryptographic techniques are currently regarded as an important type of electronic signature, a European regulatory framework must be flexible enough to cover other techniques that may be used to provide authentication.

3. There are obvious applications of electronic signature technology in closed environments, e.g. a company's local area network, or a bank system. Certificates and electronic signatures are also used for authorization purposes, e.g. to access a private account. Within the constraints of national law, the principle of contractual freedom enables contracting parties to agree among themselves the terms and conditions under which they do business, e.g. accept electronic signatures. In these areas, there is no evident need for regulation.

4. Given the range of services and their possible application, certification service providers should be allowed to offer their services without being required to obtain prior authorization. Service providers, however, may wish to benefit from the legal validity of the associated electronic signatures by means of voluntary accreditation schemes linked to common requirements. Accreditation should be regarded as a public service offered for certification service providers which would like to provide high-level services. This should by no means imply that a non-accredited service is automatically less secure.

5. A certification service provider may offer a wide range of services. The present Directive focuses particularly on certification services in connection with electronic signatures. Certificates can be used for a variety of functions and can contain different pieces of information. The information can include conventional identifiers such as name, address, registration number or social security number, VAT or tax identification number, or specific attributes of the signatory for instance, their authority to act on behalf of a company, their credit worthiness, the existence of payment guarantees, or the holding of specific permits or licenses. As a consequence, a variety of certificates are envisaged for a range of uses. However, a legal framework is mainly needed for certificates to enable the authentication of the electronic signature of a signing individual. The present Directive therefore focuses on the function of a certificate (called "qualified certificate") as a linkage to the civil identity or the role of a person.

6. The legal effects manifested by electronic signatures are a key element in an open but trustworthy system for electronic signatures. The application of the present Directive shall also contribute to a harmonized legal framework within the Community by ensuring that an electronic signature should not be denied legal validity, effect or enforcement solely on the grounds that it is in the form of electronic data, not based upon a qualified certificate or upon a certificate issued by an accredited certification service provider, and that electronic signatures should be legally recognized in the same manner as hand written signatures. Moreover, national evidence schemes should be opened up and recognize the use of electronic signatures.

7. The legal recognition of electronic signatures should be based upon objective, transparent, non-discriminatory and proportional criteria and not to be linked to any authorization or accreditation of the service provider involved. Common requirements for certification service providers would support the cross-border recognition of signatures and certificates within the European Community. The requirement catalogue shall be applicable for certification service providers, independent of the accreditation model of the individual Member State. Since the future technological or market development might demand adaptations, the requirements may need to be revised from time to time. The Commission may propose revised sets of requirements on the basis of advice received in the future.

8. Common liability rules would support the trust-building process for both consumers and business that rely on the certificates, and service providers, and thus would promote the broad acceptance of electronic signatures.

9. Cooperative mechanisms which would support the cross-border recognition of signatures and certificates with third countries are important to the development of international electronic commerce. In particular, enabling certification service providers within the Community to vouch for third-country certificates to the same extent as they guarantee for their own certificates could facilitate cross-border services in a simple but efficient way.

Proposal for a

EUROPEAN PARLIAMENT AND COUNCIL DIRECTIVE

on a common framework for electronic signatures

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 57(2) and Articles 66 and 100A thereof,

Having regard to the proposal from the Commission[5],

Having regard to the opinion of the Economic and Social Committee[6],

Having regard to the opinion of the Committee of the Regions[7],

Acting in accordance with the procedure laid down in Article 189b of the Treaty[8],

(1) Whereas on 16 April 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Region, a Communication on an European Initiative in Electronic Commerce[9];

(2) Whereas on 8 October 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, a Communication on Ensuring security and trust in electronic communication - Towards a European framework for digital signatures and encryption[10];

(3) Whereas on 1 December 1997, the Council invited the Commission to submit as soon as possible a proposal for a Directive of the European Parliament and the Council on digital signatures;

(4) Whereas electronic communication and commerce necessitate electronic signatures and related services allowing data authentication; whereas divergent rules with respect to legal recognition of electronic signatures and the accreditation of certification service providers in the Member States may create a significant barrier to the use of electronic communications and electronic

---

5 OJ C
6 OJ C
7 OJ C
8 OJ C
9 COM(97) 157 final.
10 COM(97) 503 final.

commerce and thus hinder the development of the Internal Market; whereas divergent actions in the Member States indicate the need for harmonization at Community level;

(5) Whereas the interoperability of electronic signature products should be promoted; whereas, in accordance with Article 7a of the Treaty, the Internal Market is to comprise an area in which the free movement of goods is to be ensured; whereas essential requirements specific to electronic signature products used by certification service providers must be met in order to ensure free circulation within the Internal Market and to build trust in electronic signatures;

(6) Whereas the rapid technological development and the global character of the Internet necessitate an approach which is open to various technologies and services capable of authenticating data electronically; whereas, however, digital signatures based on public-key cryptography are currently the most recognized form of electronic signature;

(7) Whereas the internal market enables certification services providers to develop their cross-border activities with a view to increasing their competitiveness, and thus to offer consumers and business new opportunities to exchange information and to trade electronically in a secure way, regardless of frontiers; whereas in order to stimulate the Community-wide provision of certification services over open networks, certification service providers should in general be free to offer their services without prior authorization; whereas there is no immediate need to ensure the free circulation of certification services by harmonizing justified and proportionate national restrictions on the provision of those services;

(8) Whereas voluntary accreditation schemes aiming at enhanced level of service provision may offer certification service providers the appropriate framework to develop further their services towards the levels of trust, security and quality demanded by the evolving market; whereas such schemes should encourage the development of best practice among certification service providers; whereas certification service providers should be left free to adhere to and benefit from such accreditation schemes; whereas Member States should not prohibit certification service providers from operating outside such accreditation schemes; whereas it should be ensured that accreditation schemes do not reduce competition for certification services; whereas it is important to strike a balance between consumer and business needs;

(9) Whereas this Directive should therefore contribute to the use and legal recognition of electronic signatures within the Community; whereas a regulatory framework is not needed for electronic signatures exclusively used within closed systems; whereas the freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data should be respected to the extent allowed by national law; whereas this Directive is not intended to harmonize national rules concerning contract law, particularly the formation and performance of contracts, or other non-contractual formalities requiring signatures; whereas for this reason the provisions concerning the legal effect of electronic signatures should be without prejudice to formal requirements prescribed by national law with regard to the conclusion of contracts or the rules determining where a contract is concluded;

(10) Whereas in order to contribute to the general acceptance of electronic signatures, an electronic signature should not be denied legal validity solely on the grounds that it is in the form of electronic data, not based upon a qualified certificate or upon a certificate issued by an accredited certification service provider, or that the service provider who has issued the related certificate is from another Member State; whereas electronic signatures which are related to a trustworthy certification service provider who complies with the essential requirements should have the same legal effect as hand written signatures; whereas it has to be ensured that electronic signatures can be used as evidence in legal proceedings in all Member States; whereas the legal recognition of electronic signatures should be based upon objective criteria and not be linked to authorization of the service provider involved; whereas harmonized rules concerning the legal effect of electronic signatures will preserve a coherent legal framework across the Community;

(11) Whereas certification service providers offering certification services to the public are subject to national liability rules; whereas differences in the scope and content of such liability rules may result in legal uncertainty, particularly concerning third parties relying on their services; whereas such uncertainty will be detrimental to the development of cross-border trade and will hamper the proper functioning of the Internal Market; whereas harmonized liability rules provide legal security and predictability for both certification service providers and consumers; whereas such rules would contribute to the general acceptance and legal recognition of electronic signatures within the Community and consequently have a beneficial effect on the functioning of the Internal Market;

(12) Whereas the development of international electronic commerce requires cross-border mechanisms which involve third countries; whereas those mechanisms should be developed at a business level; whereas in order to ensure interoperability at a global level, agreements on multilateral rules with third countries on mutual recognition of certification services could be beneficial;

(13) Whereas in order to stimulate electronic communication and electronic commerce by ensuring user confidence, Member States should oblige certification service providers to respect data protection legislation and individual privacy and should be required to provide certification services also for pseudonyms at the request of the signatory; whereas national law should lay down if and under what conditions the data revealing the identity of the data subject must be transferred for investigation of criminal offences; whereas certification service providers should inform users in advance of their conditions, in particular regarding the precise use of their certificates and limitations of their liability, in writing and in readily understandable language and using a durable means of communication;

(14) Whereas for the purposes of the application of this Directive, the Commission should be assisted by a consultative Committee;

(15) Whereas in accordance with the principles of subsidiarity and proportionality as set out in Article 3b of the Treaty, the objective of creating a harmonized legal framework for the provision of electronic signatures and related services cannot be sufficiently achieved by the Member States and can, therefore, be better achieved by the Community; whereas this Directive confines itself to the minimum required in order to achieve that objective and does not go beyond what is necessary for that purpose,

HAVE ADOPTED THIS DIRECTIVE:

Article 1
Scope

This Directive covers the legal recognition of electronic signatures.

It does not cover other aspects related to the conclusion and validity of contracts or other non-contractual formalities requiring signatures.

It establishes a legal framework for certain certification services made available to the public.

Article 2
Definitions

For the purpose of this Directive:

(1) "electronic signature" means a signature in digital form in, or attached to, or logically associated with, data which is used by a signatory to indicate his approval of the content of that data and meets the following requirements:

(a) it is uniquely linked to the signatory,

(b) it is capable of identifying the signatory,

(c) it is created using means that the signatory can maintain under his sole control, and

(d) it is linked to the data to which it relates in such a manner that any subsequent alteration of the data is revealed.

(2) "signatory" means a person who creates an electronic signature;

(3) "signature creation device" means unique data, such as codes or private cryptographic keys, or a uniquely configured physical device which is used by the signatory in creating an electronic signature;

(4) "signature verification device" means unique data, such as codes or public cryptographic keys, or a uniquely configured physical device which is used in verifying the electronic signature;

(5) "qualified certificate" means 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;

(6) "certification service provider" means a person who or an entity which issues certificates or provides other services related to electronic signatures to the public;

(7) "electronic signature product" means hardware or software, or relevant components thereof, which are intended to be used by a certification service provider for the provision of electronic signature services.

Article 3
Market access

1. Member States shall not make the provision of certification services subject to prior authorization.

2. 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. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of certification service providers for reasons which fall under the scope of this Directive.

3. The Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognized standards for electronic signature products in the *Official Journal of the European Communities*. Member States shall presume compliance with the requirements laid down in point (e) of Annex II when an electronic signature product meets those standards.

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

Article 4
Internal Market principles

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to certification service providers established on its territory and to the services they provide. Member States may not restrict the provision of certification services which originate in another Member State in the fields covered by this Directive.

2. Member States shall ensure that electronic signature products which comply with this Directive are permitted to circulate freely in the Internal Market.

Article 5
Legal effects

1. 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 is not based upon a qualified certificate, or is not based upon a certificate issued by an accredited certification service provider.

2. Member States shall ensure that electronic signatures which are based on a qualified certificate issued by a certification service provider which fulfils the requirements set out in Annex II are, on the one hand, recognized as satisfying the legal requirement of a hand written signature, and on the other, admissible as evidence in legal proceedings in the same manner as hand written signatures.

Article 6
Liability

1. Member States shall ensure that, by issuing a qualified certificate, a certification service provider is liable to any person who reasonably relies on the certificate for:

   (a) accuracy of all information in the qualified certificate as from the date on which it was issued, unless the certification service provider has stated otherwise in the certificate;

   (b) compliance with all the requirements of this Directive in issuing the qualified certificate;

   (c) assurance that the person 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 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.

3. Member States shall ensure that a certification service provider may indicate in the qualified certificate limits on the uses of a certain certificate. The certification service provider shall not be liable for damages arising from a contrary use of a qualified certificate which includes limits on its uses.

4. Member States shall ensure that a certification service provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate is valid. The certification service provider shall not be liable for damages in excess of that value limit.

5. The provisions of paragraphs 1 to 4 shall be without prejudice to Council Directive 93/13/EEC[11].

Article 7
International aspects

1. Member States shall ensure that certificates issued by a certification service provider established in a third country are recognized as legally equivalent to certificates issued by a certification service provider established within the Community:

   (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; or

   (b) if a certification service provider established within the Community, which fulfils the requirements laid down in Annex II guarantees the certificate to the same extent as its own certificates; or

   (c) if the certificate or the certification service provider is recognized under the regime of a bilateral or multilateral agreement between the Community and third countries or international organizations.

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

Article 8
Data protection

1. Member States shall ensure that certification service providers and national bodies responsible for accreditation or supervision comply with the requirements laid down in Directives 95/46/EC[12] and 97/66/EC[13] of the European Parliament and of the Council.

2. Member States shall ensure that a certification service provider may collect personal data only directly from the data subject and only in so far as it is necessary for the purposes of issuing a certificate. The data may not be collected or processed for other purposes without the consent of the data subject.

---

[11] OJ L 95, 21.4.1993, p. 29.
[12] OJ L 281, 23.11.1995, p. 31.
[13] OJ L 24, 30.1.1998, p. 1.

3. Member States shall ensure that, at the signatory's request, the certification service provider indicates in the certificate a pseudonym instead of the signatory's name.

4. Member States shall ensure that, in the case of persons using pseudonyms, the certification service provider shall transmit the data concerning the identity of those persons to public authorities upon request and with the consent of the data subject. Where according to national law the transfer of the data revealing the identity of the data subject is necessary for the investigation of criminal offences relating to the use of electronic signatures under a pseudonym, the transfer shall be recorded and the data subject informed of the transfer of the data relating to him as soon as possible after the investigation has been completed.

Article 9
Committee

The Commission shall be assisted by a Committee, called the "Electronic Signature Committee" (hereinafter referred to as "the Committee"), of an advisory nature composed of the representatives of the Member States and chaired by the representative of the Commission.

The representative of the Commission shall submit to the Committee a draft of the measures to be taken. The Committee shall deliver its opinion on the draft, within a time-limit which the Chairman may lay down according to the urgency of the matter, if necessary by taking a vote.

The opinion shall be recorded in the minutes; in addition, each Member State shall have the right to ask to have its position recorded in the minutes.

The Commission shall take the utmost account of the opinion delivered by the Committee. It shall inform the Committee of the manner in which its opinion has been taken into account.

Article 10
Consultation of the Committee

The Committee shall be consulted, where necessary, on the requirements for certification service providers laid down in Annex II and on generally recognized standards for electronic signature products pursuant to Article 3(3).

Article 11
Notification

1. Member States shall supply the Commission with the following information:

   (a) information on voluntary national accreditation regimes, including any additional requirements pursuant to Article 3(4);

(b) the names and addresses of the national bodies responsible for accreditation and supervision; and

(c) the names and addresses of accredited national certification service providers.

2. Any information supplied under paragraph 1 and changes in respect of that information shall be notified by the Member States as soon as possible.

Article 12
Review

1. The Commission shall review the operation of this Directive and report thereon to the European Parliament and to the Council by 31 December 2002 at the latest.

2. The review shall, *inter alia*, assess whether the scope of the Directive should be modified taking account of technological and legal developments. The report shall in particular include an assessment, on the basis of the experience gained, of aspects of harmonization. The report shall be accompanied, where appropriate, by complementary legislative proposals.

Article 13
Implementation

1. Member states shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 31 December 2000 at the latest. They shall immediately inform the Commission thereof.

When Member States adopt these provisions, these shall contain a reference to this Directive or shall be accompanied by such reference at the time of their official publication. The procedure for such reference shall be adopted by Member States.

2. Member States shall communicate to the Commission all provisions of national law which they adopt in the field governed by this Directive and in related fields and a correlation table between this Directive and the national provisions adopted.

Article 14
Entry into force

This Directive shall entry into force on the twentieth day following that of its publication in the *Official Journal of the European Communities*.

Article 15
Addressees

This Directive is addressed to the Member States.

Done at Brussels,

For the European Parliament
The President

For the Council
The President

ANNEX I

Requirements for qualified certificates

Qualified certificates must contain:

(a) the identifier of the certification service provider issuing it;

(b) the unmistakable name of the holder or an unmistakable pseudonym which shall be identified as such;

(c) a specific attribute of 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 licences;

(d) a signature verification device which corresponds to a signature creation device under the control of the holder;

(e) beginning and end of the operational period of the certificate;

(f) the unique identity code of the certificate;

(g) the electronic signature of the certification service provider issuing it;

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

(i) limitations on the certification service provider's liability and on the value of transactions for which the certificate is valid, if applicable.

ANNEX II

Requirements for certification service providers

Certification service providers must:

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

(b) operate a prompt and secure revocation service;

(c) verify by appropriate means the identity and capacity to act of the person to which a qualified certificate is issued;

(d) employ personnel which possesses the expert knowledge, experience, and qualifications necessary for the offered services, in particular competence at the managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also exercise administrative and management procedures and processes that are adequate and which correspond to recognized standards;

(e) use trustworthy systems, and use electronic signature products that ensure protection against modification of the products so that they can not be used to perform functions other than those for which they have been designed; they must also use electronic signature products that ensure the technical and cryptographic security of the certification processes supported by the products;

(f) take measures against forgery of certificates, and, in cases where the certification service provider generates private cryptographic signature keys, guarantee the confidentiality during the process of generating those keys;

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

(h) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular to provide evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

(i) not store or copy private cryptographic signature keys of the person to whom the certification service provider offered key management services unless that person explicitly asks for it;

(j) inform consumers before entering into a contractual relationship in writing, using readily understandable language and a durable means of communication, of the precise terms and conditions for the use of the certificate, including any limitations on the liability, the existence of a voluntary accreditation and the procedures for complaints and dispute settlement.

ISSN 0254-1475

COM(98) 297 final

DOCUMENTS

EN 15 06 10 01

Catalogue number : CB-CO-98-336-EN-C

ISBN 92-78-36440-1

Office for Official Publications of the European Communities

L-2985 Luxembourg