COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 29.04.1999

COM(1999) 195 final
98/0191(COD)

Amended proposal for a

EUROPEAN PARLIAMENT AND COUNCIL DIRECTIVE

on a common framework for electronic signatures

(presented by the Commission pursuant to Article 189b (2) of the EC Treaty)

SUMMARY

On 13 January 1999 the European Parliament adopted a legislative Resolution approving, subject to amendments contained in this resolution, the Commission proposal for a European Parliament and Council Directive on a common framework for electronic signatures (COM(1998)297 final - C4-0376/98 - 98/0191(COD)) and calling on the Commission to alter its proposal accordingly.

The Directive aims at ensuring the proper functioning of the Internal Market in the field of electronic signatures by creating a harmonised and appropriate legal framework for the use of electronic signatures within the Community. It establishes a set of criteria, which form the basis for legal recognition of electronic signatures. The legal basis for the proposal is Art. 57 (2), 66 and 100A of the European Treaty.

The Directive establishes a legal framework for certain certification services made available to the public. It focuses particularly on certification services and sets up common requirements for Certification Service Providers (CSP) and certificates to ensure the cross-border recognition of signatures and certificates within the European Community. The Directive follows a technology neutral approach by covering a broad spectrum of 'electronic signatures'. It is based on a dual concept: CSP are in general free to offer their services without prior authorisation. In parallel, Member States are allowed to introduce voluntary accreditation schemes based on common requirements and aimed at a higher level of security. The Directive is meant to contribute to a harmonised legal framework within the Community by ensuring that electronic signatures are legally recognised. To support the trust-building process for both consumers and business that rely on the certificates the proposal introduces liability rules for CSP. Co-operation mechanisms with third countries are embodied in the Directive to contribute to the global recognition of certificates.

Of the 32 amendments adopted by the European Parliament at First Reading, the Commission has accepted 22 in full (amendments 3, 11, 12, 14, 18, 20, 27, 30, 31, 32, 33 and 34) in part or in principle (amendments 2, 4, 5, 9, 13, 16, 17, 21, 22 and 25).

The Commission can not accept 10 of the proposed amendments for legal reasons (amendments 1, 10, 24, 28, 29), because they contain superfluous provisions (amendments 6 and 7) or, because they would cause implementation problems (amendments 15, 23 and 26).

EXPLANATORY MEMORANDUM

The Commission hereby presents a modified proposal for a European Parliament and Council Directive on a common framework for electronic signatures. The modified proposal incorporates those amendments proposed by the European Parliament at First Reading which are acceptable to the Commission.

1) INTRODUCTION

a) Background

As a first step, on 8 October 1997 the Commission presented a Communication on 'Ensuring Security and Trust in Electronic Communication - Towards a European framework for Digital Signatures and Encryption' (COM(97)503 final - C4-0648/97), 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 Directive on digital signatures as soon as possible. In its resolution of 17 July 1998 (A4-0189/98) the European Parliament emphasised the need to create a legal framework at European level to ensure mutual trust in digital signatures and to encourage the development of electronic commerce and electronic communication.

On 13 May 1998, the Commission adopted a proposal for a European Parliament and Council Directive on a common framework for electronic signatures (COM(1998)297 final - C4-0376/98 - 98/0191(COD)). The proposal for a directive comes in anticipation of moves by several European Union Member States to elaborate a legal framework for electronic signatures. The Directive is thus regarded as a preventive measure aimed at creating a harmonised framework for authentication services in Europe. It also takes into account the global nature of electronic communication. The legal basis for the proposal is Art. 57 (2), 66 and 100A of the European Treaty.

The proposal was formally transmitted to the European Parliament and the Council on 16 June 1998. The Economic and Social Committee gave its Opinion on the 2/3 December 1998 and the Committee of the Regions on the 13/14 January 1999. The European Parliament adopted a favourable Resolution at its First Reading on the 13th January 1999, and proposed 32 amendments to the Commission proposal.

b) Aim of the Directive

The Directive aims at ensuring the proper functioning of the Internal Market in the field of electronic signatures by creating a harmonised and appropriate legal framework for the use of electronic signatures within the Community. It establishes a set of criteria, which form the basis for legal recognition of electronic signatures. Global electronic communication and commerce are dependent upon the progressive adaptation of international and domestic laws to the rapidly evolving technological infrastructure. If the consumers and industry in Europe are to take full advantage of the opportunities offered by electronic communication, these issues must be addressed.

c) Main principles of the Directive

- Scope

The Directive establishes a legal framework for certain certification services made available to the public. It focuses particularly on certification services and sets up common requirements for Certification Service Providers (CSP) and certificates to ensure the cross-border recognition of signatures and certificates within the European Community. 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 authorisation purposes, e.g. to access a private account. In these areas, the Commission does not see an evident need for harmonisation.

- Technology neutrality

A variety of authentication mechanisms are expected to develop. Therefore the scope of the Directive must be broad enough to cover the whole spectrum of 'electronic signatures'. Although digital signatures produced using cryptographic techniques are currently regarded as an important type of electronic signature the proposal makes clear that a European regulatory framework must be flexible enough to cover other techniques that may be used to provide authentication.

- Dual approach

The Directive is based on a dual concept: The main intention is to stimulate the Community-wide provision of certification services over open networks. Given the range of services and their possible application CSP should in general be free to offer their services without prior authorisation. In this area the market should develop freely. In parallel, Member States shall be allowed to introduce voluntary accreditation schemes based on common requirements and aimed at a higher level of security. These schemes offer CSP the appropriate framework to develop their services further towards the levels of trust, security and quality demanded by the market, consumers and citizen's.

- Essential requirements

The proposed Directive sets up essential requirements for certificates and CSP to create a harmonised framework at European level. These requirements are not very detailed and they are exclusively connected to the legal recognition of electronic signatures.

- Legal recognition of electronic signatures

The Directive is meant to contribute to a harmonised legal framework within the Community by ensuring that electronic signatures are legally recognised. Legal recognition means 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, recognised 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.

- Liability rules

To support the trust-building process for both consumers and business that rely on the certificates the proposal introduces liability rules for CSP. On the basis of the proposal CSP will in particular be liable for the validity of a certificate's content.

- International dimension

Co-operation mechanisms with third countries are embodied in the Directive to contribute to the global recognition of certificates. They aim in particular at ensuring the recognition by Member States, under clear conditions, of third country certificate and to envisage the negotiation by the Commission of bilateral and multilateral agreements. This is important to the development of international electronic commerce.

- Data protection

The Directive aims at harmonising national provisions which safeguard public interest objectives such as the protection of the right to privacy and personal data in the specific context of electronic signatures. Furthermore, the Directive provides the necessary tool (certificates indicating a pseudonym instead of the signatory's name) permitting consumers to remain anonymous in on-line transactions.

2) EP AMENDMENTS ACCEPTED BY THE COMMISSION

Of the 32 amendments adopted by the European Parliament at First Reading, the Commission accepted 22 in full, in part or in principle.

Amendments accepted in full: 3, 11, 12, 14, 18, 20, 27, 30, 31, 32, 33 and 34.

Amendments accepted in part or in principle: 2, 4, 5, 9, 13, 16, 17, 21, 22 and 25.

The Commission accepted those amendments which:

- Improve the clarity and completeness of the text (amendments 2, 3, 5, 9, 11 - 14, 16 - 18, 20 - 22, 25, 27, 30 - 34)

- Give useful signals as to the direction in which the Directive should be reviewed by the end of 2002 (amendment 4).

In its modified proposal, the Commission has included the amendments in the text as proposed by the European Parliament, and made some additions to ensure consistency throughout the text.

3) EP AMENDMENTS NOT ACCEPTED BY THE COMMISSION

The reasons for non-acceptance of 10 of the proposed amendments are:

- Legal issues, in particular that the amendments are not in line with existing Community rules;
- The amendments contain superfluous provisions;
- The amendments would cause implementation problems.

a) Legal issues

- The Parliament proposes to refer in recital 3 to *electronic* signatures instead of digital signatures (amendment 1). The Commission supports the general approach of the European Parliament to concentrate in the text exclusively on electronic signatures because the Directive covers electronic signatures but recital 3 quotes a Council conclusion of 1st December 1997. Therefore it does not make sense to change the wording.

- The Parliament proposes to change the "consultative committee" into a "contact committee" (amendments 10 and 28) and to add some consultation and information obligations (amendment 28). This would not be in line with the comitology procedure laid down in Council Decision 87/373/EEC of 13 July. This Council Decision lays down different types of Committees. The proposed consultation and information obligations do not correspond to the foreseen procedures nor do they reflect current practice in existing working groups. The Commission can assure that it will contact industry, user and consumer groups on a voluntary basis.

  The task of the Committee should be the clarification of the requirements laid down in Annex I or II as well as in the field of standardisation and not the development of these requirements. Otherwise the Committee would get a quasi-legislative character.

- The distinction between the Committee type and the procedure in Article 9 and the committee's function in Article 10 improves the clarity of the text. Therefore the Commission would prefer not to delete Article 10 (amendment 29).

- In amendment 24 the Parliament suggests to submit proposals for mandates for the negotiation of bilateral and multilateral agreements not only to the Council but *also to the European Parliament*. This is against the wording of Article 113 of the EC Treaty. Article 113 foresees that the Commission only submits proposals to the Council, not to the European Parliament.

- The Parliament proposes to add an additional sentence stating that CSP are allowed to indicate in a certificate a pseudonym *provided that this is permitted by national legislation in non-electronic commercial relations* (amendment 26). There are no general national rules on pseudonyms for off-line transactions because there is no need for such provisions in off-line transactions. In principle, consumers can choose to remain anonymous. The goal of Article 8 paragraph 3 is to establish the necessary tool providing for the possibility to do on-line transactions in the same way as off-line.

should not prevent the European Union to maintain and further develop data protection rules (amendment 6). It is a matter of fact that existing data protection rules have to be respected and that agreements in the field of electronic signatures would have to respect the right to maintain and further develop existing data protection rules. Therefore, such a provision would be superfluous.

- The Parliament proposes to add a recital stating that agreements in the field of electronic signatures should also cover the issues of data protection and privacy (amendment 7). It is a matter of fact that in the framework of such an agreement existing data protection rules and in particular the provisions on international data flows would have to be taken into account. Therefore the Commission considers such a provision superfluous.

c) Implementation problems

- To add the word *independent* in the definition of the CSP in Article 2 (6) (amendment 15) would cause implementation problems. It would not be clear what exactly is meant by such a requirement; e.g. it could mean financial independence, organisational independence etc. In addition, Annex II would be the appropriate place for such a requirement, not the definition.

- For similar reasons amendment 23 can not be accepted. The Parliament proposes to add a paragraph in Article 6 stating that CSP have to confine themselves to the tasks laid down in their statutes. First of all, it remains unclear what exactly the goal of this provision would be. Secondly, CSP are not obliged to establish statutes nor is the legal meaning of such statutes clarified. Thirdly, it has to be questioned whether a CSP would be able to ensure that it is not subjected to any form of administrative control. In any case, Article 6 would not be the proper place for such a provision, because the proposed text is not related to liability.

4) CONCLUSION

The Commission has accepted 22 out of 32 amendments proposed by the European Parliament at First Reading either in whole or in part.

In accordance with Article 189b (2) of the EC Treaty, the Commission amends its initial proposal, incorporating these amendments.

Amended proposal for a

EUROPEAN PARLIAMENT AND COUNCIL DIRECTIVE

on a common framework for electronic signatures

(Text with EEA relevance)

Original text	Amended text

Recital 4

(based on amendment 2)

(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 commerce and thus hinder the development of the internal market; whereas divergent actions in the Member States indicate the need for harmonisation at Community level;	(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 commerce; whereas clear common framework conditions for electronic signatures, on the other hand, will strengthen confidence in and general acceptance of the new technologies; whereas divergent actions in the Member States must not be allowed to hinder the free movement of goods and services in the internal market;

Recital 6

(based on amendment 3)

(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 recognised form of electronic signature;	(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;

Recital 6a (new)
(based on amendment 4)

	Whereas the Commission shall bring forward a review of this Directive before 2003 in part to ensure that the advance of technology or changes to the legal environment have not created barriers to achieving the aims stated in this Directive; whereas they should examine the implications of associated technical areas ~~such as confidentiality~~, and bring forward a report to the Parliament and Council on this subject;

Recital 10a (new)
(based on amendment 5)

	(10a) Whereas the internal market comprises also the free movement of persons, as a result of which citizens of, and residents in, the European Union increasingly need to deal with authorities in Member States other than the one in which they reside; ~~whereas, for such reasons, the European Parliament has decided to accept the electronic filing of petitions;~~ whereas the availability of electronic communication could be of great service in this respect, provided that national rules on additional requirements do not pose obstacles to the possibilities thus offered for improved access to administration;

Recital 13a (new)
(based on amendment 9)

	(13a) Whereas this Directive is without prejudice to existing national provisions concerned with public policy or public security ~~or relating to provision of confidentiality services~~;

Article 1
(based on amendment 11)

Article 1 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 1 This Directive covers the legal recognition of electronic signatures. It establishes a legal framework for certain certification services made available to the public. It does not cover other aspects related to the conclusion and validity of contracts or other non-contractual formalities requiring signatures.

Article 2 paragraph 1
(based on amendment 12)

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:	1. 'electronic signature' means a signature in electronic 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:

Article 2 paragraph 2
(based on amendment 13)

2. 'signatory' means a person who creates an electronic signature;	2. 'signatory' means a natural person who, signing either on their own behalf or on the behalf of the person or the entity they represent, creates an electronic signature;

Article 2 paragraph 5
(based on amendment 14)

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;	5. 'qualified certificate' means <u>an electronic</u> 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;

Article 3 paragraph 2
(based on amendment 16)

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.	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. Member States may also recognise accreditation schemes managed by organisations independent of Member States' administrations ~~whose objective is to improve 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.

Article 3 paragraph 4
(based on amendment 17)

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.	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. Such requirements may not constitute an obstacle for cross border services to citizens ~~in the fields of social security benefits and pensions, for example~~.

Article 5
(based on amendment 18)

1. Member States shall ensure that an electronic signature is not denied legal effects, validity and enforceability solely on the grounds that the signature is in an electronic form, or is not based on a qualified certificate, or is not based on 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 requirements of a hand written signature, and on the other, admissible as evidence in legal proceedings in the same manner as hand written signatures.	1. 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 requirements of a hand written signature, and on the other, admissible as evidence in legal proceedings in the same manner as hand written signatures. 2. Member States shall ensure that an electronic signature is not denied legal effects, validity and enforceability solely on the grounds that the signature is in an electronic form, or is not based upon a qualified certificate, or is not based upon a certificate issued by an accredited certification service provider.

Article 6 paragraph 1 (b)
(based on amendment 20)

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

Article 6 paragraph 3
(based on amendment 21)

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.	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 limit must be ~~sufficiently~~ recognisable to third parties. 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.

Article 6 paragraph 4
(based on amendment 22)

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.	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 limit must be ~~sufficiently~~ recognisable to third parties. The certification service provider shall not be liable for damages in excess of that value limit.

Article 8 paragraph 2
(based on amendment 25)

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.	2. Member States shall ensure that a certification service provider may collect personal data only directly from or with the explicit consent of the data subject ~~permission~~ 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.

Article 8 paragraph 4
(based on amendment 27)

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 on 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.	4. Where, in line with Directive 95/46/EC and according to national law, the transfer of the data revealing the identity of the data subject/signatory to public authorities is necessary for the investigation of criminal offences relating to the use of electronic signatures with pseudonym certificates or necessary for legal claims related to transactions done by using electronic signatures with pseudonym certificates, the transfer shall be recorded and the data subject informed of the transfer.

Article 11
(based on amendment 30)

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; (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.	1. Member States shall supply the Commission with the following information: (a) information on voluntary national accreditation regimes, including any additional requirements according to Article 3(4); (b) the names and addresses of the national recognised bodies responsible for accreditation and supervision; (c) the names and addresses of accredited national certification service providers. 2. Any information supplied under paragraph 1 and changes in respect of this information shall be notified by the Member States and recognised bodies within one month.

Annex I(b)
(based on amendment 31)

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

Annex I(f)
(based on amendment 32)

(f) the unique identity code of the certificate;	(f) the identity code of the certificate;

Annex I(i)
(based on amendment 33)

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

Annex II(e)
(based on amendment 34)

(e) use trustworthy systems, and use electronic signature products that ensure protection against modification of the products so that they cannot 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;	(e) use trustworthy systems, and use electronic signature products that ensure protection against modification of the products; they must also use electronic signature products that ensure the technical and cryptographic security of the certification processes supported by the products;

ISSN 0254-1475

COM(1999) 195 final

DOCUMENTS

EN **15 06 10 01**

Catalogue number : CB-CO-99-217-EN-C

Office for Official Publications of the European Communities
L-2985 Luxembourg

20