COMMON POSITION (EC) NO 28/1999

adopted by the Council on 28 June 1999

with a view to adopting Directive 1999/000/EC of the European Parliament and of the Council of … on a Community framework for electronic signatures

(1999/C 243/02)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof,

Having regard to the proposal from the Commission [1],

Having regard to the opinion of the Economic and Social Committee [2],

Having regard to the opinion of the Committee of the Regions [3],

Acting in accordance with the procedure laid down in Article 251 of the Treaty [4],

(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 Regions a Communication on a European initiative in electronic commerce;

(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;

(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 of 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 commerce; whereas, on the other hand, a clear Community framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies; whereas legislation in the Member States should not hinder the free movement of goods and services in the internal market;

(5) Whereas the interoperability of electronic-signature products should be promoted; whereas, in accordance with Article 14 of the Treaty, the internal market comprises an area without internal frontiers in which the free movement of goods is ensured; whereas essential requirements specific to electronic-signature products must be met in order to ensure free movement within the internal market and to build trust in electronic signatures, without prejudice to Council Regulation (EC) No 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods [5] and Council Decision 94/942/CFSP of 19 December 1994 on the joint action adopted by the Council on the basis of Article J.3 of the Treaty on European Union concerning the control of exports of dual-use goods [6];

(6) Whereas this Directive does not harmonise the provision of services with respect to the confidentiality of information where they are covered by national provisions concerned with public policy or public security;

(7) Whereas the internal market ensures the free movement of persons, as a result of which citizens and residents of the European Union increasingly need to deal with authorities in Member States other than the one in which they reside; whereas the availability of electronic communication could be of great service in this respect;

(8) Whereas 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;

---

[1] OJ C 325, 23.10.1998, p. 5.
[2] OJ C 40, 15.2.1999, p. 29.
[3] OJ C 93, 6.4.1999, p. 33.
[4] Opinion of the European Parliament of 13 January 1999 (OJ C 104, 14.4.1999, p. 49). Council Common Position of 28 June 1999 and Decision of the European Parliament of … (not yet published in the Official Journal).
[5] OJ L 367, 31.12.1994, p. 1. Regulation as amended by Regulation (EC) No 837/95) (OJ L 90, 21.4.1995, p. 1).
[6] OJ L 367, 31.12.1994, p. 8. Decision as last amended by Decision 1999/193/CFSP (OJ L 73, 19.3.1999, p. 1).

(9) Whereas electronic signatures will be used in a large variety of circumstances and applications, resulting in a wide range of new services and products related to or using electronic signatures; whereas the definition of such products and services should not be limited to the issuance and management of certificates, but should also encompass any other service and product using, or ancillary to, electronic signatures, such as registration services, time-stamping services, directory services, computing services or consultancy services related to electronic signatures;

(10) Whereas the internal market enables certification-service-providers to develop their cross-border activities with a view to increasing their competitiveness, and thus to offer consumers and businesses new opportunities to exchange information and trade electronically in a secure way, regardless of frontiers; whereas in order to stimulate the Community–wide provision of certification services over open networks, certification–service–providers should be free to provide their services without prior authorisation; whereas prior authorisation means not only any permission whereby the certification–service–provider concerned has to obtain a decision by national authorities before being allowed to provide its certification services, but also any other measures having the same effect;

(11) Whereas voluntary accreditation schemes aiming at an enhanced level of service-provision may offer certification-service-providers the appropriate framework for developing further their services towards the levels of trust, security and quality demanded by the evolving market; 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;

(12) Whereas certification services can be offered either by a public entity or a legal or natural person, when it is established in accordance with the national law; whereas Member States should not prohibit certification-service-providers from operating outside voluntary accreditation schemes; whereas it should be ensured that such accreditation schemes do not reduce competition for certification services;

(13) Whereas Member States may decide how they ensure the supervision of compliance with the provisions laid down in this Directive; whereas this Directive does not preclude the establishment of private-sector-based supervision systems; whereas this Directive does not oblige certification-service-providers to apply to be supervised under any applicable accreditation scheme;

(14) Whereas it is important to strike a balance between consumer and business needs;

(15) Whereas Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures; whereas it does not cover the entire system environment in which such devices operate; whereas the functioning of the internal market requires the Commission and the Member States to act swiftly to enable the bodies charged with the conformity assessment of secure signature devices with Annex III to be designated; whereas in order to meet market needs conformity assessment must be timely and efficient;

(16) Whereas this Directive contributes 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; nevertheless electronic signatures which fulfil the requirements laid down in this Directive and which are used within closed user-groups should be legally recognised; 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;

(17) Whereas this Directive does not seek to harmonise national rules concerning contract law, particularly the formation and performance of contracts, or other formalities of a non-contractual nature concerning signatures; whereas for this reason the provisions concerning the legal effect of electronic signatures should be without prejudice to requirements regarding form laid down in national law with regard to the conclusion of contracts or the rules determining where a contract is concluded;

(18) Whereas the storage and copying of signature–creation data could cause a threat to the legal validity of electronic signatures;

(19) Whereas electronic signatures will be used in the public sector within national and Community administrations and in communications between such administrations and with citizens and economic operators, for example in the public procurement, taxation, social security, health and justice systems;

(20) Whereas harmonised criteria relating to the legal effects of electronic signatures will preserve a coherent legal framework across the Community; whereas national law lays down different requirements for the legal validity of handwritten signatures; whereas certificates can be used to confirm the identity of a person signing electronically; whereas advanced electronic signatures based on qualified certificates aim at a higher level of security; whereas advanced electronic signatures which are based on a qualified certificate and which are

created by a secure-signature-creation device can be regarded as legally equivalent to handwritten signatures only if the requirements for handwritten signatures are fulfilled;

(21) Whereas in order to contribute to the general acceptance of electronic authentication methods it has to be ensured that electronic signatures can be used as evidence in legal proceedings in all Member States; whereas the legal recognition of electronic signatures should be based on objective criteria and not be linked to authorisation of the certification-service-provider involved; whereas national law governs the use of electronic documents and electronic signatures; whereas this Directive is without prejudice to the power of a national court to make a ruling regarding conformity with the requirements of this Directive and does not affect national rules regarding the unfettered judicial consideration of evidence;

(22) Whereas certification-service-providers providing certification-services to the public are subject to national rules regarding liability;

(23) Whereas the development of international electronic commerce requires cross-border arrangements involving third countries;

(24) Whereas in order to increase user confidence in electronic communication and electronic commerce, certification-service-providers must observe data protection legislation and individual privacy;

(25) Whereas provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Community or national law;

(26) Whereas, for the purposes of the application of this Directive, the Commission should be assisted by a management committee;

(27) Whereas two years after its implementation the Commission will carry out a review of this Directive so as, *inter alia*, to ensure that the advance of technology or changes in the legal environment have not created barriers to achieving the aims stated in this Directive; whereas it should examine the implications of associated technical areas and submit a report to the European Parliament and the Council on this subject;

(28) Whereas, in accordance with the principles of subsidiarity and proportionality as set out in Article 5 of the Treaty, the objective of creating a harmonised 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 does not go beyond what is necessary to achieve that objective,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Scope

The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market.

It does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Community law nor does it affect rules and limits, contained in national or Community law, governing the use of documents.

Article 2

Definitions

For the purpose of this Directive:

1. 'electronic signature' means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

2. 'advanced electronic signature' means an electronic signature which 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 change of the data is detectable;

3. 'signatory' means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;

4. 'signature-creation data' means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;

5. 'signature-creation device' means configured software or hardware used to implement the signature-creation data;

6. 'secure-signature-creation device' means a signature-creation device which meets the requirements laid down in Annex III;

7. 'signature-verification-data' means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;

8. 'signature-verification device' means configured software or hardware used to implement the signature-verification-data;

9. 'certificate' means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;

10. 'qualified certificate' means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II;

11. 'certification-signature-product' means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures;

12. '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 or are intended to be used for the creation or verification of electronic signatures;

13. 'voluntary accreditation' means any permission, setting out rights and obligations specific to the provision of certification services, to be granted on request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.

Article 3

Market access

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

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 accredited certification-service-providers for reasons which fall within the scope of this Directive.

3. Each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public.

4. The conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States. The Commission shall, pursuant to the procedure laid down in Article 9, establish criteria for Member States to determine whether a body should be designated.

A determination of conformity with the requirements laid down in Annex III made by the bodies referred to in the first subparagraph shall be recognised by all Member States.

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

6. Member States and the Commission shall work together to promote the development and use of signature-verification devices in the light of the recommendations for secure signature-verification laid down in Annex IV and in the interests of the consumer.

7. Member States may make the use of electronic signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens.

Article 4

Internal market principles

1. Each Member State shall apply the national provisions which it adopts pursuant to this Directive to certification-service-providers established on its territory and to the services which they provide. Member States may not restrict the provision of certification-services originating 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 of electronic signatures

1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device;

(a) satisfay the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and

(b) are admissible as evidence in legal proceedings.

2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

— in electronic form, or

— not based on a qualified certificate, or

— not based on a qualified certificate issued by an accredited certification-service-provider, or

— not created by a secure signature-creation device.

Article 6

Liability

1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:

(a) as regards the accuracy at the time of issue of all information contained in the qualified certificate;

(b) for assurance that at the time of the issue of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;

(c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;

unless the certification-service-provider proves that he has not acted negligently.

2. As a minimum, Member States shall ensure that a certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently.

3. Member States shall ensure that a certification-service-provider may indicate in a qualified certificate limitations on the use of that certificate, provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it.

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 can be used, provided that the limit is recognisable to third parties.

5. The provisions of paragraphs 1 to 4 shall be without prejudice to Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts ([1]).

Article 7

International aspects

1. Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service-provider established within the Community if:

(a) the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or

(b) a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or

(c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.

2. In order to facilitate cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries, the Commission shall make proposals, where appropriate, to achieve the effective implementation of standards and

([1]) OJ L 95, 21.4.1993, p. 29.

international agreements applicable to certification services. In particular, and where necessary, it shall submit proposals to the Council for appropriate mandates for the negotiation of bilateral and multilateral agreements with third countries and international organisations. The Council shall decide by qualified majority.

3. Whenever the Commission is informed of any difficulties encountered by Community undertakings with respect to market access in third countries, it may, if necessary, submit proposals to the Council for an appropriate mandate for the negotiation of comparable rights for Community undertakings in these third countries. The Council shall decide by qualified majority.

Measures taken pursuant to this paragraph shall be without prejudice to the obligations of the Community and of the Member States under relevant international agreements.

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 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1].

2. Member States shall ensure that a certification-service-provider which issues certificates to the public may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only in so far as it is necessary for the purposes of issuing and maintaining the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject.

3. Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name.

Article 9

Committee

1. The Electronic-Signature Committee, hereinafter referred to as 'the committee', is hereby established. It shall be composed of representatives of the Member States and be chaired by the representative of the Commission.

2. The Commission shall be assisted by the committee.

3. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter. The opinion shall be delivered by the majority laid down in Article 205(2) of the Treaty in the case of decisions which the Council is required to adopt on a proposal from the Commission. The votes of the representatives of the Member States within the Committee shall be weighted in the manner set out in that Article. The chairman shall not vote.

4. The Commission shall adopt the measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. In that event:

— the Commission shall defer the application of the measures which it has decided for three months from the date of communication,

— the Council, acting by a qualified majority, may take a different decision within the time limit referred to in the first indent.

Article 10

Tasks of the committee

The committee shall clarify the requirements laid down in the Annexes to this Directive, the criteria referred to in Article 3(4) and the generally recognised standards for electronic signature products established and published pursuant to Article 3(5), in accordance with the procedure laid down in Article 9.

Article 11

Notification

1. Member States shall notify to the Commission and the other Member States the following:

(a) information on national voluntary accreditation schemes, including any additional requirements pursuant to Article 3(7);

(b) the names and addresses of the national bodies responsible for accreditation and supervision as well as of the bodies referred to in Article 3(4):

(c) the names and addresses of all 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] OJ L 281, 23.11.1995, p. 31.

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 (*) at the latest.

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

Article 13

Implementation

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before … (**). They shall forthwith inform the Commission thereof.

When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

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

Article 14

Entry into force

This Directive shall enter into force on the day of its publication in the *Official Journal of the European Communities*.

Article 15

Addressees

This Directive is addressed to the Member States.

Done at …

For the European Parliament	*For the Council*
The President	*The President*
…	…

(*) Three years and six months after the date of entry into force of this Directive.

(**) One year and six months after the date of entry into force of this Directive.

ANNEX I

Requirements for qualified certificates

Qualified certificates must contain:

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

(b) the identification of the certification-service-provider and the State in which it is established;

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

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

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

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

(g) the identity code of the certificate;

(h) the advanced electronic signature of the certification-service-provider issuing it;

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

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

ANNEX II

Requirements for certification-service-providers issuing qualified certificates

Certification-service-providers must:

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

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

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

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

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

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

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

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

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

(j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;

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

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

— only authorised persons can make entries and changes,

— information can be checked for authenticity,

— certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and

— any technical changes compromising these security requirements are apparent to the operator.

ANNEX III

Requirements for secure signature-creation devices

1. Secure-signature-creation devices must, by appropriate technical and procedural means, ensure at least that:

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

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

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

2. Secure signature creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

ANNEX IV

Recommendations for secure signature verification

During the signature-verification process it should be ensured with reasonable certainty that:

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

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

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

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

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

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

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

STATEMENT OF THE COUNCIL'S REASONS

I. INTRODUCTION

1. On 16 June 1998 the Commission submitted a proposal for a European Parliament and Council Directive on a common framework for electronic signatures.

2. The European Parliament delivered its opinion at first reading on 13 January 1999 and the Economic and Social Committee and the Committee of the Regions delivered their opinions on 3 December 1998 and 14 January 1999 respectively.

3. On 28 June 1999 the Council adopted its Common Position in accordance with Article 251 of the Treaty.

II. OBJECTIVE

The purpose of the proposal is to ensure the proper functioning of the internal market in the field of electronic signatures by creating a harmonised legal framework.

This framework, consisting of a set of criteria to be used as a basis for the legal recognition of electric signatures, will facilitate the use of such signatures and enable consumers and businesses in Europe to benefit fully from the opportunities offered by electronic communications.

III. ANALYSIS OF THE COMMON POSITION

A. GENERAL COMMENTS

Although the Council adopted the approach and aims proposed by the Commission and supported by the Parliament, it considered it necessary, when drawing up its Common Position, to make a number of changes to both the substance and the wording of the proposed Directive.

When making these changes the Council's main concerns were to:

— clarify the provisions of the new Directive and make it easier to read,

— provide greater security in electronic communications,

— take greater account of the various technologies and services for authenticating information transmitted electronically,

— take greater account of the diversity of national situations.

B. SPECIFIC COMMENTS

1. **Principal changes made to the Commission proposal**

(a) *Distinction made between advanced electronic signatures and other electronic signatures*

According to the approach chosen by the Council, an advanced electronic signature is a signature providing a high security level which is therefore recognised as having equivalent validity to a handwritten signature (see Article 2(2) and Article 5(1)).

Such a signature must be based on a qualified certificate drawn up and delivered in compliance with a number of requirements (see Annex I for the requirements for qualified certificates and Annex II for the requirements for certification-service-providers). It must also be created using a secure electronic signature-creation device (see requirements in Annex III).

Other electronic signatures must at least benefit from the principle of non-discrimination and cannot therefore be considered to have no legal effect for the sole reason that they are presented in electronic form or that they do not comply with the requirements for advanced electronic signatures (see Article 2(1) and Article 5(2)).

(b) *Additional measures to improve the level of service provided by the certification-service-providers*

Although the Common Position enshrines the principle of prohibiting any prior authorisation for the provision of certification services, it supports the introduction at national level of voluntary accreditation schemes to improve the level of such services and requires the Member States to establish an appropriate system for supervising service-providers which issue qualified certificates to the public (see Article 3(2) and (3)).

The Common Position also extends the responsibility of service-providers as regards the validity of the content of the approved certificates which they issue, in order to increase user confidence in those certificates (see Article 6). This responsibility covers in particular the revocation of certificates (see Article 6(2)).

(c) *Committee assisting the Commission*

The Council considered it desirable to adopt for this committee a type IIB regulatory procedure on account of the importance of the tasks entrusted to it (see Articles 9 and 10).

The committee will have the following tasks:

— clarifying the requirements laid down in the Annexes to the Directive,

— establishing the criteria for designating the national bodies responsible for verifying the Directive's conformity with secure signature-creation-devices used for advanced signatures (see Article 3(4)),

— determining the standards generally recognised for electronic signature products, compliance with which will confer a presumption that those products comply with the requirements of the Directive (see Article 3(5)).

(d) *Recommendations concerning signature-verification devices*

The Common Position sets out a number of recommendations to make the advanced electronic signature verification process as secure as possible and asks Member States and the Commission to work together to promote the development and use of signature-verification devices on the basis of those recommendations (see Article 3(6) and Annex IV).

2. **The Council's position on the European Parliament amendments**

(a) *Amendments incorporated fully or in part into the Common Position*

The Council incorporated the full wording of amendments 3, 11, 12, 14, 18, 20, 31, 32, 33 and 34, and the principle of amendments 2, 13, 21, 22 and 25.

The Council incorporated amendments 4, 9 and 17 in part, aligning its decision on the Commission's position.

(b) *Amendments not incorporated into the Common Position*

In not incorporating amendments 1, 6, 7, 10, 15, 23, 24, 26, 28 and 29, the Council followed the Commission's negative opinion.

In not incorporating amendments 5, 16, 27 and 30, the Council based its decisions on the following considerations:

— amendment 5 concerning easier access for European Union citizens to the administrative services of a Member State other than that in which they reside (new recital).

The Council considered that Article 3(7), stipulating that by regulating the use of electronic signatures in the public sector Member States could not create obstacles to cross-border services for citizens, took account of the European Parliament's concerns in this matter,

— amendment 16 concerning the recognition of accredition schemes administered by non-governmental bodies (Article 3(2)).

The Council considered that the European Parliament's concerns were taken into account in the definition of voluntary accreditation inserted into Article 2(13),

— amendment 27 concerning the transmission to public authorities of information concerning the identity of persons using pseudonyms (Article 8(4)).

The Council considered that the proposal to authorise such transmission only in the case of a criminal investigation or court proceedings was too restrictive and might involve the risk of encouraging the illegal use of electronic communications,

— amendment 30 concerning reference to 'recognised' national bodies as regards notification of the bodies responsible for accreditation and supervision (Article 11).

The Council considered that the expression 'recognised bodies', which was not defined or mentioned in the rest of the Directive, could give rise to problems of interpretation.