EUROPEAN PARLIAMENT

session documents

ENGLISH EDITION

Doc 110

20 May 1998

A4-0189/98

REPORT

on the communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on ensuring security and trust in electronic telecommunication - towards a European framework for digital signatures and encryption (COM(97)0503 - C4-0648/97)

Committee on Legal Affairs and Citizens' Rights

Rapporteur: Mr Wolfgang Ullmann

Draftsman of opinion: Mr W. G. van Velzen, Committee on Economic and Monetary Affairs and Industrial Policy (*)

(* HUGHES Procedure)

DOC_EN\RR\354\354152

PE 225.030/fin.

* Consultation procedure
simple majority
**I Cooperation procedure (first reading)
simple majority
**II Cooperation procedure (second reading)
simple majority to approve the common position
majority of Parliament's component Members to reject or amend the common position
*** Assent procedure
majority of Parliament's component Members to give assent
but simple majority under Articles 8a, 105, 106, 130d and 228 EC

***I Codecision procedure (first reading)
simple majority
***II Codecision procedure (second reading)
simple majority to approve the common position
majority of Parliament's component Members to adopt a declaration of intended rejection of the common position, and amend the common position or confirm its rejection
***III Codecision procedure (third reading)
simple majority to approve the joint text
majority of Parliament's component Members to reject the Council text

CONTENTS

(* HUGHES Procedure)

By letter of 9 October 1997 the Commission forwarded to the European Parliament a communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on ensuring security and trust in electronic telecommunication - towards a European framework for digital signatures and encryption (COM(97)0503 - C4-0648/97)

At the sitting of 15 December 1997 the President of Parliament announced that he had referred the Commission communication to the Committee on Legal Affairs and Citizens' Rights as the committee responsible and to the Committee on Economic and Monetary Affairs and Industrial Policy, the Committee on the Environment, Public Health and Consumer Protection and the Committee on Culture, Youth, Education and the Media for their opinions.

At its meeting of 27 November 1997 the Committee on Legal Affairs and Citizens' Rights had appointed Mr Ullmann rapporteur.

At the sitting of 13 March 1998, the President of Parliament announced that this report was to be drawn up under the HUGHES procedure by the Committee on Legal Affairs and Citizens' Rights, together with the Committee on Economic and Monetary Affairs and Industrial Policy.

The Committee considered the Commission communication and the draft report at its meetings of 14 April 1998 and 19 May 1998.

At the latter meeting it adopted the motion for a resolution unanimously.

The following were present for the vote: De Clercq, chairman; Malangré, vice-chairman; Ullman, rapporteur; Añoveros Trias de Bes (for C. Casini), Barzanti, Berger, Buffetaut, Cassidy, Cot, Falconer (for D. Martin), Gebhardt, Oddy, Thors and Verde I Aldea.

The opinions of the Committee on Economic and Monetary Affairs and Industrial Policy and the Committee on Culture, Youth, Education and the Media are attached; the Committee on the Environment, Public Health and Consumer Protection decided on 21 January 1998 that it would not deliver an opinion.

The report was tabled on 20 May 1998.

The deadline for tabling amendments will be indicated in the draft agenda for the relevant part-session.

A

MOTION FOR A RESOLUTION

Resolution on the communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on ensuring security and trust in electronic telecommunication - towards a European framework for digital signatures and encryption (COM(97)0503 - C4-0648/97)

The European Parliament,

- having regard to the Commission communication to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on ensuring security and trust in electronic telecommunication - towards a European framework for digital signatures and encryption (COM(97)0503 - C4-0648/97),

- having regard to its resolution of 19 September 1996 on the recommendation to the European Council on Europe and the global information society and on the Commission communication 'Europe's way to the information society: an action plan'([1]),

- having regard to the results of the European Ministerial Conference 'Global information networks: realizing the potential', which took place in Bonn from 6 to 8 July 1997,

- having regard to the report of the Committee on Legal Affairs and Citizens' Rights and the opinions of the Committee on Economic and Monetary Affairs and Industrial Policy and the Committee on Culture, Youth, Education and the Media (A4-0189/98),

A. whereas electronic communication raises three specific problems: authentication of a message, the integrity of the message transmitted and confidentiality,

B. whereas the need for legislation on authentication has been recognized in all Member States of the EU and in eight Member States legislation has already been adopted or is in the pipeline,

C. whereas electronic commerce and many other applications of the information society will only develop if confidentiality can be guaranteed in a user-friendly and cost-efficient way, whereas, however, the law enforcement authorities and national security agencies fear that further use of encryption could impede them in the fight against crime,

1. Shares the Commission's view that electronic commerce will become one of the key drivers for the development of the global information society but points out that the technology discussed in the Commission communication will become increasingly important for people in their everyday lives and not just for commerce;

2. Considers that, with regard to the problem of authentication and integrity of data, for which digital signatures can provide a solution, it is necessary to create a legal framework at European level to ensure mutual compatibility and trust in digital signatures and to encourage

---

([1]) OJ C 320, 28.10.1996, p. 164, paragraph 106 of the resolution.

the development of a range of certification arrangements that will suit different applications, particularly in electronic commerce and in electronic communication between public bodies and citizens; the legal framework must be designed primarily to abolish national restrictions on certification;

3. Considers that the necessary steps should be taken to remove obstacles to the use of digital signatures in the legal system, industry and public administration; therefore calls for digital and conventional signatures to have the same status in law;

4. Supports European Union bodies in leading the way in the use of digital signatures in communications with each other and with third parties so as to increase public acceptance of and trust in digital signatures and electronic communication in general;

5. Assumes that a technical solution can be found to both the problem of ensuring the integrity of communications and that of authentication, so that no particular action is required at Community level;

6. Considers that, with regard to the issue of ensuring confidentiality, the main priority at this stage must be to make encryption technologies available to all those using electronic communication, but that at the same time the legitimate interests of law enforcement should be taken into account;

7. Calls on the Commission and the Member States to press ahead with dialogue and agreements at international level to allow the creation of a worldwide virtual economic area through common technical standards and mutual recognition;

8. Considers that, with a view to the single market, the regulation on dual-use goods should be amended to the effect that internal Community checks on encryption products are abolished, so that there is freedom of circulation for commercial encryption products;

9. Calls on the Member States, during the discussions concerning the Wassenaar Agreement and the forthcoming proposal for the amendment of the regulation on dual-use goods, to advocate that the list of encryption products subject to export restrictions be reduced to a strict minimum and that, consequently, no new restrictions should be introduced;

10. Stresses the importance of international dialogue between the European Union and various international organizations such as the OECD, UN, ITU, ICC and WTO, to avoid a situation in which regulations form a barrier to trade with major trading partners, and underlines the need for reciprocity in the treatment of the European Union by other trading partners;

11. Believes that it is necessary for the further development of electronic commerce to engender sufficient user confidence and to formulate rules with regard to the legal reliability of, inter alia, identification, validity in law of contracts, integrity and communications;

12. Stresses that general rules must be established leading on the one hand to greater confidence in electronic commerce, while on the other hand remaining flexible and open enough to allow for new technological developments, for example in the field of biometrics, to act as an incentive for the development of electronic commerce: this would then provide a basis

for the establishment of technical specifications for the industry in the form of standards and the like;

13. Considers that one aim should be the legal recognition of digital signatures, taking admission as evidence in legal procedures and equivalence with written forms as the main basic principles;

14. Stresses the importance of mutual recognition by the Member States of digital signatures and consequently underlines the importance of drawing up 'essential requirements' at European level for digital signatures, allowing Member States to set higher standards provided that such additional standards are proportional and do not obstruct the importation of goods and services from other Member States;

15. Believes that the system of 'essential requirements' will make it possible for Member States on the one hand to generate confidence in the quality and reliability of the certification regulations in the Member States and on the other to allow the Member States to decide whether or not to operate a system of permits in this field;

16. Hopes at all events that the directive on digital signatures will provide for so-called cross-border certification, possibly with an authority to which third parties from other Member States can apply for a guarantee that certification has taken place in the Member State concerned;

17. Believes that common conditions must be laid down for the setting up and operation of certification bodies, with an obligation to register and to be independent with regard to the parties to which certificates are granted: it is recommended that each Member State should have at least one accredited body to supervise compliance with these conditions in an objective, non-discriminatory and transparent way, since this will increase confidence in the market and will also benefit the international investment climate;

18. Notes that rapid technological development of electronic commerce and, in connection with this, the proliferation of new services mean that there is no uniform model for the location of certification functions - such as the verification of identity, the granting of certificates, the cancellation of certificates and the registration of the point in time at which electronic contracts are concluded - in one or several organisations, making it desirable for the time being to allow the process to crystallize;

19. Urgently requests that a clear distinction be made between authentication and integrity services on the one hand and confidentiality services on the other and calls on the Commission to draw up without delay proposals for a directive on digital signatures, principally for the benefit of electronic commerce, employment and the competitive position of the European Union in this field; calls on the Commission to keep a close eye on new legislation initiatives in this field in the Member States in order to facilitate the proper operation of the single market;

20. Considers that, with a view to the single market, the regulation on dual-use goods should be amended to the effect that internal Community checks on encryption products are abolished, so that there is freedom of circulation for commercial encryption products;

21. Calls on the Member States, during the discussions concerning the Wassenaar Agreement and the forthcoming proposal for the amendment of the regulation on dual-use goods, to advocate that the list of encryption products subject to export restrictions be reduced to a strict minimum and that, consequently, no new restrictions should be introduced;

22. Stresses the importance of international dialogue between the European Union and various international organizations such as the OECD, UN, ITU, ICC and WTO, to avoid a situation in which regulations form a barrier to trade with major trading partners, and underlines the need for reciprocity in the treatment of the European Union by other trading partners;

23. Believes that adequate funds must be earmarked in the European Union's Fifth Framework Programme for Research and Development to give the European industry an incentive to make a greater effort in field of cryptography, and in the field of standardisation and products which are interoperable with American standards, or have a common interface with them;

24. Encourages all sectors of society, and particularly European industry, to develop common standards in this field not only at national level but also at international level bearing in mind the importance of ensuring that such standards comply with best practice and the state of the art;

25. Considers that electronic commerce may become one of the driving forces behind the development of the global information society. However, the lack of security and trust on open networks poses a threat to this new 'virtual' economic space, a source of great potential for job creation;

26. Stresses the fact that European Union action is essential in order to establish a set of common rules which facilitates the free movement of goods and services and electronic commerce on the Internet, whilst ensuring the security of encryption technologies and the recognition of digital signatures and encryption amongst Member States. Such recognition will serve to develop the services on offer in the Community and the legal regulation within the European Union of certification authorities, whose monitoring activities will, inter alia, help establish respect for copyright and for the protection of privacy on the one hand, and a climate of trust on the other;

27. Believes that establishing a European framework for encryption does indeed have its merits, despite the controversy surrounding illicit use, since such a framework would play an important role in developing electronic commerce and guaranteeing the fundamental right to privacy and to communication without interference, as enshrined in the constitutions of the Member States, Article 12 of the Universal Declaration of Human Rights and Article 8 of the European Convention on Human Rights;

28. Recalls that electronic communication transcends the geographical confines of the European Union, and that, for that reason, adopting a harmonized Community system with regard to digital signatures and encryption should also lead the Community to take the initiative in negotiations and dialogue with other international bodies such as the OECD (Organization for Economic Cooperation and Development) and the WTO (World Trade Organization);

29. Supports the programmes introduced by the Commission, especially INFOSEC II, and the research projects under the 5th framework programme (1998-2002) on electronic commerce,

particularly on techniques designed to improve the protection of privacy and personal information. Lastly, EU institutions should be encouraged to use digital signatures and encryption as a means of helping spread and build up trust in these new technologies;

30. Instructs its President to forward this resolution to the Commission and the Council.

B
EXPLANATORY STATEMENT

1. The issues

The Commission takes the view that 'electronic commerce will be one of the driving forces for the development of the global information society'.

This is undoubtedly true but it is important not to overlook the fact that technologies such as digital signatures and encryption are not only important for commerce but are becoming increasingly relevant to citizens in their daily lives and in their relations with the public authorities.

Electronic commerce, like conventional commerce, involves the conclusion of contracts. Such contracts are based on the exchange of declarations of intent that are generally given in written form. This means, for example, under German law that the document containing the declaration of intent must be signed by the party making it in his or her own hand or bear a certified handwritten signature (paragraph 126(1) of the German Civil Code). The signature must be made by hand; mechanical copies such as signature stamps and communications by telegram or telex, and the like are not sufficient unless an exception is allowed by law.

Compared with conventional commerce, electronic commerce on open networks, i.e. networks that are accessible to the general public, raises three problems in respect of the criteria and requirements described above, which must basically be the same in all European legal systems.

1.1. Authentication

The signature requirement for written declarations of intent is designed to ensure that in legal contracts a specific declaration can be attributed legally to an individual.

In electronic commerce the signature of a physical person is replaced by a so-called digital signature. A digital signature is a data string created using a private key. A valid signature can only be given if the private key is known. A procedure for authentication of the data string allows the receiver to verify that the digital communication comes from the sender. (For details see Annex I of the Commission communication).

All Member States of the EU recognize the need for regulation. France has a new telecommunications law, Germany has a law on digital signatures and Italy has a law on the use of electronic documents and contracts. In the United Kingdom, the Netherlands, Belgium, Denmark and Sweden, legislation is in preparation (see page 15 of the Commission communication). There is a risk that divergent legal approaches would adversely affect operation of the internal market.

1.2. Integrity

Electronic commerce not only fails to ensure the authentication of a communication but also that the content of a communication cannot be altered inadvertently or by a third party during transmission (integrity). The technical solution to this problem again lies in the use of a digital signature, involving not encryption of the text itself but solely encryption of the signature which is attached to the normal readable text and enables the receiver to check whether the data has been changed.

1.3. Confidentiality

In the Commission's view, electronic commerce and many other applications of the information society will only expand and unfold their economic and social benefits if confidentiality can be assured in a user-friendly and cost-efficient way (Commission communication, page 9). It is obvious that when consumers use services such as teleshopping or telebanking they have to be sure that personal data such as credit card numbers remain secret. In commercial contacts on open networks firms have to be able to protect themselves against industrial espionage relating to their business plans, invitations to tender and research results.

On the other hand, law enforcement authorities and national security agencies fear that more widespread use of encrypted communication may hinder them in the fight against crime.

France is so far the only Member State with public regulation of encryption; the use of cryptography has been subject to prior declaration in individual cases and prior authorization in all other cases since 1990 (Commission communication, page 12).

2. Solutions proposed by the Commission

2.1. Authentication

In electronic communication, the concept of digital signatures is linked to the use of a kind of electronic seal which is affixed to the data and which allows the recipient to verify the origin of the data or, more accurately, the use of a key assigned to a certain sender. However, authentication of the data source does not necessarily prove the identity of the owner of the key. The recipient of the message cannot, for instance, be sure whether the sender is really the one he claims to be. The 'public' key may be published under another name. One way for the recipient to obtain reliable information on the identity of the sender is confirmation by a third party, i.e. a person or institution mutually trusted by both parties. In the context of digital signatures, these third-parties are most commonly so-called certification authorities (for details see Commission communication, pages 3-9).

The Commission communication fails to propose a clear approach to solving these new problems of authentication.

On the one hand reference is made to the principle of mutual recognition:

> 'In a fully international framework for electronic commerce certificates issued by foreign CAs (certification authorities) must be mutually recognized in different countries ... National structures could be complemented by a coordination mechanism at the European level ...'.

Later it refers to the possibility of a uniform certification procedure:

> 'Other possibilities of ensuring cross-border recognition of certificates could be harmonised European certification services (including the procedures concerning the issuance of such a certificate) as well as common evaluation criteria and procedures.'([1])

([1]) Both quotations from point 2.4. of the Communication.

Finally the Commission gives the impression that it has made little progress in its efforts to develop a Community legal framework:

> 'The Commission will evaluate the possibility to provide for the harmonization of the different national provisions to support international mutual recognition of digital signatures'([1]).

2.2. Integrity

As mentioned earlier, technically the most effective digital signatures have been proved to consist of two keys: a 'public key' which is published and a 'private key' which is confidential. The relevant public key is used to check whether the signature has in fact been created using the private key. The recipient can also use the public key to check whether the data has been changed. This enables the recipient to check whether the sender's public and private keys form a complementary pair and whether the data has been changed during transmission.

A certification authority need not be involved at this stage and the Commission therefore makes no mention of the need for regulation.

2.3. Confidentiality

On 22 September 1997 the Commission submitted to Parliament a proposal for a directive on the legal protection of encrypted services. The Legal Affairs Committee will shortly be voting on a draft report by its rapporteur Mr Anastassopoulos. The proposal primarily concerns the protection of copyright and industrial secrets which, like protection of privacy, make the possibility of encryption essential in open networks.

The Commission is much more cautious when it comes to the corresponding right of the public to protection from the misuse of such encryption technology (for example espionage, terrorism and crime). Any regulation hindering the use of encryption products and services throughout the internal market thus hinders the secure and free flow of personal information and the provision of related goods and services. Criminals cannot be entirely prevented from having access to strong encryption and from bypassing escrowed encryption. Benefits of regulation for crime fighting are therefore not easy to assess and often expressed in fairly general language([2]).

The Commission does not see this as being an area for priority action. It will therefore confine itself to examining whether national regulations, such as the French law of 29 December 1990 on cryptography, are 'totally or partially justified, notably with respect to the free circulation provisions of the Treaty, the case law of the Court of Justice and the requirements imposed by the data protection directive'([3]).

3. Assessment

([1]) Point 3 of the Communication.
([2]) Commission communication, p. 14-15.
([3]) Commission communication, p. 17.

Of the three issues dealt with in the communication, the problem of authentication of electronic communication is the first that the Commission could and should tackle. The matters that should be dealt with are those covered by the German law on digital signatures of 22 July 1997, although that law does not deal with the question of digital signatures in the context of civil law.

The Commission's failure to tackle this area before now is all the more difficult to understand since it repeatedly states in its communication that 'a common framework at Community level is urgently needed and should be put in place at the latest by the year 2000'([1]).

The problem of the integrity of electronic communication will probably be solved if the system of two complementary 'public' and 'private' keys becomes general practice. There should consequently be no need for action at Community level.

The problem of confidentiality or data encryption is likely to remain controversial for some time to come. The Commission is clearly committed to promoting the new market for encryption technologies, services and products and regards the development of this market as essential for the information society.

([1]) Commission communication, p. 16.

23 April 1998

OPINION
(Rule 147)

for the Committee on Legal Affairs and Citizens' Rights

on the communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on ensuring security and trust in electronic communication - towards a European framework for digital signatures and encryption (COM(97)0503 - C4-0648/97); report by Mr Wolfgang Ullmann

Committee on Economic and Monetary Affairs and Industrial Policy

Draftsman: Mr W.G. van Velzen

PROCEDURE

At its meeting of 21 January 1998 the Committee on Economic and Monetary Affairs and Industrial Policy appointed Mr W.G. van Velzen draftsman.

It considered the draft opinion at its meetings of 24 March and 23 April 1998.

At the last meeting it adopted the following conclusions unanimously.

The following were present for the vote: Karl von Wogau, chairman; Katiforis and Secchi, vice-chairmen; W.G. van Velzen, draftsman; Areitio Toledo, Argyros (for de Brémond d'Ars), Arroni, Boogerd-Quaak (for Gasòliba i Böhm), Camisón Asensio (for Fourçans), Carlsson, Cassidy (for Friedrich), Caudron, Christodoulou, Cox, Donnelly, Filippi (for García-Margallo y Marfil), Funk (for Konrad), Glante, Harrison, Herman, Hoppenstedt, Ilaskivi, Kestelijn-Sierens, Kuckelkorn, Langen, de Lassus (for Castangède), Lindqvist (for Larive), Lulling, Erika Mann (for Berès), Thomas Mann (for Mather), Metten, Mezzaroma, Miller, Murphy, Paasilinna, Peijs, Pérez Royo, Peter (for Billingham), Porto (for Rübig), Rapkay, de Rose, Skinner (for Read), Soltwedel-Schäfer, Tappin (for Wibe), Thyssen, Torres Marques, Watson and Wolf (for Hautala).

BACKGROUND

1. Introduction

Open networks such as the Internet are being used more and more for electronic communication and electronic commerce. This development can make a significant contribution to the world-wide development of the information society. For the European Union, further development of electronic commerce offers considerable opportunities for economic growth and job creation. At the same time normal users can also profit more and more from new forms of electronic communication and

commerce. The lack of security inherent in open networks does however hamper optimum use of the advantages of electronic commerce and communication. Reports can be intercepted and altered, the
validity of documents can be repudiated and personal data can be collected illegally. Cryptographic technologies such as digital signatures and encryption can make a big contribution to the security of open networks and people's confidence in them. A number of Member States have already introduced legislation on the subject or made known their intention of doing so. But having a variety of systems of legislation is not conducive to the operation of the single market. This is why the establishment of a common policy on digital signatures and encryption for the European Union is an essential prerequisite for the success of electronic commerce in Europe.

2. Digital signatures

Digital signatures are already a generally accepted answer to the lack of security in the use of open networks. This does not mean that new technologies will not provide other solutions in the future. The legislation must therefore not be conditioned by present technology, meaning that it should be flexible enough to be adapted to new technological developments. At the same time the legislation should be transparent enough to communicate confidence to the user. Confidence that transactions will really be carried out, and confidence in the true identity of purchaser and seller are essential, together with confidence that communication between the two trading partners will be undisturbed and undistorted.

In response to the question of whether the sender of a report is really who he claims to be, resort is usually had to a certification authority to verify the identity of the person concerned. This authority may, for instance, have a register of approved certificates and when they are due to expire. The rapid development of the market has meant a proliferation of organisations providing parts of the certification authority function but there is certainly no standard model.

Lack of Community rules can be an obstacle to cross-border confidence in certification authorities. In the interest of the mutual recognition of certificates for digital signatures it is very important to draw up common European certification criteria. 'Essential requirements' must be laid down at European level. This will give Member States the freedom to choose whether they want a system of permits or voluntary self-regulation, always provided that the essential requirements are met. Anyone satisfying the essential requirements will be able to supply goods and services throughout the Union. There may also be a need for various categories of certificates to ensure that levels of security of and confidence in certificates is the same in all the Member States.

Bearing in mind the heated discussion surrounding access rules for encryption keys, it is very important to make a clear distinction between authentication and integrity services (digital signatures) on the one hand and confidentiality services (encryption) on the other.

3. Encryption

The encryption of data is now the most important means of ensuring the confidentiality of electronic communications and electronically stored documents. The rapid growth in demand for encryption products throughout the world is also creating increased opportunities for industry and employment in Europe. Europe has considerable opportunities in this field as long as it creates a conducive climate. This means a more concentrated research effort in this field and the development of interoperable European products and better standardisation. European citizens and companies have

a right to the best possible security conditions for their financial transactions. And here Europe must not allow itself to depend on whether or not - for reasons best known to itself -the American Administration grants export permits for cryptography.
Investigation and security services are calling for legal regulations on access to encryption keys for reasons of national security and combatting crime and terrorism. The disadvantages of this are, however, an increased possibility of misappropriation, invasion of privacy, cost and reduced efficacy. A further question is whether the storage of keys will not reduce user confidence in electronic communications. One solution would be to stipulate that access must be made available to encrypted information whenever there is a legally authorised application for this. This would be possible if everyone was obliged to deposit their personal key with a 'Trusted Third Party'. The criteria for complying with such an application are: necessity, efficacy and proportionality. The problem is that the law-abiding citizen would most probably make his key available, whereas criminal elements would not. The measure could therefore be expected not to be commensurate with the result. Furthermore, such limitative measures represent a considerable obstacle to the development of goods and services on the encryption market. So we would definitely advise against legal access rules. In any case, France is the only EU country to have legislation on encryption.

4. International dialogue

Article 19 of Council Regulation (EC) 3381/94 setting up a Community regime for the control of exports of dual-use goods includes a clause on the need for a re-examination of these measures within three years from the date of entry into force of the Regulation. These three years expired at the end of 1997. With an eye to the single market, this Regulation should be amended to the effect that internal Community controls on encryption products are phased out. A reservation could be made in the case of very advanced encryption, i.e. for military purposes and diplomatic traffic. It is at all events important to enable commercial cryptography products for electronic commerce to circulate freely on the market.

In view of the cross-border nature of electronic communications it is very important to set up an international dialogue between various international organisations such as the OECD, UN, WIPO, ITU, ILO, ICC and WTO. It is also important to avoid Europe's 'essential requirements' becoming a barrier to trade with major trading partners such as the United States and Japan.

5. Conclusions

The Committee on Economic and Monetary Affairs and Industrial Policy calls on the Committee on Legal Affairs and Citizens' Rights, as the committee responsible, to incorporate the following conclusions in its report:

1. Believes that it is necessary for the further development of electronic commerce to engender sufficient user confidence and to formulate rules with regard to the legal reliability of, inter alia, identification, validity in law of contracts, integrity and communications;

2. Stresses that general rules must be established leading on the one hand to greater confidence in electronic commerce, while on the other hand remaining flexible and open enough to allow for new technological developments, for example in the field of biometrics, to act as an incentive for the development of electronic commerce: this would then provide a bases

for the establishment of technical specifications for the industry in the form of standards and the like;

3. Considers that one aim should be the legal recognition of digital signatures, taking admission as evidence in legal procedures and equivalence with written forms as the main basic principles;

4. Stresses the importance of mutual recognition by the Member States of digital signatures and consequently underlines the importance of drawing up 'essential requirements' at European level for digital signatures, allowing Member States to set higher standards provided that such additional standards are proportional and do not obstruct the importation of goods and services from other Member States;

5. Believes that the system of 'essential requirements' will make it possible for Member States on the one hand to generate confidence in the quality and reliability of the certification regulations in the Member States and on the other to allow the Member States to decide whether or not to operate a system of permits in this field;

6. Hopes at all events that the directive on digital signatures will provide for so-called cross-border certification, possibly with an authority to which third parties from other Member States can apply for a guarantee that certification has taken place in the Member State concerned;

7. Believes that common conditions must be laid down for the setting up and operation of certification bodies, with an obligation to register and to be independent with regard to the parties to which certificates are granted: it is recommended that each Member State should have at least one accredited body to supervise compliance with these conditions in an objective, non-discriminatory and transparent way, since this will increase confidence in the market and will also benefit the international investment climate;

8. Notes that rapid technological development of electronic commerce and, in connection with this, the proliferation of new services mean that there is no uniform model for the location of certification functions - such as the verification of identity, the granting of certificates, the cancellation of certificates and the registration of the point in time at which electronic contracts are concluded - in one or several organisations, making it desirable for the time being to allow the process to crystallize;

9. Notes that a water-tight regulation of liability is essential for confidence in the use of cryptographic products, but believes that for the time being there is no need for supplementary rules on liability at European level, given that the present rules in this field are still adequate, although this does not mean that Member States may not draw up supplementary rules on liability, related amongst other things to the volume of the contracts, as long as this does not create any obstacles to the importation of goods and services from other Member States, and calls on the Commission to keep a close eye on developments in this field and, if necessary, to propose appropriate European measures;

10. Urgently requests that a clear distinction be made between authentication and integrity services on the one hand and confidentiality services on the other and calls on the Commission to draw up without delay proposals for a directive on digital signatures,

principally for the benefit of electronic commerce, employment and the competitive position of the European Union in this field; calls on the Commission to keep a close eye on new legislation initiatives in this field in the Member States in order to facilitate the proper operation of the single market;

11. Emphasizes that legal rules on access to keys should not be introduced, as the measure is not commensurate with the expected result, particularly in view of the increased possibility of misappropriation of the keys, invasion of personal privacy, cost, and lack of efficacy;

12. Considers that, with a view to the single market, the regulation on dual-use goods should be amended to the effect that internal Community checks on encryption products are abolished, so that there is freedom of circulation for commercial encryption products;

13. Calls on the Member States, during the discussions concerning the Wassenaar Agreement and the forthcoming proposal for the amendment of the regulation on dual-use goods, to advocate that the list of encryption products subject to export restrictions be reduced to a strict minimum and that, consequently, no new restrictions should be introduced;

14. Stresses the importance of international dialogue between the European Union and various international organizations such as the OECD, UN, ITU, ICC and WTO, to avoid a situation in which regulations form a barrier to trade with major trading partners, and underlines the need for reciprocity in the treatment of the European Union by other trading partners;

15. Believes that adequate funds must be earmarked in the European Union's Fifth Framework Programme for Research and Development to give the European industry an incentive to make a greater effort in field of cryptography, and in the field of standardisation and products which are interoperable with American standards, or have a common interface with them;

16. Encourages all sectors of society, and particularly European industry, to develop common standards in this field not only at national level but also at international level bearing in mind the importance of ensuring that such standards comply with best practice and the state of the art.

OPINION
(Rule 147 of the Rules of Procedure)

for the Committee on Legal Affairs and Citizens' Rights

on the communication from the Commission on ensuring security and trust in electronic communication - towards a European framework for digital signatures and encryption (COM(97) 503 final - C4-0648/97)
(report by Mr Wolfgang Ullmann)

Committee on Culture, Youth, Education and the Media

Letter from the committee chairman to Mr Willy De Clercq, chairman of the Committee on Legal Affairs and Citizens' Rights

---

Brussels, 22 April 1998

Dear Mr De Clercq,

The Committee on Culture, Youth, Education and the Media considered the above subject at its meeting of 22 April 1998.

At the meeting it adopted the following conclusions([1]):

1. The Committee on Culture, Youth, Education and the Media considers that electronic commerce may become one of the driving forces behind the development of the global information society. However, the lack of security and trust on open networks poses a threat to this new 'virtual' economic space, a source of great potential for job creation.

2. European Union action is essential in order to establish a set of common rules which facilitates the free movement of goods and services and electronic commerce on the Internet, whilst ensuring the security of encryption technologies and the recognition of digital signatures and encryption amongst Member States. Such recognition will serve to develop the services on offer in the Community and the legal regulation within the European Union of certification authorities, whose monitoring activities will, *inter alia*, help establish respect for copyright and for the protection of privacy on the one hand, and a climate of trust on the other.

3. Concern should be voiced at the potential illicit use of encryption which exploits confidentiality to further criminal and terrorist activities; a distinction must be drawn

---

([1]) The following took part in the vote: Pex, chairman; Hawlicek and Ahlqvist, vice-chairmen; Añoveros Trias de Bes, Banotti, Daskalaki (for Boniperti), De Esteban Martin (for Heinisch), Elchlepp (for De Coene), Fontaine, Guinebertière, Günther (for de Escudero), Kerr, Kuhne, Mouskouri, Pack, Ryynänen, Sanz Fernández and Todini (for Poisson).

between encryption and digital signatures, which are employed to prevent fraud by means of authentication and guarantees of integrity and to protect consumer transactions.

4. Establishing a European framework for encryption does indeed have its merits, despite the controversy surrounding illicit use, since such a framework would play an important role in developing electronic commerce and guaranteeing the fundamental right to privacy and to communication without interference, as enshrined in the constitutions of the Member States, Article 12 of the Universal Declaration of Human Rights and Article 8 of the European Convention on Human Rights.

5. Electronic communication transcends the geographical confines of the European Union, and for that reason, adopting a harmonized Community system with regard to digital signatures and encryption should also lead the Community to take the initiative in negotiations and dialogue with other international bodies such as the OECD (Organization for Economic Cooperation and Development) and the WTO (World Trade Organization).

6. Support should be given to the programmes introduced by the Commission, especially INFOSEC II, and to research projects under the 5th framework programme (1998-2002) on electronic commerce, particularly on techniques designed to improve the protection of privacy and personal information. Lastly, EU institutions should be encouraged to use digital signatures and encryption as a means of helping spread and build up trust in these new technologies.

Yours sincerely,

(sgd) Peter Pex