Procedure file

Basic information

COS - Procedure on a strategy paper (historic)	1997/2235(COS)	Procedure completed
Security in electronic communication: digital signatures and encryption Subject 3.30.05 Electronic and mobile communications, personal communications 3.30.06 Information and communication technologies, digital technologies		

Key players

European Parliament	Committee responsible	Rapporteur	Appointed
	JURI Legal Affairs, Citizens' Rights	V ULLMANN Wolfgang	27/11/1997
	Committee for opinion	Rapporteur for opinion	Appointed
	ECON Economic and Monetary Affairs, Industrial Policy	PPE VAN VELZEN W.G.	21/01/1998
	ENVI Environment, Public Health and Consumer Protection	The committee decided not to give an opinion.	
Council of the European Union	Council configuration	Meeting	Date
	Justice and Home Affairs (JHA)	2099	28/05/1998
	Telecommunications	2054	01/12/1997

Key events

06/10/1994	Additional information		Summary
08/10/1997	Non-legislative basic document published	COM(1997)0503	Summary
01/12/1997	Debate in Council	2054	
15/12/1997	Committee referral announced in Parliament		
19/05/1998	Vote in committee		Summary
19/05/1998	Committee report tabled for plenary	A4-0189/1998	
28/05/1998	Resolution/conclusions adopted by Council		
16/07/1998	Debate in Parliament		
17/07/1998	Decision by Parliament	T4-0457/1998	Summary
17/07/1998	End of procedure in Parliament		

21/09/1998	Final act published in Official Journal		

Technical information

Procedure reference	1997/2235(COS)
Procedure type	COS - Procedure on a strategy paper (historic)
Procedure subtype	Commission strategy paper
Legal basis	Rules of Procedure EP 050; Rules of Procedure EP 142
Stage reached in procedure	Procedure completed
Committee dossier	JURI/4/09386

Documentation gateway

Non-legislative basic document		COM(1997)0503	08/10/1997	EC	Summary
Economic and Social Committee: opinion, report		CES0443/1998 OJ C 157 25.05.1998, p. 0001	25/03/1998	ESC	
Committee report tabled for plenary, single reading		A4-0189/1998 OJ C 195 22.06.1998, p. 0004	19/05/1998	EP	
Text adopted by Parliament, single reading		T4-0457/1998 OJ C 292 21.09.1998, p. 0206-0217	17/07/1998	EP	Summary

Security in electronic communication: digital signatures and encryption

PREVIOUS COMMUNITY LEGISLATION: No legislation has yet been adopted at Community level concerning the encryption of telecommunications. On 31 April 1992 the Council adopted a Commission proposal[(2) Proposal COM(90)0314, OJ C 277, 5.11.1990, p.18] for a decision in the field of information security[(3) Decision 92/242/EEC, OJ L 123, 8.05.1992, p.19]. It involved the adoption of a 24-month action plan and the establishment of a Senior Officials Group on Information Security (SOGIS), comprising two representatives from each Member State and the Commission, with a mandate to advise the Commission. PREVIOUS POSITION OF THE EP: When it considered the proposal for a Council directive concerning the protection of individuals in relation to the processing of personal data[(4) COM(90)0314, OJ C 277, 5.11.1990, p. 3; opinion of the EP A3-0010/92 on the basis of a report by Mr Geoffrey W. Hoon, OJ C 94, 13.04.1992, p. 76,77, 173, 198; amended proposal COM(92)0422 final, OJ C 311, 27.11.1992, p. 30 and COM(93)0570.], Parliament did not amend Article 18 stipulating that the controller of a file must take appropriate technical and organizational measures to protect personal data from communication or any other unauthorized use. SITUATION IN THE MEMBER STATES: The Member States need to be able to monitor telecommunications closely and rapidly, as part of their policy for combating crime and espionage, by means of telephone tapping and intercepting exchanges of data. This clashes with the interests of individuals who wish to preserve a sphere of freedom and private life which the police and counter-espionage services could tend to restrict in the name of public security. Commercial groups have a similar interest in the area of commercial secrecy. However, they will also be concerned to retain the possibility of developing, producing and marketing encoding systems free of administrative constraints and without being restricted by the standardization of a system which would hold up progress in this field. France is currently the only country in the Community with a law on encryption systems (Law of 29 December 1990). Previously subject to the strict rules governing military equipment, these systems are now subject to: * a declaration procedure where they are designed to authenticate a communication or verify that a message transmitted is intact, * a more binding licensing procedure where they do not fall within the above category, the application for authorization being submitted with the encoding key to the information security service attached to the Prime Minister's office. Simplified procedures may be adopted. In the other Member States, encryption systems are freely used and freely sold, unless of course the user is bound by the rules governing state secrets or national defence. However, many countries are concerned at the proliferation of encoded telecommunications, both in the GSM network used by radiotelephones and in the exchange of electronic data. The Netherlands is an example of this attitude. A law on computer crime came into force on 1 March 1993, which provides a specific legal basis for the interception of the exchange of data, the searching of computer systems and the obtaining of decrypted data or decoding keys. In addition, a draft law of May 1994 sought to make users of encryption systems subject to a procedure for licensing and registration of code keys with a special agency bound to secrecy. The agency was to pass the keys on to the police and security services which would be given appropriate powers. Following a leak to the press, the many protests which ensued forced the government to abandon its plans. American policy is important in this field. The NSA has pursued a deliberate policy of preventing the export of sophisticated encoding systems, and promoting in communications with the authorities a standard system known as the 'Clipper chip', to which it was thought to have a universal key. The widespread use of this system would also have allowed it to consider as suspect any other form of encoding, using for example the 'Pretty Good Privacy' (PGP) software which has been transmitted widely on the Internet by its author to fight against the policy of the American government. However, faced by the reluctance of American business and private associations the efforts of the NSA and Vice-President Al Gore have failed.

Security in electronic communication: digital signatures and encryption

OBJECTIVE: defining a European policy to ensure security and trust in electronic communication and digital signatures. SUBSTANCE: the Commission's document indicates that, if nothing is done soon, the development of electronic commerce could be hampered by the insecurities typical to open networks such as Internet. Messages may be intercepted and manipulated, the validity of documents can be denied and personal data can be illicitly connected. Cryptographic technologies for instance, digital signatures and encryption may provide an essential tool for security and trust on open networks. Several Member States have already announced their intention of introducing specific regulations in this area and some of have already done so. However, divergent practices (or the absence of regulation) could constitute a serious barrier to electronic commerce. Accordingly, the objective of the Commission communication is to develop a European policy in this area. Legislative proposals could be presented as soon as 1998 in the light of responses to proposals contained in this communication. In particular, the Commission considers that a Community strategy should contain the following elements: 1) In the field of digital signatures: - laying down common legal requirements for certifying authorities (CAs) so as to create a framework for the mutual recognition of certificates issued by CAs; - establishing equivalent legal recognition for digital and conventional signatures; - encouraging international cooperation to create a suitable framework for worldwide electronic commerce and in particular establish common technical standards and commence the mutual recognition of certificates. 2) With regard to encryption: the Commission considers that encryption is frequently the only effective means of protecting data and communications on open networks. As far as the national authorities are concerned the large-scale use of encrypted communication could diminish their capacity to fight against organized crime. In this respect, the Treaty fully respects the competences of the Member States in the field of national security. However, national restrictions should not hamper electronic commerce and infringe Community law. The Commission will therefore examine national restrictions in the light of existing provisions concerning freedom of movement, the principle of proportionality, Directive 83/189/EEC concerning standards and technical regulations and Directive 95/46/EC on the protection of personal data. Additional measures could be envisaged with a view to strengthening the control of encryption (for example adjustment of Regulation (EC) No 3381/94 on the control of exports of dual-use products, improving the cooperation between police forces and the conclusion of international agreements). Finally, the following accompanying measures could be envisaged as of 1998: 1) encouraging the industry and international standardization bodies to develop their interoperable technical and infrastructural standards for digital signatures and encryption; 2) proposal for a Council and Parliament decision for an INFOSEC II programme (development of overall strategies for the security of electronic communications); 3) launching of new projects in the framework of the fifth RTD framework programme in the field of electronic communications; 4) encouraging the utilization of digital signatures and encryption by the Community's and public authorities; 5) creation of a European Internet forum as a means of information and exchange; 6) organization of an international hearing of experts on digital signatures and encryption. ?

Security in electronic communication: digital signatures and encryption

The Committee adopted the report by Wolfgang ULLMANN (Greens, D) on a Commission paper on security and trust in electronic telecommunication. Electronic commerce is set to be one of the driving forces behind the development of the global information society. The new technology will become increasingly important for people in their everyday lives and not just in commerce. The report calls on the Commission and 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. It stresses the importance of international dialogue between the European Union and various international organizations such as the OECD, UN, ITU, ICC and WTO, so as to avoid a situation in which regulations form a barrier to trade with major trading partners. At the same time, the committee underlines the need for reciprocity in trade relations. The general rules designed to strengthen trust in this area also need to be sufficiently flexible to allow for the incorporation of new technical developments. Lastly, the committee believes that the development of a market in data encryption could, despite controversy concerning illicit uses of this technique, be of considerable value to the development of electronic commerce as well as guaranteeing the fundamental right to privacy and confidentiality in communications.?

Security in electronic communication: digital signatures and encryption

Adopting the report by Mr Wolfgang Ullmann (Green, D) on security and trust in electronic communication, Parliament called for a legal framework to be created to ensure mutual trust in digital signatures and confidentiality, and for the legal framework to be designed primarily to abolish national restrictions on certification. Steps should be taken to remove obstacles to the use of digital signatures in the legal system, industry and public administration, and every effort made to ensure that digital and conventional signatures had the same status in law. European Union institutions should lead the way in the use of digital signatures. Parliament also called 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. Parliament underlined the importance of international dialogue between the European Union and various international organizations (OECD, UN, ITU, ICC and WTO) to avoid a situation in which regulations formed a barrier to trade with major trading partners and underlined the need for reciprocity in the treatment of the European Union by other trading partners. It stressed the importance of mutual recognition of digital signatures between Member States and the need to define minimum standards at European level, allowing Member States to generate confidence in the quality and reliability of the certification regulations; if necessary, Member States could set higher standards. With regard to the directive on digital signatures, Parliament called for it to provide for cross-border certification, possibly with an authority to which third parties from other Member States could apply for a guarantee that certification had taken place in the Member State concerned. Common conditions also had to be laid down for the setting-up and operation of certification bodies; each Member States should have an accrediting body to supervise compliance with these conditions in an objective, non- discriminatory way. General rules to reinforce confidence had to be sufficiently flexible to take account of new technological developments. Parliament considered that developing an encryption market could, despite the controversy surrounding the illicit use, play an important role in developing electronic commerce and guaranteeing the fundamental right to privacy and to communication without interference. It called on European enterprises to establish common rules in this area at national and international level to promote the development of digital signatures. ?