EUROPEAN UNION
THE COUNCIL

Brussels, 14 April 1998

7622/98

LIMITE

ENFOPOL 52

NOTE

from : Presidency

to : K.4 Committee

No. prev. doc. : 6051/1/98 ENFOPOL 19 REV 1

Subject : **Draft Council conclusions on encryption and law enforcement**

INTRODUCTION

Justice and Home Affairs Ministers discussed encryption at the Informal Council on 29/30 January and work has been taken forward subsequently in the Police Co-operation Working Group. At its meeting on 20 March the Working Group agreed to invite the Justice and Home Affairs Council to adopt formal conclusions on encryption and law enforcement. There is also a need for the Justice and Home Affairs Council to respond to the conclusions of the Telecommunications Council on 1 December 1997 (see doc. 12759/97 ECO 290) by explaining the law enforcement interests in the provision of cryptographic services to protect the confidentiality of information.

The Presidency has prepared the attached draft formal conclusions for the Justice and Home Affairs Council in May (see Annex). It was agreed at the Working Group's meeting on 20 March that the formal conclusions should reflect conclusions 1-4 and 9-15 in doc. 6051/1/98 ENFOPOL 19 REV 1.

K4 Committee is therefore asked to endorse the formal conclusions for the Justice and Home Affairs Council on 28/29 May on encryption and law enforcement and to forward them to the Council for adoption.

SUMMARY OF ISSUES

The intention of the draft Council Conclusions is to register the importance of law enforcement issues in developing policies on cryptographic services and products which are used for confidentiality purposes, whilst recognising the benefits of such services for electronic commerce and the individual. It is therefore important that the draft Council Conclusions complement the work underway in the First Pillar on the provision of cryptographic services for digital signature purposes.

Many Member States are still developing their national policies on the provision of cryptographic services. However, the Working Group has concluded that the widespread availability of cryptographic services for confidentiality purposes may have a serious impact on the fight against serious crime and terrorism if, where necessary and appropriate, it is not possible to get lawful access to encryption keys on a case by case basis. The Working Group has therefore agreed to monitor closely the extent to which encryption is exploited by serious criminals and terrorists.

The most immediate and serious implications of the widespread availability of such services will be on the lawful interception of communications. The Working Group has therefore concluded that law enforcement agencies may require lawful access to encryption keys, without the knowledge of the user of the cryptographic service, in order to maintain their interception capabilities. To this end, there may be a law enforcement interest in promoting the use of confidentiality services which involve the depositing of an encryption key or other information with a third party. Such services are often known as "key escrow" or "key recovery" services.

The Presidency believes it is important to reach agreement at the Justice and Home Affairs Council in May on how this work should be taken forward. In particular, there is a need to establish a common understanding of the needs of law enforcement agencies where cryptographic services are used for confidentiality purposes. A Council Resolution on Encryption and Law Enforcement would provide a focus for future work in this area. The Council Resolution would not, however, be prescriptive. It would invite Member States to take account of law enforcement needs in their national policies, but it would not require them to do so. Work on such a draft Resolution will be taken forward in the Police Co-operation Working Group.

Draft Conclusions of the Council (Justice and Home Affairs)

Encryption and Law Enforcement

1. The Telecommunications Council on 1 December 1997 welcomed the Commission Communication entitled "Security and Trust in Electronic Communication - towards a European framework for digital signatures and encryption". In acknowledging that the use of encrypted communications may diminish the capacity of Member States to fight crime and to maintain their national security, the Telecommunications Council noted the need to discuss relevant aspects of the Communication with the Justice and Home Affairs Council to ensure a co-ordinated approach. It also drew attention to the need to distinguish between authentication and integrity products and services on the one hand, and confidentiality products and services on the other.

2. There was an informal discussion of law enforcement issues associated with the Communication at a meeting of Justice and Home Affairs Ministers in Birmingham on 29/30 January 1998. Further consideration has now been given to law enforcement interests where cryptographic products and services are used for confidentiality purposes.

3. The Council acknowledges that the use of cryptographic services to ensure the integrity and confidentiality of digital communications not only has substantial benefits for electronic commerce and the privacy of individuals, but is also important for the prevention of crimes such as fraud. However, the Council is also aware that law enforcement agencies are concerned that the widespread availability of cryptographic services for confidentiality purposes may have a serious impact on the fight against serious crime and terrorism if, where necessary and appropriate, it is not possible to get lawful access to encryption keys on a case by case basis. The Council has therefore agreed to monitor closely the extent to which encryption is exploited by serious criminals and terrorists.

4. The Council Resolution of 17 January 1995 recognised that lawfully authorised interception of communications is an important tool for the investigation of serious crime. The Council notes that law enforcement agencies may require lawful access to encryption keys, without the knowledge of the user of the cryptographic service, in order to maintain this capability. To this end, the Council recognises that there may be a law enforcement interest in promoting the use of confidentiality services which involve the depositing of an encryption key or other information with a third party. Such services are often known as "key escrow" or "key recovery" services. Law enforcement agencies may also require lawful access to encryption keys where it is necessary to decrypt material which has been seized as part of a criminal investigation.

5. The Council recognises that lawful access to encryption keys may be necessary in order to protect citizens against serious crime and terrorism. However, any such measures must be proportionate and balanced against other important interests. In particular, they must take full account of the need to protect civil liberties and the importance of safeguarding the functioning of the Internal Market in order to ensure the successful development of electronic commerce. Any measures to provide lawful access to encryption keys will also need to include strong safeguards.

6. The Council believes it is important to establish a common understanding of the needs of law enforcement agencies where cryptographic services are used for confidentiality purposes. It has therefore agreed to prepare a Resolution on Encryption and Law Enforcement to complement the work underway in other fora of the Council. The Resolution will invite Member States to take account of law enforcement needs in developing their national policies, but it will not require them to do so.
