General Distribution **C(97)62/FINAL**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

OLIS : 22-May-1997
Dist. : 23-May-1997

COUNCIL

C(97)62/FINAL
General Distribution

Council

RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES FOR CRYPTOGRAPHY POLICY

(adopted by the Council at its 895th session on 27 March 1997 [C/M(97)6/PROV])

52513

THE COUNCIL,

HAVING REGARD TO:

— the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960, in particular, articles 1 b), 1 c), 3 a) and 5 b) thereof;

— the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58(Final)];

— the Declaration on Transborder Data Flows adopted by the Governments of OECD Member countries on 11 April 1985 [Annex to C(85)139];

— the Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26-27 November 1992 [C(92)188/FINAL];

— the Directive [95/46/EC] of the European Parliament and of the Council of the European Union 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;

— the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies agreed on 13 July 1996;

— the Regulation [(EC) 3381/94] and the Decision [94/942/PESC] of the Council of the European Union of 19 December 1994 concerning the control of the export of dual-use goods;

— and the Recommendation [R(95)13] of the Council of Europe of 11 September 1995 concerning problems of criminal procedural law connected with information technology;

CONSIDERING:

— that national and global information infrastructures are developing rapidly to provide a seamless network for world-wide communications and access to data;

— that this emerging information and communications network is likely to have an important impact on economic development and world trade;

— that the users of information technology must have trust in the security of information and communications infrastructures, networks and systems; in the confidentiality, integrity, and availability of data on them; and in the ability to prove the origin and receipt of data;

— that data is increasingly vulnerable to sophisticated threats to its security, and ensuring the security of data through legal, procedural and technical means is fundamentally important in order for national and international information infrastructures to reach their full potential;

RECOGNISING:

— that, as cryptography can be an effective tool for the secure use of information technology by ensuring confidentiality, integrity and availability of data and by providing authentication and non-repudiation mechanisms for that data, it is an important component of secure information and communications networks and systems;

—that cryptography has a variety of applications related to the protection of privacy, intellectual property, business and financial information, public safety and national security, and the operation of electronic commerce, including secure anonymous payments and transactions;

— that the failure to utilise cryptographic methods can adversely affect the protection of privacy, intellectual property, business and financial information, public safety and national security and the operation of electronic commerce because data and communications may be inadequately protected from unauthorised access, alteration, and improper use, and, therefore, users may not trust information and communications systems, networks and infrastructures;

— that the use of cryptography to ensure integrity of data, including authentication and non-repudiation mechanisms, is distinct from its use to ensure confidentiality of data, and that each of these uses presents different issues;

— that the quality of information protection afforded by cryptography depends not only on the selected technical means, but also on good managerial, organisational and operational procedures;

AND FURTHER RECOGNISING:

— that governments have wide-ranging responsibilities, several of which are specifically implicated in the use of cryptography, including protection of privacy and facilitating information and communications systems security; encouraging economic well-being by, in part, promoting commerce; maintaining public safety; and enabling the enforcement of laws and the protection of national security;

— that although there are legitimate governmental, commercial and individual needs and uses for cryptography, it may also be used by individuals or entities for illegal activities, which can affect public safety, national security, the enforcement of laws, business interests, consumer interests or privacy; therefore governments, together with industry and the general public, are challenged to develop balanced policies;

— that due to the inherently global nature of information and communications networks, implementation of incompatible national policies will not meet the needs of individuals, business and governments and may create obstacles to economic co-operation and development; and, therefore, national policies may require international co-ordination;

— that this Recommendation of the Council does not affect the sovereign rights of national governments and that the Guidelines contained in the Annex to this Recommendation are always subject to the requirements of national law;

On the proposal of the Committee for Information, Computer and Communications Policy;

RECOMMENDS THAT MEMBER COUNTRIES:

1. establish new, or amend existing, policies, methods, measures, practices and procedures to reflect and take into account the Principles concerning cryptography policy set forth in the Guidelines contained in the Annex to this Recommendation (hereinafter “the Guidelines”), which is an integral part hereof; in so doing, also take into account the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58(Final)] and the Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26-27 November 1992 [C(92)188/FINAL];

2. consult, co-ordinate and co-operate at the national and international level in the implementation of the Guidelines;

3. act on the need for practical and operational solutions in the area of international cryptography policy by using the Guidelines as a basis for agreements on specific issues related to international cryptography policy;

4. disseminate the Guidelines throughout the public and private sectors to promote awareness of the issues and policies related to cryptography;

5. remove, or avoid creating in the name of cryptography policy, unjustified obstacles to international trade and the development of information and communications networks;

6. state clearly and make publicly available, any national controls imposed by governments relating to the use of cryptography;

7. review the Guidelines at least every five years, with a view to improving international co-operation on issues relating to cryptography policy.

ANNEX

GUIDELINES FOR CRYPTOGRAPHY POLICY

I. AIMS

The Guidelines are intended:

— to promote the use of cryptography:

- to foster confidence in information and communications infrastructures, networks and systems and the manner in which they are used;

- to help ensure the security of data, and to protect privacy, in national and global information and communications infrastructures, networks and systems;

— to promote this use of cryptography without unduly jeopardising public safety, law enforcement, and national security;

— to raise awareness of the need for compatible cryptography policies and laws, as well as the need for interoperable, portable and mobile cryptographic methods in national and global information and communications networks;

— to assist decision-makers in the public and private sectors in developing and implementing coherent national and international policies, methods, measures, practices and procedures for the effective use of cryptography;

— to promote co-operation between the public and private sectors in the development and implementation of national and international cryptography policies, methods, measures, practices and procedures;

— to facilitate international trade by promoting cost-effective, interoperable, portable and mobile cryptographic systems;

— to promote international co-operation among governments, business and research communities, and standards-making bodies in achieving co-ordinated use of cryptographic methods.

II. SCOPE

The Guidelines are primarily aimed at governments, in terms of the policy recommendations herein, but with anticipation that they will be widely read and followed by both the private and public sectors.

It is recognised that governments have separable and distinct responsibilities for the protection of information which requires security in the national interest; the Guidelines are not intended for application in these matters.

III. DEFINITIONS

For the purposes of the Guidelines:

"Authentication" means a function for establishing the validity of a claimed identity of a user, device or another entity in an information or communications system.

"Availability" of data, information, and information and communications systems means that they are accessible and usable on a timely basis in the required manner.

"Confidentiality" of data or information means that it is not made available or disclosed to unauthorised individuals, entities, or processes.

"Cryptography" means the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorised use.

"Cryptographic key" means a parameter used with a cryptographic algorithm to transform, validate, authenticate, encrypt or decrypt data.

"Cryptographic methods" means cryptographic techniques, services, systems, products and key management systems.

"Data" means the representation of information in a manner suitable for communication, interpretation, storage, or processing.

"Decryption" means the inverse function of encryption.

"Encryption" means the transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality.

"Integrity" of data or information means that it has not been modified or altered in an unauthorised manner.

"Interoperability" of cryptographic methods means the technical ability of multiple cryptographic methods to function together.

"Key management system" means a system for generation, storage, distribution, revocation, deletion, archiving, certification or application of cryptographic keys.

"Keyholder" means an individual or entity in possession or control of cryptographic keys. A keyholder is not necessarily a user of the key.

"Law enforcement" or "enforcement of laws" refers to the enforcement of all laws, without regard to subject matter.

"Lawful access" means access by third party individuals or entities, including governments, to plaintext, or cryptographic keys, of encrypted data, in accordance with law.

"Mobility" of cryptographic methods only means the technical ability to function in multiple countries or information and communications infrastructures.

"Non-repudiation" means a property achieved through cryptographic methods, which prevents an individual or entity from denying having performed a particular action related to data (such as mechanisms for non-rejection of authority (origin); for proof of obligation, intent, or commitment; or for proof of ownership).

"Personal data" means any information relating to an identified or identifiable individual.

"Plaintext" means intelligible data.

"Portability" of cryptographic methods means the technical ability to be adapted and function in multiple systems.

IV. INTEGRATION

The principles in Section V of this Annex, each of which addresses an important policy concern, are interdependent and should be implemented as a whole so as to balance the various interests at stake. No principle should be implemented in isolation from the rest.

V. PRINCIPLES

1. TRUST IN CRYPTOGRAPHIC METHODS

CRYPTOGRAPHIC METHODS SHOULD BE TRUSTWORTHY IN ORDER TO GENERATE CONFIDENCE IN THE USE OF INFORMATION AND COMMUNICATIONS SYSTEMS.

Market forces should serve to build trust in reliable systems, and government regulation, licensing, and use of cryptographic methods may also encourage user trust. Evaluation of cryptographic methods, especially against market-accepted criteria, could also generate user trust.

In the interests of user trust, a contract dealing with the use of a key management system should indicate the jurisdiction whose laws apply to that system.

2. CHOICE OF CRYPTOGRAPHIC METHODS

USERS SHOULD HAVE A RIGHT TO CHOOSE ANY CRYPTOGRAPHIC METHOD, SUBJECT TO APPLICABLE LAW.

Users should have access to cryptography that meets their needs, so that they can trust in the security of information and communications systems, and the confidentiality and integrity of data on those systems. Individuals or entities who own, control, access, use or store data may have a responsibility to protect the confidentiality and integrity of such data, and may therefore be responsible for using appropriate cryptographic methods. It is expected that a variety of cryptographic methods may be needed to fulfil different data security requirements. Users of cryptography should be free, subject to applicable law, to determine the type and level of data security needed, and to select and implement appropriate cryptographic methods, including a key management system that suits their needs.

In order to protect an identified public interest, such as the protection of personal data or electronic commerce, governments may implement policies requiring cryptographic methods to achieve a sufficient level of protection.

Government controls on cryptographic methods should be no more than are essential to the discharge of government responsibilities and should respect user choice to the greatest extent possible. This principle should not be interpreted as implying that governments should initiate legislation which limits user choice.

3. MARKET DRIVEN DEVELOPMENT OF CRYPTOGRAPHIC METHODS

CRYPTOGRAPHIC METHODS SHOULD BE DEVELOPED IN RESPONSE TO THE NEEDS, DEMANDS AND RESPONSIBILITIES OF INDIVIDUALS, BUSINESSES AND GOVERNMENTS.

The development and provision of cryptographic methods should be determined by the market in an open and competitive environment. Such an approach would best ensure that solutions keep pace with changing technology, the demands of users and evolving threats to information and communications systems security. The development of international technical standards, criteria and protocols related to cryptographic methods should also be market driven. Governments should encourage and co-operate with business and the research community in the development of cryptographic methods.

4. STANDARDS FOR CRYPTOGRAPHIC METHODS

TECHNICAL STANDARDS, CRITERIA AND PROTOCOLS FOR CRYPTOGRAPHIC METHODS SHOULD BE DEVELOPED AND PROMULGATED AT THE NATIONAL AND INTERNATIONAL LEVEL.

In response to the needs of the market, internationally-recognised standards-making bodies, governments, business and other relevant experts should share information and collaborate to develop and promulgate interoperable technical standards, criteria and protocols for cryptographic methods. National standards for cryptographic methods, if any, should be consistent with international standards to facilitate global interoperability, portability and mobility. Mechanisms to evaluate conformity to such technical standards, criteria and protocols for interoperability, portability and mobility of cryptographic methods should be developed. To the extent that testing of conformity to, or evaluation of, standards may occur, the broad acceptance of such results should be encouraged.

5. PROTECTION OF PRIVACY AND PERSONAL DATA

THE FUNDAMENTAL RIGHTS OF INDIVIDUALS TO PRIVACY, INCLUDING SECRECY OF COMMUNICATIONS AND PROTECTION OF PERSONAL DATA, SHOULD BE RESPECTED IN NATIONAL CRYPTOGRAPHY POLICIES AND IN THE IMPLEMENTATION AND USE OF CRYPTOGRAPHIC METHODS.

Cryptographic methods can be a valuable tool for the protection of privacy, including both the confidentiality of data and communications and the protection of the identity of individuals. Cryptographic methods also offer new opportunities to minimise the collection of personal data, by enabling secure but anonymous payments, transactions and interactions. At the same time, cryptographic methods to ensure the integrity of data in electronic transactions raise privacy implications. These implications, which include the collection of personal data and the creation of systems for personal

identification, should be considered and explained, and, where appropriate, privacy safeguards should be established.

The OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data provide general guidance concerning the collection and management of personal information, and should be applied in concert with relevant national law when implementing cryptographic methods.

6. LAWFUL ACCESS

NATIONAL CRYPTOGRAPHY POLICIES MAY ALLOW LAWFUL ACCESS TO PLAINTEXT, OR CRYPTOGRAPHIC KEYS, OF ENCRYPTED DATA. THESE POLICIES MUST RESPECT THE OTHER PRINCIPLES CONTAINED IN THE GUIDELINES TO THE GREATEST EXTENT POSSIBLE.

If considering policies on cryptographic methods that provide for lawful access, governments should carefully weigh the benefits, including the benefits for public safety, law enforcement and national security, as well as the risks of misuse, the additional expense of any supporting infrastructure, the prospects of technical failure, and other costs. This principle should not be interpreted as implying that governments should, or should not, initiate legislation that would allow lawful access.

Where access to the plaintext, or cryptographic keys, of encrypted data is requested under lawful process, the individual or entity requesting access must have a legal right to possession of the plaintext, and once obtained the data must only be used for lawful purposes. The process through which lawful access is obtained should be recorded, so that the disclosure of the cryptographic keys or the data can be audited or reviewed in accordance with national law. Where lawful access is requested and obtained, such access should be granted within designated time limits appropriate to the circumstances. The conditions of lawful access should be stated clearly and published in a way that they are easily available to users, keyholders and providers of cryptographic methods.

Key management systems could provide a basis for a possible solution which could balance the interest of users and law enforcement authorities; these techniques could also be used to recover data, when keys are lost. Processes for lawful access to cryptographic keys must recognise the distinction between keys which are used to protect confidentiality and keys which are used for other purposes only. A cryptographic key that provides for identity or integrity only (as distinct from a cryptographic key that verifies identity or integrity only) should not be made available without the consent of the individual or entity in lawful possession of that key.

7. LIABILITY

WHETHER ESTABLISHED BY CONTRACT OR LEGISLATION, THE LIABILITY OF INDIVIDUALS AND ENTITIES THAT OFFER CRYPTOGRAPHIC SERVICES OR HOLD OR ACCESS CRYPTOGRAPHIC KEYS SHOULD BE CLEARLY STATED.

The liability of any individual or entity, including a government entity, that offers cryptographic services or holds or has access to cryptographic keys, should be made clear by contract or where appropriate by national legislation or international agreement. The liability of users for misuse of their own keys should also be made clear. A keyholder should not be held liable for providing cryptographic keys or plaintext of encrypted data in accordance with lawful access. The party that obtains lawful access should be liable for misuse of cryptographic keys or plaintext that it has obtained.

8. INTERNATIONAL CO-OPERATION

GOVERNMENTS SHOULD CO-OPERATE TO CO-ORDINATE CRYPTOGRAPHY POLICIES. AS PART OF THIS EFFORT, GOVERNMENTS SHOULD REMOVE, OR AVOID CREATING IN THE NAME OF CRYPTOGRAPHY POLICY, UNJUSTIFIED OBSTACLES TO TRADE.

In order to promote the broad international acceptance of cryptography and enable the full potential of the national and global information and communications networks, cryptography policies adopted by a country should be co-ordinated as much as possible with similar policies of other countries. To that end, the Guidelines should be used for national policy formulation.

If developed, national key management systems must, where appropriate, allow for international use of cryptography.

Lawful access across national borders may be achieved through bilateral and multilateral co-operation and agreement.

No government should impede the free flow of encrypted data passing through its jurisdiction merely on the basis of cryptography policy.

In order to promote international trade, governments should avoid developing cryptography policies and practices which create unjustified obstacles to global electronic commerce. Governments should avoid creating unjustified obstacles to international availability of cryptographic methods.