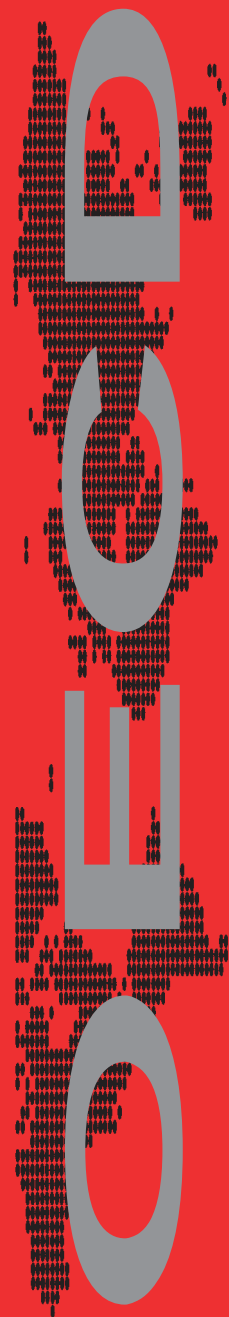


# CRYPTOGRAPHY POLICY

The Guidelines  
and the Issues



**CRYPTOGRAPHY**  
**POLICY**  
*the Guidelines*  
*and the Issues*

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

# ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Pursuant to Article 1 of the Convention signed in Paris on 14th December 1960, and which came into force on 30th September 1961, the Organisation for Economic Co-operation and Development (OECD) shall promote policies designed:

- to achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy;
- to contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and
- to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.

The original Member countries of the OECD are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became Members subsequently through accession at the dates indicated hereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996) and the Republic of Korea (12th December 1996). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).

Publié en français sous le titre

LA POLITIQUE DE CRYPTOGRAPHIE

les lignes directrices et les questions actuelles

© OECD 1998

Permission to reproduce a portion of this work for non-commercial purposes or classroom use should be obtained through the Centre français d'exploitation du droit de copie (CFC), 20, rue des Grands-Augustins, 75006 Paris, France, Tel. (33-1) 44 07 47 70, Fax (33-1) 46 34 67 19, for every country except the United States. In the United States permission should be obtained through the Copyright Clearance Center, Customer Service, (508)750-8400, 222 Rosewood Drive, Danvers, MA 01923 USA, or CCC Online: <http://www.copyright.com/>. All other applications for permission to reproduce or translate all or part of this book should be made to OECD Publications, 2, rue André-Pascal, 75775 Paris Cedex 16, France.

## TABLE OF CONTENTS

Recommendation of the Council concerning guidelines for cryptography policy .....	7
<i>Annex</i> : Guidelines for cryptography policy .....	11
Report on background and issues of cryptography policy.....	19

## PREFACE

Cryptography is a discipline that 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. It is one of the technological means to provide security for data on information and communications systems. Cryptography can be used to protect the confidentiality of data, such as financial or personal data, whether that data is in storage or in transit. Cryptography can also be used to verify the integrity of data by revealing whether data has been altered and identifying the person or device that sent it. These techniques are critical to the development and use of national and global information and communications networks and technologies, as well as the development of electronic commerce.

In recent years OECD Member countries have undertaken to develop and implement policies and laws relating to cryptography; in many countries these are still in the process of being developed. Disparities in policy may create obstacles to the evolution of national and global information and communications networks and hinder the development of international trade. The governments of Member countries have recognised the need for an internationally co-ordinated approach to facilitate the smooth development of an efficient, secure information infrastructure. The OECD is playing a role in this regard by developing consensus about specific policy and regulatory issues relating to information and communications networks and technologies, including cryptography issues.

The OECD has been active for some time in the areas of privacy and data protection and the security of information systems. In early 1996 the OECD initiated a project on cryptography policy by forming the *Ad hoc* Group of Experts on Cryptography Policy Guidelines (“*Ad hoc* Group”) under the auspices of the Committee for Information, Computer and Communications Policy (ICCP). The *Ad hoc* Group, under the chairmanship of Mr. Norman Reaburn of the Attorney-General’s Department of Australia, was charged with drafting Guidelines for Cryptography Policy (“Guidelines”) to identify the issues which should be taken into consideration in the formulation of cryptography policies at the national and international level. The *Ad hoc* Group had a one-year mandate to accomplish this task and it

completed its work in December 1996. Thereafter, the Guidelines were adopted as a Recommendation of the Council of the OECD on 27 March 1997.

The **Guidelines** are broad in nature and reflect the diversity of views among Member countries. The Secretariat has prepared a **Report** on Background and Issues of Cryptography Policy to explain the context for the Guidelines and the basic issues involved in the cryptography policy debate. The Report explains the need for international action and summarises related work carried out so far by the OECD and certain other organisations. The Report is an information document intended to assist public discussion of the Guidelines, as opposed to influencing the interpretation of the Guidelines. While it provides more detail on the breadth of the issues covered in the Guidelines, **the Report does not vary the meaning of the Guidelines and must not be used as an interpretative guide**. The Report has been drafted by the Secretariat, which has benefited from discussions with a number of national experts. However, the Report was only discussed very briefly during the meetings of the *Ad hoc* Group.

# **RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES FOR CRYPTOGRAPHY POLICY**

27 MARCH 1997

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 worldwide 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.

## **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 cryptographic 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” means the property that data, information, and information and communications systems are accessible and usable on a timely basis in the required manner.

“Confidentiality” means the property that data or information 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” means the property that data or information 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.

# REPORT ON BACKGROUND AND ISSUES OF CRYPTOGRAPHY POLICY

The Secretariat has prepared this **Report** on Background and Issues of Cryptography Policy to explain the context for the **Guidelines** for Cryptography Policy and the basic issues involved in the cryptography policy debate. The Report explains the need for international action and summarises related work carried out so far by the OECD and certain other organisations. The Report is an information document intended to assist public discussion of the Guidelines, as opposed to influencing the interpretation of the Guidelines. While it provides more detail on the breadth of the issues covered in the Guidelines, **the Report does not vary the meaning of the Guidelines and must not be used as an interpretative guide.** The Report has been drafted by the Secretariat, which has benefited from discussions with a number of national experts. However, the Report was only discussed very briefly during the meetings of the *Ad hoc* Group.

## I. GENERAL BACKGROUND

### *Transition to Electronic Transactions*

Information is becoming more valuable, and the production, distribution and use of information is an increasingly important economic activity. Information is often exchanged as a commodity and may be protected by intellectual property law. Information producers seek access to distribution channels while consumers demand access to a broad range of information sources. Furthermore, the free flow of information is a fundamental element of democracy.

Traditional telephone, broadcast and cable television, and radio systems have long used electronic means to distribute information in analogue form; however, the shift to digital technology is revolutionising the way that information is created and handled. Digital computer processing and network technologies are replacing traditional methods for producing, storing, transmitting and disseminating information. Combining different kinds of information representations – such as text, audio, images and video – is easy with digital technology, and the

distinctions between different types of information production and distribution are becoming less clear. Furthermore, emerging information and communications networks and technologies are changing the way people communicate and do business, and they have a widespread impact on the public and private sectors, necessitating changes in a variety of basic commercial, legal and other structures.

The convergence of previously separate information and communications systems into a global network of networks is creating mechanisms for new ways of conducting transactions and will soon allow virtually unlimited access to information, education and entertainment resources. This access brings with it new intellectual property issues that are peculiar to the emerging medium. While open information and communications networks make electronic transmission of all kinds of digitised data fast, cheap and simple, the ability to make and distribute perfect copies of all kinds of data creates a number of challenges for the protection of intellectual property. Trade in creative content can provide economic incentives to fuel the development of information and communications technologies, and intellectual property protection is essential to stimulate the production of, and trade in, high-quality content.

Electronic commerce offers great opportunities for the business community and consumers; however it also brings with it some significant risks. The explosive worldwide growth of open networks has raised a legitimate concern with respect to the adequacy of security and privacy measures for information and communications systems and the data which is transmitted and stored on those systems. The developing information infrastructure is a fertile environment for all kinds of computer-related crime, including fraud and privacy infringement, and electronic business will not advance until effective data security measures are adopted and trusted by users and consumers. Both technical and legal solutions are required to replace in the electronic world the physical security of the paper-based world. It is important that solutions are trustworthy and that consumers have confidence in them.

## **II. SECURITY OF INFORMATION SYSTEMS AND CRYPTOGRAPHY**

The importance of information and communications systems for society and the global economy is intensifying with the increasing value and quantity of data that is transmitted and stored on those systems. At the same time those systems and data are also increasingly vulnerable to a variety of threats, such as unauthorised access and use, misappropriation, alteration, and destruction. Proliferation of computers, increased computing power, interconnectivity, decentralisation, growth of networks and the number of users, as well as the convergence of information and communications technologies, while enhancing the utility of these systems, also increase system vulnerability.

Security of information and communications systems involves the protection of the availability, confidentiality and integrity of those systems and the data that is transmitted and stored on them. *Availability* is the property that data, information, and information and communications systems are accessible and useable on a timely basis in the required manner. *Confidentiality* is the property that data or information is not made available or disclosed to unauthorised persons, entities and processes. *Integrity* is the property that data or information has not been modified or altered in an unauthorised manner. The relative priority and significance of availability, confidentiality and integrity vary according to the information or communication systems and the ways in which those systems are used. The quality of security for information and communication systems and the data that is stored and transmitted on them depends not only on the technical measures, including the use of both hardware and software tools, but also on good managerial, organisational and operational procedures.

Cryptography is an important component of secure information and communications systems and a variety of applications have been developed that incorporate cryptographic methods to provide data security. Cryptography is an effective tool for ensuring both the confidentiality and the integrity of data, and each of these uses offers certain benefits. However, the widespread use of cryptography raises a number of important issues. Governments have wide-ranging responsibilities, several of which are specifically implicated in the use of cryptography, including protecting the privacy rights of their citizens; facilitating information and communications systems security; encouraging economic well-being by, in part, promoting electronic commerce; maintaining public safety; raising revenues to finance their activities; and enabling the enforcement of laws and the protection of national security. 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. Governments, together with industry and the general public, are challenged to develop balanced policies to address these issues.

The diverse interests which can be affected by the use of, or the failure to use, cryptography make the development of balanced cryptography policy both complex and critical. Traditionally, cryptography was most often used only by governments. However in recent years – as cryptography has become more accessible and affordable, and as users have become more aware of the benefits of using it and the risks of failing to do so – cryptography has also come to be used as a matter of course by individuals and businesses for a variety of purposes. The increasing availability of cryptography to the general public has fuelled the current debate on these issues.

### ***Secret Key Cryptography***

Historically, cryptography has been used to encode information to conceal secret messages from unauthorised parties and, as such, it is important for military and national security use. Cryptography uses an algorithm to transform data in order to render it unintelligible to anyone who does not possess certain secret information (the cryptographic “key”) necessary for decryption of the data. Today, the increased calculation power arising from the development of digital computing makes it possible to use complex mathematical algorithms for encryption of data.

The development of information and communications technologies that allow vast quantities of data to be transmitted, copied and stored quickly and easily has prompted a growing concern for the protection of privacy and the confidentiality of data, including personal data, government administrative records, and business and financial information. Effective cryptography is an essential tool in a network environment for addressing these concerns. It is also used to protect classified government information.

### ***Public Key Cryptography***

In the mid-1970s a new development in cryptography introduced the “public key” concept, which allows parties to exchange encrypted data without communicating a shared secret key in advance. Rather than sharing one secret key, this new design uses two mathematically related keys for each communicating party: a “public key” that is disclosed to the public, and a corresponding “private key” that is kept secret. A message that is encrypted with a public key can only be decrypted by the corresponding private key. In this way, a confidential communication encrypted with the recipient’s public key and decrypted with the recipient’s private key could only be understood by the recipient of the message.<sup>1</sup>

An important application for public key cryptography is “digital signature”, which can be used to verify the integrity of data or the authenticity of the sender of data. In this case, the private key is used to “sign” a message, while the corresponding public key is used to verify a “signed” message. Public key cryptography offers the benefits of confidential transmissions and digital signature in an open network environment in which parties do not know one another in advance. This development allows for broader applications of cryptographic methods, and this – together with increases in computer power and decreases in computer prices – has moved cryptography into the private sector domain.

Public key cryptography plays an important role in developing information infrastructures. Much of the interest in information and communications networks and technologies centres on their potential to accommodate electronic com-

merce; however, open networks such as the Internet present significant challenges for making enforceable electronic contracts and secure payments. In connection with certifying the integrity of data, public key cryptography offers technological solutions for both of these problems by providing mechanisms for establishing the validity of a claimed identity of a user, device or another entity in an information system (“authentication”) and for limiting the ability of an individual or entity to effectively deny having performed a particular action related to data (“non-repudiation”).

### ***Digital Signature***

There is a tremendous potential for fraud in the electronic world. Transactions take place at a distance without the benefit of physical clues that permit identification, making impersonation easy. The ability to make perfect copies and undetectable alterations of digitised data complicates the matter. Traditionally, hand-written signatures serve to determine the authenticity of an original document. In the electronic world, the concept of an “original” document is problematic, but a digital signature can verify data integrity, and provide authentication and non-repudiation functions to certify the sender of the data. If a document itself has been altered in any way after it has been “signed”, the digital signature will so demonstrate. Similarly, once a document is “signed” with a cryptographic key, the digital signature provides proof that the document was “signed” by the purported author, and the sender cannot easily deny having sent the document or claim that the information has been altered during transmission.

Cryptography can also provide technical solutions for the protection of intellectual property in digital form. For example, a digital signature together with a verifiable time-stamp can give authors some control over their work, by tying an electronic document to the issuer and ensuring that the document is not modified without detection. The same technology can be applied to ensuring the authenticity and integrity of documents archived electronically.

### ***Electronic Payments***

Secure payment systems are necessary in order for electronic commerce on open networks to flourish. One way to make electronic payments is to utilise a modified version of the existing credit card system. Cryptography can be used to protect the confidentiality of a message containing a credit card number and to confirm that the message was indeed sent by the cardholder. While this method is currently being used, it leaves the credit card number vulnerable to improper use after the message containing it has been decrypted. Another design involves verifiable security mechanisms for the transaction to occur electronically which are not simply based on the exchange of a credit card number – such as independent

confirmation by digital signature – as well as an authorisation process that is not tied to any proprietary network so that purchases can be made on open networks.

Several schemes for other kinds of electronic payment systems are in various stages of development, including a number of different “digital money” systems. Digital money systems use cryptography to create a unique electronic representation that is redeemable for payment or which can constitute legal tender that is storable, transferable and unforgeable. Most of these systems operate much like credit cards, debit cards or checks, offering varying degrees of traceability and anonymity; others act more like “digital cash”, accommodating completely anonymous transactions like coins do. While the ability to conduct untraceable and anonymous electronic transactions offers particular advantages for the protection of privacy in the electronic environment, it also raises a number of concerns for governments – particularly tax authorities – in connection with tax collection and money laundering.

### ***Certifying Public Key Relationships***

Affirming the relationship between an individual or entity and its associated public key is important to guard against impersonation in an electronic environment. In order for public key systems to work in the public domain, not only must the public key be freely accessible, but also senders and receivers must have a reliable way of determining that public keys are truly the keys of those parties with whom they wish to interact. This can be accomplished directly if the parties know one another in advance, or alternatively a formal mechanism to “certify” keys could be established. With that in mind, two basic types of solutions have emerged: an informal “web of trust” arrangement based on pre-existing relationships between parties, and a more formalised approach based on “certificate authorities”. These methods of certifying public key relationships act much like the existing means for identifying parties for social and commercial interaction.

The informal web of trust operates when keys are validated from person to person or from organisation to organisation in the context of established relationships. In this way, confidence in the relationship between an individual or entity and its associated public key extends from parties which have a direct relationship to those which do not as credentials are established through many individual instances of trust. This method of certifying public keys is currently used mainly for exchange of encrypted data among personal acquaintances, but as electronic commerce develops this method may evolve into an important element of business relationships as well.

The other basic type of solution to address this problem is a public key infrastructure where certificate authorities authenticate public keys. A certificate authority is a “trusted” entity that provides information about the identity of a

keyholder in the form of an authenticated “key certificate”. The certificate is used to verify the identity of the parties exchanging encrypted information over a network. Certificate authorities can also perform other functions, such as notary and time-stamp services. Certificate authorities can be established by either the public or private sector, and they may operate either “in-house” for an individual organisation or for the public at large.

Furthermore, the certificate authority itself must be reliable, so the certifier may need to be certified. This issue could be addressed by both a hierarchy of certificate authorities and a system of cross-certified certificate authorities. At the international level, independent international management frameworks for public key certification may be useful. The distinction between the web of trust and certificate authority methods becomes less clear when organisations which provide certificate functions cross-certify one another. Many studies have shown that the full potential of electronic commerce will not be realised until public key infrastructures emerge which generate sufficient trust for businesses and individuals to commit their information and transactions to the emerging public networks. Few jurisdictions have adopted specific legislation for certificate infrastructures at present; however, a number of Member countries are looking at this issue and considering regulation and licensing procedures for certificate authorities.

### **III. SPECIAL ISSUES FOR CONSIDERATION WITH CRYPTOGRAPHY POLICY**

#### ***User Trust***

Increasingly, individuals, enterprises and governments are affected by electronic information and communications systems, and there is an increasing dependence on their uninterrupted proper functioning. Concomitant with this is a mounting need for confidence that these systems will continue to be reliable and secure, particularly as electronic commerce and electronic payment systems develop. Lack of security or lack of confidence in the security of these systems may hinder the development and use of new information and communication technologies.

Just as in the real world – where credit cards are forged, and cash is stolen – the “virtual world” will never be completely secure. While security methods and services should be trustworthy so that the users of information and communications systems can have confidence in them, ultimately, electronic transactions will involve a calculated risk. Consumers will embrace electronic commerce when its value is greater than the perceived risks. The question then becomes not are transactions absolutely secure, but are they sufficiently secure for consumer transactions? There is a need to build consumer confidence in data security mechanisms, like cryptography, so that they will be widely used for electronic commerce.



Uncertainties may be met and confidence fostered by building consensus about use of information and communications systems. The challenge is three-fold: developing and implementing the technology; planning for avoiding and meeting the failures of the technology; and gaining public support and approval of use of the technology. Public education on the issues and technologies, including a full discussion of cryptography in the context of electronic commerce, could help raise consumer confidence. In that context, it is also important for users to understand the legal framework which governs their use of cryptography, particularly in light of the “borderless” nature of information and communications networks.

### ***User Choice***

Solutions to protect against the diverse threats to information and communications systems and the data that is stored and transmitted on them can take a number of different forms. There is considerable choice of cryptographic methods available to meet a wide variety of user requirements for systems and data security, including both hardware and software solutions, which can stand alone or be integrated into related products, and which can offer a certain level of strength and complexity depending on the algorithm and the product. Cryptographic methods can be designed to provide any combination of mechanisms to achieve confidentiality, authentication or non-repudiation and ensure data integrity. Users will choose different kinds of cryptographic methods for different purposes and to fulfil different data and systems security requirements. Furthermore, where systems for management of keys are developed, they too will offer a variety of functions for users to choose from.

Some governments have implemented regulations – and others may do so in the future – on the use of cryptography, including export controls, rules concerning key management systems, or requirements for minimum levels of protection for certain kinds of data. These regulations may have an impact on the kinds of cryptographic methods which are available for users to choose from. However, it is commonly agreed that, within these limitations, it is important for a wide variety of cryptographic methods to be available to meet the diverse needs for data and systems security. Broad options for choice of cryptographic methods will encourage the development of a wide range of products.

### ***Market-driven Development***

Because the private sector is a critical partner in the development of the information infrastructure – and primarily responsible for its construction – most experts agree that industry should develop products and determine standards based upon market needs. Although it is recognised that governments may influ-

ence product development by expressing, like any user, the need for a certain type of product, some believe governments should be careful not to drive markets in a particular direction. Others believe that governments ought to guide the market to meet their responsibilities for protecting public safety and privacy. Nevertheless, governments are also aware that if the requirements they impose on the use of cryptography are too burdensome, users of information and communications systems will not use cryptography and industry will not develop products that incorporate cryptographic techniques.

### ***Standardization***

Standardization is an important ingredient of security mechanisms. In the rapid-paced development of the information infrastructure, standards for security mechanisms, including cryptographic methods, emerge quickly, whether they be *de facto*, through market dominance, or through national or international standards-setting bodies. It is important for governments and industry to work together to provide the necessary architecture and standards so that information and communications systems can reach their full potential. A common description of an effective standards-setting process is one that is industry-led, voluntary, consensus-based and international.

For cryptography to function effectively as a security measure for information and communications systems, networks and infrastructures, it is important that cryptographic methods be interoperable, mobile and portable at the global level. *Interoperability* means the technical ability of multiple cryptographic methods to function together. *Mobility* means the technical ability of cryptographic methods to function in multiple information and communications infrastructures. *Portability* means the technical ability of cryptographic methods to be adapted and function in multiple systems. National and international standards for cryptographic methods can help to facilitate the development of these technical abilities.

### ***Protection of Privacy***

The respect of privacy and the confidentiality of personal information are important values in a democratic society. However, privacy is now at greater risk because in the emerging information and communications infrastructure neither open networks, nor many types of private networks, were designed with confidentiality of communications and storage of data in mind. However, cryptography forms the basis for a new generation of privacy enhancing technologies. The use of effective cryptography in a network environment can help protect the privacy of personal information and the secrecy of confidential information. The failure to use cryptography in an environment where data is not completely secure can put a number of interests at risk, including public safety and national security. In

some cases, such as where national law calls for maintaining the confidentiality of data, or protecting critical infrastructures, governments may require the use of cryptography of a minimum strength.

At the same time, the use of cryptography to ensure the integrity of data in electronic transactions can also have implications for privacy. The use of networks for all kinds of transactions will increasingly generate vast quantities of data that can be easily and cheaply stored, analysed, and reused. When these operations require proof of identity, the transactional data will leave detailed and perhaps irrefutable trails of an individual's commercial activity, as well as paint a picture of private, non-commercial activities such as political associations, participation in online discussions, and access to specific types of information in online libraries or other databases. The key certification process also has implications for privacy because data can be collected when a certification authority binds an individual to a key pair.

### ***Lawful Access***

A critical issue presented by cryptography – perhaps the most widely debated aspect of cryptography and the one most likely to lead to disparate national policies – is the perceived conflict between confidentiality and public safety. While the use of cryptography is important for the protection of privacy, there may be a need to consider appropriate mechanisms for lawful access to encrypted information. For example, in many countries, law enforcement can lawfully access stored data or intercept communications (or both) under certain conditions. Both of these important law enforcement tools could be curtailed by the use of cryptography which can prevent lawful access to either plaintext or cryptographic keys of encrypted data. In some cases, encryption of stored data can make law enforcement access impossible, while in other cases, the data can be lawfully accessed elsewhere (such as obtaining financial records from a bank rather than a person's home computer), or the key could be obtained to decrypt the data. For countries that permit either technique, balancing concerns for the protection of privacy and the confidentiality of business information with the needs of the law enforcement and national security communities is politically difficult.

Furthermore, the need for third-party access is not limited to governments. Individuals and businesses may need to gain access to encrypted information also: for instance, if a keyholder dies leaving encrypted information but no key to decrypt it, or if an employee who has encrypted a file resigns without leaving information concerning the decryption key. Individuals or businesses that encrypt data may wish to store a copy of cryptographic keys in a repository which would allow lawful access in such cases.

It is important to note the difference between cryptographic keys used for confidentiality and those used for authentication, data integrity and non-repudiation purposes only. The problem of lawful access to cryptographic keys is more relevant in the context of cryptography used to keep data confidential, where information is concealed. Cryptography used only to authenticate or ensure integrity of data does not necessarily conceal the information, but merely verifies the data. In this case, the information itself may be available, or the data could be lawfully obtained another way, so it would be unnecessary to gain access to the private key. An important implication of private keys used only for authentication or ensuring integrity of data is that when such a key is compromised “electronic impersonation” is possible. Since public keys are designed to be placed in the public domain, these issues do not generally apply to access to public keys.

If lawful access is to be preserved, exactly how this should be done is unclear. Governments are following different approaches and are seeking innovative solutions from industry. One approach which could provide a basis for a possible solution to balance the interests of users and law enforcement authorities would consist of using a key management system where a copy of the private cryptographic key used for confidentiality purposes would be “stored” with a “trusted third party” (TTP).<sup>2</sup> Other approaches could provide lawful third-party access to the plaintext of encrypted data. Among the variety of approaches, some could also be used to recover data when keys are lost. Again, it is important to recognise the distinction between keys which are used to protect confidentiality and keys which are used for other purposes only. Keys which are used for authentication, data integrity verification, and non-repudiation purposes would not be subject to the same kinds of lawful access by third parties.

In this context, other issues that may need to be addressed include where keys will be stored, who will be allowed to hold keys, and what will be the responsibilities and the liabilities of keyholders. Such key storage systems are distinct from public key infrastructures for certification of public keys – another kind of trusted service which a TTP could provide – although the two services could be combined.

### ***Liability***

Like many things in life, information and communications technologies do not always work perfectly: firewalls may fail to keep out intruders, networks may break down, routers may send data to the wrong destination. Moreover, human error can also play a role, for example when data is deleted by mistake or passwords are not kept secret. In the context of cryptography, system failure or human error that results in cryptographic keys being compromised can have

significant and far-reaching consequences, because the strongest cryptography becomes ineffective if keys are compromised. If cryptographic keys are compromised, users must assume that their encrypted data is no longer secure, and they run the risk that documents or transactions will be forged in their name. Where a certificate authority is compromised, there could be catastrophic consequences. Moreover, the process for revoking keys and key certificates can be complicated.

Secure handling of keys is very important for both individual users and organisations; key management systems generally have strict procedures for protecting and monitoring the use of keys to prevent keys from being compromised. However, if these practices fail and keys are compromised, it is important to know which parties must take responsibility and the extent to which they can be held liable for the repercussions. This issue is particularly important for key management services or trusted third parties, which hold or access cryptographic keys on behalf of others, given the significant impact of liability if their systems are compromised. Setting out provisions for liability can be addressed by either contract or legislation, at the individual or governmental level. Moreover, it may be important to consider liability implications at both the national and international levels.

### ***International Co-operation***

The increasingly global flow of data on information and communications networks highlights the need for an internationally co-operative approach to addressing these matters. Enforcement of existing legal regimes is based on geographically defined borders, but in the emerging network environment, information and commercial transactions may move freely across national and jurisdictional boundaries. In framing national strategies and designing regulatory structures for the information infrastructure, including those relating to cryptography, all governments are recognising that the impact of such activities will, in many instances, extend far beyond their frontiers.

Disparate national policies may impair the development of global networks and technologies, compelling the use of numerous, possibly incompatible, products to communicate and transact business, when one might suffice. Such an environment may also create barriers to international trade. Given the inherently global nature of developing information and communications networks and the difficulties of defining and enforcing jurisdictional boundaries in this environment, these issues may most effectively be addressed by international consultation and co-operation. This is particularly relevant in the case of cryptography.

## **IV. GOVERNMENT ACTIVITIES RELATED TO CRYPTOGRAPHY POLICY**

### ***National Level Activities***

Many OECD Member countries undertook the development of policy and laws relating to cryptography in the mid-1990s. National policies began to be developed in isolation from one another; however, it was recognised early on that disparities in laws could create obstacles to the development of national and global information and communications networks. When the OECD was called upon to examine cryptography policy in 1995, several OECD Member countries already had laws which addressed some aspects of cryptography policy (specifically digital signature and export regulations). Many other countries had legislative initiatives pending or were studying the problems with a view to preparing law. These national efforts and a discussion of national experiences were brought to the drafting table at the OECD to help clarify the problems and the implications of cryptography policy, and they provided a solid basis for international co-operation in this area.

### ***Cryptography Policy at the OECD***

The OECD provides an appropriate forum in which to review matters of common interest with regard to cryptography policy, since it has continuing experience in addressing policy issues that combine economic, technological and legal aspects as well as in building awareness and international consensus on issues related to security of information systems, protection of personal data and privacy, and information, computer and communication technologies. The OECD has already served in previous years as a forum for discussion of cryptography technologies and the economic and social policy issues related to the use of cryptography.

Both the *1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and the *1992 OECD Guidelines for the Security of Information Systems* identified the need for technological means to assure protection of personal data and privacy and security of information systems. Since 1989, the OECD Information, Computer and Communications Policy (ICCP) Committee has included cryptography technologies and policies in its work on security and privacy. The 1989 report by the OECD Secretariat, *Information Network Security*, included a review of cryptography technology and policy issues. These issues were discussed at the OECD Meeting on Information Security in March 1990. The Meeting of Experts on Recent Developments in Protection of Personal Data and Privacy, held on 10-11 December 1992, was the first OECD meeting to examine cryptography technologies and policies in depth. Speakers from the private sector and academia introduced cryptography, described various cryptography technologies, and discussed the relevant policy considerations. The Meeting of

Experts on Information Infrastructures, which was held at the OECD on 30 November-2 December 1994, included a session on cryptography policy. The Meeting emphasized the links between cryptography policy, protection of personal data and privacy, security of information systems, and protection of intellectual property, and stressed that the goals of security, privacy and intellectual property protection must be achieved in balance, and that solutions to one should not vitiate another or create unjustified obstacles to trade.

The OECD *Ad hoc* Meeting of Experts on Cryptography Policy, held on 18-19 December 1995, focused attention on the issues and gave Member countries an opportunity to discuss and compare their national positions on cryptography policy. The Meeting was attended by a diverse group of government representatives – including representatives of trade, industry and telecommunication ministries, data protection authorities, law enforcement and national security agencies – as well as members of the private sector, many of whom were technology experts. The discussion emphasized the need for internationally harmonized and compatible national solutions that strike the appropriate balance between data protection and law enforcement.

The private sector played an important role in the development of guidelines on cryptography policy at the OECD. In accord with the 1995 OECD Ministerial mandate that non-governmental partners be included in activities relating to global information infrastructure, the first Business-Government Forum on Global Cryptography Policy was held on 19-20 December 1995, co-organised by the International Chamber of Commerce (ICC), the Business and Industry Advisory Committee to the OECD (BIAC) and the OECD, in conjunction with the *Ad hoc* Meeting. At the Forum, the private sector presented its perspective and outlined a number of business initiatives for global cryptography policy.

The OECD Group of Experts on Security, Privacy and Intellectual Property Protection in the Global Information Infrastructure, which met for the first time on 9 February 1996 in Canberra, Australia, approved the United States' proposal for the OECD to draft guidelines on cryptography policy. At the 29th Session of the ICCP Committee on 27-29 March 1996, the *Ad hoc* Group of Experts on Cryptography Policy Guidelines was established.

The Communiqué that was issued following the 21-22 May 1996 Meeting of the OECD Council at the Ministerial Level specifically mentioned cryptography policy in its Guidelines for the Work of the Organisation:

“15. To facilitate the implementation of their commitments, bearing in mind the requirement to fit new work within a constrained budget, by concentrating on core priorities, Ministers request the OECD to:

(iv) – deepen its work on a comprehensive policy framework to facilitate further development of the Global Information Infrastructure and related

products and services, including the development of cryptography policy guidelines which would enhance security and protect intellectual property rights in this area, and analyse the economic and social impacts.”

With the issues gaining public prominence, the guidelines drafting process officially began with the First Meeting of the *Ad hoc* Group of Experts held in Washington, DC, on 8 May 1996. A second ICC/BIAC/OECD Business-Government Forum on Global Cryptography Policy held on 7 May 1996 gave Members of the *Ad hoc* Group another opportunity to discuss the issues with business representatives. The work continued through the year with three more meetings of the *Ad hoc* Group in June, September and December 1996. Prior to the September meeting, members of the *Ad hoc* Group participated in a public symposium, organised by the Electronic Privacy Information Center, which provided an opportunity to hear from leading cryptographers, technical experts, and human rights advocates regarding recent developments in cryptography policy. More than 100 delegates from governments, industry, and advocacy groups attended each meeting of the *Ad hoc* Group.

At its second meeting on 27-28 January 1997, the Group of Experts on Security, Privacy and Intellectual Property Protection in the Global Information Infrastructure reviewed and approved the draft Guidelines. The ICCP Committee gave its approval to the draft Guidelines at its 27-28 February 1997 meeting and forwarded the document to the Council. The Council adopted the Guidelines as a Recommendation of the Council concerning Guidelines for Cryptography Policy on 27 March 1997.

### ***Relevant National and International Activities Related to Cryptography Policy***

Data protection and privacy laws have been implemented in a number of countries and in the European Union in recent years. 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, for example, requires the implementation of appropriate technical and organisational measures to protect personal data against accidental loss, alteration, or unauthorised disclosure or access, in particular where data is transmitted over a network. This Directive raises specific concerns in the cryptography policy debate, because cryptography is an important means to protect the confidentiality of data.

Cryptographic products and technologies have historically been subject to export controls. The current basis for export controls is the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies (agreed on 13 July 1996), which includes cryptography products on its control lists for export. The Arrangement is implemented in national regulations.



Regulation [(EC)3381/94] and Decision [94/942/PESC] of the Council of the European Union of 19 December 1994 on the control of the export of dual-use goods are also applicable to the export of cryptography products. Some individual states have imposed other specific controls on such exports, which are subject to continuing debate.

The Council of Europe has devoted considerable resources to studying the subject of computer-related crime, issuing the Recommendation [R(95)13] of the Council of Europe of 11 September 1995 concerning problems of criminal procedural law connected with information technology, and is considering suggesting an international convention to address the issue. Such a convention could address matters such as exchange of information among government agencies in cases involving the use of cryptography.

At the G7 Summit meeting on anti-terrorism in July 1996, G7 governments announced that consultations would be accelerated, "in appropriate bilateral or multilateral fora, on the use of encryption that allows, when necessary, lawful government access to data and communications in order, *inter alia*, to prevent or investigate acts of terrorism, while protecting the privacy of legitimate communications".

In May 1996 the US National Research Council's Computer Science and Telecommunications Board published the report "Cryptography's Role in Securing the Information Society". This interagency study assesses the effect of cryptographic technologies on US national security, law enforcement, commercial and privacy interests, and reviews the impact of export controls on cryptographic technologies. This authoritative report provides a comprehensive review of the cryptography policy issues faced by the US Government.

None of these efforts, however, has attempted to address comprehensively international cryptography policy, or to identify the various interests which must be balanced in the context of international cryptography policy. In this area, these OECD Guidelines for Cryptography Policy are intended to be of assistance to Member countries by raising these issues for their consideration.

## **V. OTHER ISSUES**

### ***Non-member Countries***

The Recommendation is addressed to Member countries. Widespread recognition of the Guidelines is, however, desirable and non-member countries should be encouraged to adhere to the Recommendation. In view of the development of global information and communications networks and the need to ensure concerted solutions, efforts will be made to bring the Guidelines to the attention of non-member countries and appropriate international organisations.

### ***The Broader Policy Perspective***

Given the role of cryptography in the information and communications infrastructure and in developing electronic commerce, cryptography policy overlaps with economic, legal and political aspects of a number of related fields, including security of information systems, protection of privacy and personal data, and intellectual property protection. In order for information and communications networks and technologies to reach their full potential, national governments should address those issues related to cryptography which impede secure electronic commerce, including the lack of standards and the role of certification authorities.

The Mandate of the *Ad hoc* Group required it to develop guidelines on basic issues to be taken into consideration in the development of cryptography policy. The Guidelines constitute a new instrument complementing existing international instruments governing such issues as human rights, international trade, copyright, telecommunications, and various information services. If the need arises, the principles set out in the Guidelines could be further developed within the framework of activities undertaken by the OECD in the area of information, computer and communications policies.

## NOTES

1. For a more detailed description of how public key cryptography works, see:
  - “Cryptography’s Role in Securing the Information Society”, Computer Science and Telecommunications Board, United States National Research Council, National Academy Press, Washington, DC, 1996.
  - “Cryptography FAQ: Public Key Cryptography”; Oxford University Libraries Automation Service, World Wide Web Server, <http://www.lib.ox.ac.uk/internet/news/faq/archive/cryptography-faq.part06.html>.
  - “PUBLIC-KEY CRYPTOGRAPHY”, United States National Institute of Standards and Technology’s Computer Security Resource Clearinghouse, NIST Special Publication 800-2, <http://csrc.ncsl.nist.gov/nistpubs/800-2.txt>.
2. A TTP is an independent party, which may be either a public or private sector entity, that provides trusted services for information and communications networks. In this case, the trusted services of the TTP would be to hold the key for safekeeping subject to certain terms and conditions and upon agreement of the parties involved. Under such a system, the keys, or plaintext of encrypted data if appropriate, could be accessed pursuant to legal authority, such as a legal warrant or court order issued by the proper authority.

**MAIN SALES OUTLETS OF OECD PUBLICATIONS  
PRINCIPAUX POINTS DE VENTE DES PUBLICATIONS DE L'OCDE**

**AUSTRALIA – AUSTRALIE**

D.A. Information Services  
648 Whitehorse Road, P.O.B 163  
Mitcham, Victoria 3132 Tel. (03) 9210.7777  
Fax: (03) 9210.7788

**AUSTRIA – AUTRICHE**

Gerold & Co.  
Graben 31  
Wien I Tel. (0222) 533.50.14  
Fax: (0222) 512.47.31.29

**BELGIUM – BELGIQUE**

Jean De Lannoy  
Avenue du Roi, Koningslaan 202  
B-1060 Bruxelles Tel. (02) 538.51.69/538.08.41  
Fax: (02) 538.08.41

**CANADA**

Renouf Publishing Company Ltd.  
5369 Canotek Road  
Unit 1  
Ottawa, Ont. K1J 9J3 Tel. (613) 745.2665  
Fax: (613) 745.7660

Stores:  
71 1/2 Sparks Street  
Ottawa, Ont. K1P 5R1 Tel. (613) 238.8985  
Fax: (613) 238.6041

12 Adelaide Street West  
Toronto, QN M5H 1L6 Tel. (416) 363.3171  
Fax: (416) 363.5963

Les Éditions La Liberté Inc.  
3020 Chemin Sainte-Foy  
Sainte-Foy, PQ G1X 3V6 Tel. (418) 658.3763  
Fax: (418) 658.3763

Federal Publications Inc.  
165 University Avenue, Suite 701  
Toronto, ON M5H 3B8 Tel. (416) 860.1611  
Fax: (416) 860.1608

Les Publications Fédérales  
1185 Université  
Montréal, QC H3B 3A7 Tel. (514) 954.1633  
Fax: (514) 954.1635

**CHINA – CHINE**

Book Dept., China National Publications  
Import and Export Corporation (CNPIEC)  
16 Gongti E. Road, Chaoyang District  
Beijing 100020 Tel. (10) 6506-6688 Ext. 8402  
(10) 6506-3101

**CHINESE TAIPEI – TAIPEI CHINOIS**

Good Faith Worldwide Int'l. Co. Ltd.  
9th Floor, No. 118, Sec. 2  
Chung Hsiao E. Road  
Taipei Tel. (02) 391.7396/391.7397  
Fax: (02) 394.9176

**CZECH REPUBLIC –  
RÉPUBLIQUE TCHÈQUE**

National Information Centre  
NIS – prodejna  
Konviktská 5  
Praha 1 – 113 57 Tel. (02) 24.23.09.07  
Fax: (02) 24.22.94.33

E-mail: nkposp@dec.niz.cz  
Internet: http://www.nis.cz

**DENMARK – DANEMARK**

Munksgaard Book and Subscription Service  
35, Nørre Søgade, P.O. Box 2148  
DK-1016 København K Tel. (33) 12.85.70  
Fax: (33) 12.93.87

J. H. Schultz Information A/S,  
Herstedvang 12,  
DK – 2620 Albertslung Tel. 43 63 23 00  
Fax: 43 63 19 69

Internet: s-info@inet.uni.c.dk

**EGYPT – ÉGYPTÉ**

The Middle East Observer  
41 Sherif Street  
Cairo Tel. (2) 392.6919  
Fax: (2) 360.6804

**FINLAND – FINLANDE**

Akateeminen Kirjakauppa  
Keskuskatu 1, P.O. Box 128  
00100 Helsinki

Subscription Services/Agence d'abonnements :  
P.O. Box 23  
00100 Helsinki Tel. (358) 9.121.4403  
Fax: (358) 9.121.4450

**\*FRANCE**

OECD/OCDE  
Mail Orders/Commandes par correspondance :  
2, rue André-Pascal  
75775 Paris Cedex 16 Tel. 33 (0)1.45.24.82.00  
Fax: 33 (0)1.49.10.42.76  
Telex: 640048 OCDE  
Internet: Compte.PUBSINQ@oecd.org

Orders via Minitel, France only/  
Commandes par Minitel, France  
exclusivement : 36 15 OCDE

OECD Bookshop/Librairie de l'OCDE :  
33, rue Octave-Feuillet  
75016 Paris Tel. 33 (0)1.45.24.81.81  
Fax: 33 (0)1.45.24.81.67

Dawson  
B.P. 40  
91121 Palaiseau Cedex Tel. 01.89.10.47.00  
Fax: 01.64.54.83.26

Documentation Française  
29, quai Voltaire  
75007 Paris Tel. 01.40.15.70.00

Economica  
49, rue Héricart  
75015 Paris Tel. 01.45.78.12.92  
Fax: 01.45.75.05.67

Gibert Jeune (Droit-Économie)  
6, place Saint-Michel  
75006 Paris Tel. 01.43.25.91.19

Librairie du Commerce International  
10, avenue d'Iéna  
75016 Paris Tel. 01.40.73.34.60

Librairie Dunod  
Université Paris-Dauphine  
Place du Maréchal-de-Lattre-de-Tassigny  
75016 Paris Tel. 01.44.05.40.13

Librairie Lavoisier  
11, rue Lavoisier  
75008 Paris Tel. 01.42.65.39.95

Librairie des Sciences Politiques  
30, rue Saint-Guillaume  
75007 Paris Tel. 01.45.48.36.02

P.U.F.  
49, boulevard Saint-Michel  
75005 Paris Tel. 01.43.25.83.40

Librairie de l'Université  
12a, rue Nazareth  
13100 Aix-en-Provence Tel. 04.42.26.18.08

Documentation Française  
165, rue Garibaldi  
69003 Lyon Tel. 04.78.63.32.23

Librairie Decitre  
29, place Bellecour  
69002 Lyon Tel. 04.72.40.54.54

Librairie Sauramps  
Le Triangle  
34967 Montpellier Cedex 2 Tel. 04.67.58.85.15  
Fax: 04.67.58.27.36

A la Sorbonne Actual  
23, rue de l'Hôtel-des-Postes  
06000 Nice Tel. 04.93.13.77.75  
Fax: 04.93.80.75.69

**GERMANY – ALLEMAGNE**

OECD Bonn Centre  
August-Bebel-Allee 6  
D-53175 Bonn Tel. (0228) 959.120  
Fax: (0228) 959.12.17

**GREECE – GRÈCE**

Librairie Kauffmann  
Stadiou 28  
10564 Athens Tel. (01) 32.55.321  
Fax: (01) 32.30.320

**HONG-KONG**

Swindon Book Co. Ltd.  
Astoria Bldg. 3F  
34 Ashley Road, Tsimshatsui  
Kowloon, Hong Kong Tel. 2376.2062  
Fax: 2376.0685

**HUNGARY – HONGRIE**

Euro Info Service  
Margitsziget, Európa Ház  
1138 Budapest Tel. (1) 111.60.61  
Fax: (1) 302.50.35  
E-mail: euroinfo@mail.matav.hu  
Internet: http://www.euroinfo.hu/index.html

**ICELAND – ISLANDE**

Mál og Menning  
Laugavegi 18, Pósthólf 392  
121 Reykjavik Tel. (1) 552.4240  
Fax: (1) 562.3523

**INDIA – INDE**

Oxford Book and Stationery Co.  
Scindia House  
New Delhi 110001 Tel. (11) 331.5896/5308  
Fax: (11) 332.2639  
E-mail: oxford.publ@access.net.in

17 Park Street  
Calcutta 700016 Tel. 240832

**INDONESIA – INDONÉSIE**

Pdii-Lipi  
P.O. Box 4298  
Jakarta 12042 Tel. (21) 573.34.67  
Fax: (21) 573.34.67

**IRELAND – IRLANDE**

Government Supplies Agency  
Publications Section  
4/5 Harcourt Road  
Dublin 2 Tel. 661.31.11  
Fax: 475.27.60

**ISRAEL – ISRAËL**

Praedicta  
5 Shatner Street  
P.O. Box 34030  
Jerusalem 91430 Tel. (2) 652.84.90/1/2  
Fax: (2) 652.84.93

R.O.Y. International  
P.O. Box 13056  
Tel Aviv 61130 Tel. (3) 546 1423  
Fax: (3) 546 1442  
E-mail: royil@netvision.net.il

Palestinian Authority/Middle East:  
INDEX Information Services  
P.O.B. 19502  
Jerusalem Tel. (2) 627.16.34  
Fax: (2) 627.12.19

**ITALY – ITALIE**

Libreria Commissionaria Sansoni  
Via Duca di Calabria, 1/1  
50125 Firenze Tel. (055) 64.54.15  
Fax: (055) 64.12.57

E-mail: licosa@ftbcc.it  
Via Bartolini 29  
20155 Milano Tel. (02) 36.50.83

Editrice e Libreria Herder  
Piazza Montecitorio 120  
00186 Roma Tel. 679.46.28  
Fax: 678.47.51

Libreria Hoepfli  
Via Hoepfli 5  
20121 Milano  
Tel. (02) 86.54.46  
Fax: (02) 805.28.86

Libreria Scientifica  
Dott. Lucio de Biasio 'Aeiou'  
Via Coronelli, 6  
20146 Milano  
Tel. (02) 48.95.45.52  
Fax: (02) 48.95.45.48

**JAPAN – JAPON**  
OECD Tokyo Centre  
Landic Akasaka Building  
2-3-4 Akasaka, Minato-ku  
Tokyo 107  
Tel. (81.3) 3586.2016  
Fax: (81.3) 3584.7929

**KOREA – CORÉE**  
Kyobo Book Centre Co. Ltd.  
P.O. Box 1658, Kwang Hwa Moon  
Seoul  
Tel. 730.78.91  
Fax: 735.00.30

**MALAYSIA – MALAISIE**  
University of Malaya Bookshop  
University of Malaya  
P.O. Box 1127, Jalan Pantai Baru  
59700 Kuala Lumpur  
Malaysia  
Tel. 756.5000/756.5425  
Fax: 756.3246

**MEXICO – MEXIQUE**  
OECD Mexico Centre  
Edificio INFOTEC  
Av. San Fernando no. 37  
Col. Toriello Guerra  
Tlalpan C.P. 14050  
Mexico D.F.  
Tel. (525) 528.10.38  
Fax: (525) 606.13.07  
E-mail: oecd@rtn.net.mx

**NETHERLANDS – PAYS-BAS**  
SDU Uitgeverij Plantijnstraat  
Externe Fondsen  
Postbus 20014  
2500 EA's-Gravenhage  
Voor bestellingen:  
Tel. (070) 37.89.880  
Fax: (070) 34.75.778

Subscription Agency/Agence d'abonnements :  
SWETS & ZEITLINGER BV  
Heereweg 347B  
P.O. Box 830  
2160 SZ Lisse  
Tel. 252.435.111  
Fax: 252.415.888

**NEW ZEALAND – NOUVELLE-ZÉLANDE**  
GPLegislation Services  
P.O. Box 12418  
Thorndon, Wellington  
Tel. (04) 496.5655  
Fax: (04) 496.5698

**NORWAY – NORVÈGE**  
NIC INFO A/S  
Ostensjoveien 18  
P.O. Box 6512 Etterstad  
0606 Oslo  
Tel. (22) 97.45.00  
Fax: (22) 97.45.45

**PAKISTAN**  
Mirza Book Agency  
65 Shahrah Quaid-E-Azam  
Lahore 54000  
Tel. (42) 735.36.01  
Fax: (42) 576.37.14

**PHILIPPINE – PHILIPPINES**  
International Booksource Center Inc.  
Rm 179/920 Cityland 10 Condo Tower 2  
HV dela Costa Ext cor Valero St.  
Makati Metro Manila  
Tel. (632) 817 9676  
Fax: (632) 817 1741

**POLAND – POLOGNE**  
Ars Polona  
00-950 Warszawa  
Krakowskie Przedmiescie 7  
Tel. (22) 264760  
Fax: (22) 265334

**PORTUGAL**  
Livraria Portugal  
Rua do Carmo 70-74  
Apart. 2681  
1200 Lisboa  
Tel. (01) 347.49.82/5  
Fax: (01) 347.02.64

**SINGAPORE – SINGAPOUR**  
Ashgate Publishing  
Asia Pacific Pte. Ltd  
Golden Wheel Building, 04-03  
41, Kallang Pudding Road  
Singapore 349316  
Tel. 741.5166  
Fax: 742.9356

**SPAIN – ESPAGNE**  
Mundi-Prensa Libros S.A.  
Castelló 37, Apartado 1223  
Madrid 28001  
Tel. (91) 431.33.99  
Fax: (91) 575.39.98  
E-mail: mundiprensa@tsai.es  
Internet: <http://www.mundiprensa.es>

Mundi-Prensa Barcelona  
Consell de Cent No. 391  
08009 – Barcelona  
Tel. (93) 488.34.92  
Fax: (93) 487.76.59

Libreria de la Generalitat  
Palau Moja  
Rambla dels Estudis, 118  
08002 – Barcelona  
(Suscripciones) Tel. (93) 318.80.12  
(Publicaciones) Tel. (93) 302.67.23  
Fax: (93) 412.18.54

**SRI LANKA**  
Centre for Policy Research  
c/o Colombo Agencies Ltd.  
No. 300-304, Galle Road  
Colombo 3  
Tel. (1) 574240, 573551-2  
Fax: (1) 575394, 510711

**SWEDEN – SUÈDE**  
CE Fritzes AB  
S-106 47 Stockholm  
Tel. (08) 690.90.90  
Fax: (08) 20.50.21

For electronic publications only/  
Publications électroniques seulement  
STATISTICS SWEDEN  
Informationsservice  
S-115 81 Stockholm  
Tel. 8 783 5066  
Fax: 8 783 4045

Subscription Agency/Agence d'abonnements :  
Wennergren-Williams Info AB  
P.O. Box 1305  
171 25 Solna  
Tel. (08) 705.97.50  
Fax: (08) 27.00.71

Liber distribution  
International organizations  
Fagerstagatan 21  
S-163 52 Spanga

**SWITZERLAND – SUISSE**  
Maditec S.A. (Books and Periodicals/Livres  
et périodiques)  
Chemin des Palettes 4  
Case postale 266  
1020 Renens VD 1  
Tel. (021) 635.08.65  
Fax: (021) 635.07.80

Librairie Payot S.A.  
4, place Pépînet  
CP 3212  
1002 Lausanne  
Tel. (021) 320.25.11  
Fax: (021) 320.25.14

Librairie Unilivres  
6, rue de Candolle  
1205 Genève  
Tel. (022) 320.26.23  
Fax: (022) 329.73.18

Subscription Agency/Agence d'abonnements :  
Dynapresse Marketing S.A.  
38, avenue Vibert  
1227 Carouge  
Tel. (022) 308.08.70  
Fax: (022) 308.07.99

See also – Voir aussi :  
OECD Bonn Centre  
August-Bebel-Allee 6  
D-53175 Bonn (Germany) Tel. (0228) 959.120  
Fax: (0228) 959.12.17

**THAILAND – THAÏLANDE**  
Suksit Siam Co. Ltd.  
113, 115 Fuang Nakhon Rd.  
Opp. Wat Rajabophit  
Bangkok 10200  
Tel. (662) 225.9531/2  
Fax: (662) 222.5188

**TRINIDAD & TOBAGO, CARIBBEAN TRINITE-ET-TOBAGO, CARAÏBES**  
Systematics Studies Limited  
9' Watts Street  
Curepe  
Trinidad & Tobago, W.I. Tel. (1809) 645.3475  
Fax: (1809) 662.5654  
E-mail: tobe@trinidad.net

**TUNISIA – TUNISIE**  
Grande Librairie Spécialisée  
Fendri Ali  
Avenue Haffouz Imm El-Intilaka  
Bloc B 1 Sfax 3000  
Tel. (216-4) 296 855  
Fax: (216-4) 298.270

**TURKEY – TURQUIE**  
Kültür Yayinlari Is-Türk Ltd.  
Atatürk Bulvari No. 191/Kat 13  
06684 Kavaklıdere/Ankara  
Tel. (312) 428.11.40 Ext. 2458  
Fax : (312) 417.24.90

Dolmabahce Cad. No. 29  
Besiktas/Istanbul  
Tel. (212) 260 7188

**UNITED KINGDOM – ROYAUME-UNI**  
The Stationery Office Ltd.  
Postal orders only:  
P.O. Box 276, London SW8 5DT  
Gen. enquiries  
Tel. (171) 873 0011  
Fax: (171) 873 8463

The Stationery Office Ltd.  
Postal orders only:  
49 High Holborn, London WC1V 6HB  
Branches at: Belfast, Birmingham, Bristol,  
Edinburgh, Manchester

**UNITED STATES – ÉTATS-UNIS**  
OECD Washington Center  
2001 L Street N.W., Suite 650  
Washington, D.C. 20036-4922  
Tel. (202) 785.6323  
Fax: (202) 785.0350

Internet: [washcont@oecd.org](mailto:washcont@oecd.org)

Subscriptions to OECD periodicals may also be placed through main subscription agencies.

Les abonnements aux publications périodiques de l'OCDE peuvent être souscrits auprès des principales agences d'abonnement.

Orders and inquiries from countries where Distributors have not yet been appointed should be sent to: OECD Publications, 2, rue André-Pascal, 75775 Paris Cedex 16, France.

Les commandes provenant de pays où l'OCDE n'a pas encore désigné de distributeur peuvent être adressées aux Éditions de l'OCDE, 2, rue André-Pascal, 75775 Paris Cedex 16, France.

12-1996

OECD PUBLICATIONS, 2, rue André-Pascal, 75775 PARIS CEDEX 16

PRINTED IN FRANCE

(93 98 01 1 P) ISBN 92-64-16023-X – No. 49977 1998