Unclassified **DSTI/ICCP/REG(98)4/REV1**

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

OLIS : 06-May-1998
Dist. : 12-May-1998

Or. Eng.

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP/REG(98)4/REV1
Unclassified

Group of Experts on Information Security and Privacy

INVENTORY OF CONTROLS ON CRYPTOGRAPHY TECHNOLOGIES

This inventory of controls on cryptography technologies in OECD countries focuses on domestic controls, and export or import restrictions. The inventory report provides a mechanism to exchange information among Member countries in the field of cryptography policy to promote a further discussion of related issues, and it forms a part of the continuing work of the OECD in this area.

In accordance with the guidelines for classification of documents adopted by the Council in 1997, this document has been prepared by the Secretariat as an "unclassified" document, on the basis of independent research and input received from Member countries. A preliminary draft of this document was issued in March 1998 and Member countries were invited to provide written comments and contribute further materials. This revised version incorporates the input received.

This document will be discussed by the Group of Experts on Information Security and Privacy at its meeting on 18-19 May 1998. The Group of experts is invited to agree that the document can be widely distributed. The Group is further invited to consider future work in this area.

65226

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

Or. Eng.

TABLE OF CONTENTS

NOTE FROM THE SECRETARIAT

1. At its meeting on 20-21 October 1997, the Group of Experts on Information Security and Privacy agreed to undertake a study to review the existing laws in Member countries related to cryptography technologies. Specifically, the Group agreed that, drawing upon the input of the Group of Experts, the Secretariat will prepare a report covering the following three topics:

- To what extent do countries have domestic controls on encryption, and what amendments to domestic laws, if any, are contemplated?

- To what extent do countries have import or export controls on encryption, and what amendments to such import or export laws, if any, are contemplated?

- To what extent are the law enforcement personnel of member countries encountering encryption, and what effect has this had on protecting public safety?

2. This inventory of controls on cryptography technologies OECD Member countries focuses on domestic controls, and import or export restrictions. The preliminary draft of this inventory report was issued in March 1998 as a consultation paper to prompt further input from Member countries. Governments were invited to review the preliminary draft, to provide comments on the text, and to contribute further materials to assist the Secretariat in producing an inventory report which reflects the current state of affairs as fully and accurately as possible. In preparing contributions to this document, national delegations were invited to take the following questions into consideration:

1. Are your country's domestic controls on encryption accurately reflected in this preliminary draft? Are any amendments to these domestic laws contemplated? Is there any further information which could be reported in this regard?

2. Are your country's import or export controls on encryption accurately reflected in this preliminary draft? Are any amendments to these import or export controls contemplated? Is there any further information which could be reported in this regard?

3. To what extent are the law enforcement personnel of your country encountering encryption, and what effect has this had on protecting public safety?

3. This inventory does not include laws on the use of cryptography for authentication and certification, which will be covered by a separate report directed specifically at that issue, "Preliminary Draft: Inventory of Approaches to Authentication and Certification in a Global Networked Society" [DSTI/ICCP/REG(98)3]. These inventory reports will provide mechanisms to exchange information among Member countries in the field of cryptography policy to promote a further discussion of related issues, and they form a part of the continuing work of the OECD in this area.

4. This document has been prepared by the Secretariat on the basis of independent research and input received from Member countries. This revised version incorporates the written comments received from Member countries during the consultation period in March-April 1998. This document will be discussed by the Group of Experts on Information Security and Privacy at its meeting on 18-19 May 1998. The Group of Experts is invited to **agree** that the document can be distributed widely. The Group is further invited to **consider** future work in this area.

INVENTORY OF CONTROLS ON CRYPTOGRAPHY TECHNOLOGIES

INTERNATIONAL INSTRUMENTS

The Wassenaar Arrangement

1. For over four decades, export controls on cryptography were governed by the Coordinating Committee for Multilateral Export Controls (COCOM)[1]. COCOM was created in 1950 to respond to the threat of the Cold War by preventing the sale of arms, and controlling the export of strategic products and technical data from COCOM Member countries to the Warsaw Pact countries. Under the COCOM regime, cryptography was considered a strategic good with military applications, and thus was subject to trade restrictions. In 1991, COCOM decided to allow the export of mass-market cryptographic software (including public domain software); most COCOM Member countries reflected these changes in their national regulations.

2. In response to the diminishing Cold War threat, and in light of emerging new risks to global security, COCOM was dissolved in March 1994 as part of a plan to make a transition to a different kind of agreement. The focus had shifted from a Western screen for controlling the transfer of military technologies, toward a mechanism for addressing the proliferation of weapons of mass destruction and stemming the transfer of dual-use equipment and high technology. Negotiations were initiated by former COCOM countries to develop a regime which would differ significantly in both its goals and procedures, highlighting mechanisms for transparency. During the interim period pending the signing of a new treaty, most members of COCOM agreed in principle to maintain the status quo, and cryptography remained on export control lists.

3. Since 1995, the main international instrument dealing with export controls on cryptography technologies has been the Wassenaar Arrangement on Export Controls for Conventional Arms Dual-Use Goods and Technologies.[2] The Wassenaar Arrangement was formally approved by 33 countries, including 27 of the 29 OECD Member countries, in July 1996.[3] The Wassenaar Arrangement is a collaboration of countries that defines a set of preliminary guidelines covering both armaments and sensitive dual-use goods and technologies which need to be fully implemented at the national level. It focuses on threats to international and regional peace and security by providing for greater openness through information sharing about arms and technology transfers world-wide. The agreement provides an initial framework which depends to some extent on the way participating countries interpret it, and Member governments sometimes have differing views about how the agreement should be implemented. The agreement does not provide mechanisms in case of non-observance and it is up to national discretion as to how to handle such cases.

4. Basically, the Wassenaar Arrangement provides a global mechanism for controlling transfers of conventional armaments and sensitive dual-use items, and a venue in which governments can consider collectively the implications of various activities on international and regional security. Agreement is by

consensus, and membership is open on a global and non-discriminatory basis to all countries meeting the agreed criteria. For membership countries must be producers or exporters of arms or dual-use equipment; adhere to the major non-proliferation regimes; have responsible export policies toward states whose behaviour is a cause of concern (particularly those countries with military end-uses for sensitive technologies); and implement adequate export controls. The agreement outlines a formal process of transparency, consultation, and where appropriate, multilateral restraint.

5. Participants agree to control through their national laws, regulations and policies those items and technologies contained in a list of Dual-Use Goods and Technologies and a separate Munitions List. 1 November 1996 was set as a target date for implementation of the Lists at the national level. The Arrangement also established a Secretariat in Vienna and participants agreed to meet regularly (at least once a year). The first formal conference to review the agreement will be held in 1999. Aggregate data on transfers, denials and under-cuts is exchanged every six months[4]. Denials of sensitive/very sensitive goods have to be notified on an early and timely basis[5].

6. There are four principal objectives of the Arrangement. It aims to contribute to regional and national security by:

- promoting transparency and greater responsibility with regard to transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations;

- seeking through national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities;

- complementing and reinforcing, without duplication, the existing control regimes for weapons of mass destruction and their delivery systems, as well as other internationally recognised measures designed to promote transparency and greater responsibility, by focusing on the threats to international and regional peace and security which may arise from transfers of armaments and sensitive dual-use goods and technologies where risks are judged greatest; and,

- enhancing co-operation to prevent the acquisition of armaments and sensitive dual-use items for military end-uses, if the situation in a region or the behaviour of a state is, or becomes, a cause for serious concern to the Participating States.

7. The “Initial Elements” of the Wassenaar Arrangement include two lists of items and technologies which Member countries agree to control[6]: (1) a munitions list which covers conventional arms; and (2) a list of dual-use goods and technologies, i.e., goods that can be used both for a military and for a civil purpose. The latter list is divided into three Tiers: Tier 1 (basic list) and Tier 2 (sensitive list[7]) and Tier 3 (very sensitive list[8]). The agreement imposes a reporting requirement for the transfer or denial to a non-participant country of listed dual-use goods and technologies. The Tier 1 list requires notification be given aggregately on the usual six-monthly basis. However, sensitive Tier 2 and Tier 3 goods and technologies have a higher standard requiring individual notice to be given upon each transfer or denial to non-participant states, in no later than 60 days after the date of the occurrence. Transfers are notified on an aggregate basis, denials on an individual basis. Proposals to notify transfers for Tier 3 items have been made, but there is no consensus yet.

8. The Arrangement also requires participating countries to inform one another when a listed product is shipped to an end-user to which another participating country has denied a licence within the

preceding three years (“under-cutting”). Although participating countries are encouraged to exercise vigilance in the control of listed items, there is no specific obligation to require licenses, this is left to national discretion.

9. Cryptography technologies appear on the List of Dual-Use Goods and Technologies under Category 5, Part 2, “Information Security”. Both hardware and software cryptography technologies are listed for control. The exceptions to the provisions covering cryptography technologies are noteworthy:

5.A.2. does not control:

a. "Personalised smart cards" or specially designed components therefor, with any of the following characteristics:

1. Not capable of message traffic encryption or encryption of user-supplied data or related key management functions therefor; or

2. When restricted for use in equipment or systems excluded from control under entries 1. to 6. of the Note to 5.A.2.a.3. or under entries b. to h. of this Note;

b. Equipment containing "fixed" data compression or coding techniques;

c. Receiving equipment for radio broadcast, pay television or similar restricted audience television of the consumer type, without digital encryption and where digital decryption is limited to the video, audio or management functions;

d. Portable or mobile radiotelephones for civil use (e.g., for use with commercial civil cellular radiocommunications systems) that are not capable of end-to-end encryption;

e. Decryption functions specially designed to allow the execution of copy-protected "software", provided the decryption functions are not user-accessible;

f. Access control equipment, such as automatic teller machines, self-service statement printers or point of sale terminals, which protects password or personal identification numbers (PIN) or similar data to prevent unauthorized access to facilities but does not allow for encryption of files or text, except as directly related to the password or PIN protection;

g. Data authentication equipment which calculates a Message Authentication Code (MAC) or similar result to ensure no alteration of text has taken place, or to authenticate users, but does not allow for encryption of data, text or other media other than that needed for the authentication;

h. Cryptographic equipment specially designed and limited for use in machines for banking or money transactions, such as automatic teller machines, self-service statement printers or point of sale terminals.

10. According to the “General Technology Note” of the Dual-Use List, controls do not apply to "technology" "in the public domain", to "basic scientific research", or to the minimum necessary information for patent applications. The “General Software Note” states that:

The Lists do not control "software" which is either:

1. Generally available to the public by being:

a. Sold from stock at retail selling points without restriction, by means of:

1. Over-the-counter transactions;

2. Mail order transactions; or

3. Telephone call transactions; and

b. Designed for installation by the user without further substantial support by the supplier; or

2. "In the public domain".

European Union

Export controls

11. The Regulation and Decision of the Council of the European Union of 19 December 1994 concerning the control of the exports of dual-use goods[9] is the basis for the EU regime which governs the export of cryptography technologies.

12. The EC Regulation sets forth a license requirement for the export of certain cryptography products outside of the EU. For a transitional period, the Regulation also requires a licence procedure for intra-Community trade of certain particularly sensitive encryption products, which amounts to EU domestic controls on products shipped between Member States. However, the Regulation does not set out in full the scope, content and implementation practices of national controls. As a result, there is some divergence in national practices among EU Member States.

13. The Decision which implements the Regulation includes specific exceptions to the export controls that have an effect on the export of cryptography, and which some have interpreted as an indication that the export of cryptography via the Internet does not fall within the scope of the Regulation. In particular, the Decision states that the control of technology is limited to tangible form[10]. Furthermore, the "General Technology Note" of the Decision states that controls on technology do not apply to information "in the public domain", and the "General Software Note" indicates that the export control list does not include software which is "in the public domain" or "generally available" to the public by being (1) sold from stock at retail selling points, without restriction by means of over-the-counter transactions, mail order transactions, or telephone order transactions; and (2) designed for installation by the user without further substantial support by the supplier.

Other controls

14. There are no import controls on cryptography technologies imposed by European Union legislation.

15. The Treaty of Rome enshrines the principle of the free movement of goods within the Community, which has implications for national cryptography policies of the Member States.

16. The European Council Resolution of 17 January 1995 on the lawful interception of telecommunications[11] contains a requirement for network operators and service providers, if they use encryption, to provide intercepted communications to law-enforcement agencies "en clair", that is, to provide the signal as they received it.

General Policy Developments

17. In October 1997 the European Commission published a Communication “Ensuring security and trust in electronic Communication - Towards a European Framework for Digital Signatures and Encryption”[12], which describes both the authentication and integrity functions of cryptography, as well as confidentiality functions. The communications addresses lawful access to encryption keys (key recovery or key escrow schemes) under the latter section, on the basis that such schemes might be interpreted as domestic controls of cryptography. The Communication recognises that there are a number of commercial applications of “encryption”, including pay TV which operates commercially by using encryption where once the subscriber pays a fee to the transmission is decrypted.

18. The Communication endorses the use of encryption to enable law-abiding citizens and companies to protect themselves against criminal attacks, although noting that criminals cannot totally be prevented from using the technologies for their own ends. It states that "the public needs to have access to technical tools allowing effective protection of the confidentiality of data and communication against arbitrary intrusions. Encryption of data is very often the only effective and cost-efficient way of meeting these requirements." The Communication goes on to indicate that the Commission will be diligent in seeing that Member States’ national restrictions in the area of national security and law enforcement are justified and abide by the EU free circulation provisions, and Data Protection Directive. With regard to regulations on the use of encryption, it notes that "divergence between regulatory schemes might result in obstacles to the functioning of the Internal Market."

19. The Communication also points out that Member States must report to the Commission any proposals to impose technical rules for marketing, use manufacture or import of cryptographic products - [13]

20. The Communication advises that the dual-use Regulation should be adapted in view of the requirements for the cryptographic products market. It states that Article 19 of the Regulation contains a provision which should be re-examined, in particular to:

- progressively dismantle intra-Community controls on commercial encryption products (although not necessarily for very advanced encryption);
- launch a discussion on the scope and interpretation of certain provisions, such as the “General Software Note” (which stipulates that public-domain software is not subject to controls); and
- deal with problems like intangible means of transmission (such as fax or e-mail).

21. Finally, the Communication advocates co-operation between police forces on a European and international level, as well as international action to create a framework for electronic commerce which would involve mutual recognition of certificates and common technical standards.

22. Following on from the European Commission’s October 1997 Communication, DG XIII has issued a draft “Proposal for a European Parliament and Council Directive on a common framework for

electronic signatures", with a view to harmonising European initiatives on electronic signatures and to promote interoperability. It will be considered by the Commission on 6 May 1998.

23. The Commission has proposed a European Parliament and Council Directive on the legal protection of services based on, or consisting of conditional access. The proposal is based on a wide-ranging consultation in the context of the Green Paper on "Legal Protection for Encrypted Services In the Internal Market". The proposed Directive would cover all encoded services where encoding is used to ensure payment of a fee, including information society services provided at a distance by electronic means and at the individual request of a service receiver, as well as broadcasting services. [14]

Other European Fora

24. On 11 September 1995, the Council of Europe adopted a Recommendation[15] concerning problems of criminal procedural law connected with information technology. The document states that, "[m]easures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary." The Recommendation does not however require Member states to implement any specific policy on encryption in their jurisdictions.

25. A Ministerial level conference on Global Information Networks was held in Bonn on 6-8 July 1997. The Declaration of European Ministers[16] issued following the conference recognises the importance of strong cryptography, and declares that cryptographic products should be available internationally and users should have free choice of cryptographic technologies, subject to applicable law. It urges that measures to safeguard lawful access should be proportionate and effective.

OECD MEMBER COUNTRIES

Australia

Export controls

26. Australia is a member of the Wassenaar Arrangement. Furthermore, export regulations for the Commonwealth of Australia fall generally under the Commonwealth Regulations. [17]

27. The export of cryptographic hardware and software from Australia is regulated under the Defence and Strategic Goods List under the authority of the Department of Defence.[18] Written permission from the Department is needed for exporting "systems equipment and components" designed or modified to use cryptography or ensure information security or perform cryptoanalytic functions. This does not expressly include cryptographic software transmitted electronically, for example over the Internet. The export controls do not exclude public-domain or "generally available" cryptographic software; however, public-domain "technology" is excluded.[19] The relevant export licence is reviewed by the Defence Signals Directorate of the Department of Defence. In practice, export approval is now granted on a routine basis for encryption software with key lengths of 56 bits or less.

28. The Australian export restrictions on cryptography technologies include the same exemptions as those outlined in the Wassenaar Arrangement. The restrictions also include a personal-use exemption for

the temporary export of limited amounts of cryptographic hardware or software by Australian citizens or lawful permanent residents, according to the following limitations:

a) no transfer of hardware, software or technology takes place as a result of the exportation of the cryptographic products;

b) the cryptographic products remain under the control of and in the possession of the exporter;

c) the cryptographic products are not to be reproduced or copied;

d) the cryptographic products must be returned to Australia when the exporter returns to Australia; and

e) the cryptographic products shall not be used for demonstration, marketing or sales of controlled cryptographic products.

The quantity of cryptographic hardware or software products which may be exported under the authority of this permit is limited to one each of any hardware product, and one copy of each software product per exporter, per trip outside of Australia. Records of temporary exports and re-imports under this permit should be maintained by the exporter for a period of 3 years from the date of each temporary export.

Domestic controls and import regulations

29. There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Australia.

Austria

Export controls

30. Austria is a member of the Wassenaar Arrangement and the European Union. Export rules in Austria follow EU regulations on export of cryptographic technologies. "Generally available" software and software and technology "in the public domain" do not fall within the scope of the controls.

Domestic controls and import regulations

31. There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Austria.

32. The *Betriebsfunkverordnung* forbids the use of cryptography for in-house (i.e. internal to an organisation) radio transmissions.

Belgium

Export controls

33. Belgium is a member of the Wassenaar Arrangement and the European Union. Export rules in Belgium follow EU regulations on export of cryptographic products. An export license for exporting cryptography hardware or software outside of the Benelux countries is required. "Generally available" software and software and technology "in the public domain" do not fall within the scope of the controls.

Domestic controls and import regulations

34. There are no import restrictions on cryptography technologies, currently in place in Belgium. However, the use of cryptography systems have to be approved by the Belgian Institute for Posts and Telecommunications (BIT).

35. In 1996, there was a review of previously passed legislation[20] containing provisions which could be interpreted as forbidding the use of encryption equipment that would prevent telephone tapping by the authorities, and may require that private keys for decryption be deposited with a third party. The Belgian Ministry of Justice has stated that it is not their intention to prohibit the use of encryption, and the legislation has yet to be implemented. The agency for Belgium Information and Security (Belinfosec) is reportedly studying the issue. Recently proposed legislation would remove the provisions in question, and emphasise the everyday applications for cryptography, such as in health information systems and electronic banking. The Belgian Parliament is currently considering these issues further under a proposed amendment to the telecommunications law.

Canada

Export controls

36. Canada is a member of the Wassenaar Arrangement.

37. The Canadian Export Control List[21] includes hardware and software technologies designed or modified to use cryptography, however there are a number of exceptions, including:

- decryption functions specifically designed to allow the execution of copy-protected software;
- software designed to authenticate a message's content or the parties to a message, so long as it does not allow the encryption of the actual data or text being transmitted (includes digital signature functions);
- cryptographic functions designed or limited for use in machines for banking or money transactions, such as automatic teller machines, self-service statement printers, and point of sale terminals; and
- certain personalised smart cards.

38. In addition there are general exemptions from obtaining export licenses for any mass market software or software “in the public domain”.

39. US-origin goods not otherwise controlled under Canadian rules may require an export permit. All types of cryptography can be transported between Canada and the United States; however US-origin cryptography which is not included in the Canadian Export Control List remains under US export rules and cannot be exported from Canada if the US does not allow export. Public domain and mass-market software can be freely exported, unless it contains US-origin goods.

40. Export permits for controlled products are reviewed by the Export Controls Division of the Department of Foreign Affairs and International Trade. In practice, export approval is now granted on a routine basis for encryption products with key lengths of 56 bits or less.

Domestic controls and import regulations

41. No domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Canada.

42. ”A Survey of Legal Issues relating to the Security of Electronic Information” has been published by the Electronic Commerce Secretariat of the Department of Justice of Canada[22]. The Government of Canada Communications Security Establishment has produced the “Government of Canada Public Key Infrastructure White Paper” to give guidance to the Federal Government in providing electronic commerce and confidentiality services to public servants. The planned commencement of this program is late 1998[23].

Czech Republic

Export controls

43. The Czech Republic is a member of the Wassenaar Arrangement. The Czech Republic recently enacted the "Control of Exports and Imports of Goods and Technologies Subject to International Control Regimes."[24] This act is implemented by decree, incorporating the EU and Wassenaar lists of controlled dual-use goods.

44. Export permits for controlled products are reviewed by the Ministry of Industry and Trade. There are two kinds of licenses for export of cryptography products: an "individual license" or an "individual open license". Exporters typically receive an individual license with a written statement about the transaction. An individual open license is used for expected recurring exports of specific controlled goods within a particular territorial scope and a certain time period.

45. The Czech Republic's restrictions only apply to tangible technology and technical knowledge and, like the EU, exempt “generally available” software and public domain software and technology.

Import controls

46. The Czech Republic's export control regime described above also applies generally to the import of these controlled goods.[25] However, the Ministry has granted a general license for the import of

cryptographic products[26]. Thus, while the government retains authority to control imports of encryption, an importer of products incorporating cryptography does not currently need any special authorisation for such imports.

Domestic controls

47. No domestic controls on the use of cryptography are currently in place in the Czech Republic.

Denmark

Export controls

48. Denmark is a member of the Wassenaar Arrangement and the European Union. Export controls have been implemented according to the Wassenaar Arrangement. The authority for licensing is the Danish Agency for Trade and Industry.

Domestic controls and import regulations

49. No domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Denmark.

General Policy Developments

50. An Expert Committee On Cryptography under the auspices of the Ministry of Research and Information Technology, including representatives from other Danish Ministries, released a Report in April 1997[27]. The Committee studied the advantages and disadvantages of introducing regulation covering the use of cryptography, and the sale of cryptography. The Committee recommended that no regulation of cryptography should be introduced but that Danish cryptography policy should be viewed in light of international developments. The Expert Committee resolved to carry out an analysis to assess the possibilities and consequences of introducing incentive schemes to induce people to use key-recovery systems. The analysis of incentive schemes is expected to be concluded in May 1998.

51. In June 1996 the Danish Government's IT Security Council recommended that no limitations on the right of the individual to encrypt electronic communications should be introduced. However it was agreed that telecommunications companies using encryption integrated into the telecommunications network would be under a duty, when ordered by the court, to decode an encrypted communication in connection with the authorities investigating criminal activity. This requirement was included in the new telecommunications regulation introduced as part of the Danish tele-liberalisation in 1997.

Finland

Export controls

52. Finland is a member of the Wassenaar Arrangement and the European Union. For export of cryptographic products, a license is required through a 1996 law which implements the EU recommendation on export of dual-use goods. The licensing authority is the Ministry of Trade and Industry. A license is not needed for “generally available” software and public domain software and technology. However, Finland restricts the export of "technical assistance" and other "services,". Also, Finland restricts the export of "intangible technology," e.g., via the Internet.

Domestic controls and import regulations

53. No domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Finland.

France

Export/ import controls restrictions and domestic controls

54. France is a member of the Wassenaar Arrangement and the European Union. The government agency in charge of implementing laws related to cryptography is the “Service Central de la Sécurité des Systèmes d’Information”[28] (SCSSI), which comes under the authority of the Secretary General for National Defence.

55. The controls on encryption in France are governed by:

- law 90-1170 of 29 December 1990 (Official Journal of 30 December 1990), article 28; modified by law 91-648 of 11 July 1991 (Official Journal of 13 July 1991); and further modified by law 96-659 of 26 July 1996, notably article 17 on penalties (Official Journal of 27 July 1996);

- decree 95-613 of 5 May 1995 on the control of the export of goods with a double use (Official Journal of 7 May 1995, page 7547);

- order of 5 May 1995 on the control of export to third party countries and the transfer to member states of the European Community of goods with a double use (Official Journal of 7 May 1995, page 7561);

- order of 5 May 1995 defining the general G.502 licence for the export of encryption methods and setting out the means for establishing and using this licence (Official Journal of 7 May 1995, page 7578);

- decree 96-67 of 29 January 1996 relating to the powers of the Secretary General for National Defence (SGDN) on security in information technology (Official Journal of 30 January 1996); and

- decree 98-101 of 24 February 1998 defining the conditions in which declarations are submitted and licences granted for the import, export, use and supply of encryption products (Official Journal of 25 February 1998, page 2911)

- decree 98-102 of 24 February 1998 defining the conditions in which trusted third parties are licensed pursuant to article 28 of Law no. 90-1170 of 29 December 1990 on telecommunications regulations (Official Journal of 25 February 1998, page 2915)

56. In summary, article 28 of the "Telecommunications Law", the Law of 29 December 1990 states that for use, supply and export of cryptography with no other object than authentication of data or assuring data integrity, a prior declaration must be submitted. A copy of the acknowledgement of declaration must be presented to customs at each export. For temporary export, a user declaration will serve as an export declaration in the case of cryptography exclusively for personal use by an individual. For any other kind of cryptography, a prior authorisation is needed.

57. In June 1996, France updated its telecommunications law[29], in the "26th July Law", partly aimed toward relaxing restrictions. Article 17 of the new law deals with cryptography. The supply, import from countries outside the European Union, or export of an encryption device or service is subject to authorisation if it performs functions of confidentiality. However, the new law relaxes restrictions on the use of cryptography products in France.

58. Article 17 of the 26 July law relaxes restrictions on the use of authentication devices, stating that no prior declaration will be required for "encryption devices or services which do not provide confidentiality but are used to authenticate or guarantee the integrity of messages; where the device provides for confidentiality functions based solely on secret conventions managed under approved procedures and by an organisation approved under the conditions defined in Part II of the Article i.e. a licensed trusted third party."

59. The trusted third party will be a government licensed organisation which manages encoding keys for users. The licenses will be conditional upon the trusted third party submitting encoding keys to the appropriate authorities according to the law so that the State can, if necessary, access the information. Supply of cryptographic products remain subject to authorisation even if they are used in conjunction with a trusted third party.

60. The French Government describes a trusted third party's function as follows:

> *The trustworthy third party is a recognised organisation which manages encoding keys on the user's behalf. The user signs a contract with the trustworthy third party which regularly transmits the keys to use to encode information to the user. A clause is written into the licensing agreement with the trustworthy third party which stipulates that it must submit the encoding keys to the proper authorities according to the law. Thus, users can use an encryption professional who guarantees a high quality service to them, while the State can, if need be, have access to the information.*

Germany

Export controls

61. Germany is a member of the Wassenaar Arrangement and the European Union. Export of cryptographic products is regulated by implementation of the EU Dual-Use Regulation. "Generally available" software and software and technology 'in the public domain' do not fall within the scope of the controls. The administrating authority is the Federal Ministry of Economics (BMWi).

Domestic controls and import regulations

62. There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Germany.

General Policy Developments

63. The approach of the Ministry of Economics to electronic commerce is generally reflected in the Electronic Commerce Initiative of the Federal Government[30] of 29 October 1997. The statement declares that "[t]he German government does not presently intend to regulate by statute the marketing and use of encryption products. In Germany, encryption systems may thus be freely chosen and used."

64. At the Global Internet Project Summit in April 1997, the German Federal Government set out its views on the elements of a responsible government's cryptography policy:

1. define the conditions for the establishment of a trustworthy security infrastructure (trust should be encouraged by an officially guaranteed security level, resulting on official approval "stamps" on products);

2. guarantee that cryptographic methods are not misused by criminals;

3. promote international co-operation (cross-border key management, where copies of private keys should be escrowed anywhere in the world);

4. undertake an intense and open-minded discussion with all relevant governmental and non-governmental groups.

Greece

Export controls

65. Greece is a member of the Wassenaar Arrangement and the European Union. It has followed the EU Dual-Use Regulations.

Domestic controls and import regulations

66. There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Greece.

Hungary

Export controls

67. Hungary is a member of the Wassenaar Arrangement and has implemented controls according to the Wassenaar dual-use list. Export of "generally available" software and public domain software and technology is exempted. The licensing authority is the Ministry of Industry, Trade and Tourism.

Domestic controls and import regulations

68. There are import controls mirroring the export controls, requiring an import license if an export license would be needed in Hungary. There are no domestic laws regulating the use of cryptography.

Iceland

Export/ import controls restrictions and domestic controls

69. There are no domestic controls on the use of cryptography, nor are there export or import restrictions on cryptography technologies, currently in place in Iceland.

Ireland

Export controls

70. Ireland is a member of the Wassenaar Arrangement and the European Union and has implemented the EU Dual-Use Regulations.

Domestic controls and import regulations

71. There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Ireland.

Italy

Export controls

72. Italy is a member of the Wassenaar Arrangement and the European Union and has implemented the EU Dual-Use Regulations.

Domestic controls and import regulations

73. Prior to Law No. 59 of 15 March 1997 and to Decree of the President of the Republic No. 513 of 10 November 1997, Italy did not enforce any special domestic controls on cryptography, except the legal provisions of Articles 12 and 24 of Law No. 801 of 24 October 1977 on the specific themes of the protection of state secrets and diffusion of information, the diffusion of which is prohibited. Some other provisions are contained in the various laws on the control, export, import and transit of armaments and on the export and transit of materials of particular strategic importance [31].

74. Cryptography technologies in the Public Administration were only briefly mentioned in some of the deliberations of the Authority for Information Technology in the Public Administration (AIPA)[32], such as the Deliberation of 28 July 1994 under Article 1, No. 9. This Deliberation states that issues related to the use of encryption, of the protection and conservation of the relevant keys and the use of electronic signature systems will be regulated by subsequent legal provisions.[33] It also sets out that every file stored in an optical disc should contain information about cryptography according to rules which would be subsequently defined.

75. As concerns security issues with respect to the specific techniques for the use of optical storage devices, the explanatory notes (paragraph 3,I) of the above Deliberation state that "for confidential reasons cryptography must be allowed for storage of information on disk, but in such a case the cryptography algorithm must be normalised and also the formation and conservation procedures of the single keywords and the relevant responsibilities must be governed by specific regulations."

76. Cryptography is also mentioned in the feasibility study on the Public Administration's Unitary Network (PAUN)[34]. This wide-ranging study also states that the security of the PAUN will be made through domains. In order to guarantee the origin, contents, privacy and non-refusal of the messages exchanged by the domains there will be applications software based on the use of symmetric and/or public key cryptography. The management of the cryptography keys will be handled through a body which will be set up by and placed under the direct control of the Presidency of the Council of Ministers, composed of three distinct sections dealing with: (1) creation and distribution of the keys, located at the service centre; (2) management of notarial documents, located at the operation centre; and (3) certification of the keys, located at the Authority for Information Technology.

77. The general report also contains specific studies which make reference to the use of electronic signatures (as a guarantee of the integrity of the data and of the security of the message's origin) and to public key cryptography (ensuring the privacy of the data).

78. At the end of 1995 AIPA examined draft provisions on electronic legal and other documents in conformity with Article 3 of the Decree Law No. 39 of 3 February 1993. Since this text was the result of a study group, AIPA published it on the Internet to obtain public comments. This study also examines issues relating to the management and storage of cryptography keys.

79. In November 1996 AIPA presented the document, "Network of the automated information processing systems' Cabinets and Responsible Authorities", which also deals with the issues of network security and the use of cryptography.

80. Law No. 52 of 15 March 1997 also acknowledges the legal validity of computer documents. It delegates the government to legislate on the attribution of functions and tasks to the regions and local authorities in view of the reformation of the Public Administration and a simplification of administrative procedures. Specifically, it provides that "acts, data and documents made by the Public Administration and private parties through the use of computer and information-telecommunications systems, are legally valid and produce effects for all legal purposes."[35]

81. Pursuant to the above provision, the Decree of the President of the Republic No. 513 of 10 November 1997 was issued outlining Rules on the criteria for and ways of formulating, storing and transmitting document through computer and information-telecommunications systems. This Decree provides specific provisions for computer documents and their probative validity, and for digital signature and validation systems with reference to the use of cryptography (asymmetric key encryption systems), both in the private and in the public sectors.

82. Article 15 of Law No. 675 of 31 December 1996 on the Protection of individuals and other subjects with reference to personal data processing, deals with the problem of the security of data. It provides that the minimum standards of security to be adopted in a preventive way (including cryptography) will be defined in a set of rules to be issued in a Decree of the President of the Republic, upon proposal of the Minister of Justice, after consulting the AIPA and the Authority for the Protection of Data.

Japan

Export controls

83. Japan is a member of the Wassenaar Arrangement and has implemented export restrictions on cryptography products according to the Wassenaar dual-use list. An export licence is required for all cryptographic products and decisions on applications are made on an individual basis by the licensing authority, the Ministry of International Trade and Industry (MITI).

Domestic controls and import regulations

84. There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Japan.

General Policy Developments

85. The development of cryptography policy in Japan is generally focused in two Japanese Ministries: the Ministry of Posts and Telecommunications (MPT)[36] and the Ministry for International Trade and Industry (MITI)[37]. Recently, the National Police Agency (NPA) and the Ministry of Justice have also taken a role in this area.

86. MITI published a paper in May 1997 “Towards the Age of the Digital Economy - For Rapid Progress in the Japanese Economy and World Economic Growth in the 21st Century”[38] presenting MITI’s approach to electronic commerce issues generally. Cryptography is seen as an important tool for establishing information security in electronic commerce. Development of cryptography and investigative projects should be promoted, and network users should be provided with much more information about the various initiatives underway.

87. Since cryptography which is important to prevent crimes related to computer networks can also be misused to further various crimes, the NPA is considering the policy to promote cryptography and to prevent misuse of cryptography. In relation to this consideration, the NPA considered the cryptography policy in co-operation with an extra-departmental body, and the extra-departmental body published a paper in February 1998.

88. The policy report “Vision 21 for Info-Communications”, which was submitted by the Telecommunications Council to MPT in June 1997, pointed out that it is indispensable to establish security measures, such as encryption, in order to create an environment for electronic commerce and electronic settlement over networks, and development of cryptography technologies as well as establishment of cryptography policy needs to be promoted along with international co-operation.

Korea

Export controls

89. Korea is a member of the Wassenaar Arrangement and has implemented controls on cryptographic hardware and software accordingly. The licensing authority is the Ministry of Commerce, Industry and Energy.

Domestic controls and import regulations

90. There are no import restrictions on cryptography technologies. There are no domestic regulations specifically governing the use of cryptography, although there may some related restrictions under general telecommunications law.

General policy developments

91. The Ministry of Information and Communication of Korea is currently studying these issues.

Luxembourg

Export controls

92. Luxembourg is a member of the Wassenaar Arrangement and the European Union and has implemented controls on cryptographic hardware and software according to the EU Dual-Use Regulations.

Domestic controls and import regulations

93. There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Luxembourg.

Mexico

Export/ import controls restrictions and domestic controls

94. There are no domestic controls on the use of cryptography, nor are there export or import restrictions on cryptography technologies, currently in place in Mexico.

Netherlands

Export controls

95. Regulations apply to the export of cryptographic software and hardware. This is in compliance with national regulations, namely the 1962 Law on Import and Export (Dutch statute-book 1962, 295) and its ensuing ministerial decision on export of strategic goods (Dutch statute-book 1963, 128). Export is a national prerogative but The Netherlands has committed itself to international agreements. These include the Wassenaar Arrangement and the Council of the European Union's decision (19 December 1994) based on the Treaty on European Union concerning the control of exports on dual-use goods, and the Council Regulation (EC) which established a Community regime for the control of exports of dual-use goods.

96. The export of all cryptographic software and hardware (except for specific banking applications) requires an export license. The export, however, of public domain and mass-market software and technology does not require a license. The administering authority is the Central Agency of Import and Export, under the authority of the Ministry of Economic Affairs. Once an application has been received, an evaluation and decision process (whether or not to issue an export license) is set in process. In practice, the products are evaluated on a case-by-case basis. The criteria for granting this license is unclear.

Domestic controls and import regulations

97. There is no import restriction in place on cryptography technologies in the Netherlands. Moreover, there is no law or official policy on cryptography in the Netherlands.

98. Regarding domestic regulations in the present Telecommunications Act, the use of cryptography on closed-terrestrial radio systems (not public mobile systems) is restricted and requires a license from the telecommunication regulator. In the proposed Telecommunications Act (approved in the first term of Parliament on 7 April 1998) this restriction is not mentioned.

99. As a result of the European Council Resolution on international requirements for the Lawful Interception of Telecommunications, the Dutch Telecommunications Act includes an obligation on network operators and service providers. They must provide the signal 'en clair' when a legal warrant for interception is given.

100. In the Dutch Computer Crime Act, in the case of stored data in encrypted form and a lawful authorisation, any applicable entity (excluding the suspect) is obligated to cooperate with the law enforcement authorities. This is to obtain lawful access to 'en clair' data.

New Zealand

Export controls

101. New Zealand is a member of the Wassenaar Arrangement and implemented Wassenaar controls accordingly. However, New Zealand controls do not exclude cryptography "in the public domain" or "generally available to the public". The export of cryptographic products is regulated through the Customs Act 1966 and the Customs Prohibition Order 1996. A permit is required from the International Security and Arms Control Division of the Ministry of Foreign Affairs and Trade. All applications are considered on a case-by-case basis.

Domestic controls and import regulations

102. There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in New Zealand. While no amendments to New Zealand's domestic laws are currently being contemplated, they remain under continuous review to ensure that they take adequate account of technological and other developments.

Norway

Export controls

103. Norway is a member of the Wassenaar Arrangement and the European Union, and has implemented Wassenaar controls accordingly. Export controls are administered by the Ministry of Foreign Affairs.

Domestic controls and import regulations

104. There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Norway.

General Policy Developments

105. The Norwegian IT Security Council presented late in 1997 a report to the Ministry of Trade and Industry on the need for a cryptography policy in Norway. The report recommended that cryptography policy should be amended or established in the following prioritised areas: Public Administration, National Security, Justice Sector, Health Care, Private interaction with Public Administration, Privacy and Trusted Third Party Services.

Poland

Export controls

106. Poland is a member of the Wassenaar Arrangement and intends to become a Member of the European Union. A license is required for exporting cryptographic software or hardware, in accordance with the EU Dual-Use Goods Regulation.

Domestic controls and import regulations

107. There are no domestic controls on the use of cryptography currently in place in Poland.

108. The import of cryptography is regulated by a 1993 law which provides that a general authorisation or import certificate is required to buy cryptographic products abroad. The end-user must detail the kind of information to be encrypted and where the cryptography is to be installed.

Portugal

Export controls

109. Portugal is a member of the Wassenaar Arrangement and the European Union and has implemented controls according to the EU Dual-Use Regulations. The licensing authority is the Directorate General for Commerce.

Domestic controls and import regulations

110. There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Portugal.

Spain

Export controls

111. Spain is a member of the Wassenaar Arrangement and the European Union, and controls export of cryptographic products according to the EU Dual-Use Regulations. The Ministry with responsibility in this area is the Ministry of Economy and Finance.

Domestic controls and import regulations

112. There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Spain.

Sweden

Export controls

113. Sweden is a member of the Wassenaar Arrangement and the European Union, and controls export of cryptographic products accordingly. The licensing authority is the Inspectorate for Strategic Products (ISP).

Domestic controls and import regulations

114. There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Sweden.

General Policy Developments

115. The Swedish Cabinet Office is currently studying issues related to cryptography policy, and guidelines are being prepared. The October 1997 report by the Swedish Cabinet Office "Cryptography Policy: Possible Courses of Action for Sweden"[39] includes the following principles:

- everybody has the right to use cryptography in order to secure stored data and communication;
- prerequisites for Swedish users' voluntary deposit of their keys in Sweden should be created in response to the requirements of key deposit;
- in order to enable law enforcement agencies to fight terrorism and drug dealers, rules and regulations for lawful access to plaintext and keys must be installed;
- import of cryptography will continue to be free;
- that the export controls will remain;
- necessary regulation of Swedish cryptography issues should be introduced in co-operation with other countries and with due account to international development.

Switzerland

Export controls

116. Switzerland is a member of the Wassenaar Arrangement and has implemented controls accordingly. The licensing authority is the Federal Office of Foreign Economic Affairs. General licenses may be granted for export to designated destinations.

Domestic controls and import regulations

117. There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Switzerland.

Turkey

Export controls

118. Turkey is a member of the Wassenaar Arrangement and has implemented controls accordingly.

Domestic controls and import regulations

119. There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in Turkey.

United Kingdom

Export controls

120. The United Kingdom is a member of the Wassenaar Arrangement and the European Union. Export of cryptography technologies is controlled in accordance with the EU Dual-Use Regulation, implemented through the Export of Goods (Control) Order 1994 as amended by the Dual-Use and Related Goods (Export Control) Regulations 1996. The controls do not apply to "generally available" software or software and technology in the public domain. Exporters must apply for a two year export license for any products using cryptography. The responsible authority is the Export Control Organisation of the Department of Trade and Industry (DTI)[40]. In some circumstances the DTI will issue a more general Open Individual Export License, good for three years, which may contain specific conditions. All exporters must keep detailed records on the exports authorised by a license.

121. Applications for "Open Individual Export Licences" (OIELs) from exporters for encryption products which contain the 56-bit DES algorithm (or algorithms of an equivalent strength) are considered. Such OIELs will, depending on the individual circumstances, be limited in terms of the applicable country destinations, the type of end user, the specified use of the products and, inter-alia on any international discussions taking place on exports of cryptographic products. In addition, in line with the Government policy regarding Trusted Third Parties, it may be appropriate, in certain circumstances, for the exporter to demonstrate that their products have (or will have) the capability to inter-work with licensed TTPs.

122. From 28 January 1998 the DTI will issue a new kind of "Open General Export Licence". The new licences will permit, without further authority but subject to certain conditions, the export of goods which are not capable of on-line voice encryption or decryption which are designed to be used in conjunction with digital computers for personal use when accompanying their user.

Domestic controls and import regulations

123. There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in the United Kingdom.

General Policy Developments

124. A June 1996 DTI policy paper on provision of encryption services on public telecommunications networks states that export controls on encryption products (hardware or software) including digital encryption algorithms will remain in place, but that the Government, along with their EU partners, would try to simplify export controls for encryption products used by licensed TTP's. The government would introduce legislation for licensing and regulating Trusted Third Parties (TTPs), with aims to preserve law-enforcement access to encrypted data. Prior to legislation, a consultation process with all interested parties would be held.

125. The consultation process was launched with a "Consultation Paper on Licensing of Trusted Third Parties for the Provision of Encryption Services"[41] issued by the Department of Trade and Industry (DTI) on 19 March 1997. The Consultation paper covers aspects of cryptography related to the licensing of TTPs, their use for confidentiality purposes, lawful access for confidentiality, legal recognition of digital signatures and international issues. The proposals are directed solely towards the provision of encryption services to subscribers in the UK and not the use of encryption. The proposals would not apply to intra-company TTPs, nor encryption services as an integral part of another service(such as pay-TV). Although the licensing for all organisations providing cryptography services to UK clients would be mandatory under the proposal, users would remain at liberty to choose whether to make use of TTPs, or to make other arrangements for their encryption requirements. However it adds that the "Government recognises that further legislation may be required in the future to enable the appropriate authorities to obtain private encryption keys other than those held by licensed TTPs." The Department of Trade and Industry has been nominated as the initial licensing authority.

126. Currently Britain holds the presidency for the European Union. During a conference of EU Justice and Home Affairs Ministers at the end of January 1998, the Home Secretary stated that the UK would be using this opportunity to raise awareness of the task facing law enforcement agencies on the Internet.

127. During 1997 there was a change in government in the UK. The new Labour Government is currently studying this issue.

United States

Export controls

128. The US is a member of the Wassenaar Arrangement. Cryptography exports in the US have traditionally been controlled by the International Traffic in Arms Regulation (ITAR) and the Arms Export Control Act (AECA), administered by the US State Department. However, at the end of 1996, the regulation of non-military cryptography exports was transferred to the Department of Commerce, Bureau of Administration (BXA); at the same time cryptography technologies were moved from the US Munitions List to the Commerce Control List (CCL).

129. US export controls are implemented by the Export Administration Regulations (EAR)[42]. In 1996, the US Administration called for a relaxation of restrictions for key recovery products.[43] Interim rules implementing this policy outline export licensing policies for different categories of encryption items, and criteria for key escrow or key recovery products, agents, and development plans.[44] The new export rules distinguish five categories of "encryption items" (EI)[45]:

1. *Certain mass-market encryption software may be released from EI controls after a one-time review.*

2. *Key escrow, key recovery and recoverable encryption software (meaning that government can access keys or plaintext with a proper legal authority) will be eligible for "License Exception KMI (key management infrastructure)" to non-embargoed countries.*

3. *After a one-time review, (up to) 56-bit EIs may be granted a renewable six-month export license, provided the exporting business commits itself to develop, produce or market encryption items and services with recoverable features within two years from January 1, 1997. This relaxation will last until 31 December 1998, when this particular exemption will expire. [The interim rule allows continued service and support of non-recoverable products exported under this exemption, as well as some additional sales of those products to existing customers].*

4. *All other encryption items may be eligible for encryption licensing arrangements which may be for unlimited quantities to most destinations, but the applicant must specify the sales territory and classes of end-users; applications for the export and re-export of items not authorised under a licensing arrangement will be considered on a case-by-case basis.*

5. *"Encryption technology" will be considered for licensing for export on a case-by-case basis.*

130. The BXA is now further reviewing the US export controls. On 8 October 1997, it released a statement "seeking comments on how existing foreign policy-based export controls have affected exporters and the general public.... BXA is particularly interested in the experience of individual exporters in complying with the proliferation controls, with emphasis on economic impact and specific instances of business lost to foreign competitors".

131. Temporary export of products for personal use is exempt from the need of a license, provided the exporter take normal precautions to ensure the security of the product. In addition the product must not be intended for copying, demonstration, marketing, sale, re-export, or transfer of ownership or control. In transit, the product must remain with the exporter's accompanying baggage. The exporter must keep records of each export for five years. Export to embargoed countries is prohibited.[46] Making cryptography available for electronic transfer to locations outside the United States is an "export" unless appropriate precautions are taken to prevent such a transfer.

Domestic controls and import regulations

132. There are no domestic controls on the use of cryptography, or import restrictions on cryptography technologies, currently in place in the United States.

General Policy Developments

133. The US Administration's "Framework for Global Electronic Commerce" of July 1997[47] stated that "governments should encourage self-regulation....and support the efforts of the private sector organisations to develop mechanisms to facilitate the successful operation of the Internet". The government's Framework for Global Electronic Commerce restates the (voluntary) key recovery approach.

134. Administration officials have stated that the United States does not advocate any single product, technology, or even technical approach, but remains flexible - provided that the resulting solutions and arrangements preserve the United States' ability to protect public safety and national security [48].

135. On November 15, 1996, the US Government appointed Ambassador David Aaron as "special envoy for cryptography". He works to promote international co-operation and co-ordinate US contacts with foreign governments on encryption matters.

136. A 1996 law[49] includes an amendment requiring the US Sentencing Commission to report annually on the use of computer encryption to conceal criminal activity.

137. The Office of Management and Budget (OMB) published a white paper on "Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure" in May 1996. The paper proposes the establishment of a key management infrastructure (KMI) that incorporates key escrow. Participation in the KMI would be voluntary, and choice of encryption algorithms would be free. A "Policy Approving Authority" would certify certification authorities (CAs); it would also be responsible for setting CA performance criteria to meet law enforcement needs. Users would store keys with an "Escrow Authority" (either the CA or an independent entity) in order to get a public-key certificate. Self-escrow would be considered an acceptable option under specific circumstances, including independence from the rest of the organisation and handing over keys to law enforcement. The white paper states that such a key management infrastructure, voluntary and supported by private sector key management organisations, is the prospect of the near future. It would permit users and manufacturers free choice of encryption algorithm, facilitate international interoperability, preserve law enforcement access, and, most importantly, provide strong system security and integrity."

138. A technical advisory committee met for the first time in December 1996 to develop a Federal Information Processing Standard (FIPS) for key recovery. The next meeting is scheduled for 25 February 1998.[50]

139. The June 1996 National Research Council study "Cryptography's role in Securing the Information Society", which was prepared at the request of Congress, states that the Government should promote widespread commercial use of cryptography[51]. It recommended that export controls be progressively relaxed, but not eliminated, and that adoption of escrowed encryption (or of any other standard) should be voluntary. Products providing confidentiality at a level that meets most general commercial requirements should be easily exportable.

140. There are several pieces of proposed legislation currently at various stages of the law-making process, some seeking to impose domestic restrictions on the use of encryption technologies, others requiring mandatory or voluntary government key-recovery or key escrow provisions, and others seeking to permit free use and export of cryptography and cryptographic products:

- Representative Goodlatte's Bill, "Security and Freedom through Encryption (SAFE) Act of 1996" (H.R. 3011), reintroduced on 12 February 1997 (H.R. 695);

- Senator Leahy's Bill, "the Encrypted Communications Privacy Act", proposed on 5 March 1996 (S. 1587), reintroduced 27 February 1997 (S. 376.);

- Senator Burns' Bill, "Promotion of Commerce Online in the Digital Era (Pro-CODE) Act of 1996", proposed in May 1996 (S.1726), reintroduced 27 February 1997 (S. 377); and

- The McCain-Kerrey Bill, "Secure Public Networks Act", introduced 17 June 1997, (S.909).

141. There have been three separate court challenges to the US export regulations, claiming that the regulations violate the First Amendment of the US Constitution which protects free speech. [52]

Examples of cases where law enforcers have encountered encryption

142. US law enforcement authorities have already confronted encryption in high-profile espionage, terrorist and criminal cases. For example:

- An international terrorist was plotting to blow up 11 US-owned commercial airliners in the Far East. His laptop computer which was seized during his arrest in Manila, contained encrypted files concerning this terrorist plot.

- A subject in a child pornography case used encryption in transmitting obscene and pornographic images of children over the Internet.

- A major international drug trafficking subject used a telephone encryption device to frustrate court-approved electronic surveillance.

143. Furthermore, requests for cryptographic support pertaining to electronic surveillance interceptions from Federal Bureau of Investigation (FBI) Field Offices and other law enforcement agencies have steadily risen over the past several years. There has been an increase in the number of instances where the FBI and Drug Enforcement Administration's court-authorised electronic efforts were frustrated by the use of encryption that did not allow for law enforcement access.

Country name	European Union member	Wassenaar member	Export controls	Import controls	Domestic controls
Australia	No	*	*	No	No
Austria	*	*	*	No	* (minor)
Belgium	*	*	*	No	* (telecom)
Canada	No	*	*	No	No
Czech Rep.	No	*	*	*	No
Denmark	*	*	*	No	No
Finland	*	*	*	No	No
France	*	*	*	*	*
Germany	*	*	*	No	No
Greece	*	*	*	No	No
Hungary	No	*	*	*	No
Iceland	No	No	No	No	No
Ireland	*	*	*	No	No
Italy	*	*	*	No	*
Japan	No	*	*	No	No
Korea	No	*	*	No	* (telecom)
Luxembourg	*	*	*	No	No
Mexico	No	No	No	No	No
Netherlands	*	*	*	No	No
New Zealand	No	*	*	No	No
Norway	No	*	*	No	No
Poland	No	*	*	*	No
Portugal	*	*	*	No	No
Spain	*	*	*	No	No
Sweden	*	*	*	No	No
Switzerland	No	*	*	No	No
Turkey	No	*	*	No	No
U.K.	*	*	*	No	No
United States	No	*	*	No	No

*Yes

NOTES

1. The 17 COCOM members were Australia, Belgium, Canada, Denmark, France, Germany, Greece, Italy, Japan, Luxembourg, The Netherlands, Norway, Portugal, Spain, Turkey, United Kingdom, and the United States. Co-operating members included Austria, Finland, Hungary, Ireland, New Zealand, Poland, Singapore, Slovakia, South Korea, Sweden, Switzerland, and Taiwan.

2 Prior to it's final adoption, the agreement was provisionally called the "New Forum".

3. Wassenaar Arrangement Members are: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, Romania, the Russian Federation, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom and the United States.

4. Under-cuts (for explanation of "under-cutting" see paragraph 8) should be notified preferably within 30 days, but not later than within 60 days: Wassenaar Arrangement, Intitial Elements, Section II, paragraph 4.

5. Denials of sensitive/very sensitive goods should be notified preferably within 30 days but not later than 60 days: Wassenaar Arrangement, Initial Elements, Section V, paragraph 3.

6 See Appendix 5 of the "Initial Elements", Wassenaar Arrangement.

7. Listed in Annex 1 to the Dual-Use List.

8. Listed in Annex 2 to the Dual-Use List.

9. Regulation (EC) 3381/94 (OLJ 367/1, 31.12.94) and Decision 94/942/CFSP (OLJ 367/8, 31.12.94) of the Council of the European Union of 19 December 1994 set forth controls on the export of dual-use goods and established the list of dual-use goods which fall under the Regulation.

10. See the notes to Annex 1 of Decision 96/613/CFSP (a completely new version of the Regulation is currently under consideration).

11. European Council Resolution 96/C329/01.

12. COM(97)503, see *http://www.ispo.cec.be/eif/policy/*.

13. See Council Directive 83/189/EEC (OJL 109, 26.4.83).

14. (97/C 314/07) (Text with EEA relevance) COM(97) 356 final - 97/0198(COD).

15. Recommendation [R(95)13] of the Council of Europe, see *http://www.privacy.org/pi/intl_orgs/coe/info_tech_1995.htm.*

16. See the Bonn Declaration at *http://www.2.echo.lu/bonn/final.html.*

17. Customs (Prohibited Exports) Regulations Reg 13E, see *http://www.austlii.edu.au/au/legis/cth/consol_reg/cer439/s13e.html*

18. Cryptography is addressed under Part 3 Category 5 "Telecommunications & Information Security" of the Defence and Strategic Goods List. See the Australian Department of Defence at *http://iic.spirit.net.au/imat/publications/excontrl/excohome.htm.*

19. For more practical information on export of cryptography technologies refer to the Guide "Australian Controls on the Export of Defence and Strategic Goods".

20. Laws of 21 March 1991 and 21 December 1994.

21. For information about the cryptographic hardware and software controlled, see the relevant sections of Canada's Export Control List at *http://axion.physics.ubc.ca/ECL.html*, in particular the following sections: 1000 "General Technology Note" providing definitions and including the "General Software Note" which defines key terms*;* 1151 "Equipment Assemblies and Components" (controls cryptographic hardware); 1154 "Software"; and 1155 "Technology" (encryption technology includes any information necessary for the development, production or use of controlled cryptographic equipment or software, covering "technical data" and "technical assistance").

22. See *http://canada.justice.gc.ca/Commerce/toc_en.htm.*

23. See *http://www.cse.dnd.ca/cse/english/index.html.*

24. Act No. 21/1997, Decree Number 43/1997.

25. See Act No. 21/1997.

26. Pursuant to Decree No. 44/1997 and § 16 of Act No. 21/1997.

27. See *http://www.fsk.dk:80/fsk/publ/1997/crypt/index/htm*

28. Central service for the security of information systems.

29. No. 96-659 of 26 July 1996. For a transcript of the law (in French) see the French government site: *http://www.telecom.gouv.fr/francais/activ/telecom/nloi.htm.* For further information on the law from the French government *http://www.telecom.gouv.fr/english/activ/telecom/.*

30. See *http://www.bmwi.de.*

31. Law no.185 of 8 July 1990, Law no. 222 of 27 February 1992 and the relevant ministerial decrees of 28 October 1993, 18 November 1993, 5 May 1994 and 1 September 1995.

32. The AIPA was created by Legislative Decree No. 39 of 12 February 1993.

33. Set out in Article 9, inter alia.

34. Provided for in the 5 September 1995 Directive of the President of the Council of Ministers, published in the Official Gazette [G.U.] no. 272 of 21 November 1995

35. Article 15, paragraph 2.

36. See *http://www.mpt.go.jp.*

37. See *http://www.miti.go.jp.*

38. See *http://www.miti.go.jp/intro-e/a228101e.html.*

39. In Swedish, with English summary.

40. See the DTI web site at *http://www.dti.gov.uk.*

41. See *http://www.dtiinfo1.dti.gov.uk/pub.*

42 See *http://jya.com/eartoc/htm.*

43. This policy was announced in a statement by the Vice President on 1 October 1996 and further elaborated by an Executive Order dated 15 November 1996.

44. The interim rules are set out in the Commerce Department draft Export Administration Regulations of December 30, 1996.

45. EAR Sec. 742.15.

46. In February 1996, the ITAR rules were amended as regards personal use of cryptography. Thereafter, under the new EAR, the ITAR personal use exemption was replaced by EAR 15 CFR Part 740 License Exceptions*:* 740.9 - TMP (temporary imports, exports and reexports) and 740.14 - BAG (baggage) regarding personal effects that individuals may take out of the US. The Department of Commerce announced in February 1997 it would revise the new regulations to, among others, clarify the personal use exemption for laptop computers. See *http://jya.com/740.htm.*

47. See *http://www.whitehouse.gov.*

48. Testimony of Robert S. Litt, Principal Associate Deputy Attorney General, before the Subcommittee on the Constitution, Federalism, and Property Rights Committee on the Judiciary, United States, 17 March 1998.

49. 2 October 1996 law (HR 3723).

50 See *http://crsc.nist.gov/tacdfipsfkmi/.*

51. See *http://www.jya.com/nrc04.txt.*

52. See Karn at *http://people.qualcomm.com/karn,* Bernstein at *www.eff.org,* and Junger at *http://jya.pdj.com.*