

**Government communication  
1998/99:116**

**On cryptography**

**Skr. 1998/99:116**

---

The Government submits this communication to the Riksdag.

Stockholm, 6 May 1999

*Göran Persson*

*Leif Pagrotsky*  
(Ministry for Foreign Affairs)

**The main contents of this communication**

In this communication, the Government presents its views on certain aspects of the use of cryptography in the transmission and storing of information in electronic form, and on the export of cryptographic products.

The principal content of the Government's position is as follows.

At present there is no reason to limit the use of cryptographic technology in Sweden. All shall have the right to choose such technology themselves.

Imports of cryptographic technology shall remain free of restrictions.

There remain reasons of security policy for preventing the dissemination of cryptographic technology to unsuitable parties in certain other countries.

If developments should warrant more stringent regulations, the government will consider appropriate measures for creating means of legal access to the plaintext of encrypted information for law enforcement and supervisory authorities.

Sweden's policy should be characterised by flexibility and open-mindedness so as to be able to respond to an increased demand for secure cryptographic technology, changes in other countries' policies and the continued development of technology in the field.

## Contents

1	The subject and its treatment .....	3
2	Points of departure.....	3
2.1	Background.....	3
2.2	Use of cryptographic technology.....	5
2.3	The fight against crime and associated issues .....	9
2.4	Protection of the functioning of society.....	10
2.5	Export controls.....	11
3	Some international issues .....	12
3.1	EU co-operation.....	12
3.2	The Wassenaar Arrangement and new EU regulations .....	15
3.3	The OECD .....	16
3.4	The Council of Europe.....	17
3.5	Developments in other countries .....	17
4	The Government's deliberations and conclusions .....	18
	Appendix 1: Terminology.....	24

# **1 The subject and its treatment**

At the beginning of 1996, a Swedish Government Office Reference Group was set up to examine the use of cryptographic technology and to develop a foundation for Swedish policy in this area.

The group was also given the task of coordinating Swedish participation in international deliberations and negotiating international guidelines for encrypted communication.

In October 1997, the Reference Group presented its report “Kryptopolitik – möjliga svenska handlingslinjer” (“Cryptography Policy: Possible Courses of Action for Sweden”). This report has been published and interested parties have delivered their opinions on it. These statements are available at the Swedish Government Office (Doss. HP 24). Subsequently, the Reference Group has continued its work towards developing a foundation for a Swedish position on the use of cryptographic technology. The results of this work have formed the basis of the communication that the Government now submits to the Riksdag.

Work continues on monitoring developments in the field and deciding on measures that may be warranted in response to these developments. The Government intends to allow this process to take a partially modified form in the future, with a view to deepening the dialogue with representatives of different users and other concerned parties.

## **2 Points of departure**

### **2.1 Background**

The rapid development of technology is encouraging a dynamic evolution in national and global electronic commerce and electronic communication. This in turn leads to a vast potential for growth and effectiveness. However, this potential can only be realised to the full if public authorities, businesses and individuals can be confident that the information they exchange and store is not accessible to unauthorised parties.

The use of cryptography meets demands for security in the transmission of messages and for the protection of stored information. The technology can also be used to guarantee the authenticity of documents and signatures. Appendix 1 provides explanations of the technical terms that are employed in this communication.

Technical developments have made it possible for both public authorities and companies on the one hand, and private individuals on the other hand, to use cryptographic technology in dealing with sensitive information. At the same time, in both the national and international sphere, there is a need to prevent the improper use of such technology.

Though its areas of application have expanded in recent years, cryptographic technology was formerly used primarily within the National Defence and the Foreign Service. Since the technology still involves important security policy issues, cryptographic technology is classified as a strategic product subject to export controls.

The points that should be taken into account in defining a cryptography policy are:

- the trustworthiness of documents in electronic form that are intended to replace documents in written form,
- the trustworthiness of electronic signatures and the protection of confidentiality for electronic communication and for stored information,
- the fight against crime, and the exercise of inspection or supervision (for example, by public prosecutors, police authorities, and customs and tax authorities),
- export controls to prevent dissemination to unsuitable parties in certain countries.

Current Swedish regulations on the use of cryptographic technology can be summed up as follows:

- this technology may be freely imported, produced and used;
- applications for export licenses for cryptographic products are subject to review by the Inspectorate for Strategic Products (ISP);
- law enforcement authorities are permitted to use coercive means – e.g. the searching of premises – to obtain access to users' cryptographic keys. However, a user of encryption who is suspected of a crime cannot be compelled to participate actively in the investigation of that crime, e.g. by surrendering his or her private confidentiality key.

In a communication to the Riksdag on electronic commerce (skr. 1997/98:190), the Government has discussed various issues that are affected by the rapid development of electronic commerce. The Government has there stated that developments should be driven by actors in the market and that regulations ought to be resorted to only when industry standards and agreements prove inadequate. The communication emphasises that with respect both to cryptography and to digital signatures, the Government authorities have an overall interest in the creation of confidence in communications systems.

In the Government bill on Public Administration in the Citizens' Service (prop. 1997/98:135), it is stated that public authorities should use secure means of transmitting documents and messages over public communications networks. The Government announces here that a body of regulations will be elaborated on secure communication in public administration.

In the bill "Förändrad omvärld – omdanat försvar" ("A Changing World – A Reformed Defence") (prop. 1998/99:74), the Government states that it intends to examine the possibility of establishing a special unit for neutralising attacks on information systems, and whether there is reason to expand the sphere of responsibility of the signals protection service (protection of communications), as proposed by the Swedish Government Office working group on information warfare. The working group's proposal would entail extending the sphere of responsibility of the National Defence to include also civil information systems that are important to the overall

defence. In order to provide a basis for any decision on the introduction of an IT supervisory function for the public administration, the Government will commission the National Defence to carry out a pilot project within the defence sector during the year 2000.

The ministerial memorandum “Digitala signaturer – en teknisk och juridisk översikt” (“Digital Signatures: A Technical and Legal Overview”) (Ds 1998:14) contains material on which Swedish positions within the EU regarding digital and electronic signatures have been based. Throughout the remainder of this document, the concept “electronic signatures” will be used, since this is the term the EU will use in future regulations.

Cryptography is used in decoding equipment for encoded transmissions of television and radio programmes. This use is regulated in the law (1993:1367) on the prohibition of certain forms of decoding equipment.

## **2.2 Use of cryptographic technology**

### *Electronic information services in society*

The Government has previously expressed the view, e.g. in its communication on electronic commerce (1997/98:190), that information technology should be used in order to promote growth and employment and to improve the quality of services. This will enhance Sweden’s competitiveness and add to the welfare of its citizens. For businesses, information technology means increased efficiency and improved opportunities to meet customers’ needs. It brings quite new opportunities and conditions for economic activity in our society, and for the organisation of society, in that geographical distances do not need to be regarded as serious obstacles to establishing and running business and public operations and providing people with favourable living conditions. The Government is of the opinion that it is of great importance to grasp these opportunities.

The technological developments enable electronic messages and documents to contain text, images, sound and other data. Telephony is merging with computer communications. Old boundaries between networks and systems are being wiped out. The Internet is the most obvious example of this, and is also an illustration of the fact that the boundaries between the mass media and interactive data processing are in the process of disappearing. New applications are developing, in which, for example, the protection of copyright intensifies the demands for secure systems and the use of cryptography.

Electronic services are generating new ways for cooperation between organisations within Sweden or abroad, and are offering enhanced opportunities for distance working.

Swedish IT companies are at the forefront of technical innovation. In the software business too, Swedish companies perform well against international competition.

The new information technology and communications services are used widely in Sweden. According to the Swedish Institute of Public Opinion Research, approximately 48 per cent of the Swedish population between the ages of 12 and 79, i.e. 3.4 million people, used the Internet in March 1999. New services too have become relatively widespread. For example, approximately 700,000 bank customers have their own connection to Internet banking services. According to forecasts, 1.3 million people will shop via the Internet in 1999.

Public administration makes extensive use of information technology in its contacts with citizens and companies. One important aim for administrative policy is to introduce comprehensive electronic self-service using Internet technology. Households and companies that acquire equipment in order to use the Internet should also be able to use it for electronic communication with local and national government authorities. This will lead to better services at lower costs, freeing up resources for use in cases where personal contact is still necessary.

### ***Information security and cryptography***

The use of public communications networks began to take off at the end of the 1980s, with the foremost example today being the Internet. One of the characteristic features of the Internet is that there is no obvious owner responsible for the security of the entire network. Instead the Internet consists of numerous networks with separate owners that are linked together.

These public networks now connect activities within different sectors of society and make possible new modes of working and new partnerships. Public authorities, companies and individuals will make increasing use of the public communications networks for more and more services. One problem, however, is that users need to take special measures to protect their communication via public networks. This creates a need for measures to safeguard information, and the foremost of these is cryptography. Cryptography also presents other possibilities; it can be used, for example, to make it more difficult or impossible for a sender to deny that a message has been sent. This feature is important if electronic functions are to be able to replace paper documents, written receipts or other documents that can be used in evidence.

Fundamental security requirements that can be fulfilled by cryptography, thereby inspiring confidence in communications networks are:

- to safeguard the identity of senders and receivers of documents or messages,
- to protect documents or messages from alteration,
- to protect documents or messages from unauthorised observation,
- to render it impossible for senders to repudiate documents or messages they have sent.

Cryptography can also be used to protect information stored in computers against unwanted observation and alteration, e.g. if a computer is stolen or if an unauthorised person effects entrance to an office and attempts to gain access to data that are stored on a computer's hard disk or on floppy disks.

Cryptography is also a means of protecting privacy, e.g. when transmitting sensitive personal information.

The necessary preconditions, in terms of infrastructure and access to cryptography, are now beginning to develop in Sweden. In order to safeguard identities and to protect documents against alteration electronic signatures are required; these can replace traditional signatures and provide a higher degree of security than a physical signature in electronic communication, in terms of both identification and content. Both electronic signatures and confidentiality are generated by means of cryptographic algorithms and cryptographic keys. The cryptographic algorithms should be characterised by strength and proven reliability, and should command international acceptance.

The link between the cryptographic keys and a specific person or organisation is attested in so-called certificates. Special bodies, i.e. Trust Service Providers, provide management services for certificates and cryptographic keys, principally in three main areas: identification, signatures and confidentiality.

However, if cryptographic keys, certificates and electronic signatures are to achieve widespread use, certain problems must be solved. One issue concerns the legal status electronic signatures should have vis-à-vis conventional signatures. Further, business law regulations may be needed with respect to the activities of the Trust Service Providers. Users must be able to obtain information about the regulations that apply.

When these bodies are established in Sweden and make their services available, it is expected that more and more parties will begin to use cryptography for the purpose of secure communication, but also in order to protect stored information.

The growing number of computers in the workplace and at home, together with the spread of the Internet, will lead to greater demand for cryptographic technology for electronic signatures and for confidentiality.

Swedish cryptography has long had a solid reputation. The first Swedish cryptographic machine was constructed as early as 1786. In the 1940s, the cryptographic machines designed by the Swede Boris Hagelin were the most widely sold in the world. Swedish cryptographic products stand up well against international competition at the present day too.

### ***Joint initiatives in the business world***

In Sweden various joint efforts are in progress in the business world to promote the development and use of cryptography and to stimulate companies to develop and market cryptographic products and services. A few examples follow.

*SEIS* (Secured Electronic Information in Society) is a Swedish non-profit association with some 50 members. The purpose of the association is to administer, develop and create acceptance, on behalf of its members, for the electronic solution for identification, signing and confidentiality that the association has designed. The association also has the task of monitoring and influencing developments within its sphere of

operations so as to enable all users to communicate electronically in a safe and secure manner.

The *Federation of Swedish Industries* has identified electronic business transactions as one of the most important global business issues in the coming years. The Federation is of the opinion that solving security issues is essential if electronic business is to be able to grow at the rate that many people expect. Access to strong cryptographic products is a decisive factor for this solution.

In order to stimulate and invigorate the development of electronic business in Sweden, the Federation of Swedish Industries, in association with the Federation of Private Enterprises, the Federation of Swedish County Councils, the Swedish Agency for Administrative Development, the Swedish Federation of Trade, the Swedish Bankers' Association, the Swedish IT-companies Organisation, the Swedish Trade Council and the Swedish Association of Local Authorities, has founded the association *Gemenskapen för elektroniska affärer* (the Swedish Alliance for Electronic Commerce), GEA. One of the GEA's most important tasks is to work for enhanced security in electronic commerce.

The *Swedish Bankers' Association* monitors the field of IT security via the Banks' Security Committee and its sub-group, the IT security group. Monitoring focuses on issues including changes in the picture of potential threats, technical developments and standardisation.

The *Swedish National Committee of the International Chamber of Commerce (ICC)* has an IT security group that is heavily involved in cryptography issues. The ICC works to promote uniform international regulations and among other things has formulated a "Global Action Plan" in collaboration with other industry and users' organisations in "The Alliance for Global Business".

The *Swedish Information Processing Society*, which has approximately 28,000 members in Sweden, all of whom are active in IT, has a special interest group, SIG Security, which pursues development work and takes initiatives for exchanges of experience in the fields of IT security and cryptography.

The *Swedish IT-companies Organisation*, a trade association within the Federation of Swedish Industries that consists of more than 600 IT companies active in hardware, software and the Internet, has a working group on secure electronic business transactions. The group consists of several security-oriented IT companies together with service and systems providers. These companies produce security products, offer services such as the issuing of certificates or provide systems solutions which include cryptography in some of their components or in which cryptography is used in internal communications within the company, e.g. between units located in different parts of the world.

The *Swedish Association of Software Industry* is a trade association within the Swedish Industry Association, with about 70 software companies as members. Several are developing cryptographic technology and systems. More still are incorporating security solutions of this kind in their products and software.

## 2.3 The fight against crime and associated issues

It is very much in the interests of society that users themselves protect their information processing and communications and thereby prevent or hinder criminal activity. From this point of view, the use of cryptography is a desirable measure. However, cryptographic technology can also be used in order to conceal crime. It is essential that law enforcement authorities have effective tools at their disposal to enable them to prevent and investigate crimes that are committed with the aid of this technology.

Law enforcement authorities need access to information that is stored by suspects and must be able to study information acquired by wiretapping. If this information is encrypted, the law enforcement authorities must be in a position to decrypt it.

The Code of Judicial Procedure specifies the fundamental regulations on search and seizure in connection with investigations of crimes. Search and seizure is permitted *inter alia* in order to search for objects that are subject to confiscation or in some other fashion to investigate circumstances that are of potential significance for the investigation of a crime. An object may be confiscated if there is reason to believe that it is of significance for the investigation of a crime. There are no special regulations regarding the IT environment, but the system of regulations is at present under review by the Ministry of Justice.

Regulations regarding secret wiretapping, etc., may be found in the Code of Judicial Procedure. Secret wiretapping means that all kinds of telecom messages, including computer communication, can be secretly monitored. Such monitoring is permitted by Code of Judicial Procedure only on certain conditions. These include the requirement that a person be suspected either of a crime that carries a minimum sentence of two years' imprisonment, or of a crime preliminary to a crime of this gravity. It is required, further, that the measure be of unusual importance for the investigation of the crime. A Court decision is required for wiretapping to be permitted. A telecom operator is bound in principle to provide the plaintext of a signal that has been encrypted by the operator him or herself.

Secret wiretapping is an important tool in investigating and revealing crimes. So far, suspects who have been subjected to secret wiretapping have not exploited the possibility of using encryption to any marked extent. secret wiretapping has therefore largely functioned as intended. If the exploitation of communications networks for criminal activities grows and access to effective cryptographic technology becomes easier, it can be foreseen that the law enforcement authorities will encounter serious obstacles if they lack the means to gain access to the plaintext of encrypted communications or stored information.

The Government's communication to the Riksdag in October 1998 regarding the use of secret wiretapping, secret tele-surveillance and surveillance by hidden cameras in connection with preliminary criminal case investigations in 1997 (skr. 1998/99:21) reveals that in 1997, in cases of preliminary investigations of serious narcotics crimes, Court permission was given for secret *wiretapping* of communications to or from telephones or other telecommunications facilities that were owned or used by 281 suspected persons. Between 1988 and 1996, the number of cases ranged from

210 to 333 per year. With regard to other serious crimes for which the Code of Judicial Procedure permits the use of secret wiretapping, wiretapping occurred in 58 cases during 1997. Between 1988 and 1996, the number of cases ranged from 13 to 91 per year. In 1997, the preliminary investigations involved were mainly concerned with murder or attempted murder or preparations for or plotting to commit murder; armed robbery or aiding and abetting, attempting or preparing to commit armed robbery; kidnapping; arson; grave procuring; and grave forgery.

Wiretapping proved important for the preliminary investigation of the suspect in 41.5 per cent of cases in 1997. Between 1988 and 1996, the number of cases in which the measure was significant for the preliminary investigation ranged from 44 to 56 per cent.

In 1997, permission was given for the use of secret tele-surveillance in 165 cases, 115 of which involved narcotics crimes. The surveillance proved significant for the preliminary investigation of the suspect in 36 per cent of cases.

The tax authorities and other public authorities also need access to stored information in order to carry out inspections and exercise supervision. If the information is encrypted, it must first be transformed into plaintext.

Private individuals are obliged to co-operate in tax investigations. However, it is obvious that a system of taxation can not function solely on the basis of information provided voluntarily by persons subject to taxation. The tax authorities must have various forms of coercive measures at their disposal in order to safeguard the functioning of the tax system. If persons subject to taxation fail to fulfil their duties, the tax authority is allowed to impose penalties. If there is reason to assume that the taxable party has committed a crime, however, he or she can not be compelled to co-operate in the investigation of any question connected with the act to which the suspicion of crime applies. Further, the tax authority can carry out an audit to examine business people's books, etc. In the case of an audit, the taxable party is to make the documents available and provide the information that is needed for the audit. If certain conditions are fulfilled, the tax authority can also resort to coercive means in order to perform an audit; among other things, computer stored data can be taken into possession.

In this connection it may be mentioned that according to the Book-keeping Act, book-keeping records may not be made illegible. It must always be possible to produce book-keeping records in legible form, and they may therefore not be presented in encrypted form.

## **2.4 Protection of the functioning of society**

In order to protect Sweden's security and independence and to provide a foundation for the government's assessment of general developments concerning foreign and security policy, our National Defence carries out signal intelligence for the purpose of detecting activities aimed against our country. Swedish signal intelligence is directed solely towards other countries and is therefore not in need of regulations on the national use of cryptography.

The ability of the signal intelligence service to give advance warning of various types of threats is dependent in part on the successful prevention by export controls of the dissemination of advanced cryptographic technology to undesirable users. An augmented international use of advanced cryptographic technology risks making it more difficult or impossible for the signal intelligence service to decrypt signals and display messages in plaintext.

If crypto systems that are used by the Total Defence (i.e. military defence and civilian activities to defend the country) or the Foreign Service are marred by inherent weaknesses and alien powers gain access to sensitive information, the potential consequences in a situation of war are devastating. If the directions given in preparation for negotiations by the Government become known to counterparties, this may affect the result of the negotiations. Information can leak over a long period since those who have managed to break into a system can keep it secret.

Crypto systems that are used within the Foreign Service and the Total Defence are inspected and approved by the TSA (the Communication Security Section) before being taken into operation. The TSA also carries out inspections to ensure that the systems are used correctly. The TSA is in a position to act in an advisory capacity to enterprises in Sweden outside the Total Defence, in both the public and the private sector.

The practical management of crypto systems that have been taken into operation is vital if they are to provide the intended protection. In the view of the Working Group on Information Warfare, the TSA can serve as a suitable basis for the IT supervisory unit for the public administration that was proposed in section 2.1.

Weak systems can lead to problems, even when they are used by public authorities that do not belong to the Total Defence. A computer break-in can be carried out in the intention of disrupting the functioning of society, such as the disbursement of pensions or insurance payouts, or in order to cause problems of various kinds. A party who succeeds in forcing entrance into central computer systems can immobilise important elements of the infrastructure, such as railway traffic, aviation control and the electricity supply.

It is also in the nation's interest that the business sector use secure crypto systems to protect itself against advanced forms of crime and industrial espionage. Companies are dependent on accurate and prompt information and reliable technical systems. When foreign exchange transactions and financial systems are disrupted and important business secrets can be acquired by foreign competitors, this has consequences for the whole of society.

## **2.5 Export controls**

Export controls on certain strategic products, i.e. products that can be used for both civil and military purposes, are intended to prevent sensitive products and technology from being exported to parties who can be assumed to use them in order to produce weapons of mass destruction or for other purposes that jeopardise peace.

Instead of “strategic products”, the expressions “goods with dual areas of use” or “dual-use products” are sometimes used. Cryptographic technology is an advanced technological product of this kind, with the potential to disrupt Swedish security interests.

Export controls on strategic products differ in nature from controls on munitions. In the case of trade in munitions, a general ban on exports without special permission is in force. In the case of strategic products, on the other hand, the presumption is that export is to be permitted.

Thirty-three countries (the majority of the OECD countries together with Russia, Ukraine, Argentina, and others) participate in the Wassenaar Arrangement established in 1996, which is a forum for cooperation on the control of exports of arms and dual-use products, including cryptographic products.

Within the EU, the Council, supported by Article 113 of the Treaty establishing the European Communities, has passed a directive, (EC) No. 3381/94 of 19 December 1994, on the establishment of Community regulations for controls on exports of dual-use goods. The main consequence of the directive is that a license is required for the export (i.e. transfer to countries outside the EU) of such goods as are listed in Annex I of the Council’s decision 94/942/GUSP of 19 December 1994. For products listed in Annex IV and Annex V of the same decision, a license is required for transfer to other EU countries, i.e. for these products, free trade within the EU does not at present apply.

Swedish controls on the export of strategic products are governed by the EU’s regulations in this area. In Sweden, the Council directive and decision have been supplemented by the Strategic Products Act (1998:397) and the Directive on Strategic Products (1998:400).

Responsibility for the implementation of Swedish export controls rests with the Inspectorate for Strategic Products (ISP). On cryptography issues, the ISP consults experts from the Total Defence. Anyone desiring to export a cryptographic product of a certain type from Sweden is required to submit a written application to the ISP. Two types of license for cryptographic technology may be applied for, global and individual. A global license is valid for a product for a specified period of time, and to a specified number of countries, while an individual license is valid for one specific export occasion.

### **3 Some international issues**

#### **3.1 EU co-operation**

Cryptography issues are dealt with under the three pillars of the European Union (the internal market, security policy and legal cooperation). Measures within one pillar have an impact on the conditions and the need for measures in the two others.

Where cryptography is concerned, Sweden supports the establishment of necessary coordination. Since 1992, the task of working to promote cooperation and coordination has been assigned by the Council to the SOGIS committee (Senior Officials Group on Information Systems Security) in the area of IT security.

### ***Electronic signatures***

On 13 May 1998, the Commission presented a proposal for a common framework for electronic signatures, COM (1998) 297 final. The proposed directive is intended to promote the use of electronic signatures in the internal market and thereby to support the development of electronic commerce. This is to occur by means of a legal framework for the use of electronic signatures and by the legal recognition of these signatures.

The proposed directive contains rules on certificates and electronic signatures. “Qualified certificates” and “advanced electronic signatures” will be provided with special terms and regulations that specify the rights and responsibilities that the owners enjoy.

The proposed directive also contains regulations on the admittance to the market of certification authorities, which in the proposed directive are designated Certification Service Providers (CSPs), i.e. bodies that provide signature services. According to the regulations, Member States are not permitted to make the provision of signature services conditional on prior authorisation. However, voluntary accreditation schemes are permitted, i.e. schemes for assessing compliance with requirements that have been imposed. The Member States are to ensure appropriate supervision of bodies providing signature services. Member States are, however, permitted to attach additional requirements to the use of electronic signatures in the public sector.

An electronic signature that fulfils certain requirements is to be regarded as equivalent to a hand written signature. However, this only applies to those areas in which Member States have decided to accept the use of electronic signatures. The proposed directive also contains regulations on the liability for damages of CSPs that provide signature services and issue qualified certificates.

In April 1999, the Council adopted a common position on the proposed directive. When the European Parliament has discussed the Council’s common position, the Council will be able to make a final decision on the proposal.

### ***Export of dual-use goods and technology***

On 15 May 1998, the Commission presented a proposal for a new directive on export controls for goods and technology with dual areas of use. In the proposal (COM (1998) 257 final), the Commission states that the present regulations do not function in a satisfactory manner. No fully credible regulation of controls at the Community-wide level has been established for exports to third countries. The Commission is also of the opinion that the present regulations need to be simplified where trade within the EU is concerned.

In two judgements published in October 1995, the Court of Justice of the European Communities has found that the Community has exclusive jurisdiction in issues relating to export controls on dual-use goods. According to the Court, rules restricting exports to third countries of dual-use goods fall under Article 113 of the Treaty establishing the European Communities.

The Commission's proposed new directive also includes controls on the transmission of technology by electronic media, facsimile machines and telephones. The proposal places the physical transfer of technology on an equal footing with the transmission of technology using electronic media, facsimile machines and telephones. Under present regulations, controls apply solely to physical transfer, e.g. the sending of a drawing by post. If the drawing is instead sent as a facsimile or e-mail, the transmission is not subject to any restrictions. The proposal means that a Community-wide legal loophole will be closed.

For the field of cryptography, this proposal would have an impact on the obligation to apply for a license to export cryptographic products via electronic media to destinations outside the EU.

Another proposal of significance for cryptography is that licenses for the transfer of cryptographic products to other EU countries are to be replaced by a procedure of post factum notification. This proposal could mean that companies in the EU may come to have the entire internal market as their home market. Such a home market would be equivalent in size to the American home market for cryptographic products.

The Commission's proposal is being studied by an ad hoc group within the Council. A decision is expected in the course of 1999. When the decision comes, the Swedish body of regulations will need to be reviewed and adapted to the new Directive.

### ***The fight against crime***

Within the third pillar of the EU, discussions were initiated in the Council in spring 1998 regarding the powers of law enforcement authorities in connection with the use of encryption by criminals.

On 28 May 1998, the Council of Ministers approved certain conclusions on Encryption and Law Enforcement. The Council noted that law enforcement authorities are concerned that the widespread availability of cryptographic services for confidentiality services may have a serious impact on the fight against serious crime and terrorism if, where necessary and appropriate, it is not possible to get lawful access to decryption keys on a case by case basis. The Council has therefore agreed to monitor closely the extent to which encryption is exploited by serious criminals and terrorists.

The Council recognises that one possible approach amongst others, which might meet law enforcement interests, might be the promotion of confidentiality services which involve the deposition of a decryption key or other information with a third party. Law enforcement agencies may also require lawful access to decryption keys

where it is necessary to decrypt material which has been seized as part of a criminal investigation.

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

The Council believes it is important to establish a common understanding of the needs of law enforcement agencies where cryptographic services are used for confidentiality purposes.

The Council has therefore agreed to prepare a Resolution on Encryption and Law Enforcement to complement the work underway in other fora of the Council. The Resolution will invite Member States to take account of law enforcement needs in developing their national policies.

### **3.2 The Wassenaar Arrangement and new EU regulations**

During 1998, a review was undertaken of the lists of goods for the export controls laid down in the Wassenaar Arrangement. These lists are used in applying the EC directive on controls of exports of dual-use goods.

The new list of goods for information security, which the participating countries agreed on on 3 December 1998, is organised in such a way as to indicate clearly which exports of cryptographic products are to be restricted and hence also which are not subject to restrictions. One of the purposes is to provide clear guidance to individuals and companies that wish to export cryptographic products. A second object is to put the countries in a position to control exports in a similar fashion. The regulations are not to be difficult to interpret. An export company shall neither be discriminated against nor favoured by its own country, compared with companies in other countries. The new regulations mean that a large proportion of present cryptography use throughout the world is free from restrictions. Only cryptographic products with a key length in excess of 56 bits for symmetric crypto systems or 512 bits for asymmetric systems are subject to export controls. These limitations are to be reviewed no later than the year 2000.

The list also specifies certain substantial exceptions from restrictions. For example, cryptographic products that an individual user takes personally into another country for his or her own use are exempted from export controls.

A special note has been added on cryptography (including both software and hardware), which exempts so-called mass-market products from restrictions. The note applies to products that are sold without restrictions over the counter, via mail order, electronically or by telephone. Users are not to be able to modify the cryptographic

function and are to be able to install the software themselves, without substantial support from the seller. Further, where symmetric crypto systems are concerned, the rule is that they are not to be able to generate keys in excess of 64 bits. Suppliers are also to be able to present technical information on the cryptographic product on request to relevant authorities in their own countries. The 64-bit limit in the note on cryptography applies until 3 December 2000. If the participants in the Wassenaar Arrangement have failed to reach agreement on continued regulations by that time, this limit will cease to apply.

In future too the rule will apply that cryptographic software that is “in the public domain” shall be exempt from export controls. What is meant by “in the public domain” is that software has been made available to the general public without restrictions on its further dissemination. The government is of the opinion that software that was “in the public domain” at the time when the regulations came into effect should be exempt from export restrictions. If, on the other hand, someone has later, without permission, made cryptographic software available in contravention of the current regulations, exports should continue to be restricted.

By a decision of 9 March 1999 (1999/193/GUSP), the Council has changed the annexes to the present EU directive on export controls on dual-use goods in response to the agreement of 3 December 1998 within the Wassenaar Arrangement. The change, which came into effect on 19 April 1999, entails *inter alia* that mass-market products, irrespective of their capacity, and whether hardware or software, are included in the freedom of movement of the internal market.

As previously mentioned, the Commission has presented a proposal for a new directive on the establishment of Community-wide regulations for export controls on dual-use goods and technology, in which it is proposed that suppliers shall be able to sell all cryptographic technology on the internal market on approximately the same conditions as they face on their own home market. In connection with this liberalisation it is important that all EU countries apply restrictions on onward exports of cryptographic products to third countries outside the Union in a similar fashion. To this end, the Commission has proposed a process of consultations between the public authorities in the country of origin of the product and those in the country to which it is transferred, together with an augmented exchange of information.

### **3.3 The OECD**

The Organisation for Economic Co-operation and Development (OECD) adopted guidelines on cryptography in March 1997 (OECD/GD(97)204). The guidelines have influenced the work of a number of countries and organisations on defining a policy in the field of cryptography.

The USA and the UK, together with some other countries, have taken an initiative towards designing more concrete measures parallel to the OECD, as a step towards producing a global infrastructure for the use of cryptography. The intention is that users in different countries shall be able to communicate with one another even when their communications are signed and encrypted. Sweden is participating in these discussions.

After the Ministerial Conference on “A Borderless World: Realising the Potential of Global Electronic Commerce” that took place in Ottawa in October 1998, the OECD has begun to plan for an international workshop on the conditions for and possibilities of bringing into being regulations and solutions for the electronic authentication of parties in business transactions. According to plan, the workshop will take place in June 1999 in the USA and will be conducted by the OECD together with business organisations, the EU and member countries of the Asia Pacific Economic Cooperation.

### **3.4 The Council of Europe**

In the Council of Europe’s “Recommendation No. R (95) 13 concerning problems of criminal procedural law connected with information technology” it is stated *inter alia* that measures ought to be considered for the purpose of minimising the effects of the use of cryptography on criminal investigations. These measures should be of such a kind that the legitimate use of cryptography is not affected more than is absolutely necessary. However, the recommendation does not indicate what measures should be implemented.

The Council of Europe has launched a project on “Crime in cyberspace” that takes as its point of departure recommendation R (89) 9 on computer-related crime and the above mentioned recommendation R (95) 13. The intended result of the new project is a convention.

### **3.5 Developments in other countries**

Work is in progress at present in various countries on developing a cryptography policy. In the main, the debate has focused on the question of how to meet the needs of both users and law enforcement authorities and whether an infrastructure should be built up for key administration in which “trusted third parties” (TTPs) provide security services to users, including the management of cryptographic keys. One solution that has been discussed is that private confidentiality keys should be placed in escrow with a trusted third party. However, many people regard the storing of private confidentiality keys as a controversial issue, since those who obtain access to such keys can decrypt certain messages.

In the countries where key escrow has been considered, a major question has been whether it should be voluntary or mandatory. France formerly had a mandatory system that was linked to permit requirements for importing cryptography and using it within the country. In January 1999 the French Government decided to liberalise imports and use and to go over to a voluntary system. In the USA the Administration launched technical systems several years ago to make mandatory key escrow possible. In more recent years, however, policies have been directed more towards promoting voluntary systems.

Other countries where work is in progress towards promoting or establishing voluntary key escrow are Australia, Canada, the Netherlands, the UK and Germany, but there are differences between the solutions that are under consideration.

In Denmark, where the Government has commissioned a study of the issue of key escrow, it has been proposed that the Government should be content to await developments.

In various countries where the issue of how voluntary systems should be designed is under debate, the questions being considered include the following:

- whether the authorities/bodies responsible for escrow and recovery have to be third party authorities;
- whether large organisations should be allowed to have their own internal bodies;
- whether third party and internal bodies themselves should be allowed to choose whether they want to receive authorisation or whether this should be mandatory,
- whether the State or some other organisation in the market should authorise third party and internal bodies,
- whether authorised third party or internal bodies can require users to place their private confidentiality keys in escrow with them or whether escrow should be voluntary for the user.

A number of countries require licenses for the import or use of cryptographic technology, or have made permission to use encryption within the country conditional on the user using specific procedures or products approved by the state.

Countries that have regulated the use or import of cryptographic technology include, for example, Israel (use/import), China, incl. Hong Kong (import), Latvia (import), Poland (import), Russia (use/import), Singapore (use/import), Spain (use), South Korea (import) and Hungary (import).

## **4 The Government's deliberations and conclusions**

**The Government's opinion:** At present there is no reason to limit the use of cryptographic technology in Sweden. All shall have the right to choose such technology themselves.

Imports of cryptographic technology shall remain free of restrictions.

There remain reasons of security policy for preventing the dissemination of cryptographic technology to unsuitable parties in certain other countries.

If developments should warrant more stringent regulations, the Government will consider appropriate measures for creating means of legal access to the plaintext of encrypted information for law enforcement and supervisory authorities.

Sweden's policy should be characterised by flexibility and open-mindedness so as to be able to respond to an increased demand for secure cryptographic technology,

changes in other countries' policies and the continued development of technology in the field.

### ***Reasons for the Government's opinion***

#### *Background*

It can be observed that a number of different points of view emerge in the debate on the use of cryptographic technology.

- Users (public authorities, companies, individuals) stress the freedom to encrypt information and protect it against unauthorised observation or against criminal activity; they do not want to be subject to any restrictions in this respect. At the same time, it is in the interest of users, and of society in general, that the police, in their crime-fighting role, be in a position to decrypt messages for the purposes of surveillance and the securing of evidence.
- Users want strong protection for the information that is sent or stored in encrypted form. They also want to be able to salvage such information if their private confidentiality keys should be mislaid; in that case they want to be able to obtain a copy of the key. Law enforcement authorities must be allowed to use coercive measures to obtain legal access to private keys of this kind.
- In the case of any placing of their private confidentiality keys in escrow, users want them to be stored in a secure and trustworthy manner. If these keys have to be deposited outside the users' control, confidence diminishes. Users may then prefer means other than computer communication for delivering their messages, e.g. courier delivery or a personal journey.
- It is in the interest of the law enforcement authorities that users protect themselves by strong crypto systems in order to hinder or prevent criminal activity. At the same time, free access to cryptographic technology for protecting data and messages can obstruct or prevent the fight against crime.
- The State, which is responsible for the security of the country and protects society against terrorism and other crime, has classified cryptographic technology as a technology with both civil and military uses, which should be subject to export controls. Others are of the opinion that the export of cryptographic technology does not need to be restricted.

#### *Electronic commerce and associated issues*

In recent years electronic commerce and other electronic communication have grown to become significant areas for the use of modern information technology. This brings new business opportunities and new ways of working that lead to growth and employment. At the same time, great demands are being raised for security in the transmission of messages and documents, and for the electronic authentication of users. This can be achieved with the aid of cryptography. It is therefore in the general public interest that users are given access to strong crypto systems and that the conditions be in place for the use of electronic signatures and for the protection of confidentiality. In the government's opinion, a widespread use of cryptography will in-

crease confidence in communications systems. Further, the risk of cryptography being put to improper use is not so great as to warrant limiting its use at the present time. All shall have the right to choose cryptographic technology themselves and imports of cryptographic technology shall remain free of restrictions.

As mentioned earlier (see section 2.2), electronic signatures are used in order to safeguard identity and protect documents from alteration. A central issue for the design of Swedish regulations on electronic signatures is what form the management of certificates and cryptographic keys should take. A so-called certification service provider (CSP) is the body that makes signature services available. This body draws up and signs certificates that state the identity of the owner of the public signature key. The role of the CSP is therefore crucial for confidence in electronic signatures. Certain fundamental demands therefore need to be made on the internal organisation of such bodies and on the certificates and keys that they issue.

Users need secure electronic signatures and access to an open market for signature services. The exact form a system for the supervision and control of signature services in Sweden will take will necessarily depend on the regulations that the forthcoming EC directive on electronic signatures establishes. The basic assumption is that Member States will not be permitted to bring in mandatory license conditions for signature activities. On the other hand, there is a possibility that voluntary accreditation systems will be developed. The State will be in a potential position to function as a model in its own use of signature services.

Within the Government Offices, work has begun on the speedy development of possible courses of action and proposals for a future structure and organisation of signature services. This work will be pursued in close cooperation with public authorities, the business sector and special interest organisations in the field.

### *The fight against crime and associated issues*

Cryptography is an important aid in preventing or hindering criminal activities. Users who protect their information with the help of cryptography contribute to forestalling crime.

However, cryptographic technology can also be used for criminal purposes. Law enforcement authorities therefore need, in connection with the use of coercive measures such as search and seizure, to obtain access to the plaintext of encrypted information, and in connection with secret wiretapping, to obtain access to private confidentiality keys without the knowledge of the suspect, in order to be able to decrypt messages. Inspection or supervisory authorities similarly need to obtain access to the plaintext of stored and encrypted information in carrying out audits and other acts of inspection.

The present regulations on coercive measures would offer law enforcement and supervisory authorities certain means of obtaining access, for example, to private confidentiality keys or other existing information on their customers from special bodies that provide management services for certificates and cryptographic keys. Search of premises, the hearing of witnesses or similar measures can also be used to achieve

this. Such use of coercive measures has the support of the law and occurs in regulated forms. It is vital that the technology that is used in a particular case does not constitute an obstacle to such legal access. Cryptographic keys intended for electronic signatures should not be used also to protect confidentiality, since a private signature key ought not to be held in escrow. Instead, separate signature keys and confidentiality keys should be used.

Law enforcement and other investigative authorities' means of legal access to the plaintext of encrypted information must be safeguarded. To make this possible, in addition to the requisite national measures, initiatives may need to be taken at the international level. Should developments warrant more stringent regulations, the Government will consider appropriate measures for creating means of legal access to the plaintext of encrypted information for law enforcement and supervisory authorities.

In addition, the Government is of the opinion that Sweden ought to take an active part in the development of EU-wide regulations and other international agreements in this field.

#### *Export controls*

In the Government's opinion, there continue to be reasons of security policy to prevent the dissemination of cryptographic technology to unsuitable parties in certain other countries. The Swedish position on restrictions on the dissemination of cryptographic technology to other countries (export controls) should take into account that free trade and global electronic communication are to Sweden's benefit. At the same time, for its national security, Sweden is dependent on international cooperation, of which export controls constitute a part.

The Government is of the opinion that the following measures ought to be taken.

- Export controls on cryptographic products should continue in accordance with the EU regulations and Sweden's commitments under the Wassenaar Arrangement (WA). Sweden is working *inter alia* for the creation of a uniform and non-discriminatory application of the regulations in the countries that are cooperating within the WA and the EU, in order to ensure that Swedish companies do not suffer from competitive disadvantages.
- The present regulations for export controls favour companies in countries with a large home market. Sweden therefore welcomes the Commission's proposal that the freedom of movement within the internal market should apply to cryptographic products.
- It is important that export controls be gradually liberalised and concentrated on those sensitive cryptographic products where the interests of control outweigh the interests of free trade.
- The regulations should explicitly place the physical export of cryptographic software on an equal footing with making them available via computer networks. Network dissemination has already now attained significant dimensions and the conditions on which the current export control policy is based have therefore changed.

### *The public sector*

Like other parts of society, the public sector is in need of secure and reliable cryptographic technology. This involves being able to judge which products and techniques to use, which raises special demands for expertise and accurate judgement in public procurement and for the advice that public authorities may need in this connection.

Governmental authorities should make use of key management systems with built-in functions for key recovery. In order to promote this, internal bodies for managing certificates and cryptographic keys probably need to be set up. These governmental bodies should be regulated in such a way that they can serve as a model for the private market too. Work towards this goal is in progress in countries such as Australia, Finland, Canada, the UK and the USA.

In the Government bill on Public Administration in the Citizens' Service, the Government made it known that a common set of regulations will be elaborated for secure communication within the public administration.

### *Future developments*

Developments within the EU and in countries outside the Union, including the USA, are of significance for the design of a Swedish policy on the use of cryptography. The experience of recent years shows, however, that it is hard to assess developments, and that some countries' cryptographic policies have changed, sometimes quickly and unexpectedly. The technology and its use also change constantly. This indicates that a Swedish policy should be receptive to the demands that are raised. Decisions and measures must be open to continuous review.

The number of computers in Sweden is large, and use of the Internet is widespread. A significant proportion of information services and software sales take place via computer networks, and better and better cryptographic software is becoming available on the Internet. A sharp increase in the use of cryptography can therefore be expected in the coming years.

One important question in this connection is to what extent cryptographic technology is used to conceal criminal activities. Already now, criminals competent in the use of computers can acquire very powerful cryptographic tools and use them without there being any possibility of the law enforcement authorities being able to decrypt the messages and documents. Sweden, like other countries in the EU, is monitoring these developments. Should they warrant it, the Government will consider more stringent regulations. This too indicates that Swedish policy ought to evolve gradually.

Various courses of action are conceivable in defining a cryptographic policy. One option is to rely on the market's own development and to refrain from any initiatives to introduce regulations. If there is a desire to emphasise the role of the State, an alternative may be to create openings for the provision of signature and confidentiality

keys in Sweden, and to offer bodies that provide such services some appropriate form of authorisation. The Government wishes to promote the use of modern technology in all parts of society. Information technology creates opportunities that must be taken advantage of. Moreover, the Government is anxious to promote electronic commerce and other electronic services together with a secure exploitation of the opportunities for electronic communication. A broad use of cryptographic technology can be of advantage to the development of electronic commerce by increasing confidence in the systems. The use of cryptographic technology should therefore be facilitated and users themselves should have the right to choose which technology should be used.

With regard to the use of *signature services*, the Government Offices are preparing to introduce the coming EC directive on a common framework for electronic signatures. With regard to the issue of *confidentiality services*, it should be investigated whether there are reasons for the State to involve itself in a voluntary authorisation procedure of special trusted bodies that wish to provide such services.

Sweden's policy should be characterised by flexibility and open-mindedness, so as to be able to respond to an increased demand for secure cryptographic technology, changes in other countries' policies and the continued development of technology in the field.

## Appendix 1: Terminology

The definitions in this appendix are taken primarily from:

Terminologi för informationssäkerhet, Informationstekniska standardiseringen 1994. Rapport ITS 6, ISBN 91-630-2483-7.

The OECD guidelines for cryptography policy (March 1997).

### **asymmetric crypto system**

A crypto system in which different keys are used for encryption and decryption (ITS 6).

### **authentication**

- 1) Checking of a stated identity, e.g. when logging on in the case of communication between two systems, or when users exchange messages;
- 2) Checking that a message is genuine, in the sense that it has not been altered since it left the sender (user, computer, communications node, etc.).

Note: Authentication (1) is synonymous with the verification of identity. Authentication (2) is often termed message authentication (ITS 6).

### **Certification Authority (CA)**

A body trusted by multiple users that has the task of creating and issuing key certificates.

Note: A certification authority can also have other tasks, e.g. creating pairs of keys (public/private key) for each user, maintaining and distributing revocation lists for withdrawn certificates, etc. (ITS 6). Cf. TTP.

### **Public key certificate**

The user's public key in an asymmetric crypto system, which together with the user's name and perhaps other information is signed and issued by a certification authority (ITS 6).

### **Certification Service Provider (CPS)**

An entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.

Note: This term, which is equivalent to certification authority (see above), is introduced in the forthcoming EC directive on a common framework for electronic signatures. There is no established Swedish term.

### **decryption**

The inverse function of encryption.

### **digital signature**

Transformation of a message (or a condensed form of a message) in a manner that only the sender can carry out and that allows the recipient to check the authenticity of the message, its content and the sender's identity.

Note: A digital signature can be applied to information objects in digital form using the sender's private key in a crypto system and is checked using the public key (ITS 6).

**electronic signature**

Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

Note: this term is used instead of digital signature (see above) in the EC directive on a common framework for electronic signatures.

**integrity**

Immunity to interference, wholeness having the capacity to maintain its value by means of protection against undesired alteration, influence or observation.

Note: In the Swedish debate, the term is generally used with reference to personal integrity when personal information is treated in computer systems. Note that in this case, the term “privacy” is used in English-speaking countries. In case of doubt, the expression should be clarified: personal integrity, systems integrity (ITS 6).

**confidentiality**

The intent that the contents of an information object (or sometimes even its existence) shall not be made available or disclosed to unauthorised parties (ITS 6).

Note: Since this concept is not linked to secrecy in the legal sense, the term confidentiality is used in the present communication. However, in other connections secrecy can occur as a synonym.

**encryption**

Transformation of plaintext to crypto text by means of crypto systems and the relevant encryption key, for the purpose of preventing unauthorised access to confidential information (ITS 6).

**cryptographic algorithm**

A set of mathematical rules for cryptographic transformations (ITS 6).

**cryptography**

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 (OECD).

**crypto system**

Equipment and/or software with associated instructions and aids that are used for cryptographic applications (ITS 6, somewhat modified).

**key**

Variable information that governs a cryptographic process, e.g. encryption, decryption or the creation or verification of an electronic signature.

**key escrow**

Secure storage by someone other than the user of a copy of a crypto key for use in decryption.

Note: In the case of key escrow, the person using a crypto system voluntarily or under coercion surrenders his or her key to an independent body. After a Court ruling, the police can acquire access to the key or obtain help with decryption. Users the m-

selves may also need access to copies of the key if they have lost their own key or have happened to make it unusable. Cf. key recovery.

**key management**

Administration and technical methods for generating, storing, distributing, using and destroying cryptographic keys, together perhaps with the secure certification of cryptographic keys (ITS 6).

**key recovery**

In this communication, this term refers to any technique for obtaining a cryptographic key for use in decryption from someone other than the user.

Note: This can for example occur by a key in escrow being retrieved or by the key being recovered after some computation process. In other connections the term sometimes refers merely to the recovery of a key that accompanies a message in encrypted form (key encapsulation).

**non-repudiation**

A property of data 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) (OECD).

**symmetric crypto system**

A crypto system in which the same key is used for encryption and decryption (ITS 6).

**Trusted Third Party (TTP)**

An organisational unit that is trusted by a group of (communicating) users for specified security-related services (ITS 6).

Note: A TTP carries out services with which it is entrusted in the fields of electronic signatures and confidentiality, for example the creation and escrow of keys. Since a TTP can also offer certificate services, TTP is used in appendix 2 as a higher level term, which embraces among other things the terms certification authority and CSP. Large companies and public authorities may have an internal body that is part of the organisation.