COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 08.10.1997
COM(97) 503 final

COMMUNICATION FROM THE COMMISSION

TO THE COUNCIL, THE EUROPEAN PARLIAMENT,
THE ECONOMIC AND SOCIAL COMMITTEE
AND THE COMMITTEE OF THE REGIONS

ENSURING SECURITY AND TRUST IN ELECTRONIC COMMUNICATION

TOWARDS A EUROPEAN FRAMEWORK FOR DIGITAL SIGNATURES AND ENCRYPTION

ENSURING SECURITY AND TRUST IN ELECTRONIC COMMUNICATION

TOWARDS A EUROPEAN FRAMEWORK FOR DIGITAL SIGNATURES AND ENCRYPTION

EXECUTIVE SUMMARY

Introduction

Open electronic networks such as the Internet are increasingly being used as a platform for communication in our society. They have the capacity to create new businesses, new channels of distribution and new methods of reaching the customer. They also open up opportunities to re-engineer business conduct itself. It is now largely expected that electronic commerce will be one of the key drivers for the development of the global information society. Electronic Commerce presents the European Union with an excellent opportunity to advance its economic integration by means of a "virtual" economic area.

However, the realisation of such developments are hampered by the noticed insecurities typical to open networks: messages can be intercepted and manipulated, the validity of documents can be denied, personal data can be illicitly collected. As a result, the attractiveness and advantage of electronic commerce and communication cannot be fully exploited.

In order to make good use of the commercial opportunities offered by electronic communication via open networks, a more secure environment needs to be established. Cryptographic technologies are widely recognised as essential tools for security and trust on open networks. Two important applications of cryptography are digital signatures and encryption.

Several Member States announced their intentions to introduce specific regulation on cryptography and some already have done so. For instance, Germany and Italy already moved ahead with digital signature laws. In other Member States internal discussions are taking place, and some tend to refrain, at least for the moment, from any specific regulation at all.

Divergent and restrictive practices with regard to cryptography can be detrimental to the free circulation of goods and services within the *Internal Market* and hinder the development of electronic commerce. The European Union simply cannot afford a divided regulatory landscape in a field so vital for the economy and society.

The main objectives of this Communication are to develop a European policy in particular with a view to establishing a common framework for digital signatures, ensuring the functioning of the Internal Market for cryptographic services and products, stimulating a European industry for cryptographic services and products and stimulating and enabling users in all economical sectors to benefit from the opportunities of the global information society. As far as timing is concerned, the Commission considers that appropriate measures ought to be in place throughout the Union by the year 2000 at the latest. As a consequence, the Commission intends to come forward with detailed proposals in 1998 after the assessment of comments on this Communication.

This is in line with the April 1997 adopted Communication on Electronic Commerce, where the Commission announced the intention to prepare a policy aiming at guaranteeing the free movement of encryption technologies and products, as well as to propose a specific initiative on digital signatures.

Digital Signatures

Some Member States are in the process of introducing voluntary schemes, others of mandatory licensing schemes to build trust in Certification Authorities (CAs) and to encourage legal recognition of digital signatures. Whilst the development of a clear framework is welcomed, different national regulatory approaches and the lack of mutual recognition of each others' regulatory requirements may easily lead, due to the inherent cross-border nature of digital signatures, to a fragmentation of the

Internal Market for electronic commerce and on-line services throughout the Union.

In order to stimulate electronic commerce and the competitiveness of the European industry as well as to facilitate the use of digital signatures across national borders, a common legal framework at Community level is urgently needed. Any regulation in the field of digital signatures must meet two main requirements: create a clear framework to build trust in digital signatures on one side and be flexible enough to react to new technical developments on the other side.

Encryption

Stimulated by the rapid expansion of the Internet encryption will become an integral part of personal and business computing. Electronic commerce as well as many other applications of the information society will only receive acceptance and will only unfold their economic and social benefits if confidentiality can be assured in a user-friendly and cost-efficient way. In open networks, encryption of data is very often the only effective and cost-efficient way of protecting confidentiality of data and communications.

Law enforcement authorities and national security agencies are concerned that wide-spread use of encrypted communication will diminish their capability to fight against crime or prevent criminal and terrorist activities. For this reason, there are reflections in several Member States to establish regulation on cryptography, in addition to controls on export and intra-Community shipments. This has led to a discussion about the need, technical possibilities, effectiveness, proportionality and privacy implications of such regulations.

However, nobody can be effectively prevented from encrypting data (criminals or terrorists also can use encryption for their activities), e.g. by simply downloading strong encryption software from the Internet. As a result restricting the use of encryption could well prevent law-abiding companies and citizens from protecting themselves against criminal attacks. It would not however prevent totally criminals from using these technologies.
Proposals for regulation of encryption have generated considerable controversy. Industry expresses major concerns about encryption regulation, including key escrow and key recovery schemes. Although there is a lack of experience, as electronic communication and commerce have just begun to penetrate economy and society, this Communication makes some assessments to build a common European understanding of the subject.

Policy actions in the area of digital signatures

The at European level urgently needed framework should include common legal requirements for CAs (in particular common requirements for the establishment and operation of CAs) allowing certificates to be recognised in all Member States.

In addition, the Commission will monitor the legal developments in Member States introducing new legislation with the aim to respect Internal Market principles and will encourage Member States to rapidly implement appropriate measures to build trust in digital signatures.

In order to achieve as wide as possible acceptance of digital signatures Member States should co-ordinate activities to ensure legal recognition of digital signatures at the latest by the year 2000. The Commission will evaluate the necessity to provide for the legal recognition of digital signatures at Community level by harmonising different national regulation (e.g. form requirements, evidence rules).

The Community and Member States should take part in or initiate a dialogue with international organisations, such as the OECD, the United Nations and the WTO, notably to establish common technical standards and mutual recognition of regulations.

Policy actions in the area of encryption

The EC Treaty and the Treaty on the European Union fully respect the competence of Member States with regard to national security and law enforcement.

To ensure that the development of electronic commerce in the Internal Market is not hindered and to facilitate the free circulation and use of encryption products and services the Commission calls upon

Member States to avoid disproportionate restrictions. Moreover the Commission will examine whether restrictions are totally or partially justified, notably with respect to:

- the free circulation provisions of the Treaty, in particular Articles 30, 36, 52, 56 and 59,
- the principle of proportionality,
- the Council Directive 83/189/EEC of 28.3.1993 laying down a procedure for the provision of information in the field of technical standards and regulations and
- the EU Directive 95/46/EC of 24.10.95 on the protection of personal data.

The Commission also believes that it will be important for Member States to distinguish "digital signature services" from "encryption services", because different rules and different goals separate these two aspects.

Additional measures:

- Adapting the Dual Use Regulation (CE) 3381/94 in view of the requirements for the cryptographic products market;
- Improving the co-operation of police forces on a European and international level;
- Working towards international agreements between the Community and other countries because of the global dimension of electronic communications and commerce.

Accompanying measures

- Encouraging industry and international standards organisations to develop interoperable technical and infrastructure standards for digital signatures and encryption to ensure secure and trustworthy use of networks.

- Proposal of a Council and Parliament Decision for an INFOSEC II programme building on the INFOSEC programme carried out from 1992 until 1994. Such a programme would aim at developing overall strategies for the security of electronic communications, in particular with a view to provide the user with appropriate protection systems.

- Continuing of the current projects in the field of digital signatures and encryption within the 4th framework programme for Community activities in the field of research and technological development (1994 - 1998) and launching of new projects within the 5th framework programme (1998 - 2002).

- Support of the use of digital signatures and encryption in EU services and government administrations.

- Setting up of an European Internet-Forum in 1997 as a means to inform and exchange information on the regulatory and use aspects of digital signatures and encryption.

- Organisation of an international hearing on "digital signature and encryption" beginning of 1998.

Timeframe

4.Q./1997:	European Internet-Forum
4.Q./1997:	Commission proposal to amend the Dual-Use Regulation
1.Q./1998:	International hearing
1.Q./1998:	Assessment of the comments on the Communication, the results of the Internet-Forum and the International hearing
2.Q./1998:	Proposal for further action (e.g. Directive on digital signatures)
2.Q./1998:	Proposal for an Infosec II programme
1998-2002:	Projects within the 5th framework programme
by 2000:	Common framework on cryptography put in place throughout the Union

TABLE OF CONTENTS

1 dl

I. Introduction
The need for secure electronic communication

Open networks such as the Internet are increasingly being used as a platform for communication in our society. Open and accessible, they allow rapid and efficient world-wide exchanges at low cost. This will lead to new forms of business configuration (e.g. "virtual" enterprises, work collaboration across the globe), of private communication (e.g. e-mail) and of organisation of public services (e.g. electronic tax declaration).

Open networks also have the capacity to offer substantial opportunities for global electronic commerce in goods and services which can be ordered, supplied and paid for electronically. Already today, software packages, information, music, and videos are being delivered over the Internet. It is now largely expected that electronic commerce will be one of the key drivers for the development of the global information society[1].

Overall, the increasing use of open networks offers the possibility to create new businesses, new channels of distribution and new methods of reaching the customer. It also opens up opportunities to re-engineer business conduct itself.

However, the realisation of such developments are hampered by the noticed insecurities typical to open networks: messages can be intercepted and manipulated, the validity of documents can be denied, personal data can be illicitly collected. Fraud is already increasing in several forms. Therefore, today, important electronic documents are usually only exchanged in so-called "closed networks", that is, involving users between whom contractual relationships and mutual trust already exist. This model cannot be transferred to open networks because of the absence of such relationships between users. As a result, the attractiveness and advantage of electronic commerce and communication cannot be fully exploited.

In order to make good use of the commercial opportunities offered by electronic communication via open networks, a secure and trustworthy environment is therefore necessary. Cryptographic technologies are nowadays widely recognised as the essential tool for security and trust in electronic communication. Two important applications of cryptography are digital signatures and encryption. Digital signatures can help to prove the origin of data (*authentication*) and verify whether data has been altered (*integrity*). Encryption can help keeping data and communication *confidential*.

Several Member States announced their intentions to introduce specific regulation on cryptography and some have already done so. For example, Germany and Italy already moved ahead with digital signature laws. In other Member States internal discussions are taking place, and some tend to refrain, at least for the moment, from any specific regulation at all.

Divergent legal and technical approaches would constitute a serious obstacle to the Internal Market and would hinder the development of new economic activities linked to electronic commerce. An EU policy framework for ensuring security and trust in electronic communication and safeguarding the functioning of the Internal Market is therefore urgently needed. The European Union simply cannot afford a divided regulatory landscape in a field so vital for the economy and society.

As cryptographic services and products are more and more demanded, concerns are expressed that abuse of cryptography by criminals or terrorists would make it increasingly difficult to combat crime. Such concerns apply only to confidentiality services. Digital signatures do not pose any risk for law enforcement, since they do not prevent data from being read. Digital signatures could even bring significant law enforcement benefits as they allow for example messages to be attributed to a particular reader and/or sender. As, in addition, they need a specific regulatory framework to take into account their legal implications, the present Communication distinguishes between authentication and integrity services - *digital signatures* (part II) and confidentiality services - *encryption* (part III)[2].

[1] Communication of the Commission "A European Initiative in Electronic Commerce" (COM(97)157 final, 16.4.97), http://www.ispo.cec.be/Ecommerce.

[2] This distinction is also stated clearly in the OECD Guidelines for Cryptography Policy, 27.3.97; http://www.oecd.org/dsti/iccp/crypto_e.html

In September 1996, the *European Parliament* invited the Commission to prepare legal EU provisions concerning information security and confidentiality, digital identification as well as the protection of privacy[3]. In November 1996 the *Council of Ministers* requested the Member States and the Commission to prepare consistent measures to ensure the integrity and authentication of electronically transmitted documents[4]. In March 1997 the *OECD* adopted Guidelines for cryptography policy, setting out principles to guide countries in formulating their own policies related to the use of cryptography. These Guidelines - although non-binding - present the first attempt at international level to give policy orientations on several aspects of cryptography, including both encryption and digital signatures. The *Bonn Ministerial Declaration* of July 1997 also stressed the necessity of a legal and technical framework for digital signatures at European level as well as the importance of the availability of strong encryption technology for electronic commerce[5].

In its April 1997 Communication on Electronic Commerce, the *Commission* announced the intention to prepare a policy aiming at guaranteeing the free movement of encryption technologies and products as well as to propose a specific initiative on digital signatures. As announced the present Communication aims at developing such a policy framework with a view to:

- establishing a European framework for digital signatures;
- ensuring the functioning of the Internal Market for cryptographic products and services as well as products and services incorporating cryptographic techniques, while respecting public security concerns and contributing to a homogenous security area in the EU, as set out by the Amsterdam European Council[6];
- stimulating a European industry for cryptographic services and products;
- addressing the international questions raised by the global nature of the Internet and other electronic networks, in particular by removing trade barriers for cryptographic services and products and achieving as far as possible end-to-end communication security on a global scale;
- providing the basis for integration of cryptography within the framework of other European policies such as protection of privacy, consumer interests and intellectual property rights;
- stimulating and enabling users in all economical sectors to benefit from the opportunities of the global information society which can only be fully exploited if based on a framework of trust and security.

Discussions about the possible conflict between divergent interests on security have shown a considerable amount of confrontation and discontent between institutions and interest groups. This Communication is therefore also meant to contribute to a better understanding of the underlying issues and of the growing importance of cryptography for the information society.

II. Authentication and Integrity: Digital Signatures

Transmitting data in electronic form has many advantages compared with traditional methods. Documents can be made available almost instantly and in any quantity and the recipient is able to work on them directly. Transmission is considerably cheaper and faster - documents can be sent around the globe in a matter of seconds, without delay. However, authentication and integrity services are needed for secure and trustworthy data transmission and communication over open networks.

The speed of technological progress implies that many of the potential application fields for authentication and integrity services are difficult to ascertain at this stage. New application areas (e.g. protection of intellectual property rights, stored data, network security or electronic cash) are developing continuously. In particular for electronic communication digital signatures are considered to play a significant role.

[3] European Parliament Resolution A4-244/96, 19.9.96, OJ320, p.164, 28.10.96

[4] Council Resolution Nr. 96/C 376/01, 21.11.96 on new policy-priorities regarding the information society, OJ C376, 12.12.96

[5] European Ministerial Conference, Bonn 6-8.7.97, http://www.echo.lu/bonn/conference.html

[6] Presidency Conclusions on freedom, security and justice, Amsterdam European Council, 16/17.6.97 (http://ue.eu.int/amsterdam/en/conclusi/conclusi.htm)

1. Digital signature: what it is and how it works

(i) Several different methods exist to sign documents electronically varying from very simple methods (e.g. inserting a scanned image of a hand-written signature in a word processing document) to very advanced methods (e.g. using cryptography). Electronic signatures based on "public key cryptography" are called digital signatures and widely considered as crucial for a variety of applications [for a more detailed description see **Annex I**]:

- digital signatures used for *official communication* with public institutions (e.g. calls for tender, exchange of application forms, identity documents, tax declarations, transmission of legal documents);
- digital signatures used for *contractual relations* in open networks (e.g. electronic buying and selling, financial transactions);
- digital signatures used only for *identifying or authorising purposes* (to be certain of the identity of a correspondent or of his specific attributes e.g. an authorisation to log into a computer system, identification of Web servers);
- digital signatures used in *closed systems* (e.g. a corporate Intranet);
- digital signatures used *for personal purposes*.

(ii) In electronic communication, the concept of digital signatures is linked to the notion of data transmission using a kind of electronic seal which is affixed to the data and which allows the recipient to:

- verify the origin of the data, i.e. the use of a key assigned to a certain sender (*authentication of data source*),
- check that data are complete and unchanged and thereby safeguard their integrity (*integrity of data*).

Technically speaking, digital signatures are usually created and verified by asymmetric cryptographic techniques similar to those used for encryption. Two complementary keys are generated and assigned to a user. One of them - a signature key - is kept private (*private key*) whereas the other - a signature verification key - is published (*public key*). It is of course crucial that the private key cannot be computed from the public key.

(iii) Contrary to cryptography used for confidentiality purposes, digital signatures are annexed to the data and leave the content e.g. of the signed electronic document or the electronic transaction intact. Of course, the data can in addition be encrypted as described and discussed in chapter III. The cryptographic technology is used to protect against the illicit use of signatures in an electronic environment. Technical means exist to signal when keys are being used for functionalities other then the one for which they have been generated (e.g. a key issued for authentication for confidentiality purposes).

(iv) With the help of the sender's public key the recipient can find out whether the signed data has been altered and check that the public and private key of the sender are a complementary key-pair. Even the smallest change of the data would be discovered immediately. What appears to be a relatively complicated mathematical process is in practice carried out in a matter of seconds by the computer. The user therefore would not notice the underlying computing process.

(v) Verification of the authenticity and integrity of data does not necessarily prove the identity of the owner of the public key. How does for instance the recipient of a message know that the sender is really the one he claims to be? The public key may be attached to the message or be published in a directory, but what degree of confidence can the recipient have? Anyone can publish a public key under another name. The recipient may therefore wish to obtain more reliable information on the identity of the key owner. Such information can be given by the key owner himself, issuing the recipient with satisfactory proof. Another way is to have it confirmed by a third-party (e.g. a person or institution mutually trusted by both parties).

In the context of digital signatures these third-parties are most commonly so-called *certification authorities*.

2. Certification authorities (CAs)

The provision of public certification services is a completely new service sector. Although still in its infancy this sector is already raising a lot of interest. The sector is currently dominated by commercial undertakings based outside Europe,

although some European companies have also emerged. A significant number of new entrants will appear on the market very rapidly. They seem to focus on their national market and do not, at least initially, target markets in other EU Member States. This hesitation is also linked to legal uncertainties.

CAs can perform a range of functions with regard to digital signatures. Sometimes, publications refer to them as Trusted Third Parties (TTPs). However, TTPs which in general may provide a wide range of services very often are perceived to stand for lawful access to encryption keys [see **Annex III**].

While it is not excluded that TTPs also act as a CA - as described in this paper - the functions of both institutions are considered to be different. In particular CAs are crucial for digital signatures to become a fully accepted tool within national legal systems, for instance, to ensure legal recognition and enforceability of a signature in electronic commerce. Therefore the role and the legal basis for CAs and TTPs need to be distinguished from a regulatory standpoint.

2.1. Certification

One central task of a CA is to authenticate the ownership and the characteristics of a public key so that they can be trusted. Once a CA is satisfied that the ownership and the characteristics of a public signature key are correct, a certificate is issued containing this key and other details. This certificate is itself digitally signed i.e. the CA signs the certificate with its private key to establish the correlation with the key owner. When the CA's public key is added, a simple automatic verification is possible. However, it is necessary for the recipient to trust the CA, in other words a CA must be mutually trusted by both parties.

As a result, several categories of certificates are technically conceivable, e.g. the CA's public key can be signed by another CA leading to a certification hierarchy. It would also be possible to have the public key certified by several different CAs.

2.2. Possible contents of a certificate

A certificate can contain a whole range of informations, going beyond the mere key allocation and precisely determining its use. Some additional information will always be necessary, e.g. the algorithm to be used or the certificate expire date. Other information may be voluntary and will depend on the purpose for which the key is to be used and the level of confidence or trust required of it.

Examples of a *certificate's contents*:

- name or pseudonym of the signatory
- name of the CA
- public key of the signatory
- algorithm
- type of key
- profession
- position within an organisation (e.g. complementary to a "limited partnership", executive vice-president of a "corporation")
- qualification, licences (e.g. attorney, doctor, haulage contractor)
- official approvals (e.g. catering permit, vehicle driving licences)
- limits of liability (legal limits e.g. "commanditaire "of a "limited partnership" or voluntary limits)
- cover limits (e.g. insurance, deposits)
- confirmation that in the case of disputes pseudonyms are revealed
- certificate expire date

This might lead to a variety or different classes of certificates. For instance, a key used to authorise a large financial transfer between two banks will require a high level of trust whilst one used to validate a low value personal purchase will not need to be trusted to the same extent.

2.3. Key management

Key management implies an extensive task package, which can for instance include the generation and allocation of key-pairs, the identification of the owner, the creation of a public key directory and time stamping.

(i) Key creation and owner identification

The keys - which can also be generated by the user himself - must be effectively *unique* and tamper proof (which is practically given by the choice of an appropriate key length and generation procedure). Otherwise the digital signature cannot be allocated for legal relations in a reliable manner to data for which it has been generated and, via the key, to only one certain person or entity. This ensures that a key owner cannot refer to the fact that the digital signature was produced not with his key but with another one.

Keys may be allocated to private persons, legal persons (e.g. limited liability company) or to "entities without legal status" (e.g. department of an enterprise, working group). Keys can even be assigned to functional entities such as servers or PCs. Since the CA must guarantee the unique link between a key and its user, it has to identify the user in a reliable way and to hand out the key to the correct person.

(ii) Key directory

A directory of public keys may also be created providing information on the key owner, its validity period and other details, such as revocation. The key directory must always be kept up-to-date. Certificate revocation lists allow to determine whether a certificate has been revoked, suspended or reactivated. The effective operation of such a facility will depend on the speed and reliability of the cancellation procedure, which could be used in cases of invalidity of the certificate or loss and theft of the private key.

(iii) Time stamping

There are many situations in legal relations, where proof of the exact time of a certain action (transmission, creation or receipt of a document or the time at which a declaration of intent is made) is crucial. It is important to prove the exact time when a key was revoked to avoid liability for contracts signed with a compromised key. Therefore, digital time-stamping services able to reliably confirm the exact time of certain actions will be necessary. Time stamping services are also crucial for 'Intellectual Property Right' applications. These services could be provided by a CA, but of course also by another body.

2.4. Mutual recognition

In a fully international framework for electronic commerce certificates issued by foreign CAs must be mutually recognised in different countries. Thus the verification of any international certificate can be rapid and efficient. National structures could be complemented by a co-ordination mechanism at the European level. Such a concept is consistent with the Community's established negotiation strategy on mutual recognition and could encourage the development of certification services in Europe. Agreements with third countries will be both easier to secure and economically more beneficial if done on the basis of a common Community-wide regime.
Mutual recognition provisions in national laws could in principle facilitate cross-border trust. They would at the same time reduce potential EU Internal Market obstacles and enhance crossborder circulation of goods and services. The direct application of the Treaty (Art. 30, 52, 59, mutual recognition provisions in national legislation) could already lead to a satisfactory functioning of the Internal Market. Other possibilities of ensuring cross-border recognition of certificates could be harmonised European certification services (including the procedures concerning the issuance of such a certificate) as well as common evaluation criteria and procedures.

2.5. Privacy

Business partners sometimes do not have an interest in the precise identity of a particular person or entity, but only in the confirmation of previous contacts, in their affiliation to a defined group of persons, in their individual characteristics such as solvency and creditability or simply in unforged data.

Example: Credit card companies do not confirm the identity of the card-holder, but only whether this person has a certain line of credit.

Therefore in many cases people will have several key pairs corresponding to their different roles. Those persons not wishing or not obliged by law to communicate under their name can choose a pseudonym which safeguards their anonymity in transactions and communication (though the signatory is identified to the CA) whilst fully exploiting the integrity and authentication functions of digital signatures. This possibility is also required by the EU Data Protection Directive[7] and supported by the OECD Cryptography Policy Guidelines. Without such a privacy safeguard, digital signatures could be abused as an efficient instrument for tracing individual on-line consumption patterns and

[7] Directive 95/46/EC, 24.10.95 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, 23.11.95. See also Common Position 57/96, 12.9.96 with a view to the adoption of a European Parliament and Council Directive concerning the processing of personal data and the protection of privacy in the telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks, OJ C315, 24.10.96, which establish the specific rules for data protection and the right to privacy with regard to telecommunications networks.

communication or for intercepting, recording or misusing documents or messages.
There may be cases where the disclosure of pseudonyms may be necessary for reasons of public security and crime prevention. The EU Data Protection Directive lays down the conditions under which Member States may adopt measures restricting the right to remain anonymous.

Another privacy and data security concern results from the need that key pairs have to be unique and confidential in order to minimise the risks of "identity theft" and forgery. CAs must therefore be forbidden to store private keys. This again distinguishes CAs from TTPs which task is to keep information about private keys.

Since CAs must be able to identify the key owner and thus gather information about the individual, they are subject to the obligations concerning data processing, security and transfers to third countries laid down by the EU Data Protection Directive. For example, CAs can only collect and process personal data if the individual has given his consent or if they are authorised by law.

3. Legal Problems

While commercial products for digital signatures are already available in the market place, only a few companies in Europe have so far taken steps to offer services in this area. One of the main reasons is the weakness of demand resulting partly from the absence of legal recognition of digital signatures. Greater use of digital signatures requires adjustments and changes in many regulatory areas. In the current situation, the most important legal problems result from different national rules and regulations (or the lack of them), in particular the absence of common requirements for CAs, of technical and operational requirements to be met by certain categories of digital signature products, of liability rules and of legal recognition of digital signatures. The Commission will evaluate the possibility to provide for the harmonisation of the different national provisions to support international mutual recognition of digital signatures.

3.1.Elaborating Community requirements

At present there is no uniform legal framework specifying requirements for CAs in the European Union. This does not hinder CAs to be active on the market (there are already visible commercial activities in the US and also in the EU). But serious obstacles for cross-border trust would result from the lack of common rules.

> *Example*: Certificates issued by a CA in one Member State would not be recognised by a CA in another Member State, especially if one Member State has foreseen a licensing system for CAs and the certificate has been issued by a foreign unlicensed CA.

Establishing common criteria for the activities of CAs on Community level would allow certificates issued by a CA in one Member State to be recognised in all other Member States (mutual recognition). Since these problems and the risk that divergent national rules, or the lack of such rules, will hold back the functioning of the Internal Market and the development of electronic commerce, there is a strong case for a common legal framework to be established. A Community framework would enhance trust in digital signatures, whilst promoting their legal recognition. Such a framework could for instance establish principles for the activities of CAs.

> *Example* of fields where *common requirements for CAs* could be specified:
> - security of the CA and compliance with data protection legislation
> - reliable identification of a person (to make sure that key owners can be identified)
> - minimum insurance coverage (CAs must be able to pay in case they are liable)
> - technical components
> - qualification and security testing of personnel
> - no "self-certification" of the CA

In order to achieve the highest possible level of security, it would be appropriate to make a clear distinction between different tasks - e.g. certification or key administration - and between different certificates. The catalogue of the requirements can therefore be different - depending on the actual offer of services.

It would also be essential to establish common technical requirements for digital signature *products*, if national provisions (e.g. for key generation or storage) will not be mutually recognised and hinder the functioning of the Internal Market. Community harmonisation measures should be limited to establishing the essential requirements and leaving technical details

(e.g. through a mandate) to standardisation bodies.

3.2. Liability

Clear liability rules would contribute to the acceptance of CA services. However divergent levels of protection at national level could potentially act as a cross-border barrier to the provision of goods or services or to the use by public administrations of on-line services in a cross-border context. Liability questions may play a particular role in the relationship between users and CAs or between two CAs as well as with respect to licensing authorities (licensing CAs).

In all Member States, there are contractual rules connected to appropriate liability rules *between the user and the CA*. Liability depends very much on the concrete single cases. For instance, liability problems can be better managed if digital signatures are used within specific closed user groups.

Liability largely depends upon the concrete service offered by the CA as stipulated in the contract. A legal catalogue of requirements could form the basis for the contractual duties. It would also provide for both minimum and maximum liability of the CAs or guaranties, for example regarding the accuracy of the certificate or the correctness of the key directory. Certification practice statements, a detailed description of how certificate policies are implemented by a particular CA, could also play an important role as orientation for liability issues.

Normally there is no contractual relationship *between a CA and third parties*, like the recipient of a digitally signed message or another CA, who have confidence in the validity of certificates. Therefore Member States should examine whether there is a need for special liability rules.

Errors made by a *licensing authority* in the licensing process can be damaging to the user, the CA and third parties. Since the licensing authority has no contractual obligations and since the extra-contractual liability of public authorities is usually strictly limited, Member States should examine whether special rules for liability are necessary.

3.3. Legal recognition of digital signatures

The legal concepts behind signatures and the requirements on form and procedures, are different in each of the Member States jurisdictions. The differences, particularly in the field of civil and procedural law, have to be analysed. Member States should be encouraged to scrutinise the relevant national laws and regulations for provisions which do not allow to exploit the potential of digitally signed documents (form, evidence).

When signing a contract using a digital signature, one is confronted with different questions: does a declaration of intent have a legal value? Does the signature meet legal requirements? Is a digitally signed document recognised as evidence in court?

(i) Declarations of intent

Legal practices have emerged in Member States over the years in connection with declarations of intent. These cannot simply be translated into the context of electronic communication since the way to make a declaration of intent differs substantially from the traditional form in some respects.

> *Example*: The delivery of a document in paper form requires more time than in the electronic form. One has to put the document into an envelope, apply a postage stamp and post it. In so doing, one still has time to reconsider one's decision. An electronic document on the other hand is delivered by simply pressing a key or button.

In particular in order to guarantee an appropriate protection against hasty decisions, Member States should examine whether specific requirements are needed regarding the binding character of declarations of intent.

In addition, technical solutions must be found to make sure that users sign a document in the version which is actually visible on their screen.

> *Example:* Technically, substantial differences may exist between the document visible on the screen and the document which is actually signed or printed, e.g. if the programme works with associated files.

(ii) Non-repudiation of digital signatures

Even when a key pair has been assigned in total trust to a certain person, this does not prove that this person has actually signed a

given document. While the normal situation is that the key owner signs the document, a digital signature can in fact only be associated with certainty to a given private key. This presumption will only hold if it is certain that only the owner of the secret private key has full and unique control over his private key. Key escrow of private keys would endanger this presumption.

Example: Unlike conventional signatures, where the signatory signs with his own hand, digital signatures also allow a third - authorised or unauthorised - person to sign the document if this person is in possession of the private key, so-called "undisclosed" delegation.

Assignment is however possible if it can be legally presumed that the key owner signed himself. In that case the owner might wish to be legally liable only to a certain extent (e.g. within a limit, as with a credit-card). Member States should therefore consider appropriate legal rules.

(iii) Legal treatment of references

In order to carry business transactions faster or for cost reasons, one can refer to documents which are not part of the electronically transmitted data itself, but which are stored in another place, e.g. reference to standard-form contract conditions, technical descriptions or plans.

Problems could however result from the fact that the technical possibility of referring to other documents does not meet the legal requirements that have emerged from traditional legal relations.

Example: In a sales contract, a computer company refers to the terms of delivery indicated on the company's Internet-homepage. Under which conditions do the terms of delivery become part of the contract? Do they have to be digitally signed as well?

Special rules in Member States' civil laws will therefore be necessary for the legal treatment of references in electronic legal relations. The most important point is that references do not have other legal effects than those they would have if they were contained in the document in question.

(iv) Legal effects

Ensuring equivalent legal effects for conventional hand-written and digital signatures is not easy to realise considering their different characteristics and their different ways of being materialised.

Examples:

- Unlike conventional signatures, it is not possible in the case of digitally signed documents to distinguish between an original and a copy.
- Each person only has one hand-written signature. However, a given person can have several key sets. Digital signatures are also different for each document signed.

However, these differences do not by any means prevent digital signatures from enjoying equivalent legal value for certain legal or judicial purposes. The legal effects of documents signed with digital signatures is implicitly linked with trustworthiness of CAs and is an indispensable condition for the development of legal electronic transactions. The starting points are:

- *Recognition as evidence in legal proceedings*

In some legal systems (e.g. Belgium, France, Greece) electronic documents, even if they digitally signed, could not be accepted as evidence in legal proceedings, because written evidence is required as soon as the value of, for instance, a selling contract is beyond a certain limit. Such restrictions are clearly detrimental to the use of digital signatures.

- *Recognition as an equivalent to written form*

The use of a written form can fulfil several functions, e.g. warning, proof or authenticity. Documents provided with a digital signature can likewise fulfil these functions provided that digital signatures are safe and reliable. If documents provided with a digital signature match the requirements of a written form, this will have a very favourable impact on their implementation in the legal framework.

Member States could also implement specific rules on an electronic form in their civil laws. Thus Member States would not have to change all their regulations on written form but would be able to introduce digital signatures only where they think it would make sense.

Legal domains in which no specific legal form is prescribed, but where, for example, the use of the written form is based on voluntary business practice, would greatly benefit in terms of security - thanks to the gain of confidence - from the legal recognition of digital signatures.

4. Regulatory considerations

(i) While digital signatures are currently a recognised answer to authentication and integrity questions, the market may come up with other solutions. Therefore regulation has to create on one side a clear framework to build trust in digital signatures, but on the other side also has to be flexible enough to react to new technological developments.

(ii) Regulation should not restrict, neither *de jure* nor *de facto*, the contractual freedom of parties. Therefore any regulation should be tailored to correspond to the different possible uses of digital signatures (see II.1.). Private use of digital signatures or use within closed-user groups, for instance, might escape specific regulation entirely. Well-identified cases could become subject to regulation, for example in official communication. In any case, it must be ensured that both regulated and unregulated digital signature schemes can co-exist and are interoperable.

(iii) Some Member States are in the process of introducing voluntary schemes, and others consider mandatory licensing schemes, to build trust in CAs and to encourage legal recognition of digital signatures. However, licensing is only one of the possible trust-enhancing methods Member States may apply to promote the use of legally valid digital signatures. Non-licensed, but highly regarded private or public organisations may as well be considered as a trusted CA.

(iv) In the context of licensing, it is important to distinguish clearly between on the one hand, the procedures and conditions governing the establishment of a CA, and, on the other hand, the conditions imposed on the different services provided by a CA. The Treaty Articles 52 and 59 apply to each of these situations. Different national regulatory approaches and the lack of mutual recognition of each other's regulatory requirements may easily lead, due to the inherent cross-border nature of digital signatures, to a fragmentation of the Internal Market for electronic commerce and on-line services throughout the Union.

(v) Restrictive practices with regard to the establishment of CAs, the services they provide, the cryptographic tools they use, etc. will be detrimental to the free circulation of goods and services within the Internal Market. They should not undermine the freedom of establishment, for example by discriminating without justification on the basis of nationality or by restricting without justification the number of those providing CA services. The scope and the timeframe of Community action would be determined by the need for harmonisation. Since mandatory licensing of CAs is not the only way to ensure compliance of CA's activities with public intentions of how to promote trust in digital signatures, an EU regulatory framework would have to provide for the co-existence of both licensed and unlicensed CAs. Such a framework should be put in place at the latest by the year 2000.

III. Confidential electronic communication: Encryption

1. The economic and societal importance of encryption

(i) An encryption algorithm transforms a plaintext into an unreadable ciphered text (encryption) and vice versa (decryption) using a special key. The economics behind encryption is to transform the problem of keeping thousands of messages secret into the problem of keeping a single key secret. A useful distinction can be made between *symmetric and asymmetric encryption algorithms* [see **Annex II** for more detailed explanation].

Symmetric algorithms use the same key for encryption and decryption. This means that communicating parties have to agree on a secret key in advance. The disadvantage is that they have to find a secure way to exchange this key. This is particularly cumbersome in an open environment with many participants that may not know each other beforehand. This disadvantage is avoided in *asymmetric encryption methods* that use different keys for encryption and decryption.

At present, encryption provides the most important tool to keep electronic communication and electronically stored

documents confidential. Although new technologies will emerge sooner or later, it can be expected that encryption will remain the cornerstone for most confidentiality services on open networks for the foreseeable future.

Encryption has a long tradition in the defence area. However encryption technologies are increasingly integrated into commercial systems and applications.

Examples:

- Digital mobile telephones enjoy, thanks to encryption, stronger protection .
- Banks use strong encryption for financial messages (e.g. the S.W.I.F.T system).
- Pay-TV can only function commercially thanks to encryption which can then be decrypted on payment of a subscription fee.[8]
- Digital versatile disks (DVD), which will replace the previous video cassettes, use encryption techniques to prevent piracy in order to protect intellectual property rights.

(ii) The above examples already show that the exclusive character of encryption belongs to the past. They also show that increasingly encryption technology is integrated into products primarily to protect, for example, Intellectual Property Rights or to avoid fraud. Moreover, the fast growth of the Internet will create a fundamental change in the use of encryption: it will become an integral part of personal and business computing.

Computer stores sell cryptographic products and more and more people simply down-load encryption software from the Internet which can be easily installed on a normal PC. The integration of complete cipher machines on smart cards is a reality. PCs could be delivered with standardised smart card readers and fast crypto-chips. Various universities in the world teach cryptology and hundreds of companies in Europe and even more world-wide develop, produce and sell products and systems to be used for encryption.

A survey has identified not less than 1,400 encryption computer products world-wide[9].

[8] The protection of such encryption systems against piracy varies in Member States. The Commission has presented a proposal for a Directive aiming at establishing a Community-wide equal level of protection (COM(97)356, 9.7.97)

[9] Survey conducted by Trusted Information Systems,http://www.tis.com/docs/research/crypto/survey/ index.html

More than 400 companies from the US and about 440 companies outside the US, many of them in Europe, now offer encryption products[10]. Involved in this process are incumbents like computer, software and telecommunication companies as well as high-tech start-ups. Most of the young companies are growing fast: numerous examples exist where the annual growth rates of turnover or employment are 100% and even more.

(iii) Electronic commerce and many other applications of the information society will only expand and unfold their economic and social benefits if confidentiality can be assured in a user-friendly and cost-efficient way.

Examples:

- When using services such as tele-shopping or tele-banking, the consumer needs to be ensured that personal data such as credit card numbers are kept confidential.
- Data protection laws require safeguards like encryption to ensure privacy.
- In storing secret data and in carrying out sensitive business communication (project details, bidding information, research results, etc.) over open networks, companies wish to be protected against industrial espionage.
- Health care telematic applications must not allow for disclosure of medical histories of patients to unauthorised persons.

Cryptographic technologies are flexible, support a wide range of applications and minimise transaction costs on open networks. Continuous progress in digital technologies will make computing crypto-algorithms even more cost-efficient. European companies have developed substantial capabilities to integrate high-quality cryptographic features into their products and services. As demand for products with encryption is now growing very fast world-wide, it provides substantial opportunities for the industry and job creation in Europe.

Furthermore, the application of cryptographic products and services will have an enabling effect in all sectors of economic and social activity. Without this

[10] see also Computer Systems Policy Project CSPP: *"Perspectives on security in the information age"*, January 1996. CSPP is an affiliation of chief executive officers of leading American computer companies - http://www.podesta.com/cspp.

widescale deployment, the ability to create new, more competitive forms of business and new forms of social interaction will be substantially inhibited.

(iv) International treaties, constitutions and laws guarantee the fundamental right to privacy including secrecy of communications[11]. Consequently, in the current shift from off-line to on-line information flows, 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. Therefore, the debate about the prohibition or limitation of the use of encryption directly affects the right to privacy, its effective exercise and the harmonisation of data protection laws in the Internal Market.

2. Regulation of encryption: Potential impact on the Internal Market

2.1. Export control measures

Concerns over foreign threats to national security have been the primary motive for export controls. Whilst countries want to protect their own military and diplomatic communication through encryption, the objective of export control is precisely to deny similar benefits of cryptography to foreign opponents, in particular if they do not have equivalent technical means. Therefore, export controls are in general designed to prevent international proliferation of certain encryption technologies.

Under the *Wassenaar arrangement on export controls for conventional arms and dual-use goods and technologies* (19.12.1995)[12], replacing the COCOM[13] list, a group of 28 countries apply export controls to encryption products.

Within the European Union, the *Dual-Use Regulation* of December 1994 establishes a common framework for exports of dual-use goods[14]. Certain encryption products may only be exported on the basis of an authorisation. In order to establish an Internal Market for dual-use goods, such export authorisations are valid throughout the Community.

Moreover, according to Article 19 of this Dual-Use Regulation, Member States exercise a licence procedure for a transitional period also for intra-Community trade for certain particularly sensitive products. For the time being this also includes encryption products. This means the Regulation obliges Member States to impose not only export controls (i.e. controls on goods leaving Community territory) on dual-use goods, but also intra-Community controls on cryptography products shipped from one Member State to another.

The Dual Use Regulation however does not fully specify the scope, content and implementation practices of national controls. Consequently, a large variety of domestic licensing schemes and practices exists. These divergences can lead to distortion of competition.

2.2. Domestic control measures

Law enforcement authorities and national security agencies are concerned that wide-spread use of encrypted communication will diminish their capacity to fight against crime or prevent criminal and terrorist activities. For this reason, in several Member States consideration is being given to how their encryption policy could develop in the future. This has led to national and international discussions about the need, technical possibilities, effectiveness, proportionality and privacy implications of such a regulation.

(i) Existing regulation within the European Union and the OECD

Whilst export control measures are internationally widely applied, up to now, domestic control of encryption is quite

[11] Art. 12 Universal Declaration of Human Rights, Art. 17 International Covenant on Civil and Political Rights, Art. 8 European Convention on Human Rights, Art. F(2) Treaty on EU, EU Data Protection Directive

[12] see http://www2.nttca.com:8010/infomofa/press/c_s/wassenaar.html; http://ideath.parrhesia.com/wassenaar/wassenaar.html

[13] *Co-ordinating Committee for Multilateral Export Controls* was an international organisation for the control of the export of strategic products and technologies to proscribed destinations. Members were to a large extent NATO countries but also others like Japan and Australia.

[14] Council Regulation (EC) 3381/94, 19.12.94 setting up a Community regime for the control of exports of dual-use goods, OJ L 367/1, 31.12.94. Council Decision 94/942/CFSP, 19.12.94 establishes the lists of dual-use goods covered by the Regulation, OJ L 367/8, 31.12.94.

exceptional. In fact, currently only one Member State of the European Union (France), applies a comprehensive cryptographic regulation[15]. Although there have been discussions in other Member States, only the United Kingdom has so far launched a Public Consultation on the regulation of TTPs for the provision of encryption services (but not for use of encryption)[16].

The international picture is quite similar. Looking at the OECD countries, besides export controls there are basically no domestic regulations implemented. In the US - where up to now no domestic regulation is in place - there is an intensive debate on several legislative initiatives. In taking up the developing debate on this topic in some OECD Member countries and trying to avoid obstacles to international trade and commerce resulting from divergent national policies, the OECD has adopted Guidelines for a cryptography policy.

(ii) Regulation of use of encryption

Regulation of use would mean to rule the use of encryption without an authorisation as illegal. Alternatively or additionally, supply and import of encryption products and services could be brought under an authorisation scheme. Authorisations would either be denied or granted under certain conditions, for instance to use only weak encryption or to sell only approved software. These conditions are scaleable to satisfy any perceived needs of law enforcement and national security agencies.

Such regulations could limit the use of encryption. In addition, divergence between regulatory schemes might result in obstacles to the functioning of the Internal Market, in particular for the free circulation.

Example:

If an encryption software company which can freely develop its products in its home country, must comply with specific technical or legal requirements in other Member States, this company has to produce at least two, if not more, different versions of its encryption software. The same situation occurs if enterprises want to offer cross-border encryption services.

Today, nobody can be totally prevented from encrypting data (criminals or terrorists also can use encryption for their activities[17]): Firstly, access to encryption software is relatively easy, for instance by simply downloading it from the Internet. Secondly, it is difficult to prove that a specific person has sent an unauthorised encrypted message. Electronic communication on open networks is not like an end-to-end telephone conversation where people can be identified for instance by their voice. Thirdly, encryption is also possible using steganographic methods[18]. These methods allow one to hide a message in other data (e.g. images) in such a way that even the existence of a secret message and thus the use of encryption cannot be detected.

As a result, restricting the use of encryption could well prevent law-abiding companies and citizens from protecting themselves against criminal attacks. It would not however prevent totally criminals from using these technologies.

2.3. Lawful access to encryption keys

The underlying principle of this approach is to require that products and services incorporating encryption allow access to the respective keys. This would permit government agencies to decrypt a ciphered text otherwise difficult or impossible to crack. Different technical and institutional ways to provide key access are being discussed. The two most known concepts are *key escrow* and *key recovery*. Broadly speaking, these concepts imply that copies (escrow concept) or information (recovery

[15] Loi N° 90-1170 of 29.12.90, JORF 30.12. 90; Decret N° 92-1358, 28.12.92, JORF 30.12.92 ;. Delivery, exportation and use of cryptography are subjected to previous declaration if the cryptography can have no other object than authenticating communications or assuring the integrity of transmitted messages, and previous authorisation by the Prime Minister in all other cases. This law is currently being modified according to loi N° 96-659, 26.7.96 de réglementation des télécommunications art 17; http://www.telecom.gouv.fr/francais/activ/telecom /nloi17.htm

[16] Licensing of TTPs for the provision of encryption services - DTI Public Consultation Paper on detailed proposals for legislation, 3.1997; http://www.dti.gov.uk/pubs/

[17] Most of the (few) criminal cases involving encryption that are quoted as examples for the need of regulation concern "professional" use of encryption. It seems unlikely that in such cases the use of encryption could be effectively controlled by regulation; see also "Encryption and Evolving technologies as tools of organised crime and terrorism" by D.E. Denning and W.E. Baugh, Jr. http://guru.cosc.georgetown.edu/~denning/crypto/oc-abs.html

[18] see Annex II

concept) about relevant keys are given either directly to government agencies or to TTPs [see **Annex III**].

(i) Key access schemes are considered by law enforcement agencies as a possible solution to cope with issues like encrypted messages. However these schemes and associated TTPs raise a number of critical questions that would need to be carefully addressed before introducing them. The ongoing discussion of different legislative initiatives in the US is an illustrative example of the implied controversy. The most critical points are vulnerability, privacy, costs and effectiveness:

- Inevitably, any key access scheme introduces additional ways to break into a cryptographic system[19]. More people will know about "secret keys" and "system designs" leading to higher risks of insider abuse and the TTPs itself can become target for attacks. These new vulnerabilities are complex and need to be understood as substantial liability and privacy questions are implied.

- The costs associated with key access schemes can be very high. Up to now, questions on costs and who would bear them have not been addressed by policy makers. Important cost factors would be the specific requirements put on TTPs, e.g. response time to deliver keys, storage time for session keys, authenticate requesting government agency, secure transfer of recovered keys, internal security safeguards, etc.

  Furthermore, substantial and unknown costs would occur through the need for scaleability of key access schemes, i.e. making it work in a multi-million user environment. Up to now, such systems have at best been developed for small scale use. The costs to make them work on an economy of even global wide scale need to be looked at carefully.

- Key access schemes can be easily circumvented - even if, hypothetically speaking, everyone would be forced to pass through these systems.

Examples:

- Users could first encrypt the data with an unrecoverable key and later use a licensed escrowed encryption system. Unless encryption as such is forbidden, this would even be legal. Anyhow, such an operation could only be detected when an agency actually tries to decrypt the data. It is impossible to "scan" the network to detect the use of non-escrowed encryption. Therefore use of non-escrowed encryption would not even be able to act as a general indicator for possible illegal activities.
- Users could encrypt a relatively large number of session keys in a way that the previous key encrypts the next one, always using one or several official escrow/recovery systems. Only the last key would be used to encrypt the message. An agency would need to reverse this process and to obtain all keys in order to read the message; although technically feasible, this task would be extremely difficult to manage. To be noted, the users would have fully complied to a key recovery scheme.

(ii) Any involvement of a third party in confidential communication increases its vulnerability. The main reason for involving a third party in the management of keys for confidentiality is to allow that party to make the keys available to other than the two communicating parties, for example, to law enforcement.

Users may therefore not see many advantages in using TTPs for confidential communication, and probably not even for stored information. Regulators would thus need to offer incentives to convince users to use licensed TTPs for confidentiality purposes, for instance through a "public security label" or even by introducing a "mandatory scheme". Such a mandatory scheme would make any publicly available offer of encryption services subject to a licence that inter alia would demand key escrow/recovery.

The acceptance of such a system remains to be seen, but given its implied overheads, can not be regarded as an incentive for electronic commerce. In any case, restrictions imposed by national licensing schemes, particularly those of a mandatory nature, could lead to Internal Market obstacles and reduce the competitiveness of the European Industry.

[19] See for a comprehensive analysis the recently published study "The risks of key recovery, key escrow, and trusted third party encryption", http://www.crypto.com/key-study.

2.4. Privacy

Privacy considerations suggest not to limit the use of cryptography as a means to ensure data security and confidentiality. The fundamental right of privacy has to be ensured, but may be restricted for other legitimate reasons such as safeguarding national security or combating crime, if these restrictions are appropriate, effective, necessary and proportionate in order to achieve these other objectives. The EU Data Protection Directive harmonises the conditions under which access to personal data, their processing and transfer to third countries is lawful.

As regards data security the Directive requires Member States to provide that a data controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Cryptography is one important technical means by which data integrity and their confidentiality can be ensured. To ensure also the secure flow of personal data throughout the Internal Market, such technical means must be able to "travel" with the personal information they are securing. Any regulation hindering the use of encryption products and services throughout the Internal Market thus hinders the secure and free flow of personal information and the provision of related goods and services.

3. Assessment

Proposals for regulation of encryption have generated considerable controversy. Industry expresses major concerns about encryption regulation, including key escrow and key recovery schemes[20]. Although there is a lack of experience, as electronic communication and commerce have just begun to penetrate economy and society, a preliminary assessment can be made in order to build a common European understanding of the subject, in particular as Member States may have different views on security issues implied. Such an understanding could be founded on the following points:

(i) Problems caused by encryption to crime investigation and the finding of evidence are currently limited, but they may increase in the future. As with any new technology, there will be abuse of encryption and criminal investigations will be hindered because data was encrypted. However, widespread availability of encryption can also prevent crime. Already today, the damage caused by electronic crime is estimated in the order of billions of ECUs (industrial espionage, credit card fraud, toll fraud on cellular telephones, piracy on pay TV encryption). Therefore, there are considerable economic and legal benefits associated with encryption.

(ii) Criminals cannot be entirely prevented from having access to strong encryption and from bypassing escrowed encryption. Benefits of regulation for crime fighting are therefore not easy to assess and often expressed in a fairly general language. However control measures could make use of encryption for criminal activities more difficult and cumbersome.

(iii) In the information society, citizens and companies will increasingly carry out more aspects of their lives and business on-line. Through teleconferencing, tele-shopping, teleworking, electronic payment, e-mail, etc. a huge amount of information will be available electronically, in a way never experienced before. Therefore, if citizens and companies have to fear that their communication and transactions are monitored with the help of key access or similar schemes unduly enlarging the general surveillance possibility of government agencies, they may prefer remaining in the anonymous off-line world and electronic commerce will just not happen[21].

(iv) Key escrow or key recovery raise a number of practical and complex questions that policy makers would need to solve, in particular issues of privacy, vulnerability, effectiveness and costs. If at all required, regulation should be limited to what is absolutely necessary. Regulation would also

[20] see e.g. Industrial Declaration of the Bonn conference, July 97, http://www2.echo.lu/bonn /industry.html

[21] see Eurobarometer opinion survey 46.1 on privacy in the information society, January 1997

need to distinguish between a multitude of possible key types (storage keys, session keys, authentication keys, etc.) as there are important differences in their functionality.

(v) In the context of electronic commerce using open and global networks, the international availability, interoperability and choice of various encryption products and services is necessary. Any regulation hindering the use of encryption products and services throughout the Internal Market hinders the secure and free flow of personal information and the provision of related goods and services, and its justification needs to be examined in light of the Treaty and the EU Data Protection Directive

(vi) The ultimate objective for government agencies is to see plaintext and not necessarily to have access to keys. Furthermore traffic analysis (e.g. who communicates with whom?) is also important and would benefit from increased electronic communications. Information, even encrypted for communication, can often be found unencrypted at the source, just as with traditional forms of communication, for instance with banks, shops, travel agencies involved in communication with a suspect, or can be tapped unencrypted at certain points in a communication link. Therefore existing regulation on traditional forms of lawful access to data and communication could be explored with a view to effectively applying it to access to encrypted data and communication, e.g. regulation could require access provision to encrypted information upon legally authorised request.

(vii) A fundamental problem lies in international relations, i.e. how to ensure global communication in case key escrow/recovery regulation is introduced in some countries. Countries would probably insist that only national TTPs could hold keys of their citizens. For instance, in case of a session key recovery scheme that is linked to an e-mail communication, only the country of the sender could decrypt the message unless there is a special arrangement between the two countries.

(viii) Irrespective of the compatibility of restrictions with the Treaty provisions on the free circulation of goods and services, specific national controls on the use of encryption could also have a secondary effect on the free circulation of persons, similar to those already identified by the Veil Panel [22].

IV. Policy actions at Community level

Electronic communication via open networks is at the core of the information society. Fast and secure exchange of data offers many advantages for electronic commerce which can contribute decisively to improvements in competitiveness and job creation. The European Union has an early opportunity to create the conditions for a trend-setting infrastructure and for growth in European industry.

The Commission will seek to build trust in electronic communication via open networks to ensure the functioning of the Internal Market, to stimulate electronic commerce and to strengthen the European Industry.

1. Community framework for digital signatures

1.1. The need for European Union action

Detailed regulations for digital signatures are already under preparation in some Member States. France has already adopted a new Telecommunications Act, Germany a law on digital signatures[23], Italy a law on the use of electronic documents and contracts[24]. The UK Government has launched a Public Consultation on the regulation of TTPs. The Dutch Government has created an inter-departmental task force[25]. Denmark and Belgium[26] are also preparing draft legislation on digital signatures. The Swedish government organised a public hearing in June 1997.

Whilst the development of a clear framework is welcomed, the very divergent legal and technical approaches which have already appeared and the absence of any legal environment in other Member States - also possibly justified - might constitute a serious

[22] Report of the High Level Panel on the free movement of persons, chaired by Mrs. Simone Veil, presented to the Commission, 18.3.97
[23] Gesetz zur digitalen Signatur (SigG), 1.8.97; http://www.iid.de/rahmen/iukdgbt.html#a3
[24] Schema di Regolamento "Atti, documenti e contratti in forma elettronica", approved by the Italian Council of ministers, 5.8.97
[25] Staatscourant nr. 54, 18.3.97
[26] see http://www.agoraproject.org/

barrier to doing business and communicating throughout the European Union. This will undermine the free circulation of digital signature related products and services within the Internal Market as well as the development of new economic activities linked to electronic commerce. In order to stimulate electronic commerce and the competitiveness of the European industry as well as to abolish the free circulation obstacles and to facilitate the use of digital signatures across national borders, a common framework at Community level is urgently needed and should be put in place at the latest by the year 2000.

1.2. Scope of a Community framework

The goal of any Community initiative must be to encourage Member States to rapidly implement appropriate measures to build trust in digital signatures. The Commission therefore considers proposing - in the context of the Amsterdam Treaty - first pillar legislation on the basis of this Communication. The following steps would be necessary from the Commission's point of view:

(i) Common legal requirements for CAs

Common European certification requirements are crucial. By establishing defined common criteria for the activities of CAs, the Community could put in place a framework allowing that certificates issued by a CA in one Member State are recognised in all other Member States. A Community framework would have to refer particularly to the *setting of common requirements for the establishment and operation of CAs* allowing for the co-existence of licensed and non-licensed CAs. Common classes of certificates may also be needed so that the levels of assurance and trust for certificates are the same in all Member States. Detailed implementation and the means of applying such rules (licensing regime, self-certification) would be a matter for Member States to decide.

To support international mutual recognition of digital signatures the Commission will furthermore identify the need for common technical and operational requirements as well as common evaluation criteria and procedures, including standards, concerning digital signature *products*.

(ii) Legal recognition

In order to achieve as wide as possible acceptance of digital signatures, national legal systems may need to be adapted to ensure that they offer the same recognition and treatment to digital signatures as to conventional signatures.

The Commission will complete its currently ongoing assessment of the need to provide for the legal recognition of digital signatures at Community level. The different national provisions inhibiting the full exploitation of digitally signed electronic documents (form requirements, evidence rules), on the basis of which further proposals for action will be made will also be taken into account. Legal form requirements and the validity of signatures as evidence in legal proceedings should rapidly be submitted to examination by justice ministers.

(iii) International co-operation

Electronic communication is not limited to the European Union. Therefore - where appropriate - a framework must be developed at an international level once a Community position has been established. This requires participation of Europe (both on Community and on Member States level) in international initiatives and fora.

Many of such *international initiatives* have been initiated at different levels. Bilateral (*EU/US*, *EU/Japan*) and multilateral (e.g. *UNCITRAL*[27]) discussions have started. *UNCITRAL* has completed the work on a Model Law on Electronic Commerce[28] and has recently initiated subsequent work aiming at the preparation of uniform rules on digital signatures and the related (cross-border) services (CAs). Work in the *OECD* based on the Guidelines for cryptography policy is continuing. Other international organisations, such as the WTO, may become involved with regard to avoiding trade obstacles and other aspects related to their specific area of competence and expertise.

In the *United States*[29] almost all States have either started working on or have already legislation on digital signatures. Agencies, such as the Food and Drugs Administration,

---

[27] United Nations Commission on International Trade Law

[28] http://www.un.or.at/uncitral/index.html

[29] An update on the status of US legislation can be found on http://www.mbc.com/ds_sum.html

are promulgating regulations specific to their area of responsibility[30]. At the federal level, Congress is considering several legislative initiatives. In *Japan*, some technical and regulatory activities in the area of authentication and electronic transactions have been launched earlier this year.

At the *business level* the American Bar Association produced the "Digital Signature Guidelines"[31] and the Internet Law and Policy Forum (ILPF) is working on the role of CAs in consumer transactions[32].

In view of these world-wide activities the Commission recommends that the Community continues and initiates the dialogues on international level. The goal must be to remove existing obstacles in order to create an internationally compatible framework for electronic commerce, in particular to establish common technical standards and mutual recognition of certificates.

2. Policy orientations in the area of encryption

(i) The EC Treaty and the Treaty on the European Union fully respect the competence of Member States with regard to the areas of national security and law enforcement. If national restrictions are put into place they have to be compatible with Community law. Therefore the Commission will examine whether national restrictions are totally or partially justified, notably with respect to the free circulation provisions of the Treaty, the case law of the Court of Justice and the requirements imposed by the Data Protection Directive.

- National restrictions must respect the principle of proportionality (be appropriate, effective and not go beyond what is necessary for attaining the objective pursued).

- Member States already have to communicate to the Commission and through it, to the other Member States their intended technical rules, the observance of which is compulsory, *de jure* or *de facto*, in case of marketing, use, manufacturing or importation of a product, cryptographic products including[33]. This procedure enables the Commission, and the Member States, to identify those rules which, once adopted, will create Internal Market obstacles, and to take appropriate action, either issuing comments, a detailed opinion or by proposing Community measures.

- It will be important to distinguish "authentication and integrity services" from "confidentiality services", because different rules and goals separate, as identified above, these two aspects.

Potential impacts on trade and competitiveness will also be important considerations.

(ii) The Dual-Use Regulation should be adapted in view of the requirements for the cryptographic products market. Article 19 imposing national controls also contains a provision to re-examine the need for these controls within three years from the date of entry of the Regulation (by the end of 1997). Therefore, when the Dual-Use Regulation is reviewed it could be improved by:

- progressively dismantling intra-Community controls on commercial encryption products (i.e. not necessarily for very advanced encryption);
- launching a discussion on the scope and interpretation of certain provisions, such as the so-called "General Software Note" (stipulating that public domain software is not subject to controls);
- dealing with problems like intangible means of transmission (e.g. transmission of technology by fax or e-mail).

(iii) To create an appropriate and balanced regulatory framework within the Community, the Commission invites and supports Member States to enhance co-operation of police forces on a European and international level.

(iv) Given the global dimension of electronic communication and commerce, international agreements may be necessary between the Community and other countries, once a harmonised system has been put in place. The goal must be to remove existing obstacles in order to create an internationally compatible framework for electronic commerce, in particular to

[30] http://www.fda.gov/cder/esig/part11.htm
[31] http://www.abanet.org/scitech/ec/isc/dsg_tutorial.html
[32] http://www.ilpf.org/work/ca/draft.htm

[33] Council Directive 83/189/EEC, 28.3.83 laying down a procedure for the provision of information in the field of technical standards and regulations; OJ L109, 26.4.83

establish common technical standards and mutual recognition of certificates.

(v) The Council is also invited to initiate a debate on encryption issues.

3. Accompanying measures

(i) Interoperability

Interoperability between different encryption and digital signature applications and systems is absolutely necessary to ensure that they can be applied in and outside Europe. Services are mostly achieved by agreed standards including test criteria and procedures covering protocols, data formats and program interfaces.

By using agreed protocols and data formats it is not necessary to develop gateway services or conversion programs changing one format to another. Interoperability in a broader sense also means that application solutions can be moved from one type of software and hardware environment to another (portability) and that users can move from one place to another and still access the same trusted services (mobility).

Examples for work on standards:

- The most widely known format of certificates is X.509 v3 [34].
- The Secure Electronic Transactions (SET) standard is a protocol used by industry and designed to safely transmit sensitive personal and financial information over public networks.
- At the international level, the Internet Engineering Task Force (IETF) [35], ISO/ITU [36] and the World Wide Web Consortium (W³C) [37] are working on standards concerning public key infrastructure, certificates and digital signatures .

In order to meet the legal and market requirements, technical and management standards developed in an open, market-driven manner are needed to support interoperability. Management standards can be helpful for the operation of CAs. Technical standards are for instance necessary for digital signature and certificate formats as well as for time-stamping services and smart cards. Standards must correspond to the best current practice.

The Commission encourages industry and international standards organisations to develop technical and infrastructure standards for digital signatures and encryption to ensure secure and trustworthy use of networks and respect privacy and data protection requirements[38]. The Commission will consider specific mandates on standardisation and propose, in close co-operation with the Member States, industry as well as the user community (business, consumers, citizens) measures which will support the work in this field.

(ii) Support programme

The Commission is ready to support the development of cryptographic services, in particular it is considering proposing a Council and Parliament Decision for an INFOSEC II programme building on the INFOSEC programme carried out from 1992 until 1994[39]. The programme could aim at developing overall strategies for the security of electronic communication, in particular with a view to provide users and producers of electronic communication with appropriate protection systems.

(iii) Research projects

The Commission will continue the current projects in the field of digital signatures and encryption within the 4th framework programme for Community activities in the field of research and technological development (1994 - 1998) [see **Annex IV** for a list of ongoing projects] and will launch new projects within the 5th framework programme (1998 - 2002). Notably the proposal for the 5th framework programme foresees a key action on electronic commerce. Special importance will be attached to techniques aiming at interoperability and enhancing privacy, to stimulating best practice and encouraging its widescale deployment.

[34] The v3 version has built-in additional extension fields, which can convey additional subject identification, key attribute or policy information. It is still necessary to specify a profile for use of the extensions tailored for the Internet.
[35] Public-Key Infrastructure (X.509),ftp://ds.internic.net/internet-drafts/draft-ietf-pkix-ipki3cmp-04.txt
[36] X500 and ISO9594 series; ftp://ftp.bull.com/pub/OSIdirectory/ITU
[37] W³C Digital Signature Initiative, http://www.w3.org/Security/DSig/Overview.html

[38] see Bonn Ministerial declaration, footnote 6
[39] http://www.cordis.lu/infosec/src/itsede2.htm

(iv) The use of digital signatures and encryption by public authorities

In the near future, government administrations will use digital signatures and encryption for internal purposes or in their relations with business and citizens. Such use may require adaptations to national as well as Community laws, regulations and administrative procedures. The first Community Regulation[40] has been modified in order to allow the use of digitally signed electronic documents. The impact of national measures has to be monitored in order to identify problem areas which may require a Community intervention. Also the Union's institutions will use digital signatures[41] and encryption.

(v) European Internet-Forum

The Commission will create by the end of 1997 an electronically based European Internet-Forum as a means to exchange information on the regulatory and user aspects of digital signatures and encryption.

(vi) International hearing

The Commission intends to organise beginning of 1998 a hearing about the topic "digital signature and encryption". The aim is to consult governments, industry and consumers on which measures they feel the Community should take into consideration in order to

- enhance the trust in legally valid and user-friendly digital signatures as well as in secure communication;
- abolish identified Internal Market obstacles related to provision and free circulation of cryptographic goods and services;
- provide adequate protection of privacy of individuals and their personal data.

[40] Council Regulation (EC) N° 1290/97, 27.6.97 amending Regulation (EEC) N° 1408/71 on the application of social security schemes to employed persons, to self-employed persons and to members of their families moving within the Community and Regulation (EEC) N° 574/72 laying down the procedure for implementing Regulation (EEC) N° 1408/71 OJ L 176, 4.7.97, P. 1 insertion of a new paragraph in Article 85 ensuring that documents exchanged by electronic means are given the same status as paper documents

[41] SINCOM, the budget management application of the Commission, introduces smart cards for digital signatures purposes

4. Timeframe for Community action

4.Q./1997:	European Internet-Forum
4.Q./1997:	Commission proposal to amend the Dual-Use Regulation
1.Q./1998:	International hearing
1.Q./1998:	Assessment of the comments on the Communication, the results of the Internet-Forum and the international hearing
2.Q./1998:	Proposal for further action (e.g. Directive on digital signatures)
2.Q./1998:	Proposal for an Infosec II programme
1998-2002:	Projects within the 5th framework programme
by 2000:	Common framework for cryptography put in place throughout the Union

EUROPEAN COMMISSION

COMMUNICATION
FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

ENSURING SECURITY AND TRUST IN ELECTRONIC COMMUNICATION

TOWARDS A EUROPEAN FRAMEWORK FOR DIGITAL SIGNATURES AND ENCRYPTION

ANNEXES

TABLE OF CONTENTS

ANNEX I
Digital Signature

- **Usage**

Digital signatures can help to prove the **authenticity** and **integrity** of data. A secure digital signature system will consist of two parts: on one hand a method to sign a document in a "not forgery" way and on the other hand a method to verify that the signature was generated by whom it represents. The authentication protocols can be based on public key encryption systems (using asymmetric cryptographic algorithms). For a detailed description of symmetric and asymmetric cryptographic algorithms see **Annex II**.

A digital signature is a **string of data** created by using a private key. A public key can be used to verify that the signature was effectively generated by using the corresponding private key. It should be created in such a manner that it is impossible to create a valid signature without knowing the private key. The authentication of strings of data is a process where the receiver of, for instance, a digital message can be assured about the origin of a message.

The **string of data** can also contain pseudonyms or names to be used to read the identity of the sender. In addition the string can carry a timestamp to testify that a message (or document) existed at the stated time.

Digital signatures can also be used to certify that a certain public key belongs to a certain person.

- **Creation**

In order to create a digital signature, two steps are necessary. First the sender **computes with the help of software a digest** of the data containing its essential characteristics (so-called "hash function": a sort of short version of the data). Unlike the procedure when encrypting data to preserve confidentiality, **he encrypts the digest** - together with additional data, including place and time of the signature -**with his private key** and not with the public key of the receiver. Thus, the key does not serve to encrypt the plaintext itself, but only to encrypt the digital signature that is annexed to the readable data [for a detailed description see **Annex II**].

With the help of the sender's public key the receiver can find out whether the data has been altered. Technically speaking three steps are necessary: **firstly**, the public key of the sender is used to decrypt the digital signature and thus the digest. **Secondly**, the digest of the plaintext will be computed again by software. **Thirdly**, both computed digests are compared. Even the smallest change of the data would result in two diverging digests and therefore be discovered immediately (see Fig. 1).

Thus, the recipient of the data can now be sure that the transmitted data has not been altered and that the public and private key of the sender are a complementary key-pair.

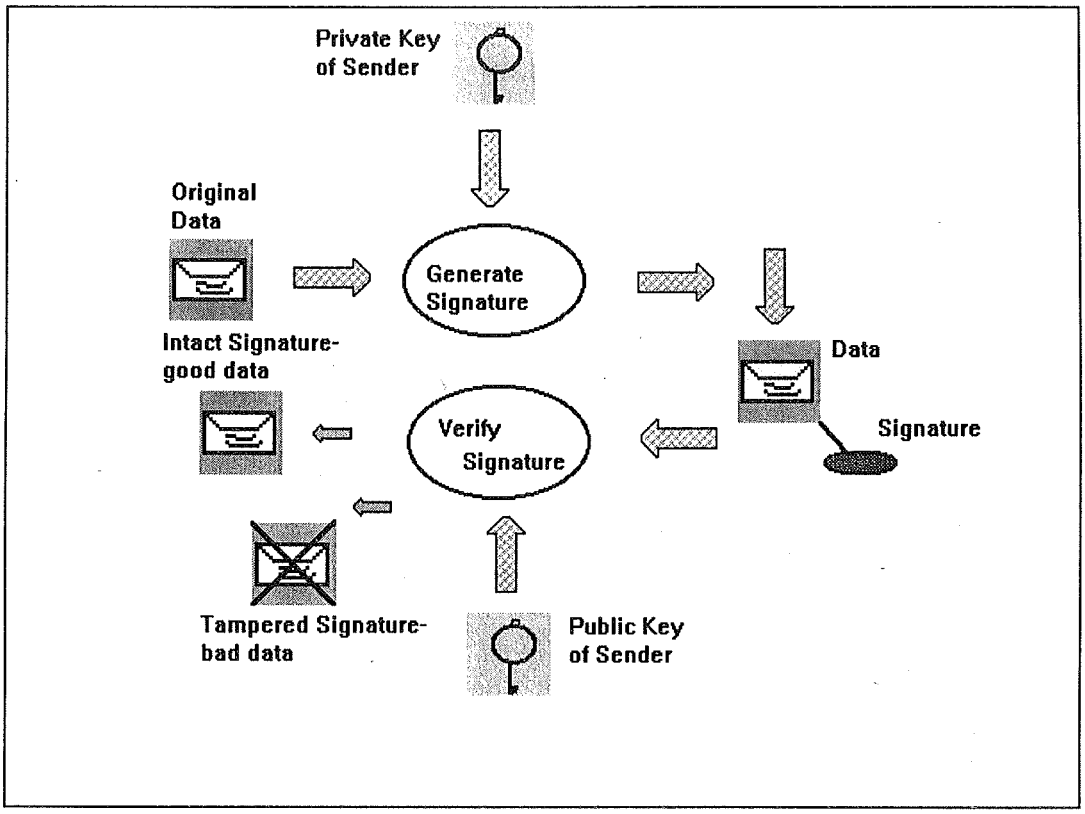

Fig. 1 Digital signature

• Hash functions

Hash functions are used to compute a data digest when making digital signatures. These functions map the data to fixed sized hash values in such a way that it would be extremely difficult to come up with a string of data that would match these particular hash values. The idea is based on the fact that a message digest represents concisely the 'original' data from which it was computed. It could be considered as a digital fingerprint of the 'larger' data string. As hash functions are a lot faster than the all data signing functions it is a lot more efficient to compute a digital signature by using the digest than using all the data.

To use the hash functions for digital authentication they must have certain properties to make them secure enough for cryptographic usage. It must be excluded that a data string can be found that hashes to a given value and that two distinct data strings hash to the same values. Cryptographic hash algorithms produce hash values of at least 128 bits.

To break into a digital signature system attacks may or will be directed at the mathematical string used by the digital signature system or the hash function used to make the data digest. In order to obtain an adequate security level it seems necessary to choose a digital signature system and a hash function that are evenly matched in difficulty to break. Attacks will take place on the weakest of both components. Therefore long modules and hash functions producing longer data digests should be used.

Examples: Message Digest-algorithms MD2, MD5 (128-bit values), Secure Hash Standards/Algorithms (SHS/SHA) and RIPEM 160.

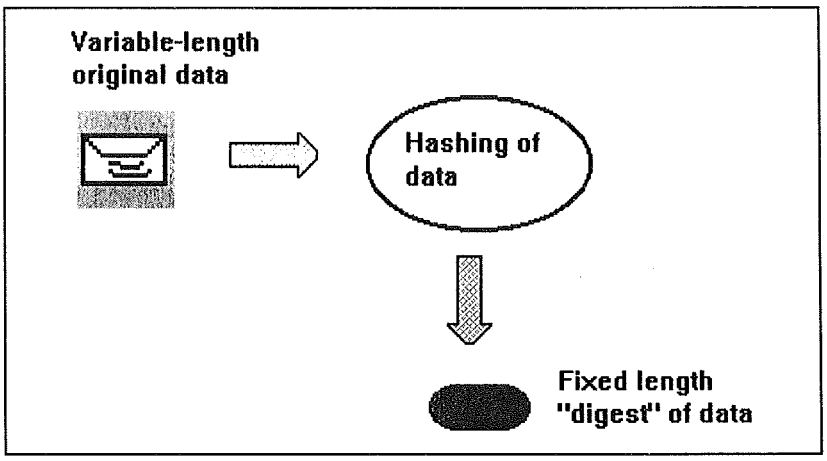

Fig. 2 Hash function

- **Overview of the different processing steps of a digital signature:**

- A unique cryptographic key pair is given or generated by the user.
- A string of data is prepared by the sender on a computer.
- The sender prepares a "data digest", using a secure hash algorithm. Digital signature creation uses a hash result derived from and unique to both the signed data and a given private key.
- The sender encrypts the data digest with his private key. The private key is applied to the data digest text using a mathematical algorithm. The digital signature consists of the encrypted data digest.
- The sender attaches his digital signature to the data or sends it separate.
- The sender sends electronically the digital signature and the (not-encrypted or encrypted) data to the receiver.
- The receiver uses the sender's public key to verify the sender's digital signature. Verification using the sender's public key proves that the data came from the sender.
- The receiver creates a "data digest" of the data, using the same secure hash algorithm.
- The receiver compares the two data digests. If they are exactly the same (without a "bit" of difference) the receiver knows that the data has not been altered after it was signed.
- The receiver obtains a certificate from a Certification Authority (or from the sender of the data). It confirms the digital signature on the sender's data. The certificate contains the public key and name or pseudonym of the sender (and eventual additional information), digitally signed by the certification authority .

- **Open network security**

As the TCP/IP (Transmission Control Protocol/Internet Protocol) was not designed to offer secure communication services over the Internet (the Internet Protocol version 6 currently under development, will include some security oriented features) additional security technologies are needed to tackle the increasing security concerns.

Secure electronic infrastructures are mainly based on SSL (Secure Sockets Layers), SET (Secure Electronic Transactions) and S/MIME (Secure Multipurpose Internet Mail Extensions). These industry-standard protocols provide the basis for a wide variety of security services (digital signatures, message integrity verification, authentication and encryption).

The most commonly used browsers (Netscape Navigator and Microsoft Internet Explorer) exploit most of these possibilities together with the use of SSL-capable servers from the leading vendors. Additional security features requested by specific computer applications can be incorporated by other API (Application Program Interface), Java scripts, Java-applets, Visual Basic, C/C++ or other programming languages.

***

ANNEX II
Symmetric and asymmetric encryption

• What is encryption?

Encryption is the transformation of data into a form unreadable by anyone without a decryption key. Cryptographic algorithms are used to transform plaintext data into encrypted data. The act of transforming the information is called The process of transforming data back into plaintext is called **decryption**. The purpose of encryption is to ensure confidentiality by keeping the information hidden from anyone for whom it is not intended, even for those who can see the encrypted data. It addresses the data protection and privacy issues, including data integrity and confidentiality, and allows secure communication over insecure channels.

There are two basic types of encryption: **symmetric and asymmetric**.

• Symmetric (or secret key) encryption systems

In **symmetric** encryption systems one key is used both to encrypt and decrypt data. To provide security for the information, the key needs to be kept as a secret between parties involved. Symmetric encryption is suitable for transforming large amounts of data since computations are performed rapidly. Management of the distribution and use of the secret key is critical as the key is vulnerable in transit to the other party.

Examples of symmetric algorithms: the Data Encryption Standard (DES) algorithm, Fast Encryption Algorithm (FEAL), International Data Encryption Algorithm (IDEA), RC4 and RC5, Secure and Fast Encryption Routine (SAFER)

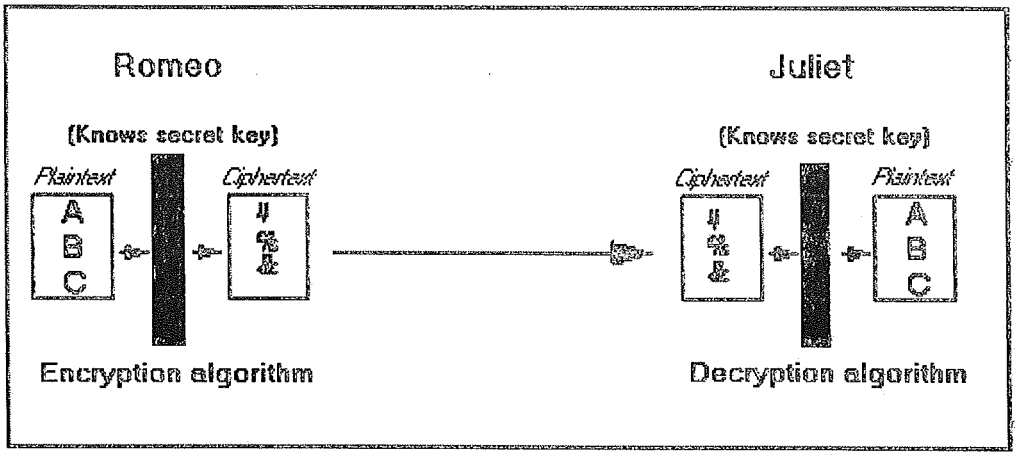

Fig. 3 Symmetric encryption

• Asymmetric (public key) encryption systems

Asymmetric encryption systems are based on the use of two keys in a single cryptographic operation: one key to encrypt, another key to decrypt. The encryption key is called the public key, the decryption key is called the private key. These keys are related in a complex way. A message encrypted with a particular public key can only be decrypted by using the corresponding private key; like data encrypted with a private key can only be decrypted by using the corresponding public key.

Examples: the RSA public key algorithm, Diffie-Hellmann.

The private key should be stored securely in a protected medium such as a smartcard, a portable computer or a smartdisk. The most common hardware solution will probably be the smartcard as the private key cannot be separated from the card and is difficult to copy. In addition the use of smartcards can be protected, for example using a PIN-number or a finger print matching technique. The public key, as the name already indicates, is published and accessible to everyone. Therefore asymmetric algorithms are often called public-key algorithms.

Example: If someone, say Romeo, wants to send a confidential message using a public-key mechanism to someone else, say Juliet, he needs to encrypt the plaintext, probably something like "I love you", with her public key. He could send the encrypted message safely over an unsecured network as only Juliet can decrypt the ciphertext with her private key. Thus, public-key cryptographic systems open the use of encryption to huge user groups.

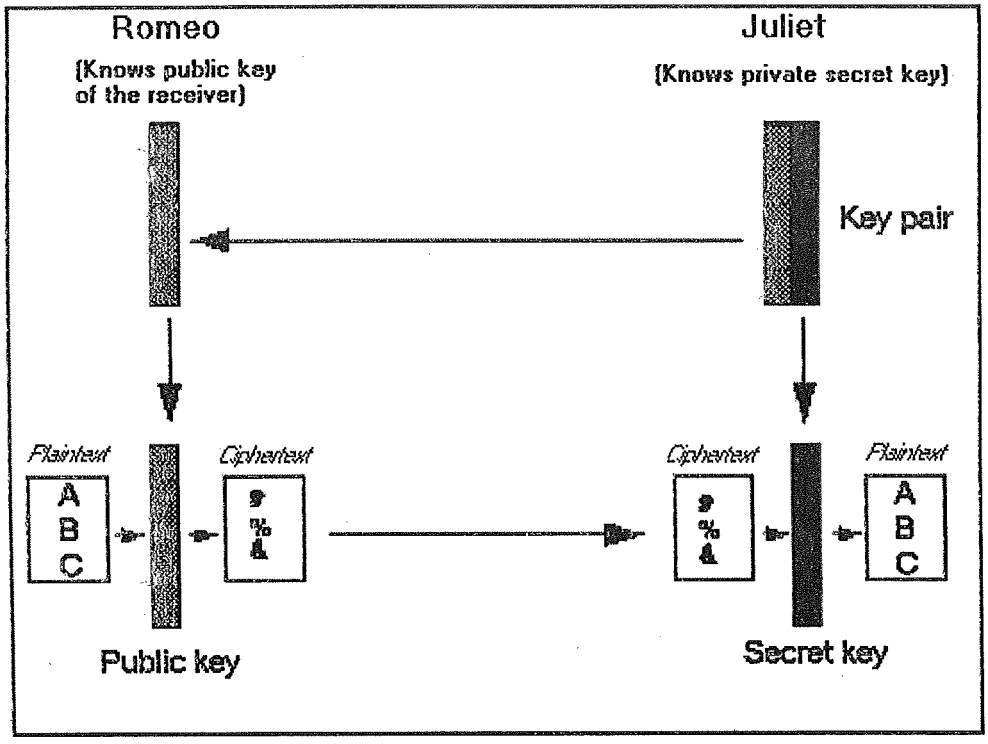

Fig. 4 Asymmetric encryption

- **Digital envelope**

A major disadvantage of asymmetric algorithms is that they are significantly slower than symmetric algorithms. This disadvantage can be overcome by using a **combination of both algorithms** in order to create a so-called **digital envelope**.

The plaintext is encrypted with a fast symmetric algorithm using a relatively short but nevertheless secure key. Additional security is provided if the key is only used once (*message or session key*) and irrecoverably destroyed as soon as the communication ends. Only this key needs to be encrypted with the public key of the receiver. For example, Romeo sends both ciphertext and encrypted *session key* to Juliet. By using her private key to decrypt the *session key* Juliet is able to decrypt the full ciphertext.

Example: Pretty Good Privacy (PGP) uses IDEA and RSA

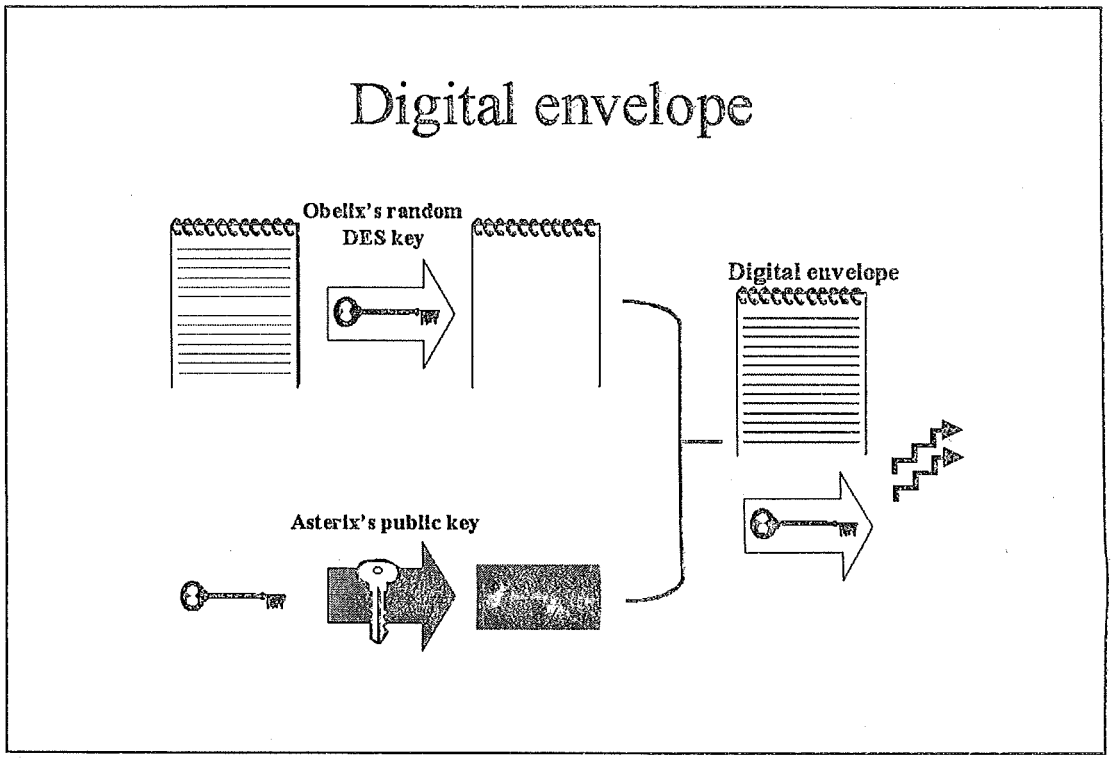

Fig 5. Digital envelope

- **Systems security**

In theory, some keys could be found on the basis of systematic trials (*"brute-force"* attacks). However the length of the key can be determined in such a way that the code could not be cracked within a practically feasible time period.

In an asymmetric, or public key, cryptographic system, keys with a length of 1,024 bits are considered to be secure at present. This corresponds to a string of more than 300 digits. Using today's computer technology, such keys would take centuries to crack. In a symmetric system like DES or IDEA, keys of 56 to 128 bits provide similar protection as a 1,024-bit public key.

28

Encryption is also useful for electronically stored information as it can not be excluded that unauthorized persons like computer hackers gain access to data. As some kind of data needs to be stored securely for long time periods, effective crypto-systems are necessary, using appropriate key lengths.

Such storage keys have the same importance as the stored data. For this reason it could be useful to make sure that the key can be recovered in case of loss, for instance if the owner of the key dies, an employee leaves the company with the key, etc. For secure communication such a key recovery mechanism is not necessary. If a message is lost during the transmission, the simplest way is to send it again, encrypted with a new key.

There is no general theory to design absolute secure systems or to assess with scientific reliability their degree of security. Hackers will try to find vulnerabilities in systems to avoid costly brute-force attacks (e.g. people that disclose information, failure in the algorithm, electromagnetic radiation emanating from computer screen, etc.). Given enough resources, time and skills, almost any system can be broken. The economic logic behind security is to make a system more difficult and expensive to break than the effort would be worth to hackers. As a result, there are different levels of security precautions, from simple passwords to very strong encryption. As any system is only as secure as its weakest link, systems security therefore needs to be continually analysed and adapted.

• Steganography

Data can be hidden using steganography. These methods reduce the chance of certain data being detected. If that data is also encrypted it gives an additional layer of security. The word steganography literally means "covered writing". It includes a vast array of methods of secret communications that conceal the very existence of the hidden data. Among these methods are invisible inks, microdots, character arrangement (other than the cryptographic methods of permutation and substitution), covert channels and spread-spectrum communications.

In contrast to cryptography, where the "enemy" can detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of steganography is to hide the wanted secret data in other data in such a way that it doesn't allow anybody to even detect that there is some hidden data present. It is not intended to replace encryption systems but it provides a supplementary difficulty for data to be cracked. These methods are no longer limited to embed text in images but can also be used for other media like voice, video etc.

***

ANNEX III

Key escrow / key recovery

• Definition

Key escrow and key recovery systems are encryption systems providing a backup decryption capability allowing authorised institutions under certain conditions to decrypt data using information supplied by one or more Trusted Third Parties (TTPs - trusted means trusted by both sides, the user and the government agency).

• Key escrow

In a **key escrow** system a copy of any secret key generated is deposited with an authorised TTP. The key could also be split into two or more parts that are deposited with different TTPs. In accordance with national law TTPs would have to hand over the key to the competent government agencies.

Once a copy of a private key is handed over to a third party, this key can no longer be regarded as fully secret. All communications and stored data encrypted with this key could eventually be decrypted.

• Key recovery

Within a **key recovery** system the private key would not be escrowed right from the beginning. The encryption system would allow authorised organisations, such as licensed TTPs, to rebuild the key on request.

Once the key is rebuilt through a key recovery system the result is the same as if the key would have been escrowed. Therefore a key recovery system would only make a difference if exclusively *session keys* (a key which is only used once and normally irrecoverably destroyed as soon as the communication ends) were recoverable. But even in such a key recovery system TTPs would theoretically be able to decrypt *all* session keys.

Technically both schemes allow access to all encrypted information. Consequently the difference depends essentially on the institutional arrangements set by national law.

***

ANNEX IV
Commission initiatives

• PROJECTS IN THE INFORMATION TECHNOLOGY PROGRAM

20563 E2S(SW): The goal of the project is to contribute to the growth of Electronic Commerce on the Internet by developing, testing and installing end-to-end security mechanisms for commercial transactions using the Internet. The plan is to deliver a professional infrastructure that is attractive to businesses and consumers, enabling the economic growth promised by the "information society".

22005 WIRE(SW): The overall goal of the WIRE project is to make it possible for organisations to deploy Secure Enterprise Webs. Today, many organizations have set up Web servers for non strategic IT applications to deliver public information to the market at a low cost compared to advertisement in other media. This current WEB technology is successful when data is public (access control is not required), small (less than thousands of pages) and simple (text, numbers, built-in .gif images). These conditions are too restrictive for professional applications. Commercial transactions require strong support for user authentication and access control.

24103 FACTMERCHANT(TBP): The pilot will demonstrate the integration of secure billing, e-mail and EDI on a platform, which provides comprehensive access to business information. This will include news and rates, world-wide market and broker research, and financial and credit analysis. The pilot will be run over Internet for access for both SMEs and larger organizations. The pilot will use knowledge-based systems technology for search, public-key cryptography and digital signatures for confidentiality, authentication, integration and non-repudiation.

22803 ICX (TBP): A business driven European User Group, to be known as the International Commerce eXchange (ICX), is proposed. ICX will be a European Forum for the discussion, identification and subsequent resolution of security issues in the electronic commerce arena.

9801 WEBCORE(SW): The W3C is an international industry consortium which seeks to promote standards for the evolution of the Web and interoperability between World Wide Web (WWW) products by producing specifications and reference software. Although W3C is funded by industrial members, it is vendor-neutral, and its products are freely available to all. In early 1996, W3C identified digital signature to be one of the major market drivers for Web security and launched the so called Digital Signature Initiative.

• PROJECTS IN "STANDARDISATION AND THE INFORMATION SOCIETY"

C-SET (Interoperable Chip-secured Electronic Transaction)

As the need for Electronic Commerce emerges, Visa and MasterCard have developed the SET (Secure Electronic Transaction) protocol to secure payment transactions on open networks by software. Worldwide card schemes will mostly apply to SET payment regulations according to which the merchant is not paid if the cardholder repudiates the

transaction. Some regional card schemes, such as CB and Banksys, enjoy a high level of security in domestic face-to-face payments thanks to the use of the micro-circuit card. They wish to enhance SET so as to support the use of microcircuit cards, thus providing the additional security needed to fully guarantee payments over open networks.

• PROJECTS IN THE ACTS PROGRAM

AC026 SEMPER

Background Networked information systems are experiencing a tremendous growth in terms of users and traffic as well as publicity. The dominating application is the Internet-based World Wide Web (WWW), with its potential of 3 million connected individual computers and an order of magnitude more actual users. WWW is still dominated by free-of-charge information systems, but this is expected to change dramatically in the near future. WWW will be used for all sorts of electronic commerce and trade, like online offering, ordering, payment, and delivery of services, information, and exchange of business documents. The same development can be expected for the IBC networks and "Information Highways."

• PROJECTS ON SECURITY OF TELECOMMUNICATIONS AND INFORMATION SYSTEMS

Interworking public key certification infrastructure for Europe (ICE-TEL)

The aim of ICE-TEL is to increase the trustworthiness of the Internet as used by industrial and academic research. The project will support security-enhanced applications by providing users with public key certification services in several European countries. It will also incorporate a security infrastructure and user platform to adapt and integrate the necessary tools and toolkits for incorporating public key-based security into applications as WWW, e-mail, electronic directories and multimedia conferencing. The three project applications selected for tools validation will involve secure communication between national computer emergency response teams and other network support groups, public administrations and protected access to electronic directories.

Multimedia European Research conference integration (MERCI)

The purpose of MERCI is to support joint research and technological development by deploying better tools for multimedia collaboration in Europe. Existing toolsets will be made easier for untrained personnel to use, with better quality audio, video and shared workspace facilities, and better support for multimedia applications in conferences. Distributed measurement, monitoring and control will be another important feature, as will improve privacy in conferencing. Verification, both within MERCI and other telematics projects, will include regular research seminars and industrial trials with commercial organisations.

Directory based EDI certificate access and management (DEDICA)

DEDICA plans to offer EU electronic data interchange (EDI) operators in sectors like banking, data security arrangements for them to network with so-called open system and distributed services, like electronic mail, which at present rely on different security standards. The proposal will involve making the certification infrastructure now employed for authenticating electronic messages in open systems compatible with EDI certification. A shared infrastructure will result in economies of scale for service providers, satisfy the global service needs of EDI operators and give e-mail users secure access to EDI.

Trustworthy health telematics (Trusthealth)

In TRUSTHEALTH, a network of bona fide national organisations working in health care computerisation will show how openly-linked European telematics systems can employ modern data security measures. Based on a 1994 EU user survey, the project will adopt coded digital signature techniques to meet legal requirements and sustain public confidence in information security. Among numerous urgent application areas are drug prescriptions, electronically exchanged laboratory data and health center invoicing. Network partners will collaborate in delivering security techniques for subsequent transfer to permanent health service operations.

Implementing secure healthcare telematics applications in Europe (ISHTAR)

Tight precautions to protect data in telematics-supported health services in Europe are the central concern of ISHTAR. The project will set up an expert group to advise and support the Commission and other personnel involved in security-sensitive health telematics projects. Existing guidelines on protection will be reinforced and products and services tested. The usefulness of telematics in handling the technicalities of data security will also be demonstrated. The project will launch publicity to heighten awareness of protection issues and also consider their legal and social implications.

Data protection in the European Union (DAPRO)

The purpose of DAPRO is to structure and demonstrate the content of the July 1995 EU Data Protection Directive as a basis for legal regulation of expanding telematics applications, and to clarify its relation to Member State law in this field. Both private and public sectors need such information, including case law, comments, data protection agency addresses, glossary and user guides, which will be published in an electronic system with a hypermedia interface. A publishing company will be responsible for implementing and marketing the system which will facilitate the extension of data protection law to other Member States.

Oparate

The aim of the project is to investigate operational and architectural aspects of TTP service provision: how a TTP should be organized and operated in order to provide TTP services effectively; how different TTP systems may be combined or made to interwork together, and in particular: how an ES/TTP network may be extended to provide confidentiality/key recovery services; how interworking may be achieved between heterogeneous TTP networks.

Eurotrust

Goal of the project is to operate a pilot Certification Authority (CA)/ Trusted Third Party service.

Oscar

The emphasis of the pilot is on certification in support of European Internal Market: how is it possible to certify business of users, to support secure messaging and any other communications services inside a country and across Europe.

Krisis

The project will try to define a key recovery scheme accepted by the commercial sector that also provides appropriate means for law enforcement.

Mandate II

It uses a functionally Trusted Third Party to provide the confidence needed for a new electronic financial negotiable instrument. Designed as a generic solution to electronic negotiability, MANDATE will ultimately be built on tamper-resistant hardware, known as a DOC-carrier, and using public-key cryptography to provide the security required.

Aequitas

The study will establish an experimental TTP, which will act as a service of certification for a group of lawyers, judges and prosecutors in their daily practice.

Euromed-ETS

The first objective of this project is using the experts' experiences and findings to identify, define and verify operational, technical, regulatory and legal aspects of the TTPs for telemedical applications over the WWW. The second objective is to implement the above adjusted findings in EUROMED's configuration, which is a telemedical application over the WWW, with regards to effectiveness, economics and acceptability.

Eagle

EAGLE will study commercial, technical and regulatory aspects of TTPs.

***

ANNEX V
World Wide Web addresses

Additional information on security and trust in electronic communications and related aspects can be found on the following Commission World Wide Web servers:

http://www.echo.lu

http://www.cordis.lu

http://www.ispo.cec.be

http://europa.eu.int/en/comm/dg13/13home.htm

http://europa.eu.int/comm/dg15/index.htm

***

ISSN 0254-1475

COM(97) 503 final

DOCUMENTS

EN 15 16

Catalogue number : CB-CO-97-522-EN-C

ISBN 92-78-25763-X

Office for Official Publications of the European Communities

L-2985 Luxembourg

36