EURIM Briefing No 16

May 1997

In the area of ICT (Information and Communications Technologies) EURIM is a link between Commerce and Industry, Parliamentarians, Whitehall and Brussels.

EUROPEAN INFORMATICS MARKET EURIM

PROMOTING SECURE ELECTRONIC FREE TRADE

Introduction

The continued economic well being of the UK and her European partners will depend on the ability to exploit electronic commerce effectively in the global marketplace. Electronic commerce operates over networks, both on privately owned and managed systems and over publicly accessible facilities such as the Internet. Networks are inherently insecure. The trust on which trade depends relies increasingly on the degree to which the actual content of stored or transmitted information can be protected from unauthorised access and alteration. Trusted means are also needed to establish other properties of information, such as who owns it, who sent it and that it was received.

The enabling tool for providing this trust technically is cryptography. Used in communications systems for many years, it was until recently tightly controlled and rarely used outside the military and Governments, and its civilian use is still illegal in some countries. Commercial pressure for use of cryptography to protect electronic information is increasing, as is the number of products using cryptography available in the marketplace. Governments are concerned to retain the ability to intercept and read communications for reasons of national security and therefore want to continue to limit the availability of cryptography. This conflict of interest could inhibit growth of secure electronic free trade.

Policy decisions must be made on whether the use of cryptography should be controlled and, if so, by whom and in what manner. Solutions must be internationally effective - but there will still be significant problems of jurisdiction. Suggestions such as that cryptography could make transmissions of pornography over the Internet difficult to trace, and make it difficult to counter terrorism and organised crime, has led to a growing pressure for "something to be done". EURIM is concerned lest over hasty legislation, triggered by the activities of one small sector of interested parties only, results in generic law that will hinder legitimate commerce.

Summary of Issues and Actions

1. There is a need for an internationally acceptable, practical, legal and commercial framework for establishing trust in electronic information.

2. The priority is to establish processes relating to integrity, authentication and non-repudiation as the basis for trust in electronic commerce.

3. A proper balance needs to be struck between the business need for an adequate level of security of information, and the requirements of national security and law enforcement.

4. Any regulations imposed should not unduly expose the honest trader or citizen to fraud resulting from them being unable to use controls of adequate strength.

5. A pan-European initiative is urgently needed to create a strong, consistent framework that encourages the unrestricted supply and use of security products across Europe that can counter the dominant US industry position.

6. Trusted Third Parties, while a key element of any solution, are themselves only part of that solution.

The Current Situation

For electronic commerce to operate with trust between the various parties, two distinct sets of facilities are required. The first need relates to proving that the content of electronic information (documents, messages, etc.) has not been altered, and that the owner, originator and recipient can be linked positively to that information - requirements such as integrity, authentication and non-repudiation. This can, broadly, be compared to the company letterhead, the written signature and seals used on paper documents. The second need relates to ensuring that only those allowed to read information can do so - a requirement known as confidentiality. This need arises because of the ease with which documents can be copied and read in electronic form. The closest paper equivalent is controlling physical access to all copies of a document at all times. All these requirements can currently be met technically by use of cryptography. However, there are equally important issues relating to the legal and commercial recognition of electronic information so protected, and to the context within which they are used.

Although this paper focuses on the non-technical issues, a basic understanding of cryptography is useful. The essence of cryptography is that the sender uses an encryption key as input to a conversion routine (or algorithm) that makes the digital message being stored or transmitted (whether words, pictures or sound) unintelligible. This can then be restored to its original form only by someone possessing the corresponding decryption key and algorithm. (See *Annex 1* for a fuller description) This technique is already being used widely in the financial industry, for example to protect funds transfers and personal information during the process of withdrawing cash from an ATM. It is also used in consumer products designed to control access, such as the set-top boxes which control access to subscription television. Cryptography is a necessary tool for electronic commerce, where it provides the solution to the requirements for integrity, authentication, non-repudiation and confidentiality. Although these requirements have similar underlying technical solutions, they raise distinct legal and commercial issues.

All users of the electronic infrastructure require a reliable means of associating users with their information. Where public key methods are used, this usually involves certification of public keys as belonging to certain users. Some governments are proposing the use of Trusted Third Parties (TTPs) to provide such certification, but for this to be acceptable there must be a high degree of trust in such TTPs. Although TTPs may be set up as commercial operations on a national basis within national law, they must be trusted internationally. TTPs may provide additional services, including access under due process of law to secret keys used for confidentiality, which will require additional safeguards against misuse. A separate paper *(Annex 2)* describes in more detail the issues relating to Trusted Third Parties.

The UK Interception of Communications Act gives the law enforcement agencies the right to intercept some types of network traffic under legal and/or political oversight in the fight against serious crime and terrorism, and most other Member States have similar powers. The widespread use of cryptography for confidentiality could hinder this process, which is why business has, in the past, been discouraged by Governments from using the most effective forms of cryptography.

Need for a Common Framework

The policy challenge is to strike an acceptable balance between the ability to combat fraud, terrorism and other criminal activity, and the business and individual citizens' rights to use appropriate technologies in their legitimate activities, including the protection of privacy. This is not an issue that can be viewed by one State in isolation; it is a global problem requiring a global solution. However, there is no time to wait for international regulatory control to be formulated. Rapidly increasing exploitation of international information and communications networks and technologies requires more rapid solutions.

At present there is concern among the business community that there is no clear or consistent policy in either the UK or the EU on a framework for the availability or use of cryptographic methods. Business needs to purchase products best suited to their needs, whatever the country of origin. Current Government controls in most countries prevent product suppliers from selling products using strong cryptography outside their own national boundaries. Business needs to use these products, and develop now systems that require them, for use over the coming years. If widespread use of the most effective forms of cryptography is effectively prohibited by government controls, there will be significant "knock-on" effects in system design, operation and commercial practices generally, which the lack of a well-defined commercial and legal

framework could further hinder. Growth of electronic commerce would be adversely affected.

It should be noted that the majority of relevant products are provided by US suppliers and, therefore, their availability outside the USA is subject to US Policy. US suppliers have a large, homogeneous home market in which to develop suitable secure products, and US Cryptography Policy is dictating the nature of technical controls on such products. Within Europe, although the total market is of comparable size, most countries prohibit the supply of products using strong cryptography outside their own country. This effectively constricts European suppliers to markets within their own country, and makes competition with US suppliers in Europe and, particularly, in the USA, difficult. It also tends to force European products and controls to follow US Cryptography Policy.

A start has been made in the OECD who have published a *Guideline on Cryptography Policy*. This sets out eight Principles that can be used as the basis for national laws on cryptography policy. They are:

- trust in cryptographic methods;
- choice of cryptographic methods;
- market driven development of cryptographic methods;
- standards for cryptographic methods;
- protection of privacy and personal data;
- lawful access;
- liability;
- international co-operation.

These Principles will be open to interpretation. and laws will inevitably vary across the world as this is an issue where differing cultural attitudes are significant. The way in which the Internet, in particular, is likely to be used will create serious issues of jurisdiction and extra-territoriality - and Internet users are developing cultural attitudes of their own which transcend national boundaries and could become very powerful. While legislation may be a necessary part of the process, it is unlikely to be sufficient to ensure arrangements that are reliable, understood and in which users have confidence.

Few countries have any legislation at present that recognises electronic information legally or commercially. Apart from matters of national security, some regulation is needed to provide consumer protection, and to provide electronic equivalents to the current paper-based legal and commercial processes. However, a more comprehensive framework is needed within which individuals, businesses and governments can operate with trust. Until now these issues have been considered in separate fora by technologists, lawyers, government agencies, privacy advocates and business people. The right solutions will be found only if all the groups involved converge and discuss their problems together. There is no obvious global forum in which to do this at present, and there is evidence of those with a particular interest, such as control of pornography, "forum hopping" to try and force their particular solution.

What are the key issues?

1. Business wants a predictable, trustworthy and practical legal and commercial framework for electronic information that is equivalent to that for existing paper processes. This should include a framework within which disputes can be resolved.

2. Parties involved in trade need to be able to check each other's credentials electronically. International infrastructures and trust frameworks need to be established to enable such checks to be made with confidence.

3. The UK wants to attract business because it is a good trading environment, and to sell abroad services, and the underlying products, that support electronic commerce. Most other Member States are believed to share these objectives, but with varying levels of priority.

4. Human rights and intellectual property rights must be adequately protected, but in a way that recognises the legitimate needs of business.

5. The continued existence of controls on cryptography between European countries creates a fragmented market, with complex controls, for European security products. This puts European industry at a disadvantage against their dominant US competition, who have a large homogeneous home market. In addition, US policy on cryptography, and associated technical solutions, has an unreasonably large influence on European policies, where European nations present a fragmented and inconsistent front.

6. All these capabilities need to be available and exploited internationally.

7. The appropriate levels for achieving each of the above must be found. The options will include, in some combination, the following:

(i). Mutual agreements within Industry – standards, Codes of Practice;
(ii). European wide initiatives;
(iii). Action by International Organisations;
(iv). National government policy framed within existing law;
(v). New or changed national laws.

It will be necessary to recognise that much legitimate activity will be outside any particular jurisdiction and that legislation might not easily by enforceable. Those who wish to circumvent regulations will continue to try and succeed but honest traders and citizens should not be placed at further disadvantage by controls on cryptography which unreasonably expose them to fraud or excessive costs.

Priority for Action

The UK and Austria will hold the Presidency of the European Union in 1998. Before then the UK should clarify its own position, take a lead in creating a model for others to follow and work to secure support from those EU Member States that share our priorities for a globally competitive European Marketplace.

The Trusted Third Party concept is well established in the commercial world, offering a range of security services. An issue that arises here is who would be trusted as a Trusted Third Party. There is an opportunity for countries such as the UK to develop internationally available centres of excellence in the provision of such services to the general public - but not if they are seen as government controlled or influenced. EURIM is concerned that the proposals made in the UK Department of Trade and Industry's consultation paper: *Licensing of Trusted Third Parties for the Provision of Encryption Services* will inhibit rather than encourage such opportunities.

There are other fundamental flaws in the document, which lead us to coincide that a further round of consultation will be needed before even the framework for possible legislation can be agreed. The paper takes no account of the impact on the UK of the development of TTP services in other countries. The paper concentrates on encryption at the expense of other services and assumes that all such services use public key, which is not true.

No attempt is made to cost justify the elaborate mechanism proposed or to assess the balance of civil rights, commercial benefits and national security. There is no acknowledgement of the fact that villains are unlikely to use licensed services and we consider an indication should be given of the extent to which, under these proposals, interception would in fact be possible.

TTP services are only one part of the framework of trust required in electronic commerce and must be considered in that wider context. The UK Government needs to clarify its policy in this area and reconsider the proposals in the consultation paper. It can give a clear lead to business by developing the legal and commercial framework, services and controls that support secure electronic commerce. The priority is to establish means of encouraging trust in electronic business processes - with a focus on those areas where trust relationships do not already exist. Regulation of those offering trust services to the general public is one such area; proposals to legitimise electronic transactions would be another. EURIM would welcome an unequivocal statement that business will be allowed to protect itself adequately whether operating nationally or internationally.

Individual Governments, such as the UK, should support the activities of Industry Associations and incorporate best practice into their own systems. They should be seeking solutions that are broadly applicable rather than of merit in one sector or one country only. They could take a lead in ensuring greater awareness of the technical practicalities among public and private sector opinion formers, and initiating an open debate on the political and organisational issues, and on the options available to balance the interests of the groups concerned, from personal privacy and corporate confidentiality through trust in the processes underlying electronic commerce to national security, and crime prevention and detection.

These debates must reflect the international nature of any potential solutions and could, for example, lead to a positive EU Directive establishing a common framework for electronic commerce across the European Community.

There are inherent problems in legislating during rapid change, but the issues will not go away or get any easier by waiting. Well-considered action is needed now or the UK, and the rest of Europe, will lose valuable business opportunities.

Annex 1 : What is Cryptography?

Principles of Cryptography

Cryptography, to most people, is concerned with keeping communications private. Indeed the protection of sensitive communications has been the purpose of cryptography for most of its history. Today, however, the use of cryptography has extended into other areas, and is becoming available in commodity software products.

The OECD Guidelines on Cryptography Policy define cryptography as: "The discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation and/or prevent its unauthorised use."

The underlying principle of cryptography in any form is the transformation of data (plaintext) into some indecipherable form (ciphertext) - *Encryption* - and the corresponding transformation back into understandable form - *decryption*. Encryption and decryption require the use of some secret information, usually referred to as a *key*. In general, the longer a key, the more secure the associated cryptographic mechanism becomes. There are two common forms of cryptographic mechanism used - known as *symmetric* or secret key, and *asymmetric* or public key. In either case, for cryptographic mechanisms to work, associated keys must be kept secret - the concern of *key management*. The extent to which this is necessary depends on the form of cryptography used.

Secret key mechanisms work as shown in Figure 1. The original information is encrypted using a key, and the ciphertext is decrypted using the *same* key. For this to work, it is essential that both parties share this secret. If this key is compromised, then all information encrypted with that key is compromised. Hence management and secure storage of the secret key is a major concern. Secret key mechanisms are usually fast to process and are, therefore, suitable for encryption of large volumes of information.

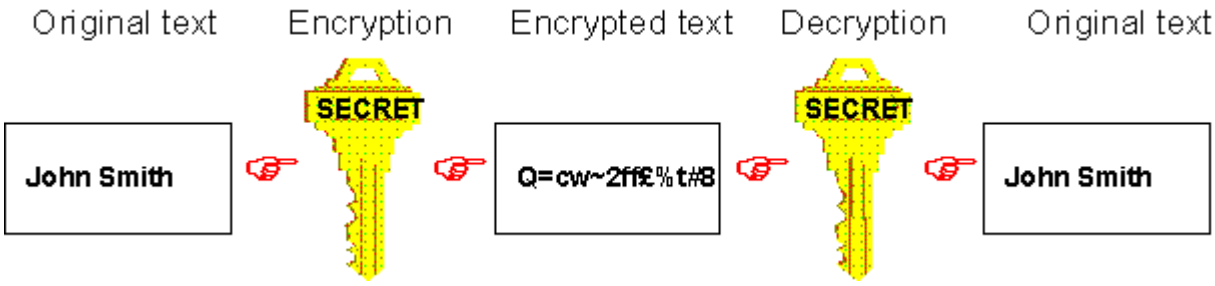

Figure 1 Symmetric (Secret Key) Cryptography

Public key mechanisms work as shown in Figure 2. Here key pairs are generated such that information encrypted using the *private* key can only be decrypted using the *public* key (and vice versa). While the private key assigned to an individual must be kept secret by that individual (or else they could be impersonated), the public key is made public, and associated with the same individual. If I want to send a confidential message to that individual, I encrypt it using their public key - and only their private key can decrypt it. Public key mechanisms are, usually, slow to process and are, therefore, better suited to encrypting small amounts of information.

Figure 2 Asymmetric (Public Key) Cryptography

For public key systems to work, there need to be trusted mechanisms that associate a public key with the individual to which it has been assigned. This requires the creation of *Certification Authorities* that certify public keys as belonging to certain individuals. Certification authorities sign public key certificates with their own private key, so that key has to be trusted. This leads to the concept of certificate hierarchies. These functions are one of the services that can be offered by Trusted Third Parties, the subject of a separate Paper.

Uses of Cryptography

A familiar use of cryptography is to conceal the information, whether stored or being communicated. This is most efficiently achieved by use of secret key methods. Common mechanisms are the Data Encryption Standard (DES), and RC2/RC4 from RSA Inc.

Public key mechanisms are more commonly used where there is a need to prove an association between an individual and some information. An example is a *digital signature* or *seal*. The originator performs a computation involving both their private key and a digest, or unique "fingerprint", of the original information. The resultant signature is attached to the information. The recipient does a similar computation involving a digest of the information, the originator's public key and the attached signature. If the result is consistent, then the information came from the owner of the associated private key and the content of the information has also not been changed. The signing process is shown in Figure 3. A common public key mechanism is RSA.

Figure 3 Creating a Digital Signature

Cryptography is also used to achieve a number of other processes useful in the electronic world. *Authentication* provides the means of ensuring the identity of a user; a *digital timestamp* bound to information can establish when it was created; the digital signature itself can be used to prove who sent a document, and prevent the originator repudiating ownership.

These basic cryptographic mechanisms can be used to build more complex processes such as *electronic cash, anonymous transactions*, and control of distribution of information to closed groups (such as subscribers to an electronic magazine).

Annex 2 : Role of Trusted Third Parties (TTPs)

Issue

Some of the security services required by commerce and by governments necessarily require involvement of a third party. Any such party is trusted in some way. These Trusted Third Parties (TTP) can also be involved in the provision of administrative services. This may satisfy business as well as law enforcement needs in all sectors.

Discussion

When a group of users wants to communicate securely using cryptographic methods, some measures must be taken to distribute and update the keys that are needed. Typically, each user must obtain a key coming from every other user he wants to communicate with, no matter which service is required. For a small, constant user group, this may be a fairly straightforward problem, which can be solved without involving any other parties than the users themselves. For larger and more open user groups, the problem quickly becomes difficult, however, and one needs to involve a so called Trusted Third Party (TTP).

Although several variants exist, there is a main distinction usually made between two types of TTPs: functionally Trusted Third Parties and unconditionally Trusted Third Parties.

The first type arises from the obvious need for reliable registration of users of the system. If public key methods are used, this will usually include certification of public keys as belonging to certain users. A TTP trusted to perform this function is called functionally trusted. It is clear that if the registration is not done in a reliable manner, users cannot even be sure with whom they are communicating. So functional trust represents a minimal amount of trust that must be placed in a TTP. Note that this type of TTP does not need to know the secret key of any user, nor does it need to know any conventional keys used for data communication between users. The functionality required in this instance is comparable to the functionality of a phone book. It provides a reliable connection between people, or their residence, rather, and their phone numbers.

The second type of TTP is typically needed in systems that use conventional cryptography only.

In addition to the registration function mentioned above, such an unconditionally trusted TTP will generate keys for data communication and then communicate them securely to the users who need them. This means that the TTP knows, and in principle could make use of, all the secret information in the system. Thus measures must be taken to prevent such misuse. This usually involves the use of tamper resistant hardware, ensuring that no key will appear in the clear outside of the trusted environment.

In any case, whichever approach is chosen, Trusted Third Parties must be introduced to handle a number of administrative functions related to the management of users, in particular registration, and the distribution of all relevant information on keys. However, a number of other functions, such as time stamping, are relevant, and all these requirements must be clearly understood to reach the objective of the project.

One single TTP world-wide is clearly impractical. So there will be one or more networks of TTPs. Some network may only support closed user groups. International networks for an open environment need some framework.

Trusted Third Party services can be considered as value-added communication services available to users wishing to enhance the trust of the services they use. Therefore TTPs have to be able to offer value added with regard to availability, integrity, confidentiality and assurance. Although TTPs may be set up on a national basis within national law, they must be trusted internationally.

There are different types of functions which may all or in part be fulfilled by TTPs. The exact nature and extent to which these functions are provided by TTPs will be dictated by practical considerations and may vary considerably.

In general the TTPs operate on the basis of information provided by the user. Certification of information is carried out on the basis of evidence of correctness provided by the user or generated by the TTP itself, eg the keys.

The major services a TTP may offer include some or all of the following:

- Name assignment, ie the function of assigning individuals' and enterprises' unique names and addresses. Individuals may possess several different and distinguished names, according to their role, eg as private citizen and as employee of a corporation.
- Certification, ie the function to validate that a name and address has certain credentials, eg a public key for signature.
- Key Management for signature, ie the generation, distribution, establishment, and administration of public and private keys.
- Key Management for confidentiality, ie the function to generate, distribute and administer keys used for confidential communications.
- Management Services for Names and Credentials, ie the function to establish, administer and make available registers with the names of individuals and their certified credentials.
- Security services, ie functions usually performed by the legal profession, mostly concerned with non-repudiation. These include:

  - Non-repudiation services
  - Claim of origin
  - Claim of ownership
  - Fair exchange of values
  - Untraceability
  - Time stamping

Common to Trusted Third Party service providers is that they have to be accredited and audited, and that they have to operate under the law of the country using common guidelines.

The information flow between constituents of a network of TTPs contains the following major elements:

- National Laws. The operation of TTPs will take place within the laws of the country in which they are located. It is conceivable that some legislation has to be updated to allow TTPs to operate in an international environment.
- Good practices, rules and regulations for the accreditation, operation and audit of TTPs.
- Standards for communications.
- Good practices, regulations and laws for the use of communication services.

Requirements of TTP programmes:

- Establishment of international framework for the operation of TTPs
- Setting up of conditions for the operation of TTPs in the EC, adapted to the needs of national and international users.

Such programmes are under way in the UK with DTI, and in the EU by EC and ETSI. All are current and at early stages of development. There is great commercial interest in TTPs, but concern as to how money can be made from acting as a TTP. The programmes are all looking at commercial models to help with this concern.

Annex 3 - Glossary

Authentication	The process of verifying the claimed identity of an individual.
Certificate	Data record that provides the *public* key of an individual, together with some other information related to the name of the individual and *the certification authority* that issued the *certificate*.
Certification Authority	*Trusted Third Party* that creates, assigns and distributes *certificates*.
Ciphertext	The output of an encryption function. Encryption transforms *plaintext* into *ciphertext.*
Confidentiality	The property that information is not made available or disclosed to unauthorised parties.
DES	Secret key cryptosystem (Data Encryption Standard).
Digital Signature	Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and *integrity* of the data unit and to protect against forgery (eg by the recipient).
Integrity	The property of ensuring that data is transmitted from a source to a destination, or stored, without undetected alteration.
Key	A sequence of symbols that controls the operations of encipherment and decipherment.
Key Management	The generation, storage, distribution, deletion, archiving and application of keys securely.
Key Pair	A set of a *public* and a *private* key that belong together.
Non-repudiation	The property of a receiver being able to prove that the sender of some data did in fact send the data even though the sender might later desire to deny ever having sent it.
Plaintext	The input of an encryption function or the output of a decryption function. Decryption transforms *ciphertext* into *plaintext*.
Private Key	Cryptographic *key* used in *public key* cryptography to sign and/or decrypt information.
Public Key	The *key* used in an asymmetric cryptosystem that is publicly available.
RC2, RC4 and RC5	*Secret key* cryptosystems.
RSA	*Public key* cryptosystem (Rivest, Shamir and Adleman).
Secret key	The *key* used in a symmetric cryptosystem that is shared between the communicating parties.
Trusted Third Party	A security authority or its agent, trusted by other entities with respect to security-related activities.