EURIM Briefing No. 28
October 1999

In the area of Information Society Technologies, EURIM is a link between Commerce and Industry Parliamentarians, Whitehall and Brussels.

PROMOTING ELECTRONIC COMMERCE
EURIM RESPONSE

This Briefing reviews the draft Electronic Communications Bill, which was published in July 1999 as part of the Consultation on Draft Legislation and the Government's Response to the Trade and Industry Committee's Report. It also summarises the response of the EURIM Secure Electronic Commerce Group to that Consultation paper.

The changes to the draft Bill as a result of previous consultations are welcome but there are still areas where it needs improvement to meet the objective of making the UK an attractive location for electronic commerce. We have two **general recommendations**:

- The same law should apply, as far as possible, on-line as off-line and separate legislation (as opposed to legislation to remove differences) should be enacted only where electronic commerce can be shown to require different treatment.
- The wording of legislation should address what it is intended to achieve and recognise the damaging uncertainty that can be caused by lack of clarity or unspecified reserve powers.

In summary, the draft Bill is in 4 parts:

Part I - Cryptography Service Providers - describes powers to create a statutory regulatory environment for cryptography service providers should industry self-regulation not prove adequate. This Part can be invoked by statutory instrument without consultation, and once invoked allows the Secretary of State to create regulations without constraint or consultation by statutory instrument.
EURIM recommends that, in the interests of creating a predictable environment for electronic business in the UK**,** this Part either be dropped, or the Bill includes statements specifying the nature and extent of the powers of intervention available to the Secretary of State

Part II - Facilitation of Electronic Commerce, Data Storage, Etc. - includes measures to allow signatures in electronic form to be admitted as evidence, and provides mechanisms to allow government departments to introduce electronic processes in place of paper processes by statutory instrument. No provision is made for the processes introduced by different departments to be co-ordinated. Equally no provisions are included to facilitate electronic commerce by updating commercial law.
EURIM recommends that this Part be revised to improve the facilitation of electronic commerce.

Part III - Investigation of Protected Electronic Data - is intended to enable law enforcement agencies to obtain the means of decrypting information obtained through due legal process and found to be encrypted. However, as written, this Part may be difficult to support technically, may conflict with the European Convention on Human Rights, extends the powers of law enforcement agencies to collect information beyond those already available to them and has inadequate safeguards. It would have a significant impact on industry and undermine confidence in the UK as a secure place in which to do business electronically.
EURIM recommends that Part III is removed from the draft Bill. A joint industry/law enforcement agencies working group should review and recommend suitable legislation on the way in which IOCA, PACE and similar legislation should be updated to extend existing law enforcement access rights to electronic information in understandable form.

Part IV - Miscellaneous and Supplemental - is concerned with amending the Telecommunications Act 1984 to introduce procedures that allow the simultaneous modification of many licences. EURIM has no particular comment on this part.

Overall Impressions

EURIM fully supports the Government's desire to make the UK the best place in which to do electronic business. We have worked closely with the DTI and others over past months to encourage an open exchange of views as the best way of achieving this goal. The draft Bill as published has taken account of many of the views and concerns expressed, and is a good basis on which to build.

In order to make the UK competitive against other trading nations as a place in which to base electronic business, it is essential that a predictable legal and regulatory environment is established. It is also necessary that business can have confidence in the security of that environment. The draft Bill, while recognising the need to achieve these objectives, can be perceived as creating a less predictable and secure environment than at present exists.

There are two prime reasons for this view of the draft Bill:

1. While it is clearly accepted that accreditation of trust service providers should be industry-led, Part I of the Bill is written in such a way that, should the Secretary of State choose to invoke the reserve powers for regulation, there is no constraint on the regulatory criteria that can be imposed. This creates an unacceptable degree of uncertainty over the regulatory environment for trust service providers.
2. Business supports the need for law enforcement to be able to obtain the plaintext associated with encrypted information legally obtained. However Part III includes legal conditions that are procedurally and technically difficult to meet and potentially costly to industry - and appear to provide law enforcement with capabilities beyond those needed to meet the declared objective. This will not inspire confidence in businesses deciding whether to locate in the UK.

General comments on each Part follow. The full set of EURIM comments submitted in response to the Consultation paper is provided in Appendix 1 to this Brief.

Part I - Cryptography Service Providers

Clause 24 allows Part I to be invoked by Statutory Instrument. While the government currently intends to allow self-regulation by industry, any decision to impose a statutory regulatory scheme could have a major adverse effect on the competitive position of UK Plc as a place to do business electronically. Invoking Part I should, therefore, explicitly require at least the relevant statutory instrument to be laid before Parliament and approved by a resolution of each House following consultation with all interested parties. However, the existence of such a possibility itself creates uncertainty - especially as it is unclear under what circumstances Government would decide to invoke Part I and with what regulations (although paragraph 28 on page 9 of the Consultation Paper does list some requirements any accreditation scheme should support). EURIM would prefer to see Part I dropped from the Bill. If this Part is retained, to remove uncertainty it should include statements indicating under what circumstances this Part would be invoked and limiting the powers available to the Secretary of State in defining the criteria for accreditation for service providers.

EURIM is concerned at the focus on cryptography as the service provision. We understand that the intention is to create confidence in trust services associated with electronic commerce and from a commercial point of view this may be an issue. However, trust services may, or may not, use cryptography. The Title, definitions and wording should be altered to reflect this.

It is assumed that the detail in Clauses 1-6 of Part I is provided to enable an understanding of the statutory regulation regime which the government would

impose should Part I be invoked. As written they do not in any way restrict the regulatory conditions that can be imposed by the Secretary of State. Clause 5 allows the ability to make regulations by statutory instrument subject to annulment in pursuance of a resolution of either House of Parliament. The process for making regulations should explicitly include a requirement to consult with all interested parties and should require approval by a resolution of each House. EURIM would like to see the regulations imposed constrained by, for example, explicitly excluding any requirement for cryptography service providers to hold customer's keys of any type and limited to matters directly related to provision of trust services. There is a real concern that even this will not create the predictable environment needed if the UK is to attract electronic business.

Part II - Facilitation of Electronic Commerce, Data Storage, Etc.

Overall the approach taken by this Part is encouraging. EURIM offers suggestions on how it might be improved to increase confidence.

Clause 7 associates electronic signatures with electronic communications. EURIM understands that this is not the intention, and that any information in electronic form associated with an electronic signature can be submitted as evidence.

Further, the definition of "electronic signature" in Clause 7(2) is different from those commonly recognised. A better definition would be that used for an *advanced electronic signature*" in the European Directive on the harmonisation of the legal recognition of electronic signatures (Article 2 (2)).

EURIM is disappointed that the opportunity has not been taken to include in this Bill changes to those few Acts that affect commercial contracts and dealings. Examples are the point of acceptance of electronic contracts, or of the passing of title for intangible goods. Such provisions would make UK law as attractive to companies doing electronic business as are the equivalent laws for financial services - where the UK has a leading international position. An initial list of such areas is included as Annex A.

EURIM welcomes the inclusion of means to allow electronic government, but is concerned that there is no explicit mechanism to ensure that departments allow electronic information exchange and transactions in a manner that is consistent and practical. Industry and citizens alike will have to communicate with a number of government agencies, and inconsistent or, worse, conflicting, technologies, processes or other regulations will increase costs and discourage use of electronic services. There are already signs of this happening with the provisions in the Finance Act for electronic access to the Inland Revenue and Customs & Excise (which are explicitly excluded from the draft Bill).

There are also no constraints on what facilities or conditions a department can impose on users of their electronic services - for example, it would be permitted to require escrow of keys of any type. EURIM would like to see constraints, such as not storing user's private keys, placed on the services they offer.

Part III - Investigation of Protected Electronic Data

EURIM accepts the need to provide legislation that enables the appropriate authorities, where they have obtained information through due legal process, to seek access to the means of obtaining the plaintext where that information is encrypted. However, as worded the balance of proof seems to be biased unreasonably against the recipient of such a request, especially where they are an innocent party involved solely through the nature of the technology. Further, it is not certain that the processes implied can be met with existing technology or systems,

even assuming the development of special UK versions of products at significant cost. The wide scope of the proposals, together with the lack of strong safeguards or effective remedies against failures in the process, could place both industry and individuals in breach of contract or trust, or in conflict with the law as proposed. As written, this Part can only undermine confidence in the UK as a place in which to invest in electronic business.

It is unclear why this Part is included in a Bill concerned with encouraging electronic commerce. Given that the intention is to extend the existing powers in IOCA, PACE and similar legislation to enable access to the means of obtaining plaintext of encrypted information that has been obtained under due process, it would seem more logical to include appropriate changes in those Acts under Home Office control rather than trying to create an omnibus set of powers in this DTI sponsored Bill. EURIM accepts that this may mean that IOCA needs to be broadened to cover the additional issues.

EURIM recommends that further work on this Part be deferred until the Government/Industry joint forum and the Technical Assistance Centre recommended in the recent PIU report on Encryption and Law Enforcement have met. We suggest that they should sponsor a joint industry/law enforcement agencies working group set up to recommend sustainable proposals that are technically neutral for legal access to electronic information. This work could include the current review of IOCA.

Part IV - Miscellaneous and Supplemental

EURIM made no specific comments on this Part. We understand that significant comments were submitted separately by telecommunications companies affected by this Part. However, we would note that OFTEL should be required to publish for reference (e.g. on a public web site) a register of Licence Terms so that the current state, proposed changes and their intended effect can easily be understood by anyone needing such information.

Attachments to this Briefing:

Appendix 1 - Detailed EURIM Comments (as submitted to the DTI in response to their consultation on the draft bill.)
Annex A - Suggestions for Immediate Legislative Changes

BR28 - APPENDIX 1 -

Detailed EURIM Comments

Part 1 - Cryptography Service Providers

EURIM has reservations as to the need for this Part. Whatever the decision on the future of this Part, EURIM has the following comments on the Clauses in Part I as presented.

1. The government has stated repeatedly that the intention of regulation is to create public confidence in trust services that support electronic commerce. Part I focuses on the provision of cryptography services. These need not be the same as trust services, which may not use cryptography to achieve their purpose. This Part should be re-focused to approve trust service providers.
2. Clause 1(1). We would prefer the Secretary of State to have the *power* rather than a *duty* to establish and maintain a register of trust service providers. This would be more consistent with a statutory voluntary scheme. This principle applies in other clauses in Part I where *power* should replace *duty*.
3. Clause 2(2)(c). It is unclear why approval should affect matters not connected with the provision of the services, as is implied here. If there are specific matters intended, they should be spelt out here - otherwise the reference to such matters should be removed. This will require parallel alteration to Clause 2(3)(c).
4. Although Clause 3(1) appears to allow the Secretary of State to appoint persons to carry out the approval process on his behalf, Clause 2(7) and (8) appear to rule out payment to such persons for carrying out those duties. This cannot be intended.
5. Clause 4 overlaps with the Data Protection Act 1998, and seems to prescribe more stringent penalties for disclosure of information than are required under that Act. It is not clear why this is so, and why the rules on public disclosure appear to be at variance with common practice and to impose unreasonable constraints. For example Clause 4(4) appears to include penalties for public disclosure of information already in the public domain for other reasons.
6. Clause 5 creates uncertainty on the scope of any regulatory scheme. It allows the Secretary of State to make any regulations affecting service providers (and even (Clause 2(2)(c)) matters not connected with the provision of those services) he desires without constraint - and by statutory instrument subject to annulment in either House. At the least this should be amended to require an explicit consultation process and approval by a resolution of each House, since any change to the regulations could have a massive effect on the ability of businesses in the UK to operate efficiently and competitively, and of the ability of UK citizens to exploit electronic commerce. The scope of regulations that can be invoked should be explicitly constrained. For example, there should be explicit prohibition on mandatory key escrow - possibly similar to that included in the US “SAFE” Bill. Fundamental changes of this nature are essential if the image of a stable, predictable environment for electronic business is to be projected.
7. Clause 6(1) incorrectly defines the purpose as approving services designed to facilitate the use of encryption. If the intent is to engender confidence in electronic commerce, the need is to create confidence in trust services, not all of which may exploit cryptography. The wording should be altered to reflect this intention. Note also that, under (a), data can be handled by automatic processes as well as by persons.
8. Clause 6(2) as worded is not comprehensible. We think the intention is that the supply of products that provide cryptography and trust service mechanisms should not be considered provision of trust services. If this is the case, this clause should be reworded to make the intention clear.
9. Clause 6(3)(b) seems to imply extra-territoriality. Given that approval for a trust service is voluntary, it is not clear why service providers outside the UK should want to seek approval under UK regulations, and why this needs to be stated in this Bill.

Part II - Facilitation of Electronic Commerce, Data Storage, Etc.

1. Clause 7 associates electronic signatures only with electronic communication (which is defined in Clause 23). This is unnecessarily restrictive. Any information in electronic form can be signed electronically whether in store or being communicated, and the wording should be changed to reflect this.

2. As written it is not clear what Clause 7 adds over existing legislation, such as the Civil Evidence Act 1995. If the intention is to reinforce the principle of admissibility of signatures in electronic form as evidence, Clause 7 needs redrafting to make this clear. However, EURIM agrees that the Bill should not prescribe what constitutes a legally acceptable signature as this is very dependent on the context, including issues of form.

3. The definition of *electronic signature* in Clause 7(2) is not correct and could lead to confusion. A better definition would be that used for an *advanced electronic signature*" in the European Directive (Article 2 (2)). An alternative definition is that produced by ETSI, as follows:

   Evidence in a digital form that can be processed to get confidence that some commitment has been explicitly endorsed under a Signature Policy, at a given time, by a signer under an identifier, e.g. a name or a pseudonym, and optionally a role.
   Signature Policy
   A set of rules for the creation and validation of an electronic signature, under which the signature can be determined to be valid.

4. The use of the word "certify" associated with signatures in a number of places in Clause 7 is confusing. A trust service provider only certifies that the possessor of a public key does possess the associated private key - and may also underwrite claims as to the identity of the public key owner. No signature created using that private key is certified by the trust service provider. Indeed, the public key certificate says nothing about who possessed the associated key pair or about the intent of the signer at the moment of signing. "certify" as used in Clause 7 should be changed to avoid confusion with the technical term.

5. EURIM regrets that no provision has been made to change aspects of commercial law to make UK law more attractive as a basis for electronic commerce. There are a few areas where changes would clarify the law as applied in the electronic environment and remove uncertainty. We have included at Annex A a suggested list of such changes.

6. While EURIM welcomes the intention expressed under Clauses 8 and 9 to allow government departments to alter by statutory instrument Acts under their control to allow the use of electronic communication and storage, we are concerned that there are no mechanisms explicitly included to establish a common framework within which such use is established. There is a grave danger that the move to electronic processes will be implemented piecemeal and in a way that presents industry and citizens with a plethora of incompatible and possibly unworkable processes that undermine the ability to benefit from the move. We would like to see explicit reference to the production of guidelines and codes of practice for the implementation of electronic services across government departments.

7. There should be an explicit statement in Clause 8 preventing departments from introducing electronic processes that require safeguards greater than those already in place in the equivalent paper processes. For example, if a paper signature does not need to be witnessed, neither should the signature in the equivalent electronic process.

8. Clause 8(3) as written is not comprehensible, and its intention not understood. It appears to require that it should be possible to reproduce in human readable form any information that exists or existed in electronic form created anywhere in a process. This seems unachievable.

9. Clause 8(4) is not technically neutral. It could be changed to read "….electronic form to be taken by any electronic information, however held or processed, the use of which…..".

10. Clause 8(7) illustrates our concern over departments developing inconsistent approaches to the use of electronic transactions. There are already signs that the relevant sections in the current Finance Bill are not consistent with those written in this Bill, and no guarantee that even the regulations developed independently by the Inland Revenue and Customs & Excise will be consistent.

Part III - Investigation of Protected Electronic Data

1. EURIM recommends that this Part be removed from this Bill and placed elsewhere - possibly in the revision to IOCA currently in hand.
2. EURIM has always supported the principle that, where information obtained through due legal process (such as is in IOCA or PACE) is found to be encrypted, the appropriate authority should be capable of obtaining the means of acquiring the associated plaintext. However, Part III appears to go significantly beyond this simple requirement. We believe that the provisions of this Part will undermine confidence in the UK as a place to base electronic business. They also raise significant concerns over conformance to the European Convention on Human Rights and on reversal of the Burden of Proof.
3. There are also real technical concerns that the intentions of this Part are not achievable in the real world. The user may enter a passphrase, for example, to enable encryption or decryption of information, but that will not mean they have access to the actual keys. Possession of a key is itself a questionable concept - particularly with information being communicated the nature of the technology is such that no record of the keys used is kept, and no mechanism exists to capture the values of the keys used. Often it will be difficult to reproduce the technical environment, including the relevant software and hardware cryptography components, on a separate platform to decrypt information legally acquired. Decryption may only be possible on the originating system, which may belong to an innocent party caught up in an investigation by the nature of the technology.
4. Part III appears to have been drawn up without an adequate understanding of the technologies involved. It requires a rewrite, taking account of the comments below. EURIM recommends that further work on this Part be deferred until the Government/Industry joint forum and the Technical Assistance Centre recommended in the recent PIU report on Encryption and Law Enforcement have met. We suggest that they should sponsor a joint industry/law enforcement agencies working group set up to recommend sustainable proposals that are technically neutral.
5. EURIM is concerned that the level of authority needed to serve a Section 10 notice, as described in Schedule 1, is far too low for certain types of information (especially that described in 10(1)(c) or (d)) and extends existing powers. This is particularly true for information that comes into the possession of the authorities other than by due legal process. The relevant clauses should be changed to require stronger approval processes.
6. Clause 10(2) is wholly unsatisfactory. However the encrypted information was obtained, the relevant authority must explicitly be required to demonstrate beyond reasonable doubt why a Section 10 notice is needed. This must include both statements on the nature of the crimes involved (which must be of a sufficiently serious nature) and on the reasons why the person on whom the notice is to be served is suspected of being in possession of the associated key(s).
7. Clause 11(3) is also flawed in that it presumes the appropriate authority understand enough about the target systems to be able to demand the key be provided and not the associated plaintext. There will be many cases where, technically, this is not possible. The law should not force people to perform technically impossible tasks.
8. Clause 12 raises grave concerns on the ability to mount a credible defence - since the recipient of a Section 10 notice is being asked to prove a negative. At the least the recipient should be allowed to challenge the reasons why the appropriate authority believes they possess the relevant key. The concept of “possession of a key” is itself flawed, as has been mentioned earlier. There are cogent arguments that this clause violates the relevant parts of the European Convention on Human Rights, and reverses the burden of proof. This needs to be addressed. Provision of a key cannot be equated to provision of a blood sample or of DNA. Many people would not even know how to provide a key if asked - and many potential targets of a Section 10 notice will be innocent parties to any criminal investigation, involved only through the nature of the encryption technology used.
9. Clause 13 also raises significant practical concerns, especially for industry. It will not always be obvious who should be contacted to provide a particular key, and the nature of business systems means that more than one person will inevitably be involved in a business of any size. There are

also major liability issues that are not addressed, including who is liable if information is compromised after provision of the associated key under a section 10 notice. It is good security practice to change a key as soon as it is suspected of compromise - which would be the case following a Section 10 notice. So any reputable business would expect to change such a key immediately to limit its liability. It is not clear whether this is possible without infringing the terms of Clause 13.

10. Clause 15 provides for no protection of the information once decrypted, and provides no redress should such information, or the associated keys, be disclosed. Further, there is a need for well-publicised effective processes for checking the authenticity of claims for rights of access, with severe penalties for impersonation and/or false claims. Misuse of the provisions of Part III will create a high risk of financial loss or loss of corporate assets and must be discouraged. Failure to address such issues will not inspire confidence in industry that the UK is a good place for electronic commerce.

11. The principle of a Code of Practice in Clause 16 is to be welcomed and we look forward to a public discussion of its contents. However we are concerned that there appears to be no sanctions or redress for violation of any aspects of the Code even where this results in material damage to a business or individual.

12. We are disappointed in the nature of the Tribunal proposed in Clauses 17, 18 and Schedule 2. We note that no member of the Tribunal is required to be technically qualified to assess the worth of a technical defence in what is technically a very complex area. We note also that the Secretary of State has the power to create any rules without constraint including, for example, whether or not the complainant can be legally represented. We would like to see a basic set of rules enshrined in law, including the right of the complainant to be legally represented and for them to be provided with all relevant information (subject only to the requirements of the Official Secrets Act).

13. Some of the definitions in Clause 19 need review. We believe the definition of "electronic signature" is provided in support of Clause 10(5). We see no reason why this should be different from that included in Clause 7 (modified, as suggested above, to be consistent with common usage).

The definitions of "key" and "protected information" are too widely drawn. EURIM has always understood that the intention is to acquire the means to access the plaintext of information obtained under due legal process and found to be encrypted. Both these definitions include reference to "access to electronic data" which implies that it is not yet in possession of the appropriate authority. Paragraph (a) should be deleted in both definitions. In addition the definition of "key" extends beyond that understood in relation to the need to decrypt encrypted information. Strictly a key is some secret information that, used in conjunction with a specific algorithm, converts plaintext into cyphertext (or vice-versa). To be able to decrypt information possession of the key might not be sufficient. However, use of other information, such as a passphrase, is likely to require direct access to the system used by the recipient of a Section 10 notice. This raises other issues, not addressed in this Part, such as the need for access to or seizure of systems - possibly disrupting the lives and financial viability of innocent businesses and individuals.

Annex A

Suggestions for Immediate Legislative Changes

The test of what should be done by immediate legislation is to consider what business people might expect to achieve by e-mail in the way of binding commitments (whether an exchange of messages is viewed with foresight or hindsight), and to rectify the position where existing "writing" requirements could provide an unmeritorious technical defence.

EURIM suggests that electronic exchanges be treated as binding between parties, such as in the way electronic patent assignments could be made binding between parties even if they need (for the time being) to be put on paper to be registered (pending adoption of procedures for registering electronic documents).

This effect could be produced in suitable cases by a provision that "writing" is, for those cases, given the meaning ascribed to it by section 178 of the Copyright, Designs and Patents Act 1988, and that, where relevant, references to "signature" include the incorporation in any such writing or anything which would amount to a signature if incorporated in any writing on paper.

On this basis the following provisions should be made:

1. Patent licences, assignments and charges should be valid as between the parties if in electronic writing.
2. Guarantees (perhaps not including guarantees by a consumer to a person acting in the course of a business) should be valid if in electronic writing.
3. Assignments of debt should be valid if in electronic writing.
4. Where electronic writing is treated as being writing for any purpose, or where a transaction for which writing is not required is effected by electronic writing, an electronic document expressed to be executed as a deed should be a deed notwithstanding the absence of paper. (Expressed in this way, the provision would not sweep up everything required to be done by deed, but would usefully prevent e.g. the release of a debt for no consideration, from being invalid.)
5. Contracts and instruments dealing with interests in land should be valid (only as between the parties in the case of those requiring to be registered or capable of benefiting from registration) if in electronic writing.
6. Transactions governed by section 63 of the Law of Property Act 1925 should be valid if in electronic writing: this would prevent unmeritorious technical defences to the validity of transactions whose validity depends on interpreting them as of a kind falling within that section.

In addition to this, the implementation of Article 15 of the UNCITRAL Model Code, dealing with the time and place of the formation of contracts, would be a helpful measure, and one likely to ensure the conformity of UK law with the principles adopted in other jurisdictions on the same points.