BUILDING CONFIDENCE IN ELECTRONIC COMMERCE

-

A CONSULTATION DOCUMENT

Unique Reference Number: URN 99/642

dti

Department of Trade and Industry

BUILDING CONFIDENCE IN ELECTRONIC COMMERCE - A CONSULTATION DOCUMENT

SUMMARY

Electronic commerce has the potential to revolutionise the way business is done and improve the competitiveness of British industry. The Government has set the ambitious goal of developing the UK as the world's best place in which to trade electronically and the Prime Minister has set the target that by 2002, 25% of dealings by citizens and businesses with government should be able to be done electronically.

People need to be confident about the identity of the person sending an electronic message, to be sure that it hasn't been tampered with, and in some cases that it has been kept confidential. The technology is available, but users need to be able to trust it and companies supplying it. The Government announced its intention to legislate in November 1998, to build trust in electronic commerce, by establishing a voluntary licensing system for providers of cryptographic services; and by enabling legal recognition of "electronic signatures".

The main purpose of this Consultation Paper, which has been prepared jointly by the DTI and the Home Office, is to seek views on the detailed implementation of this policy. Topics on which we are seeking views include: legal recognition, the criteria which applicants for licenses will have to meet, the liability of service providers towards their customers and others, and the way the law enforcement provisions will affect licensed providers, unlicensed providers and other people. We are also interested in views about the removal of obstacles in existing law so as to permit the use of electronic communication in place of paper, and other changes to legislation to promote electronic commerce.

Serious criminals, including drug traffickers, paedophiles and terrorists, are turning to encryption to conceal their activities. Unchecked, this will make the work of law enforcement increasingly difficult. The Government therefore intends to provide the agencies responsible for tackling serious crime with the ability to acquire lawful access to material necessary to decrypt communications or stored data.

While the Government remains keen to promote the development and use of encryption technologies that meet law enforcement requirements, it recognises industry concerns that making key escrow and third party key recovery a requirement for licensing could hinder the development of electronic commerce in the UK. It is therefore consulting on the basis that this will not be a requirement for licensing. However, the Government is looking to industry to help identify ways of meeting law enforcement requirements while promoting the growth of electronic commerce.

The Government is committed to introducing legislation in the current Parliamentary session. **Comments are required by Thursday 1 April.**

5 March 1999

CONTENTS

INTRODUCTION

1. In the White Paper "Our Competitive Future: Building the Knowledge-Driven Economy"[1], published in December 1998, the Government set out the ambitious goal of developing the UK as the world's best environment for electronic trading by 2002. The policy set out in this document is a central part of the Government's strategy for achieving that goal, by making progress towards meeting the commitments to establish a voluntary licensing scheme for cryptography service providers, and to remove the legal obstacles that stand in the way of electronic commerce. The Government's broader electronic commerce agenda was set out in *Net Benefit: the electronic commerce agenda for the UK*[2]. Electronic commerce is crucial to the future prosperity of our economy and to the competitive position of our industries. The UK is well placed to play a leading role. Electronic commerce can be defined as:

> using an electronic network to simplify and speed up all stages of the business process, from design and making to buying, selling and delivering.

2. Electronic commerce is already revolutionising the way business is done. Electronic commerce is changing the way businesses, of all sizes, work internally and interact with their customers and suppliers. It is also affecting individuals, who will increasingly communicate with business and other individuals through a home computer or a digital TV connected to the internet, or using a publicly available kiosk in a public library or the local supermarket etc. Many transactions, whether by individuals or businesses, are with various arms of government itself. The Government is committed to communicating electronically through the Better Government initiative; the Prime Minister has set the target that by 2002, 25% of dealings by citizens with government should be able to be done electronically. The Government is also committed to increase its use of electronic commerce in procurement.

What is an electronic signature?

It is something associated with an electronic document that is the electronic equivalent of a manual signature. Electronic signatures come in many different forms. One purpose of the policy detailed here is to set out what is needed for an electronic signature to be regarded as legally equivalent to a hand-written signature.

What is cryptography?

Cryptography is the science of how codes work and may seem of limited interest outside the military and espionage communities. However, it has long been used by banks and is an essential tool for electronic commerce. One application is to keep electronic data, ranging from an e-mail, perhaps sent over the internet, to a file stored on a floppy disk, confidential. Another use is to "prove" that an electronic document was written by someone holding a particular code, and that it has not been altered since signing. In other words cryptography can be used as an electronic signature (see also box on page 17).

---

1 See www.dti.gov.uk/comp/competitive

2 *Net Benefit: the electronic commerce agenda for the UK* is available at *www.dti.gov.uk/cii/ecom.htm*

3. This document explains the Government's proposals for legislation to promote electronic commerce, to start updating the law to reflect what is technologically possible and to ensure that the powers of law enforcement agencies are not undermined by the increasingly widespread ability to encrypt electronic information. The policy is based on the following principles:

- the Government's intention to put in place a policy and legal framework to promote electronic commerce;
- the need to promote users' confidence both in the technologies which allow integrity and confidentiality, and in the providers[3] of cryptography services;
- the law should, as far as possible, be technology neutral;
- the intention that licensed Certification Authorities[4] would be in a position to offer certificates to support electronic signatures reliable enough to be recognised as equivalent to written signatures;
- recognition that clear differences in approach need to be afforded to the development of electronic and digital signature services, and to encryption services;
- the need for new powers for law enforcement agencies to gain legal access, under proper authority and on a case by case basis, to encryption keys or other information protecting the secrecy of stored or transmitted information so as to maintain the effectiveness of the existing legislation designed to protect the public from crime and terrorism in response to new technological developments.

4. These principles have been developed through a process of formal and informal consultation in recent years. The purpose of this document is to set out how the Government intends to implement these principles, and to seek the views of industry and other interested parties on the detail. The Government is committed to introducing a Bill in the current Parliamentary session, and it is likely that these principles will be implemented using a combination of primary and secondary legislation. We invite comments by **Thursday 1 April**. It may not be possible to take into account responses received after this. This paper is available at *http://www.dti.gov.uk/CII/elec/elec_com.html*

5. Any comments should be sent in writing to Stephen de Souza either by electronic mail (preferably in Word 6.0 or text format) to:

X.400 address: S=sec O=DTI OU1=CIID P=HMG DTI A=Gold 400 C=GB

internet address: sec@ciid.dti.gov.uk

or to:

Communications and Information Industries Directorate
Department of Trade and Industry
Room 220, 151 Buckingham Palace Road
London SW1W 9SS

It would be helpful if those responding could clearly state who they are and, where relevant, who they represent. Should you wish any part (or all) of your comments to be treated in

[3] For the purposes of this document, providers of cryptography services are described as Trust Service Providers. A TSP may provide one, or more, cryptography services including acting as: a *Certification Authority* (see footnote 4), a *Trusted Third Party* (providing confidentiality services) or a *Key Recovery Agent* (see footnote 17).

[4] A *Certification Authority* (CA) is a TSP which issues certificates to link electronic signatures to particular individuals or business functions (see also box on page 20).

confidence, you should make this clear in any electronic mail or papers you send. In the absence of such an instruction, submissions will be assumed to be open, and may be shared with others or published by Ministers, or placed in the Libraries of the Houses of Parliament.

INTERNATIONAL CONTEXT

6. Electronic commerce is essentially a global, rather than a national, issue. Not surprisingly a number of initiatives concerning cryptography are taking place in various fora. Indeed recent years have witnessed a remarkable growth in the nature and range of bodies engaged in discussion of this issue. The Government believes that it is important to monitor these developments carefully to ensure consistency with our own policies. We have, therefore, involved ourselves extensively in such discussions; particularly in relation to the recent European Commission proposals on electronic signatures and electronic commerce, the OECD (Organisation for Economic Cooperation and Development) Ministerial discussions in Ottawa on electronic commerce and the current discussion in the UN on electronic signatures.

EUROPEAN UNION DIMENSION (INCLUDING DRAFT EU DIRECTIVES ON ELECTRONIC SIGNATURES AND ELECTRONIC COMMERCE)

7. In its October 1997 Communication[5], the European Commission outlined the important role which cryptography could play in the development of secure electronic commerce for both businesses and citizens. The Communication said that it was appropriate to bring forward a Directive on electronic signatures; both to encourage their use and to ensure that "signed" documents and messages were given recognition across the Community. The UK welcomed this communication and was pleased when the Commission adopted its draft Electronic Signatures Directive in May 1998. The draft Directive seeks to promote the development of electronic signature services through the introduction of a legal framework for Certification Authorities and an obligation (in certain circumstances) for member states to legally recognise electronically signed communications.

8. Although still under discussion[6] (both in the Council and in the European Parliament) the provisions of the Directive are, at present, consistent with the proposals in this document. It is anticipated that the Directive will be formally agreed in the latter half of the year. The UK proposals are therefore likely to come into force before the Directive is implemented by member states (likely to be early in 2002). In the field of electronic signatures, the UK legislation goes further: while the Directive permits member states to set up licensing schemes, it does not, require them to be set up. Our proposals would set up a licensing scheme. The directive, like our own proposals, will outline criteria which "approved" certification authorities should meet as well as describing the content of an electronic signature certificate. It also lays down requirements for user signature creation devices, and is likely to introduce liability requirements on certification authorities that provide services to the public.

9. Following its April 1997 policy statement on electronic commerce ("A European Initiative in Electronic Commerce"), the European Commission has now issued a proposal for

[5] "Ensuring Security and Trust in Electronic Communications - towards a European Framework for Digital Signatures and Encryption", October 1997, COM(97)503.

[6] Those interested in the progress of this Directive should contact nigel.hickson@ciid.gov.dti.uk.

a Directive on certain legal aspects of electronic commerce in the internal market, to remove legal barriers to electronic commerce. Its key objective is to ensure the freedom to provide services by addressing areas considered to be hindering the development of electronic commerce in the single market. It focuses on creating a framework within which European business, and Small and Medium Enterprises in particular, will have the legal certainty needed to take full advantage of the opportunities offered by electronic commerce.

10. The Electronic Commerce Directive is intended to complement, not overlap with, other Directives, such as that on electronic signatures. The "country of origin" principle is considered fundamental to achieving this aim - provided that the activities of the party providing the service comply with the national law of the Member State in which they are established other Member States would not be able to restrict or hamper the provision of the service on their own territory. This principle is subject to a number of exceptions, notably "contractual obligations concerning consumer contracts", and copyright. The main areas addressed are:

- simplifying and clarifying rules of establishment to ensure that both consumers and business benefit from the confidence of knowing whose laws apply;
- ensuring consistency in approaches to commercial communications such as definitions of advertising, restrictions on the regulated professions etc.;
- ensuring legal validity of electronic contracts; and
- clarifying the liability issues of intermediaries who transfer information from supplier to consumer, but may not be aware of its content or legality.

Negotiations have begun on the draft Directive in Brussels and the DTI has separately sought comments from interested parties[7].

11. The Government sees its proposals for powers to allow lawful access to encryption keys as being in line with the October 1997 European Commission Communication. This recognised the competence of Member States with regard to the areas of national security and law enforcement. It further recognised that the abuse of encryption will cause problems for law enforcement.

[7] For further information (including the text of the draft Directive), please consult the DTI Website at http://www.dti.gov.uk/cii/ecomdirective/index.htm, or to request a hard copy of the Directive contact Tracey-Anne Clough at ecom@ciid.dti.gov.uk or by fax on 0171 215 4161.

"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."

"…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."

European Commission Communication "Ensuring Security and Trust in Electronic Communication."

12. In May 1998, the Justice and Home Affairs Council of the European Union adopted formal Conclusions on encryption and law enforcement.[8] While acknowledging that encryption has substantial benefits for electronic commerce and the privacy of individuals, the Council recognised that lawful access to encryption keys by law enforcement agencies may be necessary in order to protect citizens from crime and terrorism. The Council concluded that any lawful access measures put in place by Member States must be proportionate and be balanced against other important interests such as civil liberties and the functioning of the internal market. The Government considers that its proposals meet these requirements.

OECD DISCUSSIONS ON CRYPTOGRAPHY

13. This policy is entirely consistent with the OECD Guidelines[9] on Cryptography Policy. The OECD acknowledged that governments have a responsibility to promote commerce and protect privacy while at the same time maintaining public safety and national security. In particular, the guidelines note the need for proportionate and accountable measures concerning law enforcement access to encryption keys; an important feature of the government's proposals. With respect to encryption, the challenge is to develop balanced policies, taking account of the needs of citizens, business and government. The Government considers that its proposals achieve this balance.

> "National cryptographic policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data."
>
> "Where access to the plaintext, or cryptographic keys, of encrypted data is requested under lawful process, the individual or entity requesting access must have a legal right to the possession of the plaintext, and once obtained the data must only be used for lawful purposes."
>
> *OECD Guidelines on Cryptography.*

14. The OECD held an important Ministerial Conference in Ottawa on Electronic Commerce in October 1998. The role of authentication and cryptography in providing user trust and confidence was an important part of a broad and comprehensive agenda. One of the declarations signed by the OECD ministers (representing 29 countries) in Ottawa concerned the need for government to adapt legislation to allow electronic signature services to flourish on a global basis. Another declaration, on data protection and privacy, stressed the need for protection of user data in an on-line environment. The UK is fully supportive of these declarations (indeed the UK was one of the driving forces behind their creation) and will ensure our own proposed legislation reflects both their spirit and content.

---

8 European Council Doc no 8856/98 (PRESSE 170/G).

9 Cryptography Policy: The Guidelines and the Issues (27 March 1997) available at *www.oecd.org*

UNCITRAL UNIFORM RULES ON ELECTRONIC SIGNATURES

15. UNCITRAL[10], the UN body most concerned with electronic commerce, has for some time been working on the legal consequences of the development of electronic commerce. In 1996 the Model Law on Electronic Commerce[11] was finalised. It comprises model provisions for legislators to adopt when considering how to make sure that electronic commerce is legally recognised. The Model Law covers, for example, the legal recognition of electronic writing and signatures. More recently a working group has been undertaking more detailed work on Uniform Rules on electronic signatures and certification authorities. Amongst other issues, the rules note the requirement for standards to be met for Certification Authorities issuing certificates used for legal recognition, and the need for mutual recognition of "trusted" certificates on a global basis.

LEGAL RECOGNITION OF ELECTRONIC INSTRUMENTS

ELECTRONIC SIGNATURES AND ELECTRONIC WRITING

16. These proposals are intended to promote the development of electronic commerce. One of the most important ways of doing this is by ensuring that, as far as possible, the law does not discriminate between traditional and electronic ways of doing business, i.e. that the law should be "technology neutral" in its application. At present, there are circumstances where there is doubt about whether a requirement in law for a signature can be met legally using an electronic signature. The position on requirements for information to be "written" or "in writing" is clearer - such a requirement cannot, at present, be met using electronic means. It is unusual for legislation to include a definition of "writing" that is capable of extending to digital information. Moreover the Interpretation Act definition of "writing", by placing emphasis on visibility, rules out electronic "writing", which is, in essence, a series of electronic impulses.

17. These uncertainties and limitations on electronic signatures and writing are important barriers to the development of electronic commerce and electronic Government, which the Government would like to reduce. However, the Government recognises that requirements for signatures and writing have developed over many hundreds of years of custom and law. It would not be sensible to impose equivalence between traditional and electronic means of communication in one fell swoop. Such a move could have unforeseen consequences. Equally, there will be cases (e.g. the registration of births, deaths and marriages) where it is not appropriate, at this stage, to allow electronic means to be used alongside traditional means, or where further consultation and public debate would be necessary, or where it may be necessary to impose specific conditions or restrictions.

18. The Government is, therefore, considering two ways of updating the law:

- One route would be to update statutory requirements for signatures and writing individually, in primary legislation. Such an option would have the advantage of avoiding the unforeseen consequences referred to above. It would, however, take time

[10] The United Nations Commission on International Trade Law (UNCITRAL).

[11] The text of the UNCITRAL Model Law on Electronic Commerce is available at *http://www.un.or.at/uncitral/english/texts/electcom/ml-ec.htm*

to assess the pros and cons of updating each individual requirement and, once a decision had been taken, would require time to be found in the timetable for primary legislation.

- The other option would be to take powers in primary legislation to enable the Government to amend legislation, by statutory instrument, on a case by case basis to facilitate legal recognition of electronic signatures and writing. Such an approach would allow the Government to adopt a tailor-made approach by introducing the recognition of electronic transactions gradually, after full consideration of the consequences in each case, but without the delay of having to find time in the legislative timetable. However, the Government recognises that there might be concerns about seeking Parliament's approval for powers to make such wide-ranging changes by means of secondary legislation. To assuage such concerns the Government would ensure that any powers were tightly focused on the specific objective of legal recognition of electronic means, and subject to appropriate safeguards.

The Government would welcome views on the appropriate means of ensuring legal recognition of electronic signatures and writing.

19. The Government has already set out its intention that licensed Certification Authorities, conforming to the procedural and technical standards which such licensing will confer, would be in a position to offer certificates to support electronic signatures reliable enough to be recognised as equivalent to written signatures[12]. This will be done by creating, in statute, a rebuttable presumption that an electronic signature, meeting certain conditions, correctly identifies the signatory it purports to identify; and, where it purports to guarantee that the accompanying data has not been altered since signature, that it has not. The exact specification of these conditions has not yet been finalised, but they will need to be compatible with what is eventually agreed at EU level, where the present draft requirements for an "advanced electronic signature" (i.e. one which has equivalence to a hand-written one) are that:

a) it is uniquely linked to the signatory;

b) it is capable of identifying the signatory;

c) it is created using means that the signatory can maintain under his sole control, and;

d) it is linked to the data to which it relates in such a manner that any subsequent alteration of the data is revealed.

20. The licensing regime will be set up in such a way that an electronic signature, backed up by a certificate from a licensed Certification Authority, will automatically satisfy the conditions necessary to be regarded as legally equivalent to a hand-written signature. In other words in the event of a dispute involving an electronic signature issued by a licensed

[12] In fact an electronic signature can provide a far higher level of assurance than a manual signature, both as to the identity of the signatory (because, correctly implemented, an electronic signature is far more difficult, if not impossible, to forge) and its integrity - an electronic signature can be used to show that a document has not been altered since it was signed. This latter function cannot be performed by a manual signature with any degree of confidence.

Certification Authority, there should, in the absence of evidence as to deficiencies in the system, be no need to prove compliance with technical requirements because they will already have been investigated by the licensing authority. The intention of this is to give parties relying on an electronic signature, backed by a certificate from a licensed Certification Authority and using an "approved" signature creation device[13], a high degree of confidence that the signature is what it claims to be. Such a degree of legal recognition will also apply where a "qualified certificate"[14] is used to back up an electronic signature created by an "approved" signature creation device. This will apply equally to electronic signatures generated in the UK or in other EU member states.

21. The Government's intention is not to deny legal recognition to electronic signatures which are not backed by certificates from licensed Certification Authorities, but parties relying on them may be taking on a higher level of risk. Such a signature, which can still be shown to meet the conditions laid down in the legislation, will not be excluded from legal recognition. Moreover, the legislation will specifically ensure that any electronic signature (regardless of who the Certification Authority is, or even if there is no Certification Authority, and regardless of what type of signature creation device is used) is capable of being given legal effect and can be submitted in evidence. However, it will be for businesses and individuals to decide for themselves whether to trust such signatures and bear the extra risk, which might arise in the event of a contractual dispute. In the event of a dispute, a party relying on such a signature may have to prove (in Court) that the standards and procedures employed were as reliable, perhaps even equivalent, to those that would be required of a licensed Certification Authority.

22. The Government also has no intention of disturbing the existing use of electronic messages between parties, usually within closed user groups, for doing business. Such arrangements, including the use of EDI (Electronic Data Interchange), have been in existence for many years in industry for messaging, invoicing and ordering goods.

OTHER POSSIBLE LEGISLATIVE CHANGES TO PROMOTE ELECTRONIC COMMERCE

23. The Government's intention is to ensure that, as far as possible, the law is technology neutral in its application, providing the same legal environment on-line as off. The proposals outlined above, on electronic signatures and electronic writing, would go some way towards achieving this. Also relevant is the draft EU Electronic Commerce Directive (see page 6) which covers the treatment of electronic contracts and provisions on the moment at which a contract is concluded. (The DTI has already received a considerable number of comments on this, and other aspects, of the Directive.) **The Government is also seeking views, subject to the constraints set out in this section, on whether there are other significant changes that should be made through UK primary legislation to promote the development of electronic commerce.**

---

[13] The method of "approving" products is currently being finalised in discussions on the EU Electronic Signatures Directive.

[14] A *qualified certificate* is one which meets the requirements of Annex I of the EU Electronic Signatures Directive and where the Certification Authority (whether or not it is licensed) meets the requirements of Annex II of the Directive.

24. Any further changes would have to unambiguously support the Government's aim of developing the UK as the best environment in the world in which to trade electronically. The Government is only likely to include additional measures in the legislation planned for the current parliamentary session where:

i) The proposal genuinely requires UK primary legislation (rather than being achievable through secondary or EU legislation, or without the need for legislation).

ii) There is likely to be a clear benefit to the UK in acting unilaterally, rather than seeking international agreement first.

iii) There is a broad consensus on what is needed so that proposals can be drawn up in order to meet the parliamentary timetable.

Nevertheless, the Government would also welcome suggestions for action on a longer timescale. The Prime Minister has set up a cross-departmental study by the Cabinet Office's Performance and Innovation Unit on electronic commerce. Ideas for longer term action will be fed into this study, which will report later this year.

EXAMPLES OF OTHER POSSIBLE LEGAL BARRIERS TO ELECTRONIC COMMERCE

25. Legal requirements for documents to be signed, or in writing, can be barriers to electronic commerce, because much legislation was originally drafted before people had conceived of being able to communicate, in a durable way, without pen and paper. There are other "accidental" barriers to electronic commerce, some of which have been considered in drafting the UNCITRAL Model Law on Electronic Commerce[15]. Requirements for writing and signatures are covered by articles 6 and 7 of the Model Law, but recipients may feel that other aspects of the model law should be brought into UK legislation (e.g. formation and validity of contracts, acknowledgement of receipt, time and place of dispatch and receipt of data messages, attribution of data messages). **The Government would welcome views on whether any of the provisions of the UNCITRAL Model Law on Electronic Commerce (other than those on signatures and writing) should be implemented by UK primary legislation**.

26. A related consideration is that there are requirements that necessitate the physical transmission, sending, delivery or publication of documents, where it might be appropriate to allow these requirements to be met by electronic means, subject to appropriate safeguards. For example, the DTI is looking at whether a provision of this kind could be used to amend the Companies Act 1985 to facilitate the electronic delivery of communications to shareholders, or the lodging of proxies by electronic means where companies so decided and where shareholders agreed. (The DTI will shortly consult separately on these Company Law proposals). The Government is also considering broadening the legal equivalence of electronic writing to encompass other digital data, e.g. images, audio-visual and similar applications that are likely to develop in the future. The intention, as with the provisions on signatures and writing, would be permissive, i.e. to allow people to take advantage of the possibilities which the Information Age is opening up rather than mandate particular technologies. Such a provision, if introduced, would be broadly drafted to allow for future technological and commercial developments, to be used for a wide range of filing of and access to electronic

[15] See footnote 11.

documentation and data.

OTHER LEGISLATIVE POSSIBILITIES

27. One of the great advantages of digital data is the ease of manipulating and changing content and the vanishingly small marginal cost of reproduction and distribution. This is already bringing great benefits to the economy and society, by reducing the costs for new businesses to enter new markets, thereby promoting competition and reducing prices and also making it easier to publish and distribute information globally. In this section the Government is seeking views on whether it should act on two particular consequences of these changes.

Unsolicited e-mail (SPAM)

28. "Spamming" is the sending of unsolicited e-mail for the purpose of commercial advertising, either to newsgroups or individuals. It presents issues similar to those of junk mail in the non-electronic world such as customer annoyance, but can also clog up the service provider's service and result in costs being incurred by both end-user and service provider. In addition, the ease and low cost of sending e-mails may mean that "spam" becomes more of a problem than physical junk mail or junk faxes.

29. Although the global nature of electronic commerce makes it difficult for the UK to act on "spam" if it originates overseas, the UK Internet industry has taken a number of useful measures to tackle unsolicited e-mail:

- Most Internet Service Providers (ISPs) have systems installed aimed at combating unsolicited mails, and the London Internet Exchange (LINX) aims to finalise their best practice guidelines for ISPs on dealing with spam later this year.
- The Direct Marketing Association (DMA) is working with the US DMA to develop a world-wide e-mail preference scheme (similar to the mail, telephone and fax preference schemes offered, but at an international level). The DMA is hoping to operate as the UK chapter of a global scheme, which would operate as an opt-out scheme.
- Some ISPs may individually offer opt-in schemes to gain commercial advantage.

30. The EU Distance Selling Directive (97/7/EC) contains provisions requiring Member States to enable consumers to register their objection to receiving unsolicited e-mails sent for the purposes of distance selling, and to have their objections respected. The UK and other Member States are obliged to implement this Directive by 4 June 2000, and the DTI is consulting[16] on its implementation. However, the Distance Selling Directive does not apply to business-to-business transactions and certain contracts are excluded including those relating to financial services. The EC Telecoms Data Protection Directive (97/66/EC) also contains provisions on unsolicited direct marketing but it does not apply to e-mail (spamming).

31. The Government believes that such industry self-regulatory initiatives, taken together with the EU legislation, are likely to be efficient and effective at tackling the problem of "spam". They should certainly be given an opportunity to work before further government regulation is contemplated. But, if industry approaches prove ineffective, further legislation may become necessary. **The Government would welcome views on whether the industry solutions being developed to combat spam are likely to be effective. Or should the**

[16] DTI publication number URN 98/771 which is available at http://www.dti.gov.uk/cacp/ca/distcon.htm

Government take further steps to regulate the use of spam? Some possibilities are illustrated in the box below:

Possible additional tools for dealing with "spam"

- Extending the EC Telecoms Data Protection Directive provisions to the use of e-mail.
- Further legislation to enforce service provider contracts to prevent the sending of unsolicited bulk e-mail. This would enable ISPs to determine their own policy with regard to "spammers" but could aid them in bringing action if the contract were violated.
- Prohibition of "spoofing" (mis-representation of the origin of the e-mail), to aid the tracking of "spammers" and any filtering.
- Establishment of labelling to support "anti-spoofing" measures and customer registration lists, e.g. by attaching the word 'advertising' to all commercial e-mail.

The role of intermediaries in electronic commerce.

32. The next section of this document elaborates the Government's proposals for voluntary licensing of Trust Service Providers, a particular kind of intermediary. One of the interesting aspects of electronic commerce is its effects on intermediaries in general. On the one hand some traditional intermediaries (e.g. retail outlets and travel agents) may lose business and see their profit margins squeezed as consumers find it easier and cheaper to buy certain products and services direct. At the same time many people believe that "internet-friendly" intermediaries will do very well, as testified by the recent spectacular rise in the prices of various internet shares. Many believe that, although the internet reduces entry costs for new businesses, brand names may become even more valuable in the on-line marketplace. The reason being the challenge that crops up time and again in this area – the challenge of generating trust on-line. The growth of electronic commerce may see the development of new types of intermediary, to make the market between purchasers and suppliers function better. **The Government would like to start a debate on whether any changes are needed to existing legislation to allow such intermediaries to prosper and would welcome views**. The box below outlines some of the functions that such intermediaries might perform. It is, however, unlikely that early legislation will be introduced in this area because the legislative issues are, as yet, unclear.

Possible roles for intermediaries in the electronic marketplace

Benefits for the consumer

- Guarantees of: order fulfilment, fitness for purpose etc.
- Collection and management of purchasing preference information (through data capture on transactions routed through the intermediary and without effort by the consumer) and its release under direct consumer control.
- Management of commodity purchases, at 'best buy' prices from multiple sources. (e.g. stationery for a Small or Medium Enterprise, or non-perishable goods for a domestic consumer)
- Management of inventory and updating (for example on software purchased or for insurance purposes).

Benefits for vendors

- Guarantees of payment.
- Local customer service and support.
- Authorised access to detailed consumer preference information, to be used in highly targeted one to one marketing and follow up.
- Access to authoritative, anonymised, data on general market development and trends.

LICENSING REGIME FOR TRUST SERVICE PROVIDERS (i.e. PROVIDERS OF CRYPTOGRAPHY SERVICES)

Cryptography, keys and how they can be used as a signature ...

The non-specialist might find an explanation of some jargon helpful at this point. One way of providing electronic signatures is to make use of what is known as *public key, or asymmetric, cryptography*. Public key cryptography uses two keys, also known as a *key pair*. (These keys are both large numbers with special mathematical properties). When this technique is used for signatures, the *private key* (which, as the term suggests, is only known to its owner) is used to transform a data file, by scrambling the information contained in it. The transformed data is the electronic signature, and can be checked against the original file using the *public key* of the person who signed it. Anyone with access to the public key (which might, for example, be available on a website) can check the signature, so verifying that it could only have been signed by someone with access to the private key. If the only person with access to the private key is its owner, then the owner must have signed the message, and cannot later deny having signed it (*repudiation*). If a third party altered the message, the fact that they had done so would be easily detectable.

...and for confidentiality.

The public key cryptography described above can also be used to keep a message, or some stored data, secret. The person sending the message would take the public key (a different pair of keys is usually used for signing and confidentiality) of the intended recipient, and use that key to scramble the message. Only the corresponding private key can be used to unscramble the message. This is what the intended recipient (whose public key was used to scramble the message) would do to read it. A third party would not be able to read the message without access to the intended recipient's private key.

33. In addition to providing for the legal recognition of electronic signatures and writing, the Government believes that it needs to do more to promote electronic commerce. Electronic signatures can be used to ensure the *integrity* of information (ensuring its content has not been altered) and to *verify* the author of the information. Another concern, particularly for those using open networks such as the internet, is *confidentiality* (keeping electronically transmitted information secret). But such technologies are complicated, and unfamiliar to many people. The Government has an important role in ensuring that users can trust both the technologies that allow such security and the commercial organisations providing it. Hence the introduction of voluntary licensing arrangements for bodies offering cryptographic services to the public, to generate confidence and thereby promote the market by ensuring that minimum standards of quality and service are met. The Government believes that users will require a high level of trust before the use of such services becomes widespread, especially for 'open' transactions. The level of trust required is, perhaps, similar to that required of a bank, or of a solicitor. These well-established services are trusted both because they are regulated and also because of the familiarity that has grown through a history of being able to rely on such services. Building such trust, virtually overnight, in the electronic world will not be easy. We recognise, however, that electronic signatures and encryption will also be provided in "closed" environments where trust already exists between the counterparties and "trust" in the provider may be less important. This is why the Government has opted for a voluntary but statutory regime.

34. This section expands on how the Government sees this licensing regime working. However, not all of this detail will be in primary legislation. The intention is for primary legislation to give the Government power to bring forward secondary legislation (Statutory Instruments) through which much of the detail will be implemented. The DTI will, of course, continue consulting on these details. The DTI's initial thinking on the licensing conditions is set out in Annex A, **and we would especially welcome views on this annex**.

35. The Government is committed to a clear policy differentiation between electronic signatures and encryption. This reflects the valid concerns expressed by industry during the consultation process launched by the previous administration, and recognises the different commercial applications of these services and the different challenges they pose to Government policy. The main differences in policy for signatures and encryption are as follows:

- Licensed Certification Authorities will not be allowed to store the private key of a key pair that is issued solely for electronic signature purposes. The responsibility for

protecting a private signature key will therefore fall unambiguously on its owner. This should encourage confidence in electronic signatures, by helping to prevent repudiation.

- There will be no access by law enforcement agencies to private signature keys (wherever they are held), unless such keys have been used to encrypt information for confidentiality purposes.
- The licensing criteria (see Annex A) clearly distinguish between providers of signature services, and providers of confidentiality services.

36. Organisations offering confidentiality, or encryption, services (e.g. key management services) where cryptography is used to protect the content of stored or transmitted data will also be encouraged to apply for licences. Businesses are increasingly recognising the importance of being able to recover critical data, which staff may have encrypted, or the text of messages they have sent to clients. The loss of an encryption key, whether through negligence, or because an employee has left etc., could be very damaging. Providers of confidentiality services are, therefore, encouraged to make the recovery of keys (or other information protecting the secrecy of the information) possible through suitable storage arrangements, or by means of key encapsulation products[17].

37. The widespread deployment of such technologies would also help law enforcement, by allowing law enforcement agencies to recover encryption keys under strictly regulated procedures. The Government is well aware of the controversy, both in the UK and abroad, over the degree to which Governments should encourage, or even mandate, the use of such key escrow and key recovery technologies. Given the differing views on the practicability, cost and desirability of this, the Government has decided to consult on the basis that neither key escrow nor third party key recovery will be requirements of having a licence for confidentiality services. Users of confidentiality services will be free to decide for themselves whether to use such services. There will be no requirement for users of encryption to store keys, but those who do not make some arrangements will risk the loss of data in the event of losing their confidentiality key.

38. This document has, so far, concentrated on two types of service: signature services and confidentiality services. The voluntary licensing regime will also cover Key Recovery Agents (see footnote 17). The Government's proposals are intended to promote the market for cryptography services and are not limited to these particular services, or technological implementations of them, or particular business models. The boxes below provide some examples of services which will be eligible to apply for licences under the proposed regime. They are intended to be illustrative, rather than prescriptive **and we would welcome**

[17] An alternative to the use of Trusted Third Parties (TTPs) and key escrow is the use of encryption products which support *key recovery*, also known as *key encapsulation*, (confusingly key recovery can be used as a generic term to cover both key storage or "key escrow", and key encapsulation; we only use it in the narrower sense in this document). Such commercial encryption products, which are already being used in the US, can incorporate the public key of an agent (usually a company) known as a *Key Recovery Agent (KRA)*. This allows the user of such products to recover their (stored or communicated) data by approaching the KRA with an encrypted portion of the message. Lawful access to the keys (which are likely to be different for each message) can also be granted if a written authorisation is served on the KRA. In both cases, namely access by the user or by law enforcement, the KRA neither holds the user's private keys, nor has access to the plaintext of their data.

comments on them. **We recognise that various organisations are considering different business models for providing cryptography services to the public and would welcome views on how they should fit into the licensing regime.**

ILLUSTRATIVE EXAMPLES OF CRYPTOGRAPHY SERVICES

One way of providing electronic signatures is to use asymmetric cryptography (see box on page 17) and sign a message with a private key; the recipient of the message can verify it with the corresponding public key. In this paper the term **Certification Authority** (CA) is used to encompass a number of potential services. It is likely that additional "value added" services will also be provided (see below). Certification Authority services include:

Registration:	The function of verifying the credentials of someone who, for whatever purpose, applies for a public key certificate. This will, inter-alia, include checking the identity, or other attributes, of the person applying for the certificate.
Certification:	The function of issuing a certificate (perhaps as part of the registration process) which asserts that the public key belongs to the named holder.
Key Generation:	Key generation is a critical part of the process whereby the key pair (both public and private) is generated for the issue of a certificate.
Certificate Revocation:	Certificates will require revocation for a variety of reasons, including natural expiry, amendment, unauthorised disclosure of the private key or a breach of contract by the certificate holder. Once revoked it is essential, as part of this service, that the Certification Authority, or their agent, makes the fact available to anyone reasonably relying on the certificate. Such a process would normally include the publication of the revoked certificate in a published list.

It is also envisaged that licences would be available for bodies providing:

Directory services:	The establishment of a public access register where public keys (either for signature or confidentiality) are securely held and updated in respect of revocation knowledge.
Time-Stamping:	A service whereby evidence can be presented that a specific electronic document existed, or that some event took place at a specific time.

39. Given the range of services that may be covered by the licensing regime, the question arises of how to avoid confusion when an organisation wishes to offer services both within and outside the licensing regime. One option would be to require that a body holding a licence for any cryptographic service covered by the licensing regime would be expected to be licensed

for any other cryptographic services which it decided to offer. Such an approach might prove to be inflexible given the rapid development of electronic commerce, by stifling innovation and the development of new value added services. Some have argued that it would be against the spirit of a voluntary licensing regime. It is important, however, to avoid sending confused messages to consumers about the quality of a particular cryptographic service. **The Government would therefore welcome views on how best to distinguish between the provision of licensed and unlicensed services in order to protect the consumer.**

THE LICENSING AUTHORITY

40. The Government intends that the power to issue and modify licences and monitor compliance against the licensing conditions would be conferred on the Secretary of State for Trade and Industry. The Secretary of State would have the power to delegate some of these powers to another body, who will have the powers to contract out some of its functions if necessary. The Government will consider carefully the details of any such delegation and may decide to retain some aspects of licensing within the DTI, rather than delegate all of its powers.

41. The key objective in setting up the voluntary licensing regime is to promote confidence among consumers that licensed bodies can be trusted. The licensing framework therefore needs to be rigorous, impartial and trusted by all sectors of industry. That is why we have opted for a statutory approach. The Government recognises that work is being done by industry to develop a self-regulatory approach and will want to build on that work in setting up the statutory regime. However, this is currently in its infancy, is not yet operational and has yet to be endorsed by all industry sectors. It is therefore appropriate that a statutory body should be responsible for overseeing the voluntary regime, although some of the responsibility for vetting individual applicants might be delegated to outside agencies. The Government has decided that they are likely to designate OFTEL as the initial licensing authority. Both DTI and OFTEL will work very closely with the industry in developing the standards to be met by licensed bodies, but the aim of promoting consumer confidence will best be achieved by making a statutory body responsible for initial assessment and enforcement of compliance with those standards. Indeed, OFTEL is also likely to contract out some of its functions as the licensing authority to industry. The Government does not rule out delegation of some or all of the licensing functions to an industry body in future.

LIABILITY

42. **The Government recognises that the issue of liability is a key concern of industry and would particularly welcome views on the issues set out in this section.** Liability in the world of electronic commerce is complex and the Government recognises the need to balance the interests of the various parties who may be involved, either directly and indirectly, in a particular transaction. Applying the principle that policy should be technology neutral, liability in the electronic world should, as far as possible, match that in the traditional world. However, given that there are no direct analogues of cryptography services in the world of pen and paper transactions some special rules may be needed. **Some general questions are:**

- **Is there a need for specific legislation?**

- **To what extent should liability be prescribed by legislation?**
- **Should legislation impose specific requirements to state the liability regime in contracts and on certificates, and other instruments which third parties might reasonably rely on?**

What minimum level of liability should be taken on by all providers of cryptography services, regardless of whether they are licensed or not?

43. A minimalist approach would be to rely solely on the contract between the service provider and their client. However this would allow a service provider the option of contracting out all of their liability and might also give a third party, e.g. someone relying on an electronic signature, no protection at all. In any case, the present draft EU Directive would make a Certification Authority liable, to any person reasonably relying on a qualified certificate[18] issued by them, for the accuracy of the information contained in it. **The Government would welcome views on what level of liability, if any, should be borne by an unlicensed Certification Authority.** The Government believes that existing law on liability is sufficient to cover unlicensed providers of other cryptography services, and that no specific additional requirements are needed.

What liability regime should apply in respect of licensed providers of cryptography services?

44. The aim of the licensing regime is to generate confidence in licensed providers. The public will need to be assured that a service, by virtue of being licensed, is high quality. There is a clear need to balance the competing demands of:

- the purchaser of a licensed service, who will expect the licence to offer some guarantee of quality, e.g. a customer will expect due care to have been taken in generating their signature key pair, and someone buying a confidentiality service will expect the TTP to take proper care of their private confidentiality keys if they store them;
- a third party relying on a licensed service, who will have similar expectations, e.g. that what is stated on a Certificate is true and that the Certification Authority will have some liability if it turns out to be false, and has an effective revocation policy;
- the service provider, which will need to be able to manage and limit on its liability and would not apply for a licence if being licensed meant taking on unlimited liability. A cap on liability would constitute an advantage of being licensed by reducing the cost of liability insurance.

45. The Government's initial view is that these competing demands could be reconciled by imposing a limit on liability[19], which cannot be decreased by contractual terms, on licensed service providers. Different levels would probably be set for different services. The consumer would be protected by knowing that a licensed provider was taking on a certain level of liability (of course, licensed providers would be free to offer higher levels). The provider's interests would also be protected by having a cap on their liability (which they can choose to

[18] See footnote 14.

[19] The EU Electronic Signatures Directive does not at present include any financial limits on liability. The Government will need to be satisfied that any such limits are consistent with the Directive before including them in UK legislation.

increase, if that is in their commercial interests). **The Government would welcome views on this approach, how the limit should be set, or suggestions for alternative approaches.**

Also should a specific "duty of care" be imposed on holders of private signature keys (e.g. to keep their private key secure, to notify a Certification Authority within so many hours of realising it has been compromised etc.)?

Are there any other liability issues concerning cryptography services which need to be addressed in legislation?

LICENSING FEES

46. Licensing fees will be set in proportion to the amount of work involved in assessing a licence application and in monitoring ongoing compliance with, and securing enforcement of, the licensing conditions, i.e. to cover the licensing authority's costs. The licensing fees will be set by the licensing authority. It is likely that the work involved, and therefore the fees charged, would vary for different services.

EXPORT CONTROLS

47. The proposed legislation will not, in itself, affect the current export controls on cryptography products, which are shaped by our international agreements. However, it is likely that it will be possible to streamline the procedures for the export of cryptographic products which facilitate legal access through a third party (such as products incorporating key storage or key recovery). One way of doing this might be to permit the export of such products which met set criteria under an open licence after a one time review.

LAW ENFORCEMENT INTERESTS IN CRYPTOGRAPHY

48. Cryptography provides clear benefits to commerce, industry and individuals. Banks rely on cryptography, for example in their payment systems and in cash dispenser machines. It will also help to prevent crime over the internet. For example, cryptography can make it much more difficult to defraud companies and individuals; and cryptography can be used to protect intellectual property. But criminals are quick to take advantage of new technologies and there is no doubt that serious criminals (e.g. drugs traffickers, terrorists and paedophiles) will exploit encryption in an effort to defeat the work of law enforcement agencies. Indeed, this is already starting to happen. The Government therefore has the dual responsibilities of promoting and facilitating the lawful use of encryption by business and others, and making it as difficult as possible for criminals to exploit it for their own purposes.

WHY DOES ENCRYPTION POSE A SERIOUS THREAT TO LAW ENFORCEMENT?

49. A number of recent investigations into a variety of serious criminal offences in the UK have been hampered by the discovery that material which might otherwise assist the investigation, or be used in evidence, has been encrypted. The problem is increasing. Law

enforcement agencies often try to "crack" the encryption key. Although this is occasionally possible after considerable effort and expense, it is likely to become increasingly difficult - if not impossible - as the technology develops.

50. The following examples give an indication of the nature of the problem (there are many others that cannot be disclosed for a variety of reasons including that they remain sub judice):

Crime:

- In 1998, police enquiries into a case of attempted murder and sexual assault were impeded by the discovery of encrypted material on a suspect's computer. The investigation was able to proceed only after the relevant encryption key was discovered by the police amongst other material seized from the suspect.
- There are numerous cases of paedophiles using encryption to conceal their illegal activity from the attentions of law enforcement. In 1995, for example, two suspected paedophiles were arrested by police in the UK on suspicion of distributing child pornography on the internet. Their computer systems were found to contain pornographic images of children and, in the case of the leading suspect, a large amount of encrypted material. The indications were that the suspects had used encrypted communications to distribute child pornography to contacts around the world via e-mail. Although both paedophiles were subsequently convicted of distributing child pornography, the police investigation into the leading suspect was severely hampered by the fact that he had used encryption.

Fraud & financial crime:

- The Serious Fraud Office currently estimates that in approximately 50% of its cases, some form of encryption is encountered. Instances of computer files protected by various complexities of encryption have been found in a number of recent investigations. The problem is growing, and attempts to overcome the encryption are absorbing resources which could otherwise be deployed elsewhere.
- Commercial interests face a range of potential threats from improper use of encryption. Individuals involved in corporate espionage and insider theft will naturally be drawn to encryption devices as a means of concealing their activities. There have been attempts to extort money from businesses by placing enciphered viruses into computer systems (so-called cryptoviral extortion). Law enforcement agencies would be better able to investigate such criminal activity if they had a power to obtain relevant encryption keys.

Terrorism:

- There are already examples of terrorists in the UK using encryption as a means of concealing their activities. In late 1996, a police operation culminated in the arrests of several leading members of a Northern Irish terrorist group and the seizure of computer equipment containing encrypted files. The files held information on potential terrorist targets such as police officers and politicians. The data was eventually retrieved but only after considerable effort.

International examples:

The following examples demonstrate that the use of encryption by criminals and terrorists is a global problem:

- In the US, the FBI found that the laptop computer belonging to Ramzi Yousef (who masterminded the terrorist bombing of the World Trade Centre in 1994 and of a Manila airliner in late 1995) contained encrypted files concerning a terrorist plot to blow up 11 US owned commercial airliners.
- In Japan, the Aum Supreme Truth Cult which was responsible for the release of Sarin nerve gas in the Tokyo subway in March 1995, killing 12 people and injuring some 6,000 more, stored its records on encrypted computer files. The authorities were able to decrypt the files and the evidence they found was crucial to the investigation.

The Director of the FBI has said:

"…the encryption issue is one of the most important issues confronting law enforcement and potentially has catastrophic implications for our ability to combat every threat to national security…Law enforcement remains in unanimous agreement that the widespread use of robust non-recovery encryption will ultimately devastate our ability to fight crime and terrorism…"

Statement to the Senate Select Committee on Intelligence; 28 January 1998

THE GOVERNMENT'S RESPONSE

51. The Government has a duty to maintain the effectiveness of existing legislation which enables the law enforcement, security and intelligence agencies to fight crime and threats to national security. New technology - particularly commercial encryption systems - presents new challenges for these agencies. There is no simple solution. The Government's response has three key elements: an updating of existing statutory powers to take account of the widespread use of encryption; encouraging the deployment of key escrow and key recovery technologies and working with industry and other interested parties to find other ways of mitigating the effects of the use of encryption by those seeking to evade the law or threaten our national security.

COMMON MYTHS

52. It is worth dispelling a number of myths about the Government's proposals:

- They do not impose a mandatory requirement on the business community or individuals to use key escrow or key recovery technologies when encrypting communications.
- Individuals and businesses will remain free to use any encryption product on the market.
- They are technology neutral and do not extend the intrusive surveillance powers of the

law enforcement, security and intelligence agencies. The purpose of the proposals is simply to maintain the effectiveness of existing legislation. The "decryption" powers will apply only where access to the encrypted information is already available under the existing law.

THE NEED TO UPDATE EXISTING LEGISLATION

53. The Government is determined to ensure that the widespread use of encryption does not significantly undermine the effectiveness of the existing statutory framework for law enforcement, security and intelligence agencies. But that is the limit of its intention. The Government does not intend to use the new measures to extend, either directly or indirectly, its intrusive surveillance powers. On the contrary, the new powers will include strong safeguards to prevent unauthorised access to encryption keys.

54. There are two obvious areas where encryption presents a serious threat to the effectiveness of existing legislation: interception of communications; and statutory powers of search and seizure.

INTERCEPTION OF COMMUNICATIONS ACT 1985

55. Under the Interception of Communications Act 1985 (IOCA), interception of any communication (including email) on a public telecommunications network requires a warrant to be signed by the Secretary of State. Interception may only be authorised where this is judged necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose of safeguarding the economic well-being of the United Kingdom. The Secretary of State authorises interception only when he is satisfied that it is necessary in order to acquire information which could not reasonably be obtained by any other method. The Act contains a number of safeguards, including the provision of a Commissioner and Tribunal who have wide powers to oversee the operation of the Act and investigate complaints.

56. Interception of communications has long been an essential tool in the fight against serious crime and threats to national security. It is long standing policy not to disclose details of interception operations so as not to prejudice ongoing investigations. But the following figures give an idea of the value of the existing power. During 1996 and 1997, lawful interception of communications played a part – often the crucial part – in operations by police and HM Customs which led to:

- 1,200 arrests;
- the seizure of nearly 3 tonnes of Class A drugs, and 112 tonnes of other drugs, with a combined street value of over £600 million;
- the seizure of over 450 firearms.

During this period, around 2600 interception warrants were issued by the Home Secretary. (In line with the practice of the Interception Commissioner, this figure relates to all warrants issued by the Home Secretary, not just those for the police and customs.)

57. The Government has decided to review existing interception legislation, as the Home Secretary announced to the House of Commons on 2 September 1998:

> "Profound changes in the technology of electronic communication have taken place in the past decade, and they, together with the decisions of the European Court in Strasbourg, have made new consideration of the regime imperative....I can therefore announce to the House today that, earlier in the summer, I had already put in hand a comprehensive review of the interception regime, and a consultation document on this will be published in due course."

58. The review of the interception legislation is underway. It is not the purpose of this document to pre-empt its wider conclusions. But the Government needs to take action now to protect the effectiveness of the existing interception regime. Encryption is not only used to protect the confidentiality of computer files and e-mail communications. It is also possible, with suitable equipment, to encrypt speech over the telephone. The convergence of telephony and computer technologies will make it easier for encrypted speech and data to be sent over a range of networks. It is therefore necessary to introduce a power to enable the intercepting agencies to decrypt communications. This means providing a power for lawful access to encryption keys. Without such a power, the widespread use of encryption represents a serious threat to the effectiveness of interception as a valuable and legitimate tool for law enforcement, security and intelligence agencies.

POWERS OF SEARCH AND SEIZURE

59. Under the Police and Criminal Evidence Act 1984 (PACE), the police may apply to the Courts for a search warrant under which material, including stored data, can be seized if it is covered by the warrant or where there are reasonable grounds for believing it is evidence of an offence or has been obtained in consequence of the commission of an offence. PACE also contains powers for the Courts to order the production of such material. Similar powers exist in other legislation (for example, the prevention of terrorism legislation).

60. It is important to recognise that PACE provides the police with powers of search and seizure which do not require a judicial authorisation in certain circumstances (for example, powers of entry and search after arrest and powers of search upon arrest).

61. PACE also contains provisions to assist the police in the seizure of computerised information. Section 20 of PACE states that powers of seizure conferred on a constable who has entered premises under statutory authority (including any enactment contained in any Act passed before or after PACE) shall be construed as a power to require any information contained in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible.

62. In effect, therefore, the police already have a power to require an individual to produce computerised information in a visible and legible form. But this does not provide the police with a clear legal basis to require disclosure of encryption keys in order to decrypt seized material. Although the police may have a lawful power to enter premises and seize computer files, encryption means that it is no longer necessarily the case that the police will be able to

read the content of the files.

63. The Government believes it is necessary to establish a new power to allow the police to require disclosure of encryption keys to maintain the effectiveness of existing statutory powers of search and seizure. This will not give law enforcement agencies any new power to seize information. Nor will it undermine the additional safeguards in PACE for access to sensitive material (for example, material subject to legal privilege; personal records held in confidence that are acquired in the course of any trade, business or profession; journalistic material; or confidential medical information).

By way of an illustrative parallel in the physical world, consider a locked safe containing evidential material. Where an officer has the power of search, he may use reasonable force to open the safe where the occupier of the premises, or another person entitled to grant access, has refused entry to it. It is difficult to imagine circumstances in which the police cannot break into a locked safe when they need to do so. But it is becoming increasingly common for the police to seize a computer containing encrypted evidential material where no amount of reasonable force will break the encryption and provide access to the material it contains. That is why new powers are needed.

LEGISLATIVE PROPOSALS

64. The Government proposes to establish a power to require any person, upon service of a written notice, to produce specified material in a comprehensible form or to disclose relevant material (e.g. an encryption key) necessary for that purpose. The ability to serve a written notice will be ancillary to existing statutory powers such as those contained in IOCA and PACE. This means that it will apply only to material which itself has been, or is being, obtained lawfully.

65. The new power will not make access to any encrypted communications or data lawful if it would otherwise be unlawful. For example, it is an offence to intercept communications on a UK public telecommunications network without a warrant issued by a Secretary of State. It will not be possible to obtain the Secretary of State's authorisation for access to encryption keys to decrypt unlawfully intercepted material.

66. The new power will, so far as possible, be technology neutral. For example, it is becoming increasingly difficult to draw a distinction between an encryption key and a password. In practice, they often serve the same purpose.

67. The Government intends to allow written notices to be served only:

- where the Secretary of State has given specific authority to require decryption of intercepted communications obtained under warrant or, in the case of the security and intelligence agencies, where he has given a specific authority which he believes is likely to be of substantial value in assisting the agencies in carrying out their statutory functions;

- where judicial authority exists under a statutory provision to search, seize, produce or otherwise obtain the protected material;

- where certain types of non-judicial statutory authority (e.g. under Section 18 of PACE, which provides for powers of entry and search after arrest) exist to search, seize or otherwise obtain the protected material. In these circumstances, it will be necessary to seek specific authority at an appropriate level (e.g. a police officer of superintendent rank or above).

- where a judicial warrant has been obtained for the specific purpose of decrypting material lawfully in the possession of a law enforcement agency.

68. The Government is not proposing to enable agencies to have access to encryption keys used solely for digital signature purposes. The power to require the disclosure of keys or material in a comprehensible form will apply to licensed and unlicensed providers of encryption services. It will also apply to other parties holding relevant keys. But this will not impose any requirement on anyone to retain copies of private encryption keys.

69. The written notice will specify the keys or material required to be disclosed. It will be for an authorised officer to decide, given the circumstances of a particular case, whether to order the production of specified material in a comprehensible form (e.g. the plaintext of a document) or order disclosure of the relevant confidentiality key. The written notice will also specify the particular authority under which it has been served and will contain sufficient information to ensure a clear audit trail for any future enquiries.

70. There are concerns about powers to require suspects to disclose their encryption keys, with some arguing that this would result in self-incrimination. The Government does not believe that its proposals would amount to self-incrimination. The proposed power will enable evidence already in the possession of law enforcement agencies to be made comprehensible, rather than requiring a suspect to disclose evidence. There are numerous examples where suspects are required to comply with statutory obligations for the purpose of maintaining the effectiveness of criminal investigations (e.g. requirements to provide fingerprint and DNA samples, or to produce documentary evidence of vehicle insurance cover). Without powers to make electronic evidence comprehensible, criminals would be able to conceal their activities with complete impunity. The Government does not believe that this would be in the public interest.

71. The Government is considering how the lawful access provisions will apply to the different policing regimes which exist in Scotland and Northern Ireland. For example, the provisions of PACE do not apply in Scotland where the law on search warrants is generally covered by the common law except in relation to certain specific forms of search covered by statutory provision. Also, there is no equivalent to the power contained in Section 20 of PACE (which assists the police in the seizure of computerised information).

Safeguards

72. The legislation will not allow for wholesale collection of encryption keys. The new

powers will come into effect only where access to the encrypted communication or data has been provided under existing legislation. It will operate only on a case by case basis.

73. There will be additional statutory safeguards to ensure that written notices are served only where necessary and appropriate. The Government will supplement these safeguards by a published Code of Practice governing the exercise of the new powers.

74. The proposed legislation will also contain strong safeguards protecting the security and privacy of encryption keys obtained under a written notice. These are likely to be analogous to those contained in Section 6 of IOCA which requires the Secretary of State to satisfy himself before issuing an interception warrant that proper safeguards are in place for the handling, disclosure, copying and destruction of intercepted material. The legislation will make it a statutory requirement for material obtained under a written notice to be destroyed as soon as its retention is no longer necessary for the purpose for which the notice was issued.

Oversight and complaints

75. The Government intends to establish oversight and complaint mechanisms for the exercise of the powers of the Secretary of State in a similar manner to those established under IOCA. In particular, this will mean that there will be independent judicial oversight of the Secretary of State's authorisation powers. The Government envisages establishing a Commissioner and Tribunal to oversee the Secretary of State's powers with the power to investigate complaints and, where appropriate, award compensation.

76. Existing complaints arrangements will apply in other circumstances involving, for example, keys obtained in pursuance of search warrants or production orders issued by a court.

Offences and Penalties

77. The Government proposes to create two new offences in relation to the new powers:

- an offence of failure to comply with the terms of a written notice without reasonable excuse;

- an offence of "tipping off" an individual about the existence of an authorisation by the Secretary of State allowing lawful access to an encryption key.

78. The offence of failure to comply is necessary to ensure that encryption keys are disclosed where available. The "tipping off" offence is consistent with existing legislation (e.g. on drug trafficking) and is designed to protect the confidentiality of covert investigations into serious crime. It is envisaged that the penalties for these offences will be commensurate with similar offences in existing legislation.

79. **The Government would welcome views on its proposals for lawful access to encryption keys.**

THE PARTNERSHIP APPROACH: MEETING THE NEEDS OF LAW ENFORCEMENT AND INDUSTRY

KEY ESCROW AND KEY RECOVERY BY THIRD PARTIES

80. The proposals described above rest on the assumption that, by serving an appropriately authorised written notice, it will be possible to decrypt communications and stored data. This will normally be true where the notice is served on the individual in control of the encryption process. But, in the case of interception of communications, law enforcement agencies need to be able to decrypt communications without the knowledge of that individual (for example, drug traffickers who encrypt their communications).

81. Encryption technologies involving key escrow or third party key recovery would, if widely adopted, maintain law enforcement agencies' interception capabilities while also providing benefits for the user. The Government has considered a number of options for promoting their use and development. The previous administration consulted on proposals for a mandatory licensing regime, which would have made it illegal to offer encryption services without key escrow. However, such a regime would not have prohibited the use of encryption without key escrow and might have caused significant damage to the growth of electronic commerce in the UK.

82. The Government remains keen to promote key escrow and third party key recovery technologies. However, the electronic commerce market is developing quickly. Industry has expressed serious concerns that imposing a requirement for key escrow or third party key recovery as part of the licensing scheme would place unreasonable constraints on the development of electronic commerce in the UK. That is why the Government is consulting on the basis that the licensing scheme will not impose the requirement that TSPs providing confidentiality services should have to provide for law enforcement access to keys in this manner.

THE PARTNERSHIP APPROACH

83. This should not be taken as an indication that the Government underestimates the serious consequences for law enforcement of the widespread availability of strong encryption. The Government will closely monitor the impact of its policy on law enforcement interests. At present, the impact of encryption is significant but is not having a major operational impact on the fight against serious crime. This could change very quickly.

84. The Government is committed to achieving its goal of developing the UK as the world's best environment for electronic trading, but also has a responsibility to society as a whole, by maintaining the effectiveness of law enforcement powers. The Government intends to develop a partnership with industry to identify ways of meeting law enforcement requirements while promoting the growth of electronic commerce. **The Government would welcome ideas on how its law enforcement and electronic commerce objectives might be promoted via the licensing scheme or otherwise.**

THE NEEDS OF LAW ENFORCEMENT AGENCIES

85. To facilitate this partnership, it is worth clarifying what is required by law enforcement agencies to maintain the effectiveness of existing statutory powers. In particular, there is considerable misunderstanding about the types of communications of interest to law enforcement agencies.

86. The most important requirement of law enforcement agencies is the ability to decrypt communications between serious criminals and other individuals without the knowledge of the parties to the communication. Law enforcement agencies do not normally need access to encrypted communications between legitimate corporate organisations or within other legitimate closed systems. Nevertheless, there are strong reasons (e.g. prevention of fraud) for corporate organisations to have the capability themselves to recover the plain text of communications (whether in transit or at rest).

87. A proportion of electronic commerce activity will occur between individuals and corporate organisations. Where this involves serious criminal activity, law enforcement agencies may need access to communications between serious criminals and corporate organisations (e.g. internet shopping, purchasing airline tickets etc.). However, law enforcement agencies would be content to seek the co-operation of the legitimate corporate organisation where this is necessary.

88. For interception purposes, there are a number of other important factors to be taken into account. The decryption process needs to be timely (as close to real-time as possible) and covert (i.e. the target of the investigation must not be aware that interception is taking place). Ideally, law enforcement agencies would want to be able to read communications both received and sent by the target by approaching a single organisation. The provision of plain text rather than encryption keys might be acceptable if the plain text is provided in such a way that neither the individual nor the provider of the encryption service is aware of its content.

89. The needs of law enforcement agencies in respect of encrypted stored data are slightly different. For example, a wide variety of encrypted stored data held by industry and individuals may be subject to statutory powers of search and seizure. There may also be a need for a law enforcement agency to prove in court that the plain text does indeed relate to a particular encrypted document seized during an investigation. In such cases, law enforcement agencies may require the decryption of stored data to take place in accordance with best practice on computer forensic evidence.

90. **The Government would welcome views from industry on the extent to which the needs of law enforcement agencies can be met by existing and forthcoming developments in encryption and communications technologies.**

ANNEX A - LICENSING CRITERIA

This annex lists some draft criteria against which the Government intends that licence applications would be assessed. The proposed criteria, which will vary depending on the service for which a licence application is made, have been set out for all services with some additional criteria for what are initially expected to be the most common cases: providers of signature services and providers of confidentiality services. This does not preclude the licensing regime applying more broadly to other cryptography services (e.g. to timestamping services etc.). The Government's intention is that the regime should be flexible enough to incorporate different services, as they arise, and technological advances.

These criteria are likely to be spelt out in secondary, rather than primary, legislation. The reasons for consulting now, before the primary legislation is in place, are twofold. Firstly, to ensure that the powers in primary legislation are sufficient. Secondly, to allow potential licence applicants to be involved in formulating the criteria and to start planning for them coming into effect.

PROPOSED LICENSING CRITERIA

(I) GENERAL LICENSING CRITERIA

The following criteria would apply to all licensed Trust Service Providers:

The owners and directors should be fit and proper people: This would oblige applicants to provide evidence that their controllers were competent to provide services and that they had not been disqualified in any sense (i.e. as directors).

Registered Office in UK: The address of an office (not just a "plate" address) in the UK would need to indicate where communications could be lodged. The licensee would be expected to make provision for real-time communication with those responsible for running the organisation.

Vetting Employees: The provider should have adequate procedures in place for vetting all employees (in terms of criminal record etc.) especially those who have contact with potential clients.

Financial viability of organisation: The provider will need to demonstrate that it has adequate resources to provide the services it intends to provide; this will typically involve the production of a business plan identifying sources and (if appropriate) guarantees of finance.

Business Plan: In addition to identifying sources of finance an applicant would be expected to produce a plan detailing its business strategy, its ability to survive in the market

place and any contingency plans it may have on how to withdraw from the market.

Agents: It is recognised that, in some situations, services will be carried out by more than one organisation. Where this is to take place, details of the agents will need to be supplied identifying the nature of their contractual relationship with the applicant.

Quality Management: The applicant and, where appropriate, any principal agents will need to demonstrate compliance with the relevant provisions of an appropriate quality system, e.g. the relevant provisions of ISO 9000.

Information Security Management: A provider would be expected to have obtained, or at least sought, accreditation (under the c:cure Scheme) to BS 7799.

Liability: Notwithstanding the possible requirements spelled out on page 21 of this Paper an applicant would need to demonstrate that they had the ability (i.e. sufficient financial resources) to meet any liability they wished to enter into with either their clients or third parties.

Data Protection: An applicant would be required to demonstrate that (in terms of customer data) they conform to the provisions of the Data Protection Act (1998) and other relevant legislation.

Key generation: An applicant would need to demonstrate the ability to issue separate key pairs for signatures and confidentiality services.

(II) LICENSING CRITERIA FOR CERTIFICATION AUTHORITIES

Technical Assurance: A provider will be expected to provide evidence, if appropriate, that the systems used for generating key pairs and storing its own private key has been independently assessed (e.g. through the issue of an ITSEC or CC Certificate[20]) in terms of security assurance.

Content of Certificate: An applicant will need to demonstrate that the certificates it issues have all the following information:

- the identity of the service provider;
- the name of the holder, or an agreed pseudonym;
- specific attributes of the holder (e.g. address or financial standing);
- the valid period of the certificate;
- a unique certificate number;
- an unambiguous statement that the certificate must not be used to validate a key being used to secure the confidentiality of information;
- any specific limitations on the use of the certificate (i.e. if it is limited on the value of

[20] An ITSEC or Common Criteria Certificate is one that has been issued by a Certification Body to verify that the product has been assessed as meeting certain security assurance criteria. Schemes to assess such products exist in Germany, France, the US, Canada and the UK.

transactions it can be used for);
- the identity of the CA who issued it.

Generation of Key Pair: A provider will need to submit details of how an asymmetric key-pair is generated and, if appropriate, delivered to the client. If the key-pair is to be client-generated then details of the process used will need to be supplied.

Private Signature Key: An applicant must provide details of the mechanism it uses to ensure that the private signature key is only known to the client on issue. It will be a breach of the licence to disclose the key to anyone but the intended owner.

Client Authentication: The applicant will be required to provide details of the procedures it intends to follow in authenticating its clients; these must include prior physical identification by the CA or an agent (e.g. a Registration Authority) to which it is contractually bound.

Revocation: An applicant will need to demonstrate that it has systems in place to offer (through some form of public channel) a revocation service that is both prompt and comprehensive.

User signature generation products: Although not a condition of the licence, a client of a licensed Certification Authority will be required to use an "approved" signature generation product to take advantage of full legal recognition (see page 12). Licensed Certification Authorities will be required to supply information on products which have been "approved"[21].

(III) CONDITIONS ON A TTP FOR THE PROVISION OF A CONFIDENTIALITY SERVICE

Key storage: Where keys are stored, the applicant must be able to demonstrate they have the ability to securely hold the encryption keys (or other appropriate information) of their clients. Such "security" will include a computer that has been independently assessed (e.g. through the issue of an ITSEC or CC Certificate) in terms of security assurance

Legal Access: The applicant must make arrangements, both technical and procedural, to be able to produce any appropriate information which it has in its possession (e.g. user private encryption keys or other relevant information) in response to a validated written authorisation within a period specified in the licensing conditions.

Authentication of Access request: The TTP must have implemented procedures to determine the authenticity of a request for a key (or other relevant information) and to refuse unauthorised requests.

[21] See footnote 13 on page 12.

(IV) CONDITIONS ON KEY RECOVERY AGENTS

Relationship with law enforcement: Agents applying for a licence must demonstrate that they can provide, electronically, the appropriate key-recovery information to the law enforcement authorities when presented with the appropriate authority.

Authentication of Access request: The Key Recovery Agent must have implemented procedures to determine the authenticity of a request for information and to prohibit unauthorised requests.

We invite views on these criteria, and would also welcome views as to the level at which the standards should be set for each of them or how they should be assessed. The intention will be to build the trust that is essential for a market in these services to develop by ensuring a high degree of consumer protection, whilst not imposing unnecessary burdens and costs on the providers of licensed services.

ANNEX B - GLOSSARY OF TERMS

This annex, and some of the boxes and footnotes in the main document, are provided as a guide through the jargon. They should not be relied on as legal definitions.

Authentication

The verification of a claimed identity.

Certification Authority (CA)

A Certification Authority (CA) is a TSP which issues certificates to link electronic signatures to particular individuals or business functions (see also box on page 20).

Confidentiality

Keeping information secret.

Cryptography

The art or science of keeping messages secure.

Electronic signature

Something associated with an electronic document that is the electronic equivalent of a manual signature (see also boxes on pages 4 and 17).

Integrity

Ensuring integrity means preventing the unauthorised modification of the content of information.

Key escrow

The storing of a user's private confidentiality key (or part thereof) by a TTP with the implicit agreement to its release, e.g. for law enforcement purposes, under defined arrangements.

Key recovery

A capability that allows authorised persons, under certain prescribed conditions, to decrypt encrypted data with the help of information supplied by one or more parties (see footnote 17).

Key management

The process of managing (i.e. generating, storing, distributing, changing, and destroying) cryptographic keys.

Key revocation

Notification that a public key (whatever its purpose) in no longer valid.

Plaintext

The original data, i.e. without any encryption.

Private Key

The private (secret) part of a cryptographic key pair, which should be strictly controlled.

Public Key

The public (i.e. non secret) part of a cryptographic key pair. This key may be widely known and no secrecy need be attached to it.

Qualified certificate

A signature certificate which meets the requirements of Annex I of the EU Electronic Signatures Directive and where the Certification Authority (whether or not it is licensed) meets the requirements of Annex II of the Directive.

Trust Service Provider (TSP)

A generic term for providers (whether licensed or unlicensed) of cryptography services (see footnote 3 on page 5 and box on page 20).

Trusted Third Party (TTP)

A specific type of TSP that provides key management services for confidentiality and offers key escrow.