



**RESPONSE TO THE DTI CONSULTATION DOCUMENT  
'BUILDING CONFIDENCE IN ELECTRONIC COMMERCE'**

**Date: 30 March 1999**

**Version: 1.0**

**John R T Brazier  
Professional Projects Co Ltd  
19 Barttelot Rd  
Horsham  
West Sussex  
RH12 1DQ**



## Table of Contents

<b>SUMMARY .....</b>	<b>3</b>
<b>INTRODUCTION.....</b>	<b>4</b>
<b>ACKNOWLEDGEMENTS.....</b>	<b>4</b>
<b>1. LEGAL RECOGNITION OF ELECTRONIC SIGNATURES.....</b>	<b>5</b>
<b>2. ELECTRONIC COMMERCE PROMOTION .....</b>	<b>6</b>
<b>3. UNCITRAL MODEL LAW .....</b>	<b>7</b>
<b>4. SPAM .....</b>	<b>8</b>
<b>5. THE ROLE OF INTERMEDIARIES .....</b>	<b>9</b>
<b>6. SERVICE LICENSING.....</b>	<b>10</b>
<b>7. LIABILITY.....</b>	<b>11</b>
<b>8. PRIVATE SIGNATURE KEYS AND 'DUTY OF CARE' .....</b>	<b>13</b>
<b>9. LAWFUL ACCESS TO ENCRYPTION KEYS .....</b>	<b>14</b>
<b>10. LAW ENFORCEMENT.....</b>	<b>15</b>
10.1 LICENSING .....	15
10.2 LAW ENFORCEMENT NEEDS AND PUBLIC PERCEPTIONS .....	15
10.3 TECHNOLOGIES .....	16
<b>11. APPENDIX A: LICENSING CRITERIA.....</b>	<b>17</b>
11.1 GENERAL LICENSING CRITERIA .....	17
11.2 LICENSING CRITERIA FOR CERTIFICATION AUTHORITIES .....	18
11.3 LICENSING CRITERIA FOR CONFIDENTIALITY SERVICE PROVISION .....	19
11.4 LICENSING CRITERIA FOR KEY RECOVERY AGENTS .....	19
<b>REFERENCES.....</b>	<b>20</b>



## Summary

This document is a response to a number of requests for comment made in the DTI document '*Building Confidence in Electronic Commerce*' (URN 99/642). It aims to support the DTI and the Government in meeting their aims to make the UK the best place for electronic commerce in the world while meeting the needs of law enforcement.

It is structured around the series of questions in the DTI document, and follows their order. Some of the questions have been grouped together where it seemed appropriate to do so.

The following list summarises the main points in the response. Naturally, there are a large number of other comments and observations within the main body of the document.

- 1) Electronic signatures should be made as equal as possible to written ones in law (although there are significant differences between the two types). The presumption of electronic signature validity should be the same as that of written ones.
- 2) Regulation should be kept to a minimum where possible.
- 3) The use of electronic commerce can be accelerated by both technological developments and the manipulation of the tax regime.
- 4) The UNCITRAL model law provides a useful basis for much legislation, although there are areas that require further development. In general, electronic documents should be made equivalent to written ones as rapidly as possible.
- 5) Spam should be dealt with separately, and there are specific comments on spoofing and anonymity.
- 6) There will be a need of further legislation, and some of this legislation may be quite radical (such as a privacy bill).
- 7) It is proposed that service providers are licensed, not their services. In addition, there should be no difference in the services which licensed and unlicensed providers can offer.
- 8) There should be a basic, low level of liability accepted by all service providers (licensed or not). Providers can then provide higher levels if they so wish. Certificates should indicate higher levels of liability.
- 9) The usage of signature keys should be differentiated between those that represent some form of identity and those that represent an authorisation. In both cases the consumer will need limitation of liability and will need protection in their contracts with service providers.
- 10) Private 'identity-based' signature keys should not be generated by the service providers, but by the key owner.
- 11) Law enforcement agencies should have access to encrypted text when given appropriate authority. The 'tipping off' offence is anomalous unless there is a key escrow regime.
- 12) If key escrow is implemented the Government will fail in its electronic commerce target.
- 13) The Government needs to improve public perception of the use of electronic interception and monitoring, and the Freedom of Information Bill would provide an opportunity to do so. Law enforcement should undertake a more holistic approach to cryptographic issues and abandon the search for a 'magic bullet' such as key escrow.
- 14) Specific comments are made about the licensing criteria, and KRAs are questioned.



## Introduction

This document is a response to the proposals outlined by the DTI in March 1999 entitled '*Building Confidence in Electronic Commerce*'. It aims to do the following:

- 1) Provide effective responses to the specific questions asked in the document by the DTI.
- 2) Discuss some issues that appear to require further elaboration.
- 3) Assist the Government in its aims of making the UK the world's best place to trade electronically.
- 4) Help in providing a balance between the needs of business, the citizen and law enforcement agencies.

This document will follow the order of questions raised in the DTI paper in its responses. Some of the responses may be applicable to more than one question, but if possible any given issue is discussed just once.

Many of the topics cannot be discussed in enough detail due to the extremely short timescale that has been given for consultation, and thus some of the ideas will be undeveloped. However, it is hoped that these can still be useful as the proposed legislation progresses.

## Acknowledgements

This document would not have been possible without the help from a large number of people, and I have attempted to ensure that references are given where possible. Where this has not been possible, I would like to take the opportunity of thanking them now. All errors and sins of omission remain my own responsibility.



# 1. Legal Recognition of Electronic Signatures

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

This section of the DTI paper (paragraphs 16 to 22) raises a number of fundamental issues. A choice is presented on how statutory requirements can be updated for the acceptance of electronic signatures: either individually by primary legislation, or via a mechanism where primary legislation confers powers on the Government to amend legislation by statutory instrument on a case by case basis. In general, and subject to the following comments, the second alternative is clearly the only workable one: it seems unlikely that there would ever be enough Governmental time for individual pieces of primary legislation.

However, the powers granted should be extremely specific and limited. In effect, they would only exist to give legal recognition to electronic signatures and writing for specific statutory requirements. They should not cover any of the technologies or mechanisms on how the systems function, nor deal with access and signature confirmation issues: these should be dealt with separately.

In addition, giving electronic signatures the equivalent force of written signatures raises further points:

- 1) It must be recognised that they are not directly equivalent; typically written signatures are tightly associated with people and weakly associated with documents, whilst digital ones are tightly bound to documents and weakly to individuals (or identities). This means that digital signatures are often shared by individuals (as in an organisation) and also often act more as permissions than as true signatures (akin to the usage of a credit card over the phone: it is an authority to carry out a purchase, and the knowledge of identity is extremely limited). Thus legislation will have to reflect that digital signatures will operate differently from written signatures, and will be used in many different ways. The legislation should allow this freedom.
- 2) Accepting point (1), where the two systems of written and digital signature can be used more or less interchangeably (such as when one signs an electronic rather than written document) then the legislation should not give priority of one over the other in terms of legal validity or general usage.
- 3) This means that the concept of 'rebuttable presumption' for digital signatures should not be implemented. This is because 'identity' may not be clear, but more importantly because written signatures do not carry any such rebuttable presumption. Many people will be less confident in using digital signatures due to lack of familiarity, and will be unsure how to protect them. If they perceive the risks and obligations of electronic signature usage to be greater than that of written signatures, then this will act as a significant barrier to the adoption of electronic versions. The presumption of the validity of an electronic signature should be the same as that of a written one.



- 4) Users of personal electronic signatures should be responsible for their generation and storage (as stated in paragraph 19 of the DTI document). This means that third parties cannot generate electronic signatures for individuals as a service (contrary to paragraph 20, which contradicts paragraph 19). The case is different when the signature is embedded as part of an overall service provided by a business supplier (such as a system using the SET protocols). Here the signature is acting as a mandate given by the service provider to the customer (equivalent to a VISA card). This is covered in more detail in Section 8, and legislation needs to cater for these different usages of electronic signatures.
- 5) The use of certificates should be optional, and the spirit of paragraph 21 encapsulates this well: people may wish to have certified signatures, and there may be benefits of so doing, but it should not be mandatory.
- 6) As indicated in paragraph 22, current usage of electronic trading systems should still continue, and be allowed to develop. The number of stand-alone CAs as apparently envisioned in the document may be relatively low: bilateral agreements between businesses, and permission-based services driven by smart cards may well form the bulk of electronic commerce.

## 2. Electronic Commerce Promotion

*'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.'*

The Government wishes to make the UK the best place for electronic commerce and, presumably, the country with the most electronically based transactions, per capita or as a percentage GDP, so that it is a major electronic trading player. Competition resides in countries such as the USA, which has two key long term advantages: (1) a cheaper cost base for its businesses (by keeping taxes and materials costs such as fuels low) and (2) a huge internal market<sup>\*</sup>. These factors interact as the large market provides economies of scale to American companies.

These benefits work in that companies in the USA can invest more in electronic commerce and take higher risks with new initiatives. Thus the UK Government needs to take positive actions to counteract this inherent advantage that lies with the USA. In addition, the Government can take actions to increase the likelihood of the usage of electronic commerce, and provide incentives to do so. Thus a number of recommendations can be made:

- 1) Where possible, regulation should be kept to a minimum with regard to electronic commerce (commensurate with the requirements of good policing and public safety). The barriers to entry should be kept low, and businesses should be free to experiment with new products, services and methods of dealing.

---

<sup>\*</sup> It might be thought that USA businesses are more deregulated, but it is no longer clear that this is true overall due to the great changes in both countries over the last twenty years. For the purposes of this paper it is assumed that the general openness and opportunities in both the UK and the USA markets are similar except for scale.



- 2) The slowness of the Internet - a real problem slowing the development of commerce - should be alleviated by developing a proper basis for the future:
  - Investing in a core of very high-speed links to provide a fast communications infrastructure within the UK. This could be done in concert with academia and industry, and would provide spin-offs in enhancing the country's technological capability in the field of advanced communications systems.
  - Encourage the telecomms companies to accelerate the provision of high-speed local links to businesses and homes. At present this provision is being carried out extremely slowly, and any links faster than the ordinary telephone line are expensive. Swift communications should be available at a low cost: the aim should be to have equal or lower costs to the USA for communications.
- 3) Businesses and the public need to be actively encouraged to use electronic commerce for transactions. There is a way to ensure that this happens by giving them an incentive. Thus if VAT were reduced to, say, 7.5% for all transactions where ordering and payment were carried out entirely electronically, there would be an enormous shift towards electronic commerce. The provision could well become self-funding as foreign businesses based themselves in the UK for the purposes of electronic commerce. It is recognised that this would be a specific market distortion put in to achieve the required goals.

### 3. UNCITRAL Model Law

*'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.'*

Currently, there are a large number of factors that reduce the benefit of electronic commerce because of the need for paper documents and their retention (sometimes for very long periods of time). In general, the UNCITRAL Model Law [UNC] is a good model, and parts of it should be put into effect as soon as possible if we are to move rapidly to large-scale use of electronic commerce. The following comments assume that there would still be an adequate period for discussion before any legislation were actually implemented.

The Model Law can be viewed as falling into several types of provision:

- 1) Those that in essence provide for the equivalence of data messages with paper documents (Articles 5, 5bis, 9, 11, 12, 16 and 17). These are crucial for the long-term development of electronic commerce, as businesses can then develop completely electronic transaction and documentation chains, without the need of paper versions. Such provisions would remove the constant concern about the validity of electronic documents.
- 2) Those that allow for a definition of 'original' electronic documents, and then describe their retention (Articles 8 and 10). These will require exacting drafting (such as the definition of an original, with its time stamps and so forth), but would open up many new areas to electronic transmission and storage (e.g. many legal documents could now be electronic from inception), and would enhance electronic commerce by this widening of scope. In addition,



other areas of commerce would benefit: for example, pharmaceutical companies could carry out Research and Development solely using electronic originals (as compared to the towers of paper that currently exist), and be confident that those originals would be accepted. This would be tremendous benefits to both the industry and its customers in terms of shorter lead times and reduced costs.

- 3) Those that define the technicalities of how data messages are originated, handled and confirmed (Articles 13, 14 and 15). Article 13 has problems in that it makes no reference to digital signatures: presumably the person who digitally signed the document should be the originator, even if the message is ostensibly from another address? Thus Article 13 requires more clarification as to how 'the originator' is defined with reference to signatures and other information in the message (such as mail headers and document content). However, the aims of Article 13 are perfectly valid, as long as it is ensured that the responsibilities between originator and receiver are effectively the same as they would be under a paper system.

There will need to be some form of definition of the validity of receipt acknowledgements. Article 14 covers this, but given the time limit it has not been possible to analyse this Article in sufficient depth. Again, responsibilities should operate in a similar manner to those of a paper system.

Article 15 should define time stamping more precisely, and more analysis and discussion should take place before adoption. Firstly, time stamping should be done on a cryptographically strong basis on document hashes, so that the time stamp is (1) accurate; (2) 'stamps' the whole document (in the way a digital signature 'signs' all the characters in a document); (3) is cryptographically strong; and (4) the stamping protocol removes the possibility of cheating. Otherwise, computer-generated times can be quite unreliable, which would be an issue in a court action. Secondly, whilst the Article attempts to define certain points at which the message has been 'sent' and 'received', these should probably be analysed further. For example, one might have two 'sent' times: one representing the last point at which the message is still under the originator's control, and one when it enters the systems outside the originator's control.

In conclusion, the UN Model Law is an excellent basis for further legislation, and some parts should be developed relatively quickly.

## 4. Spam

*The Government would welcome views on whether the industry solutions being developed to combat spam are likely to be effective. Or should the Government take further steps to regulate the use of spam?*

All the evidence is that the amount of spam reaching the intended recipients is actually decreasing at present, as the filtering systems become more effective. For now, simple monitoring of the situation would seem to be adequate (in general, the less legislation, the better). In addition, this document is probably inappropriate for a discussion about spam, as any intended legislation would



have an effect on freedom of speech. Because of the importance and likely complexity of any such proposals they would be better discussed separately.

Given the comments in the previous paragraph, it is worth making a comment on 'spoofing'. For the purposes of this document, 'spoofing' is defined as the modification of a mail header for the intention of deceiving the receiver (as compared to the frequent use of 'alias' mail headers to assist mail routing and management).

Spoofing undermines the credibility of all mail addresses, and thus undermines identification on the net (even if it is not entirely clear what identity is). If legislation became essential, the author would sooner see the proper development of anonymous remailers and the removal of spoofing. This would allow people to bulk-mail via the anonymous remailers (which would also help the filtering systems), and would open the way to get rid of spoofing if this was determined to be an important issue.

It is recognised that anonymous remailers are contentious, but they can provide valuable services to society (it is known, for example, that both the Samaritans and the Police have made use of them, and one is currently running to provide email anonymity for Kosovo Yugoslavs [KAH]).

## **5. The Role of Intermediaries**

*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.*

It is difficult to predict how the new services listed in paragraph 32 of the DTI document will develop. It seems likely that initially most legislation in addition to the recognition of electronic signatures will be that identified in Section 3 above: the need to make electronic documents legally equivalent to paper ones in all aspects, and the recognition of electronic 'originals'. These initiatives will allow business to move completely into digital space, where they will develop entirely novel services.

Other changes likely to be required will be further development of the Data Protection Act, as databases become tightly interconnected and a detailed profile on each citizen is developed.

Of course the largest intermediary will become the Government itself, as all its 'services' and methods of communication with its citizenry move into the electronic domain. Given that modern Governments typically expend over 40% of the GDP (42.8% in the UK in 1996 [GSS]), the UK Government will become by far the largest transactional force on the net in this country.

These last two factors are likely to drive more revolutionary aspects of legislation, as the amount of information on each private individual increases:

- 1) A Freedom of Information Act, which is apparently promised.



- 2) Some form of Bill of Rights, as Common Law and precedence mechanisms fail in the new electronic environment. Much of this may be encompassed in the Human Rights Act, which incorporates the European Convention on Human Rights.
- 3) Some form of privacy legislation. The pressure for this is likely to rise.

However, discussions of such topics are outside the remit of this document.

## 6. Service Licensing

*' ... services which will be eligible to apply for licenses under the proposed regime. They are intended to be illustrative, rather than prescriptive and we would welcome comments on them. We recognise that various organisations are considering different business models for providing cryptographic services to the public and would welcome views on how they should fit into the licensing regime.'*

*'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 separation of services may not occur as much as is envisaged in the DTI document, especially for certificate providers because of the requirements needed for effective certificates. For example, it is critical that a key certificate is time-stamped at generation and revocation, as it is vital to know for what period the key is valid. Presumably certificate providers will have to actually carry out the registration process, and will have to provide methods for access to the certificates (and thus a directory service). Lastly, under most protocols one might expect the issuer of the certificate to have to sign the revocation certificate\*. This immediately means that certificate providers will in most cases provide the services of registration, certification, revocation, time-stamping and directory maintenance.

The main exception to all-inclusive service providers might be in the provision of directory services, where one can envisage organisations becoming specialists in the maintenance of massive databases of directories, of which certificates and their revocations would comprise a part. It is possible that key generation might become a separate service, but it seems less likely as many keys might well require certificates. Given the relatively exacting conditions given for licensing in the Appendix A, it seems most likely that service providers that can meet them will provide as many services as they can.

The signature key generation service is discussed in more detail in Section 8.

It is proposed here that it should not be the service that is licensed, but the service provider. This would be analogous to a doctor or lawyer: these professions are licensed (but not, it should be

---

\* This might not be true where there is a pyramidal organisation of certification authorities; however, whilst OFTEL is named as an initial licensing authority the DTI document does not propose any kind of public key certification hierarchy.



noticed, by the Government), but the services they provide are not. Even the demarcation between solicitors and barristers does not affect the services each can offer in their own area.

As an example, it can be seen that a barrister can act in any court case: they are not licensed according to if they can prosecute or defend, and the type of cases they can take (libel, murder, etc). A barrister is free to specialise if he or she so wishes: but that is not the condition of the license. The same applies to the medical profession.

With this model, the provider is licensed, not the service. This avoids the difficulty of new services having to be 'licensed' or 'unlicensed', and allows the provider to freely develop new services.

## 7. Liability

*'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.'*

*'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?'*

*'The Government would welcome views on this approach, how this limit should be set, or suggestions for alternative approaches.'*

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

Several factors make liability a difficult issue:

- The differences in the services offered.
- The fact that this is a new field, where it is not clear how the services themselves will evolve.
- There are obligations to third parties (such as people who depend on certificates).

Most of the comments in this section are general. However, a brief discussion should be made about digital signature certificates, whose production, management and validity encompass a number of points, many of which can be extended to the other services.

The first is that liability of a certificate must be limited, in part at least, by its value to its owner. Thus the value of a digital signature certificate to an individual is much lower than that of one belonging to a large multinational corporation. In addition, individuals currently pay exactly nothing to have



their hand-written signatures 'certified': which implies that the current going rate for a private digital signature certificate also tends to nothing.

This is supported by the fact that whilst companies such as Thawte and VeriSign do provide individual certificates, and that they are in the low price range (typically \$10 to \$20 per year, excluding free ones that are virtually not certificates at all: see [THA] and [VER]), very few people actually take them out. There is, of course, little incentive currently to use such certificates, but cost is still an important factor: people do not wish to pay for them.

The liability models of these two companies are interesting. VeriSign's disclaimer shows a simple model: they have three 'classes' of certificate, and their liability caps go up according to the class (from \$100 for Class 1 to \$100,000 for Class 3). Thawte accept liability (excluding punitive damages) for negligence, but put no value on it. Both companies do extend their liability to third parties, although careful reading of both documents seems to show that both liability statements are undermined by other sections.

From these observations a general model can be advanced: most cryptographic services, being generally 'invisible' to the great majority of the public, will have a very low perceived value to their users (and thus liability has to be low). Yet to large corporations they are likely to have very high values (and there must be consequent high liabilities). Coupled with the fact that the services are still experimental and will change, the following approach is recommended:

- 1) In general, as little legislation as possible should cover liability. As much current consumer protection legislation should be applied to this area as possible (to ensure that goods and services are 'fit for purpose' and consumers are protected).
- 2) Basic liability ought to be held to a very low level: perhaps £50 for any single certificate (equivalent to the typical consumer liability on a single credit card). This level would be appropriate for both licensed and unlicensed service providers.
- 3) Service providers should be free to develop products where they accept higher levels of liability. It is probable that the industry will rapidly develop 'liability bands', much in the way VeriSign has, for different levels of service. Again, both licensed and unlicensed providers should be able to offer these higher levels.
- 4) It is clear that the liability associated with a certificate has to be known, especially as a third party may be dependent on the information in the certificate. An approach could be that if the certificate, contract or document makes no mention of liability then only the basic level applies, and it does so automatically (this fact should be well publicised). If a higher level of liability is being accepted then the certificate or document must state it. This may be difficult to carry out in practice because the Government will find itself having to define such information fields in certificates (no liability field exists in an X509 certificate, although it can be produced in Version 3 via the extensions). This would delay practical implementation, although a 'grace' period could be allowed where the information was incorporated however possible whilst a standard was developed.



The model proposed is simple: there is a basic liability, and both licensed and non-licensed service providers may improve on this if they so wish. Licensed and unlicensed service providers are not differentiated by their possible services or liabilities.

## 8. Private Signature Keys and 'Duty of Care'

*'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)?'*

This issue has been separated out from the rest of the liability requests because it has implications that are not directly related to liability, and relate to other parts of this document.

There are likely to be two basic systems of use for digital signatures:

- 1) Where the digital signature is 'packaged' in a complete set of electronic commerce services. We can envisage a SET-like system, with a person using a smart card or 'electronic wallet' to purchase goods and services. Whilst the system as a whole is using electronic signatures and certificates, these will in practical use be invisible to the user. In these cases it will be the card or wallet provider that will do the entire key and certificate generation and management, and the customer will have effectively no control over the signature application within the card (except via entry of some code or pin number to activate a transaction). All the customer will do is report the loss or theft of a card or wallet in such an eventuality, and the duties and liabilities of the customer should be as they are now for a credit or debit card. These are agreed when the customer acquires the card, and are between him and the provider. This type of usage of digital signatures is very much an 'authorisation to spend', and has relatively little to do with identity.
- 2) Where a person specifically generates a private/public signature key pair for their own special purposes, such as signing mail messages, documents and contracts. Firstly, the person should generate their key with their own systems (in agreement with paragraph 19 of the DTI document, despite the contradiction in paragraph 20), to ensure security. They should then get a certificate, at which point their duties and obligations would be agreed with their certificate provider. These will almost certainly be higher than the very limited liability indicated for the consumer above using a provider-generated smart card, but are still subject to agreement between the key owner and the CA. In this type of usage the electronic signature has a much stronger relationship to the identity of the individual than the first type.

In both cases it is not seen that specific legislation is necessary for obligations to be placed on key holders: Certification Authorities will do this within the free market. In fact, the opposite is true: it is much more likely that legislation will be needed to protect consumers and ensure fair contracts with the CAs. In the cases above consumers will need to have their liabilities limited, or they will not use electronic commerce.



## 9. Lawful Access to Encryption Keys

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

The author will state that he is against key escrow, on the basis that it will not work. However, the arguments will not be repeated here, mostly because the author knows that the Government is aware of many people's opposition [HEN]. If there is interest in this point then there is an excellent technical article at [ABE]. The one comment that will be made is that if key escrow does end up being incorporated into the legislation then the Government will not meet its goal in making the UK the best place in the world for electronic commerce.

The DTI paper requests views on two proposals: making an offence of the failure to comply with what might be called a 'decryption warrant', and the 'tipping off' offence.

The first appears to be a logical proposal, especially in a non-escrow regime, and would be equivalent to the obligation to provide records in the case of fraud, and even a blood sample in the case of drunk driving. The principle, as indicated in the paper, is fair. However, it should be the principle that the person must produce the plaintext versions of the documents, not the keys. This is because in a public key environment, messages can only be decrypted by the recipient, not the sender. Thus if corporations were receiving messages from criminals and had to yield their confidentiality keys, then this would require generation of entirely new replacement keys. This could become a major cost burden to large companies with complex internal public key infrastructures (especially as a large corporation might, through no fault of their own, get involved in numerous cases). Individuals could also find it a significant effort and personal cost to have to replace their keys. Most of the individuals and corporations will be entirely innocent parties.

The Government may find plaintext (or even key) recovery less workable in practice: it is easy to envisage situations where a person has encrypted material that cannot be decrypted (for example, it was encrypted with a temporary - and now deleted - key). If the suspect can demonstrate that they use a system that leads to such a result, will this be a 'reasonable excuse'?

The second proposal, creating an offence of 'tipping off', is difficult to understand outside of the context of key escrow. If there is no key escrow, then how can a key be acquired without the subject knowing about it? If this is a reference to the fact that people may place their keys voluntarily in escrow, and thus they would be available, then the legislation would appear to have some sense. However, it is difficult to envisage any person who believes that they might be targets of the security agencies placing their key in escrow (voluntarily or otherwise). As Parliament should not be in the business of generating worthless legislation, it is impossible to support this proposal unless the Government can clarify the point.



## 10. Law Enforcement

*'The Government would welcome ideas on how its law enforcement and electronic commerce objectives might be promoted via the licensing scheme or otherwise.'*

*'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.'*

### 10.1 Licensing

It is not recommended that licensing have any special relationship with law enforcement, aside from the normal co-operation required from any business in the modern age. If an attempt is made to convert service providers into quasi-law enforcement agencies then this will provide a major barrier to licensing: most providers simply will not license as they are unlikely to be trusted by their customers.

The benefits of licensing operate best in an open market with the minimum of regulation possible (along with the free use of all aspects of cryptographic technology). This will benefit electronic commerce as it will increase confidence and allow experimentation and development, giving all the services free reign. One possible outcome will be a situation where unlicensed service providers will be used for low-value transactions and licensed ones for high-value transactions. Of course, future services may well also have an impact on the development of licensed services.

### 10.2 Law Enforcement Needs and Public Perceptions

It is frequently stated that the Law Enforcement Agencies require covert access to communications channels, and the capability of being able to carry out real time decryption of such channels when required (as implied in paragraph 86 of the DTI document). Yet the evidence of this is minimal: even within the DTI document, every case referred to as evidence for law enforcement interests (paragraph 50) actually refers to stored information on computers, not in transit. It has already been agreed in Section 9 above that agencies should be able to enforce decryption of impounded documents (where possible).

This implies that the evidence for such a need is minimal, or that the law enforcement agencies have reasons for not divulging it. This very statement points to a key issue throughout the entire cryptology debate: the growing public mistrust in law enforcement and security agencies. This distrust makes proposals such as key escrow likely to fail as much for reasons of public resistance as for the many technical reasons.

This mistrust has probably grown because:

- 1) Despite the provisions in legislation such as IOCA, there is the perception that electronic interception is carried out on a far greater scale than the numbers indicated by Home Secretary warrants. In this area perception is probably more important than reality.



- 2) There is considerable evidence that many western Governments are routinely placing their entire populaces under generalised communications surveillance via systems such as Echelon [ECH].
- 3) There is further evidence that Governments are also using surveillance techniques to undertake commercial espionage operations. Many countries have been implicated, certainly countries such as France and the USA (the latter with UK help) [WOL, ECH].

The general concern is that individual privacy is vanishing in a regime where the assumption is that the state has the right to covertly monitor its subjects for any reason it sees fit. Under such conditions, the Government is most likely to see increasing resistance to any proposals that further empower the law enforcement and security agencies, however valid the proposals may be.

Clearly the Government needs to handle these perceptions more effectively. One good way to start would be firstly to find evidence for the quoted 'needs' of law enforcement agencies: otherwise they are likely to be regarded as open-ended wishes. Perhaps a better approach would be for the Government to divulge all the electronic intelligence gathering activities that are in progress, at least in overview terms, and place them under an appropriate and open Parliamentary review process. This seems to be unlikely, yet on the other hand the Freedom of Information act would be an excellent opportunity for such a step.

The point of this section is that both individuals and corporations have a rising level of mistrust with regard to Governments. They will tend to take greater care to ensure privacy in communications in what is beginning to be perceived as a hostile environment. Every action that the Government can take to reduce such mistrust will tend to enhance confidence and thus will tend to improve electronic commerce. It is also more likely to get public agreement for appropriate law enforcement support.

### **10.3 Technologies**

The law enforcement agencies should recognise that not only are there current technologies that undermine systems like key escrow (such as subliminal channels, steganography and Diffie-Hellman type protocols), there are future technologies coming that will, under certain conditions, undermine the concept of covert interception (quantum cryptography, see [SCH] for an introduction).

Thus the agencies may well at a future point find themselves without the capability of effective covert communications monitoring, notwithstanding paragraph 80. This shows that the second request above, with regard to technology, is almost certainly addressing the issue in the wrong way: it is the wrong question.

The debate throughout this decade on the whole issue of 'access to keys' and 'key escrow', and even the attempts to limit the cryptographic technology itself, have been an attempt to provide a 'magic bullet', a solve-all panacea for the law enforcement agencies. Like most panaceas, it is also a chimaera. The speed of technological development is such that any technology-based solution



will inevitably be made redundant by a newer development, especially when there is an incentive to do so.

In general, law enforcement agencies will have to become more sophisticated, with a greater general knowledge of the technologies that we have been discussing. They will have to make greater usage of methodologies such as traffic analysis rather than trying to depend on the internal message content. They will also no doubt make use of Tempest-style technologies (when authorised) to view information at the point of creation or use, rather than at the point of transfer. However, this comment should not be taken as a declaration of open season on civil rights, with massive covert monitoring on a grand scale.

This more holistic approach, grounded in an improved technological knowledge with more even use of multiple police techniques, is actually a more effective path for the law enforcement agencies in the long term. It provides policing in depth, using diverse methods. Magic bullets fail when the disease becomes resistant.

## **11. Appendix A: Licensing Criteria**

*'We would welcome 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 criteria should be set such that as many organisations as possible can become licensed if they so wish. It would be inappropriate to develop criteria that only allowed the very largest corporations to become licensed service providers: in this field it is notable that it is usually the small, new companies that have driven development and change.

Most of the criteria are sensible and valid; however, there are some comments that should be made, and these are covered below.

### **11.1 General Licensing Criteria**

- 1) The need for the registered office in the UK is questionable: many companies operate within Europe without following national boundaries (for example, most computing companies have their call centres at only one European location). The DTI states that foreign businesses will be allowed to offer services within the UK (paragraph 10), and it seems odd that they would have to set up an office in the UK for the sole purpose of obtaining a license. What this would imply is that foreign enterprises would operate in the UK in an unlicensed fashion, which presumably is not the intention of this provision.
- 2) Can it be assumed that 'vetting employees' will be a limited exercise if the companies are to stay within the law, or does the Government propose 'lending out' the security services to provide vetting capability?
- 3) It is recommended that the financial viability requirement is not too onerous, otherwise it will disbar smaller organisations from applying.



- 4) With regard to quality management, ISO 9000 makes no guarantee about the quality of service actually provided to the customer. Whilst it may indicate that there is effective quality control in place, the author's personal experience is that this is by no means certain.
- 5) Section 8 discusses the issues around the generation of signature keys.

## 11.2 Licensing Criteria for Certification Authorities

- 1) This is outside the author's own experience, but personal communications have indicated that many would not regard ITSEC as an especially good criterion on which to evaluate the true security of an enterprise.
- 2) The certificate content raises several issues:
  - The fact that the certificate is not to be used to validate confidentiality keys seems extraordinary. This would mean that there is no mechanism by which an encryption/decryption key pair can be validated by a licensed authority. It is hoped that this is a mistake, otherwise it would imply that the DTI does not wish to allow confidence in public key encryption technology. This may be an attempt to slow down the uptake of encryption; it is more likely that it will simply give more business to unlicensed CAs, that will then have no incentive to become licensed. The other alternative is that the intention is to make such certificates illegal, but it is difficult to see how this can work in the global arena.
  - As mentioned elsewhere, such fields require a development of the X509 standard, or the development of a new one. This is likely to take time.
  - If standards are to be developed or extended, then they should allow for the future addition of fields or information easily (this is catered for under X509 V3).
- 3) The comment has already been made about signature keys. If the CA generates a signature key pair, there is no way it can logically prove that its methods are 100% secure so that the key is delivered only to the client, with no possibility disclosure or leakage.
- 4) The client authentication, as described, will not work. Many clients will not be physical entities at all: they will be organisations, computers, systems and even chips in smart cards. 'Physical identification' becomes meaningless; more work on the elucidation of identity, and the concept of 'identity' versus 'authorisation to use', is needed before legislation is enacted.
- 5) Revocation may well turn into a major issue. It may be the issue that delays the spread of electronic commerce, as it is not clear how it will be handled on a global scale.
- 6) The requirement for a client to use an 'approved' signature generation product is not clear. The apparent intention is to ensure that appropriately secure products are used; however, the EU Electronic Signatures Directive has little to say on such products or the approval process [ESD]. All that can be said is that the 'approved' products are not the right ones, this will represent another barrier to licensing as CAs will support clients who use popular, if unapproved, products. For example, PGP is the most commonly used personal system in the world, but is unlikely to be approved as the same key is used for encryption and confidentiality. This comment about approval can be generalised to all the other services.



### **11.3 Licensing Criteria for Confidentiality Service Provision**

There are no special comments on confidentiality service providers, although the author suspects that in real life there will be little need for them.

### **11.4 Licensing Criteria for Key Recovery Agents**

The discussion of KRAs is not clear in the document. Footnote 17 of paragraph 38 attempts to redefine KRAs as a type of third party service provider, acting as a logical recipient of a copy of every message generated (in PGP terms it is a Corporate Message Recovery centre, with the message having an Additional Recipient Packet keyed for the recovery centre). However, this redefinition goes completely against the meaning of the term 'Key Recovery Agent': which is an agency that recovers keys.

This observation is reinforced in the Appendix, where the KRA must provide '... the appropriate key-recovery information to the law enforcement authorities ...'. Thus the KRA is, in fact, a key escrow agency and there seems to be no reason for the existence of such agencies outside of a key escrow environment.

Despite the suggestions in the text about 'key encapsulation', in the end people will not lodge their keys with such services, or create a message readable by such agencies, if they believe that they will be monitoring targets. As it is unclear that such agents will exist, no further comment is made on the licensing criteria.



## References

- [ABE] H Abelson et al, *The Risks of Key Recovery, Key Escrow, & Trusted Third Party Encryption*, [www.cdt.org/crypto/risks98](http://www.cdt.org/crypto/risks98)
- [ECH] Sunday Times Focus article on Menwith Hill and Echelon, 31 May 1998. Copy may be found at: [www.infowar.com/civil\\_de/civil\\_060298a\\_j.html-ssi](http://www.infowar.com/civil_de/civil_060298a_j.html-ssi)
- [ESD] *Proposal for a European Parliament and Council Directive on a Common Framework for Electronic Signatures*, 13 May 1998, COM(1998) 297 final.
- [GSS] Government Statistical Service, *The Nation's Accounts 1996*, [www.statsbase.gov.uk/stats/ukinfigs/natac.htm](http://www.statsbase.gov.uk/stats/ukinfigs/natac.htm)
- [HEN] D Hendon, *RE: Crypto Task Force chairman is pro-escrow?* UK Crypto Mail List, [ukcrypto@maillist.ox.ac.uk](mailto:ukcrypto@maillist.ox.ac.uk)
- [KAH] L Kahney, *Email Assist for Yugoslavs*, Wired News, 29 March 1999, [www.wired.com/news/news/politics/story/18765.html](http://www.wired.com/news/news/politics/story/18765.html)
- [SCH] B Schneier, *Applied Cryptography, Second Edition*, John Wiley & Sons, 1996.
- [THA] Thawte Digital Certificate Services, [www.thawte.com](http://www.thawte.com)
- [UNC] *UNCITRAL Model Law on Electronic Commerce*, [www.un.or.at/uncitral/english/texts/electcom/ml-ec.htm](http://www.un.or.at/uncitral/english/texts/electcom/ml-ec.htm)
- [VER] VeriSign, [www.verisign.com](http://www.verisign.com)
- [WOL] F Wolf, Representative of Virginia, accusations against France in the US House of Representatives, 28 April 1993. Text available at: [www.tactics.com/peer\\_research/frank\\_wolf.html](http://www.tactics.com/peer_research/frank_wolf.html)