EURIM POSITION PAPER
May 1997

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

EUROPEAN
INFORMATICS
MARKET
EURIM

Response to DTI Consultation Paper on Licensing of TTPs

Introduction

EURIM welcomes the publication by the DTI of its *Public Consultation Paper on the Licensing of Trusted Third Parties for the Provision of Encryption Services*. However, this first attempt at producing a framework for the control of services associated with security in the emerging electronic world has major flaws. Considerable work is needed before even an acceptable framework can be agreed. EURIM recommends that a further round of consultations be undertaken before any attempt is made to draft legislation.

Comments

The recently published OECD Guideline on *Cryptography Policy* set down a number of principles within which national cryptography policies should be framed. The DTI is to be congratulated on putting out for public consultation so quickly after publication of that Guideline a Paper that attempts to define the legislative framework within which cryptography services could be provided in the UK.

EURIM has considered these proposals carefully from both a national and an international perspective. Our conclusion is that these proposals contain fundamental flaws that need addressing before an acceptable framework for legislation can be defined. We comment on just a few of them in this response:-

1. The proposed legislation would preclude the UK from exploiting its unique advantages as the base for global trusted third party service providers - a major new service industry.
2. The paper does not take sufficient account of the development of TTP services and regimes in other countries.
3. The paper has a heavy bias towards message confidentiality and support of the Interception of Communications Act, not addressing adequately other uses of cryptography and the role of TTPs in providing public trust services.
4. The paper does not assess the balance of civil rights, commercial benefits and national security nor show that the cost - in money and freedom - of the proposed regime is justified when even unsophisticated villains could use unlicensed services.

Recommendations

A further round of public consultation is recommended before legislation is drawn up. The primary focus for this work should be to establish a framework for public trust services and to encourage a consistent pan-European environment for electronic commerce.

----

1. EURIM has always recognised that the UK is uniquely well placed to take advantage of the emerging world of electronic commerce. However, these licensing proposals, which do not recognise the way trust is established in the commercial world, would cause major problems to UK industry, particularly those involved in international business.

The current commercial legal and regulatory environment encourages new businesses to base their operations in the UK. The emergence of English as the language of the electronic world, and the traditional trust in, and perceived independence of, UK commerce also make the UK a natural place to establish such businesses. For UK industry to be able to exploit this new opportunity there must be the minimum of regulatory barriers. The proposed regime would place significant constraints on the ability of UK companies to operate internationally, a disadvantage aggravated by the lack of equivalent constraints on most of our major competitors in the same timeframe. It would also discourage non-UK companies from basing their operations in the UK, a significant lost opportunity for invisible exports.

The proposals do not acknowledge the complex ways in which international business operates:

companies form joint ventures, consortiums and subsidiaries as necessary to meet specific market opportunities. These proposals would appear to force non-UK corporations to become licensed where common trust services were involved. Such mandatory requirements would place UK industry at a significant disadvantage. Similarly, the need for an organisation to become licensed if it is involved in any service provided by a licensed TTP would impose major constraints. These proposals raise many issues that are not addressed in the practical business world and that would need to be resolved before any effective legislation could be drafted.

2. The Paper takes no account of work being undertaken elsewhere to define the way trust relationships are managed. If these proposals were followed, UK industry could find itself saddled with a restrictive licensing regime that requires its overseas partners to conform to UK licensing regulations simply to do business with UK companies. EURIM believes that the UK government is uniquely placed to establish an acceptable global framework - but this should be done on a collaborative basis and not by introducing local UK regulations. This could be a key task for the UK Presidency of the EU in 1998 - with the goal of establishing a consistent regulatory framework across Europe that recognises commercial realities. In parallel a dialogue could be held with other major trading blocks - such as North America and the Far East - to establish a common framework, possibly over a longer timescale.

3. The proposals confuse the different types of cryptography service that are needed to underpin electronic commerce, and how they are handled in a business context. They are overly focused on encryption services (that is, confidentiality) and on the need to be able to access information being communicated. Industry is more concerned to establish an infrastructure that supports functions such as authentication, non-repudiation and proof of origin - for which public key certifying authority networks are needed. Meanwhile, other cryptographic technologies for confidentiality are available for those who wish to evade surveillance.

4. EURIM recognises the legitimate needs of government for lawful access but considers that the current proposals do not strike the right balance between the needs of law enforcement and of industry - erring towards the former. Our focus is on the needs of industry and we leave others to argue the balance between security and other civil rights. We merely note that the paper does not say why the government thinks that it has struck a fair balance between the interests of the various parties. We add that our experience of informatics leads us to believe that any villains posing a serious threat to national security would find ways of evading the proposed controls.

These proposals, by focusing on the needs of law enforcement, call for a significant bureaucratic overhead with no countervailing benefit. EURIM recognises the need to protect the consumer, small businesses and others who might need to use TTP services. Whilst mandatory licensing of such trust services could help to create an appropriate degree of trust, it is inappropriate where other means already exist. The proposals appear to be based on a simplistic trust model that takes no account of the complex trust relationships which industry already operates as part of normal commercial activities. Industry is already extending current trust relationships to cope with mutual trust of public keys, and to allow the confidential exchange of information without any change to existing regulations.

Where encryption is relevant, a clear distinction should be made (which the proposals fail to do) between the encryption of stored data and of data being communicated. The legal requirements for each are different, as is the way keys are handled. The slow process of key recovery is appropriate for revealing the content of stored data but usually unsuitable for real-time interception of communications.

5. There are many other detail issues that need to be resolved before even a framework for legislation can be agreed. These include a far more precise definition of what is meant by encryption services (which should be called cryptography services), a clearer definition of what a closed group is, a better understanding of the liability issue - including the liability of a licensed TTP for damage caused by faulty services other than compromise of encryption keys, the need to make any legislation technology neutral (which these proposals manifestly are not), a better understanding of the subset of licence conditions that would apply if only some cryptography services were being offered, and how the lawful key access process will really work in a way that minimises the chance of misuse or compromise.

Conclusion

EURIM welcomes this first attempt at defining a framework for the provision of cryptography services. However, these proposals have such major flaws that EURIM recommends a further round of public consultation. Any proposed legislative framework must then show how the legitimate interests of industry have been met, and how the proposals strike the right balance between the benefit to law enforcement and national security, and the costs to industry and the individual.