CEPIS Position Statement

ELECTRONIC COMMERCE

Introduction

Electronic Commerce ("e-commerce") currently attracts a lot of attention. There is a European Initiative, COM(97)157 [1], press articles appear almost daily and scientific journals regularly discuss selected topics in the area [2]. It covers a wide variety of commerce-related activities, which have in common that some form of electronic communication is involved, using a private or a public network. Today's value of e-commerce transactions is already large and is bound to increase considerably over the next few years.

Any value in any domain is based on mutual trust. E-commerce is no exception. Trust may be relative: limited trust (implying the acceptance of a certain degree of risk) does not mean rejection, but the greater the trust, the higher will be the associated values. Hence, e-commerce may be expected to thrive especially if the set-up of both the supporting systems and the procedures for their use can be truly trusted. Thus mechanisms should be available to demonstrate correct functioning of the underlying technology, but this is not enough. Whilst the state of the art offers reasonably dependable and efficient (although never fully secure) services, personal discipline, organisational arrangements and legal regulations are often insufficient and sometimes simply counterproductive.

CEPIS's position regarding these three problem aspects and their potential cures (discipline: education, arrangements: codes of good practice, regulations: appropriate international agreements) is summarised in the following sections. In some respects, there is cause for concern.

Definition(s)

There is no generally accepted definition of "e-commerce". As viewed by CEPIS, e-commerce comprises all marketing and sales or free provision of goods and services of which some part is arranged via a private or a public electronic network. Typical examples are the use of chipcards for payments or for the storage and transmission of medical data, advertising and selling tangible or intangible goods and services via the Internet, placing banking and stock exchange orders via specialised nets, and connection to sundry information services on public cable nets.

A distinction should be made between:

1. public information (yet not always free of charge, in addition to the network connection costs),
2. information with the intent of selling goods or services (i.e. marketing),
3. transactions via a network (placing orders, order acceptance, invoicing, etc.).

The first category gradually tends to overtake other forms of public information (parliamentary records, promulgation of legal texts, telephone directories, public transport time tables, official notifications via the press and other traditionally paper based communications).

The second category is not limited to the Internet. It is a common feature of special networks (such as restricted banking services) and, strictly speaking, TV commercials are a manifestation of it, too. These forms of electronic communication based marketing may be compared to enclosing unsolicited that is enclosed with regularly contracted or occasionally acquired services (newspapers bought in a kiosk, journals one has subscribed to, bank statements, municipal services statements, etc.).
The third category is more complex, in that several steps are mostly needed before a transaction may be deemed completed. It is this category that is normally associated with "e-commerce", as such. Electronic marketing (CEPIS's second category), in general, is tacitly assumed constituting a subset of it. However, there are good reasons for separate treatment.

**Trust**

In all three categories trust in the validity of what is passed over the network and the care with which it is handled at either end is essential. Admittedly, limited trust will work if it is felt that benefits outweigh risk. However, it is especially important for the non-expert (who is not able or willing to make the necessary detailed analysis) that a high degree of trust is present.

In the case of electronic transactions the well-known qualities of security (confidentiality and integrity), authenticity and non-repudiability are desirable. Unfortunately, credit card companies, banks and mail order houses often accept insecure orders just to win customers: the weaker party in the market may have to forgo some of the desired qualities. Conversely, fraudulent use may result when an electronic invoice might be repudiated, not to mention abuse of other persons' credit.

However, the same requirements are also indirectly essential for the first two categories. CEPIS views with concern a number of current developments. Firstly, the common lack of public understanding makes it difficult to distinguish hype and truly worthwhile opportunities. Secondly, the widespread lack of discipline (both with providers and recipients of services) may lead to failures that ultimately harm potential customer acceptance. Lastly, the debate over security and "legal access" may obscure the economic issues, as well as the freedom of expression and privacy aspects.

**Current situation**

Currently, a variety of arrangements exist. Concern has been expressed regarding transactions in which unscrambled credit or bank card data is transmitted over public networks. However, in the physical counterpart of these (say handing a credit card to a waiter, a bank card to a sales person), abuse would also be possible, but does not seem to be high on anyone's agenda [3]. Even more debatable are attempts - national security and/or crime prevention inspired - at legislation and regulation - and even prohibition - of the use of "encryption".

Earlier, CEPIS has expressed the view that there should be no obstacle to the availability of strong encryption and that access to encryption keys (via so-called "trusted third parties", involving what is known as "key escrow"), should be avoided or, if deemed necessary, possible only under the strictest legal protection. Abuse of legal (but often in fact illegal) access, e.g. via wire tapping, is a characteristic not only of police states. It should not be extended to electronic communication [CEPIS Position: http://www.iig.uni-freiburg.de/cepislsi/crypto/PolicyStatement.html].

Additionally, most effort is aimed at providing security for organisations. No technology has been developed as yet to enable private users, say users of e-commerce services, to produce documents in a safe way, themselves. Especially current solutions for digital signatures tend to ignore the fact that there are many possibilities to make users sign documents that are completely different from what is shown on their screens. This is mainly caused by insecure operating systems and by the lack of secure displays, e.g. on current chipcard or signature equipment. Yet, even if these weaknesses are overcome, there remains the problem that "security between boxes" should be demonstrably supplemented by safe procedures around them.
There are not many guarantees regarding the quality of what is circulated via networks, the more so when it extends across national borders. Nationally, advertising codes of conduct may be applied, but strict enforcement is notoriously difficult. In fact, CEPIS favours self-constraint, but “complaints boards” may ultimately be accepted, both nationally and internationally.

There is definite cause for concern about the newly emerging regulations for copyright of electronically circulated material. If such publications can be and are unreasonably pirated, strong regulations make sense, provided these are workable. In particular, they should not prevent well established access to public information or practically pre-empt the economically attractive electronic distribution of interesting material.

Finally, there is a lack of awareness of the potential of e-commerce. Since increased freedom and scope of commercial interchange must be considered globally beneficial, there is a world wide task of promoting “e-commerce literacy”.

**Recommendations**

On the basis of the above, CEPIS recommends the following:

1. **E-COMMERCE CONSIDERED BENEFICIAL**
   Electronic Commerce should be considered beneficial and deserving global protection and encouragement (legal and technical), such that it will enjoy a high level of general trust.

2. **E-COMMERCE RELATED REGULATION TO BE INSTITUTED WISELY**
   - Some public regulation is needed to avoid the strongest parties dictating the rules. Users and customers need enhanced protection, e.g. when they would be forced to use unilaterally secure communication that only protects their counterparts.
   - In the full range of e-commerce-related activities, a variety of legal and other kinds of regulation are needed: public information should be subject to quality guarantees, marketing information should be truthful and unsolicited, commercial transactions should be secure and capable of legal enforcement.
   - Since the strictest forms of regulation may lead to self-defeating arrangements, one often has to settle for lesser security - however, all parties (including non-experts) should be made aware of the benefits and risks involved, and how to view a balance of these.

3. **E-COMMERCE MESSAGES TO BE ENSURED CONFIDENTIALITY**
   Messaging related to e-commerce should be ensured confidentiality, i.e. be accessible only to the parties involved in the commercial transaction intended or concluded.

4. **E-COMMERCE CHALLENGES TO GOVERNMENTS**
   Governments should be encouraged to pass suitable legislation (guaranteeing freedom of expression, promoting quality control, ensuring legally binding arrangements, including signature rules), and mutually harmonising their legislation such that internationally trusted arrangements result (providing equitable consistent taxation and effective international law enforcement).

5. **E-COMMERCE CHALLENGES TO PROFESSIONAL ORGANISATIONS**
   Professional organisations and other international institutions, such as chambers of commerce, organisations of notaries and computer societies, should promote good practice through informative and educational programmes; these should take cognisance of and add to international recommendations, such that an effective basis for development and acceptance of e-commerce will ensue.

In summary, CEPIS considers e-commerce a desirable development, given appropriate governmental and societal regulation and discipline. Specifically, the development of appropriate standards and generally accepted codes of good practice and codes of conduct are recommended. Associated with these should be the institution of competent complaint boards and other forms of assistance.
For further information, please contact CEPIS:

- CEPIS Network Legal & Security Issues
  [ lsichair@cepis.org and http://www.wi.leidenuniv.nl/~verrynst/cepislsi.html ]

- CEPIS Secretariat
  [ secretary@cepis.org and http://www.cepis.org ]

Endnotes
[3] PIN procedures are beginning to come under increased scrutiny; also it is in the interest of credit card companies to cut down on fraud.

Adopted by CEPIS Council
30-AUG-1998