24

More Than Just a Lock in the Browser: A Global Consumer-Company Transaction Security Perspective

José Luis Gómez Barroso[1], César Del Pino González[2]
1 Departamento de Economía Aplicada e Historia Económica / Applied Economics and Economic History Department
Universidad Nacional de Educación a Distancia (U.N.E.D.) / Distance Learning Spanish University
2 Technical CEO. Portal Tienda S.L.

Abstract: The views about the security in B2C e-commerce often point to a particular aspect. The role and the real value of these matters can be understood only from a broad perspective. This paper examines the security as a global problem that it is a first order concern for consumers and companies.
By reviewing the different process stages involved in an electronic transaction, five issues where security is a requirement can be identified: actor identification, communication confidentiality, protected payment methods, computer equipment security and appropriate legal scenario (rights of the consumers and personal data treatment).
Each of these issues deals with the guarantees that should be provided, those that in fact exist, and those that may be provided in the future.
Technology is only one of the incumbent causes. Others, such as the economics, strategy, lawfulness and, specially, the actor readiness are issues considered extremely important for increasing transaction-related security.

1. INTRODUCTION

It is not an unusual affirmation that e-commerce security is closely related to the Internet's general security. This simplistic opinion would actually mean that e-commerce is insecure due to it needing to "cross the jungle", that is, it uses a means of communication over which no control can be established.

Nevertheless, this is only one of the many security problems on-line businesses must deal with. In fact, it is not even the most important one, and it may be one of the easiest to resolve. Technological progress provides

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35617-4_48
J. L. Monteiro et al. (eds.), *Towards the Knowledge Society*

renewed guarantees, but not only technology is actually required. Security concerns must reach beyond the data transmission issue and cover each and every telematic transaction stage.

Another topic consists in presenting security as an obstacle for attracting inexperienced and distrustful consumers. Again, we must broaden the perspective and accept that security is, in fact, one of the first perceptions collected by every potential user. It is evident that the risk perception differs according to the personality and previous experience of the user. In any instance, regardless of the consumer having major or minor concerns, receiving guarantees that reduce them shall always result in a confidence boost. And no-one seems to doubt that confidence is the basic pillar required for the development of e-commerce.

As a consequence, companies are aware that increasing security will favourably affect their sales. This is both generally (global security levels for the overall e-commerce), and specifically, applicable: announcing a failure or an error can represent a depth charge for a company's reputation, something which is both extremely fragile and appreciated in this still immature channel. The decisions on how the security should be dealt with must be taken from the start of the activity, and they will represent the keys to the company's success or failure. They must cover the whole system and be present in the daily activities of all the members of the organisation.

All of the above seems to make up sufficient grounds to avoid dealing with the security issues separately, but as a part of a basic core question for anyone studying the e-commerce scenario instead.

The paper is organised as follows. In section 2 we will follow the steps of an electronic transaction paying attention to the main security issues involved. We will find five categories of problems: authentication, confidentiality, protected payment methods, computer equipment security and appropriate legal scenario (rights of the consumers and personal data treatment). The "ideal", "real" and "future" solutions to these problems are analysed in sections 3, 4 and 5. Finally, we extract some conclusions.

2. RISK SCENARIOS DURING A TELEMATIC TRANSACTION

Security mechanisms should cover all the stages of an electronic transaction since all of them are threatened from the participating parties' point of view. Maybe many of these threats are only probable, but they are nevertheless possible.

2.1 Surfing through the company website

Buyers lack direct contact with the company. Their confidence in that virtual store depends, in the first place, on the firm being famous (Degeratu, Rangaswamy and Wu, 2000) and, should this not be the case, of the access method. The methods providing the greatest degree of confidence are direct recommendations, appearing in the first places of a search engine or a portal "suggesting" that store.

But in fact, such store may not actually exist and the web site may have been created with the sole purpose of collecting information, or, directly, ripping off users.

Consequently, consumers would seem to be safe from these dangers in a "prestigious" company's website. Nevertheless, thanks to the IP spoofing system, the identity of another address can be taken on so as to deviate the connection to a different IP than the one typed in and display a different home page than the original one (Amor, 2000). The usage of illegitimate sites facilitates, without any doubt, web "impersonation". Virtual stores change so often their web page designs that a different aspect may not surprise usual visitors (Choi, Whinston, 2000).

The problem set out above is that of *authenticating* the vendor's.

2.2 Clicking on the checkout button

When the user has decided to make a purchase, the company will request it to enter a series of personal data. The type of data depends on the payment method used and the logistics required by the type of goods purchased. In the case of credit card payments, by entering their number, buyers are providing access to their current account.

Every time somebody fills in a form with his personal data, those data enter a path that leads to the company's router, crossing an indefinite number of routers and other devices. The communication can be intercepted and modified should no precautions have been implemented for the transmission.

In this case, the problem resides in the *confidentiality* of the communications.

2.3 Materialising the transaction

2.3.1 The selling company processes the order

A firm order does not always conclude in an actual sale. Mostly, the seller has to deal with 'false' transactions.

The transaction can be aborted due to different causes.

- The "experimenting" user tries to complete a transaction with false data in order to view the overall purchasing process and take a final decision on whether to actually materialise the purchase or not.
- "Absent-minded" users can forget to enter all the data or not review them adequately. The later the detection of inconsistent data, the greater the cost for the company.
- "Defrauding" customers can get a product and elude their payment responsibilities. The payment method strongly marks the different fraud possibilities.
  - It is a complicated matter in the case of payment in advance via bank transfer or check.
  - It is almost impossible in the case of cash on delivery, the customer will not be given the product until they pay for it.
  - Credit card payment is the most problematic issue. On one hand there is the theft problem (physically the card itself, or even the data). On the other, since internet credit card transactions are defined as "without the physical media", their holders can deny having made the transaction. And this issue does not have an easy solution: defining the responsibilities for an unauthorised card usage clashes with an intentionally fraudulent cancellation. Protecting individuals is the legally prevailing trend, and boosting the appropriate refunding mechanisms is preferred (OECD, 2000).

In the case of false identities or the rejection of previously ordered products, the problem resides in *authenticating* the customer.

In the case of receiving and not paying for a product, the problem resides in ineffective *payment methods*.

2.3.2 The customer waits for the order to be processed

Customers, on the other hand, expect vendors to meet their commitments; the product is supposed to reach in time its destination flawless, and the customer must be entitled to return it.

Fraudulent practices are greatly similar to those used in the classic business scenario (pyramid sales, products never delivered or not meeting the consumers' expectations), which are backed by anonymity and the possibility of making the fraudulent store disappear in a few hours (OECD, 1998). Sometimes, a lack of service ends up being an actual fraud procedure.

In this case there is the legal problem of *consumer rights* within an electronic exchange.

2.4 Once the transaction is completed

The company stores customer data, which is extremely precious information for the company itself, and, in the case of passwords or credit card numbers, for defrauders.

The purchaser expects the company not to use that information in an unlawful way, that is, it is not to be sold, neither compared with other databases, neither used to unauthorised spam. This is a problem that not all consumers are aware of. In a survey carried out recently, those worried about this issue also referred to the security of communications; although the reverse side is not true (Elliot, Fowell, 2000). In any instance, this does not mean that we are facing a minor problem.

This is yet another legal problem, consisting in the *unlawful usage of personal information.*

On the other hand, although the company's ethical behaviour may be correct, they are also subject to a protection duty. The consumer trusts their data will not be easily accessible to any *hacker* remotely accessing the computers or trespassers entering the company's premises.

The problem here consists in *computer and internal procedure security.*

3. SECURITY REQUIREMENTS: IDEAL SOLUTIONS

3.1 Authentication

Each electronic communication should allow relating the parties with real world entities (individuals or companies) confidently. Provided that the documents exchanged in electronic transactions are easily forged, a mechanism should guarantee the authenticity of the documents. Ideally, a *signature* must inseparably link the signer with the document and guarantee that this document has not been manipulated.

In a second step, a signature recognition mechanism is needed to establish a link between the signature and the signer. The certification system must guarantee in any way that the signature corresponds to the only person authorised to use it, so as to avoid any possibility of fraudulent impersonation.

The identification data must be as reduced as possible in order to preserve the privacy of the parties and avoid them exchanging anything more than what is strictly necessary.

3.2 Confidentiality of communications

The integrity of the information included in a communication should be granted. Using a sufficiently resilient cryptographic protocol, the impossibility of reading the information is guaranteed throughout its transit.

The key used to decode the message must be the only way available to extract decoded information. This key should be copy-proof, thus guaranteeing privacy unless the key holder makes it available, willingly or not, to third parties.

3.3 Payment methods

In general, a payment method should provide, at reasonable economic cost, enough guarantees for both the buyer an the seller.

However, it seems not to be possible to define an unique ideal payment method as it involves subjective aspects that cannot be neglected in a such important subject. These are related to users preferences and habits. The common practice greatly differs from one place of the world to another. Americans make the greater part of their purchases using their credit cards; in Europe, cash is more widespread. The figures speak for themselves: an average 1,480 cards per 1000 customers opposite only 390 in Europe (Singh, Jayashankar, Singh, 2001).

This leads us to thinking that an electronic store should provide an array of options, thus covering all their customers' preferences. These customers would be able to select the most efficient means of payment according to the circumstances, as occurs in classic stores that usually cater to all payment method requirements (Singh, 1999).

When designing a new electronic payment method, it is important not to forget some of the qualities of existing payment methods:

- It should be compatible with any amount of payment (major or small).
- The anonymity issue is other desirable characteristic in payment method. In the same way as in traditional commerce where no receipts are generated for small purchases, e-commerce should not allow reconstructing purchases made by individuals.
- Last, it should be close to achieving synchronous exchanges. It seems fair that the charge against the purchaser's account should be made at the time the product is received and the consumer stated their conformity.

3.4 Computer security

Anyone storing sensitive data, and particularly when these are third party data (basically, all companies) should implement a security policy

establishing protection mechanisms against external attacks, as well as internal fraudulent usage.

The plan starts by studying the security requirements. Based on the conclusions of this first report, and comparing them to an eventual quotation, an assessment on what is to be protected, and in what degree, is made. Although total security is not possible in any instance, security policies should adjust to the value of the item being protected. As a consequence, only third party information which can be "reasonably" protected should be handled. And this, in turn, implies that it is ethically possible to relinquish from storing customer data when they cannot be duly safeguarded.

Considering the above, a correct anti-hacker procedure must search for the vulnerable points in systems and communications and create a protection procedure which must be regularly updated in order to avoid it turning obsolete in a short period of time.

Additionally, at the internal level a clarification as to who can access specific databases, and when, must be made.

3.5 Legal framework

We have identified two issues as clearly requiring legal protection: consumer rights in electronic transactions and the protection of their data.

No-one can deny that one of the main advantages of e-commerce is that it is barrier free. As a consequence, national solutions given to these issues will always be partial: in case of a conflict, it is necessary to determine what jurisdiction should resolve the case and according to what affected legislations (often disparate). This is where legal insecurity arises since purchasers are not aware of the rights they are entitled to in each transaction.

As a consequence, to reach an ideal situation, there should exist global agreements on these issues guaranteeing that any exchange would be subject to data protection and consumer rights under the same conditions. As this objective seems utopian, the agreement should guarantee a set of basic minimum rights. Additionally, courts of law or arbitration mechanisms would have been set up with an undeniable jurisdiction regardless of the affected parties' nationalities.

4. SECURITY REQUIREMENTS: CURRENT SOLUTIONS

4.1 Authentication

The parties participating in an electronic transaction must be able to recognise each other' signatures. Should both parties know each other, they can exchange their public codes regardless of the method used for this purpose. PGP (pretty good privacy) is the world's defacto standard for e-mail encryption (Hunt, 2001).

This is perfectly valid when the parties are previously aware of each other and there is no risk of fraudulent impersonation. Nevertheless, in the e-commerce scenario, we require the intervention of a certifying entity guaranteeing that the actors are really who they claim to be.

There are certifying authorities in each country, but confidence arises when the certifier is known to both parties. Additionally, there is a second problem consisting in the need for the certifying entity signature algorithms to be implemented in the servers of the stores as well as in the customers' browser. These are the two reasons that make Thawte and VeriSign the almost universal certifying entities implemented in the greater part of the e-commerce stores.

A certifying authority is not only obliged to safeguard the security of sensitive customer data; it must also strictly comply with the requirement of accurately investigating the personality of the entity requesting the certification. In practice, it seems that the criteria are not as strict as they should be, as proven by the fact of an individual being wrongly certified as a Microsoft employee (refer to the press on 22-23 March, 2001).

Without any doubt, National certification authorities (and particularly when they are public organisations) would be better suited to carry out this previous requesting party identification task. For instance, the Spanish Ministry of Economy is obviously keen to identify the taxpayer before awarding them the certificate validating their relations on the Internet. Nevertheless, their validity covers little more than those administrative relationships since it has the same two problems described above: universal acceptance and compatibility.

An International association of these national authorities would provide an answer to these inconveniences. A useful idea would be that of implementing a hierarchy of certifying authorities as well as a cross-reference certification system for said authorities (OECD, 1997). Strangely, certifying entities certify themselves, and in practice, the browser is the element in charge of trusting a list of certifying entities. This makes browser developers the essential partners for any certification business.

All these motives (understanding that there are others) contribute to a reality where day to day e-commerce uses partial, not too technologically "elegant", solutions to try and resolve the authentication issue.

Apart from the certification-related problems listed, the truth is that there are very few individuals with their own certification. As a consequence, companies frequently require a telephone number or e-mail address for contacting the customer. This procedure could be refined: for instance, sometimes free e-mail accounts are rejected.

On the other hand, it is also usual for customers to call the company trying, first, to be certain of its existence (despite them seeing the logo of the certifying entity) and subsequently asking process-related aspects (even when this information is posted on web page and they may have even read it) in order to have a more concise opinion of the store's "responsibility".

4.2 Confidentiality of communications

Whenever a lock appears in a corner of the browser, the communication is being carried out through a secure server, which can also be identified with the letters https at the beginning of the web address. From that moment, the transmissions shall be encrypted.

Netscape-developed SSL (Secure Socket Layer) is the secure transmission protocol accepted as a defacto standard. The security is based on the usage of an encryption system and the exchange of a digital certification. TSL, SSL's successor, also allows using different encryption systems among which one is selected at the start of the negotiation between the parties.

Two issues must be focused on. In the first place, there are still problems regarding the usage of certain encryption keys. The United States have considered them as national defence issues (Glickson, 1997) and have only recently allowed exporting 128 bit encryption technology (Klang, 2001). In other countries, certain private protocols are not accepted in order to guarantee that, for instance, it is impossible to decode any message, even when required by a court of law. In these instances it is not easy to establish the frontier between secrecy of communications and public safety (OECD, 1997).

Even more problematic is the fact that, although the number of secure servers is increasing, it is still reduced and presents enormous disparities from one country to another: in July 2000, half of the OECD countries had less than five secure servers for every 100,000 inhabitants; the United States had six times the average figure for the European Union (OECD, 2001).

4.3 Payment methods

Non-trust of the payment method is one of the top reason why users do not buy on-line (Putland et al., 1999). The excessive number of alternatives, their lack of integration, the lack of dominant standards and the scarce user proficiency as regards the systems are some of the circumstances contributing to this fact (Nath et al., 1998).

So, despite the existence of a great deal of sophisticated systems, a great number of stores still choose "traditional" methods based on two reasons: many people associate greater danger threats with credit card-related payments; and, second, the companies themselves do not find these solutions economically or strategically attractive.

As a consequence, cash on delivery or payment via checks or bank transfers hold the first position in the list of the most used payment methods. Nevertheless, these methods lead to losing a great deal of the benefits related to e-commerce since. Additionally, these options are not possible in the case of "digital" products, and in practice, are limited to national transactions.

The other conventional possibility is the request and sending of a credit card number, the problems of which we have already dealt with when covering the fraud issue.

The SET (Secure Electronic Transaction) protocol provides a solution. Its implementation as a real standard seems to be very doubtful at present. Other electronic intermediaries for traditional credit card-based systems such as First Virtual, WireCard or the more known CyberCash have not been able to have any more success.

The solution for "micro payments", that is, small amounts which require a formula with costs inferior to that of the product itself, has not been commonly accepted yet either (Choi, Stahl, Whinston, 1997). Apart from the technical implementation problems, there is an added difficulty, which, in this instance, is psychological, in systems with frequent access: consumers prefer to pay a subscription fee instead of paying for each usage (Amor, 2000). The so called pre-paid cards could represent a solution; in this instance, their usage has not progressed due to the need of installing a device reading this type of cards in each purchaser's personal computer.

DigiCash was the first attempt to establish "electronic cash", virtual money stored in your hard disk drive, but it was unsuccessful. As occurred with the subsequent NetCash, CyberCoins or MilliCent. Additionally, retailers have not accepted these solutions with much enthusiasm.

The potential provided by telematic transmissions between online banks have not been leveraged for now either. The inaction of the banking system has promoted the creation of intermediary companies such as PayPal or Billpoint.

Last, we would like to focus on the fact that none of these solutions provides any added services interesting enough as to delay the moment of effectively collecting the payment until making it coincide with the reception of the item.

4.4 Computer security

Companies do not invest as much as they should in protecting their equipment or they simply do not comply with the trend of storing only what they can protect.

Despite it being worried by security, a small company should never store information as sensitive as their customer's credit card numbers. The acceptable risk must be minimum, and minimum risks lead to constructing powerful barriers, actual bunkers, the cost of which is usually too high for small firms.

Unfortunately, companies storing absolutely all their customer data in precarious security conditions are not the exception. This is not a consequence of a lack of choices: returning to the credit card number issue, prepayment systems could be used with duly protected third companies who would store this information, or else, there is the option of simply eliminating the data once the payment has been completed.

Internal company procedures are usually not efficient either (they may not even exist) in view of the data stating that a sensible number of incidents are originated by someone obtaining the information from the inside. The best firewall software is then useless if the intruder can access the premises and copy the files to a diskette (Amor, 2000). Sometimes, even a system of passwords, an extremely simple although very useful procedure, is not installed.

4.5 Legal framework

Except in cases of extremely well known brands or sales of special products, e-commerce for tangible products continues to be carried out mainly at the national level. Forgetting for a moment the logistics-related shipping problems, an eventual consumer visiting a far away store will usually think that it will be almost impossible to complain if the product is defective or if there is any incident whatsoever regarding the service. The instability and unpredictability of the legal and regulatory framework surrounding the eclectronic commerce applications is one of the biggest headaches for business (Kueter and Fisher, 2000).

Legislations are far from being harmonised, and there is no indication that this issue will be resolved in the near future. The task is arduous because we do not even have shared moral values: social, religious or politically-

related motives provide very different perspectives on the role of the Government and the contents of the Law (Klang, 2001). For instance, the United States consider that the development of e-commerce should be almost exclusively lead by private initiative while the average European declares himself more of an interventionist (Zott, Amit, Donlevy, 2000).

A clear example is the conflict generated as regards the European Union Directive on data protection (which is currently under revision and a new draft is expected shortly). This is a concern that is reflected in the surveys made on European consumers that consists in the Directive requiring any information transmitted outside Europe to be authorised by its holder while the company receiving it must prove that it does not use it for purposes other than those it was collected for (Singh, Jayashankar, Singh, 2001). Since this also has a commercial impact, it has generated legal responses by other governments (Scheibal, Gladstone, 2000).

Some authors do not see law convergence as a serious barrier, and think that it is absolutely unreal to expect any type of legislative rapprochement (Millard, 2000).

5. SECURITY REQUIREMENTS: FUTURE SOLUTIONS

In three of the sections above, the comment on what can be expected in the medium term is very brief:

- Confidentiality of communications is an issue which is pretty much resolved and to which all we can add is that the usage of encryption is bound to spread.
- The computer security issue represents the eternal fight between guardians and attackers: the defence procedures will improve, but the attack methods will be perfected.
- As regards legislative issues, we cannot really provide any speculation. Surely, no major International agreement can be expected, although there is a possibility of bringing together regional regulations.

Major innovations will occur in the authentication and payment method scenarios, either separately or combined.

Even if the certification requests made by users were to grow spectacularly, the certifying entities were to tighten the requirements for awarding them and, as a consequence, the usage of electronic signatures were to progress, there would still be an added problem. Again, the computer security issue arises, but in this case as regards domestic equipment. Obviously, consumers cannot be asked to establish security plans; the greater part of the equipment are easily subject to attacks. This is the greatest

weakness of any cryptographic system controlling access to private keys (Hunt, 2001).

On the other hand, it would be convenient if the consumer could sign their messages not only when they are in front of their computer but also when they are surfing, for instance, from a cyber cafe.

Both these reasons lead us to think of independent certification devices that anyone can carry with them at any time. Thus, two possibilities appear.

The first, specific smart cards. If all computers were equipped with devices capable of reading them, one would simply have to insert the card and type in a password for sending encrypted messages from any part of the world. Biometrics (individual vital signs, iris...) will be the way forward to replace the imperfect technology of passwords and PINs (Trask and Meyerstein, 1999).

The second option consists in incorporating that certification functionality to some other card already in use for other purposes. Mobile telephones immediately come to mind: they are strictly personal and one always carries them. The progress of these systems shall occur when e-commerce web pages display a number for the transaction in an environment where all devices are connected via wireless technology. Indeed, the integration of card technologies with emerging technologies (mobile computing, the bluetooth protocol, flash memory, etc.) will also influence the advancements in the field (M'Raïhi and Yung, 2001).

As regards payment, the possibility of incorporating smart card readers in the equipment would definitely boost the prepaid cards or other similar ones which, provided they include password-related security, would represent the solution for micro payments.

The same cards could store digital money. Some business attempts have been made based on the virtual currency scheme where a great deal of companies would provide and accept points exchangeable for electronic money. It is actually probable for digital money to reach some degree of popularity.

We are stating that the support for these payment methods are the smart cards, which is also the eventual support for authentication. The obvious conclusion is the integration of both systems.

6. CONCLUSIONS

This article has tried to prove that, against what is defended by some narrow-minded visions, the security requirements for an e-commerce transaction between consumer and company cover all the purchasing process stages.

Security of communications, which is often the most underlined aspect, is but a technological issue. One could also think that computer equipment security is also exclusively a technical issue, but in fact, the "holes" are due, much too often, to human and procedure failures.

On the other side of technology, we can find the legislative decisions, which are complicated since they require, in order to be fully operational, International agreements, and because they usually confront extremely vague frontiers (marketing vs. protection of privacy, card holder security vs. company security, privacy of communications vs. national security).

Countless new authentication procedures and payment methods are launched every day. Nevertheless, the increase of security levels depends on the solution chosen, which is usually not technically the best one, but the one that has won in a battlefield dominated by economical and strategic interests targeted at imposing a standard. In any instance, there is no doubt as to sooner or latter, these two issues shall find increasingly efficient and widespread answers. We consider that, in the medium term, smart cards will be the devices used to implement the signature and payment systems.

Companies must be aware of what they have in stake in the fight should they choose not to address the improvement of their security in a global manner. Implementing a secure system carries direct and indirect costs that are not immediately recovered. Nevertheless, it is more than likely that they will lose many opportunities and may even endanger their survival if they do not implement security.

Security is the objective condition of something as ethereal as confidence. If we do not want the future of e-commerce to be that ethereal, we will have to make a stop in the road to pay our security-related customs.

7. REFERENCES

Alexandris, N.; Burmester, M.; Chrissikopoulos, V. and Desmedt, Y (2000). "Secure linking of customers, merchants and banks in electronic commerce", *Future Generation Computer Systems*, 16 (4), 393-401.

Amor, D. (2000). *La (r)evolución e-business*. Buenos Aires: Prentice Hall.

Butler, P. and Peppard, J. (1998). "Consumer purchasing on the Internet: processes and prospects", *European Management Journal*, 16 (5), 600-610.

Choi, S.-Y.; Stahl, D.O. and Whinston, A.B. (1997). *The Economics of Electronic Commerce*. Indianapolis: Macmillan Technical Publishing.

Choi, S.-Y and Whinston, A.B. (2000). *The Internet Economy: Technology and Practice*. Austin: SmartEcon Publishing.

Degeratu, A. M.; Rangaswamy, A. and Wu, J. (2000). "Consumer choice behavior online and traditional supermarkets: The effects of brand name, price, and other search attributes", *International Journal of Research Marketing*, 17 (1), 55-78.

Elliot, S. and Fowell, S. (2000). "Expectations versus reality: a snapshot of consumer experiences with Internet retailing", *International Journal of Information Management*, 20 (5), 323-336.

Gefen, D. (2000). "E-commerce: the role of familiarity and trust", *Omega*, 28 (6), 725-737.
Glickson, S. (1997). "Point, click, and buy: contracting for online products and services", *Computer Law & Security Report*, 13 (6), 436-441.
Helander, M. G. and Khalid, H. M. (2000). "Modelling the customer electronic commerce", *Applied Ergonomics*, 31 (6), 609-619.
Hunt, R. (2001). "Technological infrastructure for PKI and digital certification", *Computer Communications*, 24(14), 1460-1471.
Klang, M. (2001). "Who do you trust? Beyond encription, secure e-business", *Decision Support Systems*, 31 (3), 293-301.
Kueter, D. and Fisher, R. (2000). "Business insights in e-commerce and trusted services", *Future Generation Computer Systems*, 16(4), 373-378.
Liao, Z. and Cheung, M. T. (2001). "Internet-based e-shopping and consumer attitudes: an empirical study", *Information & Management*, 38 (5), 299-306.
Mariotti, S. and Sgobbi, F. (2001). "Alternative paths for the growth of e-commerce", *Futures*, 33 (2), 109-125.
Millard. C. (2000). "Four key challenges for internet and e-commerce lawyers", *Computer Law & Security Report*, 16(2), 75-77.
M'Raïhi, D. and Yung, M. (2001). "E-commerce applications of smart cards", *Computer Networks*, 36(4), 453-472.
Nath, R.; Akmanligil, M.; Hjelm, K.; Sakaguchi, T. and Schultz, M. (1998). "Electronic commerce and the Internet: issues, problems, and perspectives", *International Journal of Information Management*, 18 (2), 91-101.
OECD, Organisation for Economic Co-operation and Development (2001). *Consumers the online market place*. Report DSTI/CP(2001)5.
OECD, Organisation for Economic Co-operation and Development (2000). *Recommendation on the OECD Council concerning guidelines for consumer protection the context of electronic commerce*. Paris: OECD.
OECD, Organisation for Economic Co-operation and Development (1998). *La protection des consommateurs dans le marché électronique*. Report DSTI/CP(98)13/FINAL.
OECD, Organisation for Economic Co-operation and Development (1997). *Electronic Commerce : Opportunities and Challenges for Government*. Paris: OECD.
Plouffe, C.R.; Vandenbosch, M. and Hulland, J. (2001). "Intermediating technologies and multi-group adoption: a comparison of consumer and merchant adoption intentions toward a new electronic payment system", *Journal of Product Innovation Management*, 18(2), 65-81.
Putland, P.A.; Ward, C.; Jackson, A. and Trollope, C. (1999). "Electronic payment systems", *BT Technology Journal*, 17(3), 67-71.
Scheibal, W.J. and Gladstone, J.A. (2000). "Privacy on the Net: Europe changes the rules", *Business Horizons*, 43 (3), 13-18.
Singh, S. (1999). "Electronic money: understanding its use to increase the effectiveness of policy", *Telecommunications Policy*, 23 (10-11), 753-773.
Singh, T.; Jayashankar, J. V. and Singh, J. (2001). "E-commerce the U.S. and Europe – Is Europe ready to compete?", *Business Horizons*. 44 (2), 6-16.
Sterne, J. (2000). *Customer service on the internet*. New York: John Wiley & Sons, Inc.
Trask, N.T. and Meyerstein, M.V. (1999). "Smart cards in electronic commerce", *BT Technology Journal*, 17(3), 57-66.
Ward, M. (1997). "Digital certificates and payment systems", *Information Security Technical Report*, 2(4), 23-31.
Zott, C.; Amit, R. and Donlevy, J. (2000). "Strategies for value creation e-commerce: best practice Europe", *European Management Journal*, 18 (5), 463-475.