Trust, Privacy and Security in E-business: Requirements and Solutions

Sokratis K. Katsikas[1], Javier Lopez[2] and Günther Pernul[3] [1]

[1]Dept. of Information & Communication Systems Engineering, University of the Aegean, Greece
ska@aegean.gr
[2]Dept. of Languages and Computation Sciences, University of Malaga, Spain
jlm@lcc.uma.es
[3]Dept. of Management Information Systems, University of Regensburg, Germany
guenther.pernul@wiwi.uni-regensburg.de

Abstract. An important aspect of e-business is the area of e-commerce. One of the most severe restraining factors for the proliferation of e-commerce, is the lack of trust between customers and sellers, consumer privacy concerns and the lack of security measures required to assure both businesses and customers that their business relationship and transactions will be carried out in privacy, correctly, and timely. This paper considers trust privacy and security issues in e-commerce applications and discusses methods and technologies that can be used to fulfil the pertinent requirements.

1. Introduction

Diffusion, general availability, and the benefits of information and communication technologies are rapidly changing our society, economy, and the way we do business. Digital business is much more than just buying and selling over the Net: digital business means doing business electronically, both within enterprises and externally, using computer networks or telecommunications. As such it includes any transaction completed over a computer-mediated network that transfers or supports the transfer of “value” for goods and services sold including property rights, like ownership of, or rights to make use of the goods or services.

An important aspect of digital business is the area of electronic commerce. The current state of e-commerce is a good example that the supporting technology has not yet reached its full potential. During the late 90’s there were a lot of predictions about how e-commerce would develop in the near future. For example, in 1999 Forrester Research predicted a volume of US$ 184 billion of US online retail sales in 2004 [1] whereas the actual value is only approximately US$ 69 billion [2], representing a big gap of almost 167 %. One of the major reasons for the gap between predicted value and actual development that has been suggested by the research community and

[1] Authors’ names in alphabetical order

backed by many studies is simply the lack of *trust, privacy and security in digital business*.

In order for digital business to reach its full potential the obvious conclusion is that either companies involved need to increase the level of confidence and trust provided by them to their customers or technologies need to be created having strong built-in features to protect the individuals' privacy and the security of the digital business transaction.

Because these areas transcend any single function or discipline within digital business, it is necessary to develop a global view. In this paper we are discussing the major issues involved. We will start with a general discussion on trust issues, followed by a discussion on the general meaning of privacy and privacy enforcing technologies and will conclude with the current major fields related to providing the security of the underlying technical infrastructures for digital business. Of importance are also complex psychological and social aspects how people react towards risks but due to lack of space they had to be omitted from our discussion.

2. Trust

Trust is a core issue in every business transaction. When considering an Internet-based scenario, this issue becomes extremely essential and, as we will see later, its definition is not trivial. Moreover, in order for Internet-based digital business to achieve similar levels of acceptance as traditional commerce, trust needs to become a built-in part of electronic transactions.

This is not easy because customers tend to perceive the Internet as a more or less anarchic environment that not only can provide good business liaisons but also multiple potential threats. It seems that it does not matter that the number of transactions where dishonest behaviour is detected is negligible in comparison with the number of transactions where the behaviour of participant is totally honest. Consumers and merchants are still worried about the threats, and their lack of trust has a negative influence on the wide deployment of the technology.

The problem becomes bigger if we consider the problem of the everyday more distributed nature of Internet commerce applications, where trust relationships of a specific user with other entities, companies, organizations, etc. differ depending on many different parameters. Moreover, recent pervasive aspects of the network itself provide new considerations to bear in mind [3].

2.1. Meaning of Trust

Different definitions of trust have been proposed in the literature during the last years. Some authors have tried to define the concept of trust in a global or general way, while others have defined it attending to the relation with specific types of applications.

One of the first attempts to define the concept of trust in e-commerce can be found in [4], where trust in a system is defined as "a belief that is influenced by the individual's opinion about certain critical system features". As pointed out in [5], that definition “concentrated on human trust in electronic commerce, but did not address trust between the entities involved in an e-commerce transaction”.

In fact, Grandison and Sloman in [5] argue that the lack of consensus with regards to trust led them to use the terms trust, authorization, and authentication interchangeably. Further, they define trust as "the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context (assuming dependability covers reliability and timeliness)”. Similarly, they define distrust as "the lack of firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context."

2.2. Relation with Authentication and Authorization

Trust, authorization and authentication can not be used interchangeably because authorization and authentication have to be considered as basic security services of applications, while trust can not be considered as a basic security service but as an outcome resulting as a combination of the appropriate use of basic services.

Additionally, we also agree on the importance given to authentication and authorization, as both services are essential to get trust from consumers and merchants. In this sense, the concept of digital certificate has risen as a technical solution that greatly contributes to increase trust on the e-commerce security technology in general, and on authentication and authorization services in particular.

Identity certificates (or *public-key certificates*) provide the best solution to integrate the authentication service into most applications developed for the Internet that make use of digital signatures [6]. However, new applications, particularly in the area of digital business, need an authorization service to describe what a user is allowed to do. In this case privileges to perform tasks should be considered. *Attribute certificates* provide an appropriate solution, as these data objects have been designed for use in conjunction with identity certificates [7].

It is widely known that the use of a wide-ranging authentication service based on identity certificates is not practical unless it is complemented by an efficient and trustworthy means to manage and distribute all certificates in the system. This is provided by a *Public-Key Infrastructure* (PKI), which at the same time supports encryption, integrity and non-repudiation services. Without its use, it is impractical and unrealistic to expect that large scale digital signature applications can become a reality.

Similarly, the attribute certificates framework provides a foundation upon which a *Privilege Management Infrastructure* (PMI) can be built. PKI and PMI infrastructures are linked by information contained in the identity and attribute certificates of every user. The link is justified by the fact that authorization relies on authentication to prove who you are, but it is also justified by the fact that the combined use of both types of certificates contribute to increase users’ trust. Although linked, both infrastructures can be autonomous, and managed independently. Creation and maintenance of identities can be separated from PMI, as authorities that issue certificates in each of both infrastructures are not necessarily the same ones. In fact, the entire PKI may be existing and operational prior to the establishment of the PMI.

2.3. Trust Management

When dealing with trust issues in e-commerce, its management is probably the most difficult problem to face. Blaze et al. introduced [8] the notion of trust management. In that original work they proposed the PolicyMaker scheme as a solution for trust management purposes. KeyNote was proposed [9] to improve two main aspects of PolicyMaker: to achieve standardization and to facilitate its integration into applications.

Afterwards, other similar systems have been proposed for trust management purposes. As argued in [5], a common problem is that those solutions are used to identify a static form of trust (usually at the discretion of the application coder). However, trust can change with time, and that is the reason why it is generally considered that digital certificates (identity and attribute) can be also considered for trust management purposes. More precisely, the infrastructures used to manage those certificates, PKIs and PMIs, provide procedures and functions that can be seen as an advanced method to manage trust. These are better solutions than the ones mentioned in the previous paragraph in the sense that are less static, but they are too biased towards authentication and authorization services.

In fact, trust management is tremendously dynamic, especially in digital business scenarios. Dillon et al [10] have elaborated on this issue. In their work, they argue that trust of one entity in another changes with a number of factors. Additionally, they define the dynamic nature of trust as “the change in the trustworthiness value of an entity, assigned to it by a given trusting entity with the passage of time in different time slots”.

3. Privacy

In the digital business arena privacy is usually related to the use of customer information. Transacting typically makes the exchange of large amounts of personal data necessary. This may either be necessary for the e-business transaction itself (for example: credit card information, banking account details, delivery details) or desired by the e-business partner: collecting customer data that later may be analyzed, shared with other businesses or even be sold. Altogether, privacy in our context may be defined as the individual right of humans to determine, when, how, and to what extent information is collected about them during the course of the digital business transaction; the right to be aware and to control the beginning of any interaction or data gathering process; and the right to choose when, how, and to what extent their personal information is made available to others.

At a first glance the two viewpoints, the first one supporting a corporate view and favouring the business interests and thereby strengthening the global economy, and the second one supporting the individuals view seem to be mutually exclusive. In practice, however, we face the need to reach a compromise and to arrive at a solution that is mutually beneficial to all. In the literature such a compromise is called *consumer-centric privacy*: for the individual this means to gain the maximum amount of privacy and for the e-businesses through the maximisation of privacy for their customers to gain substantial economic benefit. The economic benefit may be resulting from direct effects, like the improvement of the public image of the vendors (resulting in additional customers and in long lasting trust relationships) or from side effects, like improved brand recognition or more generally, a reduced trust barrier (as discussed in the introduction), leading to an increased e-commerce level and making many more individuals comfortable participating in digital business.

3.2. Methods to preserve privacy

These methods can generally be placed in three categories: privacy through legislation, privacy through organizational means, and privacy through technology. Combining solutions from the different fields may also be applicable.

Privacy through legislation

Governments in many countries have established legislation in order to protect consumers. Moreover, international guidelines, treaties, convention and regulation are also in place.

In the age of digital business, technology has advanced so far and so fast that the approach of protecting privacy through legal regulations is no longer as effective as it was in the past. Legislators are often far behind the new developments and the legal systems are not fast enough to properly react. Additionally, laws are generally country- specific. This means that a customer from a country that protects his privacy does purchase in a web store in a country without similar regulations does only have little or does not have any protection at all.

Privacy through organizational means

Both the shop owners as well as the users have simple organizational means that considerably help in protecting the privacy of individuals during digital business. For example, consumer data can be physically separated into personally identifiable and non-identifiable information. Of course, it should not be possible to combine the separated data buckets.

Another organizational means is to involve into the business transaction a third party transaction service. Such a service would act as a trusted intermediary that guarantees the outcome of the transaction. Other organizational means to increase trust and privacy are delivering some sort of belief to the consumer that a merchant complies with a certain privacy policy. This may be achieved by privacy seals issued by a trusted authority (for example TRUSTe, the “online privacy seal”) or through technologies such as the Platform for Privacy Preferences (P3P), that allow customers to evaluate whether the published privacy policy of the business satisfies their own preferences. However, both approaches do mainly show the awareness of a business of their customers’ privacy concerns; they cannot guarantee that the business actually will behave as expected.

Privacy through technology

Privacy Enhancing Technologies (PET) attempt to achieve anonymity by providing unlinkability between an individual and any of their personal data. Several levels of anonymity have been defined in the literature, ranging from full anonymity (no one can find out who you really are) to pseudo-anonymity (the identity is generally not known but may be disclosed if necessary) to pseudonymity (several virtual identities can be created and used under different situations). Anonymity can be achieved by either anonymising the transport medium, or by allowing anonymous access, or by using statistical databases.

Technologies for anonymising the transport medium aim at hiding the original identity of the consumer in a way that his identity cannot be revealed. One of the simplest possible ways to achieve this for a user is to simply set up an account with a free email service provider the user trusts that they will not log communication details. Another possibility is to use an anonymising server. When an individual is using such a service, all communications are routed through the anonymising server, thus the recipient has no way to determine the IP address or the identity of the user.

A further step in technical complexity is a setting without a trusted third-party. Crowds [15] groups users into large groups (crowds) and instead of directly connecting requests to a web site, the system passes it to the crowd. There the request passes a randomized number of crowd members and finally is submitted to the recipient who is not able to identify who in the crowd is the originator of the request. Another well-known and prominent technology is Chaum Mixes [16], whereby messages of equal size are cryptographically changed and finally delivered to the recipients in different order. Chaum Mixes have been extended by onion routing protocols, which use a network of dynamically changing mixes and the user submits a request in form of a data structure reminding on the layers of an onion.

In systems allowing anonymous access to a service, users are known only by a pseudonym (credential) to the organization they are doing business with. A single user can use different pseudonyms which cannot be linked to each other.

Related to anonymous access is the use of an authentication and authorisation infrastructure (AAI). Such infrastructures arose from the fact that it is not always necessary to exactly know who a user is but sufficient to know that the user is authorized to perform a certain action. Often this is outsourced to another organization, which is responsible for registering users, user authentication and equipping users with proper credentials. This of course implies that the AAI is trusted to the organization relying on such services. Different types of AAIs and their use are surveyed in [17].

A statistical database is a data collection, for example all customers and their items bought but not revealing information that uniquely identifies the individuals. The value of such databases is the statistical information, not the data itself. Therefore, techniques are essential that can keep the statistics of the data set valid but keep the individuals data itself private. All these techniques have the disadvantage that they make the data less useful. Additionally, it has been shown that by repeating slightly changing queries database trackers revealing individuals' privacy may be constructed. Statistical databases have their potential in CRM (customer relationship management) and general data mining.

4. Security

Recognising the fact that, in any given e-commerce scenario, there are five interconnected and interacting components (people, software, hardware, procedures and data), one comes to the conclusion that e-commerce systems are (and should be looked upon as) information systems, comprising a technological infrastructure and an organisational framework, rather than pure technological infrastructure. Therefore, addressing the problem of security in e-commerce must be done in an information system setting.

In such a setting, security can be defined as an organised framework consisting of concepts, beliefs, principles, policies, procedures, techniques, and measures that are required in order to protect the individual system assets as well as the system as a whole against any deliberate or accidental threat [18]. Operationally, in order to compile such a framework, the pertinent requirements must be identified first.

4.1 The security requirements

E-commerce applications may seem quite dissimilar, at a first glance. However, closer inspection reveals that there exist distinct phases in all of them, a fact that allows a generic model to be built, which can describe all of them. Such a model has been proposed in [19] for business transactions and has been shown [20] to be good for describing commercial transactions as well. In an exchange transaction, two parties, A and B, agree to and fulfill mutual conditions of satisfaction. The first party, A, is usually called the *customer* or *buyer*; the second, B, is usually called the *performer* or *seller*. B accepts A's request to provide something for A, in exchange for which A will provide a payment to B. The transaction can be visualized as a cycle of four phases:

- *Request:* A makes a request of B to provide the service. (Often this amounts to taking B up on an offer B has made).
- *Negotiation:* A and B come to an agreement on exactly what will be provided (A's condition of satisfaction) and what payment will be made (B's condition of satisfaction).
- *Performance:* B carries out the actions needed to fulfill his part of the bargain and notifies A when done.
- *Settlement:* A accepts B's work, declares it satisfactory, and pays.

The last two phases can be combined into one composite phase, called the *Execution* phase [21]. The model is good for any kind of transaction, not only electronic transactions.

During the Request phase, the buyer needs to be sure that an offer s/he is considering is valid, i.e. s/he has to be sure that the integrity of the information that is presented to her/him has not been compromised. On the other hand, the seller must be sure that the offer s/he makes is available to the buyer. If the transaction is not a retail one, the seller may want her/his offers to remain confidential to the buyer, lest any competitor interferes with the transaction. The need for confidentiality is also apparent, for both parties, in the Negotiation phase, in particular when this pertains to contract negotiations. Important in this phase is also the inability of either party to repudiate their offers. But non-repudiation is even more important in the last, the Execution, phase. In this phase, secure payment must also be ensured, as well as secure delivery of goods. Finally, observe that what is fundamentally different between e-commerce and traditional commerce is the absence of human face-to-face communication. Machines have no way of knowing who is *really* on the other end of the line once presented with pre-agreed information that convinces them of her/his identity.

Therefore, e-commerce security requirements revolve around the need to preserve the *confidentiality*, the *integrity* and the *availability* of information and systems, the *authenticity* of the communicating parties and the *non-repudiation* of transactions.

4.2 Addressing the requirements

From a structural point of view, an efficient framework for preserving security in information systems comprises actions that are categorised as legal, technical, organisational and social. Legal actions consist of adopting suitable legislation; these should be and have been undertaken by governments at an international, national, and even local level. Technical and organisational actions need to be undertaken by individual organisations (or by bodies representing organisations of a similar nature and purpose). Last, but by no means least, social actions consist of enhancing the awareness of the public on the need for security and on their rights and obligations stemming from this need.

Even though there are numerous legal issues associated with e-commerce [22-23], the major ones are:

- The protection of privacy, an issue that has already been discussed previously.
- The protection of intellectual property rights. This entails the protection of copyrights for literary, musical, dramatic, and artistic works, as well as of sound recordings, films, broadcasts, and cable programs. It also entails the protection of trademarks, as domain names may be seen as a variation of such. Related to this is the problem of cybersquatting, i.e. the practice of registering domain names in order to sell them later at a higher price. Finally, protecting patents in e-commerce settings is also an issue. National legislation for the protection of intellectual property rights exists mostly everywhere [24]. At an international level, most prominent role is played by the World Intellectual Property Organization – WIPO, who is also administering a total of 23 relevant international treaties [25]. Similar is the situation with the protection of trademarks and patents.
- The protection of the right to free speech against the need to control offensive, illegal and potentially dangerous information. This includes the issue of controlling spam.
- The protection of both consumers and merchants against fraud. This entails the protection of all parties signing electronic contracts, protection against identity fraud, protection against computer crime, regulation of taxation, protection against money laundering etc.

Legislation exists for most of the above issues in a traditional commerce setting. However, it is not always straightforward to apply laws and regulations developed for such a setting in an e-commerce environment. Therefore, legal action in the direction of ensuring the applicability of existing and/or for developing new pertinent legislation is required.

From a conceptual point of view, the task of technically securing an information system can be broken down into securing its application and communication components. Applications are secured through the combined use of technologies including those for identification and authentication, identity management, access control and authorization, trusted operating systems, secure database systems, malware detection, data integrity preservation, intrusion detection and prevention, audit, and applied cryptology. On the other hand, communications are secured through the combined use of technologies including those for applied cryptology, firewalls, secure transactions, secure messaging, secure executable content, secure network management, network oriented intrusion detection and prevention, web access control, digital rights protection.

It can be seen, therefore, that all of the security requirements of e-commerce that we have identified can be addressed by a variety of technical measures, of differing strength and efficiency. Different measures can be and are used for different aspects of these requirements. However, the only measure that can adequately address all but one (the availability) of these requirements is encryption. This is why it deserves particular discussion in the current context.

The numbers of entities involved in e-commerce applications prohibits the use of symmetric encryption. Therefore, a more automated and consolidated approach is required, based on a Public Key Infrastructure (PKI) [26].

User requirements from a PKI have been recorded in several applications, and are, understandably, quite dissimilar. However, a common ground can be and has been found [27]. A comprehensive list of services that satisfy the above requirements can be found in [28]. The functions required to perform each of these services can subsequently be defined [28].

It appears, then, that we do know the way and we do have the technologies to solve most of the technical problems associated with securing e-commerce. If this was indeed the case, then all the real security breeches that we encounter everyday in e-commerce should not have been happening. What is, then, the problem?

The most usual problem is that, while everyone recognizes the need for securing e-commerce, what they do not know is that security is more than erecting physical and electronic barriers. The strongest encryption and most robust firewall are practically worthless without a set of organizational security measures, built around a security policy that articulates how these tools are to be used, managed and maintained. Such a policy concerns risks. It is high-level and technology neutral. Its purpose is to set directions and procedures, and to define penalties and countermeasures for non-compliance [29].

5. Conclusion

Even though there are useful laws focusing on several aspects of e-commerce trust, privacy and security, common agreements between the different countries are still missing. For the seller and the consumer engaged in digital business it should not make any difference, from a legal point of view, where the user, the e-business and any intermediary service is geographically located. Such an effort must start with a common agreement and understanding leading to an all-encompassing legal and moral protection of consumers' rights. In the past, legislators had to fight against specific violations as they appeared, resulting in a patchwork of various legal protections that only help to guard against isolated aspects of trust, privacy and security in digital business.

E-businesses should better support for third-party transaction services, trust infrastructure, privacy platforms and security solutions. Consumers should more carefully choose the services and products based on statements related to privacy and security and on the existence of certified characteristics, such as privacy or site authentication seals. This would increase acceptance of the seals and put some additional pressure on e-businesses to have their conformance with their published statements certified. However, privacy through organizational means does not actually enforce individual privacy. All approaches are only a help to guide decision-making about whom to trust. This is only a first step; technologies are needed that also attempt to enforce the preservation of privacy.

Current technologies make a significant achievement to preserving the trust, privacy and security in digital business. However, more research is needed to perform this automatically (without user involvement) and with less involvement of trusted third parties. Finally there is a need to develop technologies that better fit the general security requirements. In today's world strong anonymity is sometimes regarded as a potential risk to the security of the society or a country. Additional research is needed in order to understand how the two sets of conflicting requirements can be balanced and met under a single umbrella.

Overall, the issues of trust, privacy and security seem to be attractive to the research community at large, as demonstrated by the large number of contributions presenting recent developments in a number of specialized conferences (e.g. [30]-[31]).

References

1. Forrester Research. Post-web retail. Sept. 1999. http://forrester.com/.
2. US Census Bureau – http://www.census.gov/estats
3. B. Bhargava, L. Lilien, M. Winslett. Pervasive Trust. IEEE Intelligent Systems, pp. 74-77, September 2004.
4. Anil Kini, Joobin Choobineh: Trust in Electronic Commerce: Definition and Theoretical Considerations. HICSS (4) 1998: 51-61.
5. T. Grandison, M. Sloman. A Survey of Trust in Internet Applications. IEEE Communications Surveys & Tutorials, 2000.
6. ITU-T Recommendation X.509, "Information Technology - Open systems interconnection - The Directory: Authentication Framework", June 1997.
7. ITU-T Recommendation X.509, "Information Technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks", March 2000.
8. M. Blaze, J. Feigenbaum, J. Lacy. Decentralized Trust Management. IEEE Symposium on Security and Privacy, pp.164-173, 1996.

9. M. Blaze, J. Feigenbaum, J. Ioannidis, A. Keromytis. The KeyNote Trust-Management System Version 2. RFC 2704, 1999.

10. T. Dillon, E. Chang, F. Khadeer. Managing the Dynamic Nature of Trust. IEEE Intelligent Systems, pp. 79-82, September 2004.

11. R. Clarke. Internet Privacy Concerns Confirm the Case for Intervention. Comm. of the ACM. Vol. 42, No. 2, 1999.

12. W. Chung, J. Paynter. Privacy Issues on the Internet. Proc of the 35th Hawaii Int. Conf. on System Sciences. Jan. 2002.

13. M. Brown, R. Muchira. Investigating the relationship between Internet Privacy Concerns and Online Purchasing Behaviour. Journal of Electronic Commerce Research. Vol. 5, No. 1, 2004.

14. I. Araujo. Privacy Mechanisms supporting the building of trust in e-commerce. Proc. IEEE International Workshop on Privacy Data Management, Tokyo, Japan, April 2005.

15. M. K. Reiter, A. D. Rubin. Anonymous web transaction with Crowds. Comm. of the ACM. Vol. 42, No. 2, 1999.

16. D. L. Chaum. Untraceable electronic mail, return address, and digital pseudonyms. Comm. of the ACM. Vol. 24, No. 2, 1981.

17. J. Lopez, R. Oppliger, G. Pernul. Authentication and Authorization Infrastructures (AAIs): A Comparative Survey. Computers & Security Journal. Elsevier (North Holand), Vol. 23, 2004.

18. E. Kiountouzis: Approaches to the security of information systems. In S. Katsikas, D. Gritzalis and S. Gritzalis (Eds.): Information Systems Security, New Technologies Publications, Athens, Greece, 2004 (In Greek).

19. T. Winograd and F. Flores, *Understanding Computers and Cognition*, Addison-Wesley, 1997.

20. P. J. Denning, “Electronic Commerce”, in D. E. Denning & P. J. Denning (Eds), *Internet Besieged*, Addison-Wesley & ACM Press, 1998.

21. G. Pernul, A. Rohm and G. Herrmann, “Trust for Electronic Commerce Transactions”, in *Proceedings, ADBIS ’99*, Springer-Verlag, 1999.

22. R. Burnett. Legal aspects of e-commerce. Computing & Control Engineering Journal, 2001.

23. E. Turban. Electronic Commerce A Managerial Perspective. Prentice Hall. 2004.

24. http://www.wipo.int/clea/en/index.jsp

25. http://www.wipo.int/treaties/en

26. A. Arsenault and S. Turner, IETF PKIX WG, Internet draft, Internet X.509 Public Key Infrastructure PKIX Roadmap, March 10, 2000.

27. D. Lekkas, S.K. Katsikas, D.D. Spinellis, P. Gladychev and A. Patel, “User Requirements of Trusted Third Parties in Europe”, in Proceedings, User identification and Privacy Protection Joint IFIP WG 8.5 and WG 9.6 Working Conference, pp. 229-242, 1999.

28. S. Gritzalis, S.K.Katsikas, D. Lekkas, K. Moulinos, E. Polydorou, “Securing the electronic market: The KEYSTONE Public Key Infrastructure Architecture”, Computers and Security, Vol. 19, no. 8, pp. 731-746, 2000.

29. S.K. Katsikas and S.A. Gritzalis. A Best Practice Guide for Secure Electronic Commerce. Upgrade, Vol. III, no.6, December 2002. http://www.upgrade-cepis.org. Also in Novatica Journal of the Associacion de Tecnicos de Informatica, http://www.ati.es/novatica. Also in Tecnoteca Online of ALSI, http://www.tecnoteca.it.

30. Sokratis K. Katsikas, Javier Lopez, Günther Pernul (Eds.): Trust and Privacy in Digital Business, First International Conference, TrustBus 2004, Zaragoza, Spain, August 30 - September 1, 2004, Proceedings. Lecture Notes in Computer Science 3184 Springer 2004

31. Sokratis K. Katsikas, Javier Lopez, Günther Pernul (Eds.): Trust, Privacy and Security in Digital Business, Second International Conference, TrustBus 2005, Copenhagen, Denmark, August 2005, Proceedings. Lecture Notes in Computer Science 3592, Springer 2005