

The Role of Public Key Infrastructure in Electronic Commerce

Sokratis K. Katsikas
Dept. of Information & Communication Systems
University of the Aegean
Karlovassi GR-83200
Greece
ska@aegean.gr

Abstract

According to recent surveys, one of the most severe restraining factors for the proliferation of E-commerce is 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. Several aspects of these requirements can be secured by means of cryptography, in particular public key cryptography. This paper first considers security requirements for E-commerce applications, then discusses the workings of the Public Key Infrastructure and, finally, highlights its role in developing secure, hence trustworthy, E-commerce applications.

Introduction

The Internet is changing every aspect of our lives, but no area is undergoing as rapid and significant a change as the way businesses operate. Today, companies large, medium and small are using the Internet to communicate with their customers, suppliers and partners, to facilitate the communication among their employees and among their branches, to connect with their back-end data-systems, and to transact commerce, i.e. they do e-business. In this environment, where almost every organization is increasing its reliance on information and computer-processing facilities, e-commerce is bringing with it new dependencies and new risks.

An industry survey discovered that “organizations engaged in Web commerce, electronic supply chains, and enterprise resource planning experience three times the incidents of information loss and theft of trade secrets than everybody else” [1].

The Information Security Breaches Survey of the British Department of Trade and Industry [2] indicates that 60% of the organizations surveyed (a total of 1000) have suffered a security breach in the last 2 years.

Because most people think that “many houses may have caught fire this year, but mine never will”, statistics often do not have as much impact as specific cases. Here is a selection of such cases that can serve as illustrative examples:

In November 1996, an error in using an e-commerce product called SoftCard resulted in consumer credit card numbers collected for purchase orders being exposed to the Internet-at-large [3], [4]. A hacker rifled through online retailer CDUniverse’s files.

He then attempted to extort 100,000 USD from the company by threatening to publish the information. The company refused to pay the ransom and the hacker posted some 25,000 credit card numbers on a Web site on Christmas day, 1999 [5]. Hackers infiltrated the credit card database of health products supplier Global Health Tax Inc. The incident was attributed to sabotage and a former employee was suspect for intentionally placing the information on a non-secure part of the server [6]. The infamous German cracker group, Chaos Computer Club, demonstrated in February 1997 how money can be stolen electronically over the Internet [4], [7]. X.com, an online bank based in Palo Alto, California, allowed customers who were setting up new accounts to specify the account number from which funds were being transferred. Unfortunately, X.com did not verify whether the person who was setting up the account had the right to transfer those funds. This resulted in at least one fraud case, whereby a person bragged to an Internet newsgroup that he or she had transferred 25,000 USD from an account that has millions of dollars in funds and had withdrawn 4,500 USD in cash [8]. In January 1997, a program error in discount brokerage Charles Schwab's Telebroker system resulted in incorrect information conveyed to investors that queried account information over the phone [9]. In March 1997, AOL acknowledged that it posted inaccurate stock information about a particular company, Ezra Weinstein & Co. Whether this was a result of bad information supply or of tampering (deliberately or accidentally) with data is not known [10]. In February 2000, several major Web sites, including eBay, Amazon.com, Buy.com, Yahoo, CNN.com, E*Trade, Datek, ZDNet and, also, FBI, were attacked with a denial-of-service attack that brought the servers down for a duration ranging between 30 minutes and 3 hours [11]. In May 2000, the infamous LOVELETTER worm infected several thousands of Internet sites, bringing, again, servers down [12].

But what are the financial implications of such incidents? Well, the financial risks are all but negligible. In 1999 7.6 billion USD was lost in business productivity by Melissa, the Worm and other viruses. An international bank allows 12 million USD in unauthorized wire transfers due to insufficient EFT security. Six million online consumers have been victims of credit card-related fraud or unauthorized use on the Web [13]. Citizens and businesses in the European Union have lost anywhere from 6 billion to 60 billion EUROS over the Internet, much of it apparently because of fraud [4], [14]. Visa International says that half of all credit card disputes are about internet transactions. This is despite the fact that online transactions make up only 2% of Visa's overall business [15].

It is, therefore, evident that e-commerce is not enough. What businesses should be really looking into is how to engage in *secure* e-commerce. In this paper we will address some aspects of secure e-commerce, in particular those related to public key infrastructures. The paper first considers security requirements for E-commerce applications, then discusses the workings of the Public Key Infrastructure and, finally, highlights its role in developing secure, hence trustworthy, E-commerce applications.

Electronic Commerce

The term Electronic Commerce (or, more commonly "e-commerce") has taken on several different meanings in the past decade. Originally, before the advent of the Internet and its proliferation to the commercial world, e-commerce was almost synonymous to Electronic Data Interchange (EDI). Gradually, with the increasing use

of the Internet in business applications, the meaning of the term shifted, so that today e-commerce is almost synonymous to doing business over the Internet. This probably justifies the practice of using the term “e-business” interchangeably with the term “e-commerce”. However, legacy EDI technologies and applications over proprietary networks – commonly called Value Added Networks (VANs)- have cost so much to both vendors and customers that both are understandably reluctant to accept today’s reality. Therefore, in order to both allow for flexibility and to accommodate such legacies, we can think of e-commerce as an umbrella term that describes automated business-related transactions [16]. This umbrella is quite large; a tremendous variety of transactions fit underneath. Moreover, the range of technologies, processes and practices that are represented within these diverse transactions is enormous, ranging from the Internet, through the WWW, to the use of mobile phones for what has been termed the Mobile Electronic Transactions (MeT), a joint initiative of NOKIA, ERICSSON and MOTOROLA [17]. Finally, e-commerce applies equally well to the private and public sectors.

E-commerce can be divided into two main areas:

- ?? Business-to-business transactions (or horizontal market)
- ?? Consumer-to-business transactions (or vertical market)

Historically, the horizontal market in e-commerce appeared first. Banks were pioneers in this development, having realised very early the advantages of automated transfer of funds and having the financial means to face the –initially very high- costs associated with achieving this kind of automation. Large businesses, mostly international, followed. This was due to a variety of reasons, most prevalent among them being the need of such businesses to cut down on communication costs with their customers and suppliers and to facilitate the ordering, negotiations, pricing, invoicing and payment processes in terms of both speed and integrity. The number of parties involved in business-to-business transactions is relatively small, being, for each business, the number of suppliers and customers (excluding retail customers). Moreover, they are all known to the business and many may even be its own employees, as e-commerce spans both inter- and intra- business transactions. Thus, the technological means allowing businesses to engage in this form of e-commerce were made available early enough, in the form of closed, proprietary, one-of-a-kind, private networks and accordingly designed EDI applications.

Examples of such transactions are the buying and selling of goods between businesses, the negotiation, conclusion and signing of business contracts, the communication of data among businesses or between branches of the same business, etc. The latter example may also include, from a technical perspective, the communication of data between government agencies.

The vertical market, which is certainly more visible than its horizontal counterpart, flourished only after the Internet transformed from the limited academic and research network that used to be to the vast information superhighway that we know today and the WWW became the dominant application. The immense costs associated with the establishment of private networks and the pertinent information systems were brought down to virtually zero, enabling not only medium-size, but also small enterprises to

enter the arena of e-commerce, not only for business-to-business transactions but for retailing as well.

Examples of transactions in the vertical market are the buying of goods over the WWW, the banking over the WWW (often called e-banking), the submission of forms for governmental usage (e.g. tax return or VAT forms), the advertisement over the Internet, the electronic investing – which is not only limited to the purchasing and selling of stocks over the WWW but extends to employing intelligent software agents for selecting investment opportunities [4], etc.

E-commerce, in both its facets, is today a fact of everyday life. What is more important, it is beginning to dominate everyday life. Indeed, the annual financial volume of e-commerce transactions within the European Union alone is currently in the order of 17 billion EURO and is expected to reach 340 billion EURO in the year 2003 [18]. High as it may seem, this number is very low compared to the corresponding volume in the US, which, with an economy of comparable size, shows a volume of electronic business transactions three times as high.

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. The model is built upon the observation that the most elemental building block of commerce is the *exchange transaction*. 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:

1. **Request.** A makes a request of B to provide the service. (Often this amounts to taking B up on an offer B has made).
2. **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).
3. **Performance.** B carries out the actions needed to fulfill his part of the bargain and notifies A when done.
4. **Settlement.** A accepts B's work, declares it satisfactory, and pays.

The last two phases can be –and usually are- combined into one composite phase, called the **Execution** phase [21]. The model is good for any kind of transaction, not only electronic transactions. For a transaction to qualify as electronic, at least one of the above phases must be supported by information and communication technologies.

E-commerce has certainly a lot to give to businesses. Its advantages are generally acceptable and success stories around e-businesses can be found almost everyday in newspapers. However, major corporations have been rather slow in engaging in this form of transaction, doing so with caution. They claim that the most prevalent reason for doing so is their concerns over the security of the electronic transactions [22]. Is

this justified? Well, let us take a closer look at security requirements of e-commerce in terms of our generic transaction model.

During the Request phase, the transaction parties have different security requirements. On one hand, 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. Note that some goods are also naturally intangible, therefore they can be delivered to the buyer electronically (e.g. digitally represented shares). This of course presents some quite interesting security requirements. 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.

To sum up this discussion, we can compactly state that 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.

The Public Key Infrastructure (PKI)

All of the security requirements of e-commerce that we identified in the last paragraph 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. Indeed, cryptography can be used for ensuring the confidentiality of information, whereas certificates can ensure the authenticity of the communicating parties, and electronic (usually digital) signatures can ensure the integrity of information, and the non-repudiation of transactions.

In symmetric (shared key) cryptography, both communicating parties share the same key, which they use for both encryption and decryption. As in an open environment it is difficult (if at all possible) to have an indefinite number of parties agree upon and share a secret key, the inevitable option for use in e-commerce applications is asymmetric, alias public key cryptography. In this kind of cryptography, a pair of keys is used instead: a public key, which is widely available and a different, private key, which is only known to the entity that owns the pair.

Using public key cryptography, an entity (person, service or application) may encrypt information, prior to transmitting it to another entity, with the receiving entity's public key. The message can then be decrypted only by the receiving entity owning the corresponding private key, thus ensuring confidentiality of the transmitted

information. Alternatively, or even complementarily, an entity may ensure the integrity of information by digitally signing it, i.e. by using its private key to encrypt some function of the information (commonly referred to as the *digest*) which must enjoy some properties with respect to the original information. Any entity can, in the sequel, decrypt the encrypted digest using the originator's public key, and retrieve the digest. If and only if this matches the individually (by the receiving entity) computed digest, the information has not been tampered with. Thus, the integrity of information can be maintained. The digital signature can also, clearly, be used to uniquely identify the sender of the information, thus ensuring the non-repudiation of the origin of a transaction. In order to fully provide for the non-repudiation of transactions, i.e. in order to provide for non-repudiation of receipt as well, one must employ additional measures. Finally, *public key certificates* (PKCs), i.e. digital documents that bind public keys to entities, are used for ensuring authenticity of the communicating parties.

It is, therefore, evident that public key cryptography can address most security requirements of e-commerce applications. However, consider again our primary reason for rejecting the use of symmetric cryptography in e-commerce: the numbers of entities involved. It is clear that it is impossible to maintain and manage keys and certificates for large numbers of users using small-scale, inter-organization tools, even if these are fully automated. In this case, a more automated and consolidated approach is required, based on a Public Key Infrastructure. What is, then, a PKI?

A PKI consists of five types of components [23]:

- ?? Certification Authorities (CAs) that issue and revoke PKCs;
- ?? Organizational Registration Authorities (ORAs) that vouch for the binding between public keys and certificate holder identities and other attributes;
- ?? Certificate holders that are issued certificates and can sign digital documents and encrypt documents;
- ?? Clients that validate digital signatures and their certification paths from a known public key of a trusted CA;
- ?? Repositories that store and make available certificates and Certificate Revocation Lists (CRLs).

Additionally, a Time Stamping Authority (TSA) may be thought of as part of the PKI. Entities that collectively operate as CAs, RAs, Repositories and TSAs have been commonly referred to as Trusted Third Parties (TTPs) or, more recently, as Certification Service Providers (CSPs).

Most attempts to define a set of services that a PKI should be offering have not been user-needs-oriented [24]. User requirements from a PKI have been recorded in several references [25]-[33]. Each one of these works recorded user requirements for their own application domain. However, a common ground can be and has been found [34-35]. This "minimal set" of user requirements includes authentication of users, integrity of messages, privacy and confidentiality of messages, non-repudiation of message origin and destination, availability of services, ease of use. In addition to this minimal set, issues like anonymity of participants, time stamping, uniqueness of documents, interoperability between different elements, protection from abuse of any participant by another, legal issues have been identified as important.

A comprehensive list of PKI services that satisfy the above requirements follows [36-37]; this list includes all services specified in [23]. The functions required to perform each of these services can subsequently be defined.

The specified PKI services are as follows:

1. *Registration.* In order for a user to join the PKI environments s/he must register with a RA belonging to the PKI. The primary goal of this service is to establish the reliable unique binding between a user and her/his public key. Functions supporting this service include: Initial request submission, Registration form's format validity checks on behalf of the RA, end entity authentication and identification, and anonymity assurance.
2. *Digital Signatures.* In order to satisfy the message authentication, message integrity and non-repudiation of origin user requirements, the PKI should offer digital signature services. Functions supporting this service include message hash generation and message hash encryption/decryption.
3. *Encryption.* Encryption is a basic service providing the cryptographic functions for protection of message confidentiality in a computer network. Functions supporting this service include encryption and decryption of the message.
4. *Time stamping.* Time stamping is described as the process of attaching data and time to a document in order to prove that it existed at a particular moment of time. Functions supporting this service include acceptance of a request for a time-stamp, retrieval of the time/date data for the time-stamp, appendage of time-stamps to a message and submission to the requesting entity, verification of the validity of the time-stamp certificate, selection and distribution to the public of the set of hash functions for producing message digests, selection of a digital signature scheme for signing time-stamp certificates, maintenance of a database of time-stamp certificates, generation and delivery of error messages to the requesting entity, maintenance of a log of time-stamping authority (TSA) activity, having the TSA log time-stamped, provision of secure communication channels, maintenance of procedural security controls, distribution of information to the public.
5. *Non-repudiation.* Non-repudiation involves the generation, accumulation, retrieval, and interpretation of evidence that a particular party processed a particular data item. The evidence must be capable of convincing an independent third party, potentially at a much later time, as to the validity of a claim. Functions supporting this service include initialization, revocation and dispute resolution and notary.
6. *Key Management.* Key management is a principal service within a PKI architecture. This service deals primarily with the handling of cryptographic keys in a proper, efficient, scalable and secure way. It includes key generation, random number generation, key personalization, distribution of keys, key storage, key retrieval, key recovery, backup and restore, key update, key compromise related functions, validation of requests for key accessing functions, determination of the rights of the personnel on key management functions.
7. *Certificate Management.* A digital certificate is an electronic token ensuring the binding between an entity and its public key. The functions supporting this service include generation, distribution, storage, retrieval, and revocation of digital certificates.
8. *Information Repository.* This service maintains the collection of data critical for the operation of the PKI system. It states the general means and fashion for storing,

archiving and maintaining several types of data ranging from organization's legal requirements, to system recovery needs. The functions supporting this service include determination of the items to be archived, determination of the retention period, authorization, authentication, update of the archive, retrieval of information, retrieval of authorization and consignment details of archived documents, distribution of information, deletion.

9. *Directory Services.* In order to interact, a member of a PKI must have access to information about other PKI members. This is achieved by the use of Directory Services which are supported by the following functions: update with new certificates, update with revoked certificates, distribution, replication, caching, searching, retrieval (for certification purposes), retrieval (for cross-certification purposes), returning of information.
10. *Camouflaging communications.* Camouflaging communications not only provides data confidentiality, but also hides the very fact of communication. This is achieved by adding dummy messages into the data stream enabling CSPs and users to hide real data transfers, both in terms of their occurrence and frequency. Functions supporting this service are responsible for camouflaging on-line as well off-line communications.
11. *Authorization.* The PKI should enable requesting entities to delegate access rights at will to other PKI entities. This means that a PKI user who possesses a resource may grant the right to another PKI user to access this resource. CSPs should ensure the granting of rights, including the ability to access specific information or resources. Supporting functions include authentication, group definition, rights update, group update, enrolment of a user into a group, resolving of rights, determining administrative authorities.
12. *Audit.* In order to ensure that certain operational, procedural, legal, qualitative and several other requirements are complied with, so that trust is enhanced, an auditing service is required. The functions supporting this service fall into two categories: Initial preparatory phase functions and Main operation of the audit plan phase functions.
13. *Quality assurance and trust enhancement services.* It is expected that the potential users of PKI services would require products and services of a given quality to be delivered or be available by a given time and to be priced so that best value for money is achieved. In order to achieve this level of quality, PKI services must be quality assured. Functions supporting this service include organization operations manual specification, organization operations maintenance and improvement.
14. *Customer oriented services.* This group of PKI services includes services which directly involve users or that require some contact, or some kind of dealing or bargaining with the end user. Examples of such services are legal aspects and payment negotiations between a user and a CSP. This group of services is implemented by the following functions: Liability and insurability, underwriting, accounting management, ordinary operations assistance and support provision.
15. *CSP to CSP interoperability.* It is unlikely that in a large scale PKI all users will be connected to a unique CSP. Interoperability services are concerned with the issues necessary for establishing a network of CSPs, possibly operating by different companies with different policies and different domain specialization. Functions supporting this service include: accepting a request, validating a request, return of the validation result, finding the certification path, validation of the certification path, sending cross-certification requests, accepting the certification

result, retrieval of information from other domains, response to other domains' requests, translation, other operational functions.

Detailed descriptions for all the aforementioned functions can be found in [35].

Both governments and industry have realized the importance of the PKI in developing the e-commerce. This is the reason why both national and international legislation dealing with the subject has appeared in the past few years. The European Union has issued a directive [38], dealing with the legal issue of electronic signatures. Several EU Member States have already proceeded to take legislative measures on the same issue. In the standardization arena, the IETF has come up with important work on PKI [23], whereas Europe has formed the European Electronic Signature Standardization Initiative [39] as a joint effort between the European Telecommunications Standards Institute (ETSI) and the European Standardization Committee (CEN). These efforts aim at ensuring the provision of service 15 above, namely to ensure interoperability between different CSPs.

Provided that some business has by now been convinced that PKI is the solution to its security concerns regarding e-commerce, how would it go about deploying it? According to [40], five important questions need to be considered in deploying a PKI:

- ?? **What is the organization's PKI strategy?** PKI strategy typically focuses either on enabling a specific application or on consolidating PKI functions for multiple operations.
- ?? **How will interoperability be achieved?** There are two basic approaches to achieving this end: Focus on a particular vendor's products; or focus on standards.
- ?? **Are applications PKI-ready?** In most cases, businesses have two options: Encourage software vendors to PKI-enable their applications; or use in-house programming staff or contract programmers to PKI-enable applications.
- ?? **How many clients will be involved in the initial deployment?** Vendors may imply that deployment of thousands of PKI clients is a reasonable first step. In reality, most businesses pilot with no more than a few hundred – and often less than a hundred- clients.
- ?? **What are the technical staff requirements for deployment planning and for deployment?** Less than half the cost of deploying a PKI is attributable to acquiring and installing hardware and software. The remaining costs are mostly associated with securing the technical personnel that is qualified to plan and develop the PKI. As this is a one-time task, it is preferable to outsource it to experience consultants rather than hiring and laying off highly skilled personnel, which is anyway scarce.

It appears, then, that PKI is the solution to the problem of securing e-commerce. With the exception of the requirement for availability, (which can, by the way, indirectly be addressed by the increased authentication capabilities that a PKI offers) all other requirements have been fully met. If this was indeed the case, then the real incidents presented in the introduction should not have happened. 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 security policy that articulates how these tools are to be used. 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 [22]. It is sad that only one in seven organizations in the UK have a formal information management security policy in place [2].

Conclusion

E-commerce is now a reality. Businesses must start considering how to plan and deploy secure e-commerce applications, so that they retain their competitive advantages over their competitors or gain new ones. PKI is one of the major items in the arsenal of security measures that can be brought to bear against the increasing risks and threats on doing business electronically. However, this should not detain either businesses or consumers; what is needed is a careful examination of the risks involved in the process, a comprehensive plan for managing them and the acceptance or mitigation of the remaining ones.

References

1. G. Dalton, "Acceptable Risks", *Information Week*, August 31, 1998.
2. DTI, *Information Security Breaches Survey 2000*, http://www.dti.gov.uk/cii/dtiblue/dti_site/new_pages/
3. Edupage Editors, "Revealing Software Glitch Bares Credit Card Info on the Web", *RISKS Digest*, 18:61, November 15, 1996.
4. A. Ghosh, *E-commerce Security*, John Wiley & Sons, 1998.
5. R. Conlin, "CyberCash Denies Fault in Security Breach Case", *E-Commerce Times*, January 11, 2000.
6. P. Greenberg, "Online Credit Card Security Takes Another Hit", *E-Commerce Times*, January 20, 2000.
7. K. Brunnstein, "Hostile Active-X Control Demonstrated", *RISKS Digest*, 18:82, February 14, 1997.
8. P. Greenberg and S. Caswell, "Online Banking Fraud Raises More Security Concerns", *E-Commerce Times*, February 1, 2000.
9. N. de Carteret, "Computer Glitch Gives Investors Instant Loss of Balance at Schwab", *RISKS Digest*, January 28, 1997.
10. Edupage Editors, "AOL Says It Got Incorrect Stock Info From S&P", *RISKS Digest*, 18:90, March 14, 1997.
11. G. Sandoval and T. Wolverton, "Leading Web Sites Under Attack", *CNET News.com*, February 9, 2000.
12. CERT, *CERT Advisory CA-2000-04 Love Letter Worm*, May 4, 2000.
13. *Information Security Magazine*, July 1999.
14. Edupage Editors, "EC Study Cites Fraud on the Internet", *RISKS Digest*, 18:35, August 19, 1996.
15. BBC Money Programme on Internet fraud, BBC 2, 21 November 1999 GMT 20:30.
16. W. Ford and M. Baum, *Secure Electronic Commerce*, Prentice Hall, 1997.
17. A. Saapunki, "Implementing Electronic Signatures: Views on Future", EESSI Open Seminar on Electronic Signature Standardization: The National Dimension, Paris, AFNOR, 11-12 May 2000.

18. European Commission, "Europe: Information Society for All", Announcement regarding a Commission initiative for the European Summit in Lisbon, 23-24 March 2000.
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. Andersen Consulting & CERIAS-Purdue University, Policy Framework for Interpreting Risk in eCommerce Security, 1999.
23. A. Arsenaault and S. Turner, IETF PKIX WG, Internet draft, *Internet X.509 Public Key Infrastructure PKIX Roadmap*, March 10, 2000.
24. A. van Rensburg and S. von Solms, "A reference framework for Certification Authorities / Trusted Third Parties", in *L. Yngstrom and J. Carlsen (Eds.), Proceedings, IFIP 13th International Information Security Conference*, Chapman & Hall, 1996.
25. Trusted Health Information Systems (THIS) project, *Final report: Requirements on electronic signature services and TTP services*, Swedish Institute for Health Services Development, 1995.
26. TrustHealth-ETS project, *Functional specification of TTP services*, Swedish Institute for Health Services Development, 1995.
27. TTP & Electronic Signature Trial for Inter-Modal Transport (TESTFIT) project, Final report, CEC/DGXIII/B6, 1995
28. BOLERO project, *Final Report*, CEC/DGXIII/B6, 1995.
29. Ebridge project, *Final Report*, CEC/DGXIII/B6, 1995.
30. EAGLE project, *Software description and functional specification of the TTP demonstrator*, Deliverable 3, CEC/DGXIII/B6, 1997.
31. S2101 Project, User requirements for TTP services, CEC/DGXIII/B6, 1993.
32. EUROMED-ETS project, *Final Report*, CEC/DGXIII/B6, 1998.
33. A. Nilson, *European Trusted Services (ETS) - Results of 1995 TTPs Projects. Final Report*, Marinade Ltd., 1997
34. *KEYSTONE* project, *KEYSTONE deliverable 1.1: User Requirements Statement*, 1998.
35. *KEYSTONE* project, *KEYSTONE deliverable 9.1: Final project report*, 1998.
36. S. Gritzalis, S. K. Katsikas, D. Lekkas, K. Moulinos and E. Polydorou, "Securing the electronic market: The *KEYSTONE* Public Key Infrastructure Architecture", submitted for publication.
37. D. Lekkas, S.K. Katsikas, D.D. Spinellis, P. Gladychiev 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*, Stockholm University, 1999.
38. European Union, Directive 1999/93/EC on a Community framework for electronic signatures, Official Journal of the European Communities, L13/12, 19 January 2000.
39. <http://www.ict.etsi.org/eessi/eessi-homepage.htm>
40. RSA Security Inc., *Understanding PKI Infrastructure*, 2000.