Trust, Privacy and Security in Digital Business

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

[1]Dept. of Information & Communication Systems Engineering, Univ. 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. According to recent surveys, one of the most severe restraining factors for the proliferation of e-commerce, as measured by the gap between predicted market value and actual development 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. A large number of individuals are not willing to engage in e-commerce (or are only participating at a reduced level) simply because they do not trust the e-commerce sites and the underlying information and communication technologies to be secure enough. This paper first considers privacy and security requirements for e-commerce applications; it then discusses methods and technologies that can be used to fulfil these requirements.

1. Introduction

Diffusion, general availability, and potential benefits of information and communication technologies are rapidly changing our society, economy, and the way we do business. They have an important impact on almost any sector in industry, politics and even on our daily life. Companies are constantly interacting electronically with each other and with their customers; consumers routinely use computer networks to identify sellers, to evaluate products and services, to compare prices, and to exert market leverage. However, 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 backed by many studies is simply the lack of *trust, privacy and security in digital business*. A large number of individuals are not willing to engage in e-commerce (or are only participating at a reduced level) simply because they do not trust the e-commerce sites and the underlying information and communication technologies to be secure enough.

The figures above refer to business-to-consumer transactions only and it is expected that the situation for business-to-business, business-to-government, and government-to-business transactions is slightly better but still far away from being optimal. Today the type of e-business activity making the most impact on the economy is business-to-business. In certain industries, for example automotive and mining industries, digital business has already far-reaching effects on the relationship between supplier and manufacturers. This is due to the fact that communication is often done by means of dedicated communication lines (closed and private virtual networks) and trust has developed because the business relationships are longer lasting and do already exist from earlier business in the physical world. However, even there the full potential of digital business has not yet reached. This is even more, if one considers new and unknown suppliers and small and medium enterprises in which access to the dedicated communication lines is not provided.

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.

2. Trust

During centuries, persons have carried out business transactions based on a face-to-face situation (or face-to-face commerce scenario). Regardless of the problems and difficulties associated with these different situations, the result of this type of commerce procedures has been reasonably successful. Probably, much of the success of those procedures has been based on the intrinsic trust derived from the face-to-face interactions between persons, a concept that obviously has strong sociological and psychological components.

According to the Webster dictionary, trust can be defined as: (i) An assumed reliance on some person or thing. A confident dependence on the character, ability, strength, or truth of someone or something; (ii) A charge or duty imposed in faith or confidence or as a condition of a relationship; (iii) To place confidence (in an entity).

As stated, 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 as trivial as we may have perceived in the previous paragraph. 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. For instance, consumers need to trust that merchants will not disclose their private information, while merchants need to trust that the customer has the money to pay what s/he is purchasing.

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 consideration 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

We believe that 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 (a belief, as previous authors mention) resulting of a combination of the appropriate use of basic services. In any case, we agree with the authors on the difficulty and on the lack of consensus on defining the term.

Additionally, we also agree on the importance that the authors give 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 raised 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 to be used 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 mean 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 the trust from users. 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.

One of the advantages of an attribute certificate is that it can be used for various purposes. It may contain group membership, role, clearance, or any other form of authorization. Yet another essential feature is that the attribute certificate provides the means to transport authorization information to decentralized applications. This is especially relevant because through attribute certificates, authorization information becomes "mobile", which is highly convenient for digital business applications.

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 in [8] the notion of trust management. In that original work they proposed the PolicyMaker scheme as a solution for trust management purposes. PolicyMaker is a general and powerful solution that allows the use of any programming language to encode the nature of the authority being granted as well as the entities to whom it is being granted.

KeyNote was proposed [9] to improve two main aspects of PolicyMaker: to achieve standardization and to facilitate its integration into applications. Additionally, Keynote uses a specific assertion language that is flexible enough to handle the security policies of different 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 some authors consider 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 change due to the following factors: “(i) After further dealings, the trusting entity has a better idea of the trusted entity’s capability and willingness to act the way the trusting entity wants in a given context; (ii) The trusted entity’s capability or willingness to act in a given context the way the trusting entity desires might change with time; (iii) The trusting entity, after getting recommendations from other entities, will know more about the trusted entity’s capability and willingness to act the way that the trusting entity wants in a given context.” 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”.

2.4. Challenges

As shown, even the most basic issues of trust can be still considered as open issues to be solved. However, this is only the tip of the iceberg. A group of experts identified, during the NSF Workshop on Information and Data Management, the following challenges:

a) *How to initiate and build trust?*

   How to create formal models of trust, addressing the issues of different types of trust (e.g., trust towards data, or users, or system components)? How to define trust metrics to compare different trust models? How should trust models accommodate trust characteristics (such as context dependency, bi-directionality, and asymmetry)? How should the models of trust handle both direct evidence and second-hand recommendations related to the trusted subjects or objects? How trusted parties can be used to initiate and build trust? How timeliness, precision, and accuracy affect the process of trust building?

b) *How to maintain and evaluate trust?*

   How to collect and maintain trust data (e.g., credentials, evidence on the behavior of the trusted objects, recommendations)? How and when to evaluate trust data? How to discover betrayal of trust, and how to enforce accountability for damaging *trust? How to prevent trust abuse, for example by means of access right revocation? How to motivate users to be good citizens and to contribute to trust maintenance?*

c) *How to deal with fraud?*

How to create formal models of fraud? How to define metrics to compare different fraud models? How to design efficient methods and tools for fraud prevention and detection? How to prevent, detect, and trace fraud? When to tolerate fraud? How to use trust assessment, threat avoidance and threat tolerance to prevent fraud?

d) *How to guarantee scalability, performance, and economic parameters for trust solutions?*

How to scale up trust models and solutions? What is the impact of trust solutions on system performance and economics? How and what economic incentives and penalties can be used?

e) *How to engineer trust-based applications and systems?*

How to experiment with and implement trust-based applications and systems for egovernment, e-commerce, and other applications? How to enhance system performance, security, economics, etc. with trust-based ideas (e.g., like enhancing role-based access control with trust-based mappings)? How to use incentives and penalties for building trust and preventing fraud?

Additionally, they have recommended the support of research in the following areas: (a) Social paradigm of trust (b) Liability of trust. (c) Scalable and adaptable trust infrastructure. (d) Benchmarks, test beds, and development of trust-based applications. (e) Fraud prevention and detection (f) Trust-related interdisciplinary research.

It is clear at this point that there is plenty of research work to be done in the next years in the trust area.

3. Privacy

Privacy is an interdisciplinary issue. The right of humans for keeping their privacy is debated in many fields, including the areas of law, politics, philosophy, sociology, and more recently computer sciences. 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. Customers typically have only little idea about the possible range of uses that the possession of personal information allows for, and thus have only little idea about the possible violations that might occur to their privacy. 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.

3.1 Consumers' Concerns

In the digital age distances have been shortened. Before, when a consumer acquired a good or a service customer and supplier usually knew each other from direct contact. Often, they were located in the same geographical area or country. This is no longer the case. Consumers and suppliers are now able to do business with almost anyone else in the world. The new situation is characterized by certain properties which are responsible for most of consumers' concerns regarding trust and privacy. Examples of properties are indirect contact and the lack of close interaction between all parties involved in the execution of a business transaction, usually a time delay between the buying, delivering and paying processes, easy and inexpensive collection of information which may happen without notice of the consumer at different sites and at different stages of the business transaction, and often an absence of effective regulations or if there are regulations applicable one suffers from their ineffective enforcement. The latter is in particular true if different countries are involved and different law may apply. In the literature several consumers' concerns to privacy are discussed (for example see [11] - [14]). The following are some of the most important examples:

- *Data gathering*: Once a consumer submits personal data there is usually no control how the data may be used. Personal information may be used for not authorized purposes, like marketing, data mining, or may even be sold to other companies.
- *Cookies*: Cookies may be used for legitimate purposes, like security, customer service, or session tracking. Alternatively, they may also be used for storing customer behaviour on their own computers which later may be tracked and matched with the customer database. As a result shoppers may be charged with higher prices simply because a large likelihood that they will even buy at high costs can be concluded from their profiles.
- *Lack of regulations*: Privacy laws are different in different countries. Additionally there is no means and effective way to verify that the law is observed.
- *Privacy statements*: Privacy statements may not be up-to-date, incorrect or may not even be applied at all.
- *E-mailing*: Unwanted Emails (for example spam mails) may be sent to consumers offering services or products.

- *Site spoofing*: Customers may be linked to other sides where they receive wrong information. Or they may be linked to external sites where the published privacy policy does no longer apply.

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. In the following we will give representative examples of such initiatives.

In the UK and Sweden there is a legal restriction on any entity possessing any kind of personal information without the explicit consent of the data owner, and every entity that does store such data has to register this fact with the government. Similar is the situation in Germany. The German privacy law additionally demands the principles of data minimalism and purpose limitation, meaning that only the minimum of data to perform a certain purpose may be collected and that the data may not be used for any other than the specified purpose. The European Union Data Protection Directive from 1998 aims at harmonization of laws throughout the EU and declares privacy as a fundamental human right.

In Japan the Personal Data Protection Act of 2003 regulates the commercial and governmental usage of private data. This act extends an earlier act from 1988 which regulates the storage and use of private data through governmental administration. Additionally the Ministry of International Trade and Industry has published guidelines for businesses how to handle private data and issues a seal for those businesses adhering to the guidelines. Even in China several relevant laws for data protection exist.

Canada has a very strong privacy law. The Personal Information and Electronic Documents Act (since 2004) determines for businesses how they are allowed to collect, use and disclose private information of their customers as well as their employees. In the US there is no dedicated privacy regulation; however, several different laws focus on different privacy related areas.

Besides the national laws the Organization of Economic Development issued a set of guidelines (the OECD Guidelines on Privacy and Transborder Dataflows of Personal Data, 1980) which sets out the minimum standards for data collection, storage, processing, and dissemination that both the public and private sectors should adhere to. These guidelines are commonly consulted by nations and businesses when drafting privacy laws and policies.

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 the 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. Data collected during a business transaction referring to the kind of service or the type of product purchased is non-personally identifiable as long as it is not combined with personally identifiable information, like name, birth date, address, credit card or banking information. Non-personally identifiable information may be analyzed in any way possible and privacy protection is only applicable to personally identifiable data. It goes without saying that 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. The service could hide the identity of the recipient to the merchant and only pay the merchant after successful receipt of the ordered goods. Other organizational means to increase trust and privacy are delivering some sort of believes to the consumer that a merchant is compliant to 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), giving customers the possibility 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. Although there is some monitoring involved in the before mentioned privacy sign we once again have reached a point where the users have to simply trust the e-business to keep their promises.

Privacy through technology

In order to achieve some level of consumer privacy, privacy enhancing technologies (PET) may be used. These technologies attempt to achieve anonymity by providing unlinkability between an individual and any of their personal data, i.e. they try to ensure that any information collected cannot link back to an individual’s real world identity. Several levels of anonymity have been defined in the literature, ranging from full anonymity (no one can find out who you really are) via 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 one of three main methods: anonymising the transport medium, allowing anonymous access, 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, such as IP addresses. However, this approach is practically not very feasible because many of the free email service providers require personal details to sign up, have the legal requirement to keep communication details at least for a short period of time and for business transactions involving certain monetary value those Email addresses are often blocked by the shop owners. In order to achieve anonymous web browsing 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. However, this technique makes it necessary that the anonymising party is acting as a trusted third-party and that the user can rely on not being disclosed by it.

A further step in technical complexity is a setting without a trusted third-party. Reiter and Rubin created a system, called Crowds [15] that 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 class of privacy enhancing technologies uses encryption. A well known and prominent technology which is using public key cryptography is Chaum Mixes [16]. All messages must be of equal size; they will be cryptographically changed and finally delivered to the recipients in different order. This makes it very difficult to link an incoming message and its sender to an outgoing request and to perform traffic analysis. Chaum Mixes were extended in several ways. For example, onion routing protocols 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. Each point in the communication chain can only decrypt its layer, finding out only where the next point in the route is. For onion routing there are commercial implementations available on the net providing users with anonymity.

Besides anonymising the transport medium another privacy enhancing technique is allowing anonymous access to a service. In such systems 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. Usually credentials are issued by certification authorities and a user can then prove possession of a credential to an organization without revealing his identity. One weakness of such a system is that the legitimate user may transfer credentials on to other users. While this is no risk to privacy it is often not intended by businesses or law. Such a risk may only be limited by linking the certificate to the users' private key and thereby to his identity.

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. What this means for digital business is that these technologies enable customers to buy items from an e-business by hiding their identity but proving certain facts, for example belonging to a role or group of users in possession of certain authorizations, having access to a certain bank account or having already paid in advance. 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 different approach to privacy is the use of statistical databases. 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. Examples of such techniques are query size restriction (Only queries that retrain privacy are allowed.), data perturbation (Individual data is changed in a way that does not influence the statistics but makes the individual data useless.), or output restriction (Query results are altered in the case privacy is threatened). 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.

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. 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 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.

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 the nature of some goods is also intangible; therefore, these 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.

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 (www.wipo.org) 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 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. 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, as 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. Therefore, a more automated and consolidated approach is required, based on a PKI that consists of five types of components [26]: (i) *Certification Authorities* (CAs) that issue and revoke certificates, (ii) *Organizational Registration Authorities* (ORAs) that vouch for the binding between public keys and certificate holder identities and other attributes, (iii) Certificate holders that are issued certificates and can sign digital documents and encrypt documents, (iv) Clients that validate digital signatures and their certification paths from a known public key of a trusted CA, (v) 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 CA's, RA's, Repositories and TSA's have been commonly referred to as *Trusted Third Parties* (TTPs), or as *Certification Service Providers* (CSPs).

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 appear – 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. Policies should clearly state in what countries the e-business is located and what laws do apply. They also should have a validity date and in case of changes should give the history of changes. 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.

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