International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:2, No:9, 2008

Considerations of Public Key Infrastructure (PKI), Functioning as a Chain of Trust in Electronic Payments Systems

Theodosios Tsiakis, George Stephanides, and George Pekos

***Abstract*—** The growth of open networks created the interest to commercialise it. The establishment of an electronic business mechanism must be accompanied by a digital – electronic payment system to transfer the value of transactions. Financial organizations are requested to offer a secure e-payment synthesis with equivalent level of security served in conventional paper-based payment transactions. PKI, which is functioning as a chain of trust in security architecture, can enable security services of cryptography to e-payments, in order to take advantage of the wider base either of customer or of trading partners and the reduction of cost transaction achieved by the use of Internet channels. The paper addresses the possibilities and the implementation suggestions of PKI in relevance to electronic payments by suggesting a framework that should be followed.

***Keywords*—**Electronic Payment, Security, Trust

I. Introduction

COMMERCE partners (customers, merchants and financial organizations) are no longer interacting by direct physical experience. Instead their experience is mediated through multidimensional interactive environments. Consequently, it is an uppermost issue for the transaction process of exchange of information over open heterogeneous environments (as the Internet) to create trust. The formal procurator, the World Wide Web can be thought as an untrusted environment with no trust affiliations. In contradistinction, a desired trusted environment is the one that the entities constitute it, are unique, unquestionably identifiable and ruled by a set of priorities and conditions.

Trust has a vital influence on consumer activities and thereby on e-commerce success. To address the role of trust in e-commerce, we need to answer a number of questions such as [1]:

- What factors influence the level of trust in the Internet?
- How does trust influence participation in e-commerce?

Internet and particular the services of WWW must constitute an image of life that reflects both human knowledge and human relationships.

Manuscript received May 5, 2005.
Email: {tsiakis, steph, pekos}@uom.gr

II. Identification of E-Commerce Security Skepticism

Before we give a possible approximation that can be thought as definition of security is imperative to allocate the components of a security system. We have a set of actions (A) applying on a system, a set of processes (P) functioning as a domain and a set of outputs (O) resulting the reprocess of actions. When two domains want to establish a communication channel between them, in order to exchange information, the system must designate a set of rules (security policy). Given the options and the possibilities of the information flow we can verify that a system is secure

Internet is structured as an undirected connected graph where nodes in the graph are routers and links (subnets or sub-networks). Each node and link has a unique id specified by an IP (Internet Protocol) address. In addition, each link has a cost, which can vary in time, and the distance between the two nodes is the sum of the link costs in the path between them.

Reference [2] consider the amount of time (duration) needed for a message to proceed from a network link to another, as a random variable with expected duration where the probability density function $p(t)$ for this time is known. Thus, the expected duration for the transaction is, simply:

$$\langle t \rangle = \int_0^\infty tp(t)dt \quad (1)$$

And the risk of transaction is:

$$\sigma = \sqrt{Var[t]} = \sqrt{\langle (t - \langle t \rangle)^2 \rangle} \quad (2)$$

The first step in a security project must contemplate the identification of all security requirements that can be applicable to a specific environment (the web). Next, it is critical to identify the parties that will be involved in an e-payment transaction and partition the transactions into autonomous actions that can be linked into the parties participating in an e-commerce environment. This information constitute a group of security requirements that develop security architecture (by means of procedures, mechanisms and policies [3].

By Security Architecture we mean the consideration of how a company's systems (in the widest sense) should be designed to ensure that the company meets its security objectives. It relates the security policies, and affects both systems bought and built for general use and a specific solution. A security Infrastructure is the practical realization of a security Architecture in a tangible and usable form.

Computer security refers to the process of prevention, protection and detection of the system and the data stored therein against unauthorized access, modification, destruction or use [4]. Next a question can come up, on how do we secure a faceless, non-physical, remote transaction between individuals and organisations. We must notate that the transmission of information can be materialized in two types of channels, open and secure channels. Open channels are communication channels on which communication may be intercepted by an unauthorized party, in opposition secure channels are communication channels on which data cannot be read, written or altered. This security can be achieved either physically by securing the communication link or cryptographically by securing an open channel [5].

The critical factors for an economic organization or enterprise to both implement and operate an e-commerce mechanism are the flow of money, information flow and product flow. But security and implementation cost are the fundamental. Electronic Commerce (e-commerce) can be highly beneficial in reducing business costs and in creating opportunities for new, simple and improved customer services. Attempting to define e-commerce we can suppose that is the operation of maintaining business transactions (exchange of value) with the use of telecommunication networks

Reference [6] divides e-commerce into three classes:

1. Electronic Fund Transfer (EFT): the methods or the systems of paying electronically, transferring money or funds electronically and exchange digital information by means of electronic payments.
2. Electronic Commercial Information Transfer System: the system that exchange commercial information digitally.
3. Electronic Marketplace: the domains on the Internet where the expectant buyer can seek and purchase goods and services.

But e-commerce involves more than simple on-line transactions. We consider it as a mass of diametric unconventional activities that need to perform operation market research, identification of new opportunities, products, supplying services and exchange ways.

Reference [7] differentiates e-commerce in 1) Business-to-business transactions, 2) Consumer-to-business transactions and identifies that the transaction of e-commerce process can be visualized as a cycle of four phases:

1. **Request** (request of providence)
2. **Negotiation** (conditions of satisfaction)
3. **Performance** (fulfilment and notification of realization process)
4. **Settlement** (acceptation and payment)

Although the progress that has been made for the amplification of methods for achieving secure business transaction electronically, the use of e-commerce has not reach satisfactory limits and it is not considered being a concerted system for transactions, especially financial.

This can be identified as high transactional risk [8]. Transactional risk results when markets fail to provide standard level of security in payments and services.

Inadequacy of trust to electronic commercial and security is a result of the geographical separation of buyers and sellers, often coupled with a lack of real time physical presence [9].

The electronic systems that support the infrastructure of electronic commerce are vulnerable to three aspects of risk: abuse, misuse, and failure. Examining these risks from a business perspective we can identify the primary loss of asset (both in monetary and informational value) and lack of trust to conduct business electronically. What can outspread the universal acceptation, adoption and use of electronic commerce are secure, reliable, speeder, available, renovate able and user friendly communication infrastructure. From all these perspectives the motion of security is the one that distinguish and should be addressed with our whole attention. That does not mean that the rest residue in the extent of importance.

For Internet to be accepted as a medium of conducting monetary transactions, there will need to be a higher degree of confidence in the technology's reliability and security. As with any communications medium, it has both advantages (flow of information and digital assets) and disadvantages (the risk of loss transforming progressively to damage the asset). Reference [10] in a micro and macro analysis have concluded that for Internet to be accepted as a medium to conduct monetary transactions there will need to be a higher degree of confidence in the technology's reliability and security.

The risks of enabling commercial transactions on network operation can be vitiated by the enforcement of security management and policy.

There are therefore three goals in securing electronic communications:

1. prevention from the maximum of the threats
2. detection of violations as soon as possible after they occur
3. reaction to security violations within the minimum of time

Having in mind that businesses are looking for possible ways to provide cost-effective, secure communications services that will enable them to link their business processes more closely with the partners, in a supply chain network, the issue of trust is catalyst.

III. Enabling the Trust Factor

Reference [11] identifies that the majority of trust theories and mechanisms put the emphasis on trust based on the history of transaction experiences the partners had. More specifically, the challenge of the first trade problem in electronic commerce is to develop on line services that will lead companies to build trust among them without any previous experience. To design for trust, it is necessary to determine if, and under what conditions trust mechanisms are brittle [12].

Trust is a function of context, identity, reputation, capability and stake. Trust is also conditioned by social and cultural factors; in certain cultures tradition may provide a strong influence [13] The need of trust in electronic commerce is usually explained by time asymmetry, lack of power, or inability to conclude perfect contracts. The time asymmetry argument draws on the fact that usually transactions are

performed over a period of time [14]. Reference [15] have reported that trust is a catalyst for human cooperation and that people will trust and embrace e-commerce if they perceive sufficient security. They mention that is often ignored the trade-off between functionality and security. In addition, an entity can be said to "trust" a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects [16].

There is a strain to simulate off line an on line trust. The cases might be similar (commerce transaction) and the element to be the exchange might be common however, the nature of the environment, the type of process and many more make the issue of trust variable. Reference [17] sustains this aspect and suggests that in the on-line world, there are two approaches defining relationships between trustors and objects of trust; computer-mediated communication for individual-to-individual trust relationships mediated through technology and in contrast, technology as the object of trust.

Trust and trustworthiness are the foundations of security. The basis for these trust relationships and how they are formed can dramatically affect the underlying security of any system—be it home protection or online privacy [18]. A trust relationship is a relationship involving multiple entities to trust each other having or not certain properties (the so-called trust assumptions). If the trusted entities satisfy these properties, then they are trustworthy.

Given a network of (n) participating members we can consider individuals member trust as Direct or Indirect (Recommended). The direct trust relationship exists, as the word implies, from direct experiences two members develop. In a payment framework let us suppose customer *c* and merchant *m*. The preference of member *c* to pay a curtain amount (a) is represented by $\rho_c(a) \in \{0, 1\}$, where 0 indicates that member *c* does not have sufficient trust to proceed in a payment transaction and 1 indicates the acceptance to proceed. Next the member *m* in the network operates as *c ? m* and so the function that indicates how *c* trusts direct or not *m*:

$$\rho_{cm}(a) = \begin{cases} 1 \ if \ \rho_c(a) = \rho_m(a) \\ 0 \ otherwise \end{cases} \quad (3)$$

Reference [19] defines a recommendation of trust as:

$$C \text{ trusts.rec}_x^{seq} M when\, path\, S_p when.t \arg et\, S_t \text{ Value} V$$

A recommendation trust relationship exists if C is willing to accept reports from M about experiences with third parties with respect to trust class x. Seq is the sequence of entities that mediated the experience excluding C and M. Let p be the number of positive experiences with Q which P knows about with regard to the trust class x. Then the value v_z of these experiences is computed as follows:

$$V_z(p) = 1 - a^p \quad (4)$$

This trust is restricted to experiences with entities in S_t (the target constraint set) mediated by entities in S_p (the path constraint set). If p and n represent positive and negative experiences respectively with the recommended entities, the recommendation trust value v_r is computed according to the following formula.

$$V_r(p,n) = \begin{cases} 1 - a^{p-n} \ if \ p > n \\ 0 \ else \end{cases} \quad (5)$$

According to the Figure 1, V_2 represents direct trust and V_3, V_1 represent recommendation trust.

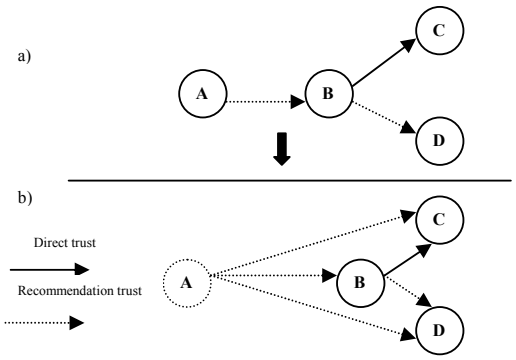

Fig. 1 Trust relationships

Due to an existing relationship, a new trust relationship can brought out between A and C as well as A and D can be derived. These processes are represented by the following equations:

Derived direct trust between A and C

$$V_1 \circ V_2 = 1 - (1 - V_2)^{V_1}$$
$$= 1 - (1 - (1 - a^p))^{V_1} \ p = number\ of\ \ positive \text{ experiences } B \text{ had about } C$$
$$= 1 - a^{v_1 p}$$

Derived recommendation trust between A and D

V_1V_3 = simply multiplication between V_1 and V_3

This multiplication shows that the value of derived recommendation trust decreases as the recommendation path grows.

IV. Need for Security

Protection of business transactions (referring to networks) and information within applications and web services from unauthorized use can be seen through the key security issues of:

Privacy: during the transmitting of the message the message in any form must be not altered or read.

Authentication: each party taking part in a communication must be sure of the identity of each other.

In addition we can see

Confidentiality: the process of keeping information in secret form.

Integrity: the role of proving that the information has not been tampered during its transit or its storage on the network.

No repudiation: the method of ensuring that the information cannot be disclaimed.

We need to ensure these properties or fundamentals security services in order to abjure and persevere the four types of possible security attacks:

Interruption: Attacks by unauthorized users can lead to system failure.

Interception: An unauthorized individual (C) intercepts the message content and changes it or uses it for malicious purposes.

Modification: The content of the message is modified by a third person C

Fabrication: Another user C, can produce messages and send them to B, by making them look just like they have been sent from A.

E-business requirements for security vary from company to company. The cost of security measures must be commercially justifiable. Risk analysis and the investigation of possible protective mechanisms must include an estimation of both the value of information and the likelihood of a security leak. They are essential tools for determining the appropriate security architecture. The final result of this process has to be a well defined security policy, which must be consistently implemented and frequently reviewed and up to last technology reports and methods.

Reference [20] distinguishes management of security networking environment in:

1. Defining a set of security policies which describes an organization's security,
2. Deploying, configuring, and monitoring a set of security, and
3. Monitoring the firing patterns of the security rules

Electronic payment systems are the most essential part of electronic commerce and electronic business. Electronic payment mechanisms provide the financial infrastructure needed to open the electronic marketplace.

There are three payment protocol models [21]:

1. Cash, tokens that can be authenticated independently by the issuer
2. Cheque, payment instruments whose validity requires reference (also called Credit/Debit instrument) to the issuer.
3. Cards, payment through existing credit card mechanism.

The problem is how to enable the traditional ways of paying for goods and services to work similarly and suitably over the Internet. Similar is the theme of what measures are needed to insure an open network as Internet, to transfer the digital image of information with compliance to security services.

There are many approaches to integrate and plan a strategy for business in the information technology place [22] The typical procedure is:

- Macro planning, for the realisation of business requirements and the outcome of this economic epicheirema.
- Micro planning, for step by step phase planning of each and every part of application.
- Information analysis, definition of technological equipment.
- System development process, the final process of design, development and implementation of e-business plan.

Skepticism can be developed about the support of e-business applications due to required level of trust that is needed to transact over the Internet. Security doubts are made about the ability to establish and perform the four services of security.

V. Involving Cryptography

As the information relies on security, cryptography plays the central role in an information security plan. It safeguards the integrity and the confidentiality of stored and transported data [23]. First we must distinct implementation between algorithms. Algorithm is a mathematical procedure with finite set of rules-actions for a problem solving and implementation is the process that defines/shows how this theoretic evaluation can be carried out in the real world. What we need to look for is the implementation. But we have to consider the existence of an algorithm that satisfies the following criteria: completion, decisiveness and affectivity. A communications system under no circumstances has to rely on the secret algorithm. The system relies on the secrecy of the deciphering key.

Cryptography can be the progenitor of every security solution. That means that a security policy, architecture and implementation cannot be without at least taking into consideration the use of cryptographic tools. Cryptography is fundamental in creating and maintaining secure information to sufficiently identify users in electronic business environments.

A typical cryptosystem consists of a plaintext P, ciphertext C, a cryptographic algorithm cipher, and a Key(s). The key or (s) is the secret information shared by the originator and the recipient that is used to secure the plaintext data by the application of the cipher. Encryption is a key-based mathematical transformation that changes plaintext to ciphertext, in such a way that the reverse operation - decryption - is very difficult without possession of the key.

Two basic kinds of cryptographic transformations exist. The single key or symmetric cryptography uses the same key for both encryption and decryption. The two key (pair) or public key or asymmetric cryptography (the one key encrypts and made public, the other decrypt and is kept secret). In the Public-Key Crypto-Systems the Keys are generated in matching pairs. The success of public key cryptography (PKC) is mainly based on the mathematical difficulty of factoring very large prime numbers.

The overall security of e-payments and online transactions is Cryptography, that can be seen as part of a hole security solution, in which her role is to obtain that the transmitted data of information in a communication systems are provable secure. Reference [24] in a confrontation between Provable Security and Practical Security led to conclusion that the perfect situation is reached when one manages to prove that, from an attack, one can describe an algorithm against the underlying problem, with almost the same success probability within almost the same amount of time.

Public Key Infrastructure is a mainstream method, to ensure key management and reliable authentication and encryption between two objects that are communicating over a single open network. The use of public-key cryptography requires a public-key infrastructure to publish and manage public-key values.

Reference [25] report that it is not clear what value a PKI brings in electronic commerce. What can be regarded as positive is that authentication protocols can verify the identity of an entity that one already knows about. On the Internet, users come into contact with businesses they have never met before.

VI. Electronic Payment (e-payment) Phase

Consumers and providers of products and services are not expected to use widely electronic commerce applications unless they are confident that electronic communications and transactions will be confidential, the origin of messages can be verified and the personal privacy can be protected [26].

Payments are considered to be the integral component of any commerce activity. The needfulness to accelerate the flow of e-commerce transaction leads to establish a scrutable, friendly and secure payment system. Acceptance of e-commerce depends on the confidence of discernible security. Only one security issue is solitary to electronic commerce, which is the electronic payment.

It is preferable to make a distinction between electronic transaction protocols and electronic payment protocols. Electronic payment deals with the actual money transfer, electronic transaction protocols deals with the transactions as a whole. Electronic transaction protocols group together operations and implement failure atomicity, permanence and serializability and electronic payment protocols transfer trust, either as cryptographically signed promises, or as digital cash [27].

Reference [28] defines "Electronic payment" or "e-payment" as the transfer of electronic means of payment from the payer to the payee through the use of an electronic payment instrument. An "electronic mean of payment" would be defined as a mean of payment that is represented and transferable in electronic form. In a similar vein, an "electronic payment instrument" can be understood to be a payment instrument where the forms are represented electronically and the processes that change the ownership of the means of payment are electronic.

Electronic payment mechanisms as mentioned before provide the infrastructure (financial) that is indispensable to open and then establish an aggregate electronic marketplace. Within similar types of electronic payment systems, the encoding and decoding mechanisms of individualized payment systems follow different procedures [29].

The first distinctive feature of e-payment systems is the money model.

- Token – when the medium of exchange represents a value
- Notational – when a value is stored and exchanged by authorisation

A payer and a payee are the conceptual parts that exchange money for goods or services, and a financial institution is the one which links "bits" to "money." Payments can be performed either on-line (real time authorisation) or off-line (without contacting any third party during payment) [30]. On-line payment means that the payment systems requires from the payee to contact a third party in order to verify the process of payment and Off-line that there is no need of contacting and verifying the transaction of payment). We can add semi-online category as the involvement of a trusted third party but not in every payment transaction. The element of order is the validation of payment

Next, the time when the monetary value is actually taken from the payer attributes e-payments into

- Pre-paid systems – customer's account debited before payment
- Pay-now systems – customer's account debited at the time of payment
- Post-pay systems – merchant's account credited before customer's account is debited

Last distinctive feature, but not final, can be considered the payment amount.

- Micro payments, when amount is less than 1€
- Small payments, amounts between 1€ and 15€
- Macro payments, when the amount is bigger than 15€

In the current evaluation process our concerns are the on-line, macro payment systems that offer the ability of interactivity and access to services and large amounts of value.

The stimulants to turn to electronic equivalent fermentations are the need to achieve inferior processing cost, payment anonymity and confidentiality and payer untraceability.

Payment Models classify the digital payment systems according to the necessary flow of information between the participants of an electronic transaction [31]. Considering payments that take action over the Internet the keys issues are to prevent double spending (digital cash is represented by bytes that can easily be copied and re-spent), counterfeiting (digital money can only represent real value) and privacy control (confidentiality, anonymity and untraceability).

VII. Using Public Key Infrastructure (PKI)

Public Key Infrastructure (acronym - PKI) is a set of services that enable the use of public key cryptography (Simplified Key distribution, Digital Signature, Long-Term encryption) in a networked environment [32]. A PKI is the set of components, people, policies and procedures which provides the foundation for the management of keys and certificates used by public key-based security services. A PKI assures the trustworthiness of public key-based security mechanisms.

Before utilization of PKI as a component of a whole security project, several issues must be addressed. Concisely we can distinguish:

- The range of interaction (global or national)
- Operational management (previous experience)
- The economic growth of entity that can lead to expand (assets)
- Acceptance of product(s) or service(s)
- The financial result (cost and outcome of implementation)

Starting to operate PKI we can find out two basics: Certification (the process of binding information such as the public-key value to an entity) and Validation (the process of verifying that a certification is still valid). The way these two operations are implemented is the basic defining characteristic of a PKI.

Public key infrastructure can only provide two basic functions [33]:

- Establish identity (by possession of the private key).

- Enable secure communication (through use of protocols that exploit properties of asymmetric algorithms) between two parties.

There are many approaches to fulfil a comprehensive list of PKI services that satisfy the security requirements [34], [35] and [36].

Security Policy: describes the business practices of the organization and defines the principles for the use of cryptography.

Certification Authorities (CA): issue digital certificates to valid applicants, set the expiry date for certificates and invalidate them when the validity period expires. There are in general two types of structure for a CA: the CA hierarchy and the cross certification. The first CA is built up in one root CA. The cross-certification is a flat and the top node in each hierarchy is connected through each other.

Registration Authorities (RA): is the interface between the user and CA. It authenticates the user and determines the level of trust.

A Certificate Distribution System divided into:

Certificate Holders: subjects or end-entities which get the certificates from CA

Certificate Repository: the storage area of PKI (storing and distributing of entities certificates)

Validation Server: an accessory sever (to provide certificate status, date of expiration etc)

The number of keys required for a setup of a communication system with n users is 2^n as against n (n-1)/2 required for a corresponding symmetric key system. It is obvious that as the number of users boosts, a symmetric key setup becomes rather incapable. Public keys can be published easily without peril the security of the pair keys especially the private or the system. The security of the cryptosystem is dependent upon the key lengths being used. The larger the key length is, the more difficult it is to attack. Regardless of strength the large length of a key lends to PKC, reduces the speed of computation analogue to symmetric key cryptosystems (the biggest disadvantage).

A PKI policy [37] contains a set of rules that must be enforced or applied by an element of the PKI. The rules include a specification about which are the sets of users controlled by them and one or more values related to the parameter. A typical categorization of rules is the Certification rules (control of validity period, key type, key length, certificate), Re-issuance rules (applied to certificates that are about to expire and control whether the certificate can be re-issued and the next validity period) and Revocation rules (specification about what should be done when a particular key is compromised).

PKI can provide higher levels of confidence for exchanging information over the Internet. It achieves this by:

- offering certainty of the quality, source and destination of information sent and received electronically;
- assuring the time that information was sent and received (if known); and
- ensuring the privacy of information sent.

Public key cryptography by its own means is not enough [38]. The reproduction of contractual commerce in the electronic environment shows that is required:

- Security policies to define the rules under which cryptographic systems should operate
- Products to generate store and manage certificates and their associated keys
- Procedures to dictate how keys and certificates are generated and distributed

A trusted and authenticated key distribution infrastructure is necessary to support the use of public keys in a public network such as the Internet.

Public Key Infrastructure is composed of three main entities [32]; the Certification Authority, the Registration Authority and the Repository or Directory Server. The PKI functions are Key Generation and Distribution, Certificate Validation, Generation, Revocation and Management of trust.

The public keys are stored in directory in order to be accessible over open networks such as Internet.

The identity of involved parties is provided by a unique key that can be used with encryption to stamp data or a transaction with a unique identification key. The transmitted data are guaranteed that they haven't been altered by digital signatures.

The implementation of a PKI requires an analysis of business objectives and the trust relationships that exist in their environment. The awareness of these trust relationships leads to the establishment of an overall trust model that the PKI enforces [38], [39].

A classification of trust models can be placed as the following:

Hierarchical: Can be considered as the simplest form of trust model, that allows end entities' certificates to be signed by a single CA.

Distributed (Web of Trust) or Pretty Good Privacy (PGP): Every entity has it's own root CA. It can be thought as a system without the incorporation of a CA. It is used by individuals to encrypt and digitally sign electronic mail messages and files.

Direct (Peer to Peer): A trusted third party does not exist in a direct trust model and each end entity in a peer-to-peer relationship establishes trust with every other entity on an individual basis.

VIII. Creation of Trust Factor and a Trusted Payment Framework

A trusted environment is characterized by a unique identification process and is considered to be the one that has a minimum number of a priori trusted entities. In a PKI a trust anchor is any CA, which is trusted without the trust being referenced through the PKI certificates [40], [41]. Simply the PKI enables the establishment of a trust hierarchy. The transaction entities are unfamiliar and they must establish a trust relationship with a CA. Next, the CA authenticates the entity (referring to established rules that noted in Certificate Practices Statement-CPS), and then issues for each entity a digital certificate. That digital certificate is now signed by the CA and can be considered as a personal identification. These certificates are capable of establishing trust between the

unknown entities as long as they trust the CA. The motive of this trust establishment is to offer a way to transmit data securely over insecure heterogeneous networks.

The public keys are placed in a storage area named *trusted party*. Both the name and public key of the entity with the digital signature of the trusted party is called a *Certificate*. The certificate is important for authentication because it is containing the name, key and signature of the entity.

To authenticate a transacting communication entity we need to authenticate it by the use of a third party. This process enables two diametrically singulars to trust indisputably each other, even though they have not previous personal relationship [42]. The party that necessitates trust to other entities participating in the information transaction, such as payment, is called Trusted Third Party (TTP). Because a TTP issues certificates, it is commonly referred as a Certification Authority or CA.

Electronic payment is confidential when all phases of the procedure are designed to satisfy the participants and their security expectations. To build up trust in the electronic payment system, three elements must be taken into consideration: data, identities and role behavior.

Knowing that commerce exchange is based on the trust between the parties and that internet is a distributed environment with no trust, we can put an end to this problem by the use of a trusted service mechanism (TSM) utilizing/exploiting the browser trust. The reason is that the browser trust list model is very common, simply, flexible and with a scalability of hierarchy. These elements satisfy the need for trust management for distributed environments.

The TSM distributes certificates of CA (root CA or subordinate CAs) in order to achieve the security services of authenticity and integrity. The relying party that has a need to consume the digital product or service of the TSM, simple corresponds as trust anchor to form a trust chain.

Figure 2 illustrates how possible user might use a trust service. The identified parts are a set of four entities (PKI system/ website/ TSM trust web and a client Customer). PKI publishes its certificate of root CA and optional subordinate CAs on the selected TSM in a security way, possible offline way (1). TSM evaluates the PKI security policies and assigned a security level to it. A future customer then, will visit the website (which has a certificate issued by a subordinate CA (2)) to buy digital goods. The n he points to the website (3) and downloads the certificate of the website (4), in order to verify the certificate and he sends a query message with the certificate to the selected TSM. TSM is capable to verify the certificate because it has known the certificate of root CA. If it validated, TSM will response a message to inform the customer about the status of the website's certificate and the level of security. Depending on the report of this message customer can decide whether or not trust the website and proceed to buy the needed digital goods from it.

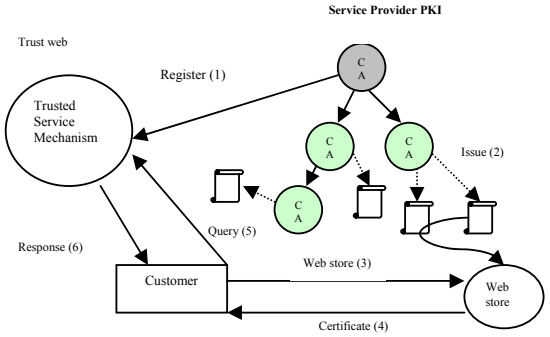

Fig. 2 A trusted framework

IX. Conclusions

If we consider establishing a PKI we must take into serious consideration, issues involving ease of use, ease of deployment, centralized management requirements and security service integration. Providence of end-users with integrated electronic identities (certificates), digital signatures and encryption facilities must be without doubt. We have to accomplish a security mechanism to lay the foundations of trust. PKI is the emergency tool for the establishment of a trust hierarchy. It is the underlying principal of every PKI, due to the fact that electronic commerce operates with trust mechanisms comfortable with risk management operation. The parties-entities (unknown to each other) transacting in open environment as the Internet, do not have sufficient trust established between them to perform business, contractual, legal, or other types of transactions. The implementation of a PKI using a CA provides this trust. This implementation of trust is capable of immunizing the essential part of electronic commerce, the electronic payments.

References

[1] B. Corbitt, T. Thanasankit, H.Yi, *Trust and e-commerce: a study of consumer perceptions*, Electronic Commerce Research and Applications, 2, 2003, pp. 203–215

[2] R. Lukose, B. Huberman, *A methodology for managing risk in electronic transactions over the Internet*, Netnomics, 2000, pp. 25–36

[3] S. Gaines, Z. Norman, *Some Security Principles and Their Application to Computer Security*, the National Science Foundation under Grant No.MCS76-00720

[4] G. Whitson, *Computer security: theory, process and management*' Consortium for Computing Sciences in Colleges, JCSC 18, 2003

[5] D. Pipkin, *Information Security*. Prentice Hall PTR, 2000

[6] L. Fera, M. Hu, G. Cheung, M. Soper, *Digital cash payment systems*, Report, 1996

[7] S. Katsikas, *The Role of Public Key Infrastructure in Electronic Commerce*' The electronic journal for e-Commerce Tools & Applications, eJETA.org, Vol.1, No.1, 2002

[8] C. Westland, *Transaction Risk in Electronic Commerce*, Decision Support Systems 33, Elsevier, 2002, pp. 82-103

[9] P. Skevington, T. Hart, *Trusted third parties in electronic commerce*, BT Technology Journal, Vol. 15, No 2, 1997

[10] S. Lancaster, S. Yen, S. Huang, *Public key infrastructure: a micro and macro analysis*, Computer Standards & Interfaces 25, Elsevier Science, 2003, pp. 437–446

[11] Y. Tan, *A Trust Matrix Model for Electronic Commerce*, Trust Management, LNCS Springer-Verlag, 2692, 2003, pp. 33–45

[12] J. Camp, *Designing for Trust*, LNAI 2631, Springer-Verlag, 2003, pp. 15–29

[13] J. Daniel, *Patterns of Trust and Policy*, New Security Paradigms Workshop Langdale, 1998, Cumbria UK
[14] S. Brainov, T. Sandholm, *Contracting with Uncertain Level of Trust*, 1999, ACM 158113-176
[15] M. Patton, A. Josang, *Technologies for Trust in Electronic Commerce*, Electronic Commerce Research, Vol. 4, 2004, pp. 9–21
[16] ITU-T Recommendation X.509 (2000) Information Technology, Open systems interconnection - The Directory: Public-key and attribute certificate frameworks
[17] C. Corritorea, B. Krachera, S. Wiedenbeck, *On-line trust: concepts, evolving themes, a model*, Int. J. Human-Computer Studies 58, 2003, pp. 737–758
[18] J. Viega, T. Kohno, B. Potter, *Trust (and mistrust) in secure applications*, Communications of the ACM, Vol. 44, No. 2, 2001
[19] T. Beth, M. Borcherding, B. Klien, *Valuation of Trust in Open Networks*, Proceedings of the European Symposium on Research in Computer Security, Brighton, 1994
[20] L Ho, *Distributed Security Management in the Internet*, Journal of Network and Systems Management, Vol. 7, No. 2, 1999
[21] H.-W.-P. Beadle, R. Gonzalez, R. Safavi-Naini, S. Bakhtiari *Review of Internet Payment Schemes*, Proceedings of ATNAC'96, 1996
[22] M. Chesher, R. Kaura, *Electronic commerce and business communications*, Springer-Verlag, 1998
[23] E. Verheul, B. Koops, H. Tilborg, *Public key infrastructure - Binding cryptography -- A fraud-detectible alternative to key-escrow proposals*, Computer Law and Security Report, Vol. 13, no.1, 1997, pp. 3-14
[24] D. Pointcheval, *Practical Security in Public-Key Cryptography*, ICICS 2001, Lecture Notes in Computer Science Vol. 2288, 2002, pp. 1–17
[25] T. Aura, D. Gollmann, *Communications security on the Internet*, Focus Software, No. 105, Volume 2, Issue 3, 2001, pp. 104-111
[26] I. Mavridis, G. Pangalos, T. Koukouvinos, S. Muftic, *A Secure Payment System for Electronic Commerce*, 10th International Workshop on Database & Expert Systems Applications, Florence, Italy, 1999
[27] P. Havinga, G. Smit, A. Helme, *Survey of electronic payment methods and systems*, University of Twente, department of Computer Science
[28] Electronic Payment Systems Observatory (ePSO), Building Security and Consumer Trust in Internet Payments, Background Paper No. 7, 2002
[29] Yu Hsiao-Cheng, His Kuo-Hua, Kuo Pei-Jen, *Electronic payment systems: an analysis and comparison of types*, Technology in Society 24, 2002, pp. 331–347
[30] D. Abrazhevich, *Classification and Characteristics of Electronic Payment Systems*, Lecture Notes in Computer Science, Vol. 2115, 2001, pp. 81-90
[31] J. L. Abad-Peiro, N. Asokan, M. Steiner, M. Waidner, *Designing a generic payment service*, Technical Report 212ZR055, IBM Zurich Research Laboratory, 1996, Availiable: http://www.semper.org/info/212ZR055.ps.gz,
[32] D. Bruschi, A. Curtil, E. Rosti, *A quantitative study of Public Key InC. Sundt, PKI — Panacea1 or Silver Bullet*, Information Security Technical Report, Vol 5, No. 4, 2000, pp.53-65frastructures, Computers & Security, Vol 22, No 1, 2003, pp. 56-67
[33] C. Sundt, *PKI — Panacea1 or Silver Bullet, Information Security Technical Report*, Vol 5, No. 4, 2000, pp.53-65
[34] S. Gritzalis, S. Katsikas, D. Lekkas, K. Moulinos, E. Polydorou, *Securing The Electronic Market: The KEYSTONE Public Key Infrastructure Architecture*, Computers & Security, Vol. 19, No. 8, 2000, pp. 731-746
[35] K. Liaquat, *Deploying Public Key Infrastructures*, Information Security Technical Report, Vol. 3, No. 2, 1998, pp. 18-33
[36] R. Hunt, *PKI and Digital Certification Infrastructure*, Proceedings of the 9th IEEE International Conference on Networks (ICON.01), 2001, pp. 234-239
[37] A. Gómez, G. Martýnez, Ó. Cánovas *New security services based on PKI*, Future Generation Computer Systems 19, 2003, pp. 251–262
[38] J. Weise, *Public Key Infrastructure Overview*, Sun BluePrints™, 2001
[39] RSA Inc. Understanding Public Key Infrastructure (PKI), An RSA Data Security White Paper, RSA Data Security, Inc., 1999
[40] M. Henderson, R. Coulter, *Modelling Trust Structures for Public Key Infrastructures*, ACISP 2002, Lecture Notes in Computer Science, Vol. 2384, 2002, pp. 56–70
[41] S. Gritzalis, D. Gritzalis, *A Digital Seal solution for deploying Trust on Commercial Transactions*, Information Management and Computer Security, Vol.9, No.2, 2001, pp.71-79
[42] M. Benantar, *The Internet public key infrastructure*, IBM, 2001

Theodosios Tsiakis is a Research Assistant teaching Introduction to Computer Science and Cryptography in the University of Macedonia, Dept. of Applied Informatics. His main research interests are financial cryptography and trust management.

George Stephanides is an Assistant Professor similarly in the University of Macedonia, Dept. of Applied Informatics teaching Object Oriented Programming, Computational Mathematics, Cryptography and Algorithms. His scientific research focus on computational number theory, cryptography and computer programming.

George Pekos is a Professor in the University of Macedonia, Dept. of Applied Informatics teaching Computational Mathematics, Cryptography and Statistics. His scientific research focus on computational mathematics, cryptography and applied economics.