Computers & Security (2005) **24**, 10–15

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

The concept of security and trust in electronic payments

Theodosios Tsiakis*, **George Sthephanides**[1]

University of Macedonia, Department of Applied Informatics, 156 Egnatia Str., 54006 Thessaloniki, Greece

Received 17 November 2004; revised 23 November 2004; accepted 23 November 2004
Available online 28 January 2005

KEYWORDS
Security;
Trust;
Electronic payments;
Cryptography;
PKI

Abstract The use of electronic communication channels to conduct businesses without the need for physical conduct or presence has already been established and accepted warmly. But the issue of paying electronically still remains risky and muddy. This article implicates the security and trust issues that are essential for every electronic payment mechanism in order to be accepted and established as a common medium of financial transactions.

The need for security in electronic environment

The growth of the Internet as a medium of transaction has made possible an economic transformation in which commerce is becoming electronic. The critical factor of success for every commercial entity to implement and operate an e-business mechanism is money flow, material flow and information flow in commerce process.

The majority of trust theories are built upon the basis that there is a history of exchanges between partners (experiences), but the fluid and dispersed nature of e-commerce market makes the issue of trust hard due to the frailness to scale the reliability of participants.

Strong and long-lasting business relationships have always been depended on trust. The transition to digital economy, forces enterprises not only to develop customer intimity but also to ensure that security requirements are part of the customer relationship strategy.

Transactions in electronic commerce can occur without any prior human contact or established interpersonal relationships. This lack of interpersonal trust creates a circumstance for a security threat. Generally, security is a set of procedures, mechanisms and computer programs to authenticate the source of information and guarantee the

* Corresponding author. Tel.: +306944757140/+302310 891873; fax: +302310891877.
E-mail addresses: p.tsiakis@psenterprise.com (T. Tsiakis), steph@uom.gr (G. Sthephanides).
[1] Tel.: +302310891872.

0167-4048/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2004.11.001

integrity and privacy of the information (data) to abstain this circumstance to lead to a hardship (economic) of data or network resources.

Three basic building blocks of security mechanisms are used:

- Encryption: provides confidentiality, authentication and integrity.
- Digital signatures: provide authentication, integrity protection and non-repudiation.
- Checksums/hash algorithms: provide integrity and can authentication.

The focus of every processing e-commerce transaction is to minimize the transaction risk. In parallel, a trust framework in e-commerce must address scalability and cost. A business process is understood as a set of logically related tasks performed to achieve a well defined business outcome (Gunasekaran et al., 2002). Electronic commerce (e-commerce) is a subset of electronic business (e-business). A well accepted definition of *e-commerce* is that it "is the sharing of business information, maintaining business relationships and conducting business transactions by the means of telecommunication networks" (Pernul et al., 1999).

E-business concepts fall in many categories such as:

- Business to Business (B2B)
- Business to Consumer (B2C)
- Consumer to Business (C2B)
- Consumer to Consumer (C2C)
- People to People (P2P)
- Government to Citizen (G2C)
- Citizen to Government (C2G)
- Exchange to Exchange (E2E)
- Intra-business (Organization Unit to Organization Unit)

To all these categories, it is characteristic that there are no face to face operations and all e-business transactions are performed electronically with the use of communication networks.

An electronic-commerce transaction can be categorized as a three-step process:

- Search and negotiation
- Trust path
- Commitment and post-monitoring

The first step can identify all the security requirements that can be applicable to the environment we need to establish the concepts of trust and security. The requirements can de considered as follows (Spinellis et al. 1999).

Identification — uniquely identification of a person or entity.

Authentication — providence of identity.

Access Control — control on the actions of a person or entity, based upon its identity.

Confidentiality — prevention of unauthorized parties to capture, interpret or understanding data.

Integrity — assureness that data have not been altered or manipulated by unauthorized parties.

Non-repudiation — prevention of denying the action of participating into a transaction by a person or entity.

Availability — continuously and uninterrupted provision of services.

This list by no means can be considered as comprehensive and can be extended to include other security requirements more specific to environment are being set for.

Security with regard to electronic payment can be categorized into three areas.

1. Systems security — technical infrastructure and implementation.
2. Transaction security — secure payment according to specific and well defined rules.
3. Legal Security — a legal frame for electronic payment.

Identification of trust

The phase of electronic payment (e-payment) is confidential when all phases of the process are capable to satisfy the needs of participants and their security expectations. A fundamental prerequisite must be that all participants ought to have absolute trust in the system that they participate. The contraction of trust in an electronic payment system must take into consideration: data, identities and role behaviour. The adoption of e-commerce must consider trust and risk as important determinants of adoption behaviour.

Trust has been defined as ''the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party'' (Mayer et al., 1995). Trust requires a party to make a rational decision based on knowledge of possible rewards for trusting and not trusting. Trust enables higher gains while distrust avoids potential loss (Jean Camp, 2003). ''Generally, 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'' (X.509 ITU, 2000).

The purpose of modelling trust is to establish a secure way to describe the decision of commerce process. A trusted environment is characterized by:

- the fact that all entities are uniquely identifiable,
- that there is a minimum number of a priori trusted entities, and
- that these entities have unquestionable trust to other participating entities.

To design for trust, it is necessary to determine if, and under what conditions trust mechanisms are brittle. Security architecture presumes that a trust model defines the trusted relationships between all involved components. Trust services are operated by sovereign organizations that are designed to protect consumers. Merchants concede to the organization's trust standards (these standards cover areas such as privacy of personal information, return policies and security policies etc.) in order to bind to legal obligations.

Trust and trustworthiness are fundamental for every security solution. The needs for these trust aspects and the means that are used to implement it, affect the security mechanism of any commercial system. But we must distinct trust form trustworthiness. Trust is an act of a trustor, in which an entity places trust in some object (trust emanates from the entity). In contrast, trustworthiness is a characteristic of someone or something that is the object of trust.

Trust is the enabling of confidence that something will or will not occur in a predictable or promised manner. The enabling of confidence is supported by identification, authentication, accountability, authorization, and availability (Andert et al., 2002).

Electronic payment (e-payment) phase

Electronic payments have been reported to be the ultimate test of security and trust in e-business environment. The notion of payment is an inborn part in any commercial transaction. The electronic payment (e-payment) systems do two things in particular: (a) emulate existing payment frameworks from the real world or (b) schematize new ways to execute payment transactions. Adoption of payment mechanisms and electronic money as other forms of payment depends upon trust in the security and reliability of the system and control of the particular transaction.

The electronic transaction process takes place via the Internet between three participants.

1. Client — every user of the Internet (client) can be considered as a potential customer. It is therefore imperative to establish mechanisms, to certificate trust and security.
2. Merchant — the typical merchant is the entity that needs to sell his goods (products or services) to the clients. In order to achieve this it has to secure transaction processes so that all participants are willing to act in a transaction.
3. Bank — the action of bank is familiar of every financial organization to validate and authorize transactions.

In a commercial context, a payment process involves a payer, a merchant and a bank. In general, the entities transacting in a payment system are appointed by the specific commercial relationship which by it self may depend on series of conditions (Asokan et al. 1997).

The electronic Payment Systems Observatory (ePSO) defines that ''*electronic payment*'' or ''*e-payment*'' is *the transfer of an electronic means of payment from the payer to the payee through the use of an electronic payment instrument*.

Forms of payment can be categorized as substantial (metal coins—paper cheques) or electronic (credit cards), depending on the payment and the transaction medium.

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 authorization.

There are three payment protocol models:

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

A distinctive feature is 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.

- Micropayments, when amount is less than 1€.
- Small payments, amounts between 1€ and 15€.
- Macropayments, when the amount is bigger than 15€.

Knowing the concept of what e-payment is, we can identify an ideal set of requirements and properties that a payment system must have in order to be considered as trusted and secure.

Security evaluation approach: properties and requirements

Requirements

1. *Integrity*: sureness that information has not been altered since the data were signed.
2. *Authentication*: persons participating in a transaction are the one they claim to be.
3. *Fraud prevention and tolerance*: prevention of parties from fraud and from financial losses in the case the system crashes or the network fails.
4. *Privacy*: information must not be revealed to unauthorized people.

Properties

1. *Divisibility*: possibility of multiple denominations (if it is a token-based system).
2. *Transferability*: spending of token without the need to contact the issuer.
3. *Double-spending prevention*: prevention of copied coins to spend repeatedly.
4. *Payment confidentiality*: payment details including payer, payee, account numbers, amounts, date and time must not become known to electronic observers able to monitor network traffic.
5. *Payment anonymity*: the payee will know only pseudonym of the payer.
6. *Payer untraceability*: payment system cannot trace payer payments.

We must mention that these properties are properties of an ideal electronic payment system. No currently working electronic payment system meets all these properties together.

Cryptography and PKI

A logical question arises concerning which is the mechanism that could establish and efficiently implement both security and trust on Internet environment, knowing that Internet is referred as ''the network of networks''; a set of interconnected networks, which is open, independent, heterogeneous and universal. It is an environment that is driven by demand, not supply.

Cryptography represents the only way in which business can work comparable to traditional paper based mechanisms. Cryptographic methods ought to be trustworthy in order to generate confidence in the use of information and communication systems. Cryptographic methods mainly should be developed in response to the needs and demands of businesses. The development of cryptographic methods should be determined by the market in an open and competitive environment. The premise approach enables that solutions are in accordance to technology, the demands of market and needs of information and communications systems. The development of standards and protocols related to cryptographic methods should also be market driven.

Cryptography is represented in two forms. The first is called symmetric or secret key cryptography, uses one common key for both encryption and decryption and a second named public key cryptography or asymmetric, uses two different keys (a private and public) to transform plaintext into ciphertext.

In symmetric schemes the sender and recipient of data, share a single encryption key, and the shared keys must not be revealed or exposed to unauthorized parties. In asymmetric schemes — two keys are used; a ''public'' and a ''private'' key. Public keys can be freely distributed but recipients still require a way to know that a key can be trusted. To certify each public key, central Certification Authority (CA) is created. All cryptography schemes are based on the concept that only the users of the encrypted information should have the keys needed to decrypt it into something understandable.

Public Key Cryptography (Sanderson and Forcht, 1996) is based on the principle that the two keys should be different, but related to each other. In a sense, they need to be inverses of one another. This form of cryptography relies heavily upon the assumption that it is computationally infeasible to

determine the decryption key if the encryption key and algorithm alone are known.

Public Key Cryptography is implemented using trap-door one-way mathematical functions (Mao, 2004). These are functions which are easy to calculate in one direction but infeasible to calculate in the other direction unless certain additional parameters are known. With additional information, the inverse can be calculated easily. Encryption is the easy direction, decryption is hard.

A trap-door function f_k has the following properties,

$Y = f_k(X)$ easy to calculate

$X = f_k^{-1}(Y)$ easy to calculate if k is known

Intractable problem if k is not known

Infeasible means that the problem cannot be solved in deterministic polynomial time and since the parameters are large and the time that indicates the problem to solve will be very large.

All commonly used Public Key encryption techniques are based on mathematical functions which are easy to compute, and hard to invert

RSA	Easy — integer multiplication Hard — factorisation of composite number
Diffie—Hellman	Easy — exponentiation (raising to a power) Hard — discrete logarithms
Merkle's Knapsacks	Easy — increasing knapsacks Hard — general knapsacks

A hash algorithm (also named hash value or a message digest) is a data transformation derived from a key-based cryptography (symmetric key or public key). A hash is a unique representation of a text but smaller in size as compared to the original document. A hash is the conversion of a piece of data of any length into a non-reversible fixed-length number by applying a one-way mathematical function. The length of the resulting hash value is large enough to make the chances of finding two pieces of data with the same hash value insignificant. The sender generates a hash of the message, encrypts it and sends it within the message. The recipient next, decrypts both the message and the hash, producing another hash from the received message, and compares the two hashes. If they are the same, the probability that the message was transmitted intact is extremely high. It is scrutable that hash functions have the following properties.

They are collision-free: it is computationally infeasible to find two different messages that have the same hash.

They are one-way: given a message hash, it is computationally infeasible to find any message with the same hash value.

A product of Public Key Cryptography is the digital signature (equivalent to a hand written signature) that both authenticates and guarantees that the message is original and is being sent by the person it was originally supposed to be sent from. Digital signature involves the reverse process of the encryption. The data are encrypted with the private key of an entity and anyone can decrypt it using the public key; since a public key can only decrypt the data from a corresponding private key, the identity of the sender is verified. Typical digital signatures attempt to solve the problem of tampering and impersonation.

The primary purpose is to discuss PKI (Public Key Infrastructure — comprises a complex infrastructure of hardware, software, networks, security procedures public key encryption techniques, policies and procedures for distribution and management of certificates, a group solution for key distribution problems; Benantar, 2001) in a business environment and how it addresses the trust issues inherent in business models. Unlike other underling technical mechanisms, cryptography scopes are to assure specific things not to happen. That means that the functionality of a system experimentally proven fails hand and foot.

PKI is a business enabling initiative. It provides a means for both trusted digital identity verification and data encryption in transit. In e-business we want to establish relationships and identify the parties (Adams and Lloyd, 2002). Certificates address the problem to verify the identity of the parties exchanging encrypted information over internet.

In the public key technology, an essential process for establishing a trust relationship is for the first entity to import a public key from the second one and protect its integrity for storage or communication to other entities. The entity that imports the public key is known as the relying party (intends to rely upon the public key) for protecting the successional exchange with the keyholder (the entity from whom the key is imported).

E-commerce and e-business as a whole involves transmit of digital information between parties in a business context that needs to be sure that guarantees are offered for:

- the identity of the parties;
- the information transmitted has not changed;

- the confidentiality of the information in transit;
- protection against denial of transaction by one of the parties (non-repudiation).

These four tenets are intellectual statedly in traditional business transactions. Only a mechanism as PKI is capable of standardizing the means of electronic payments and offering assureness, reliability and trustworthiness.

Each approach has advantages; symmetric encryption is faster than asymmetric, but distributing a symmetric key is more involved than distributing a public key from an asymmetric scheme. Until now, despite of the improvements both in algorithms and in computing equipment, public key algorithms still bear a significantly higher cost in computation time and in hardware, memory and communications bandwidth. Therefore, they are used for the protection of short, important pieces of data such as secret encryption keys for the conventional algorithms (Aura and Gollmann, 2001).

Conclusion

Building up a new payment system or an infrastructure of trust for secure transaction is escorted with a significant amount of investments. These investments will compose a worthy return only and if only the new infrastructure is widely used. Meaning that the hazards of security and trust have been confronted with a high level of success.

For public key systems to work properly in the public domain the public key must be freely accessible and also both senders and receivers must have a reliable way of designating that public keys are the keys of parties with whom they wish to transact. This can be concluded directly if the parties are familiar or a formal mechanism to certify keys is established. This sceptic leads to two forms of solutions: Web of trust — based on pre-existing relationships (informal type) between parties, and Certificate authorities — creation of relationship (formal method) achieved by means of PKI.

References

Adams Carlisle, Lloyd Steve. Understanding PKI: concepts, standards, and deployment considerations. 2nd ed. Addison-Wesley; 2002.

Andert Donna, Wakefield Robin, Weise Joel. Professional services security practice. Sun BluePrints™ OnLine—December 2002.

Asokan N, Janson Phil, Steiner Michael, Waidner Michael. Electronic payment systems. This work was partially supported by the Swiss Federal Department for Education and Science in the context of the ACTS Project AC026, SEMPER; 1997 <http://www.semper.org>.

Aura Tuomas, Gollmann Dieter. Communications security on the Internet. Software Focus 2001;2(1):104—11.

Benantar M. The internet public key infrastructure. IBM Systems Journal 2001;40(3).

Electronic payment systems observatory (ePSO), <http://www.e-pso.info/epso/index.html>.

Gunasekaran A, Marri H, McGaughey R, Nebhwani M. E-commerce and its impact on operations management. International Journal of Production Economics 2002;75:185—97.

Jean Camp L. In: Designing for trust. LNAI 2631;2003. p. 15—29.

Mayer R, Davis J, Schooman F. An integrative model of organizational trust. Academy of Management Reveiw 1995;20(3):709—34.

Mao Wenbo. Modern cryptography: theory and practice. Prentice Hall; 2004.

Pernul Günther, W. Röhm Alexander, Herrmann Gaby. Trust for electronic commerce transactions, third east-European conference on advances in databases and information systems (ADBIS'99), Maribor, Slovenia; September 13—16, 1999.

Sanderson Ethan, A. Karen Forcht. Information security in business environments. Information Management and Computer Security 1996;32—7.

Spinellis D, Kokolakis S, Gritzalis S. Security requirements, risks and recommendations for small enterprise and home-office environments. Information Management and Computer Security 1999;121—8.

X.509 ITU-T Recommendation X.509. Information technology, open systems interconnection — the directory: public-key and attribute certificate frameworks; 2000.

Theodosios Tsiakis is a Research Assistant teaching Introduction to Computer Science and Cryptography in the University of Macedonia, Department 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, Department of Applied Informatics teaching Object Oriented Programming, Computational Mathematics, Cryptography and Algorithms. His scientific research focuses on computational number theory, cryptography and computer programming.