ELECTRONIC COMMERCE SECURITY IN THE CONTEXT OF THE MEANS OF PAYMENT DEMATERIALIZATION

Alexandru Pîrjan[1]

Abstract

Some items regarding electronic commerce, electronic vulnerabilities, electronic means of payment, digital money and electronic micropayments are presented below. Then is presented a method of assessing the quality of applications and e-commerce Web sites. This method is then adapted from the operational point of view, developed and implemented in the study of the electronic micropayment systems' security, in the purpose of analyzing and evaluating their security in the context of the means of payment dematerialization.

Keywords: e-commerce, micropayment, security, encryption, digital economy, EWAM.

1. E-commerce

In the last millennium, the informational revolution has left its mark on the entire society. In this period took place the greatest discoveries in the field of science, including the information technology, leading to a big step from e-Revolution to e-Life.

The evolution from the traditional types of commerce and trade to the modern ones, electronics, alongside the evolution of the Internet are huge opportunities for everyone involved, eliminating the barriers of space and time, materializing through the emergence of electronic commerce (e-commerce), electronic business (e-Business), mobile commerce and business (m-commerce and m-Business).

In such a context, for the software applications of these services is very important to ensure an efficient and trusted security framework, by correlating concepts of IT security and law. A viable business model can be designed and implemented only through a close collaboration between computer scientists, economists and lawyers. That's why the e-commerce has a multidisciplinary nature, influencing the behavior of those involved and the links established between them during the development of economic activities. According AFCEE (French Association for Commerce and Electronic Trade) e-commerce consists of the ensemble of the totally dematerialized relationships that economic agents establish between them.

Thus e-commerce can refer both to physical and virtual goods (software, music, movies, books etc) and also to user profiles that can be used to built a business model taking into account information obtained during online transactions. Means of payment related to

[1] Alexandru Pîrjan, Ph D Candidate, Faculty of Computer Science for Business Management, Romanian-American University, 1B Expozitiei Blvd., Sector 1, code 012101, Bucharest, Romania.

transactions can be both classic (Cash, Cheques, credit transfers, interbank transfers, etc) and electronic: electronic or virtual purses, electronic or virtual checks and digital money.

Considering the nature of economic agents and the type of relationship between them, e-commerce applications can be classified as: business-to-business (where the customer is another company or another department within the same company and a characteristic of this type of relationship is the long-term stability); business-to-consumer (that is usually done via telecommunications networks); neighborhood or contact (involving face to face interaction between buyer and seller); peer to peer (that takes place without intermediaries) [7].

In the '80s, due to the necessity of reducing data processing costs supported by traders, the first e-commerce applications have emerged. The expansion of electronic commerce was stimulated by the development of mobile networks and Internet.

Providing a continuous improvement of the transactions' security and the necessity of protecting private information are essential conditions for the acceptance and development of electronic commerce. Cryptography, which has had strictly military applications until a few years ago, is now contributing substantially to ensure the necessary security to gain users' confidence.

But this is not the only obstacle that e-commerce must overcome, having to face also the difficulties of technical, financial and cultural type. The security of the telecommunications' infrastructure and of the system as a whole requires special attention. The propagation of various e-commerce techniques depends on the cultural context and also on the support of public authorities. Costs of implementing e-commerce include equipment, software, network access, staff training and of course maintenance costs over the whole life cycle of an information system.

2. Informatic vulnerabilities

Informational security affects three levels of human activities: the personal security (privacy), the security of companies, organizations and the national security. In order to consider a computer system as being reliable, it must be designed properly, assessed objectively according to an explicit set of security standards, maintain his functionality over its life cycle, lasting electronic attacks and human error. The term of information security (cyber security) refers to the confidence in network infrastructure and information. The information security involves people, processes, policies, procedures, plans, methodologies, systems, technologies, facilities, laws and regulations.

The security of communications (COMSEC) aims to protect classified information against unauthorized access during the information transmission. The computer security (COMPUSEC) is focused on protecting information from unauthorized access. The security of information systems (INFOSEC) appeared with the emphasized development of communications and computational technology, as well as their interaction. The term of security is associated with the informational privacy, so we can identify five key areas: confidentiality (the protection against unauthorized access); data integrity (the protection against unauthorized modification of information); availability (the protection against DOS attacks); authentication of the participants (the identification and authentication of parties involved in the electronic transaction); nonrepudiation (the parties involved in the electronic transaction can not deny their participation).

In addressing the problems of informatic and communication security the following facts should be considered: the Internet is an essential factor in increasing the economic productivity of European countries; economies and citizens depend on the operational status of networks; the risk of electronic attacks increased significantly due to the reduction of accessing costs of the economic information; the spread of viruses facilitated by the Internet leads to information loss and access problems.

The security is an increasing need for the growing of the e-business sector and the health of economy. Thus, special attention should be given at European level to online public services (e-government, e-learning, e-health), and also in implementing of the security's structures.

European standardization organizations should concentrate their efforts on secure interoperable products and services: establishing common criteria for certification, mutual recognition of certificates and cooperation between accreditation agencies. It requires the use of electronic signatures when offering online public services in all European states which implement these services.

ENISA (European Network and Information Security Agency) prevents and finds solutions for most issues related to information and network security, it is a center of expertise for european countries and their institutions and a real help for raising and ensuring the level of security in Europe, it promotes standards and risk management solutions, provides assistance to national regulatory authorities, developing security requirements for operators/ISPs.

In order for governmental and private organizations to transmit confidential data and access their database through Internet/Intranet, the use of encryption is required. The encryption is also imposed by the fact that internal networks of organizations can be accessed via Internet and also, credit card data is transmitted over Internet. The encryption of transmitted and received data ensure its protection by making them unintelligible without authorization. Strict authentication and encrypted sessions are the best methods of protection for companies.

OSI security architecture is, according to the ITU-T X800 standard, a systematic way to define and provide requirements of security. The security services are defined by RFC 2828 as a service of communication/processing of the system in order to provide a certain level of protection for system resources. X.800 defines them as a service provided by open communication systems' protocol, which ensures adequate security for systems and for transferring data.

In order to examine the security architecture a few elements should be taken into account: services are built on mechanisms, they enhance the security of data processing and also the transfer of information and are designed to prevent security attacks using specific mechanisms; mechanisms are implemented using algorithms and are designed to detect, prevent and provide recovery in the case of a security attack. In order to achieve these objectives, mechanisms with different functions can be used, and they all have a common element: cryptographic techniques; a security protocol provides more services. For example, SSL security protocol uses several mechanisms: for electronic signature, algorithms like DSA, RSA are implemented; for encryption, it incorporates RSA and DES algorithms; mechanisms that facilitate the calculation of hashing, using the MD5 and SHA1 algorithms.

Cryptographic hash functions are meant to ensure the integrity and the authentication of data, an essential element in cryptographic protocols. The role of a hash function (denoted h) is to transform an arbitrary length message into one of a fixed length value (128 or 160 bits). The main classes of hash functions are: OWHF- one way hash functions; CRHF – collision resistant hash functions.

A hash function is used to create a digest, a fingerprint. A hash function has the following properties: it can be applied to a data block, regardless of its length; the value of h has a fixed length; h(x) can be easily computed for any given value of x; for any given block h, it is computationally impossible to determine x so that h (x) = h; for a given block x it is impossible to determine a y different from x so that h (y) = h (x); there are no pairs (x, y) with h (x) = h (y).

The most used algorithms of hashing are: SHA-1 that produces a digest of 160 bits length, the message is completed at a multiple of 512 bits, each block of 512 bits is processed into 4 rounds of 20 operations each; MD5 that produces an output summary of 128 bits and its calculation is done in 5 steps; RIPEMD-160 in which the length of the digest is 160 bits and for computing this digest there are necessary 5 pairs of rounds, each one consisting of 16 operations.

Types of encryption:

- Symmetric-key encryption, in which both the sender and the receiver are using the same key, the system being called a shared secret key system. If we reffer to the way in which the processing of the input data is done, we can classify symmetric cryptographic systems in two categories: block ciphers and stream ciphers. When we intend to encrypt documents or databases, we usually use block ciphers and for the encryption of communication channels we use stream ciphers. Most known block encryption algorithms are: DES, Triple DES, AES, RC2, Blowfish, Twofish, IDEA, CAST. Most known stream encryption algorithms are: RC4, SEAL and WAKE.
- Asymmetric key encryption, in which each person has a public key (used for verifying the signature) and a private one (used for creating a signature). The public key can be used by anyone to encrypt, but only one person can decrypt with his private key. The most common asymmetric encryption algorithms are RSA and DSA.

Electronic signature has a decisive role during the process of electronic commerce transactions and it represents the means of authenticating the issuer of electronic document and its contents.

Electronic commerce has imposed the necessity of a permanent service of electronic signature (digital), providing identification of a person without meeting him and compelling evidence for the authorities that the transaction has been completed and executed. Public-key algorithms are often inefficient and slow in the case of using the electronic signature of a document. This is the reason why the digital signature process uses a hash function. So, through a hash function a summary of the document is obtained; this summary is encrypted (the sender encrypts it with the private key, creating a signature in this way); the document is sent to the receptor together with the signed hash; the signature is verified by the receiver: for the received document a new hash is recalculated, using the public key of the sender, the receiver decrypts the signed summary and if the obtained and received summary matches, then the verification of signature ends.

The most frequently used cryptographic algorithms for the digital signature are: MD2, MD5, SHA-1, RIPEM-160 for the hash and RSA, El Gamal, DSA for the signature [4].

3. Electronic means of payment and digital money

Financial context in which the dematerialization means of payment is produced should take into account both forms of money and classical means of payment and the modern ones, represented for example by electronic or virtual money. In the process of implementing modern means of payment, one must take into account some properties of classic money: easy to recognize; their value is relatively stable; durable; easy to transport; easy to use; costs of production are negligible.

The main forms of classical money are: fiducial money (coins or banknotes issued by the central bank); scriptural money (those issued by a bank, and traders may accept them or not); private money (tokens and shares). Payment instruments used to transfer the economic value of money between two economic agents may have a legal status or these instruments may be introduced by banks, and they are: cash, checks, credit transfer, direct debit, interbank transfers, bonds, credit cards.

The new types of payments in the form of dematerialized money are: electronic money (that is fiduciary money stored electronically); virtual money (that can be fiduciary money or tokens); digital money (whose value is stored as algorithms); private money (that can be shares or titles); electronic purses, which may be of two types: electronic money with physical support (electronic purses and electronic tokens or phone cards) and virtual money (stored in the form of software as virtual purses and virtual tokens).

The characteristics of transactions with dematerialized money are: *atomicity* (a transaction must be complete for its effects to take place, otherwise the system should revert to the previous state before the transaction); *consistency* (all parties in the transaction must agree with the critical aspect of the exchange); *isolation* (the final result of a series of transactions that may overlap or not, will be the same as if the transactions would have been executed in a certain order); *sustainability* (if during the trading a malfunction occurs, the system returns to its previous state); *anonymity* (the customer identity is not explicitly used during the transaction but sometimes this property isn’t satisfied); *non-*

traceability (consists not only in ensuring anonymity of the customer, but also the fact that two payments made by the same person may not be related one to each other).

When analyzing the main characteristics of fiducial and scriptural money some differences can be observed: analyzing their *nature*, fiduciary money are palpable, material and scriptural ones are non-material (an account managed by a credit institution); studying their *support*, we should note that for the fiducial money the support is paper or metal, while the support of those scriptural can be magnetic, optical, electronic or they may be stored in a computer; *the value* of the fiducial money can be deposited in safes or wallets, and for those scriptural in accounts maintained by credit institutions, electronic or virtual purses; from the point of view of the *representation of their value*, the fiducial money are represented in banknotes and coins, while the scriptural money by numerical values; *the payment* for the fiducial money is linked to face-to-face transactions, while in the scriptural money the payment is remote or face to face (automatic machines for retail sale); *the means* (instruments of payment) in the case of the scriptural money are checks, debit/credit cards, credit transfer or electronic funds and for the scriptural money, the means of payment are banknotes and coins.

4. Electronic micropayments

Transactions based on electronic protocols have their costs, that are justified in the case of transactions involving larger amounts (DigiCash, Open Market, Cybercash, First Virtual, NetBill). Thus, for transactions between 5 and 10 $ costs are of the order of cents plus a percentage of that amount. In the case of smaller payments, less than 50 cents for example, the cost of the transaction would become significantly compared to the amount involved and then it wouldn’t be convenient. Therefore, when buying cheaper goods and services, specific payment protocols are used. These are electronic micropayments, offering cheap and simple scheme to deal with small amounts of the order of some $, cents or even fractions of cents.

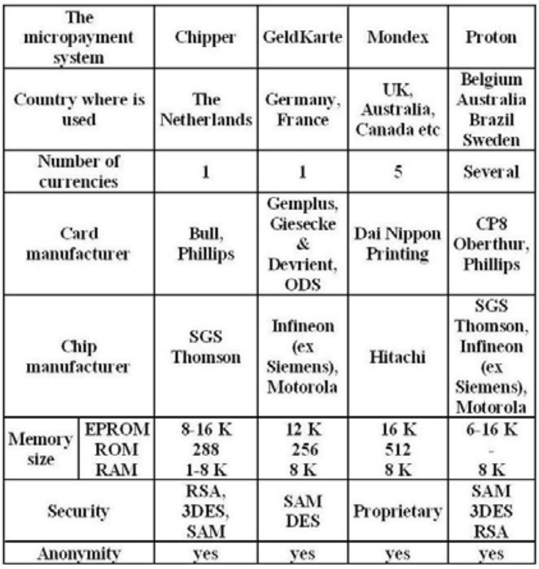
Examples of electronic micropayments systems in the 'face to face' commerce are: Chipper (Netherlands); Geldkarte (Germany, Austria, Holland, Switzerland, France), Mondex, Proton (Belgium and other countries). A comparison of the main electronic purses in face-to-face commerce is presented in Table 1 [7].

The electronic micropayment systems presented below are often incompatible in terms of protocols and services. Thus, a major inconvenience for customers is that they must have access to different micropayment systems because of the lack of interoperability, especially for payments made abroad. A solution to this problem would be an intermediary that will handle foreign trade under the supervision of a bank.

The spread of electronic purses and their lack of interoperability discourage the market, represents an obstacle for users, leads to operational difficulties especially for service providers and increase the production costs. To remove these impediments certain standards must be imposed in terms of protocols, applications and terminals. The new EMV specifications (Europay, MasterCard, Visa) will facilitate this harmonization.

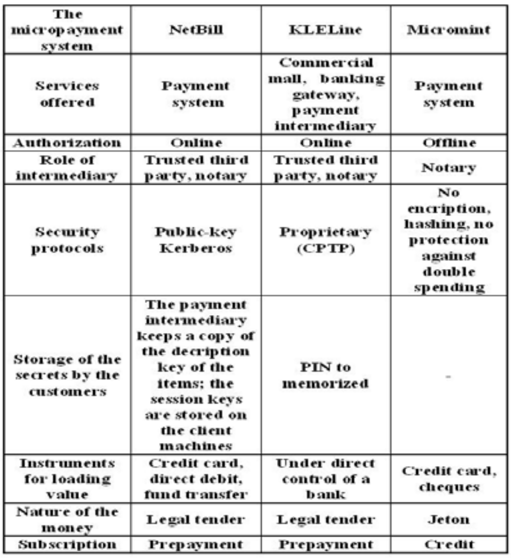
Europay (MasterCard), Visa and ZKA worked together to define CEPS, a set of features to harmonize these systems.

Electronic micropayment systems based on Internet are divided into two generations. Some examples of systems from the first generation are: First Virtual, NetBill, KLELine/Odysseo, Millicent, Ecoin (virtual tokens) PayWord (experimental) MicroMint (experimental). Their properties are depicted in Table 2, [7]. The second generation is represented by : prepaid card systems, e-mail based systems (eg PayPal), Minitel system.



The micropayment system		Chipper	GeldKarte	Mondex	Proton
Country where is used		The Netherlands	Germany, France	UK, Australia, Canada etc	Belgium Australia Brazil Sweden
Number of currencies		1	1	5	Several
Card manufacturer		Bull, Phillips	Gemplus, Giesecke & Devrient, ODS	Dai Nippon Printing	CP8 Oberthur, Phillips
Chip manufacturer		SGS Thomson	Infineon (ex Siemens), Motorola	Hitachi	SGS Thomson, Infineon (ex Siemens), Motorola
Memory size	EPROM	8-16 K	12 K	16 K	6-16 K
	ROM	288	256	512	-
	RAM	1-8 K	8 K	8 K	8 K
Security		RSA, 3DES, SAM	SAM DES	Proprietary	SAM 3DES RSA
Anonymity		yes	yes	yes	yes

Table 1. A comparison of the main electronic purses in face-to-face commerce



The micropayment system	NetBill	KLELine	Micromint
Services offered	Payment system	Commercial mall, banking gateway, payment intermediary	Payment system
Authorization	Online	Online	Offline
Role of intermediary	Trusted third party, notary	Trusted third party, notary	Notary
Security protocols	Public-key Kerberos	Proprietary (CPTP)	No encription, hashing, no protection against double spending
Storage of the secrets by the customers	The payment intermediary keeps a copy of the decription key of the items; the session keys are stored on the client machines	PIN to memorized	-
Instruments for loading value	Credit card, direct debit, fund transfer	Under direct control of a bank	Credit card, cheques
Nature of the money	Legal tender	Legal tender	Jeton
Subscription	Prepayment	Prepayment	Credit

Table 2. A comparison among a few systems of remote micropayment

5. Evaluation of electronic commerce systems through Internet

Essential elements of systems and products, software components must meet high quality standards corresponding to international agreements related to software evaluation. The quality of these products is influenced by a number of extremely complex factors and therefore multidisciplinary researches are required, based on modern methods. The quality of a software product, as it is perceived by customers, affects decisively its economic value. The lack of this quality can lead not only to customers' complaints but also to financial loss.

In order to determine the quality of electronic services, several approaches may be used, such as questioning the consumers after using these services, or experts can be involved in the evaluation of electronic services. In this way, one can obtain information about the quality of these services, but this information is limited and can't cover all phases of online transactions. In order to study the quality of electronic services and approach this study from multiple perspectives it was necessary a tight collaboration between researchers working in different fields (marketing, information technology, sociology, psychology, etc.).

A number of methods for assessing the quality of online public services have already been developed and published. These methods are based on the study of some models, related with basic concepts of service quality. Although there are many such methods, they resemble structurally because their common goal is to obtain a hierarchy of service quality characteristics, quantification and measurement procedures, techniques for calculating and determining the indicators for measuring the quality of service.

In the following it is depicted an evaluation tool which has been specifically created for the assessment of e-commerce applications and Web sites: Extended Web Assessment Method (EWAM). This method [9] builds on the Web Assessment Method developed at the University of St. Gallen, Switzerland. It defines an evaluation grid including a set of criteria to appraise the quality and success of existing e-commerce applications.

The method takes into account customer's orientation and successful implementation of specific environmental goods and services. In **the digital economy three essential elements** are considered for evaluating the success of activities:

1. Electronic markets and transaction phases: information, agreement and settlement (phases of electronic markets), the community component (as a link between the actual purchase transaction and the necessary trust relationship in the virtual realm);
2. Information technology/Media-inherent characteristics: hypermedia presentation, database interface (expert systems), 24-hour access, anonymity, ubiquity, configuration possibility of the user surface, integration with the customer and asynchronous communication;
3. Performance marketing: the customer receives an offer of additional services besides products, designed to make it more attractive and more advantageous compared to similar products offered by competitors.

The method uses 3 categories of criteria to reflect: the ease of use, the usefulness and the confidence. Each such class contains more criteria, corresponding to each of the trade phases on electronic markets and a set of criteria applied to all phases of transactions (final assessment).

Evaluation criteria used in the EWAM method for each phase of electronic transactions are: "1. Information Phase", "2 Agreement Phase", "3 Settlement Phase", "4 After-sales Phase", "5 Community Components", "6 Final Section" and a calculation of the total score. The EWAM method is based on a double assessment of each criterion :

- the assessor appreciates the importance of each criterion, giving a score from a scale of four values denoted with: (++,+,-,--), corresponding to --: minor, -: less important, +: important, + +: very important. There is also an alternative value that can be used if a criterion is not available or not relevant in a particular context, "n. a." (not applicable);
- the Web site involved is also evaluated.

In order to obtain a reliable set of results the scores given by evaluators in the first stage are very important considering the calculation algorithms involved, and we should note that an important low grade (-) would remove a considerable part of the evaluation's result for the second phase and would lead to a reduction of the impact of the evaluation criterion in the overall score.

The importance score will be multiplied by the average evaluations related to each criterion, grouped under 6 categories according to the basic algorithms of the EWAM method. The extreme values of importance will be eliminated for the analyzed criteria and levels of experience of the evaluators will be taken into account. The 6 phases of the transaction correspond to criteria grouped into 6 categories. We denote:

- criteria $X_{gi}, i \in \{1,...,26\}$, each criteria belongs to a category denoted $g \in \{1,...,6\}$;
- the importance of the criteria $W_{gi} \in \{-2,-1,0,1,2\}$, -2 corresponding to the importance --, -1 to -, 0 to n.a., +1 to +, +2 to ++;
- each individual criterion (W_i) is transformed into a range from 0 to 1 through normalization : $\overline{W}_{gi} = \frac{W_{gi}+2}{4}$;
- m is the number of assessors evaluating a criterion X_i ;
- $\overline{r_{gij}} \in \{-2,-1,0,1,2\}$ is the individual result of the criterion i from the category g, evaluated by the evaluator j;
- $\overline{r_{gi}} = \frac{\sum_{j=1}^{m} r_{gij}}{m}$ is the average assessment of each criterion;
- $R_{gi} = \overline{r_{gi}} \times \overline{W_{gi}}$ is the final result of the criterion i from the category g;
- $K_g = \sum_{i=1}^{p_g} R_{gi}$ is the result of each category, where $g \in \{1,...,6\}$ represents the phase of the electronic transaction, p_g is the number of criteria corresponding to the category g;
- $R\,min_{gi} = -2\overline{W_{gi}} \in [-2,0]$ is the minimum assessment of the criterion i from the category g;
- $R\,max_{gi} = 2\overline{W}_{gi} \in [0,2]$ is the maximum assessment of the criterion i from the category g;
- $K\,min_g = \sum_{i=1}^{p_g} R\,min_{gi}$ is the minimum obtained from the category g, p_g being the number of criteria corresponding for the category g;
- $K\,max_g = \sum_{i=1}^{p_g} R\,max_{gi}$ is the maximum obtained from the category g, p_g being the number of criteria corresponding for the category g;

- $K_{\%g} = \frac{1}{2}\left(\frac{K_g}{K\,max_g} + 1\right)$ is the percentage for achieving the maximum score for the criterion K_g, $g \in \{1,...,6\}$;
- $\overline{K}_g = 4K_{\%g} - 2$, $g \in \{1,...,6\}$, is the final result of the category g, and represents the assessment of the phase in the average of the sector;
- $\overline{W_g} = \frac{\sum_{i=1}^{p_g} W_{gi}}{p_g}$, where W_{gi} is the importance of the criteria *i* from the category g, p_g is the number of criteria corresponding to the category g, and $\overline{W_g}$ is the average score of the importance of g. Comparing the average score $\overline{W}_g$ of the final result of the category g, we obtain the degree of response to clients' expectations for the category g;
- $S_I = \sum_{g=1}^{6} K_g$, $S_{II} = \sum_{g=1}^{6} K_g$, $S_{III} = \sum_{g=1}^{6} K_g$, are the final results of the three profiles and it represents the sum of the categories for each profile. We will denote them by $S_\tau, \tau = I, II, III$;
- $S\,min_\tau = \sum_{g=1}^{6} K\,min_{\tau g}$ is the theoretical minimum of the score for all the criteria belonging to the profile τ, $K\,min_{\tau g}$ is the minimum for the cathegory g belonging to profile τ;
- $S\,max_\tau = \sum_{g=1}^{6} K\,max_{\tau g}$ is the theoretical maximum of the score for all the criteria belonging to the profile τ, $K\,max_{\tau g}$ is the maximum for the cathegory g belonging to profile τ;
- $S_{\%\tau} = \frac{1}{2}\left(\frac{S\tau}{S\,max_\tau} + 1\right)$ is the percentage for achieving the maximum score for $S_\tau, \tau = I, II, III$;
- $\overline{S_\tau} = 4S_{\%\tau} - 2$ is the evaluation of the quality for the profile τ.

The EWAM method is an useful tool for evaluating e-commerce sites, allowing their global assessment and comparative analysis. The validation of assessment criteria can be done by experiments and it is essential for establishing the viability of the method. This method can be used for a comparative study of the quality and security of electronic micropayment systems, choosing a set of relevant criteria, in accordance with the security standards that reflect the security of the sites and of transactions. Such assessment should take into account the implemented security features for each system (encryption algorithms, methods of identification, authentication, negotiation, non-repudiation, the hash function used to ensure confidentiality of the customer data).

5. References

[1] Victor Valeriu Patriciu, Monica Ene-Pietrosanu, Ion Bica, Justin Priescu - Semnaturi electronice si securitate informatica, Editura BIC ALL, Bucuresti, 2006.

[2] Victor Valeriu Patriciu, Monica Ene-Pietrosanu, Ion Bica, Calin Vaduva, Nicolae Voicu - Securitatea comertului electronic, Editura BIC ALL, Bucuresti, 2001.

[3] Alexandru Balog - Calitatea sistemelor interactive, Editura MATRIX ROM, Bucuresti, 2004.

[4] Mostafa Hashem Sherif – Protocols for Secure Electronic Commerce, CRC Press, US, 2004.

[5] Alexandru Pîrjan, “Electronic Mobile Commerce”, Information Systems & Operations Management (Isom) Workshop No. 3, April 20 - 21, 2005, pp.171 - 178, ISBN – 973-87166-8-3.

[6] Alexandru Pîrjan, “Quality Evaluation of Electronic Commerce Web Sites Using The EWAM method”, Information Systems & Operations Management (Isom) Workshop No. 4, March 1-2, 2006, pp.218-227, ISBN – 973-7643-75-5.

[7] Alexandru Pîrjan, Dana Mihaela Petrosanu, A Comparison of the Most Popular Electronic Micropayment Systems, Romanian Economic and Business Review, vol.3, no.4, pg.97-110, Bucharest, 2008.

[8] Alexandru Pîrjan, Dana Mihaela Petrosanu, Dematerialized Monies - New Means of payments, Romanian Economic and Business Review, vol.3, no.2, pg.37-47, Bucharest, 2008.

[9] Petra Schubert, Extended Web Assessment Method (EWAM) - Evaluation Of E-Commerce Applications From The Customer's Viewpoint, International Journal of Electronic Commerce Volume 7, Issue 2 (Number 2/Winter 2002/03), Pages: 51-80, 2002.