On-line Payment System Survey – eCash

Marius POPA, Adrian CALUGARU

Faculty of Cybernetics, Statistics and Economic Informatics
Department of IT&C Technologies
Academy of Economic Studies Bucharest, Romania
marius.popa@ase.ro

***Abstract**:* The paper presents the main aspects regarding an on-line payment system. Some characteristics of such system are presented and an existing system is analyzed. On its fundamental sense, the electronic commerce is a concept that represents the purchase and sale process or exchange of products, services, information, using o computer network, inclusively the Internet. In the most part of the cases, the electronic commerce imply on-line payments that lead to creation of some kinds of electronic money and some specific payment systems. There are described the some electronic payment mechanisms and the architecture and the functions of the on-line payment system E-Cash are depicted.

***Keywords**:* on-line payment, e-cash, e-payment, security of electronic money.

1. Introduction

Digital economy development determined electronic commerce widely enhancement. The traditional payment methods are still found on electronic commerce web sites, especially in the countries that have not a good developed electronic payment system.

The cash is represented by banknotes and coins, being the most spread payment method in retail trade. The cash using supposes the simultaneous physical presence of the two transaction partners. This thing leads to impossibility to use the Internet transactions.

The cheque represents a document used by a person who gives an order to a bank to pay a sum of money to a beneficiary. It is one of the most insecure payment methods, especially because the Romanian law doesn't specify a very simple method to retrieve the money in case of which the buyer issues an uncovered cheque.

The payment order represents a document issued by payer addressed to the bank that has its account. Through this document the bank has to pay a fix amount to a beneficiary.

The promissory note represents a commitment of the issuer to pay himself to the beneficiary a sum of money at an established date.
The letter of credit has as aim the replacement of the credit given to a buyer with the credit and the fame of a bank that is replaced to this buyer in the obligation to pay to the seller the merchandise price. The payment is conditioned by the bringing of a delivery proof of the merchandise to a buyer.

The traditional payment methods are boiled down to money transfer as cash or through the documents: cheques, payment orders etc. The payment supposes an account opening, the going to the bank to deposit and/or to initiate the transfer in trader's account. The payment confirmation can be or not asked by fax. The last and the most extensive stage is delivery through trader's distribution network or specialized postal service.

ISSN 2067 – 4074

2. Electronic money and payment electronic system features

In electronic commerce, it is not necessary to go to the bank to pay the suppliers of goods and services. The role of the bank is to transform the cash in bits. The cash cannot be completely erased, but they will be transformed more and more in the electronic format.

At present, there are many payment systems. The most important problem is the security one. The most part of the messages sent by e-mail are not crypted, that is anyone can intercept the message. The actual electronic payment standards use the crypting and digital signatures. Through electronic signature using can be make the identity proof of a person who accesses a bank deposit or a credit card.

The electronic money can be divided in two classes:

- with identity;
- anonymous.

If a buyer uses the money with identity, then the bank reconstitutes the transaction and the transferred money trace. If the anonymous money are used then nobody can reconstitutes the spent money trace.

In electronic commerce a transaction is perceived as an action succession developed by three participants: ***the client, the trader (supplier) and the bank***. At electronic transaction initiation, the trader and the bank come to terms how the money transfer is made, using one or more payment electronic systems. Then the client orders some thing on the trader's web site. After the order launching, some actions are carrying out: the trader sends to the client a confirmation by e-mail, the client transfers its credit card number to the bank, the bank verifies the credit card information and the buyer's solvency and if all things are in order the value of the bought goods is transferred in the seller bank account.

The bought article is delivered to the buyer and the transaction is finalized. Depending of the agreement between the bank and the supplier, the last can access the identification data of the buyer or these ones are secret.
As well as traditional systems, the biggest problem consists in the assurance that nobody cannot copy the digital money or take the credit card information. The electronic financial transactions between the banks were made before of Internet - SWIFT (Society for World-wide Interbank Financial Communication).

The payment electronic systems must accomplish the following requirements:

- *secure* – it must permit the safe financial transaction making in opened networks as Internet. Unfortunately, the electronic money are resumed to a simple file that can be copied. Copying or "double spending" of the same sum of money must be prevent by electronic payment systems;
- *anonymous* – the clients' and made transaction identity must be protected;
- *convertible* – the system users work with different banks, being necessary as a currency issued by a bank to be accepted by another one;
- *useable* – the payment system must be easy to used and accepted. The traders who want to sell on-line the products have not any chance in case in which the clients don't agree the idea to make business on web;
- *scalable* – a system is scalable if it can support new users and resources without to have performance failures. The payment system must permit to the clients and traders to integrate themselves in the system without alter its infrastructure;

- *transferability* – it refers to the capacity of a electronic bill to start the money transfer from an account in another one without a bank direct contact by supplier or client;
- *flexible* – it is necessary that the system to accept payment alternative forms in function of the guarantees asked by the parts involved in transaction, the needed time to payment making, performance requirements and transaction value. The infrastructure must support different payment methods, including credit cards, personal cheques and anonymous electronic money. These tools and payment methods must be integrated in a common framework;
- *efficient* – the term of efficiency refers to the cost necessary to make a transaction. An efficient electronic payment system must be capable to assure small costs in comparison with the benefits;
- *integrable* – it imposes that the system has to support the existent applications, to offer the means for integration with other applications indifferently of hardware platform or network;
- *reliable* – the payment system must be permanent available and to prevent the possible errors.

The presented characteristics must be assured in order to obtain with a high-level quality.

3. Electronic money payment mechanisms

The electronic commerce will evaluate beyond of certain level when the ordinary consumers will percept as an electronic payment mechanism as well as sure than the traditional one.

Internet payment – when a on-line selling system is set working, the trader sells 24 hours per day, 7 days per week everywhere when the Internet has came. The potential buyers and clients will have access to last information referring the products, services, prices and their availability. The trader will have to assure that the informatics system is always available and he will operate the order management, invoicing, payment processing and money delivery.

Real-time payment solutions – with the exception of the off-line cases, the money getting resulted as an on-line selling supposes interaction processes succession with banks and other financial institutions. In present, the invoice payment is made with credit cards, electronic money (e-cash), electronic-cheques or smart cards that are the most important payment methods used in electronic commerce. The payment methods are integrated at trader's level in its informatics system or they are offered as outsource by a commerce services provider. This one manages or intermediates the payments from the third parts.

Credit card – it represents the most used payment form on Internet. The its using is simple: the clients who browse in a web site and decide to buy a product or service must introduce the credit card information through HTML form. The completed content as card type, number card, owner's name and card expiring date is sent to web site where the information are collected and sent to the bank. If the trader's site has a direct connection with the bank then it is possible the real-time payment when the credit covers the ordered goods value. The on-line transactions that use payment with cards are cryptographic protected and the crypting way assures that only the bank and services provider for credit cards will access the credit card information.
A first phase implies some agreements with financial institutions, using cryptographic and authentication advanced technologies for messages securing sent through Internet. The trader must open a bank account, offering on-line transaction services based on

ISSN 2067 – 4074

cards. The cryptographic technology currently used SSL (Secure Socket Layer) erases the possibility that an intruder gets the card number, supposing that he intercepts the crypted data. The disadvantage is that SSL doesn't permit to the trader that a person who uses the card in a transaction is the card owner.

Also, SSL doesn't offer any way to the client to know if the trader's web site is authorized to accept the credit card payments and the site is not a pirate one, designed in order to collect data about cards.

The problem was resolved through new technology appearance called SET (Security Electronic Transaction), developed by MasterCard and Visa. SET resolves the authentication problem through digital certificates assigned to the client and trader. SET offers a biggest security than the traditional one. To interdict the trader's access to the client's card number, SET crypts it in a way that assures the access only for the client and authorized financial institutions.

Each of the actors involved in a transaction as trader, client or financial institution uses the private SET certificates that has the role of authentication in addition to public keys associated to the certificates that identifies the other actors. In practice, a third company (Verysign) offers the service for digital certificates providing to its clients, that is the credit card owners. Regarding the seller, the process is similar: in the moment of on-line shopping carrying out, before data interchange accomplishment for transaction starting, the software that includes the SET technology validates the trader's identity and credit card owner. The validation process consists of certificate verification issued by authorized providers of some kind of services.

E-invoice – the credit cards represent the most common solution in B2C and B2B models. In B2B sector, the transaction volume is biggest than transaction volume made through credit cards. Another reason is that the most part of the companies have already used this tool in its classical form and payment method changing would need a reorganization of the economic process that implies biggest costs. The payment procedure through e-invoice is following: the transaction value is automatic sent to the suppliers through an informatics system. These one respond with an invoice that will be paid by different instruments. Secured methods are needed in order to filter the access to the internal databases of the company. The EDI (Electronic Data Interchange) standard offers an infrastructure for this aim. The major problem consists of commercial law of each country that should recognize the electronic invoice validity.

Electronic cheques (Internet cheques, NetCheque) – it is a system developed at Information Sciences Institute of the University of Southern California. The buyer and the seller must have an account opened on the site of NetCheque. To assure the secure it is used the identification through the Kerberos protocol and password. To pay through cheque, it must install a special software at the client. The software works as a cheque book. A client can send a crypted cheque through this software. The trader can encash from the bank or he can use the digital cheque for another transaction with a supplier. A special account from the network verifies the cheque validity and send an acceptance message to the trader that will deliver the goods. PayNow

Debit cards – they need a personal identification number (PIN) introduction and a hardware device using that reads the information on the cards. It is possible to be replaced with the electronic chips used for smart cards that will replace the credit cards.
E-cash – they use a software application to save to the disk the cash equivalent in a digital form. The advantage of this system is given by the money transfer cost that is almost zero. To receive money it is necessary to access a virtual pay office available on web or a ATM machine where the money are encashed. The difficulty of this system is

represented by the security implementation that guarantees that the money cannot be altered. The using of cryptographic technologies, digital signatures and electronic signatures helps to reduce the fraud possibilities. Another condition is that the e-cash must reveal the identity of the person who paid them. The payment system has not to have the bank as intermediary.

4. Ecash Payment System

E-*Cash* was implemented by the company DigiCash and it represents a payment system on Internet based on the real money principle. It was invented by David Chaum in Holland and it uses the cryptography with public keys that assure both the digital signatures, and blind signatures. The system is focused on electronic money anonymity assurance, and the buyer and the seller must have an account opened at the same bank.

The electronic payment systems have some essential requirements that must be accomplished. From these, the following are parts:

- *security* – this means that two payments are not made in the same time without falsification also the protocol atomicity;
- *offline operability* – if the system has offline operability, then the transaction are executed only two parts: the buyer and the seller;
- *transferability* – if the system has transferability, the users can use the coins without to be necessary accessing of coin issuer in order to verify them. The transferability implies the anonymity in the most part of the cases;
- *anonymity* – it is a very important element for some users;
- *hardware independence* – some working systems use equipments to prevent the intrusions, double payment or to protect the master key of the system;
- *scalability* – if the system is scalable then it supports a bigger users number. Also, it is important the facility of adding and erasing the users in or from the system;
- *efficiency* – the efficiency of each process, payment, money retiring is an important factor for all the parts;
- easy to use – the interface with the user is not a cryptographic problem, but the payment system is important to be more practical.
- The E-Cash system asks the following participants:
- *participant* – any participant in the system;
- *issuer* – participant who issues the e-coins;
- *user* – participant who uses the e-coins to buy or sell merchandise;
- *payer* – participant who uses the e-coins to buy merchandise;
- *payment beneficiary* - participant who receives the e-coins in order to sell merchandise;
- *certification authority* – participant who certificates the public keys of the participants.

The E-Cash architecture is depicted in figure 1:

ISSN 2067 – 4074

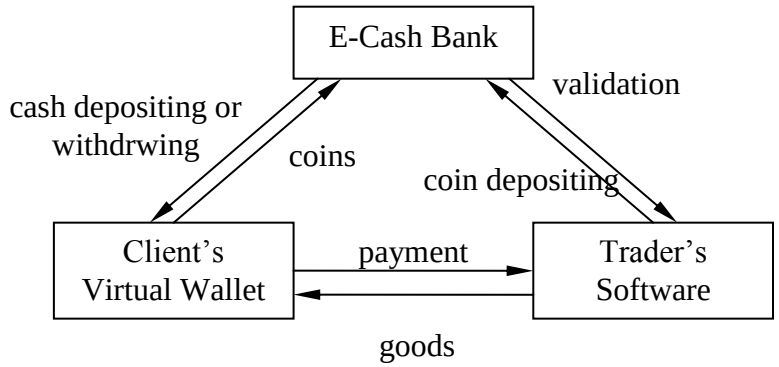

Fig. 1. E-Cash payment system architecture

Coins generating – The coins in E-Cash are simple pairs of two integer numbers. The first value is the serial number of the coin and the other is its value obtaining through a calculation. The bank signs the coin when it computes the second value. For instance, the bank uses the RSA algorithm and its private key in order to sign.

The coin is (a, f(a)) where a is the serial number of the coin and f is a hash function. An user must prepare the coin before that bank signs it. Thus, he prepares a demand let's say 50 coins for 50$ each of them. He envelopes the following information:

- sum: 50$;
- serial number: a;
- identification number: 11, 12, 13, …, 1100.

The serial number a must be different for each coin of the 50. The identification number is a combination of two parts that are generated using a separating secret protocol. The identification information is separated in two parts.
When the bank receives these ones prepared money, it uses the cut-and-choose protocol and opens 40 from the 50 coins and verifies if the sum is the same, the serial number is different and the identification number is valid.

Signing process using the blind signature – it is made because the bank has not to associate the serial number and the person who wants to sign the coin. It is introduced the bling factor r. It is a random integer number that can be multiplied in coin before that the bank signs it. The person can eliminate it after the signing.
The process has take place as follows: the person sends to the bank f(a) * r instead of f(a). When the bank signs it, only the person knows what it is the value after the r will be eliminated. It is eliminated nay identification trace after the coin is spent.

Example: the person **A** has some money and **A** wants that the person **B** signs them using blind signature. The person B has the public key **e**, the private key **d** and a public module **n**. Person **A** selects a random number **k** from **1** to **n**. After that, **A** blinds the value **a**, computing $\mathbf{t = a*k^e (mod\ n)}$. The person B signs **t** with his private key **d**: $\mathbf{t^d=(a*k^e)^d\ (mod\ n)}$. The person **A** can reveal the money when the previous result is divided by **k**.
After this process, person **A** has the money signed by person **B** without person B to know what he or she signed.

$$\frac{f^d}{k} = \frac{(a*k^e)^d \,(\mathrm{mod}\, n)}{k} = \frac{a^d * k \,(\mathrm{mod}\, n)}{k} = a^d \,(\mathrm{mod}\, n)$$

The spending of a E-Cash coin is made following the next steps, in accordance with the figure 2:

1. the trader asks the payment – if the buyer agrees then the E-Cash coins are selected and erased from the buyer, invalidating the numerical series. Then, each coin is sent to the trader;
2. the trader sends the coins to the bank to see if the coins were spent another time;
3. the bank verifies the signature and informs the trader if the coins are valid;
4. if the coins are valid, the trader receives a confirmation and the value of the coins is transferred in the trader's account;
5. the goods are transferred to the buyer.

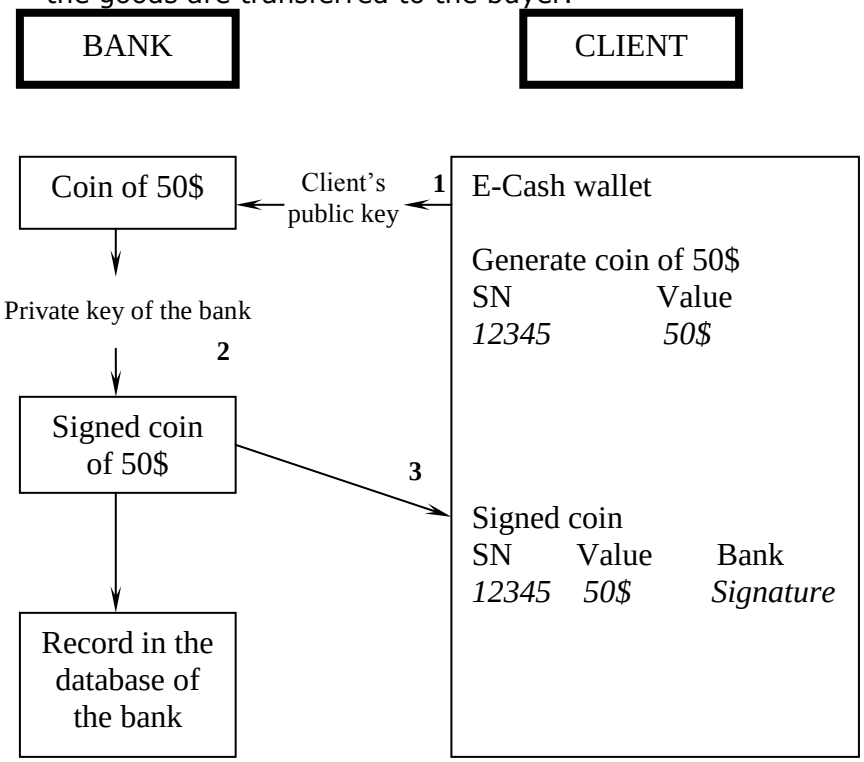

Fig. 2. One E-Cash coin spending

The secured exchanges are made in accordance with the following algorithm, as it is depicted in figure 3:

1. the buyer generates the number **n**, selects a random number **r** and he sends $\mathbf{x=nr^e}$, where **e** is the public key of the bank in order to certificate a certain sum of money;
2. the bank withdraws the sum of money from the buyer's account and uses its private key **d** to certificate the sum. The certificate is: $\mathbf{y=x^d=(nr^e)^d=n^dr^{ed}=n^dr}$. The bank send **y** to the buyer;
3. the buyer computes $\mathbf{z=y/r=n^d}$;
4. in order to buy, the buyer send **z** to the trader;
5. the trader sends **z** to the bank and it he computes $\mathbf{z^e=n}$;
6. the bank computes $z^e=n$ and records n to avoid double spending.

ISSN 2067 – 4074

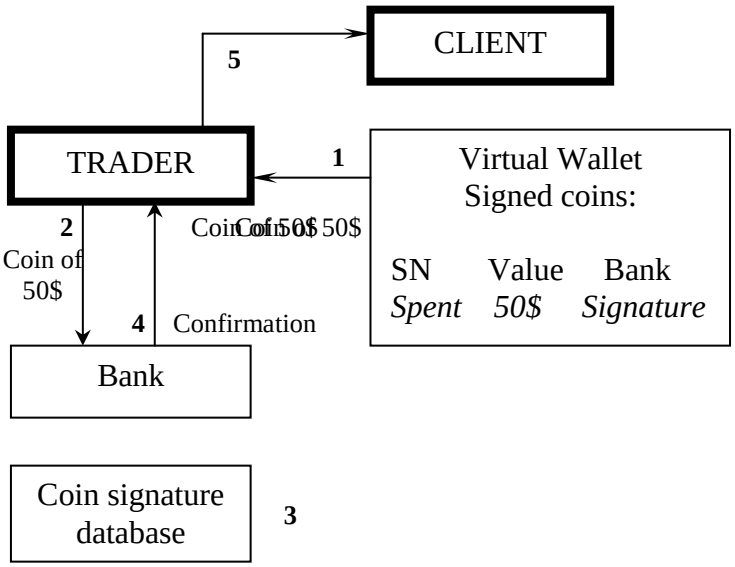

Fig. 3. E-Cash secured algorithm

The advantages of the E-Cash system are the anonymity and security. The electronic money is impossible to trace them because the blind signatures used in coin generating. Secure protocol using that utilize public cryptographic keys RSA determines that the E-Cash system to be secure against the eaves-dropping attacks.

The coins cannot be stolen while they are in transit. However, the coin protection in a local computer can be improved by passwords and crypting.
In E-Cash system, the main disadvantage is the spent coin database dimension. If a big number of persons starts to use the system, the database dimension becomes very large and the database is hard to manage. Keeping the serial number of each coin spent in the system is not a scalable solution.

Another disadvantage is that the system is not a standard one. There are many companies that offer a complete property on the E-Cash system without an interaction among them.

5. Conclusions

In present, it ascertains a big using of the electronic commerce, especially the on-line payment way using. In the first on-line payment systems it took place the system E-Cash developed by DigiCash. The system was focused on electronic money anonymity assurance, and the buyer and the seller had to have an account at the same bank.

The system was not used long time because the main disadvantage of the very large databases for the signatures. But the model E-Cash can be checked up in order to build a more reliable system.

References

[1] Vijay Atluri, "Secure Payment & E-commerce Security Guide", 2003
[2] Georg Carle, E-Cash: "Cash-like Systems", Seminar Mobilkommunikation SoSe, 2005

[3] Donal O'Mahony, Michael Peirce, Hitesh Teware, "Electronic Payment Systems for E-Commerce", Artech House, 2001
[4] Ion Ivan, Paul Pocatilu, Marius Popa, Cristian Toma, "The Digital Signature and Data Security in e-commerce", The Economic Informatics Review Nr. 3/2002, Bucharest 2002.
[5] Paul Pocatilu, Cristian Toma, Securing Mobile Commerce Applications, communication in "The Central and East European Conference in Business Information Systems", "Babeş-Bolyai" University, Cluj-Napoca, May 2004
[6] Cristian Toma, "Secure architecture used in systems of distributed applications", The 7-th International Conference on Informatics in Economy, Academia of Economic Studies Bucharest, Editura Economica-INFOREC, Bucuresti, Mai 2005, p. 1132-1138
[7] Cristian TOMA, "Security in Software Distributed Platforms", AES Publishing House, Bucharest, 2008, ISBN 978-606-505-125-6.