ELECTRONIC COMMERCE. PAYMENT INSTRUMENTS

Alin Titus PIRCALAB, PhD
"Vasile Goldis" West University, Arad
Email alin_pircalab@yahoo.com, tel. 0040744487758

Abstract: *In a "traditional" sense, electronic commerce means using in network value-added applications such as electronic transfer of documents (EDI), the fax communication, barcodes, file transfer and email.*

The extraordinary growth of interconnectivity of computers in Internet in all segments of society has led to a growing obvious trend for companies to use these networks in the area of a new type of trade, e-commerce Internet, to call - besides the old services mentioned - new ones.

For example, the posibility to make purchases over the network by reviewing electronic catalogs "online" on the web or catalogs "offline" on CD-ROM and paying via credit cards or electronic purses.

For others, Internet commerce is a business relationship through networking menus between suppliers and customers, as an alternative communication for "traditional" by fax or EDI dedicated communications lines on networks with added value. Eventually, another form of Internet commerce involves transferring documents - from pro forma contracts or orders, to pictures or voice recordings.

Keywords: data interchange, electronic commerce, electronic money;

Jel codes: A12, F02, F53, G23, G35;

1. Introduction

Electronic Data Interchange (EDI) appeared in the 60s and can be considered the ancestor of electronic commerce. EDI offers companies the opportunity to exchange business documents in a standard form, using electronic means for processing and transmitting them. At the same time banks use dedicated networks for Electronic Funds Transfer (EFT).

Lately, as the availability of Internet is increasing, electronic commerce has captured the interest of individual consumers and companies of all sizes and interests. Moreover, with the advanced technologies now available, it is more and more talking of the Digital Economy (DE). The basic idea is that through e-commerce one can achieve the exchange of ideas, goods, knowledge, beyond simply buying / selling of products and services. E-commerce technologies can be used to run a business using the Internet for communication, Intranet or other computer networks.

The concept of virtual value is very important because it offers the possibility of digital information in the usual processes occurring in runing business activities. One of the main goals of e-commerce strategies is to identify and encourage users of information via Internet, giving them the necessary support. Electronic commerce offers the ability to run a business in a flexible manner that can benefic from the various opportunities as they arise.

But bear in mind that introducing electronic commerce in a business requires some changes in the structuring, development and tracking of activities. Using multimedia techniques or adaptation facilitates the inclusion of details of disclosure forms processed. Presentation of information takes on importance as large as the content. The Internet allows

two-way exchange of information, without limits of time and space.

2. Internet payment systems based on bank cards

2.1 SET Standard

Many purchases of goods and services via the Internet are being paid by ordinary bank card (Visa, MasterCard, etc.). But such transactions on cards contain confidential information and personal information of clients, information that may be intercepted during transmission over the Internet. Without special software, any person who monitors traffic on the network can read the content of such confidential data and can use them later. It is necessary to develop specific standards of payment systems, to coordinate the parties involved in the transfer legitimate and proper use of security measures.

In 1996, MasterCard and Visa have agreed to strengthen their standards of electronic payments into one, called SET (Secure Electronic Transaction). SET protocol aims seven security objectives in e-commerce:

1. To ensure confidentiality payment instructions and application information that are transmitted with payment information;
2. Ensure the integrity of all data transmitted;
3. To provide the buyer's identification and that is a lawful user of a mark card;
4. Provide seller's identification and that it accepts card transactions in relation to a financial institution acquiring;
5. To use the best security methods to protect the parties involved in trade;
6. To be a protocol that does not depend on the security mechanisms of transport and does not prevent their use;
7. To facilitate and encourage interoperability between software providers and the network;

These requirements are accomplished by the following characteristics of this specification:

- **Confidentiality of information** - to facilitate and encourage E-commerce using credit cards, card holders is necessary to ensure that your payment information is secure. Therefore, the buyer's account and payment information must be secure when passing the network, preventing interception of account numbers and expiration dates by unauthorized persons. SET message encryption ensures confidentiality of information.
- **Data Integrity** - This specification ensures that the content does not altere their messages during transmission over the network. Payment information sent by the buyer to the seller to request for information, personal data and payment instructions. If any of this information is changed, the transaction will not be done correctly. SET protocol uses digital signature for data integrity.
- **Authentication buyer** - seller needs a check from his client stating that it is a lawful user of a valid account number. A mechanism that connects the cardholder and account number will specifically reduce the incidence of fraud and therefore the total cost of the payment process. SET uses digital signatures and certificates to authenticate its buyer.
- **Authentication seller** - This specification means to ensure the client that the provider has a relationship with a financial institution, allowing it to accept credit cards. SET uses digital signatures and certificates to authenticate its seller.

❖ **Interoperability** - SET protocol shall be applicable for a variety of hardware platforms and software. Any buyer must be able to communicate with its software with every seller. For interoperability, SET uses specific message formats and protocols.

E- buying - In a typical scenario of e-commerce, the shopping process are**:**

1. The buyer can look for goods and services having more possibilities:

- ✓ Use a browser to view online catalogs of Web page of the seller;
- ✓ Consult an additional catalog that resides on a CDROM;
- ✓ Consult a catalog on paper.

1. The purchaser chooses the goods he wishes to buy.

2. The buyer sees a list of goods, including their price and total price with all taxes. This list must be provided electronically server software seller or the purchase of electronic client computer. Sometimes price negotiation isaccepted.

3. The buyer chooses the means of payment. Consider it chose as payment credit card (the card).

4. The buyer sends the seller a request with payment instructions. In this specification, application and payment instructions are digitally signed by buyers who possess certificates.

5. The seller requests payment authorization from his client from its financial institution.

6. The seller sends acknowledgment.

7. The seller sends the goods or services covered by the application meets.

8. The seller requests payment of goods and services from the purchaser's financial institution.

Cryptography in SET - To ensure payment security, SET uses RSA key pair to create digital signatures and secrecy. Therefore, every participant in the transaction process has two pairs of asymmetric keys: a pair of "exchange" keys - used in encryption and decryption - and a pair "signature" for creating and verifying digital signatures. Note that the role of key "signature" is reversed in the digital signature where the private key is used for encryption (signing), and the public is used to decrypt (signature verification).

Authentication is reinforced by the use of certificates. Before a B recipient to receive a digitally signed message by a transmitter A, he wants to be sure that it has the public key of A and not someone who was recommended as A network. An alternative would be that the receiver B to receive public key directly from A through a secure communication channel. In most cases, however, this solution can not be practiced. Secure key transmission is performed by a "trusted third party" called Certificate Authority (CA) that it assures B that A is the owner of the public key in his possession. Certificate Authority certificate provides that link a person's name and a public key. User A has AC's identity information. The CA creates a message with his name and public key of it. This message, called certificate is digitally signed by the Certificate Authority. It contains information identifying the owner and a copy of the public key (exchange or signature). SET Participants will also have two certificates for two pairs of keys: certified "signature" and certified "parts". The certificates are created and signed simultaneously by AC.

SET protocol introduces a new application of digital signatures, namely the concept of dual signature. Consider the following scenario: B seller sends to A buyer a bid and an authorization to his bank to transfer the money, if it accepts the offer. But B wants the bank not to see terms of the offer, nor its buyer account information. In addition, B wants to make a

connection between supply and transfer, so the money will be transferred only if it accepts the offer to. However he realizes both digital signing messages in a single operation creates dual signature. A dual signature is generated by calculating summaries of both messages and concatenating the two summaries. The result obtained is calculated in turn, a summary and, finally, the latter summary is encrypted with the private key to sign the transmitter. It has included summary message for any of the other two recipients to validate the signature dual. A recipient of any message may verify the authenticity by generating its summary, summary concatenating other message, and calculate summary concatenation. If the new summary dual decrypted signature matches, the recipient can be sure of the authenticity of the message.

If A accepts B's offer, he send a message indicating the bank and its acceptance of the offer including the abstract. The bank can verify the authenticity of transfer authorization for B and ensure that consent is for the same offer by using summary authorization that he received from B and A's summary of the offer presented to validate the signature dual. Thus, the bank can check the authenticity of the offer, but can not see the terms of the offer.

In the SET protocol, dual signature is used to make the connection between a control message sent to the seller and payment instructions containing account information sent to the purchaser. When the seller sent a request for authorization purchaser includes payment instructions received from the buyer control and summary information. The purchaser uses the summary received from the seller and calculates summary payment instructions to verify the signature dual.

Currently, more e-commerce products implements the SET, which gives Internet security card payments through cryptographic means.

2.2 CyberCash

Founded in August 1994, the company Cybercash Inc. US, in April 1995 proposes a mechanism secure payment transactions with cards based on your own server and providing customer service sellers. Using Server provides the ability Cybercash immediately trace and control of transactions. On the other hand, the passage through the server makes the system slower and dependent on the response time thereof. This makes Cybercash less comfortable and more expensive, especially for small cash payment transactions. But public key encryption ensures high levels of security.

Cybercash implements a protection system that performs credit cards used in the Internet. The company - which provides software for both sellers and buyers - operates a gateway between the Internet and the networks of major companies bidding authorization cards. Buyer start by downloading specific software wallet that supports the encryption and transaction processing. Just like a physical wallet that can hold several different bank cards, wallet buyer's software can be used by the customer to register multiple cards, which will subsequently make payments. A similar software provides same thing to the seller.

Messages are encrypted using a symmetric algorithm (DES) with 56-bit key randomly generated, closed in the message encryption with public key of the receiver. Public key encryption system used is RSA, with a length of 1024 bits. Cybercash public key is stored in the wallet and the software vendor. When you register the software wallet cards that will make the payments, the buyer will generate its own public key pair - the private key. Then the key to the public will be submitted to Cybercash, which will record in a database. Although all participants in the system (buyers, sellers and Cybercash) have their own public and private key pairs, only Cybercash knows public keys of all. As a result, the company can exchange information securely with any buyer or seller, but also communicate clearly with each other. Cybercash returns as his task to authenticate all signatures with public keys it holds safely.

When making a purchase, the desired product is selected through a Web browser. The server wallet buyer sends the seller a payment request message clearly, cryptographically signed purchase and request that describes which types of cards are accepted for payment. Wallet software displays a window that allows the buyer to approve the acquisition and the amount and select the card you will pay.

A message is sent back to the seller for payment including a description of the transaction encrypted and digitally signed by the buyer and the card number used. The seller sends the message further payment gateway Cybercash with his own description of the transaction, encrypted and digitally signed. Cybercash decrypts and compares the two messages and check the two signatures. If things are OK, he grants the request by sending a specific vendor to its software. Then confirm payment wallet software seller to the buyer.

Cybercash operate its own gateway as an agent of the seller's bank. Therefore, he must be trusted to decrypt messages and transfer them to networks permit conventional banks.

As the information is encrypted with the public key of Cybercash known to the software operating system, the seller can not see which card number used by the buyer, eliminating the risk reuse this card to other unauthorized purchases.

Recently, the company expanded Cybercash initial payment system based on secure transmission cards with other facilities for electronic money payment: Secure Cash / Check and Secure Check and CyberCoin used for lower values. Also closely with Cybercash at University of Southern California have developed two similar systems: NetCash for small cash payments based on electronic money and NetCheque, a system based on electronic checks.

3. Online paying systems for electronic money

3.1 Ecash

ECash is an example of the electronic payment system that uses e-mail or Web site for implementing a virtual wallet concept. It was developed by the company DigiCash Co. from the Netherlands, founded by the famous researcher of cryptographic systems, David Chaum. The first demonstration of the system was made in 1994 at the first Conference WWW via a weblink between Geneva and Amsterdam. It was subsequently implemented by US banks (Bank of Missouri Mark Twain), Finland and other countries. It is the first entirely software solution for electronic payments.

ECash is a completely anonymous payment system, which uses numerical bank accounts and blind signatures technique. Transactions are between buyer and seller, who must have accounts at the same bank. Purchasers must notify the bank about that wish to transfer money from their accounts in the usual so-called Mint ECash account. At any time, the buyer can interact remotely, through his computer with Mint account and using a soft client can withdraw funds from here on his computer disc. The format of these funds is electronic - 0 and 1 suite of cryptographic protection. As a result, the disc purchaser becomes a veritable "electronic wallet". Then you can execute payments between individuals or by companies through these ECash.

Principle of operation ECash - ECash is private: although the bank keeps a record of each and every deposit withdrawals ECash Mint is impossible for the bank to establish further use of ECash. This property is due to the use of public key criptosisteme RSA with a key length of 768 bits. Besides anonymity payments ECash also provides non-repudiation, meaning that property which allows the resolution of any dispute between buyer and seller on the recognition of payments. Also, by checking the database of the bank, it is prevented from spending any of ECash double.

Like real money (banknotes, coins), electronic money ECash can be withdrawn from accounts or store to be traded. Also, as in the case of physical money, a person may transfer possession of ECash account to another person. But unlike conventional money when a customer pays another client, electronic bank plays a seemingly modest but essential.

ECash is a software solution on-line payments, which consists of the interaction of three entities:

• bank, issuing the coins, validates the currencies and exchange real currency for ECash;

• buyers who have a bank account, which can hold coins or they can submit ECash ECash coins;

• sellers who accept ECash currencies in exchange for goods or services.

ECash is implemented using RSA public key cryptography. Each user has his own key pair (public - and private E - D). It requires special software for managing ECash:

• Customer program called electronic wallet (cyberwallet);

• ECash a special program for the seller.

Withdrawal ECash coins from the bank - Software cyber customer's wallet calculates how many digital coins and what values are needed to meet the demand for payment. Then the program generates random serial numbers for these coins. These numbers are large enough (100 decimal digits) that is a low probability that someone else generate the same values. These serial numbers are then made "anonymous", with the aid of blind signatures. This is done by multiplying them by random factor. Money "anonymous" are then packed into a message with the private key to digitally sign the client's public key figures of the bank and then sent electronically to the bank.

When the bank receives the message, it verifies the signature. Then withdrawn amount can be debited from the customer who signed the application. Bank signed electronic key currencies to private and returns them to the client, encrypted with the public key of it.

By using blind signature, it prevents bank coins can recognize as coming from a particular account. Instead the bank to create electronic coins "white", a user's computer (in our example Dan) is the one who creates randomly coins. Then hide these coins, each in a special digital envelope, and send them over all the bank. Bank withdraws every reception dollar account validation Dan and builds digital currency as a "stamp" on the envelope that Dan just sent. Such envelope "stamped" is returned to Dan. When Dan's computer will remove the envelope, it get a digital currency as wished, but validated stamped. But because the bank has not seen the coin hidden in the envelope, it will not be able to tell when you receive a payment, from whom it derives - ie who owns the money.

After the client receives the money Anonymous sign the bank decrypts the message and cancel anonymity money by dividing the random factor. Digital currency, to be withdrawn from his account in the bank Dan will be stored on his computer's hard drive.

ECash spending coins - When Dan has ECash on its disk, can buy something from the store Vlad. Receiving a request for payment from Vlad Dan approve it by pressing the "Yes" in the window. ECash will choose its program of his wallet (disk) suitable electronic currencies to form the total payment. After this it'll erase those coins and send them over the network to store Vlad. When Vlad's program received the coins, the bank will send them automatically. Then wait until they are accepted or rejected before sending goods purchased by Dan.

Cyberwallet launches the client and Web client software. With the latter sailing until it finds a virtual store on the network. ECash client software works with server and Web client. A shop is nothing more than an HTML document with URLs representing article with products for sale. To buy a product, the customer selects a URL representing the article.

The purchase is made in the following steps:

1. Web client user sends a message HTTP request URL of the Web server vendor. URL will call a CGI program (Common Gateway Interface).
2. The CGI program is called ECash software vendor. It will send details of the selected item in the URL. Locating computer buyer will be sent through a server variable from the ECash software vendor.
3. The software seller will contact the buyer's wallet program via a TCP / IP, demanding payment.
4. When the wallet from client receives the request, he will ask the buyer whether to accept payment. If so, send the seller just necessary electronic currencies. They will be encrypted with the public key of the seller:

E_{SELLER} (Coins)
If the coins are not available to exactly satisfy the request for payment, it sends a refusal to the seller.

5. When the seller receives currencies, decrypts them with his private key; then has to verify their validity and possible double spending. For this, he contacts the bank and will be sent a message consisting of coins, key signed by the seller and then encrypted with the public key of the bank:

E_{BANK} (D_{SELLER} (Coins)

6. The bank decrypts the message with his private key and then validates money by checking the serial numbers with those recorded in the database as having already spent. If the the series seller sent are found in the database,it means that money is invalidated, they already spent. But if they are not in the database and sign right bank are key to private money call validate. Their value credited to the seller's account, money is destroyed and the series they are stored in the database. The software notifies the seller's bank deposit about the successful conclusion.
7. Returns a message-receipt signed electronically by software buyer's wallet.
8. A confirmation message is then sent from the Web server wallet.
9. Submit information to the Web server Web client of the buyer.

3.2 NetCash

NetCash is another example of electronic payment system type online. It was created at the Information Science Institute at the University of Southern California. Although the system does not ensures total anonymity as ECash payments (money can be identified), NetCash offers other means to ensure a certain degree of anonimate payments. The system relies on multiple servers distributed coins, which can be exchanged for electronic checks (including NetCheque) electronic money.

NetCash system consists of following entities:

- buyers,
- sellers,
- coin serveres (CS).

An organization that wishes to manage a currency server must obtain permission from a central authority for certification. Currency server will generate an RSA key pair, public and

private. The public key is then certified by the signature of the central certification authority. The certificate contains an identifier (ID), currency server name, public key of the server currency, issuance and expiry dates, all signed by the central authority:

$D_{central\ authority}$ (ID, Name-CS, E_{CS} , Release day, Expiration date)

Electronic coins issued by the server CS consist of the following:
- *Name CS;*
- *network address of CS;*
- *Expiration date;*
- *serial number;*
- *value.*

The money is then signed with CS server private key:

D_{CS} (Name-CS, Adress-network-CS , Expiration date, Serial number, Value)

CS series keeps track of all money released. In this case, the validity and double spending can be checked whenever you make a purchase or exchange check. When the determination is made of money are spent, their series are deleted from the database of CS and money are replaced by other series. An electronic check can be changed to an CS with electronic money.

To ensure anonymity payments, CS is not authorized to save the people and their network addresses which they issue electronic money. The holder of such coins can then go to any other CS to swap them with other coins issued by that CS

In this transaction the buyer remains anonymous because the seller wants to know only the network address where the buyer acts. NetCash make the assumption that any buyer can obtain the public key of the seller and the latter has the public key of CS.

Purchase transaction using NetCash is made in 4 steps:

1) The buyer sends currencies electronically within message payment service ID to purchase (S-Id), a secret key generated only for that transaction (KBUYER) and a public key session (ESELLER), all encrypted with the public key of the seller . The secret key K will be used by the seller to establish an encrypted channel with the buyer. The public key is then used to verify payment requests coming from that customer.

E_{SELLER} (Coins, K_{BUYER}, E_{BUYER} , S-Id)

2) The seller must verify the validity of electronic currencies received. To do this, it will send CS to swap them with other electronic currency or with a check. The seller generates a new symmetric session key secret KSELLER to be sent with money to CS. The whole message is encrypted with the public key of the server:

E_{CS} (Coins, K_{SELLER}, Kind of transaction)

3) The server verifies that the money CS are invalid, referring to the data base. A ban is valid if its serial number appears in the database. CS seller new currency will return a check or electronic, encrypted with the secret key session of the seller:

K_{SELLER} (New coins).

4) Receiving new money (or check) the seller is satisfied that it was properly paid by the buyer. Now he will return this confirmation, signed with his private key and secret key encrypted session with the buyer:

K_{BUYER} (D_{SELLER}(Sum, Id-transaction, date).

Advantages of using NetCash are scalability and security. He is scalable since it can install multiple CS. Security is ensured by its cryptographic protocols. But unlike the ECash system NetCash is completely anonymous. It is difficult - but not impossible - for MS to keep records about who is issued coins and from which receive money back. The ability to use multiple servers CS increase the anonymity of payments.

4. Micro-payment systems

As we have seen so far, there are a number of protocols for e-commerce payment transactions "big", $ 5, 10 USD and more. The cost per transaction is typically a few cents plus a percentage of the vehicle. When these costs are applied to transactions with low values (50 cents or less), the cost becomes significant in the total price of the transaction. Therefore, to actually get a minimum price for certain goods and services "cheap" to be bought, new protocols will be used.

There are a number of online services that promote newspapers, magazines, reference work and others, all of which are cheap if individual items are sold separately. The advantage of buying individual items may be cheap services more attractive to casual users of the Internet. A user who does not like the idea of opening an account ten dollars a publications editor unknown, may be willing to spend a few cents to buy an interesting article at first. An application "cheap" is to pay frequent visits to Internet sites.

As a concept and experimental projects, micro-payments scheme addresses the need of the existence of a simple, inexpensive, able to support the economic paying very small few dollars, cents and even fractions of cents. We will examine some proposals of this type of electronic payment systems.

4.1. MilliCent

Millicent is a simple and secure protocol for Internet electronic commerce. It was created to support commercial transactions involving costs lower than one cent. It is a protocol based on a decentralized validation of electronic money sellers servers without additional communication, expensive encryption or separate processing.

Millicent key innovation is to introduce the use of cooperating brokers and scrip's. Brokers, (those who sell scrip sites) are in charge of account management, billing, maintenance and establishment of functional connections with sellers accounts. Scrip-digital currency is specific to each vendor individually. Vendors have to validate the local SCIP site to prevent theft, such as for example double spending from customers.

A piece of scrip representing a client account that was established with the seller. At any time, the seller has to solve the scrip's (accounts) with the most recent clients. Account balance is updated scrip's value. When the customer makes a purchase with scrip, your shopping cost is deducted from the total scrip and the value remaining scrip new form (with a new value / balance account), which is returned as change. When the customer has completed several transactions, it can "charge" remaining scrip's value (close the account).

Brokers, serving as interim accounts between customers and sellers. Customers enter into a long term relationship with broker-ii, in roughly the same way as it would make a deal with a bank, credit card company or ISP (Internet Service Provider). Brokers, buy and sell scrip sites belonging to vendors as a service to customers and vendors. Scrip of servers cooperating brokers have a common currency for clients (used to purchase Scrip's sellers) and sellers (to return the unused money scrip).

Millicent reduces costs in several ways:

• The cost of communication is reduced by checking local scrip site, the site of the seller; This eliminates communication costs (which are absent), costs for IT equipment that would give sufficient computing power for a normal progress of a large number of transactions; also no need for centralized servers, protocols expensive etc.

• Cryptographic costs are reduced as there is no need strong cryptographic scheme and expensive to very low values which are traded. It requires a cost that does not exceed the scrip site itself.

• Account costs are reduced by using cooperating brokers who handle accounts and invoices. Customers establish accounts with a broker; broker sets its own account with the seller. This separation reduces the total number of accounts by removing all client-vendor combinations.

The security and confidence model - Millicent security model is based on the assumption that the currency "scrip" is used for small payments. Ordinary people and the business deals with different currencies depending on their value; the same happens in the case of bills, small bills are treated differently when the big bills. Like when a man buys a candy from a vending machine and does not require a receipt, he does not need any receipt when buying an item using the scrip. If a person does not want to pay for something, give up and will get back the amount involved. If this amount (currency) will be lost, he or she will be very upset. It is assumed that a user will have, at one time, just a few dollars in scrip. It follows that it is not profitable to steal a scrip.

Millicent trused model is based on an asymmetric relationship of trust composed of three entities - customer, broker and seller. Brokers, are believed to be more reliable than the sellers, and ultimately, customers. It tends to broker them to financial institutions powerful, large and well known (such as Visa, MasterCard, or banks) or a large Internet service provider or online services (such as CompuServe, NETCOM, or AOL). Is expected to be many sellers, covering a wide spectrum of activities and also a large number of customers and the trust relationships be like in the real world.

Three factors make fraud broker-building in micro-payments unprofitable:

- Customer and vendor programs can independently analyze the script and maintain account balance, so any broker fraud can be detected;
- Clients do not have, at one time, many Scripts - so the broker will have to commit more fraudulent transactions to earn any revenue, and this makes it easier to spot;
- Cooperating brokers reputation is important for attracting clients and a broker can quickly lose that reputation if there are problems in transactions of its customers. The fact of having many active customers is more valuable than stealing scrip broker accounts.

Fraud seller is not to deliver the good or service for a valid scrip. If this happens, the customer will complain to his broker, and the broker will waive a vendor that has caused many complaints. This act means a coercive mechanism because vendors need her broker to facilitate their doing business with Millicent.

As a result, the protocol is reinforced Millicent customers to prevent fraud (falsification and double spending) and indirectly promotes fraud detection cooperating brokers and sellers.

Millicent security of transactions include the following:

- All transactions are protected, each transaction requires that the customer knows the password associated script. The protocol will never send a password in clear text, so it eliminates the risk that someone pulling the "ear" is listening to

something useful. No scrip unit can not be reused. Each application is signed with a password, so there is no way to intercept and reuse a scrip.

- Low-value transactions limited amount of fraud: small transactions require a cheap security; It is not cost effective use of computational resources to steal expensive scrip Cheap. In addition, illegal use of scrip's several illegal actions to raise more money, make more likely the thief detection.
- Fraud is detectable and possibly locate: detection is done when the client does not get the desired good or returned to the customer when the balance is not correct. If a customer is cheating, then the seller only lose the cost scrip detectable false. If the seller is cheating the customer will report the issue to the broker. When the broker receives complaints from several customers against a seller can locate who provokes fraud and will cancel all agreements with the seller. If cheating broker, the seller will receive scrip fake more customers, all related to one broker.

Interaction between Client and Dealer Broker - The following steps for a full session Millicent, including the purchase by the seller's broker scrip are:

• The initial step only happens one time per session. The client makes a secure connection with your broker to obtain a scrip from the broker. The client asks a broker scrip from, for example at the beginning of the day. Broker scrip return the original and secret associate broker.

• The second step happens every time the client does not scrip for a seller. He contacts the broker using the broker's scrip which he owns in step 1, asking the seller to buy a scrip.

• The third step occurs only if the broker should contact the seller to buy the scrip. If the broker does not already scrip from the vendor, she buys. A scrip will ask the seller and he did it returns associated with secrecy.

• In the fourth step broker scrip provide the vendor to the customer. Broker scrip client returns to the seller and the rest (the broker scrip).

• In the fifth step the customer, using scrip site, make a purchase from the seller. It returns the rest (the scrip of the seller) to the customer.

Millicent typical in a transaction when the customer has already scrip seller directly using it to make a purchase. Here there are no additional or interaction with a message broker.

4.2. CyberCoin

Micropayment system CyberCoin Internet payments can be done in small amounts from a few cents to $ 10, covering an area the system using credit cards is not economical. Web vendors who sell services and products at very low prices and immediately want to deliver that cargo, need a method of payment microprocessor cards different, but comparable with cash payments being carried out and in stores. CyberCoin service from Cybercash was launched in September 1996 as a first micro-payment system on the Internet. Consumers can already use existing accounts in banks to transfer values in the software's own electronic wallet. Another possibility is to load funds directly from a credit card through a transaction with such ordinary means. In both cases, real money banks remain in custody.

Once wallet is "filled" with money, consumers can start making micro-payments from Web sites that are registered and have a program called Cybercash CashRegister. This software also supports, and payments by credit cards (VISA, MasterCard, American Express and Discover) and electronic checks PayNow.

From a user perspective, CyberCoin protocol works like an Internet browser; URL must be chosen - get the HTML command. The trader presents HTML page to address

payment (payment URL) along with the price. User not only have to select that URL to purchase particular goods or services.

CyberCoin service is implemented using a concept known as CyberCoin session. A session meets one primary function: initiating a transient sub-account under wallet account for every amount that is spent or collected. A session can resemble a checkbook containing n checks. Each "check" can be used only once. The session ends when all checks were consumed or they have expired. A check can be used only for a single payment or storage.

The runtime session protocol CyberCoin achieved optimal processing speed and reduced cost by encrypting messages with DES cipher. Initiation is an exchange of a randomly generated keys and transported (tires) in a message encrypted with RSA-768 bits. Each "check" payment transaction DES uses a single key. So by breaking the key after the session can not get any profit because it is no longer used to encrypt other messages.

5. Conclusion

Electronic commerce in its true sense has a much greater impact on business development and compress fact, not only new acquisitions, but all activities that support the objectives of marketing a company, including and advertising, sales and market research, payments, activities after-sale services, relationships with customers and others.

This new type of trade has boosted demand for new but appropriate payment methods. Under the new concept of "global village" (global village), development of commercial activities between participants situated at great geographical distances from each other can not be conceived without the use of electronic payment systems. These new means of payment allow transfers convenient, safe and fast money between business partners. Also, replacement of banknotes and coins (current traditional forms of cash) through what we call electronic money lead, besides reducing the cost of issuing and maintaining the movement of cash and an increase flexibility and security of payment systems.

In the field of electronic means of payment, investigations are underway. Well there are many systems currently being tested, others have barely been researched and analyzed. It is normal caution and safety are the key words of these efforts. This paper has presented some popular electronic payment systems, grouped into four categories:

- bankcard systems,
- online systems,
- micro payments
- electronic checks.

Payment systems are only a part of the huge gear driven by big players on the Internet. A successful business in the field of web means much more than implementing the "correct" from a technical standpoint these systems. To assert yourself and maintain best be mobilized resources you have. We tried to follow this in case studies: that the human factor remains above all other things in this area - the machines. The virtual world of the Internet is not actually one impersonal, behind every e-commerce site there is the "merchant" who try to sell the product. Its business success depends on knowing how to lure customers to its goods, to convince them to buy and, most importantly, to persuade them to return back to his shop.

6. References

[1] ISO 7498-2: *"*Open Systems Interconnection - Security Architecture*"* (CCITT X.800);

[2] ITSEC (1991): Information TechnologySecurity Evaluation Criteria; Provisional Harmonized Criteria. June, version 1.2*",* Office for Official Publications of the European Communities, Luxembourg;

[3] Kotler, PH., (1999) – „Principiile Marketingului", Editura Teora, Bucuresti;

[4] Manole, V., Stoian, M., (2004) – „Marketing", Editura ASE, Bucuresti;

[5] Manolescu Gheorghe (1997) – „Moneda si ipostazele ei", Editura Economică, Bucuresti;

[6] Patriciu V.V., Ene-Pietrosanu, M., (2001) – „Securitatea Comertului Electronic", Ed.All, Bucuresti;

[7] Pîrcălab Alin Titus – Revista Informatica Economica nr.31/2007 – *Criptografie Clasică Precomputaţională;*

[8] Pircalab Alin Titus (2008) – „Protectia bazelor de date" – Teza de doctorat – Academia de Studii Economice, Bucuresti;

[9] Pircalab Alin Titus, (2015) – „Sisteme de Gestiune a Bazelor de Date – Aplicatii Microsoft Acces", Editura „Vasile Goldis" University Press, Arad, ISBN 978-973-664-758-1.

[10] Popescu Radu, Tudorancea Cristian, Berbec Florin (1998) – „Cardul instrument modern de plată", Editura Tribuna Economica;

[11] Sabau Gh., Avram V. (1994) – „Sisteme informatice în management". Ed. Metropol, Bucuresti, 275 de pagini, ISBN 973-562-024-3;

[12] Sabau Gh., Avram V., (1998) – „Sisteme informatice si baze de date". Ed. OSCAR-PRINT, Bucuresti, ISBN 973-9264-29-8, 371 de pagini;

[13] Sabau Gh., Avram V., Sotir Al., s.a. (1989) – „Practica bazelor de date", vol.1, Editura tehnica, Bucuresti, pag.496, ISBN 973-31-0020-X şi ISBN 973-31-0021-8;

[14] Sabau Gh., Avram V., Sotir Al., ş.a.(1989) – „Practica bazelor de date", volumul 2, Editura tehnica, Bucureşti, pag.272 ISBN 973-31-0020-X şi ISBN 973-31-0022-6;

[15] Sabau Gh., Ionita C., Avram V., Carstea C. (1998) – „Baze de date relaţionale. Aplicatii in turism". Ed.CISON, Bucuresti, 338 pagini, ISBN 973-96370-2-7;

[16] Sabau Gh., Lungu I., Surcel Tr., Sofronie Gh., ş.a.(1993) – „Sisteme informatice si baze de date". Litografia A.S.E., Bucuresti.

[17] Sabau Gh., Nicolescu Ovidiu (coordonator) ş.a. (2001) – „Sistemul informaţional managerial al organizaţiei", Ed.Economica, Bucuresti, ISBN 973 - 973 – 590 – 524 – 8, pag.488;