A Comparison of the Most Popular Electronic Micropayment Systems

Alexandru PÎRJAN
Faculty of Computer Science for Business Management,
Romanian-American University, Bucharest, Romania

and

Dana - Mihaela PETROSANU
Department of Mathematics I, University Politehnica of Bucharest,
Bucharest, Romania

ABSTRACT

The buying and selling of products or services over electronic systems such as the Internet and other computer networks is known as electronic commerce. In order to reduce the costs of electronic transactions, when one exchanges cheaper goods and services, specific payment protocols must be used. These protocols are actually the foundation for electronic micropayments, which implement simplified and cheaper schemes intended for small value transactions. In this paper we shall present and compare the main characteristics of the most popular micropayment systems used in both face-to-face and remote commerce.

Keywords: e-commerce, micropayment, security, encryption, Chipper, GeldKarte, Mondex, Proton, First Virtual, NetBill, KLELine, Odysseo, MicroMint.

1. INTRODUCTION

The evolution from traditional commerce and marketing methods to the electronic modern ones, alongside the Internet represents tremendous opportunities and succeeds in breaking time and space obstacles materializing in electronic commerce (e-commerce), electronic business (e-business) and mobile commerce and business (m-commerce and m-business). Software applications designed for such services have a great need for an efficient, robust, trustful security framework, binding both informatics and legal security elements. In order to design and implement an efficient business model, informatics, economics and juridical experts must work together and this gives electronic commerce a multidisciplinary feature.
According to FACEE (French Association for Commerce and Electronic Exchanges) electronic commerce is represented by all the dematerialized relations, which are established. Electronic commerce includes both material and virtual goods (software, music, movies, books) and users` profiles on which the business model can be designed taking into account the pieces of information gathered during online transactions. The means of payment for all these transactions can be both classic (cash, cheques, credit transfers etc) and electronic (electronic or virtual purses, electronic or virtual cheques and digital money). Electronic commerce applications can be analyzed from four perspectives, depending on the nature of economic factors and the type of relations between them:

1. Business-to-Business : the client is another company or a different department from the same company and the main trait of this type of relations is the long term commitment.
2. Business-to-Consumer which is usually achieved through telecommunication networks.
3. Neighborhood or contact commerce, which implies a face-to-face interaction between the supplier and the buyer.
4. Peer-to-peer which takes place without an intermediary.

Electronic transactions can have significant costs, which are acceptable when great values are exchanged (DigiCash, Open Market, CyberCash, First Virtual, NetBill). For example, at a 5-10 $ value per transaction the cost value represents several cents plus a percentage from the transaction’s value. If the transaction value were under 50 cents, the

above-mentioned cost would be significant and so it will not be profitable. This is the reason why, when one exchanges cheaper goods and services specific payment protocols must be used. These protocols are actually the foundation for electronic micropayments, which implement simplified and cheaper schemes intended for transactions of small value (several dollars, cents or even fractions of a cent). The most popular micropayment systems for face-to-face commerce are Chipper (Netherland), GeldKarte (Germany, Austria, Netherland, Switzerland, France), Mondex, Proton (Belgium and others).

Some of the most popular sytems of the first generation are: First Virtual, NetBill, KLELine/Odysseo, Millicent, eCoin (virtual tokens), PayWord, MicroMint , while the second generation is represented by prepaid card based systems (for example Smartcode, Easycode), e-mail based systems (for example Pay Pal) and Minitel like systems.

From this point, forward we will depict some characteristics of the most popular micropayment systems.

2. ELECTRONIC MICROPAYMENT SYSTEMS USED IN FACE-TO-FACE COMMERCE

Some of the most common applications of this type of e-commerce is in public transportation systems, parking meters, bakeries, news standings and vending machines. In most of the countries, cash is the preferred mean of payment regarding face-to-face commerce, with a percentage of 90-100% of people who use fiduciary money. Because of their costs and some degree of risk, cheques and bankcards are seldom used. The physical support of these means of payment are integrated-circuit cards, which are the heart for the electronic purses that are used in face-to-face commerce. The main goal of these systems is the replacement of cash and a certain degree of personalization for the services offered. These electronic purses do not depend on special software installed on client's machine, in contrast with virtual purses. The quantity of fiduciary money is given by the electronic value no mater the type of the purse. In order to recharge the electronic value of the purse a financial institution has to step in. The term "micropayment" refers to transactions which reside within a value between 10 cents and US 10 $, while "picopayment" represents values of less then 10 cents. Some of the most important electronic micropayment systems in face-to-face commerce are:

Chipper

Chipper is an electronic purse developed in the Netherlands by KPN a telecommunication operator with the help of Postbank. CyberChipper represents the commercial offer and it allows also Internet payment. The architecture of Chipper-System is depicted in figure 1.

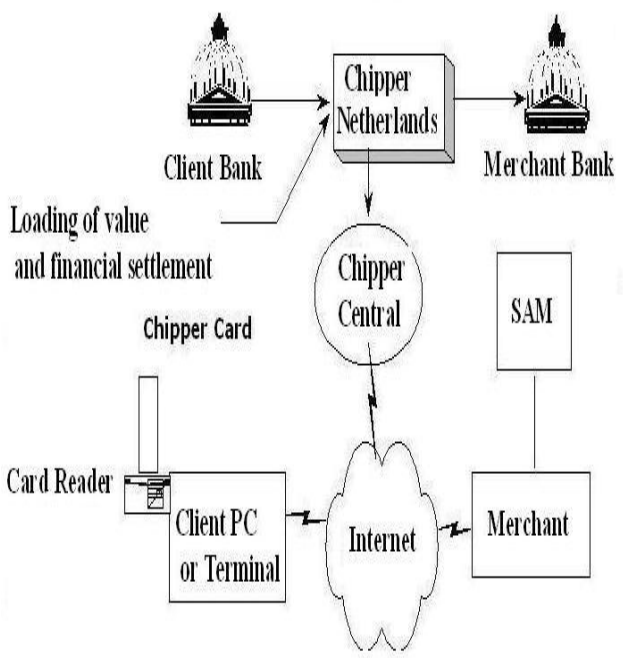

Figure 1. The architecture of Chipper system

The electronic purse is identified and authenticated by Chipper Central, which acts as an intermediary of all the transactions. The same procedures are applied in respect with the merchant terminal. Chipper Central is connected to the payment portal, Chipper Netherlands.

The Security Application Modules (SAM) controls the exchanges between the merchant's server and Chipper Central on one hand and the merchant's server and client's server on the other hand. The details of the protocol security have been kept secret, but it is a known fact that it uses symmetric encription by using triple DES (Data Encryption Standard), and the key exchange is done using the public key criptography RSA.

The electronic purse Chippper uses the multi purpose IBM card with the specification

ISO/IEC 7816-4 and ETSI TE9 (1993). The implemented protocol is IBM Smartcard Identification (ISI) a proprietary protocol which has also been used in many universitary projects in the Netherlands. It includes the ST 16SF48 chip made by SGS Thomson, with the following specifications : 19 KB ROM, 288 B RAM, 8 KB EEPROM. The card reader consists of a keyboard, a screen and specific applications for the electronic purse, applications that allow seeing the remaining value on the card. Swiss Telecom has implemented Chipper specification in his electronic purse Smart Scope

GeldKarte

GeldKarte was first used in 1968 and it reprezented an enhaced version of the Eurocheque card due to the use of a microcip. GeldKarte can be used both in face-to-face commerce and where there is a need for remote Internet payments (in this case the user must have a terminal or a PC with a card reader and the necessary software). The software displays the available value from the card, the transactions' value, the conection status, and it also logs all the transactions which have taken place.

There are many products based on GeldKarte. Deutsche Telekom, in partenership with the railway german company Deutsche Bundesbahn and VDV (The Municipal Transport Association) implemented PayCard, in 1996, Modeus/Moneo was also based on the GeldKarte technology when it replaced the paper tickets for public transportation systems with wireless payments in 2004. The cards were read at the entrance, where the card reader was integrated, from a distance of 10 cm. The antenna transmits at a frequency of 13.56 MHz and is integrated in the surface of the card. Gemplus or Giesecke & Devrient and other smart-card manufacturers based their products on GeldKarte specifications. The microcip is made by Infineon (ex Siemens) or Motorola, with the following specifications 12 KB ROM, 256 B RAM, 8 KB EEPROM (Kirschner, 1998) complying to ISO/IEC 7816-4 (1995). The GeldKarte protocol uses cryptographic algorithms in order to verify the identity of both the cardholder and the merchant.

The integrity of the messages is achieved with a symmetric encryption algorithms DES or triple and comply with the ANSI standards X9.19. The digest of the message has 128 bits and is obtained by aplying a hash function which complies to ISO/IEC 10118-2. The card holder's identification is achieved using a personal identification number (PIN). The PIN is necessary for recharging the card but not for payment.

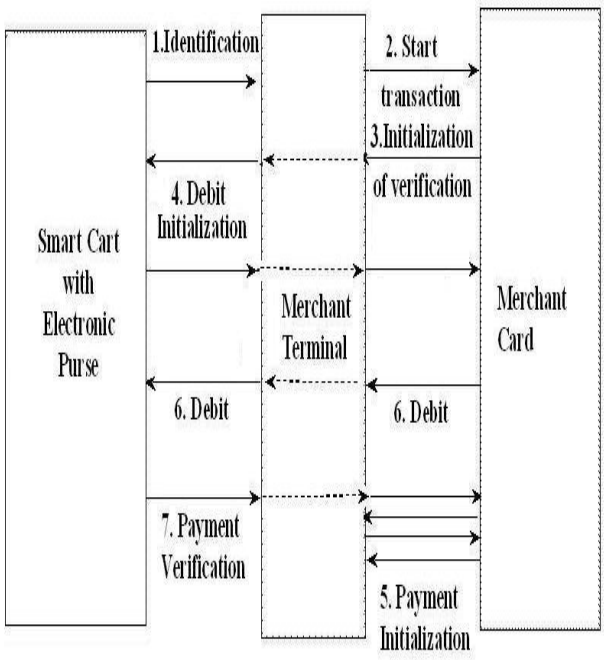

Figure 2. GeldKarte – message exchange.

The client has full anonymity regarding the merchant but not in respect to the financial authorities. Every GeldKarte has a unique identification number and a symmetric key used for encryption. The card's serial number, encryption keys and the pin are stored in a "private-protected" zone of the card. These pieces of information can also be found in an encrypted file kept under high security at the issuing bank. Each transaction has a unique identification number which prevents replay attack. The exchanges during a payment with GeldKarte are depicted in Figure 2.

Mondex

Eversince its beginning Mondex tried to replace classic money. The companies involved in the project were: Dai Nippon Printing Co for the card, Hitachi Panasonic and Oki Electric Industry for integrated circuits, BT (ex British Telecom) and Natwest became interested in obtaining the approval from the Bank of England for recognizing Mondex as a new authentic mean of payment. In the summer of

1996 Mondex International was established as an independent company, MasterCard being the main shareholder along with other 17 multinational corporations. Even if the specifications of the project are kept secret, some important details have been make public: the microchip has 16 KB ROM, 512 B RAM, 8 KB EEPROM (Kirschner 1998); the card can store up to 5 different currencies; the exchange protocol allows also the exchange of value between 2 Mondex cards, remotely (this is a unique feature of Mondex among all other electronic purses); a new type of MIME e-mail messages is used in Mondex exchanges; a Mondex transaction can resume if a break occurs right from its break point.

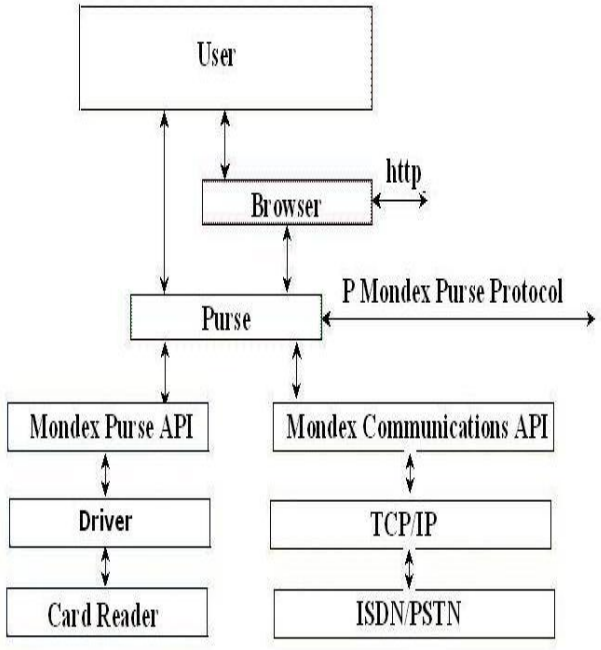

Figure 3. Configuration of a Mondex Client

The Mondex protocols can bind Internet remote payments with those specific to an electronic purse. Two different protocol stacks, which merge in the electronic purse, support the user's interface. The first one assures the Internet access through a HTTP protocol and the second one refers to the electronic purse's performance using a card reader. The intermediate layers between the browser on one side and the TCP\IP layer on the other side are proprietary. The protocols, which control the Mondex electronic purse, are also proprietary.

As a consequence of trial testing in some countries (Great Britain, USA, Canada, Hong Kong) Mondex proved to be better suited for remote micropayments. Figure 3 depicts the configuration of a Mondex client.

Proton

Banksys, an inter-banking company, responsible for electronic payments in Belgium initiated in 1993 the project Proton, which was later implemented, in 1995. This electronic purse has been available all over Belgium since 1996 and it gained international success being the second after GeldKarte regarding the number of its users.

The card used by Proton is manufactured by CP8-Oberthur and Phillips. The microcips are from GS Thomson (ST16 601), Infineon (ex Siemens), Motorola (SC46). Their memory size varies between 6 KB and 16 KB ROM and between 1 and 8 KB of EEPROM (Kirschner, 1998). In order to verify the card and to assure the authentication of both the card and the terminal the merchant terminal is equipped with a Security Application Module. The transactions` security is achieved by using the DES algorithm, for confidentiality and RSA for authentication. The security framework and the electronic purse's functionality is based on the specifications of the EN 1546 standard. Proton is also used for the payment of parking spaces in Belgium and for the access in Banksys or the French Hospital from Ganshoren.

The electronic purse Proton is available in Germany, Sweden, Switzerland, Australia, Hong Kong, New Zealand, Canada, and Brazil.

Electronic Purses Standardization

The main technical and commercial characteristics of electronic purses used in face-to-face commerce are depicted in Figure 4. A big inconvennient for these services is represented by the lack of compatibility regarding protocols and services. A major inconvenient for clients is that they must have more micropayment systems from different providers especially for payments made in foreign countries. A possible solution for this problem could be an intermediary who would handle valutary exchanges under the close supervision of a bank.

The great number of electronic purses and their lack of interoperability are discouraging the market, represents an impediment for their users and creates a lot of operational problems for services providers and

an increase of the production cost. The new EMV (EuroPay, MasterCard, Visa) specifications are targeting these specific problems.

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 ROM RAM	8-16 K 288 1-8 K	12 K 256 8 K	16 K 512 8 K	6-16 K - 8 K
Security		RSA, 3DES, SAM	SAM DES	Proprietary	SAM 3DES RSA
Anonymity		yes	yes	yes	yes

Figure 4. A comparison of the main electronic purses in face-to-face commerce

3. REMOTE ELECTRONIC MICROPAYMENT SYSTEMS

Remote electronic micropayment systems have evolved in two generations. The first generation once brought many technical innovations regarding cryptography and new types of electronic money have emerged. These systems lacked a lot of practical aspects and this was the reason why they have been surclassed by a new generation of products, which were meant to satisfy the needs of their potential users. In order to support the exchanges between the two sides involved in the transaction and to assure the required security level a third thrust party had to interfere. The exchanged products1. of these systems are non-material (information, newspaper archive, online games, zodiac and multimedia content).

We will present some of the most popular remote micropayment systems of the first generation: First Virtual, NetBill, KLELine/Odysseo, Millicent, eCoin, PayWord, MicroMint .

First Virtual

First Virtual was the first commercial offer which used secure payments for digital information and services throughout the Internet. This system didn't use cryptography for assuring the confidentiality and authentication. It was based on two independent networks which were managing the exchanges: the PSTN (Public Switched Telephone Network) and the Internet, which needed simple telematics methods like a browser and a e-mail client whithout any other additional software.

A client could subscribe to this service by means of post, telephone, fax or Internet. The First Virtual server sent a virtual personal identification number (PIN) to the client with which the client could access the payment server.

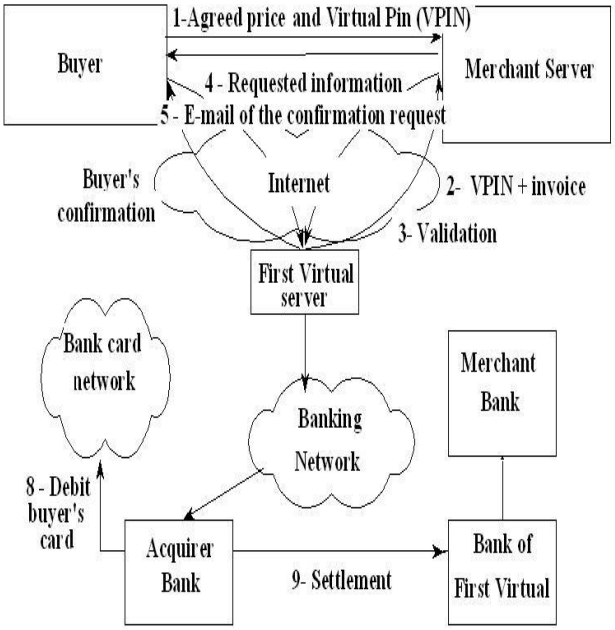

Figure 5. First Virtual

The exchanges which take place in the buying protocol, presented in Figure 5, are as follows:

1. By accessing the order form whithin the browser, the client was sending his PIN
2. Using the First Virtual application, the merchand verified the client and the invoiced details.
3. The First Virtual server would respond to the merchant's server after having verified the requested details.

4. The merchant's server would send the requested information back to the client if it received a positive answer.
5. The transaction was about to been settled after the client had been asked for an e-mail confirmation by the First Virtual server .
6. If the client confirmed, First Virtual would send the credit card number to the First USA bank, in order to debit his account.
7. The business could be settled by an interbanking exchange or through the credit card network.

Due to its simplicity, the procedure was one of the main advantages of this system and proved capable of avoiding cryptographic problems allowing the online selling of images and text. This system wasn't compatible with all the transaction types (for example for buying physical goods) so it had a limited applicability.

NetBill

NetBill consists of a set of protocols, rules and software specially designed for the selling of images, text and software through the Internet. The billing of the client takes place only after he has received the encrypted information and the decryption key which allows him to access the information is sent only after the payment has been made. These are the main characteristics and the advantages of this system.

Both the CA-function (certification authority) and that of a third trusted party is assured by the NetBill server, which also handles both the public and private RSA keys and the session key which are used to encrypt the exchanges which take place between the client and the merchant. In order to subscribe the client sends his payment coordinates encrypted with a downloadable security module (Money Tool) and after he received from the NetBill server an identifier and a pair of public and private RSA keys. The merchant receives the Product Server software and a pair of public and private RSA keys. The client prepays the service from his banking account.

In order to accomplish the four major transaction phases (negotiation, order, delivering and payment) the buying protocol uses 8 HTTP messages. Both the client and the merchant along with a payment intermediary (the NetBill server) are involved in the transaction. The NetBill server is actually a third thrust party which communicates directly with the merchant, and through him, indirectly with the client. The exchanges can be observed in Figure 6.

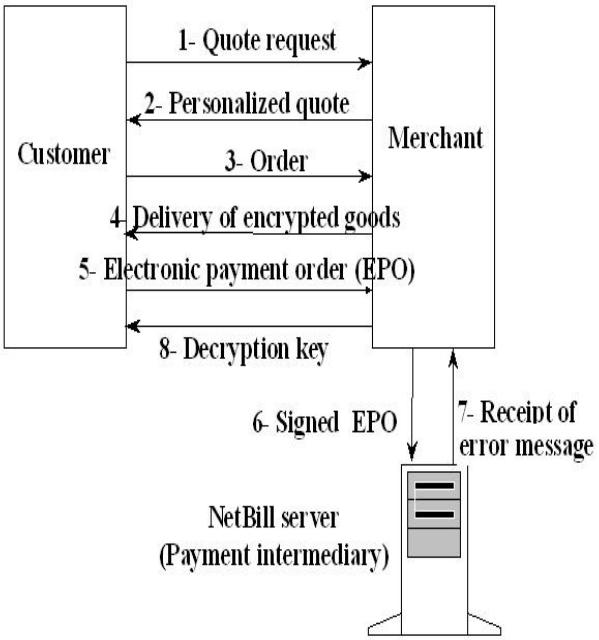

Figure 6. NetBill

Although NetBill has a lot of potential like the managing of the electronic order, the encryption of the information and the fact that the decryption occurs only after the payment has been made, this system's performance is reduced by the frequent use of digital signatures and the number of transactions which can take place simultaneously is limited by the server's technical specifications.

KLELine

The electronic micropayment system KLELine was buit from three main elements: a platform for securing the payments, a virtual store and also a payment system named Global ID, under a bank's management which handled the economic exchanges. KLELine used many payment instruments: a virtual purse (recharged from a bank account) for purchases less then 15$, a bank card for purchases of over 75 $, and for values between 15 $ and 75 $ you could have chosen whatever method you preferred. Over 183 currencies where supported and the exchange rate was updated every 6 hours. For every trasaction KLELine deducted its commision

The client received a personal identificaton number (PIN), a client identifier (CID), a software named Klebox or PACK

(Personal Autenthication and Confirmation Kit). The software was actually a plugin of the browser, which granted access at the virtual purse. The customer had to use his PIN in order to identify himself to the server. The security of the exchanged messages was assured by a pair of 512 bits RSA keys. The merchant's kit named SACK (Server Authentication and Certification Kit) was securing the communication with KLELine by using asymmetric encryption with certification and assured the offer's customization depending on the user's profile, received and logged the receipts and also updated the exchange rate.

The KLELine server was in the same time an intermediary between the customer and the merchant, assured the communication between the banking network and the Internet, a third trusted party, a virtual store, and also guaranted the confidentiality of the client's banking details.

The different phases of the transaction, including the payment, were described in the CPTP protocol (Customer Payment Server Transaction Protocol). The transaction was composed from different stages as depicted in Figure 7.

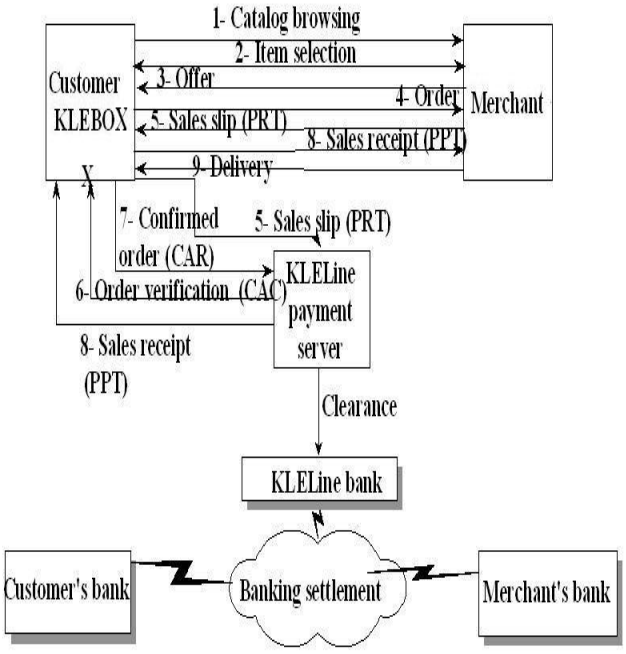

Figure 7. KLELine

KLELine used public key encryption using the RSA algorithm with a key length of 512 bits, MD5 hashing, and a symmetric unspecified algorythm for the merchant's authentication and the messages integrity.

KLELine didn't assure anonymity because all transactions were being logged and so the identity of the client was revealed. Many elements of the CPTP protocol have not been made public (for example we do not know what was the meaning of the signature, what exchanges where encrypted with the session key or what was the algorithm used), so we can't completely evaluate this system.

From the ashes of KLELine a new electronic micropayment system was born, Odysseo, wich supported multiple cards and currencies. In contrast with KLELine, Odysseo didn't require for the client to make use of dedicated software. When it comes to client authentication, KLEline uses the RSA algorithm with a key length of 512 bits, while Odysseo is basing it's infrastructure on public key encryption algorithm whose key-length is unknown. Regarding the security protocol KLEline used a proprietary CPTP protocol which hasn't been released to the public, and Odysseo used 128 bits SSL. While KLELine couldn't assure nonrepudiation, Odysseo is assuring it through the use of time-stamping.

MicroMint

MicroMint is an electronic micropayment system developed by Ronald R. Rivest si Adi Shamir, and the economic value is represented by tokens called Micromint coins. They can be validated very easily as they include a sequence of bits but their production is very expensive. The more coins are produced, the more will the unitary price decrease and the cost of their counterfeiting will be unprofitable. The necessary computation loud is greatly diminguished because it avoids the use of public key encryption. The exchange of coins can be observed in Figure 8.

MicroMint coins can be purchased from a broker by means of banking payment (credit cards, cheques, etc). The broker, which acts as an intermediary in the transaction, keeps track of all the coins he sold.

Because the security mechanism's costs are very expensive, they focus on systematic frauds. Forging of the coins is not profitable because of the small values which are exchanged and the fact that new coins are minted periodically.

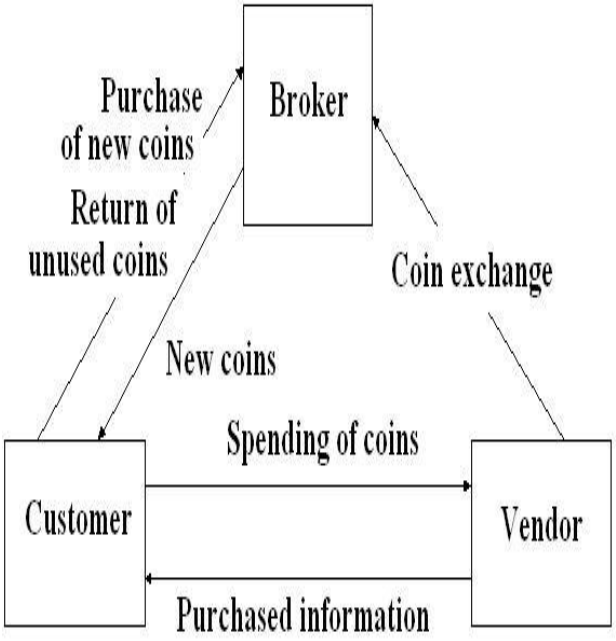

Figure 8. MicroMint cycle of coins.

The security measures include: a monthly change of the validity criteria and the broker produces new coins a few months before putting them on the market, which makes their forging more difficult. If the MicroMint server is hacked an extreme measure is taken, all the coins are withdrawn from the market and replaced with new ones.

4. CONCLUSIONS

The first generation micropayment systems that were discussed above are compared in Figure 9. Although extremely ambitious from the technical point of view, the first generation remote micropayment electronic systems proved to be unrealistic when they have been implemented, so the need for new remote electronic micropayment systems has arisen. From the technical point of view, these systems were supposed to be as simple as possible and not to request the client's details each time a transaction has occurred. This has been the starting point for the second generation remote micropayment systems: prepaid card-based systems, e-mail and Minitel like systems.

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

Figure 9. Comparison among a few systems of remote micropayment

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] Mostafa Hashem Sherif – **Protocols for Secure Electronic Commerce**, CRC Press, US, 2004

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

[5] Alexandru Pirjan, "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.

[6] Susan Hohenberger – **Phd Thesis, Advances in Signatures, Encryption, and E-Cash from Bilinear Groups**, Massachusetts Institute of Tehnology, 2006.