SECURITY OF INTERNET PAYMENTS

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

Abstract: *Recently, with the increasing availability of Internet, E-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 spoken about the Digital Economy (DE - Digital Economy). 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 conducting business activities. One of the main goals of e-commerce strategies is to identify and encourage users of information via the Internet, giving them the necessary support. Electronic commerce offers the ability to run a business in a flexible manner that can benefit from the various opportunities as they arise.*
But bear in mind that the introduction of 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.

Keywords: electronic payment system, transaction, access control, digital signatures;

Jel codes: A12, F02, G23, G35;

1. The structure of an electronic payment system

Electronic payment systems can be viewed in a hierarchical tiered system architecture derived from OSI-ISO. An architecture level contains a set of objects that cooperate in order to provide services for the upper level. To achieve this objective, use of the services provided immediately below. An EPS consists of two levels: user, which is higher hierarchical level, and system level, which is lower hierarchical level.

A whole people using EPS - called generic users - are grouped into roles, the way it interacts in business relations between them. For example, typical roles in such a system are the buyer, the seller, the issuer of electronic money (the bank). Users, playing different roles, issue commands and responses in the dialogue process at the access points of an EPS. These dialogues are transactions - for example, getting cash from your account, make a payment or deposit of electronic money in a bank.

Level system consists in the set of physical entities and the relationships established between them. By entity is a device (electronic), seen as a whole hardware and software, and playing one of the following roles: bearer of electronic money or cash book. Devices that implement

these functions are in order, electronic wallet (e-wallet) and point of sale (Point of Sale - POS). EPS in a real interaction takes place between electronic wallet - which implements the bearer of electronic money the buyer (usually a smartcard) and POS - implementing the vendor's cash register.

In summary, an electronic payment system can be defined as a set of transactions required by:

- convert the money cash (or cash account) for electronic money and vice versa;
- electronic money transfer between users of this system.

To make payments in EPS, the buyer must withdraw from his account, the issuer real money (bank), a certain amount he deposits into his account, an issuer of electronic money (bank Internet) - stream 1. In particular, the two roles mentioned, issuers of money, can be played by the same bank. As a result, the buyer can withdraw electronic money based on real money deposited in the account - electronic money flow 2. These can be used in a payment transaction, the buyer pays the seller's goods or services - flow 3. The payment transactions diminishes the value of electronic money stored in the carrier and the corresponding increase in the cash value of the seller. As a result of a payment made, the seller transfers the goods or services the buyer - flow 4. From time to time, the seller deposited the proceeds of their electronic money issuer - flow 5, which he put in the seller's account equivalent amount in real money - flow 6.

2. Devices used in electronic payment systems

1. Electronic wallet is the implementer of a bearer of electronic money. It is used by the buyer for storing electronic money. The structure depends on hardware cryptographic protocols that implement EPS transactions, the most common configurations following principles:

- *A personal computer structure* - the user has full access to the device hardware and software resources. Architecture, typical of a PC with limited resources pocket calculator type (hand-held computer), includes: CPU (around a microprocessor 8 or 16 bits), RAM (from 256 bytes to 2 kbytes), 8- 10 kbytes EPROM, EEPROM 2-10 kbytes of which the device containing the secret keys must have access restrictions. The user interface consists of a keyboard and a display. Connecting to access points of EPS is usually via a serial infrared. This type of structure penalizes banks, restless user total control over resources payment device

- *A structure that is sensitive to opening called smart card*. This takes the form of a chip embedded in a plastic card. The difference between a regular credit card and a smartcard is shown in Figure "credit card and smartcard". A typical smartcard comprises an 8-bit microprocessor (the most commonly used being from Motorola and Intel 80C51 68FC05), 256-512 bytes of RAM, 8 kbytes EPROM 8 kbytes EEPROM. Communication with the access point is through direct contact with a card reader. The user has access to the hardware and software resources, which favors banks. Security of such devices are based on assumptions made on cryptographic protocols and the impossibility of "openness" SmartCard and perform a "reverse-engineering" of its software. Smart cards are rapidly evolving architecture. Latest achievements of smartcard implements a 32-bit RISC processor that GemXpresso RAD (Rapid Applet Development) presented in Paris in 1997 by Gemplus company, which can provide Java card (www.gemplus.fr/). Also, it should be noted MC68HC05SC49 Motorola microcontroller, dedicated applications that use public key cryptography co-processor that integrates a modular arithmetic.

❖ *Electronic wallet type structure* with cumulative benefits of earlier structures observer reaching a compromise between the bank and the owner's interests. Device architecture includes two microcomputers communicating on during the transactions. The first microcomputer, the user - called Purse, has the task to communicate with the access point of the EPS. He is actually shaped like a pocket PC with keyboard and display. The second microcomputer - called observer or by abuse of language, smartcard, serves the interests of the bank. It is inserted into the first computer. While the computer allows the user to control the fairness of transactions, the computer observer prevents double spending of electronic money, endorsing each transaction made by the first computer.

2. Point of sale (POS) cash register implements, which is the entity that temporarily stores - the seller - electronic money. The device is made from a technical point of view, as a PC-type structure having both a serial link interfaces to the infrared reader and a smartcard.

3. Distributor of electronic money is the device through which electronic money charging electronic wallet buyers. Implementation of technical solutions used to recall:

❖ *Distributor account electronic money solution* that allows incrementing the value of the wallet, based on the withdrawal of a real money account opened by the buyer. The organizer has an infrared or serial link smartcard reader, the networked computers serving various banks issuing electronic money.

❖ *Distributor credit-card electronic money* solution that allows incrementing the value of the wallet, on lending by a home buyer credit. The organizer has a reading device for the credit cards (magnetic) buyers. Also, there is an infrared channel for connecting smart card and wallet. In this case, the distributor must not be networked with computers banks.

❖ *Distributor-cash electronic money wallet* solution that allows increment value from the buyer based on the collection of an amount in cash.

3. Transactions processed in an electronic payment system

User-ID transactions allows an entity to verify if a user at the other end of the connection is really the one who pretends to be. It is a preliminary stage for a "conversation" later. They are using protocols based on public key cryptographic algorithms. Recall that in these criptosisteme, each entity has a pair of the public key and secret key. A user P, called evidentiary, that made known public key can be identified before any other user V, called the verifier. V creates a random challenge message you send as a cryptogram, encrypted with the public key P. It's using the key to the secret, restores original shape of the challenge then send clear V. If the return value is identical to that originally sent, then V is convinced's true identity P. obtaining the public key of P by V is based on the transaction will be set forth below for obtaining certificate from center certification will sign its own secret key public keys to authorized users to use the system. The message format of the public key of P and signature associated center, is called public key certificate or simply certificate.

The transaction for obtaining a certificate. All public keys used in EPS for digital signature and the identification protocols are certified by one or more certification centers. The solution used to authenticate users to the center consists of public key signing with user-specific information using the secret key for this purpose center. Information assigned to a user and used during the transaction identification are called loans. A lot of credits, accompanied by their signature on the center, is referred to with the term of the certificate. Generally, these

certificates have a limited validity period so that entities involved in an EPS - if you are accepted into the system - must obtain such certificates periodically.

Access control transaction provides protection against unauthorized use of entities in the system, by checking that any user who, through an access point, try to access the entity plays an appropriate role. The protocol is started by the user who sends the information to the entity-level identification system that wishes to access. Level system analyzes user belonging to the role that verifies claims and rights with respect to access to this role. The result of the review enables user access to the system or not. This transaction access control can be used in monitoring operations, a user playing a certain role requires an entity at a specific information system. For example, a user on the buyer may want to know which is the amount of money that she possesses electronic wallet.

The charging transaction is conducted between the bank and distributor. Upstream of the transaction itself, the two sides carried out a mutual authentication, consisting of one transaction of mutual identification. The transaction is triggered by the bank issuing the message "transfer sum s" at the distributor responds with a confirmation message "received the sum s". If successful conclusion of the transaction, the system confirms that an amount s. The transaction may fail if, for example, the amount claimed exceeds a ceiling set by the bank if the amount claimed exceeds the account balance buyer requesting uploading or if one of the two devices physical at both ends (or line) is defective.

The withdrawal transaction involves the dealer and buyer. In this case the actual transaction is preceded by mutual authentication entities. Then, the distributor sends the message "transfer sum s" to the buyer responds with the message "received the sum s". In this case, the buyer obtain electronic money s worth, following an advance bank transfer, by providing direct cash or credit cards. The transaction may fail if: the amount requested by the purchaser exceeds the limit that can be loaded into the electronic wallet; amount requested exceeds the account balance or value buyer with real money bank introduced; devices at the two ends or the link between them is defective.

Payment transaction takes place between buyer and seller. There payment transactions offline or online. At the online bank is involved. The transaction is initiated by the seller, which require purchasers sum s. If it agrees, sends a message to "pay the sum s", which the seller confirms the message "received the sum s". The failure of such a transaction can be either because the buyer does not have enough money, electronic or communication devices or failure of them.

The cancellation transaction refers to the last payment transaction between buyer and seller. It is intended to correct some errors committed by the human operator in connection with the payment transaction in progress, such as typing the wrong amount of payment.

Deposit transaction involves the seller and collector. It is started by the seller by texting "transfer sum s" followed by confirmation by the message Collector 's amount received. " Possible failure of the transaction can be either because the seller does not have enough cash to electronic cash registers to cover the second or defects of the devices involved.

The clearing transaction takes place between the collector and the bank or between two banks. Is initiated by the entity transferring the money through a message like "transmit sum s". Once the bank receives money, acknowledge receipt thereof by the message "received the sum s". The transaction may fail if the electronic money transfer or bank collector are not accepted by the bank that receives them.

4. Digital signatures

Among its many applications, digital signature underlies the security of smart cards. Unlike a handwritten signature that identifies the sender, digital signatures provide a means of ensuring the integrity and content of the electronic message received.

Digital signature is a small amount of data stored on electronic media which are transmitted with the message. It is produced by certain calculations made by the transmitter based on a content key and the message. This process is called function signature. At the reception, through a check function, is another set of calculations on the signature and message, finding or signature validity.

There are some parameters in these calculations - called keys - which varies from one signature to another and which are specific to that which produces signature.

Production of digital signatures can rely on criptosisteme both symmetric and public key ones.

Digital signature methods based on traditional key systems (symmetrical) both use the same key signature and verification. Figure "Digital signature symmetrical systems" illustrates this process. In the function signature, the message M is signed using the secret key as a parameter. Verification using the same secret key and the clear message is valid or invalid verdict of the received digital signature. The disadvantage of this method is the need to establish and distribution prior to the secret key between the transmitter and receiver. Figure 4

Digital signature public key (asymmetric), illustrated in Figure "Digital signature public key" secret key used to sign the entity transmitter (Dent) and the verification of its public key (Eent). As a result, a signature can be produced only authentic transmitter, which alone knows the secret key, but it can be verified by anyone who knows the public key of the transmitter.

1. Creating digital signatures - In electronic payment systems (EPS), digital signatures are made by a slightly different procedure. First, if they use a symmetric cryptographic system would risk exposing secret key verification, which must be stored in the equipment vendor. Therefore, this equipment must be protected with a protection mode key that can be controlled only from the vendor. Therefore, public key systems is preferred that the terminal only has to store the public key. But these systems creates problems in EPS because the calculations require a fairly large volume, which are slow on a device with low computing power, such as smart card (smartcard). In addition, the smart card at risk exposing secret key that is stored.

Signing function - in this case called signature transport - it is divided into two sub-phases (Figure "Digital signature by signature concept of transport"):

- First, pre-signature, the signature intensive creation occurs once outside the smart card; outcome of this phase, specific Card and its owner, is then transported and stored in the smart card;
- second, completing the signature which requires modest resources, is in the smart card and is dependent on the signed message.

2. Using digital signatures - An alternative use of the concept of transport of the signature, if EPS is explained in Figure "Taking the concept of transportation public key signature to checks". Smart card provider, usually the bank, creates pre-specified signature of a person through a process off-line. It is as if the bank would give some white person's electronic checks. For their creation, the Bank uses the key to the secret and then stores them on the card. During a payment transaction, the card turns into a complete check with the payment

amount. Then the seller at his terminal, the check verifies the signature with the public key of the bank's key that is stored on his terminal. Company DigiCash (www.digicash.com/) has developed a technique for compacting hard that can be stored in nonvolatile memory card (1K EEPROM) hundreds or even thousands of checks.

Another option for using smart cards with public key systems is based on the concept of money transport (Figure "Taking the concept of public key signature transport the coins"). In the card balance is a counter which can be incremented by the bank. When the buyer makes a payment card, the amount will be signed (coins) with secret key exists on the card. Because the card has two sensitive information - balance value and the secret key - it must be resistant to opening. The seller through existing in-store POS terminal will verify the authenticity of coins, using the public key. Safer transport systems based payments to electronic money have a great future.

5. Schnorr signature system

Cryptographic parameters of this system are as follows:

- a prime integer n 512 bits;
- a prime integer number of 140-bit q such that q divides (n-1);
- a generator g order q modulo n used by users so that GQ mode n = 1;
- a generator G of order q used by the bank in carrying signatures so that G q = 1 mode n.

All arithmetic operations are executed in Abelian group of order q, Gq, with the operation of multiplication modulo n. System parameters are generated by a central authority that knows the value Loggia G or loggia g. The other parts of the system - the bank, the buyer and seller - I do not know this value.

EPS keys used are:

- (s,p) - public key pair secret key that is used for smart card electronic wallet of the buyer (evidential);
- (S,P) - public key pair secret key used by the bank (checker).

Keys check the following equations:

$$\mathbf{p = g^s \bmod n}$$

$$\mathbf{P = G^S \bmod n.}$$

Schnorr's identification scheme - is based on a protocol that runs between evidential and checker Ve Pr. S is the secret of Pr, he wants to prove in a manner called "zero-knowledge" of Ve. It has public information mode n p = gs, which is the public key of Pr. Here's the reliable identification of evidentiary protocol by the verifier:

1. Pr randomly pick a value w ZQ on which calculate the so-called "original control":

$$\mathbf{a = g^w \bmod n,}$$

forward it to the checker:

Pr---->Ve : [a]

2. Ve choose a random integer c of ZQ ("Challenge") which transmits Pr:

Ve----->Pr : [c]

3. Pr calculates the answer r to challenge

$$r = w + c*s \bmod q$$

using secret key to the response, which sends it to the verifier:

Pr----->Ve : [r].

4. Ve calculated "final witness" to a'

$$a' = g^r p^{-c} \bmod n,$$

the reply r, to challenge c and public key of Pr. Pr identification is acceptable if a '= a mod n, which certifies that Father used the key to the secret, known only to him.

A numerical example will simplify the understanding of the scheme. Whether the following parameters:

- How it works module n = 88667,
- module q = 1031, factor prim al lui (n-1),
- security parameter t = 10, so $q>2^t$.
- element g = 70322 is of order q în Z_n.
- keys evidences Pr:
- secret exponent (secret key), s=755;
- public key p, calculated a little differently than the submission method (solution prepared in practice) is:

$$p = g^{-s} \bmod n = 70322^{1031-755} \bmod 88667 = 13136.$$

For identification, let's say that Pr probative will choose a w = 543, which will be calculated based on the original witness:

$$a = g^w \bmod n = 70322^{543} \bmod 88667 = 84109 ,$$

which will send to Ve. It selects a challenge, for example c = 1000, provided 1 <= c <= 2t. Pr probative r will calculate the answer to the challenge, using the key to the secret and that only he knows:

$$r = w + c * s \bmod q = 543 + 1000 * 755 \bmod 1031 = 851 ,$$

that it will send to verifier Ve. This onewill make the final check, on which identifying verdict:

$$a' = g^r p^c \bmod n = 70322^{851} * 13136^{1000} \bmod 88667 = 84109 = a.$$

Therefore, a = a' and identification is successful.

Schnorr signature scheme - Based on published Schnorr identification protocol, has built a digital signature scheme protocols used in electronic payment systems. Is replaced with the result of the challenge c functions Summary (hash) H, the concatenation message applied to "witness initially." The digital signature is composed of the pair of integers (r, c), where r is the response, and c is the initial challenge. Verifier constructs "final witness" and final challenge is calculated by applying the function H concatenation of message signed "final

witness." The signature is accepted if the final challenge has the same initial challenge. Signature scheme is as follows:

- signatory of the message randomly choose an integer M w ZQ, on which calculate the so-called "original control":

$$a = g^w \bmod n.$$

Then calculates the initial challenge c:

$$c = H(M,a)$$

and with the secret key, known onlyby him, response r*:*

$$r = w + c*S \bmod q$$

This information is sent to the verifier

$$Se\text{----->}Ve : [M,c,r]$$

2. The verifier calculates "final witness" to 'a'

$$a' = g^r P^{-c} \bmod n$$

and the final challenge

$$c' = H(M, a')$$

based on the reply of r, the initial challenge c and public key of Se. Se's signature is accepted if c = c mode n.

6. The electronic payment system CAFE

Given the importance of the field, 1994 was declared as the "International Year of the Electronic Wallet".

The project, called CAFE (Conditional Access for Europe) has been developed within ESPRIT European research project, launched under the European Community funding. In it are geared strong industrial companies in computers (DigiCash, Gemplus, Ingenico, Siemens), research institutes in the field of cryptography (CWI Amsterdam, PTT Research in the Netherlands) and universities in many European countries (Arhus, Denmark, Leuven, Belgium Hildesheim and Karlsruhe, Germany). Work on CAFE started in December 1992 and is the renown David Chaum cryptography researcher at CWI of Amsterdam. The overall project goal is to develop new CAFE conditional access systems, such as access to buildings, access to confidential data or electronic payment systems.

CAFE basic device is a so-called ***electronic wallet***. It is a small pocket computer, battery powered, keyboard, display and infrared communications (Figure "electronic wallet"). Each user has his own computer, managing his rights and guarantee the security of transactions.

From a functional perspective, CAFE is a payment system offline:

- user must load electronic wallet with money from the issuing institution (eg a bank);
- during a payment is not necessary contact with a central database of a bank.

- The system was designed to make payments in POS terminals from electronic wallet. This means that the deposit paid to perform subsequent electronic money issuing institution, to get real money. CAFE wallet system can store electronic money in different currencies, that to change during payments. CAFE system uses two ways of payment:
- by electronic money - which, however, may have different values and can be divided, allowing multiple payments until your deposit is empty (for example, there is a wallet deposit of 8 euros which can be spent in several tranches, multiple 1 Euro);
- by check - to be completed and signed by the buyer device, within a meter of money saved by it and is regularly uploaded to the bank.

CAFE system based on the following initial requirements imposed on security:

- it is absolutely impossible to spend electronic money several times since the devices used are resistant to opening;
- if a device resistant to opening was "broken" electronic money users spending more than once are identified and fraud can be proved.

The main difference between CAFE other EPS systems is the very high safety standards involved in this system. Security objectives envisaged in the project CAFE we here underline the following:

Security of all stakeholders in the system - All other EPS systems that are designed based its security on only one side - the broadcaster of electronic money (the bank); all participants in the system confidence in the bank, whose security measures must guarantee security of the entire EPS. CAFE has incorporated security measures that each party has guaranteed security requirements without having to have total confidence in the other. In particular, it is necessary mutual trust between two parties whose interests may conflict (eg bank and customers). Each party must have confidence in the devices you use (or wallet POS); even if you can not verify the correctness of their operation in detail, this can be done by independent authorities (eg consumer organizations). Also, each device hardware and software should be free for inspection by the authorities designated by the other party. System security is based on assumptions cryptographic protocols used and not on these algorithms secret.

Data protection - CAFE payment system is designed for daily payments, of little value, such as shopping, mobile, transportation. Had they used credit card company that issued the card could result in extensor profile of all user movement, which is not desirable, affecting the privacy of information about individuals. Therefore, was required to CAFÉ the need of anonym payments, which led to a system of identification cryptographic protocols. For example, it has been determined that - for all lower payments that Euro 2500 - not be necessary to identify the customer, but for higher expenses. In contrast to payments, the withdrawal of electronic money from the bank and deposit requires the identification of users via cryptographic protocols, by the bank.

Tolerance to loss and failure - From the users' point of view, if they lose a electronic wallet or can't be used due to defects tolerance is that they get money back from the institution that issued the wallet (the bank). It takes the necessary measures wallet that can no longer be used by anyone, even if he knew identification code (PIN).

Let us now consider the technical solutions that are used in CAFE system to ensure implementation of these security objectives.

Digital signature scheme - This technique is used to ensure the safety of all parts involved in the system. In this case, each message must be signed by the legal significance that it has created. For example, wallet sends requests to withdraw the protocol signed by the bank. As a result, the information present in memory devices for signature must be kept secret and should not be accessible in reading. Signature scheme used is based on the algorithm of Schnorr. Payment systems where the payer can not be identified (remain anonymous) use so-called blind signature scheme. It is a protocol between two parties signatory and receiver. As a result of protocol, the receiver get a message signed by the other party. The message is unknown for signatory, but it guarantees its original form; therefore signature is called "blind". The typical use of blind signatures in payments is as follows: electronic money are represented by a message of some form signed by the bank. During protocol withdrawing electronic money, bank device makes a blind signature on the message that represents electronic money without them knowing but content. Therefore, later, after the money was spent and executed protocol for submitting them by the seller, the bank recognizes only valid signature can not determine who the buyer who made such payments.

Ensemble wallet-opening observer resistant devices - Each wallet has an observatory that is placed inside the wallet, where it can eventually be changed. The Observatory is a crypto-processor Siemens, which can not communicate directly with other devices (POS or the charging wallet with money); All communications are done through computer-wallet, the user trusts. The wallet protects the interests of the user who checks all the messages it emits or receives observer. The Observatory represents the interests of the bank, because you can not make any transaction without cooperation. No payment is accepted without the signature of the observer. The electronic wallet pocket computer with a keyboard and small display. Observatory and is mounted on a smartcard is inserted in your wallet. Centre may communicate directly only with his wallet when he communicates with the outside world via infrared.

Cryptographic protocols to detect fraud - As mentioned, CAFE is a payment system offline. Buyer's identity is encoded in the message containing electronic money. When they are used in a payment process, the purchaser must disclose parts of coded identity to the buyer. If the same money is used in two payments, the buyer will disclose two different parts coded identity. The code is constructed in such a way that, starting from the two sides disclosed, one can determine the identity of the buyer, which can be achieved using a single hand. For example, I believe that identity is encrypted with a cipher coating (one-time pad - Charge modulo 2) using key P. Money contain two parts: the identity encrypted, IL key P and P. Both are, however, hidden by -a encryption scheme C, so that the money actually contain two chips C (H W P) C (P). At first payment transaction opens a single chip, IL P or P. None of them says nothing about the identity of the payer. Only if the offense is committed paid twice - by opening and the second chip - it can determine the user's identity. To detect such actions paid twice the Bank must retain for a certain time deposits all electronic money. If there is double deposits, based on the two chips is open immediately the identity of committing fraud.

Loss tolerance is very important to users. This means that if they lose the electronic wallet, they get their money back. The basic idea is to retain somewhere outside the wallet, the user save money encrypted form. If he loses his wallet, money is valued cooperation copy the user's bank. Money is thus rebuilt, less the amount already spent and credits the user's account. The values can be determined by comparing spent rebuild deposits money deposited in the bank.

To prevent the use of electronic wallets lost by unauthorized persons, there are two values PIN (Personal Identification Number) protections. One is required to use the wallet, another should be known for accepting payments.

CAFE project was designed in two phases: the first, which ended in mid-1994, were done market studies and sociological studies were completed cryptographic protocols and technical solutions. In the second, after 1994, it began implementing hardware components: Gemplus company and wallets made of smartcards with cryptographic processors produced by Siemens. In parallel, work on studies on user reactions to these payment systems and the development of other access control systems based on wallets and observers.

7. An example of an electronic payment system

Electronic payment system to be introduced is built on the scheme Identification / Schnorr's signature, public key cryptographic method that uses discrete logarithms complexity of calculation. Detailing, as some mathematical principles underlying the system was already protocols will present the cryptographic functions in a symbolic manner, apart from mathematical calculations that are behind them.

We note with $\mathbf{E_{ent}}$ public key of an entity (buyer - C, V or bank seller - B) and $\mathbf{D_{ent}}$ secret key pair. As a result, undertaken by an entity's signature on a message M, the secret key whose sole owner is, is as follows:

$$\mathbf{S = D_{ent}\ (M)}$$

Signature verification requires them to do any entity using public key of the signer:

$$\mathbf{M =? E_{ent}\ (S) =? E_{ent}\ (\ D_{ent}\ (M)\ )}$$

Understanding of specific protocols for EPS's presented, will specify some notations used:

- meter - is the current balance of the buyer, as embodied in the wallet;
- sum_r - is the amount required during the transaction the bank withdrawal;
- max-meter - is the value of a single limit on bank withdrawals (to reduce damage when losing smartcard and PIN guess finder);
- sum_p - the amount that is payable in the transaction payment (and it is limited for reasons of reducing the damage in case of loss or theft smartcards);
- date - is the date of the transaction;
- C, V, B - identifiers purchaser (a smartcard his site), the seller and, respectively, of the bank.

Once the buyer loads his "wallet" of smartcard (1.A) and withdraw a number of blank checks from the bank (1b) can make purchases of goods or services that will be paid through the card's (2). The seller, after obtaining a completed electronic check from the buyer (2), shall deposit in the bank (3) to be credit your account. Bank between seller and buyer then carries out a transaction clearing, resulting in debiting the buyer.

7.1. Protocol withdrawal of electronic money

In this protocol, withdraw electronic money from the bank to charge a particular smartcard. The process is in two stages: the withdrawal of an amount of money and of checks from the bank account withdrawal.

1. a. Withdrawal of money from the account - At this stage the bank and the buyer executes a mutual authentication process, after which the meter's smartcard (the buyer) is transfixed corresponding amount withdrawn. Exchange protocol consists of 3 signatures (using Schnorr's scheme):

❖ The first signature is executed by the bank to persuade smartcard that dialogues with the bank, whose client is and who is only allowed to "see" the contents of electronic wallet. To prevent an attack by replay old messages and recorded, every new Protocol smartcard choose a *random value*, which is included in the signature.

❖ A second signature is executed by the smartcard, for identification to the front of the bank and to provide the correct information (genuine) on the value meter. In this case, the replay attack is avoided by including the message signed earlier part of the bank's signature. Together with signature smartcard specifies the number of checks (no) that wants to draw in what was the second phase of the protocol of withdrawal. It also will identify C, information that will allow the bank to draw from its database to the public key of the smartcard.

❖ The third signature is executed also by the bank. Thereby authorizing the smartcard operating system's meter to alter the amount requested. To avoid a replay attack, the bank signed message includes a signature component of the previous smartcard community. The entities involved are:

The buyer (through its smart card), denoted C

holding:

- Secret key – public key pair (D_C , E_C) used by the smartcard;
- BC bank ‘s public key (banca lui C), E_{BC}*;*

knows:

- counter - current counter value of the wallet;
- nr - the number of checks that are extracted;
- sum_r - amount requested (typed) by the buyer.

Buyer’s bank, notedBC

*behold*s:

- public key of the smartcard's buyer, E_C*;*
- secret key – public key pair (D_{BC} , E_{BC}) used by the bank;

knows:

- max_contor - the maximum allowable for the counter wallet;
- count_value (C) – every buyer’s card (smardcard).

Next, this protocol is detailed.

Step 1. Buyer’s smartcard-ul identifies the bank

Smartcard buyer chooses every transaction, a whole different random value m, which transmits to the bank:

$$\mathbf{C \text{ ---> } BC: [} m \mathbf{]}$$

The bank also choose, for each transaction, a whole w and calculates message's signature consists of two random values concatenated:

$$\mathbf{S=D_{BC}\,(m,w)}$$

That sends to the buyer's card:

$$\mathbf{BC \text{ ---> } C : [w,S]}$$

Buyer's smartcard identifies the bank signature with its public key by checking the value of m generated and received w:

$$\mathbf{m,w =? E_{BC}\,(S) =? E_{BC}\,(\,D_{BC}\,(m,w))}$$

Step 2. Authentication buyer to the bank

Smartcard buyer randomize every w transaction and calculates its own signature to the value on the card counter:

$$\mathbf{S= D_C\,(counter,nr,\ sum\_r,\ m,w)}$$

sends that to the bank:

$$\mathbf{C \text{ ---> } BC: [\ C,\ counter,\ nr,\ \ sum\_r,S]}$$

Bank seeks its database value public key of C, E-commerce, and authenticates with the buyer's signature:

$$\mathbf{counter,nr,\ sum\_r\ ,m,w =?\ E\text{-}commerce\ (S)}$$

then checking the legality of the withdrawal amount from the account:

$$\mathbf{counter + sum\_r\ ?<=\ max\_counter}$$

$$\mathbf{value\_account\ (C)\ ?>=\ sum\_r}$$

$$\mathbf{value\_account\ (C)\ -=\ value\_account\ (C)\ -\ sum\_r}$$

Step 3. Bank signs the amount requested for withdrawal

Bank randomize every w transaction and validates payment calculating signature to

$$\mathbf{S= D_{BC}\,(sum\_r,w)}$$

sends that card:

$$\mathbf{BC \text{ ---> } C : [\ sum\_r,\ S\ ]}$$

Smartcard buyer checks the payment:

$$\mathbf{sum\_r\ ,\ w =?\ E_{BC}\,(S)}$$

If the test is OK, it will increase the meter card:

$$\mathbf{counter=counter\ +\ sum\_r}$$

1.b Withdrawal blank checks from the bank - At this stage, after incrementing counter made of smartcard purchaser withdraw from the bank a number of blank checks (blanks). It's like a smartcard would withdraw "receipt book" containing several checks. In fact many checks retire until you've regained the maximum number smartcard, replacing checks

consumed in previous payments. The idea of the protocol is to obtain a signature from the bank, with the key to the secret DBC, the public key of each ECEC each blank check:

$$\textbf{Blank\_check} = [\ D_{BC}\ (\ \textbf{E-commerce}_{ec}, C\ )\ ]$$

It should be noted that the public and secret key pair (ECEC DCec) are different for each check. Also, each signature using DBC, the secret key of the buyer's bank. It details the withdrawal phase of the protocol, which is repeated for each blank check to banks

- **Buyer** (Smartcard), noted C *holds* **bank's public key E_{BC}**
- **Buyer's bank,** noted BC *holds* **secret key – public key used by the bank: (D_{BC} , E_{BC})**

Step 1. Buyer's smartcard ECEC calculated public key of the check - Choose a random value to each transaction and calculated according to this public key ECEC of the check, the bank and then sends that DCec secret key, which it conceals. The public key, together with the identity card is sent to the bank:

$$C \text{ ---> } BC : [\ C\ ,\ E_{Check}\ ]$$

Pasul 2. Bank signs the check's public key

$$D_{BC}\ (\ E_{Check}\ ,\ C\ )$$

Pasul 3. The bank sends the check blank, signed, back to smartcard

$$BC \text{ ---> } S : [\textbf{Blank\_check} = [\ D_{BC}\ (\ E_{Check}\ ,\ C\ )\ ]\ ]$$

Pasul 4. Smartcard buyer checks the validity of the check with the public key of the bank EBC

$$E_{Check}\ ,\ C =?\ E_{BC}\ (\textbf{Blank\_check}\ )$$

and then stores the blank check.

7.2. Protocol for electronic money payment

In this protocol services or goods are paid with electronic money. It was seen that a check Blank_check is a public key certified by the bank, different for each check, the key may be associated with the buyer's identity secret key C. correspondent DChek is used for smartcards (on behalf of the buyer) for signature message that is payment transaction. The seller, the buyer has purchased a good or a service, in this transaction receives two signatures:

- ❖ public key certificate of the check, representing the bank's public key signature E_{Check} ;
- ❖ smartcard's signature on the message payment using a secret key D_{Check}.

These two signatures make up what we call a Complete Cheque, subsequently forwarded the seller's bank for payment with cash. Bank seller will check the validity of the two signatures determined whether or not the check has coverage.

The buyer (SmartCard), has stored*:*

denoted C

the blank Blank_check = [D_{BC} (E_{Check} , C)]

and *calculates:*

Public Key of E_{Check} on the DCec secret key, stored in the card

Seller, noted V

beholds:

sum_p - amount requested for payment

E_{BC} - public key of the buyer's bank.

Step 1. Buyer's smartcard calculates E_{Check} public key

Step 2. Smartcard buyer sends the seller, for authentication, a blank check

C ---> V : blank_check = [D_{BC} (E-commerce $_{ec}$, C)]

Step 3. The seller shall verify the authenticity of the check to his bank using public key and calculating public key of the E_{Check}

E_{Check} , C =? E_{BC} (Blank_check)

Step 4. The seller calculates and sends the transaction payment specification

Vendor's computer builds payment specification by linking the following information:

specification = sum_p II data II C II V

and sends it back to the buyer:

V --->C : [specification]

Step 5. Buyer's smartcard checks the possibility of payment:

sum_p ?<= counter

iar apoi, dacă inegalitatea este satisfăcută, decrementează contorul de bani:

counter = counter - sum_p

Step 6. Buyer's smartcard specification complete and sign the check payment using a secret key D_{Cec}. Then, the check is sent back to the seller:

C ---> V : [Completed_check = [D_{BC} (E_{Check} , C) , D_{Check} (E_{Check} , a, specification)]]

As shown, the check completed contains the bank's authentication of the public key and the signature on the card's payment specification.

Step 7. The seller verifies the signature of payment, obtaining specification in clear

a, specification = E_{Check} (D_{Check} (E_{Check} ,a, specification))

To prevent a person to deposit and cash checks that do not belong to himself, in the payment transaction also includes identity of the seller, C. To prevent attacks by replay old messages, the message signed by smartcard include a random number a.

In conclusion, a payment is as follows. Smartcard is inserted into the POS terminal vendor (actually a computer) that types sum payment sum_p. If the buyer agrees to this amount, it will generate an acknowledgment, then the message sent by POS announces smartcard that can trigger the payment transaction. Smartcard read from memory to a blank check, obtained by protocol and reconstructs the public key E_{Check} withdrawal of the check. Next, send your check smartcard C (blank) to the seller, because it would show authenticity. In the event that the verification is passed, the seller sends specification of payment transaction, including payment amount (sum-p), date, identity of the buyer and seller C V. All of this message is signed with the secret key of the check D_{Check}

3. Protocol for submission of completed checks

Under this protocol, the seller gets into account the amount for which the check was completed by the card purchaser. The seller starts the protocol by sending its identity to the bank and what is called V Invoice_payment (transcript). It contains the identity of the buyer, completed the check received from the buyer and concatenated clear message:

Invoice_payment= a , sum_p , data , C , V , [Check_filled]

Bank seller out the same checks on the authenticity of filling and check that the seller. The bank also checks if the check has not been submitted previously, ie if there is no database in a transcript with the same values, specification. If all these checks are successful, the seller's account is credited with the amount written on the check-p. Detailing this protocol to do next.

The seller, noted V

Holds memorised:

- filled check:

$$D_B (E_{Check}) ,(D_{Check} (E_{Check} , a, specification))$$

- invoice:

a , sum_p , date , C , V , [filled_check]

Bank seller, denoted BV

holds:

- public key - secret key pair used by the bank (E_{BV} , D_{BV})

Public Key EBC buyer's bank

Step 1. The seller send bank bill payment and check containing completed

V ---> BV : [a , sum_p , date , C , V , [filled_check]

Step 2. If the bank of the seller and buyer is the same:

The check's authenticity:

Public Key check is calculated in two ways: using the public key of the buyer's bank and then decrypted key:

$$E_{Check1} = E_{BC} (D_{BC} (E_{Check1} , C)) \text{ şi } E_{Cec2} = E_{Check} (D_{Check} (E_{Check} , a, specification))$$

- check whether the two are identical calculated

$$E_{Cec1} =? E_{Cec2}$$

Fairness check, comparing the data transmitted in the clear with the buyer signed:

$$sum\_p , date , C , V =? E_{Check} (D_{Check} (E_{Check} , a, specification))$$

Double deposit:

- searching the database if there is another transcript with the same value, specification.

- Otherwise, the seller's account is credited with sum_p.

Double spending: - searching if the database at the client C, there is another check with the same public key ECEC. If there is, the buyer made two payments with the same check. As a result the buyer's account is debited by the amount sum_p.

If the buyer and seller's banks are different, not through step 2 of the protocol and transaction clearing pass.

4. Clearing protocol

This protocol takes place between the buyer and the seller's bank, if they are different. It is transmitted by the buyer's bank for payment transcript, for it to debit the account of the buyer. The protocol is similar to the deposit previously.

Bank seller, denoted BV, has saved:

- Public key pair secret key used by the bank (EBV DBV)

- Public Key EBC buyer's bank

- Check completed:- transcriptul (factura) de plată ce se va transmite:

a , sum_p , date , C , V , [Check_completed]

Buyer's bank, noted BC holds:

- Public key - secret key pair used by the bank (CBC, DBC)

- Public Key Bank EBV seller

Step 1. Banca vânzătorului trimite băncii cumpărătorului factura plăţii, care conţine şi cecul completat Seller's bank sends the buyer's bank the bill payment, which also contains complete check

BV ---> BC : [a , sum_p , date , C , V , BV, [Check_completed]

Step 2. Buyer's banck checks

The authenticity of the check:

- Calculate the check public key using the public key of the bank seller and then decrypted key

$$E_{Check1} = E_{BC} (D_{BC} (E_{Check} , C)) \text{ şi } E_{Check2} = E_{Check1} (D_{Check} (E_{Check} , a, specification))$$

Check if the two identical keys are calculated

$$E_{Check1} =? E_{Check2}$$

Fairness check, comparing the data transmitted in the clear with the buyer signed:

$$sum\_p , date , C , V =? E_{Check} (D_{Check} (E_{Check} , a, specification))$$

Double submission:

- Searching the database if there is another transcript with the same value, specification.

- The seller's account is credited with sum_p.

Double Spending: if searching the database, the client C, there is another check for the same public key E_{Cec}. If there is, the buyer made two payments with the same check. As a result, the buyer's account is debited by the amount sum_p.

Of course the protocols that underlie the functioning of an electronic payment system based on electronic wallet, implemented in a smart card (smartcard) seem complicated their goal simply transfer money from one person to another, payments for goods or services. But we wanted to make this presentation in order to underline the complexity of cryptographic methods used, which only provides much needed security of such protocols. Where more and

more commercial transactions begin to be carried out through Internet, electronic payment systems are a vital component of the paradigm called generic e-commerce.

Bibliography

[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] Pîrcălab Alin Titus – Revista Informatica Economica nr.31/2007 – "Criptografie Clasică Precomputaţională"*;*
[4] Kotler, PH., (1999) – „Principiile Marketingului", Editura Teora, Bucuresti;
[5] Manole, V., Stoian, M., (2004) – „Marketing", Editura ASE, Bucuresti;
[6] Manolescu Gheorghe (1997) – „Moneda si ipostazele ei", Editura Economică, Bucuresti;
[7] Patriciu V.V., Ene-Pietrosanu, M., (2001) – „Securitatea Comertului Electronic", Ed.All, Bucuresti;
[8] Popescu Radu, Tudorancea Cristian, Berbec Florin (1998) – „Cardul instrument modern de plată", Editura Tribuna Economica;
[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] Pircalab Alin Titus (2008) – „Protectia bazelor de date" – Teza de doctorat – Academia de Studii Economice, Bucuresti;
[11] Sabau Gh., Nicolescu Ovidiu (coordonator) ş.a. (2001) – „Sistemul informational managerial al organizatiei", Ed.Economica, Bucuresti, ISBN 973 - 973 – 590 – 524 – 8, pag.488;
[12] 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;
[13] Sabau Gh., Avram V. (1994) – „Sisteme informatice în management". Ed. Metropol, Bucuresti, 275 de pagini, ISBN 973-562-024-3;
[14] 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;
[15] 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;
[16] Sabau Gh., Avram V., (1998) – „Sisteme informatice si baze de date". Ed. OSCAR-PRINT, Bucuresti, ISBN 973-9264-29-8, 371 de pagini;
[17] Sabau Gh., Lungu I., Surcel Tr., Sofronie Gh., ş.a.(1993) – „Sisteme informatice si baze de date". Litografia A.S.E., Bucuresti.