17

Cybermoney in the Internet: An Overview over new Payment Systems in the Internet

Rüdiger Grimm and Kambiz Zangeneh
GMD, Institute for Telecooperation Technology
P.O.Box 100138, D-64201 Darmstadt
grimm|zangeneh@darmstadt.gmd.de

Abstract

This article gives an overview over some of the most promising electronic payment systems: iKP, SET (as harmonization of Mastercard-SEPP and VISA-STT), Express, First Virtual, CyberCash, Ecash, CAFE, Mondex, Ravensburg's GeldKarte. We describe their technical and application aspects. We highlight the role of smartcards for their usage and their applicability for the Internet.

As an introduction to the overview, we present some theoretical considerations on digital money. We formulate critical requirements for digital money and how money can appropriately be expressed by digital means. We also discuss the problem of fair exchange of money versus goods.

Keywords

The Internet, digital, dual and blind signature, digital money, electronic payment systems

1 INTRODUCTION: REQUIREMENTS AND CRITERIA FOR DIGITAL PAYMENT SYSTEMS

Legally committed telecooperation over an open and insecure network like the Internet are challenged by yet unsolved problems. A particular problem of committed telecooperation is the secured transmission of money, let alone the fair exchange of "information for money" over an open network.

Buyers and sellers are connected as well as separated from each other through the applications of the open network. They neither see nor hear each other. They communicate by means of digital data which can be forged and bugged in the network. As a consequence, their communication is volatile, unprotected and not conclusive.

No security procedures have been established in the present standard technology of the Internet [ECMA 88, OSI 89]. Therefore, authenticity of telecooperation partners and integrity of transmitted data are not guaranteed. Consequently, there is no means against

P. Horster (ed.), *Communications and Multimedia Security II*

repudiation of communication. In particular, during sale transactions sensitive data is exchanged, which are not protected against unauthorized eavesdroppers.

How could then digital coins be protected against unchecked duplication or alteration? How could one rely on a promise for payment by cheque or exchange? How could the buyer prevent the seller from making off with the money before s/he supplies the goods, and how could, vice versa, the seller protect him/herself if s/he has supplied the goods to a customer who is unwilling to pay?

An obvious solution , which is already extensively used, is payment by credit card: the buyer gives his/her credit card number to the seller over the Internet, e.g. by E-Mail or a WWW form, as it is usually being done by phone, and the seller can subsequently withdraw the money from the customer's credit card. However, every credit card dealer who knows the credit card number can also withdraw money from the respective credit card in an unauthorized way. The Internet is less tap-proof than the telephone network. There are programs which filter credit card numbers out of millions of pieces of network data for the benefit of an interested eavesdropper. Electronic Payment in this way is unprovable, not anonymous, and there is no fair exchange „goods for money".

1.1 Requirements

New electronic payment systems have to satisfy these basic *requirements*:

R1: Integrity of money and data transfer

R2: Limitation and fair share of risks

R3: Support of autonomy and privacy of all participants

R4: Provability

R5: Robust communication infrastructure and robust local systems

R6: Legal acceptance

R7: Social acceptance

R8: User friendliness

1.2 Criteria

Electronic payment systems may fulfill the following *criteria* in different ways:

C1: *Type of value transfer*: credit (pay later), debit (pre-paid), or digital money (pay now)

C2: *Online* with the Internet or *offline* without direct access to the network

C3: *Communication media*: open communication network (Internet) or closed system (e.g., with the Kerberos authentication method [KER 88]); other examples: e.g. infrared rays, cards and card readers, wallets, etc. This implies *hardware requirements* like smartcards, Internet access devices, wallets, etc.

C4: Role of a coordinating *third party*, e.g. by a bank or a credit card system

C5: *Distribution of risks*: is any partner (buyer, seller, third party) able to gain on the cost of the other partners by unfair behavior? Do they follow the rule "first money, then good" or "first good, then money"?

C6: *Security measures* for privacy, anonymity, integrity of communication data (e.g. of the digital money), provability of actions. This may imply certain *cryptographic techniques* like digital signature, dual signature, blind signature, etc.

C7: Appropriateness for *micro payment* (cents, pennies); and appropriateness for *macro payment* (thousands of dollars or pounds and more)

C8: Appropriateness for *certain types of goods*, e.g., digital information, Internet services, physical delivery of goods

C9: Dependency on a *certain currency*, e.g., is there a free choice of currency, is currency exchange possible?

C10: Possibility of *spontaneous usage*: is it possible, for example, to perform a single purchase without an established seller-buyer relationship; is there a need for money exchange before any purchase; etc.?

2 FAIR EXCHANGE OF MONEY AND GOODS

In every financial transaction, it is important that the values change hands in a fair way: by giving away a good, the seller receives the equivalent of a payment. Vice versa, the buyer receives the good by providing the equivalent value in exchange. Fraud is possible, in that one of the two receives the exchange item of his/her partner but keeps the own item. No matter how a payment transaction is carried out, it seems that one of the two, buyer or seller, has an advantage over the other one. Payment systems must also describe how they solve this dilemma.

There is a possibility to keep a balance between commitments and provable receipts. One can abstractly consider the process of a sale to be an exchange of commitments and their fulfillment. On ordering an article, the buyer commits him/herself to paying on receipt. Vice versa, the seller commits him/herself to realize a certain offer by delivering appropriately. The legally binding character of this communication process can be supported by provable "digitally signed" receipts for every entered and every settled commitment, thus keeping a continuous balance between commitments and their pieces of evidence [GRI 93].

In general, payment systems violate this balance in favor of one of the two trading partners, e.g. First Virtual to the advantage of the buyer, or cash dispensers to the advantage of the bank.

Another possibility of a fair exchange is that the protocol itself enforces it. Tygar and Bahreman have introduced two such protocols for the dispatch of a message on acknowledgment of receipt [BATY 94]. The first of these two (BCEM: "Believers' Certified Electronic Mail") uses a trusted third party, which receives the message from the sender, encrypts it symmetrically and transmits it to the receiver, who next sends the acknowledgment of receipt back to the mediator. Finally, the mediator sends the acknowledgment of receipt to the sender, and, at the same time, the decryption key to the receiver.

Tygar extended this idea to his own payment protocol "NetBill" [http://www.ini.cmu.edu/netbill]. The transaction protocol NetBill presents a settlement mecha-

nism for pre-paid as well as for post-paid payments. The authentication system through Kerberos guarantees the security of the whole settlement system, limiting it to closed circles, though. The system consists of three parties: buyer, seller, and NetBill (-server). The NetBill server keeps accounts for every buyer and seller and performs payment clearing.

The other protocol for a fair exchange of information for its acknowledgment of receipt (CEM: "Skeptics' Certified Electronic Mail") is purely bilateral. First, the encrypted message and its receipt are exchanged, and then - bit by bit - the respective decryption keys. As far as we know, this protocol has not been extended to any payment system.

3 EXCURSION ON MONEY

When transferring coins or notes in digital form, one can support various characteristics. We distinguish the following four characteristics that (ordinary) coins or notes have for the persons who deal with them:

First, *containment of value*: in other words, a coin (or a note) carries its value in itself and does not only act as a reference to a real money account, like a cheque. Whoever has the coin, has its value, too.

Second, *transferability of value*, i.e., a coin can be passed on from one person to another, without the intervening clearing process of an authorized institution, e.g. a bank.

The two characteristics above are closely related to the security requirements that coins cannot be counterfeited or copied. One should not be able to duplicate 10 DM or to convert 10 DM into 100 DM. This introduces a special challenge for digital forms of money, as digital information per se can be easily changed and duplicated.

Third, *anonymity* of the buyer as well as of the seller of a product. Anonymity may be kept not only for a single sale, but also for the whole money flow, as it will be highlighted in the following fourth characteristic.

Fourth, *untraceability*, i.e. money flow can not be traced or discovered. Untraceablity is derived from the anonymity of buyers and sellers. The money flow of real coins cannot be traced back to its source ("who spent this coin?") nor, in the other direction, to its target ("who receives this coin?"). However, this leads to the undesired possibility of illegal money washing, or hiding of black market or blackmail money. We distinguish three forms of money flow pursuit: first from buyer to seller, secondly from seller to buyer, and thirdly, the pursuit of the whole trail to buyer and seller through a third party, e.g. a credit card organization. To reveal money washing, black market or blackmail money, it is obviously necessary to control the first form of money flow pursuit, i.e. from the sender to the receiver of the money. This is realized by the electronic forms of money by David Chaum in Ecash and CAFE (see below) [CHA 92]. The second form of money flow pursuit, from the seller to buyer, is enabled by payment through personal cheques. The third form of pursuing the whole trail through a third party is common practice of credit card organizations, also used to maintain their security standard.

It can be concluded that the various payment systems over the Internet, as long as they express a digital form of money and not cheques or credit cards, support the four characteristics of coins in very different ways.

4 OVERVIEW OF THE DISCUSSED PAYMENT SYSTEMS

(a) iKP, SET (harmonization of SEPP and STT): post-paid, credit card based, partly anonymous (dual signature), provable transactions and non-repudiation through use of public-key cryptography, with certificates, support from on-line and off-line transactions, high social acceptance through recognition of credit cards, suitable for usually insecure open networks, less suitable for micro payment due to the complex protocol, low-risk payment system, high degree of integrity of the transferred data over the network, very suitable for a free choice of currency.

(b) Express: pre-paid, suitable for micro payment support of off-line and on-line transactions, anonymity of the buyer only.

(c) First Virtual: post-paid, no cryptography, possibility of the buyer to reject payment, suitable for buying digital information like articles and books, mediation of transactions and support by a trusted service which prepares the clearing through a credit card or a bank withdrawal process.

(d) CyberCash: post-paid, public-key cryptography without certificates, provable by usage of digital signatures, mediation of transactions and support by a trusted service which prepares the clearing through a credit card or a bank withdrawal process.

(e) Ecash: pre-paid, strict anonymity of the buyer (blind signature), digital money, suitable for payment in an open network like Internet, use of public-key cryptography, transactions provable by the buyer, high degree of integrity of money and data transfer.

(f) CAFE: pre-paid, strict anonymity of the buyer (blind signature), digital money, off-line payment with hardware support, use of public-key cryptography, transactions provable by the buyer, high degree of integrity of money and data transfer.

(g) Mondex: pre-paid, off-line payment with hardware support, transferability of the value of a digital coin, control of money flow by participating banks.

(h) Ravensburg's GeldKarte: pre-paid, off-line payment with chip card, full anonymity.

4.1 iKP, SET (harmonization of SEPP and STT)

"iKP" stands for "Internet Keyed Payments Protocol" and was developed by the IBM Research Laboratory in Zurich [IKP 95]. A consortium chaired by Mastercard has embedded and expanded it into an application context with key management and a more concrete clearing process through Mastercard which is specified by the name "SEPP: Secure Electronic Payment Protocol". Apart from Mastercard and IBM, other companies participated in SEPP, for example GTE, Netscape, and CyberCash.

iKP includes the three payment protocols 1KP, 2KP and 3KP. In this order, complexity and security of these three protocols increase. All protocols consist of three parties: the buyer, the seller and the "Acquirer". In the case of 3KP, all three parties are equipped with pairs of asymmetric keys, in order to have strict authentication and non-repudiation in the transactions between buyer and seller.

Credit card systems with their transfer- and clearing-mechanisms play an integral role in all three iKP protocols and SEPP. The identity of the buyer remains secret to the trader, and the contents of the transaction remain secret to the credit card organization. In this respect, the system offers a limited anonymity for the buyer.

The main role of a credit card system and the partial anonymity of the buyer are also true in the payment system "STT: Secure Transaction Technology" which was developed by a consortium chaired by VISA. In February 1996, STT and SEPP have been harmonized into one payment specification, SET "Secure Electronic Transaction" [SET 96], which contains all characteristics of the predecessor protocols.

The partial anonymity of the buyer in a SET transaction is enforced in that the contents of the purchase are revealed to the seller, but the identity of the buyer remains unknown to the seller. Conversely, the acquirer of the seller is informed about the identity of the buyer, but the contents of the purchase remain unknown to the acquirer. This is achieved by a simple and effective cryptographic mechanism known as "dual signature" [CHA 92].

Two parts of the message (in this case the buyer's name and the contents of the transaction) are "dually signed" by hashing them separately, concatenating the two hash values and signing them together digitally. One receiver receives the plain text of the first part of the message and the hash value of the second part of the message. The other receiver gets the hash value of the first and the plain text of the second part of the message. In this way, each receiver can verify the integrity of the complete message, but can only read the plain text of that part of the message specifically intended for him/her, while the other part remains as hash value, which conceals the content.

4.2 Express

This procedure is planned as a credit card supplement by the credit card organization Mastercard/Eurocard [SCHEY 96]. It is a pre-paid procedure: an Express-client pays the desired amount of Express-money to his/her "Issuer-Bank" and receives the corresponding so-called "Memorandum-Balance" registered on his/her Express-card. The value goes to the Issuer-Bank in cash or by account transfer, stays however within the Issuer-Bank, which keeps it at its disposal until the clearing with the Acquirer-Bank. No digital money (E-cash) is registered on the Express-card, but only the "Memorandum-Balance".

The client pays all sellers who have an Express-contract with the credit card organization through their Acquirer-Bank. Small amounts can also be paid. Express is therefore suitable for vending machines, e.g. for tickets and parking lots.

The seller realizes the received Express-money through a clearing procedure with his/her Acquirer-Bank, which transfers the respective sum from the buyer's Issuer-Bank to the seller's account on the Acquirer-Bank. It is only with this clearing procedure that the money is really transferred.

Mastercard/Eurocard plan Express to be a supplement of the credit card or even a separate product.

4.3 First Virtual and CyberCash

The main feature of both payment systems, First Virtual and CyberCash, is the mediation of transactions by a trusted service. Both services act as credit card dealer, to whom every buyer pays by his/her credit card. Upon receipt of the money, the mediator transfers the

money - having kept a certain commission - to the actual seller in the traditional way, e.g. remitting it through a bank. The seller of the products who uses the First Virtual or CyberCash payment system does not have to be a credit card dealer him/herself.

Nevertheless, once in advance buyer and seller must become customers of First Virtual or CyberCash: they notify the mediator of their credit card number (not over Internet in First Virtual, encrypted over the Internet in CyberCash) and sign a contract which regulates further sales over the Internet, with First Virtual or CyberCash.

The actual difference between these two payment systems is that First Virtual works without cryptography. While CyberCash protects the transaction communication by cryptographic means, First Virtual can only be as confidential as the existing Internet applications, World Wide Web and E-mail, within which buyers can appear under pseudonyms but cannot keep the contents of their communication secret with the current level of technology. Security of CyberCash is enforced by cryptographic functions. Security of First Virtual supported by a cleverly organized order of working between buyer, seller and First Virtual.

Before charging the buyer's credit card, First Virtual asks again the buyer by E-mail if s/he has really ordered the product and if s/he wants to pay. The buyer can refuse either of these. S/he is thus protected against wrong orders on his/her name, as well as against being forced to pay for faulty goods. The buyer has the right to "return" the goods. As, however, returning information is impossible in reality, the First Virtual system tolerates buyers to obtain information, without paying for. In case of misuse, a behavior policy - its details yet unpublished - becomes effective, which excludes violators from the First Virtual system.

The return-right strengthens the role of the buyer and can also prevent charge-back in the credit card system. However, this limits the value of the products traded over First Virtual to an acceptable loss, which the seller has to take into account, when dealing, for example, with articles, books and magazines.

A client to-be initiates the registration phase by asking for a prefabricated electronic letter from the First Virtual server, e.g. by pressing a button on the WWW-Home Page of First Virtual. S/he fills the form and sends it back. At the same time, a First Virtual "Account-ID" which in the future will connect the buyer with every transaction is agreed upon. Next, the client calls a telephone number of the First Virtual service and transmits his/her credit card number over the telephone network. In this way, First Virtual is enabled to charge the buyer's credit card account through its credit card dealer account. Alternatively, it would be possible that the client grants First Virtual a withdrawal right from his/her bank account per E-mail.

After registration, First Virtual clients can buy on the Internet. All kinds of information can be sold, like articles, books, magazines, pictures, entries of data banks, specific WWW-pages, moderated E-mail lists or even magazine subscriptions. General Internet services or even products out of Internet can be paid for, e.g. the services of a travel agency and conference fees. A new and exciting feature is the sale of information and information services, as these are a specific type of product.

Sales transactions in First Virtual, in contrast to the cryptographically protected communication in CyberCash, are not strictly provable.

The CyberCash service is similarly structured, in principle. However, it lacks the essential point of First Virtual, where the buyer has the opportunity to refuse even after delivery – for whatever reason. In CyberCash, if a buyer expresses the wish to buy, his credit card would always be charged. Unlike First Virtual, later complaints are out of scope of the CyberCash protocol. This is an advantage for the seller.

CyberCash offers confidentiality and integrity protection. The registration phase in CyberCash during which the credit card number and other personal information is

transmitted can securely take place over the Internet. Moreover, the buyer's purchase order is provable. Therefore, CyberCash is suitable for transactions of higher quality, too.

After a CyberCash client has installed the CyberCash-software locally on his/her computer, s/he creates his/her own pair of keys, consisting of a private and a public key. During registration, the buyer notifies the CyberCash server of his/her public key and his/her credit card number in encrypted form.

From now on, the CyberCash client can buy over the Internet. As soon as s/he has decided what to buy, s/he gets in touch with the seller and receives an offer from him/her. Next, the buyer confirms the seller's offer by sending a digitally signed message to the seller, which includes, among other things, the seller's offer and the buyer's credit card number - encrypted with the public key of the CyberCash server. This message is then sent by the seller to the CyberCash server along with the additional information. The CyberCash server sets up a connection with the corresponding credit card organization in order to activate the clearing process. The seller is informed of the response of this transaction. Finally, the buyer receives a signed receipt from the seller.

Both systems, First Virtual and CyberCash, run in real operation. Without any official sponsorship they are already handling real information and money transactions over the Internet since September 1994. The companies remain silent about their turnover sizes. First Virtual, however, claims that the number of their account-ids doubles every 3 months.

4.4 Ecash and CAFE

The spiritual father of both systems is David Chaum [CHA 85, 92]. The basic idea they have in common is a particular form of digital coins, with which a buyer remains anonymous to seller and bank, but the buyer has the opportunity, in collaboration with the bank, to uncover and prove the seller's identity. The essential difference is that Ecash is based on on-line communication in the Internet, whereas CAFE operates off-line with digital wallets.

In Ecash [CHA 92] the digital coins are stored in a local system, e.g. a smartcard, or encrypted on a workstation. Buyer and seller are connected and transfer the coins over the Internet. Before accepting a coin, the seller examines its integrity on-line with the issuing bank. A coin can only be used once, in that the bank takes note of all the serial numbers of its coins and would recognize and refuse a coin which is used a second time.

CAFE [CAFE 95] uses advanced hardware equipment as electronic wallets, which communicate with each other by infrared light. An on-line examination of coins is not always possible. Instead, the buyer provides only a part of his/her identification characteristics during the payment process, which alone gives no further information about his/her identity. However, in combination with another part of identification characteristics of the same serial number, his/her identity is revealed [CAFE 95a].

The fundamental element of both systems is the "blind signature", with the help of which every bank client can create digital coin forms with serial numbers and have them signed by a bank in such a way that the bank cannot read the serial numbers it signs. The bank runs no risk of false digital coin forms, since in any case it withdraws the value of the coin from the bank account of the creator of the digital coin form, and the signature is only worth the value of one single coin. Only when a coin is returned to the bank by the seller, the bank registers the serial number, but it cannot identify its creator any more.

Based on their technological requirements, Ecash and CAFE use different algorithms. Ecash uses [RSA 78] and CAFE uses Schnorr-variants of ElGamal [ELGA 85]. The concept of the blind signature according to RSA is easy to understand:

Let *(m,d)* be the private an *(m,e)* the public RSA keys of the bank of the potential buyer for bank signatures, which represent the exact amount of, say, 1 DM, where m is the modulus and e and d are the exponents that correspond with each other, i.e. for all x holds $x^{de} \equiv x^{ed} \equiv x \pmod m$. The potential buyer creates as a coin form for 1DM a serial number n and a random number r, which will play the role of the blinding factor: the buyer calculates: $x := n(r^e) \pmod m$ and sends x to his/her bank. Because the bank does not recognize either n or r, it cannot conclude either r or n from x. The bank "signs" x by calculating: $y := x^d \pmod m$ and sends y back to the buyer. At the same time, the bank charges the buyer's account with 1DM, in the same way as if the buyer personally withdraws 1DM from the bank's counter. The buyer then divides y by r which s/he had stored. This yields the digital bank signature z of the serial number n, because $z := y/r \equiv x^d/r \equiv (n(r^e))^d/r \equiv (n^d r^{ed})/r \equiv (n^d r)/r \equiv n^d \pmod m$. Now the buyer can pay with *(z,n)* as a 1DM coin, and both seller and bank can verify the bank digital signature z of n. The signing bank pays 1DM to everybody who provides *(z,n)* to it, by transferring it to his/her account or by issuing a new digital coin of 1DM to him/her.

Obviously, a digital coin carries its value in itself when the bank transfers this value from its liquid funds, but it cannot be passed on by the receiver without having been replaced by a new coin (or a credit entry) by the signing bank. The receiver of the coin can naturally keep it by him/herself, in the same way as one keeps real coins in his/her wallet. This is done likewise in CAFE's off-line system with the wallets, by transferring money from one wallet to the other without on-line examination, but only once. However, before its next use or credit entry, the issuing bank must be notified (telecooperatively).

4.5 CAFE, Mondex and Ravensburg's GeldKarte

Basic characteristics of both systems are the digital coins and the off-line payment as with metal coins from the wallet. These electronic off-line procedures are supported by hardware wallets and smartcards which are specially developed. The important difference is that CAFE enforces strict anonymity of the buyer, whereas Mondex records every transaction to the bank of the client with a full range of data. While CAFE supports the control of the money flow with cooperation between the buyer and his/her bank only in one direction, i.e. from the buyer to the seller. Mondex allows the issuer bank to follow the whole money flow to the buyer as well as the seller.

A second difference is that within CAFE coins keep their value but cannot be transferred. In CAFE a cashed coin must be replaced on-line by the issuing bank with a new one before it is used further. In contrast, within Mondex digital coins can be passed on transitively, by wandering from one Mondex-wallet to another and then to yet another one, thus from one person to the other.

The means of communication in CAFE are the wallets, which communicate with each other with wire or infrared. The seller's wallet shows the sum to be paid and "asks" the buyer's wallet if it is ready to pay. If "yes", the money is transferred from the buyer's wallet to the seller's wallet. The hardware of the buyer's wallet prevents a "double-spending" of digital coins. Besides, the buyer's wallet supplies a part of identification marks, which in cooperation with the signing bank in a case of "double-spending" (and only then!) would lead to the exposure of the fraud's identity [CAFE 95a]. The seller's

wallet insists on this identification mark, for its security. Wallets can be connected to bank machines and, in this way, check money received and withdraw new money. Like Ecash, it is possible to connect wallet readers to a bank over the Internet.

Within Mondex, cards communicate with wallets into which the cards are inserted through a wallet-internal hardware-channel. This way, every card holder can communicate with every wallet holder. The wallets can be connected with the bank in charge over the Mondex-communication-system and transmit information about the money flow, pay money into a bank and withdraw new money from it. There are cheap Mondex cards with card readers as small as door-keys which display the money-balance of a card. Any client can use this to exchange money with any wallet holder. It is to be expected that all sellers use wallets. Client-cards can receive fresh money from special Mondex bank machines, too.

The institute "Das deutsche Kreditgewerbe" provides a similar system, however, of different type [CARD 96]. This system uses a special chip card "GeldKarte" and is being testet in Ravensburg/Weingarten in Germany. Each "GeldKarte" - an upgrade of ec-card - could be loaded with up to a maximum of 400 DM. This pre-paid system supports full anonymity. However, there is no protection against loss of cards. 300 regional dealers and 15.000 users are involved in the first field trial. It is planned to cover the whole area of Germany until the end of 1996 or in early 1997. Main targets of the field trials are acceptance by the users and observation of money flow between the involved banks.

5 ROLE OF SMARTCARDS

Smartcards are helpful in SET to support the encrypting process. Smartcards may even be compulsory, because of the transferability of a card. A particularly interesting perspective here is to replace the traditional credit card with a modern credit card supported by SET. The encrypting parts of SET would contain the acquirer's public key as well as the client's pair of keys and could at the same time support the SET protocols, especially the strict authentication between buyer, seller and acquirer. This would be a useful alternative for the sensitive credit card number.

This opens a new perspective for the exploitation of other possibilities of smartcards, for instance, the multi-functionality with other applications and the support of pseudonyms.

In Express, cards may at the same time serve as credit cards. Anonymity, e.g. by dual signature would be supported here by this Express-card. Cards support personalization and physical transport. The main information on an Express card is the memorandum balance.

No smartcards are necessary in First Virtual, since no functions that exceed the existing Internet applications are applied here. This may become different with later cryptographic extensions.

In CyberCash, however, smartcards can be applied to support the encryption process. They would even expand the scope of applications so far by being transportable at will in contrast to their cryptographically protected software emulations.

In CAFE and Ecash smartcards can be used to support the encryption process. Moreover, they can also be used as containers of coins, and, in this way, as a means of transmission to the Internet (Ecash, card readers) or to wallets and POS-readers (CAFE).

CAFE and Mondex are both off-line payment systems and therefore depend on the support of special hardware, which the clients can carry with them. The digital wallets applied in both systems support the encrypting process and, most of all, serve as container of coins.

In CAFE, the wallets can be connected with the Internet and thus form the access point of their owners for telecooperation with their banks. Besides, buyer wallets can transfer digital money by wire or infrared to the seller wallets at a point-of-sale.

Apart from wallets, there are also smartcards in Mondex, which can be inserted in wallets in order to communicate with them. In Mondex, digital money is always transferred in the chain wallet-card-wallet-card, etc. Special bank machines can also read and write on the Mondex-cards.

Naturally, "GeldKarte" is realized with smartcards. The functionality of Mondex and GeldKarte smartcards are similar. However, the implemented protocols and technologies are not interworking.

6 SUMMERY AND CONCLUSION

Payment systems in the Internet are still in their infancy. There are numerous specifications, but only few systems are under real operation. CyberCash and First Virtual made a start in September 1994. No standards have caught on so far, although SET is a good candidate for a credit card system standard. In the next years we expect that the requirements and criteria about the technological, organizational, and legal design of payment systems will develop. The formulations in this article contribute to this aim.

In the long run, not many incompatible systems will survive. There will be a selection of the best and a harmonization of the rest.

In the European Research Project ESPRIT-E2S [http://www.ansa.co.uk/E2S/] a trial installation of SET is planned in cooperation with VISA.

In the European Research Project ACTS-SEMPER [http://www.zurich.ibm.com:80/Technology/Security/extern/semper/], trial installations with tests of the payment systems iKP and Ecash are planned in cooperation with IBM and DigiCash. CAFE and Express in cooperation with CWI and Europay, respectively, are also on the SEMPER agenda.

GMD, in cooperation with other interested users and system houses, plan to work on the First Virtual payment system. Along with the expansion towards a multi-currency and a multi-lingual Europe, we are thinking of a new-to-be-installed cryptographic protection for First Virtual through the Internet mechanisms like PGP and PEM.

For all payment systems which do not consider a fair exchange protocol, integration of new application protocols for a fair commercial exchange between buyers and sellers is an interesting challenge for research.

7 URL FOR THE INDIVIDUAL PAYMENT SYSTEMS

NetBill:	http://www.ini.cmu.edu/netbill http://www.ini.cmu.edu/netbill/publications.html http://www.ini.cmu.edu/netbill/CompCon.html
iKP:	http://www.zurich.ibm.com:80/Technology/Security/extern/ecommerce/ ftp://ietf.cnri.reston.va.us/internet-drafts/draft-tsudik-ikp-00.txt
SET:	http://www.mastercard.com/set/set.htm or http://www.visa.com/cgi-bin/vee/sf/set/setbus.html

Express: No URLs

First Virtual: http://www.fv.com/

CyberCash: http://www.cybercash.com/
ftp://ftp.cybercash.com/pub/draft-cybercash-v08-00.txt

Ecash: http://www.digicash.com
http://www.digicash.com/ecash/ecash-home.html
http://www.digicash.com/publish/ecash_intro/ecash_intro.html
http://www.digicash.com/publish/digibro.html
http://www.digicash.com/publish/sciam.html
http://www.digicash.com/ecash/faq.html
http://www.digicash.com/ecash/quickref.html

CAFE: http://www.cwi.nl/cwi/projects/cafe.html
http://www.digicash.com/products/projects/projects.html

Mondex: http://www.mondex.com/mondex/
http://www.mondex.com/mondex/home.htm
http://www.mondex.com/mondex/net.htm

For other payment systems see
http://www.darmstadt.gmd.de/~zangeneh/Payment_Systems/

8 BIBLIOGRAPHY

[BATY 94] Bahreman, A.; Tygar, D.J.: *Certified Electronic Mail.* Proceedings of the Internet Society Symposium on Network and Distributed System Security, 3-19, San Diego, Cal., Feb 3-4, 1994.

[CAFE 95] Weber, Arnd; et al.: *Secure International Payment and Information Transfer. Towards a Multi-Currency Electronic Wallet.* Principles, Results from Initial Surveys, Scenarios. CAFE, Conditional Access for Europe, © Project CAFE, Frankfurt 1995, 109 pages.

[CAFE 95a] *Deliverable Functionality of the Protocols.* ESPIRIT 7023 CAFE, Document IHS8341.

[CARD 96] Klaus R. Altenhenne, *Elektronische Gelsbörse, Multitalent ec-Karte*, a-la-CARD AKTUELL, 10-11/96, 204-206.

[CHA 85] Chaum, David: *Security without Identification. Card Computers to Make Big Brother Obsolete.* Com ACM 28(10), 1985, 1030-1044.
Also published as: *Sicherheit ohne Identifizierung.* Informatik-Spektrum, 10, 1987, 262-277.

[CHA 92] Chaum, David: *Achieving Electronic Privacy.* Scientific American, August 1992, 96-101.
Also available on http://www.digicash.com/publish/sciam.html

[DIHE 76] Diffie, W.; Hellman, M.E.: *New Directions in Cryptography.* IEEE Transactions on Information Theory. Vol.IT-22, 1976, 644-654.

[ECMA 88] ECMA TR/46: *Security in Open Systems – A Security Framework.* Edited by the European Computer Manufacturers Association (ECMA), July 1988, 71 pages.

[ELGA 85] ElGamal, T.: *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.* IEEE Transactions on Information Theory, Vol.IT-31, 469-472, 1985.

[GRI 93] Grimm, Rüdiger: Non-repudiation in Open Telecooperation, NIST, NCSC: Proceedings of the 16th National Computer Security Conference, September 20-23, 1993, Baltimore, Maryland, 16-30.

[GZ 96] Grimm, Rüdiger und Zangeneh, Kambiz: *CyberMoney und Internet.* Proceedings des 6. GMD-SmartCard Workshop, 30.-31.1.1996. Org.: Bruno Struif, Darmstadt, Januar 1996. Also published in a-la-CARD 5/96, 02-02-96, 9-13 (Teil 1) und 6-7/96, 16-02-96, 8-14 (Teil 2).

[IKP 95] *Internet Keyed Payment Protocol.* Internet-Draft, available on: ftp://ietf.cnri.reston.va.us/internet-drafts/draft-tsudik-ikp-00.txt

[JW 95] Janzon, Phil; Waidner, Michael: *Electronic Payment Systems.* SEMPER Activity Paper 211ZR015, Draft Vers. 5 (SEMPER internal), 13 December 1995, 24 pages.

[KER 88] Steiner, J.G.; Neumann, C.; Schiller, J.I.: *Kerberos: An Authentication Service for Open Network Systems.* USENIX Winter Conference, Dallas Texas, 9-12 Feb 1988. Proceedings pp. 191-202.

[OSI 89] ISO 7498-2(E): Information processing systems – *Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.* First Ed. 1989-02-15.

[RSA 78] Rivest, R.; Shamir, A.; Adleman, L.: *A Method for Obtaining Digital Signatures and Public Key Cryptosystems.* Com ACM 21(2), Feb 1978, 120-126.

[SCHEY 96] Shey, John F., Europay: *Express.* SEMPER Activity Paper 211EP021, Draft Vers. 1 (SEMPER internal), 2 Jan 1996, 11 pages.

[SET 96] *Secure Electronic Transaction (SET) Specifications.*
1. Business Description, 68 pages; 2. Technical Specifications, 269 pages. DRAFT for public comment, 23 Feb 1996. Available on:
http://www.mastercard.com/set/set.htm or
http://www.visa.com/cgi-bin/vee/sf/set/setbus.html

[X.500] ISO/IEC 9594, ITU X.500 (1988/92): Information technology – Open Systems Interconnection – *The Directory* 1993(E). Insb.: X.509 – *The Authentication Framework.*