Is Electronic *Cash* Possible?

Max Schmidt Universität Saarbrücken
Matthias Schunter Universität Saarbrücken
Arnd Weber Universität Freiburg

Technischer Bericht Nr. A/03/98

Max Schmidt <max@krypt.cs.uni-sb.de>
Matthias Schunter <schunter@acm.org>
Universität des Saarlandes
Institut für Informatik
Lehrstuhl Kryptographie und Sicherheit
Im Stadtwald 45
D-66123 Saarbrücken

Arnd Weber <aweber@iig.uni-freiburg.de>
Albert-Ludwigs-Universität
Institut für Informatik und Gesellschaft
Friedrichstraße 50
D-79098 Freiburg im Breisgau

Is Electronic *Cash* Possible?

Max Schmidt
Matthias Schunter

Universität des Saarlandes
Institut für Informatik
Lehrstuhl Kryptographie und Sicherheit
D-66123 Saarbrücken
<max@krypt.cs.uni-sb.de>
<schunter@acm.org>

Arnd Weber

Albert-Ludwigs-Universität
Institut für Informatik und Gesellschaft
D-79098 Freiburg i. B.
<aweber@iig.uni-freiburg.de>

Abstract

Cash-like payments in electronic commerce and at the traditional point of sale are expected to be beneficial, e.g., because of privacy protection, low transaction costs, and irrevocability. Therefore, we discuss how to design electronic cash in a way that it both mirrors the most important characteristics of traditional cash, but also fulfils the expectations which arise towards electronic means of payment. We analyse the problems and trade-offs between the different characteristics to be implemented. This analysis is based on a user survey and a review of existing technologies for electronic payment systems. Finally we argue why existing systems do not fulfil the critical requirements, and point out future work towards electronic cash which will meet more requirements.

1 Introduction

Electronic cash in our sense is universally usable stored value[1]. Electronic cash is discussed as a means to replace traditional cash in the physical world, and as a means of payment in the virtual world. In both cases, electronic cash could have a number of benefits even compared to future pay-now[2] or post-payment instruments. Examples include that a stored-value payment might be cheaper than a pay-now mechanism, because less on-line connections are required, and that, unlike post-payments, everybody can use it independently of creditworthiness. Furthermore, the payer's privacy can be protected. For these reasons, existing electronic payment instruments do not cover the whole potential market of electronic payments, i.e., a benefit for the issuers of electronic cash is the possibility of earning fees by conquering a larger share of the market of electronic payments.

In order to replace traditional cash, electronic cash should be easily usable and also offer robustness, off-line usability and transferability. Up to now no electronic cash system offers these characteristics. This leads to the question whether it is possible to develop electronic cash with most characteristics of today's cash, i.e., electronic cash which may eventually replace traditional cash.

---

1 Besides electronic cash (i.e., prepaid stored value), we consider debit-card-like pay-now and credit-card-like post-payment schemes.

2 Note that in all existing debit-card schemes debiting the account is deferred. Therefore, they are post-payment schemes in our sense. This, however, may not hold for future developments

Before we describe those characteristics of traditional cash which will need to be mirrored, we will describe the projected benefits of electronic cash. Then, we sketch additional requirements, such as loss-tolerance, which are not fulfilled by traditional cash but should be provided by electronic cash. After a short survey over the existing technology for electronic cash, we discuss the problems which occur if one wants to provide all desirable characteristics.

Note that this is no survey on electronic payment schemes[3]: As we will show, no system exists which offers electronic cash in our sense and only few schemes come close. Therefore, we rather survey technologies, existing building blocks, and trade-offs which become important when designing electronic *cash*.

2 Projected Benefits of Electronic Cash

Our interviews with the banking industry have shown that electronic payments have not yet turned out to be profitable. However, compared to traditional payment instruments, electronic payment schemes seem worth investigating for the following reasons:

- Today's costs of handling money (especially coins) are significant, in particular with vending machines. Thus a cheap form of payments is sought. This cost reduction may even be extended if many subsequent transfers can be done without the involvement of the banks.
- Convenient payments of any amount, i.e., no problems with missing change.
- It is possible to design electronic means of payment more secure than traditional cash. So the damage of counterfeit money might be reduced.

Using electronic cash as a form of electronic payment has additional benefits:

- With today's technology, privacy in the sense of untraceable electronic transactions can only be granted with electronic cash, unless one uses anonymous accounts, which in most countries are politically not acceptable.
- The off-line usability of electronic cash reduces costs for lines or radio networks. In particular it is being hoped that the costs per individual payment in an off-line system can be reduced if the merchants submit collected batches of transactions overnight.
- Issuers can earn fees by "conquering the cash market".
- Interest can be earned from the float, which, e.g., can be used to pay interest to the holders of electronic cash.

Also, the benefits of pay-now payment instruments hold:

- Sellers require irrevocability, e.g., in electronic commerce, which in general is not provided by post-pay payment schemes where the payer can demand cancellation.

[3] For surveys on digital payment schemes (which partially claim to be electronic cash), one may look at Asokan, Janson, Steiner, Waidner 1997, Furche and Wrightson 1996, Mahony, Peirce, Tewary 1998, or Wayner 1997.

- Pay-now instruments can be given to less creditworthy individuals than, e.g., credit cards.
- By developing alternatives to credit cards and paper cheques, it should be possible to reduce transaction costs as well by limiting fraud and reducing handling costs for cheques.

These benefits can only be earned if traditional cash can be replaced to a substantial degree, and if electronic cash can provide efficient solutions on electronic networks. Thus a powerful tool is required, having the advantages of traditional cash, but being transferable across networks as well.

3 Which Characteristics Should Electronic Cash Have?

3.1 Characteristics of Traditional Cash

In order to replace traditional cash it is important to recognise which characteristics traditional cash has: For any payment system named "cash" it is crucial to mirror the expected characteristics. Otherwise, part of the cash market cannot be reached and users may be disappointed if something is called "cash" but cannot fulfil the expected role.

Usability

Usability means very basically to be able to use a means of payment, i.e., that everybody can obtain it, store it, and pay any payee with it. To fulfil this characteristic is not trivial. A user of the world's earliest stored value chip card in Biel, Switzerland, concluded already in 1993: "Cash can be used everywhere, but the card not. You need devices to read it."[4] Also think of the usability by children. Ease of use is an obvious requirement for any form of payment. The handling of coins is easy, except if appropriate change needs to be given. Also for the recipient of large numbers of coins their handling is difficult. Usability of electronic cash would be hindered if implementations are not compatible, e.g., if electronic cash from one issuer is not usable with vending machines accepting stored value from another issuer.

An obvious aspect of usability is *portability*. A card reader or an electronic wallet must fit into existing leather wallets, men said in our surveys, or be of compact shape to be put into pockets (women have less problems with storing such somewhat larger devices). Also, of course, any form of electronic cash to be used on the Internet is not well portable if stored on hard disks of personal computers.

[4] The requirements and benefits of electronic cash in this paper are based on expert interviews and consumer surveys. The interviews mentioned have been made in the framework of three research projects, which were "Soziale Determinanten der Entwicklung alternativer POS-Zahlungssysteme" funded by Deutsche Forschungsgemeinschaft, CAFE and SEMPER, funded by the Commission of the European Communities. See Furger et al. 1998 for the consumer interviews.

Off-line Usability

Traditional cash can be used off-line; similarly this is required from electronic cash. This may change in case some day everybody and everything will always be on the Internet: vending machines, for example, are increasingly being put on-line. This is done so that the operator can easily learn when something has to be replenished, or is out of order. But as today most payees are indeed not permanently on-line, mostly because of communication costs, off-line usability is required.

Off-line Transferability

By off-line transferability we mean that received cash can be used for another payment without contacting the issuer. Coins and bank notes can very easily be transferred off-line whereas electronic payments may not. Respondents know they need off-line transferability, e.g. for "giving the children pocket money", "give one's neighbour 20 pence to buy a pint of milk", "pour boire" and asked: "How do you put a tenner in somebody's birthday card?" Someone from Biel said: "But if I have 1000 sFr on the card, I cannot split them. I cannot transfer them." And added "If everybody had a reader..."

Off-line transferability is not only useful for private account holders, but also for companies to have a means of payment to pay received money immediately.

Untraceability

Traditional cash provides privacy protection. Usage of coins means that transactions cannot be traced by third parties. For banknotes this is only the case to a smaller degree, as transactions can be linked using the note numbers. Today, sellers often do not know the identity of a customer. In our surveys some stated that "monetary affairs are primarily private affairs". Others argued "I feel entitled of the option of being anonymous when I choose to be", or they want to "minimise Big Brother's surveillance of my expenditure". Some French consider that privacy protection is a matter of "liberté personelle", a right to be enforced by the state. Others argued they need privacy protection for paying goods which fell "off the back of a lorry", in order "to avoid payment of value added tax", or for "bribery". Thus, a part of the cash market can only be covered by electronic cash with a high degree of privacy protection.

For clarity, we distinguish two levels of anonymity (Chaum 1981), namely "untraceability" and "pseudonymity". "Untraceability" means that the issuer, the acquirer and merchants cannot trace a payer, i.e. cannot tell whether two payments have been made by the same payer, not even in collaboration among each other. "Pseudonymity" means that all transactions can be linked to pseudonyms, where the pseudonyms cannot be linked to individuals if only few transactions use the same pseudonym. Telephone cards that are sold anonymously can be like this. In practice, however, these schemes enable identification if the pseudonyms are used too often: Using the phone-card for many calls can lead to identification by examining the destinations of the calls.

Transparency of Financial Status

From a simple look into one's traditional wallet, one learns the remaining funds, i.e., obtains transparency of the financial status. "With cash I can see precisely how I run out of it." "With cash, children can see the amount," respondents said. As opposed to other payment instruments, with cash a payer can easily be unable to pay even though there is enough money on his/her bank account, so this look "into one's pocket" is of crucial importance. If the display is with the merchant, this is no sufficient solution as of course users will wish to take this look anywhere. It is particularly annoying if one detects only after queuing that the funds are not sufficient.

Control over Wallets

Traditional wallets remain in one's hands. If a purse on a chip card is used, this chip card may be used for storing other functions as well, such as other payment functions, or a digital signature function to be used in electronic commerce. Therefore, users may not wish to hand over such an important card to a payee while entering the PIN into the payee's device. In case of terminals out of which the holders cannot always extract the card, one may lose important functions if the terminal erroneously withdraws the card.

Long validity

There are three types of validity of cash. First, cash is sometimes made invalid if more secure coins and notes have been produced. Secondly, cash may no longer be valid because the issuer went bankrupt (cf. Japanese Ministry of Finance 1989). Issuers of electronic cash usually limit the usability of their cash right from the beginning, in order to prevent long liabilities. Finally, the validity of cash may decrease due to inflation. Competition among different electronic currencies could, however, reduce inflation because only those will survive which provide a low rate of inflation (cf. Hayek 1977).

Security

Apart from the issuers who will protect electronic cash against fraud, also the users want to be sure that the issuer cannot deny the value of the user's cash.
The production costs of today's coins with smallest denomination is often higher than their face value. So there is obviously no risk of counterfeit money. Coins and notes of higher denominations are more or less secure if the cost of forgery is kept ahead of its gain: When colour-copiers became a cheap means to forge bank notes, many countries increased security by introducing holographic images which cannot be copied.

Robustness

Both coins and bank notes are very robust. Similarly, high robustness will be required from electronic cash. Money should neither disappear nor become unreadable. The demands regarding robustness are quite high, as users will compare it to an embossed plastic card, i.e. a credit card, which can be used quite reliably in many countries and climates. Men will bend plastic chip cards when in their hip pockets. Electronic wallets may be stepped on or dropped. Also anticipated malfunctioning of the electronic cash system should not result in loss of the users' values.

Cost Efficiency

The costs of traditional cash is a subject which is difficult to treat as often its costs are not known by the players, and also not published well by the banking system. In any case, electronic cash needs not be free, as traditional cash is not either. However, users may believe it is, or believe it is very cheap, because it is being provided by the banking system at little visible costs. So regarding costs users will be very sensitive. Merchants may be used to paying a disagio when accepting card payments. But individuals will probably find it unacceptable if electronic cash diminishes when transferred between individuals. In any case, a new instrument will have to be either as cheap as traditional cash, or the marginal cost increase must be justified by some other benefit.

3.2 Additional Requirements for Electronic Cash

We now give an overview of new requirements which are expected from electronic cash. As compared to existing characteristics, if a new requirement is not fulfilled, this type of electronic cash will not automatically look inferior to traditional cash. So users will not expect that all new requirements are fulfilled. The new characteristics may, however, form an incentive to switch from traditional to electronic cash.

Fungibility

It will be expected that with electronic cash one can pay any particular sum easily, just as one can with post- or pre-pay cards, bank transfer orders etc. This means that if one has the necessary funds available, the system should not tell that the desired payment is impossible. So electronic cash could be better than traditional cash, where one may not be able to pay because the merchant has no appropriate change.

Usability on Networks

From electronic means of payment it will be required that they can be used securely on networks such as the Internet.

Tolerance Against Loss and Theft

Tolerance against loss, theft and malfunctioning has been a selling argument for post-pay cards, so users will welcome it for electronic cash as well. Loss tolerance could even be used to design an electronic traveller's cheque. Alternatively, one can try to teach users that regarding loss electronic cash is like traditional cash. The holder, however, will arrive at the conclusion that in case of loss of a card that can only be used by the holder, the issuer still has the real money, and accordingly will expect a refund.

Usability Across Borders

This is a characteristic not well available with traditional cash, if not even illegal, but it may be expected from electronic cash, just as it is available with credit cards. It is particularly valuable for travellers, in small countries, in border regions and in trans-border electronic commerce. Currently, the issuers of the stored value cards deployed in European countries face the problem that their kind of electronic cash will not be able to inter-operate even though most of them will soon use “Euros”, as the systems are incompatible.

Ease of Reloading

If users are required to go to a cash dispenser for withdrawing electronic cash, they may consider withdrawing traditional cash instead, which can be used everywhere, at least inside the country (expert interviews, see also Furger et al. 1998). Also, users will require that reloading does not take much longer than withdrawing traditional cash or any other transaction. Reloading via network or phone from anywhere will certainly be useful (cf. Intellect 1996).

User-Friendliness and Trustworthiness

Systems must be designed in a way that they can be understood and handled properly. Users will not develop trust in the system if they believe that the system may not operate in the way they expect it. Thus, e.g., in the case of untraceability users expect that no additional information of the users is given to the payee during payment. It might be that a secure and correct system is not used because people just do not trust the system to be secure.

Backwards Compatibility

This requirement originates from the manufacturers and operators of card payment systems who argue that new payment instruments should have the form of a card so that existing card readers can be used. In the past, the argument suffered from the fact that card terminals were not able to read chip cards anyway, or were not able to deal with the technology in question. Thus it was not really convincing why new interfaces were not considered by major issuers.

4 Existing Technology

This section gives an overview of some existing technologies which can be used for electronic cash. First some basic technologies are introduced, then different types of cash-like payment systems with special techniques are discussed.

4.1 Basic Technologies for Cash-like Payment Systems

Tamper-Resistant Hardware

Electronic cash is represented by electronically stored data, which can usually be copied very easily. To prevent criminals from simply copying electronic cash, one possibility is to use special hardware. Silicon chips can be designed in a way that it is difficult to access and manipulate their memory (Rankl, Effing 1997; see Weber 1997 for the emergence of chip cards in Europe). European stored-value phone cards and cards for access to television were the first to exploit this difficulty on a large scale, and the first to have been broken. Chips can be attacked with sophisticated laboratory equipment (Anderson, Kuhn, 1996; Boneh et al. 1997). However, more powerful intrusion detection systems are becoming available but they result in modules thicker than chip cards.

Trustworthy User Devices

Achieving trust into user devices is difficult[5] but required for electronic cash: Users need not trust devices from a supplier of the issuer's choice and vice versa. A cure is the so-called "wallet with observer" concept (Chaum 1992). The basic idea is that the user has a trusted wallet of his choice. Each issuer who wants to equip a user with a device then provides a plug-in module for the user's trusted wallet instead of issuing a new device. For electronic cash, the user's wallet is trusted by the user and guarantees the user's security and privacy whereas the plug-in module, which is trusted by the issuer, protects the issuer's security.

In addition to multiple modules trusted by different parties, the wallet also needs a trustworthy display and keypad: If the user's device has neither a display not a keypad, the users have no control over the amount paid: After entering a PIN into the payee's terminal, the payee could deduct arbitrary amounts from the wallet without the user being able to prevent it.

An additional advantage of such a wallet is that contact-less interfaces could be used, such as radio, inductive or infra-red. This would make terminals possible which are both cheap and well-protected against vandalism. They would need no slots and could be under the ceiling or under glass if necessary.

[5] Some means to achieve this trust are described in Pfitzmann et al. 1997.

Authentication

Authentication is required to guarantee that communication is done with the right persons or devices. If money is for example withdrawn from an account to reload a user's device, the issuer wants to be sure that this device really belongs to the person owning the account. This problem can be solved by authentication schemes. A strong kind of authentication is the use of signatures.

Digital Signature Functions and Blinding

Digital signatures allow to prove the authenticity of messages to other parties such as courts. A digital signature on a message is produced with a so-called secret key and can then be checked by anybody with a corresponding public key which is linked to the signer's name (see Merkle 1974; Diffie, Hellman 1976; Rivest, Shamir, Adleman 1978). Unless substantial discoveries are made in mathematics, it is computationally infeasible to break signatures, and, of course, if the secret key is stored and accessed securely. An issuer could use a digital signature to sign any document, thus also an electronic coin or bank note.

Signed documents can, of course, in principle be traced. In order to achieve privacy, Chaum suggested to "blind" the signatures for making untraceable payments. Blinding means that some blinding factor is calculated into the electronic cash to be signed by the issuer. After signing, the blinding factor is removed by the holder. Thus the piece of money remains signed, but the issuer has not seen the signature which comes back after payment (Chaum 1983).

Connection Anonymity

If a payment is made on a network, the network operators can trace the transaction, whether blinding is used or not. A remedy would be to use anonymous terminals or to use network anonymity services (e.g., MIXes, see Chaum 1981).

Loss Tolerance

To build loss tolerant systems, backups of electronic cash can be kept by the issuer. In case of untraceable electronic cash, loss tolerance can be provided if the user either stores back-up information itself, or keeps it encrypted with a trustworthy party (Pfitzmann, Waidner 1990 and 1997). Essentially this information can be used to reclaim unspent cash which is determined by unblinding all recently withdrawn coins of this user.

Interest

Users might wish to earn interest on the amount of electronic cash that they keep unspent on their devices. In a simple solution a user can pay the unspent amount back to the issuer, whenever (s)he likes. The issuer credits interest on money that is left since the last withdrawal. However, the issuer needs a mechanism to see that this money was withdrawn by the user and not received from someone else.

4.2 Coin-based Payment Systems

We distinguish between coin-based and counter-based payment systems[6]. Like traditional coins, electronic coins are of a fixed value. To assure that coins can only be created by the issuer, the coins are digitally signed. In order to offer untraceability blind signature schemes can be used. Such coins can be very secure, but they come with the problem of low fungibility. Some improvements can solve or reduce these problems, but first some general extensions are shown.

Double-Spender Detection

There exists no software solution that protects electronic cash from being copied and used twice. This is the reason why on-line verification or tamper-resistant hardware is typically required for off-line use.

But security needs not depend on tamper resistance only, as there are solutions to identify a criminal who spent a value more than once after breaking the tamper resistance. Even if blind signatures are used, double spenders can be identified if an identity is encrypted into electronic coins (Chaum, Fiat, Naor 1990) so that the identity can only be decrypted if the coin was used twice.

Value-less Coins for Transferability

A value-less coin can be used to authenticate a message once while staying untraceable. Double-use leads to identification. This technique (Antwerpen, van 1990) is used to allow off-line transferability for untraceable electronic cash. The recipient of a transferred coin needs a value-less coin which is then linked to the received coin during the payment. For paying, the recipient forwards the received coin and then "pays" the value-less coin. The recipient verifies the link to the coin with value. In all following transfers the coin together with a growing list of linked value-less coins will be forwarded. After deposit, the coin together with the linked chain of value-less coins can be used to identify double users with the usual mechanisms.

The size of the transferred coins grow, because each transfer adds one value-less coin which is approximately the same size as the coin. A theoretically proven lower limit for the size of growth in each transfer is the amount of data needed to store the encrypted unique identity of the payers (Chaum, Pedersen 1993).

Schemes for Paying Interest with Coins

For paying interest on coins Chaum (1989) introduced two methods: time-stamps and receipts. In the first method, coins have a dynamic value that increases like money on an account on which interest is paid. Therefore the date of issue is „minted" into the coins. The actual value of a coin would be the issued value plus the age of the coin multiplied by the rate of interest.

---

[6] We don't consider cheques because normally they are not pre-paid and otherwise, they are similar to divisible coins.

Coin-Extensions for Fungibility

Change: Coins are of a fixed value. This leads to the problem of a lack of coins in the appropriate denominations. In traditional systems payers and payees have a reservoir of change for this reason. This solutions cannot be used in untraceable systems without payee untraceability. If, for example, an anonymous buyer pays a merchant, the problem is that the merchant knows which change (s)he gives to the buyer. If no transferability is offered the buyer has to give the change to the acquirer. In co-operation with the acquirer the merchant can then find out the identity of the buyer, because the buyer is now in the payee-role, for which no anonymity is offered.

Divisibility: Okamoto and Ohta (1992, cf. Chan, Frankel, Tsiounis 1998 for an improved protocol) suggested divisible coins, where each coin can be spent incrementally up to its monetary value. So one can pay $1 using a $10 coin and keeping $9 for other payments of different values. A drawback is that all fragments of one coin can be linked, which decreases untraceability.

Refund: Cheques have the advantage that the payer can write the amount the payee wants to have into it while paying. Chaum, Fiat and Naor (1990) describe such a system with pre-paid coins. The user withdraws „high-value“ coins from the issuer and can decide what amount up to the coin value they would like to spend. After having paid the user requests the issuer to pay the refund of the difference between the coin value and the paid amount. If there are a number of payments and deposits of the same amount, issuer and acquirer cannot link them.

Another possibility to increase fungibility is to combine coins with counter-based systems, as shown below.

4.3 Counter-Based Payment Systems

In counter-based payment systems, the electronic cash a person owns is represented by a counter. Tamper resistance is required to keep the users from manipulating the counter easily. Also authentication schemes are required to prevent illegitimate communication with the counter in order to change its value. So terminals of issuers and merchants need special keys to access a counter on a user’s smart card. Untraceability may be provided if communications with all smart cards can be done with the same key which must be kept secret using tamper-resistant hardware in the terminals. If for security reasons, different keys are used, only pseudonymity can be provided, because each key can be used as a pseudonym.

A way to increase security in counter-based systems and to detect spending of not withdrawn value is to track the value of each counter at the issuer. In off-line systems this might not always be the actual value, but it can be updated from time to time and used to detect if the counter stored on the smart card has been manipulated, i.e., if its shadow shows a negative amount. A centrally stored counter stands in conflict with untraceability, because all transactions are linked to specific counters. Pseudonymity can still be reached if the counters cannot be linked to individuals.

Shadow counters can also be seen as backups to provide tolerance against loss, theft and malfunctioning. In most existing systems, however, loss tolerance is not communicated to the holders in order to keep costs for help-desks low ("yesterday the Coke machine did not work, I want my money back").

4.4 Hybrid Schemes — In Between Coins and Counters

Counters with Value-Less Coins

A way to provide untraceability while using asymmetric authentication techniques is to use value-less coins for the authentication of payments: To increase the security in counter-based systems, one can combine counters with electronic cheques (Bos, Chaum 1990). For each payment an electronic cheque with the signature of the issuer is needed. Because each cheque can only be used up to a maximum amount, it is not possible to spend an unlimited amount of money without contacting the issuer, after the counter is broken (CAFE report 1996).

Multi-Use: To save storage space on smart cards there are techniques for using the same value-less coin multiple times (CAFE report 1996[7]). Thus, depending on how often a cheque can be used, the system provides something in between untraceability if the cheque can only be used once and pseudonymity if the cheque can be used arbitrarily often.

Tick payment: If all payments are to be made to the same payee, such as per tick with a telecom provider, one single value-less coin (signature) needs to be used. After an initialisation, one pays subsequent ticks quickly (Pedersen 1995).

Adding Value to Value-Less Coins: If one replaces the value-less coins with coins with an upper and lower value limit, one can slightly increase the security of the scheme since one has to pay the lower limit of the range for withdrawing the coins which can then, depending on the value of the counter, be used up to the maximum amount. Consider, for example, that the minimum and maximum amount only differ by 10 cents, then, the gain of breaking tamper resistance is limited to 10 cents per payment.

Coin Pools with Counter

The problem to have coins in the right denominations can also be solved by coin pools[8]. The user has many coins in all denominations but (s)he is only allowed to spend coins up to the value of the counter. If tamper resistance is broken, the user can spend all coins in the pool once without being identified. For coins the user reloads next time, (s)he has to pay. So the possible damage by breaking the tamper resistance is limited to the amount in the coin pool and a criminal would probably get less money than breaking the tamper resistance costs.

---

[7] In CAFE, the cheques could be spent twice. Thus it was possible to have 70 payments on a card chip.

[8] Personal communication with David Chaum.

5 Trade-offs in Designing Electronic Cash

Now we examine the most important trade-offs, which emerge when different characteristics are implemented in one system. First all trade-offs with costs are discussed. After this all remaining trade-offs with security, untraceability and convenience are examined.

5.1 Trade-offs with Costs

Cost efficiency is always required. An electronic cash system will be only acceptable if costs are low compared to the benefits it offers. So in all cases where the fulfilment of characteristics costs money, such as for comfortable user-devices, players should be willing to bear the cost if the benefits of using this kind of money are large enough. Another possibility would be that the issuer expects other benefits from the customer relationship and therefore bears the costs. We believe that at the time of writing (1998) it has not been sufficiently investigated whether the users are willing to pay for powerful systems having many useful characteristics. It is not even clear how much a secure system offering many characteristics will cost and whether these costs will be higher than the full costs of traditional cash or other payment schemes.

For all values in use, issuers have to store information about them[9], and the values have to be transferred between issuers and users, even if the value is one penny. Characteristics like off-line usability or off-line transferability require complex protocols which make transaction times longer. Also additional hardware will increase costs, like displays needed to provide users with more transparency about their financial status.

More money can be spent to obtain more security: Secure protocols and tamper resistant hardware have to be developed. In cases where a secret bank key has to be stored very securely, much money can be spent for protection.

Untraceability makes everything more complicated: Untraceability comes with the overhead for blinding. Untraceability in networks means anonymous connections, which can be established by the use of anonymous terminals or the use of MIXes. Both lead again to higher costs because of the additional hardware and, in the case of MIXes, also of higher transaction times.

Regarding chipcard-based untraceable systems issuers emphasise the cost of computation on the account holder side as a powerful processor is required which costs more than a simple one. In the CAFE project, the marginal costs for a cryptographic coprocessor were around US-$ 3.[10] Potential issuers emphasised that this was a major stumbling block. However, also the costs for handling all the signatures have to be considered even though the costs must not be overestimated as a large share of them can be handled off-line, i.e. after the actual payment.

---

[9] Except in systems where only counters on user devices are used. But in such systems issuers might not even recognise fraud.

[10] Under the assumption that the chip card can be used for 3 years this can be expressed as privacy for only one dollar per year.

The more convenient a system gets, the more it costs: To achieve convenient reloading for users, many withdrawal terminals will be required. It would even be better if phone and computers could be used for reloading as well. This, however, requires techniques for managing passwords securely and approval on secure displays.

Robustness and reliability are costly and always limited: The system should also be reliable so that one does not get frustrated by using it. To achieve reliability will cost money. Electronic cash stored on portable devices will never reach the robustness of traditional coins. Water, heat and strong magnetism will quite likely destroy electronic coins stored on user devices. Chip cards are known to be well portable, but they face physical pressure when stored close to coins in traditional wallets. Displays for achieving transparency need particular protection or get scratches or even break. Spending more money, one can construct more robust devices. On the other hand users might accept non-robust electronic cash if the devices are not too expensive and convenient loss- and fault-tolerance is offered.

Fungibility for untraceable coin-based systems is difficult to achieve: A payment should not be impossible because one ran out of appropriate coins. A solution not requiring change is to use coins of the smallest denomination, e.g., 1 cent. This, however, will lead to considerable memory and computing requirements, which in turn will lead to problems with portability. Consider to store 100 ECU, which means 10k coins. With current key sizes, a coin requires around 1 kbits, so one needs 10 Mbits. Even though no storage problem for a pocket calculator-sized wallet, spending, e.g., 2500 coins will still surpass its computational abilities. Furthermore, 10 Mbits is beyond the storage capacity of chip cards which is largely limited by the fact that men tend to sit on the cards, and accordingly the chips have to be small. 20 to 25 mm^2 is the largest size which comes into consideration.[11] A remedy would be to split coins or use multi-spendable coins which will make some transactions traceable.

Loss tolerance comes with additional overhead: If loss tolerance is used, one needs information for rebuilding the correct state, so this information needs to be handled. In traceable systems this can be done by the issuer. In untraceable coin-systems, users need a backup of the data that is used to create blinded coins (Pfitzmann, Waidner 1997). Even if this backup has only to be done once at the creation of the electronic purse it will make usage less convenient: One has to keep a printout, a memory card, or remember the passphrase for decrypting the backup.

5.2 Trade-offs with Security

Perfect security is not possible: Apart from the risk that someone manages to break the system with much effort and special equipment requiring considerable costs, there will be always the risk that someone steals secret information like private

[11] The latest card from EU project CASCADE can store 32 kBytes, but part of this will be needed for the operating system and the program.

keys for “minting” coins or circuit layouts to break the tamper-resistance of user devices.

If electronic cash is generally used, breaking the system is not only a risk for the issuer. Imagine a whole nation that is not able to do payments anymore because criminals produced lots of counterfeit money. It could already be problematic if there are only rumours that the system has been broken. People might wish to exchange their electronic cash into other values. This can lead to a cascading default by the inability of participants to pay off a close-of-day deficit, called systemic risk (Bonorris 1997).

Trust in the system is required: People will only use new systems if they trust them. The new protocols are difficult to understand, so it may take considerable time and effort until trust has been established.

Untraceability means more costs for fighting fraud: In untraceable systems users cannot be linked to transactions. This means that for criminals who have broken the system it may be easy to stay anonymous.

Untraceable coin systems use blind signature schemes where the issuer does not know which coins are used. For the issuer it would be very difficult to detect criminals who “mint” their own coins. Only when more coins have been received than issued fraud will become obvious.

More security results in more complex systems: A simple counter system that only relies on tamper resistance will not cause any difficulties but in security. It can be seen as a question of time until a given system with a certain technology for providing tamper resistance is broken. Updating systems with the latest tamper-resistance technology comes with regular costs and the management overhead for expiring old user devices. If one enables the users of a counter-based system to transfer amounts off-line, the issuer might not even detect that counterfeit money is in use and it will be hardly possible to accuse someone of fraud. If tamper resistance is not used alone, protocols become more complex to allow security and other characteristics. This results in longer transaction times and more powerful devices.

Coin-based systems can be designed in a very secure way and essentially only the risks remain that the underlying cryptographic schemes are broken or that the issuer loses control over its secret key. However, paying the proper amount efficiently is a challenge. It also takes longer to load coins, as opposed to just updating a balance of a counter. In a system of cheques with counters, one is in between.

The more characteristics a system offers the more risky is its security: It is a general fact that the more complex a system is the more possible weak points it could have which have been overlooked during development. So a paradox situation is reached. Secure systems are getting more complex and may need additional features like divisible coins in order to be fungible, what again leads to risks with security (Anderson 1994).

Full control over the wallet leads to a trade-off with security of the issuer: In contrast to the users, who don’t want that the devices from the issuer (e.g. card) can

be withdrawn, the issuer might wish to have them withdrawn by a terminal if they are suspect. Only in traceable systems, blacklisting helps.

Unlimited validity will not be offered by issuers: It is unknown how future fraud with a given system security will develop. Issuers will not wish to have liabilities in terms of value in the hand of holders for many years because criminals may have broken the system and the damage may continue for years. To keep this risk manageable, issuers limit the validity of cash or systems to a few years. This is inconvenient as one may not be able to pay or as outdated value has to be exchanged in an on-line connection with the issuer.

Another disadvantage of long validity is that the issuer has to store more information for double spending detection or for loss tolerance.

Backward compatibility means compatibility with insecure systems: It is problematic to be on the one hand compatible with old systems and on the other hand to allow more security. This problem occurred for example with the German telephone cards which have been broken. Even after more secure cards have been sold, public phones still accept the old possibly broken cards, for the convenience of honest users (taz 1998).

5.3 Trade-offs with Untraceability

Security: Using double spending detection in untraceable systems means also using more complex protocols, where, e.g., the identity of a payer is added in encrypted form to her/his electronic cash. Users might not trust the implementation regarding that their identity is encrypted properly.

Without transferability special techniques are needed to keep the amount of received electronic cash secret: If users do not have the possibility to transfer money, they have to deposit it with the acquirer. The acquirer would therefore get the information of how much electronic cash each person receives. Also suggested solutions for transferability don't offer full privacy. Using value-less coins means that the issuer still gets the information of how many coins each user transfers. This system is also forward-traceable, which means that a payer can recognise his money if he sees it later in the chain of payments (Chaum, Pedersen 1993). An easy method to hide somewhat the amount of received electronic cash is to pay electronic cash to oneself, but nevertheless the bank could see the difference between the amount received and withdrawn. A better method would be to use anonymous communication to exchange received electronic cash against new spendable electronic cash anonymously.

Splitting coins for fungibility: This will lead to less privacy, as the coins derived out of each other can be linked.

Backward compatibility with traceable systems decreases anonymity: The "GeldKarte" in Germany comes for example with the problem that the new chip was integrated on the old eurocheque cards that also store the user's identification. The new chip would allow for pseudonymous payments, but the old information

of the cheque-cards is nevertheless communicated to the payee and can in any case be read by the terminals.

5.4 Trade-offs with Convenience

Convenience is a trade-off in itself: Offering additional features for a convenient use of the system often leads to inconvenience somewhere else in the system. Allowing for example users to transfer electronic cash will lead to more complex protocols and in the case of coin-systems to growing coins and thus larger devices having more memory. In both, longer transaction times will be required or more powerful and thus bigger computers. As one expert put it in our interviews: “And then you need a little carriage to drag it behind you.”

Unlimited off-line transferability using double-spending detection in an untraceable system is not possible: In addition to the problems of off-line usability alone, off-line transferability using double-spending detection leads to growing coins. With each transfer the encrypted identity of the actual payer has to be stored with the electronic cash. Because memory to store the cash will always be limited, this cash can only be transferred a limited number of times.

Alternatively, one would have to force holders to give certain pieces of value which reached a limit of transfers back, i.e. differentiate between transferable and unspendable money. The latter is not in line with today's rules of handling traditional cash, but not absurd, as received credit card payments or cheques cannot immediately be used for payments either. However, it would have to be displayed to the holder if money is unspendable.

Usability is always limited: It will be very difficult to make electronic cash as usable as traditional cash. There are devices needed to store and pay. Electricity will always be required. So electronic cash systems will always suffer from an operational risk that payments are impossible because parts of the systems are down.

Some characteristics will make electronic cash more difficult to handle than coins or credit cards. Think of electronic cash which cannot be spent since unlimited transferability is not possible or the need to handle one’s electronic device carefully.

An off-line transferable, loss-tolerant system doesn’t allow long validity: When the issuer refunds electronic cash, which is claimed as lost by a user he cannot be sure that the cash was not transferred to someone else and is still in use. To be sure that the cash cannot be used later one has to wait until the electronic cash has become invalid. It would not be loss-tolerant if refund can only be made after a long time. On the other hand it makes no sense to speak of transferable cash if the validity of the electronic cash is very short and it has to be returned to the issuer or acquirer after a short period. It would be also be very inconvenient for the user to check every received amount of electronic cash whether it has to be returned soon.

Transparency of financial status versus size: Instead of carrying around a “terminal” of one’s own with a PIN-pad and a display, roughly the size of a small

pocket-calculator, it might be more convenient to just hand over the card or simply insert it in a terminal.

Portability decreases functionality: The more computational power and special features are required the bigger the devices become. To implement characteristics like untraceability, off-line usability and transferability one might require more computational power than smart cards offer. A display and a keyboard would also be required so that one needs not trust the devices of the payee. A larger device may even offer the facility to keep logs on all transaction and to use the data directly in accounting software.

A possible solution which doesn't require the user to carry an additional bigger device is to integrate payment functions in mobile phones or watches[12]. But still then some people like children might not wish to carry expensive phones or watches with them all the time, thus a payment could be impossible.

Fungibility with many coins of smallest denomination is time consuming: The necessity to reload many coins makes reloading and payment time-consuming and inconvenient.[13] In future systems, reloading is a minor problem: It could be eased with faster devices or by reloading overnight via phone, or over the Internet. Still, payments would remain a bottleneck.

6 Existing Systems

If one wishes to replace traditional cash, our surveys came to the conclusion that one needs at least off-line usability, transferability and untraceability. Of course we cannot estimate precisely how big the share of traditional cash is one could replace if these three characteristics are not fulfilled. But we believe the reader will agree that these three are important characteristics. Today, there is not a single implemented prototype fulfilling them all. All Internet payment schemes, such as ecash, cannot be used off-line. All current smart-card purses neither provide untraceability nor transferability. Among all off-line usable systems ever built, only Mondex[14] provided[15] transferability, and only CAFE fulfilled untraceability. CAFE had limited transferability to "sibling" cards (e.g., for paying from parents to children to the merchant).[16]

---

[12] As PIN-pads on watches would have to be very small and thus difficult to use, a solution would be to enter an amount elsewhere, transmit it to the watch, display it and have approval on the watch with a small fingerprint reader.

[13] In CAFE one had 1.1 second per signature at 7 MHz, including the time for unblinding.

[14] The concept for NTT's ncash (Kawahara 1998) provides transferability without anonymity but it has not been built yet.

[15] Transferability is no longer advertised on the Mondex Web-site, probably because issuers felt it made the system less audible as in case of a manipulation it was not possible to record *all* transactions made.

[16] Digicash's ecash requires on-line verification and, like all Internet payment mechanisms, does not really provide untraceability since they do not provide connection anonymity as the payer needs a TCP/IP address to establish a connection with the payee.

7 Consequences

In the European deployments of stored value cards it became apparent that it is very difficult to replace traditional cash. Except in a Mondex trial, holders were not put into a position to transfer value to anybody who participates. Aiming at paying with a vending machine or standing in a queue without knowing how much funds are left is an inherent design problem to cards. Some issuers tried to accommodate for transparency by distributing card readers. Also usability restricted to a nation seemed odd at times other cards are increasingly accepted abroad. Usability of cards for payments over networks still is very seldomly seen.[17] From our own surveys we know that users are aware of the lack of functionality as compared to traditional cash. Accordingly, Tim Jones, then CEO of Mondex, said "Cash is a great product" (Financial Times of December 11/12, 1993). If one selects only some of the characteristics required one can sell in certain niches. But such issuers should not expect that they can replace traditional cash in general. It appears some have been trapped by their own sales promotion telling that their brand is a better form of traditional cash, with subsequent disappointment among holders, merchants and issuers when it was not usable, did not provide privacy, was not transparent, etc.

Wallets

Future electronic cash systems could, however, to a higher degree justify their name. Electronic wallets could have several MB EEPROM, a display, and a keyboard which solves several problems at once: One could provide transparency. One could store many coins. One could display how much funds one has and enter a PIN on one's own device. It would be possible to use the wallet-observer concept. One could also put the initiative for paying into the wallet, so that untrusted terminals cannot take money out. As compared to other payment instruments, immediate, off-line, irrevocable, untraceable payments would be possible. With low terminal costs, they can even be cost-effective for small sums.

Unfortunately very little experience has so far been made with wallet-like devices because the semiconductor, plastic-card, and banking industries were locked into the direction of using chip cards (Arthur 1989). The question arises if users are willing to use larger devices and pay for them. First in-depth interviews with 300 frequent card users in five European countries indicate that these are willing to pay ECU 15-50 for devices which replace several cards (Furger et al. 1998). Feedback from people who were demonstrated mock-ups was quite encouraging:

> "That's quite snazzy."
> "If I had a super gadget like this in my hands, of course I'd use it for a whole variety of things."
> "It's obvious that something like this is going to come eventually."
> "Could be something like a Swatch, the latest trend to have."

[17] The Dutch Telecom "KPN" trials a stored value card in the EU-project SEMPER for payments over the Internet. See <www.semper.org>.

"That's the future, this kind of thing."

However, no large trial was made so far[18]. The willingness to own such devices may increase once users will wish to make digital signatures securely, i.e., see what they sign, and enter approval on their own machines instead of on an untrustworthy machine, potentially infected by malicious code (cf. the German Digital Signature Law, Bundesregierung 1997). This would render the usability of digital signatures at different places possible, thus also at the point of sale. In order to reduce the marginal costs of wallets, one could incorporate the payment and signature functions into other devices, such as pocket calculators, phone sets, car locks, digital cameras and organisers (see Pfitzmann, Pfitzmann, Schunter, Waidner 1997, Weber 1998) which people increasingly carry around anyway. With biometric verification, in case only approval must be given, one would not need a keyboard and then even watches could be used.

Coins in Cards

As the banking industry focuses on cards, one could attempt to put untraceable electronic cash into a smart card, but without a counter. It might be possible to design a coin system based on blind signatures using card chips. To minimise storage space one can use divisible or multi-spendable coins. Privacy will suffer somewhat because some payments will become linkable. Robustness, transparency and loss tolerance, however, will be as difficult to achieve as in any other card system. Still, this could be a system with fairly low costs for the device on the side of the holder. However, for usability balance readers will need to be supplied, so why not build wallets in the first place?

Other

Besides the two approaches sketched, a third approach is to use more powerful intrusion detection for tamper-resistant modules and rely less on signatures. Systems exist against which no attack is known. Today such carriers are thicker than normal card chips. But issuers could rely more on tamper resistance than they do today. A forth possibility might be to search for new cryptographic techniques.

Is Electronic Cash Possible?

Even with today's techniques it will be possible to bring more characteristics, like off-line usability, transparency or untraceability, into new electronic cash systems. Untraceable systems for example would be much closer to our traditional cash than existing card payment schemes. Such systems could also be cost efficient for small values. However, to build a system offering all desirable characteristics would currently still be a hard task, as the trade-offs have shown.

---

[18] In CAFE only few transactions were made using the Infrared interface, and in the UBS St. Moritz trial the radio interface was not very robust.

8 Acknowledgements

The authors wish to thank David Chaum, Franco Furger, Tatsuaki Okamoto, Birgit Pfitzmann, Ingo Pippow, Jan Reichert, and Michael Waidner for many valuable discussions. The consumer surveys have been made for the CAFE project. The authors wish to thank our interviewers and more than 300 respondents (see Furger et al. 1998, Weber 1995, Weber 1997 for the results). This work was partially supported by the ACTS SEMPER project; however, it represents the view of the authors only.

9 Literature

Anderson, Ross; Kuhn, Markus: Tamper Resistance - a Cautionary Note. The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, November 18-21, 1996, pp. 1-11

Anderson, Ross: Why Cryptosystems Fail; Communications of the ACM 37/11, 1994, pp. 32-40

Antwerpen, C. van: Electronic Cash. Master's thesis, Centre for Mathematics and Computer Science (CWI), Amsterdam 1990

Arthur, Brian: Competing Technologies, Increasing Returns, and Lock-In by Historical Events. Economic Journal March 1989, pp. 116-131

Asokan, N.; Janson, Philllipe; Steiner, Michael; Waidner, Michael: The State of the Art in Electronic Payment Systems, IEEE Computer 30/9 (1997), pp. 28-35

Boly, Jean-Paul; Bosselaers, Antoon; Cramer, Ronald; Michelsen, Rolf; Mjølsnes, Stig; Muller, Frank; Pedersen, Torben; Pfitzmann, Birgit; de Rooij, Peter; Schoenmakers, Berry; Schunter, Matthias; Vallée, Luc; Waidner, Michael (1994): The ESPRIT Project CAFE. High Security Digital Payment Systems. Paper, ESORICS‘ 94

Boneh, Dan; DeMillo, Richard; Lipton, Richard: On the Importance of Checking Cryptographic Protocols for Faults; Eurocrypt '97, LNCS 1233, Springer-Verlag, Berlin 1997, pp. 37-51

Bonorris, Steven; Digital Money: Industry and Public Policy Issues; Institute for Technology Assessment; Washington, 1997

Bos, Jurjen; Chaum, David; SmartCash: A Practical Electronic Payment System. Report CS-R9035, Centruim voor Wiskunde en Informatica, Amsterdam 1990

Brands, Stefan: Untraceable Off-line Cash in Wallet with Observers. Crypto ‘93, LNCS 773, Springer-Verlag, Berlin 1994, pp. 302-318

Bundesregierung, die: Verordnung zur digitalen Signatur (Signaturverordnung - SigV), in der Fassung des Beschlusses der Bundesregierung vom 8. Oktober 1997; This ordinance was also published in Datenschutz und Datensicherheit DuD 21/2 (1997) 102-105

Bürk, Holger; Pfitzmann, Andreas: Digital Payment Systems Enabling Security and Unobservability. Computers & Security 8/5 (1989), pp. 399-416

Bürk, Holger; Pfitzmann, Andreas; Value Exchange System Enabling Security and Unobservability. Computers & Security 9/8 1990, pp. 715-721

CAFE: The CAFE Consortium: Technical Specifications: Architecture and Protocols - Final Report Volume IIA, CAFE (Esprit 7023) Deliverable PTS9364, April 1996

Chan, Agnes; Frankel, Yair; Tsiounis, Yiannis: Easy Come - Easy Go Divisible Cash. Eurocrypt' 98, LNCS 1403, Springer-Verlag, Berlin 1998, pp. 561-575

Chaum, David: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 1981, pp. 84-88

Chaum, David: Blind Signatures for Untraceable Payments. Advances in Cryptology, Proceedings of Crypto' 82, New York 1983, pp. 199-205

Chaum, David: Security without Identification: Transaction Systems to make Big Brother Obsolete. Communications of the ACM 28/10 (1985), pp. 1030-1044

Chaum, David; Fiat, Amos; Naor, Moni: Untraceable Electronic Cash. Crypto '88, LNCS 403, Springer-Verlag, Berlin 1990, pp. 319-327

Chaum, David: Achieving Electronic Privacy. Scientific American, August 1992, pp. 96-101

Chaum, David, Pedersen, Torben: Transferred Cash Grows in Size; Eurocrypt '92, LNCS 658, Springer-Verlag, Berlin 1993, pp. 390-407

Diffie, Whitfield; Hellman, Martin: New Directions in Cryptography. IEEE Transactions on Information Theory, 1976, pp. 644-654

Ferguson, Niels: Extensions of Single-Term Coins. Crypto '93, LNCS 773, Springer-Verlag, Berlin 1994, pp. 292-301

Furger, Franco; Paul, Gerd; Weber, Arnd: Survey Results. Paper, 1998 (Project CAFE). Available at <http:/www.iig.uni-freiburg.de/~aweber/>

Furche, Andreas; Wrightson, Graham: Computer Money: a systematic overview of electronic payment systems, dpunkt Verlag, Heidelberg 1996

Hayek, Friedrich von: Entnationalisierung des Geldes. Eine Analyse der Theorie und Praxis konkurrierender Umlaufsmittel. Mohr, Tübingen 1977

Japanese Ministry of Finance: Problems Related to the Circulation of Prepaid Cards. Report from the Research Group of the Ministry of Finance on Prepaid Cards. Tokyo 1989 (in Japanese)

Intellect Australia: OSA/MicroBank - The new dimension in convenience with flexible functionality, Intellect Australia Pty Ltd, 1 Brodie-Hall Drive, Bentley, Western Australia 6102, 1996.

Kawahara, Hiroto: Survey of NTT Electronic Money System. NTT, 1998

Mahony; Peirce; Tewary: Electronic Payment Systems, Artech House, 1998[UH3]

Merkle, Ralph: Secure communications over insecure channels (1974). Weber (1997), p. 163-164. Longer version of this paper was published in: Communications of the ACM. 1978, pp. 294-299

Okamoto, Tasuaki; Ohta, Kazuo: Universal Electronic Cash. Crypto '91, LNCS 576, Springer-Verlag, Berlin 1992, p. 324-337

Özalp, Nilgün: Entwurf von Benutzerendgeräten für elektronische Zahlungssysteme. Master's thesis, Fachhochschule Hildesheim/Holzminden 1996

Pedersen, Torben: Electronic Payments of Small Amounts. Security Protocols 1996, LNCS 1189, Springer-Verlag, Berlin 1997, pp. 59-68

Pfitzmann, Birgit; Waidner Michael: Loss-Tolerance for Electronic Wallets. 20th Int. Symp. on Fault-Tolerant Computing (FTCS) 1990, IEEE Computer Society Press, Los Alamitos 1990, pp. 140-147

Pfitzmann, Birgit; Waidner, Michael: Strong Loss Tolerance of Electronic Coin Systems. ACM Transactions on Computer Systems 15/2 (1997), pp. 194-213

Pfitzmann, Andreas; Pfitzmann, Birgit; Schunter, Matthias; Waidner, Michael: Trusting Mobile User Devices and Security Modules. Computer 30/2 (1997), pp. 61-68

Rankl, Wolfgang; Effing, Wolfgang: Smart Card Handbook. John Wiley & Sons, Chichester 1997

Rivest, Ronald; Shamir, Adi; Adleman, Leonard: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM 1978, pp. 120-126

taz, die tageszeitung: Millionenbetrug mit Telefonkarten; Berlin, taz Nr. 5534, 18.05.1998, p. 8

Wayner, Peter; Digital Cash, 2nd edition; Academic Press, London 1997

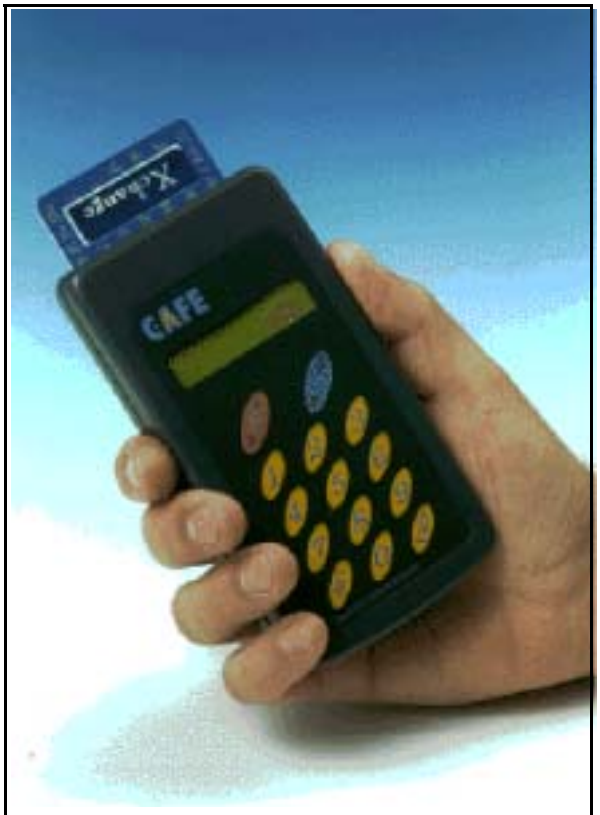
Weber, Arnd: See What You Sign. Secure Implementations of Digital Signatures. Trigala Sebastiano et al. (eds.): Intelligence in Services and Networks: Technology for Ubiquitous Telecom Services. Springer-Verlag, Berlin 1998. p. 509-520

Weber, Arnd; Carter, Bob; Pfitzmann, Birgit; Schunter, Matthias; Stanford, Chris; Waidner, Michael: Secure International Payment and Information Transfer. Towards a Multi-Currency Electronic Wallet. Frankfurt 1995 (Project CAFE)

Weber, Arnd: Soziale Alternativen in Zahlungsnetzen. Campus, Frankfurt, New York 1997

Appendix: Electronic Wallets

Proposal for a multifunctional wallet, thin enough to fit into shirt pockets. With drawers for smartcard security modules from telecom, railway company, savings banks, and certification authority. Size and functionality concluded from consumer research (cf. Özalp 1996).



CAFE-Wallet, with infra-red interface and normal chip card interface.

Backside of a variant of multi-functional wallet with opened drawer.