The ESPRIT Project CAFE — High Security Digital Payment Systems —[†]

Jean-Paul Boly[1], Antoon Bosselaers[2], Ronald Cramer[3], Rolf Michelsen[4], Stig Mjølsnes[4], Frank Muller[1], Torben Pedersen[5], Birgit Pfitzmann[6], Peter de Rooij[1], Berry Schoenmakers[3], Matthias Schunter[6], Luc Vallée[7], Michael Waidner[6,8]

Abstract. CAFE ("Conditional Access for Europe") is an ongoing project in the European Community's ESPRIT program. The goal of CAFE is to develop innovative systems for conditional access, and in particular, digital payment systems. An important aspect of CAFE is high security of all parties concerned, with the least possible requirements that they are forced to trust other parties (so-called multi-party security). This should give legal certainty to everybody at all times. Moreover, both the electronic money issuer and the individual users are less dependent on the tamper-resistance of devices than in usual digital payment systems. Since CAFE aims at the market of small everyday payments that is currently dominated by cash, payments are offline, and privacy is an important issue.

The basic devices used in CAFE are so-called electronic wallets, whose outlook is quite similar to pocket calculators or PDAs (Personal Digital Assistant). Particular advantages of the electronic wallets are that PINs can be entered directly, so that fake-terminal attacks are prevented. Other features are:

- Loss tolerance: If a user loses an electronic wallet, or the wallet breaks or is stolen, the user can be given the money back, although it is a prepaid payment system.
- Different currencies.
- Open architecture and system.

The aim is to demonstrate a set of the systems developed in one or more field trials at the end of the project. Note that these will be real hardware systems, suitable for mass production.

This paper concentrates on the basic techniques used in the CAFE protocols.

Keywords: Security in Applications (Financial); Security Versus other Requirements (Performance, Fault Tolerance).

[†] A preliminary version of this paper was presented at Securicom '94, Paris, June 1994 [BBCM 94].

[1] PTT Research, P.O. Box 421, NL-2260 AK Leidschendam, the Netherlands

[2] Katholieke Universiteit Leuven, Dept. Elektrotechniek E.S.A.T., Kardinaal Mercierlaan 94, B-3001 Heverlee, Belgium

[3] CWI, Kruislaan 413, NL-1098 SJ Amsterdam, the Netherlands

[4] SINTEF-DELAB, O.S. Bragstads Plass, N-7034 Trondheim, Norway

[5] Aarhus Universitet, Matematisk Institut, Ny Munkegade, DK-8000 Aarhus C, Denmark

[6] Universität Hildesheim, Institut für Informatik, Postfach 101363, D-31113 Hildesheim, Germany

[7] SEPT, 42 rue des Coutures, BP 6243, F-14066 Caen Cedex, France

[8] Universität Karlsruhe, Institut für Rechnerentwurf und Fehlertoleranz, Postfach, D-76128 Karlsruhe, Germany

1 The Project

1.1 Goals and Participants

CAFE ("Conditional Access for Europe") is a project in the European Community's program ESPRIT (Project 7023). Work on CAFE began in December 1992 and will probably be finished in December 1995. The consortium consists of groups for social and market studies (Cardware, Institut für Sozialforschung), software and hardware producers (DigiCash, Gemplus, Ingenico, Siemens), and designers of secure cryptographic protocols (CWI Amsterdam, PTT Research (NL), SEPT, Sintef Delab Trondheim, Universities of Århus, Hildesheim, and Leuven). The project coordinator is David Chaum for CWI.

The goal of CAFE is to develop innovative systems for conditional access, i.e., digital systems that administer certain rights of their users. The rights may be digital forms of passports, access to confidential data, entry to buildings, or — the most important example for CAFE — digital payment systems. A **digital payment system** is an information technology system for transferring money between its users. The market demands and the legal requirements of the member states of the European community on such systems are continuously studied by evaluations of existing comparable systems and by interviews with their users and experts from bank, consumer organizations, administrations, etc.

Within the project, the systems will actually be built, so that a realistic field trial can be carried out in the last year of the project.

1.2 Devices

The basic device for CAFE is an **electronic wallet**. This is a small portable computer, similar to a pocket calculator or a PDA (Personal Digital Assistant). It has its own battery, keyboard, and display, and its own means of communicating with other devices. In CAFE, the communication means will be an infrared channel. Every user of the system owns and uses her own wallet, which administers her rights and guarantees her security.

Particular advantages of the electronic wallets are that PINs can be entered directly, so that fake-terminal attacks are prevented. Furthermore, the users themselves agree on the amount paid by their device. This feature was considered very important by users in the surveys: They liked the secure feeling of not having to give their wallets into the hands of someone else, e.g., in a shop (which they would not do with their normal wallets containing cash either). They would also like to be able to look up their previous payments on the wallet.

In an application, there might be different types of wallets for users with different preferences. Compatibility is no problem because of the infrared communication. Luxury versions could combine the CAFE functions with those of a universal PDA, a mobile phone, or a notebook computer. Basic versions just contain the CAFE functions, and their keyboard only consists of a few buttons.

1.3 Basic Functionality

The basic CAFE system will be a prepaid offline payment system.

- **"Prepaid"** means that a user must buy so-called electronic money from an electronic money issuer and load it into her wallet before she can make payments.
- **"Offline"** means that no contact to a central database, usually at an electronic money issuer, is needed during a payment. The alternative, online payments, is far too costly for low-value payments because of the communication and the processing at the electronic money issuer.

This basic system is primarily intended for **payments** from wallets to POS (point-of-sale) terminals. Hence it allows just one transfer of the electronic money. This means that the payee must **deposit** the electronic money with an electronic money issuer before he can use it for his own payments (although he can, of course, locally verify that the electronic money is genuine, similar to traveler cheques).

Withdrawals of electronic money, i.e., loading it into an electronic wallet, are online transactions (usually against a debit to a normal bank account). They can be carried out from public ATM-like machines or from home terminals.

1.4 Additional Features

The basic CAFE system has the following additional features:

- **Different currencies**: It is both possible to store different currencies in the wallet and to exchange them during a payment.
- **Loss and fault tolerance**: If a user loses an electronic wallet, or the wallet breaks or gets stolen, the user can be given the money back (although it is a prepaid payment system!).

The basic CAFE system is an **open system** in many respects:

- Like cash, it is designed as a universal payment system: A user should be able to pay for arbitrary services by arbitrary service providers with her wallet. Examples are shopping, telephone, and public transport.
- Interoperability between any number of electronic money issuers is guaranteed (i.e., payments between clients of different electronic money issuers are possible). New electronic money issuers can join afterwards, and they can select some options according to their wishes.
- Only certain protocols are fixed, and not precise soft- and hardware components. Hence CAFE is open for new hardware platforms and can be integrated into other systems. The contactless communication is particularly useful here, and the system can also be used for payments over networks.
- No restrictions on the payers and payees need to be made, since the basic payment system is prepaid and of high security.

- Simple wallets can be cheap in mass production, and the use of both wallets and POS terminals can be simple. (The absolutely minimal version of a wallet displays the required amount to its user, and the user actively confirms that by pressing an "ok"-button on the wallet.) Thus from a practical point of view, too, nobody is excluded from the system.

2 The Special Security Goals of CAFE

The most important difference between the CAFE systems and other universal digital offline payment systems is in the very high security standards of CAFE. In this section, we explain the goals, and in the following section, we sketch the technical measures that make it possible to achieve all these goals simultaneously.

2.1 Multi-Party Security

Most existing digital payment systems are designed as systems with **one-sided security**: All participants have to rely on the trustworthiness of a single party, usually an electronic money issuer.

For payment systems, however, one-sided security is unsuitable, since it cannot offer legal certainty to any of the parties. For instance, let us consider ATMs (automatic teller machines): When a client uses her bank card at an ATM, her security is completely dependent on the trustworthiness of the bank: Everything she knows, the bank knows, too. Hence everything she can do, a dishonest bank insider can do, too. (There is nothing like a withdrawal order signed by the client that the bank had to store as a proof of transaction in conventional payment systems.) No court can decide whether a withdrawal was made by the client or such a fraudulent bank insider. Thus *neither* of the two parties "bank" and "client" has legal certainty about how a court would decide, and thus security from fraud by the other party.

Even if one accepts that at least some banks, as institutions, are more trustworthy than most clients, it does not change the situation: In this case, one would decide for the bank if it could prove by its internal security measures that insider fraud is impossible. However, it is currently highly improbable that any bank could show this to a satisfactory degree. On the one hand, many cases of insider fraud in spite of seemingly strong security measures have been reported [Ande 93, Neum 92]. On the other hand, the group of relevant insiders is just incalculably large: It comprises not only the bank employees, but also all those institutions and their employees who ever had anything to do with the design, production, installation, and maintenance of the hard- and software of the payment system.

If, on the other hand, courts would decide against the bank when in doubt, the banks would be completely insecure from dishonest clients.

To avoid such undecidable situations, the CAFE systems are designed as systems with **multi-party security** [Chau 85, PWP 90]: All security requirements of a party are guaranteed without forcing this party to trust other parties. In particular, mutual trust between parties with conflicting interests (like client and bank in the example) is not assumed. Ideally, a party only has to trust itself and the jurisdiction (and even the decision of a court can be verified). Multi-party security is beneficial for all parties:

- It increases legal certainty, since no undecidable situations as with one-sided security can occur. There is always enough evidence for an unambiguous decision.
- It decreases the security bottleneck of insider attacks.
- It makes the system more acceptable for potential users and is therefore a PR argument for the electronic money issuers.

Multi-party security has some implications on the design and manufacturing process as such (apart from the implications on the protocols described below):

- All designs (soft- and hardware) that are crucial for the security of a party must be available to this party for inspection. Hence secret algorithms are ruled out for CAFE (unless for internal procedures of the electronic money issuers).
- It must be ensured that parties can trust their own devices. Since most users can neither produce nor inspect their own wallets, there must be a sufficient number of competent and independent authorities that verify both the design and the devices themselves. The latter means that they verifies samples of the wallets as they are handed to the users, not near the manufacturer. Sufficient means that one can expect each user to trust at least one authority. Possible authorities are state-owned certification agencies, technical control boards like the German TÜV, and consumer organizations.

2.2 Data Protection

The CAFE payment systems are intended as mass systems for everyday use. Thus they should be particularly suited for frequent low-value payments, e.g., during the daily shopping, phone calls, and the use of public transport.

If one used, for instance, a credit card for each such payment, the credit card company would obtain an extensive profile of the user's behaviour. It would know where the user goes shopping at what time of the day (and maybe even what she buys), at what time she phones, where she goes by bus, etc. From the point of view of privacy, this is highly undesirable.

If one uses cash instead, the payer is **untraceable**: The coins used do not identify her, neither towards the payee nor towards the bank. Moreover, different payments of the same user are **unlinkable**, because one cannot see from two coins whether they were paid by the same person or not.

This form of untraceability is also desired for the users of the CAFE systems:

- In the basic CAFE system, the payee will be perfectly untraceable, i.e., neither the payee nor an electronic money issuer will learn the identity of the payer from the payment itself, and different payments are unlinkable [Chau 85].
- Just as with cash, this does not exclude that the payer is identified by other means, whether unintentionally or deliberately, e.g., by a cryptologic identification protocol.

In particular, one can fix an upper limit for the amounts that can be paid without identification. However, if all the security measures of the basic CAFE protocols are taken, this limit can be rather high, e.g., 2500 ECU, since the security of the electronic money issuer is independent of it.

Moreover, it will be useful to have an earlier limit beyond which payments must be online (e.g., 500 ECU), but are still untraceable, because that increases security for the electronic money issuers more, and does not infringe privacy.

- For payees, *no* untraceability is required. The reason is that the main use of CAFE will be purchases of goods or services from providers who are known to the payers anyway.
- In contrast to payments, withdrawals and deposits of electronic money are traceable, i.e., the client is identified towards an electronic money issuer.

The assumptions for privacy are the same as with the multi-party security against fraud: A user should not need to trust other parties for her untraceability.

Improved privacy is obviously beneficial to users, but also for electronic money issuers: On the one hand, it increases the acceptability of the system in the public and can therefore be a PR argument. On the other hand, it reduces the electronic money issuers' problem of keeping sensitive client data confidential, since there are not so many.

2.3 Loss and Fault Tolerance

For users, loss tolerance may be the most important special feature of the basic CAFE system. If a payer loses her wallet, or if it stops working or gets stolen, then with a usual prepaid system, she would lose all the money stored in the wallet. Loss tolerance means that she gets her money back.

3 Techniques

The most basic question is: how can one combine security for the electronic money issuer with offline payments, and moreover privacy and little trust in tamper-resistance? The question arises because electronic money is, after all, just bit strings. Hence even if a system is secure in the sense that users cannot produce new electronic money, i.e., new valid-looking bit strings, anybody who has seen such a bit string can copy it arbitrarily often and try to spend it more than once.

The optimal solution is as follows:

- As long as certain devices are tamper-resistant, it is completely impossible to spend electronic money more than once. This is called **strong integrity** for the electronic money issuers.
- Even if the tamper-resistance is *broken*, users who spend electronic money more than once are identified, and the fraud can be proved to them. (The only risk is then that the payer has disappeared or cannot pay the money back.)

- However, users need not trust those tamper-resistant devices (which must be provided by the electronic money issuers, whose security they protect, and whose interior the users naturally cannot verify) to protect their own security and privacy, too.

Note that online systems can achieve even more, namely that an attempt to spend electronic money more than once can be detected immediately by contact with a central database. This is why one usually fixes an upper limit on offline payments. Such online systems exist with full privacy [Chau 85, Chau 89, PWP 90].

We now consider the techniques used in such a solution one by one.

3.1 A Standard Measure: Digital Signatures Throughout

One standard measure that must be applied in many places in a payment system with multiparty security is digital signatures [DiHe 76, GoMR 88]. Such schemes simulate handwritten signatures for digital messages and are indispensable for systems with multiparty security.

Although we assume that most readers know what digital signature schemes are and some important constructions, such as RSA and the Schnorr scheme [RSA 78, Schn 91], so that we do not go into details, it has to be stressed that symmetric authentication schemes (often called MAC, *Message Authentication Code*, and based, e.g., on DES) are unsuitable as replacements for handwritten signatures as a matter of principle: The person who "signs" and the person who "tests" have the same keys, and thus a third party, such as a court, can never decide which of the two produced a certain authenticated message. Thus the recipient of an authenticated message cannot use it as credible evidence against the sender.

Note that every message of legal significance must be signed in a payment system to provide legal certainty. In particular, the wallet must send a signed order to withdraw electronic money to the electronic money issuer, and payees must get signed receipts for deposited money. Furthermore, the initialization of wallets must ensure that secrets used for generating signatures are not known to any other party.

3.2 Tamper-Resistant Devices: Guardians

The tamper-resistant devices that protect the electronic money issuers against double-spending of electronic money must be in the wallets of the payers: Since payments are offline, this is the only place where any attempt to spend the same money twice can be noticed. However, since the users are not supposed to trust the same devices, they are not "the wallets" themselves. Hence they are called **guardians.** In CAFE, the guardian is a smartcard chip with a crypto processor that is placed inside a wallet [Weik 93, GuUQ 92]. The guardian can either be fixed in the wallet or mounted on a smartcard, so that it can be exchanged — the CAFE protocols work with both these hardware platforms. In the field trial of CAFE, the guardian will have a Siemens crypto processor [BaPe 94].

How Wallets and Guardians Work Together

Since the owner of the wallet is not supposed to trust the electronic money issuer's guardian inside it, the guardian is not allowed to communicate with other devices on its own: It is only allowed to communicate via the wallet, and the wallet checks and suitably modifies the messages the guardian sends and receives.

This scenario where a wallet protects the interests of a user, and a guardian inside protects the interests of an electronic money issuer (or other service provider) was first presented in [Chau 92, ChPe 93, CrPe 94].

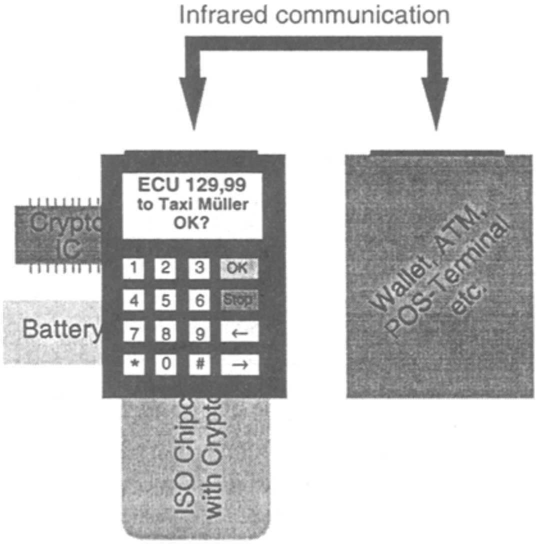

Figure 1 One hardware platform for a wallet-and-guardian protocol: The wallet is the bigger device with the keyboard and display; the guardian has been mounted on a smartcard and is inserted into the wallet. The guardian can only communicate directly with the wallet, and the wallet takes over the communication with the outside world via its infrared link.

How Guardians Protect the Electronic Money Issuer

The guardian can protect the electronic money issuer, because no transaction will be possible without its cooperation. In particular, no payment is accepted unless the guardian gives its okay, and for each unit of electronic money, the guardian gives its okay only once. The okay is something like a signature by the guardian, but a very restricted version from which neither the payee nor the electronic money issuer can derive which guardian made it, nor any other information about the payer. Details can be seen below when more about the protocols has been described.

3.3 Fall-Back Security: Cryptologic Protection

In this subsection, we describe the ideas for the fall-back security that is still guaranteed even if a user *breaks* the guardian. Breaking usually means reading out secret data, such as the keys the guardian uses to give its okay to transactions. Note that it does not matter if the guardian is destroyed in this process, because the user could build new fake guardians with the same secret information, and those would give their okay to incorrect transactions.

Of course, everybody hopes that smartcard chips will resist such attacks, but finally, it depends on the resources of a particular attacker. Hence the CAFE protocols provide a fall-back service for the electronic money issuer, where even in the unfortunate case where a guardian is broken, a user who uses this guardian to spend more money than allowed will be identified, and the identity of the user whose guardian was used for this fraud can be proved. (Note that it is necessary for multi-party security that the identity is not just found out, but proved, so that such a case could be handled in court.)

Since this protection for the electronic money issuer is not by tamper-resistant devices, it must be by **cryptologic protocols**.

Such payment systems where honest users have privacy, while double-spenders are identified, were first described in [ChFN 90]. More efficient variants were developed in, e.g., [FrYu 93, Bran 93, Ferg 94, Bran 94]. They are called **electronic offline coin** systems. Originally, they are all for a scenario with user-owned wallets only, without guardians. This is natural, since even in our scenario, we only need these protocols when the guardians are broken and thus no more protections for the electronic money issuer than the user's wallet.

We will now explain these protocols, starting with the basic primitives and working upwards until guardians are added again.

The Cryptologic Primitive: Blind Signatures

Payments where payers are untraceable all rely on **blind signature** schemes [Chau 85]. Here, signing is a protocol between two parties, the signer and the recipient. As a result of the protocol, the recipient obtains a message with a signature from the signer. The message, however, is *unknown* to the signer (thus "blind"), but the signer may be guaranteed that it has a certain form. Efficient constructions of blind signatures exist for RSA [Chau 85, Ferg 94] and the Schnorr signature scheme [ChPe 93].

The typical use of blind signatures in payment systems is as follows [Chau 85]: Electronic money is represented by messages of a certain form, which are signed by the electronic money issuer. Such signed messages are called *electronic coins*. The message signed is called the *coin number*. During withdrawal, the electronic money issuer's device makes a blind signature on a message unknown to the issuer, but of appropriate form. Thus the client obtains one electronic coin (and only one!), but the electronic money issuer does not know what it looks like. Hence, when a payee later deposits this electronic coin, the electronic money issuer cannot recognize it and therefore does not know which payer went shopping at this payee. This makes the payment untraceable (among all payments with electronic coins of the same denomination).

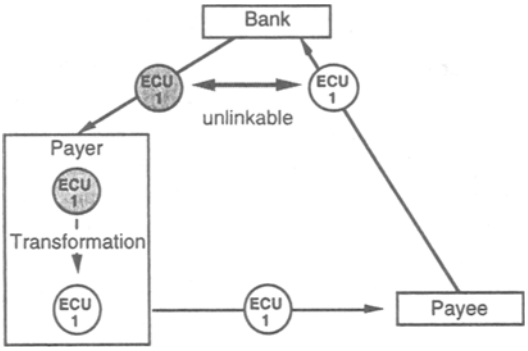

Figure 2 Basic payment system with blind signatures

"Off-Line Coins"

As describe so far, the system with blind signatures was only suitable for online payments: It guarantees that clients cannot produce new coins, but to guarantee that each coin is only spent once, a central database of spent coins (for coins from a certain electronic money issuer and issue period) must be queried.

The idea for off-line payments in [ChFN 90] is as follows: The identity of the payer is encoded into the coin number. (The blind signature protocol can guarantee, by something like a zero-knowledge proof, that the coin number is of a certain form, and this encoding of the identity will be the form required.) When a coin is used in a payment, the payer must divulge parts of the coding of the identity to the payee. If the same coin were used in two payments, the payer would have to divulge two different parts of the coding (with very high probability). Now the coding is constructed in such a way that from two parts, the identity can be found out, whereas one part alone does not give any information about the identity.

A simple version of such a coding, used in [ChFN 90], is that the identity I is encrypted perfectly with a one-time pad P, and the coin explicitly contains two parts. In one of them, the encrypted identity, $I \oplus P$, is contained, and in the other, the key P. Each part is further hidden with a commitment scheme, i.e., an encryption scheme with the following additional property: Nobody can find two keys such that the same ciphertext can be decrypted as two different messages with these two keys. Thus our coin number is constructed from two commitments $C(I \oplus P)$ and $C(P)$. In one payment,, the payer will have to open one of the commitments, and the content will be either only $I \oplus P$ or only P, which does not say anything about the identity. If, however, the other part has to be opened in another payment, the identity is found out.

In order to detect such cheating payers, each electronic money issuer must store all deposited coins for a certain time and search for pairs. This can be done in parallel with the usual clearing between different issuers.

This should give an idea how this sort of system works — describing the full system is beyond the scope of this paper. Note that in the basic form we presented, the probability that the payee is found out would only be $^1/_2$ in two payments, and a payer and a payee together could cheat. All this is taken care of in the full system. Much more efficient versions were described in [FrYu 93, Bran 93, Ferg 94, Bran 94].

Furthermore, some additional signatures are hidden in the payment protocols: On the one hand, the wallet signs to whom it pays a coin (thus, only the intended payee can deposit the coin). On the other hand, if the pure identity were contained in a coin, it would prove nothing if one found it out — anybody could have constructed such a coin. Instead, there is a kind of signature hidden that only the payer could have constructed.

The CAFE protocols are based on the system from [Bran 93, Bran 94], but with some modifications.

Adding a Guardian

If the "off-line coin" systems are combined with a guardian, the guardian prevents that an electronic coin is spent twice, as long as it is unbroken. To do this, the coins are not given to the wallet alone in a withdrawal. Instead, one part is held by the wallet, and another part by the guardian. These parts together form the secret key needed to sign the spending of a coin. The electronic money issuer can ensure that the guardian is in fact involved by requiring something like a signature of the guardian that it holds a part of this secret key, where the key is identified by a one-way image.

All this is more complicated because the messages from the wallet to the electronic money issuer are not allowed to carry any secret information, i.e., the wallet must ensure that there is no covert channel between the guardian and the electronic money issuer. Hence all the messages are transformed in transit. The first such protocols were described in [Chau 92, ChPe 93, Bran 93, Fergl 94, Bran 94].

Efficiency Improvements

So far, we described a system that resembled cash coins in the following respect, too: An amount to be paid will usually be paid with a combination of electronic coins of certain fixed denominations. This is the solution with optimal security and privacy in the long run, but for current smartcard chips it is a bit hard. Moreover, one has the problem of change, which is non-trivial in a system which distinguishes payers (clients with wallets) and payees (POS terminals).

Hence CAFE uses a mixture of several additional measures. Two related approaches are known from [OkOh 92, Fergl 94]: One can construct coins that can be split into smaller amounts if necessary (e.g., an 8-ECU coin into one 4-ECU coin and two 2-ECU coins), or coins that can be spent more than once (e.g., one would pay 8 ECU for a 1-ECU coin that the guardian and the cryptologic measures allow to spend 8 times). These measures reduce the unlinkability of payments, but not the integrity.

A different measures is known from [BoCh 90]. It corresponds to the use of cheques instead of coins in the following sense: The amount is only entered to the "electronic coin" and signed during the payment. Now the guardian has to keep a counter of the money that is still there, and it will only play its part in signing during payments if the cheque is written out up to this amount. This measure decreases the cryptologic fall-back security for the electronic money issuer in case the guardian is broken.

3.4 Loss and Fault Tolerance

For users, loss tolerance may be the most important special feature of the basic CAFE system. With a usual prepaid system, a payer who lost her wallet would lose all the money stored in the wallet. The same would happen if the wallet stopped working or got stolen. Loss tolerance means that she gets her money back.

The basic idea for loss tolerance is to keep a backup of the user's electronic money somewhere outside the wallet [WaPf 90, WaPf 91]. This backup must not infringe the privacy of the payer, hence it must be on a backup card of the user or in encrypted form at her electronic money issuer. If a user loses her wallet, the backup is evaluated in cooperation of the user and the electronic money issuer: The electronic money is reconstructed, and that part of it that has not yet been spent is credited to the user's account. What has been spent (usually between the last withdrawal and the loss) can be detected by comparing the reconstructed electronic money with the deposits. Note that the backups do not infringe the security of the electronic money issuer either: The user cannot use the copy of the electronic money in payments, since there is no guardian to give its okay to such a transaction.

In the optimal case, a user gets all the lost money back. One factor limit loss tolerance, however:

- If a lost or stolen wallet can be used *without* user identification, such as a PIN, the owner cannot get the money back that the finder or thief of the wallet spends. (But if the wallet was just broken, the money can be given back.) To limit this loss, one has to limit the amount that can be spent without intermediate entry of a PIN.

For this purpose, CAFE will offer optional payment PINs. (Withdrawals are protected with PINs anyway.) The users are urged to choose their payment PIN different from their withdrawal PIN, because payment PINs are more likely to be observed. If a user cannot remember two PINs, it is still better to have an easy to remember payment PIN or to write it down somewhere than to have none at all. (The withdrawal PIN, in contrast, must be kept more secure.)

The use of the payment PINs will be very flexible: They can be used either during a payment or for unlocking a certain amount *before* one or more payments. This is useful since the payment itself may have to be done in a hurry or in a place where the PIN could be observed too easily. The user can also lock the amount again.

Apart from tolerating losses or faults of complete wallets, the system also tolerates interruptions of individual transactions, either because the communication is interrupted or because one of the devices breaks down or loses power during this transaction (unintentionally or deliberately).

3.5 Phone Ticks

The basic CAFE protocols contain special measures for paying phone ticks, i.e., many payments of very small amounts to the same payee in very fast succession. Since there is no reason to require unlinkability of the payments of the individual ticks, they are all parts of the same coin in a special way.

4 Outlook

Until mid 1994, the end of the first half of the project, the work on CAFE concentrated on market and social studies, the design of the basic CAFE system, and preparations for the actual implementation. A software package demonstrating the CAFE features is already available*.

The second half of the project starts with the implementation, in particular of the hardware components. In particular, Gemplus wallets and smartcard(chip)s with Siemens crypto processors will be used. Then a field trial can follow. It will be accompanied by studies of user reactions.

In parallel, the time will be used for further developments in the design of the basic CAFE system and the development of other conditional access systems on the basis of CAFE wallets and guardians.

Acknowledgment

This presentation of the project (by the secure protocols group) is based on [Waid 94, WaWe 94]. We also thank the other partners in the project for their share of the work.

References

Ande 93 Ross Anderson: Why Cryptosystems Fail; 1st ACM Conference on Computer and Communications Security, acm Press, New York 1993, 215-227.

BaPe 94 Peter Bauer, Heribert Peuckert: Chipkarten mit Kryptographie erschließen neue Anwendungsfelder; Siemens-Zeitschrift Special, FuE, Frühjahr 1994, 17-20.

BBCM 94 Jean-Paul Boly, Antoon Bosselaers, Ronald Cramer, Rolf Michelsen, Stig Mjølsnes, Frank Muller, Torben Pedersen, Birgit Pfitzmann, Peter de Rooij, Berry Schoenmakers, Matthias Schunter, Luc Vallée, Michael Waidner: Digital Payment Systems in the ESPRIT Project CAFE; Proc. of Securicom '94, Paris, June 1994.

BoCh 90 Jurjen Bos, David Chaum: SmartCash: a Practical Electronic Payment System; Centrum voor Wiskunde en Informatica, Computer Science/Departement of Algorithmics and Architecture, Report CS-R9035, August 1990.

Bran 93 Stefan Brands: An Efficient Off-line Electronic Cash System Based On The Representation Problem; Centrum voor Wiskunde en Informatica, Computer Science/Departement of Algorithmics and Architecture, Report CS-R9323, March 1993.

Bran 94 Stefan Brands: Untraceable Off-line Cash in Wallets with Observers; Crypto '93, LNCS 773, Springer-Verlag, Berlin 1994, 302-318.

Chau 85 David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030-1044.

Chau 89 David Chaum: Privacy Protected Payments – Unconditional Payer and/or Payee Untraceability; SMART CARD 2000: The Future of IC Cards, Proceedings of the IFIP WG 11.6 International Conference; Laxenburg (Austria), 19.-20. 10. 1987, North-Holland, Amsterdam 1989, 69-93.

Chau 92 David Chaum: Achieving Electronic Privacy; Scientific American (August 1992) 96-101.

ChFN 90 David Chaum, Amos Fiat, Moni Naor: Untraceable Electronic Cash; Crypto '88, LNCS 403, Springer-Verlag, Berlin 1990, 319-327.

ChPe 93 David Chaum, Torben Pryds Pedersen: Wallet Databases with Observers; Crypto '92, LNCS 740, Springer Verlag, Berlin 1993, 89-105.

* Please contact Ray Hirschfeld, CWI, Phone +31 20 592 4049, e-mail cafe@cwi.nl.

CrPe 94 Ronald J. F. Cramer, Torben Pryds Pedersen: Improved Privacy in Wallets with Observers (Extended Abstract); Eurocrypt '93, LNCS 765, Springer-Verlag, Berlin 1994, 329-343.

DiHe 76 Whitfield Diffie, Martin E. Hellman: New Directions in Cryptography; IEEE Transactions on Information Theory 22/6 (1976) 644-654.

Ferg 94 Niels Ferguson: Single Term Off-Line Coins; Eurocrypt '93, LNCS 765, Springer-Verlag, Berlin 1994, 318-328.

Fergl 94 Niels Ferguson: Extensions of Single-Term Coins; Crypto '93, LNCS 773, Springer-Verlag, Berlin 1994, 292-301.

FrYu 93 Matthew Franklin, Moti Yung: Secure and Efficient Off-Line Digital Money; 20th International Colloquium on Automata, Languages and Programming (ICALP), LNCS 700, Springer-Verlag, Heidelberg 1993, 265-276.

GoMR 88 Shafi Goldwasser, Silvio Micali, Ronald L. Rivest: A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks; SIAM J. Comput. 17/2 (1988) 281-308.

GuUQ 92 Louis Claude Guillou, Michel Ugon, Jean-Jacques Quisquater: The Smart Card: A Standardized Security Device Dedicated to Public Cryptology; Gustavus J. Simmons: Contemporary Cryptology – The Science of Information Integrity; IEEE Press, Hoes Lane 1992, 561-613.

Neum 92 Peter G. Neumann: Inside Risks: Fraud by computers; Communications of the ACM 35/8 (1992), 154.

OkOh 92 Tatsuaki Okamoto, Kazuo Ohta: Universal Electronic Cash; Crypto '91, LNCS 576, Springer Verlag, Berlin 1992, 324-337.

PWP 90 Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; Datenschutz und Datensicherung DuD 14/5-6 (1990) 243-253, 305-315.

RSA 78 R. L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems; Communications of the ACM 21/2 (1978) 120-126, reprinted: 26/1 (1983) 96-99.

Schn 91 C.P. Schnorr: Efficient Signature Generation by Smart Cards; Journal of Cryptology 4/3 (1991) 161-174.

Waid 94 Michael Waidner: CAFE – Conditional Access for Europe; 4. GMD-SmartCard Workshop, 8.-9. Februar 1994, GMD Darmstadt; Multicard '94, Berlin, 23.-25. Februar 1994.

WaPf 90 Michael Waidner, Birgit Pfitzmann: Loss-Tolerance for Electronic Wallets; Proceedings 20th International Symposium on Fault-Tolerant Computing (FTCS 20), Newcastle upon Tyne (UK), 140-147.

WaPf 91 Michael Waidner, Birgit Pfitzmann: Loss-tolerant electronic wallet; David Chaum (ed.): Smart Card 2000, Selected Papers from the Second International Smart Card 2000 Conference, North-Holland, Amsterdam 1991, 127-150.

WaWe 94 Michael Waidner, Arnd Weber: Europäisches Industrie- und Forschungskonsortium entwickelt neuartiges Zahlungsverfahren; will be published in: Datenschutz-Berater, 1994.

Weik 93 Franz Weikmann: Chipkarten – Entwicklungsstand und weitere Perspektiven; PIK, Praxis der Informationsverarbeitung und Kommunikation 16/1 (1993) 28-34.