Mobile Electronic Commerce:
Research Investigations into Loading and Payment Functionality in Wireless Wallets

Ralf Keller, Guido Zavagli, Jens Hartmann and Fiona Williams
Ericsson Eurolab Deutschland GmbH

Abstract

Mobile users will increasingly demand access to Electronic Commerce services. Therefore existing technologies have to be investigated if they can be used unchanged in mobile Electronic Commerce or whether they have to be adapted to the mobile environment. This article presents an overview on the state of the art of Smart Cards for mobile Electronic Commerce. The GeldKarte system and the Home Banking Computer Interface are new concepts that will play an important role in Electronic Commerce. Both concepts were developed with stationary devices in mind and we motivate the need to have both services implemented on mobile devices. We outline how the GeldKarte system can be directly integrated into a Wireless Wallet. Based upon this we discuss several alternatives to the straightforward approach and describe in detail how both the Home Banking Computer Interface and the GeldKarte system could be combined on mobile devices to offer advanced mobile Electronic Commerce services.

1 Introduction

Mobile Electronic Commerce (MEC) is a general concept covering any business transaction executed electronically between at least two parties, whereas at least on of these parties is mobile. Being mobile implies for us that the mobile party uses a wireless transmission medium at least on the first link for the communication with the other parties.[1] Therefore MEC is a subset of Electronic Commerce as defined in [17], but it also comprises direct and indirect electronic trading of goods, i.e., is not limited in its principle functionality.[2]

Mobile users will increasingly demand access to Electronic Commerce services. Therefore existing technologies have to be investigated if they can be used unchanged in mobile Electronic Commerce or whether they have to be adapted to the mobile environment.

Smart Cards are one basic technology for mobile Electronic Commerce. Smart Cards are used today in many applications and are small enough to be carried while being mobile. The GeldKarte system is also based on the Smart Card technology. Both the GeldKarte system and the Home Banking Computer Interface are new concepts that will play an important role in Electronic Commerce. Both concepts were developed with stationary devices in mind and we need to investigate if we have to implement them on mobile devices.

---

[1] That makes the difference to a nomadic party that could also be hooked to the fixed network but with different locations over the time.

[2] Indirect E-Commerce means the electronic ordering of tangible goods; the actual goods are however delivered in a traditional form. Direct E-Commerce means the electronic ordering and delivery of intangible goods (electronic material, e.g., software, games, video, etc.).

This paper presents in section 2 an overview on the state of the art of Smart Cards for mobile Electronic Commerce. We motivate in Section 3 the need to have the GeldKarte system and the Home Banking Computer Interface implemented on mobile devices. Section 4 describes how the GeldKarte system can be directly integrated into a Wireless Wallet. Based upon this we discuss several alternatives to the straightforward approach and describe in detail how both the Home Banking Computer Interface and the GeldKarte system can be combined on mobile devices to offer advanced mobile Electronic Commerce services. The paper concludes with an outlook.

2 State of the Art of Smart Cards for Mobile Electronic Commerce

The fast evolving developments in the Smart Card area (e.g. Multos, Java Card) as well as the increasing number of mobile telecommunication users offer a lot of new sophisticated opportunities for applications in the E-Commerce world. At present a handful of leading cellular operators together with some major banks are developing the capability to offer mobile phones fitted with electronic purses or wallets.

In this chapter we describe two already existing mobile financial service solutions, namely the Mondex technology and the Barclay Card Phone 2.

2.1 Mondex

Mondex is one of the most interesting Smart Card cash schemes. It stores electronic cash on an encrypted microchip in a plastic card. Mondex requires that value is transferred from one card to another one. However, Mondex do not require on-line verifications.

The first of the product development specifications for Mondex was issued in April 1994. Currently Mondex cards are issued by multiple banks in Canada, Hong Kong, New Zealand and in the United Kingdom. Mondex International, who is responsible for managing the Mondex technology, is now owned by 51% by MasterCard International.

A Mondex Card is a Smart Card, which has been programmed to function as an *electronic purse*. The electronic purse can be loaded with value, where it is stored until it is used as payment for goods or services at retailers or service outlets or transferred to another Mondex Card [6]. The electronic purse can also be locked using a four-digit personal code so that only the card's owner can access the value on it, and so that it has no value if it is lost or stolen. The cards can be recharged at Automatic Teller Machines (ATMs) and with specific telephones.

The Mondex Smart Cards are produced by Dai Nippon Printing Company, and contain 8-bit Hitachi H3/310 microprocessor, 16K ROM, 512 bytes of RAM and 8K EEPROM for data storage.

The Mondex approach is fundamentally different from other schemes. Mondex uses a secure value transfer protocol that rely on a unique *digital signature* which is generated by the chip on the card and which can be recognised by the other Mondex card involved in the transaction [6]. The digital signature scheme guarantees that the cards involved are genuine Mondex cards and that they are dealing with untampered Mondex signals. This recognition process also identifies the party for which the cash is intended. Therefore a third party cannot intercept funds without detection.

The security mechanism implemented on each Mondex card can *be gradually updated* or improved, e.g., with new generation of cryptography, without changing the cards already issued immediately. When cards are issued, each contains two different and separate security schemes, A and B - each comprising one or more keys or one or more cryptographic algorithms - or other security features. Initially the cards will be set to operate on scheme A but have the potential to switch over to B when instructed. The

switch instruction to B will be performed by new issued cards which have the schemes B and C. Each time a new card encounters an old one, it will automatically trigger it to go over to the B scheme. The old card will also get an instruction to switch another old card to operate on scheme B. The original A/B cards can be gradually withdrawn in the course of ordinary replacement or upgraded and replaced with B/C cards.

For each currency within the Mondex system, there will be a single originator body - either a company established by participating commercial banks or a country's central bank - which alone is able to manufacture value in that currency. The originator controls the amount of value denominated in its currency which is in circulation, both domestically and abroad. Finally value destruction will take place at this single source. Originators will set a maximum limit on the value in their currencies, which can be held in any level of Mondex card, in any country and, at any point in time.

The Mondex Telephone allows direct access to a bank account. In effect, the telephone becomes a personal ATM giving 24-hour cash availability from the comfort of home, the office, the shops, the car, in fact anywhere with a mobile Mondex compatible phone. The Mondex Telephone allows the transfer of money across the telephone line. This enables payments to be made to other Mondex cardholders around the world. The Mondex Telephone also facilitates easy use of the locking and statement functions.

2.2 The Barclaycard Phone 2

With the help of a Smart Card developed by Gemplus according to the GSM [15] Phase 2+ item SIM Application Toolkit and a special version of Alcatel's One Touch Pro mobile phone, the British GSM network operator Cellnet and Barclaycard have launched a new service called Barclaycard Phone 2 (BC2).

The SIM Application Toolkit allows the SIM card to manage most of the functions of the mobile phone, to add and edit application menus, to set-up calls, to send short messages, to display company logos, etc. Basically, it allows the SIM card and the GSM phone to have a meaningful conversation in a common language.

The big advantage of this service is that the user has only to press an unique button, and a whole series of additional sub-menu options, all of which are geared towards accessing personal financial information on either the user's Barclaycard or Barclay Bank current or deposit account, is available.

The 32 value-added services accessible via the BC2 are all stored on the SIM card and, for this reason the memory of the SIM card is locked and cannot be used to store personal phone numbers [16].

For security reasons the user has to enter an additional PIN after selecting a specific service. This PIN and the number of the chosen service are send within a voice call to the account database. Thereafter the database will send an encrypted message via SMS for the presentation of the personalized service on the display of the mobile phone.

3 New Basic Concepts for Mobile Electronic Commerce

Among the new concepts arising at the horizon that will play an important role in E-Commerce in the future are Smart Cards and home banking services. Smart Cards can be used, e.g., for authentication, for the storage of private or public keys or as a data container holding private data. Home banking services offer access to a great variety of banking and other financial services from private personal computers. In this section, the German GeldKarte system and the Home Banking Computer Interface will be described as examples for new concepts.

3.1 The GeldKarte of the German banking industry

At the end of 1996, the German banking industry introduced new bankcards, so-called GeldKarte, to all their customers. The deployment of these Smart Cards is coordinated through the central banking agency ZKA (Zentraler Kreditausschuß). The four financial institution groups making up the ZKA board are private banks, public banks, coop banks and saving and loans associations [4]. They are the holders of purse charging accounts. The loading transactions of the cardholders are booked against these accounts. Each of these groups operates its own data-monitoring center.

The countrywide rollout followed a successful trial in the cities of Ravensburg and Weingarten. Several German banking institutions and numerous retailers took part in the pilot that went on from March to August 1996. Close to 80 000 cards were issued, which could be reloaded up to a maximum of 400 DM. Between September and December 1996, 25 millions of these electronic purses were issued to bank customers in Germany. By the end of 1997, a total of 55 millions Smart Cards will have been distributed.

The infrastructure of the GeldKarte system is made of Smart Cards, terminals, background systems and security management. An overview of the GeldKarte system is depicted in Figure 1.

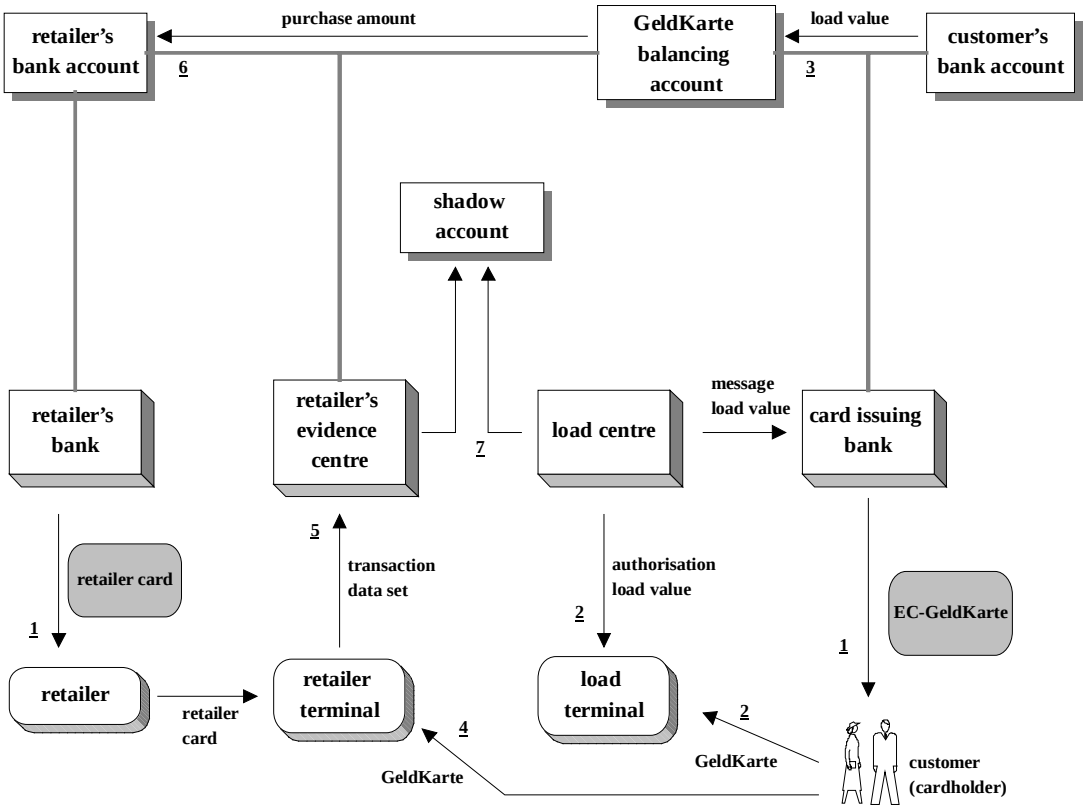

Figure 1 Overview of the EC-GeldKarte system

The current version of the *Eurocheque (ec)-GeldKarte* is a hybrid card containing a magnetic strip on the back and a chip on the front side. This is because it will take some time to replace or upgrade all of the old magnetic stripe terminals. It supports two new functions:

- PIN-based and on-line loading
- Non-PIN-based, off-line payment

The WertKarte is a special version of the GeldKarte that can be acquired at a bank without being linked to an account at a bank. Stored in the chip is an offline limit associated with a reference account number being tracked by the background banking system. It works the same as the GeldKarte, but supports a completely anonymous form of payment.

The German cash card projects are aiming at the substitution of the electronic cash as it is used today especially in the segment of small amounts between 5 and 25 Marks (3 to 17 US$). The basic application of the GeldKarte will be its usage as an electronic wallet. The client can download money (up to 400 Marks [270 US$]) from his/ her bank account at the usual ATMs, which have been equipped with devices supplying the extra functionality. Every amount downloaded is credited to a special balancing account at the issuing organization and reported to the Evidence Center. The latter has the task to trace a shadow balance logging all downloading and payment activities. This set-up allows the rapid detection of a possible manipulation of the system and enables the refunding of clients if their cards have been damaged.

The cash-less payments are anonymous without any PIN checks. The downloading is secured using an encryption protocol thus allowing a higher security than the current magnetic strip cards. The so-called "challenge response method", comprised of hard- and software, permits a check on validity and authenticity within the implemented microprocessor. All commands are integrated in the memory so that a programming from outside or a retrieval of the encryption keys is not possible, at least within a justifiable amount of time. Every attempt to manipulate the key ends up in a destruction of all data stored in the security sector, thus making the card useless.

Transaction costs for the merchant are 0.3 percent of the payment amount or a minimum fee of 5 Pfennig (0.03 US$). According to a SIZ 1996 report traditional cash transactions are at 16 to 28 Pfennig (0.10 to 0.18 US$) per transaction thereby exceeding the cash card fees, a fact that a lot of vendors do not take into consideration.

The cash card functionality is already extended, granting interested parties (such as department stores, public transport or theatres) a certain data space on the chip, enabling them to use the card additionally for special discount or ticket information. The German Sparkasse will use the chip for the authentication of the cardholder applying the German home-banking standard HBCI (Home Banking Computer Interface). This will foster the use of tele banking and abolish the use of PINs (Personal Identification Numbers) and TANs (Transaction Numbers), thus improving user comfort and security.

3.2 Home-Banking Computer Interface (HBCI)

Home Banking in Germany is available already since 1983 due to T-Online service. The prognosis was that the service would achieve 1 million users by 1986. In fact this number was crossed almost 10 years later, in January 1996 - just 10 years difference. By the end of 1997 2 millions users are supposed to use home banking on T-Online. Last year the first field trials began to introduce Home Banking in the Internet. The first German bank, which started to provide its services in the Internet was Deutsche Bank, followed by HypoBank and many others.

The beginnings where sometimes difficult. For example, first implementation of the Sparkasse Internet banking service used so-called “Human Firewall” – all transfer orders or account queries, got from the web side, were printed at the bank office and manually processed. Then the results were posted to the users through email.

The Home-Banking Computer Interface (HBCI)[1] is a new standard for handling the communication between intelligent customer systems and corresponding bank systems

to exchange home-banking transactions in Germany, though international standardization is planned. At the beginning of 1997 it was accepted by ZKA and submitted as a proposed standard to German government and standardization bodies. First implementations of HBCI are already available, e.g., from Faktum [13].

The transmission of the data is done over a net data interface, which is based on flexible delimiter syntax, similar to UN/EDIFACT. HBCI shall be used by the private customers and in the market of small and medium enterprises, which at present rely on such applications implemented for the German T-Online service. Furthermore, the HBCI system security design makes it suitable for its use on the insecure Internet, in addition to other network infrastructure.

Generally, an HBCI message consists of message header and trailer, signature header and trailer, and a number of message segments indicating the banking part of several business transactions. Optionally there exist a ciphering header for the ciphering of data and eventually additional signature headers and trailers for multiple signatures. In the first versions, many of the classic business transactions have been defined in HBCI, e.g., single credit/debit note, collective credit/debit note, balance inquiry, and sales statistics. More transactions will be added in the next versions, e.g., loading of the GeldKarte. See [14] for an overview on the standard (the actual version is 2.0).

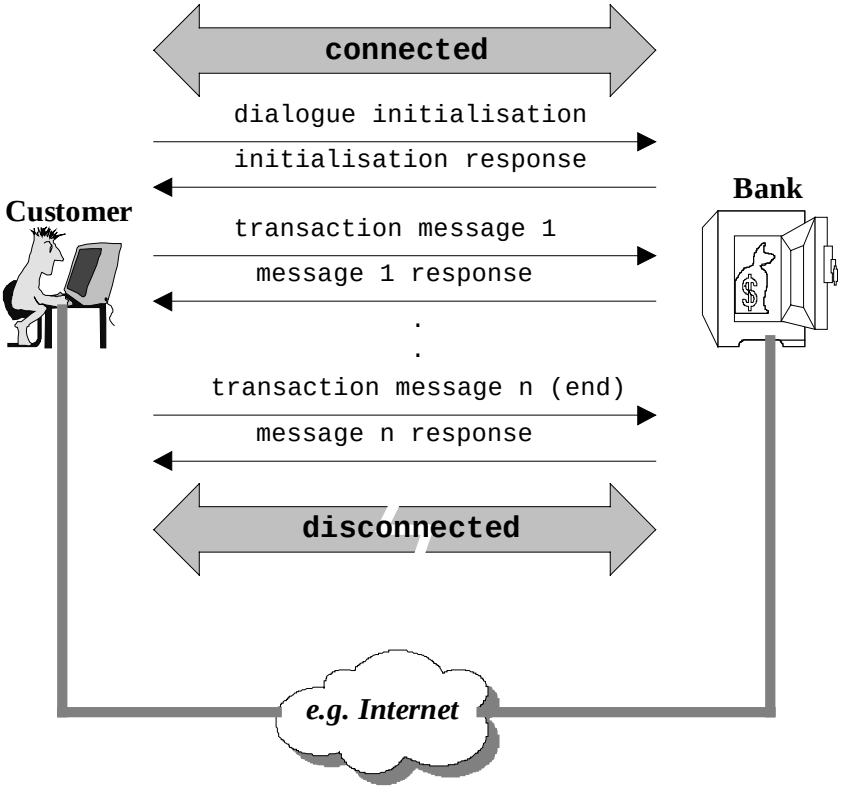

Figure 2 Dialogue flow in HBCI

The HBCI message can be transferred in form of a customer or bank message as an isolated unit within HBCI dialogue flows, as shown in Figure 2 [11]. Basically, HBCI dialogues are synchronous, i.e., before the customer sends the next message, the bank must answer the previous customer's message. In order to ensure the security of the

message exchanges during the transaction, mutual authentication of both parties, i.e. the customer and the bank, must be performed in a dialogue initialization procedure. Additionally, during the initialization, ciphering and compression methods are negotiated and other parameter data are adjusted. Specific methods are applied to synchronize the communication between the parties thereby avoiding the loss of the transaction state after, e.g. a network crash.

HBCI employs both symmetric (DES) and asymmetric (RSA) cryptography [12] for its security mechanisms. The authorization mechanism can be performed using the DES algorithm in combination with a chip card (e.g. Smart Card) or using the RSA algorithm with specialized software installed on the customer system. The mutual authentication of both parties and the proof of the origin of a message (non-repudiation) are performed with the digital signature technology. In addition, the digital signature is used to ensure the integrity of each HBCI message by calculating a specific cryptographic checksum of the message and include it in the signature trailer segment of the message using DES or RSA algorithm. Finally, the Triple-DES algorithm is used for the encryption of data generally. The target system of HBCI is to use the RSA public-key cryptography in combination with a certified chip card.

In the next section, the integration of the GeldKarte system in a mobile environment will be discussed. First a straightforward approach will be presented, followed by a more advanced combination of HBCI and GeldKarte.

4 Wireless Wallet

This section describes two alternatives for the realization of the Electronic Commerce concepts described in the previous sections. From the presented concepts, we will focus on the GeldKarte system. As mentioned before, the main operations that can be performed with the GeldKarte are on one side loading the GeldKarte, and on the other side performing payments. First studies related to the current introduction of the GeldKarte in Germany have shown that usage is less than expected. Besides some technical reasons – merchants have to acquire specific GeldKarte terminals – one major limitation is seen in the fact that the GeldKarte can currently only be loaded at the usual ATMs. The advantages of the GeldKarte compared to normal cash are not obvious to the user.

In order to overcome the problem of downloading money to the card at ATMs, we propose and discuss concepts allowing the GeldKarte loading transaction to be performed with the help of a mobile device. Such a device, together with the GeldKarte, then becomes a so-called Wireless Wallet. This wallet should enable loading of the GeldKarte, and also provide the possibility to perform payments. In the framework of this paper, we will discuss only the loading transaction.

4.1 GeldKarte Architecture

Figure 3 summarizes the general architecture of the entities involved in a GeldKarte loading transaction. There are two distinct interfaces, one between the GeldKate and the Loading Terminal (A), the other between the Loading Terminal and the Loading Center (B), which is usually part of the card issuing bank.

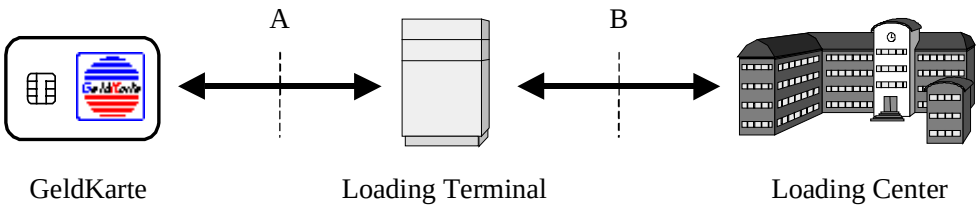

Figure 3: GeldKarte architecture

During a loading transaction, most of the messages are exhanged between the Loading Terminal and the GeldKarte (interface A). Between the Loading Terminal and the Loading Centre (interface B), in normal conditions only one pair of messages is exchanged, namely the loading request and the corresponding response.

4.2 Wireless Wallet for Loading the GeldKarte

In order to use the GeldKarte in a wireless environment (such as the GSM network [15]), the general architecture presented in the previous section must be adapted. The German GeldKarte system was originally designed to be applied in the already existing network of ATMs and POS (Point of Sale). As we will see, mapping this system to a wireless network requires some adaptations.

Wireless networks are characterised by the fact that there is an air interface between the mobile device and the base station. Mapping the GeldKarte architecture to the wireless network therefore brings different alternatives regarding the location the air interface in the GeldKarte model. The different alternatives are shown in Figure 4.

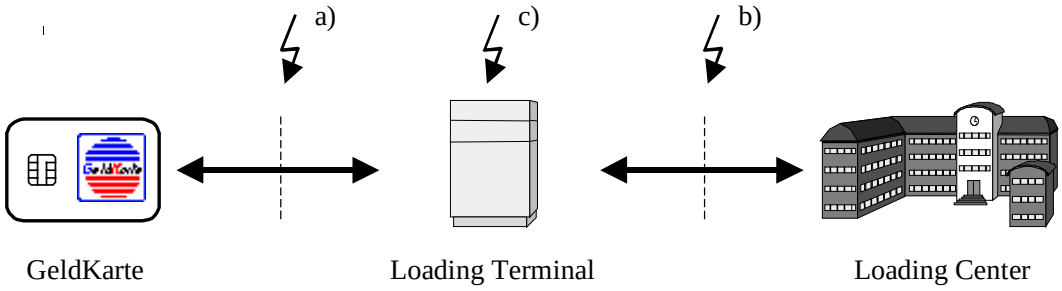

Figure 4: Alternatives for mapping the GeldKarte architecture to wireless networks

The three alternatives are:

a) The air interface is between the GeldKarte and the Loading Terminal,
b) The air interface is between the Loading Terminal and the Loading Centre,
c) The Loading Terminal is split into two components, in the middle of which the air interface is then located.

In the first alternative (Figure 4a), the air interface is located between the GeldKarte and the Loading Terminal (LT). This means that the mobile device is used only for hosting the GeldKarte, and for transporting messages between the GeldKarte and the LT, which is entirely located in the fixed network. In general, the user starts a loading transaction on the LT, when he or she inserts the card and presses a dedicated key. The interaction between the LT and the user takes place via the terminal display and the keypad. The LT must also be able to conduct a dialogue with the GeldKarte. Considering the first alternative, this means that the LT must be able to control the user interface of the mobile device, and be able to send (and receive) messages to the GeldKarte hosted by the mobile device. From today's point of view, the implementation of such a scheme is difficult

due to the lack of a common interface allowing the external access to the user interface or GeldKarte interface on the mobile device.

In the second alternative (Figure 4b), the air interface is located between the LT and the Loading Centre (LC). This means that the LT functionality is entirely implemented in the mobile device. In general, LTs can only be provided by financial institutes. Hence if a GSM network operator intends to act as an LT provider, it must co-operate with a financial institute issuing the GeldKarte. Providing the entire GeldKarte functionality in the mobile device would mean putting an ATM into the hand of every Wireless Wallet user. It is unlikely that this approach will find success.

The third alternative (Figure 4c) consists in splitting the functionality of the LT into a so-called Mobile Loading Terminal (MLT) located in the mobile device, and a Fixed Loading Terminal (FLT), which is located in the fixed network. This approach is detailed in the following section.

4.2.1 Split Terminal Approach

Figure 5 shows the overall architecture of alternative c). The Loading Terminal is split into an MLT located in the mobile device (here, a GSM phone), and an FLT located in the fixed network.

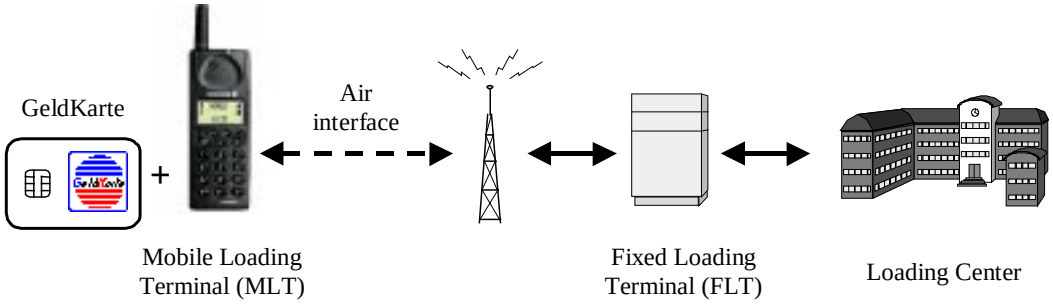

Figure 5: Split Loading Terminal approach.

Several alternatives exist on how the card reader for the GeldKarte can be integrated into a mobile device such as a GSM phone, but this discussion goes beyond the scope of this paper.

The user starts a loading transaction on the mobile terminal, and the subsequent interaction between the LT and the user takes place entirely in the mobile device. The advantage of this approach is that the function located in the mobile device can easily use the interface towards the user, as well as the interface towards the GeldKarte. The role of the FLT in this scheme lies in forwarding messages between the MLT and the LC, namely the messages *Load Request* and *Response to Load Request* for a normal loading transaction.

Comparing this approach with alternative a), it appears that the number of messages transported over the air interface is reduced to two in case of a successful loading transaction. A significant increase in the speed of the transaction can therefore be expected.

Due to the strong security requirements from the German GeldKarte system, implementing loading functionality into a mobile device results in some architectural requirements. One important requirement is related to the handling on the PIN during a loading transaction. The PIN is required when the user downloads money from a personal account to his/her GeldKarte, because a private bank account is accessed. In order to be approved, the loading terminal on which this type of operation is performed must have a secured keypad. Any information entered on this type of keypad is encrypted before it is sent to the recipient, which can be the GeldKarte for example. Furthermore, it has to be

guaranteed that a secured keypad cannot be tampered. This is usually achieved by introducing a box containing the keypad and the security components, and which will erase all the memory contents when an attempt is made to attack this box. Note that such security requirements have a major impact on the design of mobile devices, and should therefore be taken into account from the beginning of a mobile device's development.

4.2.2 HBCI for Loading the GeldKarte

Due to the strong requirements mentioned in the previous section, another type of solution was investigated for loading the German GeldKarte via a mobile device. This solution is based on HBCI.

As mentioned above, loading money to the GeldKarte using the HBCI protocol is planned in the HBCI specification version 3. One advantage of using HBCI is that this standard provides the basic functions for a wide range of financial and banking services, besides loading the GeldKarte. HBCI acts as a protocol container, providing user authentication and a secured access.

HBCI could also help lowering the security requirements on the loading terminal (the mobile device in this case). In order to overcome the security issues mentioned in the previous section, we present a solution based on an HBCI account transaction, and the loading transaction for the GeldKarte known as "loading against other payment means".

The GeldKarte loading concept presented in this section can be divided into two steps:

1. The user starts an HBCI transaction to transfer a given amount of money from his/her bank account to the account of a payment gateway.
2. In the second step, the user loads the GeldKarte against other payment means, whereby the payment gateway plays the role of the merchant. With the previous HBCI transaction, the payment gateway knows that the payment is secured, and therefore allows the subsequent loading transaction.

The corresponding structure is shown in Figure 6.

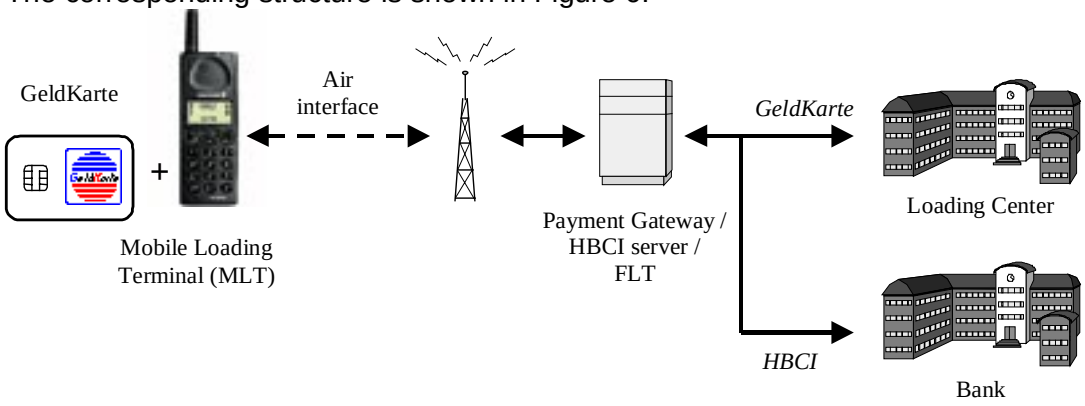

Figure 6: Loading the GeldKarte with HBCI

The operation is realised as follows. The user (i.e. the mobile device) communicates only with the Payment Gateway (PG), which is at the same time the HBCI server. An HBCI transaction is initiated and used to perform the first operation, which consists of transferring a given amount of money from the user's bank account to a temporary account controlled by the PG. This operation has to be performed via the PG so that it is aware of it, i.e. that the money has actually been transferred. Only then will the PG allow the subsequent GeldKarte loading transaction.

Following the HBCI transfer transaction, a GeldKarte transaction is performed in order to load the GeldKarte. In this case, the PG acts as the merchant, and a transaction of the type “Loading against other payment means” is performed, whereby the merchant (PG) states that the money has been received by some other means. In order to realize this transaction the PG requires a connection to the Loading Center.

A major advantage of the approach presented in the previous subsection lies in the smaller security requirements. This is due to the nature of the GeldKarte loading transaction used here, which does not require the use of a PIN.

HBCI transactions require an RSA key on the client side. It is planned that this key, which has a typical length of 768 bits, should be stored on the GeldKarte. Since the GeldKarte transaction used to load the card is nested into an HBCI transaction, a problem arises since two different applications of the GeldKarte are used at the same time, i.e. the loading transaction, and the HBCI transaction.

Currently, changing the application on a Smart Card results in the card being reset. Consequently, it is not possible to have two transactions running at the same time and involving a single card. A solution to this problem consists in starting the HBCI transaction with enabled encryption in order to perform the initial money transaction, and to continue this transaction without encryption when it comes to the GeldKarte transaction. This is possible, since the messages of the GeldKarte transaction are already signed and encrypted.

5 Conclusion and Outlook

We have presented various examples on how Electronic Commerce can be implemented on mobile terminals. From our point of view, both the GeldKarte and HBCI will play an important role in MEC in the future. We have outlined how loading of the GeldKarte can be implemented both directly and as business transaction of HBCI. We have argued that the combined solution offers advantages for the user and for the mobile terminal. The user can load his or her GeldKarte but can also use the rich collection of services implemented with HBCI. The terminal has to fulfill less security requirements compared to the direct approach.

Many optimists see E-Commerce as a technology that is just one step before everyday use for most of us. Pessimists see the many unsolved problems and conclude that E-Commerce will not break through in the next few years. As usual, the truth lies somewhere in the middle: some basic techniques are already available and systems built on top of those techniques are currently in business and field test. Techniques that are more sophisticated and especially E-Commerce protocols need more testing and have to be adapted to user requirements and to the mobile environment. The careful system design and the early involvement of potential users of such systems pave the way towards the widespread usage. However, a user-friendly design and a proven and acceptable security level are only one side of the medal. The mysterious user that shall spend her or his money has to be convinced - and this step is maybe the most complicated and most critical one.

6 References

[1] Haubner, K., HBCI - Kompendium, SIX SIGMA EDV - Konzepte und Lösungen, 1997, http://members.aol.com/sxsigma/hbci.htm.

[2] Jones, T., Mondex on 'The future of money', submission to the US House of Representatives, June 11th 1996.

[3] Schubert, P. and Zimmerman, H., Electronic Markets: the deployment of Smart Cards for payment settlements within the EM reference model, Overcoming

Barriers to Electronic Commerce (OBEC '97) Conference, Malaga, Spain, April 21-26, 1997.
[4] Fuerbeck, E., The bank card with a chip: German banking industry's "electronic purse", CardTech/SecurTech'97, Orlando, Florida, May 19-22, 1997
[5] Electronic Cash and Retail banking – Why everything will change, ICM, Phoenix, February 1996
[6] Mondex homepage http://www.mondex.com
[7] Secure Electronic Transaction (SET) Specification Book 1: Business Description, June 17, 1996
[8] Secure Electronic Transaction (SET) Specification Book 2: Programmer's Guide, June 17, 1996
[9] Secure Electronic Transaction (SET) Specification Book 3: Formal Protocol, August 1, 1996
[10] First Virtual homepage http://www.fv.com
[11] Herwono, I., Popp R., State of the Art report: Secure Transactions Processing Schemes, GSMEC-D01/04, Institute for Communication Networks, RWTH Aachen, April 30, 1997
[12] Ford, W.: Computer Communication Security. Prentice Hall, Inc., Englewood Cliffs, New Jersey, 1994.
[13] Faktum home page http://www.faktum.de
[14] Bank-Verlag Köln home page http://www.bankverlag.de
[15] M. Mouly and M. B. Pautet. The GSM System for Mobile Communications. Published by the authors, 1992.
[16] Kendrick Struthers-Watson. Need money? Your wish is my command. Published in Communications International, July 1997.
[17] Thorbjorn Thorbjornsen and Claus Descamps. What is e-Commerce? In Conference on Dismantling the Barriers to Electronic Commerce. http://www.at.infowin.org/ACTS/IENM/NEWS/NEWSCLIP/