Near Field Communication based Mobile Payment System

Gerald Madlmayr, Josef Langer
University of Applied Sciences of Upper Austria, Hagenberg
{gmadlmay, jlanger}@fh-hagenberg.at

Josef Scharinger
Johannes Kepler University
josef.scharinger@jku.at

Abstract: In daily life, ordinary cash is more and more replaced by electronic means of payment. Where on the one hand side macro payment systems are well covered by credit cards, micro payment systems still suffer from different technological and usability issues. Besides usability, security in payment systems has always been a hot topic ever since.

In this paper we present a new, promising approach for a purse-based micro payment system. Our system relies on a prepaid wallet having the money stored in a secure chip in the mobile phone. The proximity technology Near Field Communication (NFC) is used to conduct contactless payment transactions at the point of sale (POS). Additionally the wallet can be topped up over the air (OTA), anywhere and anytime.

The combination of OTA top-up and NFC payment transactions make this system very convenient as the data acquired during an eight month trial shows. Users benefit from the system as they do need to head for an ATM to load money into the wallet. This system is also advantageous for banks and payment providers as there is no need to issue smartcards. Besides the technological aspects of NFC and the implementation of the payment system, this paper also presents the results of an eight month trial with 75 participants.

1 Introduction

The use of mobile communication and wireless networks has a huge impact on the daily life. Due to the raise of participants in mobile networks, operators and application providers are searching for new applications and services to serve the consumer. Using the mobile phone for payment transaction has ever since been a hot topic [Va02]. Whereas card based payment systems are well established, mobile payment is far behind as the market so far has been unstructured with lots of proprietary solutions competing with each other [DMOZ06].

Chi Po et al. point out the four major criteria for the acceptance of mobile payment systems: Security, Cost, Convenience and Universality [CPCL07]. Khodawandi et al. show in their consumer report [KPW03] that *avoiding counting/carrying coins*, the *easy of use* as well as *time needed for a payment transaction* are among the most critical ones for using a mobile payment system in everyday life. Out of this criteria set we implemented a prepaid payment system in combination with Near Field Communication (NFC) technology

to provide a new payment experience to the consumer.

In prepaid systems there are usually two processes needed for the user in terms of cash transactions: A top-up process and a payment process. Keeping the time needed low for both transactions is the major goal of our system. We propose the implementation of a micro payment system with a prepaid wallet on the mobile phone. The money is kept in a stored value account (SVA) in the mobile device. The SVA can be recharged over-the-air (OTA). The clearing and settlement of the transactions is performed by a bank. NFC is used at the point of sale (POS) to perform the payment transaction in a quick and convenient way. Money can be topped up OTA within seconds, anytime and anywhere. Additionally users can instantly query the amount of money available and the last transactions performed on their mobile phone without establishing an online connection.

The presented payment system was tested by 75 users during an eight-month field trial. The findings show, that this system is a fast and convenient implementation of a mobile payment system. A major focus of this paper is also the implemented security. We propose a public key infrastructure (PKI) and certificates for authentication and AES encryption for secure communication during OTA top-up transactions, as security concerns are the major argument for not using a mobile payment system. Linck et al. discuss this topic extensively in [LPW06].

Section 2 of this paper introduces the reader to the functionality and integration of NFC technology in systems and applications. Moreover the implementation and the architecture of a mobile payment system are lined out in section three. In this section also covers security aspects of the system. The findings section in section four provides the reader with information on the usage data acquired during a field trial. The paper closes with a conclusion.

2 Background Related Work

2.1 NFC - Near Field Communication

NFC is a wireless communications technology for proximity transactions. NFC is defined in ISO 18092 [In04] and backward compatible to the smartcard standard ISO14443. Hence NFC devices can be integrated in already existing smartcard based infrastructures easily. NFC allows contactless transactions over a distance of up to 10 centimetres. This is a reasonable operating range for transaction at ticketing gates and POS terminals, whereas logistics and health care make use of long-range radio frequency identification (RFID) technology. Both, NFC as well as RFID, base on the same physical technology: electro magnetic waves. Whereas RFID uses several different frequency domains for communication, NFC is located in the 13.56 MHz band.

RFID is mainly used for remote tracking, tracing and identification of goods and persons without a line of sight. NFC on the other hand is used for more sophisticated and secure transactions like contactless access or payment. The benefit of the short operating distance is that transactions are usually only caused on purpose [BHS+07].

An NFC enabled device features the following operating modes [MDL+07]:

Reader/Writer Mode (Proximity Coupling Device, PCD): Operating in this mode, the NFC device can read and alter data stored in NFC compliant passive (without battery) transponders. Such tags can be found on *SmartPoster* e. g., allowing the user to retrieve additional information by reading the tag with the NFC device.

Card Emulation (Proximity Inductive Coupling Card, PICC): An NFC device can also act as smart card after being switched into card emulation mode. In this case an external reader can not distinguish between a smartcard and an NFC device. This mode is useful for payment and ticketing applications for example.

Peer-to-Peer (Near Field Communication, NFC): The NFC peer-to-peer mode allows two NFC enabled devices to establish a bidirectional connection in order to exchange contacts, Bluetooth pairing information or any other kind of data.

The protocol handling as also the conversion of the analogue into a digital signal and vice versa is performed by the NFC controller. Besides this integrated circuit, the mobile device – usually a cell phone – additionally contains a secure chip to store sensitive data. There are various ways to implement this secure chip: using the SIM Card, adding an additional smart card chip or storing data on a secure memory card [BJ05]. The data in such a secure data container – also referred to as secure element (SE) – can be access on the one hand side through the NFC interface (NFC controller chip in tag emulation mode) but also by the host controller. For example, data received over the mobile network (GSM e.g.) can be stored in the secure element then be queried over the NFC interface [MDL+07]. The secure element itself is designed to be tamper proof. Figure 1 shows the architecture of an NFC device.

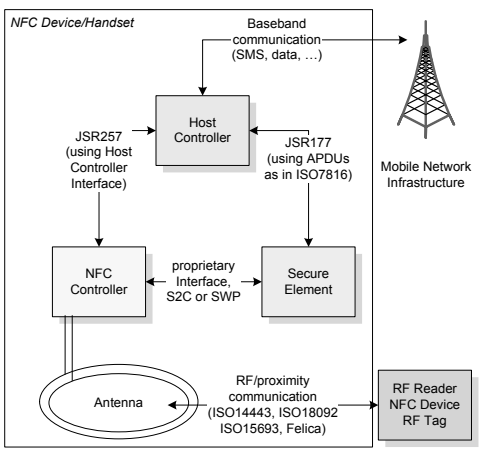

Abbildung 1: Integration of NFC into a mobile handset and communication flows/interfaces.

A major benefit of NFC is the quick setup up time (200 ms) of the communication in comparison to Bluetooth or WiFi. Usually there is no user interaction or PIN code required

to establish a connection between to NFC devices. But the data rate of an NFC connection (max. 424 kbit/sec) is significantly lower than these technologies.

Industry and academia are quite excited about NFC technology being integrated into mobile devices. As Mark Weiser mentions in [We95] it is important that the technology itself disappears and only the interaction respectively the application should be visible to the user. NFC has a good chance to meet this criteria with its *Touch and Go* philosophy. NFC enabled handsets allow the users to interact with their environment like never before [ABPW07]. Additionally the integrated secure element stores identification information for the user in a secure way, like Satyanarayanan proposes already in [Sa05].

2.2 Mobile Payment

Mobile payment refers to a system where a wireless electronic device is used for a payment transaction. Gao et al line out the extensive literature available in their work [GCPS05] for example.

A good classification of payments is given in [La06]:

- Amount of money spent: micro (<5 USD) vs. macro payment (>5 USD)
- Point of Sale: local (vending machine e.g.) or remote payment (internet e.g.)
- Clearing and settlement: prepaid, post-paid, in-time paid
- Operation method: online (centralized) or offline (distributed)

A very interesting approach for an m-payment system was presented by Fujitsu Lab's in [LAJ+04] called *Wireless Wallet*. The proposed framework allows different implementation of an online payment system with various clearing methods and POS types. They also presented a unique hardware development for an m-payment device using WLAN to conduct transaction with wireless merchants. Additionally a J2ME version for a mobile phone was implemented. In this case the mobile network was used to process payment transaction with the backend server system.

In [GCPS05], [GES05] Gao et al. propose a wireless payment system based on Bluetooth for the local transaction with a server for online verification of payer and payee. The system is capable of POS payment as well as peer-to-peer transaction in a secure way.

Both systems, the *Wireless Wallet* and the Bluetooth based implementation, require a server in the backend. Either the payer or the payee needs an online connection to verify the authenticity of the instances involved in the payment transaction. Regarding online payment systems Bao et al. give an extensive overview and related references in [BDZ00].

Offline wallets and terminals as mentioned in [MR01] follow a different approach. In such a system the individual information – usually money or tickets – is stored highly secured in a remote device/integrated circuit. Transactions do not require an online connectivity to a server and thus save time during the transaction. Although, wallets and terminals need to

be synchronized from to time to time in order to perform the clearing and settlement or to recharge the wallet with money. The implementation and management of the distributed paychip system *QUICK* is outlined by Holzmann in [Ho96]. The system is based on a contacted smartcard and is designed for micro payment transactions. The smartcard contains a secure wallet to store money. This prepaid wallet is topped up at an ATM before usage. At the POS the smartcard is inserted into the terminal and the amount due is deducted from the wallet. The terminal does not require the user to enter a PIN code to perform a payment transaction. Although, from a user's point of view, prepaid system are not very popular as Dahlberg et al. line out in [DMOZ07], this is the only technical solution of a secure offline payment system.

Akio et al. give details on a distributed public transport ticket payment system implemented by Japan Rail [WDL06]. The wallet is located on a contactless smartcard using *Sony's FeLiCa* technology. This purse – similar to *QUICK* – needs to be recharged at an ATM. Akia et al mention the following reasons for choosing a distributed purse based approach over a centralized one: better scalability, less cost for implementation and maintenance as well as simpler system architecture.

The idea of integrating a wallet in the secure element of an NFC device, using the contactless interface for payment, is self-evident [At06]. This fact in combination with the ability to alter the information in the secure element is a promising approach for new applications like payment and ticketing. Also Zmijewska lines out in [Zm05] that NFC is a promising technology for mobile payment.

3 Implementation

We implemented the system in a way that it is backwards compliant to the card based payment system at our campus. The payment infrastructure itself is a proprietary and closed ecosystem and relies on the following processes:

- Top-up of money into the SVA
- Payment Transaction at the POS
- Clearing and settlement

The already established system forces the user to go to an ATM on campus to load money into the wallet on the smartcard. Our system only modifies this process of topping up money and does not influence the other two processes (payment, clearing). In the following we describe how this process was improved by using an NFC handset.

The implementation, as shown in Fig. 2, bases on four different components:

A wallet application on the mobile phone to top-up the SVA: The application acts as a proxy between a security applet in the secure element and the backend server. This application also tells the user how much money there is available on the mobile

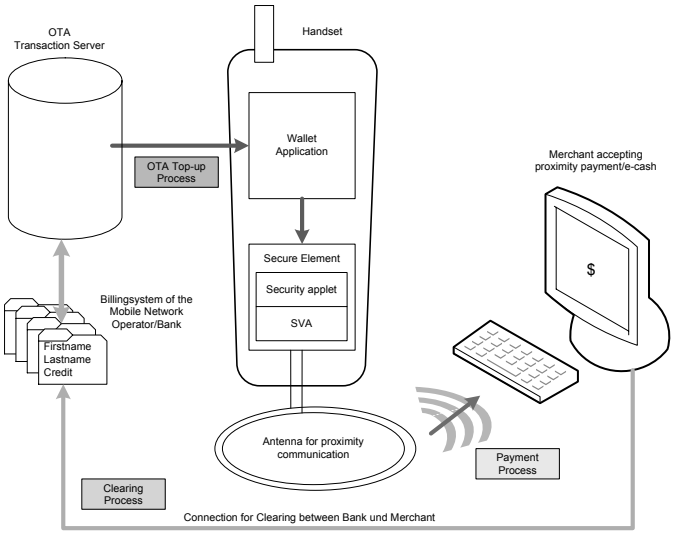

Abbildung 2: The system architecture shows the different process of the payment system: OTA top-up, payment transaction and clearing.

phone. The wallet application does not hold any keys nor does any de- or encryption. We used J2ME for the implementation (Fig. 4).

A security applet to process cryptographic functions: The security applet holds the

- public and the private key of the user, a certificate to authenticate against the server during OTA top-up,
- an AES key used for encryption during the OTA transaction,
- a certificate in order to verify the authenticity of the server and
- the keys to read and write the amount of data in the SVA.

The keys stored in the secure element can neither be read by an attacker nor will leave the security applet. The security applet uses Java Card technology.

A SVA with a contactless interface: We made use of a contactless memory card in the SE based on ISO14443-A, to be backwards compatible to our existing payment ecosystem. Besides the amount of money, the SVA stores the last 10 transactions, the last top-up date and the last payment date. The SVA contains a unique number used for anti-collision during the ISO14443 communication.

Backend: A Server in the backend to process the OTA top-up transactions.

3.1 OTA top-up Process

The OTA top-up process is used to load money into the SVA in the handset (Fig. 3). The process is implemented as a pull service and has to be triggered by the user consciously (Fig. 3, 1.1). After starting wallet application, it establishes a connection to the secure element and requests the amount of money stored in the SVA (Fig. 3, 1.2 - 1.6) which is displayed on the screen (Fig. 4, Step 1). The read operation on the SVA (Fig. 3, 1.3) is performed by the security applet as the wallet applications does not hold the keys to do so. The security applet returns the amount of money stored (Fig. 3, 1.5 and 1.6).

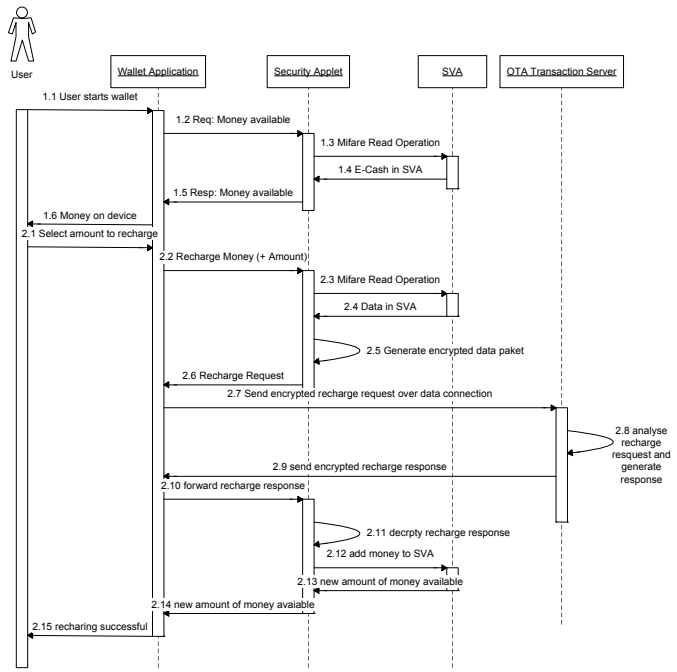

Abbildung 3: Process of recharging money: The figure shows the communication between the four components: wallet application, security applet, SVA and OTA transaction server.

The user can top-up the wallet (Fig. 3, 2.1) by selecting the amount from a list box (Fig. 4, Step 2) and confirms the operation (Fig. 4, Step 3). The amount of money selected to be topped up is handed over to the security applet (Fig. 3, 2.2). The security applet reads the information stored in the SVA, (Fig. 3, 2.3) and generates a secure random number as a session key for this transaction. This information is combined with the amount of money to be topped up. The whole data set is encrypted (AES) and signed (RSA) using the private key of the user stored in the security applet (Fig. 3, 2.5). As the secure element is optimized for cryptographic functions, encrypting and signing the data is performed without notice. Finally the wallet application receives the encrypted data packet from the security applet (Fig. 3, 2.6).

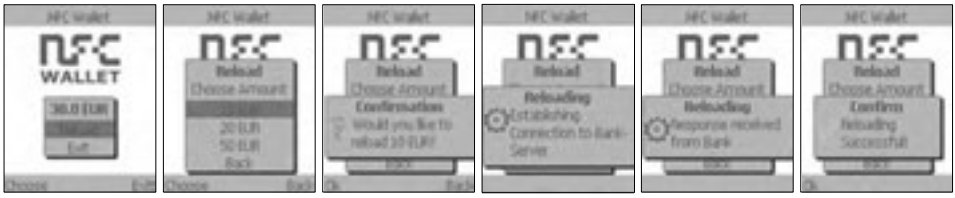

Abbildung 4: User interface at the mobile device during top-up process.

The next step taken by the wallet application is to establish an IP connection to the transaction server and hand over the encrypted data packet (Fig. 3, 2.7). The transaction server validates the signature of the packet using the public key of the wallet. Then the data packet is decrypted and an authentication of the user is performed through the IP address. This is done by querying the mobile network operator's GPRS/GSM database. The transaction server is able to match the mobile subscriber ISDN (MSISDN) number of the user with the IP address of the data package received. The transaction server also compares the ID and the date of the last top-up from the SVA with the information stored in a database (Fig. 3, 2.8).

If everything is correct the transaction server ties up a data packet with the top-up information, encrypts and signs it. A correct response is only given by the payment server if the credit line of the customer is not exceeded. Then this packet is sent back to the mobile device (Fig. 3, 2.9).

The wallet application receives the data and hands it over the security applet (Fig. 3, 2.10). The applet decrypts the data and checks the signature of the server (Fig. 3, 2.11). Additionally the applet checks the session key and the correctness of the new amount of money. If the tests are passed satisfactorily the SVA is updated (Fig. 3, 2.12). Finally the security applet confirms that everything worked out fine and sends the current amount of money available to the wallet application. The wallet application then displays the new amount of money to the user (Fig. 3, 2.13 and 2.14). This recharging process takes about 10 seconds.

3.2 Payment Process

The payment process itself is not different to using a smart card. In order to pay with the mobile phone the device must be in card emulation mode. Therefore the host controller has not to communicate with the secure element. Thus the wallet application in our case needs to close the connection to the secure element. Deducting money from the SVA takes about 0.2 seconds.

3.3 Clearing and Settlement Process

The institution in charge of the transaction server receives the money collected at the terminals. Such a transaction can be performed in different ways. In case the terminals are operating online, the transaction server receives the money spent without delay through a secure IP connection. On the other hand, offline terminals send the data after a certain period of time to the central system. In case the terminals are not wired at all, the money from the the secure access modules (SAM) in the terminals is collected in person (using a smartcard for example) and sent to the backend system through a specially designed application. At the end of an accounting period the clearing institution credits the e-cash received to the merchant's bank accounts.

4 Trial Results

The trial phase started in November 2006 and last until June 2007. 75 persons participated in the trial. Among the participants there were 50 students and 25 full time employees at the campus. 1/3 of them were female, 2/3 were male. At the campus there are two cafeterias, five coffee and one drink vending machine accepting contactless payment. For legal reasons the cash handling is performed by the bank of the mobile network operator (MNO) during our trial. In our case the MNO provides a banking license and therefore its bank is able to issue *e-cash*. At the beginning of the trial the participants had to sign a contract with the bank and decide whether the money topped-up was credited to the customer's telephone bill or credit card. MNOs without a banking license would be able to offer this service through a 3rd party payment provider.

The NFC enabled mobile phone was used as access token, as loyalty card and to use information services by the participants as well.

4.1 Findings

In order to collect feedback on the applications in the trial, a combination of three complementary studies was chosen: Diary Study, Online Survey and Idea Development Workshop. Details on the whole user study conducted during the trial can be found here [GF07].

Diary Study: At the beginning of the trial, a 7-day online diary was kept by a group of 11 users. They provided information on the services used (quantity and quality). It turned out, that the access functionality was the feature used most often, followed by payment and information services. 75 % of the participants indicated that they were *very satisfied* or *rather satisfied* with the quality and availability of the NFC services on a five point scale.

Online Survey: All participants of the trial were asked to participate in an online survey (CAWI - Computer assisted web interview). Out of them, 60 persons returned

a complete questionnaire. 83 % of the participants indicated that they were *very satisfied* or *rather satisfied* with the quality and availability of the NFC services on afive point scale. 19 % used the payment service daily and 41 % at least three times a week. 91 % of the user indicated that they were *very satisfied* or *rather satisfied* with the payment service. 89 % rated NFC payment as faster than payment in cash, 95 % as more convenient, 90 % as better, 90 % as more user friendly, and 95 % as more stylish (Fig. 5(a)). Only 40 % think, that the NFC payment system is at least as secure as cash-payment. With regards to attributes, NFC services were ranked as innovative, easy to use and simple. Also negative attributes like too technical and unpredictable were associated with NFC.

Idea Development Workshop: The 10 most active users during the first period of the trial were invited to participate in an idea workshop in order to improve the services given and come up with ideas on new services. Users explained how they like the services and which parts to be improved. On the positive side the contactless payment system was mentioned, on the negative side a lake of information on payment security. The possibility of topping up OTA was lined out as the most innovative feature of the system.

Generally, consumers are happy with the high transaction speed at the POS as also the OTA top-up functionality. The trial participants mention the time saving as the most convenient factor of this system. The users like the easy-to-use wallet application on the phone. 95 % of the users prefer the NFC payment system to using coins at automated vending machines. This is true for both students and full time employees. The major part of the users is satisfied with the system and would like to have more POS and more NFC services on campus.

With regard to the amount of money topped up, there are two different groups. There is one group which tops up a big amount of money (50 EUR e. g.). They say that they won't bother with topping up too often. This user group correlates well with the user group that is convinced that this means of payment is secure. The other group, usually topping up only 10 to 20 EUR at a time, is skeptical of technology and security. Both groups say that they are in favor of the NFC solution as they only need their handset for their every-day-life on campus as a replacement for an ordinary wallet. This is the case as the NFC device is also used as access token and loyalty card.

Out of the data collected (around 5000 transaction records) we were able to classify three different groups of user with regard to amount and value of transactions. The data was extracted form the transaction server.

Low revenue/high amount of transactions: This group has lots of transactions and uses the handset mainly for automated vending or small payments at the cafeteria. The users top-up between 10 and 20 EURs, but as the transaction value is not very high, topping up once last even up to a month or more. The speed at the POS is much more important than the time needed to top-up. The avoidance of coins is the most important argument for this group to use NFC payment.

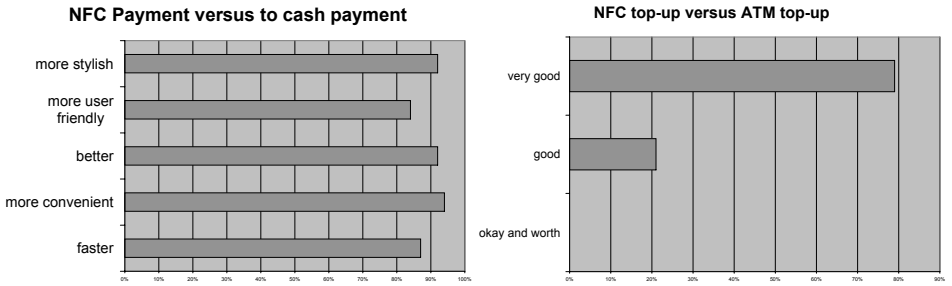

Abbildung 5: Figure (a): User were ask to compare NFC payment to cash payment and were able to choose different attributes for NFC payment; Figure (b): User were ask how the like they top-up functionality of the NFC payment system; n = 75

Medium revenue/medium amount of transactions: This group of users pays the meal at the cafeteria and occasionally gets a coffee or a drink from the vending machine. The average user usually checks the balance of the NFC wallet at the beginning and the end of the week to keep track of the money spent. These users also take this occasion to top-up money if needed. The users spend between 20 and 50 EUR a month having between zero and two transaction a day. Security is very important for this group too. The most important feature for this group is the OTA top-up.

High revenue/low amount of transactions: This user group has a high share of the revenue but only very few transactions. They usually pay for two or more meals at the cafeteria but rarely use vending machines. Some user commit that they show to friends how easy it is to top-up, even they are off campus. They enjoy NFC over cash or card payment because of lifestyle reasons.

5 Conclusion

NFC devices have the potential to change a lot of services and processes in consumer's every day life. Besides smart poster, ticketing, access, and other touch-and-go services, payment has the chance to play a major role. As already mentioned in section two the great thing about NFC devices is that they can be integrated into already existing RFID smartcard based systems without additional investment into the infrastructure itself. The implementation presented is a feasible solution for a mobile micro payment system. The findings of our trial show that user enjoy the usability and the functionality of NFC technology and applications above. Besides this euphoria on automation we still need to keep an eye and privacy and security related issues in regard to this contactless technology.

Acknowledgment

This work is funded by FFG (Austrian Research Funding Agency), Project #811408.

Literatur

[ABPW07] Anokwa, Y., Borriello, G., Pering, T., und Want, R.: A User Interaction Model for NFC Enabled Applications. *PerComW*. 5:357–361. 2007.

[At06] Atkinson, J. Contact less Credit Cards Consumer Report 2006. http://www.findcreditcards.org/. 04 2006.

[BDZ00] Bao, F., Deng, R., und Zhou, J.: Electronic payment systems with fair on-line verification. *WCC*. 16:451 – 460. 2000.

[BHS+07] Bravo, J., Hervas, R., Sanchez, C., Chavira, G., Nava, S., Martin, S., und Castro, M.: Touch based interaction: an approach through nfc. *IE07*. 3:440 – 446. 2007.

[BJ05] Bishwajit, C. und Juha, R.: *Mobile Device Security Element*. Mobey Forum. Satamaradankatu 3 B, 3rd floor 00020 Nordea, Helsinki/Finland. 02 2005.

[CPCL07] Chi Po Cheong, S. F. und Lei, P.: Efficient and secure card-based payment system based on ansi x9.59-2006. *International Conference on E-Commerce Technology and the 4th IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services, 2007. CEC/EEE 2007.* 9:247 – 254. 2007.

[DMOZ06] Dahlberg, T., Mallat, N., Ondrus, J., und Zmijewska, A.: Mobile payment market and research - past, present and future. In: *Proceedings of the 5th Mobility Roundtable.* pp. 1 – 16. 2006.

[DMOZ07] Dahlberg, T., Mallat, N., Ondrus, J., und Zmijewska, A.: Past, present and future of mobile payments research: A literature review. *Electronic Commerce Research and Applications*. 0:17. 2007.

[GCPS05] Gao, J., Cai, J., Patel, K., und Shim, S.: A wireless payment system. *Embedded Software and Systems*. 00:8. 2005.

[GES05] Gao, J., Edunuru, K., und Shim, S.: P2P-Paid: A Peer-to-Peer Wireless Payment System. *Mobile Commerce and Services*. 00:102 – 111. 2005.

[GF07] Geven, A. und Ferro, B.: Experiencing real-world interaction - results from a nfc user experience field trial. In: *Proceedings of the 9th conference on Human-computer interaction with mobile devices and services*. 2007.

[Ho96] Holzbach, A.: Security measures for the austrian "paychipëlectronic purse application. *acsac*. 00:69. 1996.

[In04] International Organization for Standardization. Near Field Communication - Interface and Protocol (NFCIP-1). ISO/IEC 18092. 2004.

[KPW03] Khodawandi, D., Pousttchi, K., und Wiedemann, D. G.: Akzeptanz mobiler bezahlverfahren in deutschland. ergebnisse der sutide mp1. In: *Mobile Commerce Anwendungen und Dienste. Proceedings zum 3. Workshop Mobile Commerce*. pp. 42 – 57. Pousttchi, K. and Turowski, K. 2003.

[La06] Lammer, T.: *Handbook on E-Money, E-Payment and M-Payment*. volume 1. chapter E-Payments Evolution, pp. 7 – 18. Springer Verlag. 2006.

[LAJ+04] Labrou, Y., Agre, J., Ji, L., Molina, J., und lun Chen, W.: Wireless wallet. *Mobiquitous*. 00:32 – 41. 2004.

[LPW06] Linck, K., Pousttchi, K., und Wiedemann, D. G.: Security issues in mobile payment from the customer viewpoint. In: *Proceedings of the 14th European Conference on Information Systems (ECIS 2006)*. pp. 1 – 11. Gteborg, Schweden. 2006.

[MDL+07] Madlmayr, G., Dillinger, O., Langer, J., Schaffer, C., Kantner, C., und Scharinger, J.: The benefit of using sim application toolkit in the context of near field communication applications for mobile applications. In: *ICMB 2007*. volume 06. p. 7. 07 2007.

[MR01] Mjolsnes, S. F. und Rong, C.: Localized credentials for server assisted mobile wallet. *iccnmc*. 00:203. 2001.

[Sa05] Satyanarayanan, M.: Swiss army knife or wallet? *IEEE Pervasive Computing*. 04(2):2–3. 2005.

[Va02] Varshney, U.: Mobile payments. *IEEE Computer*. 12:120 – 121. 12 2002.

[WDL06] Wu, X., Dandash, O., und Le, P. D.: The design and implementation of a smartphone payment system based on limited-used key generation scheme. *itng*. 00:458–463. 2006.

[We95] Weiser, M.: *Human-computer interaction: toward the year 2000*. chapter The computer for the 21st century, pp. 933–940. Morgan Kaufmann Publishers Inc. San Francisco, CA, USA. 1995.

[Zm05] Zmijewska, A.: Evaluating Wireless Technologies in Mobile Payments - A Customer Centric Approach. *ICMB*. 04:354–362. 2005.