Secure cashless transactions on mobile Bluetooth®-Devices

Sven Tuchscheerer, Jana Fruth, and Jana Dittmann

Otto-von-Guericke University of Magdeburg, Germany
Department of Computer Science
ITI Research Group for Advanced Multimedia and Security
Universitätsplatz 2
39106 Magdeburg

Abstract. The trend to realise mobile payment services are in the focus of mobile phone manufacturers for a couple of years, which is mainly based on the increased demand from potential customers for payment services and the integration of IT-Technology in infrastructures, such as shops, or buses. This paper describes a cost-effective approach for cashless transactions using mobile devices, because of waive of additionally integrated hardware[1], or communication-costs with GSM/GPRS or SMS based approaches. The advantages of the approach by using the free Bluetooth-technology are the providing of sufficient bandwidth for transfers and the availability in nearly all modern mobile devices. Due to known security lacks of Bluetooth in our concept all transferred content is encrypted, regardless of the communication-channel. This paper describes the concept (combination of three different procedures and an anonymity service), including the participating devices, services, implementation of a prototype, and results of a first evaluation-study.

Keywords: Content protection, security, anonymity, financial transactions, Bluetooth

1 Introduction, Motivation and Requirements for the Concept

A representative survey in 2004 has shown, every second German may desire a payment function on its mobile phone [14]. Based on this whishes the idea of realising payment functions on mobile devices (e.g., mobile phones) was already taken up several times in the past [1]. In these approaches, the payment function was mostly achieved by using the GSM network. For the customers this causes additional communication-costs for connection and transferring data, such as account details and price of goods or services. Apart from GSM-based security risks [2], primarily, the additional communication-costs are an obstacle for customer's exposure. Due to that, a widely available cash-free payment, using GSM,

[1] e.g. Near-Field Communication (NFC) modules

are not established, yet. Another implementation approach uses so-called Near-Field Communication (NFC), thus based on the radio-frequency identification (RFID) principle. Therefore it is necessary to integrate additional hardware – a RFID chip and a RFID reader or rather a RFID scanner – in mobile devices. These hardware components (especially RFID readers) are characterised by high power consumption. So they would result in reduced battery lifetime of mobile devices. Furthermore the use of these devices causes additional costs for modifications on mobile phones, because of the problem of electromagnetic compatibility. As well as RFID (Read out from mobile phone chip and read external chips, like product information and price), GSM, Bluetooth and – when installed - WLAN must not influence each other. Device manufacturers and their customers have to defray these additional costs, There are various reasons, why to date mobile device manufacturers integrate the NFC technology in only $\frac{1}{4}$ of new produced devices: absent infrastructure (shops, automats, etc.), high investigation costs for hard- and software development, property right demands of third parties and lacking installation space, mainly for reading units [15]. One cost efficient solution could be the use of communication channels for data transfers, which aren't associated with additional costs, are available in all mobile devices on the market and should provide sufficient bandwidth for the realisation of the payment function. The data transmission, using infrared-technology is cost-neutral, but because of the small bandwidth and the frequent lack of implementation in current mobile devices an unsuitable choice. Another alternative data transmission is the WiFi-technology. This technology offers enough bandwidth, but is not implemented in many mobile devices, yet. The Bluetooth[2]-technology, as a wireless data transmission-technology between different devices, such as mobile devices and peripheral input and output devices, seems a good choice, implementing wireless cashless paying function on mobile devices. Bluetooth offers cost-neutral data transmission, provides a sufficiently high bandwidth and supported by a very large number of mobile devices. Beside those benefits that come with Bluetooth, several security risks arise in that context. It was shown that communicated content via the Bluetooth connection can be eavesdropped and changed [3]. Potential attack techniques, reported in publication [3] are: Bluesnarfing, Bluejacking, Bluebugging and Denial of Service (force users to reconnect). In addition, a unique authentication of the communication partners is currently not implemented in the Bluetooth transmission protocol, yet [4]. Thus, the Bluetooth-based technology does not provide sufficient attack protection - in particularly against the background of the payment function including very sensitive data, typically in a financial transfer. In addition to the Bluetooth-communication between mobile devices and the service provider the backend-communication to the bank (or bank-like services), mainly data-protection issues from the customer's perspective deems relevant. The Bank should have no knowledge, which goods or services a customer buys. Of course, service providers should not know how much money the customer has in his account, only the information that the financial resources are sufficient (or not). Taking these issues

[2] http://german.Bluetooth.com/Bluetooth/

into account there is the need to anonymise communication and content. There are existing concepts and procedures, for example pseudonyms, hide in the crowd [5, 6] or asymmetric encryption [7]. The concept presented here is similar to the known principles of onion routing, with the encrypted content data, wrapped in so-called "digital envelopes" [8]. For these aspects, stated above, a couple of requirements result in an approach to secure financial transactions on mobile devices using Bluetooth communication. For our developed concept, the following four aspects are identified as central to the acceptance of potential customers, service providers (sellers) and the financial services (banks):

- Cryptographic securing of Bluetooth communications (relevant for all parties involved - all data submitted are considered as sensitive to abuse and theft)
- Clear authentication of the "trading-partners" (non-repudiation): particularly relevant for sellers - to proof the appointment, delivery and payment of a product or service
- Cryptographic securing of the backend communication (particularly relevant to customers and banks - transfer orders to be transmitted, are considered as being especially protection-worth due to the direct financial terms)

Furthermore, it is required that the strength of the algorithms, used in cryptographic procedures meet at least the current standard of known Online-Banking.

2 Security concept

Below, the developed security concept for secure and anonymous payment via Bluetooth is presented. In Table 1 the IT infrastructure components and their functions are listed, which are needed for realisation of the payment function.

Component	**Functionality**
Mobile device (e.g. mobile phone, PDA) with Bluetooth connection	Cashless payment of a product / a service (e.g. ticket)
Content service provider (e.g. ticket-terminal, vending machine) with Bluetooth -connection and Internet-access	Forwarding the payment transaction to the financial service via the anonymisation service
Anonymisation service	Establishment of an anonymous connection between content service providers and financial service (institution) / anonymisation of communication content
Server of the financial service	Payment settlement

Table 1. Components and functions for secure payments via Bluetooth

2.1 Securing the mobile - device to service provider communication

The security-mechanisms of the Bluetooth-standard had been improved since its introduction in 1999. Thus, in 2007, with version 2.1 (Enhanced Data Rate, EDR), a more secure authentication and secure simple pairing (security mode 4) were introduced [9]. The latest version of Bluetooth 4.0 [10] was expanded by the symmetric encryption (AES, 128-bit). It can not be assumed that all mobile devices support the latest Bluetooth standard and/or their security requirements. In general, for this reason Bluetooth is still stated as an insecure communication-technology [4]. Consequently we secure the Bluetooth communication between the vendor (service provider) (see Figure 1) and buyers (mobile Bluetooth-device) on higher communication protocol-level with symmetric encryption, using session keys. To negotiate the keys we use the Diffie-Hellman protocol (DH) [11]. This procedure is designed for a secure key exchange. A mutual authentication of communication parties to prevent Man-In-The-Middle attacks (MITM) could be reached with the Station-to-Station protocol, an advanced protocol based on DH. This secure protocol is not yet implemented in our current application. The special position of the content service provider as a so-called "man-in-the-middle" is clearly a potential vulnerability for security and anonymity. Due to that reason all personal banking account information are wrapped in a special digital envelop (see Figure 2). For similar scenarios, as for example online banking via internet (using Internet Service Providers) already standardised methods for secure connections were established, such as FinTS[3]/ HBCI[4] [12]. This method is consequently an integral part of our concept.

2.2 Protection of the service provider - financial institution communication

In addition to the protection of the Bluetooth connection between mobile device and the content provider / service provider the privacy of the customer has to be observed, too. The exact details of the banking business of the customer, such as name of the financial institution and height of the bank account, have to be protected from third parties, such as the content provider. In addition, the acquired product or service should not be known by the bank or payment service. For this reason an anonymisation service of the data communication between the customer and his bank in the concept for the IT infrastructure was introduced (see Figure 1).

For data privacy protection the *communication between the customer and the financial institution* is secured by FinTS / HBCI protocol. The use of FinTS / HBCI provides several advantages. Firstly it is an open standard that is suitable for everyone. Moreover FinTS / HBCI has been developed to secure communications over insecure networks (e.g. the Internet), which used security mechanisms,

[3] Financial Transaction Service (FinTS) is a German standard for online banking and a further development of HBCI standard.

[4] Home Banking Computer Interface (HBCI) is an open and standardised transfer protocol, incl. formats and security procedures.

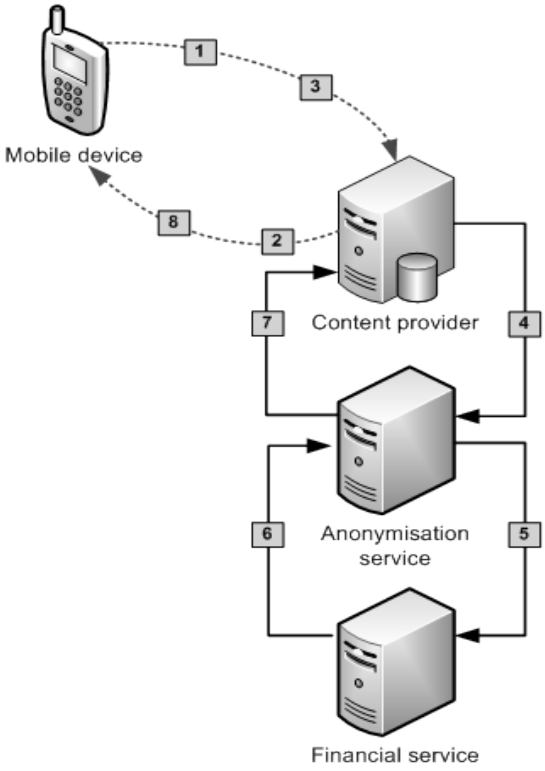

Fig. 1. Network infrastructure for secure cashless payment via Bluetooth

such as electronic signatures using asymmetric methods (RSA) and encryption (Triple DES). Therefore the additional protection of the pretended position of compromising agency can be omitted. The anonymisation service encrypts the financial data of the customers with their public keys and therefore the data are unreadable to the provider (the packets to the financial institute themselves are already encrypted anyway). In this state of communication the only task of the anonymisation service is to decode the received package, and forward the resulting FinTS / HBCI packet to the specified address of the financial institution. For each transaction the provider opens a separate port to the anonymisation service to offer a bi-directional data flow (this is for example necessary because of the challenge-response procedure).

Communication between the financial institution and the provider: Before the account of the goods the provider needs an assurance for the reception of the needed money. For reasons of anonymity the provider should not directly connect the financial institute, therefore this assurance is as well handled by the anonymisation service. For this, the system of the financial institute has to be ex-

tended so far, that the financial service sends the instruction of execution to the anonymisation service. Since the financial transaction is handled by the anonymisation service, there is no additional affect to the security and anonymity. In the next step the anonymisation service itself confirms the provider of the reception of the guarantee of the financial service.

In the following the operating sequences of the protocol (see Figure 1) are briefly shown. Firstly (1.) the symmetrical session keys are exchanged via Diffie-Hellman-Protocol. The whole Bluetooth communication between content provider and mobile device is encrypted with the session keys. Then the list of available goods (encrypted with the previously exchanged symmetric keys) is transferred (2.). In the next step (3.) the user chooses one or more of the goods he wants to purchase. The data for the settlement of the purchase are sending by the content provider to the anonymisation service using TCP / IP. The content provider keeps the connection open until a response from the anonymisation service replaced (4.). The data packet, sent by the client (mobile device) to the content provider, consisting of several nested packets (see Figure 2).

The AES encrypted (128 bit) content data packet to the content provider contains the packet, which is RSA-encrypted with the public key of the anonymisation service. The data packet of the anonymisation service includes the 1024-bit encrypted FinTS data packet for the financial service.

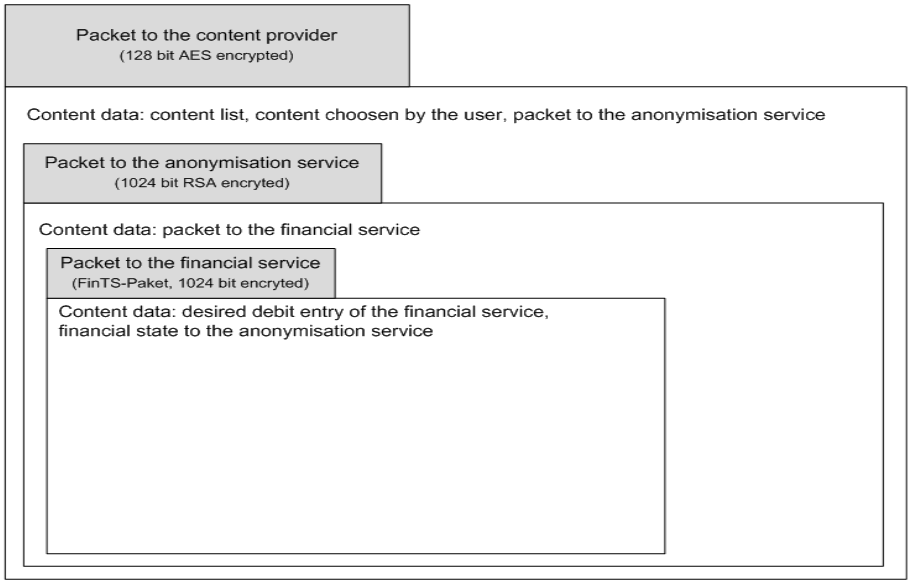

Fig. 2. Packet structure for anonymous cashless payment with a mobile device

In the next step the anonymisation service decrypts the RSA-encrypted packet with its private key and forwards the encrypted FinTS data packet with the desired debit entry to the financial service of the customer (5.) and waits for reply from the financial service. The financial service decrypts the FinTS-Packet and verifies the account status of the customer. If the account is sufficiently covered, the desired amount will be debited. Otherwise a rejection of the financial transaction will be sent to the anonymisation service via a RSA encrypted packet (encrypted with the public key of the anonymisation service) (6.). The anonymisation service validates the message of the financial service and forwards the encrypted information to the content provider (7.). In case of positive feedback of the anonymisation service the desired content will be represented by the content provider (e.g. print-out of a ticket) to the customer, otherwise the purchase order of the customer will be rejected due to the low account balance.

3 Proof of Concept and Security Evaluation

In the following section are the results from an evaluative analysis of the communication security reported. Central proofed issues are anonymity and performance, against the background for use in practice.

3.1 Communication Security

Both communication partners (mobile device and service provider / seller) exchange messages over a potentially insecure channel (Bluetooth). Computing the secret key out of these messages is called the Diffie-Hellman problem and assumed as non-solvable [8]. Therefore, the secret key cannot be computed from the pure eavesdropping. The Diffie-Hellman key exchange, however, might be potentially unsecure if an attacker between two communication partners can change the messages. This possible security vulnerability is covered by the paging-functionality (frequency hopping) and Bluetooth pairing. In addition, all the transferred content is wrapped in a nested, encrypted package (see Figure 2). Therefore we use FinTS / HBCI packages, which are established in online banking and deemed secure, so far.

Thus follows: By securing the Bluetooth connection, as described above, the customer's bank details cannot be misused for unauthorised transactions. FinTS / HBCI packages are not used in unforeseen configurations. Thus the security follows directly from the adoption of the security-level of FinTS / HBCI.

3.2 Anonymity and Anonymisation

To display and analyse the safeguarding of anonymity - especially from client's perspective - the participating entities and their available information we created Table 2, which shows that anonymity is achieved (in terms of concept, described above). It is possible that the content-provider could log and store an ID of the customer's device, but no personal information of the customer. Therefore each

provider knows what he sold when to which ID and for returning customers how much money they spend on average, but not the financial institute or bank, the customer has his account or even personal information. The anonymisation service in turn knows the bank, the seller and the amount paid, but has also no personal data available and also knows not what was sold. The anonymisation service also cannot combine identified devices with the bank details to create possibly unique user profiles. The bank has necessarily all customer data available, but does not know in which providers or even in what its customers have spent their money.

Sequence of Communication steps	Provider knows	Anonymisation service knows	Bank knows
1st: Initial situation	Content/offer	—	Customer data
2nd: Transmission of content-list	Content/offer device ID of the customer	—	Customer data
3rd: Purchase request	Content/offer device ID of the customer, product selection of these device ID	Provider,bank	Customer data,paid amount
4th: Connection to anonymisation service and financial service (bank)	Content/offer device ID of the customer, product selection of these device ID	Provider, bank	Customer data, paid amount
5th: Bank transfer	Content/offer device ID of the customer, product selection of these device ID	Provider, bank, paid amount	Customer data, paid amount
6th: Bank transfer acknowledgement to provider and customer	Content/offer device ID of the customer, product selection of these device ID, paid amount	Provider, bank, paid amount	Customer data, paid amount

Table 2. Present Information per Entity

3.3 Key management

In this section the secure key management (key generation, key distribution and key storage)[5] for our concept of secure and anonymous cashless transactions with

[5] A secure deletion of cryptographic keys is assumed, but not described in this article.

Bluetooth will be theoretically evaluated. This is, of course, no replacement of any practical evaluation, in field and under real conditions.

The **key generation** for both, mobile device and the content provider is realised with the Diffie-Hellman procedure [11]. It is assumed, that these private keys are not handled out to unauthorised third parties. Therefore a secure application and operating system is assumed as well. The generation of asymmetric key pairs (bank, anonymisation service) is realised by a trusted third party. Third party's key distribution is realised by usage of secure communication channel (e.g. with smart cards). A secure **key storage** (see Fig. 3) is realised by restricting the access on storage areas within the SIM card, which is protected through its special construction against unauthorized access and physical attacks. The secure storage of cryptographic keys at the content provider and the financial institute is protected in compliance with common security standards (e.g., ISO/IEC 2700x – information security management[6]), that are already provided by those institutions for a couple of years. This applies to the system which runs the anonymisation - application as well. In all misuse cases, when keys are compromised or invalid, e.g. caused by retirement of communication members, a **key update** is needed. This procedure is differently realised by participating instances. The Diffie-Hellman protocol generates dynamically a session key with every new communication session. Therefore a new key is available for every single session. The mobile device could update the public key of the anonymisation service within a secure communication connection session with the content provider. Content providers are easily connectable to a certain key server, where a list of valid public keys of different anonymisation services are stored. A transmission of a new private key of the anonymisation service from a trusted party should be realised over secure communication channels. The revocation and generation of new FinTS key pairs is a standard procedure, provided by the financial institute (bank) and common to online banking accounts.

3.4 Practical relevance, Applicability

The security of the concept in practice is mainly depending on the key management. Thus, following a clarification of when and how the keys can be initialized and locked. The HBCI-key (mostly independent from our concept) is most relevant to security. It is initialized as usual on at the financial service, in particular the bank. This key can easily and quickly blocked, if required by phone or online, as already known from online banking. The only other key that is needed in this concept is the public key of the anonymisation service. This could either be downloaded via a website of the anonymisation service (via SMS service or directly via internet connection) or at the content-provider terminal. The latter case would be most convenient, because it demands no additional effort by the customer. However, this would still require the signature of the key with a trusted CA. Otherwise the content-provider would have the chance for a Man-

[6] http://www.27000.org/

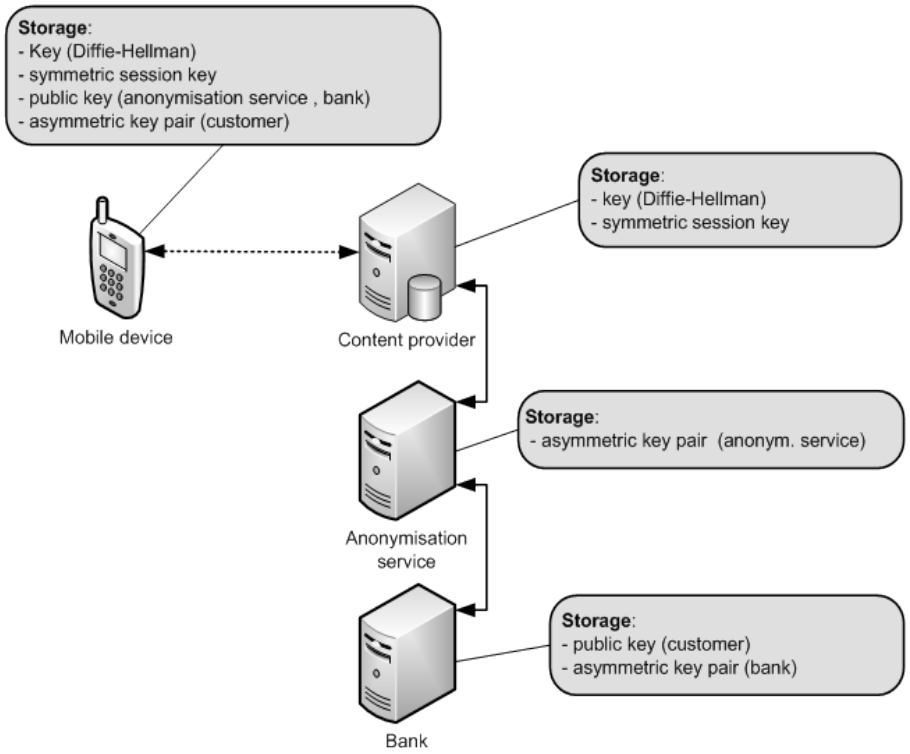

Fig. 3. Overview of key storage on different systems for secure cashless transaction application via Bluetooth

in-the-middle attack. For the practical relevance of this concept the expected user acceptance is important, well.

This is typically depending from the context, the function and from a variety of other factors, e.g. response-times [13]. In our concept, the security was outlined as central. Nevertheless we also calculated performance values for the duration of data transfers, because it is very unlikely that potential customers want to wait long for the content list or transaction acknowledges. The following values are measured in a large number (> 50) of tests in different environments. Thus, calculated means are:

- Request of content list of service providers (32 bytes) = 600 ms,
- Transmitting the content list (800 bytes) = 5700 ms and
- Sending of the transfer packet (300 bytes) = 1700 ms.

4 Future prospects

The results, which are determined from the successful prototypical implementation and the testing of the above described concept, could be relevant for a production system in practice. So far the prototype simulates only a mobile device based on Java. For the production system the software should be implemented and tested on a "real" device (e.g. a mobile device). Additionally "genuine" FinTS / HBCI packets should be used. Therefore a test- or a real bank account is needed. The proof of concept simulates FinTS / HBCI packets indeed, but the correct connection to HBCI could not be tested because of the unavailable financial account (incl. key and signature). The anonymisation service has to be extended, too. One central anonymisation service would be simulated. A total breakdown of the anonymisation service can be caused by single DoS attacked anonymisation service server. This can be avoided through the distribution of the anonymisation service out to several parallel randomly anonymisation services chosen by the content provider. Transmission interruptions during the Bluetooth transmission could be restarted if the content provider stores the ID of the mobile device and the (to transmitted) content temporarily. This routine was considered in the concept and should be implemented in a production system for a better user acceptance of the secure cashless transaction service with Bluetooth devices. That's why upcoming evaluation studies must be carried out as practical field tests to ensure a realistic change in environmental conditions and to reach a high number of "participants" and transactions. As second acceptance criteria, timeframes in interaction processes (e.g. time between content-list-request and reading the content-list) are relevant. Future studies should take those issues systematically into account, beside intrusion tests and dependability analyses.

Acknowledgements

The work described in this paper has been supported in part by the European Commission in the context of the programme COMO - Competence in Mobility (EU/EFRE) under Contract No. C(2007)5254. The information in this document is provided as is, and no guarantee or warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Jana Fruth is funded by the German Ministry of Education and Science (BMBF), project 01IM08003C. The presented work is part of the ViERforES project.

References

1. Ehlerding, S., Handys werden zum Elektro-Portemonnaie: http://www.spiegel.de/netzwelt/mobil/0,1518,627578,00.html
2. Nohl, K., Paget, C.: GSM – SRSLY?, Vortrag auf dem 26th Chaos Communication Congress, 27.-30. Berliner Congress Center, Berlin, 2009

3. Finistere, Kevin and Zoller, Thierry: All the Bluetooth Is belong to us. The rest too, In ProceedingsHack.lu, Luxembourg/Kirchberg, 2006
4. Laboid, H.; Afifi, H.; Santis C. DE: WI-FI TM, BLUETOOTH TM, ZIGBEE TM AND WIMAX TM, Springer, 2007
5. Clarke, I.: The FreeNet Project Homepage, 2004, http://freenetproject.org/
6. Reiter, M. K., Rubin, A. D.: Crowds: anonymity for Web transactions, ACM Transactions on Information and System Security (TISSEC), S. 62-92, 1998
7. Chaum, D.: Untracable electronic mail, return addresses, and digital pseudonyms, Communications of the ACM, 4(2), 1981
8. Eckert, C.: IT-Sicherheit, Konzepte - Verfahren - Protokolle, 5. überarbeitete und erweiterte Auflage, Oldenbourg Verlag, München, Wien, 2008
9. Bluetooth SIG, Inc., Bluetooth Specification Version 2.1 + EDR, Vol. 1, 2007
10. Bluetooth SIG, Inc., Bluetooth Specification, Version 4.0, Vol. 0, 2009
11. Diffie, W. and Hellman, M. E.: New Directions in Cryptography, IEEE Transactions on Information Theory (22:6), pp. 644–654, 1976
12. Huber, K.: FinTS V4.0 Kompendium – Financial Transaction Services, 2004
13. Molich, R., and Nielsen, J. (1990). Improving a human-computer dialogue, Communications of the ACM 33, 3 (March), 338-348.
14. Pousttchi und Horster: Bundesministerium für Wirtschaft und Arbeit: MobilMedia-Barometer, 2. Welle: M-Payment; Befragungszeitraum: 11.-14.09.2004, 2004
15. Wiedemann, Goeke und Pousttchi: Ausgestaltung mobiler Bezahlverfahren - Ergebnisse der Studie MP3, 2008