Assessment of Today's Mobile Banking Applications from the View of Customer Requirements

Key Pousttchi and Martin Schurig

University of Augsburg

2004

Assessment of Today's Mobile Banking Applications from the View of Customer Requirements

Key Pousttchi

University of Augsburg, Chair of Business Informatics and Systems Engineering (WI2)
e-mail: key.pousttchi@wiwi.uni-augsburg.de

Martin Schurig

Tecways AG

e-mail: mschurig@tecways.com

Abstract

Mobile banking is a subset of electronic banking which underlies not only the determinants of the banking business but also the special conditions of mobile commerce. This paper analyzes customer needs and expectations from the mobile applications' view and from the banking view in order to derive a defined set of requirements. Based on these results, existing mobile banking applications are assessed. Their major shortcomings are explained, opportunities for their improvement are shown and the impact of upcoming new technology is discussed. The outcome of the paper is a defined set of customer requirements to mobile banking applications, the identification and assessment of four standard types of current mobile banking applications and an explanation of major failure reasons along with opportunities for their improvement.

1 Introduction

Electronic banking – the execution of financial services via the Internet – changed the business of retail banks significantly, at the same time reducing costs and increasing convenience for the customer. The ever-increasing spread of Internet-enabled phones and personal digital assistants (PDA) made the transformation of banking applications to mobile devices a logical development of electronic banking. This created a new subset of electronic banking, *mobile banking*. According to the sweeping enthusiasm that characterized much of the news reporting in the years 1999 and 2000 mobile banking should by now have been firmly established as the most important distribution and communication channel for retail banking. Reality today is a different matter though. Mobile banking as an established channel still seems to be a distant prospect.

We define mobile banking (in the broader sense) as that type of execution of financial services in the course of which - within an electronic procedure - the customer uses mobile communication techniques in conjunction with mobile devices. As *mobile devices* we refer only to those whose use is typically mobile. Most notably, this restraint affects notebooks and sub notebooks, which are easily transportable, but whose use is typically stationary. The typical connection for these mobile devices up to now is realized through mobile communication. Most relevant is GSM/GPRS, also typical are comparable 2G standards (e.g. IS-136, IS-95) and soon will be evolving 3G-technologies (EDGE, CDMA-2000, UMTS). We do not focus on WLAN scenarios. The use of a banking application on a laptop computer with a WLAN connection underlies the rules of electronic banking, not the special rules of mobile banking.

As its superset electronic banking, mobile banking (in the broader sense) is divided into two main areas:
- *mobile brokerage* which covers securities transactions via mobile devices, especially stock trading, and
- *mobile banking (in the narrower sense)* which covers the account management via mobile devices.

For our purposes we use the term mobile banking – if not otherwise indicated – in the second, the narrower sense. However, methodology and results of this contribution are, mutatis mutandis, transferable to mobile brokerage.

In this paper we analyze customer requirements to mobile banking. After examining general conditions of mobile banking in section 2, we identify relevant mobile banking use cases as well as special characteristics of the mobile use of an application in order to derive a set of requirements to mobile banking applications in section 3. In section 4 we work up the state-of-the-art of mobile banking and identify four standard types of applications. In section 5, these are assessed according to the set of requirements developed before. Based on these results major shortcomings of today's mobile banking applications are identified and opportunities for their improvement are shown in section 6. The possible impact of upcoming new technology is discussed in section 7. Finally, section 8 provides conclusions and a brief outlook to the future of mobile banking.

The outcome of the paper is a defined set of requirements to mobile banking applications, the identification and assessment of four standard types of current mobile banking applications and an explanation of major failure reasons along with opportunities for their improvement.

2 General conditions of mobile banking

Electronic banking is one of the most successful business-to-consumer applications in electronic commerce (EC). Fulfilling customers' needs through the employment of EC's special property of *reduction of temporal and certain spatial limitations* (using the extension of the theory of informational added values to EC, we refer to this as an *electronic added value* [14]), electronic banking significantly changed the way in which many customers accessed their bank account. Figure 1 shows the relevance of electronic banking to the US market as an example (as from Forrester [11]). In a number of European countries 30-40% of the Internet users use electronic banking [11].
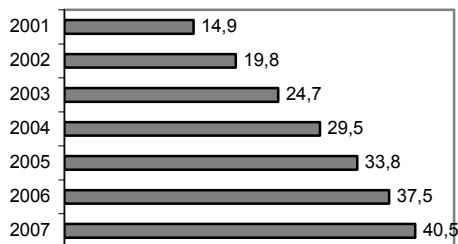

Figure 1. US households using electronic banking in mio.

Banks greatly support this not only because they could meet their customers' need for convenience but also because of the enormous economic impacts in replacing a high-cost channel (bank clerks) through a low-cost channel (a central web server) for simple transactions, with the additional benefit of eliminating the necessity for a media conversion.

This coincidences with the extremely high penetration of mobile devices, especially phones. In the US, the penetration in 2002 reached 51 mobile phones per 100 inhabitants, in Japan 59 and in Western Europe even 78 (as from Bitcom [11]).

Since users considered their mobile phone as a personal trusted device making it to an integral part of their lives and more and more of these devices became Internet-enabled, the regular conclusion was the transformation of banking applications to mobile devices as the next step of electronic banking development.

For mobile banking, the advantages even go much further than for electronic banking: The high penetration of mobile phones reaches all social levels, mobile applications disband the limitations of electronic banking as they allow for a use anytime-anywhere and the subjective and objective security of the device is higher than that of a personal computer [8]. The profit and loss account was also favorable: Taking the example of a German bank, a bank transaction via a clerk generates overall costs of 2 US-$ while a mobile banking transaction gets along with 15 cents.

As several studies showed, the willingness of users to execute financial transactions via their mobile device was also high (e.g. in a survey of 16,500 German Internet users, more than half were favorable to do this [2]).

Despite all of this, more than four years after the start of the first mobile banking applications customers simply do not use them and utilization figures stay very far behind all expectations (e.g. [1]). Mobile banking as an established channel still seems to be a distant prospect.

The reasons for this great disappointment are to be analyzed. Doing so in the following sections, we do not intend to start with current applications (which could mean biased) but from scratch, with an analysis of the customer requirements to such applications.

3 Customer requirements for mobile banking applications

3.1 General considerations

A mobile banking application is, first of all, a mobile application. To conceptualize a mobile application, additional informational added values have to be targeted, using *mobile added values* [14]. In other words, it is far from sufficiency to just porting an existing Internet application on a mobile device. Mobile applications have to be specifically made-to-measure on the one hand side to the needs and expectations of the mobile user, and on the other hand side to the specific restrictions of mobile communication techniques and mobile devices.

In order to derive a set of requirements to mobile banking applications we pursue two steps: Firstly we identify general characteristics of the mobile use which are relevant. Secondly we closely watch the user and his context when wanting to use mobile banking.

3.2 Characteristics of the mobile use

The use of mobile applications underlies several specific restrictions. We consider five characteristics of the mobile use to be particularly relevant as they greatly influence the design of mobile banking applications and the suitability of certain technical solutions.

A mobile application is used via a mobile device. For these devices (currently either a mobile phone or a PDA), special limitations are valid [8]. For the mobile banking context, above all, these are the limited input and display capabilities.

The connection is provided by a mobile network operator (MNO). This is especially important if applications need to access certain parts of the infrastructure which are under control of the MNO (e.g. the SIM card). In the case of negotiations, these have to be pursued with all MNO on the designated market.

The use of mobile data transmission is expensive. In the case of circuit-switched data transmission (e.g. GSM-CSD or HSCSD) this extends to the connection time, in

the case of packet-switched data transmission (e.g. GPRS) this extends to the transferred data volume.

Sensitive data is transmitted. This implicates the use of adequate security measures.

A disruption of the usage is possible at any time. This is principally already true for electronic banking as well (the connection may e.g. be disrupted by a breakdown of the transmission or of the operating system of the client computer) and provides a special necessity to avoid incomplete transactions. For mobile banking, it is extremely more probable as a mobile usage causes a continuous change of conditions, e.g. through geographical influences or cell-handover. Thus, it is also important for the usability of a service: It is not acceptable for a user if he almost completed a transaction and his train enters a tunnel that he has to wait until the end of the tunnel and restart his transaction from the beginning (hoping the next tunnel is far away enough).

It is important that the named restrictions have to be considered as early as possible, which means in the phase of conceptualization.

3.3 Mobile banking use cases

A mobile user has to be seen from his context when using the application. Needs and expectations are not generic, but bound to this context.

As a typical mobile banking user, we consider someone who already is an electronic banking user [2], shows significant affinity to technology and often finds himself in situations where he can not (or does not want to) rely an infrastructure necessary for electronic banking.

In the following, we introduce four use cases. These have been developed in the course of two group discussions, each group consisted of mobile banking users and mobile commerce experts. The groups focused on identifying real-life situations in which the use of mobile banking provides an informational added value [8]. The resulting situations have been aggregated to the use cases [3]. The use cases are not exhaustive, but representative: Each case stands for a series of cases, which are similar in the depth of the desired information and/or the conditions of the usage. For each use case we identify the most important, concrete need that the user has in this particular situation.

Use case 1: Request of account balance.
The user is in a mobile situation (e.g. in a department store) and intends to know his account balance, e.g. to verify his account before realizing a spontaneous purchase.
Resulting need: Quick obtainment of account balance.

Use case 2: Control of account movements.
The user is waiting for an important cash receipt on his account. He intends to have the exact details of the cash receipt.

Resulting need: Continuous control over movements on the account.

Use case 3: Instant payment.
The user is in a mobile situation and intends to make a payment by bank transfer from his account.
Resulting need: Instant execution of a bank transfer.

Use case 4: Administration of the account.
The user intends to use spare time (e.g. using a train or waiting on the airport) to administrate his account.
Resulting need:
Quick and easy-to-use execution of transactions and administration is possible.

3.4 Resulting requirements

With regard to the characteristics we identified in 3.2 and the use cases we introduced in 3.3 we develop 15 requirements to mobile banking applications which are explained in the following.

The requirements can be discerned into four categories: technical, usability, design and security. We did so in order to later locate the problem areas of applications.

Technical requirements:

- *The usage must be possible with both kinds of available mobile devices.* This requirement is resulting from the characteristic that usage will be made with a mobile device. It should be possible for the user to use his preferred device, in order to benefit from its advantages.

- *The application should adapt to the conditions of the mobile device automatically.* This is resulting from the same characteristic. The application should automatically detect the kind of device it is executed on and adapt automatically to its features.

- *The usage must be possible for customers of any MNO.* This requirement results from the characteristic that usage will be performed through the network of one the respective MNO. The usage must be possible for everybody, the customers of one operator must not be locked out.

- *The amount of the transmitted data should be as small as possible.* This requirement results from the second characteristic that mobile data transmission is expensive. Additionally to the aspects of cost, the aspect of waiting time (impacting negatively on convenience) for the transmission is also important.

Usability requirements:

- *The possibility to work offline with the application.* This requirement results from the fact that mobile data transmission is expensive (this especially for circuit-switched connections) as well as from the fact that a disruption is possible at any time. It should be possible to use the application without a permanent connection to the bank server.

- *A simplified method of data input.* This requirement is of special interest when a necessity is given to enter higher amounts of data, thus in the use cases *instant payment* and *administration of the account.* There should be a way to facilitate this for the user.
- *Resumption of usage at the same point after disruption.* This requirement is resulting from the characteristic that mobile usage can be disrupted at any time. In such a case the application should allow the user to resume his usage at same point where it was disrupted, without a complicated log-in procedure.
- *"One-Click"-Request of important data.* This requirement is resulting from the first two use cases, in which it is important to allow quick access to information. This information should be available with just a few "clicks", in the ideal case with only one.

Design requirements:

- *The possibility to personalize the application.* This requirement can be deduced from different use cases. If the user gets a lot of data displayed, there should be a the possibility to use a personalized structure to view the data.
- *The possibility to scale the application.* This concerns the easy switch of use cases for the user, e.g. if he gets an unexpected account balance and wants to find out more details. In these cases, it should be easily possible to switch to a version of the application with a wider range of functions.
- *The possibility to get announcements on important events*. In some use cases, especially in the *control of account movements*, it makes sense if the application could provide a push functionality.
- *A wide range of functionality, similar to the one in the electronic banking.* This requirement is resulting from the last use case, where the user wants administrate his account. In order to make mobile banking a real alternative to electronic banking, the customer should find complete functions there (even if they are more difficult to access as they are only occasionally used).

Security requirements:

- *The transmission of the data has to be encrypted.* This is resulting from the fact that a mobile banking application is transmitting sensitive data. To secure this data, the connection must be encrypted.
- *Before usage, access to the data must be authorized.* This is resulting from the same characteristic. Before a user can access his data he has to prove that he is entitled to do so.
- *The authorization has to be simple.* Especially in the first two use cases, where a quick access to the data is important, authorization has to be fast and simple.

As an intermediate result we possess a set of criteria representing customer requirements to mobile banking applications. The set is shown in table 1.

Table 1. Set of customer requirements

Technical requirements
Usage is possible with both kinds of devices
Adaptation to device
Usage regardless of network operator
Small amount of transmitted data
Usability requirements
Possibility to work offline
Simple data input method
Resumption of usage at the same point
„One-Click"-Request
Design requirements
Possibility to personalize the application
Possibility to scale the application
Announcement of events
Wide range of functionality
Security requirements
Encrypted data transmission
Authorization of access
Simple Authorization

The set is suitable to qualitatively assess a given (existing or prospective) application as well as to compare different applications. The mode of operation is to simply check each criterion if it is fulfilled or not. The result is a weak-point analysis where every point which is not fulfilled has to be examined closer with regard to its implications. We will use the scheme in this way in section 4 for an assessment of the four standard types of applications.

3.5 Construction of a quantitative model

Beyond the shown type of application, the scheme is also suitable to a quantitative assessment. This would take into consideration and carry on an important point we mentioned in section 3.1: the special set of needs and expectations.

A typical application for the scheme could be the choice of the optimal type of application either for a concrete user or for a bank which has a concrete profile of its target group. Using standard OR methods, the mode of operation is to

- weigh the use cases with the index $j = 1$ to 4 and attach a parameter u_j to each of the use cases corresponding to its importance for the target group (side condition: all u_j with $j = 1$ to 4 have to sum up to 1.00).
- weigh the requirements with the index $i = 1$ to 15 for the requirement and the index $j = 1$ to 4 for the use case and attach a parameter r_{ij} to each of the requirements corresponding to its importance for the target group (side condition: all r_{ij} with $i = 1$ to 15 and the same j have to sum up to 1.00); either the requirements' importance can be differentiated between the use cases or it can be determined equally across the use cases (in the latter case all r_{ij} with the same i would contain the same value).

– attach a parameter f_{ij} for the fulfillment to each of the fields in the matrix, containing "1" if the requirement i is fulfilled in the use case j and "0" if not.

For each use case the fulfillment is now measured by the row sum; the sum of all row sums results in the overall performance indicator of the assessed mobile banking application for the intended target group. An order of relevance of the requirements is measured by the column sum.

In order to refine the model it would be possible to allow any value between 0 and 1 instead of only integers to f_{ij}, corresponding to its degree of fulfillment. The model is shown in table 2.

Table 2. Quantitative model

	Requ. 1	...	Requ. i	...	Requ. n
Use Case 1	$f_{1.1}*u_1*r_{1.1}$	...	$f_{i.1}*u_1*r_{i.1}$	...	$f_{n.1}*u_1*r_{n.1}$
Use Case 2	$f_{1.2}*u_2*r_{1.2}$	...	$f_{i.2}*u_2*r_{i.2}$	...	$f_{n.2}*u_2*r_{n.2}$
Use Case 3	$f_{1.3}*u_2*r_{1.3}$	...	$f_{i.3}*u_2*r_{i.3}$	...	$f_{n.3}*u_2*r_{n.3}$
Use Case 4	$f_{1.4}*u_2*r_{1.4}$	...	$f_{i.4}*u_2*r_{i.4}$	...	$f_{n.4}*u_2*r_{n.4}$

Although not in our focus and just to give an idea to the reader how a typical order of relevance might look, we depict the result of a survey among a target group of 20 users at the University of Augsburg who were asked to determine the u_j and the r_{ij}. The resulting order of relevance is depicted in table 3.

Table 3. Customer requirements in an order of relevance

Rank	Requirement
1	Usage regardless of network operator
2	Authorization of access
3	Encrypted data transmission
4	Usage possible with both kinds of devices
5	Simple Authorization
6	Adaptation to device
7	Simple data input method
8	Resumption of usage at the same point
9	Possibility to work offline
10	Small amount of transmitted data
11	„One-Click"-Request
12	Possibility to scale the application
13	Wide range of functionality
14	Possibility to personalize the application
15	Announcement of events

4 Mobile banking applications

4.1 Examined applications

In the following, the main types of existing mobile banking applications are introduced. These build standard types as each of them is representative for a series of comparable applications. While WAP-banking and mobile banking via PDA are generic, SMS-banking and mobile banking with SIM Toolkit use specialties of the GSM standard.

4.2 WAP-banking

The most widespread solution for mobile banking is based on micro-websites following the WAP standard (Wireless Application Protocol). The function of WAP-banking is in many ways similar to the function of Electronic banking using http. The client sends a request and gets a response with page content which is stored on or dynamically generated by a standard web server. The main difference is in the usage of a WAP gateway for the conversion of the protocols. At banks must be considered that very sensitive data is processed. While a normal content provider doesn't has to observe special security precautions, and in some cases can even use the services of extern providers, a has to secure its web server and WAP Gateway specially against unauthorized access. This is especially necessary because of the fact that inside the WAP Gateway the encryption protocol is converted from SSL/TLS to WTLS with the effect that data is not encrypted while it is processed. While authentication is assured via a PIN (personal identification number) of the user, authorization for transactions is realized via transaction numbers (TAN). This concept, known from the electronic banking, forces the user to carry a TAN list with him in order to make transactions.

4.3 SMS-banking

The Short Message Service (SMS) is a GSM service to exchange text messages up to 140 byte (or 160 characters of 7 bit). The transmission of mobile-originated short messages is carried out by the short message service center (SMSC) of the particular network operator. The SMSC is receiving the message from the mobile device and routing it to the destination device. For generating mobile-terminated short messages, it is possible that a company or a special service provider runs an own SMSC. Thus, a bank could generate SMS from bank data like account balance or account movements and send it to the mobile device of the customer. This technique is used at SMS-banking: The customer sends an SMS with a request to the bank, and gets the desired data as an answer. The customer has to include a PIN for authorization in every SMS he sends to his bank. Alike the WAP banking, one should pay special attention on the security of the location of the SMSC. The operation of SMSC is offered as a service by many service providers. The usage of such a service is out of question for banks, because of the high sensitive character of the transmitted data. For this reason it is mandatory for banks to run their own SMS-Gateway and secure it from unauthorized access.

The main problem with this kind of transmission is the missing encryption of the data during the on-the-air transmission between the service center and the mobile

phone. An encryption of pure text-SMS is not possible (unless an application on the mobile device would be able to decrypt the information). So the data is transmitted unencrypted. Because of this missing encryption, banks are only offering pure information services like a request for the account balance via SMS. Thus, it is not possible to make transactions via SMS banking [5].

4.4 Mobile banking with PDA

Next to the mobile banking applications which where designed for the use on a mobile phone, there are some applications which enable mobile banking by using a PDA instead. This could eliminate a lot of technical restrictions of mobile phones. First of all, a PDA easily offers the possibility to store and execute individual software on it. In contrast to a mobile phone, data can be stored on a PDA und due to its processing power it is possible to process much more complex calculations. Additionally they are providing a bigger, often colored, display. Data input is possible via a pen and recognition of handwriting or displayed keyboard. For communication purposes PDA have to include a transmission module (e.g. GSM) or additionally need a mobile phone, with which they communicate via an infrared or Bluetooth interface. The communication between the bank an the mobile device is typically carried out via binary SMS. Binary SMS contain in contrast to pure text SMS binary data in an 8-bit format. The maximum capacity of an SMS is 140 bytes or 1120 bit [6]. The usage of binary SMS is offering the possibility to secure the data against unauthorized access. The function of the access is similar to the one at the SMS-banking. A SMS with customer data is generated by the SMS-Gateway and sent to the mobile phone of the customer. The SMS-Gateway of the bank must be able to generate binary SMS and to encrypt them for transmission. The data which should be sent to customer is split into single data packages which are packed into single SMS. For the transmission, a symmetrical encryption is used. For the exchange of the keys which are used for the symmetrical encryption, a asymmetrical encryption is used. For this encryption a so called master key is generated on the PDA, which whom the later symmetrical encryption is performed. To secure a safe transmission of this master key, the data package which contains this master key, is encrypted with the public key of the bank. This public key is installed together with banking software on the PDA. The bank can now decrypt the received package with its private key an establish a symmetrical encrypted connection with the received master key. Additionally to the encryption, every data package has a so called Message Authentication Code, a checksum which can be verified by the recipient and which secures the authentication of the data. As an additional security measure, the already known authorization with PIN and TAN is used.

4.5 Mobile banking with SIM-Toolkit

SIM Application Toolkit (SIM-Toolkit, SAT) is a GSM standard for extended communication between the SIM-card and the mobile device. A respective solution is storing the mobile banking application on the SIM Card of the user. Belgium was one of the first countries with banking applications using this technique in 2002.

On the SIM-card, several data is stored, e.g. for the authorization of customers, personal settings like phone book entries and sent and received SMS. In addition to this, there is free storage space left for individual applications. Typically, the network operator uses this to provide different applications, e.g. for information or entertainment services, which can be started by the customer via the menu structure of the mobile phone. These applications can access the whole functionality of the mobile phone, i.e. they can communicate via SMS or WAP [7]. Alike this, SAT can also be used to realize mobile banking applications. Being perhaps the most important disadvantage of SAT solutions, only the MNO is able to store applications on the SIM card [8]. Actual applications often use SMS for data transmission. As programmable elements can be executed, the use of binary SMS and encryption is possible. If the bank sends bank a binary SMS as an answer, the mobile phone recognizes the binary data and forwards the data for processing to the application on the SIM-Card which again uses the phone display to communicate with the user [9].

5 Fulfillment of Requirements

5.1 Overall assessment

The results of section 4 allow to give a qualitative assessment of the examined application types according to the scheme developed in section 3.4 (table 4).

Table 4. Assessment for the four standard types

	WAP	SMS	PDA	SIM-AT
Independent Usage	+	+	+	-
Authorized access	+	+	+	+
Encrypted transmission	+	-	+	+
Usage with both devices	+	-	-	-
Simple Authorization	-	-	-	+
Automatical adaptation	-	+	O	+
Simple input method	+	-	+	-
Resumption at the same point	-	+	+	+
Possibility to work offline	-	+	+	+
Small amount of data transmission	-	+	+	+
"One-Click"-Request	-	-	-	-
Possibility to scale application	+	-	+	+
Wide range of functions	+	-	+	+
Possibility to personalize application	+	+	+	+
Announcement of events	-	+	-	+

Legend: "+": fulfilled   "-": not fulfilled   "o": could not be rated

In the following we will comment on the individual requirements and their fulfilment.

5.2 Technical requirements

The most important technical requirement, the usage independent from the network operator is fulfilled by the most applications, only banking with SIM-Toolkit is not fulfilling the requirement. Only WAP-banking has the ability to run on both devices, the other applications are limited to mobile phones only, or the PDA. The automatic adaptation to the device can only be rated within applications for mobile phones. Here only applications which use native technology of mobile phones like SMS or the build in functions for the menus adapt in a satisfying way to the particular device. Because of the different implementations of the WAP standard into the mobile phones, WAP is not fulfilling this requirement. Also the requirement of small amount of data transmission is not fulfilled by WAP, because the whole application must be transmitted every time the banking is used. Other applications just transmit the data belonging to the respective transaction.

5.3 Usability requirements

None of the applications fulfills the requirement of a functionality to do a "One-Click"-Request. None of them has the functionality to authorize the customer automatically for the use of mobile banking. So it is not possible to process a request without input of authorization data. A simplification of the input method is only offered by applications using the WAP standard or by solutions for the PDA. The requirement of resumption at the same point after disruption and the requirement for a offline working modus, are fulfilled by all applications except WAP. Because of the fact, that WAP needs a continuous connection to the bank, this functions can not be implemented.

5.4 Design requirements

All applications except SMS-banking fulfill the requirement of a wide range of functions, and the requirement to scale the application. Because of the lack of encryption with SMS-banking, no functions for transactions are offered, and resulting from this fact, no possibility to scale the application. An announcement of events can only be realized with a technology based on SMS communication in connection with an application integrated directly in the phone. So only SMS-banking and banking with SIM-Toolkit would make such services possible. A possibility to personalize the applications is offered by all systems at least a little bit.

5.5 Security requirements

These are some of the most important requirements. The requirement of an authorization before access is fulfilled by all applications. The requirement of encrypted transmission is fulfilled by all systems except SMS-banking. As a result of this fact, the function of SMS-banking is limited (as is described already earlier). A simple authorization is only offered by SIM-Toolkit.

6 Weaknesses of current applications

As a result of the comparison, WAP-banking and banking with PDA clearly come out best. Banking with SIM-Toolkit also fulfills many of the of requirements, but the limitation of usage to single MNO and their customers is an important disadvantage and requires a devaluation. SMS is ranked last because of massive disadvantages in the field of security. Though the other two applications are significantly better than the others in the comparison, the problems of mobile banking still remain severe. The problems of the better-ranked applications are:

- *Complicated authorization:* To authorize the access with WAP-banking, it is necessary to input one or more PIN. These is not satisfying, especially in a mobile situation. A PDA solution offers theoretically the possibility to store the authorization data on the PDA, but the handling of two devices at the same time makes this solution also too complicated.
- *Unsatisfying adaptation to the particular device:* Though WAP is a common standard, it was implemented in different ways by some manufactures. This results in an inconsistent interpretation of the content on the mobile phones.
- *No offline usage possible:* WAP-banking needs a continuous connection to the bank during the usage, which must not be disrupted. It is not possible to work with data without being connected.
- *Unnecessary transmission of data:* With WAP-banking, the complete application must be transmitted to the mobile phone, every time a customer wants to use it. There is no possibility to store the application on the mobile phone.
- *Second device as problem solution inadequate:* The first four problems could be solved by using a PDA instead of a mobile phone. But the handling of two devices at the same time makes this solution typically too complicated.
- *No possibility for announcement services.* WAP-banking an banking with PDA are offering no possibility to integrate a push-service which announces events connected with the administration of the bank account.

7 Future of Mobile banking

7.1 Mobile banking with Java

One of the most discussed new developments in the field of mobile commerce, is the porting of the programming language Java onto mobile devices. The programming language Java, which was develop by the company sun for desktop computers and server has the advantage of being completely independent from any platform. Java programs for mobile devices are called midlets. In order to run a java program on a mobile device, a JVM (Java virtual machine) has to be integrated in the device. Additionally there has to be space, to store the application. To transmit the application to the mobile phone, there are a few different ways. The midlet can be loaded directly via WAP to the phone, or it is send via Bluetooth, Infrared or a data cable to the mobile phone. With the menu of the mobile phone, the application can be executed. The midlet can access a lot of the mobile phones functionality. In the actual version, midlets are able to establish a connection using http. For encryption the SSL-protocol can be used. With this technique it is no longer necessary, to send the data through a WAP-Gateway and convert them for transmission. The application accesses the data directly on the web server. With the use of SSL for encryption it is possible to establish a real end-to-end encryption.

Problem solution through java:

- Complicated authorization. Though it is possible to store authorization data in a mobile phone, with a java application and to use them for automatic authorization, but for security reasons, this is critical.
- Unsatisfying adaptation to the particular device. Here exists the same problem, as with WAP. Though there is a common standard, a lot of manufactures are expanding it on their own. This results again in different platforms.
- No offline usage possible. This problem is solved with a java application.
- Unnecessary transmission of data. Also this problem is solved through java.
- Second device inadequate problem solution. The advantages of a PDA are getting smaller with the usage of Java, but still it has some left, like i.e. display size.
- No possibility for announcement services. This problem exists still with java.

7.2 Advancement of WAP

Another big development in the field of mobile commerce technologies is the advancement of WAP. New protocols are implemented in WAP. In WAP 2.0 slightly modified Versions of http and TLS are implemented. As a result of this, mobile devices can access content on web server directly. There is no need anymore for a WAP-Gateway, which converts the requests. With the integration of TLS, it is finally possible, to establish a secure end-to-end connection between the server and the mobile device.

Push-Services are another new development in WAP 2.0 With the help of Push-Services, it is possible for the content provider to send information actively to the device of the user.

The newly introduced User Agent Profile cares about the very different features of the mobile devices. With the User Agent Profile, information about the technical features of the mobile device is send to the server with the request. The server is now able to prepare the information for the particular device in accordance to its features like display size, ability to display color etc. With this, a better adaptation to the different devices is enabled. [10]

Problem solution through advancement of WAP:

- Complicated authorization. There is still a complicated authorization procedure necessary. WAP 2.0 offers no function for automatic authorization.
- Unsatisfying adaptation to the particular device. With the introduction of the User Agent Profile, this problem is solved.
- No offline usage possible. This problem is still present, alike the first version of WAP, a continuous connection to the bank during the usage is still necessary.
- Unnecessary transmission of data. Also this problem still exists. Still the whole application is transmitted every time.
- Second device inadequate problem solution. The advantages of a PDA still exist, so the problem is not solved.
- No possibility for announcement services. With the introduction of Push-Services, this problem will be solved.

7.3 Further new developments

In the following further developments in the field of mobile commerce technology and their influence on mobile banking are discussed.

A major new development in the field of security for mobile commerce is the *digital signature*. Digital signatures are a method to clearly prove the origin of a message. Digital signature are more a method than a technology, that's why there is no concrete description of a technology in the following.

When somebody wants to secure a message with a digital signature, he has to deduce a Hash-value from the content of the message first. This Hash-value is encrypted with the private key of the sender and send together with the message to the recipient. The recipient does two things, first he deduces also a Hash-value, by using the same method like the sender. Than he takes the received en-

crypted Hash-Value and decrypts it with the public key of the sender. Finally he compares the two values. If the values are the same, he can be sure, that the message is authentic.[11]

To use this method for mobile banking, the following things would be necessary:

- A private key (only known to the sender)
- A public key (know to the bank)
- A safe place to store the public key
- An application to encrypt the deduced Hash-Value
- An application to generate the message, deduce the Hash-Value and send them both together

For the last three items, it would be possible to create an mobile banking application which stores the private key, does all the encryption, generates the message and sends them. The problem would be to equip the user with a private key, that is strong enough to be accepted by the bank as sufficient security mechanism. One way would be, that the bank is equipping all their customers with the adequate keys. The problem with this method, would be, that these keys would only be valid for transactions of the particular bank.

Another possible solutions would be to equip the user with a universally valid key. With such a key it would be possible for the user to do transactions with different banks, or even use this key for other purpose in mobile commerce, like i.e. shopping or payment. For this method it would be necessary to establish a network of institutes which are allowed to issue keys, which are universally accepted.

The big advantage of the use of digital signatures would be the solution of the problem of complicated authorization. With an application for mobile banking, which automatically signs every transaction with a digital signature, no more complicated authorization with PIN and TAN would be necessary.

7.4 New forms of devices

Not only in the field of applications, advancements are made. Also new forms of devices are promising the solution of some of the problems in the near future. There are basically two new forms of devices which are becoming more and more popular. Smartphones and PDA with integrated telephony. PDA with integrated telephony are advancements of the already known PDA. The have the same operating systems and the use the same interface, like handwriting recognition or small keyboards. They just have the features of a mobile phone integrated, which means the applications installed on them can easily communicate with various sorts of protocols. Of course also a mobile banking application can use this features.

A second new form of devices is the so called smartphone. A smartphone is a device which is primarily controlled with a telephone keyboard, and has an operating system which was specifically designed for the use in a telephone.

PDA with integrated telephony and smartphones solve the problem, that a second device is an inadequate problem solution. As described earlier a lot of the problems of mobile banking can be solved by using a PDA. But the handling of two devices is very complicated. These devices united the advantages of a mobile phone and a PDA. With the possibility to install individual applications and store data, the offer a lot of opportunities for the developer of mobile banking applications. But there's still some danger involved. With different incompatible operating systems, it is very important for the banks to use techniques which are independent from the platform, like i.e. Java.

8 Conclusions and Outlook

In the preceding sections we analyzed the relevant customer requirements to mobile banking. We examined general mobile banking conditions and identified relevant mobile banking use cases as well as special characteristics of the mobile use of an application. Based on these results we derived a set of requirements, which we employed later to assess four state-of-the-art standard types of mobile banking applications in order to identify their major shortcomings, show opportunities for their improvement and discuss the upcoming new technology along with their possible impact.

The outcome of the paper is a set of requirements to mobile banking applications, the identification and assessment of four standard types of current mobile banking applications and an explanation of major failure reasons along with opportunities for their improvement.

The major goal of the banks is to repeat – and if possible expand – the big success of electronic banking in mobile banking. But the banks have to keep in mind that the usage of mobile banking is taking place under completely different circumstances - under the application of mobile commerce rules.

Four different types of mobile banking applications (which are already in use) and some future developments where introduced and assessed. None of the technologies can provide a mobile banking solution that works completely without problems and satisfies the customer. The recommendation to the banks should be not to focus on one technology only, but to use the advantages of different technologies. The target group has to be identified, afterwards the requirements scheme from section 3.4 could already help to define its properties - ideally this should be confirmed by empirical examination. If the target group and its properties are carefully defined, these results have to be used as input for the quantitative model developed in section 3.5 which, then, clearly assesses the different applications according to this target group. Only with a respective combination of new technologies it will

be possible for banks to achieve success in mobile banking in the long run.

References

[1] *Rubrech, H. J.:* In: Mobile Business – eine Achterbahnfahrt mit Ziel. Geldinstitute, 9 (2001), pp. 30 – 32.

[2] *Speedfacts Online Research GmbH:* mBanking the future of personal financial transactions? Frankfurt 2001.

[3] *Schurig, M.:* Kontoführung unter Nutzung mobiler Endgeräte. Augsburg 2003.

[4] *Mustafa, N.; Oberweis, A.; Schnurr, T.:* Mobile banking und Sicherheit im Mobile Commerce. In: Silberer, G.; Wohlfahrt, J.; Wilhelm, T. (Hrsg.): Mobile Commerce – Grundlagen, Geschäftsmodelle, Erfolgsfaktoren. 1. Ed., Wiesbaden 2002, pp. 353 – 372.

[5] *Fun Communications:* Benutzerhandbuch Endkunde VR-NetWorld banking mobil (Version 1.06), Karlsruhe 2002.

[6] *GSMBox.de:* Technische Informationen über die SMS. http://de.gsmbox.com/gsm/sms/info-tecno.gsmbox, 2002, Abruf am 2002-12-12 .

[7] *Weißbuch Mobilkommunikation:* SIM gibt dem Handy Sinn. In: Forum Mobilkommunikation, http://www.fmk.at/mobilkom/detail.cfm?Textid=17 &Kapitelnr=8, 2001-06-29, Abruf am 2002-12-19.

[8] *Turowski, K.; Pousttchi, K.: Mobile Commerce – Grundlagen und Techniken.* 1. Ed., Heidelberg, 2003.

[9] Rankl, W.; Effing W.: Handbuch der Chipkarten, Aufbau – Funktionsweise – Einsatz von Smart Cards. 4. Ed., München 2002.

[10] Merz, M.: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien. 2. Ed., Heidelberg 2002.

[11] *Graumann, S.; Koehne, B.:* Monitoring Information Economy, 6. Fact Sheet 2003. NFO Infratest on behalf of the German ministry of Economics. Munich, 2003.

[12] *Kreyer, N.; Pousttchi, K.; Turowski, K.:* Standardized Payment Procedures as Key Enabling Factor for Mobile Commerce. In: *Bauknecht, K.; Quirchmayr, G.; Tjoa, A M. (Eds.): E-Commerce and Web Technologies. Third International Conference, EC-Web 2002.* Aix-en-Provence 2002, pp. 400-409.

[13] *Pousttchi, K.: Conditions for Acceptance and Usage of Mobile Payment Procedures.* In: Giaglis, G. M.; Werthner, H.; Tschammer, V.; Foeschl. K.: *mBusiness 2003 - The Second International Conference on Mobile Business.* Wien, 2003.

[14] *Pousttchi, K.; Turowski, K.; Weizmann, M.:* Added Value-based Approach to Analyze Electronic Commerce and Mobile Commerce Business Models. In: Andrade, R.A.E.; Gómez, J.M.; Rautenstrauch, C.; Rios, R.G.: International Conference of Management and Technology in the New Enterprise. La Habana 2003, pp. 414-423.