SECURE SMS BANKING - NEUE CHANCE FÜR MOBILE BANKING

Martin Schurig

tecways AG
Frankenthaler Str. 2
81539 München
martin.schurig@tecways.com

Abstract: Mobile Banking wurde vor dem Hintergrund des Erfolges von Electronic Banking von vielen Banken voreilig als die zukünftige Triebkraft des Mobile Commerce gelobt. Keines der von den Banken angebotenen Verfahren konnte aber bis heute den hohen Erwartungen gerecht werden. Der Grund hierfür liegt in der Nichterfüllung von Kundenanforderungen, die in diesem Beitrag vorgestellt und anhand derer die Hauptprobleme der derzeit verfügbaren Anwendungen aufgezeigt werden. Von diesem Punkt ausgehend wird das neue System Secure SMS-Banking vorgestellt, das aufgrund seines Aufbaus, der sich konsequent bereits etablierter Standards bedient, die bestehenden Probleme löst.

1 Einführung

Der große Erfolg des Electronic Banking, welches mit Recht als eine der Triebkräfte des Electronic Commerce bezeichnet werden kann, weckte bei den Banken die Hoffnung, diesen Erfolg mit Mobile Banking wiederholen zu können. Jetzt, ca. vier Jahre nach der Vorstellung der ersten Anwendungen, hat sich aber Ernüchterung in der Finanzwelt breit gemacht. Zu gering sind die Nutzungszahlen der vorhandenen Angebote. [Ru01] Worin die negative Resonanz auf die verfügbaren Angebote begründet liegt, soll im Weiteren noch erläutert werden. Die allgemeine Krise, die viele Banken, speziell diejenigen die ihren Fokus vermehrt auf neue Vertriebswege gelegt haben, in den letzten Jahren erfasst hat, hat zudem dazu geführt, dass Investitionen in neue Technologien reduziert und die verfügbaren Angebote nicht weiterentwickelt wurden.

Dass die weit hinter den Erwartungen zurückbleibenden Nutzerzahlen aber nicht in der schlichten Nichtexistenz eines Marktes für Mobile Banking, sondern vielmehr in den einfach am Kunden vorbeientwickelten Anwendungen liegen, lässt sich anhand konkreter Zahlen belegen. So brachte eine Umfrage unter 16.500 deutschen Internetnutzern das Ergebnis, dass über die Hälfte der Befragten daran Interesse hätte, Finanztransaktionen mittels eines Mobiltelefons auszuführen.[Sp01] Die Schlussfolgerung liegt nahe, dass mit einer neuen, mehr auf die konkreten Bedürfnisse, die ein Kunde in einer mobilen Situation hat, hin abgestimmten Anwendung auch die Akzeptanz von Mobile Banking sich positiv entwickeln und zum Erfolg des gesamten Mobile Commerce beitragen könnte.

Einen neuen Vorstoß im Bereich Mobile Banking stellt das Projekt Secure SMS-Banking (Short Message Service) dar, das durch den Softwareentwickler tecways AG in Zusammenarbeit mit dem SIZ, dem Informatikzentrum der Sparkassenorganisation, initiiert und in Zusammenarbeit mit der Stadtsparkasse München und dem Mobilfunkanbieter O2 im Rahmen eines Pilotprojektes erstmals einem begrenzten Teilnehmerkreis zur Verfügung gestellt wurde. Aufgrund der positiven Resonanz der Teilnehmer, die durch regelmäßige schriftliche Befragungen ermittelt wurde, wurde das im Folgenden vorgestellte System nun weiterentwickelt und wird im Laufe des ersten Halbjahres 2004 allen Kunden der Stadtsparkasse München zur Verfügung stehen. Den Kunden wird dann die Möglichkeit geboten, Banktransaktionen unter Verwendung des Kommunikationskanals SMS abzuwickeln. Anders als bei einigen bereits am Markt befindlichen Lösungen, die ebenfalls SMS zur Kommunikation verwenden, wird die Kommunikation zwischen Kunden und Bank hier verschlüsselt und es sind außer einem herkömmlichen Mobiltelefon keine weiteren Endgeräte auf Kundenseite erforderlich.

Der vorliegende Beitrag stellt das System Secure SMS-Banking vor und zeigt anhand einer Gegenüberstellung der Eigenschaften von Secure SMS-Banking und konkreten Kundenbedürfnissen, wie durch diese neue Technologie im Bereich des Mobile Banking bestehende Barrieren der Nutzung ausgeräumt werden können. Dazu werden im Folgenden zunächst einmal die Kundenbedürfnisse aufgezeigt und es wird auf die Erfüllung dieser durch die derzeit am Markt befindlichen Angebote eingegangen. Anhand dieser Gegenüberstellung können die Problemfelder der aktuellen Anwendungen identifiziert werden. Anschließend wird die neue Lösung des Secure SMS-Banking vorgestellt und diese im Zusammenhang mit den bereits ermittelten Problemfeldern von Mobile Banking betrachtet. Die übrigen Kundenanforderungen und ihre Erfüllung durch Secure SMS-Banking, sowie ein bei Secure SMS-Banking auftretendes Problem werden im zweiten Teil des Kapitels 5 beleuchtet.

2 Kundenanforderungen an Mobile Banking

Im Folgenden werden Kundenanforderungen an Mobile Banking Anwendungen vorgestellt. Die Anforderungen werden, entsprechend ihrer Priorität sortiert, beginnend mit der höchsten aufgeführt:

1. *Nutzung muss unabhängig davon möglich sein, bei welchem Mobilfunkanbieter der Nutzer Kunde ist.* Die potentiellen Nutzer sind Kunden unterschiedlicher Mobilfunkanbieter, dies sollte den Kundenkreis eines oder mehrerer Anbieter nicht von der Nutzung ausschließen.
2. *Autorisierung des Zugriffs vor der Nutzung*. Der Zugriff darf erst nach der Überprüfung der Berechtigung des Nutzers möglich sein.
3. *Verschlüsselte Übertragung der Daten.* Daten müssen auf dem gesamten Weg zwischen Endgerät des Nutzers und Banksystem verschlüsselt übertragen werden.

4. *Nutzung muss mit allen verfügbaren Endgeräten möglich sein.* Alle verfügbaren Mobiltelefone, unabhängig von der technischen Ausstattung, sowie alle verfügbaren PDA sollten eine Nutzung erlauben.
5. *Möglichst einfache Autorisierung des Zugriffs.* Die Autorisierung sollte mit möglichst wenigen Eingaben durch den Benutzer erfolgen können.
6. *Anwendung sollte sich den Gegebenheiten des jeweiligen Endgerätes automatisch anpassen*. Menüführung, Dateneingabe und Darstellung sollten die technischen Gegebenheiten des jeweiligen Geräts optimal ausnutzen
7. *Vereinfachung der Dateneingabe*. Anwendung sollte dem Nutzer eine möglichst einfache, ihm vertraute Methode der Dateneingabe ermöglichen.
8. *Wiederaufnahme der Nutzung an gleicher Stelle nach Unterbrechung.* Bei mobiler Nutzung besteht jederzeit die Gefahr einer Unterbrechung der Nutzung durch mangelnde Netzabdeckung oder Störung der Nutzung durch Umwelteinflüsse. Die Nutzung sollte später an gleicher Stelle wieder aufgenommen werden können.
9. *Möglichkeit offline zu arbeiten.* Ist bei Gebührenabrechung nach Online-Zeit relevant für die Kosten, außerdem wichtig, wenn der Nutzer sich in Bereichen ohne Netzversorgung befindet und trotzdem mit der Anwendung arbeiten möchte.
10. *Menge der übertragenen Daten sollte möglichst gering sein.* Ist bei Gebührenabrechung nach übertragenem Datenvolumen relevant für die Kosten, bei langsamen Übertragungsverfahren relevant für die Wartezeit des Kunden.
11. *Einfache Skalierbarkeit des Angebots.* Einfaches Zuschalten oder Nachladen von weiteren Funktionen sollte möglich sein.
12. *Umfangreiches Angebot an Transaktionsmöglichkeiten, analog Angebot aus dem Electronic Banking.* Der Nutzer sollte die Angebote aus dem ihm von seiner Bank bekannten Electronic Banking auf dem mobilen Endgerät wieder finden.
13. *Möglichkeit der Personalisierung des Angebots*. Das Angebot sollte vom Nutzer an seine Bedürfnisse bzgl. Darstellung und Funktionsumfang anpassbar sein.
14. *Möglichkeit sich über Ereignisse benachrichtigen zu lassen.* Informationen werden proaktiv von der Bank an den Nutzer geschickt, wenn bestimmte vom Nutzer vorher festgelegte Situationen eintreten. Solche Dienste werden auch Push-Dienste genannt.

Die Herleitung dieser Anforderungen wurde anhand von Charakteristika der mobilen Nutzung bzw. anhand von konkreten Nutzungsszenarien vorgenommen. Die Priorisierung wurde anhand von Expertenbefragungen durchgeführt, bei denen die Befragten gebeten wurden, die Wichtigkeit der Anforderungen in bestimmten Nutzungsszenarien anzugeben. Aus diesen Werten und aus einer ebenfalls in der Befragung gewonnenen Gewichtung der unterschiedlichen Szenarien konnte die Priorisierung abgeleitet werden. (Zur genaueren Herleitung und Priorisierung siehe [PS03]).

3 Aktuelle Anwendungen und ihre Problemfelder

Anhand der vorgestellten Kundenbedürfnisse können nun die Problemfelder aktuell am Markt verfügbarer Anwendungen ermittelt werden. Aktuell verfügbare Anwendungen sind:

- *WAP-Banking*. Die wohl am weitesten verbreitete Methode Mobile Banking anzubieten. Ähnlich wie beim Electronic Banking liegen die Angebote auf einem Webserver bereit. Die Angebote sind in der Auszeichnungssprache WML (Wireless Markup Language) erstellt. Die Angebote werden mittels WAP (Wireless Application Protocol) an das mobile Endgerät übertragen und dort mittels eines WAP-Browsers angezeigt. Die Anfragen der mobilen Endgeräte laufen dabei über einen so genannten WAP-Gateway, der die Anfragen in eine für den Webserver verständliche Form umsetzt. Die Datenübertragung findet dabei mittels einer der im mobilen Bereich zur Verfügung stehenden Technologien, CSD (Circuit Switched Data), HSCSD (High Speed Circuit Switched Data) oder GPRS (General Packet Radio Service) statt. Die Verschlüsselung der Daten geschieht auf dem Weg zwischen Endgerät und WAP-Gateway mit Hilfe von WTLS (Wireless Transport Layer Security) und zwischen Gateway und Webserver mittels SSL (Secure Socket Layer).
- *SMS-Banking*. Diese Variante nutzt den weit verbreiteten SMS-Dienst zur Datenübertragung, mit dem Kurzmitteilungen mit maximal 160 Zeichen an Mobiltelefone gesandt werden können. Der Nutzer schickt hierbei seine Anfrage als SMS an die Bank, diese antwortet ebenfalls mit einer Kurzmitteilung, welche die gewünschte Information, z. B. den Kontostand enthält. Der Nutzer muss für jede Abfrage, die er tätigen möchte, selbst eine SMS verfassen, in die er seine ihm von der Bank zugeteilte PIN, einen speziellen von der Bank festgelegten Code für die Art der Abfrage und seine Kontonummer integriert. Dabei muss der Nutzer sich exakt an die von der Bank vorgegebene Syntax halten, da sonst eine automatisierte Auswertung der SMS nicht möglich ist. Da hierbei keine Verschlüsselung der Daten während der Übertragung stattfindet, ist das Angebot auf reine Informationsdienste beschränkt. Die Verbreitung von SMS-Banking ist relativ gering.
- *Banking mit PDA*. Variante von Mobile Banking, die speziell für die Nutzung mit PDA (Personal Digital Assistant) konzipiert ist. Dabei wird speziell Software zur Nutzung des Angebots auf dem PDA installiert. Die Kommunikation mit der Bank erfolgt hier ebenfalls mittels SMS. Allerdings werden im Gegensatz zum SMS-Banking hier binäre SMS zur Datenübertragung genutzt. Die Datenübertragung kann auf diesem Wege verschlüsselt werden. Auch die Verbreitung dieser Mobile Banking Variante ist sehr gering. Zur Nutzung dieser Mobile Banking Variante ist, außer bei einigen neueren Geräten, die PDA und Telefon in einem Gerät vereinen, immer ein zweites Endgerät in Form eines Mobiltelefons notwendig.

Stellt man diese drei derzeit am Markt verfügbaren Anwendungen den weiter oben aufgezeigten Kundenanforderungen gegenüber, so ergibt sich folgendes Bild.

	WAP	SMS	PDA
Unabhängige Nutzung	+	+	+
Autorisierung des Zugriffs	+	+	+
Verschlüsselte Datenübertragung	+	-	+
Nutzung mit beiden Endgeräten	+	-	-
Einfache Autorisierung	-	-	-
Automatische Anpassung	-	+	O
Einfache Dateneingabe	+	-	+
Wiederaufnahme an gleicher Stelle	-	+	+
Möglichkeit offline zu Arbeiten	-	+	+
Geringe Menge der übertragenen Daten	-	+	+
Einfache Skalierung der Anwendung	+	-	+
Umfangreiche Funktionen	+	-	+
Möglichkeit Anwendung anzupassen	+	+	+
Push-Dienste	-	+	-

+ erfüllt - nicht erfüllt o nicht gewertet

Abb. 1 Anforderungserfüllung vorhandener Anwendungen

Anhand dieser Gegenüberstellung gelingt es nun leicht die Problemfelder der derzeit verfügbaren Anwendungen zu erkennen. Bei der Ermittlung der Problemfelder wurden nur WAP-Banking und Banking mit PDA betrachtet, da SMS-Banking aufgrund der massiven Defizite im Bereich Sicherheit keine verschlüsselte Übertragung der Daten, nur den Abruf von Informationen ermöglicht. Direktes Banking, das auch die Durchführung von Transaktionen umfasst, ist aufgrund des somit gegebenen Angriffspotentials mit dieser Lösung nicht möglich.

- *Umständliche Autorisierung.* Beim Zugriff auf WAP-Banking ist meistens die Eingabe von mehreren PIN notwendig. Jede Transaktion muss ähnlich wie beim Electronic Banking mit einer TAN autorisiert werden. Speziell letzteres ist in einer mobilen Situation unzulänglich, da der Nutzer gezwungen wird eine Liste mit TAN ständig bei sich zu haben. Anwendungen für den PDA bieten zwar die Möglichkeit eine Anzahl von TAN zu speichern, die Handhabung von zwei Geräten zur gleichen Zeit ist aber ebenfalls unzulänglich.
- *Unzureichende Anpassung an das jeweilige Endgerät.* Dieses Problem tritt besonders bei WAP-Anwendungen zu Tage. Obwohl WAP ein allgemeingültiger Standard ist, wurde er auf unterschiedliche Art und Weise von einigen Herstellern implementiert. Dies führt zu inkonsistenten Anzeigen der Inhalte auf verschiedenen Geräten.
- *Keine offline Nutzung möglich.* Bei WAP-Banking ist eine durchgängige Verbindung zur Bank während der gesamten Nutzungsdauer nötig. Es gibt keine Möglichkeit Daten offline zu bearbeiten oder sich anzeigen zu lassen. Das Nichtvorhandensein dieser

Nutzungsmöglichkeit macht es auch unmöglich, die Nutzung nach einer Unterbrechung an der gleichen Stelle wieder aufzunehmen.

- *Unnötige Übertragung von Daten.* Beim WAP-Banking wird bei jedem Aufruf die komplette Applikation an das Endgerät übertragen. Es besteht keine Möglichkeit diese auf dem Endgerät dauerhaft zu speichern.
- *Keine Möglichkeit für Push-Dienste*. Weder WAP-Banking noch Lösungen für den PDA bieten die Möglichkeit für Push-Dienste.
- *Zweites Endgerät als Problemlösung inadäquat.* Zwar werden einige der vorgestellten Probleme durch die Verwendung eines PDA gelöst, aber die umständliche Handhabung von zwei Endgeräten macht diesen Vorteil speziell in mobilen Situationen wieder zunichte.

Nachdem nun die Hauptprobleme der bestehenden Anwendungen aufgezeigt wurden, wird im Folgenden zunächst das neue System des Secure SMS-Banking vorgestellt, bevor es ebenso wie die anderen Systeme an den Bedürfnissen der Nutzer gemessen wird.

4 Secure SMS-Banking

4.1 Aufbau des Systems

Die zugrunde liegende Idee des Secure SMS-Banking ist es, die Abwicklung von Bank-Transaktionen über mobile Endgeräte zu ermöglichen, unter Verwendung von bereits etablierten, weit verbreiteten Standards. Die verwendeten Standards sind auf Seite des Endgeräts SIM Application Toolkit zur Realisierung der Anwendung, zur Datenübertragung SMS und auf Seiten der Bank wird die Anbindung über den HBCI (Home Banking Computer Interface) Zugang der Bank realisiert. Das gesamte System ist in seinem Aufbau sehr stark an das bekannte und bei Banken und Kunden gleichermaßen als sicher eingestufte HBCI-Banking angelehnt. HBCI-Banking bietet gegenüber anderen Homebanking-Verfahren den Vorteil, dass der Kunde seine Transaktionen nicht mehr mit TAN autorisieren muss, deren Verwaltung wenig komfortabel ist. Der Kunde erhält einen Schlüssel der Bank zur Verschlüsselung der Datenübertragung und einen persönlichen Schlüssel zur Signatur des Auftrags auf einer Chipkarte von der Bank ausgehändigt. Ein Problem des HBCI-Banking ist die Notwendigkeit eines Kartenlesers und spezieller Software um das Verfahren zu nutzen. Somit ist der Nutzer an einen Rechner gebunden, wenn er Homebanking betreiben will. Beim Secure SMS-Banking wird ein solches Verfahren in leicht abgewandelter Form von der Chipkarte auf die SIM-Karte des Nutzers übertragen und die Vorteile von HBCI werden somit in mobilen Situationen verfügbar.

Auf Bankseite wird ein Transaktionssystem, das so genannte Providersystem, implementiert, das die Aufträge entgegennimmt und an den HBCI-Server der Bank weiterleitet. Die über HBCI empfangenen Antworten werden von ihm zurück an das Endgerät beim Kunden übermittelt.

Die Kommunikation zwischen dem Endgerät und dem Banksystem erfolgt dabei unter Verwendung des speziell für diesen Einsatz entwickelten Secure Mobile Banking Protocol (SMBP), das es erlaubt Applikationen auf mobilen Endgeräten zu entwickeln die unter Verwendung dieser Schnittstelle die vorgesehen Geschäftsvorfälle abbilden. Als Transportmedium auf der Luftschnittstelle wird der SMS-Dienst in Form von binären SMS verwendet.

Die Applikation auf dem Endgerät wird mit Hilfe von SIM Application Toolkit realisiert und wird bei der Produktion der SIM-Karte direkt in diese eingebracht.

Die folgende Abbildung gibt zunächst einmal einen Überblick über den Aufbau des Systems und die Kommunikation der einzelnen Komponenten untereinander.

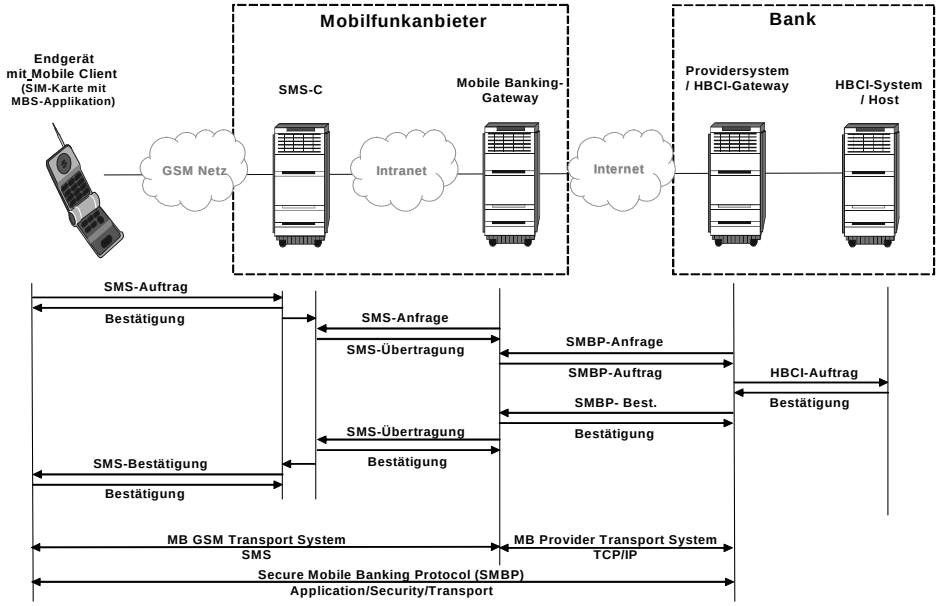

Abb. 2: Aufbau des Systems Secure SMS-Banking

Mobile Client: Die SIM-Karten erhalten eine zusätzliche Applikation gemäß ETSI Standard GSM 11.14, SIM Application Toolkit. Diese SMS-Banking Applikation beinhaltet alle Funktionen, die dem Kunden in einem neuen Menü auf seinem Mobiltelefon angeboten werden. Sie enthält auch alle internen Abläufe und Sicherheitsmechanismen. Durch die Verwendung von SIM Application Toolkit integriert sich die Anwendung als Menüerweiterung in die bereits vorhandene Menüstruktur des Telefons, unabhängig von Alter, Hersteller oder verwendetem Modell. Der Nutzer kann mit der Applikation in der gleichen Art und Weise arbeiten wie mit den restlichen Funktionen seines Telefons und findet sich somit intuitiv in ihr zurecht. Die ausgehenden Nachrichten werden als binäre SMS ver-

sandt, die es erlauben den SMS-Dienst als Medium zur Übertragung von beliebigen Daten zu verwenden.

SMS-Center (SMS-C): Zur Entgegennahme der Kurznachrichten vom Client und Weiterleitung an das Banksystem oder im Antwortfall in umgekehrter Richtung, wird ein Standardzugang des SMS Centers (SMS-C) des GSM-Netzwerks genutzt.

Mobile Banking Gateway: Das eigentliche Mobile Banking System ist in zwei Teile aufgegliedert. Zu einem das Mobile Banking Gateway, zum anderen das Providersystem. Das Mobile Banking Gateway ist für die Kommunikation mit dem SMS-C zuständig und fragt eingehende Nachrichten von diesem ab oder leitet die Nachrichten an dieses weiter. Das Mobile Banking Gateway leitet die eingehende Nachricht dann an das Providersystem. Nutzen mehrere Banken das System, erkennt das Mobile Banking Gateway, für welche Bank die Nachricht bestimmt ist und leitet sie an das entsprechende Providersystem weiter. Wenn mehrere Mobilfunkanbieter ihren Kunden die Teilnahme am Secure SMS-Banking anbieten möchten, so wird bei jedem ein solches Mobile Banking Gateway installiert.

Providersystem: Das Providersystem ist der zweite Teil des Mobile Banking Systems und das eigentlich Kernelement. Es ist auf Seiten der Bank positioniert und empfängt die Nachrichten vom Benutzer und kann sie entschlüsseln. Nach erfolgreicher Prüfung werden die Aufträge dann in HBCI-Aufträge umgewandelt und an das angeschlossene Banksystem weitergegeben. Ebenso empfängt das Providersystem die Antworten vom HBCI-Server der Bank und bereitet sie für den Versand an den Client vor. Die Kommunikation zwischen Providersystem und dem HBCI-Server der Bank erfolgt über einen HBCI-Client, den Banking Kernel, über dessen Programmierschnittstelle die für einen HBCI-Dialog notwendigen Daten übergeben bzw. empfangen werden. Der Banking Kernel kommuniziert per TCP/IP über das interne Netzwerk der Bank mit dem HBCI-Gateway und ist auch für die Sicherheitsfunktionen an dieser Schnittstelle verantwortlich.

HBCI-Host: Zur Abwicklung der Banktransaktionen wird der vorhandene HBCI-Zugang der Bank verwendet.

4.2 Sicherheit

Für die Absicherung der Kommunikation wird ein symmetrisches Verschlüsselungsverfahren verwendet. Es kommt dabei der 3-DES Algorithmus zum Einsatz. Die dafür notwendigen, kundenindividuellen Schlüssel werden auf Clientseite direkt bei der Produktion der SIM-Karten in diese eingebracht. Der zugehörige Masterkey, von dem diese Schlüssel abgeleitet wurden, wird außerdem in das Providersystem eingebracht. Kommt eine verschlüsselte Nachricht dort an, kann der zur Entschlüsselung benötigte Schlüssel im Providersystem vom Masterkey unter Verwendung einer kundenindividuellen Identifikationsnummer abgeleitet werden. Das verwendete Verfahren ist stark an das weit verbreitete HBCI-Verfahren angelehnt und bietet Ende-zu-Ende Sicherheit zwischen Client und

Bank. Die nahe Verwandtschaft zeigt sich auch in der Tatsache, dass im Laufe des durchgeführten Pilotversuches bei einigen Clients Dual-Slot Mobiltelefone eingesetzt wurden, bei denen statt eines Kundenschlüssels auf der SIM-Karte die HBCI-Karte des Kunden über den zweiten im Mobiltelefon vorhandenen Kartenschacht ausgelesen wurde. Zur Verschlüsselung der Übertragung und zur Signatur des Auftrages wurden in diesem Fall keine kundenindividuellen Schlüssel auf der Karte, sondern die HBCI-Schlüssel auf der Chipkarte verwendet. Durch die Adaption des bekannten, weit verbreiteten HBCI-Verfahrens konnte von Anfang an ein hohes Maß an Vertrauen in die Sicherheit der Anwendung von Seiten der Banken gewonnen werden.

4.3 Dynamische Erweiterungsmöglichkeiten

Einen besonderen Fokus verdient die Möglichkeit, die Anwendung durch das Nachladen von so genannten dynamischen Services beliebig zu erweitern. Dynamische Services sind Funktionserweiterungen in Form von Skripten, die per Kurznachricht an die SIM-Karte gesandt, dort in einem speziell dafür vorgesehenen Bereich abgelegt und mittels eines in der SIM vorhandenen Interpreters ausgeführt werden. Dieses Konzept ermöglicht es dem Kunden sich die Anwendung individuell zu gestalten, in dem er sich die von ihm benötigten Services auf seine Karte lädt. Für die Banken besteht die Möglichkeit, das Angebot an zusätzlichen Dienstleistungen zu einem späteren Zeitpunkt zu erweitern und dem Kunden auf diesem Wege verschiedenste, auch bankfremde Angebote zur Verfügung zu stellen. Denkbar wären hier Funktionalitäten, die über die grundlegenden Transaktionsmöglichkeiten hinausgehen, wie die Einrichtung und Verwaltung von Daueraufträgen und Terminüberweisungen oder Angebote aus dem Bereich des Wertpapierhandels. Die Anwendung kann durch diese Erweiterungsmöglichkeiten den individuellen Lebensumständen des Nutzers angepasst werden. Ein Nutzer, der mit Wertpapieren handelt, kann sich Funktionen zum Verwalten seines Depots installieren, für einen Nutzer, der viel im Ausland unterwegs ist, wäre hingegen eine Funktionalität sinnvoll, mit der er im Notfall seine Karten sperren kann oder über die er aktuelle Wechselkurse abfragen kann. Um eine Erweiterung auf sein Mobiltelefon zu laden, lädt der Nutzer sich zunächst eine Liste der verfügbaren Erweiterungen von seiner Bank und wählt dann die gewünschte Erweiterung aus. Diese wird dann per SMS von der Bank an den Nutzer gesandt. Eine Manipulation der Anwendung auf diesem Wege wird dadurch ausgeschlossen, dass die zur Versendung der Erweiterung verwendete Kurznachricht ebenso verschlüsselt ist wie die Nachrichten, mit denen die Transaktionsdaten übermittelt werden.

4.4 Geschäftsmodell und Markteinführung

Banken, die das System ihren Kunden anbieten möchten, erwerben eine Lizenz für das Providersystem, Mobilfunkanbieter für das Mobile Banking Gateway. Den Banken steht es frei die über Secure SMS-Banking ausgeführten Transaktionen separat zu bepreisen, oder aber von dem Teilnehmer an diesem Verfahren eine Grundgebühr zu verlangen. Aufgrund der Kosteneinsparung, die einer Bank durch die Verlagerung von Transaktionen auf diesen neuen Kanal entsteht, ist aber eher von einem kostenfreien Angebot auszuge-

hen. Für den Mobilfunkanbieter ergeben sich zusätzliche Einnahmen durch die Gebühren für die durch SMS-Banking erzeugten SMS.

Die Markteinführung des Systems ist für das erste Halbjahr 2004 geplant. Die gemeinsamen Kunden von Stadtsparkasse München und O_2 können dann das System zunächst nutzen. Eine Ausweitung auf andere Banken und Mobilfunkanbieter ist geplant. Ein Kunde, der Secure SMS-Banking nutzen möchte, muss bei der für sein Konto zuständigen Sparkasse eine Teilnehmervereinbarung ausfüllen. Er erhält dann wenig später eine neue SIM-Karte zugesandt, die er statt seiner bisherigen in sein Mobiltelefon einsetzt und die ihm die Teilnahme am System ermöglicht.

5 Kundenanforderungen und Secure SMS-Banking

5.1 Hauptproblemfelder und Secure SMS-Banking

Im Folgenden werden zunächst die in Kapitel 3 ermittelten Hauptproblemfelder aktuell verfügbarer Anwendungen und Secure SMS-Banking gegenübergestellt, um zu ermitteln, ob diese durch die neue Technologie gelöst werden können.

Umständliche Autorisierung. Eine umständliche Autorisierung, wie sie die meisten anderen Anwendungen verlangen, entfällt bei Secure SMS-Banking. Durch die Implementierung eines kundenindividuellen Schlüssels auf der SIM-Karte, der die Transaktionen absichert und autorisiert, genügt es den Zugang zur Banking-Applikation durch die Eingabe einer vom Kunden selbst festzulegenden und somit einfach zu behaltenden PIN zu sichern.

Unzureichende Anpassung an das jeweilige Endgerät. Durch die Verwendung des SIM Application Toolkit Standards fügt sich die Banking Anwendung perfekt in die bestehende Menüstruktur des Mobiltelefons ein. Die Möglichkeiten des Mobiltelefons bezüglich Darstellung und Eingabemethoden werden somit immer bestens ausgenützt.

Keine Offline Nutzung möglich. Secure SMS-Banking bietet die Möglichkeit der Dateneingabe ohne eine direkte Verbindung zur Bank zu unterhalten. So können Eingaben ohne kostenintensive Verbindung getätigt werden. Es können die Eingaben auch vorbereitet werden, wenn zu diesem Zeitpunkt keine Netzversorgung besteht.

Keine unnötige Übertragung von Daten. Die Applikation befindet sich beim Secure SMS-Banking direkt auf der SIM-Karte. Sie muss nicht jedes Mal neu auf das Endgerät geladen werden, wenn der Nutzer damit arbeiten möchte. Es werden zwischen Bank und Endgerät nur die für die jeweilige Transaktion und die Verschlüsselung notwendigen Daten übertragen. Die einzige Ausnahme stellt das Nachladen von Funktionen dar. Dabei werden neue Programmteile an die SIM-Karte geschickt.

Keine Möglichkeit für Push-Dienste. Bei Secure SMS-Banking ist es auch möglich so genannte Push-Dienste ohne großen Aufwand zu realisieren. Es muss dazu nur eine SMS mit Bankdaten, die durch das Providersystem sonst als Antwort auf eine Anfrage vom Endgerät generiert wird, proaktiv vom Providersystem an das Endgerät gesendet werden.

Zweites Endgerät als Problemlösung inadäquat. Da Secure SMS-Banking direkt auf dem Mobiltelefon läuft, und alle aufgeführten Problemfelder durch die Verwendung von Secure SMS-Banking eliminiert werden, ist kein zweites Endgerät mehr als Problemlösung erforderlich.

5.2 Problem des Secure SMS-Banking

Zwar werden durch die Verwendung von SMS-Banking die Probleme der bestehenden Anwendungen fast vollständig gelöst, es müssen aber auch Schwierigkeiten bei der Verwendung von Secure SMS-Banking diskutiert werden.

Betrachtet man nochmals komplett die Kundenanforderungen an eine Mobile Banking Anwendung und stellt ihnen Secure SMS-Banking gegenüber, so ergibt sich folgendes Bild:

	Secure SMS	**WAP**	**SMS**	**PDA**
Unabhängige Nutzung	-	+	+	+
Autorisierung des Zugriffs	+	+	+	+
Verschlüsselte Datenübertragung	+	+	-	+
Nutzung mit beiden Endgeräten	-	+	-	-
Einfache Autorisierung	+	-	-	-
Automatische Anpassung	+	-	+	O
Einfache Dateneingabe	+	+	-	+
Wiederaufnahme an gleicher Stelle	+	-	+	+
Möglichkeit offline zu Arbeiten	+	-	+	+
Geringe Menge der übertragenen Daten	+	-	+	+
Einfache Skalierung der Anwendung	+	+	-	+
Umfangreiche Funktionen	+	+	-	+
Möglichkeit Anwendung anzupassen	+	+	+	+
Push-Dienste	+	-	+	-

Abb. 3 Kundenanforderungen und Secure SMS-Banking im Vergleich zu anderen Anwendungen

Bei der Betrachtung fällt sofort auf, dass die wichtigste der gestellten Anforderungen, die Nutzung unabhängig vom Netzbetreiber, nicht erfüllt ist. Betrachtet man den Aufbau des Systems, wird auch der Grund für diese Nichterfüllung sofort klar. Die Banking Anwendung auf Kundenseite ist direkt auf der SIM-Karte des Kunden integriert. Eine Integration einer Anwendung auf dieser ist nur in Zusammenarbeit mit dem Netzbetreiber möglich,

der die SIM-Karte ausgibt. Im Moment ist die Nutzung von Secure SMS-Banking nur für Kunden des Mobilfunkanbieters O2 möglich. Möchte man die Nutzung von Secure SMS-Banking unabhängig vom Anbieter ermöglichen, so wäre es notwendig alle vier deutschen Anbieter von der Integration der Anwendung auf ihren SIM-Karten zu überzeugen.

6 Fazit

In den vorangegangenen Kapiteln wurden Anforderungen an Mobile Banking Anwendungen vorgestellt. Es wurden außerdem die bereits am Markt befindlichen Anwendungen aufgezeigt und ihre Problemfelder anhand der Kundenanforderungen ermittelt. Mit dem vorgestellten System des Secure SMS-Banking ist eine Lösung dieser Probleme gefunden worden. Durch die Verwendung von bereits weit verbreiteten Standards sowohl auf Endgeräten wie auch auf Bankseite ist es gelungen eine Anwendung zu schaffen, die theoretisch von fast allen Banken mit sehr geringen Kosten angeboten werden kann und die für fast alle Nutzer verwendbar ist.

Ein großes Problem bleibt bei dieser Anwendung im Moment zumindest noch bestehen. Die Nutzung ist auf die Kunden eines Mobilfunkanbieters beschränkt. Die Ausräumung dieser Barriere ist auch mit technischen Mitteln nicht möglich. Erst eine große Akzeptanz des ersten am Markt verfügbaren Angebots wird die Aufmerksamkeit der Mobilfunkanbieter auf Secure SMS-Banking lenken und die notwendigen Investitionen in die Technologie ermöglichen.

Durch das Ausräumen der Problemfelder der bestehenden Anwendungen könnte aber mit Secure SMS-Banking eine Anwendung zur Verfügung stehen, die Mobile Banking eine neue Chance geben könnte, die wichtige Rolle bei der Entwicklung des Mobile Commerce zu erfüllen, die ihm viele schon vor langer Zeit zugeschrieben haben.

Literaturverzeichnis

[PS03] *Pousttchi, K.; Schurig, M.:* Assesment of Today´s Mobile Banking Applications from the view of Customer Requirements. In: Proceedings of the Hawaii International Conference on Systems Sciences, January 5 – 8, 2004, Big Island, Hawaii (Preprint)

[Ru01] *Rubrech, H. J.:* In: Mobile Business – eine Achterbahnfahrt mit Ziel. Geldinstitute, 9 (2001), S. 30 – 32.

[Sp01] *Speedfacts Online Research GmbH:* mBanking the future of personal financial transactions? Frankfurt 2001.