Zahlungsverfahren mit Ubiquitous Computing

Sandra Gross
Institut für Technologiemanagement, Universität St. Gallen

Matthias Lampe
Institut für Pervasive Computing, ETH Zürich

René Müller
UBS AG, Zürich

Kurzfassung. Ubiquitous Computing-Technologien ermöglichen die Entwicklung neuer Zahlungsverfahren. Dieser Beitrag beleuchtet den Unterschied zwischen mobilem Bezahlen (M-Payment) und ubiquitärem Bezahlen (U-Payment). Dazu analysiert er aus der Sicht von Banken und Finanzdienstleistern Anforderungen, Technologien und Anwendungsbeispiele. Die Autoren erläutern die Ergebnisse anhand der Entwicklung einer U-Payment-Testplattform, die verschiedene Zahlungsverfahren mit Ubiquitous Computing umsetzt.

1 Einleitung

Ubiquitous Computing (UbiComp)-Technologien ermöglichen die Weiterentwicklung mobiler Zahlungsverfahren (M-Payment). Ein Beispiel für eine ubiquitäre Technologie ist die Radio Frequency Identification (RFID). Mobiltelefone können mit einem RFID-Transponder versehen werden, der kundenindividuelle Bezahlinformationen speichert. Kassensysteme mit integrierten RFID-Lesegeräten lesen diese drahtlos und automatisch aus und ermöglichen somit neue Anwendungen.

Banken haben in der Vergangenheit trotz guter Marktprognosen schon schlechte Erfahrungen mit der Wirtschaftlichkeit mobiler Zahlungsverfahren gemacht. Deshalb ist es Ziel dieses Beitrags, einerseits ubiquitäre Zahlungsverfahren vorzustellen und andererseits diese aus Sicht von Finanzdienstleistern zu bewerten. Dazu werden im Folgenden Anforderungen und Technologien von U-Payment vorgestellt und mit Beispielen aus der Praxis verdeutlicht.

Der Beitrag ist wie folgt aufgebaut: Da es für Zahlungsverfahren mit UbiComp noch keine einheitliche Definition gibt, grenzt der folgende Abschnitt den Begriff U-Payment gegen M-Payment ab. Danach werden die Anforderungen an eine Bezahlarchitektur aus den Sichten unterschiedlicher Marktteilnehmer untersucht. Die nachstehenden zwei Abschnitte evaluieren zum einen die im M-Lab-Projekt entwickelte Testarchitektur BluePay, die ausgewählte Ansprüche umsetzt, und

zum anderen bestehende Herausforderungen in der Praxis bei einer Einführung von ubiquitären Zahlungsverfahren.

2 Vom M-Payment zum U-Payment

Dieser Abschnitt zeigt eine mögliche Entwicklung vom M-Payment zum U-Payment auf. Dazu werden jeweils Definitionen und Anwendungsfelder der Verfahren zusammengefasst.

Das *M-Payment* ist ein mobiler Zahlungsvorgang, bei dem zumindest einer der Teilnehmer ein mobiles Endgerät benutzt. Dies ist häufig ein Mobiltelefon [Kru01, IWW02, KPT02]. Andere Geräte für das mobile Bezahlen sind beispielsweise Personal Digital Assistants (PDA) oder Gegenstände, in die Transponder integriert sind und die Daten per Funk an ein Lesegerät übertragen.

Mobile Zahlungsverfahren können in folgenden Bereichen eingesetzt werden [ITW02]:

- Automatische Kassensystemzahlungen (point-of-sale, POS) wie z.B. Verkaufsautomaten, Parkscheinautomaten oder Ticketautomaten,
- betreute POS-Zahlungen, z.B. in Geschäften oder in Taxis,
- direkte mobile Bezahltransaktionen im Internet über ein mobiles Endgerät (z.B. per wireless application protocol, WAP),
- mobil unterstützte Bezahltransaktionen im Internet wie Telefonanrufe als Alternative zur Kreditkarte,
- Geldtransfers zwischen Personen (peer to peer transactions).

Die Autoren verstehen unter *U-Payments* Zahlungen, welche den Kriterien des UbiComp entsprechen. UbiComp bedeutet, dass Computer allgegenwärtig, für den Benutzer unsichtbar und in der Umgebung integriert sind. Dementsprechend wird U-Payment als das allgegenwärtige, unsichtbare und in die Umgebung integrierte Bezahlen definiert. Die mobilen Zahlungssysteme unterscheiden sich hiervon durch menschliche Interaktion. Systeme mit wenig oder ganz ohne Interaktion des Menschen kommen der Definition des U-Payments in diesem Beitrag am nächsten.

Die Prozesse, die den Bezahlvorgang auslösen, dürfen nicht durch diesen unterbrochen werden, es sei denn, der Bezahlvorgang hängt mit einer Prozessänderung zusammen. Dies könnte beispielsweise der Fall sein, wenn bei der Wartung ein Maschinenteil ausgewechselt wird, und das neue Teil automatisch den Bezahlvorgang veranlasst. Ein anderes Beispiel stellen Zahlungen zwischen Unternehmen dar, bei denen eine automatische Zahlung durch eine Echtzeitmeldung an das ERP-System des Großhändlers angestoßen werden könnte, sobald eindeutig identifizierbare Paletten den Wareneingang des Kunden passieren. Anwendungsbeispiele im Endkundenbereich sind die automatische Autobahngebühr oder in Zukunft das automatische Bezahlen im Supermarkt. Diese Bezahlungen finden immer in vordefiniertem Rahmen statt oder zusätzlich durch Abfrage einer aktiven Bestätigung durch den Kunden.

Die Beratungsfirma Accenture erstellte beispielsweise ein U-Payment-Szenario, bei dem Objekte den Zahlungsvorgang einleiten. Dieses basiert auf der Annahme, dass in Zukunft neben dem Verkauf von Produkten der Verkauf von Dienstleistungen an Bedeutung gewinnen wird, die mit dem Produkt zusammenhängen [DSt01]. Dazu werden Alltagsgegenstände oder industrielle Güter mit RFID-Transpondern und Sensoren versehen, die miteinander kommunizieren können. Verknüpft man diese RFID-Infrastruktur mit einer Micro-Payment-Infrastruktur, dann können die Objekte zusammen agieren und Bezahlvorgänge auslösen. Die Objekte sind kontextsensitiv und führen entsprechend festgelegter Regeln Kaufaktionen durch [Acc02]. Der Benutzer kann sich dann auf den Gebrauch der Gegenstände konzentrieren anstatt auf den Bezahlvorgang [DSt01].

Ein weiteres Beispiel ist Speedpass. Das System wurde von Exxon Mobile eingeführt und existiert in den USA seit 1997. Heute rechnet das Unternehmen mit mehr als 6 Millionen aktiver Kunden, die mit RFID-Transpondern ausgestattete Armbanduhren tragen oder Autoschlüsselanhänger mit dieser Technologie besitzen. In den USA akzeptieren über 7 500 Geschäfte und Tankstellen den Speedpass von Exxon Mobil als Zahlungsmittel. In Chicago und in Nordwest-Indiana kann in über 440 Schnellrestaurants damit bezahlt werden. 92 % der Speedpass-Benutzer geben an, mit dem System sehr zufrieden zu sein. Viele Tankstellen verkauften seit der Einführung von Speedpass 15 % mehr Benzin und es wurde in 18 % aller Fälle mit Hilfe dieser Technologie bezahlt. In den Geschäften hat sich der Umsatz um 4 % erhöht [Exx02].

Abb. 1. Bezahlen mit der Speedpass-RFID-Timex-Uhr[1]

Speedpass ist sehr einfach zu bedienen: Zum Bezahlen wird der Transponder einfach vor einen Leser gehalten (vgl. Abbildung 1). Er speichert nur eine eindeutige Identifikationsnummer und keine Kreditkartennummer. Die Autorisierung der Zahlung wird von Speedpass initiiert, wobei Speedpass die Verbindung zum Kreditkartenherausgeber herstellt.

[1] www.speedpass.com

3 Anforderungen an eine U-Payment-Architektur

Eine hohe Marktdurchdringung von U-Payment kann nur erreicht werden, wenn man von den kritischen Erfolgsfaktoren für mobile Zahlungssysteme lernt. Diese müssen in Abhängigkeit vom Marktteilnehmer betrachtet werden. Die Erfolgsfaktoren variieren aus Sicht der Kunden, der Händler oder der Banken.

Die Anforderungen der *Kunden* betreffen mehrere Aspekte: Zunächst muss das Zahlungsverfahren für den Benutzer zweckmäßig und einfach zu bedienen sein. Es zeichnet sich idealerweise durch eine niedrige Komplexität aus, der Möglichkeit, dass der Teilnehmer das Verfahren testen kann, dass es einen hohen Verbreitungsgrad bei Händlern und Geschäften aufweist und dass es einen hohen Grad an Komfort besitzt. Der Teilnehmer hat zudem die Freiheit, die Bank, den Betreiber und das Endgerät zu wählen. Dem Kunden wie auch dem Händler muss eine möglichst hohe Sicherheit in Bezug auf Vertraulichkeit, Integrität, Authentizität und Nicht-Abstreitbarkeit bei der Nutzung mobiler Finanzdienstleitung geboten werden. Von Vorteil ist auch die Möglichkeit, das Verfahren anonym zu benutzen [HGF03, MoF00].

Der Erfolg des Systems hängt ebenfalls von der Kooperationsbereitschaft der *Händler* ab. Diese verlangen beispielsweise eine Einhaltung von Standards, einen geringen Installationsaufwand und Kosten sowie eine effiziente Zahlungsabwicklung.

Banken und Finanzdienstleister andererseits erwarten ein geringes Transaktionsrisiko, Unabhängigkeit vom Betreiber und eine einfache Integration in vorhandene Systeme. Ist es beispielsweise nicht möglich, eine Lösung einfach und mit geringem Kostenaufwand in bestehende Systemlandschaften zu integrieren, kann nur schwer eine große und damit erfolgsversprechende Marktdurchdringung erreicht werden (vgl. Tabelle 1).

Tabelle 1. Anforderungen an eine U-Payment-Architektur aus Bankensicht [MoF00]

Art der Anforderung	Beschreibung
Geschäftliche Prioritäten	• Die Banken authentifizieren einen Benutzer, damit er deren Bankdienstleistungen bzw. Zahlungssysteme nutzen kann. • Die Finanzdienstleistung bringt einen Mehrwert für alle beteiligten Parteien. • Geschäftsprozesse der unterschiedlichen Parteien müssen unabhängig voneinander sein. • Das Zahlungsverfahren kann um weitere Finanzdienstleistungen erweitert werden. • Bei mehreren an der Lösung beteiligten Geschäftspartnern kann jeder Partner sein Markenzeichen verwenden.
Technische Aspekte	• Die Lösung muss auf offenen Standards basieren und nicht-proprietäre Technologien implementieren. • Bereits bestehende Standards sollen genutzt und wo immer möglich eingesetzt werden. • Die technische Lösung darf keine Abhängigkeiten zwischen der Bank, dem Betreiber und Endgeräten schaffen.

	• Es muss eine End-to-end-Sicherheit garantiert werden (Vertraulichkeit, Integrität, Authentizität und Nicht-Abstreitbarkeit).
Implementierungsaspekte	• Die Implementierungskosten bei der Bank, dem Händler und dem Benutzer sollen möglichst tief gehalten werden. • Die Produkteinführungszeit ist einer der kritischsten Faktoren zur Sicherung des Erfolgs neuer Finanzdienstleistungen bzw. Zahlungssysteme.
Sicherheitsaspekte	• Grundanforderungen sind die Plattform-Sicherheit auf dem Endgerät sowie die sichere Übertragung von Daten. • In Zukunft sollen standardmäßig digitale Zertifikate zur Signierung von Transaktionen verwendet werden.

4 Die U-Payment-Architektur BluePay

Die U-Payment-Architektur BluePay ist eine Testplattform für Zahlungsverfahren mit Ubiquitous Computing. Sie verwendet die Technologien Bluetooth und RFID im lokalen Zahlungsverkehr. Es wurden insbesondere drei Anforderungen umgesetzt: erstens die Verwendung von offenen und bereits eingesetzten Standards wie Bluetooth und RFID, zweitens keine Abhängigkeiten zwischen Händlern und Finanzdienstleistern, da die Plattform das bestehende Finanznetzwerk zur Zahlungsabwicklung verwendet, und drittens ein geringer Implementierungsaufwand durch Anpassungen auf der Clientseite aber nicht serverseitig.

Die Testplattform baut auf der Preferred Payment Architecture (PPA) auf, die im Rahmen des Mobey Forums erarbeitet wurde [MoF00]. Das Mobey Forum vertritt die Anliegen von Finanzinstituten im Bereich mobiler Dienstleistungen und diskutiert diese mit Standardisierungsgremien, Herstellern von mobilen Endgeräten, Betreibern, Beratern und Lösungsanbietern. Die vom Mobey Forum beschriebene PPA soll keinen komplett neuen Standard definieren, sondern vielmehr eine auf den verschiedensten Standards aufbauende und auf mobile Finanzdienstleistungen angepasste, offene Architektur beschreiben. Durch die Einflussnahme in anderen Interessensvereinigungen strebt das Mobey Forum breit abgestützte Standards an, die von Finanzdienstleistern, Geräteherstellern und Mobilfunk-Betreibern anerkannt werden. Die PPA ist technologieunabhängig konzipiert. Sie gilt somit nicht nur für das M-Payment, sondern kann auch für U-Payments angewendet werden.

Auf der U-Payment-Architektur Bluepay wurden unterschiedliche Demonstratoren implementiert, die sich für verschiedene Zahlungsanwendungen einsetzen lassen, beispielsweise im Supermarkt oder im öffentlichen Nahverkehr. Das Ziel der Demonstratoren ist es, U-Payment-Systeme zu testen, die mit Hilfe dieser Technologien realisiert sind. Hierbei interessiert insbesondere, inwieweit sich die explizite Interaktion des Kunden im Verlauf des Zahlungsvorgangs reduzieren oder sogar eliminieren lässt.

4.1 Preferred Payment Architecture

Die PPA setzt unterschiedliche Kategorien von Zahlungssystemen um (vgl. Tabelle 2). Dabei bedeutet realer POS, dass ein Kunde vor Ort bezahlt, z.B. in einem Geschäft an der Kasse. Im Gegensatz dazu bezieht sich der virtuelle POS auf Zahlungen im Internet. Da sich die Testplattform Bluepay auf den grau hinterlegten Bereich stützt, wird im folgenden die PPA für Zahlungen am realen POS beschrieben. Informationen über die Umsetzung des virtuellen POS finden sich in [MoF00]. Anhand der Unterscheidung in Mikro- und Makrozahlungen können in der PPA unterschiedliche Sicherheitsstufen implementiert werden. Dieser Aspekt blieb bei Bluepay zunächst unberücksichtigt.

Tabelle 2. Typische gekaufte Produkte nach Art des Zahlungssystems [MoF00]

	Realer POS	Virtueller POS
Mikrozahlungen (bis ca. 10 EUR)	Physische Produkte, z.B. • Straßenbahnfahrkarte, • Parkschein, • Getränk am Automaten.	Digitaler Inhalt, z.B. • Elektronische Bilder, • Klingeltöne, • Logos für Mobiltelefone.
Makrozahlungen (ab ca. 10 EUR)	Physische Produkte, z.B. • Kinoticket, • Supermarktartikel.	Physische Produkte, z.B. • CDs, • DVDs, • Bücher. Digitaler Inhalt, z.B. • Zeitschriften Abonnemente, • Marktdaten.

Lokale, mobile Transaktionen bieten unterschiedliche Möglichkeiten zum Einsatz von Mobiltelefonen als digitale Geldbörse. Als Hauptanforderungen an lokale Zahlungen gelten die Benutzerfreundlichkeit, die Sicherheit einer Zahlung und die Verlässlichkeit des Systems.

Als Architektur für lokale Zahlungen in der PPA wird eine von der Bank ausgegebene Chipkarte vorgeschlagen, auf der die entsprechende Zahlungsmethode eingebettet ist (vgl. Abbildung 2). Die Chipkarte basiert auf dem EMV-Standard, wobei die Abkürzung EMV für die drei kartenherausgebenden Unternehmen Europay, Mastercard und Visa steht. Zur Umsetzung lokaler Transaktionen werden drahtlose Technologien verwendet. Bluetooth wird beispielsweise eingesetzt, wenn größere Datenmengen zwischen einem Kassensystem des Händlers und einem mobilen Endgerät bidirektional ausgetauscht werden. Andere Prototypen von innovativen Zahlungssystemen verwendeten für lokale Transaktionen RFID zur Identifikation des Kunden.

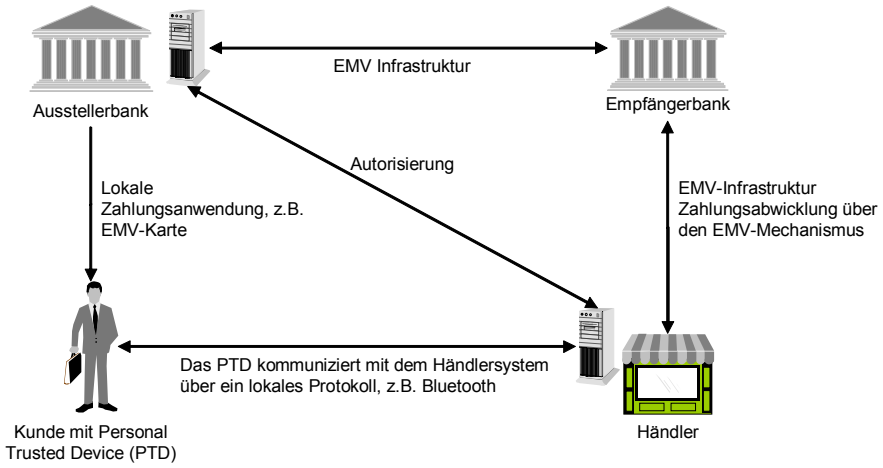

Abb. 2. PPA für Zahlungen am realen POS

4.2 Bluepay

Dieser Abschnitt geht von dem Szenario aus, dass der Kunde im Supermarkt bezahlt. Die Waren sind mit RFID-Transpondern eindeutig gekennzeichnet. Der Kunde legt die Produkte auf das Band, so dass das Kassensystem die Waren automatisch erkennt und den Warenwert für den Zahlungsvorgang berechnet.

Das Ziel der Demonstratoren war es, U-Payment-Systeme mit RFID und Bluetooth zu testen. Hierbei interessierte insbesondere, inwieweit sich die explizite Interaktion des Kunden im Verlauf des Bezahlvorgangs reduzieren oder sogar eliminieren lässt. Dazu wurden zwei Varianten betrachtet: im ersten Fall reicht eine Identifizierung des Kunden zur Bezahlung aus, im zweiten findet ein Austausch lokaler Benutzerinformation statt.

Identifizierung zur Bezahlung

Bei denjenigen Anwendungen, bei denen das System nur Identifikationsinformationen auf dem mobilen Endgerät des Kunden speichert, befinden sich alle weiteren Bezahlinformationen wie Kreditkarteninformationen in einer Datenbank, zum Beispiel im Backend-System des Händlers (vgl. Abbildung 3).

Die Bezahlung wird durch die eindeutige Identifizierung des Kunden initiiert. Der Identifikationsmechanismus, beim Demonstrator ein RFID-Transponder mit eindeutiger Identifikationsnummer, kann dabei in einem Gegenstand untergebracht sein, den der Kunde normalerweise bei sich trägt wie seine Armbanduhr oder sein Mobiltelefon. Das Kassensystem integriert einen RFID-Leser mit Antenne. Die Bezahlinformationen aus der Kundendatenbank im Backend-System werden dann über das Finanznetzwerk an den entsprechenden Finanzdienstleister

weitergeleitet, der die Zahlung autorisiert. Der Händler muss über eine ständige Netzwerkverbindung zum Finanzdienstleister verfügen. Bei dieser Variante ist keine Eingabe einer Geheimnummer durch den Kunden vorgesehen, da eine bequeme, einfache und schnelle Zahlung getätigt werden soll, hier Soft-Identification genannt. Über ein geeignetes Benutzer-Interface wird dem Kunden der Status der Zahlung angezeigt und er kann sie bestätigen oder ablehnen.

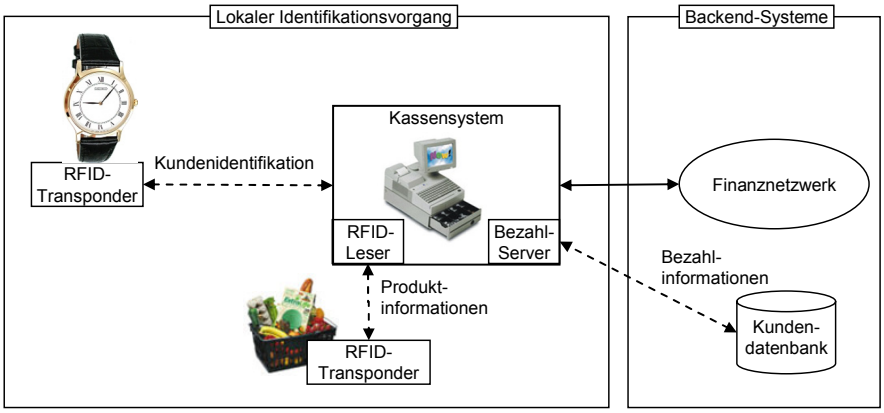

Abb. 3. Systemübersicht bei ausschließlicher Kundenidentifikation

Eine mögliche Erweiterung des Systems ist die Kombination mit einem RFID-basierten Diebstahlschutz: Produkte im Einkaufskorb, die bereits bezahlt wurden, werden auf dem RFID-Transponder markiert, so dass unbezahlte Produkte am Ausgang einen Alarm auslösen. Weiterhin kann man den Demonstrator so erweitern, dass der Kunde über das World Wide Web Zugriff auf seine Kundeninformationen erhält. So kann er Kontakt- oder Kreditkarteninformationen ändern, eine Aufstellung der getätigten Bezahlungen einsehen oder Präferenzen zu Bezahlvorgängen setzen wie Limite pro Bezahlung. Der Kunde muss sich darüber bewusst sein, dass der Händler mit der Datenbank in der Lage ist, Kundenprofile zu erstellen.

Lokaler Austausch der Bezahlinformationen

Im Unterschied zum vorher beschriebenen System benötigt der Kunde bei dieser Variante ein Gerät, auf dem sämtliche Bezahlinformationen gespeichert sind. Diese werden über eine lokale und drahtlose Verbindung ausgetauscht. Der Händler benötigt keine zusätzliche Kundendatenbank (vgl. Abbildung 4).

Die Bezahlung wird durch die Identifizierung des Bezahlgerätes initiiert, das bei diesem Demonstrator ein Mobiltelefon mit Java und Bluetooth ist. Da der Aufbau einer Bluetooth-Verbindung zwischen unbekannten Geräten im Extremfall einige Sekunden dauern kann [SiR03] und dies für den Ablauf einer automatischen Bezahlung störend ist, wird das Bezahlgerät zusätzlich über einen RFID-Transponder identifiziert, auf dem die Bluetooth-MAC-Adresse des Bezahlgerätes gespeichert ist. Dies ermöglicht ein schnelles Identifizieren des Bezahlgerätes und

dadurch einen sofortigen Aufbau der Bluetooth-Verbindung zwischen dem Bezahlgerät und der Kasse. Über diese Bluetooth-Verbindung tauschen nun das Java-Programm „Bezahl-Client“ auf dem Bezahlgerät und das Programm „Bezahl-Server“ auf der Kasse die nötigen Zahlungsinformationen aus. Hierbei können vom Kunden festgelegte Bezahlpräferenzen geprüft werden, wie beispielsweise eine explizite Zahlungsbestätigung bei einem Betrag, der ein festgesetztes Limit überschreitet. Bei einem Demonstrator des M-Lab für UBS wurde als mobiles Endgerät ein Personal Digital Assistent (PDA) verwendet, bei dem der Kunde den Händler und den zu bezahlenden Betrag angezeigt bekommt (vgl. Abbildung 5). Er muss in diesem Fall die Zahlung über eine Geheimzahl autorisieren.

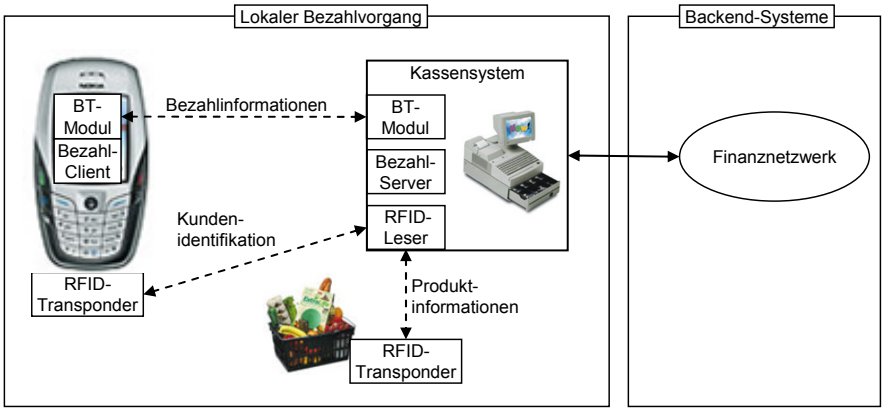

Abb. 4. Systemübersicht beim Austausch von Bezahlinformationen

Der Händler braucht keine Kundendatenbank zu führen. Wie im vorhergehenden System werden die Bezahlinformationen dann über das Finanznetzwerk an die Bezahlinstitution weitergeleitet, das die Bezahlung freigibt. Über das Benutzer-Interface wird dem Kunden der Status der Bezahlung angezeigt: entweder eine Bestätigung oder eine Warnung, falls die Bezahlung nicht freigegeben werden konnte. Der Kunde kann jederzeit auf seine Kundeninformationen über das Bezahlgerät zugreifen und sie einsehen oder ändern.

Abb. 5. Beispiel-Kundenschnittstelle beim PDA

5 Die U-Payment-Herausforderungen in der Praxis

Es gibt mehrere Herausforderungen, denen sich Banken und Finanzdienstleister bei der Umsetzung von U-Payment in der Praxis stellen müssen. Dazu zählen eine Unklarheit über Anwendungen und Geschäftsmodelle, über die technische Machbarkeit, über Datenschutz und Datensicherheit sowie über Standards. Die Standards wurden bereits im Zusammenhang mit der PPA erläutert, deshalb wird an dieser Stelle darauf verzichtet.

Für Finanzdienstleister stellt sich die Frage nach neuen *Geschäftsmodellen*, bei denen Zahlungsverfahren mit UbiComp eingesetzt werden. Sie müssen sich damit auseinandersetzen, wie die durch UbiComp entstehenden Geschäftsmodelle die Rolle der Bank verändern werden, und wie man mit den neuen Technologien im Bereich mobiler Zahlungsverfahren eine hohe Marktdurchdringung erreichen kann. Des weiteren müssen sie genaue Kosten-/Nutzenanalysen bezüglich des Mehrwertes von U-Payment durchführen.

Finanzdienstleister müssen auch die *technische Machbarkeit* beachten. Selbst bei mittlerweile etablierten Technologien wie Bluetooth ergeben sich bei deren Einsatz in der Praxis oft überraschende Probleme. Im Falle der Demonstratoren der Testplattform BluePay musste beispielsweise ein besonderes Augenmerk auf die eindeutige Kunden-Kassen-Zuordnung gelegt werden: Das bedeutet, dass der Kunde aus technischer Sicht anhand seines Identifikations- bzw. Bezahlgeräts zwar eindeutig erkannt werden konnte. Falls sich jedoch mehr als ein Kunde im Lesebereich der Kasse befindet, konnte die Kasse nicht entscheiden, welcher Kunde die Bezahlung der Produkte tätigen will. Ein ähnliches Problem ergibt sich, falls zwei Kassen denselben Kunden identifizieren. Diese Probleme lassen sich zwar nicht auf einfache Art prinzipiell lösen, aber sie können durch technische Anpassungen reduziert werden, beispielsweise indem der Lesebereich der Kasse gut an die räumliche Situation angepasst wird. Dies geschieht durch Herabsetzen der Antennensendeleistung an der Kasse und durch die Benutzung einer gerichteten Antenne.

Der *Datenschutz (privacy) und die Datensicherheit (security)* müssen sichergestellt sein. Die Daten auf dem Identifikations- bzw. Bezahlgerät dürfen für Dritte nicht zugänglich sein. Außerdem stellt sich die Frage nach dem Eigentum der Daten, d.h. wer die Hoheit über die Daten im Wertschöpfungsnetz besitzt.

Bei der Implementierung der Demonstratoren lassen sich diese Fragestellungen folgendermaßen angehen: Ein Challenge-Response-Verfahren erlaubt es, die Daten sowohl auf Hardware- wie auch auf Software-Ebene zu schützen. Es gestattet den Zugriff auf die Daten beim lokalen Austausch von Bezahlinformationen nur nach erfolgreicher Authentifizierung. Außerdem muss sichergestellt sein, dass die Daten nicht während der Übertragung zwischen Bezahlgerät und Kasse durch Dritte abgehört werden können. Dies lässt sich lösen, indem man die drahtlose Verbindung auf Hardware-Ebene verschlüsselt, wie dies bei Bluetooth der Fall ist. Eine andere Möglichkeit ist die softwaremäßige Verschlüsselung der Daten, d.h. die Programme Bezahl-Client bzw. Bezahl-Server verschlüsseln die Daten vor der Übertragung. Bei der Identifizierung durch RFID nimmt die Hardware der Funkschnittstelle die Verschlüsselung vor.

6 Schlussfolgerungen

Die Analyse der Anforderungen an Zahlungsverfahren mit UbiComp ergibt, dass Finanzdienstleister dem Endbenutzer sichere, transparente und einfache Zahlungsverfahren anbieten müssen, um eine ausreichende Akzeptanz zu erreichen. Die Händler sind bei der Auswahl der Technologien und Anwendungen von Beginn an einzubinden, da ihre Unterstützung eine der Grundvoraussetzungen für die Etablierung der Verfahren am Markt ist.

Im Rahmen der Projektzusammenarbeit von UBS und M-Lab wurden Demonstratoren im Bereich lokaler Zahlungssysteme mit Hilfe der RFID-Technologie zur automatischen Identifizierung des Kunden implementiert und getestet. Das Ziel war es, im Rahmen der technischen Anforderungen der PPA die grundsätzliche technische Machbarkeit und die Einsatzmöglichkeiten von U-Payment aufzuzeigen.

In der Zukunft kann das Potential von U-Payment auch bei Bezahlvorgängen zwischen Unternehmen liegen: durch UbiComp könnten Waren Bezahlungen selbständig einleiten, z.B. in der Logistikkette. Außerdem könnten UbiComp-Technologien den Zustand von Waren automatisch überwachen und den Finanzdienstleistern exakte Kennzahlen für die Risikoüberwachung bei Kreditrisiken und -limiten in Echtzeit liefern.

Literatur

[Acc02] Accenture (2002) Ubiquitous Commerce – Autonomous Purchasing Object, www.accenture.com/xd/xd.asp?it=enweb&xd=services\technology\tech_autopurchase.xml

[DSt01] DStar (2001) Accenture Lab works on object-to-object Internet Commerce, www.hpcwire.com/dsstar/01/1120/103711.html
[Exx02] ExxonMobil (2002) Hard-to-Shop-for People on Your Holiday List? How about an Electronic Wallet for Their Wrists? Exxon Mobil Press Release, December 4, 2002, www.exxonmobil.com/Corporate/Newsroom/Newsreleases/xom_nr_041202.asp
[HGF03] Hort C, Gross S, Fleisch E (2003) Critical Success Factors of Mobile Payment. M-Lab Working Paper No. 13
[ITW02] ITWorld (2002) Study: M-Commerce to be $25B Market by 2006, April 4, 2002, www.itworld.com/nl/ebus_insights/04042002
[IWW02] IWW (2002) Zahlungssysteme im Internet – eine Übersicht. Institut für Wirtschaftspolitik und Wirtschaftsforschung der Universität Karlsruhe
[KPT02] Kreyer N, Pousttchi K, Turowski K (2002) Characteristics of Mobile Payment Procedures. In: Proceedings of the ISMIS 2002 Workshop on M-Services
[Kru01] Krueger M (2001) The future of M-Payments – Business Options and Policy Issues. Institute for Prospective Technological Studies, European Commission
[MoF00] Mobey Forum (2000) Mobile Financial Services, White Paper
[SiR03] Siegemund F, Rohs M (2003) Rendezvous Layer Protocols for Bluetooth-Enabled Smart Devices. Journal for Personal and Ubiquitous Computing 7(2):91-101