Mobile Payment und CRM

Entwicklung eines Prototyps

Christian Kaiser, MA Wirtschaftsinformatik, Hochschule Luzern – Wirtschaft

Prof. Konrad Marfurt, Dipl. Physiker ETH, Hochschule Luzern – Wirtschaft

1 Einleitung

Dieser Konferenzbeitrag basiert auf der Masterarbeit des Hauptautors, die er im Herbstsemester 2012/13 beim International Institute of Management and Technology der Universität Freiburg im Üechtland einreichte. Die umfangreiche Originalarbeit widmet sich der Forschungsfrage „Welche Eigenschaften und Funktionen muss ein Mobile Payment System besitzen, um eine hohe Akzeptanz beim Kunden zu erreichen?“ Für den AKWI-Konferenzbeitrag konzentrieren sich die beiden Autoren auf den im Rahmen der Masterarbeit entwickelten Prototypen zur Veranschaulichung der Auswirkungen auf das Customer Relationship Management.

2 Allgemeine Anforderungen

Die Anforderungen an den Prototypen ergeben sich in erster Linie aus unseren Erkenntnissen zur Akzeptanz von Mobile Payment (MP) Systemen und zum Nutzungsverhalten von Smartphone-Besitzern. Der hohen Nutzungsbereitschaft für NFC-Payment-Services, steht laut einer Studie von YouGov eine grössere Gruppe von Personen mit Sicherheitsbedenken (52%) gegenüber [YouG12]. Wird zudem noch die aktuell geringe Verbreitung von NFC fähigen Smartphones berücksichtigt, so ist es erforderlich, alternative Technologie zu prüfen und zu integrieren.

Den fünf Regeln von Rogers für die Diffusionsgeschwindigkeit einer Innovation [Roge03] (s S.221ff.) folgend, sollte ein MP-System folgende Eigenschaften besitzen:

1. Der Kunde muss einen Mehrwert durch die Nutzung gegenüber dem bisher verwendeten Zahlungsinstrument haben (relativer Vorteil).

2. Das System muss intuitiv und einfach zu bedienen sein (geringe Komplexität).
3. Der Kunde muss es ohne hohes Risiko ausprobieren können (Probierbarkeit).
4. Es muss für andere beobachtbar sein, z.B. am POS, um es nachzuahmen (Beobachtbarkeit).
5. Es muss sich in die bisherigen Prozesse einfach eingliedern lassen, z.B. über geringe oder keine zusätzlichen Hardwareanforderungen (Kompatibilität).

Der Prototyp soll in erster Linie dazu dienen, die Einsatzmöglichkeiten eines MP-Systems für interessierte Kunden und Händler zu demonstrieren. Das funktionierende System kann von einem interessierten Händler sofort ausprobiert werden, um die Anpassbarkeit an seine Zahlungsprozesse zu prüfen. Fragen zur Zuverlässigkeit und Sicherheit können am konkreten Beispiel erläutert, statt nur abstrakt beantwortet werden. Von den gängigen Abrechnungsverfahren wird im Prototyp nur ein aufladbares Guthabenkonto implementiert. Es geht insbesondere nicht darum, bestehende Lösungen für virtuelle Kreditkarten usw. nachzubauen.
Für eine grössere Vielfalt von Abrechnungsverfahren und mehr Sicherheitsempfinden, wäre als MP-Betreiber eine Bank empfehlenswert [WiGP08] (s. S.4, 10).

3 Umsetzung der Anforderungen

Die Umsetzung aller Anforderungen ist im Prototyp nicht möglich. Sie werden jedoch auf konzeptioneller Ebene diskutiert.

3.1 Hard- und Softwareunabhängigkeit

Neben der NFC-Schnittstelle wurde auch die Übertragung mittels QR-Code realisiert. Dadurch können praktisch alle internetfähigen Smartphones das MP-System nutzen. Es wird automatisch erkannt, ob das jeweilige Smartphone eine NFC-Schnittstelle besitzt und ob diese aktiv ist. Sollte dies nicht der Fall sein, so wird dem Kunden ein QR-Code auf dem Display angezeigt. Die Gründe warum nicht ausschliesslich QR-Codes verwendet werden, liegen vor allem darin, dass die Benutzung von NFC schneller und komfortabler ist als das Scannen eines Codes.
Damit keine Beschränkungen bzgl. des Betriebssystems existieren, ist der Grossteil der Applikation als Hybrid-Applikation implementiert. D.h. die Anwendungsebene und die Grundfunktionalitäten sind in HTML-Code und JavaScript implementiert. Als erste Plattform für den Prototyp wurde Android 4.X gewählt. Die Gründe liegen vor allem im hohen Marktanteil von

Android, aber auch in der Verfügbarkeit von NFC-fähigen Smartphones. Eine Portierung auf andere Betriebssysteme ist durch die Hybrid-Technologie i.d.R. schnell und problemlos möglich. Alle sensiblen Daten werden nicht lokal, sondern auf einem externen Server gespeichert. Dadurch wird erreicht, dass kein lokales Secure-Element benutzt werden muss.

3.2 Speicherung und Übertragung der Daten

Zum Bezahlen übermittelt der Kunde einen Einmalhashwert (Ticket) an den Händler. Die Gültigkeit dieses Tickets ist auf einen Maximalbetrag und einen engen Zeitrahmen begrenzt. Letzterer kann dabei vom Kunden selbst bestimmt werden. Nach der Verwendung des Tickets wird dieses für weitere Zahlungen unbrauchbar.

Der Kunde erhält das Ticket, wenn er in der Applikation die Bezahlfunktion aufruft und sich beim Server authentifiziert. Beim erstmaligen Installieren der Applikation wird auf dem Smartphone eine Datei erzeugt und darin ein zufälliger UID-Wert gespeichert. Dieser Wert dient als „Salt“ für die Bildung des Passwortes als SHA-256 Hash gemeinsam mit der gewählten PIN. Als Benutzerkennung wird die SIM-ID (Integrated Circuit Card Identifier = ICCD) verwendet.

Die Authentisierung erfolgt im Challenge-Response Verfahren über eine verschlüsselte Verbindung (TLS, bzw. HTTPS). Auf dem Server ist eine MySQL-Datenbank mit den allgemeinen Kundendaten und dem aktuellen Guthaben realisiert. Konto- und Zahlungskartendaten müssen - sofern sie PCI[1]-konform gespeichert werden sollen - auf einem weiteren Server gelagert werden, der nicht via Internet erreichbar ist.

Hat sich der Kunde erfolgreich authentifiziert, so wird das Ticket erzeugt und an den Kunden gesendet (als JSON Objekt). In der Standardkonfiguration ist es für 60 Minuten gültig und kann für eine Transaktion verwendet werden. Sofern der Kunde noch über ein gültiges Ticket verfügt, wird er beim Aufrufen der Bezahlfunktion ohne PIN-Abfrage direkt weitergeleitet. Das ermöglicht auch das Bezahlen in Situationen, in denen *der Kunde* ortsbedingt über keine Internetverbindung verfügt.

Die Authentifizierung, Erstellung und Zusendung des Tickets für den Händler funktioniert auf die gleiche Weise wie beim Kunden. Für die Abwicklung der Bezahlung übermittelt der Händler beide Tickets an den Server. Dieser prüft deren Gültigkeit, belastet das Guthabenkonto des Kunden und bestätigt die erfolgte Gutschrift dem Händler.

---

[1] Payment Card Industry: ein Forum von Zahlungskartenanbietern mit dem Ziel der Verbreitung und Implementierung von Sicherheitsstandards für den Schutz von Kontodaten [PCIS12]

Der Unterschied besteht darin, dass das Händlerticket mehrfach verwendet werden kann. Die Gültigkeitsdauer ist durch den Händler konfigurierbar. Eine Mehrfachverwendung des gleichen Tickets stellt kein Sicherheitsrisiko dar, da dieser lediglich *zusätzlich* zur SIM-ID als Identifizierungsmerkmal des Händlers verwendet wird. Ein Diebstahl des Händlertickets ist unkritisch, da es ohne gültiges Kundenticket wertlos ist.

3.3 Externe Aufbewahrung von Bank- und Zahlungskartendaten

Datensicherheit ist eines der zentralen Themen in einem MP-System. Die grössten Bedenken gegenüber MP-Systemen beziehen sich auf die Sicherheit der persönlichen (Konto/Kreditkarten)-Daten. Gemäss PCI-Anforderungen dürfen Kartendaten nie auf einem im Internet zugänglichen Server gespeichert werden. Eine sichere Serverumgebung kann als Dienstleistung von einer Bank oder Firma betrieben werden, welche für die Datenspeicherung nach „PCI-DSS Compliance“ garantiert.

3.4 Einfache Integration in bestehende Prozesse

Händler bieten normalerweise dem Kunden mehrere Zahlungsmöglichkeiten an. Die Zahlung mit dem Mobilgerät wäre daher nur eine zusätzliche Zahlungsvariante. Wichtig ist, dass der Händler keine Änderungen an seiner Infrastruktur vornehmen muss. Ein MP-System muss sich einfach integrieren lassen. Der Prototyp kann problemlos am POS eingesetzt werden. Er ist mobil und benötigt ausser einem Smartphone als Plattform keine weitere Hardware. Die einzige Anforderung besteht darin, dass der Händler am POS entweder über eine konstante Mobilfunkverbindung oder zumindest über ein gut geschütztes WLAN (WPA2 mit deaktiviertem WPS) verfügt.

3.5 Abrechnungsmethoden

Im Prototyp wird ein virtuelles Guthabenkonto zur Verfügung gestellt. Der Kunde kann dieses über Lastschrift oder eine Zahlungskarte aufladen. Eine Verifizierung des Kontos könnte hierbei ähnlich wie bei PayCash [Payc12] über einen Buchungsprozess erfolgen. Die Erweiterung und Bereitstellung von mehreren Abrechnungsmethoden ist vom Kunden gewünscht und sollte für ein produktives MP-System unbedingt berücksichtigt werden [WiGP08] (s. S.11).
Auf dem Server des Betreibers werden alle Transaktionen protokolliert (Log-Datei) und in einer Datenbank gespeichert. Bei einer nichtanonymisierten Zahlung werden Produktname, Produktpreis, Gesamtpreis, Händler-ID, Kunden-ID, Zeit und Belegnummer gespeichert.

Für eine anonymisierte Zahlung wird lediglich die Kunden-ID nicht gespeichert. Diese Daten dienen - bei Einwilligung des Kunden - als Grundlage für die integrierbaren und personalisierten CRM-Massnahmen. Ferner werden alle genannten Transaktionsdaten in Form eines Belegs an den Kunden per E-Mail zugestellt.

3.6 MP-Betreiber

Spezialisierte Intermediäre, die als Kerngeschäft das MP-System betreiben, besitzen den grössten Nachteil im Vergleich zu Banken und Mobilfunkprovidern. Gemäss Untersuchungen wird Banken und Mobilfunkprovidern in Bezug auf Mobile Payment am ehesten vertraut. Je nach Studie liegen die Werte für Banken bei 86% (s. [GfK11]), bzw. 74% [WiGP08] (s. S.4). Das Erwerben einer Banklizenz führt der Studie nach zu keinem gesteigerten Vertrauen.

4 Architektur

Die Architektur des gesamten Systems ist nachfolgend dargestellt:

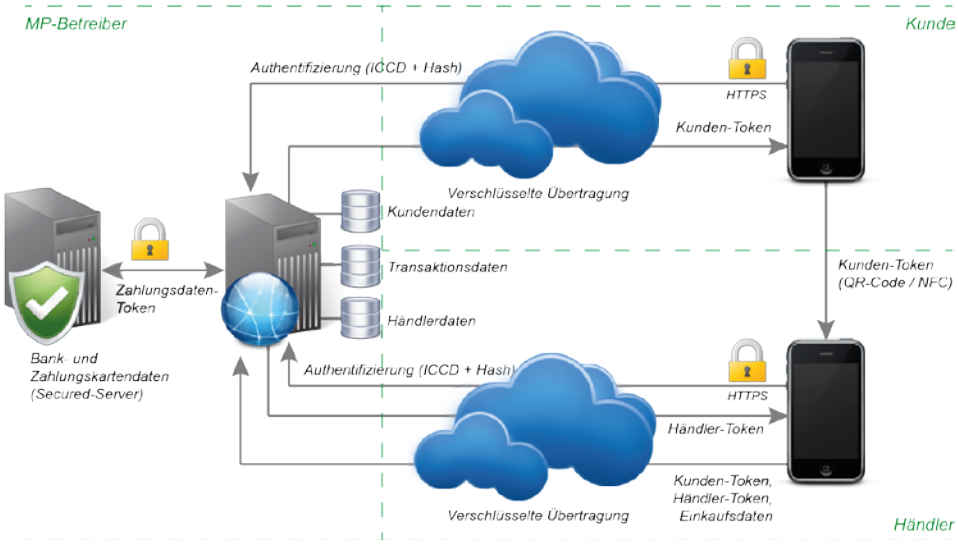

Abb. 1: Architektur des MP-Prototyps

Die Bank- und Zahlungsdaten werden auf einem separaten Server gespeichert, der die PCI-DSS-Anforderungen erfüllt. Der zweite über das Internet erreichbare Server, dient primär dazu, Kunden und Händler zu authentifizieren und die Tickets zu erzeugen.

5 Kunden-Applikation

Der Ablauf einer Bezahlung lässt sich aus der folgenden Abbildung leicht nachvollziehen:

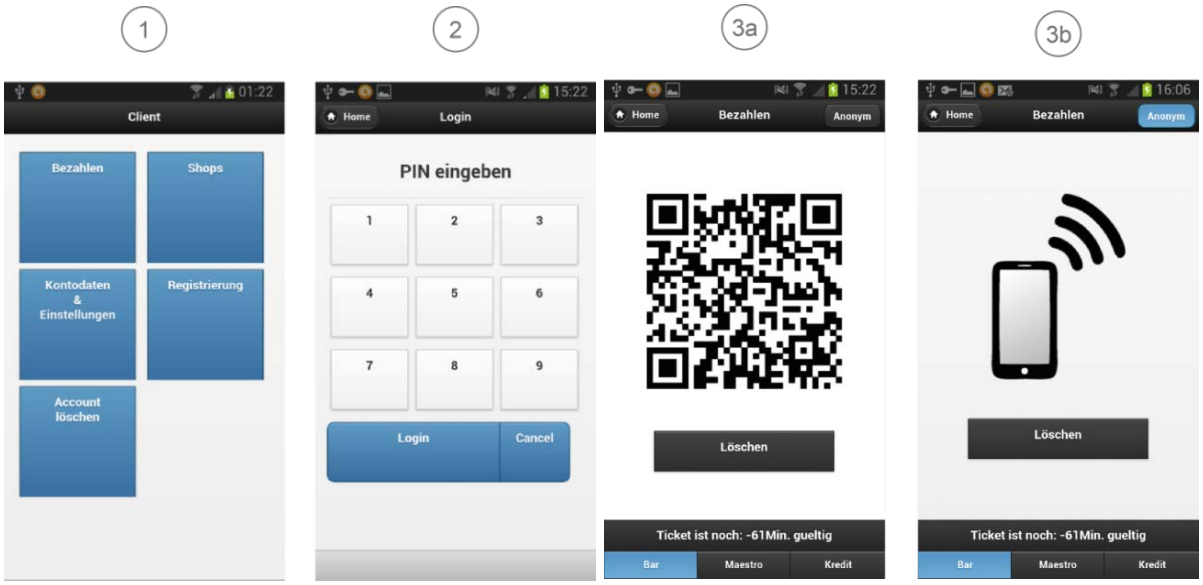

Abb. 2: Kunden Applikation – Bezahlen mit PIN-Eingabe in 3 Schritten und Fallunterscheidung ob NFC auf dem Mobilgerät verfügbar ist.

Der Kunde wählt „Bezahlen“ und gelangt zur PIN-Eingabe. Nach Aktivieren der Schaltfläche „Login“ erfolgt die Authentifizierung durch den Server. Anschliessend erhält der Kunde sein Ticket, welches er zum Zahlen einsetzen kann. Je nach Ausstattung des Gerätes wird das Ticket via NFC zum Händlergerät übertragen oder als QR-Code angezeigt, um vom Händler eingescannt zu werden.

Gemäss der Studie zu „Ausgestaltung mobiler Bezahlverfahren“ [WiGP08], wünscht sich der Kunde einerseits Sicherheit, aber andererseits auch eine einfache Bedienung. Auf eine PIN-Abfrage, wie sie im Prototyp realisiert wurde, würden lediglich 8,9% der befragten Personen verzichten. Es wird empfohlen, dass der Schwellenwert zur PIN-Abfrage vom Kunden definiert werden kann [WiGP08] (s. S.10).

Sollte dem Kunden am POS keine Internetverbindung zur Verfügung stehen, kann er das Ticket bereits im Voraus vom Server über die PIN-Eingabe anfordern und es innerhalb der (von ihm selber) definierten Gültigkeitsdauer ohne erneute PIN-Eingabe am POS einsetzen. Die Schritte bis zum Bezahlen können so unmittelbar am POS auf zwei Aktivitäten begrenzt werden.

6 Händler-Applikation

Die Händler-Applikation wurde vom Design und Layout an die Kunden-Applikation angepasst, damit der Kunde die Zugehörigkeit direkt erkennen kann (visuelle Prüfung).

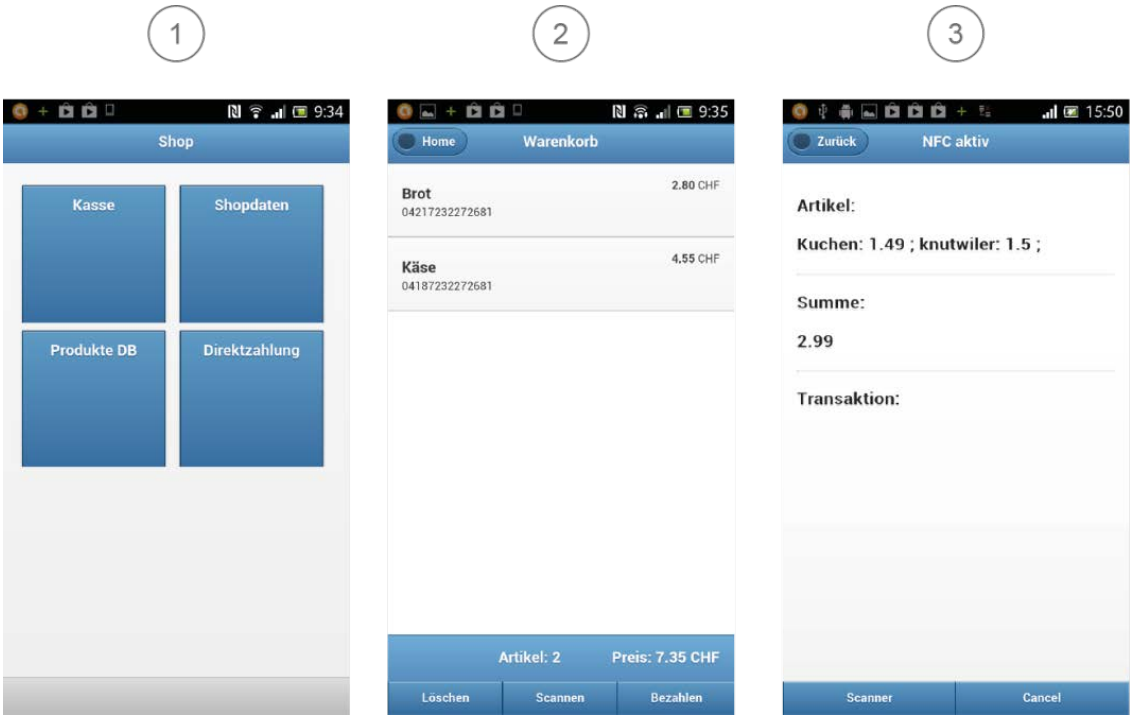

Abb. 3: Händler-Applikation – Übersicht, Kasse und Zahlungsempfang

Die Benutzerfreundlichkeit kann durch die Verwendung eindeutiger Icons für die Menüpunkte (Bild 1) weiter erhöht werden Der Menüpunkt „Kasse“ führt direkt zum Warenkorb (Bild 2). Der Händler kann Produkte über das Scannen von Barcodes oder über passive NFC-Tags erfassen. Erkannt werden nur Produkte, die zuvor in der Produktdatenbank erfasst wurden (Menüpunkt „Produkt-DB“). Diese Datenbank kann mit der Produktdatenbank des Händlers abgeglichen werden. Für den Einsatz in Restaurants oder grossen Geschäften wird so der Zahlungsempfang über mehrere Mobilgeräte möglich.

Beim Zahlungsvorgang (Bild 3) werden alle erfassten Artikel mit Preisangabe nochmals aufgelistet und mit der Gesamtsumme dargestellt. Will der Kunde mit QR-Code bezahlen, so muss der Händler links unten die Funktion „Scannen“ aktivieren. Bei aktiver NFC-Schnittstelle genügt es, wenn der Kunde sein Mobilgerät an das Händlergerät für die Übertragung anlegt. Das Scannen von Bar- und QR-Codes ist deutlich langsamer als die Übertragung via NFC.

7 Sicherheit und Erweiterungen

7.1 Sicherheit der gespeicherten Daten

Die Speicherung des „Salts“ und des Tickets erfolgen lokal auf dem festen Speicher des Smartphones. Standardmässig ist dieser Speicherbereich nur für die jeweilige Applikation zugänglich [DwCT10] (s. S. 38).

Sofern das Gerät nicht *gerootet* wurde, und sich keine Schadsoftware darauf befindet, ist dieser Bereich vor äusseren Zugriffen geschützt [Hoog11] (s. S.109). Da der MP-Betreiber nicht davon ausgehen kann, dass diese Bedingungen erfüllt sind, muss der Einsatz eines Tickets mit einer zuvor definierten Obergrenze limitiert werden. Die PIN wird generell nicht auf dem Mobilgerät gespeichert. Es gilt allgemein der Grundsatz, dass Betrug nicht zu 100% verhindert werden kann, er muss jedoch vom Betreiber erkannt werden. Die Mechanismen hierzu sind nicht Gegenstand diese Arbeit und müssen für ein produktives System ausgearbeitet werden.

7.2 Risiken und Angriffsszenarien

Ein grösseres Risiko besteht darin, dass der Kunde eine gefälschte Applikation auf dem Mobilgerät installiert. Der Angreifer zielt darauf ab, bei der Registrierung die PIN, das „Salt“ und die ICCD abzufangen und an sich übermitteln zu lassen. Über eine manipulierte Programmversion wäre er nun in der Lage mit dem Guthaben des Opfers einzukaufen. Es muss daher bei jedem Request an den Server überprüft werden, ob der Client die unveränderte Original-Applikation ist. Hierzu stehen verschiedene Mechanismen bereit, wie dass Signieren der Applikation, Prüfsummen über den Programmcode, Licensing oder dynamisches Nachladen von Programmteilen. Diese Mechanismen sind auf jeder Plattform unterschiedlich und müssen daher *native* entwickelt werden. Weitere Schutzmechanismen wie das Verschleiern (obfuscating) und Verschlüsseln des Programmcodes sind ebenso empfehlenswert. Der Prototyp erfüllt diese besonderen Anforderungen nicht und stellt lediglich einen sicheren Kommunikationskanal über HTTPS bereit. Grundsätzlich muss der MP-Betreiber bei einer Lösung ohne lokales Secure-Element davon ausgehen, dass das Gerät keine sichere Umgebung darstellt. Das Entschlüsseln und Analysieren des Programmcodes darf daher kein Sicherheitsrisiko darstellen.

8 CRM-Erweiterungen

Die Integration von Kundenbindungsprogrammen eröffnet weitere Möglichkeiten, die Akzeptanz eines MP-Systems für Kunden und Händler zu erhöhen. Im Hinblick auf eine ganzheitliche Mobile Wallet Lösung können über integrierte CRM-Erweiterungen und den damit verbundenen Dienstleistungen Gewinne erwirtschaftet werden. Die Gebühren (Merchant-Service-Charge) für Zahlungstransaktionen könnten so querfinanziert und somit reduziert werden. Die Verbindung von CRM und Payment hat daher zum Ziel, einerseits die Kosten pro Transaktion für den Händler zu senken und zum anderen dem Kunden einen Mehrwert und finanziellen Vorteil über Bonusprogramme, Rabatte und Coupons zu bieten. Letztendlich soll ihn das zur Nutzung des Gesamtsystems animieren.

8.1 Integration von mobilen Kundenkartenprogrammen

Die Integration eines virtuellen Kundenkartenprogramms stellt eine sinnvolle Erweiterung des MP-Systems dar. Der Kunde kann im Moment des Einkaufs entscheiden, ob er Bonuspunkte sammeln will oder nicht. Durch Aktivieren/Deaktivieren der Schaltfläche „Anonym“ (siehe Abb. 2) kann er diese Entscheidung bei jedem Kauf neu treffen.

Es stellt sich grundsätzlich die Frage, ob ein Single- oder Multipartner-Programm verwendet werden sollte. Hierzu sei auf eine TNS Emnid Umfrage in Deutschland aus dem Jahr 2012 verwiesen [TNEm12]. Auf die Frage: „Was muss ein Bonusprogramm, ein Rabattprogramm oder eine Kundenkarte bieten, damit sie für Sie attraktiv sind?“ war die häufigste Antwort mit 61% „Ist bei mehreren attraktiven Unternehmen einsetzbar“. Die Erwartung Coupons zu erhalten, die beim Einkauf das Sparen ermöglichen, war mit 61% ebenfalls sehr hoch. An dritter Stelle folgte der Wunsch, dass nach möglichst kurzer Zeit ein attraktiver Punktestand erreicht werden kann [TNEm12] (s. S.3-4). Wobei „attraktiv“ wahrscheinlich rein subjektiv betrachtet wird und stark vom Gegenwert der Punkte abhängt. Die gleiche Umfrage war bereits 2010 durchgeführt worden – mit einem leicht anderen Ergebnis. Ein Multipartner-Programm war den Kunden mit 68% 2010 noch um einiges wichtiger als 2012. Die Prozentpunkte haben sich zugunsten des Wunsches nach einem kurzfristig zu erreichenden attraktiven Punktestand verschoben [Ranz11] (s. S.68). Es ist den Kunden also wichtig, dass sie schnell einen Vorteil aus der Teilnahme am Bonusprogramm erzielen können. Auf die Frage, warum die Kunden eine Kundenkarte benutzen, war die mit Abstand häufigste Antwort „Ich will Geld sparen“ (52%). Erst an zweiter Stelle mit 23% folgte die Aussicht auf attraktive Prämien [TNEm12] (s. S.5). Ein MP-System, das zusätz-

lich eine Kundenkarte mit Bonuspunkten anbietet, sollte also nach Möglichkeit ein Multipartner-Programm sein, das dem Kunden schnell einen finanziellen oder geldwerten Vorteil über Rabatte oder Coupons verschafft.

8.2 Integration von Mobile-Coupons

Die Integration von mobilen Coupons in ein MP-System ermöglicht die Steigerung des Nettonutzens. Mitunter stellt sich die Frage, wann und in welcher Form ein Coupon zugestellt werden soll. Die Entscheidung über die Zustellungsart (Push oder Pull) muss in Abhängigkeit zur Relevanz getroffen werden. Der Kunde muss jedoch die Möglichkeit besitzen, Händlern generell die Push-Permission zu entziehen oder diese explizit einem Händler dauerhaft zu gewähren.
Die Relevanz eines Coupons für den jeweiligen Kunden lässt sich über verschiedene Parameter ermitteln. Im Einzelnen wären dies beispielsweise: Kundenart (Bestands- oder Neukunde), aktueller Ort, Zeitpunkt, persönliche Präferenzen und bisheriges Kaufverhalten.
Eine geeignete Parametrierung könnte dem Kunden erlauben, die Relevanz bestimmter Produktkategorien mit dem Standort zu kombinieren. Andernfalls lässt sich das Produktinteresse auch über das bisherige Kaufverhalten ermitteln, sofern ausreichend Daten vorhanden sind und der Kunde seine Einwilligung gegeben hat.
Ein weiteres Entscheidungskriterium kann der Gültigkeitszeitraum darstellen. Zeitlich stark begrenzte Angebote, wie beispielsweise Gutscheine für Mittagsmenus, erfordern ein zeitnahes Einlösen, um den Vorteil geltend machen zu können.
Es zeigt sich, dass die Entscheidung über die Art der Zustellung ein klares Konzept benötigt. Die Ausbaustufen sind praktisch unbegrenzt. Über das Einlösen von Gutscheinen liesse sich die aktuelle Strategie dynamisch prüfen und anpassen.

Abb. 4: Darstellungsentwurf für Coupons innerhalb der Kunden-Applikation

In Abbildung 4 wird eine Variante dargestellt, wie Coupons in die Kunden-Applikation eingebunden werden könnten. Wichtig ist, dass der Kunde auf den ersten Blick erkennt, ob es sich

um einen Personal-Coupon oder um einen Public-Coupon handelt. Die individualisierten Coupons, in der Abbildung rot hinterlegt, sollten in der Regel eine höhe Relevanz für den Kunden aufweisen und damit einen höheren Nettonutzen für ihn bedeuten.
Dem Kunden sollte immer die Wahl gelassen werden, ob er Coupons nur einlösen oder in Kombination mit der Bezahlfunktion einlösen möchte. Das hat den Vorteil, dass auch Kunden die Applikation nutzen können, die sich nicht für die Bezahlfunktion registriert haben.

8.3 Stufensystem für Kunden

Untersuchungen (s. [YouG12]) haben gezeigt, dass auf Seiten der Kunden in Bezug auf Mobile Payment weiterhin grosse Bedenken bzgl. der Sicherheit vorherrschen. Es stellt sich nun die Frage, wie diese verringert oder beseitigt werden können. Das Ziel besteht daher darin, dass Kunden Vertrauen in das System aufbauen. Im Folgenden soll erläutert werden, wie Kundenbindungsinstrumente dazu beitragen könnten.
Rogers hat als einen Faktor für die Adoption einer Innovation die „Probierbarkeit“ genannt [Roge03] (s. S.258). Es wird nun die Hypothese aufgestellt, dass Kunden, die ein System ausprobieren können, ohne dass sie persönliche Risiken eingehen müssen, Vertrauen gegenüber dem System aufbauen können. Die Risiken für den Kunden beziehen sich in Anlehnung an Prein (2011) auf den Kontrollverlust persönlicher Daten. In Tabelle 5 sind diese in Bezug auf den Prototyp dargestellt. Sie lassen sich in folgende Benutzerkategorien unterteilen:

- A Nicht registrierter Kunde
- B Registrierter Kunde nimmt am Bonus/Rabatt-Programm teil
- C Registrierter Kunde, nutzt die Bezahlfunktion
- D Registrierter Kunde, nutzt die Bezahlfunktion und nimmt am Bonus/Rabatt-Programm teil

Risiken (Kontrollverlust von Daten)	Kategorien			
	A	B	C	D
Personenbezogene Daten (Name, Telefonnummer, Anschrift, etc.)	-	X	X	X
Einkaufsverhalten (Händler, Produkte und Umsatz)	-	X	-	X
Bank- und Zahlungskartendaten	-	-	X	X

Tab. 5: Risiko des Kontrollverlustes über persönliche Daten nach Benutzerkategorien

Die Kategorie A wird hier als Einsteigergruppe betrachtet. Sofern der Prototyp durch die Funktionen aus den vorherigen Kapiteln erweitert wird, erleichtert dies die Probierbarkeit des vorge-

stellten MP-Systems. Der Funktionsumfang wäre für Kunden der Kategorie A auf die Suche von Händlern und Angeboten beschränkt. Geldwerte Vorteile können demnach nur durch den Einsatz von Public Coupons erreicht werden. Im Gegenzug muss sich der Kunde jedoch weder registrieren noch persönliche Daten angeben. Es ist allerdings wichtig, dass die Angebote, die über das System zur Verfügung gestellt werden, ihm in ausreichendem Masse einen Vorteil verschaffen. Der Kunde kann so das System ausprobieren, ohne persönliche Risiken einzugehen. In der nachfolgenden Tabelle 6 sind die verschiedenen Funktionen, die neben dem Bezahlen möglich sind, nach Benutzergruppen unterteilt:

Funktionen	Benutzergruppen			
	A	B	C	D
Public Coupons	X	X	X	X
Private Coupons	-	X	-	X
Teilnahme am Bonusprogramm des Systems	-	-	-	X
Zahlen mit Bonuspunkten oder Gutschriften	-	X	-	X
Zahlen mit Guthabenkonto/Zahlungskarten	-	-	X	X

Tab. 6: Nutzbare Funktionalitäten nach Benutzerkategorien

Werden beide Tabellen kombiniert betrachtet, so ergibt sich für die Benutzerkategorie B der grösste Vorteil im Vergleich zum eingegangenen Risiko. Wird der Kontrollverlust von Daten als Aufwand betrachtet, so ergibt sich für registrierte Kunden der grösste Nettonutzen. Diese Erkenntnis wird durch die Untersuchung von Prein (s. [Prei11]) bestätigt. Demnach hat der „*Kontrollverlust über Stamm- und Transaktionsdaten […] keinen signifikanten Einfluss auf den von den Befragten erwarteten Nettonutzen*“ [Prei11] (s. S.151). Dies gilt allerdings nur für die Benutzerkategorie B.

Eine Steigerung der Probierbarkeit lässt sich zusätzlich über die Funktion „Zahlen mit Bonuspunkten oder Gutschriften“ erreichen. Der Kunde kann somit auch die Grundfunktion des MP-Systems, das mobile Bezahlen, über das Einlösen von Gutschriften ausprobieren, ohne den Kontrollverlust von Bank- oder Zahlungskartendaten zu befürchten. Die Benutzerkategorie D unterscheidet sich im Vergleich zur Kategorie B lediglich in der Funktion „Zahlen mit Guthabenkonto oder virtuellen Zahlungskarten“. Der Anreiz für Benutzer der Kategorie B, in die Kategorie D zu wechseln, bestünde lediglich darin, einen höheren Bequemlichkeitsvorteil zu errei-

chen. Für eine schärfere Abgrenzung und einen grösseren Anreiz sollte daher die Teilnahme am Bonusprogramm vom MP-Betreiber selbst, nur der Kategorie D ermöglicht werden.

9 Ausblick

Der im Rahmen einer Masterarbeit entwickelte Prototyp ist nicht als Vorstufe eines globalen MP-Systems gedacht. Er darf auch nicht als Konkurrenz zu den bestehenden mobilen Kreditkartenlösungen betrachtet werden. Er kann jedoch in begrenzten Umgebungen (Firmen, Schulen, zeitlich begrenzte Anlässe wie Konzerte) durchaus eingesetzt werden, um Erfahrungen mit der Praktikabilität und der Akzeptanz der Benutzerschnittstelle zu sammeln. Für einen grösseren aussagekräftigen Feldtest wären allerdings die notwendigen Sicherheitsmechanismen vorgängig noch zu implementieren.

Der Prototyp könnte auch eine weitergehende Erforschung der diskutierten Kundenbindungsmassnahmen ermöglichen, da er für interessierte Partner aus der Wirtschaft die Möglichkeit bietet, die Wirkung und Akzeptanz von geplanten oder ins Auge gefassten CRM-Aktivitäten zeitlich und örtlich begrenzt zu erproben, statt die Entscheidungen nur auf Umfrageergebnisse abzustützen.

Die Autoren sehen auch eine Möglichkeit, den Prototyp als Anschauungsobjekt für die Steigerung der Akzeptanz von MP-Systemen einzusetzen, indem er in Vermarktungskampagnen als „hands-on“ Beispiel zur Erläuterung der Risiken und der entsprechenden Sicherheitsmechanismen eingesetzt wird.

Literatur

[DwCT10] *Dwivedi, H.; Clark, Ch.; Thiel, D.*: Mobile Application Security, USA 2010.

[GfK11] *GfK*: Internationale Studie von GfK Custom Research zu Chancen und Herausforderungen für Mobile Payment-Angebote, http://www.gfk.ch/imperia/md/ content/presse/pressemeldungen_2011/110517_mobile-payment_dfin.pdf, 2011.

[Hoog11] *Hoog, A.*: Android Forensics, Investigation, Analysis and Mobile Security for Google Android, Waltham, Massachusetts, 2011.

[PayC12] *PayCash*: AGB, http://www.paycash.eu/kontakt/agb/. Abruf am 04.01.2012.

[PCIS12] *PCI Security Standards Council*: http://de.pcisecuritystandards.org/minisite/en/. Abruf am 22.12.2012.

[Prei11] *Prein, J.*: Akzeptanz mobiler Kundenkartenprogramme bei Konsumenten, Gabler, Wiesbaden 2011.

[Ranz11] *Ranzinger, A.*: Praxiswissen Kundenbindungsprogramme – Konzeption und operative Umsetzung, Gabler Verlag, Wiesbaden 2011.

[Roge03] *Rogers, E. M.*: Diffusion of Innovations, 5th Edition, Free Press, New York, 2003.

[TNEm12] *TNS Emnid*: Bonusprogramme in Deutschland, http://www.tns-emnid.com/ prese/pdf/presseinformationen/TNS_Emnid_Studie_Bonusprogramme_2012.pdf, 2012.

[WiGP08] *Wiedermann, D.; Goeke, L.; Pousttchi, K.*: Ausgestaltung mobiler Bezahlvefahren, Ergebnisse der Studie MP3, http://www.wi-mobile.org/fileadmin/ Papers/MP/Ausgestaltung-mobiler-Bezahlverfahren_71-09.pdf, 2008.

[YouG12] *YouGov*: Pressemitteilung NFC-Technologie (2012), http://research.yougov.de/presse/2012/pressemitteilung-nfc-technologie/, Abruf am 10.01.2013.

Kontakt:

Christian Kaiser, Prof. Konrad Marfurt
Hochschule Luzern – Wirtschaft
Institut für Wirtschaftsinformatik
Zentralstrasse 9, 6002 Luzern
christian.kaiser@hslu.ch
konrad.marfurt@hslu.ch