Zur rechtsverträglichen Technikgestaltung anhand einer M-Commerce-Anwendung

Andreas Heinemann* Johannes Ranke* Tobias Straub*

Graduiertenkolleg „Infrastruktur für den elektronischen Markt“
Fachbereich Informatik
Technische Universität Darmstadt
Wilhelminenstr. 7
D-64283 Darmstadt
{aheine | ranke | tstraub}@gkec.tu-darmstadt.de

Abstract: In diesem Beitrag stellen wir die für den M-Commerce wesentlichen Rechtsfragen dar, um Systementwicklern eine Entscheidungshilfe bei der Auswahl von Technologien und der praktischen Realisierung von Anwendungen zu geben. Anhand des an der TU Darmstadt entwickelten adPASS-Systems zeigen wir exemplarisch, wie die rechtlichen Anforderungen in einer konkreten Anwendung umgesetzt werden können.

1 Einleitung

Mit steigender Verbreitung mobiler Endgeräte wie Mobiltelefonen und PDAs erfährt das Gebiet des *Mobile Commerce* (kurz: M-Commerce) in Forschung und Industrie vermehrtes Interesse. Bei der Umsetzung von konkreten Projekten stellt sich jedoch nicht nur die Frage nach der Auswahl geeigneter Technologien. Da es sich im Allgemeinen um unternehmensübergreifende Geschäftsprozesse und -beziehungen handelt, müssen immer auch die geltenden gesetzlichen Regelungen berücksichtigt werden. Fokus dieser Arbeit ist daher die Darstellung der wesentlichen Rechtsfragen des M-Commerce. Es wird anhand einer konkreten Anwendung aufgezeigt, wie eine rechtsverträgliche Realisierung aussehen kann.

Die Arbeit gliedert sich wie folgt: Zunächst werden aus rechtlicher Sicht Schutzziele kategorisiert, die im M-Commerce zu beachten sind. In den Abschnitten 3 und 4 stellen wir das System adPASS vor und beschreiben, wie dessen Systemdesign die rechtlichen Vorgaben umsetzt.

* Gefördert durch die Deutsche Forschungsgesellschaft (DFG) im Rahmen des Graduiertenkollegs „Infrastruktur für den elektronischen Markt“ an der Technischen Universität Darmstadt.

2 Schutzziele im Mobile Commerce

Spezielle auf den M-Commerce gemünzte Rechtsregeln des deutschen oder europäischen Gesetzgebers gibt es bisher kaum. So ist allein die Nutzung und Verarbeitung von Standortdaten bei Location-Based-Sevices näher geregelt, ansonsten finden die Regelungen des Telekommunikations- und Internetrechts Anwendung.

Die rechtliche Problematik besteht nun darin, allgemeine Regelungen auf die Eigenheiten des M-Commerce anzuwenden; insbesondere ist dabei stets die konkrete Technik oder Anwendung zu berücksichtigen. Allerdings lassen sich für den Geschäftsverkehr über mobile Endgeräte fünf Prinzipien nennen, die für B2C-Anwendungen allgemein gültig sind. Diese, in Abbildung 1 dargestellten Prinzipien, lassen sich aus dem Verfassungsrecht ableiten und haben sich in einer Vielzahl einfachgesetzlicher Vorschriften niedergeschlagen.

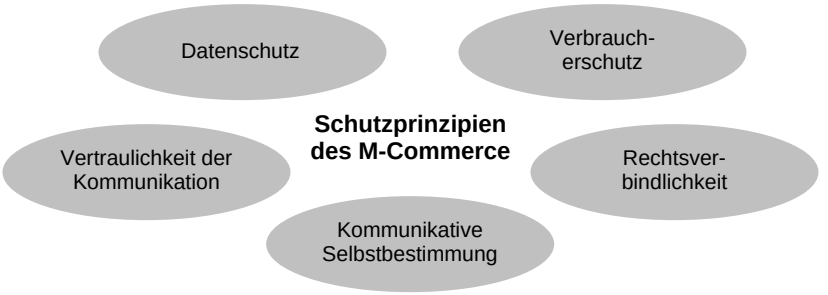

Abbildung 1: Schutzprinzipien des M-Commerce

2.1 Datenschutz und Vertraulichkeit der Kommunikation

Datenschutz und Vertraulichkeit der Kommunikation folgen sehr ähnlichen Zielen; das Unterscheidungskriterium ist der Personenbezug der Daten. Das *informationelle Selbstbestimmungsrecht*, das im einfachgesetzlichen Rahmen auch als Datenschutz bezeichnet wird, bezieht sich auf den Schutz personenbezogener Daten (z.B. Name, Adresse, Kreditkartennummer). Im M-Commerce wird dieses Prinzip besonders relevant, da die Nutzer über das mobile Endgerät ortbar sind und somit Bewegungsprofile über sie erstellt werden können.

Vertraulichkeit der Kommunikation bezieht sich auf den Schutz des Nutzers vor Ausspähen der übertragenen Nutz- und Verbindungsdaten. Aus Sicht des Technikentwicklers und –anwenders ist vor allem das Prinzip der Sicherheit relevant, welches wir im Rahmen des Datenschutzes mit besprechen.

Wir geben nun zunächst eine Abgrenzung der einschlägigen Regelungen und führen die zentralen Begriffe des personenbezogenen Datums sowie der Anonymität und Pseudonymität ein. Anschließend erläutern wir die relevanten rechtlichen Grundsätze.

Einschlägige Regelungen

Für die Verarbeitung personenbezogener Daten sind – je nach Datenform – verschiedene Datenschutzgesetze zu beachten: Für den M-Commerce sind grundsätzlich das TDDSG (Teledienstedatenschutzgesetz) oder die entsprechenden datenschutzrechtlichen Bestimmungen des MDStV (Mediendienstestaatsvertrag), das TKG (Telekommunikationsgesetz) sowie das BDSG (Bundesdatenschutzgesetz) von Belang. Für die Unterscheidung ist wichtig, auf welcher Schicht die Daten anfallen, wobei die Schicht nicht gänzlich identisch mit der Protokollebene sein muss. Reine Vermittlungs- oder Übertragungsdaten fallen in den Bereich des TKG, während auf der „Applikationsschicht", d.h. den eigentlichen Inhalten (etwa einer Email oder Webseite), vor allem TDDSG und MDStV relevant sind. Sofern in diesen Gesetzen keine speziellen Regelungen getroffen sind, findet das allgemeine Datenschutzrecht Anwendung. Unabhängig von der Anwendbarkeit der verschiedenen gesetzlichen Regelungen lassen sich aus diesen Gesetzen die generellen Kriterien der *Datenvermeidung*, *Entscheidungsfreiheit*, *Transparenz* und *Sicherheit* ableiten. Sie sind bei der Entwicklung und Bereitstellung von M-Commerce-Anwendungen in jedem Fall zu berücksichtigen.

Personenbezogene Daten

Der Datenschutz ist Ausprägung des Selbstbestimmungsrechts des Einzelnen, über die in einem System über seine Person gespeicherten Daten selbst zu entscheiden. Da sich der Schutz nur auf personenbezogene Daten bezieht, ist situationsabhängig die Frage zu beantworten, ob ein Datum den Rückschluss auf eine bestimmte Person zulässt. Es ist durchaus möglich, dass dieselbe Information je nach Datenverwender ein personenbezogenes oder aber anonymes Datum ist.

Maßstab für das Fehlen eines Personenbezugs ist, ob die Zuordnung „nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft" möglich ist (§ 3 Abs. 6 BDSG), wobei für den M-Commerce insbesondere das Kostenkriterium maßgebend ist. Man wird dann Anonymität annehmen, wenn die Kosten zur Re-Identifizierung jene der Neubeschaffung der Informationen deutlich übersteigen (siehe [KFH03] zu den Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes).

Anonymität und Pseudonymität

Das informationelle Selbstbestimmungsrecht gilt grundsätzlich nur für personenbezogene Daten, so dass die Verarbeitung von anonymen und pseudonymen Daten nach dem Datenschutzgesetz grundsätzlich erlaubt ist. Anonymität liegt vor, falls die Zuordnung der Daten zu einer Person durch den Datenverwender nur mit einem unverhältnismäßig großen Aufwand möglich ist. Im Unterschied dazu basiert das Konzept des Handelns unter einem Pseudonym darauf, dass die Identität des Nutzers im Ausnahmefall aufgedeckt werden kann [Si03: § 3 Rdnr. 222]. Sie wird als fairer Interessenausgleich zwischen dem Schutz des Nutzers, seiner informationellen Selbstbestimmung und den wirtschaftlichen Interessen des Diensteanbieters gesehen, wenn dieser seine Dienstleistung abrechnen muss [RS00].

Identität	Pseudonymität	Anonymität
Identifizierung trivial	*... aufwändig*	*... unmöglich*

Abbildung 2: Personenbezug von Daten

Um den durch Pseudonymität tatsächlich erzielten Schutzgrad zu bewerten, ist zu beachten, dass – im Gegensatz zur Anonymität – pseudonymes Handeln die Bildung von Nutzerprofilen ermöglicht. Diese beinhalten etwa Konsumgewohnheiten, persönliche Interessen sowie im M-Commerce auch Bewegungsprofile. Dies kann aber dazu führen, dass der Personenbezug im Nachhinein festgestellt werden kann und es sich eben nicht mehr um pseudonyme Daten handelt. Daneben ist beim Systementwurf weiter zu bedenken, dass auch der Nutzer, sei es durch versehentliche oder bewusste Handlungen, einen Personenbezug herstellen kann.

Gerade durch die Verkettbarkeit zahlreicher Aktionen zu einem nicht wechselbaren Pseudonym wird dessen Schutzwert für den Benutzer reduziert. Zwar sehen die Datenschutzgesetze gewisse Vorsorgeregelungen vor, um diesen Gefahren einer Re-Identifizierung zu begegnen. Es sind aber, soweit möglich, anonyme Dienste vorzuziehen.

Datenvermeidung

Wegen der massenhaften Nutzung moderner Informationstechnologien und der damit einhergehenden Datenflut hat der Gesetzgeber in § 4 Abs. 6 TDDSG bzw. § 18 Abs. 6 MDStV Diensteanbieter und indirekt auch Hersteller der Datenverarbeitungssysteme verpflichtet, Nutzern anonymes oder pseudonymes Handeln (und Bezahlen) zu ermöglichen. Gleiches gilt grundsätzlich für die dem BDSG und dem TKG unterliegenden Daten gemäß § 3a BDSG und § 3 Abs. 4 TDSV. Der Grundsatz der Datenvermeidung bedeutet, dass die Verarbeitung personenbezogener Daten zu verhindern oder zumindest im Umfang zu minimieren ist.

Ein Personenbezug kann in der Praxis etwa dadurch verhindert werden, dass – sofern möglich – keine statischen Geräte- und Kommunikationsadressen verwendet werden. Entsprechende Aspekte sind bereits beim Design eines Systems zu berücksichtigen und die Leistungsbeschreibungen so abstrakt zu fassen, dass sie wenig Informationen über einen Nutzer voraussetzen.

Entscheidungsfreiheit

Die Entscheidungsfreiheit zielt auf eine aktive Beteiligung des Nutzers am Datenverarbeitungsprozess ab. Das heißt, dass die Preisgabe personenbezogener Daten nicht ungewollt oder unbemerkt erfolgen darf, sondern nur durch einen auf freier Willensentschließung beruhenden Willensakt. Der Nutzer muss vor, während und nach der Erhebung der Daten die Möglichkeit haben, die Verarbeitung zu beeinflussen. Den Grundsatz der Einwilligung regelt § 4a BDSG. Auch für die Erhebung und Verarbeitung von Standortdaten zur Bereitstellung eines Dienstes mit Zusatznutzen wurde ein Einwilligungsvorbehalt gemäß § 96 Abs. 1 TKG-Entwurf normiert.

Wichtig ist, dass die Erbringung von Diensten nicht von der Abgabe personenbezogener Daten abhängig gemacht werden darf, die für diesen Dienst nicht erforderlich sind [Kö97, Si02].

Transparenz

Die informationelle Selbstbestimmung im M-Commerce setzt weiter voraus, dass die Datenverarbeitung gegenüber dem Nutzer transparent ist. Transparenz bedeutet, dass der betroffene Nutzer sich informieren kann, wer, was, wann, bei welcher Gelegenheit über ihn weiß. Nur in diesem Fall kann der betroffene Nutzer die Rechtmäßigkeit der Datenverarbeitung überprüfen und seine Rechte geltend machen.

Dazu muss der Betroffene natürlich Umfang und Zweck der Datenverarbeitung kennen. Dies gewährleisten Unterrichtungspflichten (§ 88 TKG, § 4 Abs. 1 TDDSG, § 18 Abs. 1 MDStV und § 4 Abs. 3 BDSG) sowie Kontroll- und Auskunftsmöglichkeiten (etwa § 4 Abs. 7 TDDSG, § 20 Abs. 1 MDStV und §§ 6 Abs. 1 i.V.m. § 19, 34 BDSG).

Sicherheit

Im Sinne des Datenschutzes umfasst der Begriff Sicherheit drei der klassischen Schutzziele der IT-Sicherheit, nämlich Vertraulichkeit, Integrität und Verfügbarkeit von Daten. Das Schutzziel Rechtsverbindlichkeit oder Nichtabstreitbarkeit wird in Abschnitt 2.3 besprochen.

Bei der Kommunikation in anonymen Benutzergruppen und offenen Netzwerken kann der Nutzer den Kommunikationspartnern und -vermittlern nicht ohne Weiteres vertrauen. Das Konzept der „mehrseitigen Sicherheit“ trägt dem Rechnung, indem es jedem Teilnehmer die Möglichkeit bietet, selbst seine Interessen zu schützen und mit dem Kooperationspartner die Bedingungen gegenseitiger Sicherheit auszuhandeln [MP97, Ra00]. Systeme sollten deshalb unbedingt so gestaltet werden, dass jeder Nutzer anderen nur minimal zu vertrauen braucht.

2.2 Kommunikative Selbstbestimmung

Das kommunikative Selbstbestimmungsrecht des Nutzers ist betroffen, wenn die Entscheidung zu einer Kommunikation durch die Technik beeinträchtigt wird oder Kommunikationsinhalt, -partner, -ort sowie die Kommunikationsart und -situation nicht autonom gewählt werden können.

Das kommunikative Selbstbestimmungsrecht dient zwar, wie auch das informationelle Selbstbestimmungsrecht, der Identitätsbildung und Selbstdarstellung [Ro90], zielt aber auf den Schutz vor Gefahren der technisch vermittelten Nachrichtenübermittlung ab. Es kann im M-Commerce etwa durch unautorisierte Push-Dienste betroffen sein. Die Möglichkeit der Kommunikation bedarf stets eines Mitwirkungsaktes des Nutzers. Das kommunikative Selbstbestimmungsrecht ist daher vor allem betroffen, wenn der Endgerätenutzer unerwünschte Nachrichten erhält oder auf andere Weise Kommunikationsort, -zeit und -partner nicht frei bestimmen kann.

Auch im Rahmen des kommunikativen Selbstbestimmungsrechts lassen sich aus dem Rechtsprinzip für die Anwendung der Technik die Grundkriterien Entscheidungsfreiheit und Transparenz ableiten, die wir bereits im Rahmen des Datenschutzes vorgefunden haben.

Entscheidungsfreiheit

Zwar ist es im Zusammenhang mit der kommunikativen Selbstbestimmung erforderlich, dass die Umstände der Kommunikation auf einer freien Willensentschließung der Beteiligten beruhen, allerdings bestehen im Gegensatz zum Datenschutz nur ausnahmsweise gesetzliche oder durch richterliche Rechtsfortbildung gewachsene Einwilligungstatbestände. Im Fall der Zusendung von Werbenachrichten ist allerdings das Erfordernis einer Einwilligung anerkannt, wobei auch die Möglichkeit einer mutmaßlichen Einwilligung besteht.

Bei Einwilligungstatbeständen ist derjenige Nutzer, dessen kommunikatives Selbstbestimmungsrecht betroffen ist, stets darauf angewiesen, dass der andere, der in sein Recht eingreift, das Einwilligungserfordernis beachtet. Einen präventiven Schutz bieten in diesem Fall mögliche Sanktionsandrohungen oder technische Verfahren, die es dem Betroffenen ermöglichen, die Kommunikation zu beeinflussen und der konkreten Situation anzupassen.

Transparenz

Auf die kommunikative Selbstbestimmung bezogen, bedeutet Transparenz, dass alle wesentlichen Merkmale der Kommunikationsbeziehung, die ausgeführten Funktionen und der Status der beteiligten Endgeräte erkennbar sein müssen [HPR93].

2.3 Rechtsverbindlichkeit

Wichtig beim Entwurf von M-Commerce-Systemen ist es, technische Möglichkeiten vorzusehen, die die Verbindlichkeit von Rechtshandlungen und deren Beweisbarkeit gewährleisten.

Für den M-Commerce gilt im Zivilprozess (wie sonst auch) der Grundsatz der freien richterlichen Beweiswürdigung (§ 286 BGB). Eine Tatsache gilt dann als bewiesen, wenn der Richter überzeugt ist, dass die fragliche Willenserklärung vom vermeintlich Erklärenden in dieser Form abgegeben wurde (Authentizität und Integrität). Da etwa Absenderadresse und Inhalt von gewöhnlichen Emails technisch nicht gegen Manipulation geschützt sind und daher leicht gefälscht werden können, wird in diesem Zusammenhang allerdings nicht von einem Anscheinsbeweis ausgegangen [Kö03, MM01, Ro02].

Wirkungsvolle Abhilfe schaffen hier digitale Signaturen. Die im Signaturgesetz (SigG) als fortgeschrittene elektronische Signaturen bezeichneten Verfahren erreichen durch Verwendung von Public-Key-Kryptografie zwar einen hohen technischen Schutz, doch einen gesetzlich normierten Anscheinsbeweis nach § 292a ZPO bieten jedoch nur die gesetzlich an hohe Anforderungen geknüpften qualifizierten Signaturen. Im Einzelfall ist deshalb unter Abwägung des Kosten-Nutzen-Verhältnisses zu entscheiden, ob qualifizierte Signa-

turen für die jeweilige Anwendung einzusetzen sind oder ob auch fortgeschrittene Signaturen ausreichen. Werden qualifizierte Signaturen innerhalb von M-Commerce-Anwendungen eingesetzt, so ist eine entsprechende Gestaltung der mobilen Infrastrukturen erforderlich [RFR03].

2.4 Verbraucherschutz

Schließlich ist im Rahmen von mobilen B2C-Anwendungen stets auch das Prinzip Verbraucherschutz zu beachten. Dieser wird durch eine Reihe von Vorschriften geregelt, die teils allgemeiner Natur sind, sich teils aus dem durch die elektronische Kommunikation ergebenden Gefährdungspotential für den Verbraucher ergeben. Dabei handelt es sich um Informations-, Hinweis- und Rechtsgestaltungsmöglichkeiten.

3 Das System adPASS

In diesem Abschnitt beschreiben wir kurz das System adPASS. Für eine ausführliche Darstellung der technischen Details verweisen wir auf [HKLM03] und [SH04].

adPASS erlaubt die Verbreitung von digitalen Anzeigen innerhalb mobiler Nutzergruppen. Die Anzeigen werden von teilnehmenden Geschäften verbreitet, wo sie lokal über ein Funknetz (z.B. Bluetooth oder WLAN 802.11 WiFi) auf die mobilen Endgeräte der Kunden übertragen werden. Dabei zeigen die Kunden über ein Benutzerprofil an, an welcher Art von Produkten sie interessiert sind.

3.1 Konzept

Die neuartige Idee von adPASS ist, die Technik und ein Anreizsystem dafür zu schaffen, dass ein Kunde Anzeigen an andere potenzielle Käufer weitergeben kann. Diese Weitergabe erfolgt ohne Benutzerinteraktion im Einzelfall und ist wiederum durch die Reichweite der Endgeräte begrenzt. Da die Benutzer mobil sind, wird die Anzeige auch physisch transportiert. Eine Anzeige, die in einem Laden des Händlers aufgenommen wurde, kann somit später in der Fußgängerzone weitergeben werden. Das Kommunikationsmodell ist dabei bewusst der „Mund-zu-Mund-Propaganda“ nachempfunden, also der Art wie sich Informationen durch Empfehlung unter Menschen mit gleichen Interessen verbreiten [HS03].

Aufgrund der Preisentwicklung werden schon in wenigen Jahren entsprechend ausgestattete mobile Endgeräte wie PDAs oder Handys einen ausreichend hohen Verbreitungsgrad erreicht haben, um neuartige Dienste zu ermöglichen, die die Fähigkeit zur spontanen Vernetzung und Kooperation ausnutzen. adPASS zielt darauf ab, diese immensen Ressourcen nutzbar zu machen. Natürlich müssen dafür wirkungsvolle Anreize für die Teilnehmer geschaffen werden. Speicher- und Batteriekapazität sind begrenzt, so dass sie nicht ohne Gegenleistung zur Verfügung gestellt werden. An dieser Stelle setzt adPASS mit einem Bonuspunkte- oder Provisionsmodell an: Teilnehmer erhalten im Fall einer erfolgreichen Empfehlung, d.h. wenn durch die von ihnen weitergegebene Anzeige

ein Kunde für das beworbene Produkt gewonnen wird, einen Bonus. Im Gegensatz zu den heute bekannten und verbreiteten Bonussystemen wie etwa Payback [Pa03] oder Webmiles [We03], ist es bei adPASS aber möglich und beabsichtigt, allein durch das erfolgreiche Weiterempfehlen Bonuspunkte zu sammeln.

Aus Sicht des Händlers ermöglicht adPASS Werbung ohne Streuverluste, da nur Bonuspunkte ausgeschüttet werden, wenn auf eine Anzeige hin tatsächlich ein Kauf stattfindet. Der Aufwand für die Verbreitung der Anzeigen wird nunmehr – zumindest teilweise – vom Kunden selbst übernommen. adPASS fördert damit die Verbreitung von Werbung an eine Vielzahl von potenziellen Kunden zu relativ niedrigen Fixkosten für die Sendeeinrichtungen im Geschäft.

Um eine hohe Akzeptanz des Systems zu schaffen, wurde bewusst von Anfang an der Schutz der Privatsphäre der Teilnehmer als Designziel berücksichtigt. adPASS ermöglicht ein vollständig anonymes Handeln – ein Konzept das diametral zu dem etablierter Bonuspunktsysteme steht.

3.2 Funktionsweise

Anhand des Beispiels in Abbildung 3 erläutern wir, wie die Kommunikation der Teilnehmer in adPASS verläuft. Neben Händlern und Kunden wirkt dabei auch eine dritte Partei, ein *Mittler*, als zentrales Bindeglied mit. Systemweit genügt ein solcher Mittler als gemeinsame Plattform aller Händler.

1. Zunächst besucht ein Kunde *A* das Geschäft eines Händlers, der digitale Anzeigen über feste Sendeeinrichtungen, so genannte *Information Sprinkler* verbreitet. Während der Zeit im Geschäft werden Anzeigen, die dem Interessenprofil des Kunden entsprechen, über das Funknetzwerk auf sein mobiles Endgerät übertragen.

2. Nachdem *A* das Geschäft verlassen hat, begegnet er einem Kunden *B* und die Anzeige wird an ihn weitergereicht. *B* seinerseits reicht später die Anzeige an *C* weiter etc. Dabei ist ausdrücklich beabsichtigt, dass Anzeigen vervielfältigt werden. Wir nehmen an, dass die potenziellen Kunden mit mobilen Endgeräten ausgestattet sind, die die adPASS-Software ausführen und zur kabellosen Spontanvernetzung fähig sind.

3. *C* hat Interesse an dem beworbenen Produkt und sucht den Händler auf. Sein mobiles Gerät überspielt dann Informationen über die an der Empfehlung beteiligten Teilnehmer (in unserem Beispiel *A* und *B*) an den Händler.

4. Der Händler informiert den Mittler, welche Teilnehmer mit Bonuspunkten belohnt werden sollen (in diesem Beispiel *A*, *B* und *C*). Dieser übernimmt die Aufgabe, angesammelte Bonuspunkte für die Teilnehmer zwischenzuspeichern, da die Endgeräte nicht über eine dauerhafte Verbindung zum Händler verfügen.

5. Über eine Internet-Verbindung zum Mittler können die Teilnehmer jederzeit nachfragen, ob ihre Teilnahme an adPASS zur Ausschüttung von Bonuspunkten

geführt hat, diese Punkte gegebenenfalls auf ihr mobiles Gerät herunterladen und z.B. bei einem späteren Kauf verwenden.

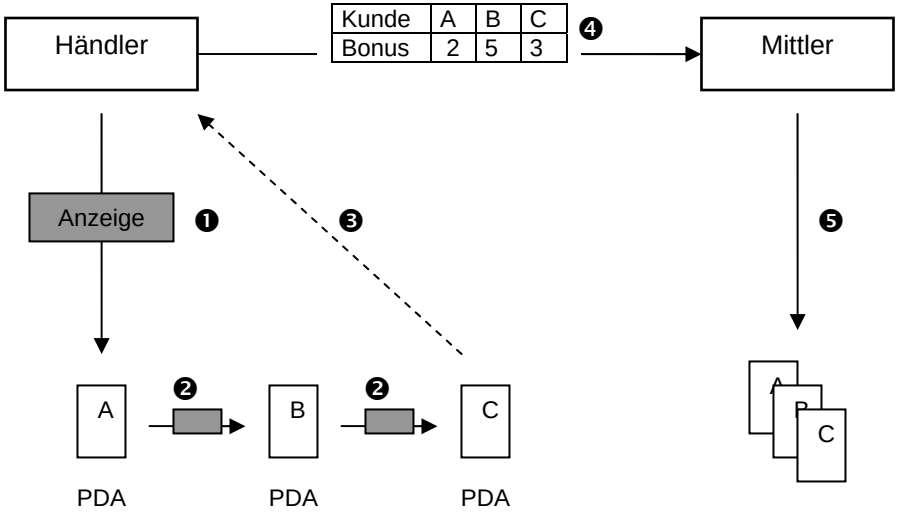

Abbildung 3: Kommunikation in adPASS

Der Händler spezifiziert in der Anzeige eine gewisse Anzahl von Bonuspunkten, die er bereit ist, *pro Kauf* auszuschütten (im Beispiel 10). Hierbei werden aber nur Kunden belohnt, die direkt an der Weitergabe der Anzeige zum Käufer beteiligt waren. Dadurch bleibt die Ausgabe von Bonuspunkten für den Händler kalkulierbar, da sie stets an einen realen Kauf gekoppelt ist.

Während die Anzeige verbreitet wird, können sich die Teilnehmer „virtuelle Bonuspunkte“, d.h. Optionen auf eine spätere Ausschüttung von Bonuspunkten, sichern. Die Unterscheidung zwischen virtuellen und tatsächlichen Bonuspunkten bildet die Unsicherheit darüber ab, ob am Ende der Empfehlungs- oder Kommunikationskette auch ein Käufer steht. Angenommen, Kunde *A* hätte im Beispiel die Anzeige auch an *D*, dieser wiederum an *E* weitergegeben, jedoch hätten weder *D* noch *E* das Produkt gekauft. *A* hätte zwar über die *Kommunikationskette* [Händler, *A*, *B*, *C*] Bonuspunkte verdient, jedoch nicht über die Kette [Händler, *A*, *D*, *E*].

adPASS lässt zu, dass jeder Teilnehmer selbst die Anzahl virtueller Bonuspunkte bestimmt, die er für sich beansprucht (im Beispiel beansprucht *A* zwei, *B* fünf und *C* drei Punkte). Dies ist ein Mittel, die Attraktivität von Anzeigen abzubilden und dient dazu, eine persönliche Strategie auszudrücken. Für eine detaillierte Beschreibung und Modellierung verweisen wir auf die Arbeit [SH04].

3.3 Geschäftsmodell

Wir skizzieren kurz ein mögliches Geschäftsmodell für adPASS: Im Gegenzug dafür, dass der Mittler den Händlern die technische Infrastruktur (Information Sprinkler, Software) bereitstellt, sichern ihm diese eine Beteiligung an dem von adPASS erzeugten Umsatz oder Gewinn zu. Der Mittler stellt den Teilnehmern die Clientsoftware kostenfrei zum Download zur Verfügung. Eine Installation des Programms setzt die Kenntnisnahme und Einwilligung in die AGBs des Mittlers voraus. Unter anderem enthalten die AGBs einen Rechtsanspruch der Teilnehmer auf Auszahlung der Bonuspunkte sowie eine Verpflichtung der teilnehmenden Händler, diese Bonuspunkte einzulösen und beworbene Produkte auch zu dem angepriesenen Preis zu veräußern, des Weiteren eine Verpflichtung zu wahrheitsgemäßen Angaben in den Anzeigen. Damit wird verhindert, dass etwa unter der Kategorie „CD-Player“ Waschmaschinen beworben werden können (zur Spam-Problematik siehe Abschnitt 4.2).

Bisher haben wir angenommen, dass es nur einen einzigen Mittler gibt. Diese Monopolstellung des Mittlers kann durch Zulassung weiterer Mittler aufgelöst werden, wobei sich alle Mittler einem gemeinsamen Rahmenwerk unterwerfen, das sowohl technische als auch rechtliche Aspekte umfasst. Hierbei ist unverzichtbar, dass Interoper-abilität zwischen den Mittlern besteht und aus Sicht der Teilnehmer vollkommene Transparenz herrscht. Das bedeutet, zwei Teilnehmer sollten Werbung austauschen können, auch wenn sie unterschiedliche Mittler bevorzugen. Die Zulassung weiterer Mittler erhöht den Wettbewerb im System und könnte zum Ausbau der Dienste seitens der Mittler führen, bspw. Anbindung der Bonuspunkte an andere verbreitete Systeme wie Payback oder Webmiles. Ähnliches kann man heutzutage schon im Kreditkartenwesen beobachten, wo das Produkt Kreditkarte ummit speziellen Leistungen und Diensten gekoppelt wird, etwa mit einer BahnCard.

3.4 Technische Realisierung

Als Techniken zur Umsetzung der gewünschten Schutzziele verwenden wir neben digitalen Signaturen auch besondere Methoden, um die Anonymität der Teilnehmer zu gewährleisten.

Public Keys als Aliasnamen

Ein Teilnehmer agiert bei adPASS nicht unter seinem eigenen, sondern unter verschiedenen Aliasnamen, die er selbst wählen kann. Anders als bei Pseudonymen, die per Definition immer einer Person zugeordnet werden können, ermöglichen selbstgenerierte und damit beliebig oft wechselbare Aliasnamen ein vollständig anonymes Handeln, da niemand außer dem Benutzer selbst einen Aliasnamen aufdecken kann. Um aber die in einer erfolgreichen Kommunikationskette anfallenden Bonuspunkte sicher zuordnen zu können, benötigen wir eine weitere Eigenschaft: Ein Benutzer muss *beweisen* können, dass er unter einem bestimmten Aliasnamen an der Verbreitung der Anzeige beteiligt war und ihm dementsprechend Bonuspunkte zustehen.

Diese Probleme lösen wir dadurch, dass wir als Aliasnamen den öffentlichen Schlüssel (Public Key) eines kryptografischen Schlüsselpaars verwenden. Solche Schlüsselpaare, z.B. für das häufig eingesetzte RSA-Verfahren [RSA78], stellen systemweit eindeutige Aliasnamen dar und lassen sich auf heute gebräuchlichen PDAs mit vertretbarem Zeitaufwand nutzen [SH04]. Nur wer im Besitz des zu einem Public Key gehörigen privaten Schlüssels ist, kann dies auch beweisen.

Schutz der Kommunikationskette

In anonymen Benutzergruppen kann sich der Einzelne nicht darauf verlassen, dass alle Teilnehmer ehrlich agieren. Da mit einer Anzeige stets auch Abrechnungsdaten, d.h. die Kommunikationskette und Angaben darüber, wie viele virtuelle Bonuspunkte jeder Teilnehmer der Kette beansprucht, übermittelt werden, sind besondere Schutzmechanismen nötig. Ein Teilnehmer könnte sonst vorherige Teilnehmer ausschließen oder deren Anteil an Punkten manipulieren.

adPASS trägt dem in einer Datenstruktur, wie sie in [SH04] spezifiziert ist, Rechnung. Bei der Weitergabe einer Anzeige, etwa von *A* nach *B*, erhält *B* einen von *A* signierten Datensatz, der die Aliasnamen von Sender (Public Key von *A*) und Empfänger (Public Key von *B*) sowie einen Bezug zur Anzeige und die Anzahl verbliebener Bonuspunkte (im Beispiel 8) enthält. Auch der Händler als Erster in der Kette reicht einen entsprechenden Datensatz an *A* weiter; diese Datensätze bilden nun eine gegen Manipulationen geschützte Kette vom Händler bis zum Käufer.

Beim Kauf erhält der Händler vom Käufer eine Kopie der Kommunikationskette und reicht diese dann zur Abrechnung an den Mittler weiter, der die Bonuspunkte unter dem jeweiligen Aliasnamen hinterlegt. Jeder Teilnehmer kann über das Internet die Liste derjenigen Aliasnamen einsehen, für die der Mittler Bonuspunkte bereithält und diese mit der Liste der eigenen Aliasnamen vergleichen. Ein Teilnehmer braucht seinen privaten Schlüssel, den er möglicherweise für mehrere Transaktionen verwendet hat, nicht einmal offenzulegen, um dessen Kenntnis nachzuweisen, wenn ein so genanntes Challenge-Response-Verfahren eingesetzt wird (siehe etwa [MOV01]).

Identifikation des Händlers

Im Gegensatz zu den Teilnehmern ist der Händler daran interessiert (und im Rahmen der Anbieterkennzeichnung auch verpflichtet), seine Identität offenzulegen. adPASS lässt im System daher nur Anzeigen zu, die eine qualifizierte Signatur tragen. Eine solche Anzeige ist gleichzeitig eine rechtsverbindliche Erklärung, das Produkt zu dem in der Anzeige genannten Preis zu verkaufen und die angegebene Anzahl von Bonuspunkten zu vergeben.

Durchsetzung der Anonymität

Die Anonymität eines Teilnehmers muss in drei Situationen geschützt werden, die sich in der Art des Kommunikationspartners (Händler, Nutzer, Mittler) unterscheiden lassen. Technisch verläuft die Kommunikation zwischen Händler und Nutzer dabei genauso ab wie zwischen zwei Nutzern. Wichtig ist, dass sich Anonymität über den gesamten Netzwerkstapel erstreckt: Nicht nur müssen auf Applikationsebene regelmäßig die Aliasnamen

gewechselt werden, sondern auch auf TCP/IP-Schicht und darunter (802.11 WiFi) müssen entsprechende Maßnahmen ergriffen werden. Der Vorteil der lokal beschränkten Kommunikation über Funk besteht darin, dass IP- und sogar MAC-Adressen selbständig und dynamisch geändert werden können. Die Kommunikation mit dem Mittler kann z.B. über Chaum'sche Mix-Netzwerke [Ch81] effektiv gesichert werden.

4 Rechtsverträglichkeit der Gestaltung

In diesem Abschnitt erläutern wir im Einzelnen, wie das Design von adPASS die rechtlichen Vorgaben umsetzt.

4.1 Datenschutz und Vertraulichkeit der Kommunikation

Datenvermeidung

Bei der Kommunikation zwischen Händler und Kunden sowie zwischen zwei Kunden und auch in der Beziehung Kunde zu Mittler werden keine personenbezogenen Angaben gespeichert oder übertragen. Kunden setzen einen zufällig gewählten öffentlichen Schlüssel als Aliasnamen ein, der nur für sehr wenige Transaktionen verwendet wird. Allein der Teilnehmer ist im Besitz des passenden privaten Schlüssels; diese Information ist ausreichend, um später Anspruch auf Bonuspunkte beim Mittler geltend zu machen. Außerdem wird es wegen der Möglichkeit, variable Kommunikations- und Gerätekennungen zu verwenden, für den Händler sinnlos, anhand dieser Profile über die Teilnehmer zu erstellen.

Ein weiteres Merkmal, das der Datenvermeidung zugute kommt, besteht in der Möglichkeit des Nutzers, seine Bonuspunkte ohne vorherige personenbezogene Authentifikation zu erhalten. Der Nutzer kann seine Anonymität gegenüber dem Mittler dadurch schützen, dass er über Anonymisierungsdienste wie Mix-Netzwerke kommuniziert.

Als klassischer Teledienst vermeidet adPASS damit jede Form von personenbezogenen Daten. Das System entspricht damit den Vorgaben des § 6 Abs. 4 TDDSG, der Teleddiensteanbietern vorschreibt, dass sie die pseudonyme und anonyme Inanspruchnahme von Diensten bereitzustellen haben. Weil adPASS nicht nur pseudonyme sondern auch anonyme Nutzer zulässt, geht es sogar über die gesetzlichen Anforderungen hinaus.

Entscheidungsfreiheit

Da keine personenbezogenen Daten verarbeitet werden, benötigt adPASS keine datenschutzrechtliche Einwilligung des Nutzers. Der Teilnehmer hat aus datenschutzrechtlicher Sicht kein schutzwürdiges Interesse, die Datenverarbeitung zu begrenzen.

Stellt der Teilnehmer jedoch versehentlich einen Personenbezug her oder kommt es zur Personenbeziehbarkeit von Daten, hat der Diensteanbieter alle Daten des Teilnehmers zu löschen oder eine Einwilligung beim Nutzer einzuholen. Diese muss auf dem freien Willen des Teilnehmers beruhen, es muss außerdem eine Unterrichtung über den Zweck der

Datenverarbeitung erfolgen und die elektronische Form nach § 126a BGB eingehalten werden.

Transparenz

Da in adPASS keine Daten erhoben werden, die ohne aktive Hilfe als personenbezogen zu bewerten sind, ist Transparenz inhärent gegeben.

Sicherheit

Auch das Prinzip der Sicherheit bezieht sich grundsätzlich nur auf personenbezogene Daten. Allerdings sollte er auch bei der Verarbeitung anderer Daten beachtet werden. Denn möglicherweise können Dritte, die über gewisses Sonderwissen verfügen, die pseudonymen oder anonymen Daten einer konkreten Person zuordnen.

Vertraulichkeit der Kommunikation

Zur Verschlüsselung der Daten können auf der Übertragungsebene entsprechende Verfahren eingesetzt werden. Dabei sollte es dem Nutzer unter dem Gesichtspunkt der „mehrseitigen" Sicherheit selbst überlassen sein, ob er seine Daten verschlüsselt. Zwar ist, da es sich in adPASS ja ohnehin um öffentlich zugängliche Anzeigen handelt, Verschlüsselung nicht zwingend notwendig, wird aber von der Technik unterstützt.

4.2 Kommunikative Selbstbestimmung

Entscheidungsfreiheit

Die adPASS-Anwendung sieht in der Benutzerschnittstelle explizit einen Schalter vor, der die willentliche Kommunikation und den Wunsch zur Übersendung von kategorisierten Werbenachrichten zum Ausdruck bringt (siehe [SH04] für einen Screenshot). Durch die Endgeräteeinstellungen bringt der Nutzer seine Entscheidung für den Empfang der Werbung zum Ausdruck, die dem Diensteanbieter dadurch zugeht, dass sie die Schnittstelle des Information Sprinklers überschreitet und dort protokolliert wird. Damit hat der Nutzer ausdrücklich zu verstehen gegeben, dass er die Werbenachricht wünscht.

Der Gefahr des Empfangs von Nachrichten, die nicht in der gewünschten Kategorie liegen (vgl. Spam-Problematik im Internet) wird mit dem Einsatz von Filtern begegnet. Da die Händler über ihre qualifizierte Signatur nur authentisiert am System teilnehmen, ist es möglich, Händler, die falsch deklarierte Werbung verbreiten, zu erkennen und nötigenfalls auszuschließen.

Transparenz

Das Kriterium der Transparenz in Bezug auf die kommunikative Selbstbestimmung wird bei adPASS dadurch berücksichtigt, dass es dem Nutzer deutlich anzeigt, welche Daten an andere Teilnehmer des ad-hoc-Netzes übermittelt werden.

Gesetzliche Anforderungen hinsichtlich der Transparenz sind allerdings nur auf Händlerseite zu beachten. Gemäß § 7 TDG hat der Diensteanbieter bei einer kommerziellen

Kommunikation besondere Informationspflichten zu berücksichtigen. Werden diese durch den Diensteanbieter beachtet, so erfüllt adPASS auch diesbezüglich die gesetzlichen Anforderungen.

4.3 Rechtsverbindlichkeit

Der Einsatz von qualifizierten Signaturen auf Seiten des Händlers führt dazu, dass der Nutzer einen Anscheinsbeweis über die Ausgabe einer gewissen Anzahl von Bonuspunkten erlangt. Des Weiteren erhält der Nutzer einen rechtsverbindlichen Nachweis darüber, dass die Anzeige vom Händler ausgegeben wird. Der Einsatz qualifizierter Verfahren fördert damit das Vertrauen in adPASS.

Weiter sind die Teilnehmer durch die in Abschnitt 3.4 beschriebenen Schutzmechanismen vor Betrug gefeit. Auch hier fördern digitale Signaturen das Vertrauen der Teilnehmer, wenngleich fortgeschrittene Signaturen ausreichen.

Das Kriterium der Rechtsverbindlichkeit erfüllt adPASS in hohem Maße. Eine gesetzliche Verpflichtung zum Einsatz digitaler Signaturen besteht zwar nicht, jedoch gelangen die Beteiligten nicht in die missliche Lage, ihre Ansprüche nicht beweisen zu können.

4.4 Verbraucherschutz

Sofern es sich beim Verbraucherschutz um Rechtsgestaltungsmöglichkeiten wie etwa Rücktrittsrechte handelt, bedarf es keiner besonderen technischen Umsetzung. Das Bereitstellen von Informationen kann im M-Commerce jedoch aufgrund der beschränkten Displaygröße mit Schwierigkeiten verbunden sein. Insbesondere umfangreiche Geschäftsbedingungen, deren Geltung der Diensteanbieter wünscht, müssen für den Nutzer nach § 305 Abs. 2 Nr. 2 BGB in zumutbarer Weise einsehbar sein. Dabei ist von dem Diensteanbieter zu beachten, dass er 6-7 Displayseiten in gut lesbarer Schrift nicht überschreiten sollte. Daneben wären jedoch auch auf konventionellem Wege oder über stationäre Endgeräte abgeschlossene Rahmenverträge über die Nutzung des adPASS-Systems denkbar. Zukünftig wäre sogar an eine maschinelle Abfrage standardisierter Vertragsklauseln zu denken. In jedem Fall kann der Diensteanbieter jedoch auf die Einbeziehung von AGBs verzichten, so dass die gesetzlichen Vorschriften anwendbar wären (siehe dazu [Ra02]).

5 Zusammenfassung und Ausblick

Im vorliegenden Beitrag haben wir zunächst die wesentlichen Rechtsregeln des Mobile Commerce aufgezeigt. Jede M-Commerce-Anwendung muss sich mit den Anforderungen *Datenschutz*, *Vertraulichkeit der Kommunikation*, *Kommunikative Selbstbestimmung*, *Rechtsverbindlichkeit* und im Anwendungsfeld des B2C mit dem *Verbraucherschutz* auseinander setzen. Am Beispiel von adPASS, einem System zur Verbreitung von Werbung in mobilen Nutzergruppen, wurde eine konkrete Umsetzung vorgestellt. Auf technische

Details konnte dabei aufgrund von Umfang und Fokus der Arbeit nur grob eingegangen werden.

adPASS zeigt, dass es prinzipiell möglich ist, ein extrem datensparsames System zu konzipieren, das Händlern und Teilnehmern gleichermaßen einen hohen Nutzen und wirtschaftliche Anreize bietet, zugleich aber dank kryptografischer Methoden sicher gegen Manipulationen ist. Gerade den hohen Schutz der Privatsphäre sehen wir als zentrales Merkmal von adPASS an. Gegenwärtig wird der Prototyp von adPASS ausgebaut, als weiterer Schritt ist eine Studie zur Benutzerakzeptanz geplant.

Literaturverzeichnis

[Ch81] Chaum, D. L.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM, 24(2), 1981, S. 84–88.

[HPR93] Hammer, V.; Pordesch, U.; Roßnagel, A.: Betriebliche Telefon- und ISDN-Anlagen rechtmäßig gestaltet. Springer, 1993.

[HKLM03] Heinemann, A.; Kangasharju, J.; Lyardet, F.; Mühlhäuser, M.: Ad Hoc Collaboration and Information Services Using Information Clouds. 3rd Workshop on Applications and Services in Wireless Networks. Bern, 2003.

[HS03] Heinemann, A.; Straub, T.: Mund-zu-Mund Propaganda mit Bonussystem in mobilen Ad-Hoc Netzen. INFORMATIK 2003. Frankfurt am Main, 2003.

[Kö03] OLG Köln, CR 2003, 55.

[Kö97] Königshofen, T.: Die Umsetzung von TKG und TDSV durch Netzbetreiber, Service-Provider und Telekommunikationsdienstanbieter. RDV 1997, S. 97–108.

[KFH03] Köpsell, S.; Federrath, H.; ansen, M.: Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes. DuD 3/2003, S. 139–143.

[MOV01] Menezes, A. J.; van Oorschot, P.C.; Vanstone, S.A.: Handbook of Applied Cryptography, CRC Press, 5. Aufl., 2001.

[MM01] Miedbrodt, A.; Mayer, P.: E-Commerce – Digitale Signaturen in der Praxis. MDR 2001, S. 432–436.

[MP97] Müller, G.; Pfitzmann, A.: Mehrseitig sichere Kommunikationen. In (Müller, G; Pfitzmann, A. Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik: Verfahren, Komponenten, Integration (Band 1), Bonn, 1997, S. 11–21.

[Pa03] Payback, Webseite www.payback.de (gesehen 11/2003).

[Ra02] Ranke, J.: M-Commerce – Einbeziehung von AGB und Erfüllung von Informationspflichten MMR 2002, 509-515.

[RFR03] Ranke, J.; Fritsch, L.; Roßnagel, H.: M-Signaturen aus rechtlicher Sicht, DuD 2003, S. 95-101.

[Ra00] Rannenberg, K.: Multilateral Security – A concept and examples for balanced security. 9th ACM New Security Paradigms Workshop, Cork, 2000.

[RSA78] Rivest, R.; Shamir, A.; Adleman, L.: A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 21(2), 1978, S. 120-126

[Ro90] Roßnagel, A.: Das Recht auf (tele-) kommunikative Selbstbestimmung. Kritische Justiz (KJ), 1990, S. 267–289.

[Ro02] Roßnagel, A.: K&R Kommentar. K&R 2002, S. 84–86.

[RS00] Roßnagel, A.; Scholz, P.: Datenschutz durch Anonymität und Pseudonymität. Rechtsfolgen der Verwendung anonymer und pseudonymer Daten. MultiMedia& Recht (MMR), 12/2000, S. 721–732.

[SH04] Straub, T.; Heinemann, A.: An Anonymous Bonus Point System For Mobile Commerce Based On Word-Of-Mouth Recommendation. Erscheint in: Proc. 19th Annual ACM Symposium on Applied Computing, Nikosia, 2004.

[Si02] Simitis, S.: Auf dem Weg zu einem neuen Datenschutzkonzept: Die zweite Novellierungsstufe des BDSG. DuD 12/2000, S. 714–726.

[Si03] Simitis, S. (Hrsg.): Kommentar zum Bundesdatenschutzgesetz, 5. Aufl., Nomos 2003.

[We03] Webmiles, Webseite www.webmiles.de (gesehen 11/2003)