# Anonymity by Design – Eine Architektur zur Gewährleistung von Kundenschutz im mobilen Marketing

Rebecca Bulander, Gunther Schiefer, Michael Decker

Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB)
Universität Karlsruhe
76128 Karlsruhe
{bulander, schiefer, decker}@aifb.uni-karlsruhe.de

**Abstract:** Mobiles Marketing stellt eine konsequente Weiterentwicklung herkömmlicher Werbeformen dar, indem sie zielgerichtet ist und Interaktion ermöglicht; doch viele Kunden sind nicht bereit, für zielgerichtete mobile Werbung ihre Anonymität aufzugeben. In diesem Beitrag soll gezeigt werden, wie die Anonymität von Kunden im mobilen Marketing und damit auch die rechtlichen Anforderungen durch die Systemarchitektur gewahrt werden können. Dies wird am Beispiel des Projekts "MoMa - Mobiles Marketing" demonstriert.

## 1 Einführung

Technologische Entwicklungen haben im Bereich des Marketings neue Kommunikationswege und Medien, wie E-Mail, Short Messaging Service (SMS) und Multimedia Messaging Service (MMS) eröffnet. Damit erhalten werbetreibende Unternehmen die Möglichkeit, ihre Kunden mit mobilem Marketing personalisiert und direkt zu erreichen sowie mit ihnen in Interaktion zu treten. Unter „mobilem Marketing“ verstehen wir Konzepte, welche unter Hinzuziehung von verfügbaren Situationsdeterminanten ein zielgerichtetes Marketing auf mobilen Endgeräten ermöglichen. Situationsdeterminanten können die Kenntnis der individuellen Präferenzen (Profil), der momentane Aufenthaltsort, die momentane Rolle und dgl. sein [SJ01]. Marketing orientiert sich im Allgemeinen an den vier P’s (Product (Produkt), Price (Preis), Place (Distribution), Promotion (Kommunikation)). Ein zentrales Element des mobilen Marketings ist die Kommunikation. Für das One-to-One-Marketing kommen neuen Kommunikationsformen wie z.B. E-Mail, SMS, MMS und sprachbasierte Anwendungen in Frage. Über das Cell Broadcasting (CB) besteht die Möglichkeit für One-to-Many-Marketing.

Bisher konnte sich mobiles Marketing am Markt noch nicht durchsetzen. Einige der Ursachen hierfür sind:

- Die rechtlichen Vorschriften legen fest, dass Push-Werbung aus Sicht des Werbetreibenden nur möglich ist, wenn eine explizite Zustimmung des Empfängers vorliegt (Option-In-Regelung) oder bereits eine Kundenbeziehung besteht bzw. eine Kundenbeziehung in der Anbahnung ist (verkaufsfördernde Maßnahmen).

In diesen Fällen hat der Kunde jedoch seine Anonymität gegenüber dem werbetreibenden Unternehmen verloren.

- Die Angst vor SMS- und MMS-Spamming schmälert die Akzeptanz der Nutzer für mobiles Marketing. Viele Nutzer kennen die Spam-Problematik bereits von E-Mails. Darüber hinaus befürchten Nutzer eine nicht korrekte Einhaltung der Datenschutzbestimmungen durch die werbetreibenden Unternehmen, so dass sie zum gläsernen Kunden werden können. Beide Aspekte führen zu einem fehlenden Vertrauen der Nutzer in mobiles Marketing.

Im diesem Beitrag wird gezeigt, wie durch eine spezielle Konzeption einer Systemarchitektur für mobiles Marketing im Rahmen des BMWA[1]-geförderten Leitprojekts „MoMa – Mobiles Marketing“ nicht nur die in Deutschland rechtlichen Rahmenbedingungen eingehalten werden können, sondern darüber hinaus Kundenanonymität sichergestellt werden kann. Damit kann die Nutzerakzeptanz im mobilen Marketing erhöht, und gleichzeitig können den werbetreibenden Unternehmen Marktinformationen aus dem MoMa-System zur Verfügung gestellt werden.

# 2 Marketing

## 2.1 Merkmale verschiedener Werbeträger

Marketing kann sich verschiedener Werbeträger bzw. Kanäle zum Kunden bedienen, welche unterschiedliche charakteristische Merkmale aufweisen (siehe Tabelle 1). In einem Überblick sind hier die Reichweite des Werbeträgers, die Möglichkeit zur Kundeninteraktion, die Güte der Kundensegmentation, die jederzeitige Erreichbarkeit und die ortsabhängige Anpassbarkeit gegenüber gestellt. Der schwarz ausgefüllte Teil der Kreise in Tabelle 1 gibt das Zutreffen des bestimmten Merkmals für den jeweiligen Werbeträger an.

- Technisch bedingt ist die Reichweite bei elektronischen Medien größer als bei Printmedien.

- Die Möglichkeit zur Interaktion erhöht sich, wenn der Beworbene eine freie Zeiteinteilung hat, keine Medienbrüche vorhanden sind und eine hohe Responsegeschwindigkeit vorliegt.

- Mit der Möglichkeit der selektiven Kundenansprache steigt die Kundensegmentierung.

- Die Erreichbarkeit zu jeder Zeit ist bei mobilen Endgeräten als persönlicher Gegenstand sehr hoch. So sind z.B. Mobiltelefone im Durchschnitt 14 Stunden pro Tag eingeschaltet [So04]. Für einige TV- oder E-Mail-Nutzer ist auch eine hohe

[1] BMWA: Bundesministerium für Wirtschaft und Arbeit

Erreichbarkeit gegeben, wenn sie lange Zeit über den Tag hinweg parallel zu anderen Aktivitäten das Fernsehgerät eingeschaltet haben oder automatisiert ihre E-Mails in kurzen Zeitabständen abrufen.

- Die Ortsabhängigkeit war bisher nur bei Printmedien gegeben (z.B. Verbreitungsgebiete von Zeitungen). Mobile Endgeräte sind aber i.d.R. sehr viel genauer ortbar und bieten daher differenziertere Möglichkeiten für ortsabhängige Werbung.

| **Merkmale** / **Werbeträger** | Reichweite | Möglichkeit zur Interaktion | Kundensegmentierung | Jederzeit erreichbar | Ortsabhängig anpassbar |
|---|---|---|---|---|---|
| TV |  |  |  |  |  |
| Printmedien |  |  |  |  |  |
| Internet |  |  |  |  |  |
| E-Mail |  |  |  |  |  |
| Mobiles Endgerät |  |  |  |  |  |

Tabelle 1: Merkmale verschiedener Werbeträger

## 2.2 Spannungsfeld: Anonymität versus Informationsbedürfnis

Ein Kunde, der prinzipiell Werbung erhalten möchte, zieht es vor, wenn diese auf seine Bedürfnisse zugeschnitten ist. Er will die Werbung gerne einfach und bequem erhalten und dabei bestimmen, wann, wie und wo er beworben wird. Trotzdem will er seine Anonymität wahren.

Ein werbetreibendes Unternehmen verfolgt die Absicht, seine Werbung ohne Streuverluste zielgerichtet an potenzielle Kunden zu senden. Dies ist um so besser möglich, je mehr Informationen es über seine bestehenden Kunden und mögliche potenzielle Interessenten hat.

Damit liegt ein Spannungsfeld zwischen der vom Kunden bevorzugten Anonymität und den Informationsbedürfnissen der werbetreibenden Unternehmen vor.

Bei Betrachtung der Werbeträger in Tabelle 1 fällt bezüglich der Kundenanonymität auf, dass diese nur beim Fernsehen und den Printmedien gegeben ist. Bei Verwendung von One-to-Many-Kommunikationsverfahren wie Cell Broadcasting oder Digital Video Broadcasting (DVB) zu mobilen Endgeräten ist eine Kundenanonymität unter Verlust der Personalisierungsmöglichkeit gegeben. Bei allen anderen Werbeträgern, wie auch dem mobilen Endgerät, ist der Kunde für das werbetreibende Unternehmen nicht mehr anonym.

## 2.3 Potenziale des mobilen Marketings

Mobiles Marketing auf mobilen Endgeräten eröffnet neue Möglichkeiten für die Werbung. Das Mobiltelefon, mit über 64 Millionen registrierten Teilnehmern in Deutschland im Jahr 2003 [Re04] das am weitesten verbreitete mobile Endgerät, zählt zu den persönlichen Gegenständen der Nutzer, wodurch die positive Reaktion auf mobile Werbung begünstigt wird. Damit bieten mobile Endgeräte einen direkten Kontakt zu einzelnen Zielgruppen, sogar zu einzelnen Personen, so dass ein zielgerichtetes One-to-One-Marketing mit minimalen Streuverlusten möglich wird [Li02].

Durch die Möglichkeit, das mobile Endgerät mit sich zu führen, ist ortsabhängig anpassbare Werbung mit hoher Erreichbarkeit realisierbar (vgl. Tabelle 1). Jedoch muss dem Nutzer die Möglichkeit gegeben werden, Zeiten festzulegen, in denen er nicht durch Werbung gestört werden möchte. Ebenso muss die Einwilligung des Kunden nach den Grundsätzen des Permission Marketings eingeholt werden [Go99]. Wird dies berücksichtigt, so ist es möglich, mit mobilem Marketing höhere Responseraten zu erzielen als mit anderen Werbeformen, wie z.B. Direkt-Mailing [Li02].

Mobiles Marketing kann damit zu den Medien gezählt werden, welche sich für kostensparende Kundengewinnung als auch -bindung eignen, eine effiziente Beurteilung von Marketing- und Werbeaktionen erlauben und Streuverluste minimieren [Li02].

Problematisch erweisen sich zwei Aspekte: Zum einen ist dies die gestalterische Limitierung durch die mobilen Endgeräte (z.B. Displaygröße). Dies kann jedoch auch einen gewissen Reiz bzw. eine Herausforderung für die Werbebranche darstellen, Werbung kurz und prägnant zu fassen und dennoch Aufmerksamkeit zu erregen. Zum anderen ist zu befürchten, dass der Kunde für auf ihn abgestimmte und an den momentanen Aufenthaltsort angepasste Angebote und Werbung seine Anonymität preisgeben muss und damit zum gläsernen Kunden wird.

# 3 Grundlagen für Kundenanonymität

## 3.1 Begriffsdefinitionen

### Anonymität und Pseudonymität

Eine juristische Definition von Anonymität findet man im § 3 Abs. 6 des Bundesdatenschutzgesetzes (BDSG): „Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können."

Bei Pseudonymen hingegen existiert eine Abbildung (Korrespondenz-Regel), die das Pseudonym einer einzelnen Person zuordnet (BDSG § 3 Abs. 6a): „Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren."

Pseudonymität kann noch weiter in Personen- und Rollenpseudonyme unterteilt werden [Pf90]: Rollenpseudonyme werden im Gegensatz zu Personenpseudonymen nur für einen klar abgegrenzten Zweck verwendet. Wird ein Rollenpseudonym nur für eine einzige Transaktion verwendet, so spricht man von einem Transaktions-Pseudonym, ansonsten von einem Geschäftsbeziehungs-Pseudonym.

Die Personenpseudonyme dagegen sind nicht auf nur einen Zweck beschränkt. Je nach Umfang des Personenkreises, dem bekannt ist, welche Identität sich hinter einem Pseudonym verbirgt, wird zwischen öffentlichen (jeder kann es in Erfahrung bringen, z.B. eine auf einer Webseite veröffentlichte E-Mail-Adresse) und nicht-öffentlichen Pseudonymen (eine E-Mail-Adresse, die nur ein eingeschränkter Personenkreis kennt) unterschieden.

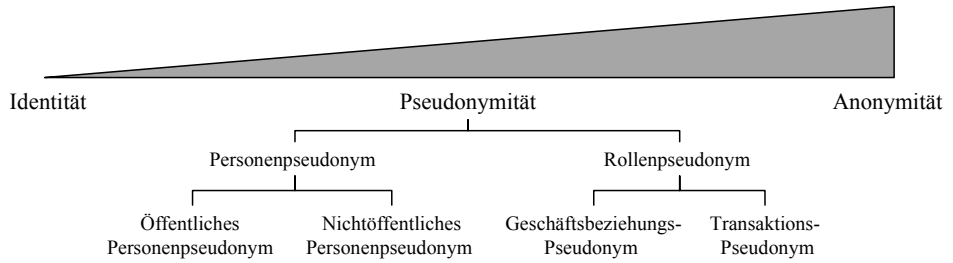


Abbildung 1: Kontinuum zwischen Identität und Anonymität

In Abbildung 1 sind alle diese Stufen der Pseudonymität mit steigendem Anonymisierungsgrad eingezeichnet; je höher dieser ist, desto schwieriger ist es, auf die tatsächliche Identität der Person zu schließen.

**Anonymität in öffentlichen Netzen**

Die bekannten Architekturen und Systeme zur Gewährleistung anonymisierter individueller Kommunikation in öffentlichen Netzwerken (etwa Chaum'sche Mix-Kaskaden [Ch81], Cyberpunk- und Mixmaster-Remailer [Bl00], AN.ON-Projekt [An04]) basieren auf der Mitwirkung mindestens einer vertrauenswürdigen Drittpartei, über die Nachrichten verschickt werden. Solch ein vertrauenswürdiger Intermediär könnte z.B. ein Datenschutzbeauftragter, eine Bürgervereinigung oder ein Unternehmen sein, dem die notwendige Diskretion zugeschrieben wird.

**Personalisierung und Profilierung**

Personalisierung ist die Anpassung oder Ausrichtung von Diensten und Informationen auf die spezifischen Anforderungen einer Person. Die Personalisierung ist damit ein Teilbereich der kontextsensitiven Anpassung von Diensten. In der Regel werden zur Personalisierung Profilinformationen benötigt.

Profilierung ist „ein kontinuierlicher Lernprozess, bei dem das Wissen über den Kunden […] ständig erweitert und aktualisiert wird" [Kl00]. Bei der aktiven Profilierung werden diese Profilinformationen durch den Nutzer selbst eingepflegt, etwa unter Verwendung eines Abfrageschemas zur Erfassung der besonderen Interessengebiete. Bei der passiven Profilierung hingegen wird das Profil ohne Zutun des Nutzers aus dessen Besuchs- und Transaktionsdaten generiert.

Die aktive Profilierung bedeutet für den Nutzer etwas mehr Aufwand, ist aber dafür ihm gegenüber vollkommen transparent.

**Kontextsensitivität von mobilen Diensten**

Unter Kontext im Zusammenhang mit mobilen Applikationen verstehen wir eine Menge von Informationen, um die Situation einer Person zu beschreiben [Sc94]. Als wohl prominentestes Beispiel sind hier die „Location Based Services" zu nennen, bei denen der aktuelle Aufenthaltsort eines Nutzers als Kontext-Information ausgewertet wird, um z.B. ortsbezogene Werbung oder Routenplanung zu verwirklichen [Kö03]. Technisch kann diese Ortsbestimmung etwa über die Funkzelle, in der sich das Endgerät des Nutzers gerade eingebucht hat, oder über eine GPS-Ortung bestimmt werden. Darüber hinaus sind aber noch weitere Kontext-Parameter denkbar, z.B. Zeitpunkt, physiologische Größen wie die Pulsfrequenz oder Körpertemperatur, Hintergrundgeräuschpegel, verfügbare technische Infrastruktur oder die soziale Situation. Da mobile Endgeräte aufgrund ihrer geringen Größe oft nur über eine sehr eingeschränkte Nutzerschnittstelle verfügen, kommt der Erfassung und Auswertung des Kontextes insbesondere im Zusammenhang mit der Benutzerfreundlichkeit eine besondere Bedeutung zu, da dem Anwender so unnötige Eingaben erspart werden können.

## 3.2 Rechtliche Grundlagen

Die gesetzlichen Vorgaben für die Kundenanonymität in Deutschland sind sehr weit reichend. Diese sind nicht in einem kompakten Gesetzeswerk zusammengefasst, sondern auf eine Vielzahl von Gesetzen und Verordnungen verteilt. Sie beziehen sich auf die personenbezogen Daten, welche im Bundesdatenschutzgesetz definiert werden, als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

Für den Anwendungsfall der Werbung auf mobilen Endgeräten in Deutschland sind vor allem das Bundesdatenschutzgesetz und das Gesetz über den Datenschutz bei Telediensten maßgebend.

**Bundesdatenschutzgesetz**

Das Bundesdatenschutzgesetz (BDSG) von 1990 wurde zuletzt im Jahr 2003 geändert. Der Zweck dieses Gesetzes ist es, den Anwender davor zu schützen, dass er durch den Umgang mit seinen eigenen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Es gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch öffentliche Stellen sowie für nicht-öffentliche Stellen, wenn sie die Daten in oder aus Dateien geschäftsmäßig oder für berufliche bzw. gewerbliche Zwecke verarbeiten oder nutzen. Für die Anwendbarkeit des Gesetzes steht nicht mehr der Zweck der Datenverarbeitung im Vordergrund, sondern vielmehr die Art und Weise, wie die Daten verarbeitet werden.

Der 2003 neu eingefügte § 3a zur Datenvermeidung und Datensparsamkeit schreibt in Satz 2 vor, dass bei der Gestaltung und Auswahl von Datenverarbeitungssystemen von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen ist, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Hierbei geht es in erster Linie darum, das Mitführen der vollen Identität Betroffener während der eigentlichen Datenverarbeitungsvorgänge zu reduzieren, soweit dies technisch möglich und sachgerecht ist [Du02].

§ 30 BDSG regelt die geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung in anonymisierter Form. Darin wird vorgeschrieben, dass die Merkmale gesondert zu speichern sind, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies für die Erfüllung des Zwecks der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist. Hier wird die für Werbung und Marktforschung wichtige Möglichkeit der Anonymisierung und Pseudonymisierung nochmals ausführlich geregelt. Die strengen Regelungen des § 29 BDSG für die nicht anonymisierte Datenerhebung und -speicherung zum Zweck der Übermittlung werden dabei explizit ausgeschlossen [Du03].

**Gesetz über den Datenschutz bei Telediensten – Teledienstedatenschutzgesetz**

Das Teledienstedatenschutzgesetz (TDDSG) dient dem Schutz personenbezogener Daten der Nutzer von Telediensten im Sinne des Teledienstegesetzes (TDG) bei der Erhebung, Verarbeitung und Nutzung dieser Daten durch Diensteanbieter. Es regelt, dass personenbezogene Daten vom Diensteanbieter zur Durchführung von Telediensten nur dann erhoben, verarbeitet und genutzt werden dürfen, wenn dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat. Das TDDSG legt weiterhin fest, dass der Diensteanbieter die für die Durchführung von Telediensten erhobenen personenbezogenen Daten für andere Zwecke nur verarbeiten und nutzen darf, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat. Des Weiteren muss der Diensteanbieter dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist und ihn ebenfalls über diese Möglichkeit unterrichten.

Wenn kein Widerspruch des Nutzers vorliegt, darf der Diensteanbieter gemäß § 6 Abs. 3 TDDSG für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Teledienste Nutzungsprofile erstellen, wenn hierbei Pseudonyme verwendet werden. Die Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Der Nutzer muss in jedem Fall aber über sein Widerspruchsrecht informiert werden, und zwar im Rahmen der obligatorischen Unterrichtung nach § 4 Abs. 1 TDDSG.

# 4 Lösungsansatz: MoMa – Mobiles Marketing

## 4.1 Systemarchitektur von MoMa

Jeder Kunde des MoMa-Systems (siehe Abbildung 4) hat eine eindeutige Nutzer-ID, unter der er auf dem Anonymisierungs-Server mindestens ein Benachrichtigungsprofil hinterlegt. Ein solches Benachrichtigungsprofil legt ein Medium zur Benachrichtigung fest (SMS, MMS, E-Mail, Text-to-Speech, etc.) sowie eine passende End-Adresse (Mobilfunk-Nummer für SMS/MMS, E-Mail-Adresse für E-Mail, etc.) und evtl. weitere zusätzliche Angaben, z.B. dass von 20.00 bis 9.00 Uhr keine Text-to-Speech-Anrufe vorgenommen werden sollen. Unter Verwendung der Benachrichtigungsprofile richtet der Kunde seine eigentlichen Nutzerprofile ein; es handelt sich hierbei um aktive Profilierung.

Zur Einstellung eines Auftrags (Abbildung 2 und 3) definiert der Nutzer seine Wünsche anhand der vorgegebenen Kategorien und Attribute und verschlüsselt seine Nutzer-ID und einen Hinweis auf das zu verwendende Benachrichtigungsprofil mit dem öffentlichen Schlüssel des Anonymisierungs-Dienstes. Zur Sicherung der Public-Key-

Verschlüsselung[2] [Ri78] ist es hierbei notwendig, diese Informationen vor der Verschlüsselung um eine zufällig erzeugte und eindeutig abtrennbare Zeichenkette zu erweitern. Der Auftrag wird dann zusammen mit der verschlüsselten Nutzer-ID, den notwendigen Teilen des gewählten Nutzerprofils und den relevanten Kontextinformationen über den Anonymisierungs-Dienst an den MoMa-Server weitergeleitet. Über diesen Umweg wird eine direkte Kommunikations-Beziehung vermieden, so dass der MoMa-Server nicht über die IP- oder MSISDN-Adresse Rückschlüsse auf die Identität des Auftraggebers ziehen kann. Da nur der Anonymisierungs-Server mit seinem privaten Schlüssel die Nutzer-ID entschlüsseln kann, ist es dem MoMa-Server nicht möglich, Rückschlüsse auf die Identität des Auftraggebers zu ziehen.


(a) Profilauswahl (b) Katalog (c) Attributspezifikation

Abbildung 2: Screenshots der MoMa-Client-Applikation

Bei der Formulierung des Auftrags greift die Client-Anwendung des Kunden bei Bedarf auf die persönlichen Kontext-Dienste zurück, etwa die Bestimmung des aktuellen Aufenthaltsortes mittels GPS-Ortung. Diese Kontext-Informationen kann der MoMa-Server nicht direkt abfragen, da ihm sonst die Identität des Nutzers bekannt sein müsste. Die Parameter des persönlichen Kontextes werden deshalb auch nach Einstellung des Auftrages vom mobilen Endgerät zyklisch abgefragt; wird dabei eine Änderung eines für einen Auftrag relevanten Parameters über einen definierten Schwellwert hinaus festgestellt, muss dieser Auftrag aktualisiert werden. Hierzu wird die bei der Auftragserstellung erzeugte Chiffre der Kunden-ID mitsamt den neuen Auftragsdaten erneut über den Anonymisierungs-Dienst an den MoMa-Server übermittelt. Dieser sucht dann nach dem Auftrag mit dieser Chiffre und ersetzt ihn.

[2] Prinzipiell kann auch ein rechentechnisch günstigeres symmetrisches Verschlüsselungsverfahren zum Einsatz kommen, wenn die einmalige sichere Übermittlung des symmetrischen Schlüssels gewährleistet ist. In diesem Fall ist ebenfalls die Zufallsinformation mitzuverschlüsseln.

Auf der anderen Seite stellt der Werbetreibende seine ebenfalls anhand der Kataloge spezifizierten Angebote ins System ein; er kann noch zusätzliche Informationen (z.B. Fotos einer angebotenen Mietwohnung, Informationen über sein Unternehmen) über den Publishing- und Rendering-Server verfügbar machen. Sein Angebot ist nicht anonymisiert. Bei der Suche von zueinander passenden Aufträgen und Angeboten fragt der MoMa-Server die je nach Auftrag benötigten öffentlichen Kontext-Informationen (z.B. Wetter- oder Verkehrslage in einem bestimmten Gebiet, Börsenkurse, etc.) vom Kontext-Server ab. Dieser Suchvorgang wird durch bestimmte System-Ereignisse angestoßen, etwa das Eintreffen neuer Aufträge/Angebote oder die Änderung relevanter öffentlicher Kontext-Parameter.


(a) Katalog auf P800 (b) Katalog PC-Client

Abbildung 3: MoMa-Client auf mobilem Endgerät und PC

Für jede gefundene passende Kombination eines Auftrags und eines Angebots wird die Angebots-ID samt der verschlüsselten Nutzer-ID an den Anonymisierungsdienst übermittelt. Dieser entschlüsselt die Chiffre, ermittelt so den Nutzer und das gewünschte Benachrichtigungsprofil und lässt beim Publishing & Rendering-Server eine Nachricht erzeugen, die ein zum ermittelten Endgerätetyp passendes Format hat und das Angebot beschreibt; ist z.B. SMS als Medium zur Benachrichtigung gewünscht, stehen nur 160 Zeichen hierfür zur Verfügung. Hierbei werden aber keine Adress-Informationen

weitergegeben. Letztendlich verschickt der Anonymisierungs-Dienst diese Nachricht an den Kunden, der dann entscheiden kann, ob er zur Wahrnehmung des Angebotes den Werbetreibenden kontaktiert.

Die Rolle des Betreibers im laufenden Betrieb beschränkt sich im Wesentlichen auf die Administration der Kataloge und die Durchführung der Abrechnung, wobei auch verschiedene statistische Auswertungen abgefragt werden können.

Die MoMa-Architektur gewährleistet, dass der Kunde gegenüber dem Werbetreibenden völlig anonym ist; trotzdem ist personalisierte Werbung ohne Streuverluste möglich. Durch die physikalische Trennung des Anonymisierungs-Dienstes vom eigentlichen MoMa-System wird zusätzliche Sicherheit erreicht, da der Werbetreibende so nicht auf die Komponente Zugriff hat, in der die Benachrichtigungsprofile gespeichert sind.

Wird der Anonymisierungs-Dienst von einer „vertrauenswürdigen Drittpartei“ betrieben, ist der Kunde darüber hinaus gegenüber dem Betreiber des MoMa-Dienstes pseudonymisiert: die Nutzer-ID wird nur für das MoMa-System verwendet und ist deshalb ein Rollenpseudonym. Da innerhalb des eigentlichen Kernsystems die Nutzer-ID nur verschlüsselt vorliegt, kann diese Chiffre sogar als Transaktions-Pseudonym aufgefasst werden, was die höchste Stufe der Pseudonymität darstellt (vgl. Abbildung 1). Die in Kapitel 4.2 erörterten rechtlichen Anforderungen werden damit erfüllt. Um einen Angriff auf den Anonymisierungsdienst zu erschweren, könnte dieser in zwei eigenständige und von voneinander unabhängigen Parteien betriebene Komponenten aufgeteilt werden: Eine Komponente hat nur Kenntnis von den Nachrichtenformaten (aber nicht der Endadressen) der einzelnen Benachrichtigungsprofile und leitet alle Aufträge an den MoMa-Server weiter. Die andere Komponente kennt zwar die Endadressen der einzelnen Benachrichtigungsprofile, hat aber keine Kenntnis über alle Aufträge der Endnutzer.

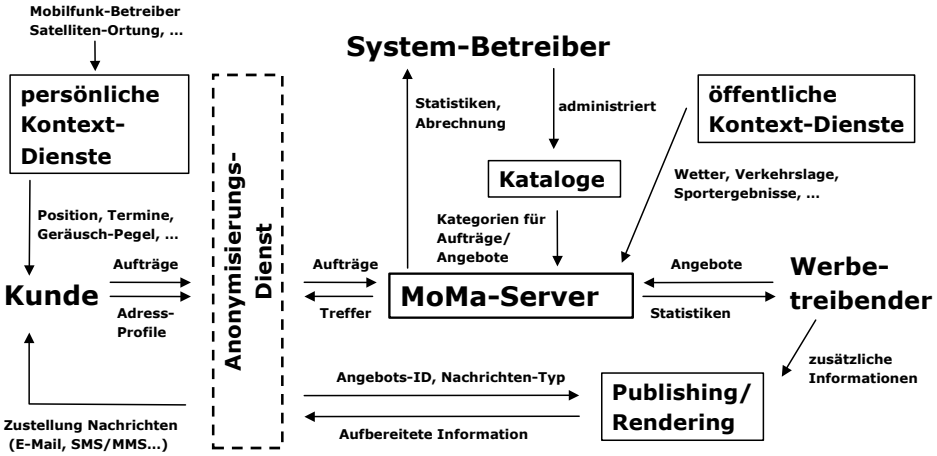


Abbildung 4: Vereinfachte schematische Darstellung des MoMa-Systems

## 4.2 Missbrauchspotenzial der Anonymität

Softwaresysteme, die Anonymität gewährleisten, setzen sich fast immer dem Vorwurf aus, u.U. auch illegale Aktivitäten zu begünstigen. Im Falle einer mobilen Marketing-Plattform wäre hier in erster Linie die Anbahnung illegalen Handels (Drogen, Waffen, Hehlerware, etc.) denkbar. Bei MoMa wird dies aber schon dadurch erschwert, dass die eingestellten Angebote und Anfragen den vorgegebenen Kategorien entsprechen müssen, der Systembetreiber wird schlichtweg keine Kategorien für illegale Produkte (z.B. "Schnellfeuerwaffen") und Dienstleistungen einrichten.

Zur Umgehung dieser Maßnahme besteht allerdings die Möglichkeit der Verwendung von Decknamen (etwa "Pizza X" für eine bestimmte Droge) seitens einschlägiger Nutzergruppen. Da das werbetreibende Unternehmen sich allerdings schon alleine wegen der Abrechnung bei der Anmeldung dem Systembetreiber gegenüber entsprechend authentifizieren muss, wäre es im Rahmen entsprechender Strafverfolgungsmaßnahmen schnell identifizierbar.

## 4.3 Geschäftsmodell

Das Geschäftsmodell von MoMa sieht vier Rollen vor:

- Kunde
- MoMa-Systembetreiber
- Vertrauenswürdige Drittpartei
- Werbetreibendes Unternehmen

Entsprechend des gewählten Benachrichtigungsprofils erhält der Kunde für seinen im MoMa-System platzierten Auftrag über den Vermittlungsdienst der vertrauenswürdigen Drittpartei die Werbung kostenfrei. Die Nutzung des MoMa-Systems (Konfiguration der Profile, Einstellung von Aufträgen) ist für den Kunden bis auf die Verbindungsentgelte seines Providers ohne Kosten.

Das werbetreibende Unternehmen formuliert sein Angebot gemäß der Kategorien des vorgegebenen Katalogs und bezahlt nur für tatsächlich erfolgte Kundenkontakte, wobei diese Kontakte in Abhängigkeit der jeweiligen Kategorie unterschiedlich bepreist sein können (z.B. kann für ein Vermittlungsangebot einer Mietwohnung ein höherer Kontaktpreis angesetzt werden als für das Bewerben der „Happy Hour“ eines Restaurants). Mit diesem Preismechanismus soll verhindert werden, dass die werbetreibenden Unternehmen ihre Angebote an möglichst viele Kunden in Form von Lockangeboten schicken und die Kunden von Angeboten überhäuft werden. Für die Bezahlung der Dienstleistung des MoMa-Systembetreibers können unterschiedliche Modelle zum Einsatz kommen: Einzelfallbezahlung, Monatspauschale sowie diverse Mischformen im konkreten Fall. Ebenso kann das werbetreibende Unternehmen anonyme Auswertungen beim MoMa-Systembetreiber kaufen, welche Marktinformationen enthalten (z.B. Winterschuhnach-

frage im November in der Region Stuttgart). Der Vorteil dieser Auswertung liegt in der Aktualität der Daten und der Möglichkeit der regionalen Begrenzung. Diese Informationen kann das werbetreibende Unternehmen in der Preis- und Produktgestaltung und der Beschaffungsplanung einsetzen. Für das werbetreibende Unternehmen stehen diese Gesamtkosten qualifizierten Kundeninteressen gegenüber, da durch die Übereinstimmung von Angebot und Nachfrage Streuverluste auf ein Minimum reduziert werden können. Diese Form der Werbung stellt damit für den Werbetreibenden eine Alternative bzw. Ergänzung zu den üblichen Werbeformen dar.

Der vertrauenswürdigen Drittpartei wird der Betrieb des Anonymisierungs-Dienstes vom MoMa-Systembetreiber entweder transaktionsabhängig oder pauschal vergütet.

## 5 Zusammenfassung

Zusammenfassend kann festgehalten werden, dass durch die Gestaltung der MoMa-Systemarchitektur, die Einführung einer dritten vertauenswürdigen Partei sowie der Bepreisungsstrategie der Katalogkategorien mobiles Marketing unter Wahrung der Kundenanonymität bzw. Pseudonymität möglich ist. Die im MoMa-System umgesetzte aktive Profilierung ermöglicht das Zuschneiden der Werbung auf die vom Kunden angegebenen Bedürfnisse. Bei dieser Personalisierung wird dabei der aktuelle Kontext berücksichtigt.

Bezogen auf das in Kapitel 2.2 beschriebene Spannungsfeld lässt sich damit festhalten, dass das MoMa-System die Kundenwünsche, dessen Anonymität und gleichzeitig das Informationsbedürfnis der werbetreibenden Unternehmen berücksichtigt.

## Literaturverzeichnis


[An04] Website http://anon.inf.tu-dresden.de, Abruf am: 20.09.2004.

[Bl00] Bleich, H.: Selbstverdunkelung – Anonymes Mailen in der Praxis, c't 16/2000, S. 156-159.

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

[Du02] Duhr, E.; Naujok, H.; Peter, M.; Seiffert, E.: Neues Datenschutzrecht für die Wirtschaft, Teil 1. Datenschutz und Datensicherheit, 2002.

[Du03] Duhr, E.; Naujok, H.; Danker, B.; Seiffert, E.: Neues Datenschutzrecht für die Wirtschaft, Teil 2. Datenschutz und Datensicherheit, 2003.

[Fe00] Federrath, H.; Berthold, O.; Köhntopp, M.; Köpsell, S.: Tarnkappen fürs Internet – Verfahren zur anonymen und unbeobachteten Kommunikation, c't Heft 16/2000, S. 148-155.

[Go99] Godin, S.: Permission Marketing: Turning Strangers into Friends, and Friends into Customers. Simon and Schuster, 1999.

[Kl00] Klein, S.; Güler, S.; Lederbogen, K.: Personalisierung im elektronischen Handel, Wisu 01/2000, S. 88-94.

[Kö03] Kölmel, B.: Location Based Services. In: Pousttchi, K.; Turowski, K. (Hrsg.): Mobile Commerce: Anwendungen und Perspektiven, Proceedings zum 3. Workshop Mobile Commerce, Bonn, 2003, S. 88-101.

[Li02] Lippert, I.: Mobiles Marketing. In: Gora, W.; Röttger-Gerik, S. (Hrsg.): Handbuch Mobile-Commerce: Technische Grundlagen, Marktchancen und Einsatzmöglichkeiten. Springer, Berlin, 2002.

[Pf90] Pfitzmann, A.; Diensteintegrierte Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz. IFB 234, Springer-Verlag, Heidelberg, 1990.

[Sc94] Schilit, B. N.; Adams, N. I., Want, R.: Context-Aware Computing Applications. Proceedings of the Workshop on Mobile Computing Systems and Applications, Santa Cruz, CA, December 1994, IEEE Computer Society, pp. 85-90.

[SJ01] Schmich, P., Juszczyk, L.: Mobile Marketing – Verlust der Privatsphäre oder Gewinn für Verbraucher? In: Kahmann, M. (Hrsg.): Mobile Business. Symposion, Düsseldorf, 2001.

[Re04] Regulierungsbehörde Telekommunikation und Post: Jahresbericht 2003 – Marktdaten der Regulierungsbehörde für Telekommunikation und Post, 2004.

[Ri78] 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.

[So04] Sokolov, D.: Rabattstreifen per SMS. Spiegel Online, 20.10.2004. http://www.spiegel.de/wirtschaft/0,1518,323749,00.html, Abruf am: 01.12.2004.