Universität Regensburg
Wirtschaftswissenschaftliches
Prüfungsamt

SS 2004

Datenschutzfreundliche Gestaltung von kostenpflichtigen, ortsabhängigen, mobilen Diensten

Diplomarbeit gemäß
§ 25 der Diplomprüfungsordnung
vom 3. August 2000
Prof. Dr.-Ing. Hannes Federrath
Lehrstuhl für Wirtschaftsinformatik IV

Vorgelegt von:
Falk Uebernickel
Vitusstraße 2, 6.29
93051 Regensburg
9. Fachsemester
Wirtschaftsinformatik

Eingereicht am:
28. Mai 2004

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

Kapitel 1

Einleitung

Motivation und Ziele

Mobile Technologien wie GSM, Wireless LAN, Bluetooth etc. fanden in den letzten Jahren weltweit eine starke Verbreitung. Eine auf diesen Technologien basierende Anwendung sind Location Based Services (LBS). Unter Zuhilfenahme von Ortungsverfahren, wie z.B. GPS oder E-OTD, können LBS ihren Nutzern zeit-, positions- und personenbezogene Dienste anbieten. Anbieter solcher Dienste können sowohl kommerzielle und nicht kommerzielle Einrichtungen, als auch Einzelpersonen sein. Einer weiten Verbreitung dieser Anwendung stehen momentan jedoch datenschutzrechtliche Bedenken entgegen. So ist es zur Zeit für einen LBS-Diensteanbieter sehr leicht möglich Bewegungsprofile seiner Kunden zu erstellen und weiter zu verwerten. Auch der Gesetzgeber hat diese Missstände wahrgenommen und versucht durch gesetzliche Regelungen unerwünschte Handlungen zu unterbinden. Dennoch greifen Gesetze i.d.R. nur ex post, wenn die Straftat bereits begangen und Personen geschädigt wurden. Aus dieser Problematik heraus läßt sich begründen, warum es notwendig ist, Verfahren zu entwickeln die ex ante wirken. Im wissenschaftlichen Umfeld finden sich einige Lösungsansätze um dem Problem der gegenüber dem Kunden „unbemerkten“ Datenerhebung Einhalt zu gebieten. Allerdings sind diese Vorschläge für den Endbenutzer oft noch unzureichend praktikabel und transparent und / oder es fehlen Möglichkeiten datenschutzfreundliche Bezahlvorgänge implementieren zu können. Auch aus wirtschaftlicher Sicht lassen sich datenschutzfreundliche Methoden wie Anonymisierung und Pseudonymisierung vertreten. Der Einsatz dieser Methoden stärkt das Vertrauen der Kunden in das Unternehmen, was wiederum direkten Einfluß auf die Kundenbindung haben kann.

Ziel dieser Diplomarbeit ist es, die vielfältigen technischen Gestaltungsmöglichkeiten von Location Based Services zu untersuchen und geeignete Vorschläge für eine datenschutzfreundliche Realisierung oder Umgestaltung aufzuzeigen. Des Weiteren sollen elektronische Bezahlverfahren auf ihre Tauglichkeit für den Einsatz in LBS-Anwendung analysiert werden.

Aufbau der Arbeit

Um die oben beschriebene Zielstellung erreichen zu können gliedert sich die Arbeit wie folgt. Kapitel 2 geht zunächst auf die Fragestellung ein, was überhaupt ortsabhängige Dienste[1] sind

[1] engl. Location Based Services

und erarbeitet anschließend eine Grunddefinition. Darauf aufbauend werden die mit Location Based Services eng verbundenen Positionsbestimmungsverfahren sowohl für den Innen- als auch Außenbereich angesprochen und klassifiziert. Des Weiteren stellt dieses Kapitel potentielle Kommunikationsnetze in einem Überblick vor und diskutiert anschließend aktuelle Anwendungsfelder von Location Based Services. Den Abschluss bildet eine Referenzarchitektur, die die Grundstruktur verschiedener Location Based Services aufzeigt.

Kapitel 3 versucht die Begriffe „Datenschutz“ und „Privacy“ in Verhältnis zueinander zu setzen, um darauf aufbauend die aktuellen Sicherheits- als auch Datenschutzvorkehrungen rund um ortsabhängige Dienste aufzuzueigen. Hierfür wird insbesondere auf die rechtliche Situation in Deutschland bezug genommen und der bisherige Einsatz von Techniken und Verfahren zur Erhöhung des Datenschutzes skizziert. Abschließend werden aus der Verwendung von ortsabhängigen Diensten resultierende Bedrohungen abgeleitet.

Die Kapitel 4 und 5 gehen auf Techniken und Verfahren zur Erhöhung der Datenschutzfreundlichkeit von ortsabhängigen Diensten und Bezahlverfahren näher ein. Dabei konzentriert sich Kapitel 4 schwerpunktmäßig auf die Vermeidung von Daten am Entstehungsort. Aber auch die Probleme der Datenverteilung und des Selbstdatenschutzes finden mit Berücksichtigung. Abgeleitet aus den gesammelten Ergebnissen wurde in Kapitel 4 eine Gesamtansicht aller verfügbaren Schutzmöglichkeiten erarbeitet. Kapitel 5 leitet einen Katalog zur Auswahl geeigneter Bezahlverfahren für LBS her und wendet diesen anhand einiger Beispiele an.

Kapitel 6 erarbeitet abschließend einen Vorschlag bestehend aus zwei verschiedenen Datenschutzpaketen der in Kombination mit intelligenten Identitätsmanagementprogrammen und -systemen zur Erhöhung der Datenschutzfreundlichkeit beiträgt.

Den Abschluss der Arbeit bildet eine Zusammenfassung (Kapitel 7) wo alle erarbeiteten Ergebnisse in kurzer Form dargestellt und weitere Forschungsrichtungen aufgezeigt werden.

Kapitel 2

Grundlagen von Location Based Services

2.1 Begriffsbestimmung

Für Location Based Services (LBS)[1] findet man in der Literatur viele unterschiedliche Definitionen. Grund für diese uneinheitliche Begriffsauffassung sind meist verschiedene Blickwinkel auf LBS. Wirtschaftliche Definitionen legen zum Beispiel besonderen Wert auf die Zuordnung von LBS in die Bereiche M-Business und M-Commerce. Technische Definitionen hingegen beziehen sich meist nur auf eine Netz- oder Positionsbestimmungstechnologie. Folgende Definition ist auf den Seiten [95] des UMTS-Forums zu finden:

> *„Mobile services and applications that make use of the subscriber´s geographical location. These could include mapping or localised shopping and entertainment services.“*[95]

Sehr allgemein gehalten, spezifiziert diese Definition keine bestimmte Technologie zur Positionsbestimmung oder die Nutzung eines Netzes, über das die mobilen Dienstleistungen erbracht werden. Interessant ist jedoch der Aspekt, dass Applikationen, die lokal auf dem mobilen Endgerät (engl. Mobile Terminal) gehalten werden und Positionsdaten zur Leistungserbringung nutzen, auch zu den LBS zählen. Die Networking & Communications Group der Kingston University grenzt den Bereich der LBS wie folgt ein:

> *„Location Based Service is a service delivered over a network to a mobile client where knowledge of the clients geographical location is used to select or enhance the information supplied in response to queries.“*[69]

Im Gegensatz zur Definition des UMTS-Forums werden in dieser Definition ausschließlich Dienste zu den LBS gezählt, die über ein Netzwerk dem Endbenutzer, durch Nutzung von Positionsdaten, Leistungen erbringen. Endgeräte basierte Anwendungen werden nicht berücksichtigt. Des Weiteren zählen nur vom Benutzer direkt ausgelöste Anfragen zu den LBS, so genannte Push-Dienste (siehe Seite 16) werden ausgeklammert.

Da die Menge der Definitionen im Bereich der LBS so unterschiedlich sind, wird für die folgende Arbeit der Begriff „Location Based Service“ wie folgt definiert:

[1] *deutsch:* standortbezogene Dienste

> Standortbezogene Dienste (LBS) sind über ein Netzwerk erbrachte mobile Dienste, die unter Zuhilfenahme von positions-, zeit- und personenabhängigen Daten dem Endbenutzer Informationen bereitstellen. Darüber hinaus ist die Diensterbringung über nicht elektronische Kanäle möglich.

Die oben stehende Definition legt nicht die Methode der Positionsbestimmung und das zu verwendende Netzwerk, wie zum Beispiel GSM, Wireless LAN etc., fest. Daneben berücksichtigt die Definition, dass LBS mit ihrem gesamten Dienstleistungsspektrum nur möglich sind, wenn positions-, zeit- und personenabhängige Daten vom Endbenutzer geliefert werden. Das Fehlen von zeit- und / oder personenabhängigen Daten ermöglicht zwar immer noch das Angebot von LBS, schränkt dieses aber ein. Der Zusatz „Darüber hinaus ist die Diensterbringung über nicht elektronische Kanäle möglich.“ erfasst zusätzlich, dass angeforderte LBS-Dienstleistungen nicht notwendigerweise elektronisch zu erbringen sind. Notrufe sind hierfür das beste Beispiel. Sendet ein LBS-Nutzer einen Notruf mit Positionsinformationen aus, so erhofft er sich schnelle medizinische Hilfe oder Streifenwagen der Polizei.

2.2 Verfahren zur Positionsbestimmung

Positionsbestimmungsverfahren bilden die Grundlage von LBS. Mithilfe dieser Verfahren kann sich ein mobiler Benutzer entweder selbst orten (mobile terminal basierte Verfahren) oder durch ein drahtloses Netz orten lassen (netzbasierte Verfahren). Neben den beiden technischen Lösungen existiert die Möglichkeit der Benutzereingabe, bei der der Benutzer Positionsangaben selbst zur Verfügung stellt. Eine weitere Einteilung schlagen Hightower und Borriello vor [44]. Sie unterteilen Positionsbestimmungsverfahren in die Kategorien: Triangulation, Umgebungsanalyse und Annäherung. Unter Triangulation subsumiert man Verfahren die Lateration (Distanzbestimmung) oder Angulation (Winkelbestimmung) verwenden, beispielsweise Enhanced-Observed Time Difference (E-OTD). Die bisher nicht breitflächig verwendete Positionsbestimmungsmethode der Umgebungsanalyse versucht aus Bildausschnitten der Umgebung des Nutzers den aktuellen Standort zu berechnen. Hierzu hat die Universität Cambridge einen ersten Prototypen[2] erstellt, mit dem die aktuelle Position anhand von Umgebungsfotografien innerhalb der Stadt Cambridge auf bis zu einem Meter genau ermittelt werden konnte. Zur weiteren Verbreitung der Umgebungsanalyse als Positionsbestimmungsverfahren könnten die in vielen Mobiltelefonen integrierten Kameras beitragen, aber dem entgegen steht der extrem hohe Erfassungsaufwand von dreidimensionalen Modellen einer gesamten Stadt. In die dritte Kategorie, die Annäherungsverfahren, fallen mehrere verschiedene Ortungsmethoden. Das einfachste Annäherungsverfahren ist das Berühren von Sensoren (Knopfdruck), in Verbindung mit der Eingabe oder Übertragung eines identifizierenden Merkmals. Eine weitere Ortungsmethode in dieser Kategorie ist das automatische Erkennen von speziellen Abzeichen (engl. Tags), sofern sie sich im Abstrahlbereich einer Antenne befinden. Bekanntestes Beispiel ist der so genannte RF-ID Tag (Radio Frequency Identification Tag), mit dem sich nicht nur Personen sondern auch Gegenstände, wie Pakete, Waren etc. verfolgen lassen.

Des Weiteren kann man zwischen relativen und absoluten Positionskoordinaten unterscheiden. Absolute Positionsangaben, wie sie vom Global Positioning System (GPS) berechnet werden, beziehen sich auf ein gemeinsam genutztes Koordinatensystem, wie zum Beispiel die

[2] siehe http://www.heise.de/tp/deutsch/inhalt/lis/17180/1.html, Abruf am: 15.04.2004

Längen- und Breitengrade der Erde. Somit liefern alle GPS-Endgeräte an ein und demselben Punkt theoretisch immer die exakt gleiche Position. Relative Koordinaten hingegen sind Positionsangaben wie: *in der Küche* oder *in der Nähe des nächsten Briefkastens* [43, S. 58]. Jedes Endgerät kann ein eigenes Koordinatensystem besitzen. Eine Eigenschaft absoluter (physischer) Koordinaten ist, dass sie leicht in relative Koordinaten umgerechnet werden können. Eine Umkehrung ist nur bedingt möglich (siehe Kapitel 4.1.4, Seite 40).

Zur Erhöhung der Übersichtlichkeit folgt eine tabellarische Zusammenfassung (Tabelle 2.1) der im Anschluß daran dargestellten Positionsbestimmungsverfahren. Zu beachten ist, dass die hier vorgenommene Abgrenzung in terminalbasierte und netzseitige Ortungsverfahren unscharf ist und beispielsweise Positionsbestimmungsverfahren auf Basis von Signalstärkemessungen sowohl terminalbasiert als auch netzseitig implementierbar sind. [90, S. 4-6]

Verfahren	**Kurzbeschreibung**
netzbasierte Positionsbestimmungsverfahren	
Zell-Id	Ein Funknetz ermittelt das Aufenthaltsgebiet eines Endgerätes anhand der Zell-Identifikationsnummer, welche jeder Funkantenne zugeordnet ist.
UL-TOA	Das Endgerät sendet an mindestens vier Funkstationen gleichzeitig ein Signal. Mithilfe einer netzseitigen Laufzeitmessung kann daraufhin die Position ermittelt werden.
terminalbasierte Positionsbestimmungsverfahren	
Benutzereingabe	Die aktuelle Position wird einfach durch den Benutzer in Form von Postleitzahlen, Straßennamen o. Ä. eingegeben.
Satellitengestützte Ortung	Ein Netz aus Satelliten sendet kontinuierlich Positionssignale zur Erde. Endgeräte können diese empfangen und über eine Laufzeitmessung in Positionskoordinaten umrechnen.
E-OTD	Das Endgerät misst die zeitliche Differenz von gleichzeitig ausgesendeten Signalen, die von verschiedenen Sendetürmen stammen. Die Zeitdifferenz, zusammen mit dem Wissen wo sich die Türme befinden, gibt Aufschluss über die aktuelle Position.
Positionssender	Ein dichtes Netz aus installierten Positionssendern strahlt ständig eine Zell-Identifikationsnummer oder die Position des Senders aus. Empfängt das Endgerät die Signale, so kennt es seine Position.
Peer-to-Peer	Endgeräte tauschen untereinander Positionsinformationen aus, um ihre eigene Position exakter bestimmen zu können.
Signalstärke	Mobile Endgeräte bilden durch Messung von Signalstärken verschiedener Sendeantennen einen „Fingerabdruck“ der aktuellen Position. Dieser wird mit vorher bestimmten Referenzdaten verglichen und dient zur Ermittlung der Position.

Tabelle 2.1: Positionsbestimmungsverfahren im Überblick

2.2.1 Netzbasierte Ortungsverfahren

Bei netzbasierten Positionsbestimmungsverfahren erfolgt die Ortung des Endgerätes ausschließlich durch das Kommunikationsnetz. Neben nur minimalen technischen Anforderungen

an die Ausrüstung der Benutzer, haben diese Methoden auch den Vorteil, dass sie sehr stromsparend und schnell sind [43, S. 58]. Besonders die zwei zuletzt genannten Punkte sind in der mobilen Kommunikation von großer Bedeutung. Mobile Endgeräte verfügen zur Zeit nur über sehr beschränkte Batteriekapazitäten, weshalb Positionsbestimmungsverfahren möglichst effizient hinsichtlich des Energieverbrauchs arbeiten sollten. Aber auch die Geschwindigkeit, mit der eine Ortung durchgeführt werden kann, ist besonders bei zeitkritischen Anwendungen sehr wichtig. Erkauft werden diese Eigenschaften meist durch die Aufgabe an Datenschutzfreundlichkeit. Da die Positionsdaten im Betreibernetzwerk ermittelt werden, hat der LBS-Nutzer keinen weiteren Einfluss auf die Verwendung der Daten. Im folgenden werden die bekanntesten Verfahren Zell-Identifikationsnummer und Uplink Time of Arrival kurz erläutert.

Zell- / Access Point-Identifikationsnummer (Cell-Id) Bei dieser Lokalisierungsmethode erfolgt die Positionsbestimmung des Endgerätes anhand der ermittelten Zell- oder Access Point-Identifikationsnummer. In der Regel strahlt eine Sendeantenne das Funksignal radial ab, wodurch die Genauigkeit des Verfahrens auf die Abstrahlentfernung (Radius) festgelegt ist. Mobilfunknetze, wie GSM oder UMTS, ermöglichen zudem eine Sektorisierung des Ausstrahlungsbereiches. Dadurch erhöht sich die Genaugkeit der Messung, sofern für jeden Sektor eine eigene Identifikationsnummer vergeben wurde. Vorteil der Zell-Id ist die Endgeräteunabhängigkeit mit der Eigenschaft, dass nur minimale Anforderungen an das Endgerät gestellt werden. Als Nachteil wäre zu nennen, dass die Messgenauigkeit stark von der Zellgröße abhängt. Innerhalb von Wireless Local Area Networks (WLANs) beträgt die Genauigkeit wenige hundert Meter. In Mobilfunknetzen können Zellgrößen aber zwischen wenigen hundert Metern bis hin zu einigen Kilometer variieren [22, S. 23]. [79, 32]

In Mobilfunknetzen bieten sich zudem die Auswertung zusätzlicher Parameter, wie Timing Advance (GSM) oder Round Trip Time (UMTS) und Angle of Arrival (Ankunftswinkel des Signals) an, mithilfe derer sich die Ortungsgenauigkeit weiter erhöhen lässt. [79][53, S. 1-9]

Neben der netzbasierten Variante könnte genauso gut eine terminalbasierte Positionsbestimmungsmethode konstruiert werden. Siehe Seite 9, Unterpunkt Positionssender.

Uplink Time of Arrival Uplink Time of Arrival (UL-TOA) ist ein weiteres netzbasiertes Ortungsverfahren. Zur Positionsbestimmung eines mobilen Endgerätes muss dieses von mindestens vier[3] Sendestationen, welche mit einer Local Mesurement Unit (LMU) ausgestattet sind, *„gesehen“* werden. Anhand der Laufzeitmessung des ankommenden Signals eines Endgerätes an der Basisstation kann die Position des Endgerätes in einem zentralen Computer berechnet werden. [32] Im Gegensatz zu der Ortung über die Zell-Id ist dieses Verfahren mit höheren Infrastrukturkosten behaftet, da das gesamte Netz mit LMU's ausgestattet werden muss. Ansonsten sind für dieses Ortungsverfahren die gleichen Vor- und Nachteile wie bei der Zell-ID zu nennen. [53, S. 5-6]

2.2.2 Terminalbasierte Ortungsverfahren

Neben den netzbasierten Positionsbestimmungsverfahren exisitieren auch eine Reihe terminalbasierter Ortungsverfahren. Charakteristisch für diese Verfahren ist, dass ausschließlich

[3] Oft wird in der Literatur das Mindestmaß von drei angegeben. Drei Sendemasten ermöglichen aber nur eine zweidimensionale Positionsbestimmung. Vier Sendemasten hingegen ein dreidimensionale. [44, S. 1]

das Endgerät seine aktuelle Position bestimmt. Dritte erhalten nur Positionsinformationen, wenn der Endgerätebenutzer dies explizit zulässt. Damit bieten terminalbasierte Ortungsverfahren ein Höchstmaß an Datenschutzfreundlichkeit [43, S. 58]. Allerdings gibt es technische Hürden bei der Installation terminalbasierter Verfahren in mobilen Endgeräten. Geringe Rechenleistung und niedrige Batteriekapazitäten hemmen aufwendige Rechenoperationen, wie sie zur Positionsbestimmung oftmals notwendig sind. Aber auch die Ausstattung der mobilen Geräte mit Zusatzgeräten die eine terminalbasierte Ortung ermöglichen, gestaltet sich aufgrund der Vielzahl an Realisierungsmöglichkeiten, wie zum Beispiel Ultraschall, GPS, etc., als sehr schwierig. Endgerätehersteller implementieren aufgrund fehlender weltweiter Standards oft keine terminalbasierten Ortungsverfahren in ihre Endgeräte. Einzig in den USA scheint ein terminalbasiertes Verfahren, Enhanced Observed Time Difference, auch auf Endgeräteebene Verbreitung zu finden.

Benutzereingabe Ein bis heute noch weit verbreitetes Verfahren zur Positionsbestimmung ist die Eingabe von Positionskoordinaten durch den Benutzer. Als Positionskoordinaten kommen beispielsweise Postleitzahlen, Telefonvorwahlen, Ortsnamen und Straßenbezeichnungen zum Einsatz. Vorteilhaft ist, dass dieses Verfahren in nahezu jedem Endgerät einsetzbar ist. Auch aus Sicht des Datenschutzes ist die Benutzereingabe positiv zu bewerten, da der Benutzer auf die Genauigkeit und Verwendung der Daten Einfluss nehmen kann. Von Nachteil ist, dass sich diese Methode der Positionsbestimmung nur für Situationen eignet, in denen Personen ihren eigenen Aufenthaltsort relativ genau kennen. Für Touristen beispielsweise ist eine solche Ortungsmethode ungeeignet, da sie typischerweise nicht über die notwendige Ortskenntnis verfügen. Überdies ist die Ortung sehr langsam und für Tracking-Anwendungen nicht einsetzbar, da ansonsten der Benutzer in regelmäßigen und relativ kurzen Zeitabständen seine Position bestimmen und eingeben müsste. Zur Zeit kommt die Benutzereingabe zur Standortbestimmung bei der Geldautomatensuche[4] zum Einsatz. [71, Folie 7-8]

Satellitengestützte Ortung Das wahrscheinlich bekannteste satellitengestützte Ortungsverfahren basiert auf dem amerikanischen NavStar *Global Positioning System* (GPS). Ferner existiert das russische GLONASS-System[5] und das noch nicht betriebsbereite europäische GALILEO-System. Da GLONASS und GALILEO in der Praxis bisher keinen relevanten Marktanteil besitzen, werden die beiden Systeme aus der Betrachtung ausgeschlossen.

GPS besteht aus 24 Low Earth Orbit (LEO) Satelliten und vier bis sechs Ersatzsatelliten. Auf der Erde stationierte mobile Endgeräte können die Signale der Satelliten empfangen und über Lateration in absolute Positionskoordinaten[6] umrechnen. Für präzise dreidimensionale Positionsangaben (Genauigkeit bis zu 10 Metern) muss das Endgerät wenigstens vier Satelliten in seinem Blickfeld haben. Aus diesem Grund sind GPS-Empfänger für den Gebrauch in stark und vor allem hoch bebauten Gebieten ungeeignet [22, S. 23], da in diesen Regionen kein direkter Sichtkontakt zu den Satelliten besteht. Dies schließt selbstverständlich auch eine Nutzung innerhalb von Gebäuden aus. Allerdings existieren bereits *pseudo* GPS-Satelliten, die innerhalb von Gebäuden installiert und genutzt werden können. Diese strahlen Signale, ähnlich denen von GPS-Satelliten aus, die von Endgeräten mit einem Softwareupdate empfangen werden können. [65, S. 22][44, 43][53, S. 17-21]

[4] siehe www.postbank.de
[5] siehe www.glonass-center.ru
[6] das Bezugssystem sind die Längen- und Breitengrade der Erde, sowie die Höhe des Nutzers

Das Problem, dass ein GPS-Empfänger für ein und denselben Punkt aufgrund von Störungen in der Ionosphäre und weiteren Störfaktoren hintereinander zwei unterschiedliche Positionsergebnisse berechnet, versucht *Differential GPS* (DGPS) zu lösen [22, S. 22]. Hierfür werden an verschiedenen (geographischen) Standorten Sendemasten aufgestellt, die ihre genaue Position kennen und einen Fehlerkorrekturwert für das aktuelle GPS-Signal an die Endgeräte weiterleiten. Die mobilen Endgeräte verwenden den Fehlerkorrekturwert zur Verbesserung ihrer eigenen Ortung. Weitere Informationen zu DGPS sind in [53, S. 19-20] zu finden.

Assisted GPS (A-GPS) bezeichnet die Kombination von GPS mit weiteren technischen Komponeneten (siehe Abbildung 2.1). Im Gegensatz zu den bisher angesprochenen GPS-Verfahren, benötigt das Endgerät beim Einsatz von A-GPS nur noch einen „low-level“ GPS-Empfänger, der selbst keine Positionsberechnung durchzuführen hat. Stattdessen versendet das Endgerät die Meßwerte an einen AGPS-Server. Dieser mit aktuellen GPS-Positionsinformationen ausgestattete Computer berechnet unter Zuhilfenahme von statistischen Verfahren aus dem „Location Fingerprint“ des Endgerätes dessen aktuelle Position. Ist der vom Endgerät gelieferte GPS-Fingerprint, bestehend aus den empfangenen GPS-Signalen, aufgrund von Umgebungseinflüssen (Aufenthalt innerhalb eines Gebäudes etc.) sehr schlecht, so kann der AGPS-Server beispielsweise die Zell-Identifikationsnummer des Mobilfunknetzes unterstützend zur Positionsbestimmung heranziehen. [21, S. 124] Außerdem bietet AGPS die Möglichkeit, dass nicht das Endgerät auf den Empfang des Almanach und der Ephemeriden warten muss [31, S. S. 10], sondern bereits von der Mobilfunkstation zugeschickt bekommt. Almanach und Ephemeriden sind grobe und feine Korrekturwerte mithilfe derer die Position der Satelliten im Weltall bestimmt werden kann. Als Folge daraus, verkürzt sich die Zeit bis zur ersten Positionsbestimmung. Ranenberg [71, Folie 13] erwähnt, dass auch Kraftfahrzeugdaten, wie Geschwindigkeit und Lenksäulenparameter, zur Anreicherung von AGPS-Daten hilfreich sein können.

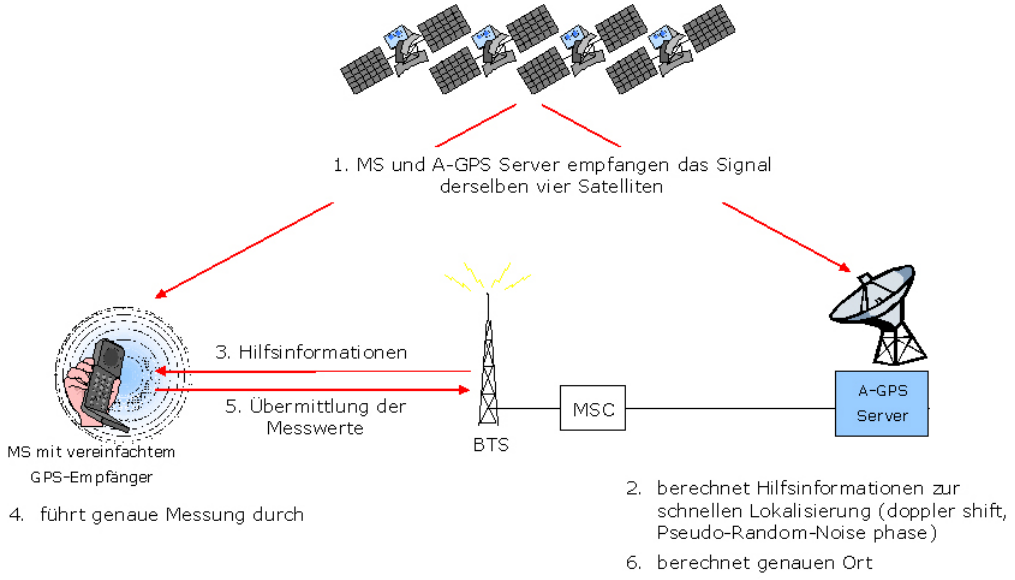

Abbildung 2.1: A-GPS Übersichtsdarstellung

Aufgrund der guten Lösungsmöglichkeiten GPS-spezifischer Probleme ist GPS weltweit eines der am weitesten verbreiteten Positionsbestimmungssysteme. Dies liegt hauptsächlich an der sehr hohen Genauigkeit, die im Idealfall bei bis zu 5-15 Metern [71, Folie 11] liegen kann.

Ferner sind Chipsätze zum Bau von GPS-Empfängern sehr preiswert und können mittlerweile leicht in Mobiltelefone integriert werden[7].

Enhanced Observed Time Difference Für das Enhanced Observed Time Difference (E-OTD) Verfahren muss das mobile Endgerät technisch in der Lage sein die zeitlichen Differenzen der eintreffenden Signale von mindestens drei Basisstationen zu messen[8]. Auf Basis der Messung kann das Endgerät entweder selbst die aktuelle Position berechnen oder die Berechnung durch eine vertrauenswürdige dritte Instanz durchführen lassen. Im Prinzip handelt es sich um eine Umkehr des UL-TOA Verfahrens (siehe Seite 6), mit dem sich eine Genauigkeit von 50 bis 100 Metern erzielen läßt.[79, S. 28] Wie bei allen terminalbasierten Positionsbestimmungsverfahren sind auch für das E-OTD Verfahren Änderungen am Endgerät erforderlich.

Positionssender Ein weiteres Positionsbestimmungsverfahren sind die so genannten Positionssender. Das häufig im Indoor-Bereich eingesetzte System wird an möglichst vielen Stellen in Gebäuden angebracht und kalibriert. Bewegt sich ein entsprechend ausgerüstetes Endgerät in den Empfangsbereich des Positionssenders, so werden ihm die Positionsdaten des Senders übermittelt. Meist wird dieses Verfahren in Verbindung mit Personal Area Networks (PAN), wie Bluetooth oder Infrarot, verwendet. Positiv zu erwähnen ist, dass neben den Positionsdaten auch Nutzdaten wie Werbung oder Informationen mitgesendet werden können. Positionssender ermöglichen des Weiteren eine Ortungsgenauigkeit von ca. 5-15 Metern. Nachteile ergeben sich durch die benötigte Infrastruktur. Die Sender müssen flächendeckend in den Räumlichkeiten in denen lokalisiert werden soll angebracht oder aufgestellt werden. Daneben benötigen die Endgeräte eine Software, die die Positions- und Nutzdaten entsprechend auswerten kann. Als Anwendungsbeispiele sind Museumsführer, Messeinformationssysteme, Warenhauswerbung und Touristenführer anzuführen. [71, Folien 14-16]

Das Ausstrahlen von Zell-Identifikationsnummern eignet sich aber nicht nur für die Anwendung innerhalb von Gebäuden. Installiert man entsprechende Vorrichtungen in Mobilfunknetzen, so lassen sich die Sendeantennen als Positionssender nutzen. Endgeräte, die sich im Abstrahlbereich der Sendeantenne befinden, können so eine eindeutige, gebietsbezogene Identifikationsnummer vom Mobilfunknetz empfangen, ohne ihre eigene Position preisgeben zu müssen. Zur Lokalisierung kann der Dienstnutzer entweder direkt die empfangene Identifikationsnummer weiterreichen oder, mithilfe einer Umrechnungsregel, in absolute oder relative Koordinaten konvertieren. Positiv zu bewerten ist, dass die bereits bestehende und sehr gut ausgebaute Infrastruktur der Mobilfunknetze genutzt und somit dem Dienstnutzer schnell eine datenschutzfreundliche Positionsbestimmungsmethode bereitgestellt werden kann. Allerdings müssten hierfür die Endgeräte über einheitliche Schnittstellen zur Abfrage der Positionsinformationen verfügen, damit zukünftige Anwendungen auf diese aufsetzen können.

Peer-to-Peer Dieses noch sehr unbekannte und nicht weit verbreitete Ortungsverfahren nutzt zur Positionsbestimmung in der Nähe befindliche Endgeräte, die ihre eigene Position kennen. Somit können Endgeräte mit ihren Ortsinformationen, in einem Netzwerk, sozusagen untereinander „handeln“. Jedoch tauchen hauptsächlich zwei Problemfelder auf. Zum einen existiert bis dato kein einheitliches Standardverfahren im Peer-to-Peer (P2P) Bereich, um

[7] siehe www.garmin.de

[8] eine vierte Basisstation ist oftmals zur Synchronisation der Endgeräteuhr notwendig

[8] siehe www.e-lba.com unter „Advertising in warehouses“

Informationen austauschen zu können. Und zum anderen muss die Frage gestellt werden, ob der Information eines anderen, unbekannten Endgerätes ohne weiteres vertraut werden kann.[71, Folie 19-20]

Signalstärke Auch unter dem Namen *„Location Fingerprinting“* [68] bekannt, wird bei diesem Verfahren die von Sendemasten ankommende Signalstärke[9] in den Endgeräten zur Positionsbestimmung genutzt. Hierfür muss spezielles Kartenmaterial angefertigt werden, welches für jeden lokalisierbaren Punkt den charakteristischen „Fingerabdruck“ der Sendestärken verschiedener Sender verzeichnet. Im Gegensatz zu anderen Ortungsverfahren nutzt das Location Fingerprinting bewusst die Multipfadausbreitung von Funkwellen zur Positionsbestimmung, wohingegen andere Verfahren gerade wegen dieser fehleranfällig sind [68]. Zudem ist diese Positionsbestimmungsmethode mit den weit verbreiteten IEEE 802.11b WLAN-Netzwerken nutzbar, was den Aufwand zur Schaffung einer Infrastruktur erheblich reduziert. Problematisch ist jedoch, dass die Sendestärken für eine Position je nach Tageszeit und Anzahl der Personen, die sich in dem Gebiet aufhalten, schwanken können. Auch die Verbreitung des Kartenmaterials auf die Endgeräte oder die netzseitige Berechnung der Position durch eine Trusted Third Party (TTP) sind derzeit noch unzureichend erforscht. [98, 68]

2.3 Drahtlose Kommunikationsnetzwerke

Nachdem eine Vielzahl von Möglichkeiten zur Positionsbestimmung aufgeführt worden sind, beschäftigt sich dieser Teil damit einen Überblick über bisher im Einsatz befindliche drahtlose Kommunikationsnetze zu schaffen. Die Einteilung der Netze erfolgt dabei, nach dem in der Netzwerktechnik überlichen Schema, in Personal Area Networks (PAN), Wireless Local Area Networks (WLAN), Wireless Metropolitan Area Networks (WMAN) und Mobilfunknetze. [4, S. 35, S. 37] Tabelle 2.2 zeigt in den letzten beiden Spalten die einsetzbaren Positionsbestimmungsverfahren. Es wurden mit Absicht die Standortbestimmungsverfahren ausgeblendet, die eine externe Quelle (wie zum Beispiel GPS) zur Positionsfestellung nutzen, da diese natürlich in jedem drahtlosen Netzwerk eingesetzt werden können.

In fast jedem Mobiltelefon integriert konnte die Infrarot-Technik in den letzten Jahren einen hohen Verbreitungsgrad erzielen. Dennoch werden mehr und mehr Bluetooth-Chipsätze in die Endgeräte eingebaut, da diese Technologie neben mehreren Betriebsmodi (Adhoc- und Infrastrukturmodus) auch die Kommunikation über größere Entfernungen hinweg ermöglicht. Zusätzlich bietet der Bluetooth-Standard auf mobile Endgeräte angepasste Energiesparstufen. Hauptvertreter der WLANs ist der IEEE 802.11b Standard (WiFi). Ähnlich wie in Bluetooth-Netzwerken kann zwischen den beiden Betriebsarten Adhoc und Infrastruktur gewählt werden. WiFi erzielt aber im Gegensatz zu Bluetooth höhere Sendereichweiten und Übertragungsraten, welche zu Lasten des Energieverbrauches gehen. Aus diesem Grund befinden sich WiFi-Module häufig in größeren mobilen Endgeräten wie zum Beispiel in Laptops und Handhelds. Zwar können auch Palmtops mit WiFi-Karten ausgerüstet werden, aber diese benötigen dann oftmals eine zweite Stromversorgung. Im Gegensatz zu den bisher angesprochenen Technologien befinden sich die MANs noch im Entwicklungsstadium. Ricochet[74], ein so genanntes Multihop-Netzwerk, kommt bisher nur in Denver und San Diego (USA) zum Einsatz. Das Gleiche gilt für IEEE 802.16 MANs, die in Boston getestet worden sind [92,

[9] engl. received signal strength (RSS)

[9] Der IEEE 802.11g Standard setzt sich momentan am Markt durch.

Technologie	Spektrum	max. Übertragungsrate	Abdeckung	Positionsbestimmung	
				netzbasiert	terminalbasiert
Personal Area Networks					
IrDA	Infrarot; 850 nm	4 Mbps	<10 m	-	E-OTD
IEEE 802.15.1 (Bluetooth)	2.4 GHz	1 Mbps	<10 m	Zell-Id	E-OTD, Positionssender
Wireless Local Area Networks					
IEEE 802.11b	2.4 GHz	22 Mbps	100 m	Zell-Id	E-OTD, Positionssender
HiperLAN2	5 GHz	32-54 Mbps	30-150 m	Zell-Id	E-OTD, Positionssender
Wireless Metropolitan Area Networks					
Ricochet	900 MHz	176 Kpbs	typische Stadt	n/a	n/a
IEEE 802.16	10-66 GHz	120 Mbps	typische Stadt	n/a	n/a
Mobilfunknetze					
CDMA2000 1xEv-DO	-	2 Mbps	Zellgebiet	Zell-Id, UL-TOA	E-OTD, Positionssender, Signalstärke
UMTS	1.9 und 2.1 GHz	2,048 Mbps	Zellgebiet	Zell-Id, UL-TOA	E-OTD, Positionssender, Signalstärke
GSM	900 MHz, 1.8 und 1.9 GHz	n / a	Zellgebiet	Zell-Id, UL-TOA	E-OTD, Positionssender, Signalstärke

Tabelle 2.2: drahtlose Kommunikationsnetzwerke

Folie 4]. Die größte Bedeutung für Location Based Services spielen zurzeit Mobilfunknetze. Allen voran das GSM-Netzwerk, welches vor allem in Europa Fuß gefaßt hat. Typisch für Mobilfunknetze ist ihre sehr weite Verbreitung, welche aus datenschutzrechtlicher Sicht kritisch zu betrachten ist. Betreiber dieser Netze können besonders leicht über netzwerkbasierte Ortungsmethoden Benutzerprofile ihrer Kundschaft im gesamten Ausbreitungsgebiet erfassen, welcher wesentlich größer ist als das heutiger WLANs oder PANs. [4, 83, 11, 49, 17]

2.4 Anwendungen in der Praxis

Zur Auflistung von bestehenden oder zukünftigen Anwendungen verwendet man typischerweise Kriterien, mit denen Anwendungen in Gruppen einteilbar sind, um somit die Übersichtlichkeit zu steigern und für den entsprechenden Anwendungsfall die Analyse zu erleichtern. Gerade im LBS-Umfeld finden sich viele Kategorisierungsmöglichkeiten zur Veranschaulichung. Christensen [15, S. 4-5] beispielsweise ordnet LBS-Anwendungen in fünf Kategorien ein,

die sich hauptsächlich daran orientieren, wie eine Person oder ein Gegenstand verfolgt wird (Tracking, Proximity-based). Van Kar und Bouwman hingegen verwenden eine dreigeteilte Gliederung in *Emergency Services*, *Public Land Mobile Network (PLMN) operator services* und *Value added services (VAS)* [50]. Die im folgenden verwendete Einteilung richtet sich hingegen nach dem Einsatzgebiet der jeweiligen Anwendung und lehnt sich an die Darstellung von Levijoki [58, S. 7-9] an.

Location Based Billing

Das Abrechnen von Dienstleistungen abhängig vom Aufenthaltsort zählt, zumindestens in Deutschland, zu einer der am weitesten verbreiteten Arten von LBS. Eine Hauptanwendung ist die standortbezogene Bestimmung des aktuellen Telefontarifes[10] im GSM-Netz. Meist als so genannte „Homezone“ deklariert, markiert dieser Bereich ein Territorium, in dem der Endnutzer zu gewöhnlichen Festnetzpreisen telefonieren kann. Außerhalb der Homezone findet eine Tarifumstellung hin zu Mobilfunktarifen statt. Mobilfunkanbieter wie O_2 (ehemals Viag Interkom) verwenden zur Positionsbestimmung der Kunden das netzbasierte Zell-ID Verfahren.

In Kooperation mit Mobilfunkanbietern versucht auch der deutsche Staat das Location Based Billing in Form der Straßenmaut[11] zu etablieren. Abgerechnet wird die mit einem Lastkraftwagen zurückgelegte Wegstrecke auf deutschen Autobahnen. Bei der Positionsbestimmung kommt das amerikanische GPS zum Einsatz. Während der Fahrt erkennt ein im Fahrzeug montiertes Gerät kostenpflichtige Straßenabschnitte und berechnet für die bereits zurückgelegte Wegstrecke die Maut-Gebühren. Ist das Fahrtziel erreicht, kontaktiert das Gerät über GPRS einen zentralen Server (Maut-Zentrale) und rechnet den bis dahin aufgelaufenen Mautbetrag ab.

Öffentliche Sicherheit

Ein weites Einsatzgebiet für LBS bietet der Bereich der öffentlichen Sicherheit. Angefangen bei der Ortung einer Person die einen Notruf abgesetzt hat bis hin zur automatischen Positionsübermittlung durch ein Kraftfahrzeug im Falle eines Unfalls. Der erste Fall ist zumindestens in den Vereinigten Staaten per Gesetz vorgeschrieben[12], wo Mobilfunkanbieter unter Einhaltung bestimmter Genauigkeitsrichtlinien den Aufenthaltsort des Hilferufenden bestimmen müssen (ohne Rückfrage beim Hilferufenden)[41][61, S. 57-58]. Aber auch in Deutschland ist in absehbarer Zeit mit einem flächendeckenden Angebot von „Notruf-LBS“ zu rechnen. So kann die Hamburger Notrufzentrale[13] mittlerweile nach Rückfrage beim Hilferufenden dessen Position über den Mobilfunknetzbetreiber ermitteln.

Auch Anwendungen für die automatische Positionsübermittlung, zum Beispiel durch Kraftfahrzeuge die in einen Unfall verwickelt sind, werden bereits eingesetzt. Meist werden dazu GPS-Empfänger, die in den Pkw integriert sind, verwendet. Anwendungen dieser Art bieten bereits Audi und Mercedes in Zusammenarbeit mit T-Traffic an[14].

[10] siehe www.o2.de (Viag Interkom)
[11] siehe www.toll-collect.de
[12] siehe www.fcc.gov/911/enhanced/
[13] siehe www.n-tv.de/5194814.html
[14] TELEAID (Mercedes) und Audi telematics, siehe www.t-traffic.de

Tracking Services

Vom Aufbau her ähnlich den Location Based Billing - Anwendungen, bieten Tracking Services Benutzern ein breites Anwendungsspektrum. Im geschäftlichen Umfeld wird das Flottenmanagement besonders häufig eingesetzt. Hierbei handelt es sich um eine Anwendung die es Unternehmen ermöglicht, Fahrtrouten ihrer im Einsatz befindlichen Fahrzeuge zu optimieren und zu überwachen. Vor allem große Versanddienstleister wie UPS setzen das Flottenmanagement erfolgreich ein.

Im nichtgewerblichen Bereich lässt sich vor allem die Personenverfolgung als Anwendungsgebiet ausmachen. Unter dem Namen „TrackYourChild“ bietet inzwischen eine deutsche Firma[15], in Zusammenarbeit mit mehreren großen Mobilfunknetzbetreibern, Eltern die Möglichkeit, ihre Kinder ständig über ein eingeschaltetes Mobilfunkgerät zu orten.

Auch die meisten bisher existierenden Touristikanwendungen sind unter dem Punkt Tracking Services einzuordnen. Elektronische Stadtführer[16] zum Beispiel geben dem Touristen mehr Freiheit und einen größeren Bewegungsradius. Diese Anwendungen können zudem gezielt auf die Interessen ihrer Kundschaft eingehen und dadurch personalisierte Führungen und Informationen anbieten [20]. Darüber hinaus sind die Anwendungen 24 Stunden verfügbar und können auf Witterung, Besucherstände und Tageszeiten Rücksicht nehmen. Stadtführungen sind auf diese Weise dynamisch, je nach Situation, während der Führung anpassbar.

Auch im medizinischen Bereich und Pflegedienst könnten sich Tracking Service-Anwendungen bald als unverzichtbar erweisen. Eine solche Healthcare-Anwendung ist das Verfolgen von geistig behinderten Personen, die eine ambulante Betreuung erhalten. Ärzte oder das Aufsichtspersonal haben die Möglichkeit Gebiete zu definieren, in denen sich der Patient aufhalten darf. Erfolgt eine Überschreitung der Gebietsgrenzen können Maßnahmen eingeleitet werden, um die Person wieder zurückzuführen. Besonders nützlich könnte sich ein solches System auch bei der Führung von sehbehinderten Menschen erweisen, falls diese die Orientierung verloren haben sollten. Ähnlich in der Funktionsweise sind Systeme zur Überwachung von Gefangenen die während des Tages Freigang erhalten. Wenn auch nicht unbedingt im Interesse der Träger von Fussfesseln, können Justizvollzugsbeamte leicht die Position feststellen und bei unerlaubten Handlungen schneller eingreifen.

Datenlieferung

Unter dem Punkt Datenlieferung fasst man Anwendungen zusammen, bei denen ein LBS-Nutzer einem LBS-Diensteanbieter Daten, die in Zusammenhang mit seiner aktuellen Position stehen, zur Verfügung stellt. Ein bekanntes Beispiel ist die Lieferung von Wetterdaten[17]. Bisher müssen Wetterdienste kostspielige Wetterstationen aufstellen, warten und pflegen. Stattdessen kann man sich in Zukunft die, oft sehr gute, Ausstattung von Kraftfahrzeugen zunutze machen, indem in Autos integrierte Temperatur- und Regenssensoren ihre Meßwerte den Wetterdiensten zur Verfügung stellen. Der Vorteil ist, dass eine viel höhere Flächenabdeckung und Aktualität der Daten erzielt werden kann. Ähnlich in der Funktionsweise sind aktive Staumelder. Bewegen sich mehrere Autos auf einer Autobahn mit einer Geschwindigkeit von nur 20 Stundenkilometern vorwärts, so kann man höchstwahrscheinlich daraus schließen, dass es einen Stau auf den Autobahnabschnitt gibt.

[15] siehe www.trackyourchild.de
[16] siehe http://www.yellowmap.de/mobile.asp
[17] siehe http://www.mowis.net/de/produkte_services/verkehrswetter-sensoren.php

Location Based Information

Der momentan zweitgrößte Anwendungsbereich für LBS sind die Location Based Information. Nach einer Studie der Firma ExperTeam hat diese Servicekategorie zukünftig die größten Marktchancen. Allen voran ist hier das Angebot von aktuellen Verkehrsinformationen zu nennen. [26] Weitere Vertreter dieser Kategorie sind die „gelben Seiten“, die Abfrage von nahegelegenen Übernachtungsmöglichkeiten oder Bankautomaten. Ferner wurde für die Dienste „Preisvergleich mit Ortsbezug“ und „Parkplatz-Finder“ in einer Studie von Kölmel und Hubschneider [52] ein sehr hoher Nutzerwert ermittelt[18]. Charakteristisch für Location Based Information ist, dass kein Tracking der LBS-Nutzer stattfindet. So sind zur Dienstnutzung oft nur einzelne Positionsangaben erforderlich und nicht ein Bewegungsprofil im Zeitablauf.

2.5 Referenzarchitektur

Abschließend wird in diesem Kapitel eine Referenzarchitektur für Location Based Services dargestellt, die die Grundkomponenten eines LBS erfasst. Elemente zur Erhöhung der Datenschutzfreundlichkeit sind hierbei noch ausgeblendet und werden erst in den nachfolgenden Kapiteln näher behandelt.

2.5.1 Teilnehmer und Rollen

Tabelle 2.3 bietet einen Überblick aller an LBS-Dienstleistungen beteiligten Personen und Institutionen.

Teilnehmer	Beschreibung
Dienstnutzer	Als Nutzer eines LBS wird jede Person bezeichnet, die unter Angabe von positions-, zeit- und personenabhängigen Daten einen mobilen Dienst nutzt. Personenabhängige Daten können nach [1, S.101] in die folgenden Untergruppen eingeteilt werden: • demographische Daten (Geschlecht, Geburtstag, etc.) • personenbezogene Aktivitäten (Hobbies, etc.) • die Sitzungshistorie • Präferenzen
Access Service Provider (ASP)	ASP stellen Nutzern einen mobilen Zugang zu einer Netzinfrastruktur bereit. In der Regel handelt es sich dabei um das Internet. Je nach Implementation erfolgt eine separate Abrechnung mit dem Kunden oder der dahinter stehende Netzbetreiber übernimmt die Abrechnungsleistung.

Fortsetzung auf der nächsten Seite.

[18] Befragung wurde unter $N = 479$ Personen durchgeführt

Teilnehmer	Beschreibung
Netzbetreiber (SP - Service Provider)	Netzbetreiber stellen den ASP die notwendige Netzinfrastruktur in Form von Einwahlknoten zur Verfügung, über die dann Benutzeranfragen an ihre Ziele geleitet werden. Weitere Aufgaben des SP sind meist die Abrechnung von Leistungen und die Nutzer-Authentifizierung. In Deutschland fallen ASP und Netzbetreiber für gewöhnlich zusammen. Dennoch wird über eine Trennung beider Instanzen, vor allem bei der Verbreitung von WLAN-Netzen, heftig diskutiert [13, S. 92-94].
Trust-Broker / Trust-Center	Diese Gruppe stellt eine vertrauenswürdige dritte Instanz dar, die in viele elektronisch abgewickelte Geschäftsverbindungen integriert ist. Ihre Hauptaufgabe ist die Überprüfung von Zertifikaten auf Echtheit (Authentisierung). Erst dadurch kann ein rechtkräftiger elektronischer Geschäftsverkehr realisiert werden.
LBS Dienstanbieter	LBS Diensteanbieter können gegenüber dem Benutzer in verschiedenen Formen auftreten: 1. als Content service provider 2. Software application provider 3. und als allgemeiner Dienstanbieter der nicht in die Gruppen a) oder b) fällt. Content service provider liefern Informationen auf Basis der vom Benutzer gelieferten Daten. Software application provider installieren positionsabhängig entsprechende Applikationen auf einem Mobile Terminal oder entfernen diese wieder. In die Gruppe c) fallen Dienste, die nicht den elektronischen Rückkanal zur Erbringung der Hauptleistung nutzen. Darunter fallen beispielsweise der Pannenservice, Notrufdienst etc.
Staat	Der Staat stellt die rechtlichen Rahmenbedingungen auf und setzt diese durch die Exekutive um. Wichtige Gesetze in Deutschland sind das BGB, BDSG, TDDG, SigG, SigV, TDG und MDStV.
Kreditinstitute	Banken nehmen nur indirekt am Prozess der Leistungserbringung teil. Sie übernehmen die Aufgabe entstandene Gebühren der Nutzer auszugleichen und Bezahlverfahren zur Verfügung zu stellen.

Tabelle 2.3: LBS Teilnehmer (Überblick)

2.5.2 Aufbau

Abbildung 2.2 zeigt den schematischen Aufbau eines LBS-Dienstes. In der Grundkonstellation, ohne Einbezug von Bezahlsystemen, sind vier Gruppen an der Diensterbringung beteiligt. Zunächst der LBS-Nutzer oder Mobile Client selbst, der vertretend für den Nutzer steht. Hierbei handelt es sich um ein kleines Endgerät, welches im besten Fall mit verschiedenen Kommunikationsnetzwerken (GSM, WLAN) in Verbindung treten kann (siehe Kapitel 2.3) und über diese LBS-Dienstleistungen bezieht. Die Netzbetreiber verkörpern in dieser einfachen Architektur sowohl den Access Service Provider (ASP) als auch den Service Provider. Neben der Bereitstellung einer ständigen Verbindung zu den verschiedenen LBS-Anbietern stellt der Netzbetreiber dem Mobile Client auch die Möglichkeit zur Verfügung, sich netzseitig orten zu

lassen. Die LBS-Anbieter nehmen über das Kommunikationsnetzwerk des Netzbetreibers eine Anfrage des Mobile Clients entgegen und erbringen dann die gewünschte Leistung, entweder über das Kommunikationsnetzwerk oder über andere Kanäle (bspw. erfolgt bei Notrufen die Alarmierung eines Krankenwagens).

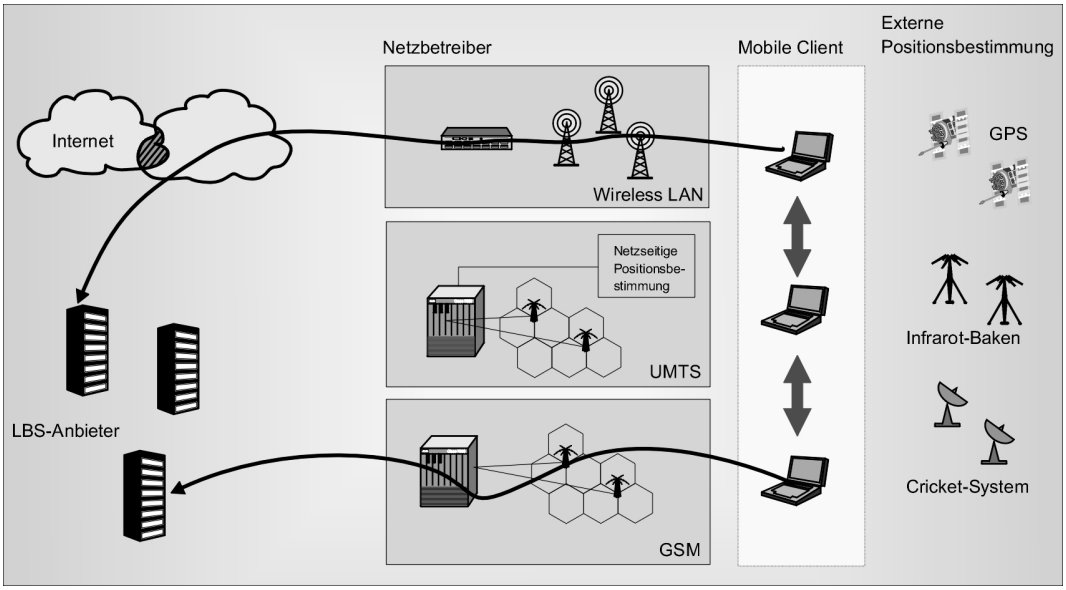

Abbildung 2.2: LBS-Referenzarchitektur

Diese Referenzarchitektur entspricht dem anfänglichen Schema beim Aufbau von LBS-Diensten, welches von Spreitzer und Theimer [89] beschrieben wurde. Nutzer vertrauen in der beschriebenen Architektur einem Agenten, der als Schnittstelle bzw. Intermediär zwischen LBS-Dienstanbieter und Nutzer fungiert. Neben der reinen Durchleitung von Daten werden dem Netzbetreiber aber heutzutage weitere Aufgaben zugeordnet. In der Realität ist festzustellen, dass der Netzbetreiber Positionsdaten des Nutzers sammelt und den Zugriff durch LBS-Dienste auf diese Informationen regelt. Die Zusammenlegung von ASP und SP spiegelt die momentane Situation in den Mobilfunknetzen wieder. Allerdings könnte in Zukunft mit dem Aufbau von UMTS Netzwerken eine neue Art von Netzwerkanbietern am Markt entstehen, die so genannten *Mobile Virtual Network Operator* (MVNO). Im Gegensatz zu herkömmlichen Netzbetreibern sind MVNO nur noch für Teilkomponenten zuständig (wie zum Beispiel Home Location Register (HLR) und (Gateway) Mobile Switching Center ((G)MSC). Die fehlenden Netzkomponenten werden von Vollnetzwerkanbietern bezogen. Hierduch würde auch im GSM eine Trennung von ASP und SP stattfinden.

2.5.3 Dienstarten

Die Interaktion zwischen LBS-Nutzer und LBS-Dienstanbieter kann auf zwei Arten erfolgen. Zum einen als **Pull**-Interaktion, welche momentan am stärksten verbreitet ist. Bei diesem Interaktionstyp sendet der Diensteanbieter nur dann Daten zu einem LBS-Nutzer, wenn dieser explizit Daten in Form einer Dienstanfrage anfordert. **Push**-Interaktionen, als zweite Dienstart, reagieren hingegen ereignis- oder zeitbasiert. Hierfür definiert der LBS-Nutzer einmalig oder jeweils zu Beginn der Diensterbringung ein Set von Ereignissen auf das hin entsprechende

Aktionen seitens des LBS-Diensteanbieters ausgelöst werden sollen. Beispielszenarios dafür sind vor allem im Marketing zu finden (siehe www.mobilesmarketing.com). [58, S. 7]

Kapitel 3

Datenschutz und Location Based Services

Nachdem im vorherigen Kapitel Location Based Services erläutert und deren Architektur skizziert wurde, wird im ersten Teil dieses Kapitels versucht die Begrifflichkeiten Privacy und Datenschutz gegeneinander abzugrenzen, sowie die Termini IT-Sicherheit und mehrseitige Sicherheit in diesen Kontext einzuordnen. Der zweite Teil, *Status Quo in der aktuellen LBS-Landschaft*, zeigt die aktuelle Anwendung von datenschutzfreundlichen Technologien und Regelungen in der Bundesrepublik Deutschland auf, um daraus resultierende Bedrohungen für LBS-Nutzer stärker hervorzuheben.

3.1 Definitionen und Begriffe

3.1.1 Privacy und Datenschutz

Warren und Brandbeis, zwei amerikanische Juristen, befassten sich bereits 1890 mit der Privacy, oder zu deutsch, der Privatsphäre des Menschen [97]. Anstoß zu diesen Überlegungen war vor allem das Aufkommen von Tageszeitschriften und der rasante Fortschritt in der Fototechnik, die einen Wandel im Verständnis des Begriffs Privacy verursachten [25, S. 44-45]. Diese damals neuen Technologien vergrößerten den Ausbreitungsbereich von Informationen in nie zuvor da gewesener Art und Weise. Blieben Informationen in früheren Zeiten in den Ortschaften in denen sie entstanden, so verbreiteten sie sich jetzt in ganzen Regionen. Auszüge aus dem Aufsatz erweisen sich dabei von der Thematik als durchaus aktuell:

„The press is overstepping in every direction the obvious bounds of propriety and decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers.“ [97, S. 196]

So entwickelte sich aus dem „right to life“ und dem „right to property“ eine ganz neue Auffassung der Privatsphäre, welche auch noch ein Jahrhundert später oft zitiert wird:

„The right to be let alone.“[97, S. 193]

Das besondere an der damaligen Definition ist, dass sie als erste nicht nur tangible Vermögensgegenstände oder Besitztümer[1] umfaßt, sondern die Reichweite des Begriffes Privatsphäre auf intangible Gegenstände erweitert. Damit erkannten die Autoren vor einem Jahrhundert, dass ein Bruch der Privatsphäre intellektuelle als auch emotionale Werte genauso schädigt, wie physische. Natürlich entspricht diese Definition für Privacy nicht mehr dem aktuellen Bild, aber dennoch kann sie als Grundpfeiler für das heutige Verständnis gesehen werden. [2, S. 154-157]

Weiterentwicklungen und Anpassungen der Auffassung von Privacy an die jeweiligen kulturellen, religiösen und technischen Gegebenheiten verfeinerten die frühe Definition von Warren und Brandeis. Im Jahr 1967 veröffentlichte Westin eine neue grundlegende Definition von Privacy: *„the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behavior to others.“* Er folgte somit der Auffassung, dass die Definition von Privacy an die sich verändernde Umgebung ständig angepasst werden muss [25, S. 47].

Clarke präzisierte 1997 den Begriff Privacy indem er ihn in vier Dimensionen einteilte: [16],

- privacy of the person,
- privacy of personal behaviour,
- privacy of personal communications und,
- privacy of personal data.

Erst durch diese Aufspaltung des Begriffes Privacy wird deutlich, dass Datenschutz[2] und Privacy nicht auf einer Ebene stehen, oder sogar die gleiche Bedeutung besitzen. Im Gegenteil, Datenschutz ist eine Bestandteil von Privacy und setzt sich aus den unteren beiden Punkten, *privacy of personal communications* und *privacy of personal data* zusammen [16]. Datenschutz dient somit dem Schutz personenbezogener Daten[3]. Diese Erkenntnis macht deutlich, dass der im allgemeinen Sprachgebrauch häufig verwendete Begriff Privacy oft nur die Unterkategorie *information privacy* oder *data privacy* meint.

Neben den zuvor genannten Bezeichnungen, die sich nicht ausschließlich auf Datenschutzaspekte in Zusammenhang mit der Computertechnologie beziehen, bildete sich in den letzten Jahren der Begriff *Web privacy* heraus. Inhaltlich ist *Web privacy* mit Datenschutz gleichbedeutend, fokussiert allerdings den Datenschutzbereich mehr auf Computertechnologien. [73, S. 41]

Datenschutz, für sich allein genommen, wird in der Literatur häufig wie folgt definiert: *„Information Privacy is the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves.“*[16]

Rossnagel, Pfitzmann und Garstka haben in ihrem Modernisierungsgutachten des Datenschutzrechts eine weitere Unterteilung des Begriffes Datenschutz vorgenommen [75, S. 39-42].

[1] im englischen „property“

[2] engl. information privacy oder data privacy

[3] gemäß §3 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Systemdatenschutz Der Systemdatenschutz beschreibt das Konzept, durch Technik in Verbindung mit organisatorischen Aspekten, Datenschutz für alle Beteiligten, vor allem durch Veränderungen auf der Dienstanbieterseite, zu erzielen. Im Vordergrund steht das Interesse, durch den Einsatz von geeigneten technischen Maßnahmen die Erhebung von personenbezogenen Daten auf ein Minimum zu reduzieren. Des Weiteren umfasst der Systemdatenschutz die Zweckbindung [75, S. 40] für erhobene Daten. Ein entscheidender Nachteil des Systemdatenschutzes ist allerdings, dass dieser mithilfe gesetzlicher Regelungen nur im Inland durchsetzbar ist. Ausländische Dienstanbieter können nicht kontrolliert werden. [39, S. 294, 310]

Selbstdatenschutz Selbstdatenschutz versucht den Mangel der begrenzten Reichweite rechtlicher Maßnahmen zu überwinden. Anstatt per Zwangsmaßnahme, welche auch nur im Inland wirken kann, zu versuchen, dass eine flächendeckende Datenvermeidung für jeden und überall eingeführt wird, ist es das Anliegen des Selbstdatenschutzes, dem Nutzer adäquate technische Instrumente in die Hand zu geben, um sich selbst zu schützen. Dadurch bleibt es der Person freigestellt in jeder beliebigen Situation selbst darüber zu entscheiden, ob und wieviel personenbezogene Daten preisgegeben werden sollen. Selbstdatenschutz verbindet gleich zwei Vorteile. Zum einen, wie eingangs schon erwähnt wurde, spielen Staatsgrenzen keine Rolle mehr. Schützt sich eine Person gleich am Ort der Datenentstehung, so verliert der Systemdatenschutz auf Datenempfängerseite seine Wichtigkeit. Und zum anderen wird dem Nutzer volle Entscheidungsfreiheit hinsichtlich der Verwendung seiner Daten gewährt.

3.1.2 IT-Sicherheit

Um die in Kapitel 3.1.1 angesprochenen Konzepte, System- und Selbstdatenschutz, realisieren zu können, bedarf es nicht nur Unterstützung von rechtlicher Seite. Das zweite „Standbein“ des Datenschutzes ist die IT-Sicherheit, die sich auf technische Konzepte und Realisierungen auswirkt.

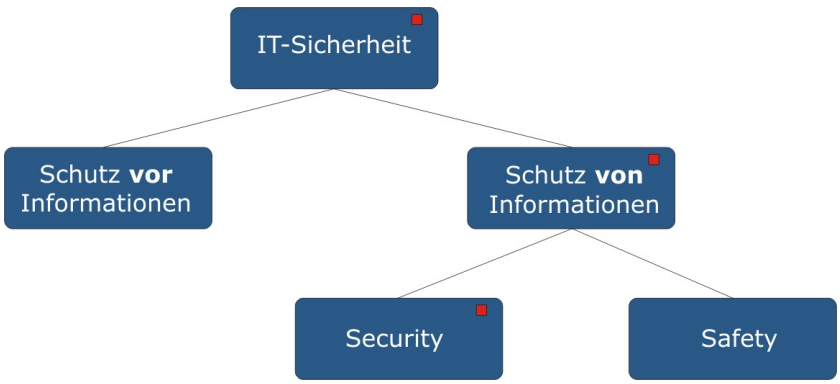

Abbildung 3.1: IT-Sicherheit

IT-Sicherheit ist in mehrere Teilbereiche zerlegbar, weshalb diejenigen zu bestimmen sind, die für den Datenschutz von Bedeutung sind, siehe Abbildung 3.1. Die roten Kästchen markieren jene Bereiche, welche aus Sicht des Datenschutzes relevant sind.

Security *versus* Safety Die Unterscheidung der beiden Begrifflichkeiten ist relativ einfach. Mit Safety wird das Ziel verfolgt, sich gegenüber ungewollten bzw. zufällig eintretenden

Ereignissen, wie Blitzschlag, Erdbeben o.ä., abzusichern. Im Vordergrund steht demnach die Verfügbarkeit, welche in Form von Funktionssicherheit und technischer Sicherheit gewährleistet werden muss. Security hingegen befasst sich mit der Abwehr von Angriffen. Vertraulichkeit, Integrität und Zurechenbarkeit sowie Verfügbarkeit sind entsprechende Schutzziele. [27, S. 84][86, S. 8] Da Safety sich mit Einwirkungen „höherer Gewalt“ auseinander setzt, wird dieser Teilaspekt der IT-Sicherheit in der nachfolgenden Arbeit nicht weiter berücksichtigt, obwohl auch von dieser Seite Einflüsse auf den Datenschutz bestehen.

Schutz von Informationen *versus* Schutz vor Informationen Der Schutz von Informationen beschäftigt sich mit der Problemstellung, das Abhören, Verändern oder Verfälschen von Daten während der Übertragung oder Archivierung zu verhindern. Hierbei handelt es sich um aktive Angriffe von schutzwürdigen Inhalten, die absichtlicher Natur sind. Schutz vor Informationen ist ein relativ neuer IT-Sicherheitsbereich, der erst mit dem Aufkommen der Spam-Problematik eine große Bedeutung erlangt hat. Im Gegensatz zu dem Bereich Schutz von Informationen erfolgen Angriffe in diesem Bereich nicht auf inhalts- oder personenbezogene Daten einer Kommunikationsverbindung, so dass die Privatsphäre hinsichtlich des Datenschutzes nicht gestört wird. Aus diesem Grund erscheint eine weitere Betrachtung des Teilbereichs Schutz vor Informationen nicht notwendig.[62, Folie 2]

3.1.3 Mehrseitige Sicherheit

Mehrseitige Sicherheit erweitert das Konzept der Datensicherheit und des Selbstdatenschutzes um den Aspekt, dass Nutzer von interaktiven Medien nicht immer nur die Rolle der „betroffenen“ Person annehmen, sondern auch selbst Datenverarbeiter sein können [75, S. 41]. Mit dieser Betrachtungsweise ist es nicht mehr möglich nur die Schutzbedürfnisse einer einzigen Person zu beachten. Es müssen vielmehr die Interessen aller am Kommunikationsprozess Beteiligten berücksichtigt werden. Das dahinter stehende Konzept der mehrseitigen Sicherheit besteht im Aushandeln von gegenseitigen Sicherheitsbedingungen.[70, S. 26]

Besonders im Hinblick auf die Nutzung von LBS-Anwendungen ist die Mehrseitige Sicherheit eine Grundvoraussetzung für viele Anwendungen. Nutzer von LBS-Anwendungen können beispielsweise Lieferant für Wetter- oder Verkehrsdaten sein. In diesem Fall fungieren LBS-Diensteanbieter gleichzeitig als Dienstnutzer und müssen dementsprechend Vertrauensbeziehungen zu ihren Datenlieferanten aushandeln und anschließend auch durchsetzen. Neben den alltäglichen Beziehungen zu Dienstanbietern sind aber auch Sicherheits- und Vertrauensaspekte in bezug auf Hardwarehersteller mit zu berücksichtigen, da einige Technologien zur Erhöhung der Datenschutzfreundlichkeit auf der ordnungsgemäßen Konstruktion von Hardware-Komponenten beruhen.

3.2 Status Quo in der aktuellen LBS-Landschaft

Im folgenden Abschnitt wird die Existenz und Anwendung von Richtlinien und Verfahren zur Erhöhung des Datenschutzes für LBS-Nutzer betrachtet. Um die Ist-Analyse zu vereinfachen, stellt Kapitel 3.2.1 zunächst die aktuelle rechtliche Situation in der Bundesrepublik Deutschland in einem kurzen Überblick dar. Kapitel 3.2.2 untersucht den bisherigen Verbreitungsgrad von datenschutzfreundlichen Technologien und organisatorischen Maßnahmen zur

Steigerung des Datenschutzes. Den Abschluss bildet eine Auflistung von daraus resultierenden Bedrohungen für LBS-Nutzer sowie eine Zusammenfassung, die Implikationen aus den vorangegangenen Unterkapiteln vereint und gemeinsam darstellt.

3.2.1 Rechtliche Regelungen

Das 1977 erstmals verabschiedete und in den Jahren 1990, 1994 und 1997 immer wieder überarbeitete Bundesdatenschutz Gesetz (BDSG) stellt in der Bundesrepublik Deutschland den Grundpfeiler zum Schutz des Einzelnen gegen Verletzungen seines Persönlichkeitsrechts dar.[24, S. 183]

Von besonderer Bedeutung ist der §3a BDSG (Datenvermeidung und Datensparsamkeit), welcher mit der Novelle des BDSG (vom Mai 2001) in das modernisierte BDSG eingang fand und das bisher normativ gehaltene Datenschutzrecht um eine neue Komponente ergänzte [9, S. 302]. Anlass für das Einbringen dieser Regelung war die Absicht Gefahren für das informationelle Recht auf Selbstbestimmung durch die Verwendung von datenschutzfreundlicher Technik zu reduzieren. In der Literatur wird dieses Konzept als Bestandteil des schon in Kapitel 3.1.1 erwähnten Systemdatenschutzes betrachtet.[9, S. 296] Insofern versucht der deutsche Gesetzgeber das Konzept *„Datenschutz durch Technik“* besonders zu betonen.

Datenvermeidung, im speziellen, ist das Streben so wenig wie möglich Daten mit Personenbezug zu *erheben* oder von Nutzerseite herauszugeben. Sie sollte wo immer möglich zum Einsatz kommen. Ein Optimum bezüglich der Datenvermeidung ist erreicht, wenn die Anzahl der personenbezogenen Daten gleich Null ist. Eine häufig genannte Methode, die die Kriterien der Datenvermeidung erfüllt, ist die Anonymisierung [39, S. 305]. Datensparsamkeit, als zweite Alternative, zielt darauf ab, die Qualität[4] und Quantität der personenbezogenen Daten zu minimieren. Hieraus resultieren die Optionen, die Anzahl der Daten mit personenbezug zu minimieren oder die Tiefe an Informationen einzuschränken.[9, S. 310] Bizer nennt für die Umsetzung der Datensparsamkeit beispielhaft den Verzicht einer nutzungsabhängigen Abrechnung, welche in vielen Fällen effektiv durch pauschale Abrechnungsverfahren abgelöst werden könnte (siehe hierzu Kapitel 5).

§3a Satz 2 BDSG konkretisiert die Umsetzungsmöglichkeiten für Datenvermeidung und -sparsamkeit durch den Vorschlag, verstärkt von den Verfahren der Anonymisierung und Pseudonymisierung (siehe Kapitel 4.1.1) Gebrauch zu machen. Allerdings impliziert die Formulierung des Gesetzestextes, dass die Verwendung rein optional und nicht zwingend zu sehen ist, da auch andere Verfahren zur Verfügung stehen.[9, S. 311]

Neben dem BDSG existieren speziell für Tele- und Mediendienste gesonderte bereichsspezifische Datenschutzvorschriften, das Teledienste-Datenschutzgesetz (TDDSG) und der Mediendienste-Staatsvertrag (MDStV)[33, S. 129]. Besonders erwähnenswert erscheint §4 TDDSG in Verbindung mit §6 TDDSG, wonach eine Profilbildung anhand der erhobenen Daten zwar grundsätzlich verboten ist, aber bei Verwendung von Pseudonymisierungs- oder Anonymisierungsverfahren dieses Verbot umgangen werden kann, wenn keine Rücktransformation zur richtigen Identität mehr möglich ist [85, S. 268]. Eine weitere Möglichkeit zur Umgehung ist das Einholen einer Einwilligung. Somit wird explizit die Profilanalyse von Nutzungsdaten zu marketing- oder vertriebstechnischen Zwecken ermöglicht. Allerdings verschärft §4 Abs. 6 TDDSG die Vorschrift in §3a BDSG bezüglich der Anonymisierung und Pseudonymisierung.

[4] beispielsweise durch Pseudonymisierung

Im Gegensatz zum BDSG müssen Anbieter von Multimediadiensten nicht erst im nachhinein den Personenbezug vermeiden, sondern schon an der Kundenschnittstelle Verfahren zur bereitstellen die diesen verhindern.[33, S. 131]

Parallel zu den bisher genannten Vorschriften zur Erhebung, Verarbeitung und Nutzung von Daten regelt der deutsche Gesetzgeber weitere Rechte für Nutzer elektronischer Dienstleistungen. Hierzu zählt auch das Informationsrecht, welches Diensteanbietern Informationspflichten gegenüber dem Dienstenutzer auferlegt. Ein Grund für die Einführung von Informationspflichten ist, dass es für einen Nutzer zunehmend schwieriger wird, beurteilen zu können, wer welche Daten erhält und in welcher Weise eine Weiternutzung stattfindet.[81, S. 109] §4 Abs. 3 BDSG regelt hierfür die Unterrichtungs-, Hinweis- und Aufklärungspflichten. Damit unterstützt das BDSG den so genannten „Transparenzgedanken“, der es einem Nutzer ermöglichen soll, selbstständig über die Preisgabe der Daten zur eigenen Person zu entscheiden.[87, S. 330] Des Weiteren wirkt sich dieses Gesetz unmittelbar auf Techniken zum Selbstdatenschutz aus, da auf Basis der vom Diensteanbieter gelieferten Informationen eine fundiertere Entscheidung seitens des Nutzers getroffen werden kann.

Das Datenschutzgesetz räumt dem Nutzer eines elektronsichen Dienstes auch das Auskunftsrecht, gemäß §6 BDSG, als unabdingbares Recht ein. Hierunter fallen insbesondere die Rechte auf Auskunft, Berichtigung, Löschung oder Sperrung der bis dato gespeicherten Daten. Die Konsequenz dieser Regelung ist, dass ein Dienstenutzer nicht nur das Recht besitzt, über die Preisgabe seiner Daten frei zu entscheiden, sondern auch auf deren Verwendung Einfluss zu nehmen.[81, S. 159-160]

Eine letzte an dieser Stelle näher zu erläuternde Vorschrift ist die Einwilligung, die im §3 Abs. 1 TDDSG geregelt ist. Gegenstand dieser Rechtsvorschrift ist, dass ein Diensteanbieter nur dann berechigt ist Daten zu erheben, verarbeiten oder zu nutzen, wenn entweder eine Rechtsvorschrift dies explizit erlaubt oder eine Einwilligung des Nutzers vorliegt. Eine gesetzliche Ausnahme stellen Daten dar, die für die Inanspruchnahme von Telediensten notwendig sind. In Verbindung mit den in Kapitel 3.1.1 vorgestellten technischen Verfahren zum Selbstdatenschutz bietet diese Vorschrift ideale Ausgangsvoraussetzungen.

Weitere hier nicht thematisierte rechtliche Regelungen sind das Kopplungsverbot und die Wiederspruchsrechte.

Fazit: Wie aus dem bisher gesagten entnommen werden kann, existieren in Deutschland bereits sehr tiefgehende und weitreichende datenschutzrechliche Regelungen deren Wurzelelemente das Grundgesetz und BDSG sind. Speziell für elektronische Dienstleistungsanbieter gelten TDDSG und MDStV. Dennoch zeigt die Praxis, dass die Anforderungen des Gesetzes häufig nicht oder nur unzureichend erfüllt werden und Verletzungshandlungen die Folge sind [81, S. 109-110][33, S. 130]. Des Weiteren ist trotz der rechtlichen Regelungen eine Profilbildung seitens des Diensteanbieters möglich. Die im Kapitel 4 vorgestellten Privacy Enhancing Technologies (PET) sollen zeigen, dass eine den Datenschutzvorschriften entsprechende Implementierung von Technologien, besonders im LBS-Bereich möglich ist. Von besonderer Bedeutung sind Techniken, die den Selbstdatenschutz durch den Nutzer fördern, da zum Beispiel (wie bereits im Kapitel 3.1.1 angesprochen) rechtliche Regelungen nicht zwingend grenzüberschreitend durchgesetzt werden können und nicht immer überprüfbar sind.

3.2.2 Aktueller Einsatz von datenschutzfreundlichen Verfahren und Technologien

Neben den rechtlichen Gestaltungsmöglichkeiten des jeweiligen Staates existieren, wie auch noch in den nächsten Kapiteln eingehender behandelt wird, weitere Möglichkeiten zur Erhöhung des Datenschutzniveaus auf Kundenseite. Zum einen sind dies einfache organisatorische Maßnahmen, die beispielsweise mithilfe der Datenverteilung das Schutzlevel erheblich erhöhen können. Andererseits stehen dem Kunden technische Schutzmöglichkeiten zur Verfügung, welche auf unterschiedlichen Datenentstehungsebenen eingreifen. Wie bisher von solchen organisatorischen und technischen Möglichkeiten Gebrauch gemacht wird und welche Bereiche verbesserungswürdig scheinen, soll in diesem Kapitel näher untersucht werden.

Organisatorische Maßnahmen Organisatorische Maßnahmen zur Steigerung der Datenschutzfreundlichkeit von LBS-Anwendungen sind Methoden der Datenverteilung zwischen Beteiligten am LBS Prozess. In dieser ersten Variante Datenschutz zu fördern und zu erhöhen, sollten monolithische Anhäufungen von Aufgaben und Kompetenzen bei Beteiligten in LBS Prozessen streng vermieden werden. So zeigt beispielsweise ein Blick in die Praxis, dass große Mobilfunkanbieter oftmals dazu neigen, selbst LBS-Dienste nach dem Motto „alles aus einer Hand“ dem Endkunden anzubieten. Damit vereint der Mobilfunkanbieter nicht nur die Kompetenzen der Verbindungsherstellung über Funknetze auf sich, sondern auch die LBS-Dienstleistungserbringung und gewinnt weitere Einblicke in das Verhalten einzelner Kunden und Kundengruppen. Als Negativbeispiele wären hierfür die Firmen O_2, Vodafone und in Japan NTT DoCoMo zu nennen, die eine solche Geschäftspraxis zeigen. Positivbeispiel ist TrackYourChild, welcher sich als selbstständiger LBS-Anbieter in Deutschland etabliert hat und dem Endkunden die Ortung von Personen - in aller Regel die eigenen Kinder - anbietet. TrackYourChild bezieht zur Diensterbringung die Ortungsdaten direkt vom zuständigen Mobilfunkanbieter, eine Rückfrage am Gerät des zu Ortenden findet nicht statt, da diese Einwilligung bereits bei Vertragsabschluss unterzeichnet werden musste.

Eine ähnliche Aufgabenteilung kann auch bereits in tieferen Schichten stattfinden und somit die Datenerhebung - welche oftmals nicht zu vermeiden ist - auf mehrere unabhängig voneinander arbeitetende Instanzen verteilen. Anzuführen wären hier die sich immer stärkerer Verbreitung findenden IEEE 802.11b Netzwerke. Im Augenblick existieren zwei Vorgehensweisen bei großen Mobilfunknetzbetreibern die WLAN-Funknetze in ihr UMTS-Netz zu integrieren. Die eine Gruppe tendiert dazu, in ganz Deutschland an ausgewählten Orten eigene WLAN-Access-Points aufzustellen und zu betreiben. Die andere Gruppe indessen versucht Fremd-Access-Points, welche von unabhängigen Betreibern aufgestellt werden, in ihr Netz aufzunehmen. Letztere unterstützt infolgedessen aktiv den Datenschutz, indem sie auf eine Anhäufung von Wissen bei nur einer Instanz verzichtet und stattdessen dieses auf mehrere unabhängig voneinander arbeitende Unternehmen verteilt. Erst ein Zusammenschluss aller Betreiber würde die gleichen Konsequenzen der Bewegungsprofilerstellung mit sich bringen, wie die erste Variante, bei der der Mobilfunknetzbetreiber alle Access-Points selbst kontrolliert.

In Hinsicht auf das bisher Angeführte lassen sich in der heutigen Zeit mehrere Richtungen bezüglich der Datenverteilung identifizieren, die unterschiedlich zu beurteilen sind. Zum einen existieren diejenigen die eine Datenanhäufung forcieren und dadurch die Privatsphäre eines einzelnen leicht gefährenden können. Auf der anderen Seite gibt es Ansätze, die eine Datenverteilung unter unabhängig voneinander arbeitenden Betreibern anstreben. Zum jetzigen

Zeitpunkt lässt sich allerdings noch nicht feststellen, welche Variante in Zukunft den Markt dominieren wird.

Ortungsverfahren Blickt man auf den bisherigen Einsatz von Ortungsverfahren in Deutschland, so lassen sich lediglich zwei häufig verbreitete identifizieren. Zum einen das sehr bekannte GPS, welches von den Vereinigten Staaten betrieben wird und zum anderen das sehr einfach einzusetzende Zell-Identifikationsnummern-Verfahren in Mobilfunknetzen. Geht man zunächst von der Annahme aus, dass dem Mobilfunknetzbetreiber uneingeschränktes Vertrauen geschenkt werden kann, so sind beide Verfahren aus Kundensicht als gleichwertig zu betrachten. Allerdings ändert sich die Beurteilung, sofern der Mobilfunkanbieter nicht mehr in den Kreis der Vertrauenswürdigen mit einbezogen wird. In diesem Fall sollten ausschließlich terminalbasierte oder wenigstens gemischte Verfahren (semiautonome) zum Einsatz kommen. Dadurch eröffnet sich dem Nutzer die Möglichkeit selbst über die Datenherausgabe zu entscheiden. Bezogen auf Deutschland hat sich jedoch herausgestellt, dass überwiegend das netzbasierte Zell-Id-Verfahren eingesetzt wird.

Ausgestaltung der Kommunikationsnetze Betrachtet man sich die Ausgestaltung der Kommunikationsnetze, über die letztendlich die LBS-Dienste abgewickelt werden, so zeigen sich im aktuellen LBS-Umfeld gravierende Mängel. So hat beispielsweise ein GSM-Netzbetreiber, unabhängig vom Einsatz terminal- oder netzbasierter Ortungsverfahren, die Möglichkeit einen Kunden mithilfe der netzeigenen Sendemasten zu orten und dessen Position zu bestimmen. Darüber hinaus werden die Positionsdaten (meist in Form des Location Area Identifiers (LAI)) zum Verbindungsmanagement verwendet. Zwar existieren in der Wissenschaft bereits seit längerem Ansätze zur Vermeidung der offenen Speicherung von Verbindungsdaten [28], dennoch wurden diese von der Mobilfunkindustrie bisher nicht angenommen. Ähnlich ist die Situation in IEEE 802.11b Funknetzen. Über die MAC-Adressen stehen den Access-Points eindeutige Identifikatoren zur Verfügung, mithilfe derer ein unbemerktes Verfolgen von Dienstnutzern bis auf wenige Meter genau in diesen Netzen möglich ist. Auch hier existieren Lösungsvorschläge, die in Kapitel 4 noch näher erläutert werden.

Insgesamt lässt sich festhalten, dass besonders dieser Bereich noch stark ausbaufähig scheint und zum jetzigen Zeitpunkt noch lange nicht alle Potentiale seitens der Netzbetreiber ausgeschöpft sind um datenschutzfreundliche LBS anbieten zu können.

Einsatz von datenschutzfreundlichen Verfahren und Techniken auf der Anwendungsschicht Einer der stärksten Schutzmechanismen in Deutschland ist zurzeit die vom Deutschen Gesetzgeber vorgeschriebene Einwilligung zur Datenerhebung. Hier kommen wiederum zwei Alternativen zum Einsatz. Wie bereits zuvor erwähnt, verlangt der Anbieter TrackYourChild bei Vertragsabschluss eine Einverständniserklärung zur Positionsfeststellung, worin geregelt wird, dass der Endgerätebesitzer im Falle einer Ortung nicht nochmals per Short Message Service (SMS) informiert werden muss. Andere LBS-Anbieter, wie zum Beispiel O_2 machen die Vertragsgestaltung abhängig von der Anwendung. Im Fall des angebotenen „Home-Tarifs“, der in die Kategorie des Location Based Billing einzuordnen ist, wird wie bei TrackYourChild eine einmalige Einverständiserklärung unterschrieben. Dahingegen verlangt O_2 bei einer einmaligen und kostenpflichtigen Endgeräteortung vom zu Ortenden die Erlaubnis, dass die Ortung durchgeführt werden darf. Zu diesem Zweck versendet O_2 eine

SMS an das Endgerät, welche innerhalb einer festgelegten Zeitspanne positiv zu beantworten ist.

Induziert durch den Deutschen Gesetzgeber, hat sich ein Schutzmechanismus gebildet der vor einer unkontrollierten Ortung schützen soll. Allerdings ist ein gravierender Nachteil anzusprechen. Der Endgerätebesitzer kann nie selbst kontrollieren, ob ein Mobilfunkbetreiber nicht doch vielleicht eine Ortung durchführt, ohne den Endgerätebesitzer darüber zu informieren. Des Weiteren wäre selbst bei späterem bekannt werden eines Mißbrauchs, die Tat bereits erfolgt, welche unter Umständen mit anderen Techniken hätte verhindert werden können.

Neben der expliziten Abfrage ob eine Ortung durchgeführt oder abgelehnt werden soll, existieren noch eine Reihe weiterer Methoden auf der Anwendungsschicht zur Steigerung der Privatsphäre, wie zum Beispiel Identitäts- und Positionsverschleierung. Jedoch konnte bei den untersuchten LBS kein Einsatz der unter Anderen in Kapitel 4 beschriebenen Verfahren gefunden werden.

3.2.3 Bedrohungen

Sowohl aus den Defiziten der rechtlichen als auch technischen Vorkehrungen zur Erhöhung des Datenschutzes in LBS ist es möglich Bedrohungen für einen Nutzer von LBS zu finden. Unterschieden werden kann zwischen zwei Ebenen. Die erste versucht anwendungsabhängig Bedrohungen für LBS-Nutzer zu quantifizieren und daraus Schutzvorkehrungen abzuleiten. Die zweite Ebene hingegen ist allgemeinerer Natur. Hier wird der Versuch unternommen allgemeingültige Gefahrenpotentiale über das gesamte LBS-Spektrum hinweg zu spezifizieren. Bei einer Auflistung von „Meta-Bedrohungen“ sind sozusagen alle anwendungsspezifischen Bedrohungen mit inbegriffen und es können über alle LBS hinweg geltende Schutzvorkehrungen gesucht werden. Innerhalb des Projekts PRIME wurde eine solche Liste aufgestellt und sie enthält folgende Bedrohungen:

Bedrohung	**Beschreibung/Beispiel**
Profilbildung	LBS speichert über längere Zeit die Nutzungs- und Bewegungsprofile der Kundschaft ab. Dadurch wird die Bildung von detaillierten Profilen ermöglicht.
Tracking	Daten über die aktuelle Position und Bewegungsrichtung werden beispielsweise für Kidnapping o.ä. mißbraucht.
Zusammenführung von Datenbeständen	Die Zusammenführung von Datenbeständen mehrerer Dienstanbieter verschärft das Problem der Profilbildung.
Verfügbarkeitsverlust	Positionsabhängig könnte ein Angreifer SPAM-Attacken auslösen, die zu einem Erreichbarkeits- und Verfügbarkeitsverlust führen.
Analyse sensibler Daten	Mithilfe von Positionsinformationen können zum Beispiel Aufenthalte in Kliniken festgestellt werden.
Analyse soziale Beziehungen	Dienstanbieter können das soziale Umfeld eines Nutzers genau analysieren.
Gruppenzwang	Es könnten Situationen entstehen, in denen Einzelpersonen Ortsinformationen über sich preisgeben, da eine für sie relevante Gruppe dies auch macht.

Tabelle 3.1: Bedrohungen für LBS-Nutzer [30, 6]

Wie Tabelle 3.1 zu entnehmen ist, wurden bisher sieben Hauptbedrohungen, aus denen sich anwendungsabhängige Gefahren ableiten lassen, gefunden.

3.2.4 Zusammenfassung

Zusammenfassend lässt sich festhalten, dass gerade in Deutschland die rechtliche Basis hinsichtlich des Datenschutzes sehr stark ausgeprägt ist. Darüberhinaus scheint sich jedoch der Einsatz von datenschutzfreundlichen Techniken und organisatorischen Maßnahmen noch nicht etabliert zu haben. Bis auf die gesetzlich vorgeschriebene Implementierung elektronischer Einwilligungen per SMS oder ähnlichem, haben die LBS-Anbieter und auch Mobilfunkanbieter kaum Schutzvorkehrungen für LBS-Teilnehmer aufgebaut, die von diesen in Anspruch genommen werden könnten. Besonders ist hier auf den Bereich der Schutzmaßnahmen zu achten, die der Nutzer selbst auf seinem Endgerät ohne Zuhilfenahme von Dritten durchführen kann. Wahrscheinlich durch die Endgeräteentwicklung bedingt, konnten bei den untersuchten Anwendungen keine solchen Schutzvorkehrungen gefunden werden.

Kapitel 4

Privacy Enhancing Technologies für LBS

In diesem Kapitel werden einzelne *Bausteine* (Verfahren und Methoden) zur Erstellung von datenschutzfreundlichen Location Based Services dargestellt und erläutert. Dazu ist das Kapitel zur näheren Darstellung und Erläuterung der Methoden in die Teilbereiche „Datenvermeidung“, „Datenverteilung“ und „Selbstdatenschutz und Selbstregulierung“, welche an die Prinzipien für Privacy Enhancing Technologies (PET) von Hansen [39, S. 305] angelehnt sind, unterteilt. Abschließend bietet Kapitel 4.5 eine kurze Zusammenfassung der dargestellten technischen und organisatorischen Vorschläge die für die Konstruktion von datenschutzfreundlichen Location Based Services in Kapitel 6 von Bedeutung sind.

4.1 Datenvermeidung auf der Anwendungsschicht

Als Datenvermeidung bezeichnet man das Prinzip von der Nutzerseite genau so viele Daten an den LBS-Dienst zu schicken wie dieser benötigt um die angeforderte Dienstleistung zu erbringen. Jede zusätzliche Dateneinheit wäre unnötig und würde eine detaillierte Erfassung der Nutzergewohnheiten auf Dienstanbieterseite nur fördern. In diesem Kapitel werden entsprechende Methoden vorgestellt, wie das Prinzip der Datenvermeidung auf der Anwendungsschicht bei LBS-Diensten effektiv umsetzbar ist.

Als Grundlage für die nachfolgenden Ausführungen wird zunächst angenommen, dass eine einfache LBS-Anfrage A ein Tritupel bestehend aus einem identitfizierenden Merkmal I, einer Positionsangabe P und einem weiteren Datenfeld D ist. Demzufolge stellt sich eine Nutzeranfrage wie folgt dar: $A = \{I, P, D\}$. Ohne besondere Schutzvorkehrungen könnte ein potentieller Angreifer die Anfrage leicht abfangen und die Position und Identität des Nutzers ermitteln. Für die nachfolgenden Unterabschnitte wird angenommen, dass ein Angreifer, der die Anonymität eines Dienstnutzers verletzen will, über folgende Möglichkeiten verfügt:

1. Der Angreifer kann Funk- als auch Festnetz-Netzwerke abhören.
2. Ihm ist es möglich Daten, die zum Beispiel der Diensteanbieter gespeichert hat, abzurufen und zu analysieren.
3. Er hat eventuell weitere Informationen über das Zielobjekt.

Die nun folgenden Untersuchungen gliedern sich wie folgt. Die Abschnitte 4.1.1 und 4.1.2 beschäftigten sich mit dem Thema, wie die Identität I einer Person möglichst effektiv geschützt werden kann. Da in den meisten Anwendungsfällen ein Schutz der reinen Identitätsinformationen jedoch nicht ausreichend ist, gehen die nachfolgenden Abschnitte auf Techniken ein, die zusätzlich die Positionsinformationen zu schützen versuchen. Wann und unter welchen Umständen die einzelnen technischen Maßnahmen eingesetzt werden sollten, wird in Kapitel 6 eingehend untersucht. Des Weiteren wird die Annahme getroffen, dass zur Realisierung der einzelnen PET-Komponenten die jeweils tiefer liegenden Anwendungsschichten wenigstens das gleiche Schutzniveau realisieren, wie die Anwendungsschicht, in der die betrachtete PET-Komponente implementiert wird.

4.1.1 Anonymisierung und Pseudonymisierung

Eine im Internet weit verbreitete Methode, Dienste für Benutzer datenschutzfreundlich zu gestalten, ist die Pseudonymisierung oder Anonymisierung der identifizierenden Merkmale innerhalb einer Benutzeranfrage A. Abbildung 4.1 zeigt die verschiedenen Arten von Pseudonymen, wobei der Schutzgrad von oben nach unten zunimmt.

Pfitzmann und Köhntopp definieren die Pseudonym-Arten wie folgt [67, S. 6]:

1. **Personen-Pseudonyme:** Ein Personen-Pseudonym ist ein Platzhalter für die wirkliche Identität einer Person, der für alle Arten von Transaktionen verwendet werden kann.
2. **Rollen-Pseudonyme:** Die Verwendung von Rollen-Pseudonymen setzt voraus, dass eine Person verschiedene Rollen im alltäglichen und so auch im „elektronischen Leben“ annehmen kann. Jeder dieser Rollen kann ein separates Pseudonym zugewiesen werden, mit dem sich der Pseudonym-Besitzer im elektronischen Verkehr zu erkennen gibt.
3. **Beziehungs-Pseudonyme:** Im Gegensatz zu den Rollen-Pseudonymen, wird für jeden Kommunikationspartner ein eigenes so genanntes Beziehungs-Pseudonym gewählt, welches auch nach einem Rollenwechsel für diesen Kommunikationspartner erhalten bleibt.
4. **Rollen-Beziehungs-Pseudonyme:** Diese Pseudonym-Art kombiniert die beiden voranstehenden Ansätze. Ein Nutzer wählt pro Rolle und Kommunikationspartner ein Pseudonym.
5. **Transaktions-Pseudonyme:** Transaktions-Pseudonyme sind die stärkste Art der Anonymisierung, da der Nutzer für jede Transaktion, unabhängig vom Wechsel der Rolle oder des Kommunikationspartners sein Pseudonym wechselt.

Pseudonyme sind hinsichtlich der Verwendung in LBS-Anwendungen sehr einfach zu implementieren, sowohl endgeräteseitig oder netzseitig. Selbst die Einführung von Transaktionspseudonymen, als stärkste Art der Pseudonymisierung, ist effizient zu bewerkstelligen, sofern das mobile Endgerät bei jeder Anfrage A sein identifizierendes Merkmal I wechselt. Eine Reihe von Anfragen mit Transaktions-Pseudonymen würde dann wie folgt aussehen: $A_1 = \{I_1, P_1, D\}$; $A_2 = \{I_2, P_2, D\}$; $A_3 = \{I_3, P_3, D\}$. Somit scheint zunächst eine Verknüpfung der verschiedenen Anfragen, seitens des LBS-Diensteanbieters, nicht möglich.

Diese Vermutung der Unverkettbarkeit bei Verwendung von Transaktions-Pseudonymen kann jedoch unter zwei Umständen wiederlegt werden. Erstens wenn die Abrufhäufigkeit des Dienstes sehr hoch ist und zweitens, sehr präzise Positionsangaben P_1, P_2, P_3 in den Anfragen geliefert werden. Trifft dies zu, so kann mithilfe geschickt konstruierter Algorithmen und unter

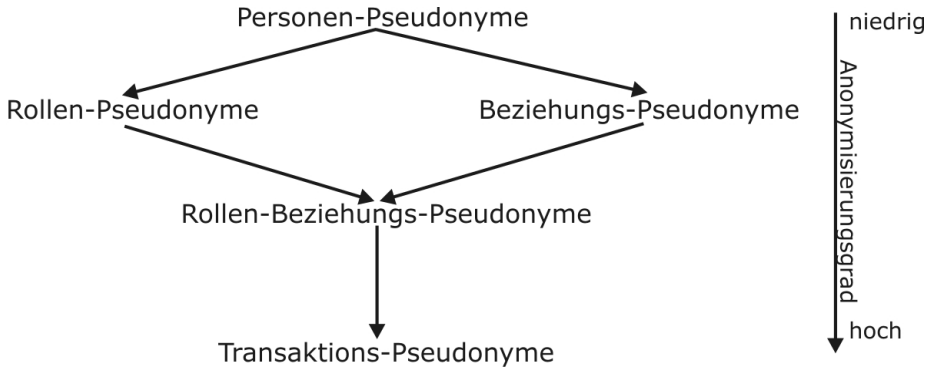

Abbildung 4.1: Pseudonym-Arten [67, S. 7]

Verwendung statistischer Verfahren die jeweilige Wegstrecke von Dienstnutzern rekonstruiert werden. Zudem haben empirische Analysen belegt, dass Menschen mit einer sehr viel höheren Wahrscheinlichkeit in die Richtung weiterlaufen in die sie bisher liefen, als sich unerwartet in die Gegenrichtung zu bewegen [7, S. 52]. Dadurch kann zu einem beliebigen Startpunkt P_x, aufgrund der hohen Auflösung hinsichtlich der Zeit und Abrufhäufigkeit, das Vorgängerpseudonym I_{x-1} und Nachfolgerpseudonym I_{x+1} ermittelt werden. [7, S. 48] Die Folge ist, dass ein Angreifer unter diesen Annahmen ein pseudonymisiertes Bewegungsprofil erstellen kann.

Die Verwendung von Langzeit-Pseudonymen, wie zum Beispiel Rollen- oder Beziehungs-Pseudonyme, ist mit höheren Risiken behaftet. In diesen Fällen entfällt der aufwändige Prozess der Pseudonym-Zusammenführung und ein Angreifer benötigt jediglich zwei Schritte zur Identifizierung des Dienstnutzers. Erstens muß er die Orte bestimmen, an denen sich der Nutzer am häufigsten aufhielt. Basis der Analyse sind die beim Diensteanbieter aufgezeichneten Datensätze $A_1, A_2, ..., A_N$. Je nach verwendeter Positionsbestimmungsmethode können dann verschiedene Indikatoren zur Bestimmung von interessanten Aufenthaltsbereichen herangezogen werden. Zum einen ist die Auswertung von Standzeiten sehr leicht möglich. Dadurch lassen sich Rückschlüsse auf Anfangs- und Endpunkte von Wegstrecken ziehen. Ein weiterer, schwächerer Indikator kann bei der Positionsbestimmung über GPS als Anhaltspunkt dienen, der GPS-Signalverlust. Solche Aufzeichnungslücken sind Anzeichen, dass der Dienstnutzer ein Gebäude betreten hat. Allerdings ist diese Methode recht fehleranfällig, da beispielsweise hoch bebaute Stadtviertel oder ein Batterieausfall zu gleichen Ergebnissen führen. Neben den eben genannten Problemen müssen auch Ungenauigkeiten während der Positionsbestimmung Berücksichtigung finden. So liefern zum Beispiel zwei GPS-Messungen an einem Punkt in der Regel zwei unterschiedliche Positionsergebnisse mit einer Abweichung von durchschnittlich 15 Metern. Eine Lösung wäre einfach einen Clustering-Algorithmus, wie beispielsweise k-Means, auf die Datenmenge anzuwenden. [3, S. 102-106]

Sind die so genannten „Heimat-Zonen“ (engl. Home-Zones) identifiziert (in Abbildung 4.2 durch die Anhäufung von roten Punkten dargestellt), kann der Angreifer im zweiten Schritt versuchen die Identität einer Person festzustellen. Identifizierungsmerkmale sind in der Regel Arbeitsplätze oder die private Wohnung des Dienstnutzers. Die Kombination beider Angriffe bezeichnet man in der Literatur als „Home-Angriffe“. [7, S. 47-48][35, S. 1-2, 4-5]

Fazit: Aus den eben geschilderten Angriffen wird deutlich, dass eine alleinige Anonymisierung oder Pseudonymisierung der Merkmale, die eine Person direkt identifizieren, unter den oben genannten Annahmen völlig unzureichend ist. Vielmehr ist die Anonymisierung nur *ein*

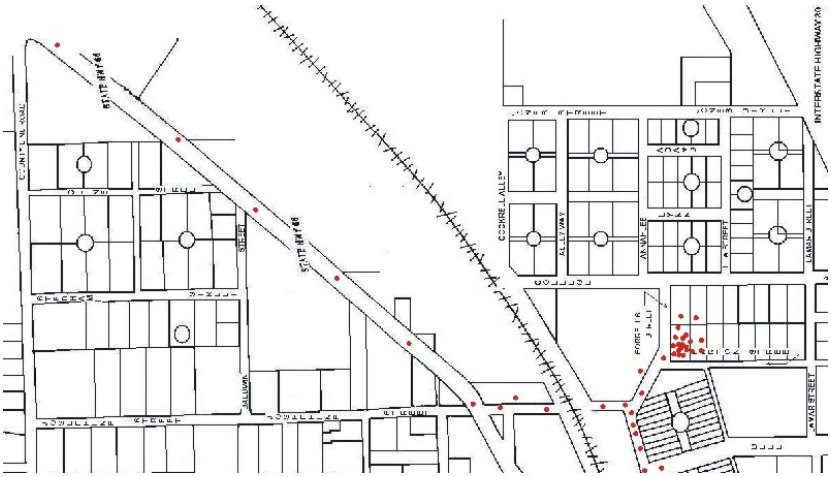

Abbildung 4.2: Identifizierung von Home-Zonen

Werkzeug um datenschutzfreundliche LBS zu konstruieren. Die Kombination mit weiteren Verfahren ist bei Langzeit-Pseudonymen oder hohen zeitlichen und geographischen Auflösungen zwingend notwendig, wenn auf einen sehr hohen Anonymisierungsgrad Wert gelegt wird.

4.1.2 Pseudonymisierung mithilfe von Mix-Zonen

Beresford und Stajano erstellten in ihrer Arbeit [7] ein Framework, dass durch kontrolliertes Wechseln von Pseudonymen die Unverkettbarkeit von unterschiedlichen pseudonymisierten Bewegungsprofilen eines LBS-Nutzers gewährleisten soll (Abbildung 4.3). Damit soll verhin-

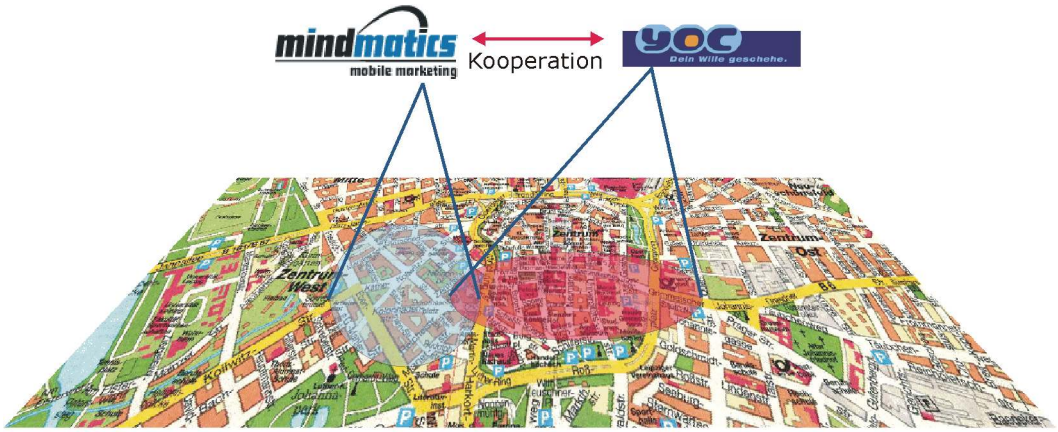

Abbildung 4.3: Mix-Zonen im Überblick

dert werden, dass zwei LBS-Anbieter ihre jeweils pseudonymisierten Bewegungsprofile zu einem großen Profil zusammenlegen können, um darauf einen Home-Angriff durchzuführen. Als Hilfsmittel wird das Konzept der *mix zones* - Mix-Zonen - eingeführt, welches bereits im Bereich des Information Hiding, unter dem Namen „Mix Network“, sehr gut erforscht ist.

Dienstnutzer müssen somit über eine Trusted Third Party (TTP) mit dem LBS-Dienstanbieter kommunizieren, um nicht direkt ihre Identität bekannt zu geben.

Die Autoren definieren die Begriffe Mix-Zone und Applikations-Zone wie folgt:

„We define a mix zone for a group of users as a connected spatial region of maximum size in which none of these users has registered any application callback; for a given group of users there might be several distinct mix zones. In contrast, we define an application zone as an area where a user has registered for a callback.“ [7, S. 50]

In Abbildung 4.4 stellen die drei Kästchen Flughafen, Cafe und Universität so genannte Applikationszonen dar, in denen ein Dienstnutzer angebotene Dienste in Anspruch nimmt. Während des Aufenthalts in einer Mix-Zone findet dagegen keine Dienstnutzung statt. Die Festlegung wo und wie groß eine Mix-Zone zu einem bestimmten Zeitpunkt ist, kann die TTP entweder statisch im voraus bestimmen oder dynamisch für jede Gruppe berechnen.

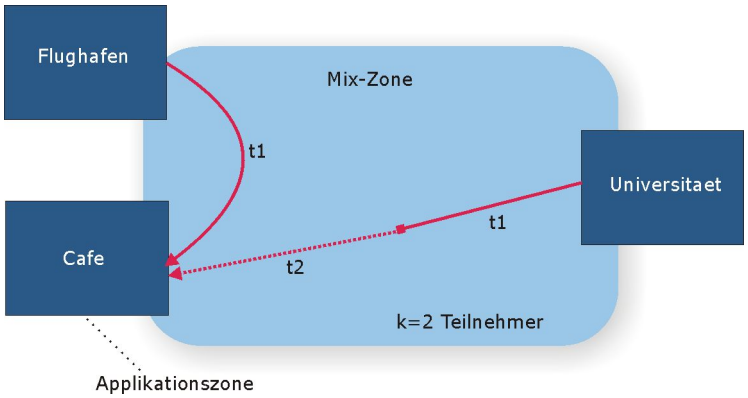

Abbildung 4.4: Mix- und Applikations-Zonen [7, S. 50]

Die Funktionsweise einer Mix-Zone läßt sich nun folgendermaßen beschreiben. Während sich ein Nutzer innerhalb einer Applikations-Zone befindet, verwendet dieser ein und dasselbe Pseudonym, um mit dem Partner zu kommunizieren. Wechselt der Nutzer aber von einer Applikations-Zone in eine Mix-Zone, werden alle abonnierten Dienste „abbestellt“ und sofort die Pseudonyme gewechselt. Befinden sich wenigstens zwei Teilnehmer innerhalb der Mix-Zone - was sinnvollerweise anzunehmen ist - sind die Personen „gemixt“. Tritt ein Nutzer wieder von einer Mix-Zone in eine Applikations-Zone ein, so erscheint dieser unter einer neuen Identität. Die Autoren schlagen in ihrer Arbeit [7, S. 49-50] zur Bestimmung der optimalen Größe einer Mix-Zone die k-Anonymitäts-Kennzahl vor. In Anlehnung an [67] und [80] definieren Gruteser und Grunwald [35] k-Anonymität wie folgt:

> „... we consider a subject as *k-anonymous* with respect to location information, if and only if the location information presented is indistinguishable from the location information of at least $k-1$ other subjects.“[35, S. 5]

Allerdings ist die Konstruktion einer Mix-Zone, die den angestrebten Anonymisierungsgrad erreicht, nicht einfach. Die Autoren beschreiben eine Beispielsituation in der trotz Verwendung einer Mix-Zone Verkettungen möglich sind. Abbildung 4.4 zeigt, dass zwei Nutzer A und B gleichzeitig zum Zeitpunkt t die Mix-Zone betreten. A verläßt den Flughafen-Bereich und B die Universität. Ziel beider Personen ist das Cafe. Problematisch ist nur, dass A einen

viel kürzeren Weg als B zurückzulegen hat. Ein Angreifer der die Situation während den Zeitpunkten t, $t+1$ und $t+2$ beobachtet hat, kann nun sofort schlussfolgern, dass A zum Zeitpunkt $t+1$ vom Bereich Flughafen zum Cafe gewechselt ist. Denn nur A konnte im Zeitpunkt $t+1$ das Cafe betreten, B hingegen war zu diesem Zeitpunkt noch auf der Hälfte seines Weges und erreichte das Cafe erst in $t+2$. Demzufolge kann man zu dem Ergebnis kommen, dass in bestimmten Situationen kein vollständiges mixen der Teilnehmer möglich ist. Das ist dann der Fall, wenn die Mix-Zone größer ist als die Wegstrecke, die ein Nutzer innerhalb eines Zeitintervalls zurücklegen kann.

Des Weiteren haben empirische Untersuchungen gezeigt [7, S. 51-52], dass die Kennzahl k-Anonymität zur alleinigen Bestimmung des Anonymitätsgrades innerhalb von Mix-Zonen nicht ausreicht. Grund dafür ist, dass die k-Anonymität nicht das Bewegungsverhalten der Personen und die Form und Größe der Räume, die sich innerhalb einer Mix-Zone befinden, berücksichtigt. Betreten beispielsweise zwei Personen einen Raum durch zwei sich gegenüberliegende Eingänge und dient der Raum als Mix-Zone, so kann ein Angreifer, trotz scheinbar gutem Mix-Verhaltens, leicht die Pseudonyme verlinken. Möglich macht dies das typische Bewegungsverhalten von Menschen. Dient die Mix-Zone als eine Art Durchgang, so ist es sehr unwahrscheinlich, dass eine Person mitten im Raum umdreht und wieder zurückläuft [7, S. 53]. Zur Messung eines solchen Verhaltens innerhalb einer Anonymitätskennzahl schlagen die Autoren Shannon's Entropie-Kennzahl vor:

$$h = -\sum_i p_i \cdot \log_2 p_i$$

Geht man von der Annahme aus, dass eine Person den Durchgang innerhalb eines Zeitintervalls t durchläuft, so kann man folgende Bewegungsmatrix[1] erstellen:

$$M = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = \begin{pmatrix} 123 & 3 \\ 22 & 175 \end{pmatrix}$$

Die Zelle c_{11} zeigt die Anzahl der Personen im Beobachtungszeitraum, die durch den Gang von links nach rechts gelaufen sind. Zelle c_{22} den dazu entgegengesetzten Fall. Die Zellen c_{12} und c_{21} beinhalten die Zählerstände für Vorfälle in denen Personen links oder rechts in den Raum eingetreten sind und den Raum durch die gleiche Tür wieder verlassen haben. Die Konstruktion zeigt deutlich, dass es sehr viel wahrscheinlicher ist durch den Gang zu laufen, als in ihm zu drehen. Die Wahrscheinlickeit umzudrehen beträgt lediglich:

$$P(Drehung) = \frac{c_{12}}{\sum_{ij} c_{ij}} + \frac{c_{21}}{\sum_{ij} c_{ij}}$$

daraus folgt, $P(Drehung) = 0,0013$. Für einen Angreifer ist aber die bedingte Wahrscheinlichkeit $P(Drehung|Beobachteter)$ von größerer Bedeutung, diese beträgt $P(Drehung|Beobachteter) = 0,00315$. Demnach dreht eine observierte Person mit einer Wahrscheinlichkeit von 0,3 Prozent um und durchschreitet die Zone mit einer Wahrscheinlichkeit von 99,7 Prozent. Die daraus resultierende Entropie nach Shannon beträgt $h = 0,0265$ Bit. Wäre die Entropie gleich 1, so könnte ein Angreifer die Pseudonyme nicht miteinander verlinken. Allerdings ist der Wert der Entropie in diesem Beispiel weit unter 1 und somit kann ein Angreifer sehr wohl in bestimmten Situationen die Pseudonyme wieder verknüpfen.

Fazit: An diesem Beispiel konnten zwei Ergebnisse herausgearbeitet werden. Erstens ist die k-Anonymität als alleinige Messgröße für die Anonymisierung in Mix-Zonen nicht ausreichend,

[1] Die Zahlenwerte sind in Anlehnung an [7] entstanden.

da zum Beispiel auch auf das Bewegungsverhalten der Dienstnutzer geachtet werden muss. Zweitens ist bei der Konstruktion der Zonen darauf zu achten, dass die typischen Bewegungsmuster von Teilnehmern eine möglichst hohe Entropie erzeugen. Zum Beispiel wäre es denkbar als Mix-Zone einen Raum mit nur einem Eingang zu wählen. Überdies ist stets darauf zu achten, für unterschiedliche Dienste auch verschiedene Pseudonyme zu Nutzen (Rollenpseudonyme) und diese, wenn möglich, ständig zu wechseln (Transaktionspseudonyme). Zum Schluß ist anzumerken, dass sich dieser Ansatz unter Berücksichtigung der jeweiligen geographischen Gegebenheiten für viele Anwendungsszenarios eignet und die bereits vorher angesprochenen Home-Angriffe wesentlich erschwert, wenn nicht sogar verhindert. Dennoch ist innerhalb einer Applikations-Zone die Erstellung von Bewegungsprofilen möglich, es sei denn der LBS-Nutzer schützt sich hier mit zusätzlichen Methoden. Dies war jedoch nicht das anvisierte Ziel des Mix-Zonen-Konzeptes. Vielmehr stand die Unverkettbarkeit von Bewegungsdatensätzen verschiedener Applikationsanbieter im Vordergrund.

4.1.3 Positionsverschleierungsmechanismen

Positionsverschleierungsmechanismen versuchen die im vorangegangenen Kapitel zur Anonymisierung und Pseudonymisierung geschilderten „Home-Angriffe“ zu hemmen und unter bestimmten Bedingungen zu verhindern. Es muss also eine Zielfunktion gefunden werden, die als Ergebnis die Positionskoordinaten oder Aufnahmezeitpunkte der Positionsbestimmung in einer Anfrage A so modifiziert, dass der angeforderte Dienst erbracht werden kann, aber ein Home-Angriff verhindert oder zumindestens abgeschwächt wird.

Abschnitt 4.1.3.1 schildert zunächst die nahe liegendste Methode, die Präzision der Positionsbestimmung zu verschlechtern (engl. spatial cloaking) bei gleichzeitiger Beibehaltung der zeitlichen Auflösung. Der zweite Abschnitt 4.1.3.2 verändert hingegen die zeitliche Auflösung (engl. temporal cloaking) und übermittelt die maximal erreichbare Positionsgenauigkeit. Im dritten Abschnitt, Hybride Methoden, wird eine Kombination aus den beiden vorherigen Verfahren beschrieben.

4.1.3.1 Räumliche Positionsverzerrung

Wie eingangs erwähnt, versuchen Methoden der räumlichen Positionsverzerrung das Positionssignal soweit zu verfälschen oder unscharf zu machen, dass eine Diensterbringung möglich ist, aber Home-Angriffe unterbunden oder abgeschwächt werden. Der Grundgedanke dieser Methoden ist durch Hinzufügen von Unschärfe U eine hoch präzise Positionsbestimmung zu verschlechtern ($P_x^R = P_x + U$) und als Resultat Dienstnutzer in einer Anonymitätsgruppe[2] verschwinden zu lassen. Das Augenmerk bei diesen Methoden liegt demnach vorrangig auf der richtigen Dimensionierung von U, um die Anonymitätsgruppe ausreichend groß zu gestalten. Voraussetzung für die Anwendung dieser PET-Komponente ist, dass der genutzte Dienst keine höhere Genauigkeit als $P_x + U$ erfordert.

Dezentraler Ansatz: Im dezentralen Ansatz erfolgt die Dimensionierung von U nicht über eine zentrale Instanz (TTP), sondern wird entweder durch den Dienstnutzer selbst gewählt oder der Dienstanbieter stellt ein maximales, für den Dienst noch sinnvolles U dem Dienstnutzer zur Verfügung. Mathematisch ist die geforderte Verschlechterung über viele Wege

[2] Definition siehe [67, S. 2]

zu erreichen. So schlagen [41, S. 4] vor einfach die letzten Stellen der Positionsinformation abzuschneiden oder einen zufälligen Fehler hinzuzufügen. Neben der mathematischen Verschlechterung der ermittelten Positionsinformationen könnte der Dienstnutzer aber auch ein Positionsbestimmungssytem nutzen, dass von Haus aus nur die geforderten Präzision liefert.

Der dezentrale Ansatz hat zwei Nachteile. Erstens kann nicht sichergestellt werden, dass das verwendete U eine ausreichend große Anonymitätsgruppe schafft. Befindet sich ein Dienstnutzer in einer dicht besiedelten Gegend, so kann bei ausreichend großem U sicherlich die Annahme getroffen werden, dass die Anonymitätsgruppe richtig dimensioniert ist. Dagegen sinkt die Wahrscheinlichkeit einer ausreichend großen Anonymitätsgruppe rapide, wenn sich der Dienstnutzer in ländlichen Gebieten mit geringen Nutzerzahlen aufhält. In diesen Gebieten könnte sogar die datenschutzfreundliche Nutzung von Wetterdiensten, mit einem U zwischen 5-10 Kilometern, in Frage gestellt werden. Als zweiter Nachteil ist zu nennen, dass der dezentraler Ansatz keine dynamische Anpassung von U zulässt und somit immer „verwendbare“ Genauigkeit verloren geht. Um diesen Nachteil zu verdeutlichen, sei folgendes Beispiel angeführt. Nimmt ein LBS-Teilnehmer an einem positionsbasierten Werbedienst teil, so würde er, um sich selbst zu schützen, in städtischen Gebieten eine maximale Positionsgenauigkeit von 300 Metern[3] in seinem Endgerät einstellen. Wären aber zur gleichen Zeit in seinem Umfeld mehrere Personen, die den gleichen Dienst nutzen, so könnte die Positionsverfälschung weiter reduziert und die Dienstqualität damit erhöht werden, da selbst mit der genaueren Positionsangabe seine präferierte Anonymitätsgruppengröße zustande gekommen wäre.

Dennoch besitzt der dezentrale Ansatz auch einen Vorteil. Im Gegensatz zu der im nachfolgenden Absatz dargestellten zentralen Architektur muss ein Dienstnutzer seine Positionsdaten nicht einer dritten Instanz überlassen. Die Entscheidung, wie groß das U gewählt wird, liegt ausschließlich im Ermessensspielraum des Dienstnutzers. Der Dienstanbieter kann zwar einen Vorschlag für U unterbreiten auf den aber der Nutzer nicht einzugehen braucht, wenn er im Gegenzug dafür die eventuell geminderte Dienstqualität akzeptiert.

Zentraler Ansatz: Im Unterschied zum dezentralen Ansatz ist im zentralen Ansatz eine vermittelnde Instanz Z (TTP) zwischen Dienstnutzer und -anbieter geschaltet (siehe Abbildung 4.5). Die TTP sorgt für die optimale Bestimmung des jeweiligen U unter dem Zielkriterium der Anonymität. Für diese Optimierung sollte Z die Positionskoordinaten von jedem Nutzer mit maximaler Auflösung als Basisdaten vorliegen haben. Demnach zählt Z zum vertrauenswürdigen Bereich des Dienstnutzers. Um das optimale U berechnen zu können verwenden Grundwald und Gruteser die bereits bei den Mix-Zonen erwähnte Anonymitätsgruppenkennzahl k-Anonymität. Der Algorithmus zur Festlegung des optimalen U muss demnach die Positionsinformationen von Dienstnutzern soweit verschlechtern, dass sich im Gebiet, dass sich daraus ergibt, weitere $k-1$ Personen aufhalten. Die Anonymitätsstufe k_{min} ist für jeden Nutzer frei definierbar und beschreibt die minimal geforderte Größe der Anonymitätsgruppe.

Dank der Positionsoptimierung werden die zwei Nachteile des dezentralen Ansatzes vermieden. Erstens ist sichergestellt, dass die Positionsinformationen immer ausreichend unscharf sind und eine Anonymitätsgruppe mit wenigstens k_{min} Teilnehmern gewählt wird. Zweitens geht durch die Optimierung keine verfügbare Genauigkeit verloren. Die Positionsinformationen werden immer so verfälscht, dass optimalerweise wenigstens die k_{min}-Anonymitätsgruppe

[3] dieser Wert wurde frei gewählt

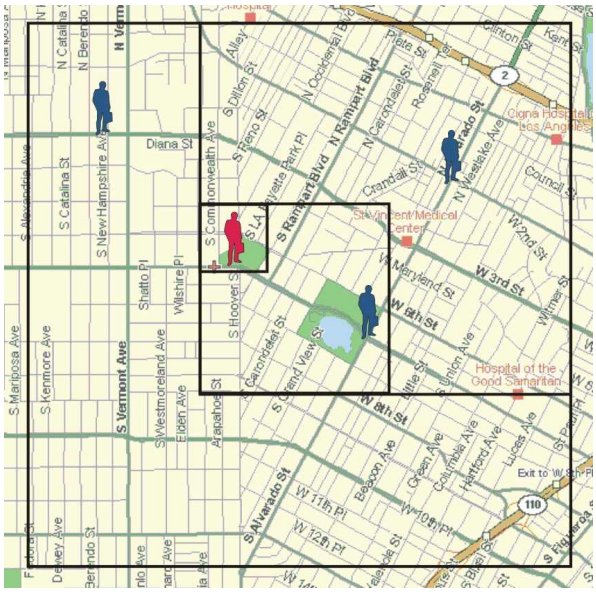

Abbildung 4.5: Algorithmus für den zentralen Ansatz zur Positionsverschleierung

realisiert wird. Eine darüber hinausgehende Verfälschung, wie sie im dezentralen Ansatz erfolgen könnte, ist nicht möglich. In Artikel [35] wird anhand einer Untersuchung verschiedener Verkehrssituationen ein deutliches Ergebnis gezeigt. Abbildung 4.6 stellt für verschiedene Gebiete (X-Achse) jeweils auf der linken Y-Achse, als Median abgetragen, die erreichte Positionsauflösung und auf der rechten Y-Achse das erreichte k als Mittelwert dar. Bei den Gebieten 1 und 2 handelt es sich um Autobahnen, die Gebiete 3 und 4 sind Hauptstraßen in größeren Stadtteilen. Man kann deutlich erkennen, dass Dienstnutzer die die Autobahn befahren Positionsangaben mit viel höherer Auflösung - zwischen 30 und 65 Metern - an ihre Diensteanbieter versenden können, als Nutzer von normalen Hauptverkehrsstraßen.

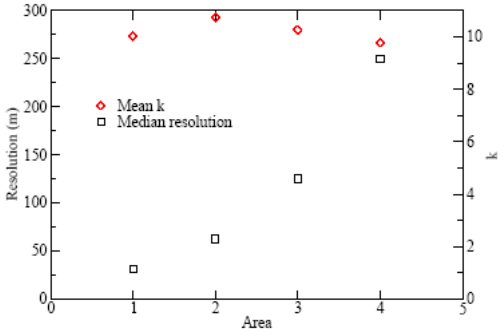

Abbildung 4.6: Beispiel für die räumliche Positionsverzerrung [35, S. 8]

Von Nachteil ist allerdings, dass jeder Dienstnutzer seine präzisen Positionsinformationen einem Dritten anvertrauen muss. Auch wenn entsprechende Zugriffsregelungen und Schutzmaßnahmen seitens der Positionsverschleierungsinstanz Z eingerichtet wurden, ist ein Missbrauch der gesammelten Daten eventuell nicht auszuschließen.

Hierarchische Positionsangaben: Die hierarchischen Positionsangaben wurden von [36] vorgeschlagen und verlagern die zentrale Instanz Z (aus dem vorherigen Ansatz) in ein vom Netzbetreiber zur Verfügung gestelltes Sensornetzwerk. Nach den Vorstellungen der Autoren soll der Anonymitätsalgorithmus in einem technischen Gerät gekapselt sein, so dass von außerhalb kein Dritter - auch nicht der Netzbetreiber - den Anonymisierungsprozess beobachten und manipulieren kann.

Als Messgröße für den Grad der Anonymität eines Dienstnutzers wurde wieder die k-Anonymität, mit k_{min} als minimale Größe der Anonymitätsgruppe, vorgeschlagen. Abbildung 4.7 zeigt beispielshaft den Aufbau eines solchen Netzwerkes. Verwendung findet ein so genanntes

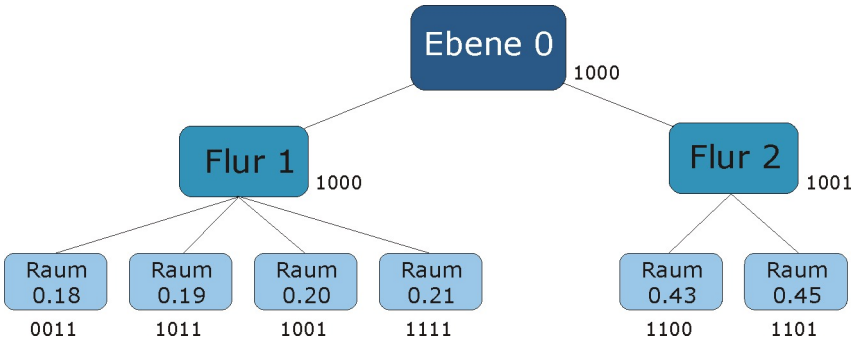

Abbildung 4.7: Hierarchische Positionsverzerrung

Multihop-Netzwerk, dass hierarchisch miteinander verkettet wurde. Die Blätter des gezeigten Baumes sind die kleinsten Positionseinheiten die das Sensornetzwerk liefern kann. Im hier abgebildeten Beispiel handelt es sich um einzelne Räume. Die nächst höher liegenden Ebenen aggregieren die darunter liegenden zu jeweils sinnvollen Einheiten - beispielsweise werden alle Räume eines Flurs in einem Knoten gebündelt. Zudem kennt jeder Knoten sein fest eingestelltes k_{min}. Stellt man sich die Positionsangaben, die das Netzwerk liefert als eine Aneinanderreihung von vierer Bit-Ketten vor, so konstruiert das Multihop-Netzwerk zur Positionsbestimmung folgende Positionskoordinaten für Raum $R0.18$ (sofern $k_{min}^{R_1}$ erfüllt ist): $0011\|1000\|1000$.

Ein Blatt R_x hat nun folgende Möglichkeit einen Nutzer zu schützen. Wird die eingerichtete Schwelle $k_{min}^{R_x}$ erreicht oder übertroffen, so liefert der Algorithmus zur nächst höheren Ebene die volle Positionsgenauigkeit. In Abbildung 4.7 würde Knoten $R0.19$ an $Flur1$ die Bit-Kette 1011 melden. Ist allerdings die notwendige Anonymisierungsschwelle nicht erreicht - es gilt $k < k_{min}$ - so muss der Algorithmus auf dieser Ebene die Position verfälschen. Eine Möglichkeit wäre, dass $R0.19$ einfach die Bit-Kette $xxxx$ zurückliefert. Diese Situation erfordert nun auch eine Berechnung durch den Knoten $Flur1$. $Flur1$ bildet sein k, indem er die einzelnen k der ihm direkt untergeordneten Knoten und Blätter aufsummiert. Gilt $k \geq k_{min}$, so liefert $Flur1$ an $Ebene0$ die Kette 1000, ansonsten werden die Bits verfälscht. Gruteser et alii verwenden zur Verfälschung einen Rundungsalgorithmus [36, S. 4].

Um Attacken auf Positionsbestimmungsnetzwerke zu verhindern erwähnen die Autoren, dass sämtliche Verbindungen entsprechend verschlüsselt und alle Datenpakete authentisiert sein müssen. Mithilfe von Dummy-Traffic, welcher ständig von allen Knoten und Blättern des Baumes zu ihren jeweils nächst höheren Elternknoten gesendet wird, sind Datenverkehrsanalysen eingeschränkt. Ein Angreifer könnte sonst relativ leicht schlussfolgern, dass in einem

Raum, in dem das dazugehörige Blatt keine Daten an die höhere Instanz sendet, keine Person anwesend ist, was wiederum eine eventuell zu verbergende Information ist.

Beim Ansatz der hierarchischen Positionsangaben muss der Nutzer sein Vertrauen vom Netzbetreiber (zentraler Ansatz) auf den Hersteller der Netzwerkkomponenten verlagern. Deshalb hat dieser mithilfe technischer Maßnahmen sicherzustellen, dass kein Dritter die technischen Komponenten „anzapfen“ und somit Positionsinformationen aufzeichnen kann. Des Weiteren ist beim Einsatz von hierarchischen Positionsbestimmungsnetzwerken zu berücksichtigen, dass diese einen maximalen Verfälschungsgrad besitzen. Betrachtet man den Extremfall, dass sich zum Beispiel Nachts null Uhr nur noch ein Mitarbeiter in einer Firma befindet, so kann dessen Positionsinformation maximal mit der obersten Ebene des Positionsbestimmungsnetzwerkes verfälscht werden. Eine Möglichkeit des Nutzers dem entgegen zu wirken wäre einfach die Dienstnutzung nicht in Anspruch zu nehmen. Ist die Dienstnutzung jedoch notwendig, so kann der Nutzer mit der Methode nicht ausreichend anonymisiert werden.

4.1.3.2 Positionsverschleierung durch zeitliche Verzerrung

Im vorangegangen Kapitel 4.1.3.1 wurde der eher intuitive Ansatz der räumlichen Positionsverzerrung ausführlich erläutert. Eine parallel zu diesem Ansatz existierende Methode ist die Positionsverschleierung durch Verzerrung der Zeitinformation innerhalb des übermittelten Positionssignals. Hierfür hat man sich den Datensatz zur Übermittlung von Positionsinformationen P wie folgt vorzustellen: $P = [x_1, x_2], [y_1, y_2], [t_1, t_2]$. Die Koordinaten $[x_1, x_2]$ und $[y_1, y_2]$ beschreiben ein zweidimensionales Aufenthaltsgebiet, in dem sich der Teilnehmer während der Zeitspanne $[t_1, t_2]$ befunden hat. Die bisher gezeigten Ansätze beschäftigten sich ausschließlich damit, eine Anonymitätsgruppe k durch Verfälschung der Positionskoordinaten zu schaffen. Diese Methode versucht die Anonymitätsgruppe durch „Dehnung“ des Zeitintervalls $[t_1, t_2]$ zu erzeugen. [35, S. 5]

Ein dezentraler Ansatz, wie er in Kapitel 4.1.3.1 für räumliche Positionsverzerrungsmethoden angesprochen wurde, scheint für die temporale Verzerrung aufgrund ähnlicher Probleme nicht sinnvoll zu sein. Dagegen lässt sich die zentrale, serverbasierte Variante gut implementieren. Als Maß für die Anonymität eines Teilnehmers wird wieder die k-Anonymität verwendet. Der Algorithmus, welcher in der zentralen Instanz Z verankert ist, könnte folgendermaßen arbeiten: Die zentrale Instanz sammelt so viele Dienstanfragen für ein Gebiet $([x_1, x_2], [y_1, y_2])$ von $k \geq k_{min}$ Teilnehmern, dass für jede der Anfragen das Zeitintervall auf $[t_1^k - Zufallszeitspanne, t_2^{aktuell}]$ geändert wird. Anschließend gibt Z alle Dienstanfragen mit korrigierten Zeitintervall an die Diensterbringer aus. Für einen Dienstanbieter ist somit nicht mehr erkennbar - sofern Pseudonymisierungstechniken für das identifizierende Merkmal eingesetzt worden sind - welcher der Teilnehmer, die sich innerhalb der Zeitspanne $[t_1^1, t_2^k]$ im Aufenthaltsgebiet befunden haben, den Dienst genutzt hat.

Wie auch für die Methoden in den vorangegangenen Abschnitten gelten weitere Zusatzannahmen, damit das Verfahren wirklich den vorgegebenen Schutz eines Teilnehmers realisiert. Abhängig vom Angreifermodell und demnach von der Stärke und den Zugangsmöglichkeiten des Angreifers, müssen zum Beispiel zwischen Z und der mobilen Station Verschlüsselungs- und Authentikationsprotokolle verwendet werden, um ein einfaches Abhören auf der Funkschnittstelle zu vermeiden. Auch die Peilbarkeit der Teilnehmer ist nicht außer acht zu lassen. Eine Möglichkeit die Peilung von Mobile Terminals zu verhindern ist nur noch Spread-Spectrum-Technologien auf der Funkschnittstelle zum Einsatz kommen zu lassen. Zudem müssen Replay-Attacken durch das Einbringen von Zeitstempeln aktiv verhindert werden.

Eine weitere ernst zu nehmende Attacke ist das kontrollierte Einspeisen von Paketen durch einen Angreifer. Gelingt es diesem $k_{min} - 1$ Pakete an den Server Z zu übermitteln, so kann er unter Umständen auf die Identität des k-ten Teilnehmers schliessen, der den Puffer von Z auf das optimale k_{min} auffüllt. Eine Variante um diesen Angriff zu verhindern ist, dass ein Benutzer maximal ein Paket in einen Puffer einbringen darf (für $k_{min} \gg 2$). [35, S. 9]

Letztendlich läßt sich festhalten, dass das Verfahren eine Möglichkeit eröffnet, trotz präziser Positionsdaten den Teilnehmer unter bestimmten Voraussetzungen effektiv zu schützen. Eine der wichtigsten ist, dass die Regionen, in denen das Verfahren implementiert wird, stark frequentiert sind. In [35] waren Autobahnstrecken Untersuchungsgegenstand und es konnten gute Ergebnisse präsentiert werden.

4.1.3.3 Hybride Methoden

Das letzte Unterkapitel der Methoden zur Positionsverschleierung bilden die hybriden Methoden, die eine Kombination aus räumlicher Positionsverzerrung und gleichzeitiger Verfälschung der Zeit darstellen. Grund für die Kombination beider Verfahren ist, dass viele Anwendungen weder eine große Verschlechterung der Positionsinformationen noch eine wesentliche Verzögerung der Dienstanfrage zulassen. In diesen Fällen können hybride Methoden mit zwei verschiedenen Prioritätsmodi - zeitliche oder räumliche Priorität - zum Einsatz kommen. In beiden Modi versucht man, unter der Einhaltung von Schranken, ein Optimum für die Anonymität der Teilnehmer zu finden. Eine obere Schranke, die bei der Optimierung Berücksichtigung finden kann, ist die maximal mögliche Positionsverschlechterung. Auf der anderen Seite kann aber auch die maximale Verzögerungszeit als Optimalitätskriterium dienen. Sind beide Beschränkungen zugleich gesetzt kann im ungünstigen Fall nicht die gewünschte k-Anonymität mit k_{min} Teilnehmern erreicht werden.

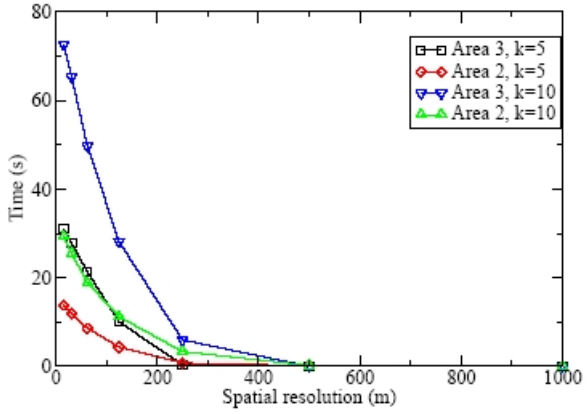

Abbildung 4.8: Tradeoff zwischen der zeitlichen und räumlichen Positionsverzerrung [35, S. 9]

Allerdings kann ein Fehlen der oberen Schranke bezüglich der temporalen Verschlechterung zu einer Nichtbeantwortung der Dienstanfrage führen, wenn während der time-out Zeit der Anwendung nicht genügend Teilnehmer zur Zusammenstellung der notwendigen Anonymitätsgruppe gefunden wurden. Wie Abbildung 4.8 nochmals verdeutlicht besteht, je nach berechnetem Autobahnbereich, - siehe Seite 36 - ein Tradeoff zwischen der zeitlichen und räumlichen Auflösung der Positionsinformation. Eine Gruppe von Dienstnutzern kann sich, je nach Auf-

enthaltsgebiet, auf einer der dargestellten Kurven bewegen, um die optimalen Parameter für die Dienstnutzung zu kalibrieren.

4.1.4 Symbolische Positionsangaben

Die im vorherigen Kapitel aufgezeigten Verfahren zur Verschleierung der Positionsinformationen beruhten ausschließlich darauf, dass einem Dienstanbieter absolute Positionsangaben zur Verfügung zu stellen sind. Im Gegensatz dazu basieren die symbolischen Positionsangaben darauf, dass nicht alle LBS zur Erbringung ihrer Dienstqualität diese benötigen, sondern diesen (die schon auf Seite 5 angesprochenen) relative Positionsangaben vollkommen ausreichen. Um diese Art der Positionsangaben zu ermöglichen sind entweder spezielle Positionsbestimmungssysteme notwendig oder es liegen Regeln vor, wie absolute Koordinaten in relative umgewandelt werden können. Bereits [56, S. 8] erwähnten, dass Sicherheit und Datenschutz symbolische Abstraktionen der Position erfordern.

Hierarchische symbolische Positionsangaben Der Aufbau von Hierarchien für symbolische Positionsangaben, in denen die Blätter und Knoten des entstehenden Baumes einem eindeutigen Gebiet [56, S. 7] zurechenbar sind, wurde von Leonhardt und Magee in den Werken [55] und [56] vorgestellt. Unter dem Namen „Augmented Areas“ fand dieses Konzept Eingang in das Nexus-Projekt und wurde dort weiter ergänzt [46]. Ein Blatt oder Knoten innerhalb der Hierarchie kann einen oder mehrere Vorgänger besitzen, um die geographischen Gegebenheiten korrekt wiedergeben zu können (siehe Abbildung 4.9). Hierarchien sind somit auch flexibel an das jeweilige Positionsbestimmungssystem anpassbar.

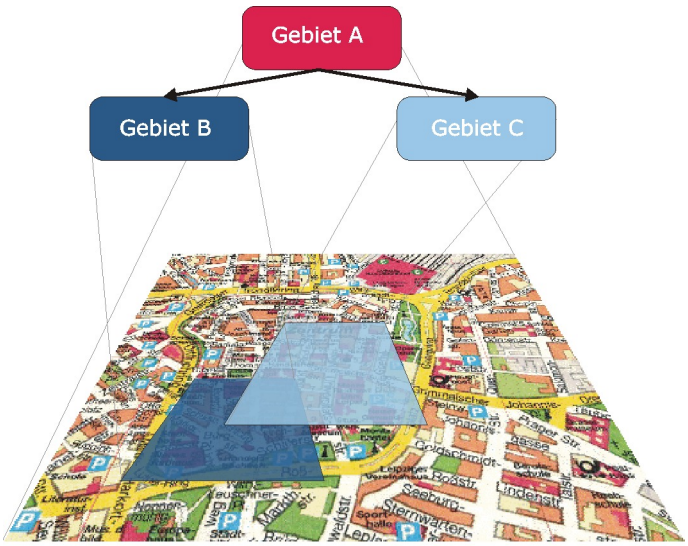

Abbildung 4.9: Hierarchische Symbolische Positionsangaben [56]

Ein Dienstnutzer, der hierarchische symbolische Positionsangaben verwendet, formuliert absolute Positionsinformationen wie folgt: /Erde/Europa/Deutschland/Bayern/Regensburg/-Universität Regensburg/Wirtschaftswissenschaftliche Fakultät. Demnach befindet sich der Nutzer in der Wirtschaftswissenschaftlichen Fakultät der Universität Regensburg.

Hierarchische symbolische Positionsangaben wandeln somit das Konzept der räumlichen Positionsverzerrung - siehe Seite 34 - leicht ab, indem sie, zum Beispiel auf Gebäude bezogen, eine schärfere und deutlichere Verzerrung ermöglichen. Teilt man bei der räumlichen Positionsverzerrung dem Dienstanbieter mit, dass man sich im „Quadranten“ X aufhält, so ermöglicht dieses Konzept, bei Beibehaltung der Unschärfe, die Aussage, dass man sich zum Beispiel an der Universität Regensburg befindet. Die Aussage Region X erlaubt keine Rückschlüsse darauf, ob sich der Nutzer wirklich an der Universität aufhält, oder vielleicht in einem anderen Gebäude, welches in X enthalten ist.

Neben der Möglichkeit Aufenthaltsorte genauer zu beschreiben und dennoch die erforderliche Unschärfe aufrecht zu erhalten, eigenen sich auch symbolische Positionsangaben zur Formulierung von Zugriffsregeln auf die eigenen Positionsdatensätze. Näheres zu diesem Thema ist in Kapitel 4.2.2 auf den Seiten 46 ff. zu lesen.

Logische Aufenthaltsgebiete Eine bedeutende Schwachstelle des vorherigen Ansatzes ist, dass trotz der Umwandlung von physischen Positionskoordinaten, weiter eine direkte Verbindung zu diesen besteht. Gelangt ein Angreifer in den Besitz der Transformationsvorschriften so kann er leicht eine symbolische Angabe - wenn die Information nicht schon direkt aus dem Namen hervorgeht - wieder in eine physische zurückrechnen. Für datenschutzfreundliche Anwendungen wären aber Transformationsvorschriften praktisch, die einer mathematischen Einwegfunktion gleichen. Das Konzept der logischen Aufenthaltsgebiete, welches in [63] ausführlich vorgestellt wurde, erweitert die hierarchischen symbolischen Positionsangaben und realisiert gleichzeitig eine Einwegtransformationsvorschrift.

Narayanan unterscheidet so genannte Realms und States [63, S. 2]. Die beiden Begrifflichkeiten und deren Abgrenzung zu den bisher erläuterten Positionsangaben lassen sich am besten anhand eines Beispiels erklären. Im Sinne des Autors bilden beispielsweise alle Universitäten innerhalb Deutschlands eine Realm mit dem Namen „Universität“. States werden als einzelne Objekte innerhalb einer Realm definiert. So ist die Freie Universität Berlin ein State der Realm „Universität“. Gleichzeitig könnte sie aber auch ein State der Realm „Gebäude im Besitz der Bundesrepublik Deutschland“ sein. Diese Positionsangaben eigenen sich demnach für Anwendungen, für die nicht die wirklich physische Position eines Dienstnutzer wichtig ist, sondern allgemeinere Aussagen ausreichen wie: in der Post, im Stadion etc. Abbildung 4.10 stellt die Zusammenhänge zwischen geographischen Gebieten, Realms und States nochmals grafisch dar.

Realms stellen somit Objekte dar, die die geforderte Einwegfunktion realisieren.

$$f : Position_{physisch} \rightarrow Position_{symbolisch}$$

Die dargestellte Transformation ist per Definition, entsprechendes Kartenmaterial vorausgesetzt, einfach durch das mobile Endgerät berechenbar. Dahingegen ist eine Rücktransformation

$$f : Position_{symbolisch} \rightarrow Position_{physisch}$$

nicht in der Hinsicht durchführbar, dass sie ein eindeutiges Ergebnis liefert. Bei der Rücktransformation der Realm „Universität“ würden wahrscheinlich mehrere hundert Universitäten und Fachhochschulen in Deutschland in Betracht kommen. Aufgrund der fehlenden Möglichkeit von symbolischen auf physische Koordinaten schließen zu können, erhöht die Konstruktion von logischen Aufenthaltsgebieten aktiv das Datenschutz-Level für einen Teilnehmer, ohne

ihn allzu sehr einzuschränken. Diese Art von Positionsangaben verhindert infolgedessen die Erstellung von Bewegungsprofilen, allerdings wird nicht das Erstellen von Nutzungsprofilen[4] unterbunden. Es wird zudem deutlich, dass die bereits vorher angesprochenen hierarchischen symbolischen Positionsangaben in diesem Modell als ein Spezialfall enthalten sind [63, S. 3].

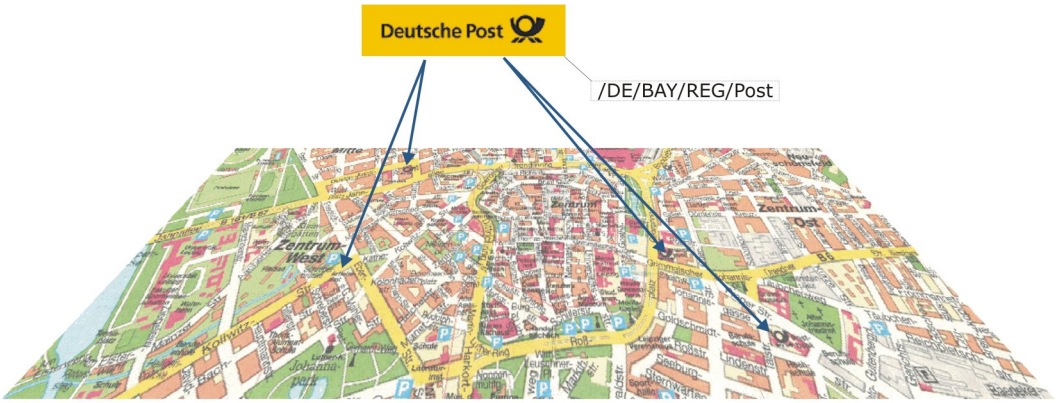

Abbildung 4.10: Logische Aufenthaltsgebiete [63, S. 3]

Neben der positiven Eigenschaft, dass diese Methode den Datenschutz erhöht, fördert sie zugleich die Flexibilität der Transformationsvorschriften. Da Realms an keine geographischen Gebiete gebunden sind, ist eine Verschiebung oder das Hinzufügen von Realms in einer Transformationskarte ohne weitere Komplikationen machbar.

Abschließend ist nochmals hervorzuheben, dass sich die Konstruktion von logischen Aufenthaltsgebieten in vielen Anwendungsfällen als möglich erweist. Bekannte Anwendungen wären zum Beispiel ortsabhängige Werbeanzeigen für Anbieter die vor allem breitflächig mit vielen Filialen vertreten sind. Somit könnte in vielen Bereichen der Datenschutz für Dienstnutzer signifikant erhöht werden, ohne das der Teilnehmer einer TTP volles Vertrauen schenken muß, denn über die Granularität und Anwendung von Realms kann letztendlich der Endgerätebesitzer selbst entscheiden.

4.1.5 Zusammenfassung

Abschließend zu dem Unterkapitel Datenvermeidung sind nochmals alle acht vorgestellten Verfahren zur Identitäts- und Positionsverschleierung zusammengefasst in Tabelle 4.1 dargestellt. Die Methoden wurden in die Kategorien Identitätsverhüllung und Positionsverschleierung unterteilt.

[4] Nutzungsprofile geben Aufschluss darüber, welche Art von Lokalitäten (bspw. Post, Univerität etc.) ein LBS-Nutzer besucht, aber nicht wo sich diese befinden

Abk.	Bezeichnung	Kurzbeschreibung
Verhüllung der Identität		
I.1	Anonymisierung & Pseudonymisierung	Verfahren nimmt keine Änderungen an den Positionsinformationen vor, sondern versucht lediglich durch permanentes Wechseln des Identifiers eine Verschleierung zu erreichen. Verwendung: seltene Dienstanfragen (z.B. täglich oder wöchentlich einmal).
I.2	Mix-Zonen	Dieser Ansatz versucht die Verkettung von gesammelten Datensätzen unter den LBS-Dienstanbietern zu verhindern. Hierfür werden zwischen sog. Applikations-Zonen, Mix-Zonen geschaltet, in denen ein Dienstnutzer seine Pseudonyme wechseln kann. Verwendung: Innerhalb einer Applikationszone sind hoch präzise, pseudonyme Anfragen notwendig und dennoch sollen Applikationszonenanbieter untereinander die gesammelten Bewegungsdatensätze nicht verketten können.
Positionsverschleierung		
P.1	Räumliche Positionsverzerrung (dezentral)	Der Dienstnutzer selbst, ohne Nutzung weiterer Informationen, verfälscht seine Positionsdaten in der Art, dass er nach seiner Einschätzung die gewünschte Anonymitätsgruppe erreicht. Verwendung: in sehr dicht besiedelten Gebieten, wenn der Dienstnutzer keine TTP nutzen will.
P.2	Räumliche Positionsverzerrung (zentral)	Unter Zuhilfenahme einer TTP verfälscht ein Nutzer seine Positionsinformationen so, dass eine Anonymitätsgruppe mit k_{min} Teilnehmern entsteht. Verwendung: wenig urbanisierte Aufenthaltsbereiche, in denen der Dienstnutzer sicherstellen will, dass er „k-Anonym“ ist.
P.3	Positionsverschleierung durch Verzerrung der Zeitinformation	Anstatt das Positionssignal zu verfälschen hält eine TTP die Anfrage solange zurück, bis sich am gleichen Ort wenigsten k weitere Personen aufgehalten haben. Verwendung: genaue Positionsinformation ist erforderlich, aber die Dringlichkeit der Anfrage ist nicht sehr hoch.
P.4	hybride Positionsverschleierung	Sowohl die Positionsinformation als auch der Zeitstempel werden verfälscht mit dem Ergebnis, dass sich wieder eine k Teilnehmer große Anonymitätsgruppe bildet.
P.5	hierarchische symbolische Positionsangaben	Ein Dienstnutzer versendet innerhalb der Dienstanfrage keine physischen Koordinaten mehr, sondern nur noch symbolische. Die symbolischen Koordinaten sind hierarchisch aufgebaut und besitzen somit einen direkten Bezug zu den physischen Koordinaten. Verwendung: wie P.1 und P.2

Fortsetzung auf der nächsten Seite.

Abk.	Bezeichnung	Kurzbeschreibung
P.6	logische Aufenthaltsgebiete	Logische Aufenthaltsgebiete schaffen eine Einwegfunktion, mit deren Hilfe symbolische Positionsangaben nicht mehr in physische zurückgerechnet werden können. Ein Dienstnutzer kann somit, bei richtiger Konstruktion der logischen Aufenthaltsgebiete sehr viele Informationen preis geben, ohne seine wirkliche physische Position bekannt geben zu müssen. Verwendung: überall einsetzbar, wo die physische Position zur Diensterbringung nicht notwendig ist.

Tabelle 4.1: Methoden zur Datenvermeidung

4.2 Datenverteilung auf der Anwendungsschicht

In diesem Kapitel geht es nicht mehr um das „principle of minimum disclosure“ [1, S. 99], wie es im vorangegangenen Kapitel vorgestellt wurde, sondern darum die Datenverteilung oder das Prinzip „separation of identity and profile“ näher zu betrachten. Dieses parallel zur Datenvermeidung existierende Konzept versucht nicht die Menge und Genauigkeit an nutzeridentifizierenden Daten so gering wie möglich zu halten, sondern die herausgegebenen Daten über möglichst viele Einheiten zu verteilen. Dabei ist natürlich die Art der Verteilung entscheidend. Die nachfolgenden Betrachtungen konzentrieren sich im ersten Teil darauf, wie Daten von Dienstnutzern streubar sind und wie diese Streuung möglichst effektiv visualisiert werden kann. Der zweite Teil beleuchtet den Aspekt der Vergabe von Zugriffsrechten auf gespeicherte Daten.

4.2.1 Privacy Enhancing Service Architectures

Angelehnt an die Arbeit von Alamäki und Kollegen [1] entstand der Titel und das Konzept dieses Unterkapitels. Untersuchungen zu dem Thema Privacy Enhancing Service Architectures (PESA) befassen sich damit, wie Nutzerdaten zwischen den Beteiligten eines LBS-Dienstes (siehe Tabelle 2.3, Seite 15) verteilbar sind. Angelehnt an die Unified Modelling Language (UML) entwickelten [1] eine Visualisierungsmethode, die die Datenverteilung anschaulich darstellt. Die gängigen UML-Symbole wie Klasse, Objekt und Paket wurden hierfür wie folgt umdefiniert:

- **Klasse:** Das Klassensymbol stellt eine Dienstart wie zum Beispiel Client, Access Provider, Profile Broker, Abrechnungsinstanz (Billing) etc. dar. Ihre Zuständigkeit beschränkt sich damit auf ein eng umgrenztes Aufgabengebiet.
- **Objekt:** Ein Objekt ist eine konkrete Realisierung einer Klasse. Somit können beispielsweise verschiedene Clients modelliert und dargestellt werden.
- **Package:** Ein Paket fasst eine in der PESA zusammengehörige Menge an Klassen (Dienstarten) zusammen. Bietet zum Beispiel ein Telekommunikationsanbieter mehr als eine Dienstart an, so würde man alle seine Dienstarten (Klassensymbol) in einem Paket, mit dem Namen des Dienstanbieters bündeln.

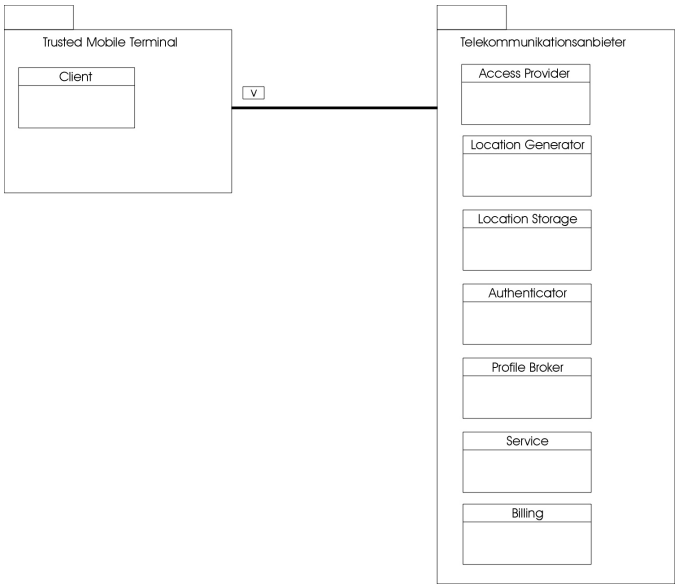

Abbildung 4.11: PESA der heutigen LBS-Landschaft

Die nachfolgende Abbildung 4.11 zeigt exemplarisch eine aus zwei Paketen bestehende PESA:

Abbildung 4.11 bedarf zunächst einer kleinen Erklärung. Dargestellt ist ein mobiles Endgerät (Trusted Mobile Terminal), welches einen LBS von einem Telekommunikationsanbieter bezieht. Leicht ersichtlich ist, dass auf dem Endgerät lediglich eine Clientanwendung - zum Beispiel in Form eines WAP-Clients - implementiert ist. Alle anderen Dienstarten wie Positionsbestimmung, Positionsspeicherung, Diensterbringung, Abrechnung und Weitere sind ausschließlich im Verfügungsbereich des Telekommunikationsanbieters. An dieser Stelle ist natürlich die Frage berechtigt, ob es sich wirklich aus Sicht des Dienstnutzers um eine PESA handelt. Prinzipiell ist dies zu verneinen, denn von Datenschutz durch Verteilung von Informationen kann hier nicht mehr die Rede sein. Allerdings wurde dieses Negativbeispiel mit aufgenommen um aufzuzeigen, wie sich die heutige Landschaft der Servicearchitekturen oftmals darstellt.

Verbessert werden könnte das zuvor genannte Beispiel, wenn der Telekommunikationsanbieter einen Teil seines Aufgabenspektrums an einen weiteren, von ihm unabhängigen Serviceanbieter auslagert. Abbildung 4.12 stellt ein solches Szenario grafisch dar. Auch hier lagert auf dem Endgerät lediglich die Client-Anwendung. Aber im Gegensatz zum vorherigen Beispiel erbringt jetzt eine dritte, vom Telekommunikationsanbieter unabhängige Instanz (LBS-Anbieter) die Servicedienstleistung. Es findet demnach eine Verteilung der Nutzerdaten statt. Vorher konnte der Telekommunikationsanbieter das gesamte Verhalten des Dienstnutzers profilieren. In dieser PESA kann der Telekommunikationsanbieter mithilfe des Location Generator's zwar Bewegungsprofile erstellen, jedoch bleiben ihm, bei entsprechenden Sicherungsmaßnahmen die Dienstanfragen selbst verborgen.

Zwei weitere interessante PESA's finden sich im Anhang A auf den Seiten 80 ff. und werden an dieser Stelle nicht näher erläutert.

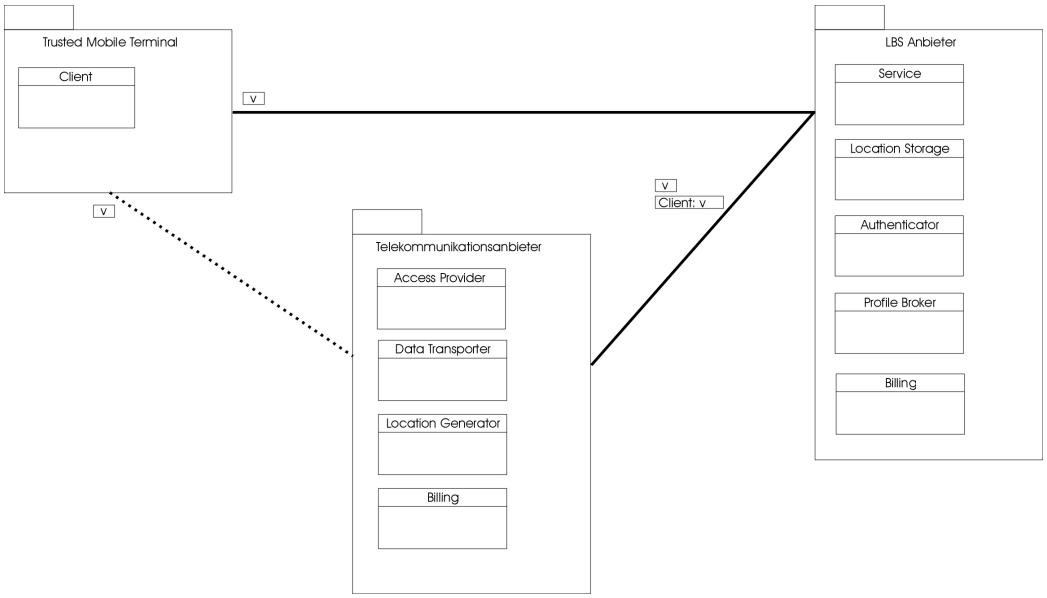

Abbildung 4.12: PESA mit unabhängigem LBS-Anbieter

4.2.2 Zugriffskontrollmechanismen (Policies)

Zugriffskontrollmechanismen gewinnen im Kontext der PESA's vor allem dann an Bedeutung, wenn das Trusted Mobile Terminal über sehr wenig Basisfunktionalität verfügt. In diesem Spezialfall (siehe Abbildung 4.12) übernimmt unter Umständen der Telekommunikationsanbieter nicht nur die Ortung des mobilen Endgerätes (Location Generator), sondern auch die Verwaltung der ermittelten Positionsdaten. Fordert ein Nutzer bei einem LBS-Dienstanbieter eine Servicedienstleistung an, so kontaktiert der LBS-Dienstanbieter den Telekommunikationsanbieter um die aktuelle Position des Teilnehmers zu erfragen. In diesem Szenario werden somit Positionsdaten nie vom Endgerät direkt an den LBS-Anbieter versendet. Aufgabe der Zugriffsregeln ist es nun, die Abfrage von Positionsinformationen beim Telekommunikationsanbieter oder einem Dritten so kontrollierbar zu machen, dass die Datenschutzinteressen des LBS-Nutzers gewahrt bleiben.

Snekkenes [88] spezifiziert hierfür folgende Komponenten, die eine Zugriffsregel berücksichtigen muss [88, S. 51]:

- Zeitpunkt der Positionsbestimmung
- Position des georteten Objektes oder der Person
- Geschwindigkeit des Objektes oder Person während der Ortung
- Identität der Person oder des Gegenstandes

Diese Komponenten lassen deutlich erkennen, dass Regeln die eine reine Ja/Nein Entscheidung treffen viel zu rudimentär wären, um die unter Umständen recht komplizierten Situationen adäquat zu schützen. Für den Autor [88] stehen Zugriffsregeln über den bisher vorgestellten „low-level“ Schutzmechanismen [34, S. 2], wie Positionsverschleierung, Verzerrung der

Zeitinformationen, Mix-Zonen etc. Zugriffsregeln machen demnach durch ihre Formulierung Gebrauch von diesen Mechanismen, indem beispielsweise durch vorformulierte Regeln in festgelegten Situationen die herausgegebene Positionsinformation verschleiert oder der Zeitraum der Aufnahme verfälscht wird. In [88] werden Konzepte zur Formulierung solcher Zugriffsregeln vorgestellt, welche aber nach Angaben des Autors noch weiter wissenschaftlich untersucht werden müssen.

Fazit: Zugriffsregeln sind ein „high level“ Instrumentarium [34, S. 2], welches vor allem Vertrauen in die Instanz, die die Regeln verwaltet, voraussetzt [34, S. 5]. In vielen Fällen wäre es der Instanz möglich, den Benutzer ohne sein Wissen leicht zu betrügen, indem einfach die von ihm spezifizierten Regeln nicht angewendet oder abgeändert werden. Mit der Folge, dass ein sofortiger Verlust an Datenschutz eintritt. Doch Görlach und Kollegen sind der Auffassung, dass solche Szenarios durch eine gut durchdachte Gesetzgebung verhindert werden können. Zudem könnte der Einsatz von Datenschutz-Audits (siehe Kapitel 4.3.4) das Vertrauen von LBS-Nutzern in diese Methoden weiter stärken.

4.3 Selbstdatenschutz, Selbstregulierung und Transparenz

Neben den eher offensichtlichen Methoden der Datenvermeidung und Datenverteilung, zählen auch der Selbstdatenschutz und Methoden zur Erhöhung der Transparenz angebotener LBS-Dienste zu den PET [39, S. 305]. Selbstdatenschutz stützt sich insbesondere auf das Recht zur informationellen Selbstbestimmung und ist *„Ausdruck der allgemeinen Handlungsfreiheit“*[76, S. 330]. Hierfür müssen dem Nutzer von LBS-Anwendungen zum einen rechtliche Rahmenbedingungen geboten und zum anderen technische Hilfsmittel zur Verfügung gestellt werden. [76, S. 327-328] Selbstdatenschutz beginnt bereits bei der Gestaltung von elementaren Bedien- und Benutzungsoberflächen mit denen der Dienstnutzer tagtäglich umgehen muss. So sollte die Benutzungsoberfläche beispielsweise mit einer adäquaten Meldung auf alle Ereignisse aufmerksam machen, bei der kritische, personenbezogene Daten nach außen an Dritte abgegeben werden. Neben Technologien, die sich besonders auf die Ermöglichung oder Verstärkung des Selbstdatenschutzes konzentrieren, ist die transparente Darstellung des gesamten LBS-Geflechtes gegenüber dem LBS-Kunden von höchster Wichtigkeit [76, S. 342-344]. Hansen formuliert den Begriff der Transparenz folgendermaßen: *„Transparenz bedeutet, dass sich die Betroffenen der Verarbeitung ihrer Daten und der näheren Umstände bewusst sind.“* [39, S. 311]. Die Autorin hebt zudem nochmals gesondert hervor, dass sich erst durch die Schaffung von Transparenz ein Bewusstsein für die Verarbeitung der eigenen Daten entwickeln kann.

Wie Selbstdatenschutz technisch als auch organisatorisch gefördert werden kann, ist Gegenstand der nächsten Unterkapitel.

4.3.1 Data Journals

Einen ersten Schritt zur Erhöhung des Selbstdatenschutzes eines LBS-Teilnehmers stellen so genannte DataJournals (im folgenden Data Journal), welche in [12] vorgestellt wurden, dar. Prinzipiell handelt es sich bei Data Journals um kleine Datenbanken, die auf den Endgeräten der einzelnen Dienstnutzer arbeiten. Aufgabe dieser ist es, alle ausgehenden personenbezogenen Daten zu erkennen und anschließend zu protokollieren. Ein Protokolldatensatz könnte dann folgende Informationen beinhalten: Server-IP, Name der Empfängerfirma, personenbezogene Daten, Datum und eventuell zur Verfügung stehende Privacy-Policy-Dateien die vom

Server zum Zeitpunkt des Absendens angeboten wurden. (Nähere Informationen zu Privacy-Policy-Dateien sind unter dem Stichpunkt P3P, Seite 48 zu finden.)

Wie trägt dieses Konzept jedoch zu einem besseren Selbstdatenschutz bei? Auf diese Frage gibt es mehrere Antworten. Zum einen kann ein Dienstnutzer sich nachträglich einen Überblick verschaffen, an welche Unternehmen und Institutionen er welche Daten und zu welchem Zeitpunkt abgegeben hat. Indirekt steigt die Transparenz für den Dienstnutzer, da er seine initiierten Datenflüsse bei Bedarf rekapitulieren kann. Hilfreich können diese Informationen zudem in Situationen sein, in denen ein Datenmißbrauch stattgefunden hat und ein Dienstnutzer unter Umständen versucht, den Urheber des Mißbrauchs ausfindig machen [12]. Außerdem eröffnet sich für Dienstnutzer erstmals die Möglichkeit, effektiv den §4 TDDSG (Gesetz über den Datenschutz bei Telediensten) in Anspruch zu nehmen. Der Inhalt dieser Rechtsvorschrift besagt, dass es jedem Dienstnutzer möglich sein muss, Erkundigungen über seine gespeicherten Daten einzuholen. Ohne Data Journals fällt es einem Teilnehmer allerdings schwer, überhaupt nachzuvollziehen mit welchen LBS-Anbietern er überhaupt in Kontakt stand. Neben der Auskunftspflicht für personenbezogene Daten steht einem Nutzer auch das Recht zu, den LBS-Betreiber dazu aufzufordern, umgehend alle mit seiner Person in Verbindung stehenden Datensätze zu löschen. Auch hier wirken Data Journals unterstützend und zeigen dem Teilnehmer auf, wo er Datenspuren hinterlassen hat.

Abschließend lässt sich anmerken, dass Data Journals besonders bei Dienstarten Anwendung finden können, bei denen Techniken der Anonymisierung oder Pseudonymisierung aufgrund der Art der Diensterbringung nicht möglich erscheinen. Bei diesen Diensten besteht zurzeit eine „Informationslücke“ [12], die zum Beispiel durch Data Journals effektiv geschlossen werden kann. Ein weiterer Vorteil der Data Journals ist, dass diese im Hintergrund, für den Benutzer sozusagen unsichtbar, implementierbar sind. Allerdings spricht der Autor in [12] auch das Problem der Beweisbarkeit an. Demzufolge können Data Journals, nach aktuellem Recht nicht als beweiskräftiges Mittel vor Gericht eingesetzt werden, um einen Datenmissbrauch gegenüber Dritten nachzuweisen. Dennoch kann festgehalten werden, dass sich durch Data Journals sicherlich das Nutzervertrauen in Technologien, wie die LBS erhöht und der Selbstdatenschutz stärker als zuvor gefördert wird.

4.3.2 Privacy Preferences Project (P3P) und APPEL

Ein weiterer Baustein, zur Steigerung des Selbstdatenschutzes ist die „Platform for Privacy Preferences Projects[5]“ (P3P), welche im April 2002 vom World Wide Web Consortium (W3C) veröffentlicht wurde [8, 18]. Ziel des Projektes ist es einen weltweit einheitlichen Standard zu schaffen, der menschen- und maschinenlesbare Datenschutzinformationen in einer Datei vereint. Die Version 1.0 der Spezifikation definiert dabei nicht nur die Art und Weise, wie Datenschutzvereinbarungen in der „eXtended Markup Language“ (XML) formuliert werden müssen, sondern auch Lokalisierungs- und Transportregeln. Eine der Spezifikation entsprechende P3P-XML-Datei ist im Anhang B auf Seite 82 zu finden.

Im Grobaufbau besteht eine P3P-Datei aus acht Hauptkomponenten die in Tabelle 4.2 näher erläutert werden. Mithilfe der aufgelisteten Konstrukte können nun LBS-Dienstanbieter ihre Datenschutzregeln sowohl für den Menschen lesbar als auch maschinenlesbar formulieren. Somit besteht für den Nutzer die Chance, Datenschutzinformationen maschinengesteuert im

[5] siehe www.w3.org/p3p

Elementname	Beschreibung
Entity	Elemente innerhalb von Entity stellen Kontaktinformationen, wie zum Beispiel Name der Organisation, Ansprechpartner etc. dar.
Access	Dieses Element gibt an, ob ein Dienstnutzer in der Lage ist, die über ihn eventuell abgespeicherten Informationen einzusehen.
Disputes	Inhalte dieses Elementtyps ermöglichen es einem Dienstbenutzer, auftretende Konflikte elektronsich und voll automatisch lösen zu lassen. (Aushandlung gegenseitiger Interessen)
Data	Data-Elemente erlauben die Auflistung von Daten, die über einen Nutzer gesammelt werden. (es existieren 17 Datenkategorien)
Purpose	Erläutert die Verwendung der erhobenen Daten. (11 Verwendungstypen sind vordefiniert)
Recipient	Ermöglicht die Formulierung von Stati, wann und unter welchen Umständen erhobene Daten mit Dritten ausgetauscht werden. Hier sind auch Wahlmöglichkeiten erlaubt.
Retention	In diesem Element kann die Aufbewahrungszeit für gesammelte Daten näher erläutert werden.
Consequence	Das Element enthält eine menschenlesbare Version, der in der P3P-Datei formulierten, maschinenlesbaren Datenschutzinformationen.

Tabelle 4.2: P3P Hauptelemente in Anlehnung an [18, S. 51]

Hintergrund analysieren zu lassen. Eine Benutzerinteraktion wäre demnach erst dann erforderlich, wenn die vom LBS-Dienstanbieter gelieferten Datenschutzvereinbarungen nicht mit den vom Nutzer formulierten Anforderungen in Einklang zu bringen sind. An dieser Stelle kommt der „A P3P Preference Exchange Language“ (APPEL) eine besondere Bedeutung zu. APPEL gibt dem Dienstnutzer - wie P3P dem LBS-Dienstanbieter - die Möglichkeit eigene Datenschutzregeln endgeräteseitig zu formulieren [54, S. 4][18, S. 52]. APPEL ist demzufolge eine regelbasierte Sprache, die von P3P-fähigen Agenten interpretierbar ist. Hiermit wird ein Instrument geschaffen, mit dem beide Seiten - Dienstnutzer und LBS-Dienstanbieter - ihre Sicherheits- und Datenschutzinteressen in einem einheitlichen, maschinenlesbaren Format ausdrücken können. Bei Konflikten muss der P3P-Agent allerdings eine Einwilligung oder Ablehnung des Dienstnutzers einholen. Eine Verhandlung in der Form, das gegenseitige Interessen abgestimmt werden, findet nicht statt. In der Literatur findet man oft die Bezeichnung „Notice and Choice“. [76, S. 343] Beide Protokolle sind somit nicht in die Kategorie „Datenschutz durch Technik“ einzuordnen. Vielmehr beruht ihr Erfolg auf rechtlichem und sozialen Druck, der von außen auf einen Anbieter ausgeübt wird. [61, S. 58]

P3P und APPEL geben somit sowohl dem Dienstnutzer als auch dem LBS-Dienstanbieter ein Werkzeug an die Hand, welches bei richtiger und vertrauenswürdiger Anwendung die Transparenz der angebotenen Dienste signifikant erhöhen und den Selbstdatenschutz für die Dienstteilnehmer vereinfachen kann [18, S. 55][76, S. 343]. Zudem ermöglichen es die Protokolle Verhandlungsspielräume zu formulieren, in denen sich jeder Nutzer frei bewegen kann. Dennoch stehen einer weiten Verbreitung - auch im LBS-Sektor - einige Hemmnisse entgegen. Kritiker von P3P argumentieren oft, dass zum Beispiel rechtliche Regelungen den freien Vereinbarungen die unter Umständen nicht eingehalten werden, vorzuziehen sind. Ein weiterer

und oft vorgetragener Mangel von P3P ist, dass es nach Meinung vieler Wissenschaftler nicht den „Fair Information Principles“ (FIP) gerecht wird, da einer einfacheren Handhabung des Protokolls Vorzug gegeben wurde [18, S. 54][76, S. 343-344]. Des Weiteren steht noch das Problem im Raum, dass Dienstanbieter oftmals zögerlich mit frei formulierten Datenschutzvereinbarungen umgehen, da unter Umständen hieraus rechtliche Ansprüche der Dienstnutzer erwachsen könnten, die für den Dienstanbieter in dieser Weise vorher nicht ersichtlich waren. Letztendlich kann auch bei den P3P-Dateien wieder argumentiert werden, dass diese zunächst keine rechtlichen Wirkungen mit sich bringen und Dienstnutzer nicht wirklich „automatisch“ auf die nach außen hin publizierten Datenschutzregeln vertrauen können. Dem entgegen zu setzen wäre eine Zertifizierung der P3P-Dateien durch eine vertrauenswürdige Dritte Instanz (TTP). Näheres dazu im Unterkapitel Datenschutz-Audits.

Zusammenfassend läßt sich feststellen, dass P3P ein Baustein unter vielen ist, der die Datenschutzfreundlichkeit von LBS-Anwendungen steigern kann [14, S. 475]. Dies geschieht nicht nur durch die Steigerung der Transparenz, sondern auch durch die Schaffung von Selbstbestimmungsmöglichkeiten für den Dienstteilnehmer. Eine Zusammenstellung von wichtigen P3P-Eigenschaften aus Datenschutzsicht kann in [8, S. 148] nachgelesen werden.

4.3.3 Privacy Awareness System (pawS)

Das in [54] beschriebene pawS erweitert den bisher nur für Internetdienste beschriebenen P3P-Ansatz für eine Vielzahl von LBS-Anwendungen. Wie P3P selbst kann pawS nicht den Mißbrauch von gesammelten Daten verhindern, aber es stellt Dienstanbietern Protokolle und Anwendungen zur Verfügung, mit denen sie ihre Datenschutzrichtlinien kommunizieren können. Wie Langheinrich schon erwähnt, reicht dieser Schutz oder schon die Zusage für ein großes Spektrum an LBS-Anwendungen aus, um einen adäquaten datenschutzfreundlichen Dienst zu realisieren. Sind höhere Schutzniveaus notwendig, so müssen sich Dienstnutzer mit zusätzlichen Mitteln schützen. [54, S. 2][61, S. 58-59]

Die Hauptanpassung von P3P an mobile Dienste durch pawS ist die Verbreitung von P3P-Dateien an die Dienstnutzer. Langheinrich unterteilt die Verbreitung in zwei Szenarios [54, S. 5]:

1. **Implizite Verbreitung:** Für gewöhnlich suchen mobile Endgeräte ständig nach verfügbaren LBS-Diensten in ihrer Umgebung. In diesem Fall könnte man die Verbreitung von P3P-Dateien in das Suchprotokoll - engl. discovery protocol - implementieren.

2. **Aktive Verbreitung:** Ein anderer, vielleicht nicht sehr oft auf LBS-Dienste zutreffender Fall ist das automatische, oft unbemerkte Tracken von Endgeräten bei Eintritt in eine bestimmte Zone. Hier empfiehlt sich ein aktives Ausstrahlen von Datenschutzinformationen, welches mithilfe des pawS gelöst werden kann.

Der erste Weg ist relativ einfach und intuitiv. So wie im Internet die P3P-Dateien immer unter einem standardisierten Uniform Resource Locator (URL) zu finden sind [18, S. 51], so kann die Suche nach P3P-Datei Angeboten auch im LBS-Suchprotokoll fest verankert werden. Die zweite Variante, die das pawS versucht zu lösen, erfordert gegebenenfalls zusätzlichen technischen Aufwand. Erstens sind auf Netzbetreiberseite Dauersender zu installieren, die permanent die lokalen Datenschutzvereinbarungen ausstrahlen. Und zweitens müssen die Endgeräte aktiv auf Broadcast-Nachrichten hören. Damit einher geht ein erhöhter Stromverbrauch der mobilen Gerätschaften.

Abschließend ist ein positiver Nebeneffekt von P3P und pawS festzustellen, falls die beiden Frameworks weitere Verbreitung finden. Unterstellt man eine flächendeckende Anwendung bei allen LBS-Anbietern, so kann P3P eine Art Selbstregulierung innerhalb der LBS-Branche bewirken. Grund für die Selbstregulierung bezüglich der Datenschutzvereinbarungen ist, dass ein Abweichen von den selbst publizierten Datenschutzrichtlinien von LBS-Dienstnutzern erkannt werden kann und diese zu einem Anbieterwechsel veranlassen könnte. Parallel dazu wäre das Angebot von einem besonders hohen Datenschutzniveau ein Differenzierungsmerkmal von Dienstanbietern gegenüber Mitbewerbern.

4.3.4 Datenschutz-Audits

Das Datenschutz-Audit greift den bisher wenig angesprochenen Punkt Selbstregulierung auf. Im Gegensatz zu einer staatlichen Regulierung - in Form von Gesetzen - vereinbart hier die entsprechende Branche oder Industrie einen eigenen Datenschutzstandard, der von allen Mitgliedern freiwillig eingehalten werden sollte [77, S. 439]. Dementsprechend fehlt natürlich der wirklich bindende Charakter der bei der Gesetzgebung vorhanden wäre. Dennoch unterstützen Marktmechanismen, welche im Fall von LBS-Diensten hauptsächlich von LBS-Teilnehmern ausgehen, aktiv die Einhaltung getroffener Vereinbarungen. Um den Entscheidungsprozess und die Transparenz bezüglich der Einhaltung der getroffenen Regeln zu fördern, sorgen so genannte Datenschutz-Audits für einmalige oder sich wiederholende Überprüfungen. Wurde ein Audit erfolgreich bestanden kann das jeweilige Unternehmen beispielsweise mit einer Plakette oder ähnlichem werben. Die Vereinbarung solcher freiwilligen Standards und Datenschutz-Audits fasst man in der Literatur oft unter dem Begriff „freiwillige Selbstregulation“ zusammen [77, S. 439].

Im Gegensatz zu Deutschland ist die freiwillige oder marktorientierte Selbstregulation in den USA bei internetbasierten Diensten viel stärker verbreitet, wohingegen die staatliche Seite nur Rahmenbedingungen vorgibt [77, S. 447-450]. Wie oben bereits angesprochen, erfolgt die Marktkoordination zum Beispiel durch die Vergabe von Siegeln, die die Einhaltung bestimmter Datenschutzregeln garantieren.

Nach [77, S. 440-442] lassen sich vier Ziele für das Datenschutz-Audit identifizieren:

1. Stärkung der Selbstverantwortung und Stimulierung von Wettbewerb
2. Hilfe bei der Gewährleistung des Datenschutzes
3. Kontinuierliche Verbesserung des Datenschutzes und der Datensicherung
4. Datenschutzaudit als Lernsystem

Eine nähere Erläuterung der Ziele findet sich in [77, S. 440-442].

Datenschutz-Audits lassen sich in zwei Kategorien einteilen: Produktaudit und Systemaudit. Diese prüfen zwei völlig unterschiedliche Bereiche technische Einrichtungen und Datenschutzkonzepte [77, S. 462-469].

Produktaudit Das Produktaudit hat ein Produkt, eine Software oder ein Datenverarbeitungsverfahren (technische Einrichtungen) zum Prüfungsgegenstand. In der Regel erfolgt eine

Auditierung des Gegenstandes immer dann, wenn Neuerungen oder Veränderungen an diesem vorgenommen worden sind. Demnach ist es zweckmäßig, dass allein der Hersteller des Produktes die Zertifizierung / Auditierung vornimmt. Unternehmen die das Endprodukt verwenden können dann auf die Ordnungsmäßigkeit bezüglich der zertifizierten Eigenschaften (welche durch Zertifikate nachgewiesen werden können) vertrauen. [77, S. 463, Rn. 65]

Systemaudit Im Gegensatz zum Produktaudit ist das Augenmerk beim Systemaudit auf Datenschutzkonzepte oder Datenschutzmanagementsysteme gerichtet. Datenschutzkonzepte stellen demnach nicht spezielle Produkte dar, sondern Prozesse und Strukturen in Unternehmen. Das Systemaudit prüft die Flexibilität, mit der ein Unternehmen auf datenschutzbezogene Veränderungen der Umwelt - hinsichtlich seiner Prozesse und Strukturen - eingehen kann. Woraus folgt, dass das Systemaudit nicht nur einen einmaligen Auditierungsprozess initiiert, sondern in kontinuierlichen Abständen wiederholt werden muss, um die Leistungsfähigkeit der Datenschutzkonzepte vor den sich ständig ändernden Umweltbedingungen neu zu evaluieren. Rossnagel präzisiert nochmals das Systemaudit wie folgt: *„Gegenstand des Datenschutzaudits ist die Funktionsfähigkeit und Zweckmäßigkeit des internen Datenschutzmanagements.“*[77, S. 463, Rn. 66]. Zudem erwähnt der Autor, dass der Begriff Datenschutz-Audit nur dem Systemaudit, aber nicht dem Produktaudit zugeordnet werden sollte. [77, S. 463, Rn. 66]

Fazit: Sowohl die Produkt- als auch Systemaudits, welche sich bisher im Bereich der internetbasierten Dienste (eBusiness) durchgesetzt haben, können auch für LBS-Anwendungen hinsichtlich des Datenschutzes einen echten Mehrwert darstellen. Hier sind nicht nur die zuvor genannten „Gütesiegel“ zu erwähnen. Weiter wäre vorstellbar, dass P3P-Dateien (siehe Kapitel 4.3.2) mithilfe von elektronischen digitalen Signaturen unterzeichnet werden. Dies würde eine sofortige elektronische Prüfung auf Kundenseite ermöglichen, ohne dass sich der Kunde durch endlose Datenschutzvereinbarungen kämpfen muss. Letztendlich lässt sich festhalten, dass Datenschutzaudits sowohl, allein als auch in Kombination mit weiteren Techniken (P3P), sich für die Erhöhung des Datenschutzes von LBS-Anwendungen eignen und somit in die Rubrik der PET zu zählen sind.

4.4 Weitere Schutztechniken

In Abgrenzung zu den vorherigen Kapiteln beschäftigt sich dieses mit Verfahren, die unterhalb der Anwendungsschicht arbeiten. So haben beispielsweise GSM-Anbieter im Rahmen ihres Location Management die Möglichkeit sehr detaillierte Bewegungsprofile von GSM-Teilnehmern aufzuzeichen. Aus diesen können Angreifer wiederum Rückschlüsse auf häufig besuchte Aufenthaltsorte ziehen. Wie dieser und andere Angriffe verhindert werden können, sollen die folgenden Abschnitte zeigen.

4.4.1 Datenschutzfreundliche Gestaltung von Kommunikationsnetzen

Aufgrund der Vielzahl an verschiedenen Netzen und deren oftmals sehr unterschiedlichen Aufbau sollen an dieser Stelle die zwei wohl am weitesten verbreiteten Funknetze untersucht und Lösungsmöglichkeiten zur datenschutzfreundlichen Gestaltung aufgezeigt werden.

Mobiltelekommunikationsmixe in GSM-Netzen In der Arbeit von FEDERRATH erstmals vorgestellt, verhindern so genannte Mobilkommunikationsmixe das Erstellen von Bewegungsprofilen im Rahmen des GSM-typischen Location Managements und somit die Verfolgbarkeit von GSM-Nutzern. Das Mixkonzept selbst setzt dabei auf die von David CHAUM publizierten Mixe auf und erweitert dieses Konzept für GSM und UMTS-Funknetze. Für die Funktionsfähigkeit der Mobilkommunikationsmixe müssen mehrere einzelne Mixknoten (wenigstens zwei) zu einer Mix-Kaskade gebündelt werden und deren Betreiber unabhängig voneinander arbeiten. Die in [28] beschriebene Anordung solcher Mix-Kaskaden ermöglicht nun das verschlüsselte und nicht mehr verkettbare Ablegen von Routinginformationen innerhalb des GSM-Netzes, weshalb keine Bewegungsprofile auf Netzbetreiberseite mehr erstellbar sind. Die genaue Funktionsweise ist in [28] detailliert erläutert.

Identitätsverschleierung in Wireless LAN's Ein ähnlich zu den Mobilkommunikationsmixen gelagertes Problem bearbeiteten GRUNWALD und GRUTESER für die sehr stark verbreiteten IEEE 802.11b WLAN's [37]. Grund dieser Untersuchung war, dass es in IEEE 802.11b WLAN's für Access-Point Betreiber leicht möglich ist Bewegungsprofile für in der Nähe befindlichen Endgeräte zu erstellen. Hierfür ist nicht einmal eine Verbindung der Geräte zu dem Access-Point erforderlich, da ein „Abhören" der vom Gerät versendeten Funksignale völlig ausreicht. Als eindeutiger Identifikator steht im Protokoll dieses Funknetzes die MAC-Adresse auf Schicht 2 des OSI-Modells zur Verfügung, die durch IEEE standardisiert weltweit einmalig für jede Netzwerkkarte vergeben wird. Über die MAC-Adresse ist es somit für einen Angreifer leicht möglich Bewegungsprofile mit einer Genauigkeit von wenigstens 50 - 100 Metern zu erstellen. Setzt ein Angreifer darüber hinaus fortgeschrittenere Analysemethoden ein, so ist eine Positionsbestimmung, beispielsweise über die Signal-Noise-Ratio (SNR) und Signal-Strength (SS), auf bis zu einem Meter möglich [37, S. 48]. Um die Verfolgbarkeit anhand der MAC-Adresse zu verhindern, erarbeiteten die Autoren einen Vorschlag, wie die MAC-Adresse in bestimmten Abständen geändert werden kann. Allerdings sind mit dem Wechsel der MAC-Adresse mehrere Probleme verbunden, die in einem Lösungsansatz Berücksichtigung finden müssen. Zum einen ist darauf zu achten, dass die neue MAC-Adresse nicht bereits von einem anderen Endgerät verwendet wird. Um dem Problem zu begegnen wurde ein modifiziertes RARP-Protokoll (reverse adress resolution protocoll) entwickelt, welches das anonyme Überprüfen der neu gewählten MAC ermöglicht. Zudem musste darauf geachtet werden, dass bestehende Verbindungen durch einen MAC-Wechsel nicht einfach verloren gehen. Die in die Arbeit [37] eingebettete quantitative Untersuchung ergab, dass mithilfe des Adresswechsels über 50 Prozent der Nutzer maximal zehn Minuten lang verfolgbar waren, wohingegen ohne Schutz mehr als 95 Prozent länger als eine Stunde beobachtbar waren. Diese Studie zeigt, dass auch in WLAN's Schutzmöglichkeiten bereits auf Schichten unterhalb der Anwendungsschicht existieren, um einen Dienstnutzer stärker gegen Angriffe auf seine Privatsphäre zu schützen. Allerdings erwähnt die Studie nicht, wie beispielsweise serverartige Dienste (Push-Basis) bei einem ständigen MAC- und IP-Adresswechsel zustande kommen sollen.

4.4.2 Passive / terminalbasierte Ortungsverfahren

Ortungsverfahren lassen sich aufgrund ihrer Charakteristik nicht direkt einer Schicht im Sinne des OSI-Schichten-Modells zuordnen. Dennoch entscheidet auch das verwendete Ortungsverfahren darüber, welches Datenschutzniveau maximal für eine LBS-Anwendung erreichbar ist.

Generell sind aus Datenschutzsicht terminalbasierte Ortungsverfahren den netzbasierten vorzuziehen [82]. So erfordern netzbasierte Positionsbestimmungsverfahren immer eine Instanz (bspw. den Netzbetreiber), die die Ortung für den Dienstteilnehmer durchführt. Somit wird automatisch die Positionsinformation in die Hände eines Dritten gegeben und der Endnutzer muss darauf vertrauen, dass diese Instanz die Ortungsdaten nicht weitergibt oder selbst mißbraucht. Terminalbasierte Verfahren hingegen vermeiden diese Problematik komplett indem sie ausschließlich dem Endgerät die Positionsbestimmung überlassen. [82, S. 136-137] Hierfür kann natürlich unterstützend ein Fremdnetzwerk, wie beispielsweise die GPS-Satelliten genutzt werden, aber dennoch verbleibt die Positionsinformation erst einmal im Endgerät.

Eine Zwischenvariante bilden die semiautonomen Positionsbestimmungsverfahren [82, S. 136]. Unter zuhilfenahme netzseitiger Verfahren versucht das Endgerät seine genaue Position terminalbasiert zu ermitteln. Im Fall eines Positionsbestimmungssystems auf Basis von Signalstärken in einem WLAN, würde das Verfahren wie folgt arbeiten: Zunächst ermittelt das Endgerät die in seiner Umgebung befindlichen Access-Points. Die Identifikationsnummer des sendestärksten Access-Points wird daraufhin an das Netz versendet, welches für diese Region eine passende Detailkarte mit allen Signalstärken („Fingerabdrücken“) an das Endgerät zurückschickt. Mithilfe der Karte kann das Endgerät nun seine Position innerhalb der Region selbst bestimmen. Bewegt sich das Gerät aus dem Kartenbereich, so wird einfach ein neuer Kartenausschnitt angefordert. Bei diesem Verfahren schickt das Endgerät lediglich grobe Positionsinformationen an das Netz und behält die detaillierten Daten für sich. So erfährt das Netz zwar, dass sich zum Zeitpunkt t_1 das beobachtete Objekt in der Region Y aufgehalten hat, kann aber nicht feststellen wo sich das Objekt zwischen dem ersten Kartenanforderungszeitpunkt und dem zweiten befunden hat. Der Schutzgrad der semiautonomen Positionsbestimmung wird maßgeblich durch die versendete Kartengröße und somit auch durch die Rechen- und Speicherkapazität des Endgerätes beeinflusst.

Nach absteigendem Datenschutzniveau geordnet ist folgende Einteilung der Ortungsverfahren möglich:

1. terminalbasierte Ortungsverfahren (passive Ortungsverfahren)
2. semiautonome Positionsbestimmungsverfahren und
3. netzseitige Ortungsverfahren

4.5 Zusammenfassung und Klassifizierung

In der nachfolgenden Abbildung 4.13 werden nochmals alle vorgestellten Ansätze zur Erhöhung der Datenschutzfreundlichkeit in LBS-Anwendungen in einem Überblick dargestellt. Hierfür wurden die Ansätze nicht nach dem bisherigen Gliederungsschema angeordnet, sondern in die zwei Hauptgruppen, „technolgiebasiert“ und „organisatorisch / regulatorisch“ eingeteilt.

Innerhalb der technologiebasierten Ansätze unterteilen sich die Verfahren in ausschließlich client- oder serverseitige Verfahren und client/serverseitige Verfahren. Der Block „organisatorisch / regulatorisch“ teilt sich in die Bereiche Selbstregulierung, staatliche Regulierung und Zugriffsregeln ein. Wie schon bei den Datenschutzaudits angesprochen, können Verfahren aus dem regulatorischen Bereich natürlich auch von technischen Verfahren profitieren und dadurch in ihrer Verbreitung gefördert werden.

Die Darstellung ermöglicht somit ein leichtes Zuordnen der PET-Bausteine in „Realisierungsgebiete“ der einzelnen LBS-Dienstteilnehmer. So bieten beispielweise alle client-basierten Bausteine einem LBS-Dienstnutzer die Möglichkeit, aktiv sein Datenschutzniveau zu erhöhen, unabhängig von allen anderen LBS-Teilnehmern. Natürlich sind innerhalb jeder Gruppe auch Abhängigkeiten zu beachten, die einen Effekt entweder verstärken oder abschwächen könnten. Serverbasierte Technologien hingegen finden im Bereich von TTPs oder LBS-Dienstanbietern Anwendung. Durch das Bereitstellen solcher Bausteine auf Anbieterseite können durch gesteigertes Vertrauen auf Kundenseite Kundenbindungseffekte erzielt werden. Parallel dazu eröffnen sich neue Möglichkeiten sich am Markt mit neuen Produkteigenschaften (zum Beispiel Anonymität) zu differenzieren.

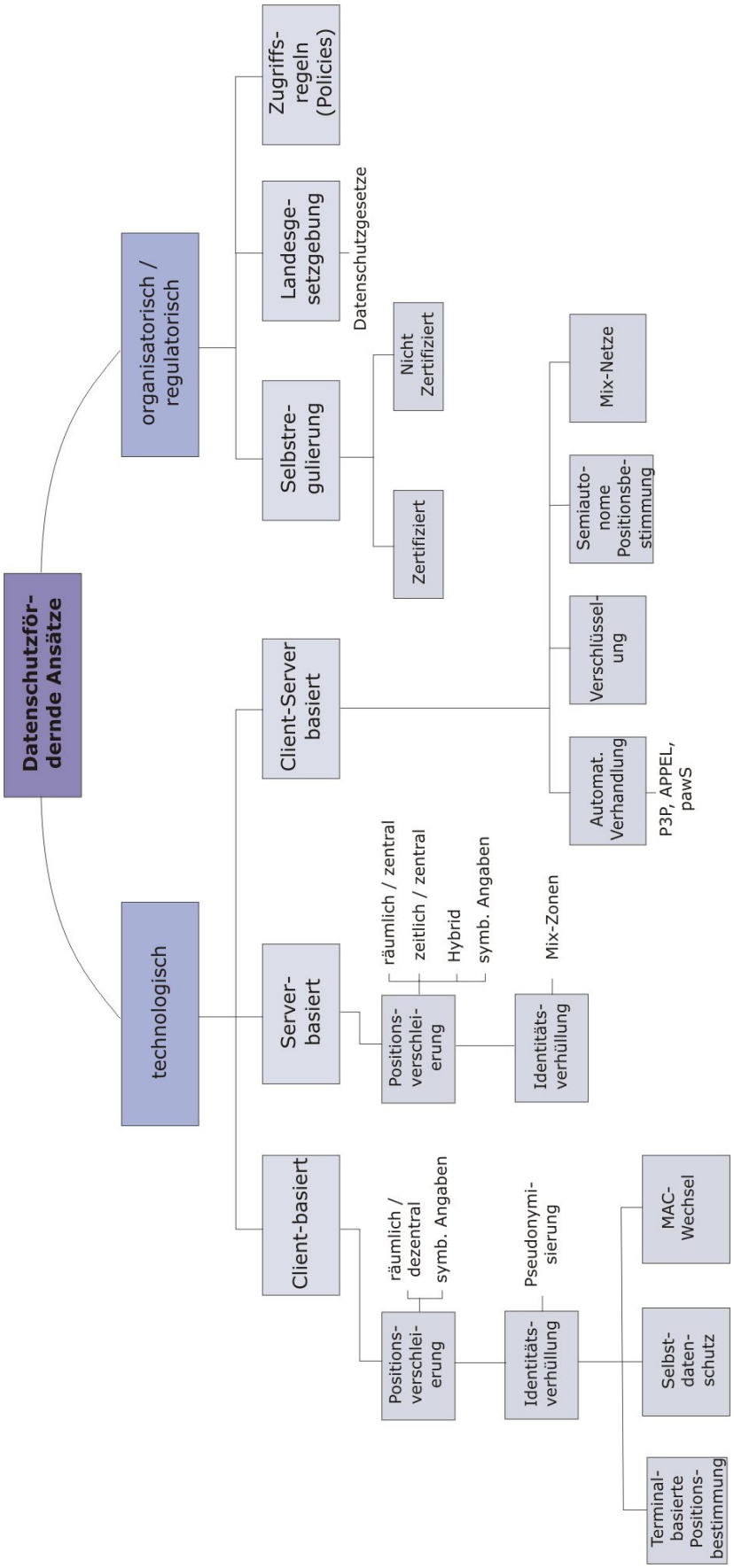

Abbildung 4.13: Verfahren und Methoden zur datenschutzfreundlichen Gestaltung von LBS im Überlick

Kapitel 5

Bezahlverfahren

Bezahlverfahren wurden in der vorangegangenen Betrachtung von LBS-Diensten (im Rahmen dieser Arbeit) nicht angesprochen. So wurden ausschließlich Komponenten zur Erhöhungen der Datenschutzfreundlichkeit vorgestellt die Bezahlverfahren komplett ausgeklammert haben. Diese sehr theoretische Betrachtungsweise hat jedoch in der wirklichen Welt kaum Bestand, da Investitionen in den Aufbau von LBS-Technologien sich amortisieren müssen und zudem Erträge für die Investoren schaffen sollten. Boddupalli und Kollegen [10, S. 1-2] machten sich zunächst Gedanken, wie Investoren aus LBS-Technologien erfolgreich Erträge generieren können.

- Kreuzsubventionierung (Cross-Subsidisation)
- Werbebasierte Finanzierung (Ad-based Revenue)
- Serviceorientierte Finanzierung (Charging for Service Use)

Dadurch kamen sie zu dem Schluss, dass die ersten beiden Varianten (Kreuzsubventionierung und werbebasierte Finanzierung) zwar Ertrag generieren können, dieser sich aber aufgrund der begrenzten Einsatzgebiete in engen Grenzen hält. Letztendlich hoben sie hervor, dass die serviceorientierte Finanzierung in Zukunft die größten Aussichten auf Erfolg hat. Aus diesem Grund befasst sich dieses Kapitel mit potentiellen elektronischen Bezahlverfahren die in LBS-Diensten zur Anwendung kommen könnten. Zunächst werden jedoch einleitend elektronische Bezahlverfahren (ePayment) klassifiziert und potentielle Anforderungen an LBS-Bezahlsysteme herausgearbeitet.

5.1 Klassifizierung von elektronischen Zahlungsverfahren

In der Literatur [93, 45, 51, 10] werden elektronische Bezahlverfahren nach unterschiedlichsten Kriterien, welche auch oftmals zur Beurteilung aus datenschutzrechtlicher Sicht dienlich sind, klassifiziert. Die im folgenden vorgestellten Klassifikationen dienen als Überblick und stellen nur eine Auswahl der wichtigsten Einteilungen dar.

post-payment, pre-payment, pay-now (Art der Zahlung) In Bezug auf den Zeitpunkt der Kontobelastung können Bezahlverfahren in diese drei Kategorien eingeteilt werden. Alle drei Varianten sind sowohl in der realen als auch in der elektronischen Welt realisierbar. Pay-now-Verfahren (debit-Verfahren) sind beispielsweise klassische EC-Kartenzahlungen oder Überweisungen. Pre-payments erfordern eine Belastung des Kontos vor dem eigentlichen Bezahlvorgang. Zu dieser Zahlungsmethode zählen insbesondere Telefonkarten, White Cards oder die Bargeldzahlung. Post-payments werden typischer Weise bei Kreditkartenzahlungen angewendet. In diese Kategorie fällt aber die klassische Rechnungsstellung. [93, S. 30-31][66, S. 403][51, S. 398]

Mit Post-payments ist allerdings keine anonyme Bezahlung im Internet möglich, da hier zumindest der Bank die notwendigen Kundendaten vorliegen müssen, um den Geldtransfer anstoßen zu können. Dahingegen ist eine Realisierung von anonymen Bezahlverfahren bei pre-payments durchaus möglich[93, S. 30].[51, S. 398]

Art des Wertetransfers Als zweite Möglichkeit zur Klassifizierung bietet sich die Art des Wertetransfers an. Man unterscheidet dabei transaktionsorientierte und bargeldorientierte Verfahren. Transaktionsorientierte Bezahlverfahren benötigen immer die Angabe eines Empfängers und Absenders, damit die fälligen Geldbeträge ordnungsgemäß transferierbar sind. Dahingegen übermitteln bargeldorientierte Verfahren nicht Geldbeträge, sondern wirkliche Geldeinheiten. Diese Art der Bezahlung kann mit der Bezeichnung „Face-to-Face“ Bezahlverfahren gleichgesetzt werden, wenn Wertetransfers zwischen zwei Kunden oder zwei Geschäftsleuten, ohne Einmischung einer dritten Instanz, möglich sind.[51, S. 398]

Bargeldorientierte Verfahren lassen sich somit auch elektronisch datenschutzfreundlich realisieren, sofern in den digitalen Münzen keine personenbezogenen Daten vermerkt werden. Transaktionsorientierte Zahlungsverfahren hingegen sind aufgrund der notwendigen Angaben nie anonym implementierbar und hinsichtlich des Datenschutzniveaus unter den bargeldorientierten Verfahren anzusiedeln.

Art des Geldkreislaufes Knorr und Schläger [51] klassifizieren darüber hinaus die Verfahren anhand des Geldkreislaufes. Hier sind wieder zwei Unterscheidungsmöglichkeiten vorhanden. Zum einen gibt es geschlossene Kreisläufe, die sich zwischen dem Kunden, Händler, der Kunden- und Händlerbank bilden. Bezüglich des Zahlungsrisikos sind geschlossene Kreisläufe mit einem niedrigen Risiko einzustufen, da zum Beispiel das Risiko für Manipulationen zwischen den genannten Instanzen sehr gering ist. Daneben existieren die schon zuvor erwähnten „Face-to-Face“-Verfahren, welche einen direkten Geldtransfer zwischen zwei Personen oder Unternehmen ermöglichen.

Insgesamt sind die geschlossenen Kreisläufe schlecht datenschutzfreundlich zu realisieren, da Kreditinstitute sehr leicht alle Zahlungsflüsse mitprotokollieren können. Dieses Risiko ist bei Face-to-Face-Verfahren nicht vorhanden.[51, S. 398]

Art der Geldbörsenplattform Ein letzte von den Autoren [51] genannte Klassifizierungsmöglichkeit besteht in der Art der verwendeten Geldbörsenplattform. So können elektronische Bezahlverfahren sowohl hardwaretechnisch - zum Beispiel chipkartengestützt - als auch hardwareunabhängig realisiert werden. Der Vorteil von chipkartengestützten Zahlungsverfahren ist die relativ hohe Manipulationssicherheit der hardwaretechnischen Komponenten. Als Beispiele für diese Verfahren können White Cards, handelsübliche Telefonkarten oder

auch EMV-Chips genannt werden. Von Nachteil ist allerdings, dass besonders im Umfeld der LBS-Anwendungen bisher kaum Endgeräte mit entsprechender Hardware existieren, die etwaige Geldchipkarten auslesen können und somit der Einsatz hardwarebasierter Verfahren gehemmt wird. [93, S. 31] Im Gegensatz dazu können hardwareunabhängige Verfahren zwar nicht mit hoher Manipulationssicherheit überzeugen, dennoch erweist sich gerade die Hardwareunabhängigkeit bei mobilen Anwendungen als Vorteil, da häufige Endgerätewechsel nicht auszuschließen sind.

Einteilung nach dem Zahlungsbetrag Neben den zuvor genannten Klassifizierungsmöglichkeiten lassen sich Bezahlverfahren zudem nach ihren üblichen Geldübermittlungsgrößen einteilen. Macro-payments sind in der Regel Bezahlverfahren, die mehr als 5 Euro pro Transfer übermitteln. Hierzu zählen beispielsweise Kreditkarten, EC-Karten etc. Entsprechend der möglichen Schadenshöhe wurden diese Verfahren in der Vergangenheit gegen Angriffe wie Betrug oder Fälschung stark abgesichert. Damit einher gehen relativ hohe Abwicklungskosten pro Transfer, weshalb sich Macro-payments nicht für den häufigen Transfer von Kleinstgeldbeträgen eignen. Zahlungsverfahren, die Beträge unter 5 Euro abwickeln, ordnet man der Gruppe der so genannten Micro-payments zu. Charakteristikum dieser Verfahren ist, dass, häufig zu Lasten der Sicherheit, die Transaktions- und Abwicklungskosten minimiert werden.[10, S. 4-5][45, S. 9]

Die zuvor erwähnte 5 Euro Grenze variiert je nach Publikation und versteht sich nicht als starre Größe. So unterteilen [93, S. 14] beispielsweise die Zahlungsverfahren in vier Gruppen (Picopayment, Micropayment, Small-/Minipayment und Macropayment) mit völlig anderen Grenzbeträgen.

5.2 Anforderungen an LBS-Bezahlsysteme

Nachdem in der Literatur häufig erwähnte Klassifikationsmöglichkeiten für Bezahlsysteme und deren Bedeutung für den Datenschutz kurz aufgezeigt wurden, sollen in diesem Abschnitt Anforderungen gefunden und definiert werden, die ein Bezahlverfahren innerhalb einer LBS-Anwendung idealerweise erfüllen sollte. Diese Anforderungen sind natürlich nicht identisch mit denen, die an herkömmliche, vielleicht schon eingesetzte Systeme gestellt werden, da LBS-Dienste teilweise völlig andere Anforderungen besitzen. Tabelle 5.1 stellt alle wesentlichen Anforderungen dar und liefert eine kurze Beschreibung dieser.

Anforderung	**Beschreibung**
Spontanität	LBS-Anwendungen sind von ihrer Charakteristik her hoch dynamisch. Deshalb ist bei den Bezahlsystemen eher von kurzzeitigen Geschäftsverbindungen, als von Langzeitverbindungen auszugehen. Die Autoren [10] bezeichnen diese Art des Bezahlens als *„pay-as-you-go“*[10, S. 3].

Fortsetzung auf der nächsten Seite.

Anforderung	**Beschreibung**
Effizienz	Bezahlverfahren im Umfeld von LBS-Anwendungen müssen besonders im Bereich der Kommunikation und Abwicklung sehr effizient arbeiten. So sollte der Kommunikations-Overhead minimiert und die Abwicklungs- und Transaktionskosten so gering wie möglich gestaltet werden. Dies gewinnt vor allem dann an Bedeutung, wenn anzunehmen ist, dass LBS-Anwendung exzessiven Gebrauch von Kleinbetragszahlungssystemen machen.
Sicherheit	Sicherheitsaspekte sind für beide Seiten - Dienstnutzer und -anbieter - von hoher Bedeutung. So muss ein Bezahlverfahren vor Diebstahl, Fälschung und anderen Betrugsversuchen schützen.
Datenschutz	Besonders bei LBS-Anwendungen besteht die Gefahr, dass personenbezogene Daten mit Positionsinformationen in Verbindung gebracht werden und so ein Erstellen von personalisierten Bewegungsprofilen möglich ist. Um dem entgegenzuwirken sollte ein Bezahlsystem auf Wunsch auch anonyme Transaktionen zulassen, ohne dass beispielsweise der LBS-Anbieter Name, Kreditkartennummer und Adresse des Kunden erfährt.
Flexibilität	Die Flexibilität von Bezahlverfahren in Bezug auf LBS-Anwendungen erstreckt sich auf zwei Gebiete. Zum einen muss das ausgewählte Verfahren unabhängig von zugrundeliegenden Geräten und Netzwerken arbeiten. Gerade in Zukunft ist mit einer technisch sehr heterogenen Umgebung zu rechnen. Zum anderen muss das Bezahlverfahren 1. in diskonnektiven Phasen arbeiten und 2. möglichst gegen die Unverfügbarkeit von Geräten resistent sein. Ersteres bedeutet, dass kurzzeitige Funkstörungen nicht zu einer Beeinträchtigung des Zahlverfahrens führen dürfen. Mit dem Schutz vor Unverfügbarkeit von Geräten ist gemeint, dass beispielsweise elektronisches Münzgeld nicht auf einem Endgerät abgelegt sein sollte, welches ausfallbedroht ist (zum Beispiel durch Stromverlust).
Benutzerfreundlichkeit	Schenkt man den zukünftigen Voraussagen glauben, so werden pro Tag und Person eine Vielzahl an Zahlungsvorgängen in Verbindung mit LBS-Diensten stattfinden. Hieraus folgt unmittelbar, dass ein eingesetztes Zahlungssystem intuitiv und einfach zu bedienen sein muss. Als Vergleichsmaßstab aus Kundensicht dienen die oftmals täglich eingesetzten Bezahlverfahren wie Kredit- oder Bankkarte.
Universalität	Ein elektronisches Bezahlverfahren sollte nach Möglichkeit sowohl für den Business-to-Customer (B2C), als auch für den Business-to-Business (B2B) Bereich einsatzbar sein.
Verbreitungsfähigkeit	Neben den zuvor genannten Punkten muss ein elektronisches Bezahlverfahren auch weitflächig einsetzbar sein. Hierzu müssen einerseits bestehende LBS-Anwendungen das Verfahren - sofern noch nicht geschehen - leicht integrieren und andererseits neue Applikationen dieses über Schnittstellen nutzen können. Daneben sollte ein Verfahren auch grenzüberschreitenden Zahlungsverkehr ermöglichen.

Tabelle 5.1: Anforderungen an elektronische Bezahlsysteme in LBS-Anwendungen in Anlehnung an [10, S. 2-4][96, S. 1-2][45, S. 51-53]

5.3 Potentielle Bezahlverfahren

Die nun folgende Auswahl an Verfahren zur elektronischen Zahlungsabwicklung versteht sich nicht als Auflistung *aller* potentiellen Bezahlverfahren, die eventuell verfügbar sind. Vielmehr handelt es sich um eine Selektion, anhand derer Probleme verschiedener Systeme, in Hinblick auf den Einsatz in LBS-Anwendungen, diskutiert werden sollen. Die Ergebnisse lassen sich dann auf hier nicht angesprochene Verfahren übertragen.

5.3.1 Elektronisches Bargeld

Elektronisches Bargeld ist ein Äquivalent zu den bisher bekannten klassischen Zahlungsmitteln wie Münzen und Banknoten. Im Gegensatz zu seinen realen Repräsentanten ist elektronisches Bargeld körperlos und wird nur durch eine Zahlenfolge aus Nullen und Einsen, die durch die emittierende Bank signiert wird, dargestellt. Wie auch reales Bargeld muss elektronisches Geld den Anforderungen an Fälschungssicherheit, Flexibilität und Anonymität (Datenschutz) genügen.

Die Funktionsweise von elektronischem Geld lässt sich wie folgt beschreiben: Zunächst muss der Nutzer des Bezahlsystems elektronische Münzen erwerben. Hierfür tauscht dieser bei einer Bank oder Nichtbank reale Geldbestände in digitale Münzen um. In der Regel werden diese in Form von Dateien entweder auf ein mobiles Endgerät übertragen oder in einem virtuellen Portemonaie serverseitig zwischengespeichert. Möchte der Kunde eine kostenpflichtige LBS-Dienstleistung beziehen, so kann er digitale Münzen direkt an den richtigen Empfänger (LBS-Anbieter) übermitteln. Der Empfänger muss nun lediglich die Gültigkeit der erhaltenen digitalen Münzen prüfen. Ist die Validität gegeben, hat der LBS-Anbieter sofort einen Gegenwert für seine Ware bzw. Dienstleistung erhalten.

5.3.1.1 eCash

eCash ist eines der bekanntesten elektronischen Münzzahlungssysteme. Es wird von der Firma Digicash angeboten und wurde von der Deutschen Bank 24 in Deutschland erfolglos bis Juni 2001 getestet[1] [78, S. 36]. Die Grundlagen von eCash bilden Verfahren die der niederländische Kryptologe Chaum entwickelte. Genaue Ablaufbeschreibungen der eingesetzten Protokolle sind in [51, S. 399] und [45, S. 36-38, 62-63] zu finden.

eCash ist nach [51] bei den bargeldorientierten Prepaid-Verfahren[2] einzuordnen. Es ermöglicht dem Nutzer vollkommen anonym gegenüber der Bank und dem LBS-Dienstanbieter aufzutreten [45, S. 62]. Das geldausgebende Institut kennt zwar den Geldbetrag, den ein Kontoinhaber in elektronische Münzen umwandelt, jedoch nicht die Seriennummer, mit der jede elektronische Münze eindeutig identifizierbar ist. Das zugrundeliegende kryptografische Verfahren ist die so genannte Blinde Signatur. Um die Fälschung von elektronischen Geldeinheiten zu erschweren wurde auf die Implementierung eines Face-to-Face Umlaufes verzichtet. Der kleinste übertragbare Geldbetrag ist 0,01 Cent, welcher in zweier Potenzschritten beliebig erhöhbar ist.

[1] siehe http://www.dradio.de/magazin/010525-01.html, Abruf am: 08.04.2004

[2] Grimm [78, S. 36] zählt eCash dahingegen zu den pay-now-Verfahren, aufgrund der Ähnlichkeit zu Bargeld.

Bewertung: Hinsichtlich des in Tabelle 5.1 auf Seite 60 dargestellten Kataloges werden fast alle Anforderungen an ein Bezahlsystem für LBS-Anwendungen nahezu vollständig erfüllt. Insbesondere der Datenschutz fand in dieser Umsetzung Beachtung, da sich sowohl gegenüber dem Händler als auch gegenüber der Bank komplett anonyme Bezahlvorgänge abwickeln lassen [51, S. 399-400][78, S. 50-51]. Einzig problematisch für LBS-Anwendungen ist die auf dem Endgerät zu installierende Software - so genannte Wallet-Software - und die damit verbundene Abhängigkeit vom Endgerät. Fällt das Endgerät zum Beispiel aufgrund eines leeren Akkus aus, so sind die digitalen Münzen bis zur Wiederherstellung eines betriebsfähigen Zustandes im Endgerät „gefangen“. Ein weiteres allgemeines Hemmnis ist die bisher schlechte Verbreitungsfähigkeit der Münzen. So kann aufgrund fehlender Kooperationen zwischen den emittierenden Instituten ein Ausländer in Deutschland nicht mit seinen im Ausland erworbenen digitalen Münzen zahlen.

5.3.1.2 Millicent

Millicent ist ein weiteres elektronisches Zahlungssystem, welches von der Digital Equipment Cooperation entwickelt wurde. Es unterstützt ausschließlich Zahlungsbeträge im Bereich von 0,001 bis 5 US-Dollar. Aufgrund der relativ geringen Transferbeträge verzichteten die Ingenieure des Systems auf hohe Sicherheitsstandards, um im Gegenzug die Effizienz des Verfahrens zu steigern. Im Gegensatz zu eCash werden nicht digitale Münzen, die bei allen angeschlossenen Händlern eingelöst werden können, verwendet, sondern händlerspezifische Münzen, so genannte Scrips. Ein Scrip ist eine Art Gutschein, der gegen Bezahlung bei dem jeweiligen Dienstanbieter erworben werden kann, um ihn später bei diesem gegen Dienstleistungen wieder einzutauschen. Dadurch verlagert sich die Gültigkeitskontrolle von der Bank in den Zuständigkeitsbereich des Händlers, was das Verfahren schneller und effizienter als eCash macht. Allerdings wird die erhöhte Performance mit einer stark eingeschränkten Nutzung der Gutscheine erkauft, weshalb in der endgültigen Millicent-Architektur ein Scrip-Broker eingesetzt wird. Möchte ein Kunde eine Dienstleistung in Anspruch nehmen, so kontaktiert er zuvor seinen Scrip-Broker und fordert für den gewünschten Dienstanbieter die benötigte Menge an Scrips an. Daraufhin erwirbt der Broker, falls notwendig, für den Kunden wenigstens die geforderte Scrip-Anzahl und übermittelt die Scrips an den Kunden. Anschließend kann der Kunde im Tausch gegen Scrips seine Dienstleistungen in Anspruch nehmen. Entspricht die angeforderte Dienstleistung nicht dem gesamten Wert des Scrip, so erhält der Kunde ein neues Scrip mit reduziertem Wert zurück. [45, S. 38-40][60]

Bewertung: Das Millicent-Bezahlverfahren ermöglicht nicht wie eCash ein vollkommen anonymes Auftreten des Kunden. So kennt der Scrip-Broker die Identität des Kunden und der LBS-Dienstanbieter das Nutzungsprofil, sofern nicht bei jeder Transaktion das übermittelte Scrip vollständig aufgebraucht wird. In der Regel ist somit eine pseudonyme Kommunikation möglich. Als Vorteil von Millicent ist jedoch herauszustellen, dass nicht wie im eCash-Verfahren alle Münzen auf dem Endgerät gehalten werden müssen, sondern nur für die aktuell genutzten Dienstleistungen die Scrips gespeichert werden. Somit kann ein LBS-Nutzer auch bei einem Geräteausfall auf sein Scrip-Broker-Konto zugreifen und muss auf die Dienstnutzung nicht verzichten. Des Weiteren unterstützt das Millicent-Protokoll viel besser als eCash die Anforderung „pay-as-you-go“. Denn im Vergleich zu eCash ist erstens die Stückelung mit 1/1000 Cent viel kleiner und zweitens betragen die Gebühren pro Transaktion nur einen Bruchteil der

von eCash geforderten. Diese Eigenschaften prädestinieren das Millicent-Protokoll besonders für Bereiche in denen häufig sehr kleine Geldbeträge zu zahlen sind.

5.3.2 Wertkartenbasierte Bezahlverfahren

Wertkartenbasierte Bezahlverfahren sind im weitesten Sinne mit Telefon-Wertkarten zu vergleichen und damit in die Kategorie der prepaid-Systeme einzuordnen. Der Ablauf der Zahlung bei den im folgenden vorgestellten Systemen ist prinzipiell immer gleich und soll an dieser Stelle kurz umrissen werden.

Möchte ein Kunde an einem der dargestellten Bezahlsysteme teilnehmen, so muss er zunächst eine Wertkarte kaufen. Hierfür stehen in der Regel verschiedene Shops, wie zum Beispiel Postfilialen oder Kioske, zur Verfügung. Jede gekaufte Wertkarte enthält ein bestimmtes Guthaben, für das entsprechende Dienstleistungen eingekauft werden können. Mithilfe dieser Karte und in Kombination mit einer PIN-Nummer kann dann in dafür ausgestatteten elektronischen Shops eingekauft werden. Ist das Guthaben auf der Wertkarte aufgebraucht muss der Teilnehmer eine neue Wertkarte erwerben. Ein Aufladen der bisher verwendeten Karte ist in der Regel nicht mehr möglich.

5.3.2.1 paysafecard

Seit 2001 bietet die österreichische Firma „paysafecard.com Wertkarten AG“ das paysafecard-System in Deutschland an [78, S. 42]. Darüber hinaus wird die paysafecard in vielen weiteren europäischen Staaten verwendet, was hinsichtlich der Verbreitungsfähigkeit eines LBS-Bezahlverfahrens zu berücksichtigen ist. Wie in der Einleitung zu diesem Kapitel beschrieben, muss ein paysafecard-Kunde zunächst eine Wertkarte käuflich erwerben um elektronische Bezahlvorgänge abwickeln zu können. Will der Nutzer einen kostenpflichtigen Dienst nutzen, so wird er vom Anbieter an einen von paysafecard betriebenen Server weiterverbunden. Auf der dort hinterlegten Eingabemaske autorisiert der Kunde durch Eingabe seiner freigerubbelten PIN den vom Händler geforderten Geldbetrag. Ist die Zahlung erfolgt erhält der Kunde seine angeforderte Dienstleistung.

Bewertung: Aus Sicht des Datenschutzes arbeitet dieses Bezahlverfahren gegenüber dem Zahlenden absolut datensparsam [78, S. 54-55]. Sowohl der Wertkartenkauf, als auch die gesamte Abwicklung der Zahlung erfolgen vollständig anonym, die Angabe von personenbezogenen Daten ist nicht erforderlich [42]. Besonders geeignet scheint dieses Verfahren bei eher selten genutzten LBS-Diensten, beispielsweise Hotelanfragen, da die erforderliche Eingabe der 16-stelligen PIN recht umständlich ist. Für Tracking-Anwendung hingegen ist dieses Verfahren nicht optimal, da eine ständige Neueingabe der PIN notwendig wäre. Ein weiterer Vorteil ist, dass keine zusätzliche Software auf dem Endgerät vorhanden sein muss und die Werteinheiten unabhängig vom Endgerät nutzbar sind.

5.3.2.2 T-Pay

T-Pay[3] ist ein Zahlungsverfahren der Deutschen Telekom, dass neben weiteren Abrechungssystemen[4] auch eine wertkartenbasierte Zahlung unterstützt (das Verfahren wird von der Telekom „Micro-Money“ genannt). Um an dem Bezahlsystem teilnehmen zu können erwirbt der Teilnehmer zunächst eine Wertkarte, auf der ein Guthaben von 15 Euro ist, in einem Telekom-Shop. Der weitere Ablauf des Bezahlvorganges ist mit dem der paysafecard gleichzusetzen.

Aufgrund der Gleichheit der beiden Systeme - sofern man bei T-Pay die Micro-Money-Variante wählt - fällt die Bewertung identisch zur paysafecard aus.

5.3.3 Kreditkartenbasierte Bezahlsysteme

Die Kreditkarte - beispielsweise von Visa oder Mastercard - ist wohl das am weitesten verbreitete und akzeptierte Zahlungsmittel weltweit. Besonders in den Vereinigten Staaten, aber auch in Europa erfreut sich die Kreditkarte einer großen Beliebtheit und hohen Akzeptanz als Zahlungsmittel. Dies war wohl einer der Hauptgründe dafür, dass kreditkartenbasierente Zahlungssysteme für elektronische Netze entwickelt wurden.

Im Voraus ist jedoch zu sagen, dass aufgrund der Entwicklungsgeschichte von Kreditkarten diese Systeme hinsichtlich Performance, Sicherheit und Transaktionskosten auf Macropayments ausgerichtet sind und sich daher in der Regel nicht für den Transfer von Kleinstgeldbeträge eignen. Damit einher geht, dass „pay-as-you-go“ Anwendungen mit diesen Bezahlsystemen nicht abgewickelt werden sollten [10]. Dennoch bietet sich eine Betrachtung der kreditkartenbasierten Verfahren an, da zum Beispiel für pauschal angebotene LBS-Anwendungen diese Zahlungssysteme sehr wohl effektiv eingesetzt werden können.

5.3.3.1 Secure Electronic Transaction

Secure Electronic Transaction (SET) ist nicht wie die nachfolgenden zwei kreditkartenbasierten Zahlungssysteme ein Zahlungsverfahren, sondern vielmehr ein Protokoll, das unter anderem von Visa, Mastercard und Microsoft entworfen wurde [42, S. 2]. Bei diesem Protokoll wird ein Nutzer des Zahlungssystems nicht mehr über seine Kreditkartennummer identifiziert, sondern über ein extra für ihn ausgestelltes Zertifikat. Somit sind seitens des Kunden drei Voraussetzungen zu erfüllen. Erstens benötigt er ein Konto mit einer dazugehörigen Kreditkarte, zweitens ein Zertifikat, dass er bei seiner kartenausgebenden Institution beantragen muss. Zudem ist eine Wallet-Software auf dem mobilen Endgerät erforderlich, die alle notwendigen Verschlüsselungsmaßnahmen während des Bezahlvorgangs durchführt.

Möchte der Kunde eine Dienstleistung über ein elektronisches Netzwerk erwerben, so versendet er folgende Informationen signiert an den Händler [45, S. 30]:

1. **Bestellinformationen** bestehend aus Menge und Preis, welche für den Händler lesbar sind

[3] siehe: http://www.t-com.de/is-bin/intershop.static/WFS/PK/PK/de_DE/content/animations/t-pay/t-pay.htm oder http://www.t-pay.de

[4] Abrechnungssysteme: Lastschrift, Kreditkartenbelastung, Abbuchung von der Telefonrechnung und Micro Money

2. **Zahlungsinformationen** die sich aus Kreditkartennummer, Ablaufdatum etc. zusammensetzen und nur für das SET-Gateway lesbar sind

Der Händler wiederum bildet aus den Bestellinformationen einen Hashwert, den er mit seiner Händler-Signatur unterschreibt. Das Paket, bestehend aus den verschlüsselten Zahlungsinformationen, dem Zahlungsbetrag und dem signierten Hashwert verschickt der Händler an ein so genanntes SET-Gateway. Das SET-Gateway entschlüsselt die vom Kunden verschlüsselten Zahlungsinformationen, prüft die Bonität des Kunden und veranlasst daraufhin die Überweisung des Geldbetrags.[72]

Eine erweiterte SET-Version, dass so genannte SET-3D (SET-Three Domain Model) verlagert die bisher endgeräteseitig gehaltene elektronische Wallet-Software auf einen Server.[78, S. 35-36]

Bewertung: Wie schon eingangs erwähnt ist SET insbesondere wegen der hohen Sicherheitsstandards und den damit einhergehenden hohen Transaktionskosten für Micropayments ungeeignet. Dennoch existieren eine Reihe von Anwendungen bei denen dieser Aspekt vernachlässigbar ist und durch den Vorteil der weiten Verbreitung von Kreditkarten mehr als aufgewogen wird. Neben der hohen Sicherheit sowohl für Kunden als auch für LBS-Dienstanbieter bietet SET dem Kunden die Möglichkeit gegenüber dem LBS-Dienstanbieter pseudonymisiert aufzutreten [42, S. 6][78, S. 50]. Eine anonyme Bezahlung ist nicht vorgesehen und wurde auch beim Design des Protokolls nicht angestrebt. Gegenüber der emittierenden Bank ist nicht einmal eine Pseudonymisierung vorgesehen. So erfährt diese auf jeden Fall den Namen, die Anschrift des Kunden und die Namen der LBS-Anbieter bei denen der Kunde Leistungen bezogen hat, aber nicht die in Anspruch genommenen Dienstleistungen.

5.3.3.2 Cybercash

Cybercash[5] ist ein klassisches post-payment-Verfahren welches für den Einsatz in Netzwerken geschaffen wurde. Als Vorgänger zum SET-Protokoll hat es sehr viel Ähnlichkeit mit diesem und unterscheidet sich nur in einer Eigenschaft grundlegend. Während im SET-Protokoll die kreditkartenausgebende Instanz den Händler und der Händler den Kreditkartenemittenten kennt, wurde bei Cybercash diese Beziehung unter zuhilfenahme einer TTP aufgelöst. Der übliche Bezahlvorgang ist wie folgt aufgebaut [51, S. 400]:

1. Der Dienstnutzer erhält auf eine Dienstanfrage hin ein Angebot des Händlers
2. Der Dienstnutzer bestätigt das vom Händler erhaltene Angebot indem er dieses, zusammen mit seiner für die TTP (CyberCash-Server) verschlüsselten Kreditkartennummer, digital signiert wieder an den Händler verschickt
3. Der Händler ergänzt die Angaben um den Gesamtzahlungsbetrag und leitet das Paket an den CyberCash-Server (TTP) weiter
4. Der CyberCash-Server entschlüsselt die Kreditkartennummer und prüft die Bonität des Dienstnutzers bei der kreditkartenemittierenden Instanz

[5] wurde 2001 in Deutschland wieder eingestellt [78, S. 33]

5. Das Zahlungsergebnis wird an den Händler weitergeleitet, der wiederum eine Abrechnung an den Dienstnutzer senden kann

Wie auch bei SET ist für das Ausführen eines solchen Bezahlvorgangs eine Software auf Nutzerseite notwendig, um die protokollspezifischen Verschlüsselungsmaßnahmen durchführen zu können.

Bewertung: Obwohl SET auf Cybercash aufbaut, ist der Schutz des Dienstnutzers im Cybercash-System höher. Cybercash ermöglicht dem Dienstnutzer ein pseudonymisiertes Auftreten gegenüber dem Händler und entspricht somit dem SET-Protokoll. Jedoch kennt im Cybercash-Bezahlsystem die kreditkartenemittierende Instanz nicht mehr den Händler und anders herum. Dadurch ist es dem Kreditkarteninstitut nicht mehr möglich, Teilprofile von Nutzern zu erstellen, es sei denn, Cybercash würde mit diesen Instituten zusammenarbeiten. Als Nachteil von Cybercash ist zu erwähnen, dass wiederum auf dem Endgerät eine Wallet-Software notwendig ist.

5.4 Zusammenfassung

Tabelle 5.2 enthält einen Überblick aller angesprochenen Bezahlverfahren und eine Bewertung dieser hinsichtlich der in Kapitel 5.2 aufgestellten Kriterien. Die Anforderungen Benutzerfreundlichkeit, Universalität und Verbreitungsfähigkeit fanden keine Berücksichtigung, da eine Bewertung der Anforderungen im Rahmen dieser Diplomarbeit zu umfangreich gewesen wäre und kein weiteres Material aus der Literatur zur Verfügung stand. Die aufgeführten Anforderungen wurden nach folgendem Schema bewertet: ++ Anforderung voll erfüllt, + Anforderung wird teilweise erfüllt, - Bezahlverfahren ist nicht ideal, - - Bezahlverfahren verfehlt die Anforderung.

	Spontanität	**Effizienz**	**Sicherheit**	**Datenschutz**	**Flexibilität**
eCash	++	-	++	++	+
Millicent	++	-	-	-	++
paysafecard	-	++	++	-	++
T-Pay	-	++	++	-	++
SET	-	++	++	-	-
CyberCash	-	++	++	+	-

Tabelle 5.2: Bewertung der Bezahlverfahren

Tabelle 5.2 ließe nun den Schluss zu, dass idealerweise das Bezahlverfahren eCash in allen LBS-Anwendungen zum Einsatz kommen sollte. Dieses Urteil wäre jedoch voreilig. eCash erfüllt zwar fast alle Idealanforderungen in Bezug auf die hier aufgelisteten Punkte, aber wenigstens genauso wichtige Punkte wie Benutzerfreundlichkeit, Akzeptanz aus Benutzersicht, Universalität etc. fanden keine Berücksichtigung. So würde wahrscheinlich ein kreditkartenbasiertes Bezahlverfahren wie SET bei der Akzeptanz viel besser abschneiden, da Kreditkarten schon seit längerem als vertrauensvolles Zahlungsmittel anerkannt sind. Des Weiteren sind anwendungsspezifische Faktoren bei der richtigen Auswahl eines Bezahlverfahrens zu beachten.

Touristenführer, beispielsweise, benötigen zur korrekten Führung des Dienstnutzers wenigstens ein Rollen-Beziehungspseudonym, damit bereits besuchte Museen oder Sehenswürdigkeiten nicht nochmals ausgewählt werden. In diesem Fall können bedenkenlos Bezahlverfahren zum Einsatz kommen, die ebenfalls nur eine pseudonymisierte Bezahlung ermöglichen, da auch hier gilt, dass die Kette nur so stark ist wie ihr schwächstes Glied. Auch bei Einsatz von anonymen Bezahlverfahren kann kein höheres Datenschutzniveau erreicht werden.

Boddupalli und Kollegen [10, S. 5] schlagen einen anderen Weg bei der Suche nach optimalen Bezahlverfahren für LBS-Dienstleistungen ein. Die Autoren orientieren sich dabei ausschließlich an der Klassifizierung in Micro- und Macropayment-Verfahren. Die Ergebnisse

Anforderung	**Macropayments**	**Micropayments**
Spontanität	nicht unterstützt	unterstützt
Kosten der Verschlüsselung	hoch	niedrig
Broker Interaktion	häufig	gelegentlich
Transaktionskosten	hoch	niedrig
Funktion bei Diskonnektivität	nicht unterstützt	unterstützt
Zahlungsverzögerung	hoch	niedrig
Anonymität	niedrig	hoch
Sicherheit	mittel-hoch	niedrig-mittel

Tabelle 5.3: Micro- vs. Macropayments [10, S. 5]

ihrer Untersuchung sind in Tabelle 5.3 zu sehen. Mithilfe dieser Untersuchung kommen sie zu dem Schluß, dass ausschließlich Micropayment-Verfahren für LBS-Anwendungen geeignet sind, berücksichtigen dabei aber nicht die teilweise sehr unterschiedlichen Anforderungen von LBS-Diensten.

Abschließend soll nochmals hervorgehoben werden, dass zwar Bezahlsysteme, die die Idealanforderungen erfüllen, generell zu bevorzugen sind, aber eine anwendungsbasierte Abwägung zwischen den einzelnen Verfahren nicht unterlassen werden darf. So kann der Anforderungskatalog bei einer ersten Selektion Verwendung finden, auf Basis derer dann eine fundierte Entscheidung getroffen werden kann.

Kapitel 6

Vorschlag zur Konstruktion von datenschutzfreundlichen LBS

In den letzten Kapiteln wurde eine Vielzahl von unterschiedlichen Methoden, Verfahren und organisatorischen Maßnahmen vorgestellt, mithilfe derer eine Konstruktion von datenschutzfreundlichen und kostenpflichtigen Location Based Services möglich ist. Jede Einheit für sich alleine genommen erzeugt in ihrem abgegrenzten Gebiet einen Nutzen, der aus Sicht des Datenschutzes zu einer Erhöhung des Datenschutzniveaus führt. Doch wie können die Einzelkomponenten auf eine gesamte LBS-Anwendung übertragen werden und wie sind sie sinnvoll zusammenzufügen? Generell ist festzuhalten, dass die große Heterogenität der Anwendungen die in den Bereich LBS eingeordnet werden, ein Hauptproblem darstellt, auf das bei der Konstruktion und Zusammenstellung unbedingt geachtet werden muss. So existieren zum einen die klassischen Pull-Anwendungen, bei denen der Nutzer die Diensterbringung „anstoßen“ muss, zum anderen die Push-Anwendungen, die genau umgekehrt funktionieren. Weitere Schwierigkeiten gibt es bei der Art der Positionsbestimmung oder bei den Methoden, mit denen die Ortungsgenauigkeit herabgesetzt werden kann. Für Werbeanwendungen eigenen sich beispielsweise symbolische Positionsangaben, wohingegen typische Tracking-Anwendungen nur auf Basis von absoluten Koordinaten arbeiten können. Zu den Eigenheiten jeder LBS-Anwendung kommen aber noch die der eingesetzten Kommunikationsnetze. GSM-Netze erfordern eine andere Absicherung gegen die Erstellung von Bewegungsprofilen als IEEE 802.11b WLANs. Ideal wäre demnach die Identifizierung von Komponententeilmengen die für alle LBS-Anwendungen anwendbar sind und anderen, die nur anwendungsspezifisch zum Einsatz kommen. Den zweiten wichtigen Punkt bei der Konstruktion bestimmen die heutigen und zukünftigen Nutzer selbst. Damit ist gemeint, dass beim Aufbau von LBS-Anwendungen Anforderungen der Dienstteilnehmer bezüglich des Datenschutzes in besonderem Maße Eingang finden sollten. Der Nutzen von hoch abgesicherten und datenschutzfreundlichen LBS-Anwendungen ist als eher gering zu bewerten, wenn sie in dieser Form nicht vom Nutzer gefordert wurden. Zudem führen umfangreiche Absicherungsmaßnahmen zu zusätzlichen Kosten, die am Ende der Konsument zu tragen hat. So könnte ein „over-engeneering“ das Gegenteil erreichen und LBS-Benutzer abschrecken.

6.1 Anwendungsspezifische Konstruktion

Zunächst soll das Problem der Heterogenität von LBS-Anwendungen und deren Folge auf den Einsatz von Komponenten zur Förderung des Datenschutzes untersucht werden. In Ab-

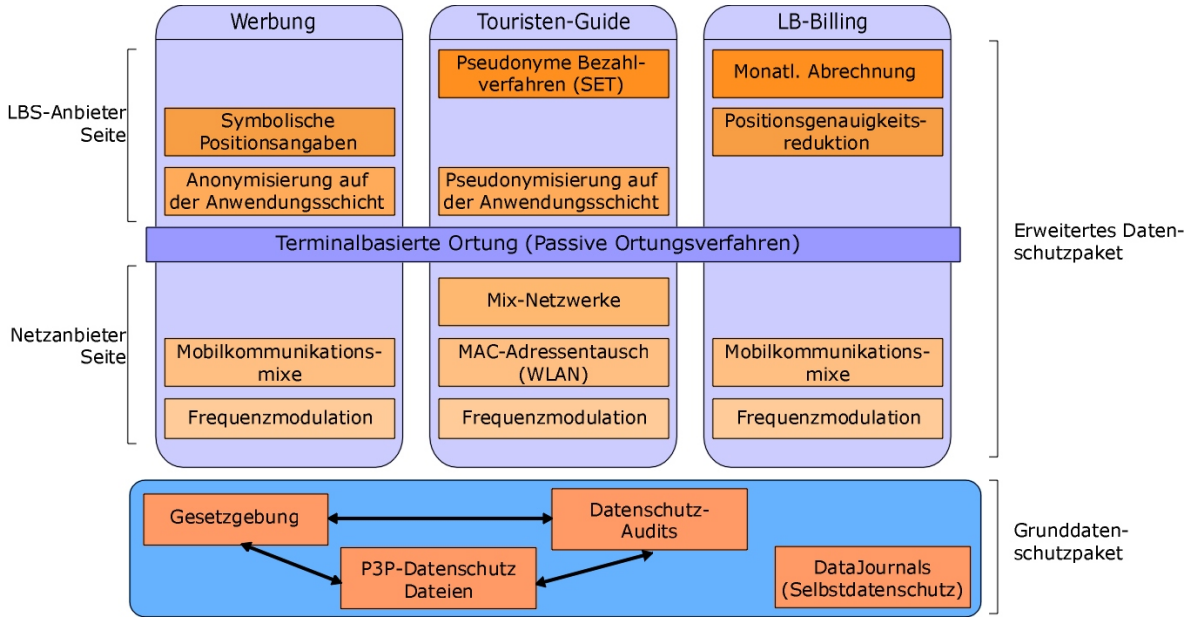

Abbildung 6.1: Anwendungsspezifische Zuteilung von datenschutzfördernden Methoden, Verfahren und organisatorischen Maßnahmen

bildung 6.1 wird für die nachfolgende Betrachtung eine anwendungsspezifische Zuordnung von datenschutzfördernden Komponenten gezeigt. Das Fundament für die datenschutzfreundliche Realisierung aller Anwendungen (ortsabhängige Werbung, Touristen-Guide und LB-Billing (Location Based Billing)) setzt sich aus Elementen der Bereiche Selbstdatenschutz, Selbstregulierung und Regulierung durch den Gesetzgeber zusammen. Die dargestellten Pfeile in der Abbildung verdeutlichen, dass diese Komponenten gegenseitig Einfluss aufeinander ausüben. Ausgehend vom Gesetzgeber kann hier Einfluss sowohl auf Auditierungs- und Zertifizierungsregeln als auch auf die Publizitätspflicht der Dienstanbieter genommen werden, mit der Konsequenz, dass sich Elemente aus dem Bereich der Selbstregulierung in den der gesetzlichen Regelungen verschieben. Vertikal zu diesem Fundament sind die einzelnen Anwendungen (hier nur drei abgebildet) mit ihren jeweils anwendungsspezifischen Komponenten zur Erhöhung des Datenschutzniveaus abgebildet. Nimmt man zunächst an, dass Netzanbieter und LBS-Dienstanbieter in einem Unternehmen vereint sind, wie dies heutzutage oft der Fall ist, so bauen die einzelnen Datenschutzkomponenten aufeinander auf und sollten zwingend in der angegebenen Reihenfolge realisiert werden. Diese Anordnung ergibt sich deshalb, weil eine datenschutzfördernde Absicherung auf hohen Schichten (beispielsweise in der Anwendungsschicht) nur dann Sinn macht, wenn alle darunter liegenden Schichten, wie die physische Netzschicht und die darauf aufbauenden Netzschichten, wenigstens das gleiche Sicherheitslevel bieten. Aus diesem Grund wurden gleich auf unterster Ebene Frequenzmodulationstechniken wie das Spread Spectrum angeführt, da diese bereits auf der niedrigsten physischen Schicht, der der Funkwellen, eine Peilung und somit Ortung des Endgerätes verhindern können. Gleich darüber angeordnet finden sich Verfahren die entweder auf der Link-Layer- oder IP-Schicht die Erzeugung von Bewegungsprofilen zu verhindern versuchen. Ist mithilfe

der Komponenten Frequenzmodulation, Mobilkommunikationsmixe, Mixe etc. sichergestellt, dass der Netzbetreiber Endgerätebesitzer nicht verfolgen und Bewegungsprofile erstellen kann, so ist auch der Einsatz von terminalbasierten Ortungsverfahren sinnvoll. Dazu sollten gleichzeitig Datenvermeidungstechniken auf der Anwendungsschicht zum Einsatz kommen. In dem hier angenommen Fall, dass Netzbetreiber und LBS-Anbieter in einem Unternehmen vereint sind, kann durch Datenvermeidungstechniken nur noch maximal ein Schutzgrad erreicht werden, wie ihn die schwächste darunterliegende Netzschicht bietet. Wie optimale Datenvermeidungstechniken selektierbar sind, wird später nochmals eingehender besprochen. Auf der letzten Ebene der Schichtung befinden sich die Bezahlverfahren. Die Entscheidung für den Einsatz eines bestimmten Bezahlverfahrens sollte sich an der Sicherheit der restlichen Komponenten ausrichten, sofern nicht ein besonderes Interesse daran besteht, gegenüber dem Finanzdienstleister zu verheimlichen, mit welchem Dienstanbieter ein Dienstleistungsverhältnis eingegangen wurde.

Hebt man die vorher getroffene Annahme der Zusammenarbeit zwischen Netzbetreiber und LBS-Anbieter wieder auf, so zerfällt die zuvor geschilderte strenge Schichtung in den vertikalen Säulen in zwei Komponenten. Grund dafür ist, dass der Dienstnutzer verschiedenen Parteien unterschiedlich viel Vertrauen schenken kann. Gesetzt den Fall, dass der Dienstnutzer dem Telekommunikationsanbieter vollständig vertraut, so sind zum Schutz des Dienstnutzers nur die Komponenten oberhalb der terminalbasierten Ortung von Bedeutung. Mithilfe dieser Techniken kann sich ein Nutzer auf der Anwendungsschicht gegen potentielle Angriffe eines LBS-Dienstanbieters schützen. Tritt der genau entgegensetzte Fall ein, dass dem Anbieter von LBS getraut wird, dem Netzbetreiber aber nicht, so könnte der Dienstnutzer entweder selbst Techniken wie Mixe und MAC-Adressenwechsel verwenden oder den Einsatz von Mobilkommunikationsmixen vom Netzbetreiber fordern. Besonders beim länderübergreifenden Roaming in fremde Netze, denen nicht unbedingt Vertrauen geschenkt werden sollte, gewinnt diese Annahme an Bedeutung. Die Zweiteilung der Schichten wird in Abbildung 6.1 auf der linken Seite durch die Einteilung in LBS-Anbieter-Seite und Netzanbieter-Seite hervorgehoben.

Neben der Feststellung, dass bei der Absicherung höherer Schichten die tieferen den noch maximal erreichbaren Schutzgrad festlegen, ist es möglich, noch zu einem weiteren Schluß zu kommen. In den vorangehenden Überlegungen wurde erwähnt, dass aufgrund der Unterschiedlichkeit von LBS-Anwendungen untereinander eine Aufteilung der Komponenten in anwendungsneutrale und anwendungsspezifische wünschenswert wäre. Das Ziel wurde durch die Spaltung der Komponenten in ein Grunddatenschutz- und ein erweitertes Datenschutzpaket erreicht (siehe Abbildung 6.1 rechte Seite). Im Grundschutzpaket sind solche Elementen enthalten, die theoretisch in allen LBS-Diensten implementiert oder durch den Staat geschaffen werden können. Besonders stark sind in dieser Hinsicht Datenschutz-Audits und die Gesetzgebung. Beide Elemente kommen vollständig ohne Einsatz von hardware- oder softwaretechnischen Komponenten aus. Wohingegen für DataJournals (aus dem Bereich des Selbstdatenschutzes) und P3P-Datenschutzvereinbarungen je nach Anwendung entweder nur softwaretechnische Erweiterungen notwendig sind oder, im Falle breitflächig ausgestrahlter P3P-Vereinbarungen (siehe pawS), zusätzliche Hardware zum Empfang vorhanden sein muss. Trotzdem ist es möglich, alle Komponenten des Grunddatenschutzpaketes über alle LBS-Anwendungen hinweg zu realisieren. Dagegen sind Elemente des erweiterten Datenschutzpaketes anwendungs- und zum Teil netzspezifisch auszuwählen.

Letztendlich stellt sich nun die Frage wieviel Anonymität das Gros der LBS-Nutzer wünscht und was als zusätzliche Leistungen für höhere Anforderungen angeboten werden sollte. Eine 2003 aufgesetzte Studie von HarrisInteractive [91], durchgeführt von Taylor, untersuchte

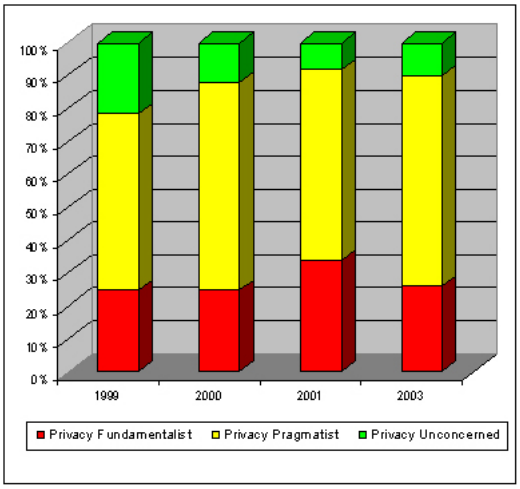

Abbildung 6.2: HarrisInteractive Befragung

Datenschutzbedenken[1] im Zusammenhang mit der Internetnutzung. Abbildung 6.2 stellt die aufbereiteten Hauptergebnisse der Umfrage dar. Wie der Abbildung zu entnehmen ist, teilte der Autor die Befragten Personen in drei Kategorien ein.

1. **unconcerned:** Personen in dieser Gruppe haben bezüglich der heute üblichen Datenerhebung und eventuellen Zusammenführung der Daten keinerlei Bedenken und halten ihre Privatsphäre für ausreichend durch den Gesetzgeber geschützt.

2. **pragmatists:** Die Pragmatiker sind im Vergleich zu den „unconcerned“ bezüglich des Datenschutzes viel mehr sensibilisiert und sehen, dass die zunehmende Datenerhebung eine Gefahr für ihre Privatsphäre darstellen kann. Aus diesem Grund bestimmen sie fallabhängig, welche Daten sie an wen herausgeben. Die Hauptanforderungskriterien für diese Gruppe sind: was für eine Leistung ich erhalte, wer erhält meine Daten und an wen werden sie unter Umständen weitergereicht.

3. **fundamentalists:** Die letzte der drei Gruppen bilden diejenigen, die ihre Privatsphäre für bereits gefährdet halten. Aus Sicht dieser Personen ist der staatliche Schutz zu gering und Vertrauen in die Anbieter nicht vorhanden, weshalb die Datenherausgabe komplett vermieden wird.

Unterstellt man zumindest eine teilweise Übertragbarkeit[2] der dargestellten Ergebnisse auf LBS-Anwendungen so lässt sich die Befragung wie folgt interpretieren. Die größte Gruppe ist nach dieser Studie die der Pragmatiker, welche anwendungs- und leistungsbezogen, sowie je nach „Aufklärungsmodalitäten“ im Hinblick auf den Datenschutz über die Preisgabe von personenbezogenen Daten entscheiden. Allein die Gruppe der *fundamentalists* mit einem Anteil von ca. 23 Prozent lehnt eine Herausgabe von zu schützenden Daten unter allen Umständen ab. Damit existiert eine Mehrheit von 77 Prozent, die vor allem Informationen über die Datenerfassung und Weiterverwendung fordert, um eine fundierte Entscheidung darüber zu treffen,

[1] Untersuchung wurde mit $N = 1010$ Personen durchgeführt

[2] Barkhuus und Dey [5] kamen mit einer viel kleineren Stichprobe ($N = 16$) auf gleiche Ergebnisse im Rahmen von LBS. Allerdings konnte festgestellt werden, das Positioning-Systeme allgemein besser akzeptiert werden als Tracking-Dienste.

ob die Bekanntgabe von persönlichen Daten lohnenswert ist. In Abbildung 6.1 entspricht diese Forderung genau dem auf der rechten Seite gekennzeichneten Grunddatenschutzpaket, in das nur Elemente Eingang gefunden haben, die die Informationslage auf der Teilnehmerseite verbessern. Die Bedürfnisse der restlichen 23 Prozent könnten durch individuelles Hinzufügen datenschutzfreundlicher Komponenten und Verfahren, wie sie im erweiterten Datenschutzpaket dargestellt sind, abgedeckt werden. Abhängig von der organisatorischen Verteilung von LBS, ASP, Netzprovider und vom Vertrauen, das ein LBS-Nutzer zu jeder dieser Instanzen hat, können dann, erweiterte Datenschutzpakete, die Anforderungen dieser Gruppe erfüllen (individuell selektierbar oder als Paket), angeboten werden.

Ausgehend vom Versuch, PET-Elemente in anwendungsneutrale und anwendungsspezifische einzuteilen ergab sich Abbildung 6.1, in der durch die Zweiteilung der Komponenten in Grunddatenschutz- und erweitertes Datenschutzpaket diese Trennung geschafft wurde. Darüber hinaus konnte auf Basis der HarrisInteractive Befragung festgestellt werden, dass das Grunddatenschutzpaket bei mehr als zweidritteln der Bevölkerung die Datenschutzbedürfnisse komplett abdeckt. An dieser Stelle ist jedoch nochmals darauf hinzuweisen, dass sich diese Studie auf die Internetnutzung und nicht auf die Nutzung von LBS bezog. So könnten Personen im Umfeld der LBS sehr viel sensibler reagieren, da zusätzlich zu den im Internet versandten personenbezogenen Daten, Positionsinformationen hinzutreten. Trifft dies zu, so müssten die Inhalte des Grunddatenschutzpaketes neu definiert werden, wobei mit hoher Wahrscheinlichkeit auch anwendungsspezifische Komponenten Eingang finden würden. Auswirkungen hätte dies insbesondere auf die weite Verteilung von LBS-Anwendungen, da anwendungsneutrale Sicherungsmaßnahmen oftmals viel leichter zu realisieren sind als anwendungsspezifische.

Wie in der Einleitung zu diesem Kapitel bereits angesprochen wurde, ist erst ab einem bestimmten Schutzniveau auf tieferen Netzschichten der Einsatz von datenschutzfördernden Elementen auf der Anwendungsschicht sinnvoll. Hierzu wurden bereits in Kapitel 4.1 insgesamt acht verschiedene Methoden zur Verschleierung der Identität oder des Aufenthaltsortes eingehender analysiert und erläutert. Wie und wo diese jedoch in ein „LBS-Geflecht“ eingebunden werden sollten wurde nur anwendungsfallunabhängig kurz angesprochen. Das in Abbildung 6.3 dargestellt dreidimensionale Diagramm soll diese Lücke füllen und fallbezogen den Einsatz von datenschutzfördernden Elementen auf Anwendungsebene untersuchen. Dargestellt wurden drei von insgesamt vier Dimensionen, die im Auswahlprozess für entsprechende Elemente eine bedeutender Rolle spielen. Die exemplarisch abgetragenen LBS innerhalb des Diagramms wurden subjektiv bezüglich ihrer Ausprägungen bewertet und eingeordnet.

Bevor die Abbildung umfassender betrachtet wird, sollen zuerst die vier Dimensionen vorgestellt werden (die Reihenfolge der Auflistung ist dabei nicht von Bedeutung):

- **Präzision der Ortung:** Das wichtigste Kriterium zur Auswahl von PET-Elementen auf der Anwendungsschicht ist die für die Diensterbringung erforderliche Positionsgenauigkeit. Fallabhängig sind Genauigkeit von einigen Zentimetern bis hin zu Kilometern möglich. Überdies ist, neben der Präzision bezogen auf absolute Koordinaten auch wichtig, ob eventuell symbolische Positionsangaben für den Dienst von ausreichender Qualität sind. Somit entscheidet dieses Kriterium, ob überhaupt Positionsverschleierungsmechanismen, wie in Kapitel 4.1.3 dargestellt, einsetzbar sind.

- **Abrufhäufigkeit:** Die Abrufhäufigkeit legt typischerweise das Risiko für die erfolgreiche Durchführng eines Home-Angriffs, bei Pseudonymisierung und fehlender Positionsverschleierung, fest. Bei einer Abrufhäufigkeit von einer Anfrage pro Jahr wäre ein

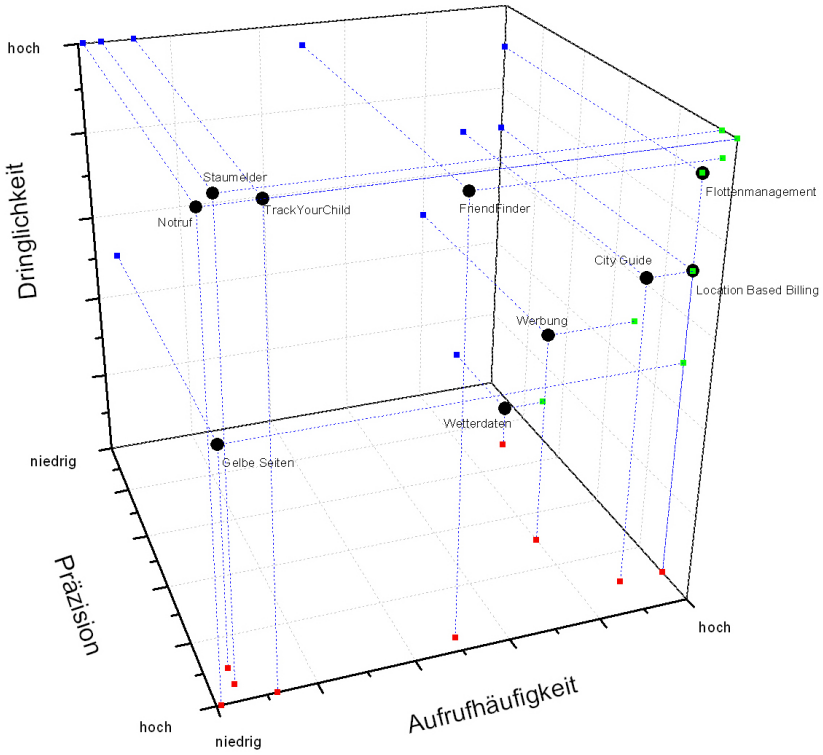

Abbildung 6.3: Dimensionenschema

solches Angriffsszenario praktisch ausgeschlossen. Dahingegen ist das Risiko bei Abfragen im Minutenbereich sehr hoch. Als Steuerungsgrößen für dieses Kriterium bieten sich sowohl Pseudonymisierungs- und Positionsverschleierungstechniken an.

- **Dringlichkeit:** Unter Dringlichkeit ist zu verstehen, wie schnell ein Anfragedatensatz an den LBS-Dienst transferiert werden muss. Realtime-Anwendungen beispielsweise erfordern eine unverzögerte Übermittlung, wohingegen beim Versenden von Wetterdaten von Kraftfahrzeugen aus Verzögerungen bis zu fünf Minuten verkraftbar wären. Die Dringlichkeit ist damit ein Indikator für die Einsetzbarkeit von Mechanismen, die die Zeitinformation in Anfragen verzerren.

- **Zurechenbarkeit:** Das letzte, aber nicht weniger wichtige Kriterium ist die Zurechenbarkeit. Gemeint ist damit, ob ein Dienst anonymisiert, pseudonymisiert oder personalisiert durchgeführt abläuft. Eine Hotelanfrage kann demnach anonym gestaltet sein, allerdings lässt sich ein elektronischer Stadtführer gegenüber dem Dienstanbieter nur pseudonymisiert realisieren. Location Based Billing Anwendungen, wie beispielsweise die streckenabhängige Berechnung des Kraftfahrzeugversicherungstarifes, sind gegenüber dem Dienstanbieter wahrscheinlich personalisiert zu realisieren. Von diesem Kriterium hängt es damit ab, wie datenschutzfreundlich das einzusetzende Bezahlverfahren zu gestalten ist.

Tabelle 6.1 zeigt exemplarisch die Anwendung des Schematas zur Auswahlunterstützung von datenschutzfreundlichen Elementen auf der Anwendungsschicht.

Abbildung 6.3 kann durch die Einführung der drei Dimensionen dazu beitragen so genannte „Anwendungscluster“ ausfindig zu machen, die ähnliche oder gleiche Eigenschaften bezüglich

Anwendung	**Präzision**	**Abrufhäufigkeit**	**Dringlichkeit**	**Zurechenbarkeit**	**Vorschlag**
Werbung	symbolisch	hoch	hoch	keine	Verwendung von symbolischen Angaben mit logischen Aufenthaltsgebieten
Touristen - Guide	10 - 20 m	alle 10 sec	hoch	pseudonym	Einsatz von Pseudonymisierungstechniken
Hotelsuche	50 - 100 m	selten	hoch	anonym	räumliche Verschleierung + Anonymisierung
Fahrbahnwetterdaten	500 m	hoch	30 sec	anonym	zeitliche Verzerrung in Kombination mit räumlicher Verschleierung

Tabelle 6.1: Beispielanwendung des Schematas zur Einordnung von LBS-Dienstanfragen

der drei Dimensionen auf sich vereinen. Für diese Cluster könnten dann standardisierte Absicherungsmodule auf den höheren Schichten entworfen und entwickelt werden, mithilfe derer eine kostengünstigere und schnellere Absicherung von LBS möglich wäre.

6.2 Identitätsmanagement als Ansatz zur anwendungsübergreifenden Datenschutzkontrolle

Die bisherige Vorgehensweise zum Aufbau datenschutzfreundlicher LBS war ausschließlich anwendungsorientiert[3] und vernachlässigte dabei zwei wichtige Aspekte. Zum einen wurde davon ausgegangen, dass Sicherheits- und Datenschutzanforderungen für einen bestimmten Anwendungstypus mit der Zeit, dem Aufenthaltsort und dem Gruppenverhalten von Nutzern beständig sind. Diese Generalisierung ist jedoch nicht für alle LBS zutreffend und muss dementsprechend mit dafür geeigneten Maßnahmen aufgehoben werden. Der zweite nicht berücksichtigte Aspekt war, dass LBS-Nutzer nicht immer nur eine Anwendung nutzen. Die bisher vorgestellte Konstruktion implizierte aber die Installation spezieller Datenschutzsoft- oder -hardware für jeden LBS. Einen Lösungsansatz für dieses Problem kann ein effektiv eingesetztes Identitätsmanagement darstellen.

In Anlehung an [48, S. 2] ist Identitätsmanagement ein Konzept, dass dem LBS-Nutzer die Möglichkeit gibt seine Sicherheits- und Datenschutzbedürfnisse mittels IT-Unterstützung abhängig von der jeweiligen Situation auszudrücken und durchzusetzen. Ziel dieses Konzepts ist die Nachbildung von Nutzerverhalten mithilfe von IT-basierten Identitätsmanagementsystemen. Um den Umfang der erforderlichen Nachahmung zu verstehen haben Schmidt und Kollegen den Kontext nach „menschlichen Faktoren“ und „physischen Faktoren“ aufgeteilt dargestellt [84, S. 896]. Menschliche Faktoren sind zum einen der Nutzer selbst, dessen soziales Umfeld und seine Aufgaben. Physische Faktoren hingegen sind die Position, die Infrastruktur (Netzinfrastruktur), Umgebungsvariablen wie beispielsweise Geschwindigkeit, Höhe, Temperatur etc. Durch diese Aufspaltung wird schnell deutlich, dass ein Identitätsmanagement auf Basis von IT-Systemen nur einen sehr begrenzten Bereich des Kontextes abdecken kann, was wiederum auf das Design der Systeme Einfluss hat. In [48, S. 6] wurde deshalb eine Einschränkung auf die wichtigsten Faktoren vorgenommen:

[3] Die Anwendungsorientierung ist durch die Säulen in Abbildung 6.1 dargestellt.

- **Aufgabe:** Die Aufgabe eines Nutzers spiegelt sich in der Auswahl der LBS wieder. Sie ist der beste Indikator für die augenblicklichen Aufgaben des Nutzers.
- **Infrastruktur:** Im Bereich der LBS ist mit Infrastruktur vornehmlich das zugrunde liegende Kommunikationsnetz gemeint.
- **soziales Umfeld:** Das Identitätsmanagementsystem muss unbedingt, soweit möglich, auf das soziale Umfeld und die damit verbundene eingeschränkte Datenherausgabe achten.
- **Position:** Zu den physischen Faktoren gehört im Rahmen des LBS natürlich auch die Position.

Alle Zustände möglicher Elemente ergeben den möglichen Raum für Konfigurationen in dem eine Situation dementsprechend eine spezifische Konfiguration darstellt. Situationen können durch Zusammenarbeit von Endgerät und LBS-Nutzer auf drei Arten bestimmt werden [48]. Erstens durch die vollständig nutzerkontrollierte Eingabe der zutreffenden Situation in das Endgerät. Zweitens mithilfe eines semi-automatischen Vorganges, bei dem das Endgerät zunächst selbstständig eine Menge an möglicherweise zutreffenden Situationen auswählt und dem Nutzer präsentiert. Dieser kann anschließend die passende Möglichkeit manuell auswählen. Und drittens steht die vollautomatische Methode zur Verfügung, bei der das Endgerät eigenständig aus allen ihm zur Verfügung stehenden Kontextinformationen eine Situation selektiert. Aus Gründen der Praktikabilität empfehlen sich für ein Identitätsmanagent die letzten zwei Varianten besonders.

In Anlehnung an [48, S. 9] lässt sich die Abbildung 6.4 herleiten, welche beide am Anfang des Kapitels angesprochenen Probleme löst. Ein so implementiertes Identitätsmanagementsystem kann situationsbezogen auf Datenschutz- und Sicherheitsanforderungen reagieren und dient für alle möglichen LBS als Filter. Die Funktionsweise lässt sich wie folgt näher beschrei-

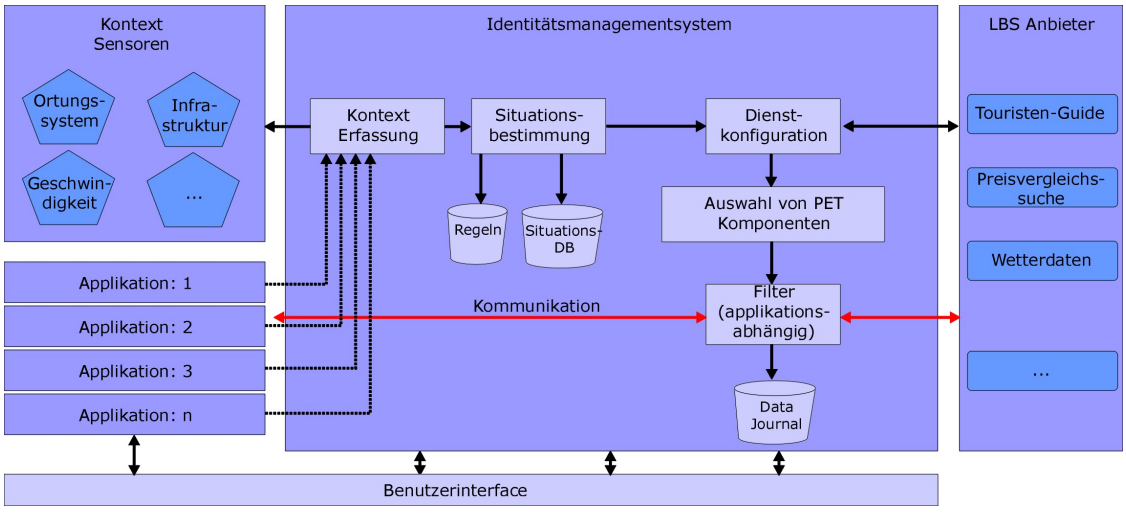

Abbildung 6.4: Architektur Identitätsmanagement in Anlehnung an [48]

ben. Fordert der Dienstnutzer eine bestimmte Dienstart an, so erfasst das Endgerät zunächst mithilfe seiner Kontext-Sensoren das Umfeld. Der Prozess „Situationsbestimmung“ ermittelt daraufhin entweder ein Set an zutreffenden Situationen und überlässt die Auswahl dem Benutzer oder selektiert automatisch die passendste Situation. Ist die Situation mit den daraus für

den LBS-Nutzer resultierenden Sicherheits- und Datenschutzeinstellungen bekannt, so wird mit der Dienstkonfiguration fortgefahren. Aufgabe der Dienstkonfiguration ist die Kontaktaufnahme zum gewünschten LBS und die Anfrage bezüglich der Datenschutzrichtlinien (P3P) und Datenerfordernisse um den Dienst ordnungsgemäß erbringen zu können. Sowohl die situationsbezogene LBS-Konfiguration durch den Benutzer als auch die Datenanforderungen und Datenschutzrichtlinien des LBS-Anbieters bestimmen im zweiten Schritt die Auswahl adäquater PET. Ein Schwerpunkt liegt dabei auf der Auswahl von Identitäts- und Positionsverschleierungsmechanismen abhängig vom LBS und den LBS-Nutzeranforderungen. Zusätzlich könnte das Identitätsmanagement in Abhängigkeit von der darunter liegenden Infrastruktur Mix-Netze oder MAC-Adresswechsel in den Kommunikationsvorgang einbeziehen und / oder Ende-zu-Ende-Verschlüsselung aktivieren. Entstehen Konflikte zwischen den Nutzer- und Dienstanforderungen bezüglich Sicherheit und Datenschutz, sollte das Identitätsmanagement entweder in der Lage sein zu verhandeln oder die Information dem Nutzer transparent darstellen, so dass dieser eine fundierte Entscheidung treffen kann [40, S. 296]. Wurden adäquate Schutzmechanismen ausgewählt, kann der rot dargestellte Kommunikationsprozess beginnen. Dieser wird während der gesamten Nutzungsdauer über den dargestellten Filter überwacht. Neben der Überwachung hat der Filter die Aufgabe, die ausgewählten PET einzusetzen und durchzusetzen. Daraus resultiert, dass die Kommunikation zwischen Clientanwendungen und LBS standardisiert ablaufen muss. Als ein Standard zur Übertragung von Positionsinformationen könnte das in [23] beschriebene „Mobile Location Protocol“ (MLP) eingesetzt werden. Diese Forderung gilt auch für die Kommunikation zwischen Identitätsmanagement und LBS. Für die automatische Übertragung von Datenschutzrichtlinien existiert das bereits angesprochene P3P, welches unter Umständen von Datenschutz-Audit Anbietern zertifiziert werden könnte. Allerdings erfüllt P3P noch nicht alle Anforderungen in diesem Kommunikationsschritt, weshalb nach Erweiterungen gesucht werden muss.

Fazit: Identitätsmanagementsysteme können in Zukunft dazu beitragen die Komplexität, welche unter anderem durch die vielen Gestaltungsmöglichkeiten von LBS auftritt, zu reduzieren. Damit einher geht, dass dem LBS-Nutzer ein Werkzeug an die Hand gegeben werden kann, welches die Transparenz des Gesamtablaufes steigert und gleichzeitig die Konfiguration von Sicherheits- und Datenschutzmechanismen automatisiert im Hintergrund ausführt. Darüber hinaus kann es in beiden Datenschutzpaketen Anwendung finden. Im Grunddatenschutzpaket in Form einer „Lite-Version“, die hauptsächlich auf die Übereinstimmung von Datenschutzvereinbarungen mit den Nutzerpräferenzen achtet. Wohingegen eine Vollversion das gesamte Management von PET auf Endgeräteseite übernehmen kann. Insbesondere sollte das System die im vorherigen Unterkapitel dargestellten anwendungsabhängigen Gestaltungsrichtlinien beachten.

Kapitel 7

Zusammenfassung

In Abgrenzung zur fast gleichnamigen Diplomarbeit von Egla [23] beschäftigte sich diese Arbeit nicht mit der Untersuchung von bestehenden Standards und Protokollen zur Erhöhung der Datenschutzfreundlichkeit, sondern mit Komponenten, Verfahren und organisatorischen Maßnahmen, die auf unterschiedlichen Schichten innerhalb der LBS zum tragen kommen. Grund der Untersuchung ist der bisher als unzureichend zu bezeichnende Einsatz von datenschutzfreundlichen Gestaltungsmöglichkeiten im Umfeld von LBS. Wie bereits Kapitel 3.2.2 zeigte, konzentrieren sich Anbieter von LBS im wesentlichen nur auf die Umsetzung rechtlicher Vorgaben. Schutzmöglichkeiten für LBS-Nutzer die über diese Regelungen hinausgehen, kamen dabei nur selten vor.

Überdies wurde in dieser Arbeit eine kleine Auswahl an elektronischen Bezahlverfahren auf ihre Tauglichkeit für den Einsatz in datenschutzfreundlichen LBS überprüft und daraus ein Anforderungskatalog abgeleitet.

7.1 Ergebnis

Ein Ergebnis dieser Arbeit war, dass ähnlich zu einem OSI-Schichtenmodell verschiedene Ebenen innerhalb von LBS vorhanden sind, die mit unterschiedlichsten Schutzmechanismen ausgestattet werden können (siehe Abbildung 7.1). Die unterste abgebildete Schicht entspricht

Abbildung 7.1: Schichten-Pyramide

der physischen Netzschicht, auf der Bandspreizverfahren zur Verhinderung von Peilung und Ortung angewendet werden sollten. Die darüber liegende Schicht enthält Verfahren, die auf

höheren Netzschichten arbeiten. In GSM-Netzen wären beispielsweise Mobilkommunikationsmixe und in WLAN's MAC-Adressenwechsel hier einzuordnen. Ist durch die eben genannten Schutzmechanismen die Gefahr der Bewegungsprofilerstellung durch den Netzanbieter vermindert oder ausgeschaltet, ist es sinnvoll terminalbasierte Ortungsverfahren einzusetzen. Alle drei Ebenen fallen typischerweise in den Zuständigkeitsbereich des Netzbetreibers, was auf der rechten Seite der Abbildung bereits angedeutet ist. Die Verfahren auf den Schichten Identitäts- und Positionsverschleierung, sowie Bezahlverfahren sind in aller Regel durch den LBS-Dienstanbieter und den LBS-Typus determiniert. Darüber hinaus existieren weitere Gestaltungsmöglichkeiten, die sich nicht direkt in das Schema einordnen lassen. Dazu gehört zum einen die nationale Gesetzgebung, die gewissermaßen ein Fundament für jede Ebene der Schichten-Pyramide bildet. Damit erhält der Gesetzgeber die Möglichkeit, innerhalb jeder Schicht zumindest Grundvoraussetzungen durch gesetzliche Vorgaben zu schaffen, die dann zwingend durch die Unternehmen umgesetzt werden müssen. Parallel zur Gesetzgebung existieren Mechanismen zur Verbesserung der Datenverteilung innerhalb des Netzwerks der Beteiligten am LBS-Prozess. Mithilfe der Datenverteilung können zwar keine Daten vermieden werden, was auch oftmals aufgrund der LBS-Ansprüche kaum möglich ist, aber auf mehrere Instanzen so verteilt werden, dass jede nur ein sehr begrenztes Teilwissen besitzt. Erst wenn einige oder alle Instanzen zusammenarbeiten, wären Bewegungs- oder Nutzungsprofile von Teilnehmern erstellbar. Die Abbildungen 4.13, Seite 56 und 6.1, Seite 69 stellen die soeben angesprochenen Module und Verfahren nochmals aus zwei verschiedenen Blickwinkeln dar.

Parallel zur Identifizierung einzelner Schichten wurden außerdem (abgeleitet aus Nutzerbedürfnissen und Effizienzgesichtspunkten bei der Verbreitung von LBS) zwei Pakete bestehend aus verschiedenen Verfahren, Methoden und organisatorischen Maßnahmen herausgearbeitet: Das Grunddatenschutzpaket und das erweiterte Datenschutzpaket (siehe Abbildung 6.1, Seite 69). Komponenten innerhalb des Grunddatenschutzpakets haben zum Ziel, dem LBS-Nutzer einen Überblick darüber zu verschaffen, was alles mit seinen Daten geschieht. Zu diesem Paket zählen insbesondere gesetzliche Regelungen, Datenschutzvereinbarungen und Techniken zur Verbreitung dieser. Eine Einschränkung oder Minimierung der preisgegebenen Datenmengen wird erst durch PET-Komponenten des erweiterten Datenschutzpakets ermöglicht. Hier sollten die pyramidenartig dargestellten PET in Abbildung 7.1 eingesetzt werden. Der Grund für die Zuordnung der meisten PET in das erweiterte Datenschutzpaket ist darin zu suchen, dass diese Technologien in der Regel anwendungsspezifisch ausgewählt und angepasst werden müssen. Wie eine solche Auswahl auf der Anwendungsebene stattfinden kann, bezüglich der in Kapitel 4.1 vorgestellten Datenvermeidungstechniken, wurde im vorhergehenden Kapitel 6 anhand von vier Dimensionen erläutert und in Abbildung 6.3 dreidimensional visualisiert.

Aufbauend auf der Fragestellung, welche Komponenten in einem erweiterten Datenschutzpaket ausgewählt werden sollten, beschäftigte sich der Abschnitt „Identitätsmanagement als Ansatz zur anwendungsübergreifenden Datenschutzkontrolle“ damit, die anwendungsabhängigen erweiterten Datenschutzpakete miteinander zu verbinden. In Abbildung 6.4 auf Seite 75 wurde in Form eines Architekturüberblicks eine Lösungsmöglichkeit vorgestellt.

Neben der Untersuchung von PET und organisatorischen Maßnahmen zur Steigerung der Datenschutzfreundlichkeit von LBS wurden in Kapitel 5 ausgewählte Bezahlverfahren auf ihre Tauglichkeit für den Einsatz in LBS-Anwendungen überprüft und auf Seite 66 zusammengefasst dargestellt. Ferner wurde auf Basis mehrerer wissenschaftlicher Untersuchungen ein Anforderungskatalog aufgestellt (siehe Tabelle 5.1, Seite 60), der idealtypische Anforderungen an ein LBS-Bezahlsystem enthält. Mithilfe dieses Instrumentariums kann eine erste Auswahl

und Evaluation bestehender Bezahlsysteme vorgenommen werden, um im Anschluß daran ein den Anwendungsbedürfnissen entsprechendes elektronisches Zahlverfahren auszuwählen.

7.2 Ausblick

Basierend auf der Arbeit von Egla und dieser können weitere Fragen aufgeworfen werden. So wurde beispielsweise in beiden Arbeiten nicht geklärt, welche Anreize es für die in Tabelle 2.3 dargestellten LBS-Beteiligten gibt, datenschutzfreundliche Technologien zu entwickeln und umzusetzen. Hier könnte unter Umständen die Vermutung aufgestellt werden, dass viele in der Wissenschaft erarbeitete Ansätze zur datenschutzfreundlichen Gestaltung von LBS scheitern, weil die dafür zuständige Instanz überhaupt kein Interesse aus betriebswirtschaftlicher Sicht daran hat[1]. Falls sich der zuvor geäußerte Verdacht bestätigt, wäre darüberhinaus interessant zu untersuchen, welche Maßnahmen eingeleitet werden müssten, um eine durch den Markt gestützte Umsetzung in Gang zu bringen.

Eine weitere nicht bearbeitete Fragestellung wäre, wie zukünftige Identitätsmanagementprogramme auf den Endgeräten mit ständig wechselnden Umgebungen umgehen können. Hier wäre es von besonderem Interesse, wie die Software nutzer-, umgebungs-, netz- und anwendungsabhängig entsprechende Sicherheitseinstellungen selektiert und für den LBS-Nutzer transparent anwendet. Besonders Augenmerk sollte darauf gerichtet werden, wie sich beispielsweise Sicherheitseinstellungen beim Wechsel in ein Fremdnetz (Roaming) ändern sollten. Erste Anhaltspunkte zu dieser Fragestellungen sind in [64] und [48] zu finden. Darüber hinaus existieren zwar Ansätze für das Internet, allerdings fehlt eine Übertragung auf die komplexeren LBS mit ihren besonderen Charakteristika bezüglich der Mobilität.

[1] in diesem Fall wurde unterstellt, dass der Staat nicht entsprechende Gesetze erlässt

Anhang A

Privacy Enhancing Service Architectures

Die im folgenden dargestellten Abbildungen sind Ergänzungen zu den im Kapitel 4.2.1 vorgestellten PESA und stellen einfach weitere Spielarten und Kombinationsmöglichkeiten von Dienstarten dar.

In Abbildung A.1 werden die Aufgabenbereiche des Telekommunikationsanbieters soweit eingeschränkt, dass dieser nur den Netzzugang zur Verfügung stellt und für den Datentransfers verantwortlich ist. Im Gegenzug wird der Location Generator, der für die Ermittlung der Po-

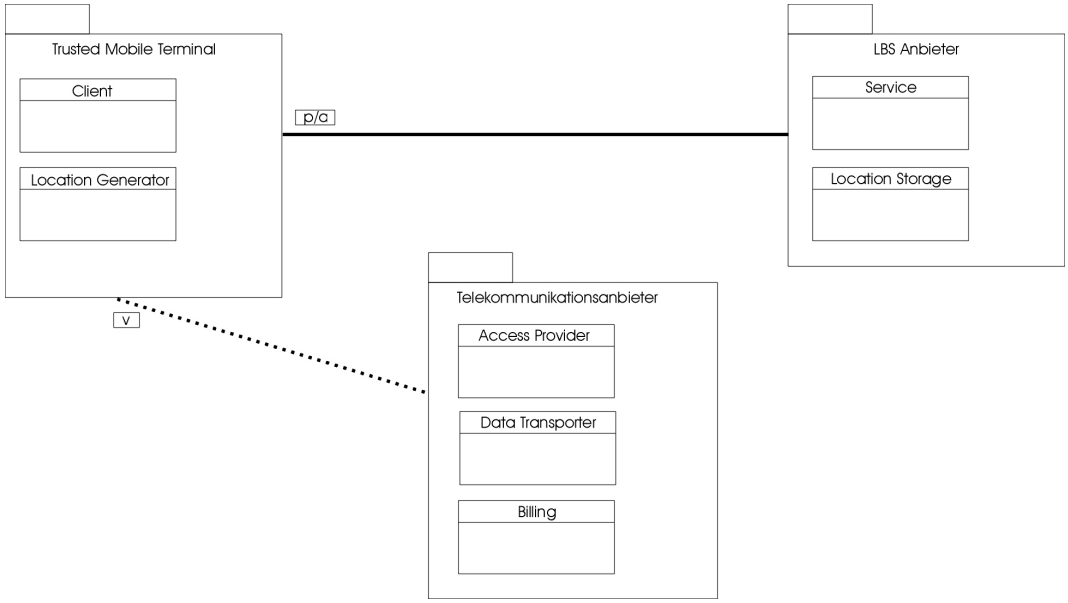

Abbildung A.1: PESA mit erweiterter Trusted mobile Terminal Funktionalität

sitionsinformationen verantwortlich ist, auf das Trusted mobile Terminal ausgelagert. Jetzt ist der Dienstnutzer in der Lage, über die Verteilung seiner - unter Umständen - personenbezogenen Daten selbst zu entscheiden. In dem dargestellten Beispiel gibt der Nutzer seine Daten pseudonymisiert oder anonymisiert - angezeigt durch das Kästchen p/a - an den LBS-Anbieter weiter.

Eine letzte hier im Anhang dargestellte Architekturvariante ist die Aufspaltung in drei diensterbringende Instanzen und dem Trusted mobile Terminal (siehe Abbildung A.2). Dieses Szenario besitzt sogar eine gewisse Aktualität, da zum Beispiel die Telekom mit weiteren Netzbetreibern WLAN-Access-Points in Bahnhöfen, Flughäfen etc. in ihr UMTS-Netz mit integrieren möchte. Die Betreiber der AP's bleiben dabei aber rechtlich weitgehend selbstständig. Der gleiche Sachverhalt ist in Abbildung A.2 abgebildet. Der Access Point Provider (APP)

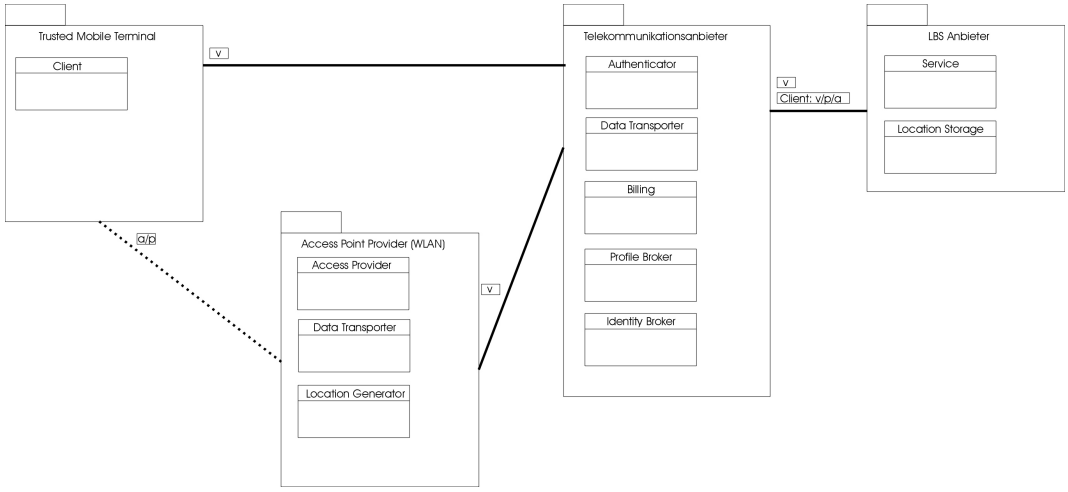

Abbildung A.2: PESA mit getrenntem ASP und Netzanbieter

stellt nur den Zugang zu einer Netzinfrastruktur zur Verfügung. Daneben - im Fall eines IEEE 802.11b WLAN's - könnte gleichzeitig eine serverbasierte oder semiautonome Positionsbestimmung durch den APP angeboten werden. Ein Vorteil dieser Architektur ist, dass in diesem Fallbeispiel der APP nur örtlich oder regional begrenzt seine Dienste anbieten kann und somit nicht die Möglichkeit hat flächendeckend Bewegungsprofile seiner Kundschaft zu erstellen. Der Telekommunikationsanbieter ist nur noch für die Weiterleitung der abgesetzten LBS-Dienstanfragen verantwortlich. Nimmt man eine Verschlüsselung der Anfragedaten an, so kann der Telekommunikationsanbieter keine Informationen aus den Anfragen ziehen. Dennoch übernimmt der Telekommunikationsanbieter die Rolle eines „Identity Brokers". Ähnlich zu einem Proxy-Server verfälscht der Broker die Identitätsdaten auf Kundenwunsch, so dass der LBS-Dienstanbieter keine Rückschlüsse auf die wirkliche Identität des Dienstnutzers ziehen kann.

Anhang B

Privacy Preferences Project (P3P)

XML-basierte P3P-Dateien lassen sich im Grundaufbau wie folgt darstellen (siehe [18, S. 51]):

```
1   <POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
2   <POLICY discuri="http://p3pbook.com/privacy.html" name="policy">
3     <ENTITY>
4     <DATA-GROUP>
5       <DATA ref="#business.contact-info.online.email">
6         privacy@p3pbook.com
7       </DATA>
8      <DATA ref="#business.name">Web Privacy With P3P</DATA>
9    </DATA-GROUP>
10    </ENTITY>
11    <ACCESS><nonident/></ACCESS>
12    <STATEMENT>
13      <CONSEQUENCE>We keep standard web server logs.</CONSEQUENCE>
14      <PURPOSE>
15        <admin/><current/><develop/>
16      </PURPOSE>
17      <RECIPIENT><ours/></RECIPIENT>
18      <RETENTION><indefinitely/></RETENTION>
19      <DATA-GROUP>
20        <DATA ref="#dynamic.clickstream"/>
21        <DATA ref="#dynamic.http"/>
22      </DATA-GROUP>
23    </STATEMENT>
24  </POLICY>
25  </POLICIES>
```

Literaturverzeichnis

[1] Alamäki, Tero; Björksten, Margareta; Dornbach, Peter; Gripenberg, Casper; Györbiro; Marton, Gabor; Nemeth, Zoltan; Skyttä, Timo; Tarkiainen, Mikko: *Privacy Enhancing Service Architectures.* In: Privacy Enhancing Technologies (2002) S. 99-109 Hrsg. Dingledine, R.; Syverson, P.

[2] Alderman, Ellen; Kennedy, Caroline: *The Right to Privacy.* Erschienen in: Alfred A. Knopf, New York 1995

[3] Ashbrook, Daniel; Starner, Thad: *Learning Significant Locations and Predicting User Movement with GPS.* Erschienen in: IEEE Sixth International Symposium on Wearable Computers, Seattle, Oktober (2002), S. 101-108

[4] Ashok, Roy L.; Agrawal, Dharma P.: *Next-Generation Wearable Networks.* In: IEEE Computer November (2003) S. 31-39

[5] Barkhuus, Louise; Dey, Anind: *Location-based Services for Mobile Telephony: a study of users privacy concerns.* URL: http://guir.berkeley.edu/pubs/interact2003/location-privacy.pdf Abruf am: 17.10.2003

[6] Beinrat, Euro: *Privacy and Location-based Services.* Erschienen in: GEO Informatics September 2001

[7] Beresford, Alastair R.; Stajano, Frank: *Location Privacy in Pervasive Computing.* In: IEEE Pervasive computing January (2003) S. 46-55

[8] Berthold, Oliver; Köhntopp, Marit: *Identity Management Based on P3P.* In: Federrath, Hannes (Hrsg.): Designing Privacy Enhancing Technologies, Springer Verlag (2001), S. 141-160

[9] Bizer, Johann: *Kommentar zum Bundesdatenschutzgesetz: §3a BDSG* 5. Auflage; Simitis, Spiros (Hrsg.); Erschienen in: Nomos Verlagsgesellschaft, Baden-Baden (2003) ISBN: 3-7890-7520-5; S. 296-315

[10] Boddupalli, P.; Al-Bin-Ali, F., Davies, N.; Friday, A.; Storz, O.; Wu, M.: *Payment Support in Ubiquitous Computing Environments.* In: WMSCA (2003)

[11] Bluetooth: *Specification of the Bluetooth System.* (2001) URL: https://www.bluetooth.org/foundry/specification/document/Bluetooth_Core_1.1_vol_1 Abruf am: 18.11.2003

[12] Brückner, Lars: *Aktiver Datenschutz mit DataJournals.* In: DuD Nr. 27 (2003) S. 300

[13] Buddhikot, Milind M.; Chandranmengon, Girish; Han, Seungjae; Lee, Yui-Wah; Miller, Scott; Salgarelli, Luca: *Design and Implementation of a WLAN/CDMA2000 Interworking Architecture.* In: IEEE Communications (2003) Vol. 41, No. 11 S. 90-100

[14] Cavoukian, Ann; Gurski, Michael; Mulligan, Deirdre; Schwartz, Ari: *P3P und Datenschutz.* In: DuD Nr. 8 (2000), S. 475-478

[15] Christensen, Fred: *Location-based Services - an assessment of the carrier market and the IBM location services platform.* In: IBM Wireless e-business, November (2001)

[16] Clarke, Roger: *Introduction to Dataveillance and Information Privacy, and Definitions of Terms.* URL: http://www.anu.edu.au/people/Roger.Clarke/DV/ Abruf am: 29.01.2004

[17] Conrads, Dieter: *Telekommunikation* Erschienen im: Vieweg Verlag (2001)

[18] Cranor, Lorrie Faith: *P3P: Making Privacy Policies More Userful.* In: IEEE Privacy & Security Vol. 1, Nr. 6 (2003), S. 50-55

[19] Cuellar, Jorge; Morris, John B. Jr.; Mulligan, Deirdre; Peterson, Jon; Polk, James: *Geopriv Requirements.* Internet draft Oktober (2003) http://www.ietf.org/internet-drafts/draft-ietf-geopriv-reqs-04.txt

[20] Davies, Nigel; Cheverst, Keith; Mitchell, Keith; Efrat, Alon: *Using and Determing Location in a Context-Sensitive Tour Guide.* In: IEEE Computer, August (2001), S. 35-41

[21] Djuknic, Goran M.; Richton, Robert E.: *Geolocation and Assisted GPS.* In: IEEE Computer Februar (2001) S. 123-125

[22] D'Roza, T.; Bilchev, G.: *An Overview of Location-Based Services.* Erschienen in: BT Technology Journal, Volume 21, Issue 1, Januar 2003, S. 20-27

[23] Egla, Tareg: *Mehrseitig sichere und datenschutzfreundliche Gestaltung von Location-Based Services.* Diplomarbeit am Institut für Informatik der Freien Universität Berlin (2003)

[24] Electronic Privacy Information Center and Privacy International: *Privacy and Human Rights 2002: An International Survey of Privacy Laws and Developments.* URL: http://www.privacyinternational.org/survey/phr2002/phr2002-part1.pdf und http://www.privacyinternational.org/survey/phr2002/phr2002-part2.pdf, Abruf am: 21.02.2004

[25] Ernst, L. Morris; Schwartz, U. Alan: *Privacy: The Right To Be Let Alone.* Erschienen in: Macgibbon and Kee, London 1968

[26] ExperTeam: Location Based Services In: Funkschau Nr. 7 (2003) S. 2

[27] Federrath, Hannes; Pfitzmann, Andreas: *Bausteine zur Realisierung mehrseitiger Sicherheit.* In: Mehrseitige Sicherheit in der Kommunikationstechnik. Addision-Wesley (1997) (Hrsg.) Müller, Günter; Pfitzmann, Andreas S. 83-104

[28] Federrath, Hannes: *Sicherheit mobiler Kommunikation.* Erschienen in: DuD-Fachbeiträge, Vieweg Verlag (1999)

[29] Fox, Susannah: *Trust and privacy online: Why Americans want to rewrite the rules.* URL: http://www.pewinternet.org/reports/pdfs/PIP_Trust_Privacy_Report.pdf, Abruf am: 01.04.2004

[30] Fritsch, Lothar: *Location Based Services und Privacy.* Vortrag im Rahmen der NETSEC und M-SEC Fachgruppentagung am 5./6. Mai 2004, Saarbrücken

[31] Garmin: *GPS GUIDE - for beginners.* URL: http://www.garmin.com/manuals/GPSGuideforBeginners_Manual.pdf Abruf am: 01.04.2004

[32] Gneiting, Stefan: *Location Based Services.* In: Funkschau Nr. 9 (2000) S. 34-37

[33] Golembiewski, Claudia: *Das Recht auf Anonymität im Internet. Gesetzliche Grundlagen und praktische Umsetzung.* In: DuD Nr. 27 (2003) S. 129-133

[34] Görlach, Andreas; Heinemann, Andreas; Terpstra, W. Wesley: *Survey on Location Privacy in Pervasive Computing.* In: Proceedings of The First Workshop on Security and Privacy at the Conference on Pervasive Computing (SPPC), Wien, Österreich, April (2004) (noch nicht veröffentlicht) URL: http://www.ito.tu-darmstadt.de/publs/pdf/pdf/SurveyOnLocationPrivacy.pdf

[35] Gruteser, Marco; Grunwald, Dirk: *Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking.* URL: http://systems.cs.colorado.edu/Papers/Generated/2003anonymousLbs.pdf, Abruf am: 17.10.2003

[36] Gruteser, Marco; Schelle, Graham; Jain, Ashish; Han, Rick; Grundwald, Dirk: *Privacy-Aware Location Sensor Networks.* URL: http://systems.cs.colorado.edu/Papers/Generated/2003PrivacyAwareSensors.pdf Abruf am: 17.10.2003

[37] Gruteser, Marco; Grunwald, Dirk: *Enhancing Location Privacy in Wireless LAN Through Disposable Interface Identifiers: A Quantitative Analysis.* In: Wireless Mobile Applications And Services On Wlan Hotspots, Proceedings of the 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots, S. 46 - 55 (2003)

[38] Gruteser, Marco; Liu, Xuan: *Protecting Privacy in Continuous Location-Tracking Applications.* Erschienen in: IEEE Privacy & Security, März/April (2004), S. 28-34

[39] Hansen, Marit: *Privacy Enhancing Technologies.* Erschienen in: Handbuch Datenschutzrecht; Verlag C.H.Beck München (2003); Roßnagel, Alexander (Hrsg.); S. 291-324

[40] Hansen, Marit; Rost, Martin: *Nutzerkontrollierte Verkettung.* Erschienen in: DUD Nr. 5 (2003), S. 293-296

[41] Hauser, Christian; Kabatnik, Matthias: *Towards Privacy Support in a Global Location Service.* In: Proceedings of the IFIP Workshop on IP and ATM Traffic Management, Paris (2001)

[42] Hermerschmidt, S.; Müller, V.: *Zahlungsverfahren im Internet.* URL: http://www.lda.brandenburg.de/material/zahlungsverfahren.pdf Abruf am: 15.11.2003

[43] Hightower, Jeffrey; Borriello, Gaetano: *Location Systems for Ubiquitous Computing.* In: IEEE Computer August (2001) S. 57-66

[44] Hightower, Jeffrey; Borriello, Gaetano: *Location Sensing Techniques.* URL: http://www.cs.washington.edu/research/portolano/papers/UW-CSE-01-07-01.pdf Abruf am: 13.11.2003

[45] Höft, Marc: *Zahlungssysteme im Electronic Commerce, ePayment im Onlineshop.* Erschienen in: Sie schaffen es! Verlag, Hamburg (2002)

[46] Hohl, Fritz; Kubach, Uwe; Leonhardi, Alexander; Rothermel, Kurt; Schwehm, Markus: *Nexus - An Open Global Infrastructure for Spatial-Aware Applications.* In: Proceedings of Mobicom'99 (1999)

[47] Ishitani, Lucila; Almeida, Virgilio; Wagner, Meira Jr.: *Masks: Bringing Anonymity and Personalization Together.* In: IEEE Privacy & Security, Mai/Juni (2003), S. 18-23

[48] Jendricke, Uwe; Kreutzer, Michael; Zugenmaier, Alf: *Pervasive Privacy with Identity Management.* URL: http://citeseer.ist.psu.edu/544380.html Abruf am: 24.10.2003

[49] Kafka, Gerhard: *Neue Standards für das WLAN.* In: Funkschau Nr. 11 (2001) S. 43-45

[50] Van Kar, Els; Bouwman, Harry: *The development of location based mobile services.* Erschienen in: Edispuut Conference, Amsterdam, 17.10.2001, URL: https://doc.telin.nl/dscgi/ds.py/Get/File-18690/Edispuut_2001_vd_Kar_The_development_of_location_based_mobile_services.pdf Abruf am: 10.11.2003

[51] Knorr, Michael; Schläger, Uwe: *Datenschutz bei elektronischem Geld.* In: DuD Nr. 7 (1997), S. 396-402

[52] Kölmel, Bernhard; Hubschneider, Martin: *Nutzererwartungen an Location Based Services, Ergebnisse einer empirischen Analyse.* URL: http://www.e-lba.com/YellowMap%20AG_Nutzererwartungen%20an%20Location%20Based%20Services.pdf Abruf am: 23.10.2003

[53] Laitinen, Heikki; Ahonen, Suvi; Kyriazakos, Sofoklis; Lähteenmäki, Jaakko; Menolascino, Raffaele; Parkkila, Seppo: *Cellular Location Technology.* URL: http://www.vtt.fi/tte/tte35/pdfs/CELLO-WP2-VTT-D03-007-Int.pdf Abruf am: 01.11.2003

[54] Langheinrich, Marc: *A Privacy Awareness System for Ubiquitous Computing Environments.* In: G. Borriello, L.E. Holmquist (Hrsg.): 4th International Conference on Ubiquitous Computing (UbiComp2002), Springer-Verlag LNCS 2498, pp. 237-245, September 2002

[55] Leonhardt, Ulf; Magee, Jeff: *Towards a General Location Service for Mobile Environments.* In: Proceedings of the Thrid IEEE Workshop on Services in Distributed and Networked Environments, Macau (1996), S. 43-50

[56] Leonhardt, Ulf; Magee, Jeff: *Security Considerations for a Distributed Location Service.* In: Journal of Network and System Management, Volume 6(1) (1998), S. 51-70

[57] Lesk, Michael: *Micropayments: An Idea Whose Time Has Passed Twice?* Erschienen in: IEEE Security & Privacy Vol. 2, Nr.1 (2004), S. 61-63

[58] Levijoki, Sami: *Privacy vs Location Awareness.* URL: http://citeseer.ist.psu.edu/401424.html Abruf am: 11.11.2003

[59] Location Interoperability Forum: *Mobile Location Protocol.* Version 3.0.0 (2002) URL: http://www.openmobilealliance.org/lif_download/LIF-TS-101-v3.0.0.zip Abruf am: 22.11.2003

[60] Glassman, Steve; Manasse, Mark; Abadi, Martin; Gauthier, Paul; Sobalvarro, Patrick: *The Millicent Protocol for Inexpensive Electronic Commerce.* URL: http://www.w3.org/Conferences/WWW4/Papers/246/, Abruf am: 08.04.2004

[61] Myles, Ginger; Friday, Adrian; Davis, Nigel: *Preserving Privacy in Environments with Location-Based Applications.* In: IEEE Pervasive computing January (2003) S. 56-64

[62] Näf, Michael: *Ubiquitous Insecurity?* URL: http://www.unm.ethz.ch/Tagungsbeilagen/Naef_Folien_definitiv.pdf Abruf am: 06.02.2004

[63] Narayanan, Ajith K.: *Realms and States: A Framework for Location Aware Mobile Computing.* URL: http://citeseer.nj.nec.com/cache/papers/cs/23169 Abruf am: 08.12.2003

[64] Ng, Alexander; Zaslavsky, Arkady: *Location Awareness and Adaptable Multilayer Security in Enterprise Applications.* URL: http://www.mobiforum.org/proceedings/papers/08/8.4.pdf Abruf am: 17.10.2003

[65] Pekkinen, Pasi; Rainio, Antti: *Market analysis of mobile map services.* URL: http://gimodig.fgi.fi/pub_deliverables/Gimodig-d221-market-anal.pdf Abruf am: 17.10.2003

[66] Peterson, Holger: *Anonymes elektronisches Geld.* In: DuD Nr. 7 (1997), S. 403-407

[67] Pfitzmann, Andreas; Köhntopp, Marit: *Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology.* Erschienen in: Designing Privacy Enhancing Technologies, Springer-Verlag Berlin Heidelberg (2001); Federrath, Hannes (Hrsg.); S. 1-9

[68] Prasithsangaree, P.; Krishnamurthy, P.; Chrysanthis, P.K.: *On Indoor Position Location with Wireless LANs.* In: IEEE PIMRC (2002)

[69] Ranchordas, J.; Lenaghan, Andrew: *A Flexible Framework for Using Positioning Technolgies in Location-Based Services.* In: IEEE Eurocon (2003) URL: http://technology.kingston.ac.uk/ncg/research/publications/2003/Eurocon2003/EUROCON2003Pres_apl.ppt Abruf am: 23.10.2003

[70] Rannenberg, Kai; Pfitzmann, Andreas; Müller, Günter: *Sicherheit, insbesondere mehrseitige IT-Sicherheit* In: Mehrseitige Sicherheit in der Kommunikationstechnik. Addision-Wesley (1997) (Hrsg.) Müller, Günter; Pfitzmann, Andreas S. 21-29

[71] Rannenberg, Kai: *Ortungsverfahren für Location Based Services.* Vorlesung *Infrastrukturen für M-Commerce* URL: http://www.m-lehrstuhl.de/veranstaltung/MCII_WS03/mc2_5_2003_11_18.pdf Abruf am: 15.11.2003

[72] Rennhard, Marc; Rafaeli, Sandro; Mathy, Laurent: *From SET to PSET - The Pseudonymous Secure Electronic Transaction Protocol.* URL: http://citeseer.nj.nec.com/cache/papers/cs/27114/http:zSzzSzwww.tik.ee.ethz.chzSz~rennhardzSzpublicationszSzPSET.pdf/from-set-to-pset.pdf Abruf am: 21.11.2003

[73] Rezgui, Abdelmounaam; Bouguettaya, Athman; Eltoweissy, Y. Mohamed: *Privacy on the Web: Facts, Challenges, and Solutions.* In: IEEE Privacy & Security, November/Dezember (2004) S. 40-48

[74] Ricochet: *Netzwerkaufbau.* URL: http://www.ricochet.com/about.aspx Abruf am: 19.11.2003

[75] Roßnagel, Alexander; Pfitzmann, Andreas; Garstka, Hansjürgen: *Modernisierungsgutachten des Datenschutzrechts. Gutachten im Auftrag des Bundesministeriums des Innern.* Hrsg: Bundesministerium des Innern

[76] Roßnagel, Alexander: *Konzepte des Selbstdatenschutzes.* In: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht (2003), S. 325-436

[77] Roßnagel, Alexander: *Datenschutzaudit.* In: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht (2003), S. 437-484

[78] Roßnagel, Alexander; Banzhaf, Jürgen; Grimm, Rüdiger: *Datenschutz im Electronic Commerce.* In: Verlag Recht und Wirtschaft GmbH Heidelberg, (Hrsg.) Holznagel, Bernd; Koenig, Christian; Scherer, Joachim; Tschentscher, Thomas; Wegerich, Thomas (2003)

[79] Sallwasser, Dirk: *Ortsbestimmung im Mobilfunk.* In: Funkschau Nr. 22 (2001) S. 26-28

[80] Samarati, Pierangela; Sweeney, Latanya: *Protecting privacy when disclosing information: k-Anonymity and its enforcement through generalization and suppression.* URL: http://citeseer.nj.nec.com/samarati98protecting.html Abruf am: 29.02.2004

[81] Schaar, Peter: *Datenschutz im Internet: Die Grundlagen.* Erschienen in: Verlag C.H. Beck (2002) ISBN: 3-406-48658-4

[82] Schilit, Bill; Hong, Jason; Gruteser, Marco: *Wireless Location Privacy Protection.* In: IEEE Computer, Dezember (2003), S. 135-137

[83] Schiller, Jochen: *Mobilkommunikation* 2. Aufl. (2003) Erschienen in: Addison-Wesley

[84] Schmidt, Albrecht; Beigl, Michael; Gellersen, Hans-W.: *There is more to Context than Location.* Erschienen in: Computer & Graphics Journal, Volume 23, Issue 6, S. 893-902, URL: http://citeseer.ist.psu.edu/schmidt98there.html

[85] Schneider, Jochen: *Handbuch des EDV-Rechts.* 3. Auflage Erschienen in: Verlag Dr. Otto Schmidt Köln ISBN: 3-504-56024-3

[86] Sobirey, Michael: *Datenschutzorientiertes Intrustion Detection.* In: DuD-Fachbeiträge Vieweg (1999)

[87] Sokol, Bettina: *Kommentar zum Bundesdatenschutzgesetz: §4 BDSG* 5. Auflage; Simitis, Spiros (Hrsg.); Erschienen in: Nomos Verlagsgesellschaft, Baden-Baden (2003) ISBN: 3-7890-7520-5; S. 316-335

[88] Snekkenes, Einar: *Concepts for Personal Location Privacy Policies.* In: Proceedings of the 3rd ACM Conference on Electronic Commerce (2001), S. 48-57

[89] Spreitzer, M.; Theimer, M: *Providing location information in a ubiquitous computing environment.* Erschienen in: ACM SOSP (1993), S. 27 ff.

[90] Steinfield, Charles: *The Development of Location Based Services in Mobile Commerce.* URL: http://www.msu.edu/~steinfie/elifelbschap.pdf Abruf am: 17.10.2003

[91] Taylor, Humphrey: *Most People Are „Privacy Pragmatists“ Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits.* URL: http://www.gsbc.com/harris_poll/printerfriend/index.asp?PID=365 Abruf am: 12.12.2003

[92] Technische Universität Dresden: *Mobile Kommunikation und Mobile Computing.* URL: http://www.rn.inf.tu-dresden.de/scripts_lsrn/lehre/mobile/print/10.pdf Abruf am: 19.11.2003

[93] Thymian, Marco; Niemeyer, Vanessa: *ePayment Systems.* Erschienen von: Institut für Bankinformatik und Bankstrategie an der Universität Regensburg (2001), ibi-Studie S 1101

[94] Toll-Collect: *Benutzerinformationen, Lkw Maut - einfach und Praktisch.* URL: http://www.toll-collect.de/pdf/benutzerinformation/web_einfuhrungstex_dt.pdf; jsessionid=DF4C419FCD82DAC56F5B95E46A5CC133 Abruf am: 12.12.2003

[95] UMTS Forum: Glossary LBS. URL: www.umts-forum.org Abruf am: 26.10.2003

[96] Vilmos, A.; Karnouskos, S.: *SEMOPS: Design of a New Payment Service.* In: IEEE 14th Int. Workshop on Database and Expert Systems Application (2003) S. 865-869

[97] Warren, D. Samuel; Brandeis, D. Louis: *The Right to Privacy.* In: Havard Law Review (1890) Nr. 4 S. 191-220

[98] Youssef, Moustafa A.; Agrawala, Ashok; Shankar, Udaya A.: *WLAN Location Determination via Clustering and Probability Distributions.* URL: http://citeseer.nj.nec.com/cache/papers/cs/27062/http:zSzzSzwww.cs.umd.eduzSz~moustafazSzpaperszSzpercom03.pdf/youssef03wlan.pdf Abruf am: 24.10.2003

Abkürzungsverzeichnis

A-GPS	Assisted Global Positioning System
APP	Access Point Provider
APPEL	A P3P Preference Exchange Language
ARP	Adress Resolution Protocol
ASP	Access Service Provider
B2B	Business-to-Business
B2C	Business-to-Customer
BDSG	Bundesdatenschutzgesetz
DGPS	Differential Global Positioning System
E-OTD	Enhanced Observed Time Difference
eBusiness	electronic Business
FIP	Fair Information Principles
GMSC	Gateway Mobile Switching Center
GPS	Global Positioning System
HLR	Home Location Register
ID	Identifikationsnummer
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
LAI	Location Area Identifier
LBS	Location Based Service
LEO	Low Earth Orbit
MDStV	Mediendienste-Staatsvertrag
MLP	Mobile Location Protocol

MSC	Mobile Switching Center
MVNO	Mobile Virtual Network Operator
P2P	Peer-to-Peer
P3P	Privacy Preferences Project
PAN	Personal Area Network
PESA	Privacy Enhancing Service Architectures
PET	Privacy Enhancing Technology
PLMN	Public Land Mobile Network
RARP	Reverse Adress Resolution Protocoll
RF	Radio Frequency
RSS	received signal strength
SET	Secure Electronic Transaction
SET-3D	SET-Three Domain Model
SMS	Short Message Service
SNR	Signal-Noise-Ratio
SP	Service Provider
SS	Signal Strength
TDDSG	Teledienstedatenschutzgesetz
TTP	Trusted Third Party
UL-TOA	Uplink Time of Arrival
UML	Unified Modelling Language
UMTS	Universal Mobile Telecommunication Service
URL	Uniform Resource Locator
VAS	Value Added Service
W3C	World Wide Web Consortium
WAP	Wireless Application Protocol
WLAN	Wireless Area Network
WMAN	Wireless Metropolitan Area Network
XML	eXtended Markup Language

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig angefertigt sowie keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe. Diese Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt.

Regensburg, den 28. Mai 2004