February 2007

Privatsphärenfreundliche topozentrische Dienste unter Berücksichtigung rechtlicher, technischer und wirtschaftlicher Restriktionen

Mike Radmacher
University of Frankfurt, mike.radmacher@m-lehrstuhl.de

Jan Zibuschka
University of Frankfurt, jan.zibuschka@m-lehrstuhl.de

Tobias Scherner
University of Frankfurt, tobias.scherner@m-lehrstuhl.de

Lothar Fritsch
University of Frankfurt, lothar.fritsch@m-lehrstuhl.de

Kai Rannenberg
University of Frankfurt, kai.rannenberg@m-lehrstuhl.de

In: Oberweis, Andreas, u.a. (Hg.) 2007. *eOrganisation: Service-, Prozess-, Market-Engineering*; 8. Internationale Tagung Wirtschaftsinformatik 2007. Karlsruhe: Universitätsverlag Karlsruhe

ISBN: 978-3-86644-094-4 (Band 1)
ISBN: 978-3-86644-095-1 (Band 2)
ISBN: 978-3-86644-093-7 (set)

Privatsphärenfreundliche topozentrische Dienste unter Berücksichtigung rechtlicher, technischer und wirtschaftlicher Restriktionen

Mike Radmacher, Jan Zibuschka, Tobias Scherner, Lothar Fritsch , Kai Rannenberg

Lehrstuhl für Mobile Commerce und Mehrseitige Sicherheit
University of Frankfurt
60054 Frankfurt am Main
{mike.radmacher, jan.zibuschka, tobias.scherner, lothar.fritsch, kai.rannenberg}
@m-lehrstuhl.de

Abstract

Die Entwicklung neuer Produkte im dynamischen Markt mobiler Datendienste stellt Anbieter und Netzbetreiber vor besonderen Herausforderungen. Kurzlebige Produkte, unbekannte Akzeptanz potentieller Nutzer und der Zwang neue Dienste auf vorhandene Infrastrukturen aufzusetzen, führt zu Schwierigkeiten bei der Umsetzung. Gerade die Datenschutz-Regulierung der Telekommunikation und die Durchdringung des Alltags mit allgegenwärtigen Kommunikations- und Ortungsmitteln stellt die Produktentwickler vor die Herausforderung geschäftliche Interessen, Datenschutzvorgaben und Nutzerpräferenzen zu modellieren, auszugleichen und in den Basisinfrastrukturen neuer mobilen Datenprodukte zu implementieren. Der vorliegende Artikel präsentiert einen Entwurf und die Implementierung eines Prototyps, der im Rahmen eines Forschungsprojektes mit Industriebeteiligung entwickelt wurde.

1 Einleitung

Die große Verbreitung, die Mobiltelefone auf Basis der GSM- oder UMTS-Standards heute erreicht haben, macht die Verwendung dieser Infrastruktur für die Ortung des Benutzers im Rahmen der Erbringung topozentrischer Dienste außerordentlich attraktiv, da so eine große Benutzerbasis angesprochen werden kann [Bund05]. Endgeräte mit integrierter Ortungsfunktion - wie GPS oder Galileo - sind nach wie vor selten [BuHE00]. Dabei kann der Netzbetreiber sel-

ber als Anbieter topozentrischer Dienste auftreten oder nur die Ortsdaten für die eigentlichen Dienstanbieter liefern.

1.1 Problemstellung

Die Verwendung sensibler Kundendaten wie die Position des Benutzers ist mit rechtlichen Anforderungen verbunden, die den Schutz der Privatsphäre des Kunden betreffen. Obwohl Netzbetreiber sehr gute Voraussetzungen haben, die Ortungstechnik für die Erbringung topozentrischer Dienste zu stellen, verbleiben in diesem Geschäftsfeld hinsichtlich der Umsetzung der rechtlichen Vorgaben noch offene Fragen, etwa nach der Verantwortlichkeit bei einem möglichen Missbrauch der benutzerbezogenen Daten. Um nicht für Verfehlungen eines Dienstanbieters verantwortlich gemacht zu werden, ergibt sich die Motivation, die tatsächliche Erbringung der Dienste auszulagern und eine Schnittstelle zu schaffen, die eine saubere Trennung von Netzbetreiber und Dienstanbieter erleichtert. Um die Weitergabe der Position eines Benutzers unabhängig vom konkret erbrachten topozentrischen Dienst zu erlauben, muss die Schnittstelle weiterhin zu einem erheblichen Umfang vom Nutzer konfigurierbar sein, um mit grundsätzlichen Datenschutzanforderungen in Einklang zu stehen. Daher ist eine Lösung erforderlich, die neben den wirtschaftlichen und rechtlichen Restriktionen die Privatsphäre des Nutzers respektiert und es ihm ermöglicht, die Herausgabe und Verwendung seiner persönlichen Daten zu kontrollieren. Ein System zum Identitätsmanagement, wie es ein aktuelles Forschungsprojekt implementiert, wird unerlässlich.

1.2 Szenario

Zur genaueren Analyse des Problems wurde ein spezielles Szenario gewählt. Dabei findet ein typischer topozentrischer Suchdienst Betrachtung, der prototypisch implementiert ist, um unter möglichst realitätsnahen Bedingungen die Eigenschaften der hier vorgestellten Lösung zu evaluieren:

Ein Handelsreisender (John) ist in einer neuen Stadt angekommen. Er stellt fest, dass er eine neue Dosis eines wichtigen Medikaments benötigt. Daher entscheidet er sich einen topozentrischen Dienst zu nutzen, der es ihm erlaubt, die nächste Apotheke zu lokalisieren. Sein Endgerät nimmt Verbindung mit dem Dienstanbieter auf, während der Netzbetreiber die eigentliche Ortung vornimmt. Die festgestellte Position wird an den Dienstanbieter übermittelt, der sie mit

seiner Datenbank vergleicht. Die Resultate - in diesem Fall die k nächsten Apotheken – werden an Johns Endgerät zurückgeliefert,.

1.3 State-of-The-Art

Es existiert heute eine große Anzahl von Techniken, mit deren Hilfe die Privatsphäre des Anwenders geschützt werden kann, zusammenfassend Privacy Enhancing Technologies (PETs) genannt [BlBO03]. Für die privatsphären-respektierende Behandlung von Ortsdaten finden sich in der Literatur verschiedene Ansätze bzw. Architekturen. Es folgt eine kurze Betrachtung ausgewählter Ansätze und Architekturen, um eine Gegenüberstellung der mit in diesem Papier dargestellten Architektur einzuleiten und die Vorteile hervorzuheben.

Die Alipes-Plattform [SNP02] bietet dem Benutzer die Möglichkeit den Zugriff auf seine Ortsdaten mittels von ihm konfigurierter Richtlinien zu kontrollieren. Weiterhin können Ortsinformationen aus unterschiedlichen Quellen aggregiert werden. Alipes bietet keinen weitergehenden Schutz der Identität des Nutzers und keine Pseudonymisierung.

Ein weiteres Beispiel stellt der von T-Systems entwickelte T-Identity Protector dar, der den Identitätsschutz unterstützen soll [Wage06]. Diese Lösung konzentriert sich auf die Pseudonymisierung von personenbezogenen Daten, bevor diese an eine weitere Instanz zur Verarbeitung weitergegeben werden. Die De-Pseudonymisierung von Nutzern ist für strittige Fälle vorgesehen. Der T-Identity Protector setzt ausschließlich auf Pseudonymisierung und umgeht die notwendige Einholung der Zustimmung des Nutzers vor der Weitergabe seiner Daten.

Durch das in [BöLR04] dargestellte Konzept wird einem Nutzer die Möglichkeit gegeben, für jeden Dienst explizit festzulegen, ob dieser eine Lokalisierung vornehmen darf oder nicht. Das Konzept liefert allerdings keinen Architekturvorschlag oder geht auf technische Details ein, wie beispielsweise die Verwendung von Pseudonymen.

In [RePr04] stellen die Autoren eine Architektur vor, die zur Reduktion der Ortsauflösung verwendet wird, um Dienste für die weniger genaue Informationen ausreichend sind, nur mit dem Notwendigen zu versorgen. Weder auf eine Zugriffkontrolle der Ortsinformationen, die Verwendung von Pseudonymen, die Einbettung in anderen Systemen noch die Verwendung kryptografischer Verfahren wird eingegangen.

Die in [JoBe04] vorgestellt Architektur adressiert topozentrische Dienste in Mobilfunkumfeld. Eine einfache Zugriffkontrolle und die Verwendung von Pseudonymen zur Verschleierung der

MSISDN werden diskutiert. Darüber hinaus findet allerdings keine Betrachtung der Informationsflüsse zwischen den an der Kommunikation beteiligten Parteien und dessen Schutz statt.
In [Oino02] werden Prozeduren zur Sicherstellung des Datenschutzes bei der Erbringung topozentrischer Dienste vorgeschlagen. Der Beitrag fokussiert sich auf die Einhaltung der gesetzlichen Vorgaben im Rahmen des Mobilfunks. Darin wird eine zentrale Entscheidungsfunktion auf Regelbasis vorgeschlagen, welche zwischen Ortsquelle und die nutzende Anwendung geschaltet ist. Genaueres wird nicht spezifiziert, insbesondere keine Sicherheitsarchitektur.
Im Gegensatz dazu wird in [MyAD03] eine regelbasierte Sicherung der Ortsdaten vorgeschlagen. Beim Versuch des Zugriffs auf die Daten durch einen Diensterbringer evaluieren Entitäten namens „Validators“ die Regeln und fällen die Zugriffsentscheidung. Über die Strukturierung der Architektur liefert das Papier keine Angaben, insbesondere über die Installation der Validatoren als 3. Partei oder als Teil einer der anderen Entitäten.
Weiterhin gibt es Ansätze, die Modellierung von Systemen, die Datenschutz-Anforderungen erfüllen müssen, zu formalisieren, um eine Berücksichtigung der Interessen der verschiedenen Parteien sicherzustellen, siehe [FrSR06]. Wissenschaftler und Industriepartner untersuchen die Architektur und Anwendung dieser Technologien in unterschiedlichen Forschungsprojekten im Rahmen des FP6/IST Programms der Europäischen Union. Neben den technischen und wirtschaftlichen Aspekten wird der Fall untersucht, dass Ortsdaten eines Benutzers von einem Netzbetreiber zur Verfügung gestellt und für die Verwendung in topozentrischen Diensten weitergeleitet werden [KFKK05] [Dumo05].
Darüber hinaus wurde zur Standardisierung von PETs im April 2005 von ISO/IEC JTC1/SC27 eine Study Period mit dem Thema Privacy eingeleitet. Ein entsprechender Identitätsmanagement-Standard wird ebenfalls seit April 2005 entwickelt.

2 Anforderungen

Die Anforderungen an das Identitätsmanagement in topozentrischen Diensten in Mobilfunknetzen sind vielseitig. Im Rahmen dieses Beitrags werden vor allem die geschäftlichen Interessen des Mobilfunk-Netzbetreibers im Verhältnis zur gesetzlichen Regulierung des Datenschutzes und den Privatsphäreninteressen der Nutzer betrachtet. Die Anbieter topozentrischer Dienste spielen in ihrer starken Abhängigkeit von den Netzanbietern hier eine untergeordnete Rolle; im Basisszenario wird uneingeschränkt davon ausgegangen, dass die Datenkommunikation zwi-

schen Dienstanbieter und Nutzern ausschließlich über die Netzanbieter stattfindet. Des Weiteren ist von einer quasi Monopolstellung der Netzanbieter für die Ortung der Nutzer-Terminals auszugehen[1]. Im resultierenden Szenario erbringt der Dienstanbieter, vermittelt vom Netzanbieter, topozentrische Datendienstleistungen auf Basis eigener Datenbestände. Diese Leistungen werden ganz oder teilweise mit dem Netzanbieter abgerechnet. Den Zugang zu Nutzern, Ortung und das Identitätsmanagement berechnet der Netzbetreiber. Ausprägungen und Diskussion dieser Konstellation wurden in [LFPR04] and [KFKK05] beschrieben.

2.1 Geschäftsmodell

Die vertriebliche Struktur von Mobilfunk-Zusatzdiensten wie Klingelton-Downloads, Handy-Logos und weiterer Dienste baut auf Wiederverkäufer-Strukturen auf. Netzbetreiber bieten die Zugangsschnittstellen zu Infrastruktur, Identitätsmanagement und Abrechnungsdienstleistungen an. Die Anforderungen des Industriepartners wurden zwischen verschiedenen Abteilungen abgestimmt und als Anforderungsdokument in das Prototyp-Projekt eingebracht [PRIM04a]. Als Grundszenario sollte ein System geschaffen werden, an welches analog zum Rufnummern- oder Klingeltongeschäft kaskadierende Wiederverkäufer für topozentrische Dienste ermöglicht, um die Vertriebsleistungen zu externalisieren und die Dienste nicht im Hause des Mobilfunkunternehmens installieren zu müssen. Die Aufstellung dieser Geschäftsvorgaben ist in Abbildung 1 dargestellt.

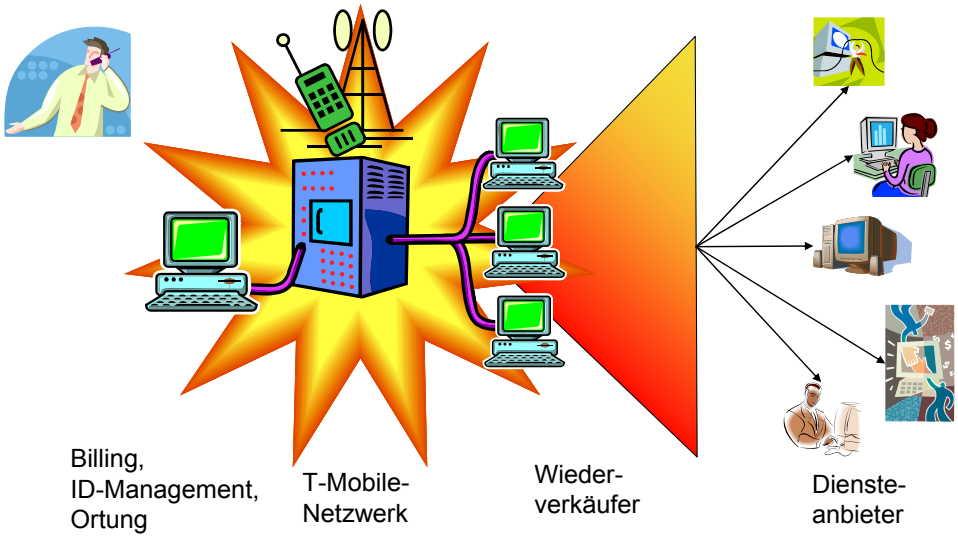

Abb. 1.: Struktur des Geschäftsmodells für topozentrische Dienste mit Wiederverkäufern.

[1] Es existieren zwar Terminals z.B. mit eingebauten Empfängern zur Satellitenpositionierung, diese sind aktuell jedoch nicht weit verbreitet. Diese Geräte stehen spezialisierten Nutzergruppen derzeit nur durch teure Neuanschaffung zur Verfügung.

2.2 Intermediäre bei Informationsdiensten

Die pyramidenförmige Struktur der Dienstanbindung der Mobilfunkbetreiber legt einen Blick auf die Intermediärstheorie nahe. Neben der effizienten Organisation des Vertriebs über Dienstanbieter können Prozesse, Informationsprodukte und andere Leistungen an der zentralen Schnittstelle angeboten und gebündelt werden. Die Vorzüge von Intermediären bzgl. der Suchzeiten und Preisstrukturen von gehandelten Produkten sind wissenschaftlich erforscht. Einen guten Überblick für Intermediäre von Informationsprodukten findet man bei Rose in [Rose99] sowie in [ScLi02]. Zur Wertsteigerung durch Intermediation eignen sich im Kontext topozentrischer Netz-Mehrwertdienste besonders:

- Identitätsmanagement und Datenschutz nach Telekommunikationsrecht (siehe [KFKK05] oder in einem rudimentären Ansatz in [BöLR02])
- Bündelung von Abrechnungs- und Risikomanagementdienstleistungen
- Verkauf von Zusatzdiensten wie Geoinformationen, Profilierung (wie zum Beispiel in [Figg04])

Privatsphärenmanagement im Spannungsfeld von Regulierung und Kundenzufriedenheit ist ein kostenintensives Feld, wie in [Pone04] aufgezeigt wurde. Daher ist bei der Gestaltung der Wiederverkäufer-Szenarien die Berücksichtigung von Identitäts- und Privatsphärenmanagement als Posten in der Wertschöpfungskette besonders attraktiv.

2.3 Datenschutz

Neben den wirtschaftlich orientierten Anforderungen aus den Abschnitten 2.1 und 2.2 ergeben sich weitere Anforderungen aus der Regulierung. Telekommunikation in Europa wird durch Richtlinien reguliert, welche sich nach der Umsetzung in nationalen Gesetzen einzelner Ländern wieder finden. Relevant für die Implementierung ist die Richtlinie 2002/58/EC [Euro02], in welcher in Artikel 9 die unterschiedliche rechtliche Betrachtung der Verwendung personenbezogener Ortsdaten einerseits zum Zweck der Anruf-Durchstellung und andererseits zur weiteren Nutzung vorgeschrieben wird. Zur anderweitigen Nutzung, beispielsweise für topozentrische Dienste, muss die explizite Datenverarbeitung erklärt und eine juristisch wirksame Einwilligung der betroffenen Person eingeholt werden. Des Weiteren ist sicherzustellen, dass der Nutzer seine Einwilligung kurzfristig widerrufen kann. Unklar ist hierbei allerdings die Homogenität der lokalen Umsetzung in nationales Recht. Zudem gibt es bislang wenige einheitliche Rege-

lungen zur Ausprägung der Einwilligungen – besonders für Ad-hoc-Nutzung von Diensten auf Mobiltelefonen. Hier gibt es bislang zwar Lösungsideen wie [Ross04], aber noch keine Standards. Aus Sicht von Nutzern und Netzbetreibern ist es erforderlich, die Einwilligungen beweissicher einzuholen und nachweisen zu können. Da der Netzanbieter zunächst bei der Herausgabe von Ortsdaten haftet, muss er eine Einwilligungsentscheidung treffen, bevor der Anbieter eines topozentrischen Dienstes persönliche Daten übermittelt bekommt. Dienstanbieter werden im Rahmen ihrer individuellen Angebote weitere Datenschutzvereinbarungen für ihre Nutzer vorrätig halten.

Eine Detailanalyse der rechtlichen Voraussetzungen netzbasierter topozentrischer Dienste findet sich in einem Forschungsprojekt des FP6/IST Programms der Europäischen Union in zwei Anforderungsanalysen für privatsphären-respektierende Anwendungen wieder [PRIM04a] [PRIM04b].

Wichtig neben der Erfüllung der formalen Datenschutzanforderungen ist in diesem Kontext für Netzbetreiber besonders die Flexibilität der Detailausprägung der Infrastrukturkomponente für Privatsphärenmanagement. Sowohl die Geschäftsstrategie als auch die Nutzer mobiler Dienste verstehen diese Dienste als über nationale Grenzen hinausgehende Dienstleistungen. Für Sprachtelefonie und Daten existiert hierfür bereits das „International Roaming“. Bei der Implementierung internationaler Infrastrukturen für privatsphärenfreundliche topozentrische Dienste müssen lokal unterschiedlich ausgestaltete Gesetzgebungen zu Datenschutz, Daten-Vorratsspeicherung oder Überwachung durch Bedarfsträger berücksichtigt werden. Zur Vermeidung von Neuprojektierungen für jedes einzelne Land, in dem ein Netzbetreiber ein Geschäftsfeld eröffnet, lohnt es sich, konfigurierbare Intermediärsdienstleistungen für Privatsphärenmanagement einheitlich bereit zu halten und zu konfigurieren. Aus diesem Blickwinkel betrachtet stützt die inhomogene Rechtslage die Abwicklung von Identitäts- und Privatsphärenmanagement über einen Intermediär.

3 Lösungsansatz

Basierend auf den Anforderungen aus Kapitel 2 ist im Rahmen eines europäischen Forschungsprojektes der folgende Lösungsansatz für die Umsetzung eines datenschutz- und privatsphärenfreundlichen topozentrischen Prototypen entwickelt worden.

Der Lösungsansatz beinhaltet die Integration eines Intermediärs als zusätzliche Partei neben dem Netzbetreiber, dem Anbieter topzentrischer Dienste und deren Nutzer in der bisherigen Wertschöpfungskette des Mobile Commerce [KFKK05].

Der Intermediär erfüllt in dem Szenario drei wesentliche Aufgaben. Die erste Aufgabe beinhaltet die Gewährleistung der Anonymität des Nutzers gegenüber den an der Kommunikation beteiligten Parteien. Damit ist gemeint, dass seine Identität gegenüber dem Dienstanbieter topozentrischer Dienste und der konkrete angefragte Dienst gegenüber dem Netzbetreiber verschleiert wird. Jede Kommunikation zwischen Netzbetreiber und Dienstanbieter erfolgt ausschließlich über den Intermediär. Die dritte Aufgabe des Intermediärs ist die Repräsentation des Nutzers und die damit verbundene Vertretung seiner Interessen während der gesamten Kommunikationsbeziehung, wie dargestellt in [PRIM06a]. Die Vertretung erfolgt durch die Definition feingranularer Regeln mit deren Hilfe die Dienstverwendung bestimmt und/oder eingeschränkt wird. Ziel ist die Transparenz der zu übertragenden persönlichen Daten zu gewährleisten.

Der im Rahmen der Projektarbeit entwickelte Prototyp basiert auf einer bereits existierenden Struktur eines Netzbetreibers und stellt einen ortbasierten Dienst zum Finden von Apotheken zur Verfügung. Alle im Kommunikationsprozess involvierten Parteien, mit Ausnahme des Nutzers, integrierten Softwarekomponenten in ihre bestehenden internen Strukturen. Der Nutzer erhält über ein Webinterface direkten Zugriff auf den Intermediär, um mit der für ihn vorgesehenen Identitäts- und Zugriffskontrollinstanz zu interagieren [PRIM06a]. Im dargelegten Szenario ist der Intermediär physisch der Infrastruktur des Netzbetreibers zugeordnet. Die Architektur ist in Abbildung 2 dargelegt.

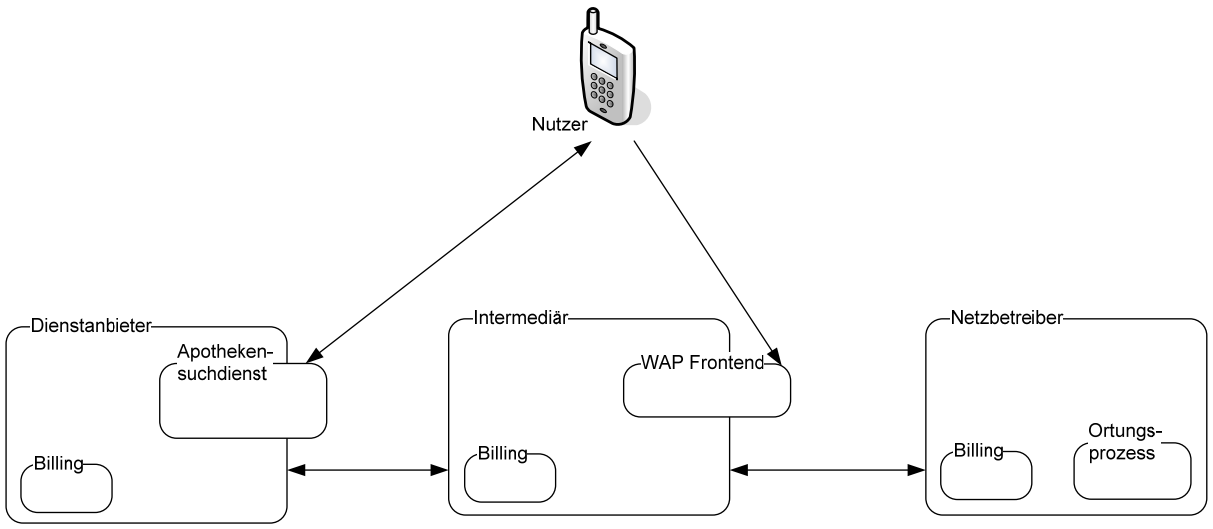

Abb. 2.: Architektur des Apothekensuchdienstes

Im Weiteren wird zunächst die Benutzerführung des Prototyps dargestellt.

3.1 Benutzerführung

Der Service begrüßt den Nutzer mit einem Bildschirm, von dem aus die Lokalisierung der nächstgelegenen Apotheke initiiert werden kann. Darüber hinaus ist es möglich, weitere Informationen über die Datenschutz-Funktionen des Prototyps abzurufen.

Abb. 3.: Hauptbildschirm

Wird der Dienst zum ersten Mal genutzt oder ist aus anderen Gründen keine gültige Richtlinie für die Handhabung der Ortsinformationen des Nutzers vorhanden, wird der Benutzer zu seiner Konsole beim Intermediär umgeleitet, wo er die Parameter der Datenschutzrichtlinie bearbeiten kann, bevor er sie bestätigt. Nach erfolgter Bestätigung wird der Benutzer – abhängig von seiner Eingabe – zurück zum Dienstanbieter oder aber zu einer Übersicht der eingestellten Datenschutzrichtlinien weitergeleitet. Sollte der Benutzer sich entscheiden, die neue Richtlinie nicht zu bestätigen, kann keine Nutzung des Dienstes erfolgen.

Abb. 4.: Einstellen einer Datenschutz-Richtlinie

Da nun ein durch die Benutzer-Richtlinie gesteuerter Datenaustausch zwischen Dienstanbieter und Intermediär erfolgen kann, ist eine Erbringung des Dienstes möglich - der Nutzer erhält das Ergebnis seiner Anfrage.

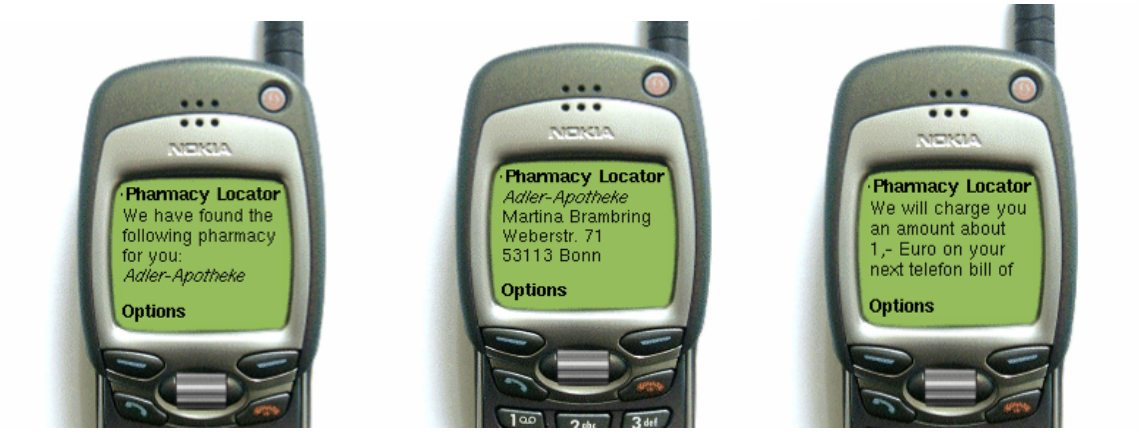

Abb. 5.: Ergebnis einer Ortung

3.2 Architektur

Die nachfolgenden Abschnitte betrachten den Nutzer, Dienstanbieter, Intermediär und Netzbetreiber im Detail. Neben der generellen Aufgabenbeschreibung wird auf die Beschreibung des Kommunikationsablaufs innerhalb des zugrunde liegenden Szenarios eingegangen. Abschließend wird in Abbildung 6 der gesamte Kommunikationsprozess zusammengefasst.

3.2.1 Nutzer

Bei einer Betrachtung aus der Perspektive des Nutzers ergeben sich besondere Anforderungen, die im Rahmen der Umsetzung berücksichtigt wurden. Der Nutzer des Apothekensuchdienstes ist im Besitz eines mobilen Endgerätes, das über ein kleines Display, eine beschränkte Eingabefunktionalität, geringe Rechenleistung und eine geringe Datenübertragungsrate verfügt. Diese Merkmale spiegeln die in der Masse der Bevölkerung vorzufindenden Endgeräte wieder [PRIM04a], die der Netzbetreiber als Zielgruppe adressiert. Des Weiteren ist vorgesehen, dass keine zusätzliche Software auf dem mobilen Endgerät des Nutzers zu installieren ist. Ein WAP Browser muss vorhanden sein, der zur Standardausstattung nahezu aller mobilen Endgeräte gehört [PRIM04a] [PRIM06a] [PRIM06b]. Der Zugriff auf die Identitäts- und Zugriffskontrolleinstanz des Nutzers ist durch ein WAP-Interface über den Intermediär möglich, dessen Verwendung dem Nutzer eine intuitive Handhabung erlaubt. Dadurch wird der Nutzer in die

Lage versetzt, Zugriffsregeln für Dienste, die er über einen Dienstanbieter in Anspruch nehmen möchte, zu setzen.

Verwendet ein Nutzer einen Dienst zum ersten Mal, ist keine Zugriffregel beim Intermediär definiert, die den Zugriff auf Ortinformationen oder Nutzerpräferenzen regelt. In diesem Fall wird eine Standardregel vorgeschlagen. Der Regelvorschlag wird beim Intermediär hinterlegt. Der Nutzer wird zum Intermediär weitergeleitet und erhält die Optionen den Regelvorschlag zu akzeptieren, zu überarbeiten oder abzulehnen [PRIM06a]. Dieser Mechanismus verhindert, dass personenbezogene Informationen über einen Nutzer ohne dessen explizite Einwilligung verarbeitet werden. Das Entgelt für die Diensterbringung wird durch den Netzbetreiber in einem monatlichen Intervall abgerechnet. Durch den Intermediär ist ein weiterer Schutzmechanismus geschaffen, der keinem Anbieter die Möglichkeit offeriert, einen Geldwert für die Inanspruchnahme in Rechnung zu stellen, ohne dass der Nutzer explizit, beispielsweise durch eine Zugriffregeln dieser Dienstnutzung zugestimmt hat.

3.2.2 Dienstanbieter

Im vorliegenden Abschnitt wird der Blickwinkel des Dienstanbieters (Apothekensuchdienst) detailliert betrachtet. Dafür ist es notwenig Annahmen zu treffen. Der Dienstanbieter ist eine Partei innerhalb des gesamten Kommunikationsablaufs, die einer Nutzergruppe durch das Betreiben eines Webservers gegen Entgelt einen oder mehrere Dienste zur Verfügung stellt. Die Preise für die Nutzung eines Dienstes entsprechen definierten Preiskategorien des Netzbetreibers. Nach jeder autorisierten Transaktion (Dienstnutzung) belastet der Intermediär ein virtuelles Konto des Nutzers. Die dort auflaufenden Beträge werden einmal im Monat durch den Netzbetreiber abgerechnet [PRIM06a]. Damit der Intermediär die entstandenen Kosten des Dienstanbieters gegenüber dem Netzanbieter vertreten darf, sind an dieser Stelle weitere Verträge zwischen beiden Parteien notwendig. Als Identifikationsmerkmal des Nutzers wird die IP-Adresse verwendet. Um die Dienstnutzung aus Sicht des Dienstanbieters vollständig nachzuvollziehen, wird diese am Beispiel der Erstnutzung des Apothekensuchdienstes betrachtet.

Der Apothekensuchdienst ist durch einen beim Dienstanbieter betriebenen Webserver im Internet erreichbar. Der Nutzer meldet sich beim Dienstanbieter an, um einen Dienst zu verwenden. Dabei wird eine Instanz der sich beim Dienstanbieter befindlichen Softwarekomponente initialisiert. Diese sorgt für den datenschutz- und privatsphärenfreundlichen Austausch personenbezogener Daten. Nachdem sich der Nutzer beim Dienstanbieter für die Nutzung eines Dienstes angemeldet hat, benötigt dieser zusätzliche Informationen zur Diensterbringung, wie beispielswei-

se den Aufenthaltsort des Nutzers. Darüber hinaus ist sicherzustellen, dass der Anbieter des Dienstes den Geldwert für die Dienstnutzung abrechnen kann [PRIM06a].
Um Zugriff auf die Ortsinformation des Nutzers zu erlangen und den Geldwert für die Dienstnutzung einzufordern, hat der Dienstanbieter dem Intermediär den Dienstnamen und die Kosten für die Dienstnutzung mitzuteilen. Vorausgehend ist eine Authentifizierung des Dienstanbieters beim Intermediär erforderlich. Nach dem Abgleich der Dienstinformationen mit den durch den Nutzer hinterlegten Regeln (Intermediär) ist der Zugriff auf die Ortsinformationen gestattet oder versperrt. Für den Fall, dass der Zugriff auf die Ortsinformation und die Reservierung des Geldwertes, aufgrund fehlender oder sperrender Regeln, verwehrt ist, meldet die Softwarekomponente einen Fehler [PRIM06a]. Nach Erhalt der Fehlermeldung wird die Dienstanbieterseite einen Regelentwurf für die Nutzung des Dienstes generieren und an den Intermediär übertragen. Der Nutzer wird über den Regelvorschlag informiert und wahlweise direkt zum Intermediär weitergeleitet. Dort nimmt der Nutzer Zugriff auf seine Identitäts- und Zugriffskontrollinstanz. Die Regelvorlage des Dienstanbieters wird angezeigt. Der Nutzer hat die Möglichkeit diese Regel zu überprüfen, anzunehmen oder abzulehnen. Im Fall der Annahme erfolgt erneut eine Weiterleitung zum Dienstanbieter, der aufgrund der akzeptierten Regeln alle notwendigen Informationen für die Diensterbringung erhält [PRIM06a]. Ein virtuelles Konto des Nutzers, hinterlegt beim Intermediär, wird mit dem Geldwert der Dienstnutzung belastet, ein weiteres virtuelles Konto für Dienstanbieter mit den Kosten für die Ortung. Auf Basis der übermittelten Daten ist der Dienstanbieter in der Lage, seine Datenbank zu durchsuchen und dem Nutzer die nächstliegende Apotheke mitzuteilen. Alle benutzerrelevanten Daten werden nach Beendigung der Diensterbringung mit der Zerstörung der Session verworfen.

3.2.3 Intermediär

Der Intermediär ist eine zentrale Komponente der Architektur und befindet sich zwischen Dienstanbieter, Netzbetreiber und Nutzer [KFKK05]. Zu den ihm zugeteilten Aufgaben (siehe Kapitel 3 Einleitung) gehört die Repräsentation des Nutzers. Der Intermediär erhält Anfragen eines Dienstanbieters, dessen Dienst der Nutzer verwenden möchte. Eine Überprüfung der Nutzung hinsichtlich der vom Nutzer hinterlegten Regeln und der möglichen Zahlungsfähigkeit wird durchgeführt. Der detaillierte Ablauf der Kommunikation wird im Folgenden dargestellt.
Der Dienstanbieter, der mit dem Nutzer verbunden ist und diesen über eine IP-Adresse identifiziert, erfragt beim Intermediär die Ortsinformation der zugeordneten IP-Adresse an. Darüber hinaus teilt der Dienstanbieter dem Intermediär den festgesetzten Preis für die Inanspruchnahme

des Dienstes mit. Der Intermediär löst mit Hilfe des Netzbetreibers die IP-Adresse auf und überprüft die vom Nutzer beim Intermediär hinterlegten Regeln für die Dienstnutzung. Die aktuelle IP-Adresse stellt ein temporäres Identifikationsmerkmal dar, dass sich nach erneutem Verbindungsaufbau verändert. Aus diesem Grund wird die IP-Adresse in ein Transaktionspseudonym überführt, das zwischen Intermediär und Dienstanbieter kommuniziert wird. Falls keine für die Dienstnutzung adäquate Regel existiert, ist die Nutzung ausgeschlossen und dem Dienstanbieter wird eine Fehlermeldung gemeldet. Die Übermittlung eines Regelentwurfs für die Nutzung des Dienstes erfolgt. Nach Zustimmung wird die Regel angewendet. Die Ortsinformation des Nutzers wird über den Intermediär beim Netzbetreiber angefragt, ohne Informationen über den zu verwendenden Dienst mitzuteilen. Ferner wird überprüft, ob die Zahlungsfähigkeit des Nutzers gegeben ist. Ist dies der Fall, wird die Ortsinformation über den Intermediär an den Dienstanbieter übermittelt. Die Kosten für die Ortung werden dem Dienstanbieter in einem virtuellen Konto beim Intermediär in Rechnung gestellt. Auf Basis der übertragenden Ortsinformation wird der Dienst durch den Dienstanbieter erbracht. Dem Nutzer werden die Kosten für den Dienst in Rechnung gestellt. Das virtuelle Konto des Nutzers wird mit den Kosten der Dienstnutzung belastet [PRIM06a]. Am Ende des Monats stellt der Intermediär zwei Rechnungen. Eine Rechnung, die dem Netzbetreiber zugestellt wird, beinhaltet die Kosten der Dienstnutzung ohne Bekanntgabe des Dienstes. Die zweite Rechnung über die Anzahl der Ortungen in Verbindung mit dem jeweiligen Transaktionspseudonym erhält der Dienstanbieter.

3.2.4 Netzbetreiber

Der Netzbetreiber ist die Partei, die eine traditionelle Geschäftsbeziehung mit dem Nutzer unterhält. Diese ermöglicht die Kommunikation, die Ortung und die Abrechnung zwischen Nutzer und Dienstanbieter. Die Softwarekomponente, die beim Netzbetreiber integriert ist, dient einerseits zur Übertragung der personenbezogenen Daten und anderseits als Kotrollinstanz zum Nachweis autorisierter Transaktionen [PRIM06a] [PRIM06c].

Der Netzbereiter wird im Szenario des Apothekensuchdiensts mehrfach involviert. Zu Beginn erfragt der Intermediär die Ortsinformation der ihm bekannten IP-Adresse. Im Anschluss wird erfragt, ob der Nutzer in der Lage ist, den zu verwendenden Dienst zu bezahlen. Die Antwort auf beide Fragen wird an den Intermediär übertragen. Da der Netzbetreiber den Dienstanbieter nicht kennt, werden die Kosten der Ortung dem Intermediär in Rechnung gestellt. Nach erfolgreicher Dienstnutzung informiert der Intermediär den Netzbetreiber, so dass dieser dem Nutzer

die Kosten der Dienstnutzung in Rechnung stellen kann [PRIM06a]. Die Abrechnung erfolgt einmal im Monat.

Zusammenfassend veranschaulicht das UML-Sequenzdiagramm in Abbildung. 6 nochmals den Kommunikationsablauf.

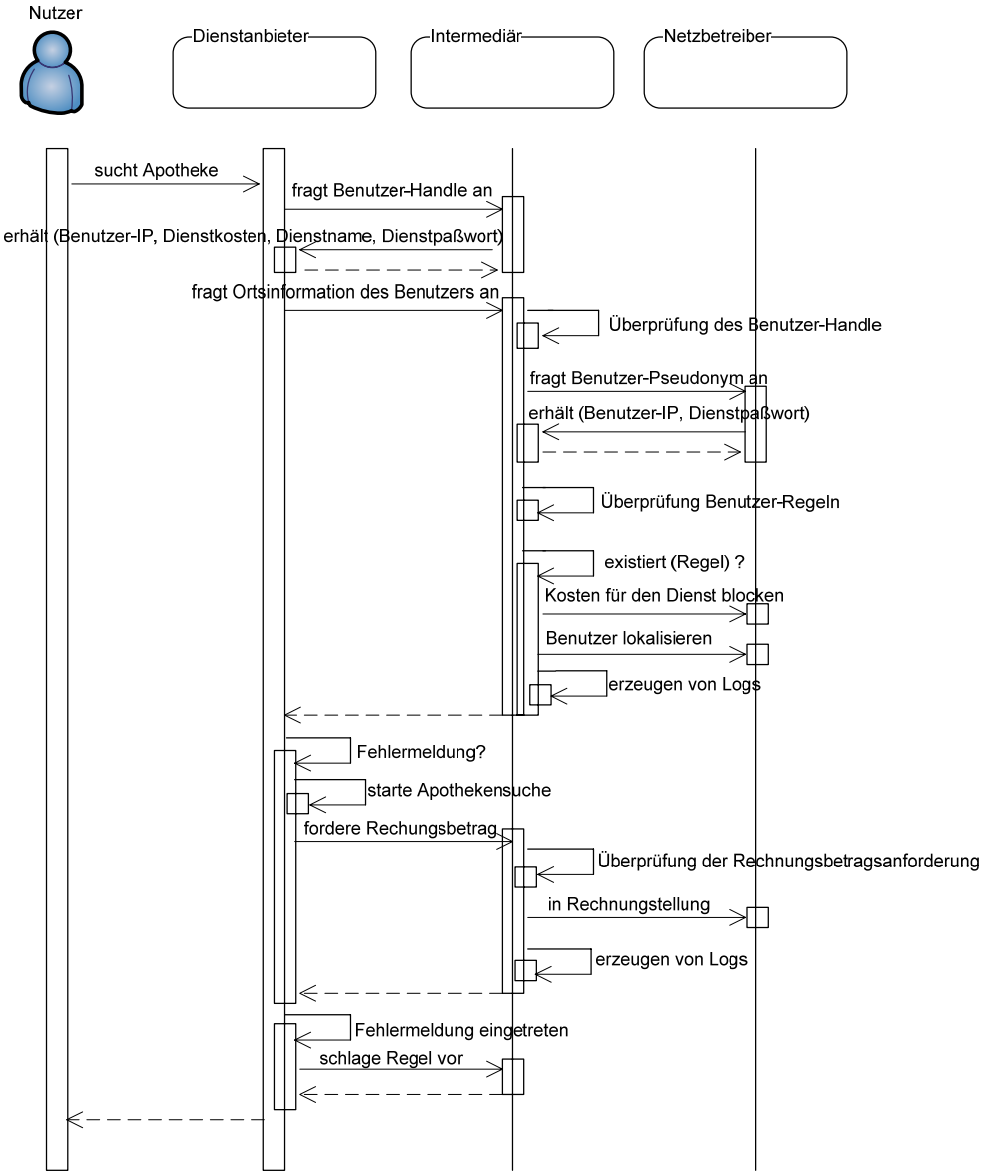

Abb. 6.: Sequenzdiagramm

4 Zusammenfassung und Ausblick

Wie gezeigt wurde, lässt sich unter den besonderen Rahmenbedingungen mobiler Datenprodukte auf bestehenden Infrastrukturen ein Ausgleich der Interessen der Beteiligten erreichen. Im Rahmen des bestehenden Prototyps für privatsphären-respektierende topozentrische Dienste

wurde eine Architektur erprobt, welche die Geschäfts- und Privatsphäreninteressen der Beteiligten umsetzt. Die wurde aus der Sicht verschiedener Disziplinen evaluiert [PRIM06d]. Die Spezialisten aus den Bereichen Recht, Assurance, HCI, und Sozioökonomie hatten die Aufgabe, in ihrem Spezialbereich die Prototypen auf Anwendbarkeit für Nutzer und beteiligte Businesspartner zu untersuchen. Die dabei gewonnenen Erkenntnissewurden in einem Evaluationsbericht [PRIM05] zusammengefasst.

Die beteiligten Disziplinen sind in ihrem Resümee zu dem Urteil gekommen, dass der Prototyp für topozentrische Diensteerbringung eine sehr gute Balance zwischen den Interessen der einzelnen Beteiligten darstellt. Insbesondere konnte gezeigt werden, dass die Berücksichtigung der Privatsphäre eine positive Voraussetzung für Anwendungsfälle sein kann, ohne dass die zugehörigen Prozesse für Nutzer und Dienstanbieter hochkomplex in Betrieb und Nutzung und somit unattraktiv für Anbieter und Nutzer werden.

Eine Standardisierung der Intermediärsschnittstelle würde eine vom Netzbetreiber unabhängige Verwendung topozentrischer Dienste, etwa im Falle von International Roaming, erlauben. Zusätzlich könnte eine solche Identitätsmanagement-Funktionalität dem Benutzer eine konsistente Kontrolle seiner persönlichen Informationen ermöglichen, was - gerade bei kritischen Nutzern - eine höhere Akzeptanz nach sich ziehen könnte. Daher regen die Autoren an, die Vereinheitlichung von Intermediationsschnittstellen für Identitäts- und Privatsphärenmanagement im internationalen Rahmen anzustreben und diese im industriellen Rahmen umzusetzen. So könnte ein internationaler Durchbruch für topozentrische Dienstleistungen erreicht - und beispielsweise von aktuellen europäischen Bestrebungen bei der Ortung von Notrufen bereits eingesetzt werden oder der Verbreiterung des Szenarios im Sinne von [FrSc05] dienen.

Danksagung

Die Inhalte dieses Papiers wurden im Rahmen der Projektarbeit im PRIME Projekt erarbeitet, repräsentieren allerdings nur die Ansicht der Autoren.

Literaturverzeichnis

[BlBO03] Blarkom, G.W.; Borking, J.; Olk, J.G.: Handbook of Privacy and Privacy-Enhancing Technologies. College bescherming persoonsgegevens, The Hague. 2003.

[BöLR02] Böhm, A.; Leiber, T.; Reufenheuser, B.: Trust and Transparency in Location-Based Services: Making Users lose their Fear of Big Brother In: Workshop on Location Systems Privacy and Control, 2004.

[BuHE00] Bulusu, N.; Heidemann, H.; Estrin, D.: GPS-less low cost outdoor localization for very small devices. In: Technical report 00-729, Computer science department, University of Southern California. 2000.

[Bund05] Bundesnetzagentur: Jahresbericht. 2005.

[Comm05] Common Criteria Project: The Common Criteria Part 1 - Introduction and general model, Version 2.3, similar to IS 18045. 2005.

[Dumo05] Dumortier, J.: Combining Personalised Communications Services with Privacy-Friendly Identity Management. In: Proceedings of the 44th FITCE Congress, 2005, 142-146.

[Euro02] European Parliament: Directive 2002/58/EC of the European Parliament and of the council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Brussels: 2002.

[Euro95] European Parliament: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Luxembourg. 1995.

[Figg04] Figge, S.: Situation-dependent services - a challenge for mobile network operators. In: Journal of Business Research, 57, 2004, 1416-1422.

[FrSc05] Fritsch, L. und Scherner, T.: A Multilaterally Secure, Privacy-Friendly Location-based Service for Disaster Management and Civil Protection. In Proceedings of the AICED/ICN 2005, (Springer Lecture Notes on Computer Science LNCS 3421), Berlin, Heidelberg, New York 2005 S. 1130-1137.2005, 1130-1137.

[FrSR06] Fritsch, L.; Scherner, T.; Rannenberg, K.: Von Anforderungen zur verteilten, Privatsphären-respektierenden Infrastruktur. In: Praxis in der Informationsverarbeitung und Kommunikation (PIK), 29, 2006, 37-42.

[Inter05a] International Organization for Standardization (ISO): The Common Criteria Part 2 - Security functional requirements, Version 2.3, similar to IS 18045:2004. 2005.

[Inter05b] International Organization for Standardization (ISO): The Common Criteria Part 3: Security assurance requirements - Version 2.3, similar to IS 18405. 2005.

[JoBe04] Jorns, O, -Bessler, S.: PRIVES: A privacy enhanced location based scheme. In: Workshop on Location Systems, Privacy and Control, 2004.

[KFKK05] Koelsch, T.; Fritsch, L.; Kohlweiss, M.; Kesdogan, D.: Privacy for Profitable Location Based Services. In: Proceedings of the Security in Pervasive Computing Workshop (SPC), 2005, 164-179.

[LFPR04] Lindner, T.; Fritsch, L.; Plank, K.; Rannenberg, K.: Exploitation of Public and Private WiFi Coverage for New Business Models. In: Proceedings of the 4th IFIP Conference on E-Commerce, E-Business, and E-Government (I3E),2004.

[MyAD03] Myles, G., Friday, A. and Davies, N.: Preserving Privacy in Environments with Location Based Applications. In: IEEE Pervasive Computing 2, (2003) 1, S. 56-64.

[Oino02] Oinonen K. TR101 - LIF Privacy Guidelines. 2002.

[PRIM04a] PRIME Project: Application Requirements. In deliverable 1.1.a part 3, 2004.

[PRIM04b] PRIME Project: Legal Requirements. In part 1 of deliverable 1.1a of IST PRIME EU. Arizona, 2004

[PRIM05] PRIME Project: Framework V.1. In deliverable 14.1.a. 2005

[PRIM06a] PRIME Project: Pharmacy Search - High Level Design. In deliverable 4.1.a.3.8, 2006.

[PRIM06b] PRIME Project: LBS Installation Guide. In deliverable 4.1.a.3.10, 2006

[PRIM06c] PRIME Project: User documentation on the LBS application prototype – pharmacy search. In Deliverable 4.1.a.3.10, 2006

[PRIM06d] PRIME Project: Evaluation of initial Application Prototypes. 2006.

[Pone04] Ponemon Institute: The Cost of Privacy - Study, Tucson, Arizona, 2004.

[RePr04] Cheng, Reynold; Prabhakar, Sunil: Using Uncertainty to Provide-Preserving and High-Quality Location-Based Services, in: Workshop on Location Systems, Privacy and Control, 2004.

[Rose99] Rose, F.: The economics, concept and design of information intermediaries. Physica-Verlag, Heidelberg, 1999

[Ross04] Rossnagel, H.: Mobile Qualified Electronic Signatures and Certification on Demand, in: Proceedings of the 1st European PKI Workshop - Research and Applications. 2004.

[ScLi02] Schackmann, J.; Link, H.: Intermediaries for the Provision of Mass Customized Digital Goods in Electronic Commerce, in: Moving into Mass Customization, 2002.

[SNP02] Synnes, K.; North, J.; Parnes, P.: Location Privacy in the Alipes Platform. Institutionen för Systemteknik; Lulea University of Technology; 2002

[Wage06] Wagner, F.: T-Identity Protector – Functional operation. In W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement, Ispra. 2006