UNIVERSITÄT
KOBLENZ · LANDAU
Institut für Wirtschafts- und Verwaltungsinformatik

FB 4
Informatik

Entwicklung einer Architektur für komplexe kontextbezogene Dienste im mobilen Umfeld

Stefan Stein

Nr. 7/2008

Arbeitsberichte aus dem Fachbereich Informatik

Arbeitsberichte des Fachbereichs Informatik

ISSN (Print): 1864-0346
ISSN (Online): 1864-0850

Herausgeber / Edited by:

Der Dekan:
Prof. Dr. Zöbel

Kontaktdaten der Verfasser

Stefan Stein
Institut für Wirtschafts- und Verwaltungsinformatik
Fachbereich Informatik
Universität Koblenz-Landau
Universitätsstraße 1
D-56070 Koblenz
EMail: stein@uni-koblenz.de

Entwicklung einer Architektur für komplexe kontextbezogene Dienste im mobilen Umfeld

Stefan Stein

Institut für Wirtschafts- und Verwaltungsinformatik
Universität Koblenz-Landau
Universitätsstraße 1
56070 Koblenz

stein@uni-koblenz.de

Abstract: Dieser Arbeitsbericht behandelt die Entwicklung einer Architektur für komplexe kontextbezogene Dienste im mobilen Umfeld. Der folgende Arbeitsbericht beschreibt die grundlegende Problemstellung und einen theoretischen Lösungsansatz, der im weiteren Forschungsprozess konkretisiert, prototypisch implementiert und evaluiert wird.

Durch die gestiegene Mobilität vieler Menschen besteht ein stetig steigender Bedarf an mobilen Kommunikations- und Informationsdiensten. Im mobilen Umfeld werden die meisten Mehrwertdienste zum jetzigen Zeitpunkt von den Mobilfunkprovidern angeboten. Es handelt sich primär um Dienste für den Massenmarkt, die keine nennenswerte Personalisierung zulassen. Aufgrund der funktionell einfachen Dienste und des damit verbundenen niedrigen Komforts sowie der durch die Nutzung entstehenden Kosten werden derartige Dienste nur in begrenztem Maße vom Massenmarkt angenommen. Dazu besteht keine Möglichkeit, kostengünstig kontextbezogene Dienste für spezielle Personengruppen anzubieten, da das Dienstangebot vom jeweiligen Mobilfunkprovider festgelegt wird.

Diese Arbeit betrachtet nicht nur die heutigen Hemmnisse, sondern auch die Anforderungen, die einer Akzeptanz besonders von komplexen kontextbezogenen Diensten noch im Wege stehen. Ziel ist es, eine Architektur bereitzustellen, die zukünftig personalisierte Dienste ermöglichen soll. Durch die Verwendung von sensiblen Kontextinformationen bei der Diensterbringung muss bei der Konzeption dieser Architektur der Schutz der Privatsphäre als ein wichtiger Punkt betrachtet werden. Basierend auf diesen ermittelten Anforderungen schlägt diese Arbeit eine Architektur vor, die es ermöglicht, kontextbezogene Dienste geräte- und providerunabhängig in einem wirtschaftlichen Umfeld, unter Berücksichtigung des Schutzes der Privatsphäre des Benutzers, anzubieten.

Inhaltsverzeichnis

1. Einleitung

Die Gesellschaft verlangt von vielen Arbeitnehmern eine sehr hohe Flexibilität und Mobilität. Möglich wurde dieser nomadische Lebensstil [LK95] erst durch die breite Verfügbarkeit von Kommunikations- und Informationsdiensten, die für einen Massenmarkt bereitgestellt wurden. Kommunikationsdienste werden durch den Einsatz von Mobilfunktelefonen realisiert. Über diese Geräte besteht auch die Möglichkeit, mobile Informationsdienste abzurufen. Zum jetzigen Zeitpunkt handelt es sich dabei noch um Dienste, die nicht personalisiert sind. Durch die nicht vorhandene Personalisierung können sie zwar dem Massenmarkt angeboten werden, sind aber nicht an die Bedürfnisse des Einzelnen angepasst. Sie können nur realisiert werden, indem Kontextinformationen der Benutzer bei der Diensterbringung berücksichtigt werden. Es handelt sich in diesem Fall um kontextsensitive Dienste. Mithilfe des Kontextes kann die Situation des Benutzers direkt bei der Diensterbringung berücksichtigt werden. Bei den Kontextinformationen kann es sich beispielsweise um den Standort des Benutzers, die Uhrzeit oder weitere personenbezogene Informationen handeln. Durch die Integration derartiger Informationen ist es möglich, einen personalisierten Dienst für den Massenmarkt zu erstellen. Das Problem, das sich durch derartige Dienste jedoch stellt, ist die Tatsache, dass die Verwendung von personalisierten Informationen auch Risiken für den Benutzer birgt. Um eine bereits in einfacher Form existierende Art von kontextbezogenen Diensten handelt es sich bei ortsbezogenen Diensten. Die Nutzung von Ortsinformationen kann dabei zu einem Akzeptanzproblem führen, da eine Abfrage der Benutzerposition viele Rückschlüsse auf die Interessen und Einstellungen des Benutzers zulässt. Besonders, wenn der Benutzer den Dienst regelmäßig verwendet und somit der Dienstanbieter den Zugriff auf mehrere Positionsinformationen besitzt. Der Dienstanbieter ist somit in der Lage, die Informationen auszuwerten und dabei abzuleiten, welche wirtschaftlichen Interessen bzw. politischen oder religiösen Ausrichtungen der Benutzer besitzt. Derartige Informationen sind auch für die Werbewirtschaft von Interesse, da sie das Käufer- oder Nutzungsverhalten ableiten kann. Das Risiko für den Benutzer besteht somit darin, dass durch die Dienstnutzung dem Dienstanbieter ein Einblick in die Privatsphäre ermöglicht wird, den er für andere Tätigkeiten als die der reinen Diensterbringung verwenden kann. Daher ist es notwendig, dass der Dienstanbieter vertrauenswürdig ist. Er muss die notwendigen Geschäftsprozesse darauf ausrichten, dass sensible Informationen nicht für Tätigkeiten verwendet werden, die dem Benutzer nicht bekannt sind und nicht zur Dienstleistungserbringung benötigt werden.

Im Rahmen dieser Arbeit wird eine Architektur für kontextsensitive Dienste entwickelt, die speziell an die Anforderungen des mobilen Umfeldes angepasst ist. Die zentrale Anforderung an diese Architektur besteht darin, den Schutz der Privatsphäre des Benutzers sicherzustellen. Dies wird dadurch realisiert, dass der Benutzer die Möglichkeit besitzt, aktiv entscheiden zu können, welche Dienste auf die Kontextinformationen zugreifen sollen. Er besitzt zusätzlich die Möglichkeit, sich jederzeit über die definierten Einstellungen zu informieren. Die Berechtigungen kann er mithilfe von Regelsätzen realisieren. Bei der Diensterbringung sind mehrere Instanzen beteiligt. Ein weiterer Kernbestandteil dieser Architektur besteht darin, dass die daran beteiligten Instanzen nur zu einer minimalen Informationsmenge Zugriff haben. Die Informationsmenge ist dabei so bemessen, dass sie ausreicht, um die Dienstleistung zu erbringen. Dadurch sollen Rückschlüsse auf das Benutzerverhalten vermieden werden oder nur in eingeschränkter Form möglich sein. Durch die Minimierung der Anzahl von Instanzen, die vom Benutzer bei der Dienstleistungserbringung einbezogen

werden, soll die Akzeptanz eines derartigen Architektureinsatzes gesteigert werden. Diese Architektur soll sowohl Push- wie auch Pull-Dienste ermöglichen.

Im heutigen mobilen Umfeld dominieren primär Dienste, die von den Mobilfunkprovidern oder ihren Vertragspartnern angeboten werden. Für den Benutzer besitzt die durch den Mobilfunkprovider dominierte Situation sowohl Vor- als auch Nachteile:

Es ist für den Kunden vorteilhaft, dass für einen bestimmten Dienst zumeist nur ein Dienstanbieter vorhanden ist, der speziell die Anforderungen des Providers berücksichtigt. Aus Sicht des Mobilfunkproviders ist somit eine ideale, massenmarkttaugliche Diensterbringung möglich. Die Abrechnung der Dienstleistung kann über die Mobilfunkrechnung erfolgen. Der Mobilfunkprovider übernimmt somit in vielen Fällen die technische Umsetzung des Dienstes im eigenen Netzwerk, wie auch die Abrechnung der Dienstleistungsnutzung z.B. über die monatliche Rechnung des bereits bestehenden Vertragsverhältnisses.

Auf der anderen Seite besitzt dieses Vorgehen jedoch auch den Nachteil, dass der Mobilfunkprovider entscheiden kann, welche Dienste von welchen Unternehmen er seinen Kunden anbietet. Dies führt dazu, dass es zu einem bestimmten Zeitpunkt für einen bestimmten Dienst nicht mehrere Anbieter gibt, die sich in einem Wettbewerb befinden. Daher ist es für den Kunden nicht möglich, sich einen Dienstanbieter zu suchen, der einen Dienst bereitstellt, der günstiger als andere Anbieter ist oder bestimmte Eigenschaften aufweist. Zusätzlich werden vom Provider nur Dienste ausgewählt, die große Umsatzzahlen und somit großen Gewinn versprechen. Anwendungen, die auf spezielle Unternehmen oder eng begrenzte Personengruppen zugeschnitten sind, werden wegen fehlender Gewinnerwartung nicht realisiert.

.

2. Anforderungsanalyse

Zur Erstellung einer Anforderungsanalyse wird zu Beginn der aktuelle Stand des Marktes und der Forschung betrachtet (Ist-Zustand). Basierend auf dieser Ausgangsposition wird im zweiten Schritt der Soll-Zustand definiert.

2.1 Ist-Zustand

Heutige mobile Dienste werden primär im Mobilfunkbereich angeboten. Dabei handelt es sich hauptsächlich um für den Massenmarkt angepasste Informationsdienste. Die zur Diensterbringung benötigten Informationen existieren bereits z.B. in Form von Nachrichten in einer Datenbank oder müssen unter Berücksichtigung von Kontextinformationen berechnet werden. Falls es sich um personenbezogene Kontextinformationen handelt, so werden sie manuell vom Benutzer bereitgestellt. Dies kann beispielsweise dadurch erfolgen, dass der Dienst sie per SMS vom Benutzer anfragt und die notwendigen Informationen der Anforderungs-SMS angefügt werden. Eine derartige Vorgehensweise ist besonders deshalb umständlich, da der Benutzer im Vorfeld die Syntax des Dienstaufrufs kennen muss. Je nach Situation sind die von ihm bereit zu stellenden Informationen auch nur sehr ungenau, z.B. die zu hinterlegende Postleitzahl für den Aufruf eines Informationsdienstes muss bekannt sein. Nur wenige Informationsdienste benötigen zum jetzigen Zeitpunkt Kontextinformationen vom Benutzer. Dies führt dazu, dass Dienste ohne Kontextinformationen keinen Grad an Personalisierung bereitstellen. Die Gruppe von Diensten mit dem höchsten Grad an Personalisierung sind ortsbezogene Dienste. Die Ortsinformationen werden zumeist per Cell-ID des Mobilfunkproviders oder durch eine manuelle Angabe des Benutzers bereitgestellt. Diese Art von Diensten kann von allen im Umlauf befindlichen Endgeräten angefordert werden, da keine besonderen Eigenschaften des Endgerätes benötigt werden (wie z.B. vorhandener GPS-Empfänger). Die Dienste nutzen SMS, MMS oder WAP als Medium zur Dienstbereitstellung. Diese Ansätze besitzen jedoch nur sehr beschränkte Tauglichkeit im Bereich der Visualisierung und Interaktion. Ihre Komplexität ist nicht vergleichbar mit Diensten im Internet. Visualisierung und der Umfang der Interaktion sind eingeschränkt.

2.2 Aktueller Stand im Bereich LBS

Da ortsbezogene Dienste zurzeit den höchsten Grad an Personalisierung durch die Integration von persönlichen Kontextinformationen des Benutzers ermöglichen, wird diese Gruppe näher betrachtet:

Ortsbezogene Informationsdienste
Bei diesen Diensten werden, abhängig von der Position des Benutzers, Informationen zu einem vorher definierten Thema oder einer Kategorie bereitgestellt. Dies können z.B. Adressen von Hotels, Restaurants, Tankstellen oder Geldautomaten sein. Der Benutzer erhält nach der Abfrage oft mehrere Treffer zugesendet. Die genauen Adressen und die Entfernungen von der jetzigen Position sind angegeben.

Navigationsdienste

Mit Hilfe von Navigationsdiensten kann der Benutzer eine Wegbeschreibung von seiner aktuellen Position zu einem vorher festgelegten Ort erhalten. Je nach System werden ihm während der Fahrt weitere detaillierte Informationen zur Strecke gegeben. Durch die Verknüpfung mit zusätzlichen Datensätzen (z.B. Daten aus einer Staudatenbank) lässt sich während der Fahrt die Streckenführung so anpassen, dass der Fahrer nicht in einen Stau gerät.

Flottenmanagement

Im gewerblichen Umfeld werden Flottenmanagement-Systeme (Vehicle Tracking Services) als Location-based Service angeboten. Mit diesem Dienst haben Fuhrunternehmer die Möglichkeit, die Positionen ihrer Lastkraftwagen oder die bestimmter Ladungen zu ermitteln. Diese Informationen können dazu verwendet werden, um eine optimale Auslastung der vorhandenen Fahrzeuge zu erreichen.

Positionsermittlung von Handys, Kindern usw.

Die Position des Mobiltelefons kann auch dazu verwendet werden, um z.B. den Aufenthaltsort von Kindern zu bestimmen. Es handelt sich dabei um sogenannte „Phonetracker-Dienste“. Die Dienste können durch die Eltern genutzt werden. Ein weiterer „Phonetracker-Dienst“ nennt sich „Handyfinder[1]“ und wird von o2 angeboten. Er ermöglicht es dem Benutzer, sein Mobilfunktelefon zu finden, falls er dieses verlegt hat. Der Kunde kann über eine Webseite des Mobilfunkbetreibers das Telefon suchen lassen. Das Ergebnis wird auf einer Karte angezeigt. Zur Ermittlung der Position muss das Telefon allerdings angeschaltet sein, da andernfalls nur die letzte Position dem Mobilfunkprovider bekannt ist, bei der das Gerät verwendet worden ist.

Notrufsysteme

Ein ständig wachsender Anteil der Notrufe trifft heutzutage bereits von Mobilfunktelefonen ein. Diese Anschlüsse besitzen den Nachteil, dass die Rettungszentrale nicht anhand der Telefonnummer und der damit hinterlegten Adresse ermitteln kann, wo sich der Anschlussinhaber befindet. Bei vielen Notfällen ist die Reaktionszeit ein entscheidender Faktor. Deshalb muss auch bei mobilen Endgeräten gewährleistet sein, dass diese Geräte im Notfall schnell lokalisiert werden können. Dies ist deshalb notwendig, da z.B. der Anrufer oft nicht genau weiß, wo er sich im Moment befindet. Um den Rettungszentralen die Positionsinformation bereitzustellen, wird bereits in Amerika (E-911) und Europa (E-112) ein Standard entwickelt, der auf die Anforderungen dieses Falles angepasst ist und zukünftig zum Einsatz kommen soll. [FCC05], [EUP02]

[1] O2 Handy Finder: http://www.o2online.de/nw/meino2/profil/handyfinder/index.html

Steuerung von Servicefunktionen des Telekommunikationsnetzes

Im Telekommunikationsnetz eines Mobilfunkproviders kann die Position des Endgerätes bei der Abrechnung oder Erbringung von Diensten berücksichtigt werden. Dies ist zum Beispiel der Fall, wenn dem Benutzer eine deutschlandweit einheitliche Rufnummer angeboten wird, um z.B. eine Notrufstelle zu erreichen oder ein Taxi zu bestellen. In diesem Fall wird der Benutzer abhängig von seiner Position mit der nächsten zuständigen Zentrale verbunden. Viele Mobilfunkprovider bieten mittlerweile auch spezielle Tarife an, die abhängig von dem Standort die ein- und ausgehenden Gespräche abrechnen. Ein Beispiel für einen derartigen Tarif ist Genion von o2[2]. Bei diesem Tarif erhält der Kunde neben der Mobilfunk- auch eine Festnetzrufnummer. Dazu wird jedem Kunden eine persönliche Homezone eingerichtet. Bei dieser Homezone handelt es sich um ein Gebiet (meistens die Wohn- oder Arbeitsanschrift), in dem vergünstigte Tarife gelten. Eingehende Gespräche auf der Mobilfunkrufnummer sind innerhalb von Deutschland durchgehend kostenlos. Telefonate auf die Festnetzrufnummer sind nur solange kostenfrei, wie sich der Benutzer beim Annehmen des Anrufes innerhalb seiner Homezone befindet. Möchte der Benutzer Telefonate führen, so werden innerhalb der Homezone vergünstigte Tarife angeboten.

Friend-Finder

Bei einem Friend-Finder-Dienst kann es sich je nach Realisierung um einen komplexen ortsbezogenen Dienst handeln. Diese Dienste zeigen dem Benutzer seine Freunde oder Kollegen an, die sich in seiner Nähe befinden. Die Personen, die bei diesem Dienst angezeigt werden, müssen ebenfalls den Dienst verwenden und aktiv ihrer Lokalisierung zugestimmt haben. Spontane Verabredungen sind so leicht möglich. Eine andere Variante sind Dating-Dienste. Leute mit gleichen Interessen sind in einer Datenbank festgehalten. Mit Hilfe von aktuellen Standortangaben lassen sich interessante Personen in der Nähe finden. Eine Ausprägung derartiger Dienste bietet z.B. der Anbieter Mobiloco[3].

2.3 Location-based Supply Chain

Je nach Komplexität der angebotenen Dienstleistung kann diese nicht mehr von einem einzigen Dienstleister bereitgestellt werden. In diesem Fall werden Vorleistungen, z.B. für den Dienst notwendige Informationen oder Logikbestandteile, bei der Dienstleistungserbringung integriert. Diese Bestandteile können über Webservice-Schnittstellen von den beteiligten Unternehmen abgefragt werden. In diesem Fall bilden die am Location-based Supply Chain beteiligten Unternehmen eine virtuelle Organisation [BGS07], um die Dienstleistung in ihrer gesamten Komplexität bereitstellen zu können..

Die verschiedenen Instanzen in Form der unterschiedlich spezialisierten Unternehmen, die an der Erbringung von fortschrittlichen Location-based Services beteiligt sind, bilden das Location-based Supply Chain (LBS Supply Chain) (siehe Abbildung 1).
Fortschrittliche Location-based Services sind wesentlich komplexer, als dies bei aktuell vorhandenen LBS-Diensten der Fall ist. In einem LBS Supply-Chain kann eine Instanz mehrere Aufgaben wahrnehmen.

[2] O2 Genion: http://shop2.o2online.de/nw/produkte/tarife/genionsml/easys/pageframe.html
[3] Mobiloco: http://www.mobiloco.de/

Es kann generell aus folgenden Instanzen bestehen [Kü05]:

- Ziel (*Target*)
- Positionsermittler (*Position Originator*)
- Location Provider
- LBS Provider
- Content Provider
- Benutzer (*LBS user*)

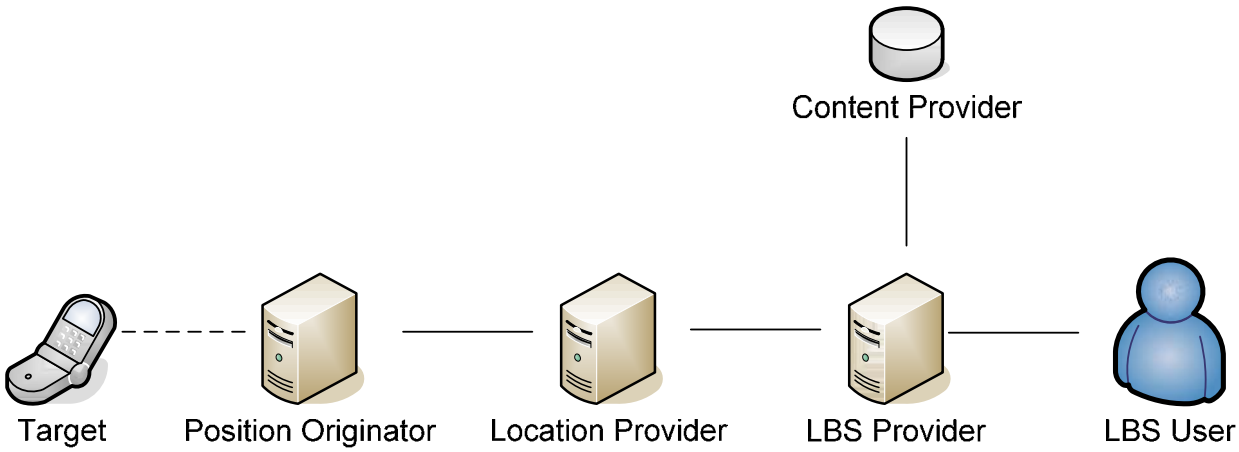


Abbildung 1 - Location-based Supply Chain (angelehnt an [Kü05])

Ziel (*Target*)
Bei einem Ziel handelt es sich um ein Objekt oder eine Person, deren Position festgestellt werden soll. Diese Positionsinformation bildet die Grundlage für den später zu erbringenden Dienst. Um die Position des Ziels ermitteln zu können, muss das dazugehörige Endgerät oder das Kommunikationsnetz, das eingesetzt wird, Mechanismen bereithalten, die eine Positionsbestimmung ermöglichen.

Positionsermittler (*Position Orginiator*)
Der Positionsermittler ist die erste Stelle innerhalb des LBS Supply Chains, dem die Position des Ziels bekannt ist. Je nach verwendeter Positionierungstechnik wurde die Position durch das Endgerät (Terminal-based) oder das Kommunikationsnetzwerk (Network-based) ermittelt. Zusätzlich besteht die Möglichkeit, dass sich durch eine Kombination der Positionsdaten aus dem Endgerät und Netzwerk eine genauere Positionsinformation berechnen lässt. (Terminal-assisted bzw. Network-assisted). Der Positionsermittler kann sich somit:

- auf der Seite des Ziels im Endgerät befinden.
- auf der Seite des Providers befinden, falls das Kommunikationsnetzwerk für die Positionierung verwendet wird.

Falls eine autarke Infrastruktur zum Einsatz kommt, kann die Positionsermittlung auch als eine eigenständige Instanz realisiert sein.

Location Provider
Bei dem Location Provider handelt es sich um einen Vermittler zwischen dem Positionsermittler (Position Originator) und dem LBS Provider. Der Location Provider ermittelt und kontrolliert für die Zeit der Dienstnutzung die Position der Ziele für den LBS Provider. Der LBS Provider erhält die Positionsangaben fortlaufend innerhalb bestimmter Zeitintervalle. Falls es gewünscht wird, werden unabhängig von der Zeit die Positionsveränderungen mitgeteilt.

LBS Provider
Die wichtigste Aufgabe innerhalb des LBS Supply Chains besitzt der LBS Provider. Dieser realisiert den eigentlichen Dienst. Der LBS Provider besitzt die eigentliche Logik, die für die Erbringung der Dienstleistung notwendig ist. Er verwendet die Positionsinformationen der Endgeräte, die zu diesem Zeitpunkt einen Dienst nutzen. Die Positionsinformationen der Benutzer kombiniert der LBS Provider mit weiteren Informationen und erstellt dadurch höherwertigere Daten, die den eigentlichen Dienst darstellen. Diese Daten werden dem Benutzer, der die Dienstleistung angefragt hat, beispielsweise auf seinem Endgerät präsentiert.

Content Provider
Die Content Provider unterstützen den LBS Provider bei der Diensterbringung, indem sie ihm Inhalte liefern, die für die Erstellung der Dienstleistung benötigt werden. Bei diesen Inhalten kann es sich um aktuelle Informationen wie z.B. Börsenwerte, Wetterdaten und Nachrichten handeln. Für Location-based Services sind jedoch ortsbezogene Informationen von größerer Bedeutung, wie z.B. Kartendaten und POI (Point of Interests)-Datensätze. Diese Daten ermöglichen beispielsweise die Bereitstellung von Routenplanungsdiensten.

Benutzer (*LBS User*)
Der Benutzer fragt beim LBS Provider die Dienstleistung an. Je nach Dienstleistung kann der Benutzer (LBS User) mit dem Ziel (Target) übereinstimmen. Dies wäre beispielsweise bei einem Touristeninformationsdienst der Fall.

2.4 Bereitstellung von ortsbezogenen Diensten im Mobilfunknetz

Heutige Location-based Services können vom Mobilfunkprovider und auch von externen Unternehmen angeboten werden. Diese Unternehmen besitzen die Möglichkeit, auf die Infrastruktur des Mobilfunkproviders, im Beispiel bei o2 über einen „Competence Partner“, zuzugreifen [o207]. Die „Competence Partner“ wiederum können Bereiche des Providers abfragen und über die Datenbank die Positionsdaten der Endgeräte ermitteln, die den Dienst nutzen. Damit dies möglich ist, müssen jedoch die Benutzer der Nutzung von ortsbezogenen Diensten zugestimmt haben. Je nach „Competence Partner“ hat dieser Zugang zu mehreren Mobilfunknetzen. Somit kann dieser Dienst in unterschiedlichen Mobilfunknetzen angeboten werden. Andernfalls ist es notwendig, dass der Dienstanbieter seine Anwendung über mehrere „Compentence Partner“ anbietet. Um den Schutz der sensiblen Daten sicherzustellen, werden alle Dienste vom „Competence Partner“ geprüft und auf den eigenen Servern betrieben. Somit ist sichergestellt, dass sensible Positionsinformationen nicht an Dritte gelangen. Neben der Positionsermittlung und dem Hosting bieten viele Dienstanbieter auch noch weitere

Dienstleistungen an. Dies könnten z.B. Kartendarstellung, Routenplanfunktion, Gateways um SMS und MMS zu versenden, sein. Sie können somit die Funktionen einiger Instanzen des LBS Supply-Chain bereitstellen. Die Kosten für die Ermittlung einer Endgerätepositon durch einen „Competence Partner“ ist sehr kostenintensiv. So kostet eine einmalige Funkzellenabfrage zwischen 0,09 und 0,16 Euro (je nach Anzahl der Anfragen pro Rechnungszeitraum). Das Erstellen einer Kartenansicht mit Wegbeschreibung zwischen 0,015 und 0,03 Euro [ME05]. Anhand dieser Preise sieht man, dass zum jetzigen Zeitpunkt primär nur einfache ortsbezogene Informationsdienste angeboten werden können, da diese auf nur einer einmaligen Positionsermittlung basieren und dadurch die entstehenden Kosten gering gehalten werden. Fortschrittliche ortsbezogene Dienste müssen im Intervall die Position des Benutzers neu ermitteln. Bei den heutigen Preisen würde eine derartige Anwendung jedoch zu kostenintensiv. Dies würde dazu führen, dass ein derartiger Dienst nicht vom Markt akzeptiert wird. Zu beachten ist auch, dass entgegen dem Trend im Mobilfunkmarkt, die Preise für die Positionsermittlung seit 2 Jahren gleich geblieben sind [ME05]. Um fortschrittliche ortsbezogene Dienste anbieten zu können, die auf eine mehrmalige Positionsermittlung angewiesen sind, müssen diese Kosten reduziert werden oder die Lokalisierung muss z.B. durch das Endgerät des Benutzers oder eine kostengünstigere Infrastruktur realisiert werden.

2.5 Mobiles Internet

Eine Entwicklung, die seit 2008 vermehrt von den Kunden angenommen wird, ist das „mobile Internet“. Aufgrund von günstigeren Datentarifen ist es auch für Privatpersonen erschwinglich geworden, Datendienste im Mobilfunknetz zu verwenden. Beim „mobilen Internet“ handelt es sich um einen vollständigen Zugang zum Internet. Vorherige Zugänge waren oft auf WAP-Seiten oder die jeweiligen Portale der Provider begrenzt gewesen. Es besteht hierbei auch die Möglichkeit, Seiten und Dienste zu verwenden, die nicht speziell für mobile Benutzer entwickelt worden sind. Benutzer, die einen derartigen Zugang nutzen möchten, benötigen ein Endgerät, das auch normale Webseiten darstellen kann. Zusätzlich können auch weiterhin WAP-Inhalte abgerufen werden. Ein Problem dieser Dienste ist es, dass viele Seiten für die Nutzung auf normalen Computern konzipiert worden sind. Dies bedeutet, dass ein Seitenaufbau sehr zeitintensiv ist. Die Seite ist dabei oft um ein Mehrfaches größer als die nutzbare Fläche des Displays beim mobilen Endgerät, so dass der Benutzer sich auf Einschränkungen bei der Darstellung einstellen muss. Das zu übermittelnde Datenvolumen ist dazu auch nicht für das mobile Umfeld optimiert worden, so dass der Abruf einer derartigen Seite je nach Datentarif zu hohen Kosten führen kann.
Dienste, die im Internet besonders für die mobilen Endgeräte bereitgestellt werden, besitzen zumeist nicht die oben genannten Einschränkungen. Problematisch sind jedoch Dienste, die kostenpflichtig sind. Im mobilen Internet tritt der Mobilfunkprovider nur als Datenprovider auf. Er kann somit bei diesen Diensten nicht die Abrechnung übernehmen. Der Benutzer muss daher für jeden verwendeten Dienst z.B. ein Account erstellen und die notwendigen Zahlungsdaten hinterlegen und ggf. vorab ausreichend Guthaben bereitstellen. Dieses Vorgehen ist jedoch sehr zeitraubend und erlaubt keine spontane Nutzung der Dienste. Zusätzlich entstehen so sehr viele Geschäftsverhältnisse, bei denen personenbezogene Informationen bekannt gegeben werden müssen.

2.6 Bestehende Probleme beim Angebot von fortschrittlichen mobilen Diensten

Zum jetzigen Zeitpunkt ist das Bereitstellen von fortschrittlichen mobilen Diensten ein komplexer Vorgang. Die folgenden Probleme behindern die Entwicklung oder führen zu einem Akzeptanzproblem beim Benutzer:

Vorhandene Endgeräte auf dem Markt

Die auf dem Markt befindlichen und somit von den Benutzern eingesetzten Endgeräte haben sehr unterschiedliche Eigenschaften. Alle Geräte besitzen die gemeinsamen Fähigkeiten, Telefonate zu führen und Kurznachrichten zu versenden. Alle weiteren Funktionen sind auf unterschiedlichste Weise realisiert. Die für den Bereich der mobilen Dienste notwendigen Funktionen wie z.B. Anbindung, Displaygröße, Rechenleistung, der für Anwendungen verfügbare Speicher sowie die Möglichkeit, neben dem Zugriff per WAP oder mobilem Internet auch Anwendungen auf dem Endgerät ausführen zu können, sind je nach Gerät in unterschiedlicher Ausprägung vorhanden. Diese Heterogenität der Endgeräte führt dazu, dass bei der Entwicklung von mobilen Diensten sehr viele Endgeräte auf Kompatibilität geprüft werden müssen, bevor ein Dienst Marktreife erlangt. Durch die Verwendung von herstellerspezifischen Schnittstellen ist zusätzlich der Zugriff auf bestimmte Funktionen der Geräte nicht einheitlich möglich. Dies erhöht die Kosten bei der Entwicklung sehr stark. Um einen großen Markt ansprechen zu können, müssen Funktionen verwendet werden, die bei den meisten Endgeräten vorhanden sind. Dadurch werden die Leistungsmöglichkeiten der einzelnen Geräte nicht ausgeschöpft.

Qualität der Kontextdaten

Die bei der Diensterbringung verwendeten Kontextdaten werden in den meisten Fällen manuell von Benutzern oder durch den Mobilfunkprovider gestellt. Diese Informationen besitzen nur eine begrenzte Genauigkeit. Die Genauigkeit ist durch die Fehlerfreiheit der manuell vom Benutzer hinterlegten Informationen oder bei Positionsinformationen durch die Zellgröße vorgegeben. Da vom Benutzer nur eine begrenzte Menge an Informationen abgefragt werden kann, schränkt dies den Umfang der realisierbaren Dienste ein. Die Freigabe der Kontextinformationen erfolgt zum jetzigen Zeitpunkt per SMS-Kommandos oder bei WAP-Nutzung über einen Dialog bei der Dienstnutzung. Der Benutzer besitzt nach diesem Vorgang jedoch keine Möglichkeit, an einem zentralen Punkt abzufragen, welchen Diensten er den Zugriff auf die Kontextinformationen erlaubt hat.

Schutz der Privatsphäre (Positionsinformationen)

Damit Dienste, die regelmäßig verwendet werden, Zugriff zu den Positionsinformationen des Endgerätes erhalten, muss der Benutzer dies im Vorfeld erlauben. Das wird im Folgenden am Beispiel des Dienstes „*trackyourhandy*“ [TYH08] gezeigt. Der Benutzer hat bei diesem Dienst die Möglichkeit, sein Handy auffinden zu lassen, wenn er es beispielsweise verlegt hat. Vor dem Verlust muss er dazu den Dienst aktiviert haben. Die Abbildung 2 und 3 zeigt die notwendigen Schritte zur Aktivierung.

Um trackyourhandy zu aktivieren, muss der Benutzer eine SMS von dem zu ortenden Handy mit dem Text: `LBS TYK ON` an die Kurzwahlnummer `72927` senden.

Im nächsten Schritt muss eine zweite SMS von dem zu ortenden Handy mit dem Text: `+LBS2WEB` an die Kurzwahlnummer `27637` gesendet werden.

Abbildung 2 und 3 - Aktiveren eines ortsbezogenen Dienstes per SMS am Beispiel „trackyourhandy“ [THY08]

Der Benutzer muss sich bei einer Dienstnutzung bereits im Vorfeld über die Aktivierung des Dienstes informieren. Diese Informationen kann er vornehmlich aus dem Internet erhalten. Dies führt zum heutigen Zeitpunkt oft zu einem Medienbruch. Die Kommandos zur Aktivierung sind in diesem Zusammenhang oft sehr kryptisch. Wenn der Benutzer mehrere Dienste auf diese Art aktiviert, muss er nach dem Nutzungszeitraum die Dienste wieder deaktivieren. Dazu muss er sich jedoch selbst merken, welche Dienste Zugriff auf die sensiblen Daten haben und wie er diese deaktivieren kann. Die fehlende Transparenz kann dazu führen, dass Dienste weiterhin Zugriff auf sensible Daten haben, die eigentlich nicht mehr genutzt werden. Falls Dritte Zugriff auf die notwendigen Zugangsdaten erhalten, besitzen sie die Möglichkeit, beispielsweise den Standort des Benutzers zu ermitteln und diesen für ihre Zwecke zu verwenden. Um das Sicherheitsrisiko durch Dritte zu reduzieren, wird in Deutschland der Benutzer über einen Trackingvorgang per SMS informiert.

Kosten

In Mobilfunknetzen entstehen bei der Dienstnutzung dem Benutzer bei fast allen Diensten Kosten. Diese Kosten sind je nach Anbieter und Dienst nicht transparent. So kann es dazu kommen, dass der Benutzer einen Abovertrag eingeht, wobei er nur an einer einmaligen Dienstnutzung interessiert war. Die laufenden Aboverträge kann er seiner monatlichen Rechnung entnehmen. Die Beendigung der Abos erfolgt in den meisten Fällen über einen Code, den man per SMS an den jeweiligen Dienstbetreiber senden muss. Der Mobilfunkprovider ermöglicht eine Abrechnung der in Anspruch genommenen mobilen Dienste. Dienste, die kostenpflichtig im (mobilen) Internet verfügbar sind, können über diesen Weg jedoch nicht abgerechnet werden.

Auffinden der Dienste

Damit ein Benutzer einen Dienst verwenden kann, muss er wissen, wie er die Dienstleistung abrufen kann. Jedem Dienst ist eine spezielle Rufnummer oder Adresse zugewiesen. Verwendet ein Dienst eine spezielle Rufnummer, so muss der Benutzer sich im Vorfeld informieren, damit er die richtige Nummer zum Zeitpunkt der Dienstnutzung besitzt. Rufnummern von Diensten, die vom Provider angeboten werden, speichert der Provider oft auf der bereitgestellten SIM-Karte oder beschreibt diese Dienste in einem speziellen Informationsheft, das der Kunde beim Vertragsabschluss erhält. Dienste von Dritten hingegen müssen über Werbung bekannt gemacht werden. Verwendet ein Dienst WAP zur Diensterbringung, so besteht die Möglichkeit, dass der Dienst über das Betreiberportal aufgefunden werden kann. Je nach Dienst existiert dieses nur im Netz eines Providers. Oder Dienstzugänge werden unter den gleichen oder je nach Netz unterschiedlichen Nummern bereitgestellt. Der Provider kann in diesem Zusammenhang auch entscheiden, welche Dienste

in seinem Netz angeboten werden. Diese beherrschende Position des Providers führt dazu, dass die Bereitstellung sehr kostenintensiv ist. Eine Bereitstellung von Diensten für einen kleinen Personenkreis, wie dies beispielsweise im Internet möglich ist, ist im Mobilfunknetz nicht wirtschaftlich realisierbar.

Nutzung von Diensten im Ausland

Durch die vielfältigen Roaming-Abkommen der Provider können Benutzer auch im Ausland in Fremdnetzen Dienste verwenden. Die dabei entstehenden Kosten für die Dienstnutzung oder den Datentransfer unterscheiden sich je nach Netz und Land stark von den Gebühren, die im eigenen Netz anfallen würden. Abgeschlossene Flatrates oder Tarifpakete greifen bei ausländischen Netzen nicht. Über die entstehenden Kosten muss der Benutzer sich im Vorfeld selbst erkundigen. Da Dienste meistens nur von einer begrenzten Anzahl von Providern angeboten werden, können bekannte Dienste oft im Ausland nicht verwendet werden. Besonders im Bereich der ortsbezogenen Dienste sind diese meistens für das jeweilige Land konzipiert. Je nach Provider besteht für den Dienstanbieter auch keine Möglichkeit der Positionsfeststellung im Fremdnetzwerk. Der Benutzer muss sich im Fremdnetz informieren, welche Dienste angeboten werden. Diese werden zumeist in der jeweiligen Landessprache angeboten, was für den Benutzer zu Problemen führen kann, falls er diese Sprache nicht beherrscht. Der Benutzer muss sich im Ausland auch der Tatsache bewusst sein, dass die jeweilige Rechtsprechung des Landes bei der Diensterbringung berücksichtigt wird. Die Verarbeitung von sensiblen Informationen, wie z.B. Positionsinformationen, besitzt je nach Dienst nicht den gewohnten Sicherheitsstandard.

2.7 Fragestellung des Forschungsgebietes

Unter Berücksichtigung der Einschränkungen, die bei der Nutzung von Diensten im Mobilfunknetz existieren und der offensichtlichen Möglichkeiten, die durch die Verwendung des „mobilen Internets“ bestehen, existiert ein noch nicht genutztes Potenzial für den Benutzer. Um dieses zu heben, muss eine Architektur erstellt werden, die die vorhandenen Eigenschaften auch den Diensten des „mobilen Internets“ zur Verfügung stellt. Eine besondere Herausforderung bedeutet die Realisierung von kontextbezogenen Diensten. Sie werden in dieser Arbeit vornehmlich in Form von aufgewerteten ortsbezogenen Diensten dargestellt, da die Positionsinformation des Benutzers zu den sensibelsten Informationen zählt und dazu noch mit aufwendigen Methoden bereitgestellt werden muss. Da für die Bereitstellung dieser Art von komplexen Diensten mehreren Instanzen Teilaufgaben zukommen, (siehe LBS Supply Chain – Kapitel 2.3) besitzt dieser Bereich besondere Brisanz was den Schutz der Privatsphäre des Benutzers betrifft. Die Brisanz entsteht durch den Antagonismus zwischen den Interessen des Dienstanbieters und denen der Benutzer. Die Benutzer sind daran interessiert, keine sensiblen Daten über sich preiszugeben; der Dienstanbieter dagegen benötigt jedoch hochgradig sensible Informationen, wie die Position des Benutzers, für die eigentliche Erbringung des kontextbezogenen Dienstes.

Zukünftige mobile Dienste sollen nicht mehr durch die Begrenzung eines Mobilfunknetzes festgelegt werden, da die Benutzer auch andere Netzwerke für den Zugang zum Internet verwenden können. Das bedeutet, dass die Mobilfunkprovider keine Monopolstellung mehr besitzen und daher nicht allein bestimmen können, welche Dienste dem Benutzer bereitgestellt werden. Da ein Benutzer neben dem Mobilfunknetz auch andere Technologien besitzt, um auf das Internet zuzugreifen, sollen die Mobilfunknetze nur als Netzwerke zur Datenkommunikation verwendet werden. Durch den Wegfall spezieller Aufgaben, die der

Mobilfunkprovider bei aktuellen Diensten bereitgestellt hat, muss das Supply Chain um weitere Instanzen erweitert werden. Diese haben die Aufgabe, den Schutz der Privatsphäre, die Lokalisierung und zum Beispiel das Billing zu realisieren.

Bei der somit neugeschaffenen Architektur muss der Widerspruch zwischen den Interessen der Dienstanbieter und der Benutzer entschärft werden. Jedem Glied eines „Supply Chain" darf nur so viel Zugriff auf sensible Informationen zugestanden werden, wie unbedingt benötigt wird. Die Identität des Benutzers darf nur in den Fällen dem Dienst bekannt gegeben werden, bei denen sie in die Dienstnutzung einfließt. Die Einschränkungen, die zum jetzigen Zeitpunkt noch existieren, wie die Intransparenz der vergebenen Zugriffsrechte auf die sensiblen Informationen, die bei der Dienstnutzung anfallenden Kosten und die Auswahl von vorhandenen Diensten, müssen in der zukünftigen Architektur behoben sein. Der Benutzer muss die Möglichkeit besitzen, frei festzulegen, welche Daten er über sich preisgibt. In der Architektur muss eine Instanz für die Umsetzung dieser vom Benutzer festgelegten Regeln bereitstehen.
Die Architektur muss zudem in der Lage sein, mehrere Endgeräte zuzulassen, die unterschiedliche technische Voraussetzungen mitbringen. Bei einer Nutzung im Ausland sollen dem Benutzer die gleichen Möglichkeiten wie zuhause zur Verfügung stehen. Über die Kosten, die bei der Nutzung entstehen, wird er im Voraus informiert.

Meine Arbeit beschreibt einen theoretischen Lösungsvorschlag für eine derartige Architektur. Dieser wird im Laufe des Forschungsvorhabens unter Verwendung des Forschungsansatzes des Design Researchs [SP02, VK06] prototypisch umgesetzt. Der entwickelte Prototyp wird evaluiert und die Informationen fließen im nächsten Schritt in die Spezifikation der Instanzen ein.

Die folgenden Forschungsfragen werden im Rahmen dieses Forschungsvorhabens behandelt:

- Welche Veränderungen sind im Bereich der mobilen Dienste, Endgeräte und Netzwerke zu erwarten? Welche Auswirkungen haben diese Änderungen für den Bereich der mobilen Dienstleistungen? Zu welchen Problemen oder Herausforderungen führen diese?

- Wie kann eine Architektur für komplexe kontextbezogene Dienste im mobilen Umfeld aussehen, die bereits die zukünftigen Veränderungen berücksichtigt? Wie kann diese Architektur konzeptioniert werden, damit die Privatsphäre der Benutzer geschützt wird? Wie kann ein Zugriff auf sensible Kontextinformationen realisiert werden, um eine Diensterbringung von komplexen kontextbezogenen Diensten zu ermöglichen? Wie kann eine derartige Architektur gestaltet werden, damit zukünftige Veränderungen in einer generischen Form integriert werden können?

- Wie kann eine derartige Architektur eine Basis für Dienste im wirtschaftlichen Umfeld bilden, die eine offene Bereitstellung von weiteren Diensten durch Dritte ermöglicht, ohne dass der Netzwerk-Provider im Vorfeld den Anbieterkreis oder die Art der Dienstleistung beeinflussen kann.

- Ist die Struktur des heutigen „Location-based Supply Chain" (siehe Kapitel 2.3) bereits ausreichend für die Realisierung einer derartigen Architektur? Gibt es Aufgabenbereiche, die durch zusätzliche Instanzen abgedeckt werden müssen?

2.8 Zukünftige Dienste

Mobile Dienste stellen zukünftig eine Haupteinnahmequelle für die Provider und Dienstanbieter dar, da Grunddienste wie z.B. Telefonie und Datenkommunikation in Form von Tarifpaketen und Flatrates keine Möglichkeit zur Umsatzsteigerung mehr eröffnen. Durch den steigenden Wettbewerb fallen dazu noch die Preise für die Grunddienste, so dass die Dienstanbieter weitere Einnahmequellen schaffen müssen. Bei den heutigen Diensten handelt es sich um Pull-Dienste. Bei dieser Variante fragt der Benutzer aktiv eine Dienstleistung ab. Dies kann per Sprache, Kurznachricht oder WAP geschehen. Bei heutigen kontextbezogenen Diensten muss der Benutzer noch je nach Dienst oft manuell Kontextinformationen bereitstellen. Diese Dienste sind für den Massenmarkt entwickelt, bieten aber keine ausreichende Möglichkeit zur Personalisierung. Die Personalisierung jedoch gestattet es, zukünftige Dienste speziell an die Anforderungen des Benutzers anzupassen. Sie ermöglicht eine einfachere Nutzung, trägt zur Zeiteinsparung bei und fördert eine höhere Kundenzufriedenheit. Derartige Dienste benötigen jedoch mehr Kontextinformationen als die heutigen, um eine ausreichende Personalisierung zu ermöglichen. Neben den Pull-Diensten müssen auch Push-Dienste möglich sein. Bei diesen fragt nicht der Benutzer die eigentliche Dienstleistung ab, wenn er z.B. Informationen haben möchte, sondern er aktiviert einen Dienst und bekommt aktiv vom Server die Daten bereitgestellt, wenn neue Informationen verfügbar sind. Derartige Dienste müssen durchgehend über die Situation des Benutzers informiert sein und reagieren auf unterschiedliche Ereignisse. Sie senden dem Benutzer die benötigten Informationen oder stellen erforderliche Leistungen bereit. Durch den durchgehenden Zugriff auf sensible Daten besitzen sie ein höheres Risikopotenzial als Pull-Dienste. Daher muss der Benutzer die Möglichkeit besitzen, entscheiden zu können, welchen Dienstanbietern er vertrauen kann.

3. Soll-Konzeption

Eine Architektur, die fortschrittliche kontextbezogene Dienste unterstützen soll, muss bereits zu Beginn den Wandel im mobilen Sektor betrachten. Basierend auf den zukünftigen Anforderungen der Dienste, der Benutzer und Dienstleistungsakteure, erhält diese Architektur eine wesentlich höhere Komplexität, als durch das heutige Location-based Supply Chain (siehe Kapitel 2.3) ersichtlich wird. Zur Erstellung einer Architektur für fortschrittliche kontextbezogene Dienste müssen die folgenden Punkte berücksichtigt werden:

- Bei den heutigen ortsbezogenen Diensten, als eine Ausprägung der kontextbezogenen Dienste, handelt es sich zumeist um nur einfache Informationsdienste. Zukünftige Dienste benötigen zur Realisierung von komplexen Dienstleistungen eine Vielzahl von Informationen vom Benutzer und von weiteren beteiligten Instanzen. Bei den Instanzen kann es sich beispielsweise um Dienstleister handeln, die Kartendaten, Nachrichten oder weitere Programmbestandteile bereitstellen. Da bei diesen Diensten eine größere Anzahl von sensiblen Kontextinformationen zur Dienstleistungserbringung benötigt wird, die Lokalisierungsinformationen eine sehr hohe Genauigkeit aufweisen und die Anzahl der beteiligten Instanzen zur Diensterbringung steigt, müssen besonders die Sicherheit und der Schutz der Privatsphäre schon bei der Konzipierung der Architektur berücksichtigt werden

- Da diese Architektur die Basis für fortschrittliche kontextsensitive Anwendungen und Dienste bereitstellt, muss bereits bei der Konzipierung berücksichtigt werden, dass die Bearbeitung von sensiblen Daten nur in einer vertrauenswürdigen Umgebung stattfinden darf. Dazu sollten nur die Instanzen die minimale Menge an sensible Informationen erhalten, die diese für die eigentliche Diensterbringung benötigen. Nach Möglichkeit sollte die Identität des Benutzers weitgehend anonym bleiben, um mögliche personenbezogene Datensammlungen zu unterbinden.

- Die zukünftigen kontextbezogenen Dienste, hier im besonderen Fall Dienste mit Ortsbezug, werden primär für mobile Endgeräte entwickelt. Bei dieser Betrachtung muss jedoch berücksichtigt werden, dass nicht nur Geräte, die das Mobilfunknetzwerk nutzen, als mögliche mobile Endgerät verwendet werden können. Die heutigen Mobilfunknetze wandeln sich zu weiteren Zugangsplattformen zum Internet. Dies führt dazu, dass Dienste, die zuerst nur vom Mobilfunkprovider oder einem seiner Vertragspartner angeboten worden sind, nun von einem beliebigen Dienstanbieter im Internet angeboten werden könnten. Dieser Dienstanbieter benötigt in diesem Fall auch keinen speziellen Rahmenvertrag mit dem Provider. Dies führt zu einer Flexibilität, die der Benutzer aus dem Internet kennt. Die Kosten für den Datentransfer sinken. Dadurch wird es möglich, innovative Dienste einer großen Masse von Benutzern zur Verfügung zu stellen. Die Architektur muss grundsätzlich davon abstrahieren, wie die Daten ausgetauscht werden. Je nach Standort besitzt der Benutzer die Möglichkeit, auf unterschiedliche Netzwerke mit Zugang zum Internet zuzugreifen. Diese Auswahl des geeigneten Netzwerks kann er anhand unterschiedlicher Kriterien wie z.B. Abdeckung, Verfügbarkeit, Kosten, Bandbreite, usw. treffen.

- Da von Beginn an jede Art des Zugangs berücksichtigt wird, muss beachtet werden, dass öffentliche Netze die Sicherheit der Daten nicht gewährleisten können. Das bedeutet, dass es bei der Übertragung zu Fehlern kommen kann. Viel wichtiger ist jedoch, dass Daten durch unbefugte Dritte ausgespäht oder manipuliert werden können. Aus diesem Grund müssen Mechanismen eingesetzt werden, damit Dritte keinen inhaltlichen Zugriff zu den Daten erhalten und mögliche Manipulationsversuche schnell erkannt werden.

- Um sicherzustellen, dass nur am Dienst beteiligte Instanzen Zugriff zu Daten erhalten, müssen diese Datensätze verschlüsselt werden. Bei der Verschlüsselung muss sichergestellt werden, dass nur die für den jeweiligen Arbeitsschritt befugte Instanz die zugehörigen Daten verwerten kann. Zusätzlich muss nachweisbar sein, ob der Absender der ist, den er vorgibt zu sein. Durch dieses Vorgehen kann sichergestellt werden, dass nur die im Vorfeld definierten Instanzen an der Diensterbringung beteiligt sind.

- Softwarefehler können dazu führen, dass sensible Informationen an unbefugte Dritte gelangen. Sensible Informationen und kritische Berechnungen können dadurch geschützt werden, dass die Verarbeitung der Daten im Bereich von einer Trusted Computing Umgebungen geschieht.

- Ein Dienstanbieter kann, um den Benutzer von dem vertrauenswürdigen Umgang mit seinen Daten zu überzeugen, ein anerkanntes und neutrales Auditing-Unternehmen beauftragen. Dieses überprüft die Logik und den Workflow der Diensterbringung. Die erfolgreiche Überprüfung des Dienstes kann das Auditing-Unternehmen durch eine weitere Signatur des Dienstleister-Zertifikates mit weiteren Attributen ausweisen. Dadurch kann der Benutzer bei einer Dienstsuche zwischen Diensten unterscheiden, die nachweislich den Schutz der Privatsphäre berücksichtigen und Anbietern ohne diesen Nachweis. Der Nachweis kann somit als Qualitätszeichen für zukünftige Dienste angesehen werden.

- Ähnlich wie bei P3P kann der Benutzer im Vorfeld definieren, welche Anforderungen er an einen Dienst stellt. Dies bedeutet z.B., welche Daten er bereit ist von sich aus preiszugeben, bzw. zu welchen Rahmenbedingungen er Dienste nutzen möchte. Jeder Dienstanbieter kann diese Rahmendaten in Form von Metadaten bereitstellen. Im dem Fall, in dem ein Dienst diesen Anforderungen nicht genügt, kann er aus dem Suchergebnis entfernt oder besonders gekennzeichnet werden.

- Der Einsatz von standardisierten Schnittstellen ermöglicht eine Integration der an dem Supply Chain beteiligten Instanzen. Durch die Verwendung von Web Services können Dienstleistungsbestandteile flexibel integriert werden. Dieses Vorgehen garantiert eine ausreichende Skalierbarkeit der Dienste für den Massenmarkt. Ebenso lassen sich große Teile der Logik von externen Anbietern integrieren. Die Modularität der beteiligten Instanzen erlaubt zusätzlich, dass Logikbestandteile in einer Reihe von Diensten wieder verwendbar sind. Dieses Vorgehen ermöglicht eine ausgeprägte Flexibilität beim Dienstleistungsangebot. Die so geschaffenen Dienstleistungen werden in diesem Fall von virtuellen Organisationen angeboten. Durch die offenen Schnittstellen ist auch eine einfache Integration in weitere Geräteplattformen gewährleistet.

- Die Modularisierung der an der Dienstleistungserbringung beteiligten Instanzen bringt den Vorteil, dass, wenn alle nachweislich die Privatsphäre des Benutzers schützen und den Datenschutz einhalten, es möglich ist, in sehr kurzer Zeit komplexe Dienste bereitzustellen, die ebenfalls die gesetzlichen Anforderungen umsetzen. Dies ist deshalb wichtig, weil der Benutzer nur die Identität des Dienstanbieters kennt und nicht die Vertrauenswürdigkeit der beteiligten Instanzen vor der Dienstnutzung prüfen wird. Der Nachweis der Sicherheit des gesamten Dienstes mit allen beteiligten Instanzen stellt eine essentielle Herausforderung dar, die andernfalls zu einem Hemmnis bei der Dienstnutzung führen würde.

- Da diese Architektur speziell auch ortsbezogene Dienste unterstützen soll, muss von Beginn an berücksichtigt werden, wie und von wem die Ortsinformationen ermittelt werden. Im Bereich des Mobilfunknetzes ermitteln primär die Mobilfunkprovider den Standort der mobilen Endgeräte. Da aber bei dieser Architektur keine Verpflichtung besteht, einen Mobilfunkprovider zur Datenkommunikation zu verwenden, müssen weitere Technologien berücksichtigt und integriert werden, um unabhängig von einem Mobilfunkprovider ortsbezogene Dienste zu realisieren. Abhängig von den situativ verfügbaren Techniken muss eine oder es müssen mehrere zur Positionsbestimmung verwendet werden. Die Architektur beschränkt sich zu Beginn nicht auf nur vorhandene Technologien, sondern erlaubt eine generische Erweiterung um weitere Sensoren. Eine weitere Möglichkeit besteht darin, dass unterschiedliche Positionsinformationen sich gegenseitig präzisieren können und somit besonders in Grenzsituationen weiterhin eine genaue Lokalisierung ermöglichen. Dies ist dann besonders wichtig, wenn Dienste sowohl innerhalb wie auch außerhalb von Gebäuden angeboten werden sollen.

- Die Architektur soll darauf ausgelegt sein, dass Dienste aus dem Bereich des mCommerce realisiert werden können. Für diese Dienste ist zumeist für die Nutzung ein Micropayment notwendig. Im Bereich des Mobilfunknetzes wird diese Aufgabe zumeist vom Mobilfunkprovider übernommen. Er berechnet die in Anspruch genommenen Dienstleistungen auf der nächsten Telefonrechnung. Da bei dieser Architektur im Vorfeld definiert worden ist, dass die Diensterbringung und Datenübermittlung auch unabhängig vom Mobilfunkprovider erfolgen kann, so muss für diese Stelle eine eigenständige Instanz diese Aufgabe übernehmen.

- Die Architektur muss auf die Bedürfnisse des mobilen Umfelds hin entwickelt werden. Dies bedeutet, dass unabhängig von dem verwendeten Endgerät die Dienste genutzt werden können. Dies ist besonders deshalb wichtig, da auf dem Markt eine sehr große Anzahl von Endgeräten erhältlich ist. Im Weiteren ist zu berücksichtigen, dass die Nutzungszeit eines Endgerätes meistens nur 2 Jahre beträgt. Daher muss die Möglichkeit bestehen, Einstellungen auf ein anderes Gerät zu übertragen. Da ein Großteil der Benutzer nicht technikafin ist, sollte die Benutzung möglichst einfach gehalten werden. Die Komplexität der Anwendung, speziell im Bereich der Nutzung, muss somit möglichst ergonomisch realisiert werden. Besonders grundlegende Konfigurationen sollten mit Hilfe von automatischen Mechanismen erfolgen, damit das Endgerät sich auf möglicherweise geänderte Anforderungen der Dienste oder die unterschiedlichen verfügbaren Netze einstellen kann. Im Weiteren müssen neben den Geräten aus dem Bereich der Mobilfunktelefone auch alle weiteren Geräte berücksichtigt werden, die im mobilen Umfeld benutzt werden und Zugang zum Internet haben und somit die theoretische Möglichkeit besitzen, kontextbezogene Dienste zu verwenden.

- Da die Datenkommunikation im mobilen Umfeld oft kostenintensiver und fehleranfälliger ist und dazu nicht die Bandbreite bereitstellen kann, wie z.B. ein kabelgebundener Anschluss, muss bereits bei der Entwicklung der Architektur und der Dienste darauf geachtet werden, dass die Datenmenge, die bei der Dienstnutzung anfällt, minimiert wird. Somit kann ein optimales Verhältnis zwischen Kosten und benötiger Zeit für den Datentransfer erreicht werden.

- Da diese Architektur den Massenmarkt anspricht, muss auch die Möglichkeit existieren, eine ausreichende Skalierung der Dienste zu erreichen. Dies ist besonders deshalb wichtig, da die räumliche Verfügbarkeit nicht nur den Bedürfnissen von privaten Gruppen, sondern auch globalen Ansprüchen genügen muss.

- Die Architektur muss die Möglichkeit bieten, sowohl Push- als auch Pull-Dienste zu unterstützen. Dafür ist es notwendig, dass im Bereich der ortsbezogenen Dienste auch ein Tracking-Modus realisierbar ist. In diesem Modus wird die Position des Benutzers in definierten Zeitabständen oder nach einer definierten Veränderung an den Dienst gemeldet. Diese Form der Push-Dienste lässt neuartige Dienstformen zu. Denkbar wäre hier auch ein Werbedienst, der kontextbezogene Werbung bereitstellt. Die Benutzer, die derartige Dienste zulassen, brauchen als Gegenleistung keine Gebühren zu zahlen. Die Klasse der Werbedienste stellt eine Herausforderung an die Architektur dar, da die Werbedienstbetreiber an allen Daten der Kunden interessiert sind.

- Da sich die Position eines Endgerätes leicht ermittelt lässt, eröffnen sich neue Wege, die Benutzerfreundlichkeit (z.B. von Suchanfragen) zu steigern. Oft werden Informationen aus dem direkten Umfeld abgefragt. Da die räumliche Relevanz von ortsbezogenen Informationen und Diensten beschränkt ist, und reguläre Dienste zumeist nur für einen bestimmten räumlichen Bereich konzipiert sind, ist es für den Benutzer interessant zu wissen, welche Dienste an seinem Standort angeboten werden. Um die Suche möglichst komfortabel und für den Benutzer zeitlich kurz zu gestalten, müssen Portale und Suchmaschinen erstellt werden, über die der Benutzer unter Zuhilfenahme seiner Kontextinformationen nach Informationen und Diensten suchen kann.

- Da heutige Suchmaschinen primär die Inhalte nach Stichwörtern sortieren, muss ein zukünftiges Service Register zusätzliche Informationen speichern, um eine komfortable Suche zu ermöglichen. Ein wichtiger Punkt wäre hier z.B. die geographische Ausbreitung des Dienstes. Eine Kategorisierung der Daten würde die Auswahl bereits zu Beginn erleichtern. An diesem Punkt muss beachtet werden, dass ein Benutzer im mobilen Umfeld normalerweise nur eine minimale Zeit für eine Suche nach dem geeigneten Dienst oder der geeigneten Information in Anspruch nehmen möchten. Daher muss die Suchfunktion bereits zu Beginn so optimiert sein, dass die Anzahl der möglichen Treffer eingeschränkt ist. Zu jedem Dienst muss zusätzlich beim zuständigen Service Register (siehe Kapitel 4.6) ein Eintrag mit Metadaten zum Dienst hinterlegt werden.

In dieser Datei befinden sich allgemeine Informationen über den Dienst wie z.B.

- Wer ist der Dienstanbieter?
- Wo befindet sich der Erfüllungsort / Gerichtsstand des Vertrags?
- Handelt es sich um eine kostenpflichtige Dienstnutzung?
- Handelt es sich um einen einmaligen Preis oder ein Abo?
- Kurzbeschreibung des Dienstes
- Kategorie des Dienstes
- Welche räumliche Ausbreitung besitzt der Dienst?
- Werden Kontextinformationen verwendet?
- Sind Dritte an der Service-Erbringung beteiligt?
- Erhalten Dritte personalisierten Zugang zu Kontext-Informationen?
- Link zu den AGBs

- Möchte der Benutzer ermitteln, welche Dienste an seinem Standort angeboten werden, so kann er beim Service Register anfragen. Die Ergebnisse können vom Endgerät oder vom Service Portal visualisiert werden. Das Portal berücksichtigt dabei besonders die räumliche Verfügbarkeit der Dienste und zeigt nur diese an, die an dem Standort angeboten werden. Damit der Benutzer nach seinen Interessen gezielt Angebote erhält, kann er mit Hilfe von Kategorien das geeignete Angebot ermitteln. Zusätzlich besitzt das Portal die Möglichkeit, weitere personenbezogene Informationen bei der Suche zu berücksichtigen. Somit steigt die Wahrscheinlichkeit, dass die Suche relevante Ergebnisse bereits mit den ersten Treffern bringt. Dazu entfällt in diesem Fall die möglicherweise langwierige Konfiguration eines Suchagenten, weil der Benutzer die notwendigen Einstellungen nur einmal tätigen muss.

- Damit der Kunde die Möglichkeit hat, beeinflussen zu können, welche Dienste und Personen Zugriff auf personenbezogene Daten erhalten, muss ein Regelsystem bereitstehen. Dieses muss von einer vertrauenswürdigen Instanz realisiert werden. Mit einer Regelsprache kann der Zugriff auf die bei der Diensterstellung verwendeten Informationen eingeschränkt werden. Ihre Genauigkeit lässt sich variieren. Durch personenbezogene Regelsatz-Sammlungen kann dies unabhängig vom Endgerät von der zuständigen Instanz realisiert werden. Diese Instanz stellt das Bindeglied zwischen Endgerät und dem jeweiligen Dienst dar. Es müssen Regelsätze für die verwendeten Dienste erstellt werden. Zusätzlich können Regelsätze formuliert werden, die spezielle Situationen abdecken, weil dann die normalen Regeln nicht ausreichen. Es muss also ein Regelsystem erstellt werden, das umfassend genug ist, diesen Anspruch zu erfüllen. Neben global gehaltenen Regeln sollten auch Feinabstimmungen möglich sein, die die Rahmenbedingungen für den Dienst oder für bestimmte Personen definieren. Dies bedeutet, dass beispielsweise die Genauigkeit oder Verfügbarkeit von Informationen eingeschränkt werden kann. Derartige Regeln können auch für einen zeitlich begrenzten Bereich festgelegt werden. Nach diesem Zeitbereich werden die Regeln deaktiviert oder entfernt.

- Die festgelegten Regeln müssen in einer übersichtlichen Form dargestellt werden. Dabei ist zu beachten, dass sich die Regeln vom Benutzer auch modifizieren lassen oder entfernt werden können, wenn ein Dienst nicht mehr in Anspruch genommen wird. Diese Darstellung muss es dem Benutzer auch ermöglichen, zu erkennen, welchen Diensten er Zugriff auf sensible Daten gegeben hat und wann der jeweilige Dienst zuletzt Zugriff auf Daten hatte. Aus der Übersicht sollte sich auch ermitteln lassen, ob Dienste verwendet werden, die über einen Abovertrag berechnet werden. Die Kündigung von laufenden Verträgen sollte an dieser Stelle auch möglich sein. Zu den Verträgen sind auch weiterführende Information wie z.B. Links zu den aktuellen Preislisten, AGBs und Kontaktinformationen usw. anzugeben.

4. Architektur

Bei der Konzeption der Architektur wurden die Anforderungen aus Kapitel 3 berücksichtigt. Ein Ziel der Aufgliederung in eine große Anzahl von unterschiedlichen Instanzen ist es, die Menge der vorhandenen Daten, die eine Instanz enthält, auf das Maß zu beschränken, das zur Diensterbringung unbedingt notwendig ist. Durch dieses Vorgehen erhält keine Instanz außerhalb des Bereichs „Security“ Zugriff zu einer solchen Menge an sensiblen Daten, die es erlauben würden, den Benutzer zu identifizieren, falls dieser eine anonymisierte Dienstnutzung wünscht. In dem Bereich „Security“ befinden sich die sicherheitsrelevanten Instanzen, die sicherheitskritische Informationen des Benutzers verwalten oder aufbereiten.
Die Architektur ermöglicht eine generische Integration von Technologien zur Datenübertragung, Lokalisierung sowie die beliebige Erweiterung um zusätzliche Dienste.

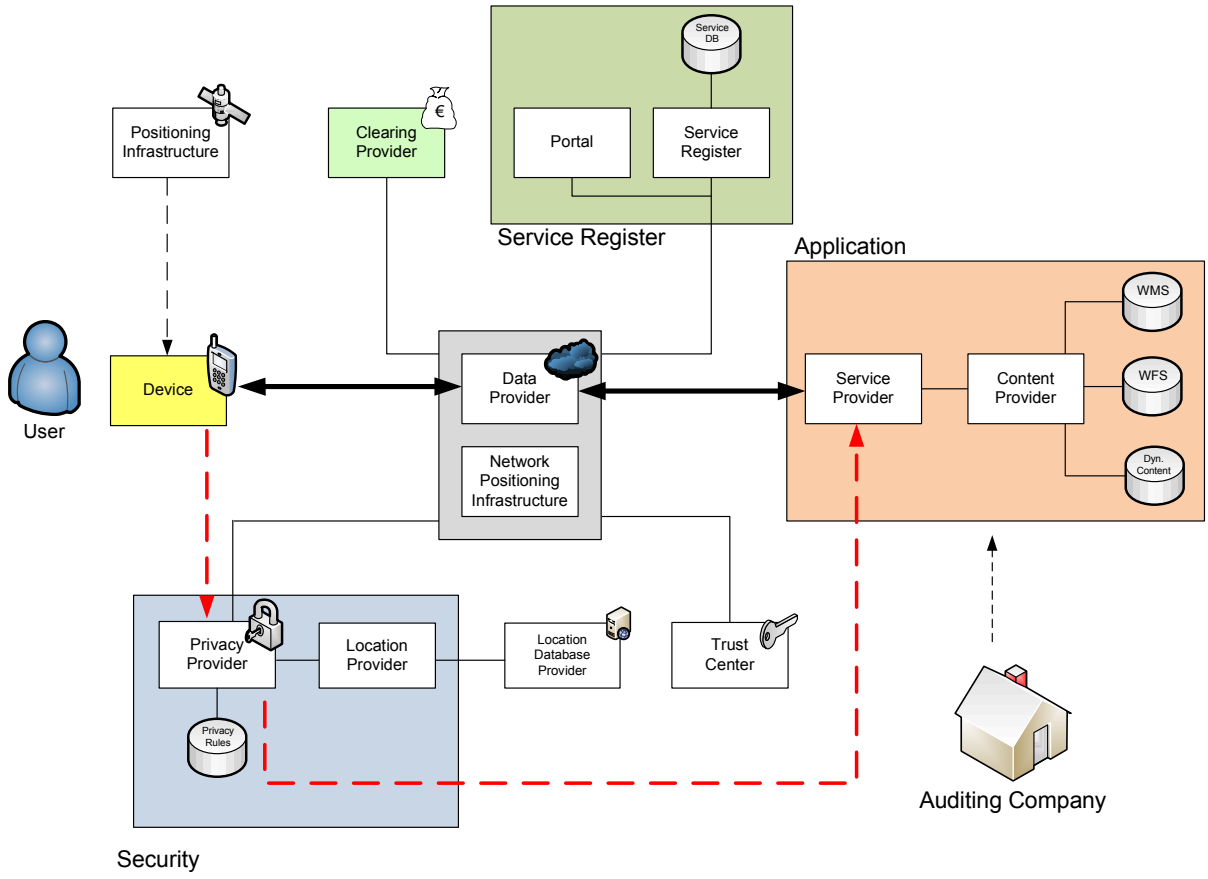


Abbildung 4 - Darstellung der Gesamthierarchie

Die zur Architektur gehörenden Instanzen werden in dem folgenden Abschnitt einzeln mit ihrer Aufgabe vorgestellt:

4.1 Device

Bei den Endgeräten (Device) handelt es sich um primär tragbare Systeme wie z.B. Smartphones (Mobiltelefone), PDAs und Notebooks. Bei dieser Arbeit wird davon ausgegangen, dass die Entwicklung der Mobilfunktelefone weiterhin dazu führt, dass diese Geräte von Generation zu Generation höhere Leistungsfähigkeit (Prozessorleistung, Speicherausstattung, Funktionsvielfalt, Darstellung sowie Interaktionsmöglichkeiten) erhalten. Daher wird in der folgenden Arbeit davon ausgegangen, dass alle zukünftigen Mobilfunktelefone die Leistungsfähigkeit von heutigen[4] Smartphones besitzen. Dies ermöglicht eine sehr flexible Erweiterungsfähigkeit mit zusätzlicher Software, Eingabe- und Darstellungsmöglichkeiten für komplexe Dienste sowie Zugriff aufs Internet.
Basierend auf dieser Entwicklung wird die Leistungsfähigkeit der mobilen Endgeräte der von stationären Systemen vor etwa 7 Jahren gleichen. Diese Entwicklung zeigt, dass die Geräteklasse der mobilen Endgeräte von ihrem Potential her immer mehr Leistungen von PCs erreicht, obwohl diese Geräte für ihren speziellen Anwendungsbereich entwickelt worden sind. Neben den Mobiltelefonen werden im mobilen Umfeld noch PDAs und Notebooks verwendet. PDAs besitzen im Vergleich zu Smartphones keine Möglichkeit, sich mit einem Mobilfunknetz zu verbinden. Jedoch können sie über andere Technologien wie z.B. WLAN oder Bluetooth mit dem Internet kommunizieren. PDAs besitzen oft leistungsstärkere CPUs im Vergleich zu Smartphones. In dem letzten Jahr entwickelte sich die Markttendenz dahin, dass mehr Smartphones verkauft worden sind, da dieses Gerät dem Benutzer auch den Komfort eines Mobiltelefons in einem Gerät ermöglicht. Notebooks werden auch dem mobilen Umfeld zugeordnet, jedoch ist keine derartig spontane Nutzung, wie sie z.B. von Smartphones ermöglicht wird, zu realisieren. Das Notebook muss für eine Nutzung auf eine Fläche abgestellt werden, wohingegen das Smartphone in der Hand bedient werden kann. Das Notebook hingegen besitzt den Vorteil, dass es im Bereich der Rechenleistung, Speicherung und Darstellung den Leistungsumfang eines stationären Systems besitzt, während das Smartphone zumeist auf Stifteingabe oder eine miniaturisierte Tastatur zurückgreifen muss. Zusätzlich zu den Geräten, die für den mobilen Einsatz konzipiert worden sind, werden in dieser Architektur auch stationäre Systeme berücksichtigt, da diese Systeme auch Vorteile durch die Nutzung von kontextsensitiven Diensten besitzen. Im Bereich der stationären Systeme sind bestimmte Kontextinformationen keiner Änderung unterworfen. Beispielsweise verändert sich die Position des Gerätes nicht. Diese Informationen können statisch hinterlegt werden. Eine gemeinsame Eigenschaft aller Geräte muss die Kommunikationsfähigkeit mit dem Internet sein. Detailliert wird dies im Kapitel 4.2 besprochen.

Je nach Endgerät verfügen diese Systeme über Sensoren, um Kontextinformationen automatisch zu gewinnen. Bei diesen Sensoren kann es sich beispielsweise um einen GPS-Empfänger handeln, der die eigene Position ermittelt. Die Notwendigkeit von unterschiedlichen Sensorinformationen zur Realisierung von ortsbezogenen Diensten und Anwendungen wird detailliert in Kapitel 5 beschrieben.

[4] Entwicklungsstand 2007

4.2 Data Provider

Eine einheitliche Funktion aller Endgeräte ist der Datenaustausch mit dem Internet. Der Zugang zum Internet kann dabei je nach Gerät über unterschiedliche Technologien erfolgen. Es bieten sich dazu kabellose wie auch kabelgebundene Zugangsarten an. Je nach den verwendeten Technologien unterscheiden sich die Verfügbarkeit, Bandbreite, Latenz und die Kosten stark. Die Datenübermittlung wird über die Instanz eines „Data Providers" abgewickelt. Jeder Betreiber eines Netzwerkes, das die oben genannten Voraussetzungen erfüllt, kann als Data Provider fungieren. Diese Instanzen haben die Aufgabe, die Kommunikation mit dem Internet zu ermöglichen. Ein Data Provider kann somit ein:

- Internetprovider
- Mobilfunkprovider
- Unternehmensnetzwerk
- Öffentliches Netzwerk (z.B. einer Universität)

sein.

Eine entscheidende Eigenschaft dieser Instanz besteht darin, dass sie Wahlmöglichkeiten des Kunden nicht einschränkt. Das bedeutet, dass der Data Provider nicht wie ein Mobilfunkprovider entscheidet, zu welchen Diensten ein Kunde, der sein Netz verwendet, Zugang hat. Dem Benutzer steht somit der Zugriff auf alle Dienste und Ressourcen des Internets zur Verfügung.

Manche Endgeräte können unterschiedliche Zugangsformen nutzen. Beispielsweise besitzt eine steigende Anzahl an Smartphones die Möglichkeit, per WLAN oder über das Mobilfunknetz Zugriff zum Internet zu erhalten. Da sich die Eigenschaften der beiden Zugangsformen unterscheiden, lässt sich durch die Wahl der optimalen Zugangsart z.B. eine Kostenoptimierung erreichen.

Alle an der Dienstleistungserbringung beteiligten Instanzen sind ebenfalls mit dem Internet verbunden. Somit handelt es sich beim Data Provider um ein zentrales Bindeglied der Architektur, da die Kommunikation aller Instanzen über dieses öffentliche Netzwerk abgewickelt wird. Dadurch, dass es sich beim Internet um ein öffentliches und damit unsicheres Netzwerk handelt, müssen alle Daten verschlüsselt werden. Detailliert wird die Kommunikation im Kapitel 7 behandelt.

4.3 Service Provider

Die Instanz des Service Providers stellt den eigentlichen Dienst für den Benutzer bereit. Bei diesen Diensten kann es sich um die bereits vorhandenen einfachen Informationsdienste oder um komplexere Dienste mit umfangreicher Interaktion handeln. Je nach zu erbringender Dienstleistung werden unterschiedliche Kontextinformationen des Benutzers bei der Diensterbringung berücksichtigt. Die primäre Logik der jeweiligen Dienste befindet sich in den meisten Fällen in den Servern der Dienstanbieter. Denkbar wären jedoch auch Hybriddienste, die Logikbestandteile verwenden, die sich auf den jeweiligen Endgeräten befinden. Durch diese Vorgehensweise lässt sich die Kernlogik des Dienstes durch den Anbieter durchgehend anpassen. Zusätzlich besitzen reine Dienste den Vorteil, dass der Benutzer nicht vor der Dienstnutzung Anwendungsbestandteile auf seinem Endgerät installieren muss. Diese müssten andernfalls für jede unterschiedliche Klasse von Endgeräten (jede Klasse besitzt eigene spezifische Eigenschaften wie z.B. das verwendete Betriebssystem und die vorhandenen Systemressourcen) entwickelt und gewartet werden. Die Darstellung der Dienste kann mithilfe vorhandener Internet-Technologien erfolgen. Da diese Technologien plattformunabhängig sind, können Dienste sehr schnell für die unterschiedlichen Plattformen bereitgestellt werden. Da die Plattformen sich jedoch im Bereich der Interaktions- und Darstellungsmöglichkeiten unterscheiden, entsteht für den Dienstbetreiber je nach Dienst die Notwendigkeit, die Anwendungen mit einem Multi-Frontend-Zugang auszustatten. Abhängig von den gegeben Fähigkeiten des Endgerätes wird ein geeignetes Frontend zur Darstellung gewählt.

Da die Dienste dieser Architektur, vergleichbar mit Webangeboten, von jeder Person erstellt und angeboten werden können, besteht die Möglichkeit, eine weitaus breitere Vielfalt bereitzustellen. Sie müssen somit nicht mehr nur ausschließlich für den Massenmarkt konzipiert sein, sondern es kann sich um Spartenanwendungen für ein spezielles Unternehmen oder eine bestimmte Personengruppe handeln. Die Verwendung der in dieser Arbeit vorgeschlagenen Architektur ermöglicht es den Anbietern, diese Dienste anzubieten, ohne dass dies mit jedem Provider abgeklärt werden muss. Besonders der Zugriff auf Kontextdaten gestaltet sich durch die in der Architektur vorhandenen Schnittstellen wesentlich einfacher und kostengünstiger. Optional besteht natürlich weiterhin die Möglichkeit, spezielle Anwendungen für die jeweiligen Endgeräte zu entwickeln, die beispielsweise die Rechenleistung oder die vorhandenen Datensätze des Endgerätes nutzen.

Die Architektur soll sowohl die bereits primär verwendeten Pull-Dienste, aber auch Push-Dienste unterstützen. Bei Pull-Diensten sendet das Endgerät aktiv eine Anfrage an den Dienst, um Informationen abzufragen. Bei Push-Diensten hingegen sendet der Dienst in dem Moment die relevanten Daten, wenn ihm diese zur Verfügung stehen. Besonders bei Diensten, bei denen die Informationen nur zu unregelmäßigen Zeitpunkten anfallen und die Anzahl der Aktionen, die an das Endgerät gemeldet werden, eher gering ist, ist das intervallmäßige Abfragen nicht wirtschaftlich, da bei den meisten Anfragen keine neuen Daten bereitliegen. Um dieses unwirtschaftliche Verhalten zu unterbinden, sendet der Server über einen Push-Mechanismus nur dann Informationen an das Endgerät, wenn diese auch für die Diensterbringung Relevanz besitzen. Um dies zu ermöglichen, muss die Architektur Mechanismen bereithalten, um dem Endgerät im Bedarfsfall Informationen senden zu können.
Um einen komplexen kontextbezogenen Dienst handelt es sich zum Beispiel bei einem Instant-Messaging Dienst mit Ortsbezug. Bei diesem Dienst können Benutzer untereinander

kommunizieren. Auch besteht die Möglichkeit, dass befugte Personen Standortinformationen von anderen Teilnehmern abfragen oder dass der Dienst abhängig von weiteren Kontextinformationen unterschiedlich reagiert. Beispielsweise wird automatisch „Nicht stören“ als Status angezeigt, wenn der Benutzer sich im Besprechungszimmer befindet, oder er ist ab einer bestimmten Uhrzeit für bestimmte Teilnehmer, „unsichtbar“. Ein derartiger Dienst würde je nach Komplexität der Logik unterschiedliche Kontextinformationen berücksichtigen. Im Weiteren könnte er auch von Push-Mechanismen profitieren.

4.4 Content Provider

Komplexe Dienste sind dadurch charakterisiert, dass der Anbieter in den meisten Fällen nicht mehr alle Bestandteile des Dienstes selbst bereitstellen kann. Das bedeutet, dass diese Bestandteile von weiteren externen Anbietern hinzugekauft werden müssen. Bei einem Routenplanerdienst z.B. müssen unterschiedliche Informationsquellen benutzt werden, um den Dienst realisieren zu können. Bei diesen Diensten stellt der eigentliche Dienstanbieter die Logik zur optimalen Wegfindung zur Verfügung. Er selbst ist jedoch nicht in der Lage, eine Straßenkarte zu erstellen. Deshalb kauft er die notwendigen Daten hinzu oder bezieht sie von einem Dienstanbieter per Anfrage. Die beteiligten Dienstanbieter können sich in diesem Fall um ihre eigentliche Kernkompetenz kümmern. Die Anbieter von mobilen Diensten bieten durch die bereitgestellten Dienstleistungsbestandteile ihren Kunden wesentlich komplexere Dienste an, als die, die nur auf den eigenen Informationsbestandteilen basieren würden.

Content Provider zeichnen sich dadurch aus, dass ihre Kernkompetenz darin liegt, dass sie Dienstleistungsbestandteile Service Providern bereitstellen. Bei diesen Bestandteilen kann es sich um eine Logik für Zwischenergebnisse handeln oder den Zugriff auf spezielle Informationsdatenbanken.

Beispiele für Content Provider sind z.B.:

Informations-Content Provider
- Geodaten (z.B. Kartendaten)
- POI (Points of Interest)
- Nachrichten, Wetter, Börse
- …

Logik-Content Provider
- optimierte Suchanfragen
- Übersetzungsdienste (Umrechnen von Maßeinheiten, Sprachwörterbücher…)
- Routenplaner
- …

Ein Content Provider kann mehrere Dienstleistungen anbietet. Im Weiteren kann er selbst weitere Content Provider verwenden, um sein Angebot abzurunden oder zu ergänzen.

4.5 Service Portal

Benutzer im mobilen Umfeld benötigen in den meisten Situationen sehr kurzfristig Zugriff auf Dienste und Informationen. Um dies zu ermöglichen, muss die Informationsrecherche im mobilen Umfeld eine wesentlich zielgerichtetere Suche nach relevanten Informationen oder Diensten bereitstellen. Im klassischen Internet nutzt der Anwender Stichwörter, um eine Anzahl von geeigneten Webseiten von einer Suchmaschine angezeigt zu bekommen. Je nach Wahl der Stichwörter muss dieser Vorgang mehrfach wiederholt werden. Potentiell geeignete Treffer müssen ausgewählt und auf Nutzbarkeit überprüft werden. Im mobilen Umfeld sind die Eingabemöglichkeiten und die Bandbreite begrenzt, so dass eine derartige Suche sich zeitaufwendig gestaltet. Bei einer Nutzung von regulären Suchmaschinen würden viele Treffer angezeigt, die speziell für stationäre Systeme konzipiert sind. Das würde dazu führen, dass diese Inhalte mit den mobilen Endgeräten nur begrenzt verwendet werden könnten.

Mit Hilfe des Service Portals wird dem Benutzer im mobilen Umfeld eine zielgerichtete Suche nach Informationen und Diensten dadurch bereitgestellt, dass bei der Suchanfrage Kontextinformationen berücksichtigt werden. Diese Kontextinformationen führen dazu, dass die Treffermenge eines Suchdienstes eingeschränkt wird. Im mobilen Umfeld besitzen oft Informationen aus der eigenen Umgebung eine hohe Relevanz. Durch die Nutzung von Ortsinformationen bei der Suchanfrage können vorberechtigt Dienste aus dem eigenen Umfeld angegeben werden.

Bei dem Service Portal handelt es sich um eine reine Visualisierungskomponente. Die Anbieter der unterschiedlichen Service Portale verwenden als Grundlage die Informationen aus dem Service Register. Die unterschiedlichen Service Portale können sich anhand ihres Personalisierungsgrades und Schwerpunktes unterscheiden. Dem Benutzer steht es frei, vergleichbar wie bei Suchmaschinen im Internet, einen für ihn geeigneten Dienst zu wählen.

4.6 Service Register

Bei dem Service Register handelt es sich um eine geographische Hierarchie von verteilten Servern. Mit Hilfe dieser Server kann ermittelt werden, welche Dienste innerhalb eines bestimmten Bereiches angeboten werden. Das Service Register wird von den Endgeräten und Service-Portalen als Informationsquelle verwendet. Jeder frei verfügbare Dienst muss von einem Service Register-Server, der für die geographische Ausbreitung seines Dienstes zuständig ist, gelistet werden. Anhand einer Suchanfrage mit integrierten Informationen über den geographischen Bereich und optional weiteren Attributen, liefern die beteiligten Service Register-Server als Antwort die Treffer der Suchanfrage.

Abbildung 5 zeigt eine mögliche Hierarchie eines Service Registers. Diese Hierarchie berücksichtigt fünf geographische Hierarchie-Ebenen, die je nach Anwendungsfall um weitere optionale Hierarchiestufen erweitert werden können. Alle Dienste sind mit ihrer räumlichen Ausbreitung in der Datenbank des Servers eingetragen. Basierend auf den Anfrageinformationen wie z.B. Standort des Benutzers, Suchumfeld und optionalen Kriterien der Suche, werden mögliche Treffer in der Datenbasis der Service Register-Server ermittelt. Ein Dienst ist jeweils auf dem Server gespeichert, der für die räumliche Ausbreitung zuständig ist. Der Root-Server besitzt eine Datenbasis über Dienste, die weltweit kontextbezogene Dienste anbieten. Zusätzlich verweist er auf die zurzeit gültigen Netzwerkadressen der beteiligten Server der tiefer liegenden Hierarchien.

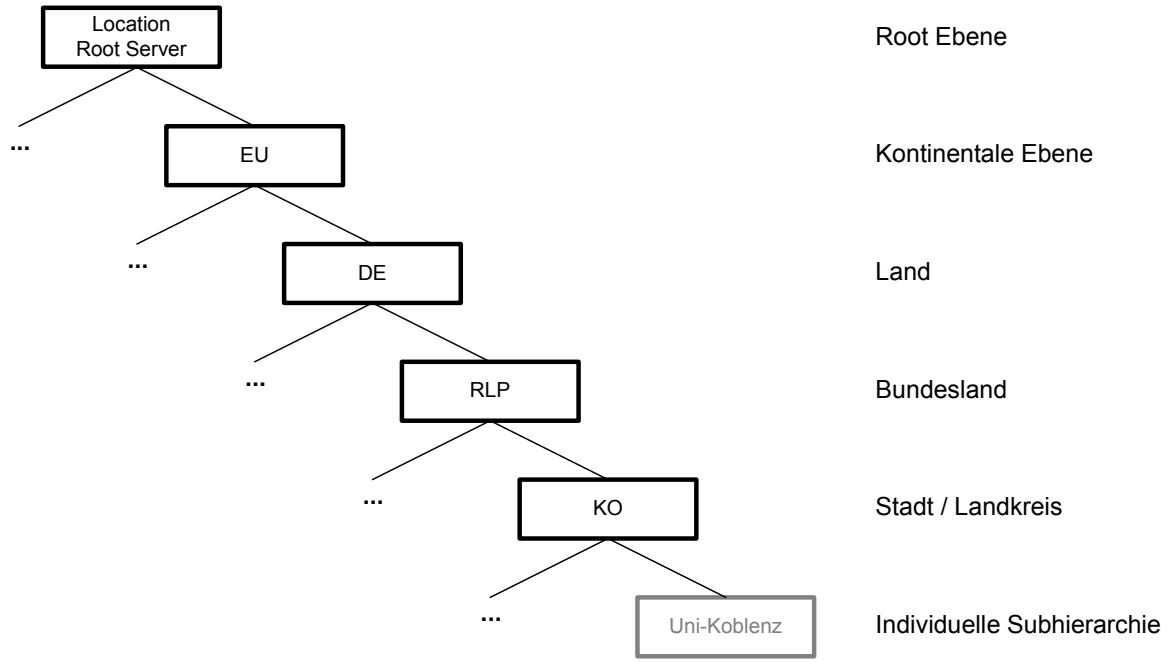


Abbildung 5 - Mögliche Server-Hierarchie des Service Registers

Dienste werden immer in die Hierarchiestufe eingetragen, in der sie nur mit Hilfe eines Eintrages repräsentiert werden können. Beispielsweise würde ein Dienst, der sowohl in Deutschland als auch in der Schweiz angeboten wird in der Hierarchiestufe „EU“ gespeichert. Dieses Vorgehen soll sicherstellen, dass die Anzahl der Einträge minimiert wird. Innerhalb des Eintrags zum Dienst werden detaillierte Informationen zu dem Bereich gegeben, in dem der Dienst verfügbar ist.

Die niedrigste Hierarchiestufe stellt das räumliche Gebiet einer Stadt bzw. eines Landkreises dar. Existiert in diesem Bereich jedoch eine sehr große Anzahl von Angeboten, z.B. auf dem Gelände einer Institution, so besteht zusätzlich auch die Möglichkeit, die Hierarchie noch zu erweitern. Das erlaubt dieser Institution, ein Service Register einer individuellen Subhierarchie zu betreiben. In diesem Register befinden sich die ortsbezogenen Dienste, die auf dem Bereich des eigenen Geländes verfügbar sind. Dieses Vorgehen ermöglicht den Administratoren eine sehr schnelle Verwaltung derartiger Dienstleistungen. Dies könnte beispielsweise bei Veranstaltungen zweckmäßig sein, bei denen Informationsdiensten nur eine sehr kurze Zeit zur Verfügung steht.

Abbildung 6 beschreibt die Nutzung der beteiligten Instanzen innerhalb der Architektur, um eine Dienstabfrage mit Hilfe der Service Register zu ermöglichen. Die Visualisierung erfolgt dabei durch das Service Portal. Das Endgerät stellt die Dienstanfrage über den Privacy Provider. Dieser erhält die Positionsinformation, die zuvor mit Hilfe der beteiligten Sensoren ermittelt worden ist. Die Kontextinformationen, die basierend auf dem Regelsatz zur Nutzung des Service Portals verwendet werden dürfen, werden an das Service Portal übermittelt. Es handelt sich dabei um eine anonymisierte Anfrage. Das Service Portal erhält diese Anfrage mit dem Absender des Privacy Providers. Somit besteht keine Möglichkeit, die Suchanfrage mit einem konkreten Endgerät oder einem Benutzer zu verbinden. Das Service Portal fragt die beteiligten Service Register ab. Die Treffermenge wird für den Benutzer aufbereitet und zur Verfügung gestellt. Optional besteht zusätzlich die Möglichkeit, dass das Endgerät die Service Register ohne Verwendung des Service Portals abfragt, um die Ergebnisse eigenständig aufzubereiten und darzustellen. Basierend auf dieser Ergebnismenge besitzt der Benutzer nun die Möglichkeit, einen Dienst auszuwählen.

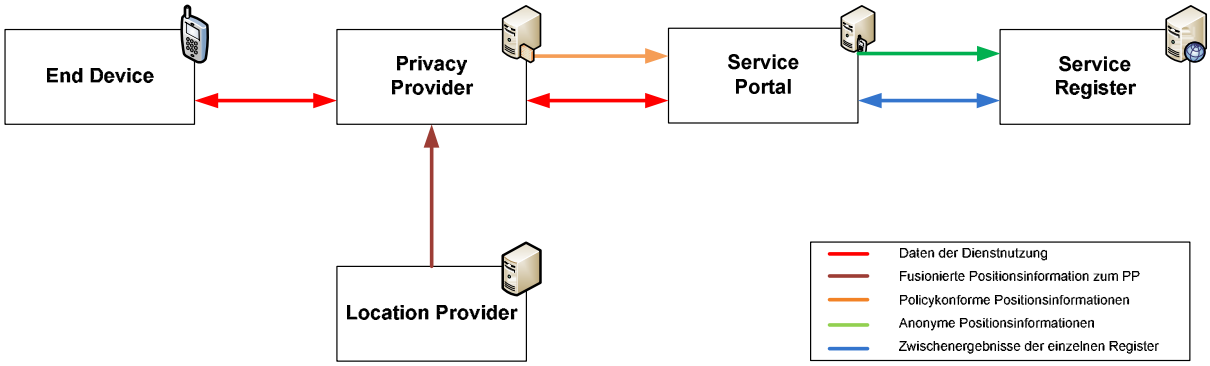


Abbildung 6 - Architekturübersicht bei der Nutzung der Service Register

Abbildung 6 zeigt die bei der Verwendung des Service Portals beteiligten Instanzen. Alle Kommunikation wird über den Privacy Provider abgewickelt. Dieser erhält vom Location Provider die ermittelten Positionsinformationen. Diese werden bei der Suchanfrage mit optional weiteren Kontextinformationen verwendet, um beim Service Portal geeignete Dienste zu ermitteln. Das Service Portal sendet diese Anfrage an die beteiligten Server des Service Registers. Die so erhaltenen Informationen visualisiert das Service Portal und stellt sie über den Privacy Provider dem Endgerät zur Verfügung.

4.7 Clearing Provider

Der Clearing Provider ermöglicht die Abrechnung von kostenpflichtigen Diensten. Es wird in diesem Zusammenhang davon ausgegangen, dass personalisierte Dienste zum größten Teil auf kostenpflichtiger Basis angeboten werden. Die bei der Nutzung entstehenden Kosten bewegen sich im Eurocent Bereich. Da eine Nutzung von mobilen Diensten zumeist nur sehr unregelmäßig erfolgt, und dabei eine große Anzahl von Dienstanbietern die nachgefragten Dienste anbietet, muss eine Instanz existieren, über die eine Bezahlung der Dienstnutzung ermöglicht wird. Diese Instanz muss auf die Verrechnung von Micro-Payment-Zahlungen spezialisiert sein. Das bedeutet, dass neben den eigentlichen Kosten für die Dienstnutzung für den Benutzer keine weiteren Transaktionskosten anfallen, da diese andernfalls ein Hindernis für die Dienstakzeptanz darstellen würden. Der Kunde, der Privacy Provider und der Service Provider müssen ein Account bei einem Clearing Provider besitzen. Dieser Provider agiert vergleichbar wie Paypal[5]. Die Instanzen können über ihn anderen Teilnehmern Geld senden oder von diesen empfangen.

Die beteiligten Instanzen sollen nur die jeweils minimale Informationsmenge vom Benutzer erhalten. Damit der Clearing Provider keine Informationen über die eigentliche Dienstnutzung und der Service Provider keine Informationen über den Benutzer erhält, werden neben der Übermittlung der Dienstleistungsdaten auch die monitären Flüsse über den Privacy Provider abgewickelt. Die Zahlung an den Dienst erfolgt somit vom Privacy Provider. Dem Privacy Provider ist der Account des Benutzers beim Clearing Provider bekannt. Die so entstandenen Kosten werden von ihm dem Kunden in Rechnung gestellt. In diesem Zusammenhang bucht er die entstandenen Kosten vom Kundenaccount. Da es auch Dienste gibt, bei denen der Kunde bei der Nutzung Geld verdienen kann (z.B. Werbeplattformen, Darstellung von Werbung auf dem Endgerät, Teilnahme an anonymisierten Befragungen usw.), wird diese Verrechnung am Ende einer Rechnungsperiode (z.B. am Ende eines Tages) ausgeführt. Die Abbuchung zeigt nur den gesamten Betrag sowie im Betreff eine Transaktionsnummer. Diese Transaktionsnummer kann vom Kunden genutzt werden, um beim Privacy Provider die Abrechnung einzusehen. Der Clearing Provider hingegen erhält keine Informationen über die verwendeten Dienste oder weitere Kontextinformationen des Benutzers.

Abbildung 7 zeigt einen Zahlungsvorgang bei einer Dienstnutzung. Die eigentliche Dienstnutzung erfolgt vom Endgerät über den Privacy Provider mit dem Service Provider. Für den Service Provider ist in erster Linie nur der Privacy Provider sichtbar, sofern aufgrund des Dienstes keine personenbezogenen Informationen benötigt werden. Die eigentliche monetäre Transaktion spielt sich zwischen dem Service Provider und dem Privacy Provider und zwischen dem Privacy Provider und dem Benutzer ab. In dieser Abbildung wird angenommen, dass alle drei Instanzen den gleichen Clearing Provider besitzen. Verwenden die beteiligten Instanzen unterschiedliche Clearing Provider, müssen diese untereinander einen monetären Austausch ermöglichen.

Da für eine wirtschaftliche Nutzung der Nachweis der Dienstnutzung gewährleistet sein muss, muss zum Zeitpunkt der Dienstleistungsanfrage bzw. -erbringung ermittelt werden, dass es sich bei den beteiligten Instanzen um die vorgegebenen Transaktionspartner handelt. Dies wird mit Hilfe der vorhandenen Zertifikate und PKI-Infrastruktur (siehe Kapitel 6.4) ermöglicht. Vor jeder Transaktion wird die Richtigkeit und Gültigkeit der an der Transaktion beteiligten Instanzen geprüft. Zur Prüfung werden die standardisierten Schnittstellen der

[5] Homepage Paypal: http://www.paypal.de/de

Validation Authority (VA) des Trust Centers genutzt. Das Trust Center verwaltet die öffentlichen Schlüssel und eine Datenbank mit Informationen über die Gültigkeit der von ihr signierten Zertifikate. Bei der Abfrage der Gültigkeit wird im Besonderen die Liste der Zertifikate überprüft, die als ungültig eingestuft worden sind. Bei dieser Liste handelt es sich um die Certificate Revocation List (CRL).

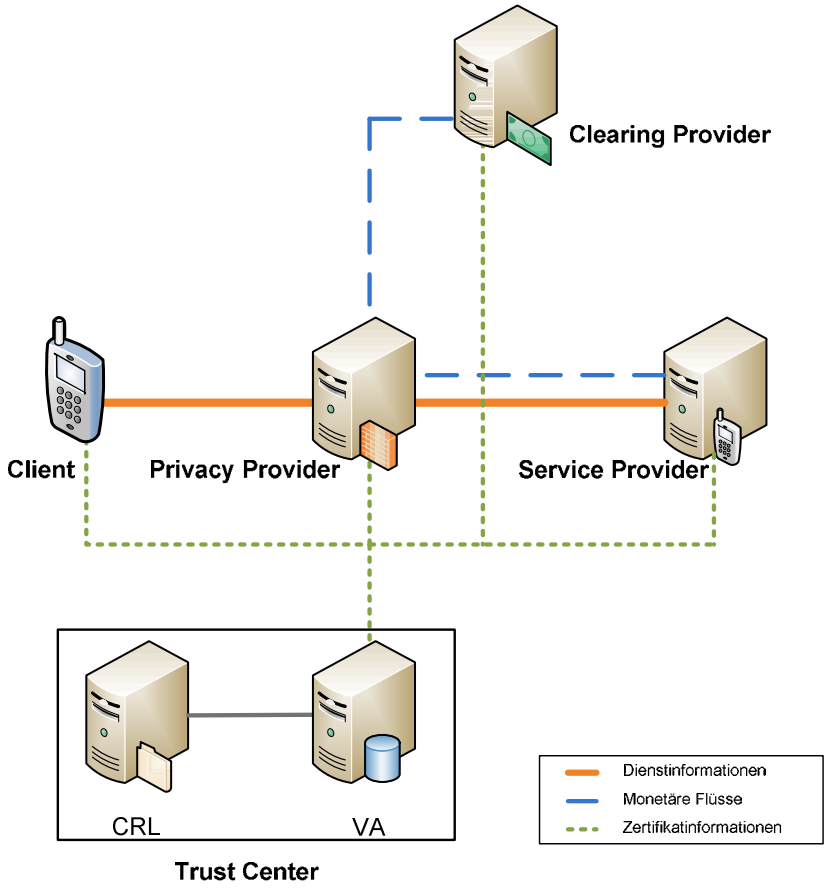


Abbildung 7 - Zahlungsvorgang bei einer Dienstnutzung

4.8 Auditing-Unternehmen

Da bei dieser Architektur jede Person und Institution die Möglichkeit besitzt, Dienste anzubieten, die auch in unterschiedlichen Ländern realisiert werden können, ist es für den Benutzer aufwendig, nachzuvollziehen, welchen Diensten und Anbietern er vertrauen kann. Das Vertrauen bezieht sich dabei auf die Nutzung von personenbezogenen Daten. (Werden nur die Daten der notwendigen Detaillierungsstufe angefragt, die für die Dienstleistung notwendig sind? Geschieht dies zum Beispiel durch eine Bereitstellung des idealen „Default-Regelsatzes“ für die Dienstnutzung? Werden diese Kontextinformationen nach der Dienstleistungserbringung für andere Aufgaben verwendet, über die der Benutzer nicht informiert worden ist? Ist die Kostenstruktur für den Benutzer transparent?) Da dem Benutzer die Möglichkeit gegeben werden soll, schnell die geeigneten Dienste zu ermitteln, können sich Dienstanbieter von einem unabhängigen Auditing-Unternehmen prüfen lassen. Bei einer erfolgreichen Prüfung erhält ein vorliegendes Zertifikat weitere Attribute und eine Signierung vom Auditing-Unternehmen, so dass ersichtlich ist, dass die definierten Anforderungen erfüllt worden sind. Der Benutzer kann bei einer Suche nach Diensten die Ergebnismenge so festlegen, dass nur geprüfte Anbieter angezeigt werden. Die Prüfung besitzt somit für diese zusätzlich einen Werbe-Effekt. Bei Diensten ohne diese Prüfung muss der Benutzer manuell prüfen, ob die von ihm definierten Anforderungen eingehalten werden.

5 Bereitstellung von ortsbezogenen Kontextinformationen für die Dienste und Anwendungen

Bei ortsbezogenen Kontextinformationen handelt es sich um eine spezielle Form der Kontextdaten. Diese Daten besitzen eine hohe Schutzwürdigkeit, da sie einen großen Einblick in das Umfeld des Benutzers ermöglichen. Zusätzlich müssen ortsbezogene Kontextinformationen oft aktualisiert werden. Zur Ermittlung der Position eines Benutzers eigenen sich unterschiedliche Technologien. In diesem Kapitel werden die möglichen Technologien vorgestellt und die Instanzen der Architektur beschrieben. Eine Herausforderung in diesem Zusammenhang besteht darin, dass es keine Technologie gibt, die in jeder Situation eingesetzt werden kann und dabei eine identisch hohe Genauigkeit bereitstellt. Im Besonderen muss unterschieden werden zwischen Technologien, die für den In-Door- bzw. Out-Door-Bereich eingesetzt werden können. Beim In-Door-Bereich handelt es sich um die Technologien, die innerhalb von Gebäuden eingesetzt werden. Je nach verwendeter Technologie unterscheiden sich das Einsatzgebiet, die Genauigkeit, die Abdeckung, der Zeitbedarf und die Kosten für eine Positionsermittlung. Abbildung 8 zeigt die unterschiedlichen Technologien zur Positionsbestimmung. Bei diesen Technologien wird zwischen den zumeist weltweit verfügbaren Satellitennavigationstechnologien, den oft räumlich begrenzten netzwerkgestützten Anwendungen und den Verfahren unterschieden, die speziell für die Ermittlung der Position innerhalb von Gebäuden entwickelt worden sind. Keine Positionsbestimmungstechnologie liefert für jede Situation die idealen Ergebnisse. Das folgende Kapitel beschreibt die Berücksichtigung unterschiedlicher Technologien innerhalb der Architektur mit dem Ziel, ortsbezogene Kontextinformationen in Form von Positionskoordinaten den jeweiligen Diensten bereitzustellen.

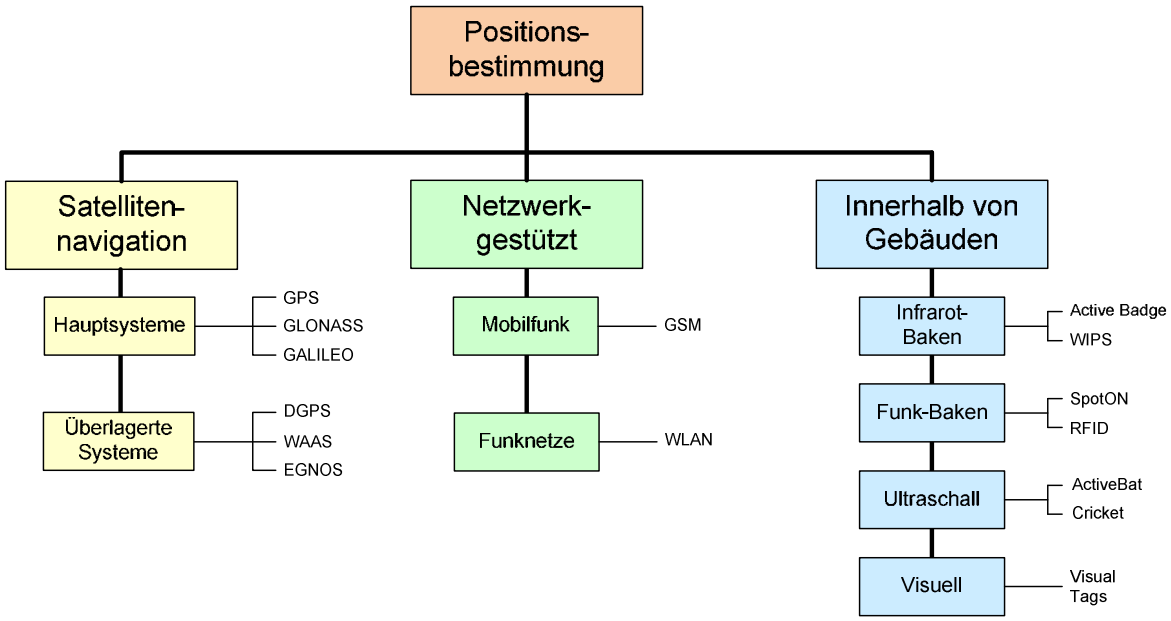
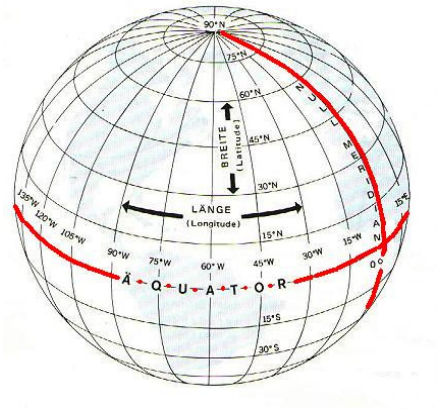


Abbildung 8 - Lokalisierungtechnologien (in Anlehnung an [Ro05])

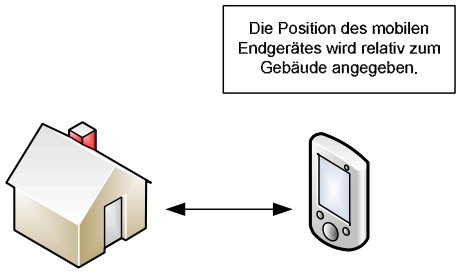
Unterschieden werden die Technologien nach der Stelle an der die Positionsbestimmung erfolgt. Terminal-based Technologien wie z.B. GPS ermitteln im Endgerät die Position. Bei network-based Technologien hingegen wird die Position innerhalb des Netzwerkes durch einen speziellen Dienst berechnet. Zusätzlich gibt es terminal-assisted Technologien, die basierend auf einem Ergebnis des Endgerätes im Netzwerk die Position ermitteln.

Ortsbezogene Anwendungen und Dienste benötigen für die Diensterbringung die Position einer Person oder die eines beteiligten Objektes. Der Dienst oder die Anwendung muss dazu die Eigenschaft der „Location Awareness“ besitzen. Dieser Begriff gehört zu dem Oberbegriff „Context Awareness“ [Ro05]. Nach Dey und Abowed handelt es sich bei Kontext-Informationen um Informationen, die die Situation einer am Dienst beteiligten Einheit, wie z.B. einer Person oder eines Objektes, charakterisieren und bei der Diensterbringung berücksichtigt werden [De99].
Das folgende Kapitel beschreibt Lokalisierungstechnologien, die bei ortsbezogenen Diensten Anwendung finden. Positionsinformationen können dabei in unterschiedlicher Form repräsentiert werden [Ro05]:



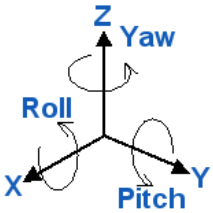
Die Position kann in Form von Längengrad, Breitengrad und der Höhe eines Objektes dargestellt werden. Dieses weltweit geläufige Format wird von vielen Anwendungen genutzt. Je nach Anwendung oder Land kommen spezielle Koordinatensysteme zum Einsatz. Bei Bedarf kann die ermittelte Position in ein anderes System transformiert werden.

Abbildung 9 - Längen- und Breitengrade der Erde [Ha05]



Die Positionsangabe kann relativ zu einem angegebenen Objekt erfolgen. Bei dieser Form handelt es sich um die relative Position. Derartige Angaben werden primär bei Diensten und Anwendungen genutzt, die räumlich begrenzt operieren.

Abbildung 10 - Relative Position eines mobilen Endgerätes zu einem Objekt



Wird zu der Positionsinformation zusätzlich noch die Orientierung im Raum benötigt, so werden die Roll-Nick-Gier-Winkel (Roll-Pitch-Yaw) ermittelt.

Abbildung 11 - Roll-Nick-Gier-Winkel (Roll-Pitch-Yaw) [Va06]

Die Position eines Objektes wird zumeist in Form einer Koordinate innerhalb eines Koordinatensystems repräsentiert. Je nach Anwendung wird dabei eine 2D-, 2,5D- oder 3D-Koordinate verwendet. Bei 2D-Koordinaten handelt es sich um eine Position auf einer Fläche. Die 2,5-Koordinaten werden um eine Höheninformation ergänzt, die nur für ein spezielles Objekt gilt. Dabei kann es sich z.B. um die Information handeln, in welcher Etage sich ein Objekt befindet. Diese Höhe ist somit nur relativ zum Gebäude. Bei einer 3D-Koordinate wird die Höhe einheitlich repräsentiert. Dabei kann es sich z.B. um die Höhe über Normalnull handeln [KS05].

Für den Benutzer selbst ist die Positionsinformation in Form einer Koordinate oft zu abstrakt. Für ihn zählt die semantische Bedeutung einer Position. Verständlicher für den Benutzer ist es deshalb anzugeben, wie die Postadresse zu der vorhandenen Position lautet oder wie das Gebäude heißt und wo er sich innerhalb dieses befindet (Gebäude, Etage, Raum, ..). [Ro05]

Um Anwendungen zu erstellen, die für die globale Ebene angeboten werden, muss das System zwischen unterschiedlichen Koordinatensystemen umrechnen oder ein Koordinatensystem verwenden, das im globalen Umfeld gebräuchlich ist. Innerhalb von Deutschland wird beispielsweise das Gauss-Krüger-Koordinatensystem verwendet. Dieses ist jedoch auf die Bedürfnisse der Kartenerstellung in Deutschland angepasst und wird somit im Ausland nicht verwendet. Auf globaler Basis bietet sich das UTM-Koordinatensystem (Universal Trasverse Mercator) oder WGS 1984 an. Bei WGS 1984 handelt es sich um die Darstellung der Position in Form von Längen- und Breitengraden (siehe Abbildung 9). Dieses System wird auch von den meisten GPS-Empfängern verwendet.[Ja07]

Zur Ermittlung der Position wird entweder eine Methode oder eine Kombination aus mehreren verwendet. Abhängig von der verwendeten Methode handelt es sich um einen „Tracking-“ oder „Positioning“-Ansatz. Beim Tracking-Ansatz wird die Position eines Objektes durch externe Infrastruktur, wie z.B. ein Sensorennetzwerk ermittelt. Beim Positioning-Ansatz hingegen erfolgt die Positionsbestimmung direkt beim zu lokalisierenden Objekt. Das Endgerät verwendet in diesem Fall die vorhandene Infrastruktur, um die eigene Position zu ermitteln. Der „Tracking“-Ansatz besitzt das folgende Risiko: Dadurch, dass an einer externen Stelle die Position bekannt ist, kann diese Information auch an unbefugte Dritte gelangen. Bei dem Ansatz „Positioning“ hingegen hat der mobile Benutzer bzw. das mobile Objekt vollständig die Kontrolle darüber, wie die Informationen verwendet werden und wer Zugriff auf diese erhält [Ro05].
Die folgenden Ansätze können zur Positionsermittlung verwendet werden [Kü05]:

- Proximity Sensing
  Bei diesem Ansatz wird ermittelt, ob die mobile Gegenstelle sich im Umfeld einer stationären Infrastruktur befindet. Ermittelt das mobile Endgerät, dass es sich in der Fläche befindet, die von einem Bestandteil der Infrastruktur (z.B. einem Sender) abgedeckt wird, so wird die bekannte Position des stationären Bestandteils als Ortsinformation für die Diensterbringung verwendet. Die Genauigkeit dieser Methode ist abhängig von der Fläche, die vom stationären Bestandteil abgedeckt wird.

- Trilateration (Lateration)
  Bei der Lateration werden die Entfernungen zwischen dem mobilen Endgerät und mehreren Basisstationen ermittelt. Dadurch, dass die Standorte der Basisstationen als stationäre Bestandteile bekannt sind, können mehrere Entfernungen zwischen dem mobilen Endgerät und den jeweiligen Basisstationen ermittelt werden. Die Ermittlung der Entfernungen kann durch die Signallaufzeit erfolgen. Das ist sehr einfach, da die Wellenausbreitung von Schall, Funk oder Licht bekannt sind. Zusätzlich kann auch die Signalstärke bei der Berechnung berücksichtigt werden. Anhand der ermittelten Entfernungen von den Basisstationen kann ein Überschneidungspunkt gefunden werden. Bei diesem Punkt handelt es sich um die Position des mobilen Endgerätes. Eine Hauptschwierigkeit bei diesem Ansatz ist z.B. die exakte Messung der Zeit für die Signalausbreitung. Je nach verwendetem Signal können auch noch weitere Einflüsse wie z.B. die Mehrwegausbreitung von Signalen die Messung beeinträchtigen.

- Triangulierung (Angulation)
  Bei der Triangulierung kann die Position eines mobilen Endgerätes auf einer 2D-Fläche ermittelt werden. Notwendig ist dafür wieder, dass die Position der stationären Bestandteile bekannt ist. Im Weiteren besitzen diese Basisstationen Antennen mit Richtcharakteristika. Somit kann ermittelt werden, aus welcher Richtung ein Signal eintrifft. Anhand von Messwerten von 3 unterschiedlichen stationären Bestandteilen kann ein Punkt ermittelt werden, an dem sich diese Linien schneiden. An diesem Punkt befindet sich die mobile Gegenstelle. Problematisch bei diesem Ansatz ist, dass die Richtcharakteristika z.B. der Richtantennen nur aus einem Winkelbereich die Signale empfangen. Das verursacht Ungenauigkeiten bei der Winkelmessung. Für das Problem bei trigonometrischen Ansätzen ist grundlegend, dass sich Winkelfehler, desto weiter ein Objekt entfernt ist, noch weiter verstärken.

- Trägheitsmessung (Dead Reckonig)
  Diese Methode verwendet unterschiedliche Sensorenwerte, um eine Position durchgehend weiter berechnen zu können. Dazu besitzt ein Objekt beispielsweise folgende Sensoren: Odometer (zurückgelegte Strecke), Gyroskope (Richtungswerte), Beschleunigungsmesser (Beschleunigung). Zu Beginn muss das Objekt die eigene Position kennen. Darauffolgend wird die neue Position anhand der Sensorenwerten berechnet. Dies ist besonders dann vorteilhaft, wenn keine externe Infrastruktur verfügbar ist. Die Genauigkeit dieses Ansatzes hängt jedoch stark davon ab, wie gut die verwendeten Sensoren sind.

- Mustererkennung der Signalcharakteristik (Pattern Matching)
  Bei der Mustererkennung werden Informationen ermittelt, die später mit bereits gespeicherten Mustern verglichen werden. Bei diesem Verfahren werden als Messwerte z.B. bei Funksignalen Signalstärke und Rauschverhältnis ermittelt. Für eine optische Ermittlung wird z.B. ein Bild erstellt. Diese Werte werden mit den bereits gespeicherten Mustern verglichen. Das Muster, das die höchste Ähnlichkeit aufweist, und eine vordefinierte Schwelle überschreitet, befindet sich somit im direkten Umfeld des mobilen Endgeräts. Die Standorte der gespeicherten Muster sind bekannt. Deshalb wird der Standort des ermittelten Musters als Ortsinformation für die spätere Diensterbringung verwendet.

- Hybride Ansätze
  Eine Kombination aus mehreren Ansätzen ermöglicht es oft, die Genauigkeit zu steigern oder Messfehler zu reduzieren. Zusätzlich werden hybride Ansätze verwendet, falls eine Methode allein an einem bestimmten Punkt keine Position ermitteln kann.

Eine besondere Herausforderung sind Dienstleistungen, die sowohl außerhalb wie auch innerhalb von Gebäuden angeboten werden. Außerhalb von Gebäuden werden Techniken benötigt, die oft weitflächig verfügbar sind. Diese Techniken sind meistens innerhalb von Gebäuden zu ungenau oder überhaupt nicht nutzbar. Daher müssen meistens speziell in diesem Umfeld hybride Verfahren eingesetzt werden, die eine Positionsbestimmung mit Hilfe von mehreren unterschiedlichen Messverfahren realisieren.

Innerhalb von Gebäuden besteht je nach Anwendung die Aufgabe der Lokalisierungstechnologien darin, zu ermitteln, in welchem Zimmer und welcher Etage sich eine Person oder ein Objekt befindet. Genauigkeiten, wie sie von Verfahren bereitgestellt werden, die vornehmlich außerhalb von Gebäuden eingesetzt werden, würden innerhalb von

Gebäuden nicht die benötigte Präzision besitzen. Zusätzlich führen Hindernisse in einem Raum dazu, dass die Positionsfeststellung oft nur sehr ungenau ist. Um diesen unterschiedlichen Anforderungen gerecht zu werden, wurden spezielle Techniken entwickelt, die für das spezielle Umfeld oder für die speziellen Anforderungen eine ausreichende Genauigkeit bieten.

Bei den unterschiedlichen Techniken zur Positionsbestimmung kann man zwischen den folgenden drei Kategorien unterscheiden (siehe Abbildung 8) [Ro05]:

- Satellitenbasierte Positionsbestimmung
- Netzwerkgestützte Positionsbestimmung
- Positionsbestimmung innerhalb von Gebäuden

5.1 Satellitenbasierte Positionsbestimmung

Der Hauptbestandteil der satellitenbasierten Infrastruktur befindet sich im Orbit um die Erde. Neben den Satelliten benötigt ein derartiges System noch eine Kontrollinfrastruktur, die sich um die Wartung und Aufrechterhaltung des Dienstes kümmert. Im Weiteren besitzen die mobilen Endgeräte spezielle Empfänger, um die Signale des Satelliten zu empfangen.

Das bekannteste satellitenbasierte System ist GPS (Navstar Global Positioning System). Es handelt sich um ein global verfügbares System, das aus mindestens 24 Satelliten besteht, bei dem die Satelliten auf unterschiedlichen Orbits die Erde umkreisen. Zu jedem Zeitpunkt ist dadurch sichergestellt, dass ein Empfänger mindestens 4 Satelliten in Empfangsreichweite hat. Dieses System verwendet als Lokalisierungsmethode die Lateration. Jeder Satellit sendet ein sehr präzises Zeitsignal und weitere Informationsdaten, wie z.B. die Flugbahn der Satelliten, aus. Dadurch weiß der Empfänger, wo sich die Satelliten bei einer Messung befinden. Aus den unterschiedlichen Zeitsignalen, die er von den Satelliten in seiner Empfangsreichweite erhält, kann er die Entfernung zu jedem Satelliten berechen. Durch diese Daten erhält er seine eigene Position. Ein Vorteil dieses Systems ist, dass die Positionsermittlung im Endgerät erfolgt. Somit besitzt es keine Begrenzung der Benutzerzahl, da keine Kommunikation mit den Satelliten notwendig ist. Die Genauigkeit dieses Systems liegt im Normalfall im Bereich von 10 m. Je nach Außeneinflüssen kann diese Genauigkeit aber auch stark variieren. Besonders problematisch sind Situationen, in denen keine direkte Sichtlinie zu den Satelliten existiert. Dies tritt z.B. in Straßenschluchten, Gebirgen, Wäldern oder innerhalb von Gebäuden auf. In diesem Fall ist die Positionsermittlung nur eingeschränkt oder sogar überhaupt nicht möglich. Daher ist das GPS nicht für die Positionierung innerhalb von Gebäuden geeignet, da in diesem Fall die Decke und Wände das Signal zu stark abschwächen. Ausreichend sensible Empfänger ermöglichen mit Hilfe von GPS eine Positionsermittlung im Nahbereich eines Fensters, falls sie die ausreichende Anzahl an Satelliten empfangen können.

Ein Problem dieses Systems besteht darin, dass vor der eigentlichen Positionsermittlung der vollständige Datensatz Almanach-Daten (Ephemeris) vom Satellit empfangen werden muss. Aus diesem Datensatz kann der Empfänger die Standorte der sichtbaren Satelliten berechnen. Dieser Datensatz wird jedoch mit einer sehr geringen Datenrate gesendet (50 Baud), so dass die erste Ermittlung der Position, je nach Empfänger und bereits vorhandenen Daten, mehrere Minuten dauern kann. Der Empfänger benötigt dazu beim Empfang relativ viel Strom.

Um die Genauigkeit des Systems weiter steigern zu können, müssen die Fehlerquellen der Positionsermittlung reduziert oder bei der Berechnung korrigiert werden. Die folgenden Punkte reduzieren die Genauigkeit der Positionsermittlung (der Wert in der Klammer bezeichnet den durchschnittlichen Fehler durch diese Fehlerquelle) [Ro05]:

- Uhrfehler (1,5 m)
  - Ungenauigkeit der Uhr im Empfänger

- Schwankungen in der Umlaufbahn (2,5 m)
  - Einflüsse durch Gravitationskräfte (Mond, Sonne) – beeinflussen die Laufbahn.

- Störungen in der Atmosphäre (0,5 m)
  - Änderung der Druck- und Wetterverhältnisse beeinflussen das Signal.

- Störungen in der Ionosphäre (5,0 m)
  - Geladene Teilchen stören die Signalausbreitung.

- Multipath-Fehler (0,6 m)
  - Reflektierte Signale in der Umgebung des Empfängers.

- Selected Availability-Signal (24,0 m)
  - Dieses Signal verfälscht absichtlich die frei verfügbaren Informationen, um somit die Genauigkeit zu reduzieren. Das Signal wurde im Mai 2000 deaktiviert.

Mit Hilfe von D-GPS (Differential GPS) besteht die Möglichkeit, die Fehler, die durch atmosphärische Störungen aufgetreten sind, zu reduzieren. Dafür wird zusätzlich ein stationärer Empfänger (Referenzstation) verwendet, dessen Position im Vorfeld genau vermessen wurde. Er befindet sich im gleichen Gebiet wie der mobile Empfänger. Er empfängt somit zu jedem Zeitpunkt die gleichen Satelliten wie der mobile Empfänger und kann bei Bedarf die Korrekturdaten erzeugen. Diese Referenzstation ermittelt zu diesem Zweck per GPS die eigene Position. Aus dieser ermittelten Position und der bekannten Position wird ein Differenzdatensatz gebildet. Dieser Differenzdatensatz wird an den mobilen Empfänger übermittelt. Er verwendet ihn, um die ermittelten Daten zu korrigieren. Dadurch sind Genauigkeiten im Bereich von 1-3 m möglich [Ro05]. Die D-GPS Korrekturdaten können vom mobilen Empfänger über Daten- oder Funkverbindungen bezogen werden. Mit Hilfe der überlagernden Satellitennavigationsdienste (Satellite-Based Augmentation Systems) werden diese Daten auch über spezielle geostationäre Satelliten übermittelt (z.B. EGNOS - Geostationary Navigation Overlay System). Noch genauere Positionsermittlung ist dann möglich, wenn Empfänger mit sehr genauen Uhren verwendet werden und eine eigene Referenzstation sich im direkten Umfeld befindet. In diesem Fall kann GPS auch für den Bereich der Vermessung verwendet werden, da Genauigkeiten unter einem Meter erreicht werden.

Um besonders im mobilen Umfeld den Zeitbedarf für die erste Positionsermittlung zu reduzieren, gibt es die Erweiterung A-GPS (Assisted GPS). Bei dieser Erweiterung werden die notwendigen Daten zur Flugbahnbestimmung (Ephemeris) der Satelliten dem mobilen Endgerät z.B. über eine mobile Datenverbindung bereitgestellt. Dadurch entfällt der Schritt, dass der Empfänger diese Daten vom Satelliten empfangen muss. Eine Positionsbestimmung ist somit innerhalb von wenigen Sekunden möglich. Ein zusätzlicher Vorteil dieser Erweiterung besteht darin, dass der Empfänger, falls eine Position seltener ermittelt wird, nicht durchgehend die Signale zu empfangen und zu verarbeiten braucht. Dies reduziert den Stromverbrauch und dadurch die Akkulaufzeit. Zusätzlich kann dieser Ansatz mit D-GPS kombiniert werden, so dass eine schnelle Ermittlung von sehr genauen Daten auch im mobilen Umfeld möglich wird.

Neben dem amerikanischen Satellitensystem GPS existieren noch zwei weitere Systeme, die jedoch zum jetzigen Zeitpunkt[6] noch nicht weltweit nutzbar sind. Bei dem System „Galileo“ handelt es sich um das europäische Gegenstück zu GPS. Dieses soll nach der Fertigstellung jedoch eine höhere Genauigkeit ermöglichen und unterschiedliche Leistungsklassen anbieten. Zusätzlich bietet dieses System die Weiterleitung von empfangenen Notrufen [EuK07, Wil07].

Bei dem System Glonass (Globalnaya Navigationmaya Sputnikovaya Sistema)
handelt es sich um ein russisches Satelliten-Navigationssystem. Dieses wurde jedoch aufgrund von Finanzierungsproblemen längere Zeit nur noch unzureichend gewartet, so dass es zurzeit nur zu einem Bruchteil zur Verfügung steht [Ro05]. Die Russische Förderation hat sich jedoch das Ziel gesetzt, dieses System in verbesserter Form bis zum Jahr 2011 wieder weltweit mit einer Genauigkeit von bis zu einem Meter zur Verfügung zu stellen [Ger07].

Eine weitere Steigerung der Genauigkeit kann dadurch erreicht werden, dass zukünftig Empfänger produziert werden, die alle Satelliten der verfügbaren Satellitennavigationssysteme nutzen.

5.2 Netzwerkbasierte Infrastruktur (Cellular Infrastructure)

Bei Lokalisierung innerhalb von netzwerkbasierten Infrastrukturen wie z.B. Mobilfunknetzen stehen unterschiedliche Methoden bereit, um den Standort von mobilen Endgeräten zu ermitteln. Die Genauigkeit und der notwendige Aufwand der unterschiedlichen Methoden unterscheiden sich dabei zum Teil recht stark.

Der nächste Abschnitt beschreibt die folgenden Verfahren zur Positionsbestimmung [TVM03]:

- CI – Cell Identifier
- TOA – Time of Arrival
- AOA – Angle of Arrival
- E-OTD – Enhanced Observed Time Difference
- U-TDoA – Uplink Time of Arrival

[6] August 2007

CI – Cell Identifier

Der Standort jeder Mobilfunkzelle ist im Vorfeld bekannt und sie besitzt eine eindeutige Identifizierung (Cell Identifier). Durch diese Information lässt sich die Zelle, in der ein mobiles Endgerät eingebucht ist, sehr einfach ermitteln. Bei dieser Methode wird der Proximity-sensing-Ansatz verwendet. Sowohl das mobile Endgerät, als auch das Netzwerk können den Cell Identifier ermitteln. Routinemäßig wird dieser Vorgang im Netzwerk vorgenommen, da der Cell Identifier bereits für den regulären Betrieb ermittelt werden muss. Zusätzlich müssen nur an einer zentralen Stelle die Standorte der Basisstationen vermerkt werden.

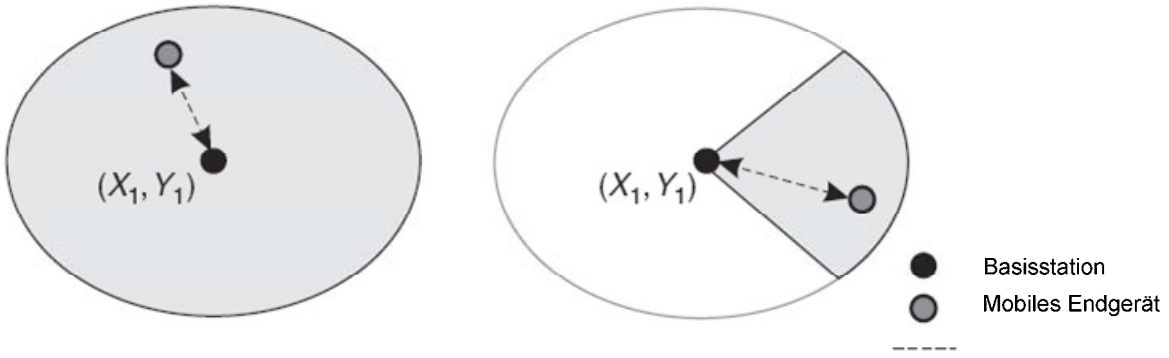


Abbildung 12 - Ermittlung der Position mit Hilfe des Cell Identifiers [Kü05]

Abbildung 12 zeigt die Ermittlung der Position mit Hilfe des Cell Identifiers. Die linke Grafik zeigt dabei eine Zelle, die eine Antenne zur Versorgung verwendet. Wird in der Zelle ein mobiles Endgerät ermittelt, so wird der Standort der Basisstation als Position des Endgerätes verwendet. In der rechten Grafik kann diese Information dadurch präzisiert werden, dass eine Zelle durch mehrere Antennen abgedeckt wird, die einzelne Sektoren versorgen. In diesem Fall wird der Sektor mit der höchsten Signalstärke bei der Positionsermittlung berücksichtigt. Ein Problem dieses Ansatzes ist es, dass sich die Größen der Zellen stark unterscheiden. Sie sind abhängig von ihrem Standort und der Verwendung. Zum Beispiel ist eine Positionsermittlung innerhalb einer Stadt wesentlich genauer als auf dem Land, da die Zellengröße aufgrund der starken Nutzung kleiner sind. Der Durchmesser einer Zelle kann im D-Netz bis zu 35 km und im E-Netz bis zu 8 km betragen [Ro05]. Dies führt dazu, dass diese Methode als ungenau angesehen werden muss. Der Vorteil dieser Methode besteht darin, dass alle notwendigen Daten bereits beim normalen Betrieb des Netzwerks erhoben werden und somit keine nachträglichen Ergänzungen an der Infrastruktur notwendig sind.

TOA – Time of Arrival

Die heutigen Mobilfunknetze verwenden unter anderem das Zeitmultiplexverfahren, um einzelne Kanäle für mehrere Teilnehmer zur Verfügung zu stellen. Um sicherzugehen, dass die einzelnen Teilnehmer ihren zugewiesenen Zeitschlitz auch ohne Beeinflussung der anderen Teilnehmer nutzen, ermittelt das Netzwerk die Signallaufzeit zwischen dem mobilen Endgerät und der Basisstation. Dieser Wert (TA – Time Advance) wird dazu verwendet, um dem Endgerät den richtigen Beginn und das exakte Ende des nutzbaren Zeitschlitzes zu signalisieren, so dass die Teilnehmer sich nicht gegenseitig stören.
Die Signallaufzeit zwischen einem mobilen Endgerät und der Basisstation kann zur Entfernungsberechnung verwendet werden, da im Vorfeld die Ausbreitungsgeschwindigkeit des Funksignals bekannt ist.

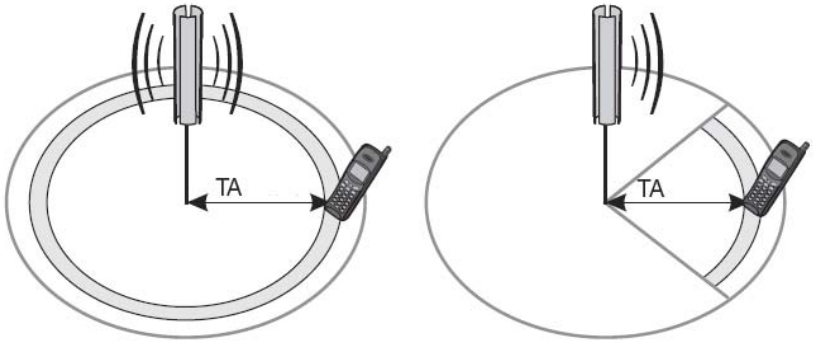


Abbildung 13 - Ermittlung der Position mit Hilfe von Time Advance [Kü05]

Abbildung 13 zeigt, dass durch die Ermittlung des TA-Wertes und des Cell Identifiers, die Fläche innerhalb der Zelle ermittelt werden kann, in der sich das mobile Endgerät befindet. Diese Fläche ist viel genauer zu bestimmen als dies nur unter Zuhilfenahme des Cell Identifiers geschehen kann. Die rechte Abbildung zeigt, dass, wenn die Zelle durch mehrere Antennen abgedeckt wird, die jeweils einen eigenen Sektor haben, eine präzisere Ortsangabe möglich ist.

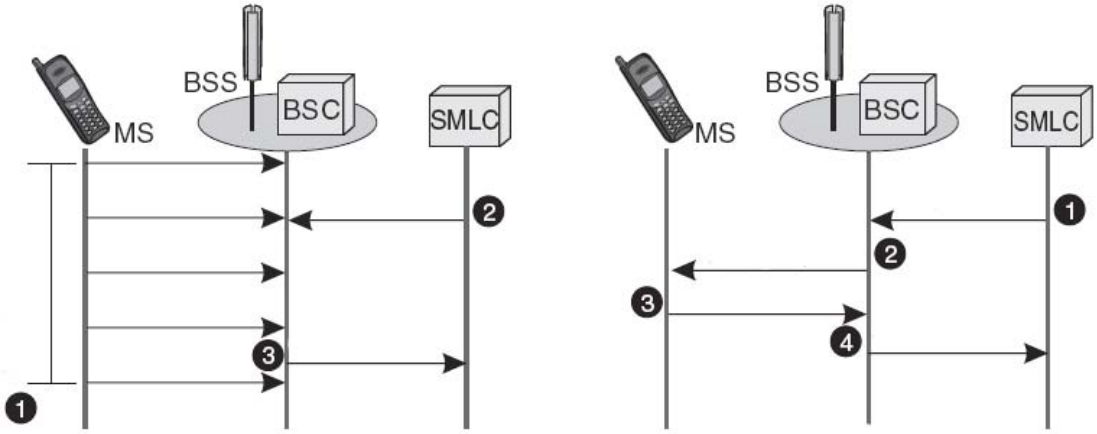


Abbildung 14 - Ermittlung des TA-Wertes [Kü05]

Für die Ermittlung des TA-Wertes muss eine aktive Funkverbindung zwischen dem mobilen Endgerät und der Basisstation bestehen. Allerdings unterscheidet sich der Vorgang der Ermittlung des TA-Wertes darin, ob sich ein mobiles Endgerät im Idle-Mode befindet (Gerät wartet auf eingehende Verbindungen), oder ob es aktiv das Mobilfunknetz benutzt (z.B. bei einer Datenverbindung oder einem Telefonat).

Abbildung 14 zeigt auf der linken Seite das Vorgehen bei einer aktiven Verbindung. In diesem Fall sendet das mobile Endgerät (MS) durchgehend Signale zur Basisstation (BSS). Zur Standortermittlung fragt der SMLC (Serving Mobile Location Center) bei der Basisstation, wo der Benutzer angemeldet ist, den zurzeit aktuellen TA-Wert ab. Bei einer aktiven Verbindung ermittelt der BSC (Base Station Controller) durchgehend den TA-Wert, um die fehlerfreie Nutzung der Zeitschlitze zu gewährleisten.

Die rechte Seite der Abbildung zeigt hingegen das mobile Endgerät im Idle-Mode. Zu Beginn muss der SMLC den TA-Wert beim BSC anfragen. Da zu diesem Zeitpunkt der Wert noch nicht bekannt ist, muss er ermittelt werden. Dafür wird im nächsten Schritt ein Paging-Signal an das mobile Endgerät gesendet. Da das Endgerät dadurch gezwungen wird zu antworten, kann der TA-Wert ermittelt werden. Die so ermittelten Werte werden vom BSC zum SMLC übertragen.

AOA – Angle of Arrival

Besitzt eine Basisstation eine Antenne mit Richtwirkung, so kann mit ihrer Hilfe der Winkel zwischen der Basisstation und dem mobilen Endgerät ermittelt werden. Durch den Einsatz von mehreren Basisstationen werden mehrere Winkel gemessen. Dadurch besteht die Möglichkeit zur Kreuzpeilung. Es wird hier das Verfahren der Angulation angewandt. Die Position des mobilen Endgeräts befindet sich genau im Schnittpunkt der von den Basisstationen ausgehenden und durch Winkel definierten gedachten Linien. Bei diesem Verfahren muss jedoch berücksichtigt werden, dass Antennen nicht auf den Grad genau das Signal ermitteln. Daher enthält die Messung eine gewisse Ungenauigkeit. Diese Ungenauigkeit verstärkt sich abhängig von dem Abstand zwischen der Basisstation und dem mobilen Endgerät. Eine Kreuzpeilung ermittelt somit nicht einen Punkt, an dem sich das mobile Endgerät befindet, sondern abhängig von den technischen Eigenschaften der Antenne eine Fläche, auf der sich das mobile Endgerät befinden kann (siehe Abbildung 15).

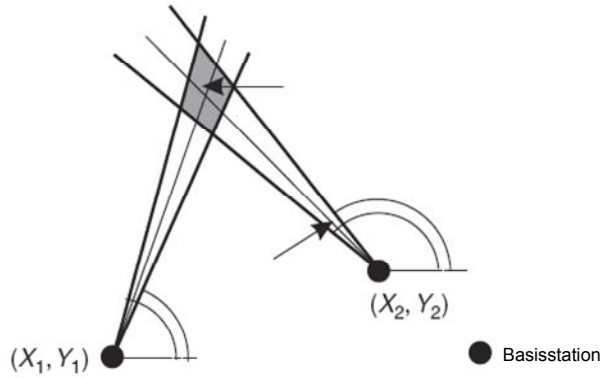


Abbildung 15 - Probleme bei der Ermittlung der Position mit Hilfe von AOA [Kü05]

Hybride Ansätze

Durch die Kombination mehrerer Methoden lässt sich die Genauigkeit einer Positionsermittlung weiter steigern. In Abbildung 16 werden auf der linken Seite der Cell Identifier und der TA-Wert dazu genutzt, die Fläche zu ermitteln, auf der sich das mobile Endgerät befindet. Auf der rechten Seite hingegen wird zusätzlich der Empfangswinkel der Signale zwischen der Basisstation und dem mobilen Endgerät berücksichtigt. Diese Kombination von Informationen erlaubt die Aussage, in welcher Zelle sich das Endgerät befindet, welchen Abstand es zur Basisstation besitzt und in welchem Winkel es zu ihr steht. Das Ergebnis ist dadurch um ein Mehrfaches genauer als die jeweiligen Einzelinformationen.

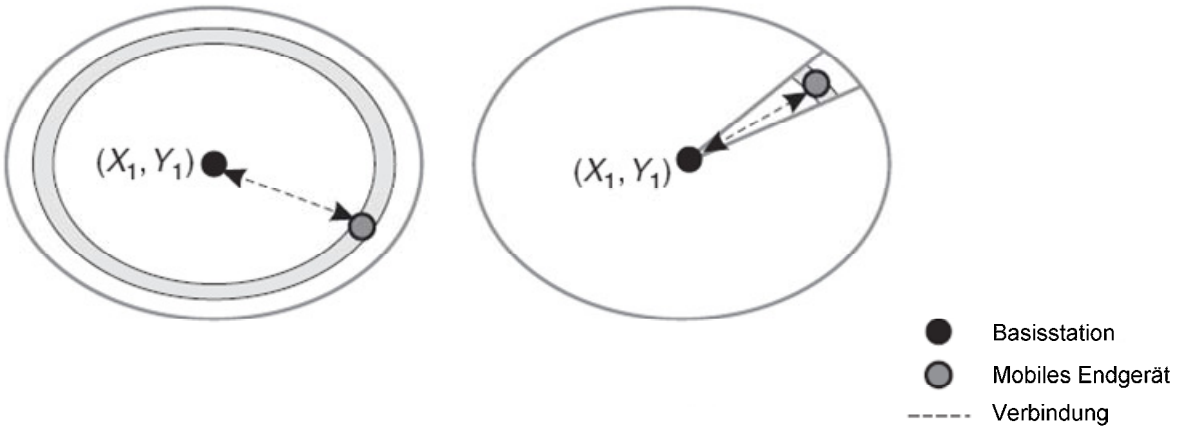


Abbildung 16 - Lokalisierung mit Hilfe von hybriden Ansätzen [Kü05]

E-OTD – Enhanced Observed Time Difference

Bei diesem Verfahren wird die Genauigkeit der Positionsermittlung dadurch erhöht, dass drei Basisstationen Ortungssignale an das mobile Endgerät senden (siehe Abbildung 17). Diese Signale werden vom Endgerät empfangen. Die Signale besitzen dabei abhängig von der Entfernung zu ihrer Basisstation eine unterschiedliche Laufzeit. Das Endgerät ist für diese Positionierungsart ausgelegt und erfasst die Laufzeitunterschiede (OTD – Observed Time Difference).

Da dem mobilen Endgerät die Positionen der Basisstationen nicht bekannt sind, kann es aus den Werten nicht die eigene Position ermitteln. Deshalb sendet das Endgerät die Informationen zurück an die Basisstationen, die diese Daten an das LMU (Location Measurement Unit) weiterleiten.

Die LMU empfängt die Signale der Basisstationen (RIT) und kann somit intern eine zeitlich synchrone Basis ermitteln. Dies ist notwendig, da die Basisstationen nicht synchrone Zeitschlitze verwenden. Die Zeitdifferenz, die das LMU ermittelt und die zusätzlichen vom mobilen Endgerät gesendeten Werte, werden dazu genutzt, die Position des mobilen Endgerätes zu berechnen [Kü05].

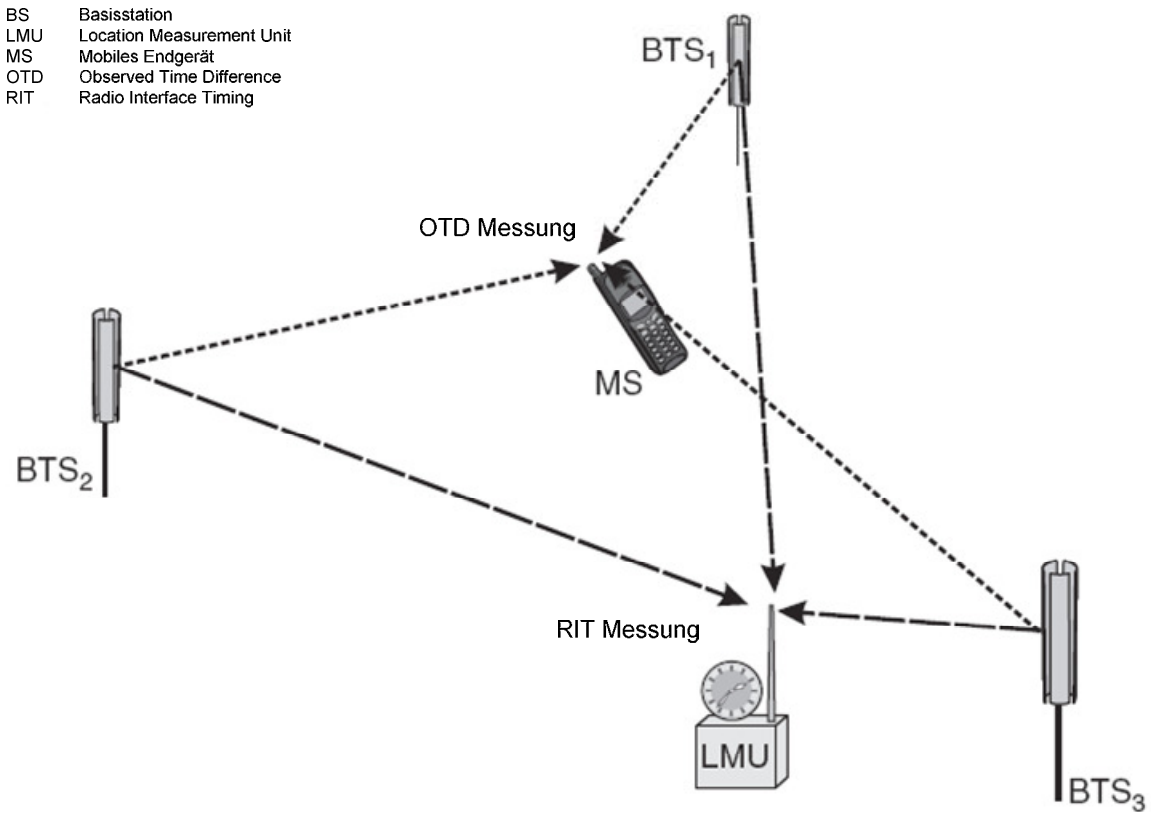


Abbildung 17 - RIT und OTD Messung [Kü05]

U-TDoA – Uplink Time of Arrival

Dieses Verfahren bietet eine sehr genaue Lokalisierung des mobilen Teilnehmers mit einer Genauigkeit von 50-150 m. Voraussetzung ist jedoch, dass der Teilnehmer sich in einem Gebiet befindet, in dem er in der Empfangsreichweite von mindestens vier Basisstationen steht. Die Laufzeitmessung der Signale, die zwischen dem mobilen Endgerät und den Basisstationen ausgetauscht werden, kann dazu verwendet werden, die Position, (vergleichbar

mit der Vorgehensweise beim GPS-System), zu berechnen. Dieses Verfahren benutzt die Zeitsignale der GPS-Satelliten zur Synchronisation der Basisstationen. Optional besteht auch die Möglichkeit, das mobile Endgerät ebenfalls mit einem GPS-Empfänger auszustatten.
Die bei diesem Verfahren gesammelten Entfernungen werden zum MPC (Mobile Positioning Center) übermittelt. Diese zentrale Stelle verarbeitet die Informationen und speichert sie zwischen. Sie können von Diensten abgerufen werden. Da es sich um sensible Daten handelt, sind für den Zugriff eine Benutzerkennung und ein Passwort notwendig [Ro05].

Vergleich der unterschiedlichen Lokalisierungsverfahren im Mobilfunknetz

Die in den vorherigen Seiten vorgestellten Lokalisierungsverfahren im Mobilfunknetz unterschieden sich teilweise stark im Bereich der Genauigkeit (siehe Tabelle 1). Zu beachten ist hier auch, dass aufgrund der Zellenstruktur des Netzes, sich die Genauigkeit zwischen ländlichen und städtischen Gebieten sehr stark unterscheiden kann. Zusätzlich sind bestimmte Anforderungen, die ein Lokalisierungsverfahren voraussetzt, wie z.B., dass sich ein mobiles Endgerät in einem Bereich befindet, in dem es mehrere Basisstationen in Reichweite gibt, nicht überall gegeben, was die Einsatzfähigkeit mancher Methoden einschränkt.

	Präzision der Position				
	Land	**Vorstadt**	**Stadt**	**Genauigkeit**	**Verfügbarkeit**
Cell-ID	> 10 km	2 – 10 km	50 – 1000 m	schlecht	gut
E-OTD & OTDoA	50 – 150 m	50 – 250 m	50 – 300 m	durchschnittlich	durchschnittlich
U-TDoA	50 – 120 m	40 – 50 m	40 – 50 m	durchschnittlich	durchschnittlich
A-GPS	10 – 40 m	20 – 100 m	30 – 150 m	gut	gut

Tabelle 1 - Leistung der unterschiedlichen Positionierungstechniken im Mobilfunknetz [Kü05]

Die vorgestellten Lokalisierungsverfahren unterscheiden sich nicht nur in der Qualität der Positionsermittlung, sondern auch in dem Aufwand, der für derartige Verfahren notwendig ist (siehe Tabelle 2). Den niedrigsten Aufwand besitzen Verfahren, die auf Werten basieren, die schon beim normalen Betrieb ermittelt werden. Diese Verfahren verursachen keine weiteren Kosten auf Seiten des Netzwerkbetreibers oder Endnutzers. Andere Verfahren fordern die Erweiterung der Infrastruktur um weitere Komponenten, wie z.B. das LMU oder SMLC. Zusätzlich sind je nach genutztem Verfahren auch Änderungen am Endgerät selber notwendig, damit dieses das Verfahren unterstützen kann. Bei manchen Verfahren werden zusätzliche Informationen über Funk zum mobilen Endgerät gesendet, um so eine Positionsermittlung überhaupt erst möglich zu machen. Dies führt zu einer zusätzlichen Belastung des Netzwerks und somit zu einem Overhead. Entscheidend für manche Anwendungen ist auch der Zeitbedarf bis zur ersten Positionsermittlung (TTFF – Time To First Fix).

Die zusätzlichen Investitionen und der durch die Positionierungsverfahren verursachte Overhead führen dazu, dass in vielen Netzen Lokalisierungsverfahren mit einer hohen Präzision noch nicht verfügbar sind.

	TTFF	**Endgerät**	**Overhead**	**Kosten**
Cell-ID	~ 1 sek.	Keine Änderungen	sehr niedrig	Sehr niedrig
E-OTD & OTDoA	5 – 10 sek.	Spezielle Software	mittelmäßig / hoch	hoch
U-TDoA	5 – 10 sek.	Keine Änderungen	mittelmäßig	mittelmäßig
A-GPS	5 – 10 sek.	Spezielle Software	mittelmäßig / hoch	niedrig bis mittelmäßig

Tabelle 2 - Aufwand für die unterschiedlichen Positionierungstechniken im Mobilfunknetz [Kü05]

5.3 Lokalisierung innerhalb von Gebäuden (Indoor Infrastructure)

Die Lokalisierung innerhalb von Gebäuden stellt an die Technik wesentlich höhere Ansprüche. Die meisten Anwendungen benötigen eine Genauigkeit, die ausreicht, um den Raum und das Stockwerk zu ermitteln. Somit können solche Techniken nicht verwendet werden, die nur eine Genauigkeit von 3 m oder schlechter aufweisen. Außerdem darf die Genauigkeit der ermittelten Werte nicht zu stark schwanken. Eine zusätzliche Herausforderung dieses Umfeldes ist es, dass sich innerhalb von Räumen viele Hindernisse (z.B. Möbel, Menschen und Geräte) befinden, die eine Ortsbestimmung beeinflussen können. Zudem können der Standort und die Menge der Hindernisse innerhalb der Nutzungszeit variieren.

Um eine hohe Genauigkeit zu erreichen, muss innerhalb des Gebäudes eine Infrastruktur aufgebaut werden, die eine ausreichend hohe Abdeckung erzielt. Folgende Ansätze können verwendet werden:

5.3.1 Funkbasierte In-Door-Lokalisierungstechniken

Die folgenden Ansätze verwenden Funksignale zur Lokalisierung:

WLAN (Wireless Area Network)

In vielen Gebäuden besteht bereits eine Infrastruktur, basierend auf WLAN (Wireless Local Area Network). Dieses Netz kann auch zur Lokalisierung eines mobilen Endgerätes verwendet werden. Die Infrastruktur erhält somit neben der primären Aufgabe, einen Datenaustausch zwischen den drahtlos angebundenen Endgeräten und dem kabelgebundenen Netzwerk zu ermöglichen, eine weitere zusätzliche Aufgabe. Sie kann zur Positionsermittlung verwendet werden. Um diese zu erfüllen, muss eine ausreichende Anzahl von Access-Points bereitstehen, die es ermöglichen, dass an jedem Ort der versorgten Fläche mehr als ein Access-Point empfangen werden kann. Die mobilen Endgeräte müssen mit WLAN-Modulen ausgestattet sein. Diese suchen durchgehend nach Access-Points im Empfangsbereich. Von den erkannten Access-Points werden im regelmäßigen Abstand die Signalstärke und der Signal-Rausch-Abstand ermittelt. Eine eindeutige Identifikation des Access-Points ist anhand der MAC-Adresse möglich.

Um aus diesen Informationen die Position des mobilen Endgeräts zu erhalten, müssen im Vorfeld die Standorte der Access Points und die spezifischen Eigenschaften der Umgebung ermittelt werden. Zu diesem Zweck wird das Umfeld vermessen. Dazu werden Referenzpunkte definiert. An diesen Punkten wird gemessen, welche Access-Points verfügbar sind und welches charakteristische Signal an diesem Referenzpunkt vom mobilen Endgerät empfangen wird. Diese Informationen werden als eine Art „Fingerabdruck“ in einer Datei oder einer Datenbank gespeichert.

Abbildung 18 zeigt, wie in Form einer Karte die Referenzpunkte im Vorfeld festgelegt werden können. In dieser Karte sind auch die Access-Points mit ihrem Standort vermerkt. Durch diese Messung kann auch schon eingeschätzt werden, welche Genauigkeit in diesem Umfeld erreicht wird. Ist die Abdeckung durch die Access-Points nicht ausreichend, so können weitere an geeigneten Punkten platziert werden. Zu beachten ist hierbei, dass eine Veränderung der Konfiguration ein erneutes Ausmessen notwendig macht. Falls nun ein mobiles Endgerät seine eigene Position ermitteln möchte, so muss es am aktuellen Standort die Anzahl und Signalqualität der Signale des Access-Points ermitteln. Mit Hilfe der zuvor ermittelten Referenzpunkte wird per Pattern Matching nun der Punkt gesucht, der die höchste Ähnlichkeit aufweist. Problematisch bei diesem Ansatz ist, dass die Funkwellen, die bei WLAN verwendet werden, durch Hindernisse beeinflusst (reflektiert oder abgedämpft) werden können. Dies führt zu einer ungenaueren Positionsermittlung. Bei diesen Hindernissen kann es sich zum Beispiel um Personen oder Einrichtungsgegenstände handeln, die ihren Standort besonders im Büroumfeld oft ändern können. Dadurch ändern sich auch die Werte an den Referenzpunkten.

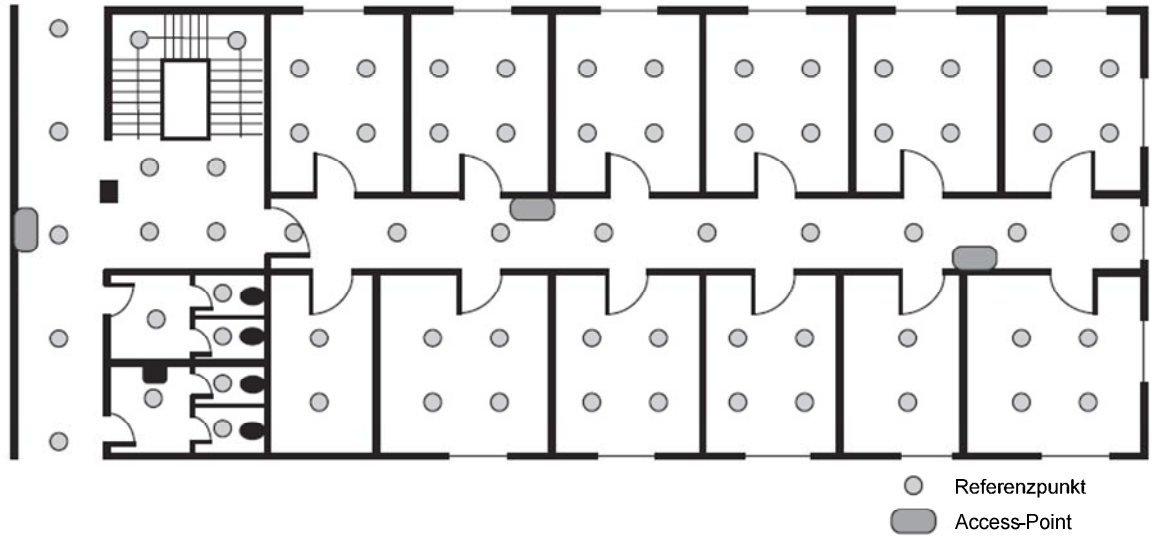


Abbildung 18 - Erstellen eines WLAN-Fingerprints (nach [Kü05])

Eine derartige Positionsermittlung kann auf drei unterschiedlichen Arten erfolgen (siehe Abbildung 19):

- Terminal-assisted mode
- Terminal-based mode
- Network-based mode

Die Modi unterscheiden sich durch die Instanzen, die an der Positionsbestimmung beteiligt sind. Der Ort, an dem das Ergebnis berechnet wird, ist ebenfalls verschieden.

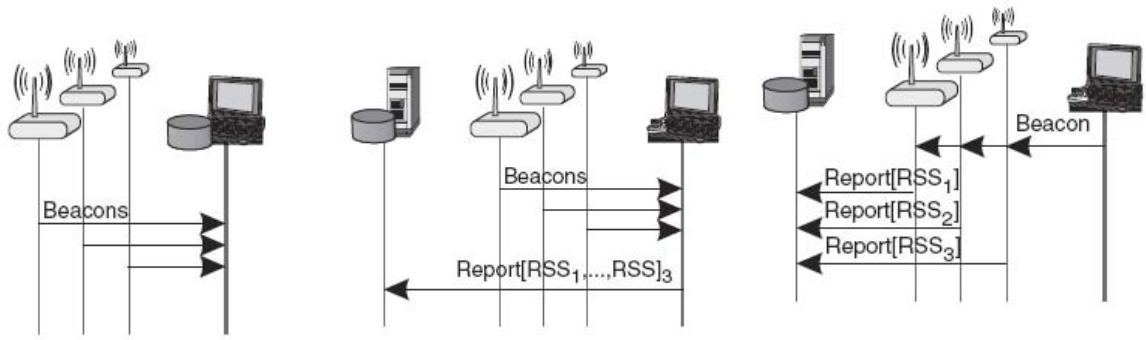


Abbildung 19 - Unterschiedliche Modi zur Ermittlung von WLAN Fingerprints [Kü05]

Beim „Terminal-based mode“ handelt es sich um den einfachsten Modus. In diesem Fall besitzt das mobile Endgerät alle Informationen über die Referenzpunkte. Das Gerät ermittelt die Signalqualität der Access-Points im Umfeld und findet anhand des Wissens über die Referenzpunkte die eigene Position. Bei einem derartigen Vorgehen ist keine Modifikation an einer bestehenden Infrastruktur notwendig.

Eine Ergänzung der Infrastruktur ist hingegen beim „Terminal-assisted mode“ notwendig. Bei diesem Modus verfügt das Netzwerk über eine zentrale Instanz, die alle Informationen über Referenzpunkte besitzt. Das mobile Endgerät übermittelt die gemessene Signalqualität an diese Instanz. Dort wird die Position des mobilen Endgeräts gefunden. Dieser Modus hat besonders dann Vorteile, wenn das Endgerät selbst nur wenig Speicher und Rechenleistung aufweist.

Der „Network-based mode“ erfordert eine spezielle Infrastruktur. Die Access-Points müssen die Fähigkeit besitzen, die Signalparameter der Clients zu ermitteln. Diese Informationen werden von den Access-Points an eine zentrale Instanz im Netzwerk weitergeleitet. Diese Instanz hat wie beim „Terminal-assisted mode“ genaue Informationen über die Referenzpunkte und berechnet die Position des mobilen Endgeräts. Der „Network-based mode“ benötigt die kostenintensivste Infrastruktur, besitzt aber den Vorteil, dass das mobile Endgerät nur die Möglichkeit besitzen muss, sich mit dem WLAN zu verbinden. Weitere Modifikationen an der Soft- oder Hardware sind nicht notwendig. Bei diesem Vorgehen kann auch der Benutzer des mobilen Gerätes nicht erkennen, ob eine Standortermittlung durchgeführt worden ist.

Dadurch, dass die Reichweite von WLAN-Access-Points bis zu 300 m betragen kann und diese auch außerhalb von Gebäuden platziert werden können, besteht die Möglichkeit, diese Technik auch auf einer begrenzten Fläche außerhalb von Gebäuden zu verwenden.

Das Positioning mit Hilfe von WLAN-Netzwerken wird primär verwendet, um in einem begrenzten räumlichen Gebiet eine Lokalisierung zu ermöglichen. Zukünftig werden spezielle Dienstanbieter Datenbanken aufbauen, um mit Hilfe von WLAN eine annähernd flächendeckende Lokalisierung zu erreichen. Dazu ermittelt der Anbieter die Position der vorhandenen Access Points und stellt eine Datenbank mit diesen Informationen zur Verfügung. [SHW07]

Bluetooth

Mit Hilfe von Bluetooth kann externe Peripherie über eine Funkschnittstelle an einen Computer angebunden werden. Zu Beginn wurde Bluetooth primär als PAN-Adapter (Personal Area Network) für Peripherie im Umkreis von 10 m ausgelegt. Mittlerweile gibt es Adapter mit unterschiedlichen Leistungsklassen, die auch eine Kommunikation in einem Umfeld von bis zu 100 m ermöglichen. Die Methoden die zur Lokalisierung bei WLAN-Netzwerken verwendet werden, können auch bei Bluetooth zum Einsatz kommen. Durch Adapter mit einer niedrigeren Sendeleistung können auch mehrere Sender pro Raum platziert werden. Somit kann durch Proximity Sensing je nach Anzahl der Bluetooth Geräte auch eine genaue Position innerhalb eines Raums ermittelt werden.

Ein wesentlicher Vorteil von WLAN und Bluetooth ist es, dass aktuelle Geräte (Notebooks, PDAs, usw.) bereits derartige Module integriert haben. Somit können ohne weitere Kosten für den Benutzer derartige Techniken zur Positionsbestimmung verwendet werden.

RFID

Die RFID (Radio Frequency Identification) wird zurzeit primär für Logistikanwendungen verwendet. Sie besteht aus einer Anzahl von Tags (z.B. in Form von Klebe-Etiketten), die einen Chip und eine Antenne besitzen. Befindet sich ein Lesegerät im Nahbereich um den Tag, so induziert das Lesegerät einen Strom in die Antenne des RFID-Tags, der ausreicht, dass die im Chip befindlichen Informationen zurückgesendet werden. Je nach Tag kann dabei die Reichweite oder die Speicherkapazität variieren. Dazu existieren für speziellere Anwendungen auch noch aktive Tags, die durch die eigene Stromversorgung einen weiteren Wirkungskreis haben und zusätzliche Sensoren oder eine komplexere Logik besitzen.

Die günstigen RFID-Tags können auch zur Lokalisierung verwendet werden. Dabei wird die Eigenschaft des geringen Wirkungskreises des Empfängers dazu ausgenutzt. Ein Empfänger erhält nur die Informationen der RFID-Tags, die sich in seinem direkten Umfeld befinden. Ist die Reichweite des Empfängers und sind die Standorte der Tags bekannt, so kann mit Hilfe des Proximity-Ansatzes die Position des mobilen Endgerätes ermittelt werden. Um mit dem relativ ungenauen Ansatz des Proximity Sensings eine genaue Lokalisierung zu realisieren, muss das Umfeld mit einer ausreichenden Anzahl an RFID-Tags ausgestattet werden.Vorteilhaft bei diesem System ist, dass RFID-Tags nur wenige Cents pro Stück kosten. Zusätzlich können sie für den Benutzer unsichtbar platziert werden.

Die Genauigkeit und Verfügbarkeit der Positionsermittlung ist durch die Auswahl der geeigneten RFID-Technik sowie eine angemessene Anzahl von Tags und deren entsprechende Positionierung zu erreichen.

5.3.2 Infrarotbasierte Indoor-Lokalisierungstechniken

Bei den Projekten ActiveBadge und WIPS (Wireless Indoor Positioning System) handelt es sich um infrarotbasierte Indoor-Lokalisierungstechniken. Ein Vorteil der Infrarottechnik ist, dass Sender und Empfänger sehr kostengünstig hergestellt werden können. Jedoch besitzt dieses System den Nachteil, dass auch das Tageslicht einen Infrarotanteil besitzt. Somit ist dieses Verfahren störungsanfällig und kann primär nur innerhalb von Gebäuden verwendet werden.

ActiveBadge

Bei ActiveBadge existiert als mobiles Endgerät ein Badge (in Form einer Marke), der die Möglichkeit besitzt, mit einer Identifikationsadresse kodierte Infrarotsignale zu versenden. Diese Signale werden von Sensoren, die sich in jedem Raum befinden, empfangen. Die Sensoren liefern diese Information an eine dahinter befindliche Infrastruktur weiter. Die Standorte der Sensoren sind im Vorfeld ermittelt worden. Somit kann die Infrastruktur einfach erkennen, in welchem Raum sich der Badge befindet. Dieses System nutzt die Tatsache, dass ein Infrarotsignal meist nur in einem Raum empfangen werden kann [WHF92].

WIPS (Wireless Indoor Positioning System)

Bei WIPS befindet sich in jedem Raum ein Infrarotsender. Dieser Sender sendet im Infrarotsignal eine eindeutige Identifizierung mit. Der Badge ist so konstruiert, dass er Infrarotsignale empfangen kann. Empfängt er ein Infrarotsignal mit einer Identifizierung, so sendet er diese Information per WLAN an die zuständige Infrastruktur weiter. Die Infrastruktur kennt die Standorte der Infrarotsignalsender und kann dadurch die Position des Badge ermitteln [RIT00].

5.3.3 Ultraschallbasierte Indoor-Lokalisierungstechniken

Lokalisierungstechniken, die auf Ultraschall basieren, verwenden ein Ultraschall-Sensorennetzwerk. Dieses Netzwerk befindet sich idealerweise an der Decke eines Raumes. Diese Position hat den Vorteil, dass es nur wenige Hindernisse zwischen Sender und Empfänger gibt. Das mobile Endgerät besitzt einen Ultraschallsender, der ein Signal aussendet. Mit Hilfe des Sensorennetzes wird das Ultraschallsignal empfangen und die Laufzeit gemessen. Aus den unterschiedlichen Laufzeiten zwischen den Sensoren und dem mobilen Endgerät kann seine Position ermittelt werden. Dadurch, dass die Schallgeschwindigkeit wesentlich niedriger als die Lichtgeschwindigkeit ist, kann diese Positionsermittlung mit einfacheren Mitteln realisiert werden. Das Projekt „ActiveBat“ ist ein exemplarisches Beispiel für ultraschallbasierte Lokalisierungstechniken. Es erreicht eine Genauigkeit von bis zu 10 cm, wenn das Raster der verwendeten Sensoren einen Abstand von 1,2 m besitzt [WJH97]. Beim Cricket-System handelt es sich um ein System, bei dem sich in einem Raum Sender befinden, die durchgehend ein Ultraschallsignal mit ihrer Identifikation senden. Bei diesem System wird keine Infrastruktur benötigt, da die Ermittlung der Position im Endgerät ausgeführt wird [PCB00].

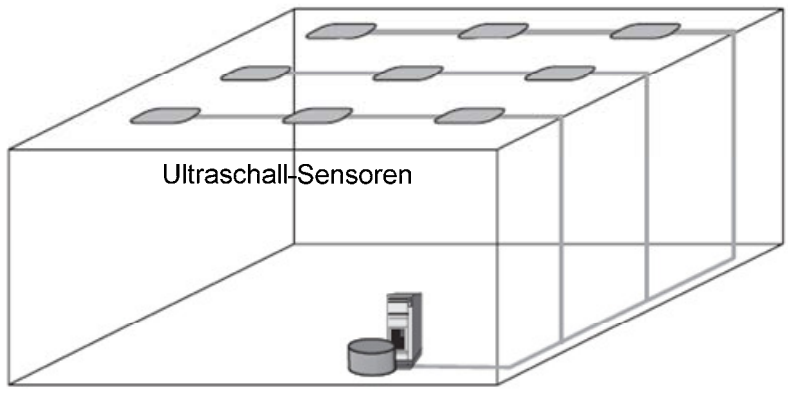


Abbildung 20 - Infrastruktur zur Lokalisierung mit Hilfe von Ultraschall am Beispiel ActiveBat [Kü05]

Optische Lokalisierungstechniken

Eine sehr hohe Genauigkeit im Zentimeterbereich kann mit Hilfe von Markern erreicht werden. Ein Projekt, das diesen Ansatz verwendet, ist z.B. AR-Toolkit. Das mobile Endgerät besitzt eine Kamera, die durchgehend das Videosignal daraufhin überprüft, ob sich im Blickbereich ein Marker befindet. Ist dies der Fall, wird ermittelt, ob der Marker dem System bekannt ist. Die Position des Markers wurde im Vorfeld festgelegt. Da die Marker nur erkannt werden können, wenn der Benutzer sich im direkten Umfeld befindet, ist die Position des Markers auch eine verhältnismäßig genaue Schätzung der Position des Benutzers. Die Genauigkeit kann zusätzlich noch weiter gesteigert werden, wenn in dem Blickbereich mehr als nur ein Marker sichtbar ist. In diesem Fall kann auch noch die Entfernung und Ausrichtung zu anderen Markern ermittelt werden. Ein Nachteil dieses Systems ist, dass ein flächendeckender Einsatz nicht möglich ist. Aus ästhetischen Gründen würde z.B. im Bereich von Kundenkontakten eine Anhäufung von Markern stören. Folgende Tatsachen wirken sich ebenfalls nachteilig aus: Damit ein Marker erkannt werden kann, muss die Kamera sich in unmittelbarer Nähe befinden. Dazu ist die Anzahl der möglichen Marker begrenzt, die das System unterscheiden kann. Zusätzlich ist die Genauigkeit davon abhängig, ob der Benutzer aktiv die Marker sucht und mit der Kamera aufnimmt.

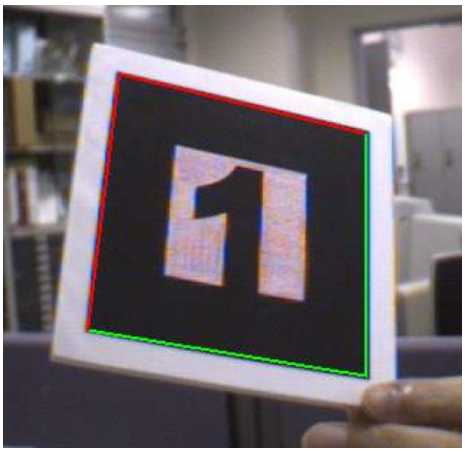


Abbildung 21 zeigt einen optischen Marker, der vom Projekt AR-Toolkit verwendet werden kann. Charakteristisch an derartigen Markern ist die quadratische Form mit dem ausgeprägten schwarzen Rand. In der Mitte befindet sich ein Zeichen oder Symbol, das vom mobilen Gerät ermittelt wird. Im Vorfeld muss dieses Zeichen mit den dazugehörigen Metadaten dem System bekannt gemacht werden. [ATK00]

Abbildung 21 - Optischer Marker vom Projekt AR-Toolkit [ATK00]

5.4 Entwicklung

Ein Großteil der im Jahr 2007 genutzten Mobilfunktelefone besitzt keine Möglichkeit, selbstständig die eigene Position zu ermitteln. Ein GPS-Empfänger wird erst in einige Geräte der preislichen Oberklasse eingebaut. Diese Geräte sind z.B. zumeist dafür ausgelegt, auch als Navigationsgerät verwendet zu werden. Geräte, die keinen GPS-Empfänger besitzen, können zum Teil über die Bluetooth Schnittstelle mit einem externen Empfänger ausgestattet werden. Dieses Vorgehen ist jedoch für den Benutzer nicht komfortabel, da er nun mehrere Geräte mit sich herumtragen und auch aufladen muss. Dazu benötigt die Funkverbindung zwischen den beiden Geräten zusätzlich Strom, was zu einer starken Reduzierung der Nutzungszeit führt. Das erklärt, warum diese Funktion nur im seltensten Fall genutzt wird. Um nun die Geräte so auszustatten, dass sie ihre eigene Position feststellen können, hat die Firma Blue Sky Positioning eine neuartige SIM-Karte entwickelt, auf der sich auch ein GPS-Empfänger samt Antenne befindet [Ho07a] [BSP07]. Auf die Positionsdaten des GPS-Empfängers können die Endgeräte mit Hilfe des SIM Toolkits zugreifen. Da diese Möglichkeit bei jedem aktuellen

Gerät gegeben ist, können ortsbezogene Dienste wie z.B. Notrufdienste (E-112 / E-911) umgesetzt und auch Benutzern zur Verfügung gestellt werden, die nicht in kurzen Abständen sich ein neues Endgerät kaufen. Die Karte verwendet zur schnellen Lokalisierung des Endgeräts A-GPS. Bei diesem Verfahren wird die Infrastruktur des Mobilfunknetzes dazu verwendet, dass die Position des mobilen Endgerätes schneller ermittelt werden kann. Dazu werden dem mobilen Endgerät vom Mobilfunkprovider die Bahndaten der Satelliten sowie seine grobe Position bereitgestellt. Dies ermöglicht dem eingebauten GPS-Empfänger wesentlich schneller eine genaue Position zu berechnen [Wi05]. Weiter geht auch die Bestrebung dahin, dass zukünftige Notebooks auch einen GPS-Empfänger enthalten sollen [Ho07a, Ho07b].

Zusätzlich wird die Genauigkeit von satellitenbasierten Navigationssystemen weiter steigen. Dies hat mit der Verbesserung der Satelliten, mit der Verfügbarkeit von mehreren Systemen, wie auch qualitativ besseren, somit empfindlicheren Empfängern, zu tun. Mit Hilfe von Galileo soll zukünftig auch eine Lokalisierung von Personen innerhalb von Menschenmengen möglich sein [Mey07]. WLAN kann zukünftig in Bereichen eingesetzt werden, wo GPS durch bauliche Behinderungen nicht ausreichend genutzt werden kann. Besonders in Innenstädten ist die Dichte der Hotspots dermaßen hoch, dass diese zur Positionsermittlung herangezogen werden können. [Bro06]

5.5 Bereitstellung von Ortsinformationen innerhalb der Architektur

Für die Bereitstellung von Ortsinformationen müssen unterschiedliche Technologien eingesetzt werden, um den Standort von mobilen Endgeräten oder beteiligten Objekten zu ermitteln. Einige der zuvor vorgestellten Techniken und Infrastrukturen können bei Diensten für den Massenmarkt nicht verwendet werden, da der Aufbau der notwendigen Infrastruktur zu kostenintensiv ist oder andere Technologien in der gleichen Situation ebenfalls verwendet werden können, die bereits eine breite Verfügbarkeit aufweisen. Daher werden im Rahmen der Konzipierung die folgenden Techniken zur Positionsbestimmung berücksichtigt:

- Satellitenbasierte Lokalisierung (z.B. mit Hilfe von GPS) (Outdoor)
- Netzwerkbasierte Lokalisierung (In- / Outdoor)
- WLAN (In- / Outdoor)

Die Architektur wird jedoch bereits zu Beginn so ausgelegt, dass eine nachträgliche Integration weiterer Techniken ohne Probleme realisierbar ist. Zusätzlich besteht die Möglichkeit, die Positionsinformationen aus unterschiedlichen Quellen zu kombinieren, um dadurch eine höhere Genauigkeit zu erzielen. Durch diese Auswahl der verwendeten Technologien sind sowohl Dienste innerhalb wie außerhalb von Gebäuden möglich. Durch die Verfügbarkeit von mehreren Informationsquellen zum gleichen Zeitpunkt, besteht zusätzlich der Vorteil, dass beim Ausfall einer Technologie, weiterhin der Einsatz von ortsbezogenen Diensten ermöglicht wird.

Innerhalb der Architektur werden Ortsinformationen durch die folgenden Instanzen bereitgestellt (siehe Abbildung 4):

- Positioning Infrastructure
- Network Positioning Infrastructure
- Location Provider
- Location Database Provider

5.6 Positioning Infrastructure

Bei der Instanz der „Positioning Infrastructure“ handelt es sich um externe Infrastrukturen, die speziell zur Positionsermittlung entwickelt worden sind. Neben den primär zur Positionsermittlung entwickelten Infrastrukturen werden zusätzlich auch Signale von Funknetzwerken als Grundlage zur Positionsfeststellung verwendet. Ein Beispiel für eine speziell zur Positionsermittlung entwickelte Infrastruktur ist das GPS-System (siehe auch Kapitel 5.1). Es handelt sich dabei um ein weltweit verfügbares Satellitennetz, das die Aufgabe hat, ein hoch präzises Zeitsignal von jedem Satelliten auszusenden. Der Empfänger kann anhand der Laufzeitunterschiede der empfangenen Signale seine Position berechnen.

Es handelt sich bei einem derartigen System um eine Technologie, die „terminal-based“ aufgebaut ist. Diese Vorgehensweise besitzt einen sehr guten Skalierungsfaktor, so dass einer nahezu unbegrenzt großen Anzahl von Teilnehmern die Möglichkeit gegeben wird, ihre Position zu ermitteln. Die jeweiligen Endgeräte führen die eigentliche Berechnung aus, um die Position zu ermitteln. Die große Anzahl von möglichen Nutzern erklärt sich dadurch, dass die Teilnehmer das Endgerät nur als reinen Empfänger verwenden und somit keine Informationen zurück zum Satelliten senden. Durch dieses Vorgehen entsteht kein Flaschenhals, da die Informationen vom Satelliten zu allen Empfängern versendet werden. Das System muss durch diesen Aufbau nicht wissen, welche Empfänger aktiv den Dienst nutzen.

Bei der Nutzung von Funknetzwerken, die nicht dafür entwickelt worden sind, um eine Positionsermittlung zu ermöglichen, wird zumeist die Position vom Endgerät anhand der Signalstärke oder des Signal-Rausch-Abstandes berechnet. Im Vorfeld besitzt das Endgerät jedoch das Wissen über den Standort, der am Netzwerk beteiligten Sender.

Die Positioning-Infrastructure-Instanz kann auf den folgenden Technologien basieren:

- Satellitenbasierte Lokalisierungssysteme (GPS, Galileo,…) mit ihren überlagernden Systemen zur Genauigkeitssteigerung
- Funknetzwerke (WLAN, Bluetooth, RFID, …)
- Erweiterter DHCP Dienst [Sch06] – Bei diesem Verfahren werden dem Endgerät zusätzlich bei der Adressvergabe weitere Positionsinformationen über das Netzwerk übermittelt, mit dem es sich verbunden hat.

Die Positioning Infrastructure zeichnet sich dadurch aus, dass es sich um eine terminal-based Lokalisierungstechnologie handelt. Ein Endgerät mit geeigneten Sensoren kann die ausgesendeten Daten verwenden, um die eigene Position zu ermitteln. Durch die Broadcast-Aussendung hat die beteiligte Positioning-Infrastructure-Instanz kein Wissen über die Endgeräte, die diese Technik verwenden.

5.7 Network Positioning Infrastructure

Die Instanz der „Network Positioning Infrastructure“ stellt innerhalb eines Netzwerkes, das vom Benutzer auch zur Kommunikation verwendet wird, Technologien zur Positionsermittlung zur Verfügung. Der Unterschied zwischen der Positioning Infrastructure und der Network Positioning Infrastructure besteht darin, dass die Positionsermittlung durch eigenständige Bestandteile innerhalb des Netzwerkes erfolgt. Somit handelt es sich um ein network-based Verfahren. Das zu lokalisierende Endgerät muss bei diesem Vorgang, neben der regulären Nutzung des Kommunikationsnetzes, keine aktive Aufgabe zur Positionsermittlung wahrnehmen. Die Ausnahme stellen nur die terminal-assisted Verfahren dar, bei denen das Endgerät Teilaufgaben bei der Positionsfeststellung übernimmt. Bei diesem Vorgang kann es sich beispielsweise darum handeln, dass unverarbeitete Sensorwerte an die dedizierte Instanz weitergeleitet werden. Beim reinen network-based Verfahren werden beispielsweise ausschließlich die Sensorwerte der festen Sendestationen verwendet. Diese Verfahren besitzen den Vorteil, dass die Endgeräte durch die Positionsermittlung nicht in Anspruch genommen werden und dass die Auslagerung dieser Aufgabe zu einer längeren Akkulaufzeit führt. Im Weiteren besteht die Möglichkeit, spezielle Antennenanlagen in den Funkstationen zu verwenden, die eine genauere Standortbestimmung zulassen.

Eine network-based Lokalisierung kann mit Hilfe der folgenden Technologien erreicht werden:

- Es kann ein spezielles WLAN verwendet werden, das die Fähigkeit besitzt, die Empfangswerte der Endgeräte vom Access-Point in einer zentralen Instanz zu verarbeiten. Anhand der bekannten Positionen der Access-Points wird unter Berücksichtigung der ermittelten Signalstärken aus der Datenbasis ein Fingerprint gesucht, der Ähnlichkeit mit zuvor ermittelten Daten besitzt. Bei der Verwendung eines Fingerprint-Verfahrens werden im Vorfeld, in dem vom Netzwerk abgedeckten Bereich, in regelmäßigen Abständen punktuell „Fingerprints“ entnommen. Das heißt, es werden ortscharakteristische Daten wie Signalstärke und Signal-Rausch-Abstand gemessen. Auf diesen Informationen basiert die spätere Positionsermittlung (siehe Kapitel 5.3.1).

- Von Endgeräten, die ein Mobilfunknetz verwenden, wird durchgehend die Position ermittelt. Diese Informationen werden benötigt, um einen Handover zwischen den einzelnen Funkzellen zu ermöglichen, damit die Geräte bei einem eingehenden Telefonat aufgefunden und erreicht werden können. Die Positionsinformationen werden Dienstanbietern über besondere Schnittstellen auch zur Realisierung von speziellen Dienstleistungen angeboten (siehe Kapitel 5.9). Mobilfunknetze besitzen den Vorteil, dass eine Lokalisierungskomponente für die Grundfunktionen des Netzwerkes benötigt wird und somit innerhalb des Netzwerkes flächendeckend zur Verfügung steht. Im Weiteren decken Mobilfunknetze sehr große Flächen ab, so dass diese Art der Positionsermittlung eine hohe Verfügbarkeit besitzt. Die Positionsermittlung im Rahmen des Netzwerkbetriebs benötigt jedoch keine sehr genaue Positionsfeststellung. Die Genauigkeit ist sehr stark abhängig von der Größe der Mobilfunkzelle und der eingesetzten Antennentechnik. Daher ist die Qualität der Positionsinformation sehr unterschiedlich und reicht für manche Dienste nicht aus. Durch die Integration weiterer Technologien besteht jedoch die Möglichkeit, dass die Positionsermittlung mit Hilfe von Mobilfunknetzen weiter präzisiert wird (siehe Kapitel 5.2).

5.8 Location Provider

Um auf dem Massenmarkt ortsbezogene Dienste etablieren zu können, ist es notwendig, dass von jedem Endgerät möglichst durchgehend die Position ermittelt werden kann. Je nach Endgerät sind bereits Sensoren integriert, die zur Lokalisierung verwendet werden können. Da im mobilen Umfeld jedoch eine sehr große Menge von verschiedenartigen Endgeräten existiert, die sich in ihrer technischen Ausstattung und ihren Leistungen unterscheiden, müssen unterschiedliche Technologien verwendet werden, um eine Positionsermittlung zu ermöglichen. Der Einsatz unterschiedlicher Technologien ist auch deshalb wichtig, da je nach Situation des Benutzers, bestimmte Sensoren keine ausreichend genauen Werte ermitteln können.
Aus diesem Grund werden gleichzeitig alle verfügbaren Informationen, die eine Lokalisierung ermöglichen, im Location Provider gesammelt. Anhand dieser Datenbasis lässt sich feststellen, wann und in welcher Situation ein Sensor an Genauigkeit verliert. Durch die Kombination von Sensorenwerten kann auf Veränderungen im Umfeld (z.B. der Benutzer geht in ein Gebäude und einige Sensorenwerte fallen aus) reagiert werden. Die große Datenmenge erlaubt die Kombination von Datensätzen, um dadurch eine Steigerung der Genauigkeit zu erzielen. Da derartige Berechnungen in einem kurzen Intervall erfolgen müssen und das Endgerät z.B. nicht auf alle Daten aus dem Netzwerk Zugang hat, wird dieser Vorgang vom Location Provider realisiert. Das hat den Vorteil, dass Berechnungsfunktionen auf neue Sensoren und Netze durchgehend angepasst und optimiert werden, ohne dass der Benutzer seine Software auf dem Endgerät aktualisieren muss.

Abhängig von der benutzten Technologie, liegen Sensorwerte noch nicht als direkt nutzbare Positionsinformation vor. Eine Aufgabe des Location Providers besteht darin, die Informationen auf eine einheitliche Koordinatenbasis zu konvertieren. Im Weiteren müssen aus den Sensordaten erst Positionsinformationen berechnet werden. Dies ist z.B. der Fall, wenn WLAN-Signalstärken zur Positionsermittlung genutzt werden. Die grundlegenden Basisinformationen, z.B. über die Position der ermittelten Access-Points, beschafft sich der Location Provider von der Instanz des Location Database Providers.

Dienste, die die Position eines Benutzers über einen längeren Nutzungszeitraum erfordern, melden sich beim Location Provider an. Bei dieser Anmeldung hinterlegen sie zusätzlich die Information, in welchem Zeitraum sie die nächste Position benötigen.Sie geben auch an, ob sie Positionsinformationen nur für einen bestimmten räumlichen Bereich brauchen. Zum Beispiel könnte der Dienst nur dann verwendet werden, wenn der Benutzer ein bestimmtes Areal betritt oder verlässt. Da es sich bei Ortsinformationen um sensible Daten handelt, muss diese Instanz von einem vertrauenswürdigen Anbieter realisiert werden.

Die mit Hilfe des Location Providers bereitgestellten Positionsinformationen stehen über den Privacy Provider den Anwendungen auf dem Endgerät oder den benutzten Diensten zur Verfügung. Der Location Provider ermöglicht es dem Privacy Provider, die Positionsinformation in unterschiedlichen Qualitätsstufen abzufragen. Je nach Anwendung wird nicht die höchste Genauigkeit benötigt. Die Reduzierung der Informationsqualität zielt somit auf die Minimierung der verwendeten personenbezogenen Informationen.

Durch den zentralisierten Ansatz der Positionsberechnung und –bereitstellung über den Location Provider bietet sich für den Anwendungsentwickler eine einheitliche Softwareschnittstelle. Diese Schnittstelle kann genutzt werden, ohne dass der Programmierer sich mit dem Leistungsvermögen des Endgerätes auseinandersetzen muss. In den jeweiligen

Endgeräten weist das Betriebssystem einen Treiber auf, der die Sensorinformationen über den Privacy Provider an den Location Provider meldet. Somit besteht nur selten die Notwendigkeit, die Treibersoftware auf dem Endgerät zu aktualisieren. Sind Anpassungen an der Logik notwendig, so kann das zentral beim Location Provider erfolgen. Die Anpassungen und Erweiterungen stehen folglich ohne Updateprozess allen Benutzern zur Verfügung.

Das Endgerät selbst kann über den Privacy Provider Positionsinformationen vom Location Provider erhalten. Dadurch können Anwendungen auf dem Endgerät von der Integration der unterschiedlichen Positionsinformationen ebenfalls profitieren.

Um eine Lokalisierung zu ermöglichen, muss neben dem zu lokalisierenden mobilen Endgerät auch eine stationäre Infrastruktur zur Verfügung stehen. Nur innerhalb ihres Bereiches ist eine automatische Positionsermittlung möglich [TVM03]. Daher unterstützt der Location Provider Techniken mit einem hohen Verbreitungsgrad. Die Architektur soll eine Plattform für eine große Anzahl von Diensten und Anwendungen bieten. Daher muss es möglich sein, zu einem späteren Zeitpunkt die Plattform um weitere Technologien zu erweitern oder die speziellen Leistungsmöglichkeiten des verwendeten Endgerätes zu nutzen. Der Location Provider kommt diesen Anforderungen durch seinen modularen Aufbau entgegen.

Der Location Provider muss in der ersten Ausbaustufe sowohl Lokalisierungstechnologien für eine Nutzung im In- und Outdoor-Umfeld bereitstellen. Dabei werden speziell die Technologien betrachtet, die einen hohen Verbreitungsgrad besitzen und eine möglichst hohe Genauigkeit der Positionsermittlung ermöglichen. Bei der Berechnung der Position werden die Eigenschaften, der zu diesem Zeitpunkt verfügbaren Technologie berücksichtigt, ebenso ihre Verfügbarkeit, ihre Kosten und ihr Zeitbedarf. Besonders Technologien, die Kosten verursachen oder sehr zeitaufwendig sind, werden, sofern die Möglichkeit besteht, durch andere substituiert. Diese müssen verfügbar sein und annähernd die gleichen Eigenschaften besitzen. Der Benutzer hat jedoch bei der Konfiguration die Gelegenheit, durchgehend eine kostenpflichtige Positionsermittlung über das Mobilfunknetz integrieren zu lassen. Die Dienste können ihrerseits die Rohdaten eines Sensortypen anfordern.

Für zukünftige Dienste und Anwendungen sollen vom Location Provider nur eine Position und Informationen über den Grad der Genauigkeit angeboten werden. In diesem Fall muss der Entwickler sich nicht mehr mit den Details der Positionsbestimmung auseinandersetzen. Die Berücksichtigung des speziellen Sensorverhaltens in unterschiedlichen Situationen entfällt ebenfalls. Dadurch lassen sich Endgeräte mit unterschiedlichen Leistungsmerkmalen einsetzen oder nachträglich Sensornetze integrieren. Die Erweiterung des Location Providers um weitere Sensortypen, hat den Vorteil, dass diese Erweiterung automatisch allen Benutzern zur Verfügung steht. Eine Aktualisierung des beteiligten Betriebssystembereiches wird dadurch seltener notwendig.

5.9 Location Database Provider

Beim Location Database Provider handelt es sich um einen speziellen Anbieter von Informationen, die zur Positionsbestimmung benötigt werden. Diese speichert er in seiner Datenbank. Er erstellt und pflegt diese Datensätze dauerhaft, die vom Location Provider z.B. über eine Web-Service-Schnittstelle in Anspruch genommen werden können. Diese Datensätze werden verwendet, damit der Location Provider aus Sensorendaten konkrete Positionsinformationen ermitteln kann. Bei den folgenden Beispielen bietet sich die Nutzung von Daten vom Location Database Provider an:

- Bei Mobilfunknetzen ist die Positionsfeststellung durch den Mobilfunkprovider gebührenpflichtig. Benötigt der verwendete Dienst nur eine sehr grobe Positionsangabe, so kann eine derartige Position mit Hilfe der Mobilfunkzellen-Identifikation (Cell-ID) ermittelt werden. Jedes Endgerät, das mit einem Mobilfunknetz verbunden ist, kann die Signalstärke einer und ggf. auch weiterer Basisstationen ermitteln. Die Position des Mobilfunksenders kann als Näherungswert genutzt werden, um den Standort des Benutzers zu definieren. Diese Information kann durch die Berücksichtigung benachbarter Zellen noch präzisiert werden. Da innerhalb der Cell-ID keine Positionsinformation enthalten ist, wird eine Datenbank benötigt, die den Standort der Mobilfunksender beinhaltet.

- Werden Informationen über WLAN-Access-Points zur Positionsermittlung verwendet, so muss eine Datenbank mit den Positionen der Sendestationen bereitstehen. Bei der Verwendung von WLAN zur Positionsermittlung muss jedoch berücksichtigt werden, dass die Verfügbarkeit der in der Datenbank hinterlegten WLAN-Access-Points starken Schwankungen unterliegen kann. Das kommt dadurch, dass diese Sendestationen durch Privatpersonen betrieben werden. Je nach Nutzung sind sie nur zeitlich begrenzt verfügbar oder müssen mit der Zeit neu positioniert werden. Durch die geringere Flächenabdeckung einer einzelnen Station, aber die hohe Zahl an oft gleichzeitig empfangbaren Stationen, führt die Nutzung von WLAN zu genaueren Positionsinformationen als die Verwendung von Cell-ID. Da keine zentrale Institution existiert, die den Standort von Access-Points ermittelt bzw. ihre Verfügbarkeit prüft, handelt es sich in diesem Bereich um sehr flexible Daten. Durch die geringe Flächenabdeckung muss eine kurzfristige Aktualisierung durch einen Dienstanbieter gewährleistet werden. Um die Datenbasis aktuell zu halten, besteht die Möglichkeit, mit Hilfe eines kombinierten Sensoransatzes die Position der WLAN-Access-Points automatisch vom Endgerät in einer Datenbank zu hinterlegen und bestehende Datensätze zu aktualisieren. Die Aktualisierung kann durch Endgeräte erfolgen, die beispielsweise neben einer WLAN-Karte zusätzlich auch einen GPS-Empfänger besitzen. Geräte, die sich an der Aktualisierung der Datensätze beteiligen, melden die genaue Position der empfangenen Access-Points. Zusätzlich besteht die Möglichkeit, in der Datenbank Fingerprint-Informationen zu hinterlegen. Somit kann innerhalb der Funkzelle des Access-Points, durch die Berücksichtigung weiterer Signale angrenzender Access-Points, eine wesentlich genauere Position ermittelt werden. Von diesen Informationen profitieren besonders Endgeräte, die nur als Sensor über eine WLAN-Karte verfügen, da diese, basierend auf den vorliegenden Signalstärken und Rausch-Signal-Abständen eine Position ermitteln können.

- Abhängig von der Netzwerktechnologie, die der Client zur Kommunikation mit dem Internet verwendet, wird ihm dynamisch eine Netzwerkadresse vergeben. Große Netzwerke sind zumeist in einzelne Subnetzwerke aufgeteilt. Durch die Unterscheidung in Subnetze kann eine geographische Verbindung zwischen dem Netzwerk und dem Client hergestellt werden. Der Location Database Provider muss für diesen Anwendungsfall eine Datenbank aufbauen und pflegen, um die vergebenen Netzwerkadressen des Clients einer geographischen Lokation zuzuordnen. Diese Vorgehensart ermöglicht es beispielsweise, einen Client einem bestimmten Stadtgebiet (bei großen Internetprovidern) oder einem Firmenstandort (wie z.B. beim Universitäts-Campus) zuzuordnen. Eine derartige Lokalisierung garantiert eine flächendeckende aber zumeist nur sehr ungenaue Positionsermittlung. Solche Systeme zur Positionsermittlung können jedoch Dienste mit Informationen versorgen, die nur eine sehr ungenaue Positionsinformation benötigen, um ihre Dienstleistung bereitzustellen.

Dadurch, dass die Positionsinformationen zentral vom Location Provider realisiert werden, wird die Menge der Datenübertragungen und Berechnungen beim Client minimiert. Deshalb müssen nur die zentralen Serverdienste große Informationsmengen speichern und verarbeiten. Die Endgeräte können somit technisch einfacher konzipiert und günstiger gebaut werden. Durch die geringe Anzahl von Berechnungen wird die Laufzeit der Geräte optimiert.

5.10 Ermittlung von verteilten Positionsinformationen

Innerhalb der Architektur werden Kontextdaten aus den unterschiedlichsten Quellen verwendet. Besonders die Ermittlung der Positionsinformationen stellt besondere Anforderungen an die Architektur. Ein Problem bei der Lokalisierung ist es, dass es keine Technologie gibt, die in jeder Situation eine ausreichend genaue Positionsinformation ermitteln kann. Durch den Einsatz unterschiedlicher Netzwerktechnologien stehen bestimmte Ansätze nicht kontinuierlich zur Verfügung. Abbildung 22 zeigt die Bereitstellung der einzelnen Positionsinformationen, sowie die Kombination dieser zu einer exakten Information, die dem Dienst bereitgestellt wird.

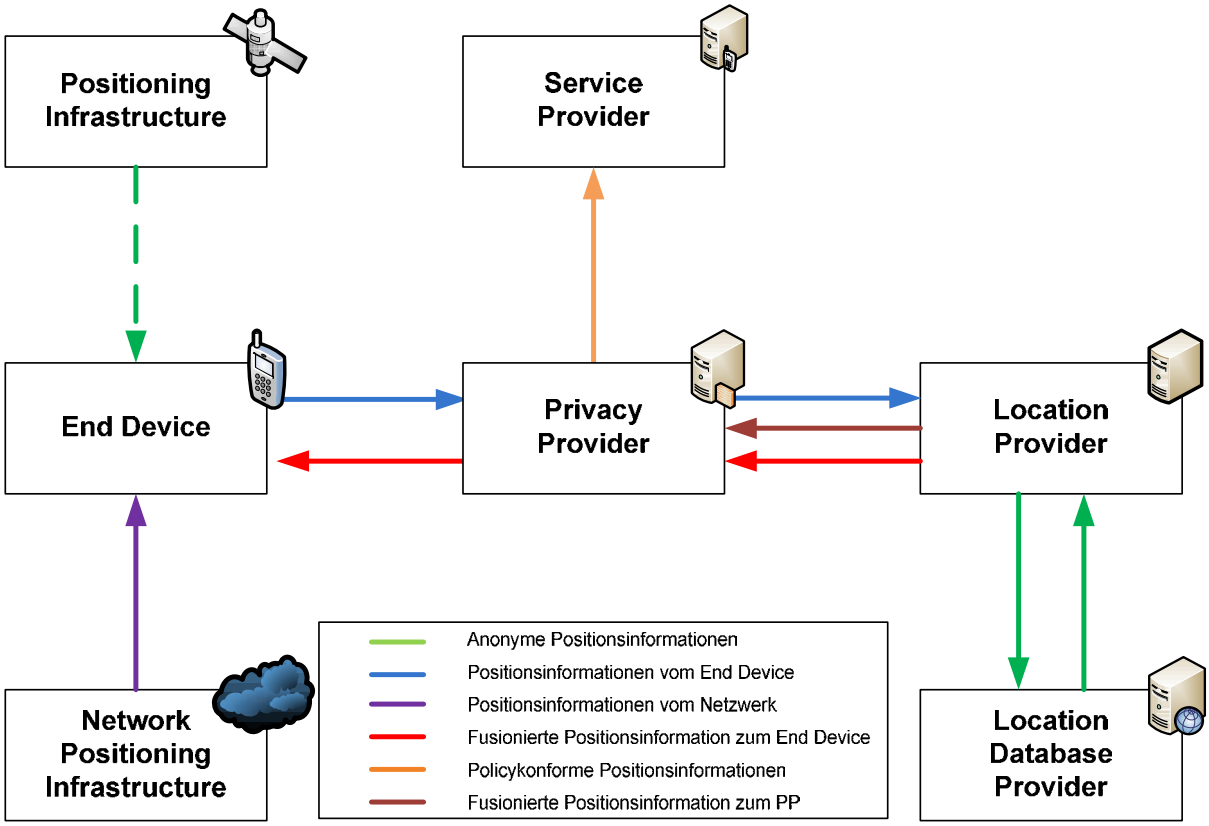


Abbildung 22 - Bereitstellung von Positionsinformationen aus unterschiedlichen Quellen

Eine Positionsermittlung kann bereits durch Sensoren im Endgerät (*End Device*) erfolgen. Sensoren, wie z.B. GPS-Empfänger, empfangen dabei Funksignale von einer externen Infrastruktur (*Positioning Infrastructure*). Beim GPS-System wären dies Signale von den empfangbaren Satelliten. Die Satelliten senden ein Zeitsignal, mit dessen Hilfe eine Position berechnet wird. Da dieses System keinen Rückkanal besitzt, kann es nicht ermitteln, welche Benutzer von ihm Gebrauch machen und wo sie sich befinden. Die Daten des Systems sind anonym und bieten keine Möglichkeit, dass Dritte Informationen ableiten können. Eine Alternative wäre ein WLAN-Netzwerk, bei dem nur anhand der Signalstärke und des Rausch-Signalverhältnisses eine Positionsinformation berechnet wird.
Besitzt das Netzwerk, mit dem der Benutzer verbunden ist, die Möglichkeit, mit Hilfe einer speziellen Infrastruktur (*Network Positioning Infrastructure*) den Standort des Endgeräts zu lokalisieren, so können diese Informationen ebenfalls bei der Positionsbestimmung mit verwendet werden. Diese Informationen können direkt vom Endgerät abgefragt werden. Das Endgerät kann seine Informationsquelle direkt einfließen lassen, wenn beispielsweise das Kommunikationsnetz gewechselt worden ist. Zur Positionsbestimmung können unterschiedliche Technologien zum Einsatz kommen. Beispielsweise besteht die Möglichkeit,

dass WLAN-Netzwerke um eine Komponente erweitert werden, die basierend auf der Signalstärke und den verwendeten Access-Points die Position feststellen. Ein vergleichbares System existiert auch im Mobilfunknetz. In diesem Fall wird die verwendete Mobilfunkzelle, die Signalstärke, die Signallaufzeit und ggf. der Winkel (z.B. bei Zellen, die mit Hilfe von unterschiedlich ausgerichteten Antennen versorgt werden) ermittelt. Abhängig von dem verwendeten Netzwerk kann die Position auch ermittelt werden, ohne dass das Endgerät aktiv wird. Es besteht somit die Möglichkeit, dass das Endgerät die Informationsquelle angibt, wo diese Informationen erhältlich sind. Dieses Vorgehen spart dem Endgerät Energie und ermöglicht somit eine längere Laufzeit.
Alle Informationen, die vom Endgerät ermittelt worden sind, werden über den *Privacy Provider* an den *Location Provider* übermittelt. Der Privacy Provider prüft dabei, dass nur befugte Instanzen Informationen liefern oder abfragen. Diese werden an den Location Provider weitergereicht. In dieser Instanz werden alle Positionsinformationen aus den unterschiedlichsten Quellen gesammelt. Basierend auf der Verfügbarkeit und Gültigkeit der Daten werden die unterschiedlichen Informationsquellen verwendet, um aus den Einzeldaten eine kombinierte und damit oft genauere Positionsinformation zu erstellen. Dieses Verfahren ist besonders dann vorteilhaft, wenn der Benutzer einen Bereich verlässt, der von einem Sensortyp nicht mehr abgedeckt wird oder eine niedrigere Genauigkeit ausweist. Durch die zentrale Instanz des Location Providers können die unterschiedlichsten Sensorenquellen auch während des Betriebs nachgerüstet werden. Die Logik kann an einem Punkt optimiert und erweitert werden, ohne dass in den jeweiligen Endgeräten eine Aktualisierung notwendig ist. Durch dieses Vorgehen werden auch Geräte einer niedrigeren Leistungsklasse in diese Architektur integriert. Je nach verwendetem Sensortyp müssen die Sensorwerte jedoch noch konvertiert werden. Dies ist abhängig von dem verwendeten Koordinatensystem oder der Umrechnung von relativen Koordinationen zu globalen. Zusätzlich lässt sich mit Hilfe der zugeteilten Netzwerkadresse oder des verwendeten Zugriffspunkts eine geographische Position ableiten. Die Konvertierung zwischen den Koordinatensystemen wird vom Location Provider ausgeführt. Die zur Positionsermittlung benötigten Daten, um aus Sensorinformationen Positionsinformationen zu berechnen, stellt der *Location Database Provider* bereit.
Die so gewonnenen Positionsinformationen werden dem Privacy Provider zur Verfügung gestellt. Dieser speichert die Informationen in seiner Kontextdatenbank ab. Auf diese können nun sowohl der Benutzer (z.B. für spezielle lokale Anwendungen), wie auch befugte Dienste (*Service Provider*) zugreifen. Der Privacy Provider stellt dabei sicher, dass die definierten Regelsätze beachtet werden. Somit kann die Positionsinformation beim Location Provider auch mit einer niedrigeren Genauigkeit abgefragt werden, wenn diese in dem vorliegenden Fall ausreicht. Der Provider kann die Information in unterschiedlichen, für die Anwendung nutzbaren Genauigkeiten und Formaten liefern.

6 Bereitstellung der Kontextdaten und Schutz der Privatsphäre

Die Verwaltung, Sicherung und Bereitstellung von Kontextinformationen stellt die besondere Herausforderung für diese Architektur dar. Das folgende Kapitel beschreibt die Instanzen, die den Schutz der Kontextdaten realisieren.

6.1 Privacy Provider

Der Privacy Server stellt eine Kernkomponente für den Schutz der Kontextinformationen innerhalb der Architektur dar. Mit Hilfe dieser Instanz wird die Privatsphäre der Benutzer bei der Nutzung von kontextbezogenen Diensten geschützt. Jeder Benutzer muss vor der ersten Dienstnutzung einen Account bei einem Privacy Provider einrichten lassen. Er kann unter unterschiedlichen Anbietern wählen. Da diese Instanz Zugriff zu allen sensiblen Informationen hat, sollte der Benutzer, vergleichbar mit der Auswahl einer Bank, einen Privacy-Anbieter aussuchen, der sein Vertrauen genießt. Nach erfolgreicher Authentisierung (siehe Kapitel 6) kann der Benutzer die Schutz- und Regelfunktionen des Privacy Providers nutzen. Der Privacy Provider agiert bei der Dienstnutzung als Mittler zwischen dem Dienst und dem Benutzer.

Die meisten Daten werden im Privacy-Server nur zwischengespeichert und zu der zuständigen Instanz weitergeleitet. An diesem Punkt wird geprüft, ob die Daten passieren dürfen. Dies erfolgt entsprechend der definierten Regelsätze des Benutzers. Zusätzlich werden die entstandenen Kosten sowie die Abrechnung geprüft und protokolliert. Beim Clearing Provider (siehe Kapitel 4.7) besitzt der Benutzer ein Konto, über das die genutzten Dienste abgerechnet werden.

Der Privacy Provider verfügt über eine Benutzerverwaltungsdatenbank mit Informationen über alle Benutzer. Zusätzlich existieren vier weitere Datenbanken (siehe Abbildung 23), in denen jeder Benutzer eine eigene Tabelle besitzt.

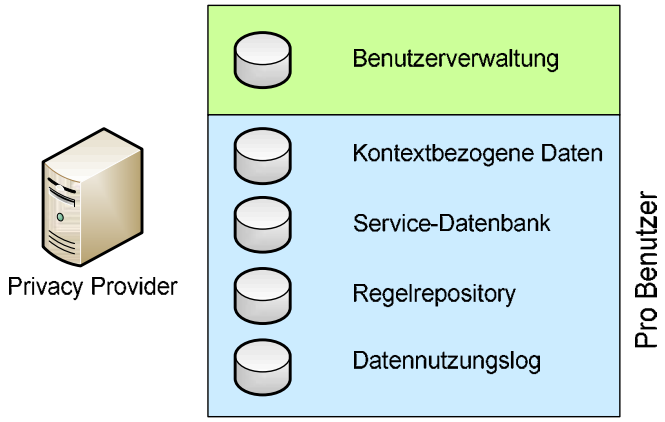


Abbildung 23 - Datenbanken des Privacy Providers

6.1.1 Benutzerverwaltung

In der Benutzerverwaltung werden die grundlegenden Informationen über die Benutzer des Privacy Providers hinterlegt. Diese Informationen werden beim Erstellen des Accounts erhoben. Sie stehen nur dem Privacy Provider zur Verfügung. Bei ihnen handelt es sich beispielsweise um:

- Benutzerprofile (Anzahl der verwendeten Zertifikate – Zugehörige DB)
- Status des Accounts (Wurde die Identifikation des Benutzers nachgewiesen?)
- Zahlungsinformationen (Kennung bei Clearing Provider)
- Aktive TANs zur Einbindung weiterer Endgeräte

6.1.2 Kontextbezogene Daten

In der Datenbank für kontextbezogene Daten besitzt jeder Benutzer des Privacy Providers eine eigene Tabelle. In dieser Tabelle werden alle kontextbezogenen Daten hinterlegt. Sie besitzt bereits eine große Anzahl von standardisierten Feldern. Es handelt sich bei den Informationen, die in diesen Feldern gespeichert werden, primär um solche, die auch in jeder Adressverwaltung einer Personal Information Management Software wie z.B. Outlook gespeichert werden. Der Benutzer kann auch unterschiedliche Informationen, die seine soziale Rolle betreffen, eingeben. Somit ist es möglich, sowohl private als auch gewerbliche Adressinformationen zu hinterlegen. Zusätzlich zu den grundlegenden personenbezogenen Informationen existieren hier auch bereits Felder, die für die Nutzung von sozialen Netzwerken vorgesehen sind.
Dem Benutzer steht es frei, welche Informationen er in diesem System hinterlegt. Der zentrale Sinn dieser Informationssammlung ist es, dass Teilbereiche Diensten und Anwendungen zur Verfügung gestellt werden können. Durch die zentrale Speicherung sind Änderungen nur an einem Punkt nötig. Die Dienste erhalten bei der darauffolgenden Nutzung die freigegebenen aktualisierten Informationen. Durch den definierten Feldnamen besteht nicht das Risiko, dass inhaltlich redundante Felder angelegt werden.

Da neuartige Dienste und Anwendungen unterschiedliche Informationen benötigen, die von Beginn an nicht durch die standardisierten Felder abgedeckt werden, besteht jederzeit die Möglichkeit, weitere Felder für kontextbezogene Daten eines Benutzers zu erstellen. Im Namen der Felder ist ersichtlich, welcher Dienst oder welche Anwendung sie angelegt hat. Durch dieses Vorgehen ist eine flexible Erweiterung der Datenbasis jederzeit gewährleistet. Etablieren sich neben den zu Beginn standardisierten Feldern weitere, so können mit der Erlaubnis des Benutzers auch andere Dienste darauf zugreifen. Die Felder enthalten neben den statischen auch dynamische Informationen (z.B. Verfügbarkeitsstatus bei Instant Messaging Diensten usw.). Es lassen sich auch Informationen in unterschiedlichen Detaillierungsgraden hinterlegen. Auf diese kann im Bedarfsfall zugegriffen werden.

Bei dieser Architektur müssen somit die Dienste und Anwendungen die benötigten personenbezogenen Informationen nicht in ihrer eigenen Datenbasis speichern. Dies spart ihnen einen großen Speicherbedarf. Für den Benutzer hat es den Vorteil, dass er bei jeder Dienstnutzung erneut entscheiden kann, welche Informationen er bekannt geben muss. Zusätzlich ist sichergestellt, dass die Diensterbringung durch die zentrale Datenspeicherung auf den aktuellsten Informationen, die der Benutzer bereitgestellt hat, basiert.

Dadurch, dass in den standardisierten Feldern und in ihren Erweiterungen zunehmend Informationen hinterlegt werden, sammelt sich im Laufe der Nutzungszeit eine große Menge von personenbezogenen Informationen an. Die Menge an Informationen, die der Benutzer

pflegen muss, steigt somit. Manche werden möglicherweise nicht mehr benötigt, weil bestimmte Dienste nicht mehr in Anspruch genommen werden. Daher werden alle Informationen mit einem Zeitstempel versehen. Sie können manuell entfernt werden. Der Benutzer kann sich auch die Daten anzeigen lassen, die seit einem bestimmten Zeitbereich nicht mehr für eine Dienstnutzung verwendet worden sind. Diese kann er automatisch aus der Datenbank entfernen lassen.

6.1.3 Service-Datenbank

Jeder Benutzer besitzt in der Service-Datenbank eine eigene Tabelle. Diese Tabelle beinhaltet die Dienste, die der Benutzer aktiv verwendet bzw. für die er einen oder mehrere Regelsätze definiert hat. Die zu jedem Dienst gehörigen Regelsätze befinden sich in der zugehörigen Tabelle des Regelrepository. Diese Tabelle ist ein zentraler Bereich, in dem ein Benutzer überprüfen kann, welchen Diensten er Zugriff zu seinen sensiblen Informationen gegeben hat. Bei den einzelnen Diensten sind in dieser Tabelle auch Informationen hinterlegt, wie die bei der Nutzung entstehenden Kosten bzw. die laufenden Aboverträge. Der Zeitpunkt der letzten Nutzung ist hinterlegt, ebenso der Zeitpunkt, an dem zuletzt von einem Dienst Informationen angefordert wurden.
Basierend auf diesen Informationen kann der Benutzer entscheiden, ob er weiterhin dem Dienst Zugang zu den sensiblen Informationen erlauben möchte. Entscheidet er sich dazu, einen Dienst aus dieser Liste zu entfernen, so wird auch automatisch der dazugehörige Regelsatz entfernt oder deaktiviert. Handelt es sich um einen Dienst mit Abovertrag, so wird der entsprechende Dienst informiert, dass zum frühestmöglichen Zeitpunkt der Vertrag vom Kunden beendet wird. Eine Möglichkeit, die Anzahl der Regeln zu optimieren, besteht darin, dass Regelsätze von Diensten, die in einem vorher definierten Zeitintervall nicht mehr in Anspruch genommen wurden, automatisch entfernt und deaktiviert werden. Dienste, die nur einmalig genutzt werden sollen, kann der Benutzer beim Einfügen des Regelsatzes markieren, so dass nach der Dienstnutzung der Regelsatz automatisch entfernt wird. Dadurch entsteht eine übersichtliche Liste von Diensten, die regelmäßig genutzt werden.

6.1.4 Regelrepository

Zu jedem vom Benutzer berechtigten Dienst, der in der Service-Datenbank eingetragen ist, existiert mindestens ein Regelsatz. Dieser Regelsatz definiert, zu welchen Informationen der einzelne Dienst Zugriff hat. Bei einer Dienstnutzung können diese Dienste Informationen beim Privacy Provider anfragen. Existiert zu diesem Dienst in der Service Datenbank ein Eintrag, so wird der dort vorhandene Verweis auf den Regelsatz ausgelesen. Die Regeln werden im nächsten Schritt mit der Informationsanfrage verglichen. Hat der Benutzer bereits Informationen hinterlegt, so werden diese dem Dienst zur Verfügung gestellt, sofern dies vorgesehen ist. Falls noch keine Informationen hinterlegt worden sind, wird der Benutzer darüber informiert. Er besitzt zu diesem Zeitpunkt die Möglichkeit, die fehlenden Informationen in seinen Kontextdaten zu hinterlegen.

Bei der ersten Dienstnutzung muss ein Regelsatz in das Regelrepository eingefügt werden. Damit der Benutzer nicht selbst spezifizieren muss, welche Befugnisse der jeweilige Dienst erhält, stellen die Dienste bereits Default-Regelsätze bereit. Bei diesen Regelsätzen handelt es sich im idealen Fall um solche, die nur die minimale Menge an Informationen mit der für den Dienst notwendigen niedrigsten Informationsgenauigkeit fordern. Diese Regelsätze kann der Benutzer akzeptieren, ablehnen oder modifizieren. Akzeptiert er den Default-Regelsatz, so kann er sicher sein, dass die ausreichende Menge an Informationen zur Diensterbringung bereitsteht. Lehnt er den Regelsatz ab und erstellt auch keinen eigenen, so wird der Dienst nicht für die Nutzung freigegeben. Basierend auf dem Defaultregelsatz oder unabhängig davon, kann der Benutzer auch einen eigenen Regelsatz für den Dienst erstellen. Damit

ermöglicht er die Dienstnutzung. Dadurch, dass er vielleicht nicht die ausreichende Menge an Informationen bereitstellt, unterbleiben bestimmte Leistungen des Dienstes, da eine Diensterbringung auf bestimmten Informationen basiert (z.B. Positionsinformation für einen Routenplaner). Im normalen Fall kann der Benutzer bei einem vertrauenswürdigen Dienst den Default-Regelsatz verwenden.

Der Regelsatz kann aus einer beliebigen Anzahl von Regeln bestehen. Die Regelsätze werden unterschieden in Grundregeln, die für alle Dienste und Anwendungen gelten, und solche, die in direktem Zusammenhang mit einem Dienst definiert worden sind. Dieser Ansatz bietet den Vorteil, dass bestimmte Regeln nicht bei jeder Dienstnutzung erneut festgelegt werden müssen. Die folgenden Regelbestandteile können genutzt werden, um einen Regelsatz an die Situation des Benutzers anzupassen (basierend auf [Kü05]):

Dienst-Regeln (*service constraints*)
Ein Benutzer muss prinzipiell bestimmte Dienste erlauben bzw. unterbinden können.

Personen-Regeln (*actor constraints*)
Bei location-based Services ist es erforderlich, die Beteiligten festzulegen, denen man Zugriff auf die Positionsdaten erlaubt.

Bei diesen Beteiligten kann es sich handeln um:
- Provider von location-based Services
- Dritte, die über einen Dienst die Position eines Kunden ermitteln wollen

Zeit-Regeln (*time constraints*)
Die erstellten Regeln können nur in einem bestimmten Zeitraum Gültigkeit besitzen. Es werden für bestimmte Dienste oder Personen mehrere Regeln für unterschiedliche Zeiträume festgelegt. Diese Regeln ermöglichen es beispielsweise, dass ein Arbeitgeber nur während der Arbeitszeit den Standort eines Mitarbeiters detektieren kann, und dass in der Freizeit des Arbeitsnehmers diese Möglichkeit nicht besteht.

Orts-Regeln (*location constraints*)
Der Benutzer bestimmt Orte, an denen Dienste und Personen Zugang zu seinen Positionsinformationen erhalten können. Für die Anwendung dieser Regeln muss der Benutzer Hilfsmittel bereitgestellt bekommen, damit er einen Ort definieren kann. Er kann zum Beispiel durch Postadressen, Ortsnamen, Namen von Stadtteilen und spezieller Software den Raum bestimmen, an dem eine definierte Regel gelten soll.

Benachrichtigungs-Regeln (*notification constraints*)
Wenn ein autorisierter Dienst oder eine Person eine Position abfragen, so kann der Benutzer sich mit Hilfe dieser Regeln über den Vorgang unterrichten lassen. Dadurch kann er feststellen, wann Informationen angefragt werden. Auf Grund dieser Informationen kann er die Entscheidung treffen, ob er weiterhin einem Dienst oder einer Person die Erlaubnis zum Zugriff auf seine Kontextdaten geben will, bzw. die Berechtigung einschränken möchte.

Informations-Regeln (*information constraints*)
Mit Hilfe der Informations-Regeln legt der Benutzer fest, auf welche Daten der Dienst zugreifen kann (z.B. Positionsinformation aus der Datenbank für kontextbezogene Daten).

Genauigkeits-Regeln (*accuracy constraints*)
Für viele Dienste reicht oft eine Positionsinformation aus, die nicht die höchst mögliche Genauigkeit der verwendeten Positionierungstechnologie besitzt. Der Benutzer kann darüber entscheiden, welche Positionsgenauigkeit er an einen Dienst oder eine Person weiterleitet. Positionsinformationen, die ungenauer sind, lassen weniger Rückschlüsse über eine Person zu. Beispielsweise reicht eine Positionsinformation, die auf 10 m genau ist, aus, um einen speziellen Ort zu ermitteln, während eine Positionsinformation, die auf 100 m genau ist, nur besagt, dass eine Person sich im Umkreis eines "Häuserblocks" befindet. Für einen reinen Informationsdienst, der beispielsweise Restaurants in einem Stadtteil nennen soll, ist es nicht notwendig, die Positionsinformation mit der höchsten Genauigkeit bereitzustellen. Neben den Ortsinformationen können auch weitere Daten im Detaillierungsgrad reduziert werden. Beispielsweise kann der Benutzer festlegen, dass der Dienst nicht sein genaues Alter erfahren darf, sondern dass nur eine Kategorie (wie z.B. zwischen 18 und 25 Jahren) angegeben wird.

Identifikation-Regeln (*identity constraints*)
Bei diesem Vorgang kann der Benutzer entscheiden, dass seine Informationen nur anonymisiert weitergeben werden dürfen. Entscheidet er sich für die Anonymisierung, ist z.B. nur der Privacy Provider sichtbar oder es wird ein Pseudonym verwendet. Dieses Pseudonym darf jedoch keine weiteren Merkmale besitzen, anhand derer eine Ermittlung der eigentlichen Identität durch Dritte möglich ist. Je nach Dienst wird das Pseudonym automatisch von dem Privacy Server generiert. Dadurch ist ausgeschlossen, dass bei unterschiedlichen Diensten das gleiche Pseudonym verwendet wird und somit durch die Sammlung von Informationsstücken weitere Rückschlüsse auf den Benutzer möglich sind. Wünscht der Benutzer keine Verschleierung seiner Identität, so kann er das angeben.

Endgerät-Regeln (*end-device constraints*)
Basierend auf dem verwendeten Endgerät kann der Benutzer festlegen, welche Regelsätze aktiv oder inaktiv sind. Abhängig von der Aktivierung dient sein Endgerät privaten oder geschäftlichen Zwecken. Das erlaubt eine klare Trennung der beiden Kommunikationsfelder, ohne dass unterschiedliche Accounts benötigt werden. Dadurch wird der Verwaltungsaufwand reduziert und Daten aus arbeitsplatzbezogenen Anwendungen lassen keine Rückschlüsse auf privates Verhalten zu.

6.1.5 Erstellung eigener Regelsätze durch den Benutzer

Die Kombination der einzelnen Regeln ermöglicht es dem Benutzer, für jeden Dienst einen idealen Regelsatz zu erstellen. Die Flexibilität, die sich damit eröffnet, führt bei vielen Personen zur Überforderung. Resigniert könnten sie den kompletten Zugriff auf ihre Daten erlauben. Bei einem dilettantischen Vorgehen können sich Regeln widersprechen oder blockieren. Das Ergebnis wäre verminderte Qualität der Dienste und zunehmend geringere Akzeptanz durch die Kunden. Daher bieten alle Dienste einen Defaultregelsatz an. Dieser kann vom Benutzer eingesehen und bei Bedarf modifiziert werden. Zur Erstellung und Bearbeitung von Regelsätzen muss dem Benutzer ein Werkzeug zur Verfügung gestellt werden, um diese Aufgabe möglichst intuitiv bewerkstelligen zu können. Der Editor sollte den Benutzer bei der Bearbeitung unterstützen und auf mögliche Sicherheitsrisiken und Fehler im Regelsatz hinweisen.

6.2 Datennutzungslog

Im Datennutzungslog wird vermerkt, welche Dienste wann verwendet worden sind. Dabei wird der Zugriff auf alle sensiblen Daten im Zusammenhang mit der Nutzung eines Dienstes protokolliert. Der Datensatz beinhaltet nicht die eigentlichen sensiblen Informationen, sondern nur den Hinweis, dass diese im Rahmen der Dienstnutzung für einen bestimmten Zweck verwendet worden sind. Zusätzlich werden Änderungen in den Regelsätzen und Zahlungstransaktionen protokolliert. Basierend auf diesen Informationen kann der Benutzer während des Betriebs abschätzen, ob ein Dienst oder eine mit einem Dienst verbundene Person (z.B. bei einem Instant-Messaging-Dienst) weiterhin Zugriff zu freigegebenen Daten erhalten soll. Sollte der Benutzer beispielsweise eine mögliche missbräuchliche Nutzung feststellen, so kann er diese mit Hilfe der Regeln einschränken oder dem Dienst bzw. der Person den Zugriff zu den jeweiligen Information nicht oder nur mit reduzierter Genauigkeit erlauben. Dies wäre z.B. der Fall, wenn eine Person in regelmäßigen Abständen die Position des Benutzers abrufen würde, ohne dass dafür eine Notwendigkeit besteht. Eine geeignete Oberfläche erlaubt die Übersicht über die genutzten Dienste, die dabei verwendeten Daten und die angefallenen Kosten. Basierend auf den Logdateien lässt sich feststellen, ob Informationen mit reduzierter Qualität transferiert worden sind. Das lässt Rückschlüsse auf Störquellen zu. Im Weiteren kann auch anhand der über einen längeren Zeitraum nachgefragten Informationen ermittelt werden, ob ein Regelsatz Zugriff auf mehr Informationen erlaubt, als für die eigentliche Diensterbringung notwendig ist. Im Datennutzungslog hinterlegte Daten ermöglichen eine Methode zur automatischen Optimierung von Regelsätzen.

6.2.1 Registrierungsstelle (Registration Authority)

Jeder Privacy Provider beinhaltet eine Registrierungsstelle von einer angeschlossen PKI. Mit Hilfe dieser Registrierungsstelle besitzen die Benutzer die Möglichkeit, selbst erstellte öffentliche Schlüssel einzureichen und von der Zertifizierungsstelle im Trust Center signieren zu lassen. Derartige Zertifikate besitzen die notwendigen Attribute, die für eine Nutzung innerhalb dieser Architektur notwendig sind. Der Privacy Provider stellt sicher, dass die Identitätsinformationen korrekt vorliegen, da andernfalls keine Signierung des öffentlichen Schlüssels möglich ist. Das Zertifikat wird zur Authentifizierung und Verschlüsselung verwendet. Basierend auf den Möglichkeiten der asymmetrischen Verschlüsselung, kann dadurch eine Unabstreitbarkeit (non-repudation) erreicht werden, die notwendig ist, um kommerzielle Dienste realisieren zu können. Die Unabstreitbarkeit ist eine wichtige Eigenschaft, damit der Dienstanbieter nachweisen kann, dass ein Kunde einen kostenpflichtigen Dienst genutzt hat und er somit Anspruch auf die Nutzungsgebühren hat.

6.3 Anmelden beim Privacy Provider

Damit ein Benutzer kontextbezogene Dienste verwenden kann, muss er sich zuerst einen Account bei einem Privacy Provider einrichten. Dazu muss er die folgenden Schritte ausführen, damit der Account auch vollständig aktiviert wird:

Der Benutzer wählt sich einen beliebigen Privacy Provider, bei dem er einen Account erstellen möchte. Die Auswahl sollte auf einen Anbieter fallen, der das Vertrauen genießt. Es sollte ein ähnliches Vertrauensverhältnis wie zu einer Bank bestehen, da dieser Anbieter auf alle sensiblen Informationen zugreifen kann und auch als Mittelsmann bei den Zahlungen an den jeweiligen Dienst fungiert.

Der Benutzer ruft die Webseite des Privacy Providers auf und erstellt einen Account. In diesem Zusammenhang legt er einen Benutzernamen und ein Kennwort für den Webzugang des Privacy Providers fest. Im darauf folgenden Schritt gibt er Informationen zu seiner Person frei, die zur Identifikation verwendet werden. Abschließend gibt er an, wie viele Endgeräte er von Beginn an mit diesem Account verwalten möchte.

Der Privacy Provider erstellt für jedes Endgerät, das der Benutzer einsetzen möchte, eine zeitlich begrenzte TAN. Zusätzlich erhält der Benutzer eine persönliche PIN, die beispielsweise benötigt wird, um Zertifikate zu widerrufen oder weitere TANs zu beantragen. Diese Nummern werden dem Benutzer auf dem Postweg zugesendet. Diese TANs erhält der Benutzer nur, wenn er seine Identität mit Hilfe des Post-Identverfahrens nachweisen kann. Damit ist sichergestellt, dass die personenbezogenen Informationen auch tatsächlich vom Benutzer stammen. Der Nachweis der Identität ist für die Abwicklung von Rechtsgeschäften wie z.B. von Kaufverträgen oder bei der Nutzung von kostenpflichtigen Diensten notwendig, damit die entstandenen Kosten einer Person zugerechnet werden können.

Mit Hilfe der TANs besitzt nur der Benutzer die Möglichkeit, Endgeräte mit seinem Privacy Provider Account zu verknüpfen. In dem Endgerät werden die Accountinformationen und eine TAN eingegeben. Das Endgerät generiert sich ein eigenes Schlüsselpaar. Der öffentliche Schlüssel wird mit einer gültigen TAN an den Privacy Provider gesendet. Anhand der TAN, die nur ein einziges Mal verwendet werden kann, wird geprüft, ob der Benutzer berechtigt ist, weitere Geräte unter dem Account laufen zu lassen. Die TANs sind zeitlich nur begrenzt gültig. Dies stellt sicher, dass der Benutzer nicht im Voraus mehr TANs beantragt hat, als er benötigt. Bei ungenutzten TANs besteht die Gefahr, dass sie an unbefugte Dritte gelangen.

Der Privacy Provider besitzt eine Registrierungsstelle von einer PKI. Er prüft die Gültigkeit der TAN, der Accountdaten und des Schlüssels. Sind die Informationen gültig, so werden sie an eine angeschlossene Zertifizierungsstelle weitergereicht. Der öffentliche Schlüssel wird in der Zertifizierungsstelle signiert. Das Zertifikat wird bei diesem Vorgang um die notwendigen Informationen ergänzt, die bei der Nutzung innerhalb der Architektur benötigt werden (z.B. zugehöriger Privacy Provider, Funktion innerhalb der Architektur usw.). Das so signierte Zertifikat wird dem Benutzer zur Verfügung gestellt. Dazu wird es zentral in der PKI gespeichert. Dienste können mit Hilfe der Validierungsstelle prüfen, ob ein Zertifikat noch Gültigkeit besitzt.

Der im Endgerät generierte private Schlüssel wird in einem vertrauenswürdigen Bereich des Betriebssystems verschlüsselt gespeichert. Dadurch ist sichergestellt, dass nur befugte Anwendungen Zugriff besitzen. Dadurch, dass das Schlüsselpaar im Endgerät generiert worden ist, ist ausgeschlossen, dass andere Instanzen Zugriff zu den privaten Schlüsseln erhalten.

6.4 Trust-Center

Innerhalb der Architektur sind alle Bestandteile einer PKI-Infrastruktur integriert[7]. Das Trust-Center beinhaltet die folgenden Komponenten [CE05]:

Zertifizierungsstelle	(*Certificate Authority*, CA)
Zertifikatssperrliste	(*Certificate Revocation* List, CRL)
Validierungsdienst	(*Validation Authority*, VA)
Verzeichnisdienst	(*Directory Service, DS*)

Innerhalb des Privacy Providers befindet sich die

Registrierungsstelle	(*Registration Authority*, RA).

Der folgende Abschnitt beschreibt die Vorteile, die durch den Einsatz von asymmetrischen Verschlüsselungen entstehen. Abbildung 24 zeigt schrittweise den Erstellungsvorgang eines Zertifikates. Es wird davon ausgegangen, dass der Benutzer sich bereits per Post-Identverfahren ausgewiesen hat. Dadurch ist er im Besitz von gültigen TANs.

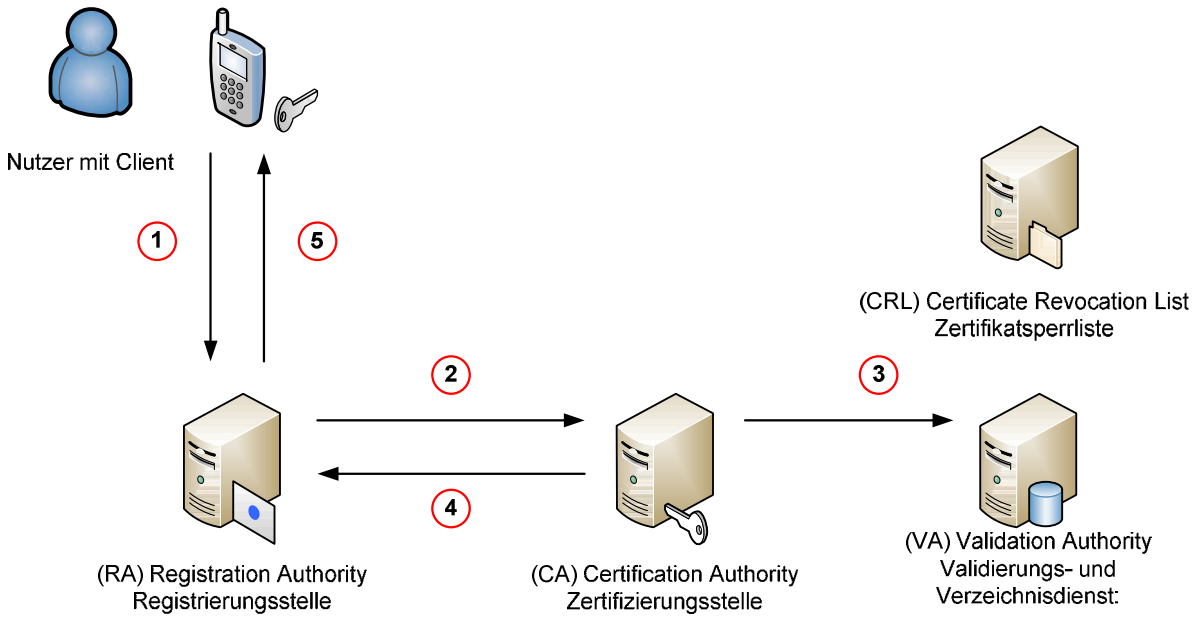


Abbildung 24 - Erstellen eines Zertifikats

Im ersten Schritt erstellt der Benutzer nach dem Anmeldevorgang beim Privacy Provider für das jeweilige Endgerät (siehe Kapitel 6.3) ein Schlüsselpaar. Damit der öffentliche Schlüssel innerhalb der Architektur verwendet werden kann, muss er signiert werden. Dazu wird dieser an die Registrierungsstelle des Privacy Providers mit einer TAN übermittelt. Durch den Besitz der TAN ist schon mit Hilfe des Post-Identverfahrens nachgewiesen worden, dass die bei der Anmeldung hinterlegten Informationen wahrheitsgemäß angegeben worden sind. Jeder

[7] Eine ausführliche Einführung in das Thema PKI entnehmen Sie bitte [CE05].

Privacy Provider besitzt eine Registrierungsstelle eines PKI-Anbieters. Über diese werden die öffentlichen Schlüssel angenommen und es wird geprüft, ob die TANs zum Zeitpunkt der Anfrage gültig sind. Falls dies der Fall ist, werden im 2. Schritt der Schlüssel sowie die notwendigen Informationen an die Zertifizierungsstelle des PKI-Anbieters weitergeleitet. Dieser zertifiziert den öffentlichen Schlüssel. Durch die Integration weiterer Informationen für die Verwendung des Schlüssels und die Signierung durch die Zertifizierungsstelle wird aus dem öffentlichen Schlüssel ein Zertifikat. Das so erstellte Zertifikat wird im 3. Schritt an den Verzeichnisdienst übermittelt. Dieser ermöglicht es, dass Instanzen das Zertifikat abfragen oder mit Hilfe des Validierungsdienstes überprüfen können. Im 4. Schritt wird es an die Registrierungsstelle übermittelt und es wird im Kundendatensatz des Privacy Providers gespeichert. Im 5. Schritt wird es auch an den Benutzer weitergeleitet. Dieser besitzt nur ein gültiges Zertifikat für die Nutzung der Architektur.

Durch den Einsatz von asymmetrischer Verschlüsselung erfolgt

- der Nachweis der Identität
- die Verschlüsselung der Daten
- die Signierung der Informationen
- die Nichtabstreitbarkeit der Dienstnutzung
- die Bekanntgabe der Funktion einer Instanz innerhalb der Architektur

Durch den Einsatz einer für alle vertrauenswürdigen Instanz, des Trust Centers, die den öffentlichen Schlüssel um Verwendungsdaten aufwertet, die Korrektheit der Daten prüft und dies mit einer eigenen Signatur nachweist, wird eine Nutzung von gewerblichen und somit potentiell kostenpflichtigen Diensten ermöglicht. Für derartige Dienste ist der Nachweis der Identität notwendig, um die entstandenen Gebühren eindeutig abzurechnen. Dadurch, dass das Schlüsselpaar vom Benutzer auf seinem Endgerät erstellt worden ist, besteht keine Gefahr, dass der private Schlüssel durch Dritte missbraucht wird.

6.4.1 Attribute eines Zertifikates

Die verwendeten Zertifikate benutzen die Version X.509v3 [CFS03, PFS02]. Dadurch können sie um zusätzliche Attribute erweitert werden. Diese Erweiterungsfähigkeit wird benötigt, da nicht nur die Endgeräte der Benutzer, sondern alle Instanzen innerhalb der Architektur Zertifikate für den Betrieb benötigen. Je nach Instanz besitzen sie besondere Berechtigungen oder erfüllen spezielle Aufgaben bei der Diensterbringung.

Abbildung 25 zeigt das Zertifikat des „Regionalen Hochschulrechenzentrums Kaiserslautern“ als ein exemplarisches Beispiel für das X.509v3-Zertifikat. Die gelb markierten Felder werden vom Privacy Provider analysiert. Anhand des Bereichs „Subject“ kann der Privacy Provider sicherstellen, dass die Daten vom vorgesehenen Absender sind bzw. an einen berechtigten Empfänger gesendet werden.

```
C:\OpenSSL\bin>openssl x509 -inform DER -in g_cacert.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 169296693 (0xa174335)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN-Verein PCA Global - G01
        Validity
            Not Before: Mar 14 09:51:34 2007 GMT
            Not After : Mar 13 00:00:00 2019 GMT
        Subject: C=DE, O=Regionales Hochschulrechenzentrum Kaiserslautern, CN=RHRK-CA - G02/emailAddress=ca@rhrk.uni-kl.de
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:ae:40:43:1d:d2:06:b6:d9:0e:c3:b5:98:74:9d:
                    81:8a:c3:a7:8a:e1:e5:24:23:de:a7:fd:29:51:e4:
                    db:f5:01:4b:65:aa:6b:a1:d7:9e:46:6e:a4:16:2c:
                    76:5c:69:77:87:88:a6:2e:ee:dd:1b:0b:6e:f2:84:
                    51:a4:67:19:ea:d9:b7:8b:65:52:a7:0d:73:c7:19:
                    3d:b9:45:76:b0:c8:91:1c:ad:87:56:43:77:a9:61:
                    70:ab:f4:41:3a:03:c4:69:53:61:74:5e:61:33:3e:
                    d0:66:36:6b:75:7b:57:38:ce:0b:18:6f:24:05:9a:
                    83:ef:94:3e:53:49:9b:b4:36:a0:38:bd:4d:23:0b:
                    49:b9:8d:d8:aa:72:ff:e8:7b:e9:b5:be:05:df:44:
                    43:55:49:d8:9a:1b:16:55:7f:91:08:d6:8c:bc:ed:
                    6b:53:d8:07:1c:e3:48:08:4b:fc:00:03:f5:5c:a4:
                    57:e0:be:e5:07:be:f0:0e:93:59:2f:a0:88:98:fa:
                    7e:c4:f1:f2:6e:75:3a:7b:df:10:8d:36:b7:22:73:
                    b8:d0:4f:2c:08:a7:21:5e:b5:9f:a4:a7:ae:c1:6f:
                    22:5d:24:f0:8c:4a:7b:ce:e8:52:df:da:03:3f:01:
                    e6:35:8c:cf:2c:41:78:34:ed:4b:49:42:8a:d4:f3:
                    45:b3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                2F:DD:13:98:63:5C:0B:C3:6F:B8:ED:86:E0:03:27:C1:6F:BA:B6:02
            X509v3 Authority Key Identifier:
                keyid:49:B7:C6:CF:E8:3D:1F:7F:EA:44:7B:13:29:F7:F1:0A:70:3E:DE:64

            X509v3 Subject Alternative Name:
                email:ca@rhrk.uni-kl.de
            X509v3 CRL Distribution Points:
                URI:http://cdp1.pca.dfn.de/global-root-ca/pub/crl/cacrl.crl
                URI:http://cdp2.pca.dfn.de/global-root-ca/pub/crl/cacrl.crl

            Authority Information Access:
                CA Issuers - URI:http://cdp1.pca.dfn.de/global-root-ca/pub/cacert/cacert.crt
                CA Issuers - URI:http://cdp2.pca.dfn.de/global-root-ca/pub/cacert/cacert.crt

    Signature Algorithm: sha1WithRSAEncryption
        d4:a8:6a:d8:b4:5c:86:5c:4a:31:ad:9f:b0:df:4e:46:82:29:
        59:84:34:aa:81:ce:0f:4c:95:d1:66:2b:75:57:db:97:66:da:
        84:06:3a:76:78:ea:22:06:d9:12:4e:7f:22:b4:8c:e3:9d:44:
        7b:d6:56:21:fd:d0:d3:65:13:77:5a:80:7f:d3:94:18:af:cc:
        71:4f:85:68:cc:9c:35:1d:46:51:fb:a5:f4:49:af:72:5d:ab:
        0d:60:21:ad:ab:57:a6:5c:40:dd:4e:32:58:55:24:45:2f:d8:
        2c:eb:d8:6a:85:ba:dd:d2:b2:26:5f:ab:83:0b:0a:3d:83:95:
        1b:ac:41:62:ec:d3:7c:6a:83:ba:42:cf:59:c0:91:87:5b:bc:
        6f:41:64:17:39:56:97:42:11:49:a1:5d:48:85:1f:08:b4:ff:
        5f:c2:f6:fd:7f:cc:33:bd:d7:57:c5:11:c6:d6:4a:96:fd:e9:
        f6:bc:38:5c:5c:6b:57:bc:ef:08:96:cf:b3:99:69:e8:07:98:
        68:db:a3:f4:56:01:54:1b:31:10:e4:c5:6c:2e:a4:39:2e:2d:
        53:72:5a:b6:13:08:e6:83:4c:e3:96:fc:a8:c6:f4:4b:c7:da:
        00:04:24:97:55:f0:40:5d:94:39:7a:d9:05:4b:46:5c:50:19:
        78:cb:c0:4f
```

Abbildung 25 - X.509v3-Zertifikat

Im Bereich der „X509v3 extensions“ befinden sich im Rahmen dieser Architektur alle Informationen, die die Funktion einer Instanz im Besonderen auszeichnet.
In den Zertifikaten sind folgende Attribute hinterlegt:

- Trust Center
- Endgerät mit zuständigem Privacy Provider
- Clearing Provider
- Privacy Provider
- Service Provider
- Location Provider
- Location Data Sources

Entsprechend ihrer Aufgabe besitzen die Instanzen unterschiedliche Möglichkeiten auf Informationen zuzugreifen oder diese zu liefern.

Die Eigenschaften der beteiligten Instanzen werden im Folgenden beschrieben:

Trust Center

Das Trust Center hat als einzige Instanz die Berechtigung, öffentliche Schlüssel zu signieren. Nur Teilnehmer mit gültigen Zertifikaten haben die Erlaubnis, Dienste zu nutzen. Ein Trust Center ist in eine bestehende PKI-Infrastruktur eingebunden.

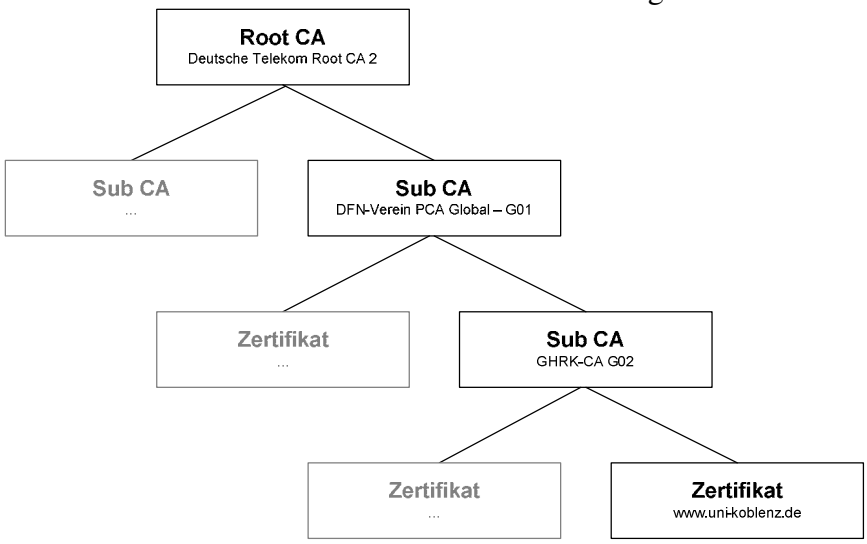


Abbildung 26 - PKI Hierarchie

Abbildung 26 stellt einen Ausschnitt der PKI-Infrastruktur dar, über die Zertifikate, hier am Beispiel der Universität Koblenz, bereitgestellt werden. Ein Trust Center kann in eine vergleichbare Hierarchie eingebunden und beispielsweise als Sub CA tätig sein. Durch die Erweiterbarkeit des X.509v3-Standards ist es möglich, dass bereits bestehende PKI-Infrastruktur durch die Erweiterung der Attribute für die Aufgabe verwendet werden kann. Abhängig von den vorhandenen Attributen ist es der jeweiligen Instanz gestattet, auf unterschiedliche Daten oder Ressourcen zuzugreifen.

Endgerät

Einem Endgerät ist es erlaubt, Dienste zu nutzen, wenn ein Account bei einem Privacy Provider vorhanden ist. Dieser ist auch zuständig für die Abrechnung der angefallenen Kosten der Dienstnutzung. Nur Benutzer mit einem gültigen Zertifikat dürfen Regelsätze ändern, Informationen einsehen oder Kontextinformationen verändern.

Location Data Sources

Innerhalb der Architektur besitzen unterschiedliche Instanzen die Möglichkeit, Positions- oder Sensorinformationen der Benutzer bereitzustellen. Nur die Informationen von qualifizierten Instanzen werden von dem Location Provider bei der Berechnung einer fusionierten Positionsinformation berücksichtigt. Dies hat den Vorteil, dass Dritte keine Position vorgeben können, die zum Nachteil des Benutzers ausgelegt werden könnte oder die zu festgelegten Aktionen führt.

Location Provider
Nur Location Provider ist es gestattet, Informationen von Location Data Sources zu erhalten oder abzufragen (abhängig von der verwendeten Technologie der Positionsbestimmung). Ein Location Provider ist immer mit einem bestimmten Privacy Provider exklusiv verbunden. Somit kann die Location Data Source anhand des Zertifikats des Benutzers ermitteln, ob der anfragende Location Provider befugt ist, diese Information abzufragen.

Clearing Provider
Die Clearing Provider realisieren die Abrechnung der in Anspruch genommenen Dienste und die Verrechnung von Gutschriften. Damit die Anzahl der Transaktionen zum eigentlichen Bankkonto reduziert wird, sammelt der Clearing Provider die Zahlungsein- und -abgänge und berechnet an einem festgelegten Zeitpunkt die Differenz. Der Differenzbetrag wird mit dem Kundenkonto verrechnet. In dem Zertifikat, das vom Clearing Provider verwendet wird, sind zusätzliche Attribute enthalten, die nachweisen, dass diese Instanz Geldgeschäfte abwickeln darf. Dadurch ist sichergestellt, dass keine Unbefugten sich als Clearing Provider ausgeben können. Optional besteht die Möglichkeit, dass im Zertifikat noch weitere Angaben enthalten sind, wie die maximale Deckungssumme, die bei einer Transaktion möglich ist. Verwendet ein Benutzer einen Clearing Provider, der nicht nur auf Mikro-Payment spezialisiert ist, sondern auch die Buchung von größeren Geldbeträgen ermöglicht, so können auch Dienstleistungen und Warenlieferungen abgerechnet werden.

Privacy Provider
Der Privacy Provider als zentrales Bindeglied zwischen dem Dienst und dem Benutzer hat als einzige Instanz die Möglichkeit, Kontextinformationen bekanntzugeben. Über diese Instanz fließen alle Informationen der Dienstnutzung, damit sichergestellt ist, dass die Regelsätze bei der Dienstnutzung berücksichtigt werden. Im Weiteren fungiert der Privacy Provider als eine Instanz, die Dienste im Namen von Benutzern aufrufen kann und die Dienstnutzung stellvertretend über den Clearing Provider bezahlt.

Service Provider
Der Service Provider fragt im Rahmen der Diensterbringung Kontextinformationen ab und verfügt Zahlungsanweisungen.

Auditing Attribute
Mit Hilfe von anerkannten Auditing-Unternehmen wird die Qualität von Instanzen geprüft. Der Benutzer kann hinterlegte Kriterien verwenden, um abzuklären, ob die genutzten Dienste seine Anforderungen erfüllen. Das Anforderungsprofil muss er zu Beginn festgelegt haben. Bei einer Dienstnutzung wird dieses mit den Leistungen des Dienstes verglichen. Entspricht der Dienst nicht den Erwartungen, so kann der Benutzer zunächst darüber informiert werden oder die Nutzung wird sofort unterbunden.

6.4.2 Widerruf eines Zertifikates

Die ausgestellten Zertifikate besitzen einen fest definierten Gültigkeitszeitraum. Innerhalb dieses Zeitraums besteht jedoch die Möglichkeit, die Gültigkeit des Zertifikats zu widerrufen. Dies wäre z.B. dann erforderlich, wenn ein Gerät abhanden gekommen ist oder der Benutzer den Account beim Privacy Provider löscht. Die in Abbildung 27 gezeigten Schritte sind notwendig, um ein noch gültiges Zertifikat zu widerrufen.

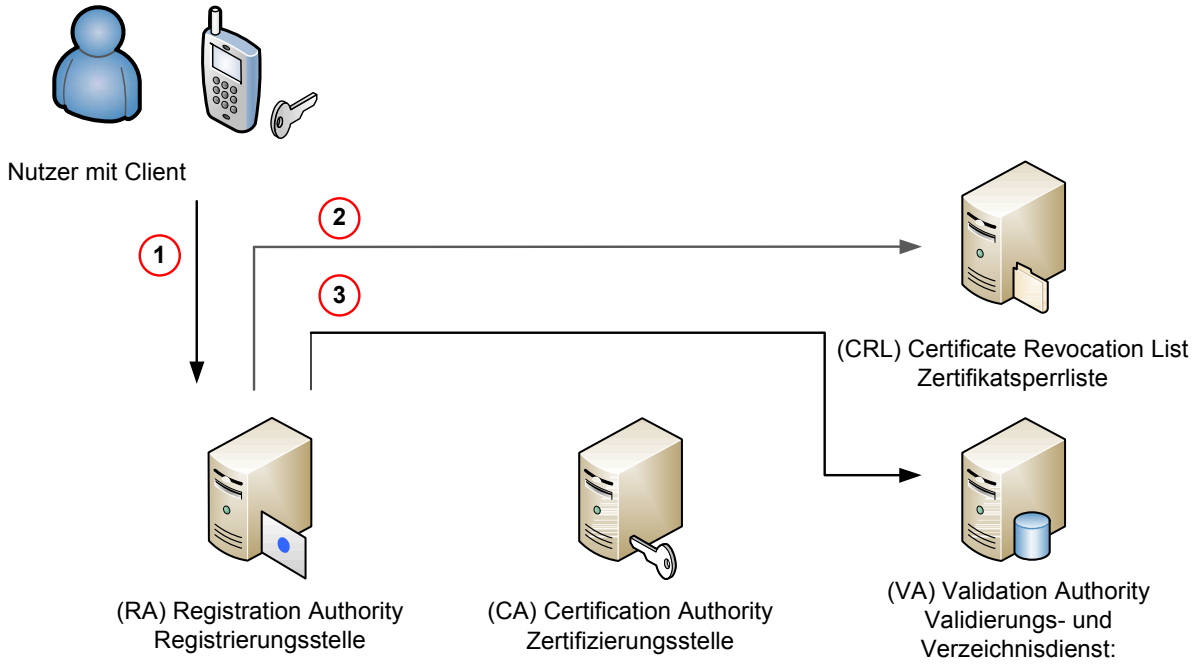


Abbildung 27 - Widerrufen eines Zertifikates

Möchte ein Benutzer ein Zertifikat widerrufen, so muss er im ersten Schritt die Registrierungsstelle davon in Kenntnis setzen. Er loggt sich in den Verwaltungsbereich des Privacy Providers ein oder verwendet das dazugehörige Telefondialogsystem. Mit Hilfe der Accountinformationen und der zugeteilten PIN ist er berechtigt, einzelne Zertifikate zu widerrufen oder im Bedarfsfall neue TANs zu bestellen. Die erfolgreich widerrufenen Zertifikate werden im nächsten Schritt in die Zertifikatssperrliste eingetragen. Die Zertifikatssperrliste enthält nur die Zertifikate, die während des Gültigkeitszeitraums für ungültig erklärt worden sind. Im dritten Schritt wird das Zertifikat im Verzeichnisdienst als ungültig markiert. Allen Instanzen, die sich von diesem Zeitpunkt an mit Hilfe des Validierungsdienstes darüber informieren, wird mitgeteilt, dass das Zertifikat als ungültig eingestuft wurde. Dadurch ist keine Dienstnutzung des Endgerätes mehr möglich, da vor jeder sensiblen Aktion die Gültigkeit des Zertifikats geprüft wird.

6.4.3 Validierungsdienst

Mit Hilfe des Validierungsdienstes überprüfen die Instanzen die Gültigkeit eines Zertifikates. Dieser Überprüfungsprozess wird zu Beginn jeder Transaktion aufgerufen. Dadurch wird sichergestellt, dass nur befugte Endgeräte Zugriff zu sensiblen Informationen erhalten. Somit ist ausgeschlossen, dass z.B. mit gestohlenen Geräten kostenpflichtige Dienste genutzt werden, sofern der Benutzer direkt nach dem Verlust das Zertifikat widerruft. Die dazu notwendigen Informationen erhält der Validierungsdienst aus der Zertifikatssperrliste. Der Validierungsdienst bietet zusätzlich die Möglichkeit, gültige Zertifikate aus dem Verzeichnisdienst aufzurufen.

7 Kommunikation zwischen den Instanzen der Architektur

Eine wichtige Forderung bei der Entwicklung der Architektur besteht darin, dass die beteiligten Instanzen nur Zugriff auf die Informationen erhalten, die für sie Relevanz besitzen. Daher ist es notwendig, dass bestimmte Informationsabschnitte gezielt nur bestimmten Instanzen bereitstehen. Ermöglicht wird dies durch das für diesen Fall entwickelte Nachrichtenformat. In diesem Format besitzen die beteiligten Instanzklassen einen definierten Abschnitt innerhalb der Nachricht (siehe Abbildung 28).

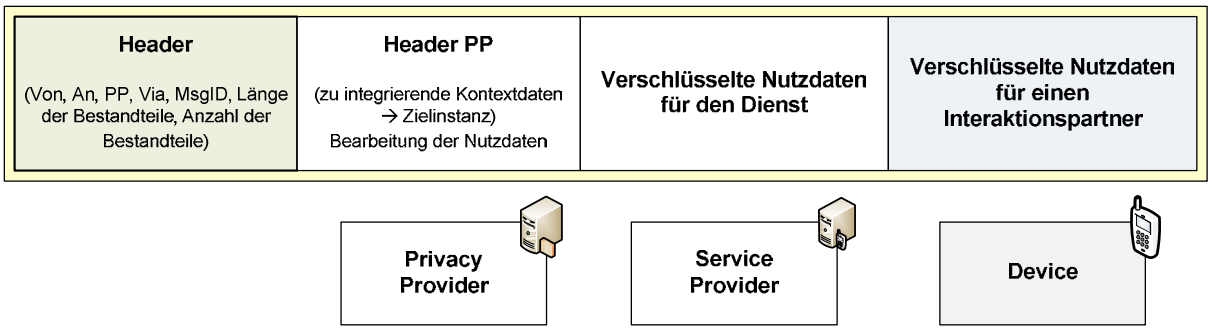


Abbildung 28 – Nachrichtenformat für die instanzenübergreifende Kommunikation

Eine Nachricht ist in folgende Bereiche aufgeteilt:

- Header
- Header für den Privacy Provider (PP)
- Verschlüsselte Nutzdaten für den Dienst
- Verschlüsselte Nutzdaten für einen Interaktionspartner (optional)

Die Nachricht wird bei der Übertragung zwischen den Instanzen per SSL verschlüsselt. Bis auf den Header (grüner Bereich in der Abbildung 28) liegen alle Abschnitte in zusätzlich asymmetrisch verschlüsselter Form vor. Diese Abschnitte können nur von dem befugten Empfänger entschlüsselt werden. Zusätzlich wird die Nachricht signiert, um sicherzustellen, dass sie von einem bekannten Absender stammt und während der Übermittlung nicht verändert worden ist.

Header

Der Header liefert alle Informationen zum grundlegenden Nachrichtenrouting und zur Verarbeitung. Im Header ist ersichtlich, von welcher Instanz an welche Instanz die Nachricht gesendet wird. Des Weiteren enthält der Header Informationen über die Nachricht selber. Da das Nachrichtenformat auch optionale Bestandteile besitzt, bzw. während der Verarbeitung Teile entfernt werden, wird im Header vermerkt, aus wie vielen Bereichen die Nachricht besteht. Dadurch wird überprüfbar, ob die Nachricht vollständig übermittelt worden ist. Zusätzlich kann dies die Verarbeitung der Nachrichten beschleunigen. Wird eine Nachricht an eine weitere beteiligte Instanz weitergeleitet, so wird der Header angepasst. Zur Datenreduzierung werden Bereiche geleert, die für die nachfolgenden Instanzen keine Relevanz besitzen. Zusätzlich werden bei anonymisierter Dienstnutzung die Absendeinformationen so verändert, dass als Absender nur der Privacy Provider sichtbar ist. Somit ist es unmöglich, dass der eigentliche Benutzer mit der Dienstleistungsnutzung in Verbindung gebracht wird. Anhand der verwendeten Message-ID, die jeweils über einen

Zufallsmechanismus gebildet wird, kann die Antwort später vom Privacy Provider zugeordnet und weitergeleitet werden.

Header PP
Im Bereich „Header PP“ sind Nachrichten an den Privacy Provider oder von ihm enthalten. Dieser Bereich wird für die Anfrage, Übermittlung und Modifikation von Kontextinformationen verwendet. Im Weiteren enthält er Informationen oder Einstellungen zu den verwendeten Regelsätzen, die die Dienstnutzung betreffen. Bei der Nutzung von kostenpflichtigen Diensten werden über dieses Feld auch Zahlungsanweisungen und –informationen übermittelt.

Verschlüsselte Nutzdaten für den Dienst
Der Privacy Provider ist zuständig für die Einhaltung der vom Benutzer definierten Regeln. Dadurch ist sichergestellt, dass nur freigegebene Kontextinformationen bei der Dienstnutzung verwendet werden. Informationen über die eigentliche inhaltliche Dienstnutzung sind jedoch für den Entscheidungsprozess des Privacy Providers nicht relevant. Zur Datenminimierung besitzen nur die an der Dienstnutzung beteiligten Instanzen, somit der Benutzer und der Dienst selber, die Möglichkeit, Daten auszutauschen. Diese Informationen werden über den Privacy Provider übermittelt. Bei Diensten, die der Benutzer in personalisierter Form verwendet, werden die Nutzdaten so verschlüsselt, dass nur der Benutzer und der Dienst Zugriff auf die Daten erhalten. Soll ein Dienst in anonymisierter Weise benutzt werden, so muss dieser Bereich vom Privacy Provider verschlüsselt werden. Nur so ist sichergestellt, dass keine Rückschlüsse auf den Benutzer möglich sind. Das anonymisierte Verfahren führt jedoch dazu, dass der Privacy Provider auch tiefere Einsichten in die Inhalte des verwendeten Dienstes erhält.

Verschlüsselte Nutzdaten für einen Interaktionspartner
Das Nachrichtenformat erlaubt es optional, Informationen mit einem am Dienst beteiligten Interaktionspartner auszutauschen. Das wird beispielsweise von Diensten wie einem Instant Messanger genutzt. Diese Dienste stellen nur eine Zwischeninstanz zu weiteren am Dienst beteiligten Instanzen dar, die als eigenständige Interaktionspartner auftreten. Informationen über die eigentlichen Inhalte der Kommunikation zwischen den Interaktionspartnern werden nicht benötigt. Diese werden in einem speziellen Bereich des Nachrichtenformats verschlüsselt übertragen.

Das Nachrichtenformat gestattet es, noch weitere Organisations- und Konfigurationsinhalte zu übermitteln. Eine Nachricht kann folgende Informationen enthalten:

- Statusinformationen
- Dienstnutzung
- Regeln / Kontextdaten
- Zahlungsinformationen

Der folgende Abschnitt beschreibt die Funktionsweise und die Kommunikation der beteiligten Instanzen im Falle der oben genannten Informationen (Statusinformationen, etc.).

7.1 Statusinformationen

Bei der Nutzung von Diensten werden je nach Situation Statusinformationen an den Benutzer gesendet. Diese Nachrichten beinhalten Informationen zur aktuellen Dienstnutzung. Beispielsweise kann ein Benutzer sich darüber informieren lassen, wann ein Dienst eine bestimmte Kontextinformation abfragt. Je nach Regelsatz muss der Benutzer den Zugriff auf diese Information freigeben. Die Statusinformation kann somit mit Interaktionsbestandteilen erweitert werden. Der Benutzer kann neben dem Zustimmen und Ablehnen einer Dienstnutzung oder einer Freigabe von Informationen auch Zugangskennungen wie z.B. Passwörter oder PINs eingeben, um sicherheitskritische Dienste vor einer unbedachten Nutzung zu schützen.

7.2 Dienstnutzung

Bei der Dienstnutzung werden Informationen zwischen dem Benutzer und dem Dienst ausgetauscht. Komplexe Dienste wie z.B. Instant-Messaging-Dienste bieten über den Dienst die Kommunikation mit weiteren Kommunikationspartnern. Zur reinen Übermittlung der Daten für den Dienst werden die folgenden zwei Bereiche des Nachrichtenformats verwendet:

- Verschlüsselte Nutzdaten für den Dienst
- Verschlüsselte Nutzdaten für den Interaktionspartner (optional)

Bei einer Dienstnutzung muss zwischen einer personalisierten und anonymisierten Form unterschieden werden. Abbildung 29 zeigt die Dienstnutzung in personalisierter Form, bei der die Identität des Benutzers dem Dienst bekannt gegeben wird. Die personalisierte Form hat den Vorteil, dass sowohl die Daten an den Dienst, als auch die optionalen Daten an den Interaktionspartner, vom Benutzer verschlüsselt werden. Dadurch ist es dem Privacy Provider unmöglich, die eigentlichen Inhalte der Nachrichten einzusehen.

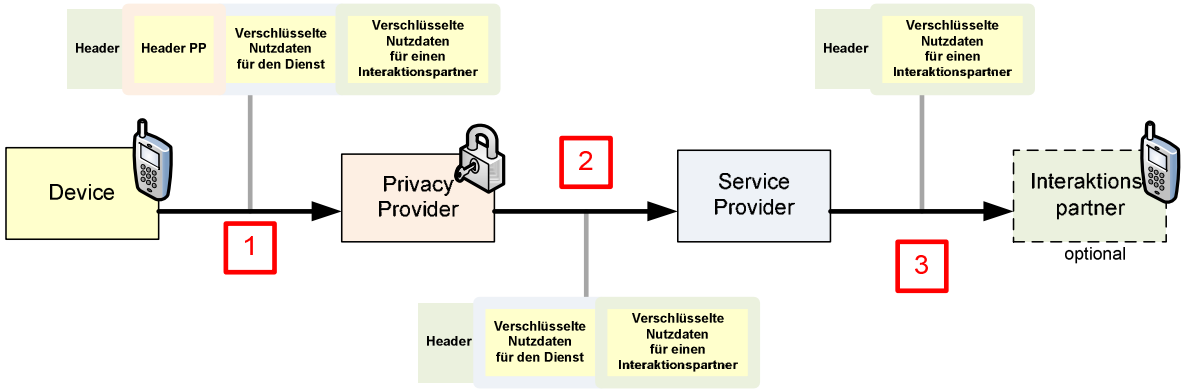


Abbildung 29 - Kommunikation bei einer personalisierten Dienstnutzung[8]

Bei einer personalisierten Kommunikation sendet das Endgerät des Benutzers (Device) eine vollständige Nachricht mit allen Bestandteilen des Nachrichtenformats an den Privacy Provider. Im Header ist ersichtlich, an welchen Dienst die Nachricht geleitet werden soll. Der Header PP kann nur durch den Privacy Provider entschlüsselt werden. In diesem Bereich können beispielsweise Kommandos zur Anpassung der Regelsätze enthalten sein.

[8] In der Grafik beschreibt die Hintergrundfarbe den für andere Instanzen sichtbaren Absender. Die Rahmen um die Abschnitte des Nachrichtenformats bezeichnen die Instanz, die aufgrund der asymmetrischen Verschlüsselung Zugriff zu den Daten erhält.

Zunächst überprüft der Privacy Provider, ob eine Dienstnutzung möglich ist. Für den Fall, dass der Dienst genutzt werden kann, wird die Nachricht weitergeleitet. Der Teil des Headers, der an den Privacy Provider gerichtet war, wird dabei entfernt, da dieser Bestandteil für den Dienst und die weiteren Instanzen keine Relevanz besitzt. Für die Übermittlung muss der Privacy Provider den Header anpassen.

Die Nachricht wird vom Service Provider empfangen. Die Nutzdaten können von dieser Instanz entschlüsselt werden. Die Daten werden abhängig vom Dienst interpretiert. Handelt es sich um einen Dienst mit weiteren angeschlossenen Interaktionspartnern, so werden die Nutzdaten für den Interaktionspartner an die zugehörige Instanz weitergeleitet. Da dieser Bereich ebenfalls asymmetrisch verschlüsselt ist, besitzt nur ein berechtigter Interaktionspartner die Möglichkeit, diesen Datenbereich zu entschlüsseln. Somit ist auch sichergestellt, dass der Dienstanbieter keine Inhalte der eigentlichen Kommunikation z.B. zwischen Nutzern von Instant-Messaging-Diensten enthält.

In Abbildung 30 fungiert der Privacy Provider als Mittler zwischen dem Benutzer und dem Dienst. Dadurch, dass der Privacy Provider die Dienstnutzung in seinem Namen ausführt, wird die Identität des Benutzers verschleiert.

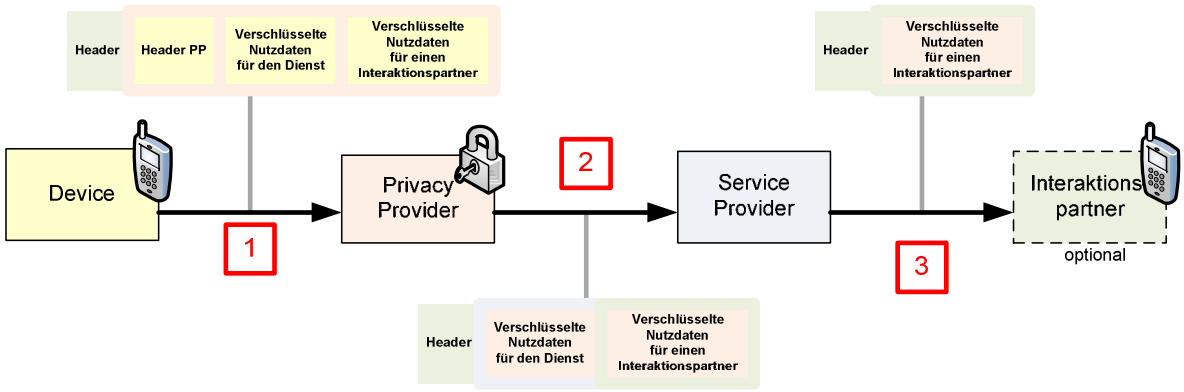


Abbildung 30 - Kommunikation bei einer anonymisierten Dienstnutzung

Bei der anonymisierten Nutzung von Diensten muss der Benutzer dem Privacy Provider den Zugriff zu allen Inhalten frei geben. Im ersten Schritt sendet der Benutzer die Nachricht zum Privacy Provider. Anders als bei einer personalisierten Nutzung kann der Privacy Provider jedoch den Inhalt aller Nachrichtenbestandteile einsehen. Der Privacy Provider interpretiert, falls notwendig, den Inhalt des „Header PP“.

Ist eine Dienstnutzung basierend auf den bestehenden Regeln erlaubt, so fragt nun der Privacy Provider die vom Benutzer geforderte Dienstleistung an. Dazu speichert er das Tupel aus Absender, Identifikation und Message ID mit seiner eigenen Identifikation, die an den Dienst gesendet wurde, in einer Tabelle ab. Dadurch kann der Privacy Provider später die Antworten dem jeweiligen Benutzer zuordnen. Damit der Dienst keinen Zugriff auf die optionalen Inhalte des Interaktionspartners erhält, werden diese Bestandteile asymmetrisch verschlüsselt. Somit ist gewährleistet, dass nur die befugten Instanzen Zugriff zu den jeweiligen Informationen erhalten.

Wenn der Dienst eine Nachricht erhält, verarbeitet er diese genauso wie bei einer personalisierten Dienstnutzung. In dem anonymisierten Fall erscheint jedoch der Privacy Provider als Dienstnutzer.

7.3 Nutzung der Architektur durch mobile Anwendungen

Dienste und Anwendungen auf mobilen Endgeräten unterscheiden sich bei dieser Architektur darin, wie viel Programmlogik auf dem jeweiligen Endgerät ausgeführt wird. Bei Diensten besitzt das Endgerät nur die Eigenschaft eines Thin Clients. Somit besteht die Aufgabe des Clients primär im Bereich der Präsentation der Ergebnisse. Bei Anwendungen befindet sich weitere Programmlogik auf dem Endgerät. Dienste werden beispielsweise eingesetzt, um Berechnungen mit dynamischen Daten aufzuwerten oder komplette Berechnungen auszulagern. Der auf dem Endgerät befindliche Client ermöglicht die Kommunikation mit den beteiligten Instanzen innerhalb der Architektur. Er kann genutzte Dienste mit Hilfe eines Webbrowsers darstellen. Zur Integration von Anwendungen besteht die Möglichkeit der Kommunikation über einen Netzwerk-Port mit dem Client auf dem Endgerät (siehe Abbildung 31).

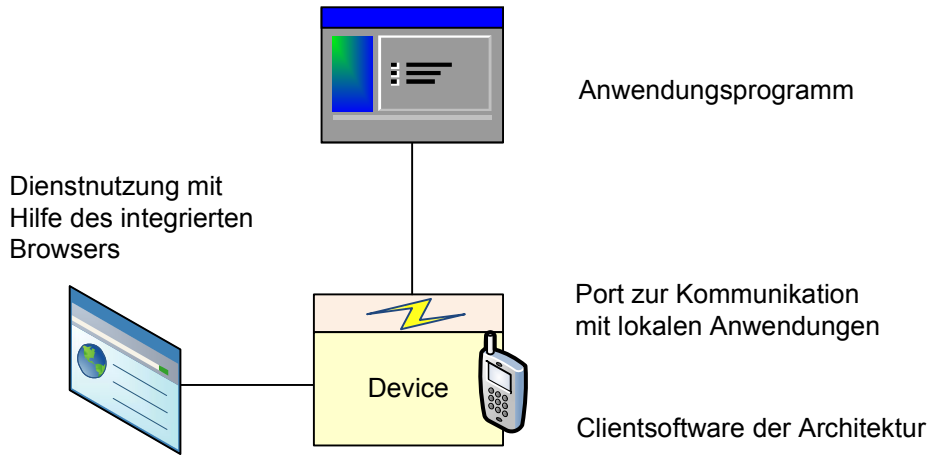


Abbildung 31 - Clientsoftware zur Nutzung von Anwendungen und Diensten

Um sicherzustellen, dass diese Schnittstelle nicht von unbefugten Anwendungen verwendet oder belauscht wird, wird die Kommunikation zusätzlich asymmetrisch verschlüsselt. Der Benutzer kann, vergleichbar mit der ersten Dienstnutzung, festlegen, welche Anwendungen Zugriff dieser Schnittstelle besitzen sollen. Unbefugte Anwendungen ist es verwehrt sich dieser Schnittstelle zu bemächtigen. Dadurch ist sichergestellt, dass das Endgerät durch seine freie Erweiterbarkeit kein mögliches Sicherheitsrisiko darstellt. Abbildung 31 zeigt die Kommunikation von Anwendungen, die sich auf dem Endgerät befinden, mit der Architektur.

7.4 Regeln / Kontextdaten

Basierend auf den Regelsätzen, die ein Benutzer beim Privacy Provider gespeichert hat, ist eine Dienstnutzung oder die Bereitstellung von Kontextdaten möglich. Da nach der Einrichtung des Benutzer-Accounts nur eine minimale Anzahl an Regeln hinterlegt ist, muss der Benutzer für die Dienste, die er verwenden möchte, Regelsätze anlegen.

Abbildung 32 zeigt die Schritte, die bei einer ersten Nutzung eines Dienstes ausgeführt werden.

Nachdem im Privacy Provider Regelsätze existieren, die eine Dienstnutzung zulassen, besteht für den Dienst die Möglichkeit, kontextbezogene Informationen abzufragen. Die Vorgänge, die bei der Bereitstellung von Kontextinformationen berücksichtigt werden, zeigt Abbildung 33.

7.4.1 Erstellen von Regelsätzen bei einer ersten Dienstnutzung

Verwendet ein Benutzer einen Dienst zum ersten Mal, so existieren noch keine aktiven Regelsätze, die eine Nutzung erlauben. Um eine Nutzung zu ermöglichen, müssen somit im ersten Schritt Regelsätze erstellt werden. Besitzt der Benutzer einen neuen Account, so verfügt er zu diesem Zeitpunkt nur über die vom Privacy Provider vorgegebenen globalen Regelsätze. Diese sind dafür zuständig, dass bei Diensten, die bestimmte Merkmale aufweisen, der Benutzer informiert wird. Diese Funktion kann beispielsweise dazu genutzt werden, den Benutzer vor kostenpflichtigen Angeboten zu warnen. Auch können Dienste, die bestimmte Mängel aufweisen, permanent blockiert werden. Beispielsweise werden Dienste blockiert, die ihre Leistung von einem Land aus anbieten, bei dem der Datenschutz nicht gewährleistet wird.

Sollte ein Dienst aufgrund der globalen Richtlinien blockiert werden, so wird der Benutzer darüber in Kenntnis gesetzt. Er kann im Einzelfall die Dienstnutzung erlauben, indem für diesen Dienst eine Ausnahmeregel festgelegt wird. Soll keine Ausnahmeregel gelten, so wird die Dienstnutzung abgebrochen. Der Vorgang wird im Datennutzungslog protokolliert und der Benutzer darüber informiert.

Im darauffolgenden Schritt wird geprüft, ob zu diesem Dienst bereits inaktive Regelsätze existieren. Inaktive Regelsätze können vorhanden sein, wenn ein Benutzer den Dienst bereits verwendet hat. Nutzt er den Dienst nur unregelmäßig oder liegt die letzte Nutzung länger zurück, so kann er die Regeln löschen oder deaktivieren. Dadurch ist sichergestellt, dass er Diensten, die er nicht regelmäßig nutzt, keine permanenten Zugriffsrechte auf sensible Informationen gestattet. Bei Bedarf können die inaktiven Regelsätze auch aktiviert werden.

Möchte er die vorhandenen inaktiven Regeln nicht verwenden oder sind keine inaktiven Regeln vorhanden, so werden die Defaultregeln des Dienstanbieters geladen. Dieser Regelsatz dient dem Benutzer als Basis. Die Anbieter sollten Defaultregelsätze definieren, die nur Kontextinformationen anfragen, die zur Diensterbringung notwendig sind. Zusätzlich sollte der Detaillierungsgrad nur die minimale Genauigkeitsstufe fordern, die zur Diensterbringung benötigt wird.

Dem Benutzer werden die ausgewählten Regelsätze (reaktivierter Regelsatz / Defaulregelsatz) angezeigt. Diese können je nach den aktuellen Erfordernissen modifiziert und den Anforderungen angepasst werden. Beispielsweise kann er die Zugriffszeiten auf seine sensiblen Daten festlegen und den Personenkreis, der Einsicht nehmen darf. Ein Außendienstmitarbeiter könnte seiner Firma erlauben, nachzufragen, wo er sich befindet und welchen Auftrag er gerade bearbeitet. Wenn die Abfragen nur während der Arbeitszeit erlaubt sind, erhöht das die Effektivität des betrieblichen Ablaufs und schützt gleichzeitig die Privatsphäre.

Akzeptiert der Benutzer die Defaultregeln oder die modifizierten Regelsätze, so werden diese vom Privacy Provider übernommen. Dazu wird ein Eintrag in der Service-Datenbank erstellt. Diese Datenbank beinhaltet die Dienste, zu denen Regeln existieren. Zu diesem Eintrag existiert auch ein Verweis zu den eigentlichen Regeln, die sich in dem Regel- Repository befinden. Diese Regeln werden im darauffolgenden Schritt eingetragen.

Die so durchgeführten Änderungen werden im Datennutzungslog protokolliert. Der Benutzer wird anschließend über die Änderungen informiert.

Nach diesen Vorarbeiten kann der Dienst genutzt werden.

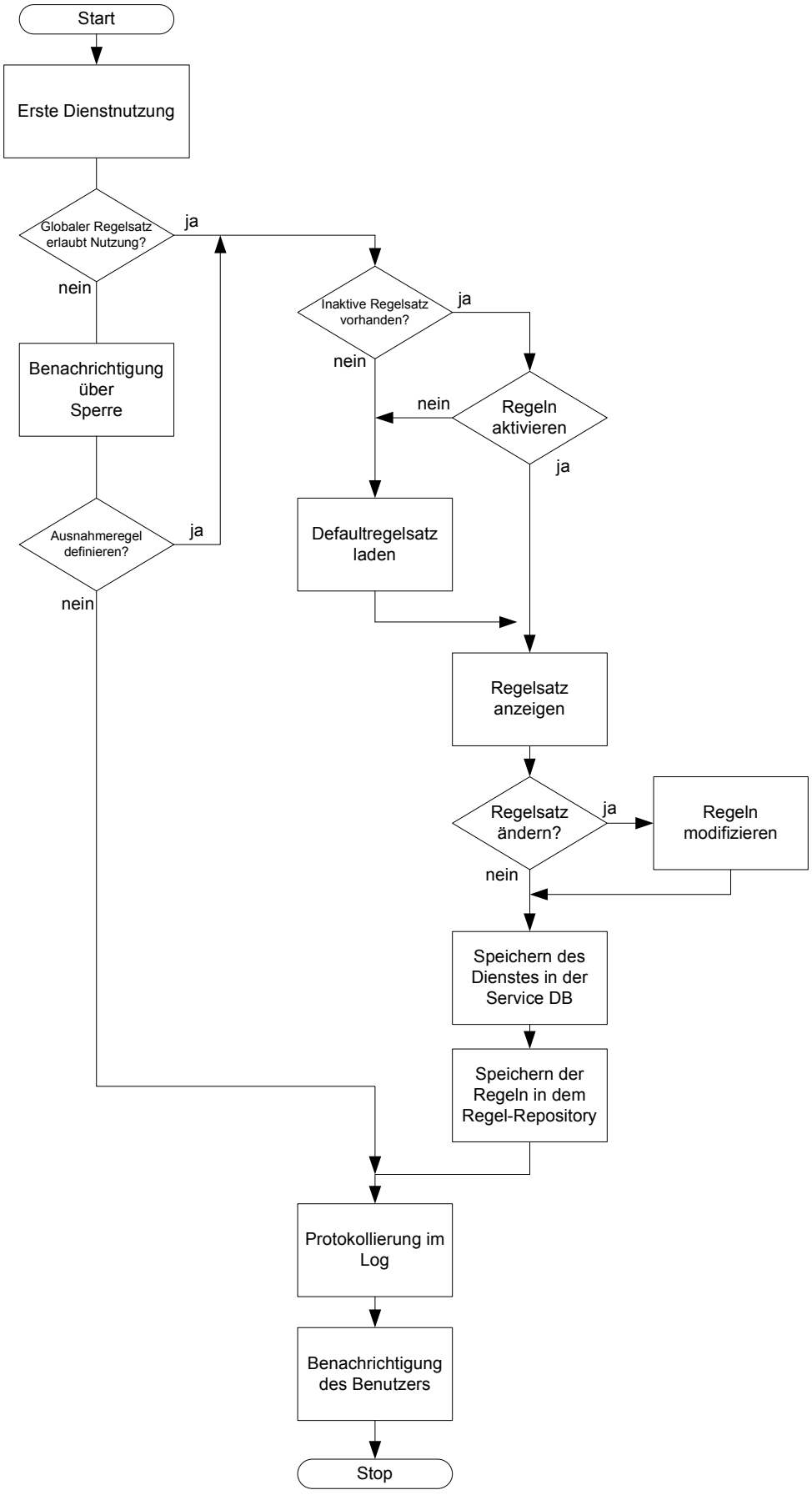


Abbildung 32 - Erste Nutzung eines Dienstes

7.4.2 Überprüfung der Regelsätze zur Bereitstellung von Kontextinformationen

Ist eine Dienstnutzung basierend auf den Regelsätzen des Benutzers möglich, so kann der Dienst für die Leistungserbringung Kontextdaten anfordern. In diesem Fall enthält das Nachrichtenformat eine Anfrage an den Privacy Provider. Abbildung 33 zeigt die Überprüfung der Anfrage beim Privacy Provider, bevor dieser Kontextinformationen an den Dienstleister sendet.

Fragt ein Dienst Kontextinformationen beim Privacy Provider an, so prüft dieser, ob der Dienst dazu die Berechtigung besitzt. Diese Prüfung beginnt bei der Service-Datenbank. Alle Dienste, die vom Benutzer eine Erlaubnis erhalten haben, besitzen einen Eintrag in der Service-Datenbank mit einem Verweis auf die Regelsätze, die sich in dem Regel-Repository befinden. Existiert in der Service-Datenbank kein Eintrag, so handelt es sich um eine unberechtigte Anfrage. In diesem Fall erhält der Dienstanbieter keinen Zugang zu den Informationen. Entsprechend den globalen Regelsätzen wird der Benutzer über diesen Vorgang informiert. Der Dienst erhält eine Fehlermeldung, dass er nicht befugt ist, die angeforderten Daten zu erhalten. Die Anfrage wird daraufhin im Datennutzungslog gespeichert. Der Benutzer besitzt hier die Möglichkeit, bei Störungen der Dienstleistungserbringung, mögliche Fehlerquellen aufzufinden.

Besitzt der Dienst hingegen einen Eintrag in der Service-Datenbank, so werden die dazugehörigen Regelsätze aus dem Regel-Repository abgefragt. Anhand dieser Regeln wird entschieden, ob ein Zugriff auf die geforderten Daten zugelassen wird. Ist dies nicht möglich, so erhält der Dienst eine Fehlermeldung und der Benutzer wird entsprechend seinen Anordnungen über diesen Vorgang informiert. Der Zugriff wird protokolliert.

Erlauben die Regelsätze den Zugriff auf die Kontextinformationen, wird geprüft, ob der Benutzer einen Benachrichtungsregelsatz eingerichtet hat. Dieser Regelsatz kann auf zwei Arten konfiguriert werden. Im ersten Fall wird der Benutzer darüber informiert, dass der Dienst bestimmte Informationen angefordert hat. Im zweiten Fall kann er festlegen, dass der Dienst diese Informationen erst erhält, wenn er selbst manuell die Freigabe gibt. In dem Fall, in dem der Benutzer keinen Zugriff auf die Daten erlaubt, wird der Dienst ebenfalls informiert. Eine Benachrichtigung erfolgt auch, wenn die Regelsätze für den Zugriff nicht ausreichen. Die Fehlermeldung gibt die Ursache für die verweigerte Datenfreigabe an.

Ist keine manuelle Freigabe erforderlich oder wird diese vom Benutzer gewährt, so werden nun die angeforderten Kontextinformationen dem Dienst bereitgestellt. In diesem Schritt werden die Kontextdaten so aufbereitet, dass der Dienst den vom Benutzer freigegeben Detaillierungsgrad erhält. Dazu wird geprüft, ob der Dienst in personalisierter oder anonymisierter Form genutzt wird. Handelt es sich um eine anonymisierte Nutzung, so ist es dem Dienst nicht möglich, die Person zu ermitteln, die ihn nutzt.

Im Datennutzungslog wird abschließend vermerkt, wann welchem Dienste Informationen bereitgestellt worden sind.

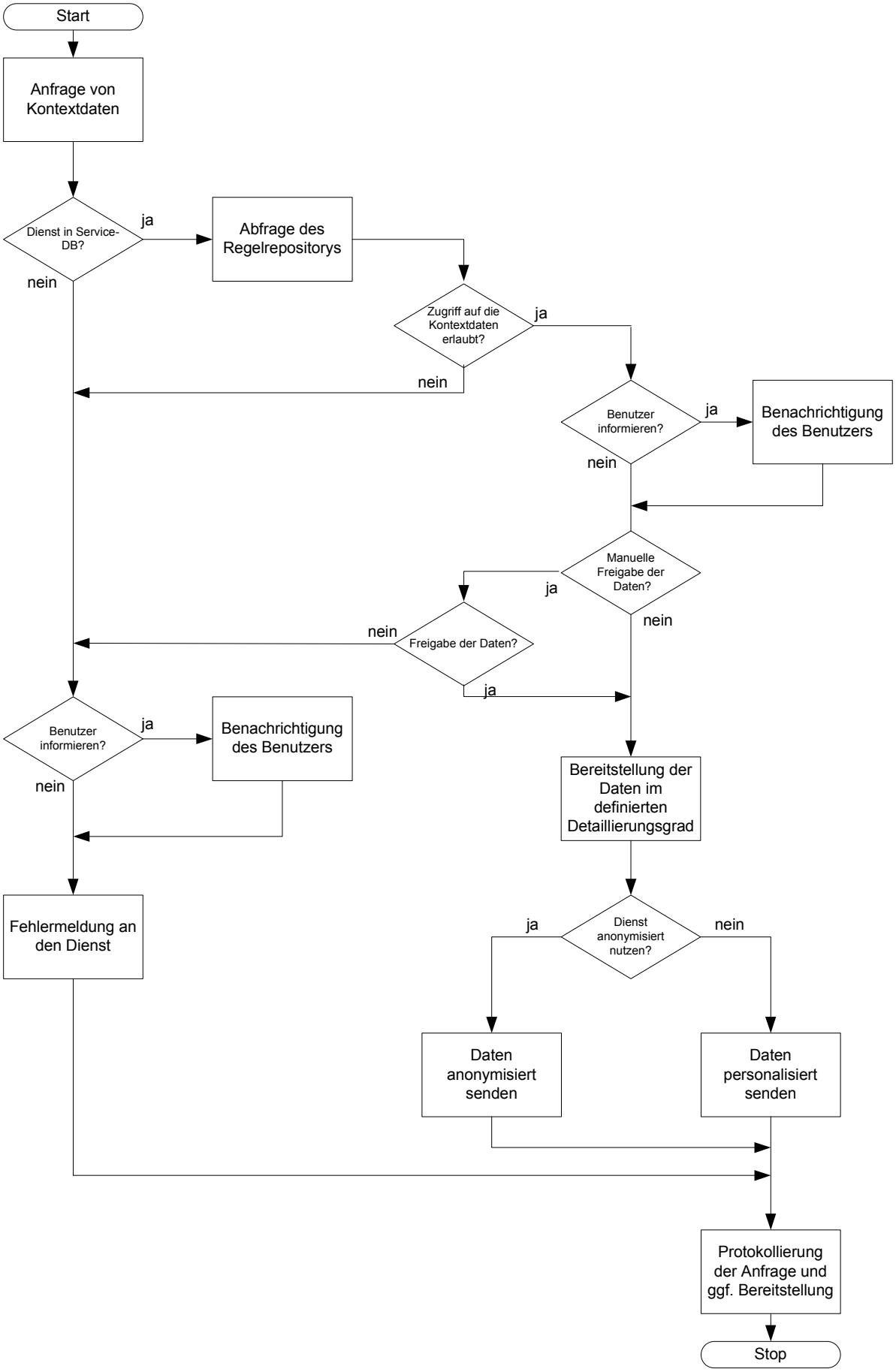


Abbildung 33 - Bereitstellung von Kontextinformationen

7.5 Bezahlung von Dienstleistungen

Da mit Hilfe dieser Architektur auch kommerzielle Dienstleistungen angeboten werden, müssen auch Zahlungsanweisungen übermittelt werden. Abbildung 34 zeigt das notwendige Vorgehen, um den Dienstanbietern in anonymisierter Form Zahlungen vom Benutzer zu überweisen. Der Privacy Provider fungiert in diesem Fall als Mittelsmann. In diesem Rahmen besitzt er die folgenden Aufgaben:

- Berechtigung und Gültigkeit der Zahlungsaufforderung prüfen
- Liquidität des Benutzers prüfen
- Zahlungstransfer vom Benutzer zum Privacy Provider vornehmen
- Zahlungstransfer vom Privacy Provider zum Service Provider vornehmen

Die Architektur ermöglicht es nicht nur, Zahlungsanforderungen zu regeln, sondern auch Gutschriften vom Dienstanbieter an den Nutzer zu übermitteln. Ein solcher Fall tritt ein, wenn der Benutzer werbefinanzierte Dienste in Anspruch nimmt. Es könnte sich um einen Werbedienst handeln, der an anonymisierten Benutzerdaten Interesse hat. Benutzer, die diesen Dienst verwenden, erhalten dafür eine Gutschrift.

In dem folgenden Fall nimmt ein Benutzer einen kostenpflichtigen Dienst in Anspruch. Dieser wird stellvertretend durch den Privacy Provider nach Prüfung der Regelsätze aufgerufen. Vor der Diensterbringung fordert der Service Provider die Gebühren für den kostenpflichtigen Dienst. Dazu sendet er eine Zahlungsaufforderung. Diese Aufforderung an den Privacy Provider schreibt der Service Provider im Nachrichtenformat in den Header für den Privacy Provider. Der Privacy Provider ist Mittelsmann zwischen dem Dienst und dem Benutzer und überprüft zunächst, ob der Benutzer über ausreichende Liquidität verfügt. In der Benutzerverwaltung ist vermerkt, welcher Clearing Provider für den jeweiligen Benutzer zuständig ist. Bei diesem fragt er an, ob eine Zahlung in der geforderten Höhe des Betrages möglich ist. Der Clearing Provider gibt dem Privacy Provider diese Information. Bevor er die Antwort interpretiert, überprüft der Privacy Provider, ob das Zertifikat des Clearing Providers gültig ist. Damit schützt er sich vor Man-in-the-middle-Attacken, die vortäuschen, dass ausreichendes Guthaben vorhanden ist.

Besitzt der Benutzer kein ausreichendes Kapital oder ist das Zertifikat nicht gültig, so wird die Bearbeitung der Zahlung abgebrochen. In diesem Fall erhält der Dienst eine Fehlermeldung und der Benutzer wird über den Abbruch der Dienstleistung unter Angabe von Gründen informiert. Der Vorgang wird mit genauer Fehlerangabe im Datennutzungslog protokolliert.
Der Service Provider beendet mit diesem Schritt die geforderte Dienstleistung.

Weist der Clearing Provider die Liquidität dem Benutzer nach, so bucht der Privacy Provider den geforderten Betrag vom Konto des Benutzers ab. Im nächsten Schritt überweist er diesen Geldbetrag in seinem Namen an den Dienstanbieter. Wenn dieser den Geldbetrag erhält, stellt er dem Benutzer die erforderte Dienstleistung zur Verfügung. Der Privacy Provider protokolliert die Dienstnutzung und die damit entstandenen Kosten und leitet die Kommunikationspakete an den Client weiter, der somit den Dienst dem Benutzer bereitstellt.

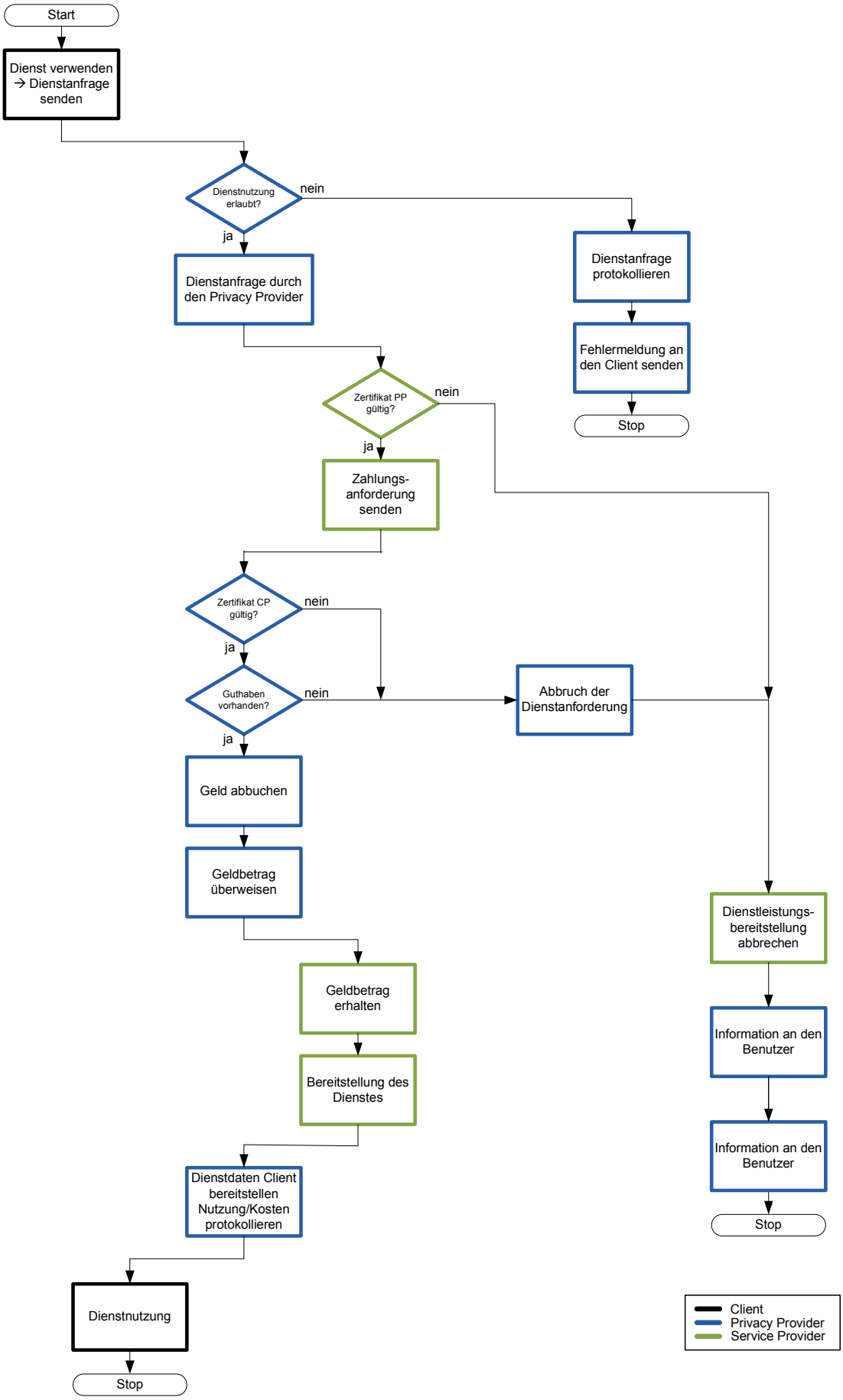


Abbildung 34 - Bezahlung von Dienstleistungen

7.6 Schnittstellen der Instanzen

Die Instanzen der Architektur besitzen standardisierte Schnittstellen, die von den beteiligten Kommunikationspartnern verwendet werden. Der folgende Abschnitt beschreibt die grundlegenden Schnittstellen, die bis auf die Client-Schnittstelle als Web-Service-Schnittstellen realisiert worden sind.

Client	
Push-Mechanismus	Der Client kann bei Bedarf Informationen abrufen oder Push-Dienste verwenden. In diesem Fall sendet der Dienst die Information, sobald er darüber verfügt. Dies erspart dem Client ein regelmäßiges Abfragen. Um den Client informieren zu können, besitzt er eine Schnittstelle, die den Push-Mechanismus aktiviert. Es handelt sich dabei um einen Netzwerkport, mit dem durchgehend eine Verbindung mit dem Privacy Provider besteht. Der Privacy Provider sendet an den Client über diese Verbindung nur dann eine Information, wenn der Client beim Privacy Provider Informationen abfragt. Aufgrund der wechselnden Anbindung des Clients, wird diese Verbindung vom ihm aufgebaut und überwacht. Falls ein Verbindungsausfall oder Netzwerkwechsel eingetreten ist, so wird diese Verbindung erneut von ihm aufgebaut.

Privacy Provider	
Benutzeraccount verwalten	
Angaben ändern	Die vom Benutzer beim Anmeldevorgang hinterlegten Informationen können bei einer späteren Nutzung aktualisiert werden. Über diese Schnittstelle wird entschieden, welche Informationen verändert werden. Der Benutzer hat Zugang zu allen veränderbaren Feldern. Veränderungen in diesem Bereich werden protokolliert.
Gerät hinzufügen	Der Benutzer kann über seinen Account mehr als ein Gerät verwenden. Dazu hat er nach der Anmeldung eine Anzahl an TANs erhalten. Zu einem späteren Zeitpunkt kann er weitere TANs beantragen. Mit einer TAN können weitere Endgeräte einem Account hinzugefügt werden. Das Endgerät übermittelt in diesem Zusammenhang den selbst erstellten öffentlichen Schlüssel mit einer gültigen TAN an den Privacy Provider. Dieser fungiert als Registierungsstelle und lässt vom Trust Center ein Zertifikat für dieses Endgerät erstellen. Die notwendigen Informationen zur Erstellung entnimmt er den Daten des Benutzeraccounts.

Gerät entfernen	Wird ein Gerät nicht mehr weiter verwendet, so kann der Benutzer über diese Schnittstelle ein bestehendes Zertifikat als ungültig erklären lassen.
Log anzeigen	Über diese Schnittstelle kann der Benutzer auf das Datennutzungslog des Privacy Providers zugreifen. Mit Hilfe weiterer Attribute kann die Menge der Informationen beschränkt werden.
<u>Regeln</u> Service DB abfragen	Diese Schnittstelle listet alle Dienste auf, die in der Service-Datenbank eingetragen sind.
Eintrag aus der Service DB entfernen	Wird ein Dienst nicht weiter verwendet, so wird der Eintrag aus der Service-Datenbank entfernt. Die damit zusammenhängenden hinterlegten Regeln werden ebenfalls gelöscht.
Service deaktivieren	Besteht die Möglichkeit, dass ein Dienst erst zu einem späteren Zeitpunkt erneut verwendet wird, so kann er auch deaktiviert werden. Eine Dienstnutzung ist somit bis zur erneuten Aktivierung nicht möglich.
Regeln abfragen	Zu jedem Dienst aus der Service-Datenbank sind Regelsätze hinterlegt. Die Auflistung der hinterlegten Regelsätze kann der Benutzer mit Hilfe dieser Schnittstelle abfragen.
Regeln eintragen	Ein bestehender Regelsatz kann über diese Funktion erweitert werden.
Regeln ändern	Muss ein bestehender Regelsatz angepasst werden, so kann er über diese Schnittstelle modifiziert werden.
Regeln löschen	Möchte ein Benutzer Bestandteile eines Regelsatzes entfernen, so kann er sie über diese Schnittstelle löschen.
<u>Kontextdaten</u> Kontextdaten abfragen	Die Kontextinformationen eines Benutzers liegen in unterschiedlichen Detaillierungsgraden im Privacy Provider vor. Die Detaillierungsgrade werden durch eine Logik oder durch eine Umrechnung bereitgestellt. Diese Schnittstelle erlaubt es, Kontextdaten abzufragen. Als Wert dieser Abfrage wird der Detaillierungsgrad hinzugefügt. Fehlt dieser Wert, so wird immer von der genausten Information ausgegangen.
Kontextdaten eintragen bzw. ändern.	Kontextinformationen ändern sich je nach Informationsart in regelmäßigen Abständen. Informationsbereiche, die innerhalb eines kurzen Zeitbereichs Änderungen unterworfen sind, werden automatisch ermittelt. Bereiche, die sich nur unregelmäßig verändern, können vom Benutzer modifiziert werden. Diese Schnittstelle ermöglicht es, die hinterlegten Informationen zu

	verändern. Zu Beginn wird bereits eine große Anzahl von Feldern zur Verfügung gestellt, die von Diensten und Anwendungen adressiert werden kann. Da nicht alle Felder ausgefüllt werden müssen, sind diese von Beginn an leer. Bei der Änderung der Kontextdaten bietet diese Schnittstelle auch das Attribut des Detaillierungsgrades. Dadurch können Informationen in unterschiedlichen Komplexitätsgraden hinterlegt werden.
Datenbankfelder hinzufügen	Die von Beginn an vom Privacy Provider bereitgestellten Felder bieten bereits vielen Anwendungen eine Basis für Kontextinformationen an. Da beispielsweise branchenspezifische Anwendungen zusätzliche Kontextinformationen für den Betrieb benötigen, können weitere Felder in der Datenbank hinterlegt werden. Diese Änderung wird in diesem Fall nur im Datensatz des jeweiligen Benutzers ausgeführt. Dadurch unterstützt das System Spartenanwendungen und bietet ausreichende Zukunftssicherheit.
<u>Sonstiges</u> Regelsätze exportieren	Der Benutzer kann den Privacy Provider frei wählen. Möchte er diesen wechseln, so kann er die bis dahin definierten Regelsätze über diese Schnittstelle exportieren. Er erhält als Ergebnis eine signierte XML-Datei. Diese kann er seinem neuen Privacy Provider übergeben. Dadurch ist sichergestellt, dass er nicht erneut alle Regelsätze definieren muss.
Regelsätze importieren	Die von einem anderen Privacy Provider exportierten Regelsätze kann der Benutzer mit Hilfe dieser Schnittstelle importieren.
Service-Datenbank exportieren	Die vom Benutzer verwendeten Dienste werden in der Service-Datenbank gespeichert. Bei einem Wechsel des Privacy Providers können sie mit Hilfe dieser Schnittstelle exportiert werden.
Service-Datenbank importieren	Der Benutzer kann die zuvor konfigurierten Einstellungen der Service-Datenbank über diese Schnittstelle importieren.
Kontextbezogene Daten exportieren	Der Benutzer hat bei der Nutzung der Architektur personen- und kontextbezogene Daten in der Datenbank des Privacy Providers gespeichert. Sie werden über diese Schnittstelle exportiert.
Kontextbezogene Daten importieren	Die personen- und kontextbezogenen Daten können über diese Schnittstelle dem neuen Privacy Provider bereitgestellt werden.
Netzwerkzugang wechseln	Der Benutzer hat die Möglichkeit, während der Nutzung eines Dienstes das verwendete Netzwerk zu wechseln. Dadurch stehen ihm leistungsfähige und kostengünstigere Netze offen. Über diese Schnittstelle informiert der Benutzer den Privacy Provider über einen ausgeführten Netzwechsel.

Location Provider	
	Verwendet der Benutzer Anwendungen, die Positionsinformationen benötigten, so übermittelt der Location Provider entweder durchgehend Positionen an den zuständigen Privacy Provider oder er stellt sie auf Anfrage zur Verfügung. Die folgenden Schnittstellen stellt der Location Provider bereit.
Position abfragen	Der Privacy Provider kann die Position eines Benutzers abfragen. Er erhält die Ortsangabe entweder im höchsten Genauigkeitsgrad oder in verschiedenen Abstufungen. (Zum Beispiel: Straße mit Hausnummer, Straße, Stadtteil, Ort) Der Location Provider stützt sich bei seinen Angaben auf eine Datenbank.
Position transformieren	Diese speziellen Datenbanken können von Anwendungen ebenfalls verwendet werden. Zusätzlich können über diese Schnittstelle Positionsinformationen in unterschiedliche kartesische Formate umgewandelt werden. Dies ist beispielsweise bei Diensten notwendig, die auf eine Positionsangabe im nationalen Format bestehen.
Trigger bei definierter Positionsänderung	Über diese Schnittstelle können Bereiche definiert werden, bei denen eine Positionsbenachrichtigung erfolgen soll. Eine derartige Funktion kann beispielsweise bei ortsbezogenen Anwendungen benötigt werden, die nur für ein begrenztes Gebiet zuständig sind. Der Dienst muss nicht über die Position eines Benutzers informiert werden, wenn sich dieser außerhalb des Gebietes befindet, in dem der Dienst angeboten wird. Befindet er sich innerhalb des Gebietes, wird der Dienst darüber in Kenntnis gesetzt.

Clearing Provider	
Liquidität abfragen	Diese Schnittstelle ermöglicht es einem Privacy Provider zu überprüfen, ob für eine Dienstleistung eine ausreichende Liquidität existiert. Dazu nennt er den notwendigen Betrag und erhält vom Dienst die Information, ob diese Zahlung möglich ist. Das eigentliche Guthaben wird dem Privacy Provider nicht genannt.
Guthaben abfragen	Benutzer hingegen besitzen die Möglichkeit, ihr aktuelles Guthaben abzufragen.
Transaktion ausführen	Zur Nutzung von kostenpflichtigen Diensten müssen Geldbeträge zwischen Benutzer und Privacy Provider sowie zwischen Privacy Provider und Service Provider transferiert werden. Diese Transaktionen können von berechtigten Instanzen ausgeführt werden. Der Privacy Provider hat die Erlaubnis, sofern der Benutzer ihm diese gegeben hat, Beträge von dem dazugehörigen Konto abzubuchen.
Transaktionen abfragen	Eine Übersicht der so getätigten Transaktionen kann der Benutzer über diese Schnittstelle abrufen. Er kann als Suchbegriff z.B. einen Zeitraum verwenden, um die Treffermenge zu reduzieren.

Service Provider	
Defaultregel abfragen	Bei jedem Dienst kann über diese Schnittstelle der Defaultregelsatz abgefragt werden. Es handelt sich hierbei um eine signierte XML-Datei. Diese wird vom Privacy Provider als Regelsatzvorschlag interpretiert.
Dienstspezifische Schnittstellen	Abhängig von der bereitgestellten Dienstleistung stehen dem Benutzer weitere Schnittstellen zur Verfügung. Anwendungen können über diese Schnittstellen Dienstleistungsbestandteile abfragen, die sie auf dem Endgerät weiter bearbeiten. Der Service Provider bietet sonst seine Dienstleistung in Form eines Webservers an. Dies hat den Vorteil, dass Darstellung und Interaktion bereits standardisiert sind.

Service Register	
	Bei einem Service Register handelt es sich um eine besondere Form einer Dienstleistung. Daher besitzt ein Service Provider folgende Schnittstellen:
Dienstabfrage	Diese Schnittstelle erlaubt die Suche nach spezifischen Diensten. Die Treffermenge lässt sich durch geeignete Kategorien, kontextbezogene Daten (Position des Benutzers, Interesse, Alter, Situation, …)oder eine Kombination aus beiden einschränken.
Dienst eintragen	Da Dienste in Form von Service Providern von vielen Personen oder Unternehmen angeboten werden, kommen in kurzen Abständen neue Dienste hinzu. Alle Dienste, die das Zertifikat Service Provider erhalten, können mit Hilfe dieser Schnittstelle ihren Dienst der Datenbank des Service Registers hinzufügen.
Dienst löschen	Werden bestimmte Dienste nicht mehr angeboten oder verändern sich die Inhalte, so muss der Dienst aus der Datenbank entfernt werden. Ein Dienst kann nur von der gleichen Person entfernt werden, die diesen auch eingetragen hat.

8 Weiteres Vorgehen

Diese Arbeit beschreibt das Grobkonzept einer Architektur zum Schutz der Privatsphäre im mobilen Umfeld. Im nächsten Schritt werden die beteiligten Komponenten im Detail für die prototypische Realisierung spezifiziert. Basierend auf dieser Spezifizierung wird eine erste Stufe der prototypischen Realisierung angestrebt. Ein Prototyp der Gesamtarchitektur und Prototypen der beteiligten Dienste stehen zukünftig zur Verfügung. Mit Hilfe von exemplarischen Anwendungen werden die neu geschaffenen Rahmenbedingungen evaluiert. Zur Evaluation werden Kommunikationsnachrichten als Samples verwendet, um zu prüfen, ob die definierten Anforderungen an die Architektur eine ausreichende Grundlage bieten, um im mobilen Umfeld Dienste mit sensiblen kontextbezogenen Daten anbieten zu können. Hierbei wird genau analysiert, ob zwischen den beteiligten Instanzen nur die minimalen vom Benutzer freigegeben Informationen ausgetauscht werden. Die im Rahmen dieser Evaluation gewonnenen Ergebnisse werden in die Spezifikation integriert. Die prototypische Implementierung nutzt den Forschungsansatz des Design Researchs. Die aus der Evaluierung des Prototyps gewonnenen Ergebnisse fließen im nächsten Schritt in die Spezifikation und Implementation der Architektur ein.

Als exemplarische Anwendung wird der im Rahmen der Laborforschung entwickelte mGeoWiki-Prototyp [ELZ07, SLZ08] modifiziert, um basierend auf der implementierten Architektur zu operieren. Die Anwendung steht exemplarisch für kontextbezogene mobile Dienstleistungen. Sie bietet in diesem Zusammenhang die Abfrage von ortsbezogenen Informationen und eine personalisierte kontextbezogene Informationssuche.

Zur Prüfung der Rahmenbedingungen beim Einsatz oder der Nutzung von Diensten mit sensiblen Informationen befinden sich zum jetzigen Zeitpunkt[9] zwei weitere Projekte in Bearbeitung, deren Ergebnisse ebenfalls bei der Weiterentwicklung der Architektur berücksichtigt werden. Das erste Projekt betrachtet die verteilten Datenspuren, die ein Benutzer hinterlässt, wenn er Objekte mit RFID-Tags verwendet. Da diese Technologie, ebenfalls wie ortsbezogene Dienste, für den Benutzer eher im Verborgenen operieren, ist dem Benutzer das existierende Gefahrenpotential oft nicht bewusst. Im Rahmen eines Feldversuches wird in diesem Projekt einer größeren Anzahl von Probanten (geplant ca. 800 Probanten) eine Karte mit einem RFID-Tag überreicht, die sie bei einer Veranstaltung einsetzen. Anhand der so gesammelten Daten sollen im darauffolgenden Schritt Aussagen über Interesse, Intension und soziales Umfeld abgeleitet werden. Da derartige Informationen im Rahmen der Nutzung von ortsbezogenen Diensten ebenfalls anfallen, wird geprüft, ob die Ergebnisse dieses Projektes zur Analyse des Gefahrenpotentials im Rahmen dieser Architektur genutzt werden können. Die so gewonnenen Ergebnisse werden verwendet, um die Sicherheitsmechanismen der Architektur zu optimieren. Ein besonderer Schwerpunkt wird auf die Betrachtung der automatischen Interpretation der Daten und der damit möglichen Fehlinterpretation gelegt.

Ein weiteres laufendes und in Kürze abschließendes Projekt mit dem Arbeitstitel „PIP – Push Information Plattform“, wird bei der zukünftigen Präzisierung der Anforderungen der Architektur berücksichtigt. Dieses Projekt realisiert eine mobile Socialing-Plattform, die neben den Funktionen eines Friendfinders, zusätzlich orts- und kontextbezogene Werbung den Benutzern zur Finanzierung der Dienstnutzung bereitstellt. Die so zur Verfügung gestellten Informationen werden dem mobilen Endgerät per Push-Mechanismus gesendet. Die

[9] Stand: Mai 2008

zentrale Fragestellung dieses Projektes ist es, eine Plattform zu schaffen, die einen Push-Dienst aufbaut, der bei der Nutzung des Friendfinder-Dienstes und der Nutzung von orts- und kontextbezogener Werbung für den Benutzer zu keinem Sicherheitsrisiko führt. Der Benutzer hat bei diesem Dienst den Überblick, wem er welche Daten zur Verfügung stellt.

Im weiteren Forschungsprozess werden die wirtschaftlichen Aspekte von mobilen Diensten besonders betrachtet. Die so gewonnenen Erkenntnisse dienen der Präzisierung der Anfordeurngen an die Architektur. Sie fließen ebenfalls in den darauffolgenden Evaluationsprozess ein.

9 Literaturverzeichnis

[ATK00] ARToolKit Homepage, www.hitl.washington.edu/artoolkit/ [Zugriff am 10.08.2007]

[BGS07] Bizer, J.; Grimm, R., et al.: SOAinVO - Chancen und Risiken von Service-orientierten Architekturen in Virtuellen Organisationen, https://www.datenschutzzentrum.de/soa/SOAinVO-Analyse.pdf, [Zugriff am 14.03.2008]

[Bro06] Brodersen, B.: Probelauf für Fußgänger-Navigation per WLAN, http://www.teltarif.de/arch/2006/kw51/s24252.html, [Zugriff am 20.12.2006]

[BSP07] Blue Sky Positioning: Homepage Blue Sky Positioning - Products, http://www.blueskypositioning.com/products.htm, [Zugriff am 04.05.2007]

[CE05] Eckert, C.: IT-Sicherheit. München: Oldenbourg Verlag, 2005.

[CFS03] Chokhani, S.; Ford, W., et al.: RFC 2647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, http://www.ietf.org/rfc/rfc3647.txt, [Zugriff am 26.03.2008]

[De99] Dey, A. K. Abowd, G. D.: "Towards a better understanding of context and context-awareness," Georgie Institute of Technology, GVU Technical Report GIT-GVU-99-22 1999.

[ELZ07] Ehrenstein, M.; Lange, T., et al.: mGeoWiki - Ortsbezogenes Mobiles Wiki. Arbeitsbericht, Universität Koblenz-Landau, Koblenz, 2007.

[EuK07] Europäische Kommision: Generaldirektion Energie und Verkehr: GALILEO: Europäisches Satellitennavigationssystem, http://ec.europa.eu/dgs/energy_transport/galileo/index_de.htm, [Zugriff am 16.08.2007]

[EUP02] Europäischen Parlament: Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0051:0077:DE:PDF, [Zugriff am 20.04.2008]

[FCC05] FCC: FCC Amended Report to Contress on the Deployment of E-911 Phase II Services by Tier III Service Providers, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-257964A1.pdf, [Zugriff am 20.04.2008]

[Ger07] Gerber, T.: Russische Regierung unterstützt weiteren Ausbau des Navigationssystems GLONASS, http://www.heise.de/newsticker/meldung/print/93482, [Zugriff am 16.08.2007]

[Ha05] Haas, J. d.: Breitenkreisen und Längenkreisen http://www.explorermagazin.de/gps/gpsbas1.jpg, [Zugriff am 26.03.2008]

[Ho07a] Horn, C.: SIM-Karte mit eingebautem GPS-Empfänger, http://www.teltarif.de/arch/2007/kw18/s25834.html, [Zugriff am 02.05.2007]

[Ho07b] Horn, C.: Günstigere GPS-Lösung für Mobiltelefone, http://www.teltarif.de/arch/2007/kw33/s26859.html, [Zugriff am 14.08.2007]

[Ja07] Jazajeri, P.: Geo Information System for mobile value-added services. Diplomarbeit, Universität Koblenz-Landau, Koblenz, 2007.

[KS05] Krumm, J. Shafer, S.: Data Store Issues for Location-Based Services, http://research.microsoft.com/~jckrumm/Publications%202005/data%20store%20for%20lbs%20final.pdf, [Zugriff am 26.03.2008]

[Kü05] Küpper, A.: Location-based services : fundamentals and operation. Chichester, England ; Hoboken, NJ: John Wiley, 2005.

[LK95] Kleinrock, L.: Nomadic Computing and Communications, http://www.nap.edu/html/whitepapers/ch-40.html, [Zugriff am 29.05.2008]

[ME05] MECOMO: Preisliste SMS-MMS-LBS Deutschland, http://www.mecomo.com/web/mob_serv/Preisliste_SMS_MMS_LBS_050402.pdf, [Zugriff am 02.02.2007]

[Mey07] Meyer, C.: Galileo-Testbetrieb startet http://www.heise.de/newsticker/meldung/83074, [Zugriff am 01.01.2007]

[o207] o2: Competence Partner, http://www.o2online.de/o2/business/loesungen/grossmittel/produkte/wholesale/partner/partner-link-art.html, [Zugriff am 23.03.2007]

[PCB00] Priyantha, N. B.; Chakraborty, A., et al.: "The Cricket Location-Support System," in *6. Annual International Conference on Mobile Computing and Networking*, Boston, 2000.

[PFS02] Housley, R.; Polk, W., et al.: RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, http://www.ietf.org/rfc/rfc3280.txt, [Zugriff am 31.03.2008]

[RIT00] Royal Institute of Technology: WIPS Technical Documentation, http://2g1319.ssvl.kth.se/2000/group12/technical.html, [Zugriff am 17.08.2006]

[Ro05] Roth, J.: Mobile Computing Grundlagen, Technik, Konzepte. 2., aktualisierte Aufl. ed. Heidelberg: dpunkt.verlag, 2005.

[Sch06] Schulzrinne, H.: RFC 4676 - Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information, http://www.ietf.org/rfc/rfc4676.txt, [Zugriff am 30.03.2008]

[SHW07] Skyhook Wireless: Homepage Skyhook Wireless, http://www.skyhookwireless.com/, [Zugriff am 22.03.2007]

[SLZ08] Stein, S.; Lange, T., et al.: "mGeoWiki," in *Proceedings der 3. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2008) - MKWI 2008*, München, 2008.

[SP02] Purao, S.: Design Research in the Technology of Information Systems: Truth or Dare, http://iris.nyit.edu/~kkhoo/Spring2008/Topics/DS/000DesignSc_TechISResearch-2002.pdf, [Zugriff am 26.03.2007]

[TVM03] Tsalgatidou, A.; Veijalainen, J., et al.: *Mobile E-Commerce and Location-Based Services:Technology and Requirements.* 2003.

[TYH08] trackyourhandy, http://www.trackyourhandy.de, [Zugriff am 17.04.2008]

[Va06] Valve Developer Community: QAngle, http://developer.valvesoftware.com/wiki/QAngle, [Zugriff am 16.08.2007]

[VK06] Vaishnavi, V. Kuechler, B.: Design Research in Information Systems, http://www.isworld.org/Researchdesign/drisISworld.htm, [Zugriff am 27.03.2007]

[WHF92] Want, R.; Hopper, A., et al.: *The Active Badge Location System. ACM Transactions on Information Systems,* vol. 10, pp. 91-102, 1992.

[Wi05] Winter, M.-A.: Ortung: Verbessertes GPS für Handynutzer, http://www.teltarif.de/arch/2005/kw16/s16847.html, [Zugriff am 04.05.2007]

[Wil07] Wilkens, A.: Galileo will zur weltweiten Rettungssuche beitragen, http://www.heise.de/newsticker/meldung/print/94186, [Zugriff am 10.08.2007]

[WJH97] Ward, A.; Jones, A., et al.: *A New Location Technique for the Active Office. IEEE Personal Communications,* vol. 4, pp. 42-47, 1997.

Bisher erschienen

Arbeitsberichte aus dem Fachbereich Informatik

(http://www.uni-koblenz.de/fb4/publikationen/arbeitsberichte)

Stefan Stein, Entwicklung einer Architektur für komplexe kontextbezogene Dienste im mobilen Umfeld, Arbeitsberichte aus dem Fachbereich Informatik 7/2008

Matthias Bohnen, Lina Brühl, Sebastian Bzdak, RoboCup 2008 Mixed Reality League Team Description, Arbeitsberichte aus dem Fachbereich Informatik 6/2008

Bernhard Beckert, Reiner Hähnle, Tests and Proofs: Papers Presented at the Second International Conference, TAP 2008, Prato, Italy, April 2008, Arbeitsberichte aus dem Fachbereich Informatik 5/2008

Klaas Dellschaft, Steffen Staab, Unterstützung und Dokumentation kollaborativer Entwurfs- und Entscheidungsprozesse, Arbeitsberichte aus dem Fachbereich Informatik 4/2008

Rüdiger Grimm: IT-Sicherheitsmodelle, Arbeitsberichte aus dem Fachbereich Informatik 3/2008

Rüdiger Grimm, Helge Hundacker, Anastasia Meletiadou: Anwendungsbeispiele für Kryptographie, Arbeitsberichte aus dem Fachbereich Informatik 2/2008

Markus Maron, Kevin Read, Michael Schulze: CAMPUS NEWS – Artificial Intelligence Methods Combined for an Intelligent Information Network, Arbeitsberichte aus dem Fachbereich Informatik 1/2008

Lutz Priese,Frank Schmitt, Patrick Sturm, Haojun Wang: BMBF-Verbundprojekt 3D-RETISEG Abschlussbericht des Labors Bilderkennen der Universität Koblenz-Landau, Arbeitsberichte aus dem Fachbereich Informatik 26/2007

Stephan Philippi, Alexander Pinl: Proceedings 14. Workshop 20.-21. September 2007 Algorithmen und Werkzeuge für Petrinetze, Arbeitsberichte aus dem Fachbereich Informatik 25/2007

Ulrich Furbach, Markus Maron, Kevin Read: CAMPUS NEWS – an Intelligent Bluetooth-based Mobile Information Network, Arbeitsberichte aus dem Fachbereich Informatik 24/2007

Ulrich Furbach, Markus Maron, Kevin Read: CAMPUS NEWS - an Information Network for Pervasive Universities, Arbeitsberichte aus dem Fachbereich Informatik 23/2007

Lutz Priese: Finite Automata on Unranked and Unordered DAGs Extented Version, Arbeitsberichte aus dem Fachbereich Informatik 22/2007

Mario Schaarschmidt, Harald F.O. von Kortzfleisch: Modularität als alternative Technologie- und Innovationsstrategie, Arbeitsberichte aus dem Fachbereich Informatik 21/2007

Kurt Lautenbach, Alexander Pinl: Probability Propagation Nets, Arbeitsberichte aus dem Fachbereich Informatik 20/2007

Rüdiger Grimm, Farid Mehr, Anastasia Meletiadou, Daniel Pähler, Ilka Uerz: SOA-Security, Arbeitsberichte aus dem Fachbereich Informatik 19/2007

Christoph Wernhard: Tableaux Between Proving, Projection and Compilation, Arbeitsberichte aus dem Fachbereich Informatik 18/2007

Ulrich Furbach, Claudia Obermaier: Knowledge Compilation for Description Logics, Arbeitsberichte aus dem Fachbereich Informatik 17/2007

Fernando Silva Parreiras, Steffen Staab, Andreas Winter: TwoUse: Integrating UML Models and OWL Ontologies, Arbeitsberichte aus dem Fachbereich Informatik 16/2007

Rüdiger Grimm, Anastasia Meletiadou: Rollenbasierte Zugriffskontrolle (RBAC) im Gesundheitswesen, Arbeitsberichte aud dem Fachbereich Informatik 15/2007

Ulrich Furbach, Jan Murray, Falk Schmidsberger, Frieder Stolzenburg: Hybrid Multiagent Systems with Timed Synchronization-Specification and Model Checking, Arbeitsberichte aus dem Fachbereich Informatik 14/2007

Björn Pelzer, Christoph Wernhard: System Description:“E-KRHyper“, Arbeitsberichte aus dem Fachbereich Informatik, 13/2007

Ulrich Furbach, Peter Baumgartner, Björn Pelzer: Hyper Tableaux with Equality, Arbeitsberichte aus dem Fachbereich Informatik, 12/2007

Ulrich Furbach, Markus Maron, Kevin Read: Location based Informationsystems, Arbeitsberichte aus dem Fachbereich Informatik, 11/2007

Philipp Schaer, Marco Thum: State-of-the-Art: Interaktion in erweiterten Realitäten, Arbeitsberichte aus dem Fachbereich Informatik, 10/2007

Ulrich Furbach, Claudia Obermaier: Applications of Automated Reasoning, Arbeitsberichte aus dem Fachbereich Informatik, 9/2007

Jürgen Ebert, Kerstin Falkowski: A First Proposal for an Overall Structure of an Enhanced Reality Framework, Arbeitsberichte aus dem Fachbereich Informatik, 8/2007

Lutz Priese, Frank Schmitt, Paul Lemke: Automatische See-Through Kalibrierung, Arbeitsberichte aus dem Fachbereich Informatik, 7/2007

Rüdiger Grimm, Robert Krimmer, Nils Meißner, Kai Reinhard, Melanie Volkamer, Marcel Weinand, Jörg Helbach: Security Requirements for Non-political Internet Voting, Arbeitsberichte aus dem Fachbereich Informatik, 6/2007

Daniel Bildhauer, Volker Riediger, Hannes Schwarz, Sascha Strauß, „grUML – Eine UML-basierte Modellierungssprache für T-Graphen“, Arbeitsberichte aus dem Fachbereich Informatik, 5/2007

Richard Arndt, Steffen Staab, Raphaël Troncy, Lynda Hardman: Adding Formal Semantics to MPEG-7: Designing a Well Founded Multimedia Ontology for the Web, Arbeitsberichte aus dem Fachbereich Informatik, 4/2007

Simon Schenk, Steffen Staab: Networked RDF Graphs, Arbeitsberichte aus dem Fachbereich Informatik, 3/2007

Rüdiger Grimm, Helge Hundacker, Anastasia Meletiadou: Anwendungsbeispiele für Kryptographie, Arbeitsberichte aus dem Fachbereich Informatik, 2/2007

Anastasia Meletiadou, J. Felix Hampe: Begriffsbestimmung und erwartete Trends im IT-Risk-Management, Arbeitsberichte aus dem Fachbereich Informatik, 1/2007

„Gelbe Reihe“

(http://www.uni-koblenz.de/fb4/publikationen/gelbereihe)

Lutz Priese: Some Examples of Semi-rational and Non-semi-rational DAG Languages. Extended Version, Fachberichte Informatik 3-2006

Kurt Lautenbach, Stephan Philippi, and Alexander Pinl: Bayesian Networks and Petri Nets, Fachberichte Informatik 2-2006

Rainer Gimnich and Andreas Winter: Workshop Software-Reengineering und Services, Fachberichte Informatik 1-2006

Kurt Lautenbach and Alexander Pinl: Probability Propagation in Petri Nets, Fachberichte Informatik 16-2005

Rainer Gimnich, Uwe Kaiser, and Andreas Winter: 2. Workshop "Reengineering Prozesse" – Software Migration, Fachberichte Informatik 15-2005

Jan Murray, Frieder Stolzenburg, and Toshiaki Arai: Hybrid State Machines with Timed Synchronization for Multi-Robot System Specification, Fachberichte Informatik 14-2005

Reinhold Letz: FTP 2005 – Fifth International Workshop on First-Order Theorem Proving, Fachberichte Informatik 13-2005

Bernhard Beckert: TABLEAUX 2005 – Position Papers and Tutorial Descriptions, Fachberichte Informatik 12-2005

Dietrich Paulus and Detlev Droege: Mixed-reality as a challenge to image understanding and artificial intelligence, Fachberichte Informatik 11-2005

Jürgen Sauer: 19. Workshop Planen, Scheduling und Konfigurieren / Entwerfen, Fachberichte Informatik 10-2005

Pascal Hitzler, Carsten Lutz, and Gerd Stumme: Foundational Aspects of Ontologies, Fachberichte Informatik 9-2005

Joachim Baumeister and Dietmar Seipel: Knowledge Engineering and Software Engineering, Fachberichte Informatik 8-2005

Benno Stein and Sven Meier zu Eißen: Proceedings of the Second International Workshop on Text-Based Information Retrieval, Fachberichte Informatik 7-2005

Andreas Winter and Jürgen Ebert: Metamodel-driven Service Interoperability, Fachberichte Informatik 6-2005

Joschka Boedecker, Norbert Michael Mayer, Masaki Ogino, Rodrigo da Silva Guerra, Masaaki Kikuchi, and Minoru Asada: Getting closer: How Simulation and Humanoid League can benefit from each other, Fachberichte Informatik 5-2005

Torsten Gipp and Jürgen Ebert: Web Engineering does profit from a Functional Approach, Fachberichte Informatik 4-2005

Oliver Obst, Anita Maas, and Joschka Boedecker: HTN Planning for Flexible Coordination Of Multiagent Team Behavior, Fachberichte Informatik 3-2005

Andreas von Hessling, Thomas Kleemann, and Alex Sinner: Semantic User Profiles and their Applications in a Mobile Environment, Fachberichte Informatik 2-2005

Heni Ben Amor and Achim Rettinger: Intelligent Exploration for Genetic Algorithms – Using Self-Organizing Maps in Evolutionary Computation, Fachberichte Informatik 1-2005