

Mit IDM und Mittler zu mehr Privatsphäre in LBS

Tobias Kölsch* Lothar Fritsch† Markulf Kohlweiss†
Dogan Kesdogan*

Zusammenfassung

In dieser Arbeit stellen wir eine Architektur und ein Protokoll für ortsbezogene Dienste vor, die die Privatsphäre der Benutzer schützen und den Verwaltungsaufwand zur Einrichtung eines Dienstes erheblich reduzieren. Dazu führen wir einen Ortsdatenvermittler ein, der Aufgaben der Ortsdatenverarbeitung übernimmt und so den Dienstanbieter von der Ortsdatenquelle trennt. Ein Großteil der Autorisierung und der Datenverwaltung wird dabei durch ein System zur automatischen Identitätsverwaltung geleistet. In dieser Arbeit betrachten wir passive Dienste, welche Datenschutzrechtlich problematischer sind, da die Benutzerposition bei ihnen über einen längeren Zeitraum verfolgt wird.

1 Einleitung und Problembeschreibung

Mit der weiten Verbreitung des Mobilfunks ist das Interesse an der Standortinformation von mobilen Telekommunikationsteilnehmern für kontextbezogene Dienste gewachsen. Viele Mobilfunkanbieter bieten bereits jetzt selbst oder über Drittanbieter ortsbezogene Dienste an. Diese reichen von ortsbezogener Tarifierung über ortssensitiven Auskunftsdiensten bis hin zur Flottenüberwachung. Allerdings ist die Einrichtung eines solchen Dienstes recht aufwändig. Da flexible, standardisierte Schnittstellen zur Übermittlung von Standortinformation von Benutzern fehlen, müssen diese häufig neu definiert werden. Außerdem müssen mangels existierender technischer Lösungen viele Aspekte, wie die Spezifikation der Zuständigkeit für die Benutzereinstimmung zur Datenweitergabe, auf vertraglicher Ebene geregelt werden. Dies führt zu einer erhöhten Einstiegsschwelle für neue Dienstleister. Eine Automatisierung dieser Schritte kann existierende Prozesse erheblich vereinfachen und

*{koelsch,kesdogan}@i4.informatik.rwth-aachen.de, RWTH Aachen

†{fritsch,kohlweiss}@whatismobile.de, JWG Universität Frankfurt am Main

erlaubt neue Geschäftsmodelle. Existierende Ansätze auf diesem Gebiet, wie z.B. [2] erfüllen nicht unsere Anforderungen an Datenschutz und Flexibilität.

In dieser Arbeit stellen wir eine Architektur vor, in der die Ortsinformation vom Mobilfunkanbieter nicht direkt an den Dienstanbieter weitergeleitet wird. Statt dessen fragt der Dienstanbieter die Daten über einen Mittler ab. Eine umfassende Begründung für die Sinnhaftigkeit eines solchen Mittler findet sich in [1]. Soweit möglich, verarbeitet der Mittler die Daten lokal und übermittelt nur das Ergebnis der Berechnung an den Dienstanbieter. Die Gewährleistung der Einwilligung durch den Benutzer und die Identitätsverwaltung wird dabei automatisch durch ein Programm erledigt.

2 Beschreibung der Architektur

Unsere Architektur beschreibt den Fall, dass wir einen Mobilfunkanbieter (MO) und einen von ihm getrennten Ortsbasierten Dienstanbieter (DA) haben, die dem Benutzer (B) gemeinsam einen Dienst zur Verfügung stellen. Der MO dient dabei sowohl als Kommunikationsanbieter, als auch als Positionsanbieter. Der DA implementiert die Funktionalität des Dienstes. Wie gesagt kommunizieren die beiden Anbieter nicht direkt, sondern über einen Mittler (LM). Der Aufbau ist auf der Grafik 1 dargestellt.

Die vier beteiligten Parteien sind mit einem automatischen Identitätsverwalter (IDM) ausgestattet. Konkret handelt es sich um den IDM, welcher im Rahmen des Prime Projektes [3] entwickelt wird.

2.1 Beschreibung des IDM

Ziel des Prime Projektes ist es ein Werkzeug zum ganzheitlichen Schutz der Privatsphäre und zur automatischen Verwaltung partieller Identitäten zu

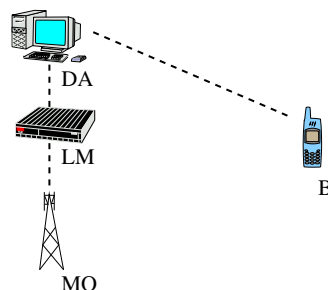


Abbildung 1: Der Benutzer fragt einen Dienst beim Dienstanbieter an. Dieser benutzt den Mittler um die Ortsinformation des Benutzers vom Mobilfunkbetreiber zu ermitteln.

erstellen. So trifft das System regelbasiert bei der Interaktion mit anderen Systemen Vereinbarungen darüber welche Daten über den Benutzer enthüllt werden. Das beinhaltet auch Abmachungen über Aufbewahrungsfristen der übermittelten Daten. Außerdem soll das System die Weitergabe von Informationen verfolgen. Anhand dieser protokollierten Daten kann der Benutzer sich dann darüber informieren, wem welche Daten über ihn bekannt sind.

Um Dienste zu ermöglichen, die es verlangen, dass bestimmte Eigenschaften des Benutzers bewiesen werden, bietet der IDM auch die Möglichkeit einzelne Aspekte eines Benutzers zusammen mit einer Zertifizierungsanstalt anonym zu beglaubigen. Bezahlung kann ebenfalls mittels des IDM erfolgen. Um die Privatsphäre des Benutzers auf allen Ebenen zu schützen, kann außerdem die gesamte Kommunikation anonymisiert werden.

2.2 Beschreibung des Protokolles

Es wird nun das Protokoll beschrieben, das in der vorhin beschriebenen Architektur die benötigte Funktionalität für ortsbasierte Dienste bietet. Wir betrachten hier nur passive, ereignisgesteuerte Dienste, wie z.B. einen ortsbasierten Stauwarndienst, oder einen Pollenwarndienst. Bei diesen wird der Benutzer gewarnt, wenn er sich innerhalb eines bestimmten Bereiches befindet.

Das Protokoll beinhaltet dabei zwei Einrichtungs- und einen Ausführungsschritt. Bei der Einrichtung veranlasst das Benutzergerät sowohl den MO als auch den LM dazu jeweils einen logischen Kanal zu erzeugen. Diese dienen von da an als Pseudonyme für den Benutzer. Zusätzlich werden noch Zugangsbeschränkungen für die Kanäle übermittelt. Außerdem erhält der LM noch einen Kryptoschlüssel.

Will der Benutzer einen Dienst initiieren, verbindet er sich zum DA, nehmen wir an es handle sich dabei um einen Pollenwarndienst, und übermittelt eine Liste seiner Allergien. Dann übermittelt er dem Anbieter die Zugangsdaten zu dem logischen Kanal bei dem LM und ein verschlüsseltes Datenpaket in dem sich die Zugangsdaten zu dem logischen Kanal des MO befinden. Dieses Paket ist mit dem Schlüssel der sich bei dem LM befindet verschlüsselt worden.

Beachte, dass die Kommunikation zwischen dem Benutzer und dem Anbieter anonymisiert werden muss, da der MO ansonsten über die Datenleitung erfahren kann, welche Dienste der Kunde nutzt.

Der DA berechnet nun die Regionen, die für den Benutzer von Interesse sind und verbindet sich zu dem Kanal der durch den LM geöffnet wurde. Er autorisiert seinen Zugriff mit den Daten, die ihm vom Benutzer mitgegeben wurden und übermittelt sowohl die Allergengebiete, als auch das

verschlüsselte Datenpaket.

Der LM kann nun das Paket entschlüsseln und sich anhand der in ihm befindlichen Daten zum MO verbinden. Die Zugriffsbeschränkungen des Kanals bestimmen, in welchem Maße dem LM Daten über den Benutzer übermittelt werden. Es kann auch die Genauigkeit der Übertragenen Daten eingeschränkt werden. Wenn die Verbindung steht und der LM sich autorisiert hat, kann er in dem benötigten Intervall die Benutzerposition abfragen. Diese vergleicht er dann mit den Allergengebieten und teilt dem DA mit, wenn er eine Übereinstimmung gefunden hat. Dieser kann dann die betreffende Information daraus ziehen und seinerseits den Benutzer informieren.

Zum Unterbrechen des Dienstes, teilt der Benutzer dem MO mit, dass er den Kanal schließen soll. Die Schließung wird dann weiterpropagiert.

3 Bewertung

Dieser Ansatz bringt auf verschiedenen Ebenen Vorteile. Zum einen abstrahiert der Mittler von der eigentlichen Ortsdatenquelle. Ein Dienstanbieter verbindet sich zu ihm unabhängig davon, ob die Daten aus einem WLAN-, einem GSM-Netz, oder vom Mobilgerät des Benutzers selbst stammen. Es könnten theoretisch sogar verschiedene Datenquellen gleichzeitig genutzt werden, um die Genauigkeit zu erhöhen. Außerdem erfährt die Datenquelle wenig über den Dienst, der vom Benutzer beansprucht wird.

Die Verwendung des IDM bietet den Vorteil, dass eine standardisierte Schnittstelle zur Verfügung steht. Außerdem macht der Autorisierungsmechanismus und die direkte Bezahlung das Abschließen von Verträgen zwischen Dienstanbieter und Mobilfunkbetreiber überflüssig. Und zu letzt garantiert das System die Zustimmung des Benutzers zur Weitergabe seiner Daten und gibt ihm mehr Kontrolle über seine persönlichen Daten.

Danksagung Vielen Dank an Lexi Pimenidis für seine Unterstützung.

Literatur

- [1] T. Kölsch, L. Fritsch, M. Kohlweiss, and D. Kesdogan. Privacy for profitable location based services. volume 3450 of *LNCS*. Springer, 2005.
- [2] Marwa Marbrouk and et. al. OpenGIS Location Services (OpenLS): Core Services. 2004.
- [3] PRIME WP 14.0. Prime Framework V1, 2005. <http://www.prime-project.eu.int>.