Die datenschutz- und sicherheitskonforme Ausgestaltung von Location Based Services am Beispiel eines mobilen Touristenführers

Silvio Becher[1], Philip Laue[2], Monika Maidl[3], Marko Modsching[4]

[1]Siemens AG, Corporate Technology, Otto-Hahn-Ring 6, 81739 München,
silvio.becher@siemens.com
[2]Universität Kassel - provet -, Wilhelmshöher Allee 64, 34109 Kassel,
p.laue@uni-kassel.de
[3]Siemens AG, Corporate Technology, Otto-Hahn-Ring 6, 81739 München,
monika.maidl@siemens.com
[4]Hochschule Zittau/Görlitz, Obermarkt 17, 02826 Görlitz,
mmodsching@hs-zigr.de

Abstract: Location Based Services eröffnen die Möglichkeit neuartiger, individuell auf den Nutzer abgestimmter Dienste. Gleichzeitig stellen sie die herkömmlichen datenschutzrechtlichen Konzepte zum Schutz der informationellen Selbstbestimmung vor eine neue Herausforderung. Der folgende Beitrag stellt am Beispiel eines mobilen Touristenführers dar, wie sich durch eine vorausschauende Technikgestaltung die Vorteile und Potentiale eines Location Based Service realisieren lassen, ohne dabei datenschutzrechtliche Grundsätze zu vernachlässigen.

1. Einleitung

Die weite Verbreitung der Mobilfunktechnologie und die Entwicklung von Lokalisierungsverfahren sind Grundbedingung für Entwicklung und Angebot ortsbezogener Dienste. Darunter sind Mobilfunk-Online-Dienstleistungen zu verstehen, die dem Nutzer entweder abhängig von seinem Standort zur Verfügung gestellt werden, die gleichen Anfragen in Abhängigkeit vom Nutzerstandort unterschiedlich beantworten oder deren Inhalt sich auf den Standort Dritter beziehen. Die Einsatzgebiete solcher Location Based Services sind vielfältig. So bestehen bereits in den Bereichen Navigation (Reiseroute für PKW), Verkehrstelematik (Stau), Notrufdienste (Krankenwagen), Informationen (Wetter, Veranstaltungen), Unterhaltung (Handy-Parties, Community-Spiele), Wirtschaft (Werbung, Preisvergleiche) und Sicherheit (Fahrzeugüberwachung, Statusüberwachung von Personen) ortsbezogene Diensteangebote.

Wie die meisten mobilen Dienste werden sie zunehmend auf die individuellen Bedürfnisse der Nutzer abgestimmt. Neben dem Aufenthaltsort werden dabei zahlreiche weitere Informationen über den Nutzer gesammelt. Für den Nutzer bietet dies den Vorteil, dass er nicht mit einer unüberschaubaren Anzahl von Diensteangeboten belastet wird. Er erhält die seinen Interessen entsprechenden Angebote genau zu dem Zeitpunkt und an dem Ort, an dem er sie benötigt.

Diese neue Form der IuK-Technologie lässt sich dazu nutzen, auch im Bereich des Tourismus neue Wege der Erlebnis- und Wissensvermittlung zu beschreiten. Durch ein Informationsangebot, das auf den Standort, die Interessen und den zur Verfügung stehenden Zeitrahmen des Touristen abgestimmt ist, können mobile Touristenführer dem Benutzer ein individuelles Freizeiterlebnis verschaffen. Dabei besteht ein besonderer Vorteil darin, dass die Nutzer mobiler Assistenz Attraktionen wahrnehmen, die sie sonst womöglich nicht entdeckt hätten. Dadurch können Touristenströme besser in der Stadt verteilt und vorhandene Tourismusangebote effizienter genutzt werden. Für das Destination Management einer Stadt eröffnen sich neue Möglichkeiten, die Destination zielgerichteter und kundennah zu vermarkten.

2. Datenschutzrechtliche Anforderungen an das Techniksystem

Die für den Dienst notwendige Individualisierung ist in der Regel jedoch nur dann zu erreichen, wenn der Diensteanbieter auf eine große Anzahl personenbezogener Daten zugreifen kann. Die einem mobilen Touristenführer zugrunde liegende Location Based Service (LBS)-Technologie stellt dabei eine neue Herausforderung für den Datenschutz dar. So kann das Streben nach einem möglichst umfassenden und individualisierten Diensteangebot mit den datenschutzrechtlichen Grundsätzen von Datenvermeidung und Datensparsamkeit in Konflikt geraten. Zugleich können entsprechend personalisierte Dienste neue Profilsrisiken begründen und damit eine Gefahr für die informationelle Selbstbestimmung des Nutzers hervorrufen. Der folgende Beitrag stellt daher am Beispiel eines mobilen Touristenführers dar, wie sich durch eine vorausschauende Technikgestaltung die Vorteile und Potentiale eines LBS realisieren lassen, ohne dabei datenschutzrechtliche Grundsätze zu vernachlässigen.

2.1 Personenbezogene Daten

Die Gefahr eines Eingriffs in das aus Artikel 1 Absatz 1 GG i.V.m. Artikel 2 Absatz 1 GG entwickelte informationelle Selbstbestimmungsrecht des Nutzers besteht grundsätzlich immer dann, wenn es im Zusammenhang mit dem Betrieb eines LBS zu einem Umgang mit personenbezogenen Daten kommt. Diese werden in § 3 Absatz 1 Bundesdatenschutzgesetz (BDSG) gesetzlich definiert als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

Unter Einzelangaben sind dabei Informationen zu verstehen, die sich auf eine bestimmte – einzelne – Person beziehen oder geeignet sind, einen Bezug zu ihr herzustellen [GS05, § 3 Rn.3]. Über persönliche oder sachliche Verhältnisse geben sie dann Aufschluss, wenn die Informationen den Betroffenen selbst charakterisieren oder einen auf ihn beziehbaren Sachverhalt beschreiben [Sc03]. Der Begriff ist umfassend zu verstehen und nicht auf Daten beschränkt, die ihrer Natur nach personenbezogen sind wie etwa menschliche Eigenschaften [Sc03].[1] Die Daten sind dann personenbezogen, wenn sie

[1] Für Beispiele von Daten über „persönliche oder sachliche“ Verhältnisse s. auch [Sc03, 184] und [GK03, 40].

sich auf eine bestimmte oder bestimmbare Person beziehen. So können die Daten entweder selbst einen unmittelbaren Rückschluss auf die Identität des Betroffenen zulassen oder aufgrund von Zusatzinformationen bestimmbar sein [Sc03]. Für die Bestimmbarkeit kommt es auf die Kenntnisse, Mittel und Möglichkeiten der speichernden Stelle an [Sc03; GS05, § 3 Rn. 9]. Ob eine Information personenbeziehbar ist, lässt sich also nicht aus der Angabe allein ableiten, sondern ist abhängig vom jeweiligen Zusatzwissen. Ob es sich um personenbezogene Daten handelt erfordert daher gegebenenfalls, die Relation zwischen Daten, Datenverarbeiter und Nutzer zu betrachten. So können sich gegenüber dem Betreiber des mobilen Touristenführers nicht nur der Name und die Adresse des Touristen als personenbezogene Daten darstellen, sondern auch seine persönlichen Vorlieben und Interessen oder Angaben über Gehgeschwindigkeit, Alter und mögliche Aufenthaltsdauer vor Ort. Ein Umgang mit personenbezogenen Daten im Bereich des E-Tourismus kann somit nicht von vornherein ausgeschlossen werden.

2.2 Profilerstellung als Risiko für die informationelle Selbstbestimmung

Um dem Nutzer einen auf seine Bedürfnisse angepassten Dienst anbieten zu können, werden bei LBS in der Regel die Daten zusammengeführt und zu einem umfangreichen Datenbestand angereichert. Dies begründet die Gefahr, dass eine solche Datensammlung zu Persönlichkeitsprofilen und, bei Verwertung von Standortdaten, zu umfassenden Bewegungsprofilen zusammengesetzt wird.[2] Wie das Bundesverfassungsgericht bereits 1983 feststellte, können von einer Profilbildung besondere Risiken für das Selbstbestimmungsrecht des Betroffenen ausgehen.[3]

Grundsätzlich bezeichnet ein Profil einen Datensatz über eine Person, der zumindest ein Teilabbild über seine Persönlichkeit gibt [Po72; Wi00]. Eine genauere Definition des Profils findet sich aber weder in den unterschiedlichen Datenschutzgesetzen noch in der Rechtsprechung oder Literatur. Die Verfassungsrichter etablierten den Begriff, um eine mit besonderen Risken behaftete Form der Datenverarbeitung auf Tatbestandsebene zu umschreiben und so an die Erstellung von Profilen besondere Rechtsfolgen knüpfen zu können.[4] Ebenso wie sich die Technik seit damals drastisch weiterentwickelt hat, muss jedoch auch der Profilbegriff den modernen Risiken entsprechend stets neu angepasst werden.

Die Grundrechtsrelevanz der Profilbildung ergibt sich damit nicht bereits aus Art und Umfang der erhobenen Daten. Vielmehr kommt es auf das Risikopotential und die denkbaren Verwendungen an.[5] Dabei sind unter den Bedingungen der bei LBS zum Einsatz kommenden Informations- und Kommunikationstechnologie zahlreiche Persönlichkeitsgefährdungen vorstellbar, die sich auf die Erstellung und Verwendung von Profilen zurückführen lassen.

So soll das Persönlichkeitsrecht jedem ermöglichen, selbst zu entscheiden, wie er sich

---

[2] Zum Umgang mit Standortdaten und Bewegungsprofilen s. ausführlich [JL06].
[3] BVerfGE 65, 1, 6.
[4] Eine solche Rechtsfolge enthält seit 1997 z.B. § 6 Abs. 3 TDDSG.
[5] BVerfGE 65, 1, 46.

Dritten gegenüber, in der Öffentlichkeit oder in bestimmten Situationen darstellen will. Werden in Profilen alle verfügbaren Daten zusammengefügt und in Umlauf gebracht, besteht die Gefahr, dass sich Dritte aufgrund dieser Informationen bereits ein Bild über eine Person gemacht haben, ohne dass ein vorheriger Kontakt bestand. Der Betroffene ist dann für die Zukunft in seiner Selbstdarstellungsbefugnis eingeschränkt.[6]

Darüber hinaus besteht die Gefahr, dass der Nutzer jegliche Kontrollmöglichkeit über den Inhalt eines zu seiner Person erstellten Profils verliert. Aus einer umfangreichen Datensammlung können Prognosen für ein zukünftiges Verhalten und die zu erwartenden Aufenthaltsorte der Person in der Zukunft abgeleitet werden. Da der Profilersteller mehr über den Nutzer weiß, als dieser sich selbst bewusst ist, kann er gezielt auf diesen Einfluss nehmen. Dies kann ein Gefühl des Ausgeliefertseins und der Fremdbeobachtung bewirken sowie eine Verhaltensbeeinflussung des Betroffenen erleichtern und so sein Recht auf informationelle Selbstbestimmung gefährden.[7]

Um diesen Risiken vorzubeugen, ist bei der Systemgestaltung eines LBS durch technisch-organisatorische Maßnahmen sicherzustellen, dass es bei der Datenspeicherung nicht zu einer entsprechenden Profilbildung kommt.

2.3 Notwendigkeit einer rechtsgemäßen Technikgestaltung

Stellt sich beim Betrieb des LBS heraus, dass ein Umgang mit personenbezogenen stattfindet, so greift ein umfangreiches Schutzkonzept datenschutzrechtlicher Grundsätze ein, um die informationelle Selbstbestimmung des Nutzers zu gewährleisten [Gi07]. Dies hängt jedoch wiederum wesentlich von der technischen Ausgestaltung des Gesamtsystems ab.

Technikentwicklung wird jedoch meist zu einem Zeitpunkt in Gang gesetzt, zu dem nur wenig über die Risiken und Chancen des Einsatzes nachgedacht, der Nutzen nicht evaluiert, die Technikziele und ihre Erreichbarkeit nicht hinreichend überprüft und die Frage nach Technikalternativen – wenn überhaupt – vordringlich unter ökonomischen Gesichtspunkten geprüft werden [Sc03; St05]. Im Vordergrund steht die Herstellbarkeit und Funktionstüchtigkeit der Technik selbst [Ro93].

Technik und Recht sind jedoch auf verschiedene Art und Weise in einem wechselseitigen Prozess miteinander verbunden und beeinflussen sich gegenseitig [Ho05]. Technische Entwicklungen können unmittelbar auf rechtliche Bewertungen Einfluss nehmen und soziale sowie gesellschaftliche Verhältnisse beeinflussen.[8] Wird dabei das Recht zu spät angewandt, besteht die Gefahr verfestigter Strukturen und Abläufe, so dass das Recht einem fortwährenden Anpassungsdruck ausgesetzt wird [Sc03; Ho05]. Zugleich kann eine verspätete rechtliche Begleitung der Systementwicklung dazu führen, dass

---

[6] So auch [RPG01], die von einer Einschränkung der eigenen Rolleninterpretation in sozialen Zusammenhängen sprechen.

[7] S. zu den Risiken der Profilbildung und den Merkmalen, die ein entsprechender Datensatz aufzuweisen hat, um die Profilrisiken zu begründen ausführlich auch näher [JL06].

[8] Ausführlich zur Notwendigkeit und Methode rechtswissenschaftlicher Technikfolgenforschung [Ro93].

sich IuK-Systeme nachträglich als rechtlich unzulässig und damit für den Praxiseinsatz untauglich herausstellen. Dann ist ein u.U. kosten- und zeitaufwändiges Nachjustieren der Technik erforderlich oder schlimmstenfalls die Technik als Ganzes nicht einsetzbar.

Ziel muss es daher sein, datenschutzrechtliche Schutzkonzepte im Sinne einer rechtsgemäßen Technikgestaltung bereits bei der Systementwicklung zu berücksichtigen. So lässt sich nicht nur ein datenschutzfreundliches Gesamtkonzept realisieren, sondern es können auch die Verwirklichungsbedingungen von Recht und Technik optimiert werden.

2.4 System- und Selbstdatenschutz zur Datensparsamkeit und Datenvermeidung

Ein zentrales datenschutzrechtliches Schutzkonzept stellen dabei die in § 3a Satz 1 BDSG definierten Grundsätze der Datenvermeidung und Datensparsamkeit dar. Danach haben sich Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Durch die Regelung wird der datenschutzrechtliche Erforderlichkeitsgrundsatz präzisiert, wonach ein Umgang mit personenbezogenen Daten nur stattfinden darf, soweit dies zur Erreichung eines gesetzlich normierten oder aufgrund einer Einwilligung des Betroffenen festgelegten Zwecks erforderlich ist [RPG01].

Durch die Regelung nimmt der Gesetzgeber schon im Vorfeld der Technikentwicklung Einfluss auf ihre Ausgestaltung und fördert so die Integration datenschutzrechtlicher Anforderungen in technische Gestaltungsprozesse [Sc03a]. Die Elemente eines solchen Systemdatenschutzes sollen einer unzulässigen Datenverarbeitung vorbeugen und die Selbstbestimmung des Betroffenen sicherstellen [Ro99]. So können beispielsweise automatische Löschungsroutinen aber auch Verschlüsselungsmethoden technisch dazu beitragen, den Nutzer vor einem unzulässigen Datenumgang zu schützen.

Der Grundsatz der Datenvermeidung hat aber nicht nur für den Systemdatenschutz Bedeutung, sondern zielt ebenso auf eine Förderung des Selbstdatenschutzes [Si06, § 3a Rn. 26]. Darunter sind Regelungselemente zu verstehen, die dem Betroffenen eigene Instrumente in die Hand geben, seine informationelle Selbstbestimmung zu schützen und damit seine Autonomie stärken [Ro99; Si06, § 3a Rn. 26]. Geeignete Mittel des Selbstdatenschutzes stellen neben organisatorischen Vorkehrungen zur Datenkontrolle durch den betroffenen Nutzer insbesondere die Möglichkeiten der anonymen oder pseudonymen Nutzung des Systems dar. Sie können (teilweise) dazu beitragen, einen etwaigen Personenbezug zu beseitigen und so einen aktiven Beitrag zur Datenvermeidung leisten.

Anonymität ist dann gegeben, wenn die Wahrscheinlichkeit, die Daten einer Person zuordnen zu können, so gering ist, dass sie nach der Lebenserfahrung oder dem Stand der Wissenschaft praktisch ausscheidet und ein Personenbezug somit nicht vorliegt [RS00; Ro03]. Dabei kann die Möglichkeit, den Personenbezug herzustellen, aufgrund der Umstände unterschiedlich wahrscheinlich sein [Ro03]. Werden daher beispielsweise anonyme Daten an eine Stelle übermittelt, die in der Lage ist, den Personenbezug herzustellen, so handelt es sich für sie um personenbezogene Daten mit der Folge, dass für ihn die datenschutzrechtlichen Vorschriften zur Anwendung kommen [GS05, § 3 Rn. 9].

Pseudonymität liegt dagegen vor, wenn der Nutzer ein Kennzeichen benutzt, durch das die Wahrscheinlichkeit, dass Daten ihm zugeordnet werden können, so gering ist, dass sie ohne Kenntnis der jeweiligen Zuordnungsregel zwischen Kennzeichen und Person nach der Lebenserfahrung oder dem Stand der Wissenschaft praktisch ausscheidet [Ro03]. Im Gegensatz zur Anonymität gibt es bei Pseudonymität eine Regel (oder Liste), über die ein Zuordnung zu einer Person möglich ist. Es ist daher zwischen den Personen, die die Zuordnungsregel kennen und denen, die sie nicht kennen, zu unterscheiden. Pseudonyme Daten sind für den Kenner der Zuordnungsregel personenbeziehbar, für alle anderen sind sie anonyme und damit nicht personenbezogene Daten [Ro03].

3. Sicherheitstechnische Anforderungen an das Techniksystem

Werden von einem mobilen Touristenführer Bilder, Audio-Files oder Filme genutzt, so können diese urheberrechtlichen Einschränkungen unterliegen. Vor allem das Anfertigen von Kopien durch den Anwender wird in vielen Fällen unzulässig sein. Darüber hinaus wird es, je nach Businessmodell, in der Regel gewollt sein, dass die Daten nur einem eingeschränkten Benutzerkreis zugänglich sind, nämlich denen, die für diese Dienstleistung entsprechend gezahlt haben. Um die Umsetzung beider Ziele zu gewährleisten, bedarf es daher im Rahmen der Architektur eines LBS einer entsprechenden Sicherheitsinfrastruktur in Form von Verschlüsselungstechniken.

Eine entsprechende Techniklösung erfordert jedoch grundsätzlich die Einführung einer Sitzung, beispielsweise mittels einer SessionID, um autorisierte von nicht-autorisierten Benutzern zu unterscheiden. Im Rahmen mobiler Touristenführer ist daher während einer Sitzung, d.h. während des Tourverlaufs, das Verhalten eines einzelnen Benutzers auf Serverseite nachvollziehbar. Im Prinzip könnten also Personendaten, nämlich Daten darüber wann sich der Benutzer wo aufgehalten hat, gesammelt werden. Im Gegensatz zu den Benutzerprofil- und Tourdaten gibt der Anwender diese Daten nicht explizit selbst an, sondern sie werden automatisch erfasst. Darüber hinaus ist es im Bezahlmodus eventuell erforderlich, dass der Anwender auch seinen Namen und Kontodaten angibt, während diese Angaben im Nichtbezahlfall unnötig sind.

Werden Daten jedoch ohne das Einverständnis des Betroffenen und ohne gesetzliche Grundlage gesammelt, so stellt dies einen grundsätzlich unzulässigen Datenumgang dar. Im Rahmen einer notwendigen Sicherheitsinfrastruktur ist daher darauf zu achten, dass durch die Einführung von Verschlüsselungstechniken keine neuen Möglichkeiten geschaffen werden, in unzulässiger Weise vom Nutzer unbemerkt personenbezogene Daten über ihn zu sammeln. Gleichzeitig muss sich auch bei der sicherheitstechnischen Unterstützung von Bezahlverfahren die Systemarchitektur am Grundsatz der Datensparsamkeit ausrichten.

4. Der Dynamic Tour Guide (DTG)

Unter Berücksichtigung der dargestellten datenschutzrechtlichen und sicherheitstechni-

schen Anforderungen wurde im Rahmen des interdisziplinären VESUV-Projekts[9] mit dem Dynamic Tour Guide (DTG) ein dynamischer Touristenführer für mobile Endgeräte entwickelt, dessen Systemarchitektur nachfolgend kurz erläutert wird.

Die Idee des DTG besteht darin, dass Menschen schon in naher Zukunft über Mobiltelefone verfügen werden, die über integrierte Sensoren (GPS, Bluetooth, RFID/NFC, WLAN), große Displays, Zugangsmöglichkeiten zum Internet und eine leistungsstarke Plattform verfügen [HMK05]. Diese Möglichkeiten lassen sich dazu nutzen, auf dem mobilen Endgerät persönliche Vorlieben und Angaben des Touristen zu erfassen sowie sukzessive zu erweitern und anzupassen. Der persönliche Kontext kann mit dem lokalen Kontext (Attraktionen, Wetter, Events, usw.) verglichen und bewertet werden, um so Aktivitäten zu finden, die in der momentanen Situation am besten geeignet sind. Mit diesen gewonnenen Informationen kann dem Nutzer ein höherwertiger personalisierter Dienst angeboten werden. Ein Beispiel dafür ist die Zusammenstellung einer individuellen Stadtführung, die mit dem DTG zur Verfügung gestellt wurde.

Ein Schwerpunkt ist dabei, in adäquater Zeit eine adaptive Tour zu generieren, die der vom Nutzer eingegebenen Spezifikation genügt. Diese kann sowohl Sehenswürdigkeiten und Lokalitäten, als auch Naturparks oder Museen umfassen. Im Kontext des DTG werden diese touristischen Attraktionen auch als Tourbausteine bezeichnet. Über das eingebaute GPS ist es möglich, den ortsfremden Touristen über audio-visuelle Navigationsanweisungen zu den einzelnen Attraktionen (POIs – Point of Interests) zu leiten und ihm dort automatisch multimediale Informationen anzubieten. Dabei stellt sich das System adaptiv auf die aktuellen Tourgegebenheiten ein. So kann es z.B. sein, dass der Nutzer selbständig vom Tourplan abweicht, um weitere Attraktionen zu besuchen. Das System kann auf derartige spontane Änderungen reagieren und die Tour anpassen.

Für die Umsetzung der beschriebenen Szenarien müssen vom Touristen diverse Daten erfasst werden. Diese kann man in zwei verschiedene Klassen unterteilen: So genannte *Profildaten* und *Tourdaten*. Die Profildaten umfassen die Interessen des Nutzers, die in einer Taxonomie ausschließlich auf dem Endgerät des Benutzers abgelegt werden.

Die Tourdaten setzten sich aus folgenden Inhalten zusammen:

- Zielpunkt der Tour,
- Tourdauer,
- Restaurantdaten (Typ, Nationalität, Biergarten, usw.).

Sie werden wie die Profildaten für den Planungsprozess benötigt, der die Tour berechnet. Im Gegensatz zu den Profildaten können sich die Tourdaten für jeden Planungsprozess unterscheiden. Sie müssen daher bei jeder Neuplanung erneut eingegeben werden. Die Daten werden dabei nur für die Dauer der Tour auf dem Endgerät gespeichert und bei einer weiteren Tour vom System bei einer erneuten Berechnung gelöscht.

[9] http://www.vesuv-projekt.de.

Im Anschluss an die Dateneingabe wird die Tour berechnet. Dieser sehr komplexe Prozess benötigt einen hohen Rechenaufwand. Daher wird dieser Arbeitsschritt nicht auf dem leistungsärmeren mobilen Endgerät ausgeführt, sondern auf einen Server ausgelagert. Dazu werden die erfassten Daten an diesen geschickt, um die Planung der Tour durchzuführen. Die Daten werden auf dem Server nur flüchtig im Arbeitsspeicher gehalten und nach der Tourberechnung sofort wieder gelöscht. Da die Leistungsfähigkeit mobiler Endgeräte in den letzten Jahren stark gestiegen ist, ist anzunehmen, dass man derartige Prozesse in Zukunft ebenfalls auf dem mobilen Endgerät durchführen kann.

Nach der Tourberechnung über den im Backend sitzenden Server verfügt der mobile Client über eine Metainformationsliste von Tourbausteinen, die vom Server übertragen werden. Diese Metainformationen (Descriptoren) enthalten folgende Tourbausteindaten:

- Adresse (postal) des Tourbausteins,
- Profil im Sinne einer Einordnung in die Taxonomie sowie
- Identifier.

Diese Informationen sind ausreichend, um mit der Führung zu den einzelnen Sehenswürdigkeiten zu beginnen. Die zu den Tourbausteinen gehörenden multimedialen Informationen müssen allerdings wiederum separat über einen Content-Server herunter geladen werden, da sie für einen einzelnen Aufruf zu große Datenmengen aufweisen.

4.1 Sicherheitsinfrastruktur

Um die in Kapitel 3 dargestellten sicherheitstechnischen Anforderungen zu erfüllen, wurde in den DTG eine entsprechende Sicherheitsinfrastruktur integriert. Folgendes Ablaufdiagramm zeigt die Umsetzung für den DTG:

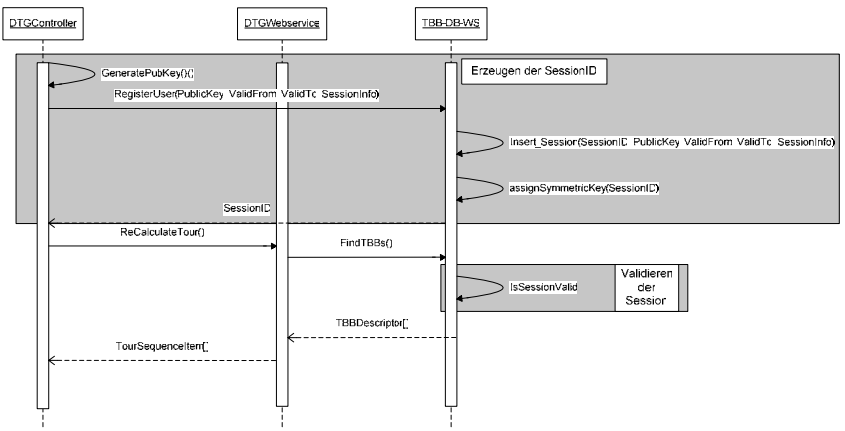

Abbildung 1: Sequenzdiagram für Verschlüsselung.

Auf dem Client wird zunächst ein zufälliges asymmetrisches Schlüsselpaar erzeugt. Der private Schlüssel ist an das Gerät gebunden und wird nicht weitergegeben, während der öffentliche Schlüssel anschließend an den zentralen Contentserver übermittelt wird. Der Server erzeugt eine zufällige SessionID und legt diese dann zusammen mit Sitzungsdaten wie Gültigkeitsdauer, Typ der Sitzung und dem öffentlichen Schlüssel in einer Datenbank ab. Die SessionID wird anschließend an den Client zurückgegeben. In allen darauf folgenden Aufrufen in den Server Backend schickt der Client nun die erzeugte SessionID mit, so dass der Server den Aufruf authentisieren, die Gültigkeit prüfen und die Daten für das Gerät verschlüsseln kann. Die zu schützenden Tourbausteininhalte gelangen also nur verschlüsselt auf das Gerät und sind somit dort vor einem unbefugten Zugriff oder Kopieren geschützt. Lediglich der befugte Client ist in der Lage, mit seinem privaten Schlüssel die Daten zu entschlüsseln und die Informationen zu extrahieren.

4.2 Architektur

Auf der technischen Seite des DTG wurde eine klassische Client-Server Architektur mit einer Service orientierten Architektur (SOA) im Server Backend realisiert (Abbildung 2). Auf der Client-Seite befindet sich das mobile Gerät mit einem installierten Thick-Client. Dieser integriert die verschiedenen Software-Module und übernimmt damit den größtmöglichen Teil der kontext-bezogenen Guidance, sowie das Triggern von Tourneuberechnungen für Touradaptionsvorgänge. Auf der Server-Seite befindet sich der VESUV-Server mit drei verschiedenen Webservices:

Server-Modul	**Beschreibung**
TBB-DB-Webservice	Dient als einheitliches Datenbeschaffungsmodul für die dynamischen Inhalte einer Tour. Realisiert weiterhin die serverseitige Verschlüsselung
DTG-Webservice	Ist zentraler Anlaufpunkt für Tourberechnungsaufrufe. Von hier aus wird das Matching der Profile und die Beschaffung der Descriptoren durchgeführt.
Tourcalculation	Ordnet verschiedene gewichtete Tourbausteine zu einer Tour zusammen, um eine möglichst optimale Tour zu erhalten.

Tabelle 1: Servermodule im Backend.

Der Relay Server dient dazu, die Performance der oben beschriebenen Web Service-Aufrufe zu verbessern. Web Service-Aufrufe werden mittels eines XML-basierten Protokolls (SOAP) durchgeführt. Dies führt bei mobilen Endgeräten aufgrund relativ geringer Rechenkapazitäten zu einer geminderten Performance. Dies ist unter anderem auf die dabei entstehenden komplexen XML-Strukturen zurückzuführen, die zum einen erzeugt und zum anderen geparst werden müssen. Um dieses Problem zu umgehen, delegiert der WSCommunicator Client einen Web Service-Aufruf über ein eigens dafür definiertes Protokoll zum Relay Server. Der WSCommunicator Server erzeugt und verarbeitet den Web Service-Aufruf und sendet das Ergebnis über das gleiche Protokoll an den Client

zurück. Für die aufrufende DTG-Applikation bleibt dieser Vorgang technisch transparent. Der rechenintensive Vorgang des Web Service-Aufrufs findet nur auf der Server-Seite im Backend statt.

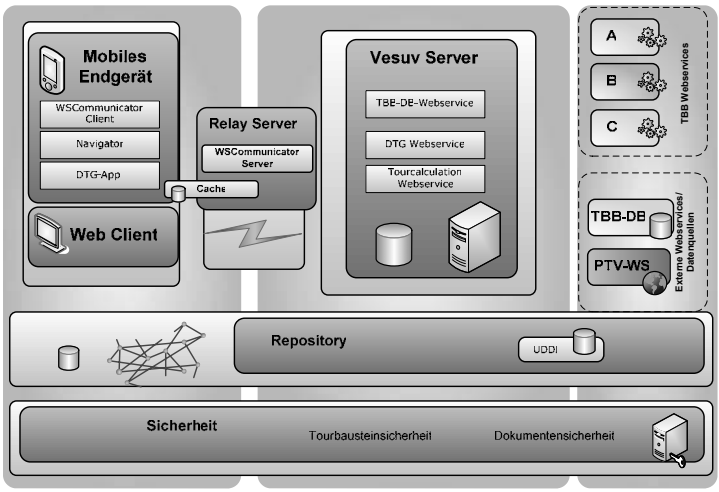

Abbildung 2: Allgemeine Architektur des DTG.

5. Datenschutzrechtliche und sicherheitstechnische Beurteilung

Beim Entwurf der Architektur des DTG wurde darauf geachtet, die in Kapitel 2 und 3 geschilderten datenschutzrechtlichen und sicherheitstechnischen Risiken und Anforderungen zu berücksichtigen. Die getroffenen Maßnahmen bestehen einerseits in einer sparsamen Datenerhebung und andererseits in einer eingeschränkten Datenspeicherung.

5.1 Sparsames Erfassen von Benutzerdaten

Die wirksamste Maßnahme besteht darin, den Bedarf an Benutzerdaten genau zu analysieren und unnötige Daten erst gar nicht zu erfassen. Im DTG führt diese Maßname bereits sehr weit, wie im Folgenden beschrieben wird. Da wie in Kapitel 3 beschrieben, die Verwendung der Sicherheitsinfrastruktur zusätzliche datenschutzrechtliche Risiken hervorrufen, werden dabei die verschiedenen Anwendungsfälle getrennt behandelt.

Ohne Aktivierung der Sicherheitsinfrastruktur

Grundsätzlich sind die zur Interessenerfassung und Tourplanung benötigten Profil- und Tourdaten für den Betreiber des DTG nicht aussagekräftig genug, um sie mit hinreichender Wahrscheinlichkeit einer bestimmten Person zuordnen zu können, da der Name des Anwenders nicht erfasst wird. Mangels Personenbezug sind sie also, unabhängig vom konkreten Datenumgang, für den Betreiber anonyme Daten und beugen so wirksam der Gefahr einer Profilbildung vor. Auch während des Tourverlaufs werden keine an-

wenderspezifischen Daten gesammelt. Die zu einer Sehenswürdigkeit gehörigen Inhalte, die der Server im Tourverlauf anfordert, werden nur durch den Tourbaustein-Identifier bezeichnet. Auf Serverseite ist es daher nicht möglich, eine Anfrage nach einem Tourbaustein einer bestimmten Tour oder einem bestimmten Anwender zuzuordnen.

Sicherheitsinfrastruktur für Urheberschutz

Soll nur der Urheberschutz der Inhalte sichergestellt werden, ist es ebenfalls nicht nötig, den Namen des Nutzers zu erfassen. Im Gegensatz zum vorherigen Fall muss allerdings bei einer Anfrage klar sein, von welchem Gerät die Anfrage stammt, da gerätespezifisch verschlüsselt werden muss. Im DTG wird die SessionID zufällig erzeugt und die damit verbundenen Daten – der öffentliche Geräteschlüssel und Angaben zur Gültigkeitsdauer der Sitzung – erlauben ebenfalls keine Rückschlüsse auf den Anwender. Damit ist der Nutzer auch in diesem Fall anonym. Im Gegensatz zum vorherigen Fall ist es allerdings auf der Serverseite prinzipiell möglich, den Ablauf der Tour nachzuvollziehen. Hier greifen dann die Maßnahmen zur Einschränkung des Speicherns, wie unten beschrieben.

Sicherheitsinfrastruktur für Bezahlmodus

Der Bezahlmodus wird mit denselben Methoden wie der Urheberschutz abgesichert und ist damit in gleicher Weise unkritisch. Es muss aber ein Bezahlschritt vorausgehen. Hier muss unterschieden werden zwischen dem Fall, dass der Anwender ein Leihgerät benutzt und dem Fall, dass er sein eigenes Gerät verwendet. Im ersten Fall wird beim Ausleihen des Geräts vor Ort bezahlt. Der Bezahlvorgang ist damit unabhängig vom DTG. Im zweiten Fall kann sich der Anwender die DTG Software online auf das Gerät laden und muss dann auch online bezahlen und sich entsprechend ausweisen. Dabei muss sichergestellt werden, dass der Bezahlvorgang vom DTG getrennt ist. Insbesondere dürfen der Name und die Kontodaten nicht zusammen mit der SessionID gespeichert werden.

5.2 Eingeschränktes Speichern der Daten

Die zweite beim Entwurf des DTG verwendete Methode besteht darin, Daten nur nach Bedarf und nach Möglichkeit im Zugriffsbereich des Anwenders zu speichern. So werden im DTG die Profil- und Tourdaten grundsätzlich nur auf dem mobilen Endgerät und damit im Zugriffsbereich des Nutzers gespeichert. Bei Beendigung der Tour werden die Daten zum weiteren Schutz vor einer zweckentfremdeten Verwendung vollständig gelöscht. Soweit die Daten derzeit zur Tourberechnung noch vorübergehend im Arbeitsspeicher des Servers zwischengespeichert werden müssen, ist dies aufgrund des fehlenden konkreten Personenbezugs sowie der kurzfristigen Speicherdauer von wenigen Sekunden datenschutzrechtlich vertretbar.

Wie oben dargestellt wäre bei Verwendung einer SessionID der Ablauf der Tour eines Anwenders im Server nachvollziehbar. Es ist aber für die Funktionalität des Systems nicht nötig, tatsächlich abzuspeichern, welche Tourbausteine wann unter einer gegeben SessionID angefordert werden. Entsprechend wird im DTG diese Information auch nicht erfasst: Zu einer gegeben SessionID speichert der Server nur den zugehörigen öffentlichen Geräteschlüssel und gegebenenfalls Angaben darüber, für welchen Rechte bezahlt

wurde. Damit werden also keine Daten über den Tourablauf eines Anwenders erhoben.

5. Fazit

Die Architektur des DTG zeigt, dass durch ein interdisziplinäres Zusammenwirken von Recht und Informatik eine datenschutzkonforme Realisierung von LBS grundsätzlich möglich ist. Indem Fragen und Anforderungen der informationellen Selbstbestimmung bereits auf der Entwicklungsebene in die Architektur einflossen, war es möglich, eine Anwendung zu realisieren, die datenschutzrechtlichen Anforderungen genügt, ohne dabei das Individualisierungserfordernis, wirtschaftliche Interessen des Betreibers oder den Anwendungskomfort auf Nutzerseite zu behindern. Recht und Technik müssen somit nicht im Widerspruch zueinander stehen, sondern können sich in sinnvoller Weise im Sinne einer rechtsgemäßen Technikgestaltung ergänzen.

Literaturverzeichnis

[Gi07] Gitter, R.: Softwareagenten im elektronischen Geschäftsverkehr, Kassel, 2007 i.E.

[GK03] Gola, P.; Klug, C.: Grundzüge des Datenschutzrechts, Beck-Verlag, München, 2003

[GS05] Gola, P.; Schomerus, R.: Bundesdatenschutzgesetz – Kommentar, 8. Auflage, Beck-Verlag, München, 2005.

[HMK05] ten Hagen, K.; Modsching, M.; Kramer, R.: A location aware mobile tourist guide selection and interpreting sights and services by context matching. In: The second annual international conference on Mobile and Ubiquitous Systems: Networking and Services (Mobiquitous 2005), San Diego, California, 2005.

[Ho05] Hornung, G.: Die digitale Identität, Nomos-Verlag, Baden-Baden, 2005.

[JL06] Jandt, S.; Laue, P.: Voraussetzungen und Grenzen der Profilbildung bei Location Based Services, K&R 2006, 316.

[Po72] Podlech, A.: Verfassungsrechtliche Probleme öffentlicher Informationssysteme, DVR 1972/1973, 149.

[Ro93] Roßnagel, A.: Rechtswissenschaftliche Technikfolgenforschung, Nomos-Verlag, Baden-Baden, 1993.

[Ro99] Roßnagel, A.: Datenschutz in globalen Netzen, DuD 1999, 253.

[Ro03] Roßnagel, A.: Datenschutz in Tele- und Mediendiensten. In (Roßnagel, A., Hrsg.): Handbuch Datenschutzrecht, Beck-Verlag, München, 2003.

[RPG01] Roßnagel, A.; Pfitzmann, A.; Garstka, H.-J.: Modernisierung des Dateschutztrechts, Gutachten im Auftrag des BMI, 2001.

[RS00] Roßnagel, A.; Scholz, P.: Datenschutz durch Anonymität und Pseudonymität – Rechts folgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721.

[Sc03] Scholz, P.: Datenschutz beim Internet-Einkauf, Nomos-Verlag, Baden-Baden, 2003.

[Sc03a] Scholz, P.: Datenschutz bei Data Warehousing und Data Mining. In (Roßnagel, A., Hrsg.): Handbuch Datenschutzrecht, Beck-Verlag, München, 2003.

[Si06] Simitis, S., Hrsg.: Bundesdatenschutzgesetz – Kommentar, 6. Auflage, Nomos-Verlag, Baden-Baden, 2006.

[St05] Steidle, R.: Multimedia-Assistenten im Betrieb, Deutscher Universitäts-Verlag, Wiesbaden, 2005.

[Wi00] Wittig, P.: Die datenschutzrechtliche Problematik der Anfertigung von Persönlichkeitsprofilen zu Marketingzwecken, RDV 2000, 59.