VDV Die Verkehrsunternehmen

VDV-Schrift Nr. 430

01/2014

Mobile Kundeninformation im ÖV

Systemarchitektur

Gesamtbearbeitung
Ausschuss für Kundenservice, -information und -dialog (K3),
Fachausschuss für Telematik und Informationssysteme (ATI) und
Unterausschuss „intermodal transport control system" (UA itcs)

Sachbearbeitung
Dipl.-Ing. Berthold Radermacher, VDV, Köln
Dipl.-Ing. (FH) Andreas Wehrmann, VDV, Köln
AK2 des IP-KOM-ÖV Forschungsprojektes

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Das dieser VDV-Schrift zugrundeliegende Vorhaben IP-KOM-ÖV wurde mit Mitteln des Bundesministeriums für Wirtschaft und Energie unter dem Förderkennzeichen 19P10003 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

Bearbeiter im AK 2 des IP-KOM-ÖV Forschungsprojektes:

u. a.:

Dipl.-Inform. Anselmo Stelzer, TU Darmstadt, Darmstadt

M. Sc. Frank Englert, TU Darmstadt, Darmstadt

Dipl.-Inf. Christine Keller, TU Dresden, Dresden

Dipl.-Medieninf. Romina Kühn, TU Dresden, Dresden

Dipl.-Inf. Katja Tietze, TU Dresden, Dresden

Dipl.-Ing. Stephan Hörold, TU Ilmenau, Ilmenau

Dipl.-Medienwiss. Cindy Mayas, TU Ilmenau, Ilmenau

Dipl.-Inform. Günther Gruber, Mentz Datenverarbeitung GmbH, München

Dipl.-Math. Werner Kohl, Mentz Datenverarbeitung GmbH, München

Dipl.-Ing. (FH) Eberhardt Kurtz, SSB AG

Dipl.-Ing. ETH Walter Meier-Leu, Weisskopf Engineering AG, Schaffhausen

Inhaltsverzeichnis

Inhaltsverzeichnis ... 3
Vorwort ... 8
1. Einleitung ... 10
2. Anwendungsbereich ... 11
3. Systemaufbau Grobübersicht ... 11
4. Architektur Portalsystem und umliegende Komponenten ... 15
4.1. Einleitung ... 15
4.2. Personalisierung ... 15
4.2.1. Migrationsfähigkeit des Personalisierungsdienstes ... 15
4.3. Semantik (Modellserver) ... 16
4.3.1. Integrationsfähigkeit semantischer Modelle ... 16
4.4. Push-Dienst ... 19
4.4.1. Systemunabhängigkeit des Push-Dienstes ... 19
4.5. Zugriffskontrolle ... 20
4.5.1. Umsetzungsgrad von Autorisierung und Authentifizierung ... 20
4.5.1.1 Zertifikatbasierte Authentifizierung für Portal Dienste ... 21
4.5.1.2 Rollenbasierte Autorisierung von Kommunikationspartnern ... 21
4.6. Anfragesteuerung im Portalsystem ... 21
4.7. Mobiles Endgerät ... 23
4.7.1. Schnittstelle zum Benutzer ... 23
4.7.2. Technische Schnittstelle zum Mobilen Endgerät ... 23
4.8. Mehrwertdienste ... 23
4.8.1. Integrationsfähigkeit von Mehrwert-Diensten ... 24
5. Dienste (inkl. Detailarchitekturen) ... 27
5.1. Fahrtinformation EKAP - SV2.Fahrtinformation_EKAP ... 28
5.1.1. Zweck ... 28
5.1.2. Interaktionen ... 28
5.1.3. Betroffene Komponenten ... 29
5.1.4. Funktion 1: Fahrgastfahrt mit Haltepunkten anzeigen ... 29
5.1.5. Funktion 2: Fahrzeugpositionen anzeigen ... 29
5.1.6. Funktion 3: Reisezeit anzeigen ... 30
5.1.7. Funktion 4: Fahrzeugdetails anzeigen ... 30
5.1.8. Funktion 5: Streckendetails anzeigen ... 30

5.1.9. Funktion 6: Haltestellendetails anzeigen (nicht genauer spezifiziert) 31
5.1.10. Funktion 7: Auslastung anzeigen 31
5.1.11. Funktion 8: Zuständigkeit ermitteln 31
5.1.12. Funktion 9: Fahrtinformation abonnieren 32
5.1.13. Funktion 10: Abo der Fahrtinformation löschen 32
5.2. Fahrtinformation Fahrzeug - SV2.Fahrtinformation_Fahrzeug 32
5.2.1. Zweck 32
5.2.2. Interaktionen 32
5.2.3. Betroffene Komponenten 33
5.2.4. Funktion 1: Fahrzeug identifizieren 33
5.2.5. Funktion 2: Fahrgastfahrt mit Haltepunkten anzeigen 33
5.2.6. Funktion 3: Fahrzeugpositionen anzeigen 33
5.2.7. Funktion 4: Ankunftszeit anzeigen 34
5.2.8. Funktion 5: Fahrzeugdetails anzeigen 34
5.2.9. Funktion 6: Auslastung anzeigen 34
5.2.10. Funktion 7: Dienste-Auskunft 34
5.2.11. Funktion 8: Fahrgastinnendurchsagen 35
5.3. Haltewunsch – SV2.Haltewunsch 35
5.3.1. Zweck 35
5.3.2. Interaktionen 35
5.3.3. Betroffene Komponenten 35
5.3.4. Funktion 1: Anbieten der Haltewunsch-Option 36
5.3.5. Funktion 2: Senden des Haltewunsches 36
5.4. Personalisierungsdienst – SV2.Personalisierung 36
5.4.1. Zweck 36
5.4.2. Interaktionen 36
5.4.2.1 Werte speichern und abrufen 37
5.4.2.2 Lebenszyklus eines Wertes 39
5.4.2.3 Werteliste ermitteln 39
5.4.3. Betroffene Komponenten: 40
5.4.4. Funktion 1: Speichern eines Werts 40
5.4.5. Funktion 2: Abrufen eines Werts 40
5.4.6. Funktion 3: Löschen eines Werts 40
5.4.7. Funktion 4: Verfügbare Werte auflisten 41
5.5. Verwaltung semantischer Datenmodelle - SV2.Modellverwaltung 41

5.5.1. Zweck 41
5.5.2. Betroffene Komponenten 41
5.5.3. Funktion 1: Auflisten der Modellversionen 41
5.5.4. Funktion 2: Ausliefern einer Modelldatei 41
5.6. Pushdienst – SV2.Pushdienst 41
5.6.1. Zweck 41
5.6.2. Interaktionen 41
5.6.3. Betroffene Komponenten 42
5.6.4. Funktion 1: Mobiles Endgerät für den Pushdienst registrieren 42
5.6.5. Funktion 2: Eine Mitteilung übermitteln 42
5.6.6. Funktion 3: Mobiles Endgerät vom Pushdienst abmelden 42
5.7. Mehrwertdienste - SV2.Mehrwertdienste 43
5.7.1. Zweck 43
5.7.2. Interaktionen 45
5.7.3. Betroffene Komponenten 45
5.7.4. Funktion 1: Datenerhebung 46
5.7.5. Funktion 2: Datensicherung und -verwaltung 46
5.7.6. Funktion 3: Datenübertragung 46
5.7.7. Funktion 4: Meldungen an Fahrgast 46
5.7.8. Funktion 5: Anbindung an geräteexterne Dienste 47
5.8. EKAP-Registerdienst – SV2.EKAPRegisterdienst 47
5.8.1. Zweck 47
5.8.2. Interaktionen 47
5.8.3. Betroffene Komponenten: 48
5.8.4. Funktion 1: Registrieren einer EKAP 48
5.8.5. Funktion 2: Aktualisieren einer EKAP 48
5.8.6. Funktion 3: Löschen einer EKAP 49
5.8.7. Funktion 4: Liste der EKAPs abrufen 49
5.9. Anfragesteuerungsdienst - SV2. Anfragesteuerung 49
5.9.1. Zweck 49
5.9.2. Interaktionen 49
5.9.3. Betroffene Komponenten 50
5.9.4. Funktion 50
5.10. Physikalische Ortung - SV2.Physikalische_Ortung 50
5.10.1. Zweck 50

5.10.2. Interaktionen 50
5.10.3. Betroffene Komponenten 50
5.10.4. Funktion 1: Abfrage der Positionierung 50
8. Abkürzungen 55
9. Abbildungsverzeichnis 57
10. Tabellenverzeichnis 59
Anhang 60
Anhang I. Normativ 60
Anhang II. Informativ 60
A II.1 Pushdienste 60
A II.1.1. Proprietäre Pushdienste 60
A II.1.2. Apple Push Notification Service (APNs) 61
A II.1.3. Registrierung von mobilen Endgeräten 62
A II.1.4. Registrierung des Providers 62
A II.1.5. Benachrichtigung von Interessenten und Abruf von Daten 63
A II.1.6. Abmeldung von Benachrichtigungen 64
A II.1.6.1. Google Cloud to Device Messaging (C2DM) 64
A II.1.7. Fazit 64
A II.2 Sonstige Systeme für Personalisierungsdaten 65
A II.2.1. Generelle Bemerkungen 68
A II.2.2. Fazit 68
A II.3 Schnittstelle zwischen mobilen Kundenendgerät und Fahrzeug 70
A II.3.1. Technische Realisierung der Schnittstelle zum mobilen Endgerät 70
A II.3.2. Machbarkeitsbetrachtung der Verbindung mit dem Fahrzeug-W-LAN 71
Benennung und Auswahl der SSID im Fahrzeug 71
Fahrzeugspezifische Benennung von SSIDs 71
Einheitliche Benennung der SSID 72
A II.3.3. Beschreibung der Problemstellung 73
Lösungsansatz bei einheitlicher SSID 73
Lösungsansatz für ein Ad-Hoc-Netzwerk zwischen Fahrzeugen 74
Identifikation des Fahrzeuges, in dem sich der Fahrgast aufhält 75
Kommunikation zwischen dem Fahrgast und dem jeweiligen Fahrzeug 77
Machbarkeitsbetrachtung im Rahmen von IP-KOM-ÖV und Fazit 77
Verbindungsaufbau aus Nutzersicht 78

Fazit **81**

A II.3.4. Parallele Nutzung von Fahrzeug-W-LAN und Internet **81**

Vorwort

Auf Initiative des VDV und gefördert durch das BMWi begann im September 2010 das Forschungs- und Standardisierungsprojekt

Internet Protokoll basierte Kommunikationsdienste im öffentlichen Verkehr (IP-KOM-ÖV).

Das Projekt wird von 14 Partnern aus Industrie, Universitäten und Verkehrsunternehmen getragen. Es dient der Erarbeitung moderner Kommunikationskonzepte für die umfassende und kontinuierliche Fahrgastinformation.

Eine umfassende Fahrgastinformation stellt heutzutage ein entscheidendes Wettbewerbsmerkmal im öffentlichen Personenverkehr dar, nicht nur im Vergleich mit anderen Verkehrsunternehmen sondern auch im Vergleich zum Individualverkehr.

Bereits heute ist es üblich, dass Verkehrsunternehmen ihre Fahrgäste nicht nur über die geplanten Fahrten informieren, sondern auch Echtzeitinformationen, z. B. zu Verspätungen, Störungen oder Fahrtzieländerungen, bereitstellen. Diese Informationen werden zum einen über öffentliche Anzeiger bzw. Ansagen in Fahrzeugen oder an Haltestellen allen dort befindlichen Personen zur Verfügung gestellt. Zum anderen lassen sich solche Informationen mit speziellen Applikationen oder über Web-Angebote individuell abfragen.

Bislang ist es aber nicht möglich, Fahrgäste im öffentlichen Verkehr direkt mit Informationen zu ihrer persönlich relevanten Fahrt zu versorgen, den Fahrgast also auch im Störungsfall mit Hilfe des öffentlichen Verkehrs auf dem schnellsten Weg zu seinem Ziel zu führen.

Die weit verbreiteten Smartphones und Tablets bieten hierfür vielfältige Möglichkeiten und ermöglichen eine hohe Akzeptanz der Benutzer. Die Informationsübertragung erfolgt dabei IP-basiert und sollte bevorzugt zwischen einem zentralen Informations-Server und dem Kundenendgerät erfolgen. Für den Fall, dass der zentrale Datenserver nicht erreichbar ist, sollte auch eine Kommunikation zwischen Kundenendgerät und Fahrzeug möglich sein.

Das Forschungs- und Standardisierungsprojekt IP-KOM-ÖV arbeitet deshalb an drei Schwerpunkten (vgl. Abbildung 1).

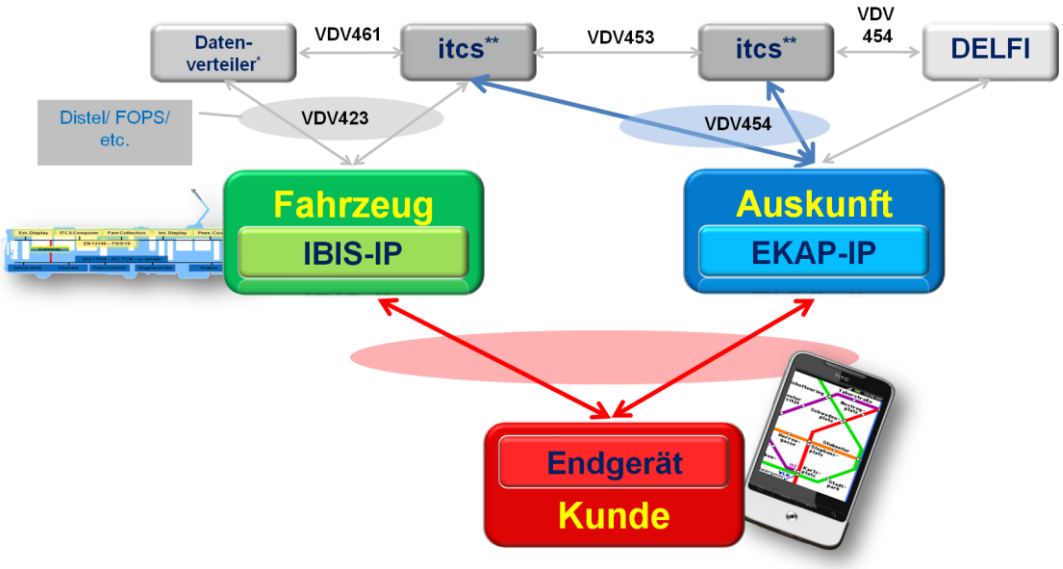

Abbildung 1: Umfeld und Schwerpunkte im Projekt IP-KOM-ÖV

Erster Schwerpunkt (grün in Abbildung 1) ist die Spezifikation eines performanten IP-basierten Kommunikationsprotokolls im Fahrzeug (IBIS-IP). Dabei geht es zum einen darum, den gewachsenen Bedürfnissen der Fahrgastinformation gerecht zu werden und zum anderen um die Definition einer IP-basierten Schnittstelle zur Übertragung der Informationen vom Fahrzeug zum mobilen Kundenendgerät. Hierzu wird der in den achtziger Jahren entwickelte IBIS-Wagenbus aus der VDV-Schrift 300 auf eine moderne Ethernet-Informationsarchitektur umgesetzt.

Zweiter Schwerpunkt (rot in Abbildung 1) ist die individuelle Fahrgastinformation unter Verwendung mobiler Geräte des Fahrgastes (Smartphones, Tablet-PC u. ä.) Hierzu wurden im ersten Schritt die Bedürfnisse von Fahrgästen zu individuellen Informationen ermittelt. Im zweiten Schritt werden einheitliche Schnittstellen zwischen der Echtzeit-Kommunikations- und Auskunftsplattform (EKAP) und den mobilen Kundenendgeräten bzw. zwischen der EKAP und den Hintergrundsystemen entwickelt. Hierbei werden ausschließlich die Datenmodellierungen und Architekturen erforscht und spezifiziert. Aufbauend auf diesen Datenmodellierungen werden semantische Modelle erarbeitet, die helfen, die Fahrgastinformationsdaten für Kommunikationsdienste auf Basis von innovativen Technologien des Semantic Web zur Verfügung zu stellen. Die Entwicklung einer Applikation für mobile Endgeräte ist ausdrücklich nicht vorgesehen.

Dritter Schwerpunkt (blau in Abbildung 1) ist die Definition und Schaffung einer Echtzeit-Kommunikations- und Auskunftsplattform (EKAP). Die EKAP bündelt Informationen von itcs- und anderen Auskunfts- und Informationssystemen und stellt die Vielzahl an Informationen über geeignete Schnittstellen den Applikationen auf den Kundenendgeräten zur Verfügung. Diese Plattform ermöglicht es, Kunden dynamisch mit individuellen Störungsmeldungen versorgen zu können.

Neben den Forschungsarbeiten ist die Standardisierung der Ergebnisse ein wesentliches Ziel des Projektes, um eine nachhaltige Nutzung zu gewährleisten.

Darüber hinaus wird die Praxistauglichkeit dieses neuen Standards in Labor- und Feldtests verifiziert.

1. Einleitung

Der Ausschuss für Kundenservice, -information und -dialog (K³) und der Unterausschuss „intermodaltransport control system“ (UA itcs) im Ausschuss für Telematik und Informationssysteme (ATI) begleitet und unterstützen die Arbeiten von IP-KOM-ÖV und den Entwicklungsprozess für die betrieblichen Anforderungen an die Kundeninformation.

Das Hauptziel dieser Schrift ist es, die Architektur und die Schnittstellen als Basis für eine individualisierte und schnelle Bereitstellung von ÖV- und Störungsinformationen zu definieren und zu entwickeln. Ein essentieller Bestandteil ist dabei die Echtzeit Kommunikations- und Auskunftsplattform EKAP. In ihr werden alle Informationen, die für die individuelle Begleitung des Fahrgastes notwendig sind, gebündelt. Zur Ermittlung aller für den Fahrgast notwendigen Informationen wurden anhand einer Analyse, stereotypisch die Bedürfnisse anhand sieben Personas und 19 Szenarien ermittelt (vgl. VDV-Mitteilung 7023). Aufbauend auf diesen Ergebnissen wurden die möglichen Störungs- und Informationssituationen in einen Katalog aus Anwendungsfällen zusammengetragen und in Relation zu den beteiligten Systemen und Nutzern gesetzt. Hierdurch wurden die Informationswege sowie die beteiligten Stellen bzw. Personen ermittelt. Basierend auf diesen Katalog werden nun in dieser Schrift die dazugehörigen funktionalen Systemarchitekturen definiert die notwendig sind um den Kunden umfassend und dynamisch zu informieren.

Auf Basis einer Dienstorientierten Architektur (engl. Service oriented Architecture -SOA) werden gekapselte Funktionseinheiten spezifiziert, die eine standardisierte Systemarchitektur für ein sogenanntes Protalsystem definieren. Diese Schrift soll daher bei Ausschreibungen und der homogenen Umsetzung der Schnittstellen helfen. Denn betrachtet man die Prozesse die notwendig sind um ein Smartphone mit Daten zu versorgen, so wird schnell klar, dass die Systemlandschaft sehr heterogen gestaltet ist. Herstellerspezifische Schnittstellen und Kommunikationstechniken auf Seiten der Betriebssystemhersteller moderner Smartphones stellen dabei besondere Hürden für die Definition einheitlicher Schnittstellen dar. Daher war es eine besondere Herausforderung eine ÖV-spezifische Schnittstelle in die Systemlandschaft der „mobile Apps“ zu integrieren. Das Portalsystem, das die sich in den Hintergrundsystemen befindliche, eng mit dem Betriebssystem der Smartphones verzahnte Serverseite darstellt, ermöglicht neben Ad-Hoc Nachrichten (sog. „Push-Notifications“), auch eine Vielzahl weiterer Dienste im Sinne der SOA. Das zurückgriffen auf nationale und europäische Standardschnittstellen gewährleistet hierbei eine standardkonforme Erweiterung der bereits bestehenden Datenwege.

2. Anwendungsbereich

Die zunehmenden Abfragen von ÖV-Informationen durch internetfähige mobile Endgeräte stellen immer weitere Anforderungen an die Schnittstellen der Verkehrsunternehmen. Die derweil verfügbaren Schnittstellen bieten dem Fahrgast lediglich durch den Betrieb und die Disposition erzeugte Informationen an. Einheitliche Schnittstellen oder Informationen sind allenfalls regional begrenzt oder als proprietäre Schnittstellen der Systemanbieter verfügbar. Immer mehr sehen sich die Fahrgäste jedoch auch mit inkonsistenten Daten konfrontiert, sowie einer Flut an verfügbaren Apps. Die Chance, Zugangshürden zum ÖV über dieses Medium abzubauen, scheitert bereits bei der Bezugsquelle der „richtigen“ App.

Es wird eine serviceorientierte Architektur spezifiziert, die eine Integration verschiedener Kommunikationsdienste zu Fahrgastinformationsdiensten auf mobilen Endgeräten ermöglicht. Ein wichtiges Kriterium für die Praxistauglichkeit ist die modellbasierte Beschreibung der Kommunikationsdienste. Das serviceorientierte Konzept soll insbesondere auch die Kombination von Diensten unterschiedlicher Anbieter ermöglichen. Auch für Dienste von ÖV fernen Anbietern sollen diese Kommunikationsdienste verwendet werden können, um auf dieser Basis, zukunftsweisende Hilfen zu ermöglichen.

3. Systemaufbau Grobübersicht

Unter dem Gesamtkontext des ÖV-Systems wurde die zunächst dezentral entwickelte Architektur als Grobarchitektur in dem folgenden Bild zusammengebracht. Als oberstes Ziel galt hier eine SOA aufzubauen, sodass sich in dieser Darstellung logische Komponenten wiederfinden, die aufbauend auf den Anforderungen von VDV 3001, VDV 7023 und VDV 7025 definiert wurden. Die folgende Abbildung zeigt das geschaffene System mit seiner Einbettung in die reale ÖV-Systemlandschaft. Auch wenn sich diese Schrift nur mit einem Teilbereich des ÖV-Systems befasst, so hilft diese Vogelperspektive dem Verständnis der Zusammenhänge zwischen den Entitäten und deutet die nicht im Diskusions-Fokus liegenden Komponenten mit einer grauen Schattierung an. Zu der Entwicklung einer Dienste-basierten Architektur gehören selbstverständlich auch Schnittstellen zwischen den Systemen. Hierzu werden bereits vorhandene Schnittstellen wie VDV 453/454/452 verwendet jedoch auch notwendige neue Schnittstellen spezifiziert.

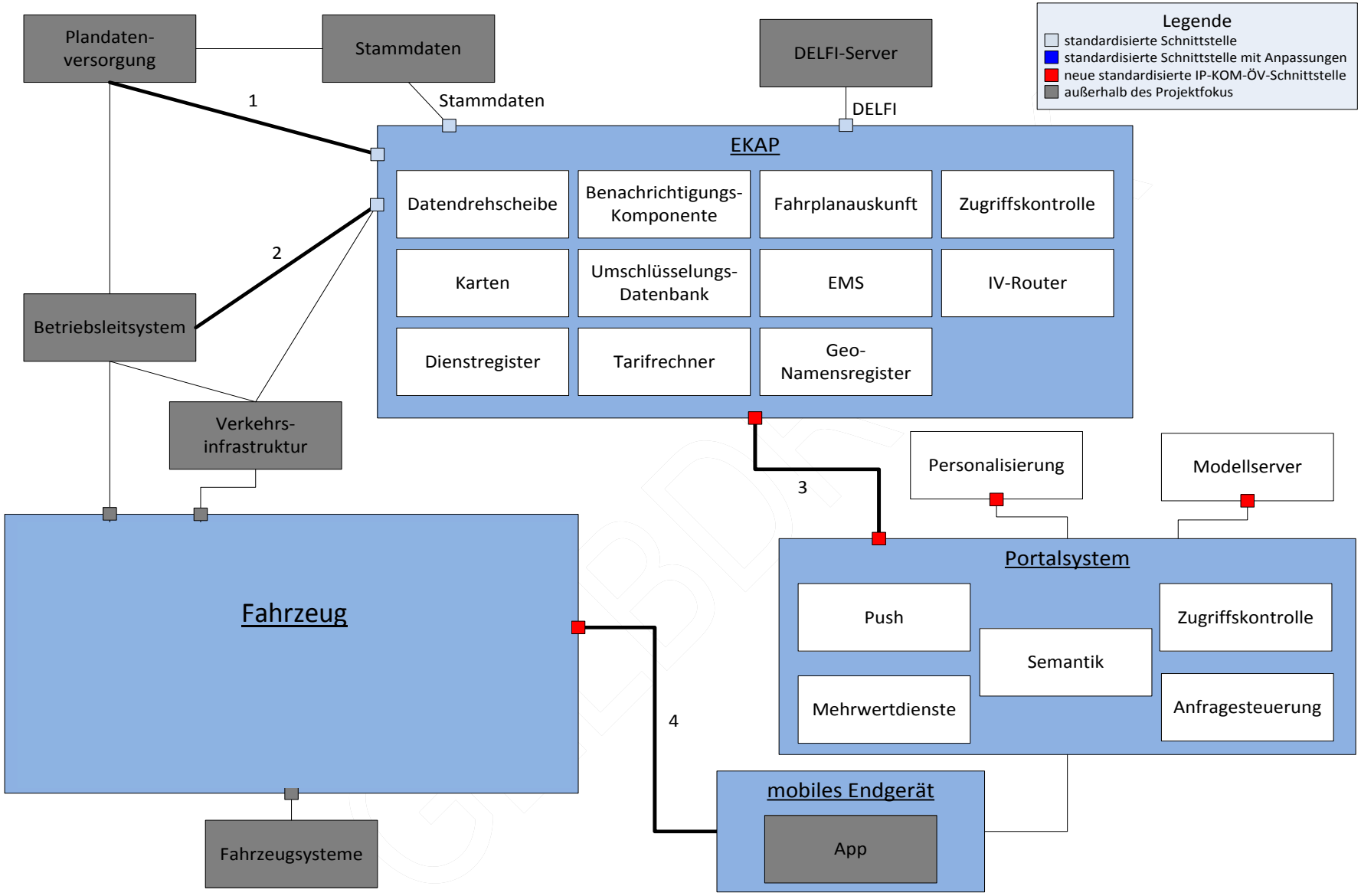

Abbildung 2: Grobarchitektur ÖV-Umfeld

Kurzerläuterungen:

Komponente	**Beschreibung**
App	Eine mobile Applikation, die das System nutzt.
Betriebsleitsystem	Das Betriebsleitsystem (itcs) fasst alle Einrichtungen zusammen, die für die Überwachung und Steuerung des Fahrbetriebs erforderlich sind. I. d. R. beinhaltet das itcs eine Vielzahl von Unterkomponenten.
DELFI-Server	DELFI stellt der EKAP die Funktionalitäten des DELFI-Verbundes zur Verfügung. So kann eine EKAP z. B. auf die verteilte Verbindungssuche über mehrere Landesauskunftssysteme hinweg zugreifen.
Fahrzeugsysteme	Hierbei handelt es sich um die Schnittstelle zum jeweiligen Fahrzeug-Chassis.
Verkehrsinfrastruktur	Beinhaltet hier Aspekte wie die Fahrwegsteuerung, Haltestellen, etc.
Planungsdatenversorgung	Soll-Fahrplandaten, Fahrzeugumläufen, Dienstpläne, etc.
Stammdaten	Datenversorgung mit selten ändernden Daten (Haltestellendaten o. ä.)
Portalsystem	Vermittlungsschicht zwischen dem mobilen Endgerät und der EKAP. Die Schnittstelle wird innerhalb dieser Schrift standardisiert.
EKAP-Register	Datenbank mit bekannten EKAP-Adressen.
Mehrwertdienste	Zusammenfassung von zusätzlichen Funktionen, die durch diese Architektur flexibel angebunden werden können, z. B. Socialmedia.
Mobiles Endgerät	Das mobile Endgerät ist das persönliche Gerät des Fahrgastes. Es kann sich hierbei um Smartphones, aber auch Tablet-PCs, Laptops oder ähnliche mobile Geräte handeln.
Modellserver	Ermöglicht es Diensten, sich die aktuellen Versionen des Klassifikations- und Interaktionsmodells sowie des Kontextmodells anzeigen zu lassen und liefert die Modelldateien auf Anfrage aus.
Personalisierung	Standardisierte Datenbank, auf der personenbezogene Attribute des Benutzers in einem Standard Datenbankformat hinterlegt werden können.
Push	Ermöglicht eine ereignisgesteuerte Mitteilung an das Endgerät.
Semantik	Verknüpfung der drei Modelle Interaktionsmodell, Klassifikationsmodell und Interaktionsmodell.
Zugriffskontrolle	Fasst die Mechanismen für die Autorisierung und Authentifizierung zusammen.
EKAP	Echtzeit-Kommunikations- und Auskunftsplattform. Verfügt über eine standardisierte Schnittstelle zum Portalsystem. Es werden darüber hinaus Anforderungen an die datenversor-

	genden Schnittstellen definiert.
Benachrichtigungs-Komponente	Entgegennahme von Abonnements der Benutzer aus dem Portalsystem und der Benachrichtigung dieser über neue vorliegende Ereignisse, für die sie sich eingeschrieben haben.
Datendrehscheibe	Eine bereits heute vorhandene Datenvermittlungsschicht für den Austausch von Informationen über Verkehrsunternehmen oder Auskunftsplattformen hinweg.
Diensteregister	Verzeichnis der Dienste, die diese EKAP anbieten und nutzen. Für jeden registrierten Dienst werden definierte Merkmale festgehalten.
EMS	Ein Ereignis-Management-System kann für folgende Aufgabenstellungen herangezogen werden: • Erfassen von Störungs- und Ereignismeldungen • Verfeinern bestehender Meldungen • Konvertieren von Meldungen in andere Formate • Weiterleitung von Meldungen an andere Systeme
Fahrplanauskunft	Beauskunftung von Reisewünschen auf Basis der Solldatenlage ggf. unter Berücksichtigung der Istdatenlage.
Geo-Namensregister	Beinhaltet Informationen zu verschiedenen geografischen Ortsobjekten, was typischerweise Haltestellen, Adressen und POIs umfassen kann.
IV-Router	Berechnet Routen des Individualverkehrs auf dem öffentlichen Straßen- bzw. Wegenetz.
Karten	Generiert für einen gegebenen Kartenausschnitt eine Karte in Bildform und hält hierzu die erforderlichen Kartendaten vor.
Tarifrechner	Berechnet zu einer bestimmten Verbindungsauskunft die Kosten für die Fahrscheine für die gesamte Verbindung oder Teile der Verbindung und gibt in Frage kommende Tarifinformationen oder Fahrscheine zurück.
Umschlüsselungsdatenbank	Speichert für einzelne Objekte Zuordnungen von verschiedenen Schlüsseln (Objekt-Identifikatoren, IDs). So ist es möglich, ein Objekt, welches in einem bekannten Schlüsselsystem identifiziert wurde, in ein anderes Schlüsselsystem zu transferieren. Dies ist notwendig, wenn Systeme (mehrere EKAPs) miteinander kooperieren sollen, die unterschiedliche Schlüsselsysteme verwenden.
Zugriffskontrolle	Fasst die Mechanismen für die Autorisierung und Authentifizierung zusammen.
Verbindungen	
1	Kommunikationsweg lässt sich durch die VDV-Schrift 452 und NeTEx beschreiben.
2	Hier kommen die Standards VDV453/454 und SIRI SX, SIRI FM zum Tragen. An diese Standards werden aus der VDV-Schrift 431-1 heraus noch weitere Anforderungen festgelegt.
3	Diese Übertragungsstrecke wird in der VDV-Schrift 431-2 schnittstellenseitig standardisiert.

4	Für diesen Übertragungsweg zwischen Fahrzeug und dem mobilen Gerät des Fahrgastes stellt diese Schrift Anforderungen an die IP-Fähigkeit.

Tabelle 1: Erläuterungen zur Grobarchitektur

Ohne an dieser Stelle näher auf die Komponenten einzugehen, sei klargestellt, dass dieses Schaubild eine „durchschnittliche“ Variante eines solchen Gesamtsystems darstellt. Vielfach sind sicher auch die internen sowie externen Komponenten zusammenfassbar. Denkbar ist außerdem eine Vielzahl von Varianten mit lediglich nur vereinzelten oder weiteren, aus dem System herausgelösten, Komponenten. Hier wird es sicherlich einen längeren Migrationszeitraum geben, sodass zukünftig keine einheitliche, jedoch VDV 430-konforme Architektur entstehen wird.

Die Komponenten selbst beschreiben in ihrer Eigenschaft die Konsolidierung von Diensten, auf deren Basis die Kommunikation innerhalb der Systeme und nach außen definiert wird. Hierbei gibt es selbstverständlich viele unterschiedliche Ausprägungen, so: kann es durchaus sein, dass eine Komponente lediglich einen Dienst kapselt.

Auf Kommunikationswege innerhalb der Systeme (IBIS-IP/Portalsystem/EKAP) wurde in dieser Darstellung bewusst weitestgehend verzichtet, da diese sich auf verschiedenste Art und Weise ausprägen können und erst mit den Diensten endgültig definiert und somit nach außen transparent werden.

4. Architektur Portalsystem und umliegende Komponenten

4.1. Einleitung

Im Weiteren werden die wesentlichen Komponenten des hier betreffenden Portalsystems definiert. Hierbei werden auch bereits Hinweise zur möglichen praktischen Umsetzung gegeben sowie auf wissenschaftliche Analysen im Anhang verwiesen. Selbstverständlich hilft hierbei die Kenntnis der begleitenden VDV-Schriften 431/301/etc.

4.2. Personalisierung

Diese Komponente verwaltet personalisierte Konfigurationsdaten beliebiger anderer Komponenten. Konfigurationsdaten sind dabei beliebige benutzerbezogene Informationen, die das Verhalten jener Komponenten beeinflussen. Die Funktionen zur Verwaltung der Daten werden standardisiert zur Verfügung gestellt.

Nicht in der standardisierten Schnittstelle enthalten, aber anbieterspezifisch möglich, sind Funktionen zur Kopplung von Daten an bestimmte Komponenten sowie zur benutzerübergreifenden Administration der Daten.

Bestehende CRM-Systeme können ausgebaut werden, um in konformen Systemen die Rolle dieser Komponente zu übernehmen. Die ohnehin im CRM-System vorhandenen Kundendaten (zum Beispiel Kontaktinformationen für Benachrichtigungen) können dazu auch über die Schnittstelle des Personalisierungsdienstes zur Verfügung gestellt werden.

4.2.1. Migrationsfähigkeit des Personalisierungsdienstes

Im Personalisierungsdienst ist definiert, dass in Verbindung mit Benutzerkonten Daten gespeichert werden können. Diese Daten werden in Form von Schlüssel-Wert-Paaren vorgehalten, sodass einzelne Datenwerte über ihren Schlüssel zugreifbar sind. Dieser Datenspeicher kann von beliebigen anderen Diensten – beispielsweise Mehrwertdiens-

ten – verwendet werden, um Benutzereinstellungen und Ähnliches dauerhaft abzulegen und zu einem späteren Zeitpunkt wieder abzurufen.

Durch die Ablage in Form von Schlüssel-Wert-Paaren wird eine maximale Erweiterbarkeit gewährleistet, da beliebige Dienste Daten unter ihren eigenen Schlüsseln ablegen können. Bei geeigneter – den Diensten überlassener – Wahl der Schlüssel kann die Gefahr von Schlüsselkollisionen minimiert werden (beispielsweise, wenn unter anderem Name und Hersteller/Anbieter des Dienstes Teil des Schlüsselnamens sind). Gleichermaßen sind Dienste nicht in der Strukturierung ihrer Daten eingeschränkt, da das Format der Werte frei wählbar ist und es Diensten auch freisteht, mehrere Werte abzulegen. Der Personalisierungsdienst ist somit auf die vorgesehene Systemarchitektur hin optimiert, da dem Hersteller und Anbieter einer Personalisierungskomponente nicht bekannt sein muss, welche anderen Dienste, die den Personalisierungsdienst möglicherweise verwenden könnten, noch existieren oder vom Benutzer eingesetzt werden.

Im Anhang A II.2 befindet sich eine Analyse, die aufbauend auf vorhandenem CRM-Systemen eine mögliche Eingliederung in die vorgestellte Systemarchitektur ermöglicht.

4.3. Semantik (Modellserver)

Modellserver stellen die semantischen Datenmodelle, namentlich das Klassifikations- und Interaktionsmodell sowie das Kontextmodell zur Verfügung. Hierzu muss ein Modellserver mindestens eine Liste der verfügbaren Modellversionen (arten der verfügbaren semantischen Komponenten) zur Verfügung stellen, sowie diese als Datei ausliefern können. Ein Modellserver kann weitere Funktionen zur Verfügung stellen, beispielsweise die Auslieferung von Modellfragmenten. Der Modellserver in seiner schlankesten Variante kann die verfügbaren Modelle inklusive ihrer Versionen und Dateinamen auflisten. Jede dieser Modelldateien kann der Modellserver dann auf Anfrage ausliefern. Die Umsetzung dieser Funktionen ist die Minimalanforderung an jeden Modellserver. Darüber hinaus ist in dieser Minimalkonfiguration ein Pull-Schema zu implementieren. Betroffene Dienste und Komponenten (so beispielsweise auch weitere Modellserver) müssen von sich aus nach aktualisierten Modellen anfragen und diese bei Bedarf vom Modellserver herunterladen. Weitere Ausbaustufen des Modellservers sind in jedem Fall möglich.

4.3.1. Integrationsfähigkeit semantischer Modelle

Die semantischen Technologien wurden innerhalb der letzten Jahre verstärkt in der Praxis eingesetzt. Die zweite Generation von Standards für die semantische Modellierung und den Zugriff auf semantische Daten wird von einer Vielzahl an ausgereiften Frameworks und Werkzeugen unterstützt. Ein Beispiel für ein solches Framework ist das Jena Framework, das mittlerweile als Apache Open Source Projekt entwickelt wird (http://jena.apache.org/). Es bietet verschiedene Bibliotheken für Java zur Entwicklung semantischer Software, beispielsweise eine API für das Schreiben und Lesen von RDF-Daten in verschiedenen Formaten (http://jena.apache.org/documentation/rdf/). Zur Speicherung von semantischen Daten gibt es verschiedene ausgereifte Triple-Stores, ebenfalls im Rahmen des Jena Frameworksoder (http://jena.apache.org/documentation/tdb/) Sesame (http://www.openrdf.org/).

Es sind verschiedene Funktionalitäten nötig, um ein Portalsystem semantisch zu unterstützen. Hierzu gehören zunächst ein oder mehrere Modellserver, die die semantischen Modelle an die Komponenten ausliefern können, die sie benötigen. Die Verarbeitung semantischer Daten, ihre Interpretation, das automatische Schlussfolgern (Inferenz) und darauf aufbauend die Veranlassung entsprechender Reaktionen wird in der Semantik-Komponente gekapselt dargestellt. Diese Komponente, oder auch Teile davon, können

entweder im Portalsystem oder in der Applikation der Anwendung realisiert werden, wie in den Abbildungen Abbildung 3 und Abbildung 4 dargestellt. Weiterhin wird eine Annotationskomponente nötig, die die Daten der Schnittstelle zwischen EKAP und Portalsystem semantisch annotiert.

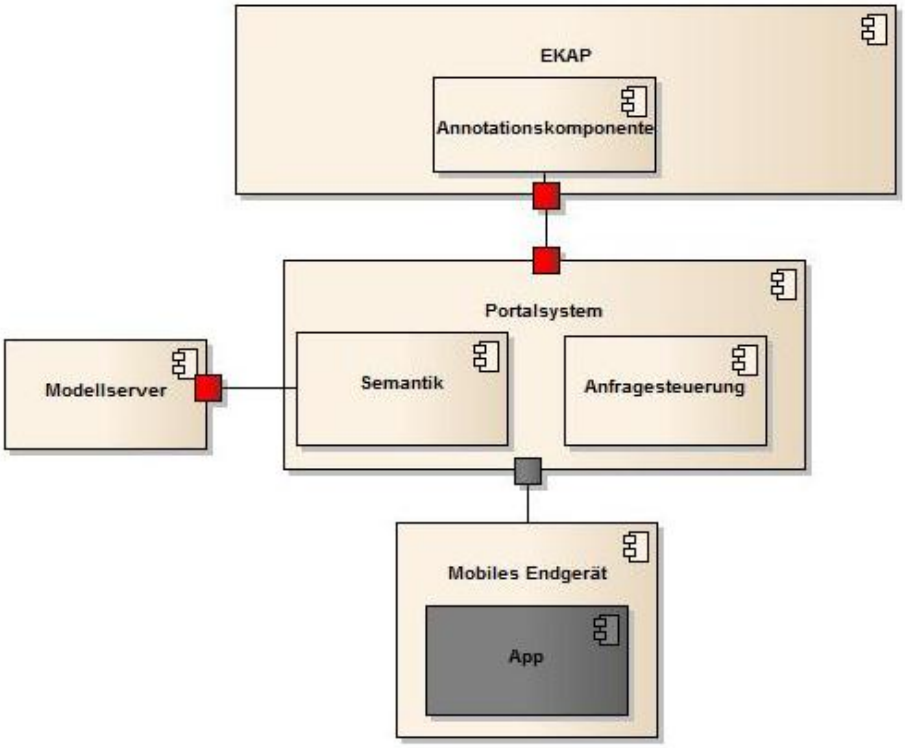

Abbildung 3: Architekturdiagramm Semantik-Komponente im Portalsystem

Die vorgegebene Schnittstelle des Modellservers besteht in einem Dienst. Dieser Dienst spezifiziert zwei Funktionen:

- eine Auflistung von Modellversionen, die der Server vorhält und
- die Funktion der Auslieferung einer angeforderten Modelldatei.

Diese Funktionalität lässt sich mit jeder Art Webserver umsetzen. **Ein Modellserver ist daher mit aktueller Technologie problemlos umsetzbar**.

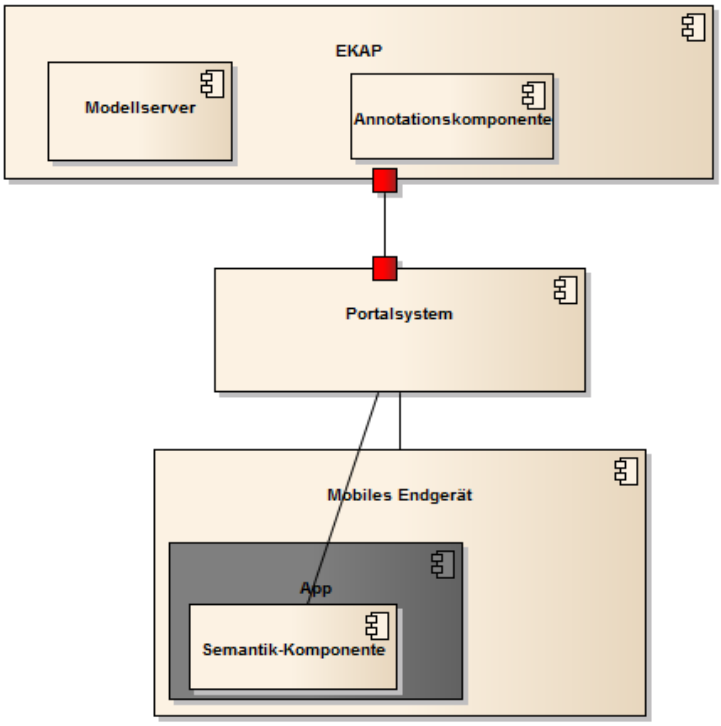

Abbildung 4: Semantik-Komponente im mobilen Endgerät

Die Annotationskomponente liefert die semantisch annotierten Schnittstellendaten, das heißt, sie reichert die Schnittstellendaten um semantische Information an. Der Umfang einer Annotationskomponente kann stark variieren. So können beispielsweise einfache Mapping-Tabellen bereits zur Annotation von Daten genutzt werden.

Der Annotationskomponente muss es möglich sein, all diejenigen Schnittstellendaten semantisch aufzubereiten, die für die jeweils geplanten semantisch aufgewerteten Kommunikationsdienste nötig sind. Dies können die Daten einer einzelnen Komponente der EKAP sein, beispielsweise die Daten der Fahrplanauskunft. In diesem Fall sollte die Annotationskomponente direkt an die Schnittstelle dieser betroffenen Komponente gesetzt werden. Je nach Umsetzung der EKAP und des jeweiligen Portalsystems sind verschiedene Einsatzmöglichkeiten einer oder auch mehrerer möglicher Annotationskomponenten denkbar. So ist beispielsweise die Implementierung einer Annotationskomponente als Teil der Anfragesteuerung möglich, die alle eingehenden Daten der EKAP behandelt.

Die Semantik-Komponente verwendet

- die Daten des Modellservers,
- die durch die Annotationskomponente annotierten EKAP Daten sowie
- optionale externe semantische Datenquellen.

Sie erweitert das Portalsystem damit um die Fähigkeit, semantische Anfragen zu verarbeiten.

Für die Funktionalitäten, die in der Semantik-Komponente gekapselt werden, werden keine festen Architektur-Komponenten vorgegeben. Es ist denkbar, verschiedene Funktionen auch als Erweiterung bestehender Komponenten umzusetzen. Da dies keine Schnittstelle, sondern nur Funktionalität betrifft, sind die Portalsystembetreiber und Applikationsentwickler nicht eingeschränkt. Es kann eine zentrale Semantik-Komponente umgesetzt werden, die diese Funktionalität bündelt. Die Implementierung verschiedener

Semantik-Dienste ist allerdings ebenso möglich. Die Verarbeitung semantischer Schnittstellendaten, die Inferenz und darauf aufbauende Funktionalität sind daher ohne weiteres machbar und umsetzbar, wenn semantisch annotierte Schnittstellendaten verfügbar sind. Durch die Verwendung von standardisierten semantischen Formaten für die Darstellung der Modelle und der Annotationen können externe Datenquellen und semantische Dienste problemlos in die Semantik-Komponente integriert werden. Externe semantische Dienste können über die Komponente „Mehrwertdienste“ im System verfügbar gemacht werden.

4.4. Push-Dienst

Diese Komponente kapselt die Abstraktion verschiedener proaktiver (Push-) Benachrichtigungsmechanismen, die bei unterschiedlichen Betriebssystemen der mobilen Endgeräte eingesetzt werden. Dieser sogenannte Push-Dienst ermöglicht es erstmals, den Benutzer des öffentlichen Verkehrs aktiv mit aktuellen Daten zu versorgen. Eine solche Funktionalität ist dabei eng mit dem Zielsystem (Smartphone Betriebssystem) verzahnt. Die Umsetzung in einem Push-Dienst zeigt die Systemunabhängigkeit, im Besonderen bei der Verwendung der Push-Dienste externer Stellen, wie sie von Apple oder Google angeboten werden.

4.4.1. Systemunabhängigkeit des Push-Dienstes

Bei der Realisierung einer aktiven Benachrichtigung bestehen zwei technische Herausforderungen. Zum einen ist das Ansprechen eines mobilen Endgerätes über das öffentliche Telekommunikationsnetz nicht möglich, auch wenn jedes Gerät nach außen über eine IP-Adresse verfügt. Dies liegt im Paradigma begründet, dass ein Server nur auf die Anfrage eines Clients (Mobilgerät) antworten, jedoch keine eigene Anfrage an einen Client absetzen kann. Zur Lösung dieses Problems entwickelten die Hersteller der Betriebssysteme für mobile Endgeräte spezielle Push-Dienste, die es erlauben, dennoch eine Nachricht an das jeweilige Endgerät zu schicken. Diese Lösungen bedienen sich der Möglichkeit, aufbauend auf einer Anfrage durch den Client einen Rückkanal für Antworten aufzubauen und offen zu halten. Diese Dienste sind proprietär, können jedoch von der Öffentlichkeit in Anspruch genommen werden.

Das zweite Problem ist die Tatsache, dass je nach Betriebssystem des mobilen Endgerätes des Nutzers ein anderer herstellerspezifischer Push-Dienst verwendet werden muss, um eine entsprechende Benachrichtigung auszuliefern. Je nach Betriebssystem müssen verschiedene Routineabläufe durchgeführt werden. Der Push-Dienst kapselt die Geschäftslogik und bietet nach außen jeder EKAP sowie anderen Diensten die Möglichkeit, einen Endgerätbenutzer über das Vorliegen aktueller Informationen zu informieren. Ein solcher Dienst (beziehungsweise die jeweilige gekapselte Funktionalität für das entsprechende Betriebssystem, das die Daten an die Interessenten verteilen möchte) wird im Nachfolgenden als Provider bezeichnet. Der eingeführte Push-Dienst befindet sich außerhalb einer EKAP und kann nicht Teil eines mobilen Endgerätes sein, da er andernfalls nicht von außerhalb angesprochen werden kann. Deshalb ist ein Portalsystem notwendig, das durch die Umsetzung des Push-Dienstes als eine Art Bindeglied zwischen der EKAP und dem mobilen Endgerät fungiert.

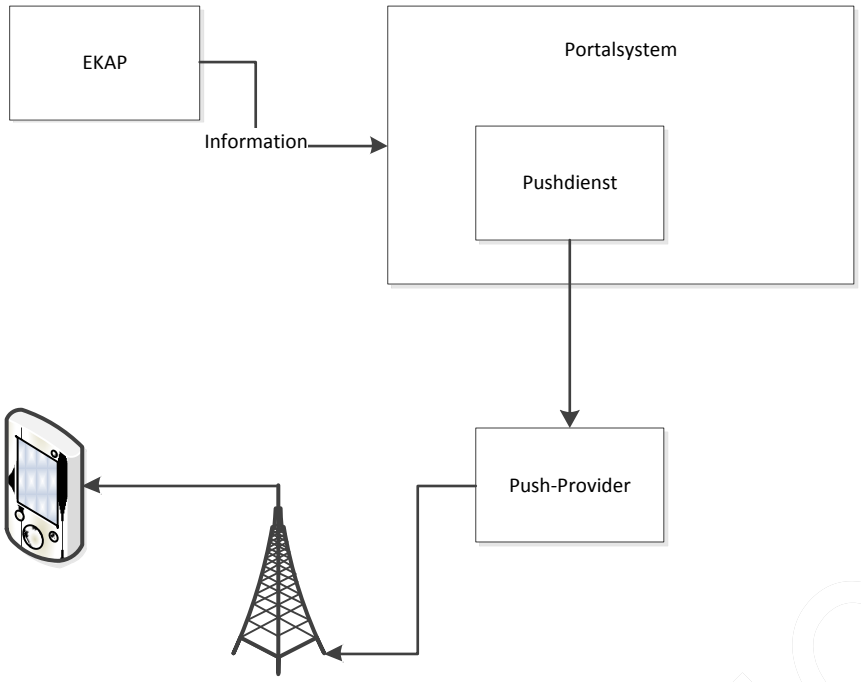

Abbildung 5: Schematische Darstellung des Informationsflusses beim Pushdienst

Im Anhang A II.1 findet sich hierzu eine mögliche detaillierte Umsetzung eines Push-Dienstes.

4.5. Zugriffskontrolle

Diese Komponente kapselt die für die Zugriffskontrolle relevanten Dienste Authentifikation und Autorisierung. Sie ermöglicht damit eine transparente Zugriffskontrolle bei jedem Aufruf einer Methode. Zur Autorisierung gehört auch das Verwalten von Rechten. Die beiden Dienste sind so entworfen, dass sie bei jeder anderen Komponenten oder jedem anderen Dienst eingesetzt werden können, um eine sichere Kommunikation zu gewährleisten. Hintergrund ist hier, dass die möglicherweise sensiblen Echtzeitdaten nicht allen möglichen Abnehmern frei zur Verfügung gestellt werden sollen bzw. können. Daher müssen die abgreifenden Systeme bzw. deren Zugriffe authentifiziert werden können.

4.5.1. Umsetzungsgrad von Autorisierung und Authentifizierung

Bei einer Architektur, die darauf basiert, dass viele unabhängige Teilnehmer miteinander kommunizieren und Daten austauschen, bedarf es eines angemessenen Sicherheitskonzeptes. Dieses muss in der Lage sein, eine sichere Kommunikation sowohl im Sinne der Vertraulichkeit als auch im Sinne von Integrität und Authentizität zu garantieren.

Doch neben einer sicheren Kommunikation bedarf es auch einer Zugriffskontrolle auf die Daten und Funktionalitäten. Schließlich kann ein Dienstanbieter seinen Konsumenten je nach Auslegung der vertraglichen Rahmenbedingungen verschiedene Daten und Funktionen zur Verfügung stellen. Hierbei fiel die Entscheidung auf eine baumstruktur- und rollenbasierte Zugriffssteuerung (vgl. Anhang A II.1.5).

Der Schritt der Authentifikation bildet eine Vorbedingung für die Autorisierung der Kommunikationspartner beim Zugriff auf die Daten und Funktionalitäten.

4.5.1.1 Zertifikatbasierte Authentifizierung für Portal Dienste

Das Konzept von asymmetrischen Schlüsseln, in diesem Fall von Zertifikaten, basiert auf der Annahme, dass eine zentrale Stelle existiert, der man absolutes Vertrauen bezüglich der Authentifizierung schenkt. In Deutschland wird diese Stelle von der Bundesnetzagentur wahrgenommen, die als Wurzel für weitere Unterknoten agiert. Solche Zertifizierungsketten erlauben es, Bäume mit Unterpfaden für einzelne Unternehmen, Organisationen und Universitäten aufzuspannen, ohne dass der Benutzer eines Zertifikates sich bei der Wurzel anmelden muss.

Weitere Anwendungsfälle von digitalen Zertifikaten finden sich in herkömmlichen Browsern, die für eine sichere Kommunikation, zum Beispiel beim Online-Banking, verwendet werden. Die Anwendungsbreite, Beschaffenheit und die etablierte sowie erprobte Infrastruktur machen die Verwendung von Zertifikaten für eine sichere Kommunikation zwischen den einzelnen Diensten zu einer idealen Lösung.

4.5.1.2 Rollenbasierte Autorisierung von Kommunikationspartnern

Jeder Dienst, der seine Daten und Funktionalitäten in Abhängigkeit des aktuellen Kommunikationspartners bereitstellen möchte, erfordert neben einer Authentifizierung auch eine Zugriffsverwaltung, genannt Autorisierung. Eine weitverbreitete und beliebte Methode der Realisierung ist das Rollenkonzept. Dabei werden Rollen angelegt, die mit bestimmten Rechten ausgestattet sind. Den einzelnen Kommunikationspartnern werden dann eine oder mehrere Rollen zugewiesen. Dieses Konzept hat den Vorteil, dass es in den meisten Fällen deutlich weniger Rollen als Kommunikationspartner gibt, wodurch sich die Rechteverwaltung deutlich einfacher gestalten lässt.

Für eine SOA bedeutet dies, dass jeder Dienst über eine eigene Rechteverwaltung verfügen muss, wenn er seine Daten und Funktionalitäten nur in einer bestimmten Abhängigkeit zum aktuellen Kommunikationspartner bereitstellen möchte. Da wiederum bei den Dienstanbietern von Unternehmen und nicht von Privatpersonen auszugehen ist, kann die Rechteverwaltung mit einem überschaubaren Aufwand umgesetzt und verwaltet werden. Meist ist eine einfache Integration in bereits bestehende Autorisierungs- und Authentifizierungssysteme möglich.

4.6. Anfragesteuerung im Portalsystem

Der folgende Teil beschreibt die Anfragesteuerung für ein Portalsystem, im Folgenden nur „Anfragesteuerung“ genannt. Darüber hinausgehend gibt es auch eine Anfragesteuerung für die EKAPs, die ähnliche Aufgaben erledigt. Sie wird als „EKAP-Anfragesteuerung“ bezeichnet, um Verwechslungen vorzubeugen. Die Anfragesteuerung nimmt jegliche Anfragen entgegen, die an Teile des Portalsystems gerichtet sind oder über das Portalsystem weitergeleitet werden. Abhängig von der individuellen Anfrage ruft sie dann die zuständigen Funktionen auf.

Der Zugriff von EKAPs untereinander ist nicht Gegenstand dieses Dokumentabschnitts (siehe VDV 431). Jedoch werden bei Bedarf auch Befehle an EKAPs von der Anfragesteuerung (an die EKAP-Anfragesteuerung) weitergeleitet. Dazu verwaltet die Anfragesteuerung auch Informationen über EKAPs in einem Verzeichnisdienst für alle dem Portalsystem bereits bekannten EKAPs. In diesem EKAP-Register werden zu jeder registrierten EKAP die folgenden Angaben gespeichert:

- **EKAP-ID:** Die EKAP-ID wird bei der Registrierung automatisch vom EKAP-Register vergeben und ist innerhalb dieses Registers eindeutig.

- **EKAP-Adresse:** Die EKAP-Adresse beinhaltet die Daten, die zur Kontaktaufnahme mit der EKAP notwendig sind. Hierbei kann es sich beispielsweise um Adressinformationen in URL-Form handeln, über welche die EKAP beziehungsweise ihre Dienste erreichbar sind.
- **Anbieter-ID:** Die Anbieter-ID kennzeichnet analog zum Diensteregister den Anbieter der EKAP. Für die Verwaltung der Anbieter-IDs gibt es noch keine zentrale Instanz oder Organisation. Bis auf weiteres muss sich jeder Verbund von kooperierenden EKAPs damit behelfen, selbst auf die Eindeutigkeit der IDs zu achten.
- **Schnittstellenversion:** Die Schnittstellenversion gibt die Version der Schnittstellen an, die zur Verwendung der EKAP notwendig sind, also zumindest die Version des Diensteregister-Dienstes.

EKAPs können im EKAP-Register registriert werden. Ebenso können die über sie gespeicherten Informationen nachträglich geändert und wieder entfernt werden. Die Registrierung kann je nach Wunsch des Anbieters auf unterschiedliche Weise vorgenommen werden. All die im Folgenden exemplarisch genannten Umsetzungsmöglichkeiten lassen sich entsprechend den Wünschen der Anbieter beliebig automatisieren oder manuell durchführen:

- Der Betreiber des EKAP-Registers registriert die EKAP und gibt Informationen zur EKAP ein, die vom EKAP-Anbieter bei Vertragsschluss übermittelt wurden.
- Der Betreiber des EKAP-Registers bietet einen Dienst zur Registrierung von EKAPs an. Dieser kann von EKAP-Anbietern genutzt werden, um eigene zur Verfügung stehende EKAPs zu melden. Wird die EKAP-Meldung akzeptiert, trägt der Betreiber des EKAP-Registers die EKAP mitsamt allen Angaben im EKAP-Register ein.
- Der Betreiber des EKAP-Registers lässt den externen Zugriff auf den EKAP-Registerdienst zu, um eine Selbsteintragung durch EKAP-Betreiber zu ermöglichen. EKAP-Anbieter tragen dort ihre EKAPs ein beziehungsweise führen Aktualisierungen selber durch.

Erhält die Anfragesteuerung eine Anfrage, so wird auf anbieterspezifische Weise ermittelt, welche Verarbeitungskomponente im Portalsystem die benötigten Funktionen zur Verfügung stellt und wie diese Komponente erreichbar ist. Erfordert die Anfrage den Aufruf einer Funktion in einer EKAP, so können die im EKAP-Register gespeicherten Informationen abgerufen werden.

Ist mehr als eine EKAP registriert, so ist nicht festgelegt, welche EKAP die Anfragesteuerung für welche Anfrage heranzieht. Diese Entscheidung ist anbieterspezifisch und hängt von der Implementierung bzw. Ausschreibung des EKAP-Registers und der Anfragesteuerung ab. Zudem erfordert sie möglicherweise, dass das EKAP-Register oder das Portalsystem Zusatzinformationen mit den EKAP-IDs verknüpfen (beispielsweise den Zuständigkeitsbereich von EKAPs). Das standardisierte EKAP-Register bietet somit die Grundfunktionalität an, um eine Reihe von Verweisen auf EKAPs zu verwalten. Folgende Strategien sind möglich aber nicht nur auf diese begrenzt:

- **Auswahl nach fester Priorisierung und Erreichbarkeit:** Die registrierten EKAPs haben eine feste Reihenfolge, in der sie kontaktiert werden. Sind EKAPs nicht erreichbar, dienen die jeweils nächsten EKAPs im Register als Rückfallebenen.

- **Auswahl nach Funktionalität:** Es werden gezielt diejenigen EKAPs aufgerufen, die bestimmte Dienste und Funktionen anbieten. Die Ermittlung dieser Dienste kann bei jeder Anfrage geschehen. Dazu muss (zusätzlich zu den sonstigen EKAP-Informationen) die Adresse gespeichert werden, unter der das Diensteregister der EKAP erreichbar ist, sodass im Fall einer Anfrage bei den registrierten EKAPs angefragt werden kann, ob sie bestimmte Dienste anbieten. Ebenso kann zu den EKAPs auch eine Liste der jeweils angebotenen Funktionen vorgehalten werden. Ob diese manuell vom registrierenden Akteur zusammengestellt oder über das Diensteregister der EKAP ermittelt wird, und ob diese Liste regelmäßig oder auf Hinweis des EKAP-Anbieters hin aktualisiert wird, bleibt den jeweiligen Anbietern überlassen und wird nicht standardisiert.
- **Auswahl nach Zuständigkeitsbereich:** Basierend auf zusätzlichen Angaben der Anbieter wird eine EKAP für eine Anfrage passend zu ihrem geografischen, tariflichen oder anderweitig ausgeprägten Zuständigkeitsbereich ausgewählt.

Diese Strategien können durch weitere ergänzt und auch untereinander kombiniert werden.

Weiterhin ist anbieterabhängig, ob etwaige Zusatzinformationen im EKAP-Register oder in der Anfragesteuerung abgelegt werden. Dies wird in dieser Schrift nicht explizit festgelegt.

4.7. Mobiles Endgerät

Die Komponente mobiles Endgerät stellt das tatsächliche Gerät des Fahrgastes sowie das Betriebssystem des Gerätes dar und kapselt den Dienst „Physikalische Ortung“, welcher eine Ortung des Fahrgastes beispielsweise per GPS-Sensor, über die Fahrzeugschnittstelle (z. B. im Tunnel) oder über Lokalisierung im Funknetz ermöglicht. Dieser Dienst ist eine wichtige Voraussetzung für die Nutzung der Fahrtinformation und weiterer ortsbezogener Informationsdienste. Das mobile Endgerät ist zu unterscheiden von der Applikation auf dem Gerät, die im Wesentlichen die Schnittstelle zum Benutzer darstellt und von den technischen Schnittstellen für die Kommunikation.

4.7.1. Schnittstelle zum Benutzer

Über die Komponente des mobilen Endgeräts wird weiterhin die „Schnittstelle“ zwischen Fahrgast und Plattform dargestellt. Das bedeutet, dass alle Eingaben und Abfragen, die vom Fahrgast getätigt werden, über das mobile Endgerät an die jeweils zuständige Komponente weitergeleitet werden und die Ausgaben über das mobile Endgerät an den Fahrgast übermittelt wird.

4.7.2. Technische Schnittstelle zum Mobilen Endgerät

Grundsätzlich lässt sich auch hier eine Unterscheidung bezogen auf die Schnittstellen treffen: diejenige zum Portalsystem sowie die zum Fahrzeug. Aufgrund technischer Rahmenbedingungen lässt sich hier jedoch lediglich die Spezifikation auf IP-Basis durchführen. Der physikalische Weg für den Datenaustausch muss dem Stand der Technik folgen.

4.8. Mehrwertdienste

Die Komponente „Mehrwertdienste“ ermöglicht die Einbindung bzw. Nutzung externer Dienste von Drittanbietern. Beispiele sind Dienste für Buchung, Reservierung, Fahrgeldmanagement, Wetterinformationen, Soziale Netzwerke etc. Diese werden nicht vom

Portalsystem selbst bereitgestellt, sondern von anderen angeboten, z. B. von ÖPV-Unternehmen, Reiseveranstaltern, usw.

Die Komponente „Mehrwertdienste“, die zum Portalsystem gehört, bietet der Applikation auf dem mobilen Endgerät die Möglichkeit eines einheitlichen Zugriffs auf solche Dienstleistungen Dritter. Dies ist sinnvoll, da die verschiedenen Anbieter unterschiedliche Plattformen, Programmiersprachen, Methoden, Datenstrukturen usw. nutzen. Ohne eine abstrahierende Komponente wie Mehrwertdienste müsste entsprechend die Kommunikation für jeden Drittanbieter fest in der Applikation implementiert und bei Änderungen an mehreren Stellen angepasst werden. Hoher Wartungs- und Verwaltungsaufwand sowie höhere Fehleranfälligkeit wären die Folge.

Die Komponente beinhaltet das Auffinden geeigneter Dienste sowie die Übersetzung der Aufrufe und Daten in das vom Drittanbieter geforderte Format und umgekehrt. Letzteres bedeutet, dass die Komponente selbst die Übersetzung vornimmt oder in der Lage ist, zu diesem Zweck eine andere Komponente im Portalsystem bzw. bei einem externen Anbieter zu nutzen.

4.8.1. Integrationsfähigkeit von Mehrwert-Diensten

Es wurde bereits angeführt, dass Mehrwertdienste die Leistungen der Reiseauskunft erweitern können. Beispiele sind die Einbindung von Wettervorhersagen, Ticketbuchungen, Sitzplatzreservierungen oder das Auffinden von z. B. Ärzten in einem bestimmten Zielgebiet. Bezüglich verschiedener MWD gibt es folgende Möglichkeiten (siehe Abbildung 6) der Einbindung:

(1) MWD können **Teil eines Portalsystems** sein (interner MWD), also vom Portalsystemanbieter entwickelt und betrieben werden, oder
(2) MWD können externe Dienste sein, die **unabhängig von einem Portalsystem** entwickelt und betrieben werden. In diesem Fall kann entweder
    a. das Portalsystem den externen MWD nutzen um Daten oder Funktionalitäten anzufragen oder
    b. die externen MWD-Funktionen des Portalsystems nutzen, z. B. um Daten von der EKAP zu erhalten oder um Informationen an einen Kunden (mobile Anwendung) ausliefern zu lassen. In diesem Fall fungiert das Portalsystem für einen externen MWD als Mittler.

Offensichtlich ist Fall (1) trivial. Wenn ein MWD von einem Portalsystembetreiber implementiert, verwaltet und betrieben wird, ist dieser unabhängig und in seiner Funktionalität frei realisierbar. Dies gilt auch, wenn das Portalsystem als Teil der Anwendung auf dem mobilen Endgerät umgesetzt wird. Aufgrund der begrenzten Ressourcen (z. B. Rechenkapazität, Akkulaufzeit) ist jedoch davon auszugehen, dass in einem solchen Fall die MWD nicht im Portalsystem integriert werden, sondern Fall (2) realisiert wird. Bezüglich des Falls (2) ist eine Anbindung von externen Diensten an ein Portalsystem notwendig, also Kommunikation zwischen diesen beiden abgeschlossenen Systemen. Darauf, sowie im Zuge dessen auf die Fälle (2a) und (2b), wird nachfolgend näher eingegangen.

Dem EKAP-Register sind in einem Portalsystem verschiedene EKAPs bekannt zu machen, sodass das Portalsystem die Dienste und Daten dieser EKAPs nutzen kann (vgl. Kapitel 4.6). Auf diese Weise können beliebig neue EKAPs und Portalsysteme geschaffen und nahtlos in die Systemlandschaft integriert werden. Ähnliche Funktionalität bietet der Diensteregisterdienst einer EKAP.

Auf ähnliche Weise kann die Einbindung von externen Mehrwertdiensten (MWD) realisiert werden. So ist ein **MWD-Register** möglich (vgl. Abbildung 9), mittels dessen sich MWD bei einem Portalsystem registrieren. Die Anfragesteuerung des Portalsystems kann dann bei Bedarf einen benötigten MWD über dieses MWD-Register auffinden, ansprechen und dessen Angebote nutzen (dies entspricht Fall (2a)). Die meisten Dienste (z. B. Wetterauskunft, Buchungs- und Reservierungssysteme, Ticketing, soziale Netzwerke) bieten dazu sogenannte **API**s (application programming interface). Das sind Schnittstellen, die es ermöglichen, von außen (also z. B. vom Portalsystem aus) eine Anfrage an den Dienst zu stellen. Um Fall a. zu lösen, muss also ein externer MWD eine API bereitstellen. Dies entspricht bereits dem Stand der Technik und wird von den meisten Dienstbetreibern umgesetzt. Der entsprechende externe MWD erhält also eine Anfrage seitens des Portalsystems über das vom MWD bereitgestellte API, verarbeitet diese intern und liefert das Ergebnis ans Portalsystem zurück. Im Portalsystem können die so erhaltenen Anfragen entsprechend weiterverarbeitet und/oder angereichert werden (vgl. Abbildung 6). Die dazu benötigte Programmlogik kann im Portalsystem z. B. als Teil der Anfragesteuerung umgesetzt werden. Somit liegt der Umfang der Funktionalität (also auch die Einbindung von MWD) komplett beim Anbieter des Portalsystems. Darüber hinaus können neu entwickelte MWD in Zukunft speziell darauf ausgelegt werden, Portalsysteme zu unterstützen und spezielle Daten zu liefern oder ihrerseits für die Bearbeitung einer Anfrage Daten einer EKAP zu nutzen. So wird eine engere Verzahnung von verschiedenen Diensten mit Verkehrsdaten und -planungen möglich.

Unabhängig davon können natürlich externe MWD die Funktionen eines Portalsystems nutzen (dies entspricht Fall (2b)). Zu diesem Zweck muss das Portalsystem selbst eine Schnittstelle anbieten, z. B. ein eigenes API. Diese Schnittstelle wird hier nicht standardisiert, da sie hersteller- und betreiberabhängig sein kann und Mehrwertdienste generell nicht zum Kern dieses Dokumentes gehören.

Natürlich kann ein Portalsystem auch die Fälle (2a) und (2b) verknüpfen und sowohl fremde APIs anfragen als auch eine eigene bereitstellen. In der Folge ergibt sich eine ähnliche Leistungsfähigkeit wie bei Fall (1), da zur Lösung von Aufgaben beliebige existierende Dienste herangezogen, genauso aber auch EKAP-eigene, bisher nicht existierende Funktionen anderen zur Verfügung gestellt werden können.

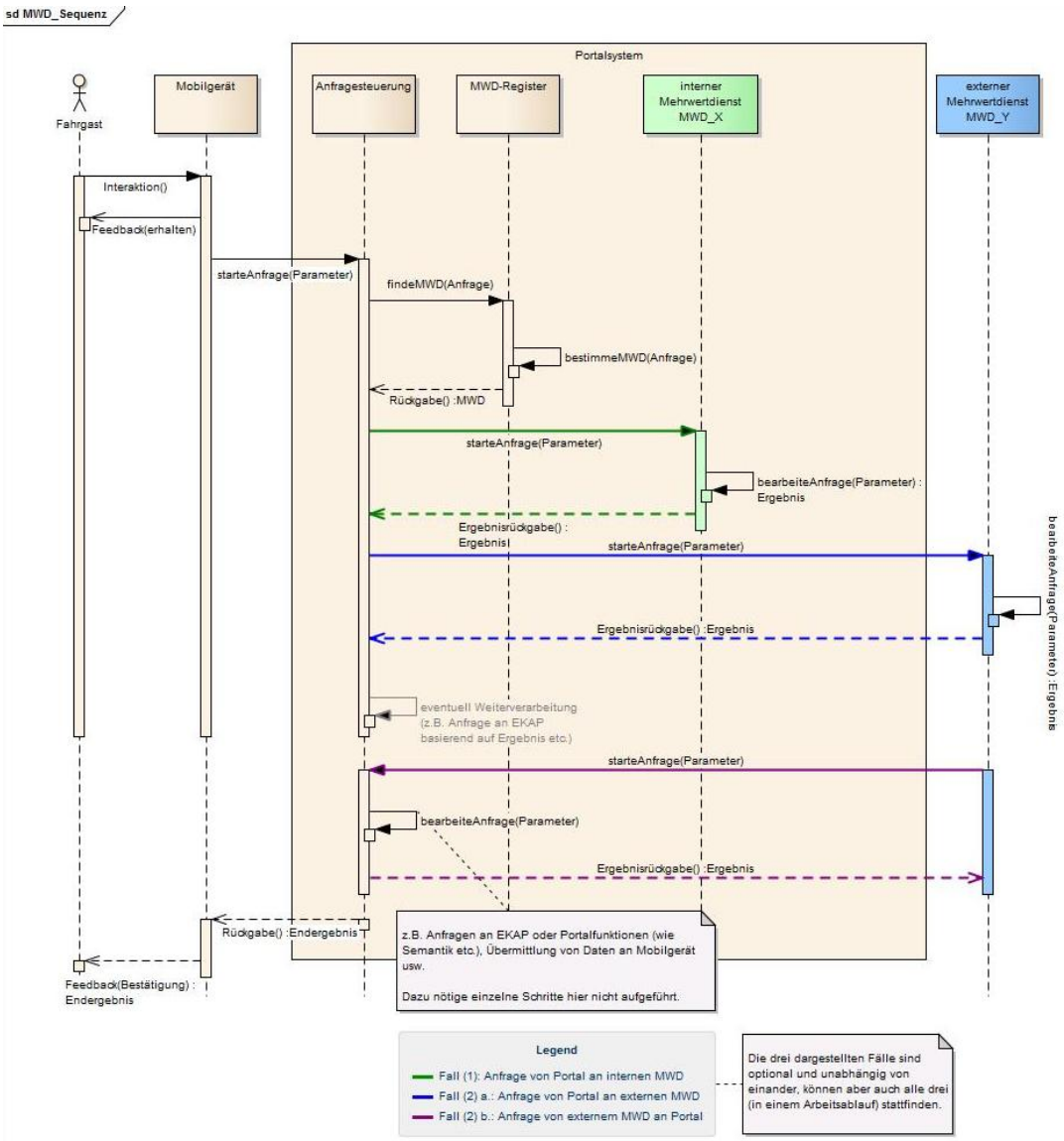

Abbildung 6: Sequenzdiagramm der Nutzung von Mehrwertdiensten für die Fälle (1) „Anfrage eines internen MWD durch das Portalsystem“ sowie (2) „Anfrage eines externen MWD“. Fall (2) wird unterschieden in Fall a. „Anfrage eines externen Dienstes durch das Portalsystem“ bzw. Fall b. „Anfrage des Portalsystems durch einen externen MWD“.

5. Dienste (inkl. Detailarchitekturen)

Im Folgenden werden die einzelnen Dienste spezifiziert indem eine grobe Beschreibung der Funktion erfolgt. Zunächst zeigt die Tabelle 2 die Zuordnungen der Dienste zu den jeweiligen Komponenten. Dabei ist zu beachten, dass hier sowohl Dienste des Portalsystems, aber aufgrund der engen Verzahnung auch der EKAP (VDV-Schrift 431), ebenfalls aufgeführt sind.

Dienste \ Komponenten	Anfragesteuerung	Benachrichtigungs-Komponente	Betriebsleitsystem	Datendrehscheibe	DELFI (ext.)	Diensteregister	Ereignis-Management-System	Fahrplanauskunft	Fahrzeug (IBIS-IP)	Geo-Namensregister	IV-Router	Karten	Mehrwertdienste	Mobiles Endgerät	Modellserver	Personalisierung	Push	Solldatenversorgung (ext.)	Tarifrechner	Umschlüsselungsdatenbank	Zugriffskontrolle
Abfahrtstafeln								X													
Adresssuche zu Koordinate										X											
Anfragesteuerungsdienst	X																				
Anschlussstatus			X	X																	
Anschlussmeldung			X	X																	
Info bei Anschlussverlust			X	X																	
Authentifizierungsdienst																					X
Autorisierungsdienst																					X
Benachrichtigungsdienst		X																			
Buchen von AST			X																		
Diensteregisterdienst						X															
Ereignisinformationsdienst			X	X			X														
EKAP-Registerdienst	X																				
Fahrtinformation EKAP								X													
Fahrtinformation Fahrzeug									X												
Geo-Kontextdienst										X											
Haltewunsch									X												
IV-Routen-Suche											X										
Kartendienst												X									
Logische Ortung								X	X												
Mehrwertdienste													X								
Modellverwaltung															X						
Objektinformationsdienst										X											
Ortsauflösung										X											
Personalisierungsdienst																X					
Physikalische Ortung														X							
Prozessfahrplandienst			X	X																	
Push-Dienst																	X				
Referenzfahrplandienst			X	X																	
Schadensmeldung			X	X																	
Solldatendienst			X	X														X			
Tarifinformationen																			X		
Verbindungssuche								X													

Tabelle 2: Komponenten-Dienste-Matrix

5.1. Fahrtinformation EKAP - SV2.Fahrtinformation_EKAP

5.1.1. Zweck

Die Fahrtinformation beschreibt den Dienst zwischen der EKAP und dem mobilen Endgerät des Fahrgastes bzw. dem Portalsystem, der den Fahrgast mit den relevanten Informationen zur Fahrt versorgt. Zu diesen gehören u. a. Fahrweg, Haltepunkte, aktuelle Fahrzeugposition, Prognose-Daten und Ausstattung des Fahrzeuges.

5.1.2. Interaktionen

Der Fahrgast bzw. das mobile Endgerät meldet die für die gewünschte Information der Fahrtinformation notwendigen Eingangsdaten an das Portalsystem. Dieses richtet eine Anfrage an EKAP bzw. hat die entsprechenden Informationen bei der EKAP abonniert und meldet nach Erhalt der Informationen diese an den Fahrgast/mobiles Endgerät zurück.

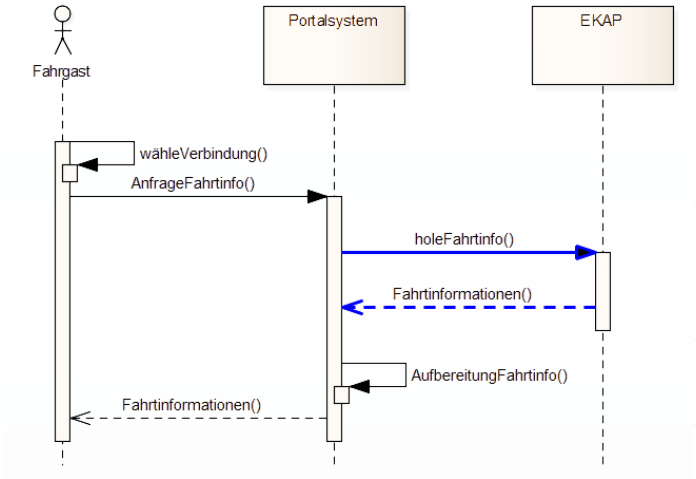

Abbildung 7: Sequenzdiagramm Fahrtinformation EKAP

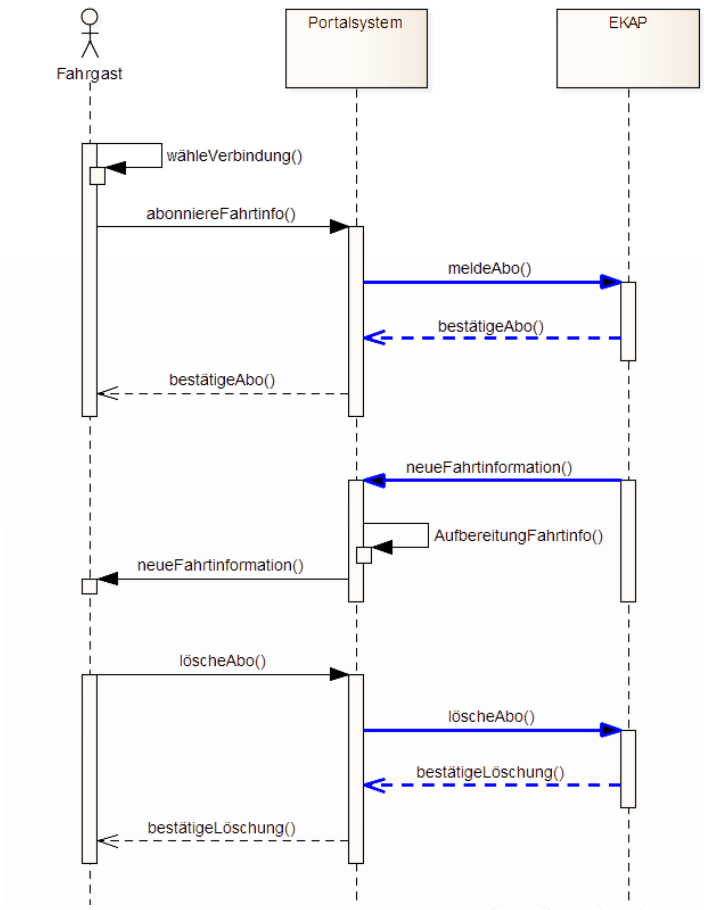

Abbildung 8: Sequenzdiagramm Abonnement

5.1.3. Betroffene Komponenten

Dienstanbieter: Fahrplanauskunft (EKAP)
Dienstabnehmer: Mobiles Endgerät/Portalsystem

5.1.4. Funktion 1: Fahrgastfahrt mit Haltepunkten anzeigen

Eingangsdaten

- Verbindung
- Linien
- Planfahrten
- Fahrzeug-IDs
- Angeforderte Inhalte (siehe mögliche Ausgangsdaten)

Ausgangsdaten

- Fahrweg
- Fahrwegstrecke
- Fahrwegpunkte
- Haltepunkte
- Fahrzeugfahrt
- Fahrgastfahrt
- Hinweis auf Bedarfsfahrten/AST
- Fehlermeldung
- Zeitstempel

5.1.5. Funktion 2: Fahrzeugpositionen anzeigen

Eingangsdaten

- Verbindung
- Linien
- Planfahrten
- Fahrzeug-IDs

Ausgangsdaten
- Fahrzeugfahrt
- Fahrzeugposition
- Fehlermeldung
- Zeitstempel der Information

5.1.6. Funktion 3: Reisezeit anzeigen

Eingangsdaten
- Verbindung
- Linien
- Planfahrten
- Fahrzeug-IDs

Ausgangsdaten
- Datenart (Halbjahres-Soll-Fahrplan oder Tages-Soll-Fahrplan oder Echtzeit-Daten)
- Datenqualität
- Prognosedaten
- Fehlermeldung
- Zeitstempel

5.1.7. Funktion 4: Fahrzeugdetails anzeigen

Eingangsdaten
- Verbindung
- Linien
- Planfahrten
- Fahrzeug-IDs

Ausgangsdaten
- Fahrzeugart
- Niederflur / niveaugleicher Einstieg
- Fahrradmitnahme
- Rollstuhl-Platz / Kinderwagen-Platz
- Mutter-Kind-Platz
- Steh- und Sitzplätze
- Ticketautomat
- Vordereinstieg
- Funktionsauskunft des Fahrzeuges
- Speisewagen
- weitere Fahrzeugbesonderheiten
- Fehlermeldung
- Funktion wird nicht unterstützt

5.1.8. Funktion 5: Streckendetails anzeigen

Eingangsdaten
- Verbindung

Entwurf

- Linien

Ausgangsdaten (erweiterbar)
- Touristische Information
- W-LAN-/ Handy-Netzzugang
- Weitere Streckenbesonderheiten (dauerhafte Abweichungen,…)
- Fehlermeldung
- Funktion wird nicht unterstützt

5.1.9. Funktion 6: Haltestellendetails anzeigen (nicht genauer spezifiziert)

Eingangsdaten
- Verbindung
- Haltestelle
- Haltepunkt

Ausgangsdaten
- Art der Haltestelle (Gebäude, mit Unterstand, ohne Unterstand)
- Sanitäranlagen
- Wickelraum
- Verpflegungsmöglichkeit
- Fahrkartenautomat
- Service-Point
- Weitere Einrichtungen (Polizei, Bahnhofsmission, Erste Hilfe etc.)
- Barrierefreiheit (Aufzüge, Treppen etc.)
- weitere Haltestellenbesonderheiten
- Fehlermeldung
- Funktion wird nicht unterstützt

5.1.10. Funktion 7: Auslastung anzeigen

Eingangsdaten
- Verbindung
- Linien
- Planfahrten
- Fahrzeug-IDs

Ausgangsdaten
Die Ausgangsdaten können bezogen auf ein Fahrzeug oder auf einzelne Abteile ausgegeben werden.
- Aktuelle Auslastung (z. B. „starke Auslastung“)
- Auslastungsprognose (textuell)
- Datenqualität
- Fehlermeldung
- Funktion wird nicht unterstützt
- Zeitstempel

5.1.11. Funktion 8: Zuständigkeit ermitteln

Die Identifikation der Zuständigkeit erfolgt über die Fahrzeug-ID. Sofern diese nicht vorhanden ist, erfolgt die Identifikation über die weiteren Eingangsdaten.

Eingangsdaten
- Fahrt-ID

Entwurf

- Fahrzeug-ID
- Fahrzeugfahrt
- Fahrgastfahrt

Ausgangsdaten
- Verantwortliches Betriebsleitsystem
- Verantwortliches Verkehrsunternehmen
- Fehlermeldung
- Funktion wird nicht unterstützt

5.1.12. Funktion 9: Fahrtinformation abonnieren

Eingangsdaten
- angeforderte Fahrtinformation
- Verbindung
- Linien
- Planfahrten
- Störungen/Ereignisse
- Fahrzeug-IDs
- Dauer des Abos (Löschbedingung)

Ausgangsdaten
- Bestätigung des Abos
- Abo-ID
- Fehlermeldung
- Funktion wird nicht unterstützt

5.1.13. Funktion 10: Abo der Fahrtinformation löschen

Eingangsdaten
- Abo-ID

Ausgangsdaten
- Bestätigung der Löschung
- Fehlermeldung

5.2. Fahrtinformation Fahrzeug - SV2.Fahrtinformation_Fahrzeug

5.2.1. Zweck

Die Fahrtinformation beschreibt den Dienst zwischen Fahrzeug und mobilen Endgerät des Fahrgastes, der den Fahrgast mit den relevanten Informationen zur Fahrt versorgt. Zu diesen gehören u. a. Fahrweg, Haltepunkte, aktuelle Fahrzeugposition und Ausstattung des aktuellen Fahrzeuges, sofern sie dem Fahrzeug bekannt sind. Mit der Kommunikation zwischen Fahrzeug und mobilem Endgerät wird hier eine zusätzliche Datenquelle hinzugefügt, weswegen es zu Dateninkonsistenzen kommen kann. Eine Diskussion dieser Problematik findet sich im Anhang A II.3.

5.2.2. Interaktionen

Das Fahrzeug meldet die vorhanden Informationen (Ausgangsdaten) an das mobile Endgerät des Fahrgastes, welches aus den Daten die benötigten Informationen auswählen kann.

©VDV Druck

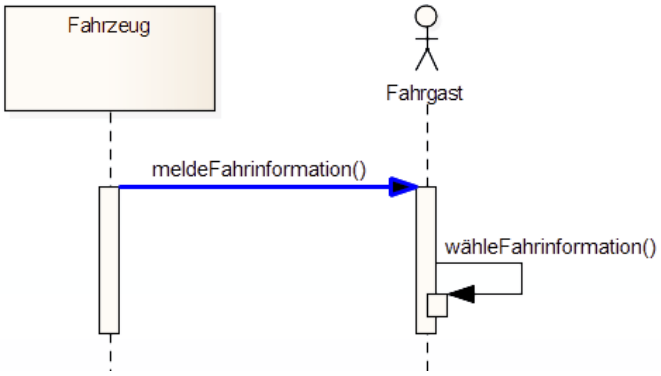

Abbildung 9: Sequenzdiagramm Fahrtinformation Fahrzeug

5.2.3. Betroffene Komponenten

Dienstanbieter: Fahrzeug
Dienstabnehmer: Mobiles Endgerät

5.2.4. Funktion 1: Fahrzeug identifizieren

Die Identifikation des Fahrzeuges erfolgt über die Fahrzeug-ID. Sofern diese nicht vorhanden ist, erfolgt die Identifikation über die weiteren Ausgangsdaten.

Eingangsdaten

- Keine Eingangsdaten

Ausgangsdaten

- Fahrzeug-ID
- Zielfilm
- Fahrt-ID
- Linie
- Umlaufnummer

5.2.5. Funktion 2: Fahrgastfahrt mit Haltepunkten anzeigen

Eingangsdaten

- Keine Eingangsdaten

Ausgangsdaten

- Fahrweg des Fahrzeugs
- Fahrwegstrecke des Fahrzeugs
- Fahrwegpunkte des Fahrzeugs
- Haltepunkte des Fahrzeugs
- Fahrzeugfahrt
- Fehlermeldung
- Umsteigehinweise/-beziehungen
- Zeitstempel

5.2.6. Funktion 3: Fahrzeugpositionen anzeigen

Eingangsdaten

- Keine Eingangsdaten

Ausgangsdaten

- Fahrzeugfahrt
- Fahrzeugposition

- Zeitstempel der Information
- Fehlermeldung
- Funktion wird nicht unterstützt

5.2.7. Funktion 4: Ankunftszeit anzeigen

Eingangsdaten

- Keine Eingangsdaten

Ausgangsdaten

- Halbjahres-Soll-Fahrplan oder Tages-Soll-Fahrplan oder Echtzeit-Daten
- Datenqualität
- Aktuelle Fahrplanlage
- Fehlermeldung
- Zeitstempel

5.2.8. Funktion 5: Fahrzeugdetails anzeigen

Eingangsdaten

- Keine Eingangsdaten

Ausgangsdaten

- Fahrzeugtyp
- niveaugleicher Ausstieg
- Funktionsauskunft des Fahrzeuges
- Speisewagen/ Sanitäranlagen
- Fahrkartenautomat
- weitere Fahrzeugbesonderheiten
- Fehlermeldung
- Funktion wird nicht unterstützt

5.2.9. Funktion 6: Auslastung anzeigen

Eingangsdaten

- Keine Eingangsdaten

Ausgangsdaten

- Aktuelle Auslastung (z. B. „starke Auslastung“)
- Fahrzeugbereich
- Zeitstempel
- Fehlermeldung
- Funktion wird nicht unterstützt

5.2.10. Funktion 7: Dienste-Auskunft

Eingangsdaten

- Keine Eingangsdaten

Ausgangsdaten

- Dienst-ID
- Art des Diensts
- Schnittstellenversion
- Dienstadresse
- Ein- oder ausgehender Dienst
- Anbieter-ID

ENTWURF

- Dienstspezifische Merkmale (wie z. B. Funktionsumfang, Datenumfang etc.)
- Fehlermeldung

5.2.11. Funktion 8: Fahrgastinnendurchsagen

Eingangsdaten

- Keine Eingangsdaten

Ausgangsdaten

- Durchsagen als Audiostream
- Durchsagen in Textform
- Inhaltskategorie der Durchsage

5.3. Haltewunsch – SV2.Haltewunsch

5.3.1. Zweck

Dieser Dienst umfasst die Übermittlung des Haltewunsches für eine spezifische Haltestelle (z. B. bei der Reiseplanung) und den Haltewunsch für die nächste Haltestelle (unabhängig von der Reiseplanung).

5.3.2. Interaktionen

Der Fahrgast bzw. die Anwendung auf dem mobilen Endgerät erhält vom Fahrzeug den Hinweis darauf, dass eine Haltestelle erreicht wird. Daraufhin bietet die Anwendung dem Fahrgast die Haltewunsch-Option an. Bei Bestätigung wird der Haltewunsch an das Fahrzeug übermittelt. Gegebenenfalls kann das Fahrzeug dem Fahrgast ein Feedback geben, dass der Haltewunsch übermittelt wurde, z. B. durch das Aufleuchten einer Signallampe und einer akustischen Quittung im Fahrzeug und/oder auf der Fahrgastanwendung (siehe auch Abbildung 10).

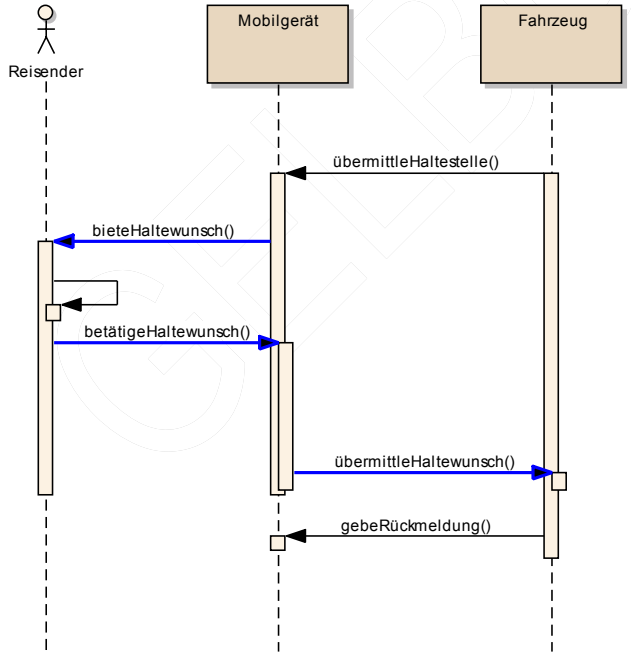

Abbildung 10: Sequenzdiagramm Haltewunsch

5.3.3. Betroffene Komponenten

Dienstanbieter: Fahrzeug
Dienstabnehmer: Mobiles Endgerät

5.3.4. Funktion 1: Anbieten der Haltewunsch-Option

Eingangsdaten

- Positionsdaten des Fahrzeugs
- Daten zur nächsten Haltestelle (Name/ID)

Ausgangsdaten

- Haltewunsch-Option zur entsprechenden Haltestelle
- Im Fehlerfall: Fehlermeldung zurück geben
- Bei nicht implementierter Funktion Hinweis hierauf als Fehlercode

5.3.5. Funktion 2: Senden des Haltewunsches

Eingangsdaten

- Bestätigung des Haltewunschs

Ausgangsdaten

- Bestätigung des angenommenen Haltewunsches (Feedback)
- Im Fehlerfall: Fehlermeldung zurück geben
- Bei nicht implementierter Funktion Hinweis hierauf als Fehlercode

5.4. Personalisierungsdienst – SV2.Personalisierung

5.4.1. Zweck

Dieser Dienst stellt Funktionen bereit, über die Daten für die personalisierte Konfiguration beliebiger Dienste hinterlegt werden können. Unter „Konfiguration“ sind hier nicht nur explizite Einstellungen im engeren Sinn zu verstehen, sondern allgemein benutzerbezogene Daten. All diese Informationen können das Verhalten derjenigen Dienste, die den Personalisierungsdienst benutzen, beeinflussen und stellen somit eine Konfiguration für den verwendenden Dienst dar.

Der Dienst verwaltet lediglich Benutzereinstellungen und stellt keine eigenen personalisierten Funktionen zur Verfügung. Andere Dienste können auf den Personalisierungsdienst zurückgreifen, um ihre Funktionen personalisiert zur Verfügung zu stellen. Der Zugriff auf die personalisierten Daten erfolgt auf Basis des Authentifizierungsdienstes, um einen Schutz der Daten, entsprechend der rechtlichen Vorgaben zum Datenschutz, zu ermöglichen. Diese Vorgaben sind bei der Umsetzung des Personalisierungsdienstes zu berücksichtigen, werden in der Dienstbeschreibung des Personalisierungsdienstes jedoch nicht behandelt.

Der Dienst bietet keine Zuordnung von Werten zu einem oder mehreren anderen Diensten an. Diese kann über herstellerspezifische Schnittstellen unterstützt werden.

5.4.2. Interaktionen

Die Funktionen dieses Dienstes stehen oft für sich alleine und sind sehr generisch. Daher werden im Folgenden drei beispielhafte Abläufe im Zusammenhang mit dem Dienst beschrieben, bei denen die Funktionsaufrufe in einen größeren Zusammenhang eingebettet sind.

Auf den Personalisierungsdienst kann von verschiedenen Komponenten aus zugegriffen werden, zum Beispiel von der EKAP oder von Mehrwertdiensten aus. Um zu unterstreichen, dass es sich bei den im Folgenden gezeigten Zugriffen auf den Personalisierungsdienst um beispielhafte Abläufe ohne konkrete Festlegung der anderen Kompo-

nenten handelt, wird in den untenstehenden Diagrammen von beliebigen Mehrwertdiensten — welche in beliebigen Ausprägungen vorkommen können und hier nicht näher spezifiziert werden — gesprochen. Zugriffe von anderen Komponenten aus finden nach demselben Muster statt.

5.4.2.1 Werte speichern und abrufen

Im ersten Beispiel wird gezeigt, wie ein Reisender auf unterschiedliche Mehrwertdienste zugreift, welche den Personalisierungsdienst nutzen, um Konfigurationseinstellungen abzulegen und wieder abzurufen.

Dabei wird illustriert, dass zu jedem gespeicherten Wert ein eindeutiger Identifikator gehört. Erstmaliges Speichern eines Wertes für einen Identifikator legt einen Wert im Speicher an, erneutes Speichern unter demselben Identifikator überschreibt den ursprünglichen Wert.

Des Weiteren wird im Beispiel gezeigt, dass die Werte vom Personalisierungsdienst dauerhaft gespeichert werden, auch wenn beispielsweise inzwischen ein anderer Mehrwertdienst genutzt wird.

Um klarzustellen, dass in der standardisierten Form keine Zuordnung zwischen Werten und Diensten stattfindet (der Dienst kann bei Bedarf durch herstellerspezifische Schnittstellen um diese Funktionalität erweitert werden), dass ein Mehrwertdienst einen ursprünglich von einem anderen Mehrwertdienst abgelegten Wert überschreiben kann.

ELBDRUCK

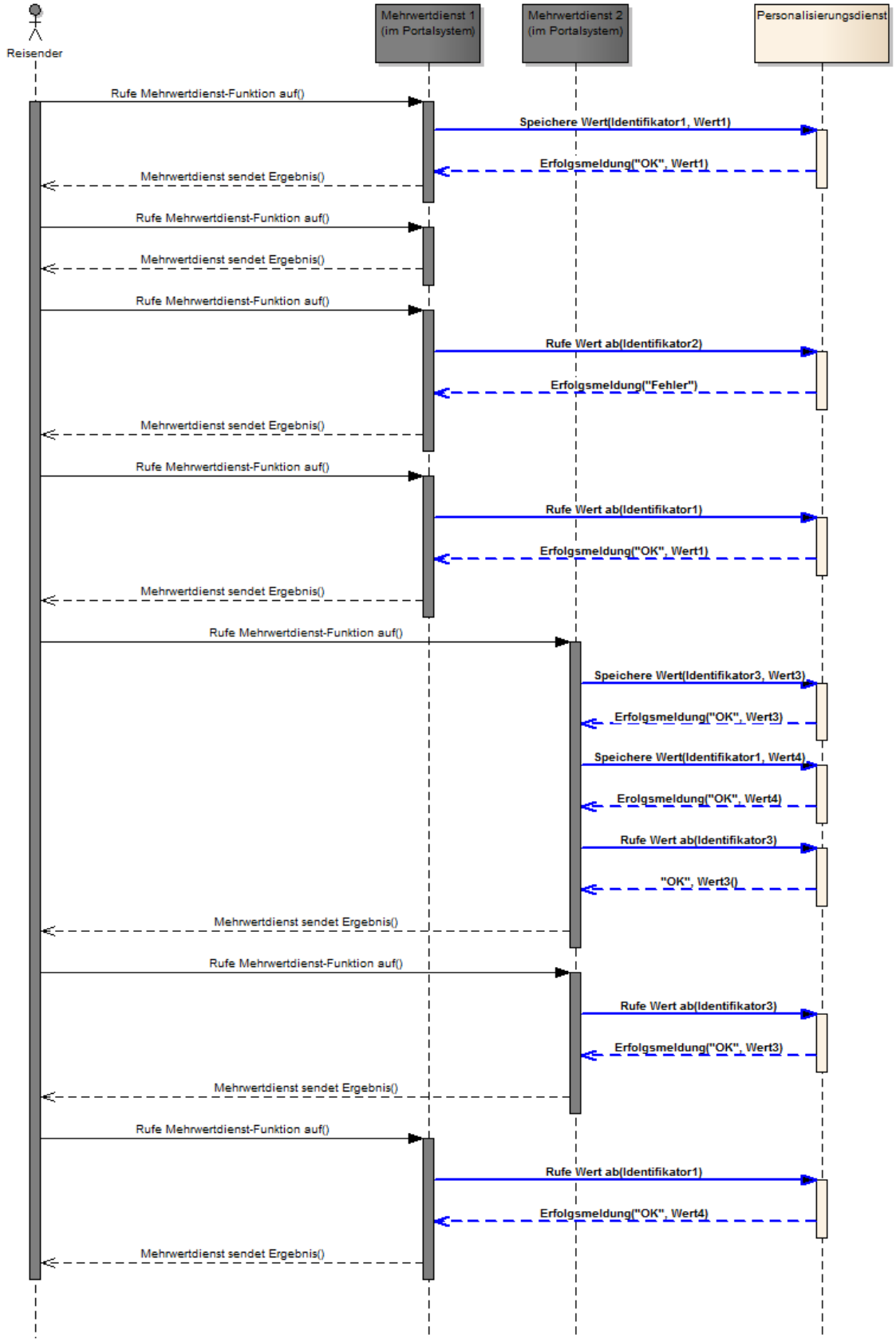

Abbildung 11: Sequenzdiagramm Personalisierung

5.4.2.2 Lebenszyklus eines Wertes

Das folgende Beispiel zeigt auf, wie ein Wert über den Personalisierungsdienst abgelegt und wieder gelöscht werden kann.

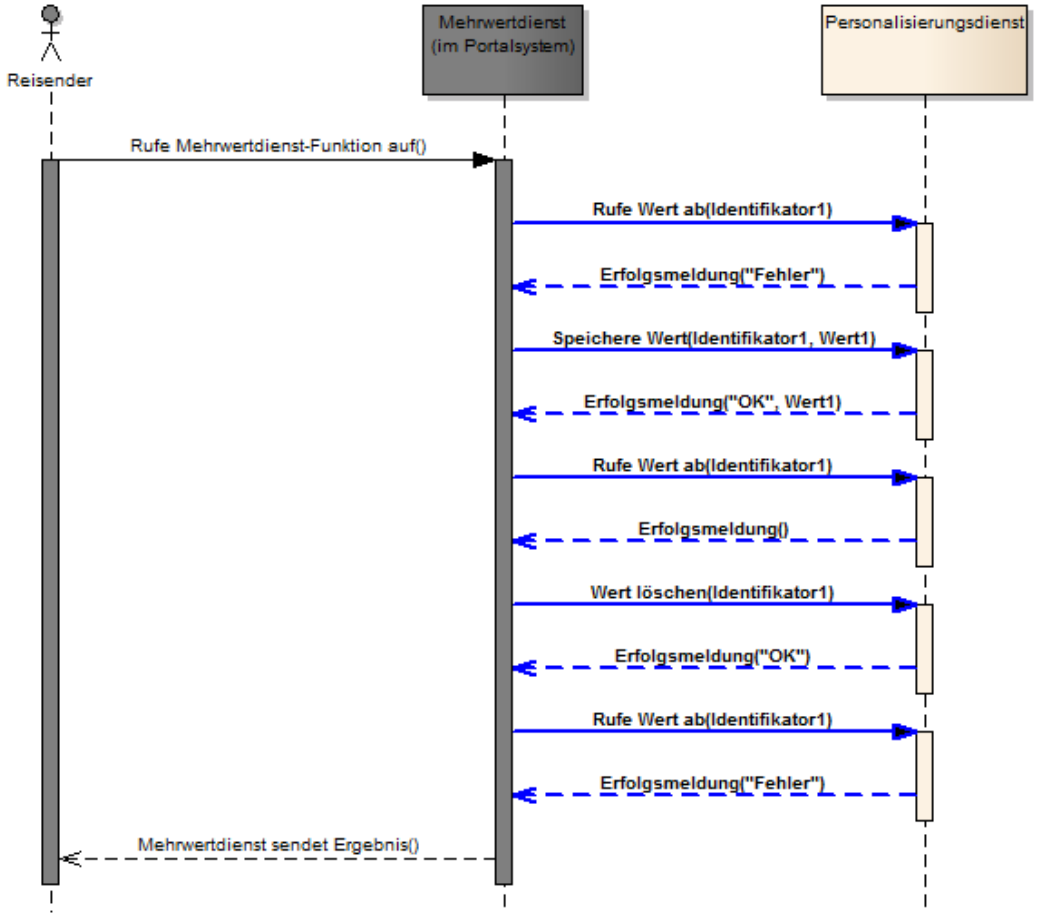

Abbildung 12: Sequenzdiagramm Lebenszyklus eines Wertes

5.4.2.3 Werteliste ermitteln

In diesem Beispiel ist dargestellt, wie die Funktion zum Auflisten der verfügbaren Werte funktioniert.

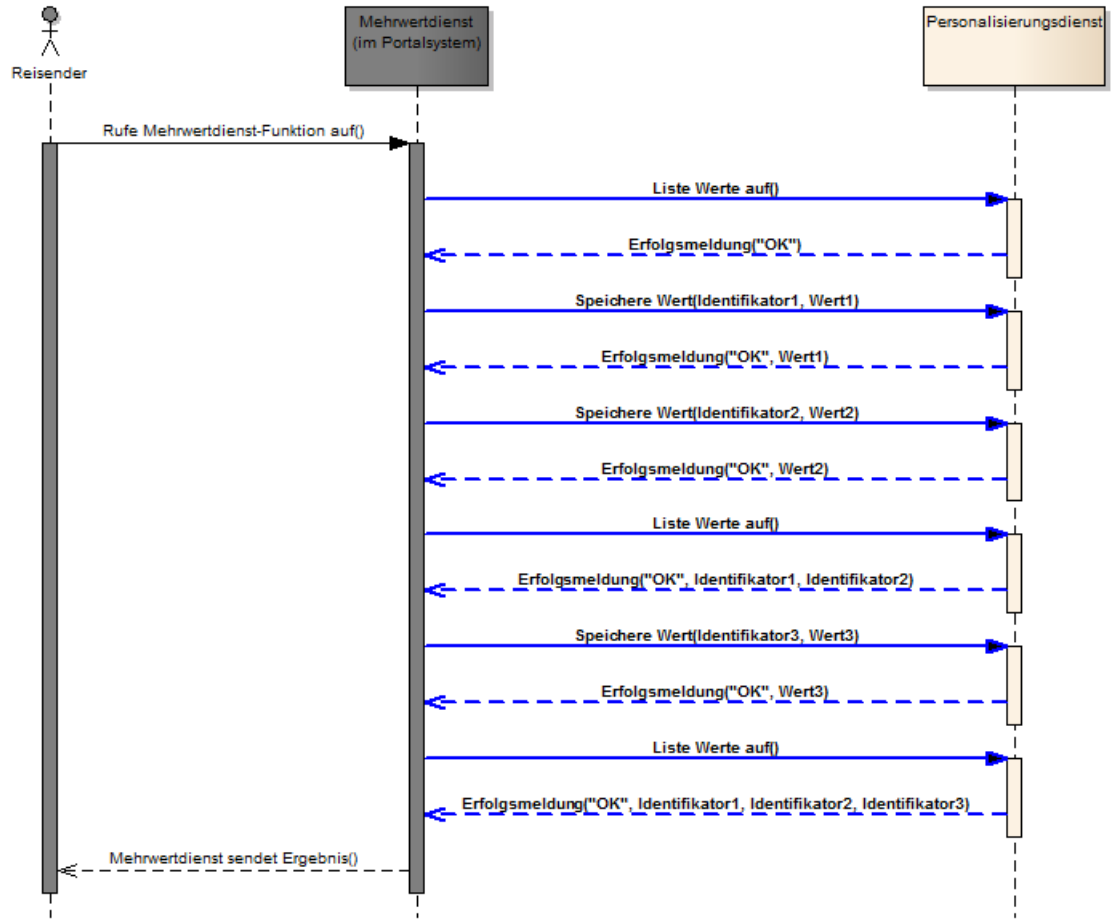

Abbildung 13: Sequenzdiagramm Werteliste ermitteln

5.4.3. Betroffene Komponenten:

Dienstanbieter: Personalisierungskomponente
Dienstabnehmer: Komponenten des Portalsystems und der EKAP

5.4.4. Funktion 1: Speichern eines Werts

Eingangsdaten

- Identifikator des Werts
- Wert

Ausgangsdaten

- Erfolgsmeldung
- gespeicherter Wert

5.4.5. Funktion 2: Abrufen eines Werts

Eingangsdaten

- Identifikator des Werts

Ausgangsdaten

- Erfolgsmeldung
- Wenn vorhanden: abgerufener Wert

5.4.6. Funktion 3: Löschen eines Werts

Eingangsdaten

- Identifikator des Werts

Ausgangsdaten
- Erfolgsmeldung

5.4.7. Funktion 4: Verfügbare Werte auflisten

Eingangsdaten
- (keine)

Ausgangsdaten
- Erfolgsmeldung
- Liste der Identifikatoren aller gespeicherten Werte

5.5. Verwaltung semantischer Datenmodelle - SV2.Modellverwaltung

5.5.1. Zweck

Der Modellverwaltungsdienst ermöglicht es anderen Diensten, sich die aktuellen Versionen des Klassifikations- und Interaktionsmodells sowie des Kontextmodells anzeigen zu lassen und liefert die Modelldateien auf Anfrage aus. Diese Dienstebeschreibung stellt die Minimalkonfiguration des Dienstes dar. Ein Modellverwaltungs-Dienst muss die unten gelisteten Funktionen in jedem Fall umsetzen. Weitere Ausbaustufen sind möglich.

5.5.2. Betroffene Komponenten

Dienstanbieter: Modellserver
Dienstabnehmer: Semantik-Komponente, Drittanbieter

5.5.3. Funktion 1: Auflisten der Modellversionen

Eingangsdaten:
- Modellname, nach dem angefragt wird

Ausgangsdaten:
- Liste der verfügbaren Versionen und ihrer Dateinamen
- Im Fehlerfall: Fehlermeldung zurückgeben

5.5.4. Funktion 2: Ausliefern einer Modelldatei

Eingangsdaten:
- Dateiname

Ausgangsdaten:
- Angefragte Datei
- Im Fehlerfall: Fehlermeldung zurückgeben

5.6. Pushdienst – SV2.Pushdienst

5.6.1. Zweck

Dieser Dienst abstrahiert von den verschiedenen Pushtechnologien der Mobiltelefonanbieter und ermöglicht dadurch neue Mitteilungen auf das mobile Telefon proaktiv zuzustellen.

5.6.2. Interaktionen

Dienste des Portalsystems interagieren mit dem Pushdienst, um zum einen die Mobiltelefonanwender für den Pushdienst zu registrieren und zum anderen die Mitteilungen auf die entsprechenden Geräte proaktiv zukommen zu lassen.

5.6.3. Betroffene Komponenten

Dienstanbieter: Portalsystem
Dienstabnehmer: Portalsystem

5.6.4. Funktion 1: Mobiles Endgerät für den Pushdienst registrieren

Diese Methode ermöglicht es einen Mobiltelefonanwender, sich für den Pushdienst seines Betriebssystemherstellers anzumelden. Hierbei kann es sich zum Beispiel um den Pushdienst von Apple oder Android handeln.

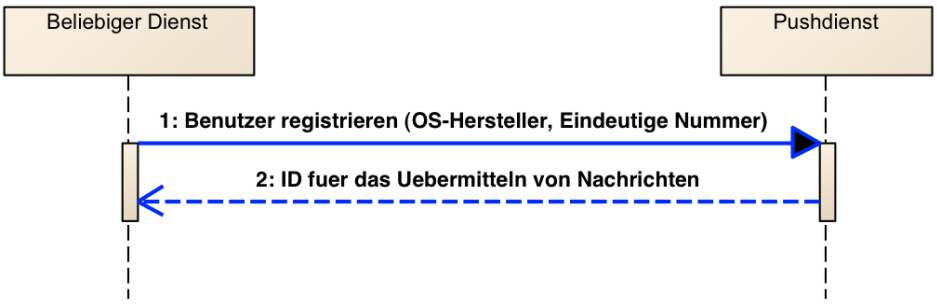

Abbildung 14: Pushdienst - Benutzer registrieren

Eingangsdaten:

- Betriebssystemhersteller (OS-Hersteller)
- Eindeutige Nummer, die jedes mobile Endgerät identifiziert

Ausgangsdaten:

- Als Ergebnis wird eine ID zurückgeliefert, die für das aktive Übermitteln der Nachrichten an das mobile Endgerät notwendig ist.

5.6.5. Funktion 2: Eine Mitteilung übermitteln

Diese Methode erlaubt das Übermitteln einer beliebigen Freitextnachricht an den Endanwender.

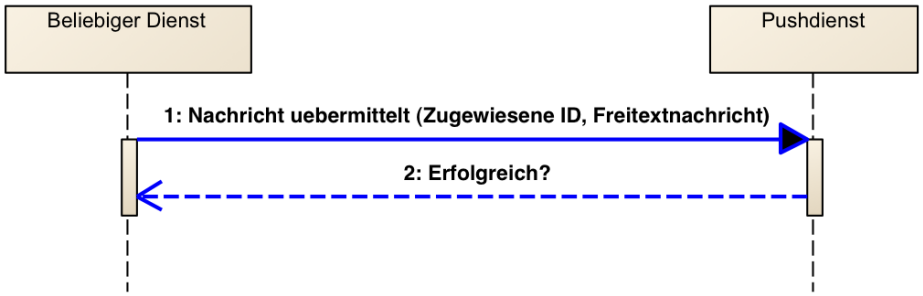

Abbildung 15: Pushdienst - Nachricht übermitteln

Eingangsdaten:

- Die bei der Registrierung zugewiesene ID
- Freitextnachricht

Ausgangsdaten:

- Zurückgeliefert werden kann eine Zustandsmeldung über den Erfolg des Vorganges.

5.6.6. Funktion 3: Mobiles Endgerät vom Pushdienst abmelden

Erlaubt das Abmelden eines zuvor angemeldeten mobilen Endgerätes von der Liste des Pushdienstes.
Eingangsdaten:

- Eindeutige Nummer, die jedes mobile Endgerät identifiziert

Ausgangsdaten:

- Erfolgsmeldung

5.7. Mehrwertdienste - SV2.Mehrwertdienste

5.7.1. Zweck

Die Mehrwertdienste sind Dienste externer Anbieter, die vom mobilen Endgerät bzw. dem Portalsystem genutzt werden können. Beispielsweise gehören dazu Dienste für Buchungen, Reservierungen, Fahrgeldmanagement oder zusätzliche Informationsdienstleistungen, z. B. Wetterdienste. Solche Mehrwertdienste liegen außerhalb des Projektfokus‘ und werden daher an dieser Stelle nur abstrakt betrachtet. Im weiteren Projektverlauf werden die Mehrwertdienste nicht weiter behandelt. Einzelne der für diese Mehrwertdienste nötigen, im Folgenden beschriebenen Grundfunktionalitäten werden allerdings auch durch im Projekt bearbeitete Dienste umgesetzt oder verwendet werden. Dies ergibt sich durch die jeweiligen Dienstebeschreibungen.

Abstrahiert und zusammengefasst ergeben sich folgende einzelne Grundfunktionalitäten von Mehrwertdiensten (siehe Tabelle 3). *Datenerhebung*, *Datensicherung und -verwaltung*, *Datenübertragung* sowie *Meldungen an Fahrgast* bilden allerdings die Grundlage für die Umsetzung. Die *Anbindung an geräteexterne Dienste* ist nur bei Vorhandensein dieser Grundfunktionalitäten überhaupt möglich.

Datenerhebung	*Implizite Datenerhebung:* Das Portalsystem muss vom mobilen Endgerät bzw. der Anwendung auf dem mobilen Endgerät Daten implizit, also ohne direkte Eingabe durch den Nutzer, erheben können. Das betrifft mindestens Positionsdaten (z. B. GPS), die etwa über Gerätesensoren/-dienste oder Kommunikation mit externen Diensten (z. B. EKAP, Fahrzeug) erhoben werden können. *Explizite Datenerhebung:* Das Portalsystem muss über das mobile Endgerät bzw. die Anwendung Daten explizit vom Nutzer erheben können. Dies betrifft z. B. Präferenzen, Konfigurationsdaten (z. B. welche Reiseinformationen geteilt werden sollen), Kontaktdaten etc.
Datensicherung und -verwaltung	Das mobile Endgerät bzw. die Anwendung oder das Portalsystem muss solche erhobenen Daten speichern können, z. B. auf dem Gerät, einem wechselbaren Speichermedium oder in einer Datenbank. Die abgespeicherten Daten müssen durch den Fahrgast verwaltet – also geändert, gelöscht etc. – werden können. Eventuelle externe Speicherung von Daten, also außerhalb von Gerät und Portalsystem z. B. in einem Profildienst, ist ein von einem Drittanbieter angebotener Mehrwertdienst und gehört daher zur Funktionalität *Anbindung an geräteexterne Dienste*. Ein Beispiel hierfür ist der Personalisierungsdienst, der nutzerbezogene Daten zwecks zukünftiger Individualisierung von Diensten (z. B. Suchkriterien, Vorlieben, Reiseeinschränkungen etc.) speichert und entsprechend bereitstellt.

Datenübertragung	*Nutzerinitiierte Datenübertragung:* Das Portalsystem muss mittels mobilem Endgerät bzw. Anwendung (erhobene) Daten übermitteln können, z. B. an die EKAP oder Drittanbieter. Dies betrifft neben textbasierten auch multimediale Inhalte wie Bilder, Videos, Audio etc. Der Initiator dieser Datenübertragung ist der Fahrgast. *Automatische Datenübertragung (Updates):* Das Portalsystem muss Daten automatisch, also ohne Nutzerinitiierung übertragen können. Dies betrifft (a) Datenübertragung im Rahmen von Updates sowie (b) bei Kommunikation mit der EKAP. Das bedeutet für (a), im Falle von Änderungen an zuvor nutzerinitiiert an einen Kommunikationspartner A übertragenen Daten (s.o.) müssen diese Änderungen ebenfalls an A übertragen werden. Dies betrifft z. B. Reiseinformationen. Für (b) bedeutet es, dass nutzerinitiierte Datenübertragung mit vorhandenen implizit erhobenen Daten (z. B. Fahrzeuginformationen) angereichert wird. Diese zusätzlich angereicherten Daten müssen für den Nutzer einzusehen sein. Der Nutzer muss automatische Datenübermittlung verhindern/verbieten können.
Meldungen an Fahrgast	Das Portalsystem muss über das mobile Endgerät bzw. die Anwendung zu Nutzerbenachrichtigungen in der Lage sein. Dies betrifft zwei Arten von Meldungen: • Notifikation • Feedback Bei Notifikationen wird der Fahrgast über geänderte Zustände informiert, z. B. bei Änderungen an Fahrtdaten oder beim Eingang von Anfragen oder Meldungen der EKAP, Drittanbieter oder anderer Fahrgäste. Notifikationen werden zumeist von der Datenquelle oder einer die Daten überwachenden Instanz initiiert. Für das Projekt sind dies Portalsystem oder Drittanbieter bzw. EKAP. Bei Feedback wird der Nutzer über den Zustand der Ausführung einer geräteeigenen Funktion (z. B. Vibration, Blinken) informiert, z. B. über eine abgeschlossene Datenübertragung. Dazu muss der Fahrgast den Zustand und die betreffenden Daten einsehen können.
Anbindung an geräteexterne Dienste	Das Portalsystem muss eine Anbindung an geräteexterne Dienste haben. Dies betrifft unter anderem die Anbindung an die EKAP über die TRIAS-Schnittstelle, aber auch Anbindungen an Dienste von Drittanbietern. Diese Anbindung soll über Schnittstellen erfolgen, über die Daten vom Portalsystem aus an diese geräteexternen Dienste übermittelt sowie von ihnen empfangen werden können. Dies ermöglicht die Inanspruchnahme externer Dienste, z. B. von Buchungsdiensten, e-Ticketing, externen Informationsdiensten etc.

Tabelle 3: Übersicht über die Grundfunktionalitäten von Mehrwertdiensten

5.7.2. Interaktionen

Das mobile Endgerät muss über die technischen Voraussetzungen zu Dateneingabe durch den Nutzer, Datenvorhaltung (festes oder wechselbares Speichermedium) sowie Datenübermittlung verfügen. Daten müssen vom Nutzer angefordert werden können.

Fahrzeugidentifikationsdaten (z. B. Fahrt-ID, Fahrzeug-ID, Perlschnur) sowie Positionsdaten sollten bekannt sein.

Das mobile Endgerät muss über Kommunikationskanäle zu Geräte externen Diensten verfügen z. B. über eine Datenverbindung mit Drittanbietern. Für die Kommunikation im Rahmen von Mehrwertdiensten müssen folgende Schnittstellen bereitstehen:

mobile Endgerät ↔ Portalsystem

Portalsystem ↔ EKAP

Portalsystem ↔ Drittanbieter.

Portalsysteme kommunizieren unter einander auch über die Schnittstelle „Drittanbieter“.

Sind diese Voraussetzungen erfüllt, finden für diesen Dienst folgende Interaktionen statt:

mobile Endgerät bzw. Portalsystem zu Dritten (vgl. Abbildung 16)

mobile Endgerät bzw. Portalsystem zu EKAP

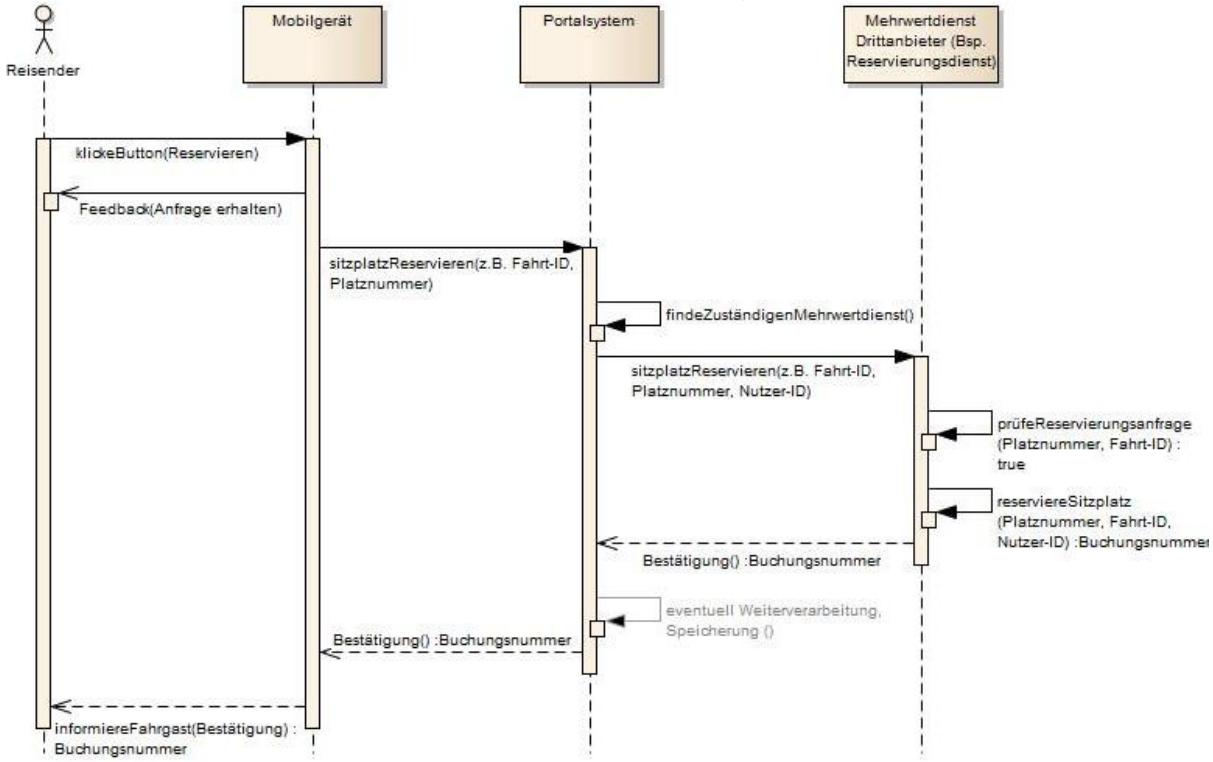

Abbildung 16: Beispielhafter, vereinfachter Interaktionsablauf für eine Sitzplatzreservierung via Drittanbieter

5.7.3. Betroffene Komponenten

Dienstanbieter: EKAP, Drittanbieter, Portalsystem
Dienstabnehmer: Mobiles Endgerät, Portalsystem

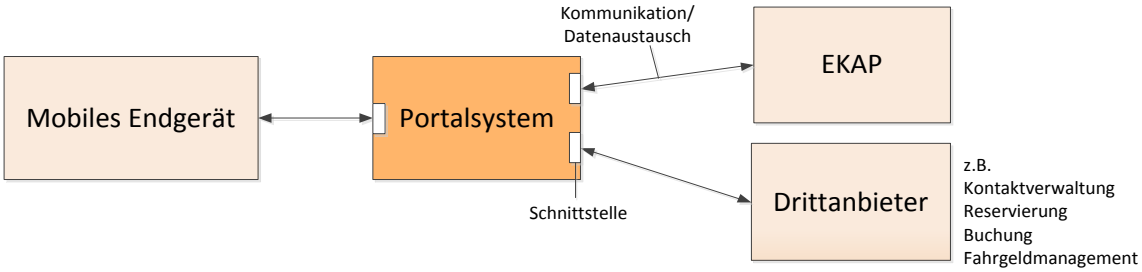

Abbildung 17: Darstellung der Komponenten und Schnittstellen für die Kommunikation

5.7.4. Funktion 1: Datenerhebung

Eingangsdaten

- Implizit oder explizit erhobene Daten, z. B.
- Fahrzeugidentifikationsdaten
- Positionsdaten (z. B. GPS)
- Fahrgasteingaben (Konfigurationsinformationen, Präferenzen, Kontaktdaten etc.)
- Informationen zum Fahrschein (Ticket-ID/TicketKlasse) und Fahrweg (aus Reiseinformationen)

Ausgangsdaten

- Ggfs. Bestätigung der Dateneingabe (vgl. Feedback, Funktion 4)
- Falls angefordert: Anzeige der erhobenen Daten für Fahrgast
- Im Fehlerfall: Fehlermeldung zurückgeben (vgl. Feedback, Funktion 4)
- Bei nicht implementierter Funktion: Hinweis hierauf als Fehlercode

5.7.5. Funktion 2: Datensicherung und -verwaltung

Eingangsdaten

- Kontaktdaten
- Weitere Daten aus Mehrwertdiensten (optional)

Ausgangsdaten

- Bestätigung der Datenspeicherung bzw. -änderung (vgl. Feedback, Funktion 4)
- Im Fehlerfall: Fehlermeldung zurückgeben (vgl. Feedback, Funktion 4)

5.7.6. Funktion 3: Datenübertragung

Eingangsdaten

- Explizit oder implizit erhobene Daten (Präferenzen, Favoriten, Reiseinformationen, Fahrzeugidentifikations-/Positionsdaten)
- Explizit referenzierte Multimedia-Daten (z. B. Bilder, Videos, Audio) Updates (z. B. Änderungen von Reiseinformationen) bzw. Störungsmeldungen für zuvor übermittelte (Reise-)Daten

Ausgangsdaten

- Ggfs. Bestätigung der Datenübertragung (vgl. Feedback, Funktion 4)
- Optional: von Drittanbietern (Dienste, andere Fahrgäste) erhaltene Daten (z. B. Anfragen, Reiseinformationen, Resultate von Anfragen)
- Im Fehlerfall: Fehlermeldung zurückgeben (vgl. Feedback, Funktion 4)

5.7.7. Funktion 4: Meldungen an Fahrgast

Eingangsdaten

- Geräte-/anwendungsinterne, z. B.

    - Resultat einer geräteintern ausgeführten Funktion wie Speichervorgang
    - Bestätigungsanforderung zum Zweck der Funktionsausführung, z. B. Einfordern der Bestätigung/Ablehnung für Übermittlung (implizit) erhobener Daten (z. B. GPS-Daten)
- Geräte-/anwendungsexterne, z. B.
    - von Kontaktperson eingehende Anfrage
    - Resultat einer Datenübertragung
    - Resultat einer Kommunikation mit Drittanbieter/EKAP bzw. von Drittanbieter eingehende Anforderungen

Ausgangsdaten
- Meldung an Nutzer
- gemäß den vom mobilen Endgerät bereitgestellten Funktionalitäten (z. B. Audio, Vibration, Anzeige etc.)
- Ggfs. Bestätigungs-/Eingabeaufforderung

5.7.8. Funktion 5: Anbindung an geräteexterne Dienste

Eingangsdaten
- Vom externen Dienst angeforderte Daten, z. B. Funktionsparameter wie
- Reisedaten
- Kontaktdaten
- Fahrtinformationen, Positionsdaten, o. ä.
- Daten sind explizit (Fahrgasteingaben) oder implizit (z. B. GPS-Daten) erhoben

Ausgangsdaten
- Ggfs. Bestätigung der Datenübertragung (vgl. Feedback, Funktion 4)
- Resultat der Anfrage/vom Drittanbieter erhaltene Daten
- Endresultat der Kommunikation, z. B. Reiseauskünfte, Meldung/Resultat für ausgeführten Reservierungs-/Buchungsvorgang, erworbenes e-Ticket
- Zwischenstand wie Meldung an Nutzer, z. B. Nachfordern von Daten durch externen Dienst, weiterer Transaktionsschritt etc.
- Im Fehlerfall: Fehlermeldung zurückgeben (vgl. Feedback, Funktion 4)

5.8. EKAP-Registerdienst – SV2.EKAPRegisterdienst

5.8.1. Zweck

Mit den Funktionen dieses Dienstes lassen sich die Informationen über EKAPs (vgl. Komponentenbeschreibung in Abschnitt 4.6) über EKAPs verwalten, auf die ein Portalsystem zugreifen kann. Dies umfasst Verwaltungsfunktionen für die EKAP-Datensätze, die zum Registrieren und Entfernen von EKAPs verwendet werden können. Ebenso wird eine Funktion bereitgestellt, über die ein Portalsystem die im EKAP-Register gespeicherten Informationen zu den ihm bekannten EKAPs ermitteln kann.

5.8.2. Interaktionen

Im folgenden beispielhaften Ablauf wird gezeigt, wie eine EKAP bei einem EKAP-Registerdienst registriert wird und dann in der Liste der verfügbaren EKAPs auftaucht. Anschließend wird die EKAP wieder bei dem Registerdienst abgemeldet und ist danach nicht mehr in der zurückgegebenen Liste enthalten.

Schließlich wird noch versucht, eine überhaupt nicht beim betrachteten EKAP-Register registrierte EKAP von dort zu löschen, was in einer Fehlermeldung resultiert.

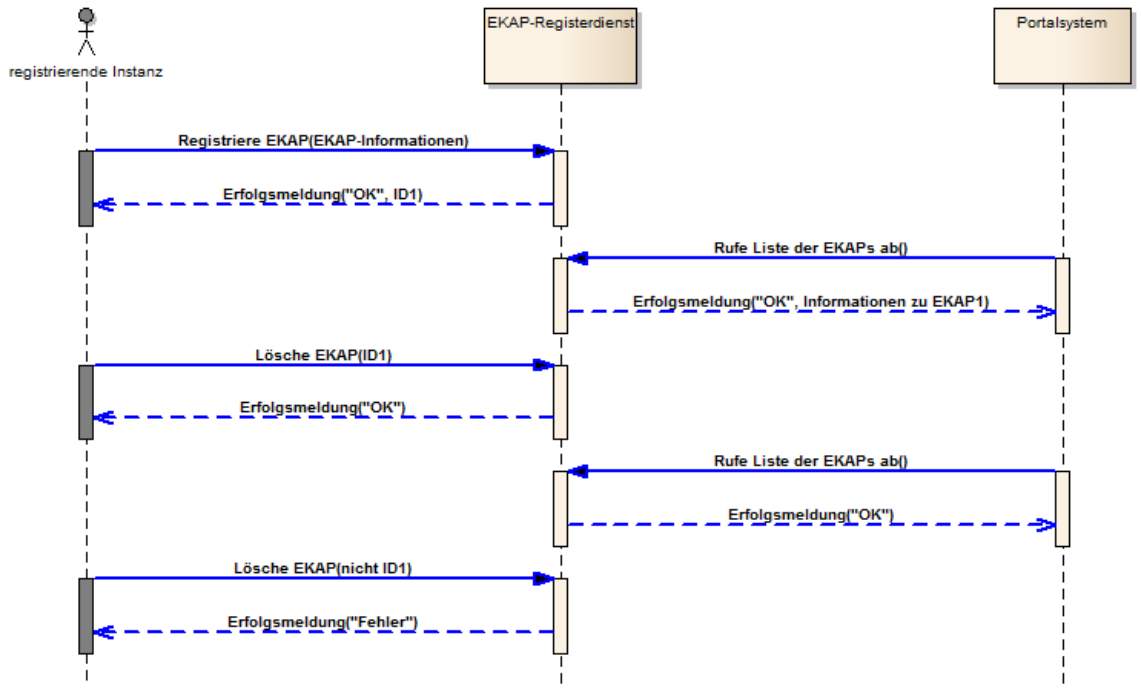

Abbildung 18: Sequenzdiagramm EKAP-Registerdienst

Diejenige Instanz, welche die Registrierung und Entfernung einer EKAP durchführt, ist hier nicht genauer beschrieben. Wie in der Komponentenbeschreibung zur Anfragesteuerung beschrieben, kann es sich hierbei sowohl um Personen, die manuell Eingaben vornehmen, als auch um automatische Dienste handeln, bei denen die benötigten Angaben zur EKAP hinterlegt sind und die somit die Eintragung selber durchführen können.

5.8.3. Betroffene Komponenten:

Dienstanbieter: Portalsystem (Anfragesteuerung)
Dienstabnehmer: Portalsystem (insbesondere Anfragesteuerung), EKAP

5.8.4. Funktion 1: Registrieren einer EKAP

Eingangsdaten

- EKAP-Adresse
- Anbieter-ID
- Schnittstellenversion

Ausgangsdaten

- Erfolgsmeldung
- EKAP-ID

5.8.5. Funktion 2: Aktualisieren einer EKAP

Eingangsdaten

- EKAP-ID
- EKAP-Adresse
- Anbieter-ID
- Schnittstellenversion

Ausgangsdaten

- Erfolgsmeldung

5.8.6. Funktion 3: Löschen einer EKAP

Eingangsdaten

- EKAP-ID

Ausgangsdaten

- Erfolgsmeldung

5.8.7. Funktion 4: Liste der EKAPs abrufen

Eingangsdaten

- Suchkriterien wie:
- erlaubte EKAP-IDs
- erlaubte EKAP-Adressen
- erlaubte Anbieter-IDs
- minimale Schnittstellenversion

Ausgangsdaten

- Erfolgsmeldung
- Eine Liste von passenden EKAPs jeweils mit:
    - EKAP-ID
    - EKAP-Adresse
    - Anbieter-ID
    - Schnittstellenversion

5.9. Anfragesteuerungsdienst - SV2. Anfragesteuerung

5.9.1. Zweck

Diese Stelle bietet den Anlaufpunkt für sämtliche Anfragen, die innerhalb des Portalsystems erzeugt oder von außerhalb an das Portalsystem adressiert wurden. Die Aufgabe dieses Dienstes ist die Koordination dieser Funktionsaufrufe. Daher benötigt die Anfragesteuerung weitere Informationen über die entsprechenden Dienste, die außerhalb des Portalsystems liegen, um die Anfragen weiterleiten zu können. Neben der wichtigen Aufgabe der Weiterleitung der Methodenaufrufe bietet der Dienst auch die Möglichkeit mehrere Anfragen zusammenzufassen. Dies ist beispielsweise bei einer Meldung von Umstiegszahlen relevant: An Stelle einer separaten Meldung für jeden Benutzer wird eine kumulative Nachricht erzeugt.

5.9.2. Interaktionen

Das Sequenzdiagramm verdeutlicht die Funktionsweise des Dienstes anhand einer beispielhaften Schadensmeldung, die von einem mobilen Endgerät abgesetzt wird. Dabei nimmt der Anfragesteuerungsdienst die Meldung entgegen und erkundigt sich nach der entsprechenden EKAP-Adresse im EKAP-Registerdienst. Auf Basis der Rückmeldung wird die Nachricht an die EKAP weitergeleitet.

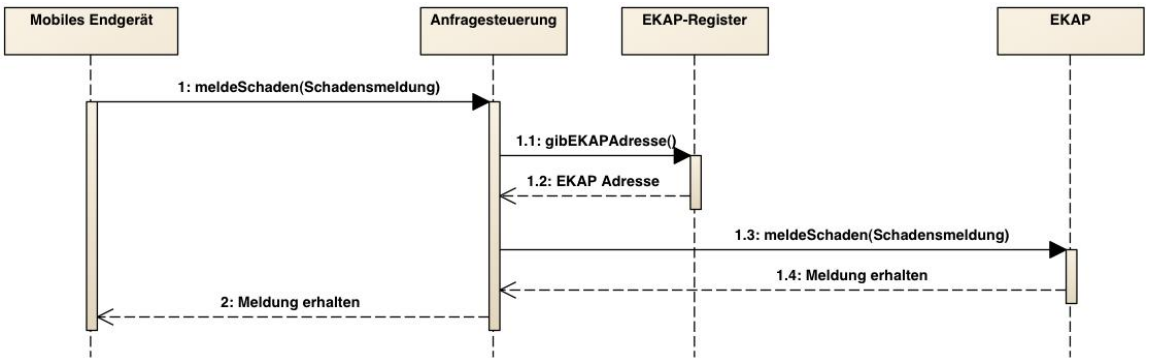

Abbildung 19: Anfragesteuerung

5.9.3. Betroffene Komponenten

Dienstanbieter: Portalsystem
Dienstabnehmer: Portalsystem, EKAP, Mobiles Endgerät

5.9.4. Funktion

Der Dienst implementiert sämtliche Schnittstellen des Portalsystems, der mobilen Endanwendung und der EKAP. Sämtliche Schnittstellenfunktionen leiten die jeweiligen Aufrufe an die entsprechenden Ziele weiter. Die Schnittstelle dieses Dienstes besitzt keine eigenen zusätzlichen Funktionen.

5.10. Physikalische Ortung - SV2.Physikalische_Ortung

5.10.1. Zweck

Der primäre Zweck des Dienstes ist die physikalische Ortung des Benutzers, um einen Startpunkt oder die Position bei der Fußgängernavigation zu bestimmen und unter Umständen eine Assoziation zu einem Fahrzeug oder einer Haltestelle des ÖV herstellen zu können. Dafür werden unter anderem Sensorinformationen des mobilen Endgerätes verwendet.

5.10.2. Interaktionen

Die Interaktionen sind den Sequenzdiagrammen zu entnehmen.

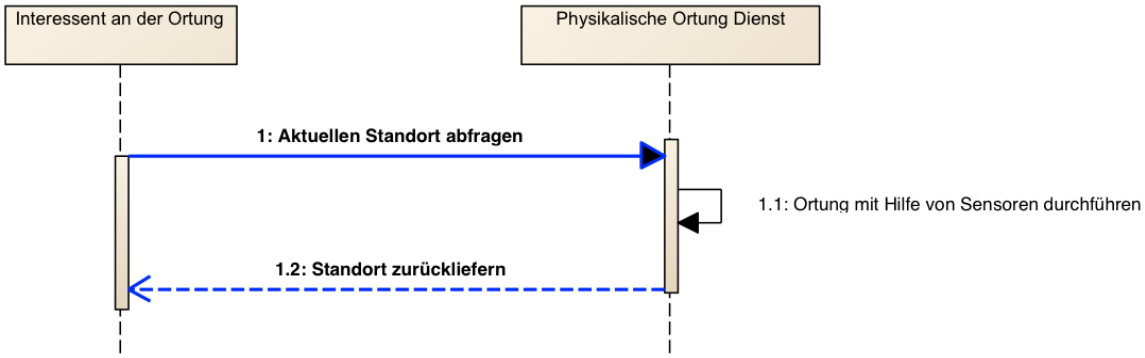

Abbildung 20: Sequenzdiagramm Physikalische Ortung

5.10.3. Betroffene Komponenten

Dienstanbieter: mobiles Endgerät
Dienstabnehmer: jegliche Dienste des Portalsystems, des mobilen Gerätes, die an der aktuellen Positionierung des Benutzers interessiert sind

5.10.4. Funktion 1: Abfrage der Positionierung

Diese Funktion erlaubt eine Positionierung des Benutzers.

Eingangsdaten

- Da der Dienst auf dem mobilen Endgerät läuft, bedarf es keiner Eingangsdaten.

Ausgangsdaten

- Aktuell bestmöglich ermittelte Position des Benutzers

GELBDRUCK

6. Normative Referenzen

- VDV 452 „VDV-Schnittstellen Liniennetz/Fahrplan“
- VDV 453 „Ist-Daten-Schnittstellen“
- VDV 454 „Erweiterung der Ist-Daten-Schnittstellen“
- VDV 455 „VDV-Schnittstelle Dienstplan“
- VDV 7023 „Kommunikation im ÖV (IP-KOM-ÖV) - Szenarien & Personen sowie deren Anforderungen an die Kundeninformation“
- VDV 7025 „Kommunikation im ÖV (IP-KOM-ÖV) - Anwendungsfälle im Umfeld der Echtzeit-Kundeninformation“
- VDV 720 „Kundeninformationen über Abweichungen vom Regelfahrplan“
- VDV 730 „Funktionale Anforderungen an ein itcs - Leitfaden für die itcs-Ausschreibung“

7. Begriffe

Benachrichtigungs-Komponente	Entgegennahme von Abonnements der Benutzer aus dem Portalsystem und der Benachrichtigung dieser über neue vorliegende Ereignisse, für die sie sich eingeschrieben haben.
Betriebsleitsystem	Das Betriebsleitsystem (itcs) fasst alle Einrichtungen zusammen, die für die Überwachung und Steuerung des Fahrbetriebs erforderlich sind. I. d. R. beinhaltet das itcs eine Vielzahl von Unterkomponenten.
Datendrehscheibe	Eine bereits heute vorhandene Datenvermittlungsschicht für den Austausch von Informationen über Verkehrsunternehmen oder Auskunftsplattformen hinweg.
DELFI-Server	DELFI stellt der EKAP die Funktionalitäten des DELFI-Verbundes zur Verfügung. So kann eine EKAP z. B. auf die verteilte Verbindungssuche über mehrere Landesauskunftssysteme hinweg zugreifen.
Dienst	Ist die kleinste Funktionseinheit für die Kommunikation im Netzwerk.
Dienste orientierte Architektur	Eine Software- und Netzwerkstruktur hinter der sich komplexe Zusammenhänge verbergen, die für den Nutzer aber aufgrund der Kapselung von Funktionen in Dienste nicht von Relevanz sind.
Diensteregister	Verzeichnis der Dienste, die diese EKAP anbietet und nutzt. Für jeden registrierten Dienst werden definierte Merkmale festgehalten.

EKAP	Echtzeit-Kommunikations- und Auskunftsplattform, verfügt über eine standardisierte Schnittstelle zum Portalsystem. Es werden darüber hinaus Anforderungen an die datenversorgenden Schnittstellen definiert.
EKAP-Register	Datenbank mit bekannten EKAP-Adressen.
EMS	Ein Ereignis-Management-System kann für folgende Aufgabenstellungen herangezogen werden: • Erfassen von Störungs- und Ereignismeldungen • Verfeinern bestehender Meldungen • Konvertieren von Meldungen in andere Formate • Weiterleitung von Meldungen an andere Systeme
Fahrplanauskunft	Beauskunftung von Reisewünschen auf Basis der Solldatenlage ggf. unter Berücksichtigung der Istdatenlage
Fahrzeugsysteme	Hierbei handelt es sich um die Schnittstelle zum jeweiligen Fahrzeug-Chassis.
Geo-Namensregister	Beinhaltet Informationen zu verschiedenen geografischen Ortsobjekten, was typischerweise Haltestellen, Adressen und POIs umfassen kann.
IV-Router	Berechnet Routen des Individualverkehrs auf dem öffentlichen Straßen- bzw. Wegenetz.
Karten	Generiert für einen gegebenen Kartenausschnitt eine Karte in Bildform, und hält hierzu die erforderlichen Kartendaten vor.
Komponente	Funktionale Einheit in der Systemarchitektur
Mehrwertdienste	Zusammenfassung von zusätzlichen Funktionen, die durch diese Architektur flexibel angebunden werden können, z. B. Socialmedia.
Mobiles Endgerät	Das mobile Endgerät ist das persönliche Gerät des Fahrgastes. Es kann sich hierbei um Smartphones, aber auch Tablet-PCs, Laptops oder ähnliche mobile Geräte handeln.
Modellserver	Ermöglicht es Diensten, sich die aktuellen Versionen des Klassifikations- und Interaktionsmodells sowie des Kontextmodells anzeigen zu lassen und liefert

	die Modelldateien auf Anfrage aus. Hierzu wird in der VDV 431 eine Schnittstelle standardisiert.
Personalisierung	Standardisierte Datenbank, auf der personenbezogene Attribute des Benutzers in einem Standard Datenbankformat hinterlegt werden können.
Planungdatenversorgung	Soll-Fahrplandaten, Fahrzeugumläufen, Dienstpläne, etc.
Portalsystem	Vermittlungsschicht zwischen dem mobilen Endgerät und der EKAP. Die Schnittstelle wird innerhalb von dieser Schrift standardisiert.
Push	Ermöglicht eine ereignisgesteuerte Mitteilung an ein Endgerät.
Semantik	Verknüpfung der drei Modelle Interaktionsmodell, Klassifikationsmodell und Interaktionsmodell.
Stammdaten	Datenversorgung mit selten geänderten Daten (Haltestellendaten o. ä.)
Tarifrechner	Berechnet zu einer bestimmten Verbindungsauskunft die Kosten für die Fahrscheine für die gesamte Verbindung oder Teile der Verbindung und gibt in Frage kommende Fahrscheine zurück.
TRIAS	Travellers‘ Realtime Information and Advisory Standard gemäß der VDV 431-2.
Umschlüsselungsdatenbank	Speichert für einzelne Objekte Zuordnungen von verschiedenen Schlüsseln (Objekt-Identifikatoren, IDs). So ist es möglich, ein Objekt, welches in einem bekannten Schlüsselsystem identifiziert wurde, in ein anderes Schlüsselsystem zu transferieren. Dies ist notwendig, wenn Systeme (mehrere EKAPs) miteinander kooperieren sollen, die unterschiedliche Schlüsselsysteme verwenden.
Verkehrsinfrastruktur	Beinhaltet hier Aspekte wie die Fahrwegsteuerung, Haltestellen, etc.
Zugriffskontrolle	Fasst die Mechanismen für die Autorisierung und Authentifizierung zusammen.

Tabelle 4: Begriffe

8. Abkürzungen

Begriff	Beschreibung
ABAP	Advanced Business Application Programming
ABO	Abonnement
API	Application Programming Interface
APN	Apple Push Notification Service
App	Eine „App“-likation auf dem mobilen Endgerät, die das IP-KOM-ÖV-System nutzt.
BGH	Bundesgerichtshof
BLOB	Binary Large Objects
C2DM	Google Cloud to Device Messaging
COM	Datenbank Element
CRM	Costumer Relation Management
DB AG	Deutsche Bahn Aktiengesellschaft
DELFI	Durchgängige elektronische Fahrplaninformation
EKAP	Echtzeit Kommunikations- und Auskunftsplattform
EMS	Ereignis Management System
GPS	Global Positioning System
IBIS-IP	Integriertes-Bord-Informations-System auf Internet-Protokoll Basis
IBSS	Independent Basic Service Sets
IC	Inter City
ICE	Inter City Express
ID	Identifikation
iOS	iPhone Operation System (Betriebssystem)
IP	Internet Protokoll
IP-KOM-ÖV	Internet Protokoll basierte Kommunikationsdienste für den öffentlichen Verkehr

IRE	Inter Regio Express
itcs	Intermodal-Transport-Control-System
IV	Individual Verkehr
MWD	Mehrwertdienst
NET	Microsoft Programmiersprache
NFC	Near Field Communication
ÖPV	Öffentlicher Personen Verkehr
OS	Operation System
ÖV	Öffentlicher Verkehr
PKI	Public Key Infrastruktur
QR	Quick Response (-Code)
RDF	Resource Description Framework
SAP	Software der Firma SAP
SAP AG	Softwarefirma
SDK	Software Development Kit
SOA	Service Oriented Architecture (Dienste-basierte-Architektur)
SOAP	Simple Object Access Protocol
SSID	Service Set Identifier
SV x	Service x
TRIAS	Travellers‘ Realtime Information and Advisory Standard
W-LAN	Wireless Local Area Network

Tabelle 5: Abkürzungen

9. Abbildungsverzeichnis

Abbildung 1: Umfeld und Schwerpunkte im Projekt IP-KOM-ÖV 9

Abbildung 2: Grobarchitektur ÖV-Umfeld 12

Abbildung 3: Architekturdiagramm Semantik-Komponente im Portalsystem 17

Abbildung 4: Semantik-Komponente im mobilen Endgerät 18

Abbildung 5: Schematische Darstellung des Informationsflusses beim Pushdienst..... 20

Abbildung 6: Sequenzdiagramm der Nutzung von Mehrwertdiensten für die Fälle (1) „Anfrage eines internen MWD durch das Portalsystem“ sowie (2) „Anfrage eines externen MWD“. Fall (2) wird unterschieden in Fall a. „Anfrage eines externen Dienstes durch das Portalsystem“ bzw. Fall b. „Anfrage des Portalsystems durch einen externen MWD“. 26

Abbildung 7: Sequenzdiagramm Fahrtinformation EKAP 28

Abbildung 8: Sequenzdiagramm Abonnement 29

Abbildung 9: Sequenzdiagramm Fahrtinformation Fahrzeug 33

Abbildung 10: Sequenzdiagramm Haltewunsch 35

Abbildung 11: Sequenzdiagramm Personalisierung 38

Abbildung 12: Sequenzdiagramm Lebenszyklus eines Wertes 39

Abbildung 13: Sequenzdiagramm Werteliste ermitteln 40

Abbildung 14: Pushdienst - Benutzer registrieren 42

Abbildung 15: Pushdienst - Nachricht übermitteln 42

Abbildung 16: Beispielhafter, vereinfachter Interaktionsablauf für eine Sitzplatzreservierung via Drittanbieter 45

Abbildung 17: Darstellung der Komponenten und Schnittstellen für die Kommunikation 46

Abbildung 18: Sequenzdiagramm EKAP-Registerdienst 48

Abbildung 19: Anfragesteuerung 50

Abbildung 20: Sequenzdiagramm Physikalische Ortung 50

Abbildung 21: Smartphone Marktanteile USA (Stand: Juli 2011) 60

Abbildung 22: Entwicklung bei dem Kauf eines neuen Smartphones (Stand: August 2011) 61

Abbildung 23: Benachrichtigungsablauf für iOS mit mehreren Anbietern und Konsumenten 61

Abbildung 24: Registrierung 62

Abbildung 25: Authentifizierung des Providers beim APN-Dienst 63

Abbildung 26: Benachrichtigungsablauf für iOS 64

Abbildung 27: Ad-Hoc-Netz mit Multihop [Grafik gemeinfrei] 74

Abbildung 28: Kombination Infrastruktur-Modus und Ad-Hoc-Modus 75

Abbildung 29: Erstellung der Liste 76

Abbildung 30: Auswahl des richtigen Fahrzeuges 76

Abbildung 31: Fahrgast-zu-Fahrzeug Nachrichten 77

Abbildung 32: Fahrzeug-zu-Fahrgast Nachrichten 77

Abbildung 33: Stufen der Belastung 79

Abbildung 34: Aktivitätsdiagramme für manuelle Auswahl und Ad-Hoc-Netzwerk zum Verbindungsaufbau mit dem Fahrzeug-W-LAN am Beispiel einer Reise ohne gespeicherte Reiseplanung 80

Abbildung 35: Aktivitätsdiagramme für den Einsatz von QR-Code und NFC zum Verbindungsaufbau mit dem Fahrzeug-W-LAN am Beispiel einer Reise ohne gespeicherte Reiseplanung 80

Abbildung 36: Marktanteile der Smartphone-Plattformen weltweit im ersten Quartal 2012 83

GELBDRUCK

10. Tabellenverzeichnis

Tabelle 1: Erläuterungen zur Grobarchitektur 15

Tabelle 2: Komponenten-Dienste-Matrix 27

Tabelle 3: Übersicht über die Grundfunktionalitäten von Mehrwertdiensten 44

Tabelle 4: Begriffe 54

Tabelle 5: Abkürzungen 56

Tabelle 6: Vergleich Kommunikationsmedien aus dem Meilenstein „Systemarchitektur“ 70

Tabelle 7: Vergleich der Varianten für den Verbindungsaufbau aus Nutzersicht 81

GELBDRUCK

Anhang

Anhang I. Normativ

Hier werden Beispiele Aufgenommen die zu mächtig für den Fliesstext sind.

Anhang II. Informativ

In diesem informativen Anhang werden drei wesentliche Bereiche bereitgestellt:

A II.1 Pushdienste

Im Rahmen dieses Kapitels soll die Machbarkeit der bestehenden proprietären Push-Dienste auf ihre Anwendung für das Szenario des öffentlichen Personenverkehrs untersucht werden. Primär wird dabei die Funktionsweise von ausgewählten proprietären Push-Diensten beschrieben und auf die einzelnen Rahmenbedingungen eingegangen.

A II.1.1. Proprietäre Pushdienste

Auf dem Markt existiert eine Vielzahl unterschiedlicher Betriebssysteme für mobile Endgeräte. Jeder Betriebssystemhersteller hat ein eigenes proprietäres Protokoll mit einem entsprechenden Dienst entwickelt, um mobile Endgeräte aktiv über das Vorliegen von neuen Informationen zu informieren. Um nicht jeden dieser Dienste in Detail zu analysieren, aber dennoch einen Großteil der Endgeräte abzudecken, wird sich im Rahmen von IP-KOM-ÖV auf bereits vorhandene Marktanalysen berufen, um die Marktanteile der jeweiligen Smartphone-Hersteller zu identifizieren.

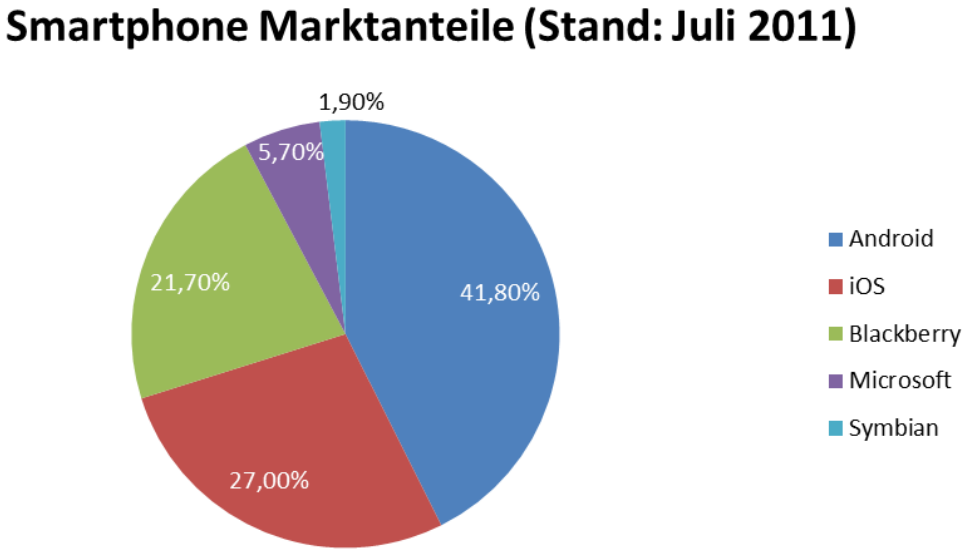

Abbildung 21: Smartphone Marktanteile USA (Stand: Juli 2011)

Die Abbildung 21 demonstriert die Marktanteile der fünf meistverbreiteten Betriebssysteme für Smartphones. Dabei ist zu beachten, dass alleine Android und iOS zusammen auf einen Marktanteil von ca. 70 % kommen. Diese Statistik ist auch von einer anderen Quelle bestätigt worden und ist der Abbildung 22 zu entnehmen. Weiterhin ist es auffällig, dass der Marktanteil von Android stark ansteigt, während der Anteil von iOS kon-

stant bleibt. Angesichts dieser Entwicklung wird im Rahmen dieses Machbarkeitsnachweises ein Fokus auf die Betriebssysteme Android und iOS gelegt, wobei für die Untersuchung gilt, dass die Grundkonzepte sehr ähnlich und auf andere proprietäre Push-Dienste übertragbar sind.

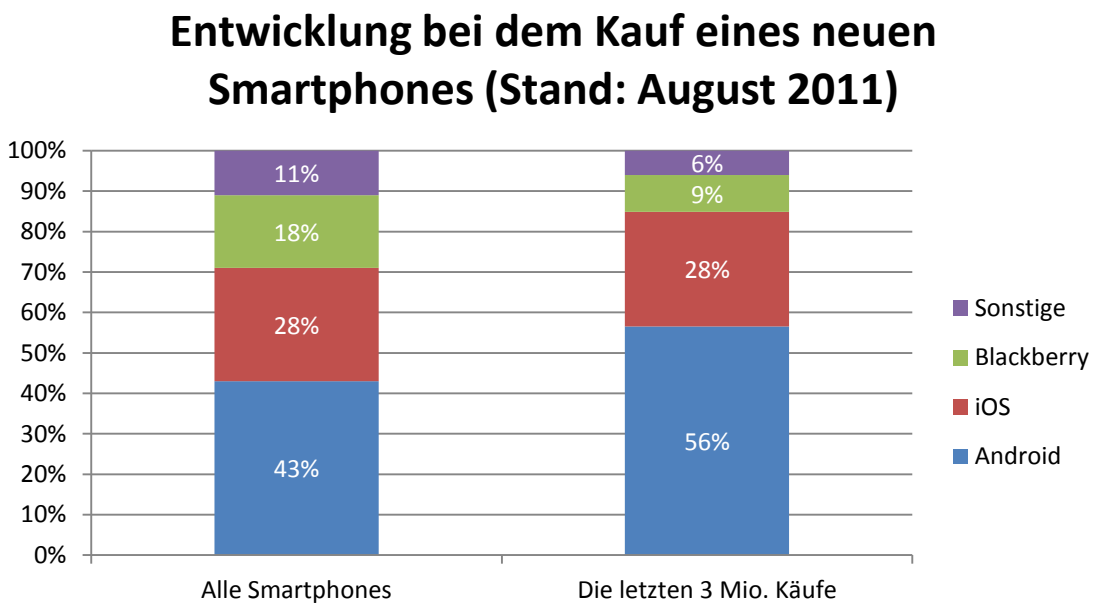

Abbildung 22: Entwicklung bei dem Kauf eines neuen Smartphones (Stand: August 2011)

A II.1.2. Apple Push Notification Service (APNs)

Der von Apple für das Betriebssystem iOS angebotene Push-Dienst agiert als Intermediär zwischen einem mobilen Endgerät und einer dritten Partei, die eine Benachrichtigung zustellen möchte. Das Adressierungsproblem von mobilen Endgeräten in einem öffentlichen Telekommunikationsnetz wird sowohl von iOS als auch von Android, wie später ebenfalls beschrieben, durch eine offene und dauerhafte Verbindung zwischen dem Apple Push Notification Service (APNs) und dem mobilen Endgerät realisiert. Die Idee ist, das mobile Endgerät die Verbindung zum APN-Dienst aufbauen zu lassen und den Rückkanal für die Auslieferung der Benachrichtigungen zu nutzen. Ein abstrahierter Ablauf für mehrere Anbieter und Konsumenten ist in der Abbildung 23 dargestellt.

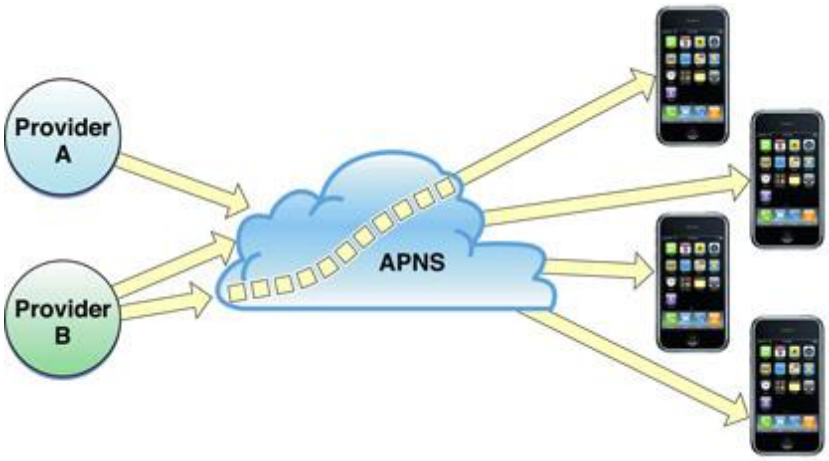

Abbildung 23: Benachrichtigungsablauf für iOS mit mehreren Anbietern und Konsumenten

Nachfolgend werden die Schritte der Registrierung von mobilen Endgeräten, Registrierung des Providers und Benachrichtigung der Interessenten im Detail beschrieben und auf die Anwendbarkeit im Rahmen von IP-KOM-ÖV analysiert.

A II.1.3. Registrierung von mobilen Endgeräten

Um als mobiles Endgerät Benachrichtigungen zu empfangen und um als Anbieter entsprechende Informationen den Fahrgästen zukommen zu lassen, bedarf es beim APN-Dienst einer vierstufigen Registrierung.

Sobald eine erste Applikation, die die Push-Funktionalität unterstützt, auf einem iOS-Gerät installiert wird, erfolgt ein Aufbau zum APN-Dienst mit der Bitte um Erstellung eines eindeutigen Geräte-Tokens (Identifizierungszeichen) ohne ein Gültigkeitsdatum. Ab diesem Augenblick steht das mobile Endgerät dauerhaft mit dem APN-Dienst in Verbindung und wartet darauf, mögliche Benachrichtigungen zu empfangen. Der erstellte Geräte-Token wird an das mobile Endgerät zurückgeschickt, damit er in nachfolgenden Interaktionen als Referenz genutzt werden kann. Alle weiteren Anwendungen können diesen Token direkt am mobilen Endgerät erfragen. Das ist als Schritt drei dargestellt. Im abschließenden Schritt wird er an den Datenanbieter (Provider) weitergeleitet. Die Abbildung 24 demonstriert die beschriebenen Schritte.

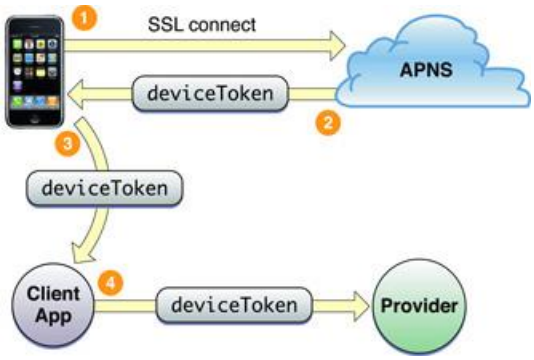

Abbildung 24: Registrierung

Dieser Ablauf stellt für den Einsatz im Rahmen von der spezifizierten SOA kein Problem oder Hindernis dar, da die Anwendung keine domainspezifischen Anforderungen mit sich bringt.

A II.1.4. Registrierung des Providers

Damit ein Provider Benachrichtigungen an eine mobile, auf dem Endgerät des Benutzers installierte Anwendung senden kann, ist eine Authentifizierung beim APN-Dienst nötig. So wird sichergestellt, dass kein unbefugter Dritter Nachrichten verschicken kann. Der entsprechende Ablauf ist in der Abbildung 25 dargestellt.

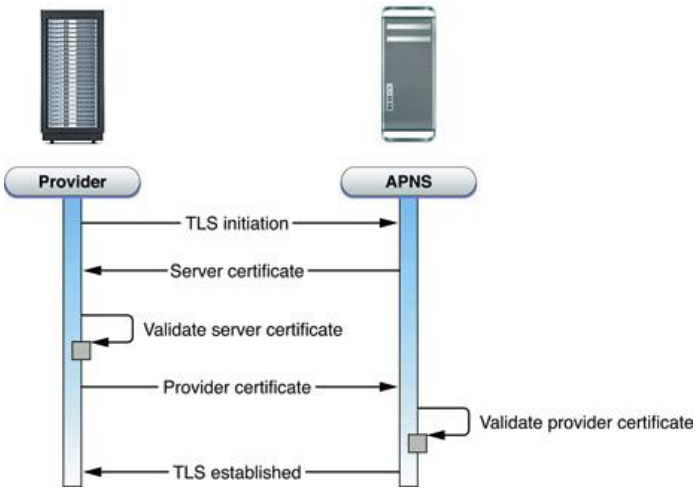

Abbildung 25: Authentifizierung des Providers beim APN-Dienst

Für eine detaillierte Beschreibung der einzelnen Schritte wird auf die Dokumentation des APN-Dienstes verwiesen. Hervorzuheben gilt jedoch die Tatsache, dass lediglich der Hersteller der mobilen Anwendung die Erlaubnis hat, auch tatsächlich Benachrichtigungen an diese zukommen zu lassen. Dies wird durch das Verwenden von Zertifikaten sichergestellt. In Hinblick auf die ÖV-SOA bedeutet dies, dass bei der Umsetzung des eigenen Push-Dienstes, der als Abstraktion für die einzelnen Hersteller gilt und die Abläufe in sich kapselt, darauf geachtet werden muss, dass für jede zu benachrichtigende mobile Anwendung auch ein entsprechendes Zertifikat vorliegen muss. Solche Zertifikate für die Entwicklung und Veröffentlichung von Applikationen können von jeder Person bei Apple erworben werden.

A II.1.5. Benachrichtigung von Interessenten und Abruf von Daten

Nachdem sich sowohl die Anwendung, beziehungsweise das mobile Endgerät, als auch der Provider beim APN-Dienst registriert und authentifiziert haben, kann ein Nachrichtenaustausch stattfinden.

Beim Vorliegen von neuen Informationen auf der Providerseite erstellt dieser eine Benachrichtigung, die an die Interessenten gesendet wird. Der Hersteller Apple beruft sich in der Dokumentation des APN-Dienstes stets darauf, keine tatsächlichen Inhalte in eine Benachrichtigung einzufügen, da das Zustellen einer solchen nicht garantiert werden kann. Vielmehr soll die Nachricht einen Prozess auf dem mobilen Endgerät anstoßen, der dafür sorgt, dass die Daten beim Provider abgefragt werden. Der Inhalt einer solchen Benachrichtigung in iOS beziehungsweise im APN-Dienst ist vom Typ „String“ und ist somit lediglich eine Zeichenkette.

Die nachfolgende Abbildung 26 demonstriert die Zustellung einer Benachrichtigung, wobei der Provider die erstellte Nachricht an den APN-Dienst zusammen mit dem erhaltenen Geräte-Token schickt. Der APN-Dienst überprüft die Echtheit des Tokens, findet den Adressaten und leitet die Benachrichtigung an das entsprechende mobile Endgerät weiter. Die eingegangene Nachricht wird an die Anwendung delegiert.

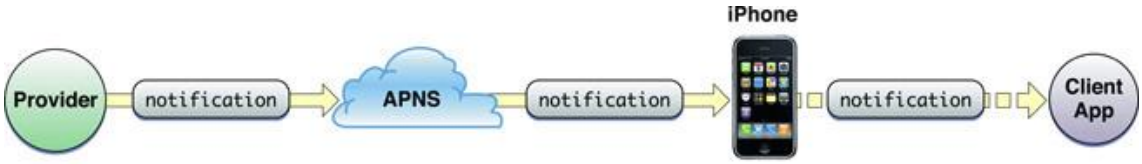

Abbildung 26: Benachrichtigungsablauf für iOS

Wie bereits angemerkt, wird nach Erhalt der Benachrichtigung bei der Anwendung empfohlen, eine Verbindung zum Provider aufzubauen, um die neuen Daten abzurufen. Es bleibt jedoch in der Verantwortung der jeweiligen Anwendung, dies auch zu tun.

A II.1.6. Abmeldung von Benachrichtigungen

Der APN-Dienst stellt nicht für jede Anwendung einen Token aus, der als Adressat von einem Provider verwendet werden kann, sondern lediglich für ein Gerät. Wünscht eine mobile Anwendung keine weiteren Benachrichtigungen zu empfangen, so obliegt es der Implementierung der Anwendung, den Provider diesbezüglich zu informieren. Apple nimmt an dieser Stelle an, dass der Provider auch der Anbieter der entsprechenden mobilen Anwendung ist. Das wird insbesondere aus der Registrierungsphase deutlich, bei der sowohl die mobile Anwendung als auch der Provider über das gleiche Zertifikat verfügen müssen.

A II.1.6.1. Google Cloud to Device Messaging (C2DM)

Der Ansatz von Google für das Betriebssystem Android mit dem „Cloud to Device Messaging“ (C2DM) Dienst ähnelt stark dem von Apple, schließlich lösen beide die gleiche Aufgabe auf eine möglichst einfache Art und Weise. Deshalb wird an dieser Stelle auf die Beschreibung der Abläufe weitgehend verzichtet und auf den vorhergehenden Abschnitt verwiesen. Nachfolgend sollen die wenigen Unterschiede genannt und ihre Implikation auf das System analysiert werden.

Der größte Unterschied liegt in der Tatsache, dass sich bei C2DM die Anwendungen einzeln beim Push-Dienst von Google registrieren müssen. Dadurch wird eine eindeutige Zuordnung zwischen Benachrichtigung und Applikation nicht mehr nur innerhalb des Betriebssystems geregelt, sondern bereits bei der Registrierung bei dem C2DM-Dienst.

Ein weiterer Unterschied zum APN-Dienst ist die Tatsache, dass die erstellten Tokens für die Anwendungen über eine begrenzte Lebenszeit verfügen und in gewissen Abständen aktualisiert werden müssen. Die Granularität der Tokens auf einzelne Anwendungen und nicht auf das gesamte Gerät ermöglichen auch explizite Abmeldung von Benachrichtigungen direkt beim C2DM-Dienst. Somit wird im Gegensatz zu Apple nicht die Annahme getroffen, dass der Provider der Daten auch der Hersteller der mobilen Applikation sei. Diese Änderung hat eine große, positive Auswirkung auf die spezifizierte Architektur: Ein unabhängiger Push-Dienst kann eine mobile Applikation und einen Provider verbinden, obgleich diese nicht vom gleichen Hersteller sind, da die Zertifikatauthentifizierung entfällt.

A II.1.7. Fazit

Die betrachtete Machbarkeit der Verwendung von proaktiv-basierten Benachrichtigungen zur Information von Benutzern im öffentlichen Personenverkehr über das Vorliegen von neuen Informationen. Dabei wurde auf die proprietären Push-Dienste von Apple und Google eingegangen, die im Bereich der Smartphones einen Marktanteil von ca.

70% mit einer steigenden Tendenz abdecken. Die Analyse der Machbarkeit hat ergeben, dass die Dienste durch die Anforderungen in IP-KOM-ÖV nicht eingeschränkt werden und problemlos eingesetzt werden können. Die Auswirkungen der einzelnen Details auf das Projekt und seine Ergebnisse wurden entsprechend beleuchtet, mit einem positiven Ergebnis hinsichtlich des Machbarkeitsnachweises.

A II.2 Sonstige Systeme für Personalisierungsdaten

Auf Grundlage diverser Quellen ergibt sich eine Aufstellung der am weitesten verbreiteten Hersteller von CRM-Systemen. Es ist jeweils angegeben, ob zusätzliche Daten als BLOB und/oder als zusätzliche Tabelle/Tabellenfelder abgelegt werden können. Ebenfalls ist aufgelistet, ob von eigenem Programmcode aus auf die Daten zugegriffen werden kann, was eine zwingende Voraussetzung für die Anknüpfung einer eigenen Komponente, welche die Personalisierungsschnittstelle implementiert, an ein bestehendes CRM-System ist.

Einzelne der gefundenen CRM-Angebote verwenden dabei keine eigene Software, sondern greifen ausschließlich auf Systeme anderer Anbieter zurück (die im Allgemeinen auch in dieser Auflistung enthalten sind). Für diese Angebote wird keine Aussage zur Erweiterbarkeit getroffen, da ihr Funktionsumfang von externen Komponenten abhängt, die vom Anbieter eventuell ausgetauscht werden könnten. Die betreffenden CRM-Angebote sind hier dennoch enthalten, damit sie bei einer späteren Implementierung des Personalisierungsdienstes nicht von Neuem untersucht werden müssen.

Wo sich nicht ermitteln ließ, ob eine bestimmte Erweiterungsart unterstützt wird, ist dies ebenfalls vermerkt.

Name: Amdocs

Die CRM-Systeme von Amdocs scheinen laut Produktbeschreibung keine Datenhaltung über Kunden zu beinhalten. Sie bieten lediglich die Verwaltung des Kontakts an, es gibt jedoch keine Informationen über die Kundendatenverwaltung, sodass diese offenbar durch andere Systeme erledigt wird.
Speichermöglichkeit als BLOB: Nicht zutreffend
Speichermöglichkeit als Tabelle: Nicht zutreffend
Programmseitiger Zugriff auf Daten: Nicht zutreffend

Name: C2CRM

Die Produkte von C2CRM können mit Visual Basic-Skripten erweitert werden, in denen auch zusätzliche Felder angelegt werden können. Es ist daher davon auszugehen, dass hier auch BLOBs abgelegt werden können.
Speichermöglichkeit als BLOB: Ja
Speichermöglichkeit als Tabelle: Ja
Programmseitiger Zugriff auf Daten: Ja, mit Visual Basic-Skripten

Name: esalestrack

Das Cloud-basierte System von eSalesTrack bietet nicht standardmäßig die Funktionalität an, die für den Personalisierungsdienst benötigt wird, jedoch bietet der Hersteller eine Anpassung seines Systems an, sodass sich die Schnittstelle des Personalisierungsdienstes umsetzen ließe.
Speichermöglichkeit als BLOB: Ja, mit Anpassungen durch den Hersteller
Speichermöglichkeit als Tabelle: Ja, mit Anpassungen durch den Hersteller
Programmseitiger Zugriff auf Daten: Ja, da der Hersteller selber Anpassungen anbietet

Name: GoldMine

In der Beschreibung zu den „GoldMine"-CRM-Produkten von FrontRange Solutions wird aufgeführt, dass alles auf einem erweiterbaren Datenmodell basiere. Die Integration mit Erweiterungen kann über SQL-Datenbankschnittstellen und über .NET vorgenommen werden. Somit ist es möglich, GoldMine zur Implementierung des Personalisierungsdienstes aus IP-KOM-ÖV einzusetzen.
Speichermöglichkeit als BLOB: Ja
Speichermöglichkeit als Tabelle: Ja
Programmseitiger Zugriff auf Daten: Ja, per SQL und .NET-API

Name: Infusionsoft

Infusionsoft bietet einen Cloud-basierten CRM-Dienst an, der sich an kleinere Unternehmen und Organisationen richtet. Wie in Infusionsoft beschrieben, lassen sich zu Kundendatensätzen benutzerdefinierte Felder hinzufügen. Der Zugriff auf diese kann über eine PHP-API erfolgen.
Speichermöglichkeit als BLOB: Unbekannt
Speichermöglichkeit als Tabelle: Ja
Programmseitiger Zugriff auf Daten: Ja, per PHP-API

Name: Microsoft Dynamics CRM

Die Microsoft Dynamics CRM-Funktionen sind über WebServices zugänglich. Das Datenmodell kann angepasst werden. Somit ist es möglich, mittels Microsoft Dynamics CRM den Personalisierungsdienst zu implementieren.
Speichermöglichkeit als BLOB: Ja
Speichermöglichkeit als Tabelle: Ja
Programmseitiger Zugriff auf Daten: Ja, per WebService-API
Programmseitiger Zugriff auf Daten: Unbekannt

Name: Oracle Customer Hub

Laut der Produktbeschreibung basieren die Kundendaten in dieser Software auf einem erweiterbaren Datenmodell. So ist also zumindest die Einbindung der Benutzerinformationen als BLOB möglich. Zum Zugriff auf die Daten kann eine von der Software bereitgestellte SOA-Schicht verwendet werden.
Speichermöglichkeit als BLOB: Ja
Speichermöglichkeit als Tabelle: Unbekannt
Programmseitiger Zugriff auf Daten: Ja, per SOA-Schicht

Name: RunE2E

RunE2E bietet CRM-Dienste an, verwendet dazu jedoch ausschließlich Systeme anderer Anbieter wie SAP und Salesforce.
Speichermöglichkeit als BLOB: Nicht zutreffend
Speichermöglichkeit als Tabelle: Nicht zutreffend
Programmseitiger Zugriff auf Daten: Nicht zutreffend

Name: Sage CRM

Sage CRM erlaubt das Anlegen benutzerdefinierter Tabellen, sodass hier die personalisierten Daten in Tabellenform und auch als BLOBs gespeichert werden können. Dies ist dadurch möglich, dass hier handelsübliche Datenbanksysteme eingebunden werden können. Der Zugriff auf die Daten ist sowohl über ein COM-Objekt als auch über .NET möglich. Ein SDK dafür liegt vor. So können benutzerdefinierte Skripte auch als ASP eingebunden werden.
Speichermöglichkeit als BLOB: Ja
Speichermöglichkeit als Tabelle: Ja
Programmseitiger Zugriff auf Daten: Ja, per COM-Objekt und .NET-API

Name: Salesforce.com

Salesforce.com ist ein CRM-Anbieter, der sein System als Cloudservice anbietet. Salesforce erlaubt das Speichern beliebiger angehängter BLOBs in Verbindung mit Datensätzen. Über eine WebService-API kann auf die Daten zugegriffen werden.
Speichermöglichkeit als BLOB: Ja
Speichermöglichkeit als Tabelle: Unbekannt
Programmseitiger Zugriff auf Daten: Ja, per WebService-API

Name: Salesnet CRM

Die Cloud-basierte CRM-Lösung von Salesnet unterstützt das Anlegen benutzerdefinierter Felder in der Benutzerdatenbank. Dabei ist jedoch unklar, ob BLOB-Felder oder Ähnliches unterstützt werden. Sollte dies der Fall sein, so ließe sich die Personalisierungsschnittstelle mittels der XML-basierten WebService-API anbinden.
Speichermöglichkeit als BLOB: Unbekannt
Speichermöglichkeit als Tabelle: Wahrscheinlich
Programmseitiger Zugriff auf Daten: Ja, per WebService-API

Name: SAP CRM

Das CRM-System der SAP AG zählt weltweit zu den am häufigsten eingesetzten CRM-Systemen. Wie im SAP Community Network beschrieben, lassen sich hier zusätzliche Tabellen einfügen. Demnach ist SAP CRM auf Erweiterbarkeit ausgelegt, sodass sich der Zugriff auf solche zusätzlichen Daten realisieren lässt. Diese Erweiterbarkeit mit Zugriff auf benutzerdefinierte Tabellen ist unter anderem über die Programmiersprache ABAP gegeben.
Speichermöglichkeit als BLOB: Ja
Speichermöglichkeit als Tabelle: Ja
Programmseitiger Zugriff auf Daten: Ja, z. B. ABAP

Name: SugarCRM

SugarCRM verwendet handelsübliche Datenbanken, wodurch das Anlegen benutzerdefinierter Tabellen möglich ist. SugarCRM ermöglicht den Zugriff auf die Daten über WebServices und eine SOAP-API. Der Personalisierungsdienst lässt sich folglich basierend auf den verfügbaren Informationen mit SugarCRM implementieren.
Speichermöglichkeit als BLOB: Ja
Speichermöglichkeit als Tabelle: Ja
Programmseitiger Zugriff auf Daten: Ja, per WebServices und SOAP-API sowie direkten Zugriff auf die Datenbanken

Name: TechExcel ServiceWise

Die CRM-Software ServiceWise von TechExcel unterstützt ebenfalls das Anlegen benutzerdefinierter Felder zu Kundendatensätzen. Es wird aus der Produktbeschreibung jedoch nicht klar, ob dabei auch BLOBs abgelegt werden können, sodass hier potenziell keine Speicherung von Daten aus dem Personalisierungsdienst möglich ist. Falls doch, ist der Zugriff auf die Daten über eine SOAP-API möglich.
Speichermöglichkeit als BLOB: Unbekannt
Speichermöglichkeit als Tabelle: Ja
Programmseitiger Zugriff auf Daten: Ja, per SOAP-API

Name: Workbooks.com

Workbooks.com bietet Cloud-basierte CRM-Dienste an. Laut der Produktbeschreibung unterstützen die Datenbanken benutzerdefinierte Felder für Benutzerkonten, sodass hier Daten des Personalisierungsdienstes tabellarisch oder als BLOB abgelegt werden könnten. Der Zugriff auf die Daten ist über eine REST-basierte API möglich.
Speichermöglichkeit als BLOB: Ja
Speichermöglichkeit als Tabelle: Ja
Programmseitiger Zugriff auf Daten: Ja, per REST-basierter API

A II.2.1. Generelle Bemerkungen

Unter den vorangegangenen Systemen existieren einige, zu denen keine Aussage bezüglich der Machbarkeit getroffen werden konnte oder die von Haus aus keine Funktionalität anbieten, um benutzerdefinierte Tabellen oder BLOB-Felder einzufügen. Zumindest die lokal installierbaren Systeme greifen jedoch im Allgemeinen immer auf handelsübliche Datenbanksysteme zurück, die vom Betreiber separat verwaltet werden können. In diesen Systemen ist es grundsätzlich möglich, eigene Tabellen anzulegen. Normalerweise beinhaltet dies die Möglichkeit, auf bestehende Tabellen zu verweisen, sodass generell auch zusätzliche Tabellen mit Informationen des Personalisierungsdienstes, die auf bestehende Benutzerkonten aus existierenden Benutzertabellen verweisen, machbar sind.

A II.2.2. Fazit

Die große Mehrzahl der untersuchten Systeme bietet zumindest eine grundlegende eingebaute Unterstützung zum Ablegen weiterer Daten, sodass die Implementierung des Personalisierungsdienstes auf Grundlage jener CRM-Systeme einen vertretbaren Aufwand darstellt. In denjenigen Systemen, die lokal installiert werden, kann zudem Einfluss auf die lokal vorhandenen Datenbanksysteme genommen werden, um die zusätz-

lichen Daten abzulegen. Der Personalisierungsdienst ist somit wie entworfen auch aufbauend auf bestehender Software umsetzbar.

A II.3 Schnittstelle zwischen mobilen Kundenendgerät und Fahrzeug

Die Schnittstelle zwischen mobilem Kundenendgerät und Fahrzeug stellt für die spätere praktische Umsetzung der IP-KOM-ÖV Ergebnisse bei den Verkehrsunternehmen eine besondere Herausforderung dar. Aus diesem Grund müssen im Machbarkeitsnachweis bereits frühzeitig Ausgestaltungsmöglichkeiten für die Kommunikation und den Datenaustausch zwischen mobilem Endgerät und Fahrzeug beleuchtet und hinsichtlich der technischen Umsetzbarkeit und der Nutzerorientierung evaluiert werden.

Die Schwerpunkte des Machbarkeitsnachweises liegen aus diesen Gründen auf der Benennung von Kennungen (SSIDs) für die Kommunikation mittels W-LAN, einer möglichen Nutzung von Ad-Hoc-Netzwerken und dem Verbindungsaufbau aus Nutzersicht. In diesem Rahmen wird auch die Problemstellung eines möglichen Verlustes der Internetverbindung bei Einwahl ins Fahrzeug-W-LAN sowie die Störerhaftung bei Bereitstellung eines Internetzugangs durch das Verkehrsunternehmen im Fahrzeug beleuchtet.

A II.3.1. Technische Realisierung der Schnittstelle zum mobilen Endgerät

Die technischen Ausgestaltungsmöglichkeiten der Schnittstelle zwischen mobilem Endgerät und Fahrzeug wurden bereits im Meilensteindokument „Systemarchitektur“ behandelt. Diese Technologien sind

Tabelle 6: Vergleich Kommunikationsmedien aus dem Meilenstein „Systemarchitektur“

	W-LAN	Bluetooth	NFC
Reichweite	Bis zu 100m (laut Spez.)	10m - 100m	Wenige cm
Datenrate	54 Mbit/s	Ca. 3 Mbit/s	424 Kbit/s
Sicherheit	Bereits eingebaute Lösungen sind vorhanden	Bereits eingebaute Lösungen sind vorhanden	Unterschiedliche Lösungen existieren
Robustheit	Kann zu Störungen kommen. Besonders bei mehreren W-LANs im kleinen Bereich	Unempfindlich gegenüber Überlagerungen, keine Störanfälligkeiten	Unempfindlich, da die Reichweite sehr gering ist
Geräteanzahl	Mehrere hundert Geräte	Bis zu 8 Geräte gleichzeitig	Gleichzeitige Kommunikation nur mit einem Gerät möglich
Verbreitungsgrad	In fast allen modernen mobilen Endgeräten	In fast allen modernen mobilen Endgeräten	Bisher nur in wenigen mobilen Endgeräten
Energie	Mehr als Bluetooth	Sparsam, weniger als W-LAN	Je nach Umsetzung. Ein passiver Tag benötigt keine Energie
Empfohlen für	Größere Netze / Teilnehmerzahl	Energieeingeschränkt / Vermeidung von Störungen	Kurzer Datenaustausch als Initiator für weitere Abläufe

Es ist vorgesehen die Umsetzung der Schnittstelle mittels einer Kombination aus W-LAN und NFC durchzuführen. Diese Entscheidung setzt voraus, dass das W-LAN-Netz des Fahrzeugs entweder manuell vom Kunden oder automatisch von der Applikation auf dem mobilen Endgerät unter Einbeziehung von NFC, z. B. auch in Kombination mit einem Ticketingsystem, ausgewählt und so eine Verbindung mit dem Fahrzeug, in dem der Fahrgast sitzt, hergestellt wird. Allerdings ist dies nicht in jedem Fall problemlos möglich. Eine genauere Auseinandersetzung mit der Problematik findet sich in den folgenden Abschnitten.

Weiterhin muss für die Auswahl der technischen Umsetzung betrachtet werden, wie die SSID für eine solche Verbindungsaufnahme ausgestaltet werden muss. Im Machbarkeitsnachweis gilt es, diese Empfehlung hinsichtlich der technischen Umsetzbarkeit und der Nutzerorientierung sowie möglicher Auswirkungen auf die Nutzung des mobilen Kundenendgerätes zu prüfen.

A II.3.2. Machbarkeitsbetrachtung der Verbindung mit dem Fahrzeug-W-LAN

Benennung und Auswahl der SSID im Fahrzeug

Fahrzeugspezifische Benennung von SSIDs

Technisch ist die Zeichenzahl für eine SSID auf 32 Zeichen begrenzt. Um die SSID, so man diese dem Nutzer anzeigen kann, möglichst transparent zu gestalten, ist ein Aufbau der SSID wie folgt vorzusehen. Erstens soll der Nutzer anhand des SSID-Bezeichners einfach und schnell erkennen können, dass seine mobile Applikation mit dem W-LAN eines Fahrzeugs verbunden ist, das IP-KOM-ÖV-Funktionalität unterstützt. Zweitens soll er auf einfache Art und Weise feststellen können, ob er mit dem W-LAN des Fahrzeugs verbunden ist, in dem er sich gerade befindet oder in das er einsteigt.

Die SSID soll im IP-KOM-ÖV-Verbreitungsgebiet eindeutig sein. Deshalb wird ein Aufbau der SSID in der folgenden Form angestrebt:
($Produktkennung)_($ProduktID)@($Verkehrsunternehmen).($Landeskürzel)

Da die Rahmenbedingungen im Nah- und Fernverkehr deutlich unterschiedlich sind, obliegt es dem einzelnen Verkehrsunternehmen, die Angaben für die Produktkennung und die ProduktID so zu wählen, dass der Nutzer auf einen einfachen Blick die zuvor erwähnte Zuordnung zu einem Fahrzeug vornehmen kann. Im Nahverkehr könnte sich der Teil der SSID links des „@“-Zeichens aus Kürzeln wie „Bus“, „S-Bahn“, „U-Bahn“, „Tram“ oder „Strab“ sowie der Fahrzeugnummer zusammensetzen. Im Fernverkehr bei der DB AG wird wohl eher eine Produktklasse wie „ICE“, „IC“, „IRE“ samt zugehöriger veröffentlichter Zugnummer zum Einsatz kommen.

Der Teil der SSID rechts des „@“-Zeichens sollte eine übliche Internet-Domain abbilden. Es bietet sich hier an, die Domain-Adresse des Verkehrsunternehmens zu verwenden (z. B. „evag.de“ oder „deutsche-bahn.de“). Das Unternehmen, welches die SSID im Fahrzeug vergibt, hat dafür Sorge zu tragen, dass die Kombination aus Produktkennung, ProduktID sowie Domain-Bezeichner über alle Fahrzeuge hinweg eindeutig ist.

Im Falle der Lösung mit individuellen SSIDs besteht für den Benutzer die Möglichkeit, über das Mobiltelefonmenü den richtigen Access Point (AP) des Fahrzeuges anhand

der SSID auszuwählen. Ebenso können Applikationen einen automatischen Wechsel nach Bestätigung durch den Anwender durchführen. Bei einer fehlerhaften Auswahl oder einem Fahrzeugwechsel muss die SSID neu ausgewählt werden. Die Option einer automatischen Auswahl der SSIDs wird bisher jedoch nur von Googles Betriebssystem Android unterstützt. Auf Endgeräten mit anderen Betriebssystemen, wie beispielsweise dem iOS von Apple, muss der Nutzer die Auswahl manuell durchführen. Deshalb erfordert jeder Wechsel eine manuelle Interaktion des Nutzers, der zusätzlich jederzeit die korrekte Bezeichnung der SSID kennen muss. Dies sollte von einem Fahrgast im ÖPNV nicht verlangt werden. Abgesehen von den damit einhergehenden Unannehmlichkeiten verfügen viele Anwender nicht über den notwendigen technischen Kenntnisstand. Insgesamt kann von einem nicht zu vernachlässigenden Anteil an mobilen Endgeräten mit dieser Einschränkung auf dem Markt ausgegangen werden.

Ein deutlicher Nachteil der Vergabe fahrzeugspezifischer SSIDs ist daher die potentielle Benutzerunfreundlichkeit des Ansatzes durch die Notwendigkeit einer manuellen Auswahl von SSIDs. Sie würde bei jeder Fahrt in einem neuen Fahrzeug notwendig. Ferner sammelt sich eine enorme Menge an gewählten SSIDs in den W-LAN-Einstellungen des Endgeräts, die dort für zusätzliche Unübersichtlichkeit und damit zu einer weiteren Unzufriedenheit des Nutzers führen würde.

Zusätzlich besteht bei individuellen SSIDs die oben beschriebene Herausforderung der Schaffung einer SSID-Struktur, die für alle Verkehrsunternehmen in Deutschland zutrifft und einen statischen Charakter aufweist. Zwar kann diese durch eine formale Vorgabe aufgelöst werden. Dennoch müsste die Einhaltung der Form durchgesetzt werden.

Ein anderer Nachteil des Ansatzes fahrzeugspezifischer SSIDs ist, dass trotz einer normierten Benennung ein Register gepflegt werden muss, aus dem die Applikation die für sie relevanten SSIDs auslesen kann, um sich anschließend mit ihnen verbinden zu können. Das Register kann lokal durch Beschilderung, durch das Auslesen von QR-Codes bzw. NFC-Tags oder auch zentral angelegt sein.

Einheitliche Benennung der SSID

In diesem Abschnitt wird ein W-LAN-basierter Lösungsansatz für die Kommunikation zwischen Fahrzeug und Fahrgast mit einheitlicher SSID als zuverlässige Methode für die Auswahl des "richtigen" Fahrzeugs beschrieben. Einheitliche SSID bedeutet hier, dass in den teilnehmenden Fahrzeugen identische SSIDs verwendet werden.

Nach einer Analyse der verfügbaren Kommunikationsalternativen (s. Kapitel A II.3.1) wurde entschieden, W-LAN zu nutzen. Eine entsprechende kritische Diskussion bezüglich der Auswahl der Kommunikationstechnik ist dem Meilensteindokument für die Architekturbeschreibung zu entnehmen. Eine der zentralen Problemstellungen für das mobile Endgerät (und damit für den für die Benachrichtigung der Fahrgäste zuständigen Teil des Systems) liegt in der Erkennung des Fahrzeuges, in dem sich ein Benutzer zum gegebenen Zeitpunkt befindet oder in das er einsteigen will. Erst mit dem Vorhandensein dieser Information kann eine direkte Kommunikation zwischen einem Fahrgast und dem für ihn relevanten Fahrzeug stattfinden.

Im Nachfolgenden findet eine Beschreibung der Problemstellung und des Lösungsansatzes statt, der es ermöglicht, dem Fahrgast unter der Verwendung einer einheitlichen SSID für die W-LAN APs der Fahrzeuge eine zuverlässige Liste der möglichen alternativen Fahrzeuge anzuzeigen. Dabei wird eines der Fahrzeuge vorausgewählt, sodass

die endgültige Auswahl durch Bestätigung des Fahrzeugs oder durch Auswahl eines anderen Fahrzeugs und anschließende Bestätigung stattfindet. Dadurch kommt eine Kommunikation zwischen dem Endgerät und dem gewählten Fahrzeug zu Stande. Die Bestätigung durch den Fahrgast löst dabei eventuell auftretende Unklarheiten auf, z. B. wenn mehrere W-LAN-Access Points in der näheren Umgebung des Mobilgeräts und damit mehrere potentielle Fahrzeuge erkannt wurden. Solche Probleme können leicht auftreten, etwa wenn zwei oder mehr Fahrzeuge direkt nebeneinander stehen. Die Nutzerbestätigung ist dabei die sicherste Methode, um bei einem Zweifel über die Wahl des richtigen Fahrzeugs die Auswahl korrekt abzuschließen. Nähere Details dazu werden im Folgenden behandelt.

A II.3.3. Beschreibung der Problemstellung

Um die Erkennung und Auswahl des richtigen Fahrzeuges automatisch und ohne Benutzerinteraktion realisieren zu können, sind verschiedene Alternativen denkbar, wie zum Beispiel akustische Signale, die im nicht hörbaren Frequenzbereich über die im Fahrzeug verbauten Lautsprecher periodisch abgespielt werden oder die Auswahl des W-LAN-APs mit der größten Signalstärke. Möglichkeiten, die eine Benutzerinterkation erfordern, reichen von der Verwendung der NFC Technologie, über den Einsatz von QR-Codes bis hin zur Eingabe des zutreffenden Fahrzeuges über eine bestimmte Kennung.

Da keine der genannten Lösungsmöglichkeiten eine stets zuverlässige und fehlerfreie Erkennung des Fahrzeuges garantieren kann, bedarf es Korrekturmechanismen, die eine Interaktion des Benutzers erfordern. Die Gestaltung solcher Mechanismen ist von der Beantwortung der zentralen Fragestellung nach der Benennung der SSIDs der APs der Fahrzeuge abhängig. Dabei wird zwischen einer einheitlichen (also global geltenden) und einer individuellen SSID-Benennung (je eine eigene SSID pro Fahrzeug) unterschieden, wobei jede der Lösungen ihre Vor- und Nachteile birgt. Die Problematik beim Einsatz fahrzeugspezifischer SSIDs wird später dargelegt. Im Folgenden wird ein Lösungsansatz mittels einheitlicher SSIDs präsentiert.

Lösungsansatz bei einheitlicher SSID

Bei der Variante mit einer einheitlichen SSID besteht für den Benutzer keine Möglichkeit, sich direkt mit dem richtigen Fahrzeug zu verbinden, da das Gerät nur eine einheitliche SSID kennt und sich automatisch mit dem AP verbindet, der die höchste Signalstärke aufweist. Eine manuelle Wahl des AP ist in der Regel nicht vorgesehen, sodass ein Wechsel des AP bei einheitlichen SSIDs durch den Endanwender nicht ohne weiteres möglich ist. Nichtsdestotrotz bietet die Lösung der einheitlichen SSID einen deutlichen Vorteil für den Endanwender gegenüber der Lösung mit individuellen SSIDs: Der Endanwender muss sich nicht mit der Auswahl der korrekten SSIDs auseinandersetzen, falls er ein Betriebssystem nutzt, das die Wahl des APs durch eine Applikation nicht zulässt. Somit muss er diese SSIDs auch nicht zusätzlich vorher in Erfahrung bringen. Stattdessen muss sich der Nutzer (oder auch die Applikation) nur ein einziges Mal mit dem AP verbinden und eine automatische Verbindung zu dem Netz zulassen. Anschließend ist die SSID in den W-LAN-Einstellungen des Betriebssystems gespeichert und das mobile Endgerät kann sich zukünftig automatisch zu jedem IP-KOM-ÖV Access Point verbinden. Die Kommunikation läuft für den Nutzer in einer transparenten Art und Weise ab.

Problematisch ist allerdings der Fall, dass sich das mobile Endgerät auf den AP eines Fahrzeugs verbindet, in dem sich der Kunde nicht befindet. Um dennoch die gewünsch-

ten Informationen zu erhalten, muss auf ein Inter-Fahrzeug-Routing zurückgegriffen werden. Um die Vorteile der einheitlichen SSID nutzen zu können, ohne auf Informationen vom „richtigen“ Fahrzeug verzichten zu müssen, wird im nachfolgenden Abschnitt ein Lösungsansatz beschrieben. Dieser sorgt dafür, dass jeder Fahrgast auch tatsächlich mit dem Fahrzeug kommuniziert, in dem er sich zum gegebenen Augenblick befindet - trotz der Tatsache, dass ein bewusster Wechsel zwischen APs bei einheitlicher SSID nicht möglich ist.

Lösungsansatz für ein Ad-Hoc-Netzwerk zwischen Fahrzeugen

Bei der Kommunikation mit W-LAN existieren zwei alternative Modi. Der erste Modus wird Infrastruktur-Modus genannt und sollte den meisten Betreibern von Heim-W-LAN bekannt sein. Dabei wird eine baumförmige Struktur an den entsprechenden Geräten aufgebaut, wobei an der Wurzel des Baumes der zentrale Access Point angebracht ist. Im Heimszenario ist es meist der W-LAN-Router, der den zentralen Knoten für die Verbindung mit allen W-LAN-fähigen Endgeräten darstellt.

Der Ad-Hoc-Modus ist die Alternative dazu. Hierbei existiert kein direkter Zentralknoten, vielmehr kommunizieren alle Knoten direkt miteinander. Neue Knoten treten dem Netzwerk automatisch bei. Dies kann über vermaschte Netzwerke (Mesh-Netze) verwirklicht werden. Bei diesen ist jeder Knoten mit einem oder mehreren anderen Knoten verbunden. Entsprechend übernehmen Knoten Routingfunktionen. Durch dieses Weiterleiten von Nachrichten werden Nachrichtenwege von einem Startknoten zu einem Zielknoten aufgebaut, auch wenn der Startknoten keinen direkten Zugriff auf den Zielknoten seiner Nachricht hat. Ein Beispiel für ein solches Ad-Hoc-Netz ist in Abbildung 27 dargestellt.

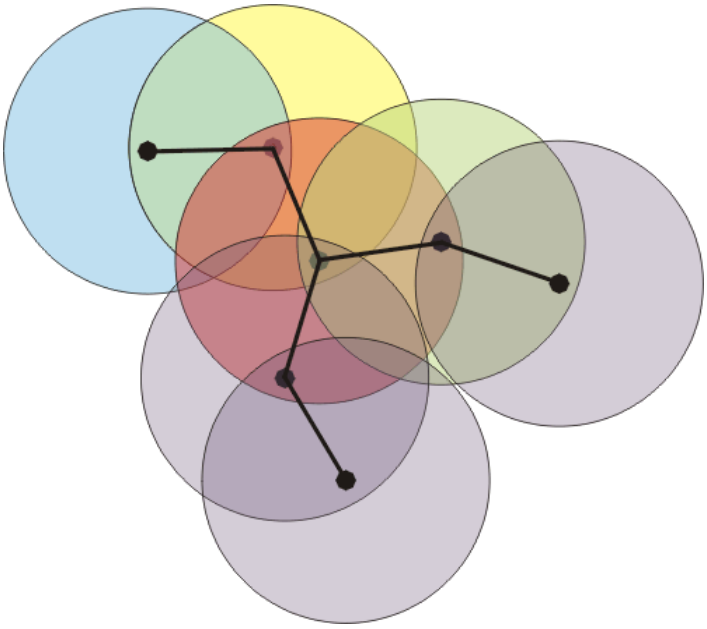

Abbildung 27: Ad-Hoc-Netz mit Multihop [Grafik gemeinfrei]

Die Idee ist nun, diese beiden Modi zu kombinieren: Während die Fahrgäste im Infrastruktur-Modus mit einem Fahrzeug kommunizieren (unabhängig davon, ob es das Fahrzeug ist, in dem sich der Fahrgast gerade befindet), tauschen die Fahrzeuge die entsprechenden Daten untereinander im Ad-Hoc-Modus aus. Diese Möglichkeit einer Fahrzeug-zu-Fahrzeug-Kommunikation erlaubt es Fahrgästen, (indirekt) mit dem für sie relevanten Fahrzeug zu kommunizieren, selbst wenn sich ihr mobiles Endgerät mit einem falschen Fahrzeug verbunden hat. Der vorgeschlagene Ansatz ist in der Abbildung

28 dargestellt. Im Nachfolgenden soll demonstriert werden, wie diese Lösung sowohl für die Identifikation des für den Fahrgast relevanten Fahrzeugs als auch für die Übermittlung der Daten zwischen den beiden Parteien genutzt werden kann.

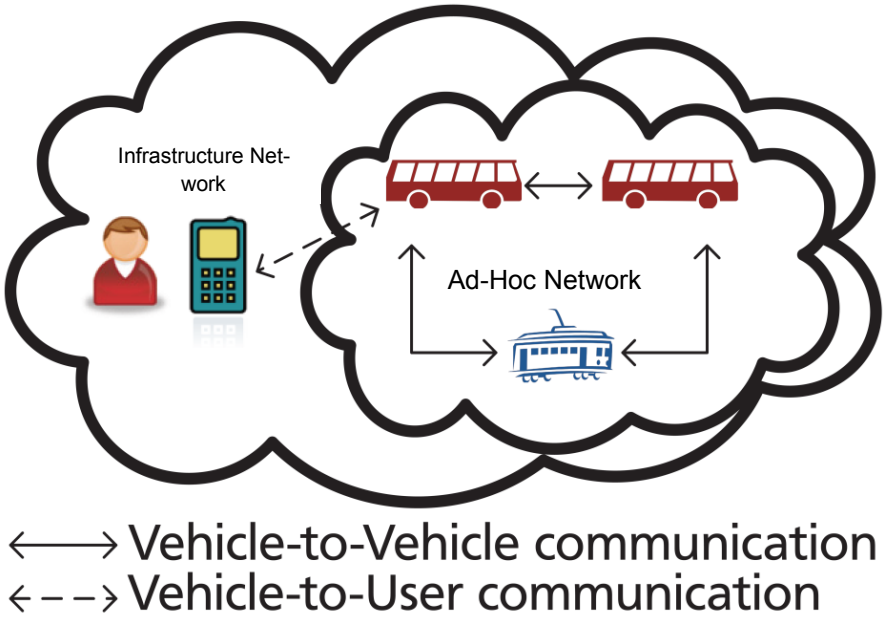

Abbildung 28: Kombination Infrastruktur-Modus und Ad-Hoc-Modus

Identifikation des Fahrzeuges, in dem sich der Fahrgast aufhält

Bei der Lösung mit einer einheitlichen SSID ist es weder für den Benutzer noch für eine Applikation möglich, sich innerhalb des Bereiches einer SSID mit dem Access Point genau des Fahrzeuges zu verbinden, in dem er sich zum gegebenen Augenblick befindet. Deshalb müssen die Fahrzeuge die Informationen über das aufgespannte Ad-Hoc-Netz an das korrekte Fahrzeug weiterleiten. Um dies realisieren zu können, muss die Zuordnung zwischen dem Fahrgast und dem entsprechenden Fahrzeug sichergestellt werden.

Die Lösung sieht vor, dass die Fahrzeuge in einem gewissen Abstand über die Broadcastoption in Form einer „Hallo-Nachricht“ alle anderen Fahrzeuge in der unmittelbaren Umgebung über die eigene Existenz informieren. Das empfangende Fahrzeug kann daraufhin eine Liste mit „kürzlich gesichteten“ Fahrzeugen führen und diese bei Bedarf der Anwenderapplikation bereitstellen. Durch eine visuelle Darstellung der Liste auf dem mobilen Endgerät des Fahrgastes kann eine Bestätigung des Fahrzeugvorschlags eingeholt werden, in dem sich der Nutzer befindet. Die Abbildung 29 demonstriert den Aufbau einer solchen Liste innerhalb eines jeweiligen Fahrzeuges.

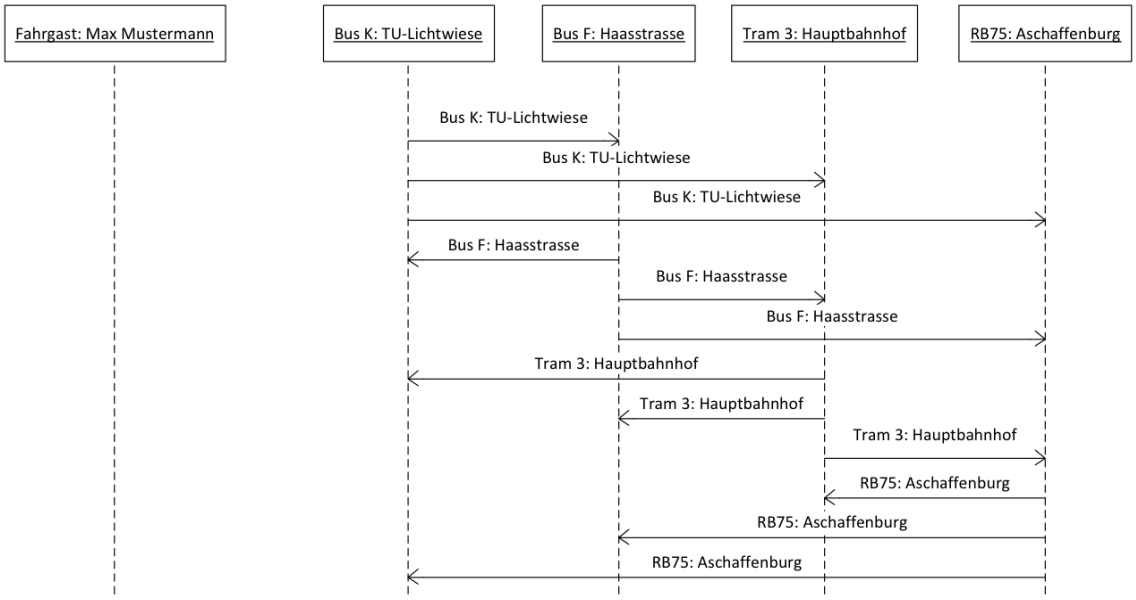

Abbildung 29: Erstellung der Liste

Falls die Applikation selbstständig eine Zuordnung treffen kann, wählt das Endgerät des Fahrgastes aus der übermittelten Liste das entsprechende Fahrzeug. Andernfalls bittet es bei einem verbleibenden Restzweifel den Fahrgast, die Auswahl zu bestätigen. Die getroffene Entscheidung wird an das entsprechende Fahrzeug zurückgeschickt, wie es in der Abbildung 30 dargestellt ist.

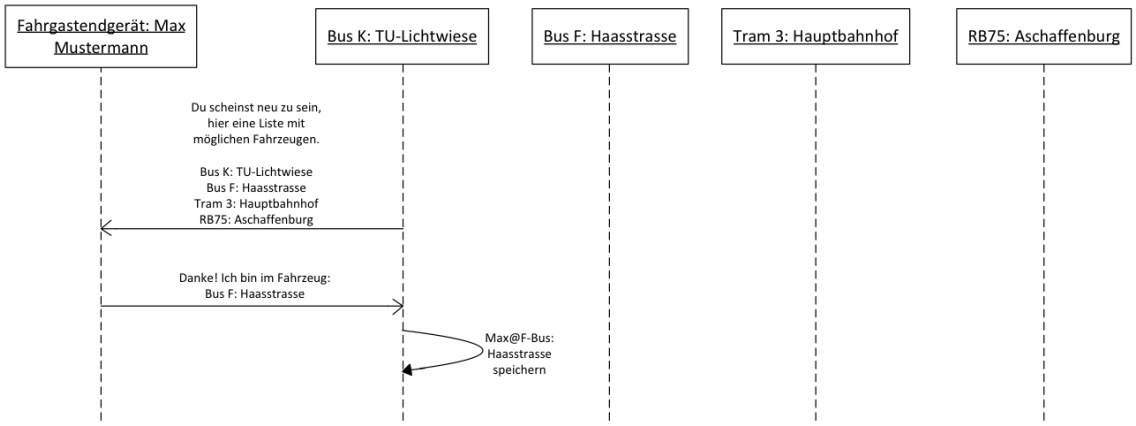

Abbildung 30: Auswahl des richtigen Fahrzeuges

Die Zuordnung kann dahingehend optimiert werden, dass dem mobilen Endgerät bei der Verbindung mit dem Access Point über eine Indexdatei das eigene Fahrzeug kommuniziert wird. Gerade in dünn befahrenen Bereichen ist dabei die Wahrscheinlichkeit sehr hoch, dass der Endkunde sich direkt mit dem AP des Fahrzeugs verbindet, in dem er sich befindet. Der Fahrgast bestätigt dies lediglich durch eine einzige Aktion auf dem Endgerät. Diese Transparenz erhöht das Sicherheitsempfinden und sorgt für bessere Steuerbarkeit des Systems. Alternativ reagiert der Nutzer gar nicht und die Anwendung geht von dem von ihr vorausgewählten Fahrzeug aus, d. h., das Ausbleiben einer Reaktion des Benutzers entspricht einer impliziten Bestätigung, die jedoch jederzeit durch eine Handlung seitens des Nutzers revidiert werden kann.

Kommunikation zwischen dem Fahrgast und dem jeweiligen Fahrzeug

Nach der erfolgreichen Zuordnung zwischen einem Fahrgast und einem Fahrzeug kann die Übermittlung der Informationen in beide Richtungen stattfinden. Die Abbildung 31 demonstriert, wie ein Fahrgast eine Mitteilung an das entsprechende Fahrzeug übermitteln kann. Dabei wird sie zuerst an das Fahrzeug geschickt, mit dem der Benutzer verbunden ist, wo sie anhand der lokalen Zuordnungsliste an das Zielfahrzeug über das Ad-Hoc-Netz weitergeschickt wird.

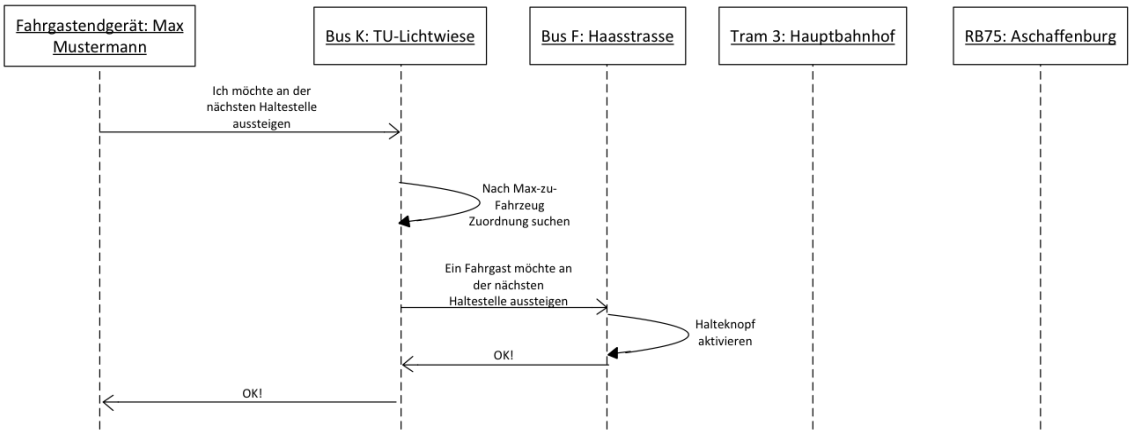

Abbildung 31: Fahrgast-zu-Fahrzeug Nachrichten

Die umgekehrte Kommunikationsrichtung funktioniert ähnlich wie es in Abbildung 32 dargestellt ist. Hierbei übermittelt das Fahrzeug die Nachricht über das Ad-Hoc-Netz an alle sich in Reichweite befindlichen Fahrzeuge. Jedes Fahrzeug, das die Nachricht empfängt, iteriert über eine interne Liste mit möglichen Fahrgästen, für die diese Nachricht relevant sein könnte, und leitet die Nachricht an die betreffenden Mobilgeräte weiter.

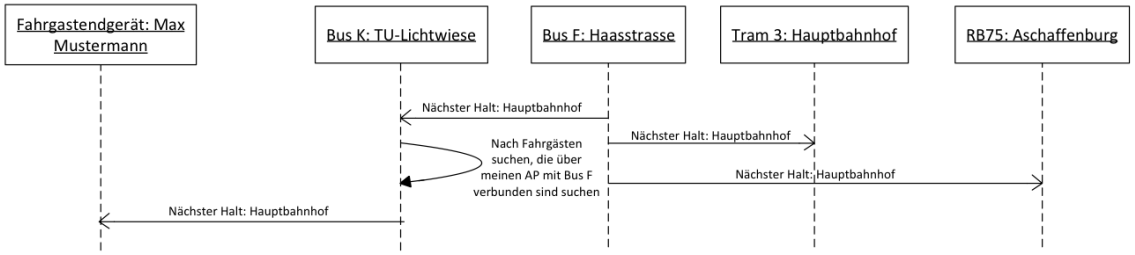

Abbildung 32: Fahrzeug-zu-Fahrgast Nachrichten

Machbarkeitsbetrachtung im Rahmen von IP-KOM-ÖV und Fazit

Die vorgestellte Lösung überwindet die Notwendigkeit der Schaffung einer deutschlandweiten SSID-Struktur und erspart einem Fahrgast die aufwändige Auswahl der korrekten SSID. Es bleibt lediglich das Fahrzeug zu bestätigen, in dem sich der Fahrgast zum gegebenen Zeitpunkt befindet.

Die Kombination eines Ad-Hoc-Netzes mit einem Infrastrukturnetz ist notwendig, da die mobilen Endgeräte auf eine Infrastrukturnetzkommunikation ausgelegt sind und nur ineffektiv im Ad-Hoc-Modus operieren können. Einige Geräte stellen diese Option gar nicht zur Verfügung. Deshalb erfolgt die Fahrzeug-zu-Mobilgerät Kommunikation im Infrastrukturmodus. Die Access Points eines Fahrzeuges unterliegen jedoch nicht den Einschränkungen eines mobilen Endgerätes, sodass bei der Fahrzeug-zu-Fahrzeug Kommunikation im Ad-Hoc-Modus operiert werden kann.

Gegen mögliche Einwände bezüglich der Sicherheit der Fahrzeug-zu-Fahrzeug-Kommunikation sowie der Teilung von unternehmensrelevanten Informationen mit den Fahrzeugen anderer Unternehmen kann wie folgt argumentiert werden. Erstens befinden sich zwei Fahrzeuge nur selten über einen längeren Zeitraum in der unmittelbaren Reichweite des Ad-Hoc-Netzes, sodass ein dauerhaftes Profil über ein Fahrzeug nicht erstellt werden kann. Zweitens ist insbesondere diese Problematik nicht auf das Ad-Hoc-Netz zurückzuführen, denn die ausgetauschten Informationen sind öffentlich. Ein böswilliger Angreifer kann sich jederzeit als Fahrgast ausgeben und unter Verwendung des Infrastrukturmodus an die Informationen kommen.

Natürlich muss auch erwähnt werden, dass der Aufbau von zwei kombinierten Netzarten mit dem Einbau von zwei Access Points in entsprechenden Fahrzeugen verbunden ist. So kann die Umsetzung des Vorschlags einer einheitlichen SSID zu höheren Kosten führen. Man könnte nun argumentieren, dass eine Lösung mit individuellen SSIDs durch die Einsparung eines AP pro Fahrzeug kostensparender und schneller auf der bestehenden Fahrzeuginfrastruktur umsetzbar wäre. Dabei darf aber der Aspekt der Kundenfreundlichkeit keinesfalls unterschätzt werden. Eine solche Lösung, die letztendlich zu einem wenig benutzbaren System führt, würde entsprechend potentielle Nutzer abschrecken und damit den Einsatz der Ergebnisse aus IP-KOM-ÖV gefährden.

Verbindungsaufbau aus Nutzersicht

Der Verbindungsaufbau aus Nutzersicht stellt, wie bereits im Meilenstein zur Systemarchitektur beschrieben, eine anspruchsvolle Aufgabe für den Nutzer dar. Dabei sind Aufgaben, in denen kognitive Leistungen erbracht werden müssen, z. B. Informationsvergleiche oder die Suche nach Informationen, für den Benutzer neben seinem gewohnten Reiseablauf eine zusätzliche Belastung. Dagegen können andere Aufgaben, die mit einfachen Tätigkeiten ohne weitere kognitive Leistungen verbunden sind, wie das Vorbeiführen an einem NFC-Chip, für den Benutzer mit weniger Belastung verbunden sein. Bei der Auswahl einer geeigneten Technologie für die Schnittstelle zwischen Fahrzeug und mobilem Endgerät des Fahrgastes müssen diese zusätzlichen Belastungen berücksichtigt werden, um die Akzeptanz auf Seiten des Nutzers zu gewährleisten.

Im Kontext der heterogenen Nutzer des öffentlichen Personenverkehrs, wie sie bereits in der Anforderungsanalyse beschrieben sind, muss beachtet werden, dass von den individuellen Kenntnissen und Fähigkeiten des Nutzers abhängig ist, wie stark diese Belastung auch als Beanspruchung empfunden wird, die wiederum zu vermehrtem Stressempfinden führen kann. So könnte beispielsweise das Einscannen eines QR-Codes für die Persona Kevin Schubert, der diese Tätigkeit schon häufiger ausgeführt hat, eine sehr geringe Belastung darstellen, während diese Tätigkeit für Persona Hildegard Krause vollkommen ungewohnt ist und daher zu einer größeren Beanspruchung führt.
Daher wurden die aktuellen technischen Möglichkeiten zur Herstellung der Verbindung mit dem Fahrzeug-W-LAN anhand von Aktivitätsdiagrammen, wie in Abbildung 34 und Abbildung 35 dargestellt, analysiert. Die Aktivitätsdiagramme zeigen zum einen die Anzahl und den Ablauf der erforderlichen Benutzeraktionen und verdeutlichen zum anderen durch ihre farbliche Codierung, wie stark der Benutzer durch die jeweilige Interaktion kognitiv belastet ist. Abbildung 33 zeigt die für die Analyse und Darstellung der Belastung in den Aktivitätsdiagrammen zu Grunde gelegten Abstufungen.

Abbildung 33: Stufen der Belastung

Des Weiteren wurde für die Auswertung zusätzlich die Genauigkeit der Identifizierung des aktuellen Fahrzeugs bewertet. Diese ist für die Nutzung des Systems durch den Fahrgast wichtig, damit die Zahl der nicht richtig identifizierten Fahrzeuge nicht zu Gunsten einer nutzerfreundlicheren Auswahl negativ beeinflusst wird und somit ggf. die Akzeptanz des Systems leidet.

Für die Analyse und die Bewertung der Genauigkeit der Identifizierung des aktuellen Fahrzeuges sind aus Perspektive der Nutzer zwei Szenarien von Bedeutung:

- Szenario 1: Verbindungsaufbau ohne gespeicherte Reiseplanung
- Szenario 2: Verbindungsaufbau mit gespeicherter Reiseplanung

Aufgrund der besonderen Einschränkungen einiger Betriebssysteme, z. B. des Apple-Betriebssystems iOS, können technische Unterstützungen wie QR-Codes oder NFC-Tags dem Nutzer lediglich Informationen zur Auswahl des Fahrzeug-W-LAN bieten, allerdings den Aufbau der Verbindung nicht immer selbst initiieren. Aus diesem Grund wäre für Apple-Benutzer eine nur einmalige manuelle Registrierung im Ad-Hoc-Netzwerk eine Erleichterung. Die konkrete Betrachtung einzelner Betriebssysteme wird im Kontext dieser Belastungsanalyse zu Gunsten einer breiteren Analyse mit Fokussierung auf die Nutzer zurückgestellt.

Für die Betrachtung ergeben sich folgende vier Verfahren des Verbindungsaufbaus, die unterschiedliche Aufgaben und Interaktionen zur Folge haben:

- Manuelle Auswahl und Prüfung der SSID
- Manuelle Auswahl und Prüfung des Fahrzeugs im Ad-Hoc-Netzwerk
- Auswahl via QR-Code
- Auswahl via NFC

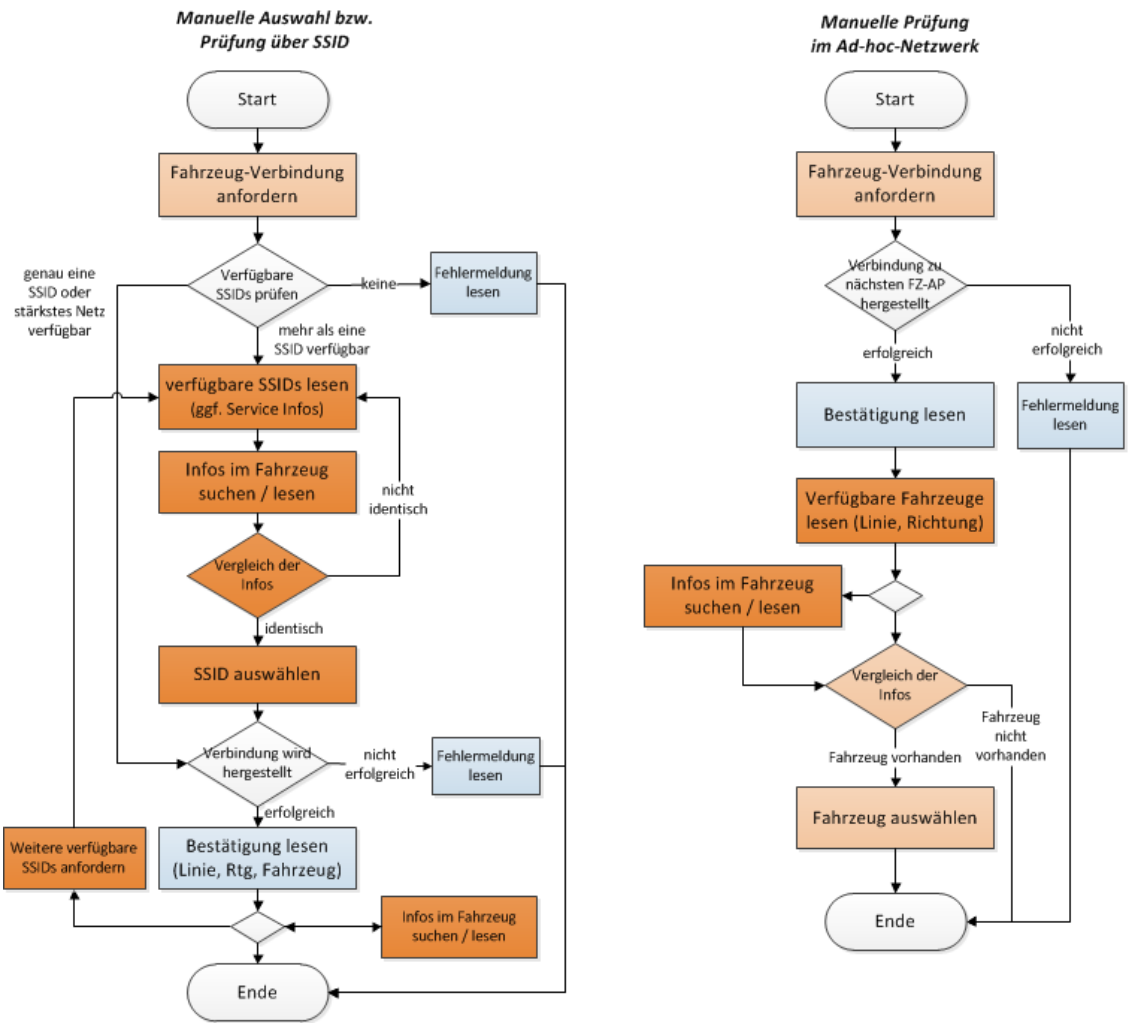

Abbildung 34: Aktivitätsdiagramme für manuelle Auswahl und Ad-Hoc-Netzwerk zum Verbindungsaufbau mit dem Fahrzeug-W-LAN am Beispiel einer Reise ohne gespeicherte Reiseplanung

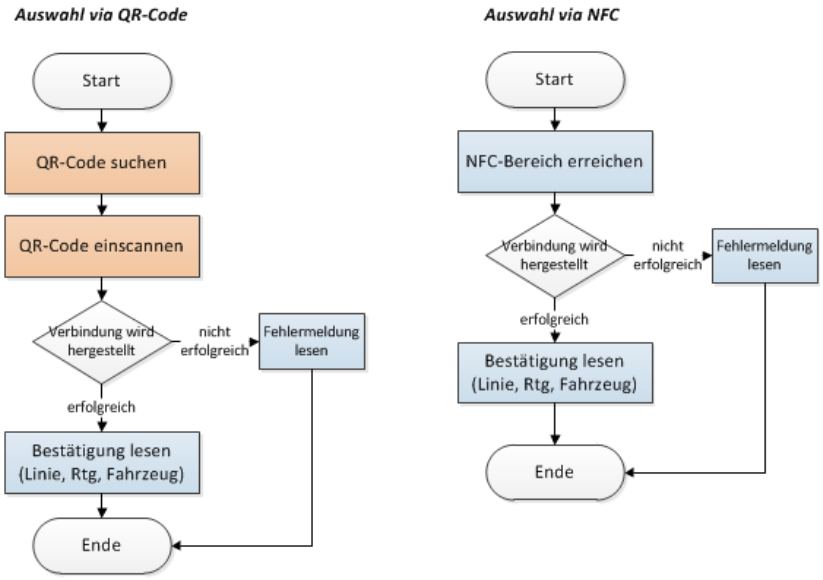

Abbildung 35: Aktivitätsdiagramme für den Einsatz von QR-Code und NFC zum Verbindungsaufbau mit dem Fahrzeug-W-LAN am Beispiel einer Reise ohne gespeicherte Reiseplanung

Die in Tabelle 7 zusammengefassten Ergebnisse zeigen, dass die Spanne der notwendigen Nutzeraktionen sowie der Nutzerbelastung beim Einsatz der unterschiedlichen Techniken stark variiert. Eine Verbindungsaufnahme mit NFC oder mit QR-Code liegt dabei im geringen und mittleren Belastungsbereich, während die manuelle SSID Auswahl den Nutzer sehr stark belastet. Durch den Einsatz zusätzlicher technischer Hilfsmittel, zu denen QR-Codes und NFC gezählt werden können, steigt zudem die Genauigkeit der Fahrzeugerkennung.

Tabelle 7: Vergleich der Varianten für den Verbindungsaufbau aus Nutzersicht

Verbindungs-auswahl	Nutzer-aktionen	Nutzer-belastung	Fahrzeug-erkennung
Manuell (SSID)	2 bis 9	sehr hoch	unsicher
Manuell (Ad-Hoc)	2 bis 7	Mittel	unsicher
QR-Code	3	Mittel	sicher
NFC	2	Gering	sehr sicher

Fazit

Für eine möglichst hohe Akzeptanz der Fahrgastinformation über das Fahrzeugnetz, sollte angestrebt werden, dass sich der Verbindungsaufbau mit dem Fahrzeugnetz für jeden Nutzer einfach und ohne Zusatzaufwand in seinen natürlichen Reiseablauf einfügt. Dazu ist beispielsweise eine Unterstützung der Netzauswahl durch NFC, wie sie im Meilensteinbericht zur Systemarchitektur beschrieben ist, eine technische Lösungsmöglichkeit.

A II.3.4. Parallele Nutzung von Fahrzeug-W-LAN und Internet

Problemstellung Verbindungsaufbau mit W-LAN und 3G

Die wesentlichen Argumente waren erstens, dass mit W-LAN eine preiswerte Standardtechnik zur Verfügung steht, die einfach im Fahrzeug installiert werden kann. Zweitens verfügen die mobilen Endgeräte der Kunden in der Regel über eine W-LAN-Schnittstelle. Das Fahrzeug stellt hierfür einen W-LAN-Access-Point zur Verfügung, mit dem sich das mobile Endgerät verbindet.

Dieser Access-Point wird unverschlüsselt sein, da er dem mobilen Endgerät gegenüber offen sein soll. Das mobile Endgerät des Kunden kann sich nun mit dem W-LAN-Access-Point des Fahrzeugs verbinden, um mit dem Fahrzeug über die IP-Schnittstelle zu kommunizieren. Das Fahrzeug stellt hierfür über den W-LAN-Access-Point in der Regel lediglich ein lokales Netzwerk zur Verfügung, welches üblicherweise nicht mit dem Internet verbunden sein wird. Die Gründe hierfür sind zum einen die zusätzlich entstehenden Kosten für die Online-Anbindung des Fahrzeug-Access-Points, die in der Regel über einen externen Service Provider erfolgt. Zum anderen ergeben sich durch das Verfügbarmachen eines freien, nicht kontrollierten Internet-Zugangs Probleme mit der Störerhaftung .

Diese Konstellation beinhaltet allerdings ein grundlegendes Problem bzgl. des Internetzuganges des mobilen Endgerätes. Je nach Verhalten und Funktionalität auf Betriebssystemebene des Smartphones steht nämlich nach dem Verbinden mit dem Fahrzeug-W-LAN kein Internetzugang mehr zur Verfügung.

Wenn sich das Endgerät in Reichweite eines Fahrzeug-W-LANs befindet, wird es üblicherweise anzeigen, dass es sich im Einzugsbereich eines W-LANs befindet und ggf. den Nutzer fragen, ob es sich mit dem W-LAN verbinden soll. Bejaht der Nutzer, wird die Verbindung hergestellt und eine IP-Adresse aus dem lokalen Fahrzeug-Netzwerk bezogen. In der Standardkonfiguration wird die hergestellte W-LAN-Verbindung nun zur Standard-Internet-Verbindung des mobilen Endgerätes. Da das Fahrzeugnetzwerk aber in der Regel keine direkte Verbindung ins Internet bietet, werden Anfragen ins Internet (Web-Browser, E-Mail, Apps, EKAP, etc.) nicht mehr erfolgreich sein.

Heutige Smartphones leben von einer permanenten Internet-Verfügbarkeit. Auf den Geräten werden mehrere Applikationen parallel oder im schnellen Wechsel genutzt, die auf eine Internet-Verbindung angewiesen sind (Web-Browser, Nachrichten, Wetter, E-Mail, Navigation, etc.). Der Nutzer hat sich an diesen Zustand gewöhnt, sodass eine Unterbrechung der Internet-Verbindung - insbesondere wenn die Gründe dafür nicht nachvollziehbar sind - zu Verärgerung führen wird.

Daher wird im Folgenden untersucht, ob grundsätzliche Lösungsmöglichkeiten existieren, W-LAN zur Kommunikation mit dem Fahrzeug zu nutzen, ohne dabei die restliche Funktionalität des Smartphones einzuschränken. Ihre Umsetzbarkeit hängt maßgeblich von der Plattform (iOS, Android, Blackberry, Windows Mobile 7 etc.), aber auch von der jeweiligen Betriebssystem-Version ab. Durch den raschen technologischen Wandel kann es auch in Zukunft zu Veränderungen der Umsetzbarkeit der verschiedenen Lösungsansätze kommen.

Folgende grundsätzliche Lösungsansätze sind denkbar, wenn nicht auf die Variante „Internetzugang über den Access Point des Fahrzeugs“ zurückgegriffen werden kann:

1) Schlaues Betriebssystem

Das Betriebssystem des Smartphones erkennt, dass die W-LAN-Verbindung nicht ins Internet führt und belässt die bisherige Internet-Verbindung (meist das Mobilfunknetz) als Standard. Trotzdem wird die W-LAN-Verbindung aktiviert und steht Apps auf Verlangen zur Verfügung. Auf diese Weise könnte genau die App gezielt auf diese W-LAN-Verbindung zugreifen, alle anderen Apps verwenden sie nicht. Die Fähigkeiten des Betriebssystems (inklusive der Nutzung von mehreren Verbindungen, z. B. W-LAN und 3G gleichzeitig) können nicht beeinflusst werden.

2) Schlaue App

Die App erkennt, dass das Betriebssystem eine W-LAN-Verbindung zu einem Fahrzeug aufgebaut und diese als Standard-Internet-Verbindung angenommen hat. Die App revidiert diese Entscheidung, macht das Mobilfunknetz wieder zur Standard-Internet-Verbindung und nutzt selbst die W-LAN-Verbindung weiter. Diese Funktionalität ist nur dann realisierbar, wenn sie durch das Betriebssystem des Smartphones unterstützt wird; dies ist zum Beispiel bei aktuellen iOS-Versionen nicht der Fall.

3) Zeitscheiben

Die App erkennt, dass das Betriebssystem eine W-LAN-Verbindung zu einem Fahrzeug aufgebaut hat. Sie kann das Betriebssystem aber nicht anweisen, diese Verbindung nicht ins Internet zu benutzen. Die App könnte daraufhin das regelmäßige Trennen der

W-LAN-Verbindung initiieren. So wäre die Internet-Verbindung jeweils nur für relativ kurze Zeit unterbrochen.

Auf aktuellen Android-Geräten haben App-Entwickler relativ weitgehende Möglichkeiten, Einfluss auf das Betriebssystemverhalten zu nehmen. Es ist anzunehmen, dass dies auch zukünftig so bleiben wird. Bei iOS-Geräten hingegen haben Apps keinerlei Zugriff auf die Netzwerkschicht. Eine App kann dort keinen Einfluss auf die Internet-Verbindung nehmen. Inwieweit sich dies in zukünftigen Betriebssystem-Versionen ändert, lässt sich aufgrund von Apples verschlossener Firmenpolitik nicht vorhersagen.

Aufrechterhaltung von W-LAN- und 3G-Netzverbindung gleichzeitig

Ausgehend von der vorgestellten Problembeschreibung sollen nachfolgend Lösungen präsentiert werden, wie es aktuell möglich ist, auf einem mobilen Endgerät gleichzeitig, bzw. nahezu gleichzeitig, sowohl eine W-LAN- als auch eine 3G-Verbindung zu nutzen. Repräsentativ werden dazu die beiden mobilen Plattformen Android (Google) und iOS (Apple) betrachtet, die zusammen einen Marktanteil von knapp 80% aufweisen (vgl. Abbildung 36).

Plattform	Anzahl Geräte in Mio.	Martkanteil in %
Android	81,07	56,1
iOS	33,12	22,9
Symbian	12,47	8,6
Blackberry OS	9,94	6,9
Bada	3,84	2,7
Windows Phone	2,71	1,9
Smartphone-Plattformen im ersten Quartal 2012 (Quelle: Gartner)		

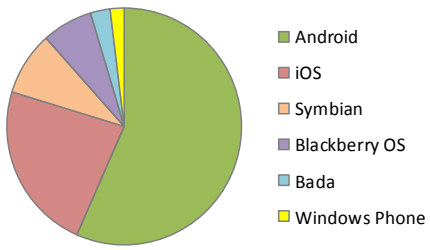

Abbildung 36: Marktanteile der Smartphone-Plattformen weltweit im ersten Quartal 2012

Simultane Netzwerknutzung mit Android

Offiziell ist es nicht möglich, beide Kommunikationswege (3G und W-LAN) gleichzeitig mit einem Android-Smartphone zu nutzen. Sobald W-LAN als Verbindung vorhanden ist, wird automatisch die 3G-Verbindung deaktiviert. Die einzige Situation, in der beide Verbindungen genutzt werden können, ist das sog. **Tethering**, wobei das Mobiltelefon die 3G-Verbindung benutzt um ein W-LAN-Netzwerk für andere Geräte aufzubauen. Es wird somit selbst zum Hotspot. Allerdings liegen dann zwei unabhängige W-LAN vor (das W-LAN des Fahrzeugs und das durch Tethering erzeugte W-LAN des Mobilgeräts). Es ist nicht möglich, dass zwei verschiedene W-LAN miteinander Nachrichten austauschen.

Inoffiziell kann das Mobilgerät beide Verbindungswege gleichzeitig nur durch einen Umweg, also einen „Hack“ des *Connectivity Service* erreichen. Dieser ist dafür zuständig, die Kommunikation des Gerätes via 3G und W-LAN zu kontrollieren und den jeweiligen Status festzuhalten. Um also die simultane Verbindung zu ermöglichen, muss der *Message Handler* des Connectivity Service wie folgt angepasst werden:

```
private class MyHandler extends Handler {
    @Override
    public void handleMessage(Message msg) {
        NetworkInfo info;
        //added to disable Connectivity Service
```

```
            int networkState = 8; //not any following state
            // use static google dns server for wifi and 3g
            if (msg.what == NetworkStateTracker.EVENT_STATE_CHANGED) {
                SystemProperties.set("net.dns1", "8.8.8.8");
                SystemProperties.set("net.dns2", "8.8.4.4");
                bumpDns();
            }

            //switch (msg.what) {
            switch (networkState) {
                case NetworkStateTracker.EVENT_STATE_CHANGED:
                info = (NetworkInfo) msg.obj;
                int type = info.getType();
                …..
            }
        }
    }
```

Anschließend muss die veränderte *ConnectivityService.java* im Android Quellcode kompiliert werden, wodurch eine neue *services.jar* Datei im Framework-Ordner erzeugt wird. Die existierende *services.jar* kann auf dem Smartphone mit den folgenden adb Kommandos ersetzt werden:

```
adb shell "mount -o rw,remount -t yaffs2 /dev/block/mtdblock3 /system"
adb shell "chmod 0777 /system/framework"
adb push services.jar /system/framework
adb shell "chmod 0644 /system/framework/services.jar"
adb shell "chmod 0755 /system/framework"
```

Im Anschluss muss das Smartphone neu gestartet werden. Es wird deutlich, dass diese Lösung nur für Nutzer mit technischem und sogar programmiertechnischem Verständnis möglich ist. Die meisten Anwender werden dies nicht umsetzen können. Zudem birgt dies die Gefahr der Störung von Betriebssystemfunktionalitäten im Fehlerfall. Weiterhin verbraucht die gleichzeitige Verwendung von beiden Kommunikationswegen sehr viel Energie, wodurch die Akkulaufzeit des Gerätes sich stark verkürzt. Gerade auf (längeren) Reisen ist dies inakzeptabel.

Eine andere Lösungsmöglichkeit ist es, das W-LAN nur dann zu verwenden, wenn das Gerät eine Anfrage an das Fahrzeug sendet. Somit würde die 3G-Verbindung verwendet bis das Gerät mit dem Fahrzeug kommunizieren möchte, woraufhin sie abgebrochen und eine W-LAN-Verbindung aufgebaut würde. Diese Lösung ist ebenfalls nicht uneingeschränkt zu empfehlen. Einerseits ist der wiederkehrende Verlust der Internetverbindung aus Nutzersicht unangenehm, etwa im Falle einer stehenden Verbindung zu Diensten für synchrone Kommunikation, z. B. Google Talk, ICQ, o. ä. Der Anwender wäre gezwungen, sich mit jeder neuen Verbindung auch neu beim entsprechenden Dienst anzumelden. Andererseits muss bei diesem Ansatz die Initiative vom Smartphone ausgehen. Nachrichten vom Fahrzeug können also nur als Antwort auf eine zuvor eingegangene Anfrage geschickt werden. Das Fahrzeug ist nicht in der Lage, seinerseits (wichtige) Informationen an das Gerät zu schicken. Außerdem nimmt das An- und Abmelden sowie das Suchen einer verfügbaren Verbindung einige Zeit in Anspruch, was höhere Kommunikationslatenz verursacht. Weiterhin bedeutet auch das ständige

Wechseln zwischen 3G und W-LAN einen stark erhöhten Energiebedarf und führt somit zu kurzer Akkulaufzeit.

Simultane Netzwerknutzung mit dem iPhone

Es ist dem iPhone nicht nativ möglich, eine 3G-Datenverbindung mit dem Internet zu betreiben, wenn gleichzeitig Zugriff auf ein W-LAN besteht. Die Datenverbindung zum Internet über die 3G-Mobilfunkverbindung wird automatisch deaktiviert, sobald das Gerät eine Verbindung zu einem W-LAN erkennt. Apple sieht keine Möglichkeit zur Veränderung dieses Verhaltens vor.

Allerdings zeigen Anwendungen (z. B. die „*wireless direct print*"-Funktion von HP), dass Independent Basic Service Sets (IBSS), also als Ad-Hoc-Netzwerk betriebene W-LAN, die simultane Nutzung der 3G-Internetverbindung des iPhone nicht beeinträchtigen. Durch manuell zu tätigende Einstellungen ist der Zugang zu einem isolierten W-LAN bei gleichzeitiger 3G-Internetnutzung möglich. Dazu muss in den Netzwerkeinstellungen des iPhones eine statische IP-Adresse eingestellt werden, während die Angaben zum DNS-Server und Router undefiniert bzw. unausgefüllt bleiben. Entsprechend wird dem Nutzer kein W-LAN-Symbol angezeigt. Natürlich ist dieser Weg eher umständlich und für Anwender ohne fundiertes technisches Hintergrundwissen kaum umzusetzen.

Außerdem ergibt sich ein weiteres Problem, selbst wenn es dem Nutzer gelingt, die W-LAN-Schnittstelle des iPhones entsprechend zu konfigurieren, sodass ein isoliertes W-LAN zusammen mit der 3G-Verbindung betrieben werden kann. Das iPhone merkt sich bekannte W-LANs und verbindet sich mit diesen automatisch bei erkannter Verfügbarkeit. Im Kontext von IP-KOM-ÖV bedeutet das ein schwierig zu handhabendes praktisches Problem: Steigt der Fahrgast in ein Verkehrsmittel ein, kann dennoch eine Verbindung zu einem anderen Fahrzeug hergestellt werden. Dies kann beispielsweise passieren, wenn sich in W-LAN-Reichweite ein weiteres Fahrzeug befindet, dessen W-LAN dem Mobilgerät bereits bekannt ist. Sind beide W-LAN bereits bekannt, wird vermutlich eine Verbindung zum stärkeren Signal hergestellt, was (z. B. aufgrund von Interferenzen oder örtlicher Entfernung vom Hotspot im Verkehrsmittel) ebenfalls nicht zwangsläufig das W-LAN des Fahrzeugs sein muss, in dem der Fahrgast sitzt. Über die W-LAN-Einwahl erhält der Nutzer keine Rückmeldung, damit muss er sich also dieses Umstandes bewusst sein und das richtige Netzwerk selbst auswählen können. Somit ist auch dies eine unzumutbare Belastung für einen technisch weniger versierten Nutzer.

Zusammenfassend lässt sich sagen, dass keine der vorgestellten Lösungen ein zufriedenstellendes Ergebnis liefern kann. Nativ besteht also keine Internetverbindung, während der Fahrgast mit dem Fahrzeug via W-LAN kommuniziert. Wenn also der Fahrgast nicht auf eine Internetverbindung verzichten kann und will (Nutzerakzeptanz, Nutzererleben) und das W-LAN des Fahrzeugs keine Internetanbindung bereitstellt (legale Aspekte), müssten Kompromisslösungen näher betrachtet werden. So könnte etwa die Datenmenge und -häufigkeit bei der Kommunikation zwischen Fahrzeug und Gerät minimiert werden, um so auch die Anzahl an Verbindungswechseln zu verringern und die Verbindungs- bzw. Synchronisationsintervalle zu vergrößern.

Störerhaftung bei öffentlichem Internet im Fahrzeug

Bei der Bereitstellung von Internetzugängen für die Fahrgäste des öffentlichen Personenverkehrs, z. B. durch W-LAN, ist zu beachten, dass es auf Seiten des Anschlussinhabers bzw. Anbieters des Internetzugangs zur sogenannten Störerhaftung kommen kann, wenn die Nutzer über den bereitgestellten Zugang z. B. Urheberrechtsverletzun-

gen begehen. Dabei ist in der mit „Sommer unseres Lebens“ betitelten Urteilsbegründung des BGH vom 12.05.2010 in Berufung auf vorhergehende Urteile definiert:

„Als Störer kann bei der Verletzung absoluter Rechte auf Unterlassung in Anspruch genommen werden, wer — ohne Täter oder Teilnehmer zu sein — in irgendeiner Weise willentlich und adäquat kausal zur Verletzung des geschützten Rechts beiträgt (BGH, Urt. v. 18.10.2001 — I ZR 22/99, GRUR 2002, 618, 619 = WRP 2002, 532 — Meißner Dekor I; BGH, Urt. v. 30.4.2008 — I ZR 73/05, GRUR 2008, 702 Tz. 50 = WRP 2008, 1104 — Internet-Versteigerung III)“.

Für die Haftung als Störer ist nicht der Wille bzw. ein tatsächliches Verschulden relevant, sondern die Wahrung bzw. nicht Wahrnehmung von Prüf- und Vorsorgepflichten. Für Privatpersonen sieht das Urteil des BGH unter diesen Pflichten den Einsatz von zum Zeitpunkt des Erwerbs des Gerätes üblichen Sicherungsmaßnahmen vor. Für den Einsatz in Verkehrsmitteln des öffentlichen Personenverkehrs, in Hotels oder Gaststätten könnte eine verschärfte Haftungspflicht entstehen, wenn diese die Netze nicht mit marktüblichen Sicherungsverfahren schützen und den Zugang für Nutzer, z. B. über Verfahren mit Nutzerkennung, nicht beschränken.

Soweit eine Änderung der Störerhaftung für öffentliche W-LAN Netze mit Nutzung des Internets nicht durch den Gesetzgeber angestrebt und umgesetzt wird, muss davon ausgegangen werden, dass ein freier Zugang für Fahrten im öffentlichen Personennahverkehr nicht gewährleistet bzw. vorausgesetzt werden kann.

Fazit

Die Analyse des Verbindungsaufbaus aus Nutzersicht in Kapitel 6.2.1.4 zeigt deutlich, dass die Verwendung der je Fahrzeug eindeutigen SSID mit manueller Auswahl den Benutzer vor große Hürden stellt.

Etwas einfacher stellt sich nach einmaliger Konfiguration der Verbindungsaufbau bei der Verwendung eines Ad-Hoc-Netzes dar, weil hier die Auswahl der richtigen SSID entfällt. Als Nachteil wird hierbei jedoch der erhöhte Hardware-Aufwand im Fahrzeug gesehen, weil jedes Fahrzeug mit einem zweiten W-LAN Access Point ausgerüstet werden müsste. Dabei wäre ein Access Point für die Kommunikation mit den mobilen Endgeräten des Fahrgastes zuständig, während der andere die Kommunikation mit den anderen Fahrzeugen über Ad-Hoc Meshes übernehmen würde. Die Existenz eines Ad-Hoc-Netzwerks zwischen den Fahrzeugen wäre allerdings unabhängig vom gewählten Kommunikationskanal zwischen Fahrzeug und mobilem Endgerät.

Die beiden Varianten über QR-Code und NFC bieten zwar den deutlich einfachsten Weg für Benutzer, können jedoch nicht bei allen Betriebssystemen eine automatische Einwahl in ein Netzwerk vornehmen, so dass sie eigentlich eher als Hilfsmittel zur SSID-Auswahl vor allem bei fahrzeugspezifischen SSIDs angesehen werden können.

Die größten Herausforderungen stellen die aktuellen mobilen Endgeräte dar. Ohne Manipulation der Betriebssysteme sind die mobilen Endgeräte auf die Verbindung mit einem Netzwerk beschränkt. Für den Einsatz eines W-LAN als Kommunikationskanal zwischen Fahrzeug und mobilem Endgerät würde das bedeuten, dass

(1) der Fahrgast nicht mehr ins Internet kommt, wenn sein mobiles Endgerät mit einem Fahrzeug verbunden ist, oder

(2) das Fahrzeug einen öffentlichen Internetzugang, ggf. mit Anmeldung, anbieten muss.

Variante 1 wird erheblich den Mehrwert des Dienstes und dessen Akzeptanz beim Nutzer verringern. Die zweite Variante ist aktuell nicht absehbar, da der Aufwand und die aktuellen rechtlichen Konsequenzen für die Verkehrsunternehmen zu groß wären.

Für den Machbarkeitsnachweis resultiert demnach, dass die geplante Umsetzung mit W-LAN und einer eindeutigen SSID, aber auch mit Alternativen wie dem Ad-Hoc-Netz, keine in allen Bereichen zufriedenstellende Lösung darstellt.

Daher wird abschließend festgestellt, dass die Schnittstelle vom Fahrzeug zum mobilen Endgerät unabhängig von W-LAN und weiteren möglichen Kommunikationskanälen, wie beispielsweise Bluetooth und NFC, entwickelt werden muss, um für zukünftige technische Entwicklungen offen zu sein. Für den Demonstrator wird auf Basis aktueller Technologien eine Umsetzung mit W-LAN vorgenommen.

Verband Deutscher Verkehrsunternehmen e. V. (VDV)
Kamekestraße 37-39 · 50672 Köln
T 0221 57979-0 · F 0221 57979-8000
info@vdv.de · www.vdv.de