Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Abschlussarbeit

Stephan Hölscher

Die Anwendung des Bluetooth Low Energy Standards bei der Zutrittskontrolle im öffentlichen Personenverkehr

Fakultät Technik und Informatik
Department Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Stephan Hölscher

Die Anwendung des Bluetooth Low Energy Standards bei der Zutrittskontrolle im öffentlichen Personenverkehr

Bachelorarbeit eingereicht im Rahmen des Studiums der
Wirtschaftsinformatik

im Studiengang Wirtschaftsinformatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer : Prof. Dr. Sarstedt
Zweitgutachter : Prof. Dr. Lehmann

Abgegeben am 12. Januar 2015

Autor
Stephan Hölscher
Thema der Bachelorarbeit
Die Anwendung des Bluetooth Low Energy Standards bei der Zutrittskontrolle im öffentlichen Personenverkehr
Stichworte
Bluetooth Low Energy, VDV Kernapplikation, Zutrittskontrolle, Nutzermedium, ÖPNV, Mobiltelefon, Android, JavaScript
Kurzzusammenfassung
Automatisierte Zutrittskontrollen werden im europäischen Ausland für die Regulierung im öffentlichen Personenverkehr eingesetzt. Um diese Zutrittskontrollen nutzen zu können, werden elektronisch lesbare Nutzermedien benötigt. Dazu gehören der 2D-Barcode, die Chipkarte, die Magnetstreifenkarte und das NFC-fähige Mobiltelefon. Diese Arbeit beschäftigt sich mit Bluetooth Low Energy als neuartige Technologie für die Nutzung von automatisierten Zutrittskontrollen. Dabei werden bestehende Nutzermedien mit dieser Technologie vergleichen. Anschließend folgt eine Anforderungsanalyse, aus der ein Konzept für den Anwendungsfall abgeleitet wird. Als Ergebnis wird eine prototypische Umsetzung dieses Konzeptes präsentiert, welche Bluetooth Low Energy in der Kommunikation zwischen Nutzermedium und Lesegerät verwendet. Dieser Prototyp zeigt, dass Bluetooth Low Energy zur Anwendung als Zutrittskontrolle geeignet ist. Abschliessend werden im Ausblick mögliche Weiterentwicklungen skizziert.

Author
Stephan Hoelscher
Title of the paper
The usage of bluetooth low energy for the access control at a public transport scenario
Keywords
Bluetooth Low Energy, VDV core application, access control, user media, public transport, mobile, Android, JavaScript
Abstract
Automated access controls are used in several European countries for the regulation in public transport. To use this access controls you need some electronically readable user media. These are, for example, the 2D barcode, the chip card, the magnetic stripe cards and the NFC-enabled mobile phones. This thesis deals with Bluetooth Low Energy as novel technology for automated access controls. Here, existing user media will be compared with this technology. Subsequently, this thesis derives the concept for the realization of a use case from a requirements analysis. As a result a prototype will be implemented from this concept, which uses Bluetooth Low Energy for the communication between user media and reader device. The prototype shows that Bluetooth Low Energy can be used for an access control. Finally this thesis concludes with possible future enhancements of the approach.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Die deutschen Verkehrsunternehmen haben ein entscheidendes Problem. Die Infrastruktur des öffentlichen Personenverkehrs kommt langsam, aber sicher in die Jahre und es steht nicht genug Geld für die Instandsetzung und den Neubau bereit. „Eine umfangreiche Finanzierungsstudie des [... Verbands der deutschen Verkehrsunternehmen...] VDV zusammen mit 13 Bundesländern und dem Deutschen Städtetag hatte ergeben, dass statt der jährlich rund 1,6 Milliarden Euro mindestens 1,9 Milliarden zur Verfügung stehen müssten... [BEEL2013]“. Das bedeutet, dass laut dieser Finanzierungsstudie rund 300 Mio. Euro für den Ausbau und die Instandhaltung der Verkehrsinfrastruktur fehlen. Dieses Geld soll durch den Bund und die Länder zur Verfügung gestellt werden. Dabei haben die Verkehrsunternehmen auch an anderer Stelle die Möglichkeit, Mehreinnahmen zu generieren. Damit ist aber nicht die Erhöhung der Fahrkartenpreise gemeint. Vielmehr gehen ihnen durch Schwarzfahrer – also Nutzer des öffentlichen Personenverkehrs, die kein Nutzungsentgelt zahlen – Millionenbeträge verloren, die nicht in der Erhaltung und im Ausbau des Schienennetzes oder der Transportmittel eingesetzt werden können.

Abbildung 1 zeigt die Statistik über die Einnahmeverluste durch Schwarzfahrer bei Nahverkehrsunternehmen ausgewählter Städte in Deutschland im Jahr 2012 der Wirtschaftswoche, nach der allein den Verkehrsunternehmen in Berlin und Hamburg Einnahmen von 44 Mio. € entgehen (vgl. [SCHL2012]). Das entspricht fast 15 % der fehlenden Summe aus der Finanzierungsstudie des VDV. Dementsprechend macht es für die Verkehrsunternehmen durchaus Sinn, konsequent gegen Schwarzfahrer vorzugehen. Eine Möglichkeit ist die Ausweitung von stichprobenartigen Kontrollen im Verkehrsablauf. Allerdings besteht hier immer noch der Nachteil, dass eine Vielzahl der Schwarzfahrer nicht erwischt wird.

Eine andere Lösung wäre die Einführung von Einstiegskontrollen. Laut dem oben genannten Artikel der Wirtschaftswoche wurde im Bereich der Hamburger Hochbahn der Zwang zur Vorlage eines gültigen Tickets, welches vor Fahrtantritt vorhanden sein muss, für die Nutzung der Buslinien eingeführt. Dadurch sank die Schwarzfahrerquote bei der Busnutzung von 5% auf 2 % und es konnten Mehreinnahmen von 3 Mio. Euro generiert werden.

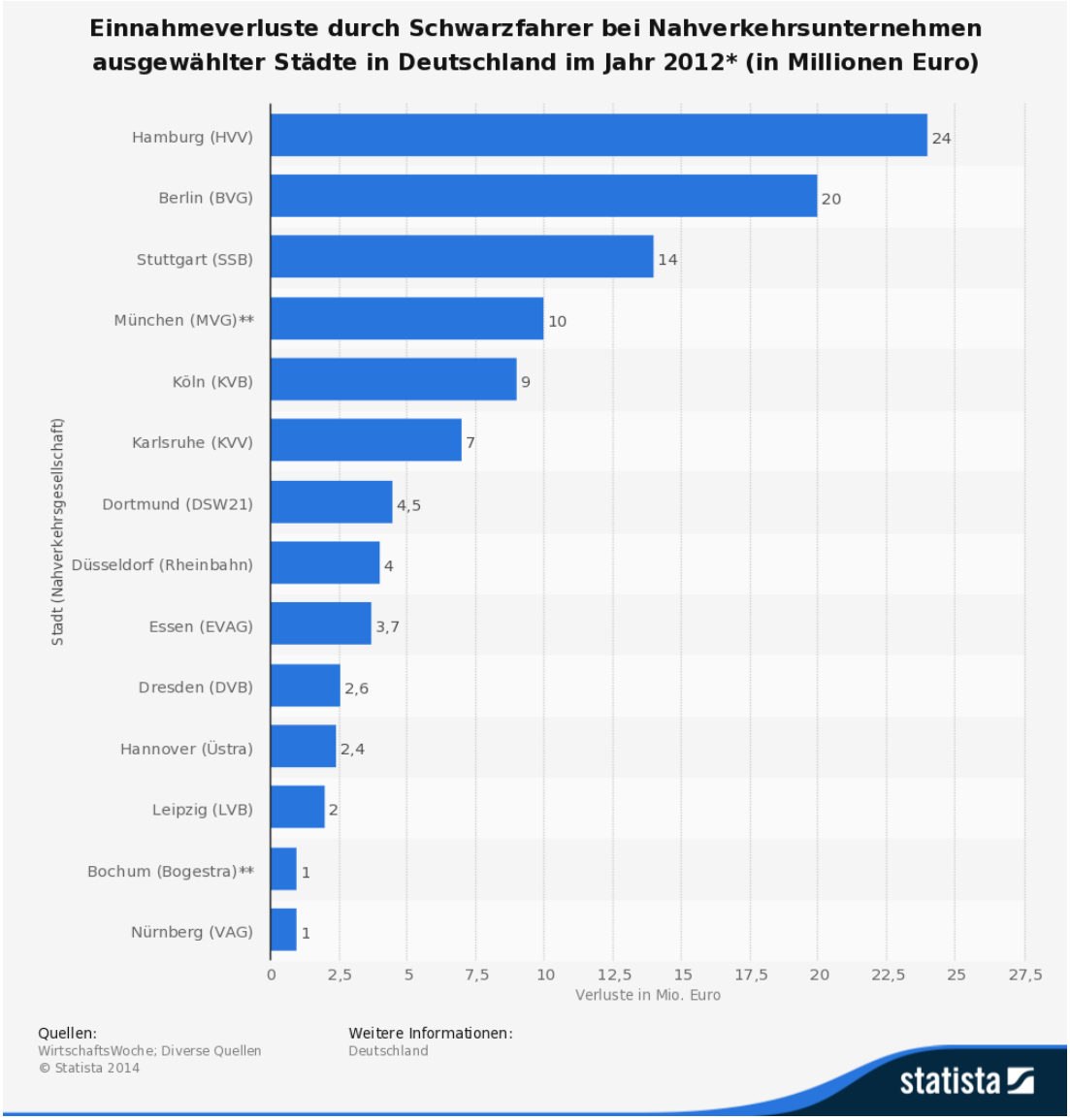

Abbildung 1 - Einnahmeverluste deutscher Verkehrsverbünde 2012

1.1 Aufgabenstellung

Der Vorteil von Einstiegskontrollen in Bussen liegt in der Tatsache, dass mit dem Busfahrer ein Kontrolleur anwesend ist. So kann verhindert werden, dass ein Fahrgast zusteigt, ohne seinen Fahrausweis vorzuweisen. Dieses Konzept kann jedoch nur schwer auf andere Arten des öffentlichen Personenverkehrs wie der Bahn angewendet werden. Hier ist es nicht möglich, die Fahrgäste beim Betreten der Transportmittel durch den Fahrer überprüft zu lassen. Die Fahrgäste müssen also schon beim Betreten des Bahnsteiges kontrolliert werden können. Aber auch hier ist der Einsatz von

zusätzlichen Kontrolleuren eher schwer. Der Personalaufwand für solche Kontrollen wäre enorm. Abhilfe kann durch eine automatisierte Zutrittskontrolle auf Basis von elektronisch lesbaren Fahrscheinen geschafft werden.

Obwohl dieses Verfahren im europäischen Raum schon sehr oft zur Anwendung kommt, gibt es in Deutschland bisher jedoch keinen Einsatzraum. Um das Anmelden des Fahrgastes bei den Zutrittskontrollen zu gewährleisten, ist der Einsatz technischer Einrichtungen notwendig. Dazu verfügen die Bahnhöfe des europäischen Vergleichsraumes über Zutrittskontrollgeräte mit Lesegeräten, die gegebenenfalls verschiedene Nutzermedien der Fahrgäste auslesen können.

Bei diesen Nutzermedien handelt es sich entweder um eine Chipkarte, eine Magnetstreifenkarte oder um ein Smartphone. Die Chipkarte kommuniziert über Kurzwellenfunk mit dem Lesegerät. Als Smartphone werden Mobiltelefone bezeichnet, die meist über einen berührungsempfindlichen Bildschirm verfügen und mit dem Internet über das GSM/LTE-Netz kommunizieren können (vgl. [KOPP2012]). Damit die stationären Leseeinheiten mit einem Smartphone eine Verbindung aufbauen können, wird zurzeit die Kommunikation über den in vielen Smartphone integrierten NFC-Chipsatz oder ein 2D-Barcode nach VDV-Kernapplikationsstandard genutzt. Magnetstreifenkarten können nur bei entsprechenden Lesegeräten genutzt werden.

Unabhängig vom Nutzermedium werden die Informationen zur Zutrittskontrolle elektronisch ausgelesen. Im Anschluss stellt das Zutrittskontrollgerät fest, ob der Fahrgast mit diesem Nutzermedium berechtigt ist, den Bahnhof zu betreten und das Verkehrsmittel zu nutzen. Ist dies der Fall, so meldet das Lesegerät über ein optisches oder akustisches Signal, dass der Fahrgast für die Nutzung des Verkehrsmittels angemeldet ist. Ist der Fahrgast nicht berechtigt, das Verkehrsmittel zu nutzen, so wird dies ebenfalls optisch oder akustisch mitgeteilt. Außerdem werden physikalische Mittel wie zum Beispiel Schranken verwendet, um den Zutritt zu verhindern.

Da sich die Nutzung von Smartphones immer mehr durchsetzt (vgl. [COMS2014]), werden diese auch vermehrt als Nutzermedium im öffentlichen Personenverkehr eingesetzt. Beispielsweise können Fahrgäste ihre Smartphones schon jetzt nutzen, um damit Fahrkarten zu kaufen. Dabei werden die Nachteile von NFC und 2D-Barcode schnell deutlich. Ein Beispiel ist die Tatsache, dass die NFC-Technologie auf einigen populären Smartphones (wie zum Beispiel dem Apple iPhone) nicht verfügbar ist. Ein weiterer Nachteil ist die geringe Reichweite von NFC und 2D-Barcode. Bei beiden Techniken muss der Fahrgast mit seinem Nutzermedium nah an das Lesegerät des Verkehrsmittels oder der Zutrittskontrolle herantreten, um mit ihm zu interagieren. NFC ist auf 20 bis 25 cm begrenzt. Der 2D-Barcode muss auf eine viel kürzere Distanz gescannt werden, um Fehler zu vermeiden.

Aufgrund der kurzen Reichweiten ist es notwendig, sich mit einer weiteren Technologie zur Kommunikation zwischen Leseeinheit der Zutrittskontrolle und dem

Smartphone des Fahrgastes als Nutzermedium zu beschäftigen. Eine dieser Technologien stellt Bluetooth Low Energy dar. Bluetooth Low Energy basiert auf dem Bluetooth-Standard und verfügt über einen geringeren Energieverbrauch als herkömmliche Bluetooth-Verbindungen. Dies wird durch optimierte Technologie und eine geringere Sendeleistung ermöglicht, die einen größeren Abstand zwischen den beteiligten Parteien zulässt und außerdem in allen neueren Smartphones verfügbar ist (vgl. [TOWN2014]).

Diese Bachelorarbeit soll sich sowohl mit der Erarbeitung als auch mit der technischen Umsetzung eines Konzeptes zur Zutrittskontrolle auf Basis von Bluetooth Low Energy beschäftigen. Der Einsatz von Smartphones als Nutzermedium wird vorausgesetzt. Dazu werden die bestehenden Ansätze der Nutzung von Chipkarten, Magnetstreifenkarten, NFC-fähigen Mobiltelefonen und 2D-Barcodes mit dem Bluetooth Low Energy-Ansatz verglichen. Basierend auf diesen Vergleichsergebnissen soll ein Konzept entstehen, das eine mögliche Nutzung von Bluetooth Low Energy zur Kommunikation zwischen Lesegerät und Smartphone bei der An- und Abmeldung in Verkehrsmitteln aufzeigt. Dieses Konzept ist in einem Prototyp umzusetzen. Bei diesem Prototyp handelt es sich um eine Machbarkeitsstudie unter Laborbedingungen. Demzufolge soll abschließend auf mögliche Probleme in einem realen Szenario für eine solche Lösung eingegangen werden.

2 Grundlagen

Der Einsatz von modernen Technologien wie Bluetooth Low Energy bei der Zutrittskontrolle im öffentlichen Personenverkehr berührt eine Vielzahl von Themenbereichen. In den folgenden Kapiteln soll auf diese verschiedenen Themen eingegangen werden. Dabei wird erklärt, welche Zusammenhänge zwischen den einzelnen Bereichen bestehen und welche Anforderungen an die Verbünde im öffentlichen Personenverkehr gestellt werden. Auch die technischen Fragen sowie die Unterschiede zwischen den Nutzermedien werden beleuchtet.

2.1 Der öffentliche Personenverkehr

Der öffentliche Personenverkehr dient der „...Beförderung von Personen durch Unternehmen des öffentlichen Verkehrs... [STAC2014]“. Dabei wird dieser unterteilt in Personennah- und Personenfernverkehr. Die Unterteilung erfolgt anhand der zurückzulegenden Strecke, wobei der Regionalverkehr zur Verbindung einer Stadt mit ihrem Umland auch bei größerer Entfernung noch dem Personennahverkehr zugeordnet wird. „...Je nach benutztem Verkehrsweg wird weiter unterschieden zwischen Schienenverkehr, öffentlichen Straßenpersonenverkehr und Luftverkehr. [STAC2014]“ Dem öffentlichen Personenverkehr ist gemein, dass die Verkehrsmittel durch mehrere Personen gemeinsam und gleichzeitig genutzt werden können. Das Verkehrsmittel hält sich dabei an einen Zeitplan und an vordefinierte Haltepunkte. Dem entgegen steht der sogenannte Individualverkehr, bei dem eine Person oder eine begrenzte Anzahl von Personen auf eigene Verantwortung z.B. mit dem Auto ein individuelles Ziel ansteuern. „...Taxi- und Mietwagenverkehr haben sowohl öffentlichen als auch individuellen Charakter, weil sie zwar den Bestimmungen des Personenbeförderungsgesetzes unterliegen und hier als öffentliches Verkehrsmittel aufgefasst werden, aber individuell genutzt werden können... [STAC2014]“ .

2.2 Verband deutscher Verkehrsunternehmen

Die Unternehmen des öffentlichen Personenverkehrs sind im Verband deutscher Verkehrsunternehmen (VDV) organisiert. Der VDV wurde 1991 gegründet und besteht in seiner derzeitigen Form seit 2003. „Rund 600 Mitglieder aus dem öffentlichen Personenverkehr und dem Schienengüterverkehr sind im VDV in 9 Landesgruppen und 5 Sparten organisiert: Bus, Tram, Personenverkehr mit Eisenbahnen, Schienengüterverkehr sowie Verbund- und Aufgabenträgerorganisationen... [VDVE2012]“. Neben der gemeinsamen Öffentlichkeitsarbeit und der Vertretung der Verkehrsunternehmen in der Politik hat es sich der VDV zur Aufgabe gemacht, ein gemeinsames, regional übergreifendes elektronisches Ticket in Deutschland (kurz (((eTicket Deutschland) zu etablieren. Dazu wurde im Jahr 2003 die VDV eTicket Service GmbH und Co. KG gegründet, welche auf Basis des eTicket-Standards VDV-Kernapplikation die Ausbreitung und den Ausbau der eTicket-Infrastruktur in Deutschland vorantreibt.

2.2.1 VDV-Kernapplikation

VDV-Kernapplikation (VDV-KA) ist der „...offene Daten- und Schnittstellen-Standard für Electronic Ticketing bzw. Elektronisches Fahrgeldmanagement (EFM) im Öffentlichen Personenverkehr... [VDVK2014]“ Als Grundbaustein des elektronischen Fahrkartensystems wird es für (((eTicket Deutschland verwendet, auf dem deutschlandweit alle eingeführten EFM-Systeme von Verkehrsverbünden und -unternehmen basieren. Dieser Standard wird dabei von der VDV eTicket Service GmbH

weiterentwickelt und angepasst. Bei einem eTicket handelt es sich um eine Fahrkarte, welche auf einem Nutzermedium ausgegeben wird und elektronisch lesbar ist. Nutzermedien sind beispielsweise eine Chipkarte, ein Mobiltelefon oder eine Papierfahrkarte mit einem aufgedrucktem 2D-Barcode.

Verkehrsunternehmen, die am (((eTicket Deutschland teilnehmen, müssen sich organisatorisch, technisch und fachlich an den Standard der VDV Kernapplikation halten. Die Teilnahme wird durch einen Teilnahmevertrag geregelt. Mit diesem wird festgelegt, dass die Systeme der teilnehmenden Verkehrsunternehmen gleichberechtigt über wohldefinierte Schnittstellen miteinander Daten austauschen können. So soll auch die Interoperabilität – also der Verkauf von elektronischen Tickets über die Grenzen von Verkehrsverbünden hinweg – realisiert werden.

Die Verkehrsunternehmen können sich für eine der Ausbauvarianten der Kernapplikation entscheiden. Dabei handelt es sich um das eBezahlen (eine bargeldlose Prepaid-Variante zum Kauf von Fahrkarten), das elektronische Ticket selbst (elektronischer Fahrschein, welches auf dem Medium des Fahrgastes gespeichert wird) und das elektronische Ticket mit automatischer Fahrpreisberechnung. Bei der letzten Ausbaustufe meldet sich der Fahrgast bei Fahrtbeginn für die Nutzung des Verkehrsmittels an und bei Fahrtende wieder vom Verkehrsmittel ab. Das An- und Abmelden kann mit Interaktion (CheckIn/CheckOut, siehe Kapitel 2.2.2) oder ohne Interaktion (BeIn/BeOut, siehe Kapitel 2.2.3) des Kunden geschehen. Die Vorgänge zum An- und Abmelden werden registriert und an das eTicket-Hintergrundsystem übermittelt. Dieses berechnet dann automatisch den vom Fahrgast zu entrichtenden Fahrpreis. Hier wird dann der für den Fahrgast günstigste Fahrpreis berechnet.

Als Medium für die Aufnahme der elektronischen Tickets bzw. der Ab- und Anmeldevorgänge in der dritten Ausbaustufe bietet die Kernapplikation verschiedene Wege an. So können Chipkarten, NFC-taugliche Mobiltelefone oder 2D-Barcodes als Träger für ein eTicket verwendet werden. Als Medium für die Aufnahme der elektronischen Tickets bzw. der Ab- und Anmeldevorgänge mit automatischer Fahrpreisberechnung empfiehlt die Kernapplikation die Chipkarte. „... [Diese] unterstützen rein technisch alle vorhandenen Ausbauvarianten, auch wenn im jeweiligen Einsatzgebiet nur bestimmte Funktionen freigeschaltet sein sollten... [VDVK2014]“.

Das elektronische Ticket mit automatischer Fahrpreisberechnung der Kernapplikation ermöglicht auch eine Umsetzung der Zutrittskontrolle auf Basis von Bluetooth Low Energy. Die An- und Abmeldung der Fahrgäste stellen dabei das Einlesen der Nutzermedien an den Zutrittskontrollgeräten dar. Auf Grund dieser Möglichkeiten wird im Rahmen dieser Arbeit die dritte Ausbaustufe der Kernapplikation vorausgesetzt.

2.2.2 CheckIn/CheckOut

Ein Verfahren zum An- und Abmelden eines Fahrgastes im Verkehrsmittel ist das

sogenannte CheckIn/CheckOut-Verfahren. CheckIn/CheckOut bedeutet eine gewollte Interaktion des Fahrgastes, wobei dieser mit Hilfe seines Nutzermediums mit einem Lesegerät kommuniziert und so entweder den Anmelde- oder den Abmeldevorgang durchführt. Das Gelingen wird am Lesegerät durch ein Signal verdeutlicht. Beim Abmelden wird ebenfalls eine Interaktion durch den Nutzer an einem Lesegerät durchgeführt. Bei einer Zutrittskontrolle wird außerdem der Durchgang erst im Moment des Erfolges freigegeben. Basierend auf diesen Vorgängen wird dann die Fahrpreisberechnung durchgeführt.

Für dieses Verfahren ist die Art des Nutzermediums nicht relevant. Es ist sowohl das kontaktlose Lesen von einer Chipkarte oder eines NFC-fähiges Handy, das kontaktlose Scannen eines 2D-Barcodes als auch das kontaktbehaftete Lesen einer Magnetstreifenkarten oder einer Chipkarte möglich. Die Lesegeräte können sich dabei sowohl direkt im Fahrzeug als auch an den Haltestellen befinden. Außerdem ist es möglich, dass diese Lesegeräte mit einer Zutrittskontrolle verbunden sind (siehe Kapitel 2.3.1).

In dieser Arbeit wird das CheckIn/CheckOut-Verfahren betrachtet.

2.2.3 BeIn/BeOut

Ein weiteres Verfahren zum An- und Abmelden eines Fahrgastes im Verkehrsmittel ist das BeIn/BeOut-Verfahren. Ein am BeIn/BeOut-Verfahren teilnehmender Nutzer wird beim Betreten eines Verkehrsmittel oder einer Haltestelle automatisch erkannt und registriert. Verlässt der Fahrgast am Ende seiner Fahrt das Verkehrsmittel wieder, wird auch dieses Ereignis bemerkt und die Fahrt im Hintergrundsystem registriert. Der Fahrgast muss keine Interaktion mit Lesegeräten durchführen. Gemein zum CheckIn/CheckOut-Verfahren ist das Berechnen des Fahrpreises aus den gewonnenen Daten. Bei beiden Verfahren wird dem Fahrgast die möglich günstigste Fahrt in Rechnung gestellt („Best-Price-Berechnung“). „Eine automatische Raumerfassung der Fahrgäste ohne aktive Handlungen bei Aus- und Einstieg ist nötig, da in Deutschland kontrollierte Zugangssysteme zum ....[öffentlichen Personenverkehr]... in Form von Schranken oder Drehkreuze zur Zeit keine Akzeptanz finden. Im Zuge einer Raumerfassung kann die durch den Fahrgast in Anspruch genommene Leistung in Bezug zu benutzten Haltestellen und Fahrzeugen (fahrzeugscharfe Fahrtenbildung) genau erfasst werden. Diese Information bildet die Grundlage für eTarife, die eine nutzungsabhängige Preisberechnung ermöglichen... [NACH2014]“.

Um dieses Verfahren zu nutzen, benötigt der Nutzer ein Nutzermedium, welches über eine gewisse Entfernung und ohne Sichtverbindung von einem Lesegerät erfasst werden kann. Damit scheiden hier Magnetstreifenkarten und 2D-Barcodes als Medium aus. Bestimmte Chipkarten mit RFID-Chips oder NFC-fähige Mobiltelefone bieten diese Funktionalität an und können für BeIn/BeOut-Verfahren verwendet werden. Allerdings gibt es bei der Erfassung von elektronischen Tickets noch Probleme bezüglich der

Genauigkeit und Zuverlässigkeit des Lesevorgangs. Deswegen befinden sich BeIn/BeOut-Systeme und Ansätze in Deutschland in der Erprobungsphase.

2.2.4 Unterschiede zwischen CheckIn/CheckOut und BeIn/BeOut

Der Hauptunterschied zwischen den Verfahren zur An- und Abmeldung von Fahrgästen im Verkehrsmittel besteht in der vorgenommen Interaktion des Nutzers mit einem Lesegerät. Beim CheckIn/CheckOut-Verfahren muss der Fahrgast aktiv mittels seines Nutzermediums mit dem Lesegerät im Verkehrsmittel oder an der Haltstelle interagieren. Es findet also eine für den Nutzer bewusste Erfassung des Ein- oder Ausstiegs statt. Das ist beim BeIn/BeOut-Verfahren nicht notwendig. Der Fahrgast muss nicht zu einem Lesegerät gehen. Es findet kein aktiver Vorgang statt. Die Lesegeräte erfassen selbstständig den Ein- oder Ausstieg des Nutzers mittels einer Funkverbindung mit dem Nutzermedium. Es handelt sich somit um eine für den Nutzer unbewusste, automatisierte Erfassung seines Ein- oder Ausstiegs.

Ein weiterer Unterschied lässt sich bei den Nutzermedien finden, die sich für das jeweilige Verfahren eignen. Bei einem CheckIn/CheckOut-Verfahren kommen Medien zum Einsatz, die durch ein elektronisches Lesegerät verarbeitet werden können. Hierbei ist nebensächlich, welche Art von Verbindung zwischen Lesegerät und Medium vorliegt. Das bedeutet, dass sowohl Sichtverbindung wie 2D-Barcodes als auch kontaktbehaftete Verbindungen wie Magnetstreifenkarten oder Funkverbindungen und kontaktlose Verbindungen wie NFC oder RFID zum Einsatz kommen können. Beim BeIn/BeOut-Verfahren ist das anders. Hier soll jede Interaktion des Fahrgastes vermieden werden. Das bedeutet, dass das für Sicht- und kontaktbehaftete Verbindungen notwendige Hervorholen des Nutzermediums nicht möglich ist. Aus diesem Grund ist das BeIn/BeOut-Verfahren für Nutzermedien, die auf Sicht- bzw. kontaktbehafteten Verbindungen basieren, nicht geeignet. Es eignen sich ausschließlich kontaktlose Funkverbindungen wie RFID, NFC und andere Funktechnologien.

Darüberhinaus muss die Zuverlässigkeit des Erfassens eines Ein- bzw. eines Ausstiegs gewährleistet sein. Hier befindet sich BeIn/BeOut erst in der Erprobung, während es für den CheckIn/CheckOut-Ansatz schon produktive Beispiele wie zum Beispiel im öffentlichen Personenverkehr in Hanau gibt (vgl. [HASB2011]).

2.3 Zutrittskontrolle im öffentlichen Personenverkehrs

Beim Einsatz des CheckIn/CheckOut-Verfahren ist es für den Fahrgast notwendig, eine Interaktion mit einem Lesegerät durchzuführen. Diese Interaktion lässt sich nutzen, um festzustellen, ob der Fahrgast überhaupt berechtigt ist das Verkehrsmittel zu nutzen. Dies erfolgt beispielsweise durch eine bestimmte Fahrtberechtigung oder durch eine Authentifizierung zur Teilnahme am öffentlichen Personenverkehr. Wird diese Überprüfung durch die Systeme des Verkehrsunternehmens durchgeführt, so handelt es sich dabei um ein System mit Zutrittskontrolle. Dem entgegen steht ein offenes

System, bei dem die Fahrgäste einem Verkehrsmittel ohne eine Zutrittskontrolle zusteigen können. Ein Vergleich dieser beiden Systeme erfolgt in Kapitel 2.3.1, während die bisherigen Technologien bei der Zutrittskontrolle in Kapitel 2.3.2 vorgestellt werden.

2.3.1 Offenes System vs. System mit Zutrittskontrolle

Es wird zwischen offenen Systemen auf der einen und Systemen mit Zutrittskontrolle auf der anderen Seite unterschieden. Bei einem offenen System ist der Fahrgast selbstverantwortlich die notwendigen An- und Abmeldevorgänge durchzuführen. Die Vorgänge werden zum Zu- oder Ausstieg nicht unmittelbar kontrolliert, sondern durch stichprobenartige Überprüfungen während der Fahrt ähnlich der Sichtprüfungen von Papierfahrkarten durch Kontrolleure mit entsprechenden Lesegeräten durchgeführt. Bei solchen Kontrollen muss der Fahrgast ein entsprechend validiertes Nutzermedium vorweisen. Anderenfalls befindet er sich unberechtigt im Verkehrsmittel.

Um den unberechtigten Zutritt zum Verkehrsmittel zu erschweren, wird das System mit Zutrittskontrolle verwendet. Hierbei wird vor dem Zutritt zum Verkehrsmittel oder zur Haltestelle durch Vorlage der Fahrtberechtigung überprüft, ob der Fahrgast zur Teilnahme am öffentlichen Personenverkehr berechtigt ist. Da beim CheckIn/CheckOut-Verfahren eine Interaktion vom Fahrgast mit einem Lesegerät durchgeführt werden muss, werden Zutrittskontrolle und An- und Abmeldung oft verbunden. Die Überprüfung der Zutrittsberechtigung folgt dazu einem manuellen oder einem automatisierten Ansatz. Beim manuellen Ansatz überprüft ein Kontrolleur das Vorhandensein der Berechtigung. Er wertet hierbei das Ergebnis des Lesegerätes aus. Beim automatisierten Ansatz werden hingegen technische Hilfsmittel eingesetzt, beispielsweise Durchgangssperren wie Schranken oder Drehkreuze. Diese werden in der Regel aufgrund ihrer Größe bei der Zutrittskontrolle an Haltestellen und Bahnhöfen eingesetzt. Die Überprüfung der Berechtigungen wird vom System automatisch durchgeführt.

Der Einsatz von Systemen mit automatischer Zutrittskontrolle ist in Deutschland ein Politikum und hat zurzeit keine große Akzeptanz. Allenfalls eine manuelle Zutrittskontrolle im Rahmen von Buseinstiegen findet statt. Zumeist findet man jedoch im öffentlichen Personenverkehr offene Systeme, bei denen die Berechtigungskontrolle vorzugsweise stichprobenartig stattfindet. Dagegen ist im europäischen bzw. im internationalen Ausland die automatische Zutrittskontrolle mehr verbreitet. Ein Beispiel ist hierfür das Oyster-System von des britischen Verkehrsunternehmen Transport for London, welches an Bahnhöfen im Londoner Stadtgebiet auf ein CheckIn/CheckOut-Verfahren mit Durchgangssperre zur Zutrittskontrolle und Chipkarten als Nutzermedium setzt.

Im Rahmen dieser Arbeit soll ein weiterer Ansatz für eine automatische Zutrittskontrolle gefunden werden.

2.3.2 Im Einsatz befindliche Technologien bei der Zutrittskontrolle

Da in dieser Arbeit das CheckIn/CheckOut-Verfahren betrachtet wird, werden im folgenden nur Technologien betrachtet, die für diese Verfahren verwendetet werden. Andere Technologie werden nicht vorgestellt. Für den Einsatz einer automatischen Zutrittskontrolle ist es notwendig, Nutzermedien zu verwenden, die von einem elektronischen Lesegerät ausgelesen und verarbeitet werden. Zu den geeigneten Nutzermedien gehören Magnetstreifenkarten, Chipkarten, 2D-Barcodes und Mobiltelefone mit NFC-Chip.

Magnetstreifenkarten

Beim Lesen einer Magnetstreifenkarte durch ein Lesegerät handelt es sich um eine kontaktbehaftete Verbindung zwischen Nutzermedium und Lesegerät. Die Magnetstreifenkarte hat eine Standardgröße von 85,6 mm x 54 mm x 0,76 mm. „In die Magnetstreifenkarte ist ein i.d.R. 12,7 mm breiter Magnetstreifen (Magnetspur) integriert, auf dem Daten in drei Spuren aufgezeichnet bzw. gelesen werden können... [METZ2014-2]“. Dabei unterscheidet man zwischen Low Coercivity- (LowCo) und High Coercivity-Karten (HighCo). Der Unterschied liegt in der Dichte des Magnetflusses, mit der die Karten beschrieben werden. Bei LowCo-Karten liegt diese mit 30 mT deutlich unter der Flussdichte von HighCo-Karten, die zwischen 275 mT und 400 mT liegt. Das bedeutet, dass das Be- und Überschreiben von HighCo-Karten wesentlich schwerer als bei LowCo-Karten ist.

Abbildung 2 - Magnetstreifenkarte aus London

„Eine Magnetstreifenkarte besitzt drei Spuren auf denen Informationen gespeichert werden können. Die erst Spur hat eine Kapazität von 553 Bit (79 Zeichen, 6Bit+Parity), die zweite kann 200 Bit (40 Zeichen, 4 Bit+Parity) speichern. Die Spur 3 hat mit 535 (107 Zeichen, 4 Bit+Parity) Bit die zweithöchste Datendichte... [MAIE2014]“. Auf Grund der preiswerten und einfachen Erstellung werden Magnetstreifenkarten verbreitet eingesetzt. Bank- und EC-Karten sowie Zugangskontrollkarten sind bekannte Beispiele für den Einsatz solcher Karten. Im öffentlichen Personenverkehr werden Magnetstreifenkarten beim Lesen von Zugangsberechtigungen durch technische Zutrittskontrollen genutzt. Dabei enthält die Fahrkarte einen Magnetstreifen, welche die Informationen über der Gültigkeit der Fahrkarte in maschinenlesbarer Form enthält, siehe Abbildung 2. So kann eine technische Einrichtung diese Informationen auswerten.

Inzwischen gehören Magnetstreifenkarten aber zu den unsicheren Nutzermedien. „Das Problem ist schnell erkannt: Der Magnetstreifen kann ohne weiteres von jedem gelesen werden. Er ist wie eine elektronische Prägungszone bzw. Beschriftung auf der Karte. Man kann einen Magnetstreifen nicht vor unberechtigtem Lesen schützen. Man könnte ihn verschlüsseln, aber er ist immer noch lesbar und damit auch kopierbar... [MAIE2014]“. Damit können auch die Informationen einer Fahrkarte nicht mehr sicher verwahrt werden. Deshalb wird die Magnetstreifenkarte auch im öffentlichen Personenverkehr immer öfter durch Chipkarten abgelöst, die ein sichereres Medium darstellen.

Chipkarten

Chipkarten wurden entwickelt, um die Nachteile von Magnetstreifenkarten aufzufangen und für eine höhere Sicherheit und mehr Speicherkapazität zu sorgen. Dabei handelt es sich um „... eine spezielle Plastikkarte in die ein Chip integriert ist, der unterschiedliche Funktionen übernehmen kann... [METZ2014]“. Es gibt die Chipkarte in verschiedenen Ausprägungen. Als reine Speicherkarte wird der Speicherplatz auf dem Chip nur zum Lesen und Schreiben von Daten genutzt. Die Lesegeräte können diesen Speicher auslesen, mit den Daten arbeiten und diese wieder auf die Karte schreiben. Diese Art von Chipkarte kommt zum Beispiel als Telefonkarte oder als Zugangskarte zu Hotelzimmern zum Einsatz.

Im öffentlichen Personenverkehr kommt eine andere Variante der Chipkarten zum Einsatz. Hierbei handelt es sich um Prozessorkarten. Bei diesen Karten wird der Speicherplatz nicht alleine zum Speichern der Daten genutzt. Vielmehr können auf dem Chip Prozesse ausgeführt werden, welche mit den Daten arbeiten. Diese Prozesse sind meistens kryptografische Prozesse, so dass die Daten auf der Chipkarte nicht einfach ausgelesen werden können. Die zugreifenden Lesegeräte benötigen deshalb spezielle Schlüssel, um mit der Chipkarte kommunizieren zu können. Die VDV-Kernapplikation setzt eine SAM-Architektur voraus, damit eine sichere Kommunikation ermöglicht werden kann. Anderenfalls können diese Karten nicht mit den auf VDV-Kernapplikation basierenden Systemen bearbeitet werden.

Abbildung 3 - Oyster-Card mit Lesegerät

Außerdem unterscheidet man zwischen kontaktbehafteten und kontaktlosen Chipkarten. Bei den kontaktbehafteten Karten muss zwischen Karte und Lesegerät ein direkter physischer Kontakt bestehen, um eine Kommunikation zu ermöglichen. Die Karte wird dabei oft in ein Lesegerät eingesteckt. Diese Technik kommt beispielsweise bei Krankenkassenkarten zum Einsatz. Kontaktlose Chipkarten benötigen dagegen keinen physischen Kontakt zwischen Karte und Lesegeräte. „Die Übertragung der Daten zwischen der kontaktlosen Chipkarte und dem RFID-Lesegerät erfolgt drahtlos über die Luftschnittstelle, das Contactless Chipcard Interface (CCI), mittels induktiver oder kapazitiver Kopplung, ohne dass sich die Chipkarte in einer bestimmten Lage befinden muss. [... Auch die Strom-] Versorgung der kontaktlosen Chipkarte erfolgt durch Induktion über die CCI-Schnittstelle vom Lesegerät aus... [IT-W2014-2]“.

Die Vorteile der kontaktlosen Chipkarte liegen in der schnellen Verarbeitung, da die Position auf dem Lesegerät nicht wichtig ist. Deshalb wird sie auch im öffentlichen Personenverkehr eingesetzt. Die Einrichtungen für die Zutrittskontrolle und das An- und Abmelden beim CheckIn/CheckOut-Verfahren verfügen dabei über entsprechende Lesegeräte. Dieses übernimmt dann die Kommunikation mit der Karte, verarbeitet die Daten und schreibt das Ergebnis wieder auf die Karte. Die Chipkarte ist das am weitesten verbreitete Nutzermedium bei der Nutzung des CheckIn/CheckOut-Verfahren mit und ohne Zutrittskontrolle. Ein Beispiel dafür ist das Oyster-System in London, siehe Abbildung 3.

2D-Barcode

Ein weiteres Nutzermedium, welches von der VDV-Kernapplikation für die Nutzung eines elektronischen Tickets vorgesehen ist, ist der 2D-Barcode. Dabei handelt es sich um einen QR (Quick Response)-Barcode. „Das QR-Barcode-Symbol hat ein quadratisches Format und ist gekennzeichnet durch schwarz-weiße Quadrate, die sich an drei Ecken befinden. Diese Kennzeichnung dient der Positionierung des 2D-Codes, der omnidirektional lesbar ist. Die Daten werden [....] in den schwarz-weißen Informationen gespeichert, wobei die Strichausrichtung in zwei Dimensionen verläuft. Mit dem Standard-QR-Code können binäre, numerische und alphanumerische Zeichen dargestellt.... [IT-W2014-3]“. Ein nach den Richtlinien der VDV-Kernapplikation erzeugter Barcode enthält alle notwendigen Informationen über die Fahrtberechtigung und wird unter Verwendung der schon erwähnten SAM-Architektur erzeugt. Er gilt als gültige Berechtigung. Beispielsweise wird der 2D-Barcode als Bordkarte im Flugbereich verwendet, siehe Abbildung 4.

Abbildung 4 - Bordkarte der Lufthansa

Dargestellt wird er entweder als gedruckte Version auf einer Papierfahrkarte oder elektronisch als mobiles Ticket auf einem Handydisplay. Ein 2D-Barcode ist in beiden Fällen maschinenlesbar. Um die Informationen von einem 2D-Barcode auslesen und prüfen zu können, benötigt das Lesegerät eine Sichtverbindung zu dem dargestellten Barcode. Mit Sichtkontakt kann er eingescannt und unter Verwendung eines SAMs entschlüsselt werden. Dies kann als Nachteil betrachtet werden, da der Fahrgast den Barcode immer in der richtigen Position vor das Lesegerät halten muss. Passiert das nicht, kann der Code nicht korrekt eingelesen und verarbeitet werden. Außerdem besteht die Gefahr, gerade bei Papierfahrkarten, dass der QR-Code durch ein Knick in der Fahrkarte beschädigt wird. Das bedeutet, dass die Verwendung des 2D-Barcode beim CheckIn/CheckOut-Verfahren möglich, aber fehleranfällig und umständlich ist.

Mobiltelefone mit NFC-Chip

Ähnlich wie die kontaktlosen Chipkarten bieten auch Mobiltelefone mit einem integrierten NFC-Chip die Möglichkeit, ohne physischen Kontakt mit einem Lesegerät zu kommunizieren. NFC steht hierbei für Near Field Communication. Bei einem NFC-Chip handelt es sich ähnlich wie bei dem in den Chipkarten verwendeten RFID-Chips um „... eine drahtlose Übertragungstechnik, die zum kontaktlosen Datenaustausch zwischen Geräten mit einer Distanz von bis zu 4 Zentimeter dienen soll... [ELEK2014]“. NFC-Chips sind in vielen aktuellen Mobiltelefonen eingebaut. Zurzeit werden sie hauptsächlich zur Abwicklung von Bezahlvorgängen wie beispielsweise bei Apple Pay verwendet (vgl. [GREI2014].

Auch im öffentlichen Personenverkehr kommen NFC-Chips in Mobiltelefonen bereits zur Anwendung. „ConTags (passive NFC-Tags) sind [zum Beispiel] an allen Haltestellen im Stadtgebiet Frankfurt angebracht. [... Die Fahrgäste] finden diese entweder an den Ticketautomaten oder an den Haltestellenmasten... [RMVG2008]“. Diese enthalten Informationen über den Standort und die aktuelle Haltestelle und können von den Applikationen auf dem Mobiltelefon zur Lokalisierung des Fahrgastes verwendet werden. Einen ähnlichen Ansatz verwendet die Deutsche Bahn bei ihrem Ansatz zum mobilen Ticketing „Touch&Travel“ (vgl. [NEUH2011]).

Allgemein werden keine Informationen über Fahrberechtigungen oder Fahrkarten auf den NFC-Chip im Mobiltelefon geschrieben. Durch einen Einsatz von VDV-Kernapplikation ist es jedoch möglich elektronische Fahrscheine analog zur Fahrkartenausgabe auf eine Chipkarte auch an den NFC-Chip eines Mobiltelefons ausgegeben. Dabei kommen auch die bekannten Verschlüsselungsverfahren mit der zuvor genannten SAM-Architektur zum Einsatz. Das Auslesen im Rahmen des CheckIn/CheckOut-Verfahrens funktioniert in diesem Fall genauso wie bei kontaktlosen Chipkarten. Dazu muss das Mobiltelefon an das Lesegerät gehalten werden. Dieses führt dann die Kommunikation mit dem NFC-Chip durch und verarbeitet die ausgelesenen Daten. Grundbedingungen dafür sind, dass die Stromversorgung des NFC-Chips sichergestellt und die Batterie des Mobiltelefons entsprechend aufgeladen ist. Während in Deutschland NFC-fähige Mobiltelefone noch nicht als Chipkartenersatz verwendet werden, wird NFC im öffentlichen Personenverkehr mit der RioCard in Rio de Janeiro eingesetzt. Diese elektronische Fahrkarte kann auch auf NFC-fähigen Mobiltelefonen ausgegeben werden (vgl. [HAIK2013]).

2.4 Ein neuer Ansatz bei der Zutrittskontrolle – Bluetooth Low Energy

Mit allen zuvor genannten Nutzermedien (siehe Kapitel 2.3.2) ist es möglich, das CheckIn/CheckOut-Verfahren mit Zutrittskontrolle zu realisieren. Dabei vereinen alle Nutzermedien die Tatsache, dass der Fahrgast gezwungen ist, das Medium in kurzer Entfernung zum Lesegerät vorzuzeigen. Damit ähnelt der An-/Abmeldevorgang dem

Vorzeigen einer Papierfahrkarte bei einem Kontrolleur, was für den Fahrgast unbequem ist. Um die Kontrolle zu erleichtern und den Fahrgast zu entlasten, werden Methoden gesucht, die den Vorgang ohne das direkte Vorzeigen des Nutzermediums durchführen. Das bedeutet, dass ein kontaktloses Medium benötigt wird, bei dem die Verbindung nicht wie bei einer Chipkarte oder einem NFC-fähigem Mobiltelefon auf wenige Zentimeter begrenzt ist.

Eine Möglichkeit für ein neues, kontaktloses Nutzermedium mit größerer Reichweite bietet die Funktechnik Bluetooth Low Energy. Dabei handelt es sich um eine Erweiterung des weit verbreiteten Funkstandards Bluetooth für die Vernetzung von Geräten in einer Umgebung von ca. 10m. Bluetooth Low Energy, welches auch als Bluetooth Smart bekannt ist, arbeitet dabei stromsparender und günstiger als das normale Bluetooth.

2.4.1 Definition von Bluetooth Low Energy?

Bluetooth Low Energy ist seit 2009 optionaler Bestandteil der Bluetooth-Spezifikation in der Version 4.0. Das bedeutet, dass Geräte, welche diese Version des Standards erfüllen, nicht zwingend auch den Bluetooth Low Energy Standard unterstützen. Dennoch sind die meisten aktuellen Mobiltelefone auch Bluetooth Low Energy fähig, weshalb die Möglichkeit zur Nutzung bei einem CheckIn/CheckOut-Verfahren gegeben wäre. Bluetooth Low Energy ist für eine Entfernung von ca. 10m ausgelegt und sendet in diesem Bereich stromsparend mit 2,4 Ghz (vgl. [DEME2013]). Das stromsparende Senden der Daten verringert allerdings die Qualität des Datendurchsatzes. Während das normale Bluetooth einen Durchsatz von 2,1 Mbit/s bietet, muss Bluetooth Low Energy mit einem Durchsatz von 1 Mbit/s auskommen. Vorteilhaft ist die Optimierung der Sicherheit und Robustheit von Bluetooth Low Energy für eine direkte Verbindung zwischen zwei Geräte, und die Möglichkeit einer Broadcast-Funktionalität, mit der Verbindungen zu vielen Empfängern aufgebaut werden können (vgl. [BLUE2014]).

2.4.2 Bluetooth Low Energy in Mobiltelefonen

Bluetooth Low Energy ist in den meisten aktuellen Mobiltelefonen enthalten siehe Kapitel 2.4.1. Vor allem trifft das auf die Geräte der iPhone-Reihe von Apple und die Mobiltelefone mit dem Betriebssystem Android von Google zu. Bei Android wurde Bluetooth Low Energy im Juli 2013 mit dem Erscheinen von Android Jelly Bean (Version 4.3) eingeführt (vgl. [GOOG2014]). Apple integrierte Bluetooth Low Energy bereits in die iPhone-Version 4s, welche im Oktober 2011 angekündigt wurde (vgl. [HODG2011]). NFC hingegen ist nur auf einigen Anroid-Geräten und auf dem iPhone 6 von Apple verfügbar, in eingeschränkter Form für den Bezahldienst Apple Pay. Andere ältere Versionen des iPhones unterstützen NFC gar nicht. Daher kann man davon ausgehen, dass Bluetooth Low Energy weiter verbreitet ist als NFC.

2.4.3 Aktuelle Einsatzmöglichkeiten von Bluetooth Low Energy

Bluetooth Low Energy dient zur Verbindung von zwei Geräten in einer Master-Slave-Beziehung. Dabei dient ein Gerät als Master und das andere Gerät nimmt die Slave-Rolle ein. Diese Art der Verbindung eignet sich gut für das Auslesen oder Senden von Daten, welche vom Master-Gerät verarbeitet oder erstellt wurden. Hauptsächlich wird BLE deswegen auch beim Auslesen von verschiedenen Messdaten genutzt, beispielsweise die Verbindung zwischen einer Pulsuhr und dem dazu passsenden Brustgurt. In diesem Beispiel sammelt der Brustgurt die Daten und stellt sie als Slave bereit, während die Pulsuhr als Master auftritt und die Daten abruft.

Hingegen, ist die Funkverbindung zwischen Kopfhörer und Telefon ein Beispiel für das Senden von Daten über Bluetooth Low Energy.. Dabei ist der Kopfhörer in der Slave-Rolle und empfängt die Daten, während das Telefon als Master die Daten an den Empfänger sendet.

2.4.4 Verschiedene Betriebsmodi (Central/Peripheral)

Bei Bluetooth Low Energy wird eine Master-Slave-Verbindung zwischen Bluetooth Low Energy fähigen Geräten aufgebaut (vgl. Kapitel 2.4.3). Dabei wird die Master-Rolle als Central und die Slave-Rolle als Peripheral bezeichnet. Das bedeutet für ein BLE-fähiges Gerät, dass es entweder als Central oder als Peripheral auftreten kann.

Das Central sammelt die Daten, welche von einem Peripheral angeboten werden. Diesen Daten werden verarbeitet und genutzt, um Aufgaben durchzuführen. Die Kommunikation zwischen Central und Peripheral ist bidirektional, was bedeutet, dass das Central auch Daten an das Peripheral übermitteln. Um Peripherals zu erkennen, scannt das Central seine Umgebung. Es übernimmt den aktiven Teil der Kommunikation und ist verantwortlich für den Aufbau der Verbindung. Dadurch hat es einen höheren Energieverbrauch als das Peripheral. Um nicht unnötige Verbindungen mit fremden Peripherals aufzubauen, kann das Central das Scannen auf bekannte Services eines Peripherals einschränken. Dann erkennt es automatisch, wenn ein Peripheral einen bestimmten Service anbietet.

Das Peripheral stellt Daten bereit, welche über Services mit Characteristics bereitgestellt werden. Service bedeutet in diesem Fall eine Sammlung von Daten, die einen gemeinsamen Zwecke haben und über die Bluetooth Low Energy Schnittstelle zur Verfügung gestellt werden. Damit ist ein Service vergleichbar mit einer Webschnittstelle vergleichen, die Funktionen bereitstellt. Characteristics stellen verschiedene Daten in einem Service da, die entweder von einem Central gelesen, geschrieben oder gleichzeitig gelesen und geschrieben werden können. Ebenfalls vergleichbar stellen Characteristics die Funktionen der Webschnittstelle dar. Das Peripheral ist dafür verantwortlich, dass es auf die Anfragen des Centrals angemessen mit der Bereitstellung von Daten reagiert. Deswegen übernimmt das Peripheral den passiven Teil der Kommunikation und hat dadurch einen geringeren Energieverbrauch

als das Central.

Eine Ausnahme zu der oben vorgestellten Verbindung stellt die Broadcast-Funktion von Bluetooth Low Energy dar. Typischerweise löst das Central die Schreib- oder Lesevorgänge auf Anfrage auf dem Peripheral aus. Unter der Verwendung der Broadcast-Funktion registriert sich ein Central aktiv bei einem Peripheral, um zukünftige Benachrichtigungen über Wertänderungen zu erhalten. Das Peripheral benachrichtigt darauf aktiv alle registrierten Centrals über einen Wertwechsel (vgl. [TOWN2014] und [HEYD2012]).

2.4.5 Unterschiede zu herkömmlichen Nutzermedien

Der Hauptunterschied zwischen den bekannten Nutzermedien und einem Bluetooth Low Energy fähigem Mobiltelefon besteht in der Reichweite der Verbindung. Während bei einem 2D-Barcode die Fahrkarte direkt über das Lesegerät gehalten werden muss, ist bei der Chipkarte und dem NFC-fähigem Mobiltelefon als Nutzermedium die Reichweite auf wenige Zentimeter beschränkt. In der Praxis muss das Medium direkt über das Lesegerät platziert werden, um das Auslesen zu ermöglichen. Anders ist es bei Bluetooth Low Energy. Hier ist die Reichweite wesentlich größer, so dass das Nutzermedium nicht direkt über Lesegerät gehalten werden, sondern sich nur im Empfangsbereich befinden muss.

Für eine Verbindung über Bluetooth Low Energy muss das Telefon jedoch aktiv sein, weswegen der Stromverbrauch höher als bei der Chipkarte, dem NFC-fähigem Telefon und dem 2D-Barcode in Papierform ist. Bei einem 2D-Barcode auf einem Handydisplay ist der Verbrauch vergleichbar mit dem Einsatz von Bluetooth Low Energy.

Ein weiterer Unterschied ist der Sicherheitsaspekt. Durch die geringere Reichweite von NFC, Chipkarte und 2D-Barcode ist die Gefahr des unberechtigten Auslesens gering. Bei Bluetooth Low Energy muss aufgrund der höheren Reichweite sichergestellt werden, dass die Kommunikation zwischen Lesegerät und Medium ungestört und abhörsicher ist.

3 Analyseteil

In den folgenden Kapiteln wird der Anwendungsfall FutureGate beschrieben. Bei FutureGate handelt es sich um eine Zutrittskontrolle auf Basis von Bluetooth Low Energy. Abgeleitet von diesem Anwendungsfall werden die Anforderungen definiert, die für eine erfolgreiche Umsetzung des Anwendungsfalls notwendig sind. Diese werden anschließend bewertet. Anhand dieser Bewertung werden dann Entscheidungen bezüglich der Umsetzung des Anwendungsfalls getroffen.

3.1 Der Anwendungsfall

Ziel dieser Arbeit ist, den CheckIn-Vorgang bei einer Zutrittskontrolle im öffentlichen Personenverkehr „Hands free“ zu machen. Das bedeutet, dass sich der Fahrgast keine Gedanken über die Positionierung des Lesegerätes machen muss. Er benötigt nur sein Mobiltelefon und kann so, natürlich nur mit gültigem Fahrausweis, durch die Zutrittskontrolle gehen. Das Vorhalten oder Zeigen von Chipkarten oder von Fahrkarten wird damit abgelöst.

Wie auf Abbildung 5 zu sehen ist, begibt sich der Fahrgast in den Durchgang der Zutrittskontrolle. Dabei handelt es sich um einen schmalen Durchgang, damit die Fahrgäste einzeln durchtreten können. Das Mobiltelefon registriert das Betreten der Bluetooth Low Energy Felder der Zutrittskontrolle (die türkisen Felder in der Abbildung) und startet eine bereits im Hintergrund laufende FutureGate-Anwendung auf dem Mobiltelefon. Der Fahrgast bewegt sich nun durch den Durchgang auf die Zutrittskontrolle zu. Diese Bewegung durch die Bluetooth Low Energy Felder wird vom System registriert. Erreicht der Fahrgast die Zutrittskontrolle, wird die CheckIn-Möglichkeit auf dem Mobiltelefon freigeschaltet und der CheckIn-Vorgang kann beginnen.

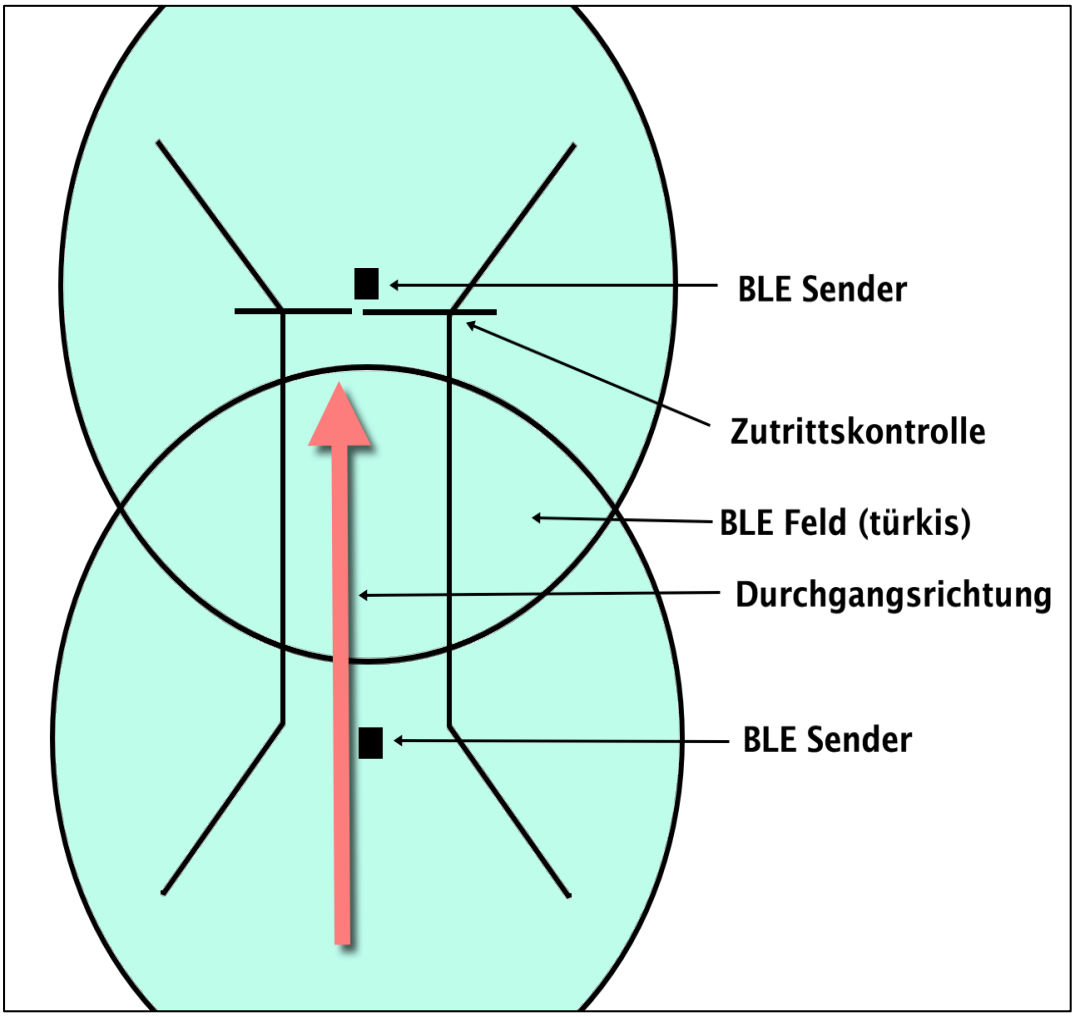

Abbildung 5 - Konzeptzeichnung FutureGate

Im Falle des erfolgreichen CheckIns checkt der Fahrgast ein und wird durch das Hintergrundsystem registriert. Hier wird eine gegenseitige Authentifizierung durchgeführt, um sicherzustellen, dass es sich um berechtigte Kommunikationsteilnehmer handelt. Am Ende wird dem Fahrgast durch ein akustisches oder optisches Signal deutlich gemacht, dass der CheckIn-Vorgang erfolgreich. Er kann die Zutrittskontrolle passieren.

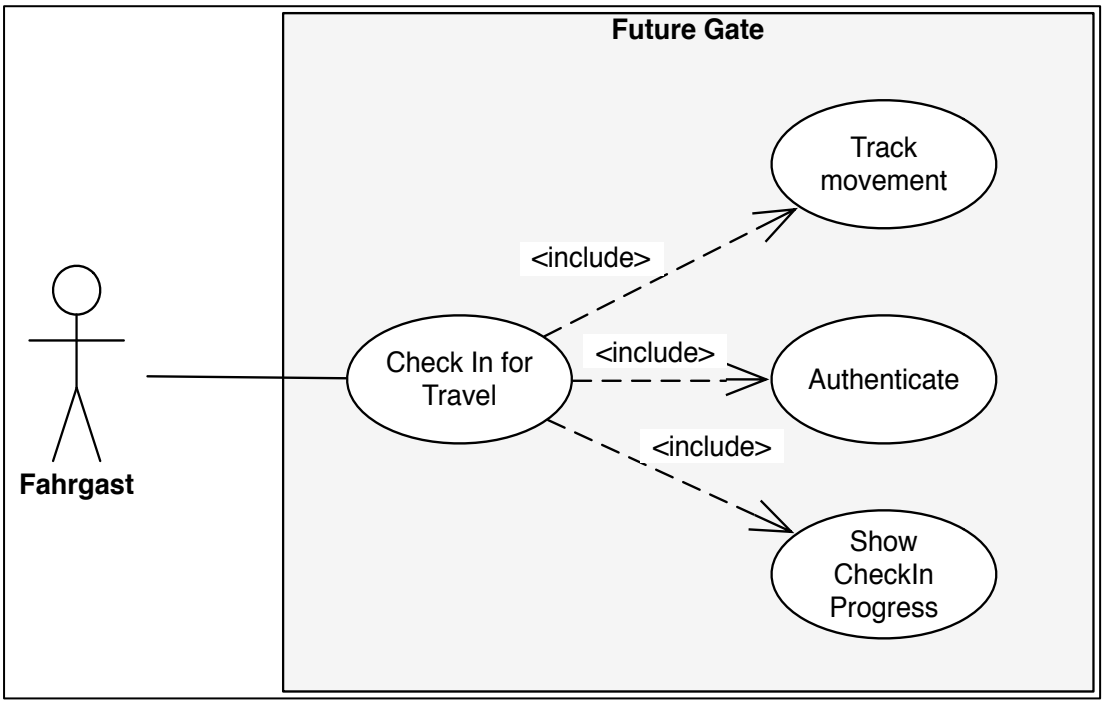

Abbildung 6 - UseCase Diagramm FutureGate

Verläuft der CheckIn-Vorgang negativ, kann sich der Fahrgast nicht einchecken. Dafür kann es mehrere Gründe haben. Zum einen ist er nicht berechtigt, den Vorgang durchzuführen. Zum anderen kann es technische Gründe handeln. Die Authentifizierung zwischen Mobiltelefon und Lesegerät schlägt fehl oder das Mobiltelefon des Fahrgastes steht auf der Sperrliste. Dann erkennt das Hintergrundsystem, dass hier ein unberechtigter Versuch vorliegt. Durch ein akustisches oder ein optisches Signal wird dem Fahrgast deutlich gemacht, dass der CheckIn entweder nicht erfolgreich war oder nicht stattgefunden hat.

Aus diesem Anwendungsfall gehen 4 Teilfälle hervor (vgl. Abbildung 6). Der umfassende Anwendungsfall ist der eigentliche CheckIn-Vorgang. Das entspricht dem Ziel des Fahrgastes. Der CheckIn-Vorgang besteht aus mehreren Unteranwendungsfällen. Erstens wird die Bewegung des Fahrgastes durch das Gate registriert und bewertet. Hat er den CheckIn-Bereich erreicht, wird der CheckIn zweitens freigeschaltet und der Fahrgast bestätigt den Vorgang. Drittens findet die Authentifizierung statt. Viertens wird das Ergebnis des CheckIn-Vorgangs für den Nutzer dargestellt.

3.2 Anforderungsanalyse

Im Folgenden werden die Anforderungen aus dem Anwendungsfall abgeleitet und tabellarisch dargestellt. Diese Anforderungen lassen sich in obligatorische und optionale Punkte unterteilen. Obligatorische Punkte sind zwingend für die Umsetzung, weil diese Punkte für den erfolgreichen CheckIn notwendig sind. Optionale Punkte unterstützen den Vorgang. Zusätzlich werden sie in funktionale, sicherheitsbezogene, nutzbarkeitsbetreffende und nichtfunktionale Anforderungen unterteilt. Funktionale Anforderungen sind für die Durchführung des Anwendungsfalls notwendig. Sicherheitsbezogene Anforderungen beziehen sich auf die gesicherte Durchführung des Anwendungsfalls und garantieren die Sicherheit der Kommunikation zwischen Mobiltelefon und Lesegerät während des Anwendungsfalls. Die nutzbarkeitsbetreffenden Anforderungen stellen ein bequemes Nutzungserlebnis des Gesamtsystems für den Fahrgast sicher. Die nichtfunktionalen Aspekte beziehen sich auf die Durchführungsgeschwindigkeit des CheckIns.

Alle Anforderungen sind in Tabelle 1 dargestellt. Die erste Spalte enthält eine kurze Erklärung der Anforderung. In der zweiten Spalte kann man erkennen, ob es sich bei der Anforderung um eine obligatorische (z) oder um eine optionale (o) Anforderung handelt.

Anforderung	Voraussetzung
Funktional	
• Es findet ein CheckIn-Vorgang am FutureGate statt.	z
• Ergebnis des CheckIn-Vorgangs wird optisch oder akustisch dargestellt.	z
• Gate und Mobiltelefon „erkennen“ sich gegenseitig und können miteinander kommunizieren.	z
• Die Position des Fahrgastes muss bestimmbar sein.	z
• Die Bewegungsrichtung des Fahrgastes muss vom System ermittelbar sein.	o
• Es muss das korrekte Gate durch das Mobiltelefon identifiziert werden.	z
• Gate und Mobiltelefon müssen die Kommunikation und die Authentifizierung ohne Abfrage im Internet autark durchführen	o
Sicherheit der Kommunikation	
• Es findet eine Authentifizierung zwischen Gate und Mobiltelefon statt, bei der festgestellt wird, ob die Partner berechtigt sind, miteinander zu kommunizieren.	z

• Die Verschlüsselung muss durch die an der Kommunikation beteiligten Partner eigenständig geschehen.	o
• Kommunikation kann nicht abgehört oder von Dritten nachvollzogen werden.	z
Nutzbarkeitsbetreffend	
• Das Programm auf dem Mobiltelefon soll automatisch gestartet werden.	o
• Es findet eine automatische Kommunikation zwischen dem Gate und dem Mobiltelefon statt.	o
Nicht-Funktional	
• Die Kommunikation zwischen dem Gate und dem Mobiltelefon muss ausreichend schnell stattfinden.	o
• Der Akku des Mobiltelefons soll möglichst gering belastet werden.	z
• Ist eine Kommunikation beendet, kann sie von den Partnern wiederholt werden.	o
• Eine stabile Kommunikation zwischen Gate und Mobiltelefon muss sichergestellt werde.	o

Tabelle 1 - Allgemeine Anforderungen

Neben den Anforderungen an die Gesamtlösung wurden außerdem noch Anforderungen aufgenommen, die eine Authentifizierung zwischen Mobiltelefon und Lesegerät betreffen. Diese werden in **Tabelle 2** dargestellt. Auch hier wird zwischen obligatorischen und optionalen Anforderungen unterschieden.

Anforderung	Voraussetzung
• Das Gate muss erkennen, dass das Mobiltelefon berechtigt ist, den CheckIn Vorgang durchzuführen.	z
• Die Authentifizierung darf erst beginnen, wenn sich Mobiltelefon in unmittelbarer Nähe zum Gate befindet.	z
• Das Mobiltelefon muss erkennen, dass das Gate als solches berechtigt ist, den Check In einzuleiten und durchzuführen.	z
◦ Es muss erkennbar sein, dass es sich um ein Gate handelt.	o
◦ Es muss erkennbar sein, dass die Richtung des Durchlaufens korrekt ist.	o

• Die Authentifizierung muss schnell durchgeführt werden.	z
• Die Authentifizierung muss abhörsicher sein.	z
• Die Authentifizierung darf nicht von Dritten wiederholbar sein.	z
• Die Authentifizierung darf nicht von Dritten „simuliert“ werden, um einen Partner zu täuschen.	z

Tabelle 2 - Anforderungen an die Authentifizierung

3.3 Möglichkeiten der Umsetzung

Aus den Anforderungen wird deutlich, dass die wichtigsten Entscheidungen in der Positionierung der Bluetooth Low Energy Sender, der Verteilung der Bluetooth Low Energy Centrals/Peripherals und in der Art der Authentifizierung liegen. In den folgenden Kapiteln werden die verschiedenen Möglichkeiten zur Umsetzung und die dazugehörigen Anforderungen gegenüber gestellt.

3.3.1 Positionierung der Bluetooth Low Energy Sender

Die Positionierung der Bluetooth Low Energy Sender ist entscheidend, um die Bewegungsrichtung und die Position des Fahrgastes zu bestimmen. Für beide Bestimmungen benötigt man zwei Bluetooth Low Energy Sender. Mit nur einem Sender könnte man nur die Entfernung zum Sender berechnen. Zwei Sender können entweder parallel oder hintereinander entsprechend zur zu Laufrichtung des Fahrgastes positioniert werden, siehe Abbildung 7. Der Abstand muss in beiden Fällen so gewählt werden, dass sich die Bluetooth Low Energy Felder beider Sender überschneiden. So hat man die Möglichkeit, die Position des Fahrgastes zu bestimmen.

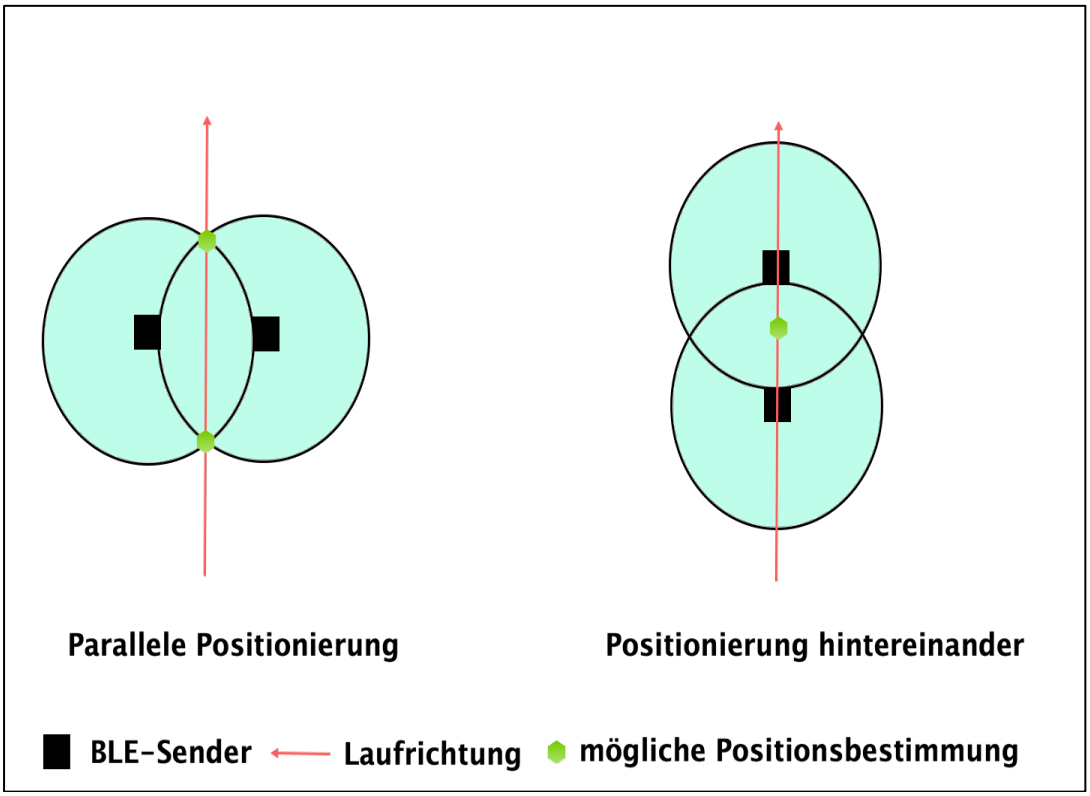

Abbildung 7 - Skizze zur Positionierung der Sender

Bei der parallelen Aufstellung der Sender ist es möglich, die Position auf 2 Möglichkeiten einzugrenzen. Dazu werden die Feldstärkemessungen der beiden Sender ins Verhältnis gesetzt. In Abbildung 7 ist ersichtlich, dass das dann auf zwei Positionen in Laufrichtung vor oder hinter den Sendern zutrifft. Deswegen muss die Laufrichtung mit in Betracht gezogen werden, welche bei einer Positionierung der Sender „in Reihe“ automatisch mit der Laufrichtung bestimmen werden kann. Hier kann man dann durch die Veränderung der Feldstärkung bestimmen, an welcher genauen Position sich der Fahrgast in diesem Moment befindet.

3.3.2 Verteilung der Bluetooth Low Energy Centrals/Peripherals

Die Wahl der Verteilung von Central und Peripheral hängt mit dem Stromverbrauch und dem Datenfluss zwischen Central und Peripheral zusammen. Allgemein ist es so, dass die Central-Komponente mehr Strom als die Peripheral-Komponente benötigt. In diesem Szenario werden die Daten vom Peripheral angeboten und vom Central verarbeitet.

Wenn nur den Stromverbrauch betrachtet wird, sollte dass das stationäre Lesegerät als Central operieren. Das Bluetooth Low Energy fähige Mobiltelefon kann Strom sparen, in dem es als Peripheral operiert. Allerdings würde das eine ständige Verfügbarkeit des

Mobiltelefons notwendig machen, da man nicht genau weiß, wann das Scannen durchgeführt wird. Wenn das Mobiltelefon als Central operiert, kann das Scannen erst erfolgen, wenn das Telefon in die Nähe eines Lesegerätes kommt, welches dann als Peripheral fungiert.

Die Richtung des Datenflusses bestimmt, von welcher Komponente die Interaktion zwischen Lesegerät und Mobiltelefon ausgeht. Das Central initiiert dabei den Kommunikationsbeginn und entscheidet somit über den Versuch, einen CheckIn-Vorgang durchzuführen. Diese Entscheidung sollte prinzipiell in den Händen des Fahrgastes liegen, welcher das Mobiltelefon bedient.

3.3.3 Authentifizierung

Um die Sicherheit der Kommunikation zwischen Central und Peripheral zu gewährlisten, muss eine Authentifizierung stattfinden. Dazu stehen drei Methoden zur Diskussion. Das erste Verfahren ist das Challenge Response Verfahren. Dabei stellt ein Teilnehmer dem Gegenüber eine Aufgabe durch das Senden einer Zufallszahl. Der zweite Teilnehmer muss diese Aufgabe lösen und die Antwort an den Sender zurückschicken. Bei einer korrekten Antwort gelten die Teilnehmer als authentifiziert. Beispielsweise kann der Empfänger ein Passwort an die Zufallszahl und unter der Nutzung einer bestimmten Hashfunktion kodieren. Zum Überprüfen der Antwort verwendet der Sender die gleiche Hashfunktion und vergleicht anschließend das angehängte Passwort mit seinem eigenen. Dabei ist es notwendig, dass Passwort und Hashfunktion bei beiden Teilnehmern bekannt sind. Die Sicherheit ist durch die Verwendung eines Zufallselements und durch dem unberechtigten Nutzer unbekannten Faktoren, wie der Hashfunktion und dem Passwort, sichergestellt (vgl. [IT-W2014]).

Die zweite Möglichkeit ist die Verwendung von Nutzernamen und Passwort. Dieses Verfahren ist auch als Basic Authentication bekannt. Hierbei kommt es zur Übertragung von Nutzername und Passwort zwischen den Kommunikationsteilnehmern. Dabei kann das Passwort zwar codiert, aber nicht verschlüsselt sein. Aus diesem Grund ist die Kommunikation nicht abhörsicher (vgl. [LEAC1999].

Die dritte Möglichkeit ist eine Lösung über Client-Server-Zertifikate. Dafür besitzen beide Kommunikationspartner Zertifikate, mit denen sie sich vor der eigentlichen Kommunikation ausweisen müssen. „Ein digitales Zertifikat ist eine durch eine vertrauenswürdige Instanz digital signierte Beglaubigung von sicherheitskritischen Informationen.... [NOCH2014]“. Diese Zertifikate sind auf Mobiltelefon und Lesegerät gespeichert. Dabei gibt es zwei Möglichkeiten, Zertifikate zu erzeugen. Erstens, Zertifikaten können von jedem Kommunikationspartner selbst erstellt werden. Sie stellen aber keine hohe Sicherheit dar, da sie nicht von unabhängiger Stelle abgenommen werden. Dies ist in der zweiten Variante der Fall. Hier wird das Zertifikat von einem unabhängigen Aussteller wie zum Beispiel Thawte erzeugt. Diese werden dann entsprechend akzeptiert. Diese werden dann entsprechend eines bestimmten

Entgelts, abhängig von der Authentifizierungsstelle, ausgestellt.

3.4 Gewählte Umsetzungen in dieser Arbeit

In dieser Arbeit wird die Positionierung der Bluetooth Low Energy Sender so gewählt, dass die Sender hintereinander in Laufrichtung platziert werden. Dadurch wird nicht nur die Anforderung der Positionsbestimmung erfüllt, sondern es wird möglich, die Laufrichtung des Fahrgastes zu erkennen. Das kann mit einer Platzierung der Sender parallel zur Laufrichtung des Kunden aus den oben genannten Gründen (siehe Kapitel 3.3.1) nicht erreicht werden.

Bezüglich der Verteilung der Central- und Peripheral-Rolle soll das Mobiltelefon als Central agieren. Dementsprechend wird die Rolle des Peripherals vom Lesegerät ausgefüllt. Obwohl damit der höhere Stromverbrauch vom Mobiltelefon geleistet werden muss, überwiegen die Vorteile dieser Variante.. So ist der aktive Part der Kommunikation auch tatsächlich in der Hand des Fahrgastes. Weiterhin muss das Lesegerät nicht durchgängig nach in der Umgebung potentiell anwesenden Mobiltelefonen scannen. Das Lesegerät stellt nur die Funktionen zur Verfügung, welche für den CheckIn notwendig sind und reagiert auf die Statuswechsel im Verlauf eines Vorgangs. Die eigentliche Rechenleistung wird vom Mobiltelefon übernommen, wozu die aktuellen Gerät im Stande sind.

Eine weitere Dimension stellt die Verarbeitungsgeschwindigkeit dar. Tests bei der Entwicklung haben ergeben, dass bei einem Einsatz des Lesegeräts als Central die Dauer eines CheckIn-Vorgangs ca. 1000 Millisekunden beträgt. Stellt das Gate das Peripheral dar, beträgt der CheckIn-Vorgang nur ca. 500 Millisekunden. Der Zeitunterschied entsteht durch den abweichenden Verbindungsaufbau zwischen Central und dem Peripheral. Dieser wird immer vom Central initiiert. Stellt das Mobiltelefon das Central dar, so kann die Verbindung schon beim Erreichen des CheckIn-Bereiches aufgebaut werden. Somit ist sie vor der eigentlichen Anmeldung schon verfügbar. Ist das Gate das Central, so kann die Verbindung hingegen erst aufgebaut werden, wenn sich der Fahrgast tatsächlich zum CheckIn entschließt, weil das Peripheral erst dann freigegeben ist.

Zur Authentifizierung stellt der Einsatz von einem Zertifikat die beste Lösung dar. Allerdings würden hier Kosten aufgrund des Einkaufes der Zertifikate anfallen. Aus diesem Grund verwendet die vorliegende Arbeit das Challenge-Response-Verfahren. Es lässt sich auf beiden Geräte (Lesegerät und Mobiltelefon) gut umsetzen.

3.5 Auswahl der eingesetzten Technologien

Bei der Wahl der Technologien muss auf die Gegebenheiten der Umgebung und des Anwendungsfalls geachtet werden. Dabei werden Technologien sowohl für das als Nutzermedium genutzte Mobiltelefon als auch für das Lesegerät gesucht.

3.5.1 Umsetzung auf dem Mobiltelefon

Bei der Umsetzung auf dem Mobiltelefon kommen drei Plattformen in Frage, die mit Bluetooth Low Energy umgehen können. Zum einen wären es die Geräte mit dem Betriebssystem Android. Diese Telefone bieten ab API Level 18 (Version 4.3) die Möglichkeit, Bluetooth Low Energy als Central zu nutzen. Die verwendete Programmiersprache ist bei Android Java.

Die zweite Plattform stellen die Telefone mit dem Betriebssystem iOS von Apple dar. Hier ist es seit Betriebssystemversion 5 möglich, das Mobiltelefon mit Bluetooth Low Energy als Central oder als Peripheral zu nutzen. Die verwendete Programmiersprache bei den iOS-Geräten ist ObjectiveC.

Die dritte Möglichkeit ist die Umsetzung auf einem Gerät mit dem Betriebssystem Windows Phone von Microsoft. Hier hat der Hersteller die BLE-Funktionen mit der Version 8 aktiviert. Als Programmiersprache wird auf den Windows Phone Geräten C# eingesetzt.

Von allen drei Geräten sind die Android-Geräte am weitesten verbreitet. Außerdem wird hier die Programmiersprache Java verwendet. Das ermöglicht die Nutzung verschiedener Entwicklungsumgebungen auf verschiedenen Systemen (z.B. Linux, Windows, MacOS). Die anderen beiden Plattformen sind jeweils auf ein System beschränkt. Bei Windows Phone und C# ist es Visual Studio auf einem Windows-System. Bei iOS und ObjectiveC wird zwingend xCode und MacOS vorausgesetzt. Um diese Einschränkungen zu umgehen, erfolgt in dieser Arbeit die Umsetzung mit einem Android-Gerät.

3.5.2 Umsetzung für das Lesegerät

Während bei den Mobiltelefonen die integrierten Bluetooth Low Energy Chipsätze verwendet werden können, sind in den meisten Systemen (zum Beispiel Computer) keine derartigen Adapter integriert. Aus diesem Grund sollen für das Lesegerät Bluetooth Low Energy USB-Adapter verwendet werden, mit denen ein Rechner um die Bluetooth Low Energy Funktionalität erweitert wird. Um diese Erweiterung nutzen zu können, wird ein Framework benötigt, mit der die Adapter angesprochen werden, beispielsweise mit Bleno (vgl [MIST2014]). Bleno ist ein Plugin für die JavaScript-Umgebung NodeJS, welche auf der JavaScript-Implementierung des Webbrowsers Chrome von Google basiert. Die Nutzung dieses Plugins setzt die Programmiersprache JavaScript voraus. Um außerdem bestimmte Funktionen dieses Plugins nutzen zu können, ist das Betriebssystem Linux notwendig.

Somit erfolgt die Umsetzung für das Lesegerät auf einem Rechner mit dem Betriebssystem. Dort kommt dann die JavaScript-Umgebung NodeJS und das Plugin Bleno zum Einsatz. Als Programmiersprache ist dementsprechend JavaScript vorgesehen.

4 Syntheseteil

4.1 Komponentenbeschreibung

Das FutureGate-System besteht aus insgesamt drei unterschiedlichen Komponenten. Die erste Komponente ist die Android-Applikation, welche das Nutzermedium des Fahrgastes darstellt. Auf der Seite des Lesegerätes befinden sich zwei Komponenten. Dabei dient die Marker-Komponente als Bezugspunkt für die Standortlokalisierung. Die Gate-Komponente übernimmt die Authentifizierung und den CheckIn-Vorgang. Außerdem visualisiert sie das Ergebnis.

Die Android-Applikation FutureGate ist in der Programmiersprache Java geschrieben und nutzt die Laufzeitumgebung im Android-Betriebssystem. Der API-Level in der Version 18 wird vorausgesetzt. Die Applikation besteht aus 4 Komponenten (vgl. Abbildung 8). Die Hauptkomponente stellt dabei die Klasse namens ‚MainActivity' dar. Sie vereint sowohl den Controller für die grafische Anzeige als auch für die Bluetooth-Funktionalitäten. Diese sind in einer eigenen Komponente ‚BLE-Framework' gekapselt, welche in der ‚MainActivity'-Komponente inkludiert ist. Diese Komponente übernimmt die Implementierung der Bluetooth Low Energy-Protokolle, die von der Android-Laufzeitumgebung zur Verfügung gestellt werden. Aus diesem Grund übernimmt die Bluetooth-Komponente auch die Kommunikation mit der Schnittstelle der FutureGate-Komponente. Wie die Kommunikation abläuft, wird von der ‚StateMachine'-Komponente bestimmt. Diese Komponente hält den aktuellen Status der Applikation. Dadurch ist hier auch der Fortschritt des CheckIn-Vorgangs abgelegt. Außer diesen Komponenten enthält die Android-Applikation noch eine Utility-Komponente. Diese enthält Funktionen zur Erzeugung von Hashwerten oder neuen Tokens beziehungsweise Zufallszahlen.

Während die Android-Applikation in einer Java-Laufzeitumgebung läuft, benötigen die Komponenten des FutureGates eine JavaScript-Laufzeitumgebung. Deswegen kommt hier NodeJS zum Einsatz(siehe Kapitel 3.5.2). Zum einen wird diese durch die Marker-Komponente genutzt. Die Marker-Komponente bietet einen Bluetooth-Service an, wofür sie das Bleno-Framework nutzt und damit die Verbindung zur Bluetooth-Hardware herstellt. Über diese wird die Bluetooth Low Energy Schnittstelle zur Verfügung gestellt, welche von der Android-Applikation zur Berechnung der Position genutzt wird. Zum anderen nutzt die Gate-Komponente ebenfalls die NodeJS-JavaScript-Laufzeitumgebung und das Bleno-Framework für die Bluetooth-Anbindung. Die Gate-Komponente Komponente besteht dabei aus 3 Komponenten (siehe Abbildung 8). Der GateService stellt dabei die Bluetooth-Schnittstelle für die Authentifizierung

und den CheckIn bereit. Dafür ist ein Service definiert, welche jeweils eine Characteristic für die Authentifizierung und den CheckIn anbietet. Der Zustandsübergangsautomat der Android-Applikation entscheidet dann, in welcher Reihenfolge diese Schnittstelle aufgerufen wird (siehe Kapitel 4.2). Ein weiterer Bestandteil der Gate-Komponente ist die ‚GUI'-Komponente. Diese empfängt Nachrichten, welche von der GateService-Komponente über das Socket.IO-Framework versendet werden. Die ‚GUI'-Komponente dient zur Visualisierung des CheckIn-Fortschrittes. Außerdem enthält die Gate-Komponente noch eine Utility-Komponente für unterstützende Prozesse wie zum Beispiel das Erzeugen von Hashwerten.

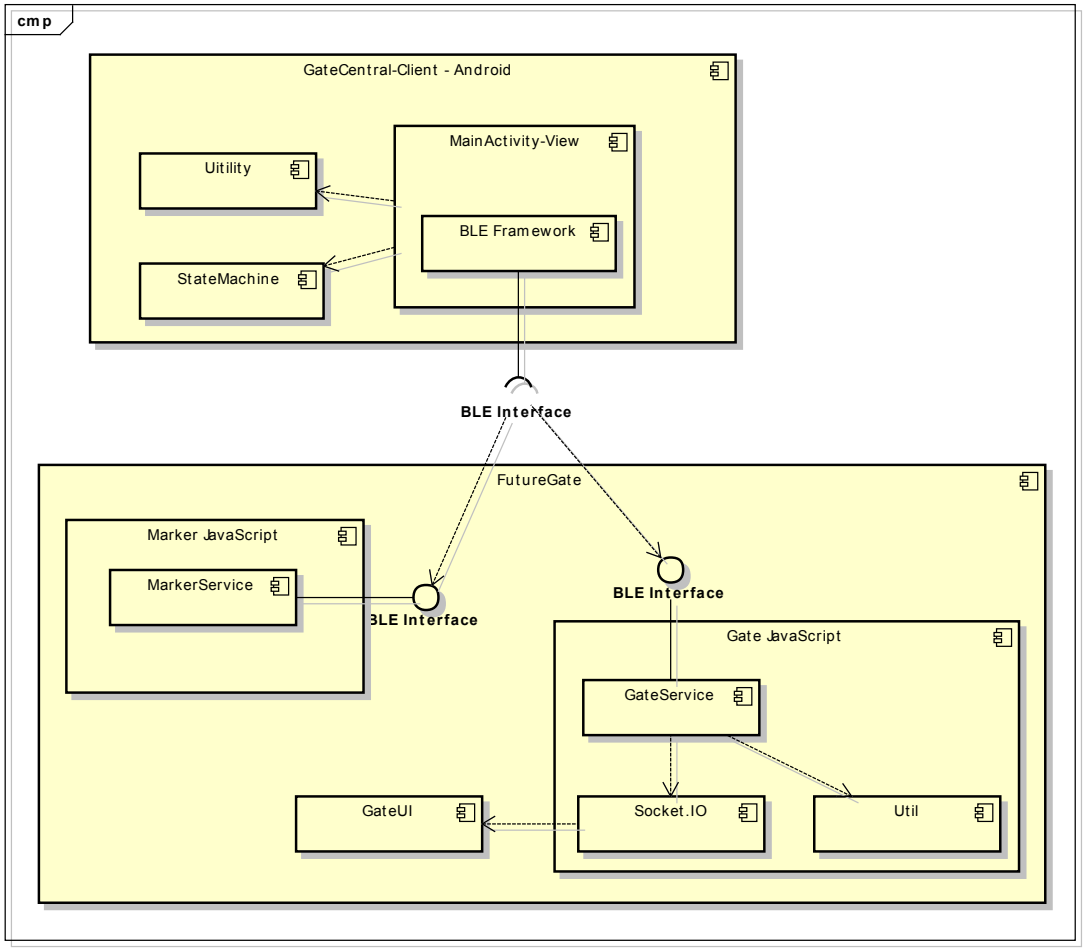

Abbildung 8 - Komponentendiagramm FutureGate

4.2 Zustände der FutureGate-Applikation

Die Android-Applikation bildet den aktuellen Zustand des CheckIn-Vorgangs mit einem Zustandsübergangsautomat ab, welche fest definierte Zustände und Übergänge

zwischen den Zuständen nutzt, siehe Abbildung 9). Der Automat hat einen Endzustand mit der Bezeichnung ‚CheckIn done'. Dieser Zustand wird bei einem erfolgreichen Durchlaufen der Zustände erreicht. Dieses Durchlaufen ist Voraussetzung für einen erfolgreichen CheckIn-Vorgang. Ein weiterer Endzustand ist der Zustand ‚Failure'. Dieser Zustand ist der Fehlerzustand der Zustandsübergangmaschine. Schlägt ein Teil des CheckIn-Vorgangs jedoch fehl, wechselt die Applikation in den Zustand ‚Failure', dem Fehlerzustand des Zustandsübergangsautomat.

Sobald sich die Applikation mit der Bluetooth Low Energy Schnittstelle des Gates verbunden hat, startet der Zustandsübergangsautomat im Zustand ‚New'. In diesem Zustand werden die Authentifizierungsparameter an das Gate gesendet. Ist die Übertragung abgeschlossen, wechselt der Zustandsübergangsautomat in den Zustand ‚Perform Auth'. In diesem Zustand erwartet die Applikation eine Rückmeldung auf die eigene Authentifizierung. Diese wird durch einen Lesezugriff auf die Schnittstelle des Gates abgerufen. Bei einer positiven Rückmeldung und gleichzeitiger erfolgreicher Authentifizierung seitens des Gates wechselt der Zustandsübergangsautomat in den Zustand ‚Auth Complete'. Schlägt eine der beiden Authentifizierungen fehl, so findet hingegen ein Wechsel in den Zustand ‚Failure' statt. Der CheckIn-Vorgang ist dann fehlgeschlagen.

Im Zustand ‚Auth Complete' beginnt die Applikation mit der Übertragung der CheckIn-Informationen. Diese werden mittels eines Schreibezugriffes auf die Bluetooth-Schnittstelle an das Gate gesendet. Anschließend findet ein Zustandsübergang in den Zustand ‚Perform CheckIn' statt. Hier wird auf das Ergebnis des CheckIn-Vorgangs gewartet. Dieses fragt die Applikation mittels eines Lesezugriffes von der Gateschnittstelle ab. Ist das Ergebnis positiv, so wechselt die Applikation in den Zustand ‚CheckIn Done'. Der CheckIn-Vorgang ist erfolgreich dadurch abgeschlossen. Scheitert der CheckIn-Vorgang jedoch, so wechselt die Applikation auch hier in den Zustand ‚Failure'. Der CheckIn-Vorgang ist somit fehlgeschlagen.

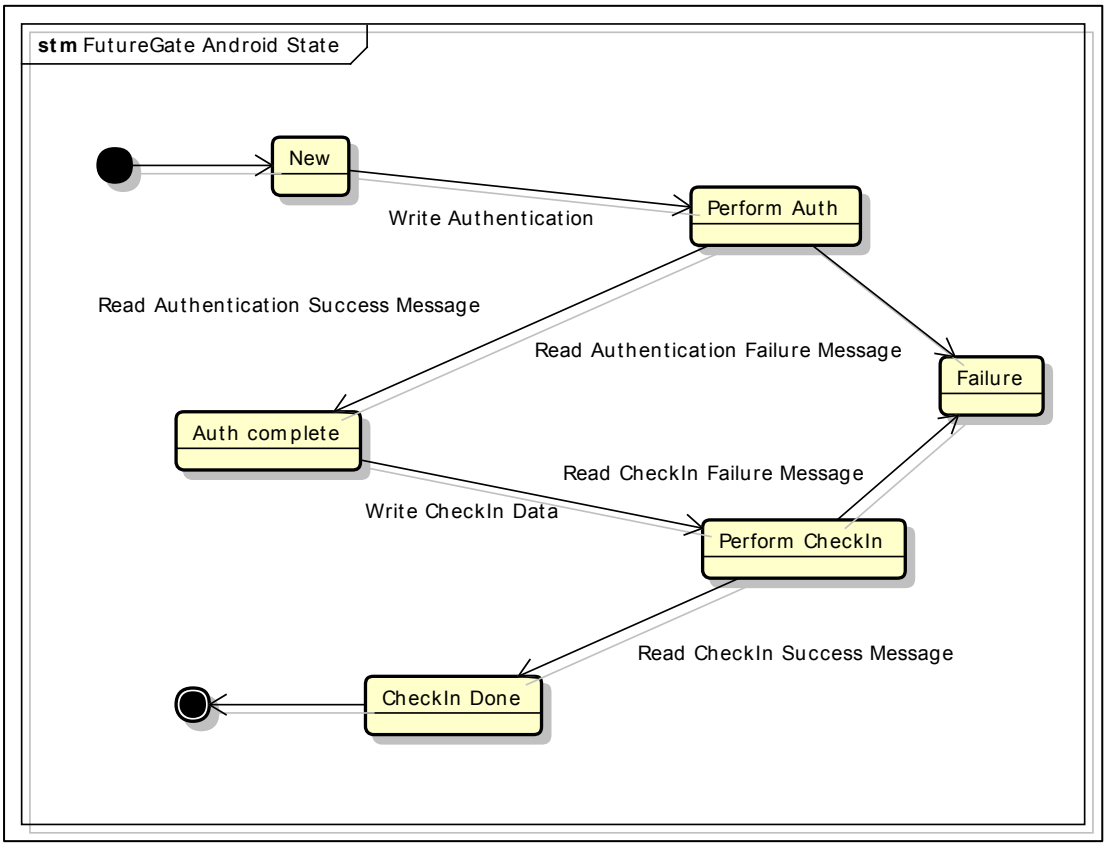

Abbildung 9 - Zustandsübergänge der Android-Applikation

4.3 Schnittstelle zwischen Gate und Mobiltelefon

Das FutureGate stellt bei einem CheckIn-Vorgang die Kommunikation zwischen dem Mobiltelefon als Nutzermedium und dem Gate als Lesegerät her. Diese Kommunikation findet über eine Bluetooth Low Energy Schnittstelle statt. Sie besteht aus einem Bluetooth Low Energy Service, welcher die Characteristics zur Verfügung stellt. Sowohl Service als auch die Characteristics sind über Universally Unique Identifiers (UUIDs) eindeutig identifizierbar. Der Applikation auf dem Mobiltelefon sind diese UUIDs bekannt. Die in dieser Arbeit verwendeten UUIDs sind im Rahmen der Arbeit erzeugt worden.

Die Bluetooth Low Energy Schnittstelle basiert auf der GATT-Spezifikation (vgl. [TOWN2014]). In ihr werden Services als Sammlung von Characteristics beschrieben. Der Service hat die Bezeichnung ‚GateDevice' und kann unter der UUID ‚fbc5eb86-0b74-40a9-a8bd-7553a65af1ef' erreicht werden (siehe Abbildung 10). Er bietet die Characteristics ‚authCharacteristic' und ‚tokenCharacteristic' an. Diese beiden Characteristics stellen die Funktionalität für den Service bereit und werden in den folgenden Abschnitten näher erläutert.

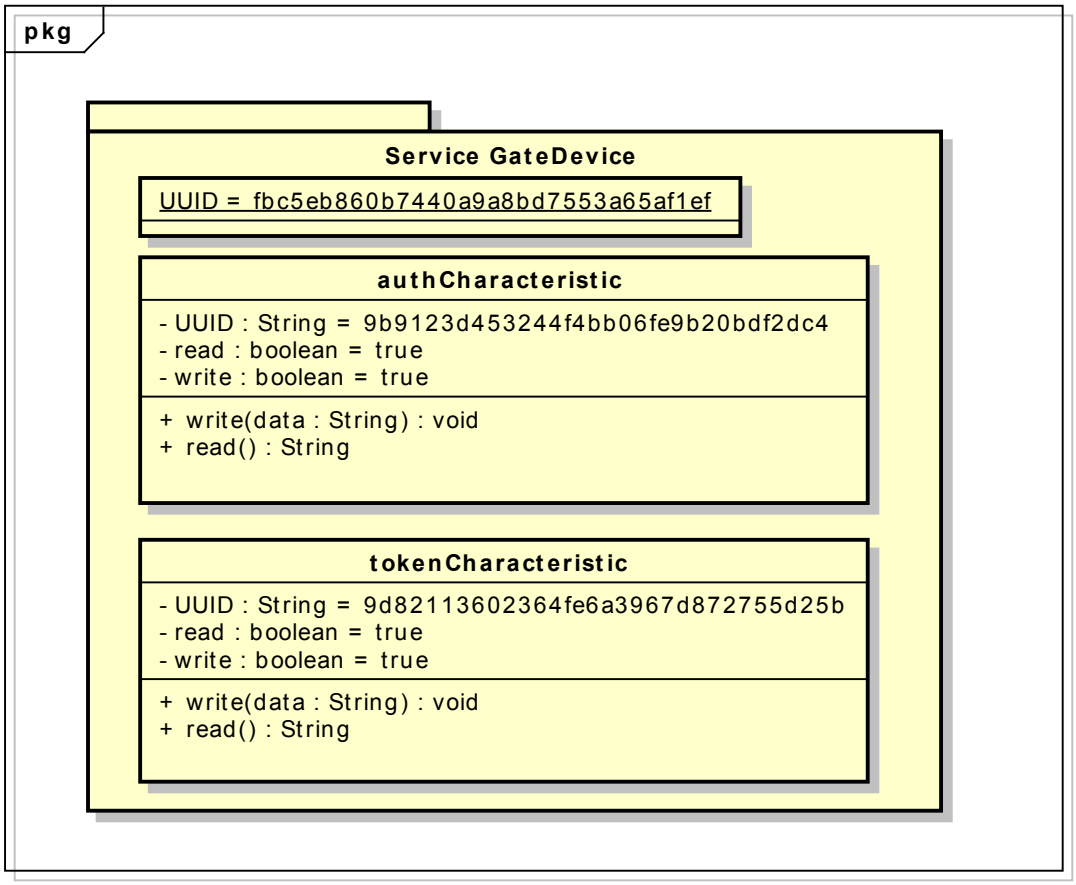

Abbildung 10 - Schnittstelle Gate – Mobiltelefon

Bei der Characteristic ‚authCharacteristic' handelt es sich um die Funktion, welche die Authentifizierung zwischen Gate und Mobiltelefon vornimmt. Sie kann über die UUID ‚9b9123d4-5324-4f4b-b06f-e9b20bdf2dc4' angesprochen werden. Diese Characteristic kann sowohl geschrieben als auch gelesen werden. Dementsprechend enthält sie eine Lese-und eine Schreibfunktion. Die Characteristic ist dabei nicht zustandsfrei. Sie muss zuerst geschrieben werden, bevor die Authentifizierungsergebnisse ausgelesen werden können. Im Anwendungsfall bedeutet das, dass die aufrufende Applikation zuerst die Authentifizierungsdaten in die Schnittstellenfunktion schreibt. Nun wird überprüft, ob die aufrufende Applikation berechtigt ist, die Schnittstelle zu nutzen. Anschließend werden in der Lesefunktion das Ergebnis und bei positiver Authentifizierung die Authentifizierungsdaten des Gates zur Verfügung gestellt, welche von der Applikation nun eingelesen werden können.

Analog ist die Characteristic ‚tokenCharacteristic' umgesetzt. Sie kann unter der UUID ‚9d821136-0236-4fe6-a396-7d872755d25b' angesprochen werden. Sie stellt ebenfalls

eine Lese- sowie Schreibfunktion zur Verfügung. Außerdem ist diese Characteristic auch nicht zustandslos. Im Anwendungsfall schreibt die aufrufende Applikation nach erfolgreicher Authentifizierung den Zugangstoken in die Lesefunktion der Characteristic. Anschließend bearbeitet das Gate die übergebenen Daten und stellt fest, ob das Token für den CheckIn des Fahrgastes berechtigt ist. Das Ergebnis wird dann in der Schreibfunktion der Characteristic veröffentlich, wo es von der aufrufenden Applikation abgerufen werden kann.

4.4 Ablauf des Anwendungsfall

Der Ablauf des Anwendungsfalls wird durch zwei Anwendungsdiagramme in Abbildung 11 und in Abbildung 12 verdeutlicht. Abbildung 11 zeigt den Ablauf vor dem Aktivieren des CheckIns, während Abbildung 12 schließlich den eigentlichen CheckIn-Vorgang zeigt. Dabei wird von einem positiven Durchlauf des Anwendungsfalls ausgegangen.

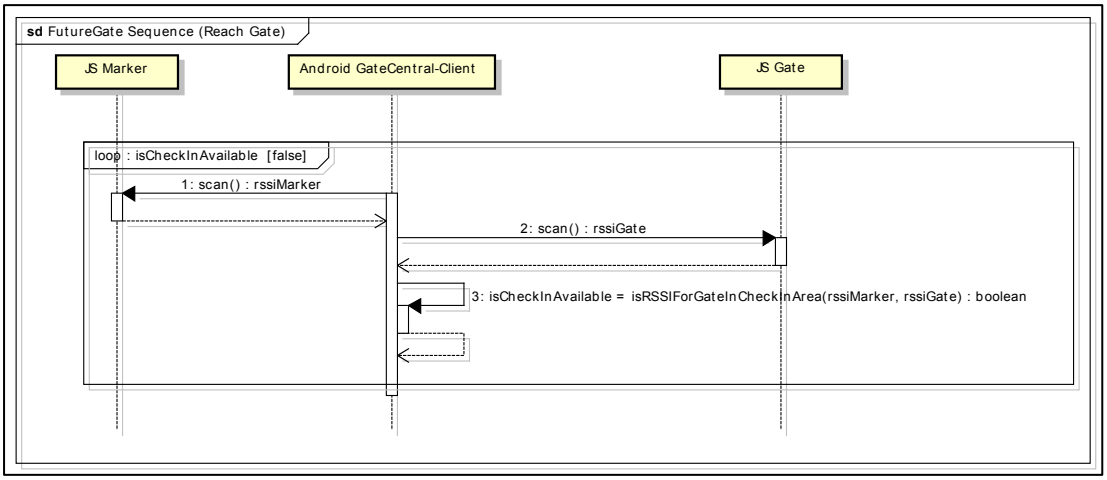

Abbildung 11 - Ablaufdiagramm ‚Erreichen des Gates'

Bevor der CheckIn an einem Gate möglich ist, muss der Fahrgast eine bestimmte Position direkt vor dem Gate einnehmen. Um zu erkennen, ob sich das Mobiltelefon schon dort befindet, beginnt das Telefon mit dem Start der FutureGate-App zu scannen, ob sich die beiden Bluetooth Low Energy Peripherals Gate und Marker im Bereich des Telefons befinden. Wird einer dieser Sender gefunden, so beginnt das Mobiltelefon, die RSSI-Werte der gefundenen Sender zu erfassen und zu speichern. Bei dem RSSI-Wert (Received Signal Strength Indication) handelt es sich um einen Indikator für die Feldstärke des Bluetooth Low Energy Feldes. Anschließend wird berechnet, ob der CheckIn-Bereich des Gates erreicht wurde. Solange das nicht der Fall ist, wird das Scannen fortgesetzt.

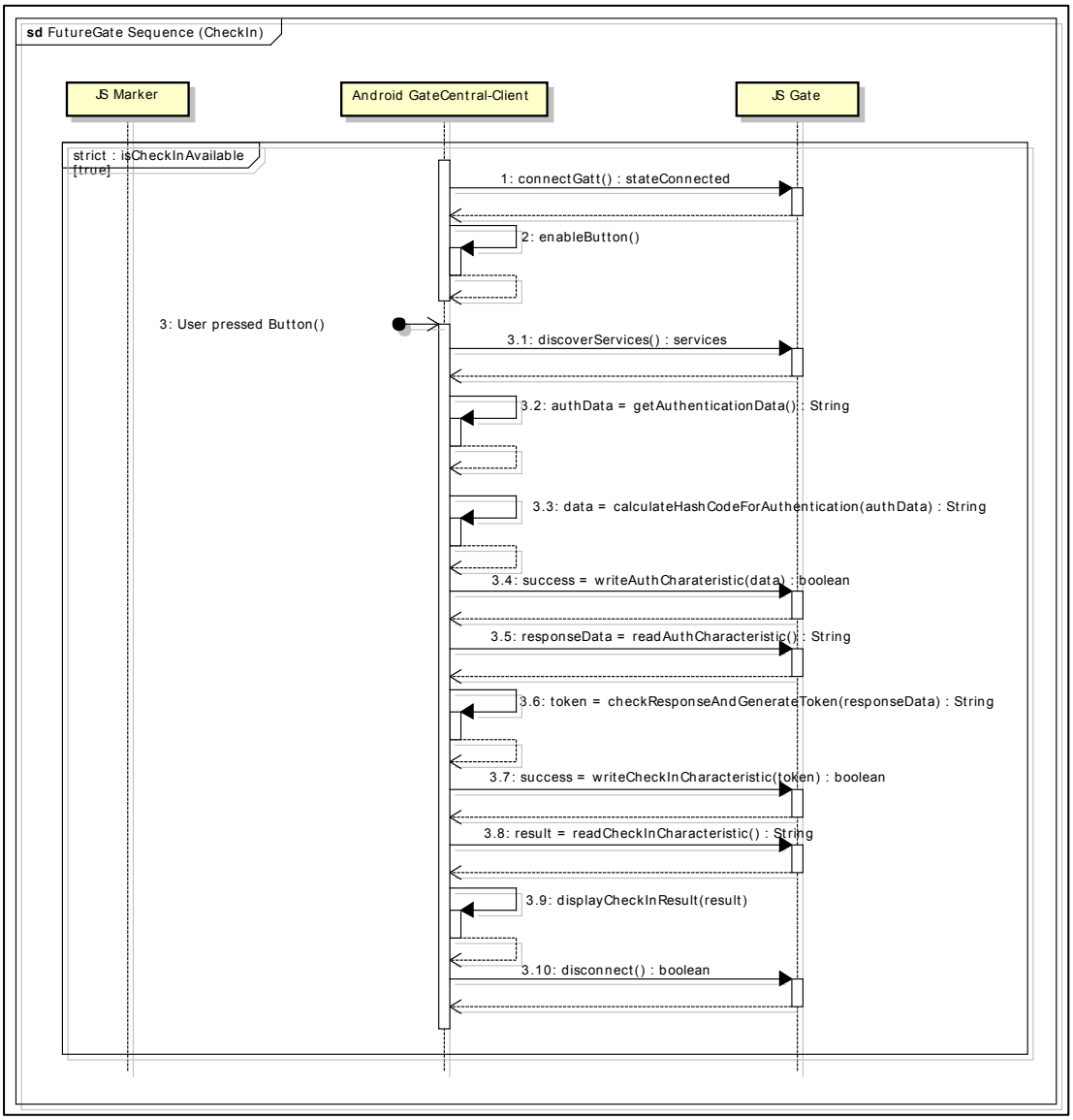

Abbildung 12 - Ablaufdiagramm ‚CheckIn'

Sobald der CheckIn-Bereich des Gates erreicht wurde, verbindet sich das Mobiltelefon mit der Bluetooth Low Energy Schnittstelle des Gates. Ist dieser Schritt erfolgreich, wird auf der Oberfläche der FutureGate-Applikation ein Button dargestellt, durch dessen Betätigung der CheckIn-Vorgang ausgelöst wird. Drückt der Fahrgast diesen Knopf, so beginnt der CheckIn am Gate. Danach werden die Gate-Characteristics überprüft. Es erfolgt die Berechnung der Authentifizierungsdaten, welche mit Hilfe der ‚authCharacteristic' an das Gate gegeben werden. Anschließend wird das Ergebnis der Authentifizierung vom Gate gelesen. Bei einem positiven Ergebnis wird nun den CheckIn-Token erzeugt, mit dem sich das Mobiltelefon beim Gate anmeldet. Der Token

wird an die ‚checkInCharacterristic' übermittelt. Das Gate führt den CheckIn durch und das Ergebnis wird vom Mobiltelefon durch das erneute Auslesen der Characteristic abgerufen. Das gelesene Ergebnis wird dem Fahrgast anschließend auf seinem Mobiltelefon und am FutureGate visualisiert. Nach Beendigung des CheckIn-Vorgangs wird die Verbindung zwischen Mobiltelefon und Gate getrennt. Der Anwendungsfall wurde erfolgreich durchlaufen.

4.5 Berechnung des CheckIn-Bereiches

Der Fahrgast soll sich beim CheckIn durch FutureGate genau an der Position vor der Zutrittskontrolle befinden. Diese Anforderung wird durch die personenvereinzelnde Wirkung des Gates bestimmt. Somit kann nur der Fahrgast den CheckIn am Gate ausführen, der auch wirklich direkt vor der Zutrittskontrolle steht. Damit wird sichergestellt, dass kein anderer Fahrgast versehentlich oder gewollt den CheckIn-Vorgang durchführt.

Um den Bereich des Gates zu identifizieren, in dem sich der Fahrgast genau in dem Bereich vor der Schranke befindet, wird der übermittelte RSSI-Wert der Gate-Komponenten genutzt. Im Rahmen dieser Arbeit wurde dazu eine weitere Scan-Applikation implementiert, welche bei verschiedenen Durchläufen durch das Gate die entsprechenden RSSI-Werte ermittelt und mit einem Zeitstempel versehen zur Auswertung bereitstellt. Die komplette Auswertung befindet sich zusammen mit den Messwerten im Anhang, während die folgenden Abschnitte einzelne Ergebnisse präsentieren.

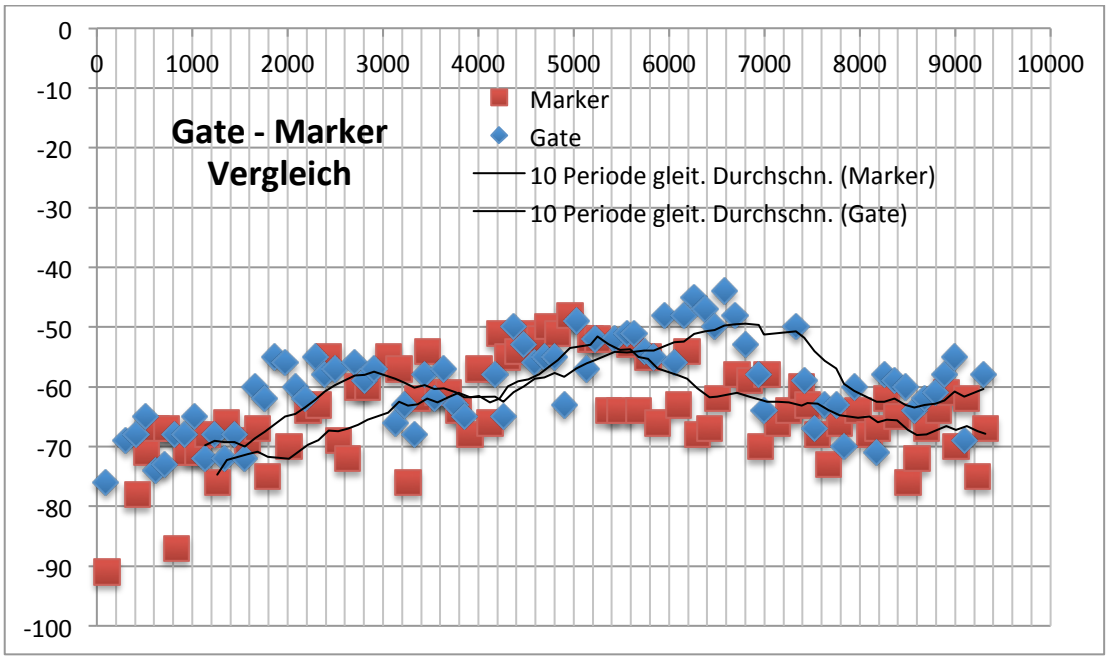

Abbildung 13 - RSSI-Messwerte von Gate und Marker

In Abbildung 13 wird dargestellt, wie sich der RSSI-Wert während der Dauer des Gate-Durchganges verändert. Die Zeit ist dabei in Millisekunden angeben. Der Punkt, an dem der CheckIn verfügbar sein soll, befindet sich bei diesen Messdaten bei 7000 Millisekunden. Bei den Linien im Diagramm handelt es sich um die Trendlinien der gleitenden Durchschnitte beider Werte über eine Spanne von 10 Werten. Aus den Daten wird deutlich, dass sich die RSSI-Werte von Gate und Marker zuerst gleichmäßig entwickeln, bis die Werte des Markers sich verringern. Die Werte des Gates hingegen steigen weiterhin an und verringern sich erst zu einem späteren Zeitraum.

Anschließend, um die Daten besser miteinander vergleichen zu können, wurden sie gemäß folgender Formel normiert:

$$x_{norm} = p * \frac{x}{\sum_{i=0}^{i<p} x_i}$$

Dabei steht p für die Anzahl der Messwerte. Die Variable x ist der zu berechnende Messwert. Die normierten Messwerte des Gates und die normierten Messwerte des Markers werden voneinander subtrahiert. Dabei wurde darauf geachtet, dass nur zeitlich ähnliche Werte voneinander abgezogen werden, um die zeitliche Korrelation zu wahren. In Abbildung 14 ist eine solche Differenz für die oben verwendeten Messwerte sichtbar.

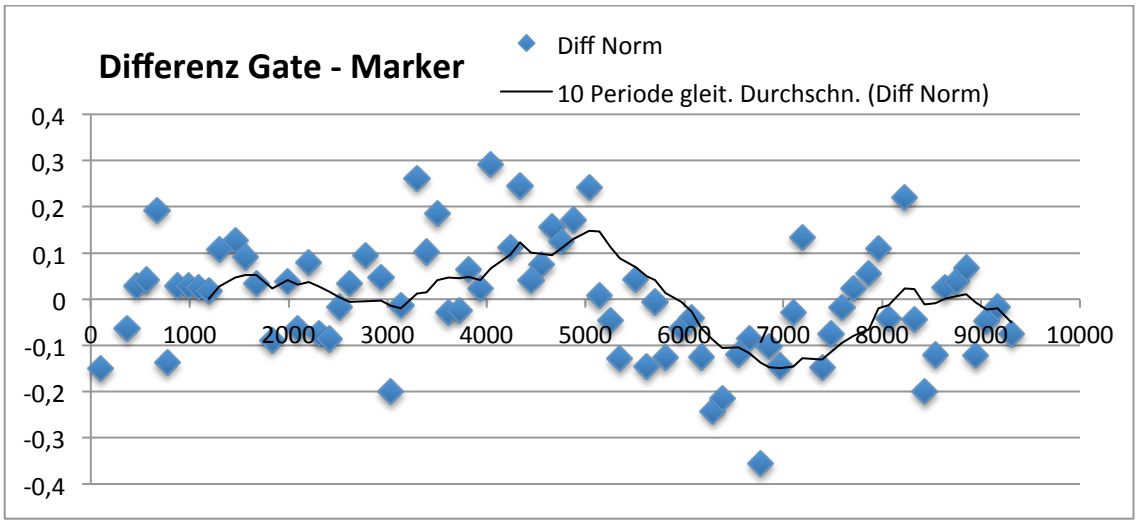

Abbildung 14 - Differenz zwischen normierten Gate- und Markerwerten

Hier werden die Daten wieder in Zusammenhang mit der zeitlichen Dimension dargestellt. Die eingezeichnete Linie ist wiederum die Trendlinie des gleitenden Durchschnitts der Differenz über eine Spanne von 10 Werten. Daraus lässt sich ein markantes Verhalten der RSSI-Werte vor dem Erreichen des CheckIn-Bereiches ablesen. Es wird deutlich, dass sich die Differenz aus den RSSI-Werten von Gate und Marker immer im positiven Bereich befinden, bis sie beim Erreichen des Marker-Senders in den negativen Bereich rutscht. Dann steigt die Differenz wieder, um beim Erreichen des CheckIn-Bereiches wieder in den positiven Bereich zu gelangen.

Es ist erkennbar, dass das zuvor beschriebene Verhalten den CheckIn-Bereich markiert. Die Differenz bewegt sich zu Beginn der Messung um den Nullpunkt und steigt dann in den positiven Bereich. Beim Erreichen des Markers kippt das Verhalten und die Differenz verläuft in den negativen Bereich. Beim Erreichen des Gates beginnt die Kurve wieder zu steigen. Daraus kann abgeleitet werden, dass das Gate mit der vorgestellten Bluetooth Low Energy Methode gut erkannt werden kann. Es handelt sich um den Punkt, ab dem die Kurve wieder ansteigt, nachdem sie von ihrem Höchstwert gefallen ist. Ist dieser Punkt erreicht, hat der Fahrgast den CheckIn-Bereich vor der Schranke erreicht und der CheckIn wird freigeschaltet.

4.6 Rahmenbedingungen der Umsetzung

Nachdem im bisherigen Syntheseteil die Implementierung und deren konzeptioneller Aufbau erläutert wurden, sollen nachfolgend die Voraussetzungen für die Umsetzung des FutureGates beschrieben werden. Zuerst wird die genutzte Entwicklungsumgebung beschrieben. Anschließend folgt die verwendete Laufzeitumgebung. Das letzte Kapitel enthält eine Installationsanleitung.

4.6.1 Eingesetzte Entwicklungsumgebung

Bei der Entwicklungsumgebung sind die einzelnen Komponenten zu trennen. Auf der einen Seite benötigt die FutureGate-Applikation, welche auf dem Mobiltelefon zum Einsatz kommt, eine Java-Entwicklungsumgebung. Auf der anderen Seite stehen dazu die JavaScript-Komponenten Marker und Gate. Diese benötigen zum Erstellen der JavaScript-Dateien die zuvor schon erwähnte NodeJS-JavaScript-Laufzeitumgebung samt den beschriebenen Plugins.

Als Java-Entwicklungsumgebung kam die IDE Eclipse in der Juno-Version zum Einsatz. Da für die Android-Entwicklung auch eine Android-Umgebung benötigt wird, wurde die Eclipse-Plattform um die Android-Laufzeitumgebung im API-Level 18 erweitert. Als Java-Umgebung wurde Java Enterprise Edition 1.7 verwendet. Es wurde auf einem MacBook Pro mit MacOS X Yosemite entwickelt.

Für die Implementierung der JavaScript-Komponenten hätte ein normaler Editor ausgereicht. Da jedoch Funktionen wie Syntaxhighlighting oder Autovervollständigung für den Einsatz einer Entwicklungsumgebung sprachen, wurde die JavaScript-IDE WebStorm der Firma JetBrains in der Version 9.0.1 genutzt. Diese benötigt Java 7 als Laufzeitumgebung. Darüber hinaus wurde die JavaScript-Laufzeitumgebung NodeJS in der Version 0.10.15 installiert. Das Bluetooth Low Energy Framework Bleno lag in Version 0.1.8 vor. Das Framework zur Kommunikation mit dem Browser Socket.IO lag in Version 1.2.0 vor. Da die Bleno-Funktionen betriebsabhängig sind und deswegen eine Linux-Installation verwendet werden muss, kam ein MacBook mit einer Linux Mint Installation in der Version 16 zum Einsatz.

4.6.2 Laufzeitumgebung

Die Laufzeitumgebung der JavaScript-Komponenten unterscheidet sich kaum von der für die Entwicklung genutzten Umgebung (vgl. Abbildung 15). Lediglich auf die eingesetzte IDE kann verzichtet werden. Jedoch werden zusätzlich zwei Bluetooth Low Energy fähige USB-Adapter verwendet, welche die Bluetooth Low Energy Funktionen zur Verfügung stellen. Diese werden von Marker- und Gate-Komponente angesteuert. Bei der Entwicklung kamen dabei zwei USB Bluetooth 4.0 Low Energy USB Adapter der Firma Rocketek zum Einsatz. Diese sind für den Gebrauch am FutureGate geeignet, da sie den Anforderungen an Reichweite und Sendestärke entsprechen. Um die USB-Adapter positionieren zu können, werden außerdem USB-Verlängerungskabel benötigt.

Auf der Seite der Laufzeitumgebung für die FutureGate-Applikation wird ein Mobiltelefon mit dem Betriebssystem Android benötigt. Dieses muss API-Level 18 anbieten. Das entspricht der Android-Version 4.3 Jelly Bean. Außerdem muss bei diesem Gerät die Nutzung von Bluetooth Low Energy erlaubt sein. Bei den Entwicklungsarbeiten kam ein Samsung Galaxy S3 Mini zum Einsatz.

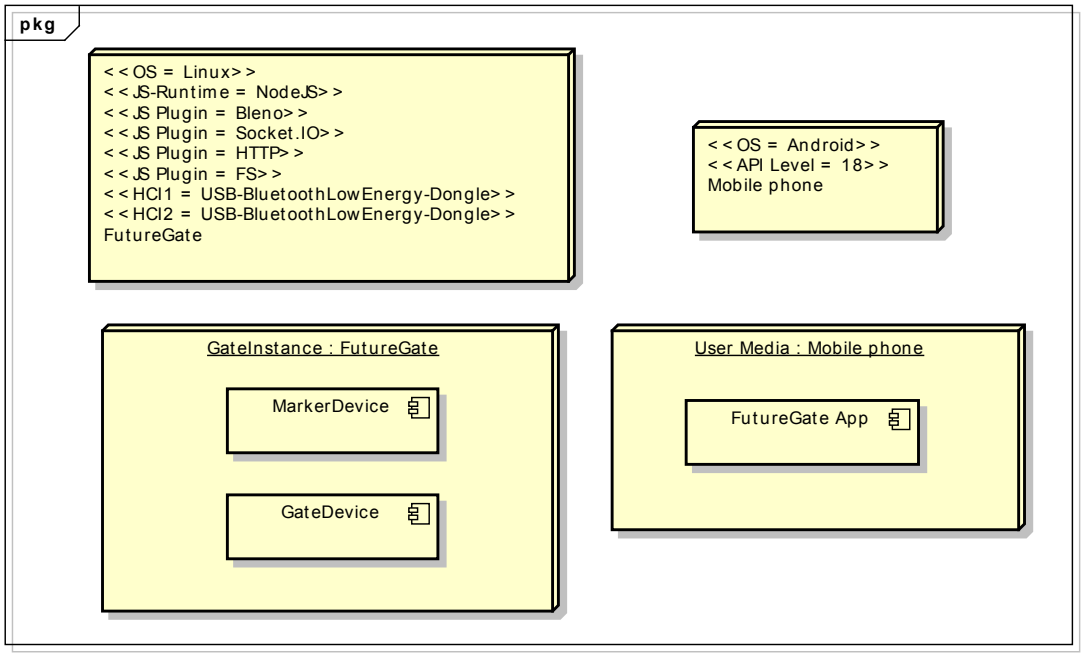

Abbildung 15 - Laufzeitumgebung

4.6.3 Installationsanleitung

Um das FutureGate zu installieren und zu starten, müssen Komponenten auf zwei verschiedenen Entwicklungsumgebungen installiert werden. Zum einen muss die FutureGate-Applikation auf dem Mobiltelefon installiert sein. Dazu schließt man das Gerät per USB an einen Rechner mit der entsprechenden Entwicklungsumgebung an. Dieses Gerät muss für die Verwendung als USB-Debuggable freigeschaltet sein. Diese Einstellung kann in den Systemeinstellungen auf dem Gerät durchgeführt werden. Ist diese Vorbedingung erfüllt, kann das Applikationsprojekt in die Entwicklungsumgebung importiert werden. Dieses importierte Projekt wird nun automatisch gebaut. Wird das ohne Fehler abgeschlossen, kann die Applikation nun auf das angeschlossene Mobiltelefon übertragen werden. Anschließend kann die Verbindung zwischen Mobiltelefon und Entwicklungssystem getrennt werden. Die Applikation ist nun auf dem Gerät installiert.

Anders ist es bei der Gate-Komponente. Hier wird vorausgesetzt, dass die Laufzeitumgebung mit Linux Mint und NodeJS schon besteht. Die USB-Bluetooth Low Energy Adapter sind noch nicht angeschlossen. Nun muss das FutureGate-Verzeichnis auf die dafür vorgesehene Laufzeitumgebung kopiert werden. Anschließend beginnt die Vorbereitung der Installation. Ein eventuell vorhandener Bluetooth Sender wird mit folgendem Befehl deaktiviert.

- hciconfig hci0 down

Anschließend werden die beiden Bluetooth Low Energy USB-Adapter mit dem System verbunden. Sobald sie eingesteckt sind, sind sie im System verfügbar als HCI1 und HCI2. Da beide Adapter nicht von sich aus scannen sollen, wird bei beiden das automatische Scannen ausgeschaltet:

- hciconfig hci1 noscan
- hciconfig hci2 noscan

Nun folgt die Positionierung der USB-Geräte. Diese werden in einem Abstand von 135 cm und in einer Höhe von 130 cm entlang der geplanten Durchlaufrichtung im Gate positioniert. Dabei ist sicherzustellen, dass in Durchlaufrichtung der USB-Adapter HCI1 als erstes steht und danach HCI2, weil die Marker-Komponente räumlich vor der Gate-Komponente stehen muss. Diese können mit den folgenden Befehlen aus dem Installationsordner gestartet werden.

- BLENO_HCI_DEVICE_ID=1 GATE_DEVICE_NAME=Marker-GateDevice nodejs bleno-marker-service.js
- BLENO_HCI_DEVICE_ID=2 GATE_DEVICE_NAME=GateDevice-1 USE_AUTH_SECRET=0 nodejs bleno-gate-service.js

Schließlich ist das FutureGate einsatzbereit.

5 Schlussteil

Die Umsetzung der Zutrittskontrolle unter Anwendung des Bluetooth Low Energy Standards in dieser Arbeit zeigt, dass die technische Entwicklung nicht bei der Nutzung von Chipkarten oder NFC-fähigen Mobiltelefon aufhört. Das FutureGate macht es möglich, Funktechniken mit einer höheren Reichweite für Zutrittskontrollen zu nutzen. Folgend soll die Lösung der Aufgabe zusammengefasst und evaluiert werden. Nach einem Ausblick über die möglichen Weiterentwicklungen folgt dann ein abschließendes Fazit.

5.1 Zusammenfassung

Die Aufgabe, eine Zutrittskontrolle für den öffentlichen Personenverkehr auf Basis der Funktechnik Bluetooth Low Energy zu erstellen, umfasste neben der eigentlichen Soft- und Hardwareimplementierung drei grundlegende Herausforderungen.

Erstens musste sichergestellt werden, dass nur Personen mit Nutzermedien, die für die Nutzung des FutureGates zugelassen sind, die Zutrittskontrolle nutzen können. Hierbei gilt natürlich auch, dass nur FutureGates mit den Mobiltelefonen kommunizieren sollen und ein Missbrauch von Dritten wie dem Auslesen von Zutrittstoken verhindert wird. Dieses Problem wird durch eine beidseitige Authentifizierung auf Basis des Challenge-Response-Verfahrens gelöst. So kann sichergestellt werden, dass nur authentifizierte Kommunikationspartner an einem Vorgang teilnehmen.

Die zweite Herausforderung betrifft die Frage, wann sich der Fahrgast genau an der richtigen Position vor der Schranke des FutureGates befindet. Dieses Problem impliziert die Frage, ob es sich bei der Person, die den CheckIn-Vorgang durchführt, auch um die Person handelt, die vor der Schranke steht. Hier zeigt die Arbeit, wie mit Hilfe der Positionierung der Bluetooth Low Energy Adapter entlang der Laufstrecke und der Auswertung der gewonnen RSSI-Werte ein entsprechender Punkt gefunden werden kann. Damit lässt sich mit hoher Sicherheit feststellen, dass sich der Nutzer genau an der richtigen Position zum CheckIn befindet.

Ist die Positionierung des Fahrgastes im CheckIn-Bereich des Gates möglich, so stellt sich drittens die Frage nach der Geschwindigkeit des CheckIn-Vorganges. Sollte sich der Bluetooth Low Energy Ansatz als zu langsam herausstellen, so kann er in einer Umgebung wie einem hochfrequentiertem Bahnhof nicht angewendet werden, da sich aufgrund des zu erwartenden Fahrgastaufkommen schnell lange Wartezeiten vor der Zutrittskontrolle entstehen können. In dieser Arbeit wurde festgestellt, dass für den CheckIn-Vorgang an einem FutureGate ca. 500 Millisekunden benötigt werden Möglich wurde dies durch den Einsatz der richtigen Bluetooth Low Energy Betriebsmodi. Tests hatten ergeben, dass die Implementierung des Mobiltelefons als Peripheral und des Gates als Central zu einer doppelt so langen Dauer von ca. 1000 Millisekunden geführt hatte. Aus diesem Grund wurde die Aufgabe mit dem Mobiltelefon als Central und dem Gate als Peripheral umgesetzt.

5.2 Anwendung in der Praxis

Da die Herausforderungen an die Authentifizierung zwischen Gate und Mobiltelefon, die Positionierung des Fahrgastes im FutureGate und die Geschwindigkeit beim CheckIn-Vorgang zufriedenstellend gelöst wurden, stellt die in dieser Arbeit entwickelte Lösung einen interessanten Ansatz für die Zutrittskontrolle im öffentlichen Personenverkehr dar. FutureGate wurde prototypisch als Machbarkeitsstudie umgesetzt, die in dieser Weise auch zur Umsetzung einer Zutrittskontrolle im öffentlichen Personenverkehr verwendet werden kann. So kann herausgefunden

werden, ob sich Ansätze und Konzepte auch praktisch anwenden und umsetzen lassen. Da die Herausforderungen an die Authentifizierung zwischen Gate und Mobiltelefon, die Positionierung des Fahrgastes im FutureGate und die Geschwindigkeit beim CheckIn-Vorgang zufriedenstellend gelöst wurden, stellt die angegebene Lösung einen interessanten Ansatz für die Zutrittskontrolle im öffentlichen Personenverkehr dar. Auch wenn das Konzept der Zutrittskontrolle im deutschen Personenverkehr keine weite Verbreitung findet, betrachtet die Industrie die Weiterentwicklung von etablierten Systemen unter Einbeziehung von neuen Technologien sehr wohlwollend.

Gerade in den europäischen Nachbarländern haben sich im Gegensatz zu Deutschland Systeme mit automatisierten Zutrittskontrollen im öffentlichen Personenverkehr etabliert. Diesen Systemen bietet sich mit Bluetooth Low Energy eine weitere Möglichkeit, den CheckIn-Vorgang umzusetzen.

5.3 Fazit

Diese Arbeit hat gezeigt, dass die Anwendung des Bluetooth Low Energy Standards bei der Zutrittskontrolle im öffentlichen Personenverkehr möglich ist. Die verfügbare Technologie in Mobiltelefonen und Lesegeräten lässt eine Lösung zu, welche die Anforderungen an ein solches System erfüllt. Die beschriebene Machbarkeitsstudie erfüllt die gestellten Aufgaben unter Laborbedingungen. Unter diesen Bedingungen wird der Nutzer zuverlässig an der richtigen Position erkannt und der gesamte Vorgang in akzeptabler Zeit abgeschlossen. In weiteren Arbeiten gilt es jetzt, diesen Ansatz unter realen Bedingungen zu überprüfen und weiter auszubauen.

5.4 Ausblick

Die prototypische Umsetzung zeigt, dass eine Zutrittskontrolle auf Bluetooth Low Energy Basis möglich ist. Bis ein solches Produkt aber die für einen öffentlichen Einsatz nötige Marktreife erlangt, sind jedoch einige Weiterentwicklungen und Tests notwendig. Zum einen wurde das FutureGate bisher nur als einzelnes Gate ausprobiert. Unter diesen Bedingungen genügen zwei Bluetooth Low Energy Adapter, um eine ausreichende Genauigkeit bei der Positionsbestimmung des Nutzers zu erreichen. In einem realen Szenario stehen aber viele Gates in Bahnhof eng nebeneinander. Das bedeutet, dass sich die Bluetooth-Felder der einzelnen Gates wahrscheinlich stark überschneiden. Dadurch wird die Positionsbestimmung des Nutzers ungenauer, weil nicht genau erkannt werden kann, in welchem Gate der Nutzer sich gerade befindet. Aus diesem Grund kommt hier der Einsatz von 4 Bluetooth Low Energy Adaptern in Frage. Diese werden um das Gate platziert. Beim Durchlaufen des Gates durch den Nutzer können nun 4 Positionswerte genutzt werden, um die Positionsberechnung durchzuführen.

Ein weiterer Punkt ist die Optimierung der Dauer eines CheckIn-Vorgangs. 500 Millisekunden scheinen ein ausreichender Wert zu sein, allerdings setzt die Nutzermedienspezifikation der Kernapplikation eine Dauer von maximal 300 Millisekunden voraus. Davon dürfen maximal 200 Millisekunden für die Authentifizierung und den eigentlichen CheckIn-Vorgang genutzt werden. 100 Millisekunden sind der Kommunikation zwischen Nutzermedium und Lesegerät vorbehalten (vgl. [INFI2013]). Demnach wird deutlich, dass die Lösung auf Bluetooth Low Energy Basis optimiert werden muss. Optimierungspotentiale sind dabei die Verwendung eines anderen Authentifizierungsmechanismus und die Verwendung der VDV Kernapplikation-spezifischen Datenstrukturen. Bisher werden für diesen Zweck definierte Datenstrukturen für den Austausch zwischen Mobiltelefon und Lesegerät verwendet.

Neben der Weiterentwicklungen der Anwendung in einem realen Szenario gibt es außerdem die Möglichkeit, die Lösung von einem CheckIn/CheckOut-Szenario in ein BeIn/BeOut-Szenario weiter zu entwickeln. Bei der entwickelten Lösung muss der Nutzer nach Erreichen der CheckIn-Position aktiv mit dem Lesegerät interagieren, um die Schranke der Zutrittskontrolle öffnen zu können. Funktioniert die Positionsbestimmung jedoch zuverlässig, so kann auf die aktive Interaktion des Nutzers verzichtet werden. Ebenso ist die Schranke dann nicht mehr nötig, weil das Mobiltelefon die Anwesenheit automatisch an das Lesegerät meldet. Der Nutzer würde nur durch das Gate gehen und könnte so ungehindert am öffentlichen Personenverkehr teilnehmen. Das wäre die maximale Ausbaustufe der Kernapplikation des Verbunds deutscher Verkehrsunternehmen.

6 Versicherung der Selbstständigkeit

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbstständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, den _____ _____

7 Literaturverzeichnis

[COMS2014] comScore MobiLens, "Anzahl der Smartphone-Nutzer in Deutschland bis 2014 | Statistik," Statista, 04-Jan-2014. [Online]. Available: http://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/. [Accessed: 08-Jan-2015].

[GREI2014] B. Greif, "Apple beschränkt NFC-Funktion des iPhone 6 auf seinen Bezahldienst Pay," ZDNet.de, 16-Sep-2014. [Online]. Available: http://www.zdnet.de/88205955/apple-beschraenkt-nfc-funktion-des-iphone-6-auf-seinen-bezahldienst-pay/. [Accessed: 05-Jan-2015].

[NEUH2011] T. Neuhetzki, "Bahn startet Regelbetrieb bei Touch & Travel - teltarif.de News," 11-Jan-2011. [Online]. Available: http://www.teltarif.de/touch-travel-regelbetrieb-deutsche-bahn/news/44460.html. [Accessed: 05-Jan-2015].

[MIST2014] S. Mistry, "BleNo," *GitHub*, 12-Jun-2014. [Online]. Available: https://github.com/sandeepmistry/bleno. [Accessed: 18-Dec-2014].

[HEYD2012] R. Heydon, *Bluetooth Low Energy: The Developer's Handbook*, 1 edition. Upper Saddle River, NJ: Prentice Hall, 2012.

[HODG2011] K. Hodgkins, "Bluetooth Smart announced, iPhone 4S is ready," *TUAW: Apple news, reviews and how-tos since 2004*, 25-Nov-2011. [Online]. Available: http://www.tuaw.com/2011/10/25/bluetooth-smart-announced-iphone-4s-is-ready/. [Accessed: 18-Dec-2014].

[IT-W2014] IT-wissen, "Challenge-Response-Verfahren," *IT-Wissen Das große Online-Lexikon der Informationstechnologie*, 18-Dec-2014. [Online]. Available: http://www.itwissen.info/definition/lexikon/Challenge-Response-Verfahren-challenge-response.html. [Accessed: 18-Dec-2014].

[METZ2014] J. Metzger, P. D. R. Lackes, and D. M. Siepermann, "Chipkarte," *Gabler Wirtschaftslexikon*, 18-Dec-2014. [Online]. Available: http://wirtschaftslexikon.gabler.de/Archiv/1515/chipkarte-v12.html. [Accessed: 18-Dec-2014].

[VDVE2012] Verband Deutscher Verkehrsunternehmen e.V., "Der VDV – Verband Deutscher Verkehrsunternehmen Die starke Basis für Ihren Erfolg." 2012.

[BEEL2013] U. Beele, "Deutschland-Tag des Nahverkehrs: Sanierungsstau bei Bus und Bahn," *NWL Info*, 09-Dec-2013. [Online]. Available: http://www.nwl-info.de/aktuelles/pressemitteilungen/2013/09/12/sanierungsstau-bei-bus-und-bahn.php. [Accessed: 18-Dec-2014].

[VDVK2014] VDV KA GmbH, "Die VDV-Kernapplikation," *eTicket Deutschland*, 18-Dec-2014. [Online]. Available: http://www.eticket-deutschland.de/vdv-kernapplikation.aspx. [Accessed: 18-Dec-2014].

[NACH2014] R. Nachbar, "(((eSIM 2020 - Be-In/Be-Out-Verfahren im öffentlichen Nahverkehr," *rhein-main-service Consult GmbH*, 18-Dec-2014. [Online]. Available: http://www.rms-consult.de/aktuelle-projekte/esim-2020---bein-beout-verfahren-im-oeffentlichen-nahverkehr/esim-2020---efmsystemintegration-und-migration.html. [Accessed: 18-Dec-2014].

[KOPP2012] H. Koppay, Entwicklung und Vermarktung von Handy-Apps: Einstieg in die Welt der mobilen Applikationen. disserta Verlag, 2012.

[TOWN2014] K. Townsend, C. Cufí, Akiba, and R. Davidson, *Getting Started with Bluetooth Low Energy: Tools and Techniques for Low-Power Networking*, Auflage: 1. O'Reilly & Associates, 2014.

[HASB2011] HSB, "Hanauer Straßenbahn GmbH - get>>in," 02-Sep-2011. [Online]. Available: http://www.hsb.de/preise/getin/. [Accessed: 05-Jan-2015].

[GOOG2014] Google Android Team, "Jelly Bean," *Android Developers*, 18-Dec-2014. [Online]. Available: http://developer.android.com/about/versions/jelly-bean.html. [Accessed: 18-Dec-2014].

[LEAC1999] P. J. Leach, J. Franks, A. Luotonen, P. M. Hallam-Baker, S. D. Lawrence, J. L. Hostetler, and L. C. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," 01-Jun-1999. [Online]. Available: http://tools.ietf.org/html/rfc2617. [Accessed: 19-Dec-2014].

[NOCH2014] D. Z. Nochta, "Katalog der Deutschen Nationalbibliothek," *Katalog der Deutschen Nationalbibliothek*, 04-Jan-2014. [Online]. Available: https://portal.dnb.de/opac.htm;jsessionid=0DB11931095C94CA7D4995779F9D167C.prod-worker0?query=idn%3D97363927X&cqlMode=true&method=simpleSearch. [Accessed: 18-Dec-2014].

[IT-W2014-2] IT-wissen, "Kontaktlose Chipkarte," *IT-Wissen Das große Online-Lexikon der Informationstechnologie*. [Online]. Available: http://www.itwissen.info/definition/lexikon/Kontaktlose-Chipkarte-contactless-chipcard.html. [Accessed: 18-Dec-2014].

[METZ2014-2] J. Metzger, P. D. R. Lackes, and D. M. Siepermann, "Magnetstreifenkarte," *Gabler Wirtschaftslexikon*. [Online]. Available: http://wirtschaftslexikon.gabler.de/Archiv/1516/magnetstreifenkarte-v12.html. [Accessed: 18-Dec-2014].

[ELEK2014] Elektronik Kompendium, "NFC - Near Field Communication," *Elektronik Kompendium*, 18-Dec-2014. [Online]. Available: http://www.elektronik-kompendium.de/sites/kom/1107181.htm. [Accessed: 18-Dec-2014].

[STAC2014] D. F. von Stackelberg and D. R. Malina, "Öffentlicher Personenverkehr,"

Gabler Wirtschaftslexikon, 18-Dec-2014. [Online]. Available: http://wirtschaftslexikon.gabler.de/Archiv/78689/oeffentlicher-personenverkehr-v6.html. [Accessed: 18-Dec-2014].

[IT-W2014-3] IT-wissen, "QR-Code," *IT-Wissen Das große Online-Lexikon der Informationstechnologie*, 18-Dec-2014. [Online]. Available: http://www.itwissen.info/definition/lexikon/quick-response-QR-QR-Code.html. [Accessed: 18-Dec-2014].

[HAIK2013] E. Haikewitsch, P. Edoire, P. Lelievre, and N. Smith, "Rio de Janeiro launches pilot for public transportation NFC ticketing with smartphones," *Gemalto*, 18-Oct-2013. [Online]. Available: http://www.gemalto.com/press/Pages/news_1688.aspx. [Accessed: 18-Dec-2018].

[RMVG2008] Rhein-Main-Verkehrsverbund GmbH, "NFC-HandyTicket Bedienungsanleitung - für Nokia 6131 NFC." 19-Feb-2008.

[DEME2013] A. Dementyev, S. Hodges, S. Taylor, and J. Smith, "Power consumption analysis of Bluetooth Low Energy, ZigBee and ANT sensor nodes in a cyclic sleep scenario," 2013, pp. 1–4.

[MAIE2014] P. Maier, "The Lab - Magnetkarten," *RunningServer.com*, 18-Dec-2014. [Online]. Available: http://www.runningserver.com/?page=runningserver.content.thelab.magnetcards. [Accessed: 18-Dec-2014].

[BLUE2014] Bluetooth SIG, "The Low Energy Technology Behind Bluetooth Smart," *Bluetooth SIG*, 18-Dec-2014. [Online]. Available: http://www.bluetooth.com/Pages/low-energy-tech-info.aspx. [Accessed: 18-Dec-2014].

[INFI2013] Infineon Technologies AG, Siemens Schweiz AG, T-Systems GEI GmbH, "VDV-Kernapplikation Spezifikation Nutzermedium." 05-Jan-2013.

[SCHL2012] C. Schlesiger, "Wie Städte Schwarzfahrer jagen," *Wirtschaftswoche Online*, 19-Apr-2012. [Online]. Available: http://www.wiwo.de/unternehmen/dienstleister/nahverkehr-wie-staedte-schwarzfahrer-jagen/6503938.html. [Accessed: 18-Dec-2014].

8 Anhang

Der Anhang umfasst die Messwerte zur Berechnung des korrekten CheckIn-Bereichs (siehe Kapitel 4.5) und alle im Syntheseteil verwendeten UML-Diagramme im PNG-Format (siehe Kapitel 4). Er befindet sich im Verzeichnis ‚Anhang' auf dem der Arbeit beigelegten Datenträger.

I. Messwerte zur Berechnung des CheckIn-Bereiches (Dateiname: Anhang-I-Messwerte.xlsx)
II. Abbildung 8 - Komponentendiagramm FutureGate (Dateiname: Anhang-II-Komponentendiagramm.png)
III. Abbildung 9 - Zustandsübergänge der Android-Applikation (Dateiname: Anhang-III-Zustandsuebergaenge.png)
IV. Abbildung 10 - Schnittstelle Gate – Mobiltelefon (Dateiname: Anhang-IV-Schnittstelle.png)
V. Abbildung 11 - Ablaufdiagramm ‚Erreichen des Gates' (Dateiname: Anhang-V-Ablaufdiagramm-Erreichen.png)
VI. Abbildung 12 - Ablaufdiagramm ‚CheckIn' (Dateiname: Anhang-VI-Ablaufdiagramm-CheckIn.png)
VII. Abbildung 15 - Laufzeitumgebung (Dateiname: Anhang-VII-Laufzeitumgebung.png)
VIII. Abbildung 6 - UseCase Diagramm FutureGate (Dateiname: Anhang-VIII-Use-Case-Diagramm.png)