Gutscheinvalidierung im Mobile Couponing - eine Evaluierung bestehender Technologien

Daniel Herbert Lichtenegger, BSc.
(Matr. Nr. 0630157)

MASTERARBEIT

eingereicht am
Masterstudiengang

Softwareentwicklung-Wirtschaft
(F 066 924)

der Technischen Universität in Graz

im Feber 2011

Deutsche Fassung:
Beschluss der Curricula-Kommission für Bachelor-, Master- und Diplomstudien vom 10.11.2008
Genehmigung des Senates am 1.12.2008

EIDESSTATTLICHE ERKLÄRUNG

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst, andere als die angegebenen Quellen/Hilfsmittel nicht benutzt, und die den benutzten Quellen wörtlich und inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

Graz, am ……. ……..
(Unterschrift)

Englische Fassung:

STATUTORY DECLARATION

I declare that I have authored this thesis independently, that I have not used other than the declared sources / resources, and that I have explicitly marked all material which has been quoted either literally or by content from the used sources.

……. ……..
date (signature)

Inhaltsverzeichnis

Danksagung

Ich möchte mich an dieser Stelle bei all jenen bedanken, die mich bei der Erstellung dieser Diplomarbeit unterstützt haben. Ein besonderer Dank ergeht an meinen Professor und Betreuer Herrn Univ.-Prof. Dipl.-Ing. Dr.techn.Frank Kappe und an meine Betreuer bei der Firma vooch GmbH, Herrn Dr. Tobias Hann und Herrn Dipl.-Ing. Mag. Michael Meier, die mir hilfreich zur Seite gestanden sind. Dies gilt auch für all jene, die mir unterstützen zur Seite standen und meine Arbeit korrekturgelesen haben.
Weiters möchte ich mich herzlichst bei meiner ganzen Familie bedanken, die mich auf meinem ganzen Lebensweg bis jetzt kräftig unterstützt und mir das Studium an der Technischen Universität in Graz ermöglicht hat.
Nicht zuletzt gebührt der Dank auch all meinen Freunden, die mir den Einstieg und das Leben in Graz erleichtert haben und auch allen, deren Bekanntschaft ich in Graz machen durfte, woraus sich tolle und hoffentlich auch langwährende Freundschaften entwickelten. Ganz besonders bedanken möchte ich mich noch bei meinem Kollegen Georg Kitz mit dem ich ziemlich jedes der universitären Projekte gemeinsam gemeistert habe und durch den einiges erst möglich wurde.

Kurzfassung

Das österreichische Startup Unternehmen vooch GmbH mit Sitz in Tulln befasst sich nun seit zwei Jahren mit dem Thema "Mobile Couponing". Mittlerweile wurden schon eigene Anwendungen für die gängigsten mobilen Plattformen entwickelt, welche dem Benutzer Gutscheine in seiner nahen Umgebung präsentieren und digital eingelöst werden können. Um Geschäftskunden ein möglichst realitätsgetreues Feedback und eine korrekte Abrechnung ihrer Aktionen gewährleisten zu können, lässt vooch Gutscheine nur in Nähe eines jeweiligen Geschäftslokals einlösen. Leider ist das Unternehmen schon seit längerem mit einer gewissen Ungenauigkeit konfrontiert, welche eine Verfälschung der Daten hervorruft. Dies lässt sich hauptsächlich auf die Abweichungen der verwendeten Lokalisierungstechnologien zurückführen.
Diese Arbeit befasst sich mit der Problematik des Einlöseverfahrens der vooch GmbH, untersucht alternative Technologien und bewerte diese. Das erste Kapitel gibt dem Leser einen kurzen Einblick in das unternehmerische Umfeld des Unternehmens und definiert die Problematik. Im darauf folgenden Kapitel 2 werden die derzeit verwendeten, aber vor allem alternative oder ergänzende Lokalisierungstechnologien detailliert betrachtet, deren Funktionsweise analysiert und die sich daraus ergebenden Vor- und Nachteile hervorgehoben. Im dritten Kapitel werden für vooch wichtige Kriterien definiert und ein Bewertungsschema aufgestellt. Die in Kapitel 2 vorgestellten Technologien werden zusammen mit ihren Vor- und Nachteilen nochmals kurz zusammengefasst und anhand des aufgestellten Schemas und der Kriterien bewertet. Die damit ausgewählte Technologie wird im vierten und letzten Kapitel als Prototyp umgesetzt um einen sogenannten "Proof of Concept" durchzuführen, also die Funktionsfähigkeit zu demonstrieren, weiters wird die weitere Vorgehensweise beschrieben.

Abstract

Vooch Gmbh, an Austrian start up company, has been dealing with the topic "mobile couponing" for two years now. Meanwhile they have already developed their own applications for the most popular mobile platforms that present the user with vouchers within his or her vicinity. These coupons can be redeemed digitally. To assure business clients the most realistic feedback as well as the most accurate billing for their services, vouchers can only be redeemed in close proximity to the actual business location. Unfortunately the company is confronted with a certain lack of precision that causes a distortion of the data. This is mainly due to the deviation of the location technologies used.
This paper focuses on the problem in the redeeming process of vooch, examines alternative technologies and rates them. The first chapter gives the reader an insight into the company vooch, and the field it operates in. In addition current company problems are defined. In chapter 2, the currently used, but mainly the alternative or complementary location technologies are examined in detail, their functionality is analyzed and the resulting advantages and disadvantages are highlighted. In the third chapter important criteria for vooch are defined, and a rating scale developed. The technologies presented in chapter 2 combined with their advantages and disadvantages are briefly repeated and evaluated based on the established scale and criteria. The fourth and last chapter is a prototype based on the selected technology. A so-called "proof of concept" is developed and carried out to demonstrate the operability. In addition the further proceeding is described.

Kapitel 1

Einleitung

Diese Arbeit entstand im Rahmen eines Forschungsauftrages der Firma vooch GmbH, dem eine Verfahrensverbesserung zu Grunde liegt. Der Auftrag erging am 30. August 2010 an das Institut für Informationssysteme und Computer Medien Fakultät für Informatik an der Technischen Universität in Graz. Kontaktperson und Betreuer an der TU Graz ist der derzeit aktive Institutsleiter Univ.-Prof. Dipl.-Ing. Dr. Frank Kappe und bei vooch die beiden Inhaber Dr. Tobias Hann und Dipl.-Ing. Mag. Michael Meier.
Doch um zu verstehen, worum es in dieser Diplomarbeit geht und was das eigentliche Problem ist, muss zuerst der Grundgedanke von vooch verstanden werden.

1.1 Was ist vooch?

Das System vooch entsprang einer Marketingidee, welche den Werbemarkt revolutionieren sollte. Seit vielen Jahren setzt die Werbeindustrie auf veraltete Medien wie Postwurfsendungen, Gutscheinhefte, Zeitungsannoncen, und andere, welche im Vergleich zu den hohen Druck- und Vertriebskosten nur einen geringen Rücklauf erhoffen lassen. Dazu kommen auch noch die hohen Streuverluste, welche durch die kaum vorhandenen Lenkungsmöglichkeiten in Richtung Zielgruppe entstehen. Wie wäre es, wenn Unternehmen ihre Zielgruppe punktgenau und direkt erreichen könnten? Das Ganze auch noch ohne hohe Produktionskosten auf einem der neuesten Werbemedien die der Markt zu bieten hat und ohne dass Werbung als eben diese wahrgenommen wird? – Denn wer findet es nicht mühsam, jeden Tag den Postkasten erstmal von den vielen Werbesendungen und Gutscheinheften, welche sehr "persönlich" mit "an einen Haushalt" betitelt werden, zu befreien bevor man zu seiner eigentlichen Post kommt? – All diese Wünsche kann vooch erfüllen.
Doch bevor man näher darauf eingeht, ist erstmal zu klären, WAS denn überhaupt dieses neue Werbemedium ist. Wenn man Kunden direkt errei-

chen will, benötigt man etwas, was dieser meistens bei sich trägt. Und was liegt da näher, als ein Mobiltelefon. In der heutigen vernetzten und hektischen Welt besitzt nahezu jeder zweite Mensch ein Mobiltelefon. Im Jahr 2008 gab es weltweit bereits vier Milliarden Handyverträge (Seifert et al., 2009) (siehe Abbildung 1.1), wobei man die Werte etwas differenziert betrachten muss, da nicht jeder ein Mobiltelefon besitzt, manche jedoch gleich mehrere (vgl. Entwicklungsländer und Industrieländer). Das Handy ist also ständiger Wegbegleiter seines Besitzers und eignet sich somit hervorragend als Medium.
Durch die Verwendung des Mobiltelefons als Werbeträger werden die Druck- und Vertriebskosten eingespart, da die Werbung nur noch digital existiert, und somit auch die Umwelt geschont wird. Weiters entfällt auch das lästige Vergessen etwaiger Gutscheinhefte, da diese dann in der Hosentasche oder in der Handtasche immer dabei sind.

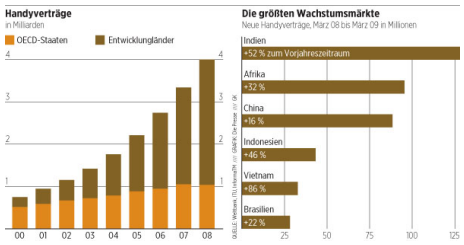


Abbildung 1.1: Handyverträge weltweit 2008(Seifert et al., 2009)

Stellt sich nur noch die Frage, welcher Grund sich dahinter verbirgt, dass ein Konsument Werbung nicht mehr als belästigend empfindet? Bislang wurde man ja beim Holen der Post mit Werbung nahezu überhäuft. vooch verfolgt hier ein einfaches Konzept, und zwar holt sich der Benutzer die Werbung selbst, in dem er sie im System nach gewissen Kriterien (Nähe zum derzeitigen Standort, Kategorien, Schlagwörter, etc.) sucht und auswählt. Er bestimmt damit selbst welche Produkte, Dienstleistungen, etc. er sich ansehen will und welche nicht. Durch diesen einfachen psychologischen Hintergrund der Eigenkontrolle und Selbstbestimmung wird die von ihm angesehene Werbung als angenehm und passend empfunden. Da sich der Konsument die Werbung nun selbst holt, werden auch die Streuverluste minimiert, da diese den Weg zu ihrer Zielgruppe selbst findet.

Aus dieser Idee heraus gründeten der damalige Mag. Tobias Hann zusammen mit Dipl.-Ing. Mag. Michael Meier Anfang 2009 die niederösterreichische GmbH[1] vooch mit Sitz in Tulln, die seitdem ihre österreichweit einzigartige Gutscheinlösung am Markt anbietet. Seither setzen bereits vie-

[1] Gesellschaft mit beschränkter Haftung

le namhafte Unternehmen, wie die österreischischen Mobilfunkunternehmen mobilkom austria[2] und Hutchison 3G Austria[3], aber auch Unternehmen wie OMV, Starbucks, Burger King, Ankerbrot und viele andere auf die Dienstleistungen von vooch. Das Unternehmen wurde auch bereits mehrfach mit Auszeichnungen prämiert, unter anderem:

- Seedcamp in Berlin
- Mobile Monday Berlin und Wien
- i2b Sieger 2009
- Genius Award
- WebAd 2010 (beste Platzierung in der Kategorie "Consumer Benefit")
- etc.

vooch verfügt derzeit über beinahe 100.000 Benutzer und unterstützt mehr als 95%[4] aller gängigen Mobiltelefone am Markt auf folgenden Plattformen:

- iPhone
- Android
- Java ME
- XHTML (eine mobile Webseite, welche den kleinen Anteil aller noch nicht unterstützten Mobiltelefone abdecken soll)

Als Grundlage für die Verteilung und Selektion der dem Benutzer präsentierten Gutscheine (siehe Abbildung 1.2) dient der vom mobilen Endgerät ermittelte Standort des Benutzers, wodurch ihm diese nach ihrem Abstand aufsteigend sortiert angezeigt werden. Filtermöglichkeiten bestehen unter anderem auch durch eine Kategorieauswahl, eine textuelle Suche und diverse Benutzerpräferenzen.

Für die Aktivierung eines Gutscheins hat vooch ein eigenes Verfahren entwickelt, welches sicherstellt, dass ein Gutschein nur am Standort des Unternehmens (ausgenommen der mobilen Webseite) und innerhalb der Öffnungszeiten eingelöst werden kann. Dabei wird berechnet, ob sich der Benutzer innerhalb eines bestimmten Radius des am nächsten liegenden Standortes befindet. Nur dann kann das Angebot erfolgreich in Anspruch genommen werden und ein Bild erscheint für einen bestimmten Gültigkeitszeitraum am

[2] http://www.a1telekom.at/
[3] http://www.drei.at/
[4] Stand September 2010

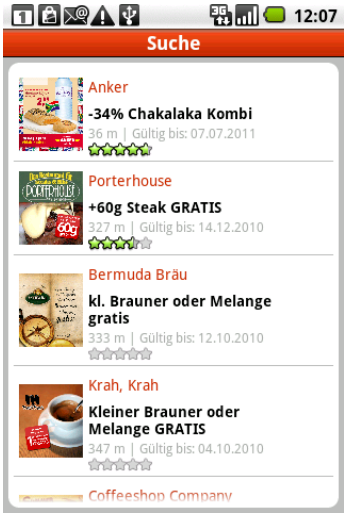


Abbildung 1.2: Gutscheinliste

Bildschirm des Endgerätes. Weiters wird eine Verfälschung und Vervielfältigung durch ein während des Einlöseprozesses generiertes Sicherheitssiegel verhindert (siehe Abbildung 1.3).

Abbildung 1.3: eingelöster Gutschein

1.2 Problembeschreibung

Das System weist bei dem vorher beschriebenen Einlöseverfahren jedoch gewisse Schwachstellen in Bezug auf die Standortfeststellung auf. Derzeit werden für die Lokalisierung folgende Technologien verwendet (in Reihenfolge ihrer Priorität):

- Global Positioning System (GPS)
- Netzwerktriangulierung
- GeoIP (Lokalisierung anhand der IP-Adresse)

Das große Problem liegt in der Ungenauigkeit dieser Technologien welche aber aus Gründen der Vollständigkeit in die Abstandsberechnung miteinfließen muss. Diese Ungenauigkeit ist eine relative Abweichung vom festgestellten Standort, welche durch einen kreisförmigen Bereich mit Radius der Abweichung und dem Standort als Zentrum dargestellt wird (siehe Abbildung 1.4), innerhalb wessen sich der tatsächliche Standort befinden kann. Der Abweichungsbereich liegt zwischen fünf Metern bis zu einem Abstand im zweistelligen Kilometerbereich. Dadurch kann eine exakte Lokalisierung und somit eine Sicherstellung, dass sich ein Kunde tatsächlich in einem Geschäftslokal des jeweiligen Unternehmens befindet, nicht mehr gewährleistet werden. Da die Standortfeststellung aber eines der zentralen Funktionalitäten des Systems und sowohl für die Rechnungslegung als auch für statistische Zwecke von enormer Bedeutung ist, kann diese Ungenauigkeit so nicht akzeptiert werden.
Im vooch-System kommt es manchmal zu sogenannten “unechten“ Einlösungen, welche sich größtenteils auf das testweise Drücken des Einlöse-Knopfes durch einen Benutzer zurückführen lassen. Diese können durch die Ungenauigkeit in der Lokalisierung jedoch nicht immer von “echten“ Einlösungen unterschieden werden und scheinen so fälschlicherweise auf der Abrechnung des Geschäftskunden auf. Von einer normalen Entwicklung stark abweichende Einlösungen werden dann meist auf Kulanz rückerstattet. Um den falschen Einlösungen vorzubeugen und so eine korrekte Abrechnung zu garantieren, soll das Lokalisierungs- bzw. Einlöseverfahren verbessert werden.

1.3 Aufgabenstellung

Aufgabe ist die Erforschung von Technologien und Entwicklung von Verfahren zur Gutscheinvalidierung und Gutscheinclearing beim Mobile Couponing, welche die Ungenauigkeit der Lokalisierung auf ein Minimum reduzieren oder

Abbildung 1.4: Ungenauigkeit in der Standortbestimmung

sogar komplett ausmerzen sollen. Dazu sollen Prozesse und mögliche Anwendungen zur Weiterentwicklung von bestehenden und vor allem verfügbaren Technologien definiert werden, wobei ein spezieller Fokus auf visuelle- (QR-Codes, Barcodes, etc.), akkustische- und funkbasierte- (NFC, Bluetooth, Wi-Fi, etc.) Verfahren gelegt werden soll. Von den erhaltenen Erkenntnissen sind Handlungsempfehlungen und Machbarkeiten abzuleiten, eine passende Variante auszuwählen und in einem Prototypen umzusetzen.

Kapitel 2

Verfügbare Lokalisierungstechnologien

Dieses Kapitel befasst sich mit den einzelnen verfügbaren Technologien, die eigenständig oder in Kombination zur Standortfeststellung verwendet werden können. Jede wird genau definiert, beschrieben und mit anderen Technologien verglichen und kombiniert. Diese Zusammenstellung soll eine gute Übersicht liefern und eine ausreichende Grundlage zur Verfahrensauswahl und Entscheidungsfindung bieten.

2.1 Global Positioning System (GPS)

GPS ist ein vom US-Verteidigungsministerium entwickeltes globales Satellitensystem zur Zeit- und Positionsbestimmung. Sein vollständiger Name lautet NAVSTAR GPS, welcher für *Nav*igational *S*atellite *T*iming and *R*anging - *G*lobal *P*ositioning *S*ystem steht.
Entwickelt wurde GPS in den Siebzigern und war vorerst nur für militärische Zwecke angedacht. Seitdem im Jahr 2000 die künstliche Signalverschlechterung abgestellt wurde (die eine zivile Verwendung einschränken sollte), ist es auch für die Zivilbevölkerung frei zugänglich und findet in vielen Bereichen Verwendung, wie:

- Seefahrt
- Luftfahrt
- Straßenverkehr
- Outdoor
- Leistungssport
- Landwirtschaft

- Mobiltelefone
- uvm.

GPS besteht prinzipiell aus drei Teilsystemen: (Bauer, 2003; Kaplan, 1996)

1. den Satelliten, welche laufend ihre Position und Zeit Richtung Erde senden,
2. den Kontrollzentren rund um den Globus, welche die Satelliten warten und koordinieren und
3. den Satellitenempfängern, welche das Signal verarbeiten und somit die dreidimensionale Position und Zeit des Benutzers bestimmen.

Wie man der obigen Aufzählung entnehmen kann, ist GPS ein Einwegesystem. Es werden also vom Satelliten nur Signale gesendet und keine empfangen. Genauso sendet der Empfänger auch nichts, sondern empfängt nur die Satellitensignale. Diese Konstellation ist vor allem auf den anfänglichen militärischen Zweck dieses Systems zurückzuführen und sollte die feindliche Ortung des Satellitenempfängers verhindern.
Für normale zivile Zwecke kann eine Genauigkeit in der Größenordnung von 13 bis hin zu 2 Metern erreicht werden. Dies hängt von mehreren Faktoren ab: (Bauer, 2003; Kaplan, 1996)

- Alter der verfügbaren Satelliten
  Aufgrund des Technologiefortschritts sind neuere Satelliten natürlich genauer als ältere
- Stellung der verfügbaren Satelliten
  Je nach Konstellation der Satelliten (Höhe, Winkel, Abstand zueinander, ...) kommt eine gewisse mathematische Ungenauigkeit dazu. Beste Voraussetzungen würden Satelliten in verschiedenen Himmelsrichtungen liefern.
- Anzahl der verfügbaren Satelliten
  Je mehr, desto besser. Theoretisch werden zur Positionsbestimmung nur drei Satelliten benötigt, aufgrund diverser Ungenauigkeiten sind aber in der Praxis mindestens vier Satelliten erforderlich.
- Störfaktoren
  Signalrauschen, Wetterverhältnisse, atmosphärische Störungen, hohe Gebäude, etc. können das Signal verschlechtern. Mittlerweile ist aber unter günstigen Bedingungen, durch neueste Technik im Empfänger, sogar eine Positionsbestimmung in geschlossenen Räumen möglich.
- Verwendung von Differential GPS (DGPS)
  Hierbei wird eine Referenzstation benutzt, welche aufgrund ihrer fixen

Position die Ungenauigkeit von Satelliten berechnet. Die daraus gewonnenen Korrektursignale werden vom DGPS-Empfänger zusätzlich in die Berechnung der Position miteinbezogen. Dadurch lässt sich eine theoretische Genauigkeit von bis zu unter einem Meter erreichen.

Neben der Position (inklusive Höhe) und der Zeit lässt sich auch die Geschwindigkeit bestimmen.
Prinzipiell genügen drei verfügbare Satelliten zur Positionsbestimmung. Da die Berechnung aber auf den Signallaufzeiten basiert und die meisten Empfänger nur über eine zu ungenaue Uhr verfügen, wird ein vierter Satellit zur Zeitbestimmung benötigt. Dass die Ortsbestimmung mit drei Satellitensignalen auskommt, hat einen recht simplen mathematischen Hintergrund. Basis der Berechnungen ist der gemessene Abstand zwischen Satellit und Empfänger. Diesen Abstand stellt man sich nun in einem dreidimensionalen Raum als Kugel vor, deren Mittelpunkt der Satellit und deren Radius der eben gemessene Abstand ist. Der Empfänger kann sich also an jedem Punkt der imaginären Kugeloberfläche befinden. Da wir uns in einem (theoretisch) 3D-Raum befinden, benötigen wir auch drei Signale (vgl. Koordinatensystem (x, y, z)), um die Position des Empfängers bestimmen zu können. Diese ergibt sich dann aus dem Schnittpunkt der drei imaginären Kugeloberflächen, also aus der Lösung eines Gleichungssystems mit drei Gleichungen, die die jeweiligen Abstände als Parameter haben.
Nachteil des Systems ist, dass der GPS-Empfänger „Sichtkontakt“ zum Satelliten benötigt und daher beispielsweise in geschlossenen Räumen nicht bzw. nur bedingt funktioniert. Dies kann die Funktionsfähigkeit in Großstädten stark beeinflussen, wenn Hochhäuser die Sicht einschränken oder es zwischen hohen Gebäuden zu Signalreflektionen kommt. Weiters kann eine längere Deaktivierung des Empfängers zu langen Positionsbestimmungszeiten führen. Je älter die zwischengespeicherten Daten sind, desto mehr Daten müssen von den Satelliten empfangen werden um die Signallaufzeiten korrekt berechnen zu können. Die dauerhafte Verbindung zwischen Empfänger und Satellit erhöht natürlich auch den Stromverbrauch und verringert die Akkuleistung bei mobilen Geräten stark.

2.2 Netzwerktriangulierung

Die Ortung über das Mobilfunknetz stellt eine Alternative zur Standortbestimmung über GPS (siehe Abschnitt 2.1) dar, welche zwar ungenauer ist aber den Vorteil hat, dass im oder am Endgerät kein spezielles Hardwareteil (=> GPS-Empfänger) benötigt wird. Sie tritt aber nicht nur als Konkurrent oder Mitbewerber auf, sondern wird auch als unterstützende Technologie zur GPS-Ortung (siehe Abschnitt 2.3) verwendet. Die Funkzellenortung basiert darauf, dass jedes Mobilfunknetz in sogenannte Zellen unterteilt ist. Dabei ist jede Zelle eindeutig durch ihre International Mobile Subscriber Identity

(IMSI) identifizierbar und hat einen fixen Standort. Die IMSI besteht aus folgenden Elementen: (3rd Generation Partnership Project, 2009)

- *Mobile Country Code (MCC)*
  Die ersten drei Zahlen der IMSI kennzeichnen das Land, in welchem sich die Mobilfunkzelle befindet.

- *Mobile Network Code (MNC)*
  Der MNC identifiziert den Netzwerkbetreiber eindeutig in einem Land und ordnet die Zelle diesem zu. Er besteht aus den nächsten zwei oder drei Ziffern (nur wenige Länder verwenden einen dreistelligen Code) der IMSI.

- *Mobile Station Identification Number (MSIN)*
  Die MSIN kennzeichnet eine einzelne Zelle innerhalb eines Mobilfunknetzes.

Diese drei Nummern ergeben zusammen eine weltweit eindeutige ID für jede Zelle. Jede dieser Zellen wird von einer Antenne bzw. Basisstation ausgestrahlt, deren Standort bekannt ist. Somit kann auch jeder Zelle ein ungefährer Standortbereich zugeordnet werden. Die logische Verknüpfung zwischen Zelle und Endgerät wird geschaffen, sobald ein Mobiltelefon in deren Empfangsbereich kommt und sich bei einer Sendestation anmeldet.
Es gibt mehrere Verfahren zur Standortbestimmung innerhalb eines Funknetzes. Hier werden die drei meist Verbreiteten angeführt und kurz erklärt. Die erste Variante stellt die einfachste dar, welche ohne Zusatzhardware auskommt, während hingegen die anderen zwei zusätzliche Hardware benötigen, was aber auch zu einer erhöhten Genauigkeit führt.

- Bei der simpelsten Variante der Funkzellenortung wird für den Standort einfach über die Zelle, in welcher das mobile Endgerät angemeldet ist, ermittelt und dem Standort der Zelle gleichgesetzt. Vorteil dieser Variante ist die Einfachheit, welche es erlaubt, ohne Zusatzgeräte auszukommen. Nachteil ist die relativ hohe Ungenauigkeit, welche vor allem vom Ausstrahlungsbereich der Basisstation und der Zellendichte abhängt. Im Stadtbereich liegt die Genauigkeit im dreistelligen Meterbereich, wohin diese in ländlichen Bereich hingegen sogar mehrere Kilometer betragen kann. (3rd Generation Partnership Project, 2008b)

- Das etwas komplexere Verfahren kommt dem bei GPS schon nahe und basiert ebenfalls auf der Messung von Signallaufzeiten. Dabei kann über die Laufzeit der ungefähre Abstand zur Basisstation berechnet und somit der Ortungsbereich eingeschränkt werden. Für die Messung wird allerdings zusätzliche Hardware benötigt, die so genannten LMUs[1]. Das Endgerät bleibt hiervon aber unberührt. Diese Methode

[1] Location Measurement Units

erlaubt eine Genauigkeit von bis zu unter hundert Metern. (3rd Generation Partnership Project, 2008a)

- Das dritte Verfahren ist eine Erweiterung der vorherigen Methode und erfordert auch am Endgerät eine Erweiterung, um Messungen durchzuführen und die Messdaten übertragen zu können. Hier werden nicht nur die Signallaufzeiten zu einer Station, sondern gleich zu mehreren Stationen gemessen. Genauso wie bei GPS gilt auch hier: je mehr, desto besser. Ähnlich wie bei GPS kann hier aufgrund der Daten von mehreren Basisstationen ein Schnittpunkt berechnet und somit der Standort trianguliert werden (siehe Abschnitt 2.1). Dies erlaubt eine Genauigkeit von bis zu 25 Metern. (3rd Generation Partnership Project, 2008a)

Das Verfahren der Netzwerktriangulierung findet schon seit Jahren Anwendung für verschiedenste Zwecke, angefangen von Marketingerscheinungen wie Überwachung der Kinder, Ehepartner, etc. bis hin zu sicherheitstechnischen Systemen wie Notrufortung, Strafverfolgung und Ähnlichem.
Wie auch GPS ist die Netzwerktriangulierung gewissen Störfaktoren, welche die Genauigkeit beeinträchtigen, unterworfen.

- Signallaufzeitverzögerung durch eingeschränkten Sichtkontakt
- Signalreflektionen
- Signalbeugungen
- etc.

Vorteil dieses Systems gegenüber GPS ist vor allem die bessere Erreichbarkeit, denn sofern man mit dem Mobiltelefon Empfang hat, kann auch die eigene Position bestimmt werden. Nachteil ist allerdings die Ungenauigkeit, vor allem in ländlichen Gebieten, wo die Antennendichte nicht allzu hoch ist.

2.3 Assisted Global Positioning System (A-GPS)

Wie bereits in Abschnitt 2.1 erwähnt, ist GPS so konzipiert, dass es auf eine ständige Verbindung zum Satelliten angewiesen ist. Um eine stör- und unterbrechungsfreie Datenübertragung zum GPS-Empfänger zu gewährleisten sollte außerdem ein “freier Sichtkontakt“ zu den Satelliten bestehen. Dies führt auf Mobiltelefonen vor allem dann zu Problemen, wenn

- der GPS-Empfänger länger deaktiviert war und der Standort gewechselt wurde.
  Es kommt zu einem sprunghaften Ortswechsel wodurch die neuen Satellitenlaufbahnen erst übertragen werden müssen. Je länger der Empfänger inaktiv war und je weiter sich das Endgerät bewegt hat, umso

mehr Daten müssen übertragen werden, was zu einer verzögerten Berechnung des neuen Standortes führt. In Fachkreisen wird diese Zeit als "Time To First Fix[2]" (TTFF) bezeichnet.

- die direkte Sicht zum Satelliten eingeschränkt oder ganz versperrt ist. Durch atmosphärische Störungen (Gewitterwolken, ...), hohe Gebäude und Ähnliches kann es zur Störung des GPS-Signals kommen und führt zu Ungenauigkeiten in der Berechnung der Position.

Aus diesem Grund wurde Assisted GPS ins Leben gerufen. Diese Technologie ist eine Kombination der beiden vorherigen (2.1 GPS und 2.2 Netzwerktriangulierung) und vereint die Vorteile beider um deren Nachteile zu dezimieren. Dabei werden Hilfsdaten zur Positionsbestimmung durch GPS über ein Fremdnetz übertragen. In diesem konkreten Fall werden die Hilfsdaten (grober Standort, Satellitenlaufbahninformationen, etc.) über das schnellere Mobilfunknetz übertragen. Dadurch wird der GPS-Empfänger entlastet (da die Assistenzinformationen nicht mehr über das langsamere GPS-Band übertragen werden müssen) und die Berechnung des Standortes wird beschleunigt.
Um sich ein genaueres Bild des Geschwindigkeitsvorteiles machen zu können, sind der Tabelle 2.1 ein paar technische Daten zu entnehmen.

	GPS	A-GPS	
	L1	GSM	UMTS
Frequenzband	1575,42 MHz	824 - 1990 MHz	824 - 2170 MHz
Reichweite	20.200 km	35 km	2 km
Datenrate	50 bit/sec	13 - 220 kbit/sec	384 kbit/sec - 7,2 Mbit/sec

Tabelle 2.1: Vergleich der Übertragungsgeschwindigkeiten zwischen GPS und A-GPS (Bauer, 2003; Kaplan, 1996; Joeckel et al., 2008; Schnabel, 2008; Walke, 2001)

L1 bezeichnet die erste von derzeit insgesamt drei Frequenzen (L1, L2 und L5) und wird zur Übertragung des zivilen GPS-Signals, des so genannten C/A-Codes (Coarse/Acquisition), verwendet.
GSM steht für Global System for Mobile Communications und ist das weltweit verbreitetste Mobilfunknetz und Standard der zweiten Generation (2G). Das Frequenzband reicht von 380 bis 1990 MHz und ist in diverse Gruppen aufgeteilt, welche wiederum das ihnen zugewiesene Frequenzband für Up- und Downlink aufspalten. Das tatsächlich verwendete Frequenzband erstreckt sich von 824 bis 1990 MHz. Alle anderen Frequenzen sind vom Mobilfunk unberührt oder werden nur vereinzelt verwendet. GSM selbst erlaubt

[2]als Fix bezeichnet man das vom GPS-Empfänger erhaltene Positionsupdate

eine Übertragungsgeschwindigkeit von bis zu 13 kbit/sec. Die Standarderweiterungen HSCSD[3] und GPRS[4] erlauben eine Steigerung auf die Geschwindigkeit eines veralteten 56k-Modems, während EDGE[5] sogar 220 kbit/sec ermöglicht. (Schnabel, 2008; Walke, 2001)
Das Universal Telecommunications System (UMTS) wurde 2001[6] eingeführt und ist ein Standard der dritten Mobilfunkgeneration (3G). Das Funkband reicht von 830 bis 2170 MHz, wobei tatsächlich nur die Frequenzen von 824 bis 2170 MHz genutzt werden (ähnlich wie bei GSM), abhängig von Land und Kontinent. UMTS ermöglicht eine Datenübertragungsrate von 384 kbit/sec, welche aber durch Erweiterungen wie HSDPA[7] und HSUPA[8] auf einen tatsächlichen Wert von 7,2 Mbit/sec gesteigert werden kann. (Schnabel, 2008; Walke, 2001)

Assisted GPS bringt also im Vergleich zu GPS einen klaren Geschwindigkeitsvorteil in der Berechnung des Standortes (zurückzuführen auf die schnellere Verfügbarkeit der (Hilfs-)Daten). Durch die Verwendung der neuesten Mobilfunktechnologien lässt sich bei der Datenübertragung eine derzeitige Verbesserung um den Faktor 100.000 erreichen, was die Zeit bis zum ersten Fix (TTFF), vor allem nach längerer Inaktivität, erheblich verkürzt.
Während die meisten modernen Mobiltelefone bereits über einen GPS-Empfänger verfügen, ist A-GPS derzeit noch nicht so verbreitet, aber immer mehr im kommen.

2.4 GeoIP

GeoIP ist ein Teilbereich des Geotargeting, wo es darum geht, Inhalt anhand geografischer Daten auszuwählen und zu präsentieren. Als simples Beispiel kann die Landesauswahl auf der Homepage eines länderübergreifend agierenden Unternehmens herangezogen werden. GeoIP bietet die Möglichkeit Standortinformationen, wie

- Koordinaten (Breiten- und Längengrad)
- Stadt
- Bundesland, Landkreis, Kanton, etc.
- Land

[3] High Speed Circuit Switched Data
[4] General Packet Radio Service
[5] Enhanced Data Rates for GSM Evolution
[6] Das Unternehmen Manx Telecom nahm damals das weltweit erste UMTS Netz auf der Isle of Man in Betrieb
[7] High Speed Downlink Packet Access
[8] High Speed Uplink Packet Access

- Kontinent
- Providerinformationen
- uvm.

anhand der IP-Adresse des Clients zu bestimmen. Kurz gesagt bedeutet dies, dass jeder IP Adresse ein Standort zugeordnet ist. Jedem Teilnehmer/Endgerät(Computer, Smartphone, etc.) ist eine Internet Protokoll (IP) Adresse zugeordnet. Die Zuordnung wird über den jeweiligen Internet Service Provider (ISP) geregelt und verwaltet. Dabei wird jedem Endgerät bei der Einwahl oder Verbindungsherstellung ins Internet eine einzigartige Adresse zugeordnet, wodurch sich auch jeder Teilnehmer eindeutig identifizieren und über diese auch erreichen lässt. Jedem ISP ist ein Adressraum zugewiesen, welcher zu seiner freien Verfügung steht. Es gibt zwei Versionen von IP Adressen:

- *Version 4 (IPv4)* (Information Sciences Institute, 1981)
  IPv4 ist die am weitesten verbreitete und meist verwendete Version des Internet Protokolls. Eine Adresse besteht aus insgesamt 32 Bit, welche in vier Gruppen zu je einem Oktett aufgeteilt sind (siehe Tabelle 2.2).

Format	aaaaaaaa.bbbbbbbb.cccccccc.dddddddd
Beispiel	11000000.10101000.00000000.00000001

Tabelle 2.2: IPv4 in Binärdarstellung

Um diese Adressen aber auch für jeden Menschen lesbar zu machen, werden diese vier Oktette meist in dezimaler Schreibweise dargestellt, wodurch das obige Beispiel aus Tabelle 2.2 in Tabelle 2.3 dargestellt wird.

Format	aaa.bbb.ccc.ddd
Beispiel	192.168.0.1

Tabelle 2.3: IPv4 in Dezimaldarstellung

Wie bereits vorher erwähnt, ist das Internet in verschiedene Adressbereiche oder Subnetzwerke aufgeteilt. Dies geschieht durch die sogenannte Subnet-Maske, welche angibt, welche Bits zur Identifizierung des Netzwerks und welche zum Client innerhalb des Netzwerks gehören. Die Netzmaske besteht aus gleich vielen Bits wie die Adresse, ist ebenfalls in vier Oktetts aufgeteilt und wird gleich dargestellt. Die gebräuchlichste Darstellung der Netzmaske ist allerdings folgende:

192.168.0.1/24. Die Zahl 24 bezeichnet hierbei die Anzahl der Bits, welche für das Netzwerk verwendet werden, in diesem Fall also die ersten drei Oktetts. Diese Zahl muss aber nicht immer ein vielfaches von 8 sein, sondern es ist jede beliebige Zahl möglich, sofern noch Bits für die Clients übrig bleiben. Zur Illustration der Subnetzmaske ist der Tabelle 2.4 ein kleines Rechenbeispiel zu entnehmen.

IP Adresse (IP)	192.168.7.112/18	11000000 10101000 00000111 01110000
Netzmaske (M)	255.255.3.0	11111111 11111111 00000011 00000000
Netzwerk (IP AND M)	192.168.004.000	11000000 10101000 00000100 00000000
Client (IP AND NOT M)	3.112	00000000 00000000 00000011 01110000

Tabelle 2.4: IPv4 Subnetzmaske: Rechenbeispiel

Mit Version 4 sind insgesamt 2^{32}, also 4.294.967.296 verschiedene Adressen darstellbar. Damals war noch nicht klar, dass dies bei dem ständigen Wachstum des Internets und der Weltbevölkerung (die derzeit bei über acht Milliarden Menschen liegt) zu einem Engpass führen wird, woraus IPv6 entstand. Derzeit wird der zu kleine Adressraum mit Diensten wie NAT[9] oder Proxy-Servern virtuell erweitert, welche unter anderem auch die Ortung von Endgeräten einschränken, da diese dadurch keine eigene öffentliche Adresse haben. Mehr dazu jedoch später.

- *Version 6 (IPv6)* (Deering et al., 1998)
  IPv6 ist der offizielle Nachfolger von IPv4 im Internet und hebt unter anderem das Problem des zu kleinen Adressraumes auf. Es werden nun acht Gruppen zu je 16 Bit verwendet, was einen Adressraum von $2^{128} \approx 3,4 * 10^{38}$ Adressen ermöglicht. Dargestellt werden diese in hexadezimaler Notation. Die Subnetzmaske wird nur noch in der vorher erwähnten "/"-Notation angegeben, wobei diese eine beliebige Zweierpotenz ist. Zur Veranschaulichung ist der Tabelle 2.5 ein Beispiel in hexadezimaler IPv6 Notation zu entnehmen.

IP Adresse (IP)	2010:2809:0f00:beef:00c0:00a8:0000:0075/64
Netzwerk ID	2010:2809:0f00:beef::/64
Client ID	00a8:0000:0075

Tabelle 2.5: IPv6 in hexadzimaler Notation

Der immens große Adressraum von IPv6 sollte die nächsten Jahrzehnte

[9] Network Address Translation

ausreichen, um jeden einzelnen Internetteilnehmer eindeutig identifizieren zu können (dies dachte man sich bei der Einführung von IPv4 aber auch). Dadurch wird auch der von IPv4 verwendete Dienst NAT, welcher zur Überbrückung der Adressenknappheit diente und Adressen eines Netzes in Adressen eines anderen Netzes übersetzte, überflüssig und ein Problem von GeoIP eliminiert. Jedoch wird ab Version 6 Mobile IP verwendet, ein Dienst, welcher es ermöglicht, dass ein Endgerät immer unter der gleichen Adresse erreichbar ist, egal ob es sich gerade im Heimnetz oder in irgend einem anderen Netzwerk befindet. Erreicht wird dies durch einen "Home Agent", welcher das Endgerät im Heimnetzwerk sozusagen vertritt und bei welchem es sich aus dem Fremdnetz aus anmeldet, um weiterhin unter der selben Adresse erreichbar zu sein. Dies erschwert die Lokalisierung anhand der IP wieder, da sich das Endgerät nicht am eigentlichen Standort der IP befindet.

Da sich IP-Adressen von Endgeräten ständig ändern ($\rightarrow$ DHCP[10]) und somit auch der Standort der jeweiligen Adresse, ist es sehr wichtig, dass die Daten laufend auf den neuesten Stand gebracht werden. Diese, bei einem Adressraum von über vier Milliarden Adressen nicht unbeachtliche, Aufgabe wird mit Hilfe von speziellen Algorithmen, von sogenannten "IP Spiders", erledigt. Dies sind Dienste, welche den Adressraum analysieren, Informationen (Standort, ...) darüber sammeln und in einer Datenbank ablegen.
GeoIP stößt bei den oben erwähnten Diensten wie NAT, Proxy oder Mobile IP aber an seine Grenzen. Das Problem liegt vor allem daran, dass die IP, mit welcher die Anfragen des Clients an das Internet gesendet werden, nicht die IP des Clients sondern zum Beispiel die des Proxy Servers ist. Dadurch wird der Client am Standort des vor ihm geschaltenen Servers und nicht an seinem eigenen lokalisiert. Dieses Szenario ist kein seltenes, da viele Mobilfunkbetreiber ihre Kunden über einen Proxy-Server ins Internet leiten, welcher auch im Ausland stehen kann.
Die Lokalisierung mittels GeoIP kann also im schlimmsten Fall sogar mehrere hundert Kilometer daneben liegen, was bei sich ständig bewegenden mobilen Endgeräten wie Smartphones und Ähnlichem ständig der Fall ist. Dadurch eignet sich GeoIP nur zur groben Standortfeststellung, beispielsweise um festzustellen in welchem Land sich der Benutzer befindet um ihm dann den entsprechenden Inhalt zur Verfügung zu stellen.

2.5 Strichcode

Die hier angeführte Lokalisierungsart mittels eines eindimensionalen Strichodes (engl. Barcode) ist eine eher etwas ungewöhnliche aber durchaus funkti-

[10] Dynamic Host Configuration Protocol: ein Dienst von IPv4, welcher eine automatische Adresszuteilung an die Clients ermöglicht

onsfähige Möglichkeit. Die Idee besteht darin, signifikante Orte oder Positionen (wie zum Beispiel ein Geschäftslokal) mit einem eindeutigen Strichcode zu versehen. Wird dieser mit dem mobilen Endgerät eingescannt, weiß man genau, wo er sich gerade befindet. Dazu jedoch später mehr.
Der Barcode entsprang eigentlich dem Warenhandel und wurde gemeinsam mit dem Aufschwung der Supermarktketten groß. Ziel war es, Artikel mit einem Code zu versehen, um sie damit elektronisch zu identifizieren, organisieren und verwalten zu können. Erste Versuche mit dem eindimensionalen Strichcode gab es bereits in den Fünfzigern, durchgesetzt hat sich dieser aber erst auf Druck der amerikanischen Supermarktkette "Wal-Mart" in den Siebzigern. Es entstanden verschiedene Codearten, welche alle eigens nach ISO[11]/IEC[12] genormt wurden. Gemeinsam haben sie jedoch alle, dass sie aus einer linear angeordneten Folge von Strichen bestehen, wobei die Breite der Striche und die Abstände dazwischen ausschlaggebend für den codierten Inhalt sind. Mit einigen wenigen Ausnahmen wird dieser Inhalt auch in menschlich lesbarer Form unter dem Barcode angeführt. Je nach Art können Ziffern, alphanumerische Zeichen und Sonderzeichen codiert werden. Die verbreitetsten und/oder für den Zweck dieser Arbeit entsprechenden Arten wurden ausgewählt und in den folgenden Abschnitten genauer beschrieben.

2.5.1 EAN - European Article Number / GTIN - Global Trade Item Number

Die EAN (seit 2009 offiziell GTIN) ist in ISO/IEC 15420 genormt und kann die Ziffern 0-9 darstellen. Es gibt zwei Arten:

- *EAN-13*
  Sie besteht aus 13 Ziffern (siehe Abbildung 2.1), welche in folgende Gruppen aufgeteilt werden: (Lenk, 2000; Rosenbaum, 1997)

  1. einem dreistelligen Länderpräfix
  2. einer vier- bis sechsstelligen Unternehmensnummer
  3. einer fünf- bis dreistelligen Artikelnummer
  4. einer Prüfziffer

- *EAN-8 / GTIN Kurznummer*
  Sie besteht aus acht Ziffern (siehe Abbildung 2.2), welche in folgende Gruppen aufgeteilt werden: (Lenk, 2000; Rosenbaum, 1997)

  1. einem zwei- bis dreistelligen Länderpräfix
  2. einer fünf- bis vierstelligen Artikelnummer
  3. einer Prüfziffer

[11] International Organization for Standardization
[12] International Electrotechnical Commission

Abbildung 2.1: EAN-13 (http://barcode.tec-it.com/barcode-generator.aspx)

Abbildung 2.2: EAN-8 (http://barcode.tec-it.com/barcode-generator.aspx)

Verwaltet werden die EANs von der Global Standards One (GS1) Organisation, welche einen verwechslungsfreien Einsatz garantiert. Es gibt allerdings auch eine Möglichkeit die EANs in einem abgegrenzten Raum (beispielsweise unternehmensintern) frei zu verwenden. Hierzu muss die Nummer lediglich mit der Ziffer 2 beginnen, die restlichen Ziffern stehen frei zur Verfügung.
Kodiert wird jede Ziffer mit sieben Bereichen, wobei jeder dieser Bereiche schwarz oder weiß sein kann mit der Einschränkung von maximal vier aufeinander folgenden gleichen Bereichen. Diese Bereiche repräsentieren die codierte Darstellung der Ziffer (0 = Weiß, 1 = Schwarz), somit besteht jede aus sieben Bits. Dabei werden die Ziffern der linken Hälfte immer so kodiert, dass sie mit einem leeren Bereich, und die der rechten so, dass sie immer mit einem vollen Bereich beginnen. Zusätzlich kann jede Ziffer der linken Hälfte mit gerader oder ungerader Parität kodiert werden. Die der rechten Hälfte sind immer mit gerader Parität kodiert. Das genaue Schema ist der Abbildung 2.3 zu entnehmen. Durch dieses aufwändige aber durchaus effektive Verfahren ist es vollkommen egal, von welcher Richtung der Barcode gescannt wird, da die linke Hälfte immer mit einer 0, also einem weißen Bereich, und die rechte Hälfte immer mit einer 1, einem schwarzen Bereich beginnt.(Lenk, 2000; Rosenbaum, 1997)

Jede EAN beginnt und endet mit einem fixen Randzeichen, welches dem binären Wert 101 entspricht. In der Mitte befindet sich ein Trennzeichen mit dem Wert 01010. (Lenk, 2000) Diese Zeichen werden optisch durch längere Striche hervorgehoben (siehe Abbildung 2.4).
Durch diese Codierung ergibt sich für die EAN-13 eine fixe Länge von 102

Ziffer	Muster			Liniendicken		Kodierung der 13. Ziffer
	links		rechts	rechts,		
	ungerade	gerade	(gerade)	li. ung.	li. ger.	
0	0001101	0100111	1110010	3211	1123	UUUUUU GGGGGG
1	0011001	0110011	1100110	2221	1222	UUGUGG GGGGGG
2	0010011	0011011	1101100	2122	2212	UUGGUG GGGGGG
3	0111101	0100001	1000010	1411	1141	UUGGGU GGGGGG
4	0100011	0011101	1011100	1132	2311	UGUUGG GGGGGG
5	0110001	0111001	1001110	1231	1321	UGGUUG GGGGGG
6	0101111	0000101	1010000	1114	4111	UGGGUU GGGGGG
7	0111011	0010001	1000100	1312	2131	UGUGUG GGGGGG
8	0110111	0001001	1001000	1213	3121	UGUGGU GGGGGG
9	0001011	0010111	1110100	3112	2113	UGGUGU GGGGGG

Abbildung 2.3: EAN Kodierungstabelle(Wikipedia, a)

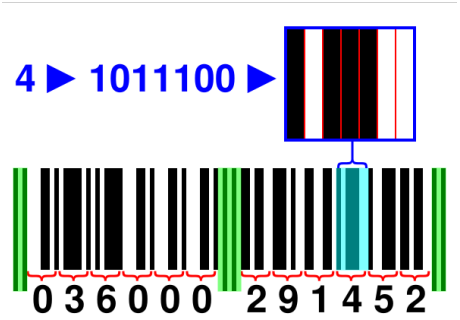


Abbildung 2.4: EAN Kodierungsbeispiel(Wikipedia, a)

Bereichen (= 2 * 3 Randbereiche + 5 Trennbereiche + 13 * 7 Ziffernbereiche) und für die EAN-8 von 67 Bereichen (= 2 * 3 Randbereiche + 5 Trennbereiche + 8 * 7 Ziffernbereiche), wobei die letzten sieben Bereiche auf die Prüfziffer entfallen, woraus sich zwölf beziehungsweise sieben nutzbare Ziffern ergeben.
Die Berechnung der Prüfziffer erfolgt durch eine einfache Formel. Hierfür werden alle Ziffern, beginnend mit der letzten, abwechselnd mit 3 und mit 1 multipliziert und die Produkte aufsummiert. Zieht man nun diese Summe vom nächsten vielfachen von 10 ab, so erhält man die Prüfziffer. Zur Illustration folgt nun die Berechnung der Prüfziffer aus Abbildung 2.2:

EAN: $9031101 - 7$
Summe: $1 * 3 + 0 * 1 + 1 * 3 + 1 * 1 + 3 * 3 + 0 * 1 + 9 * 3 = 43$
Prüfziffer: $50 - 43 = 7$

Vereinfacht kann man die Formel für die Berechung der Prüfziffer wie folgt niederschreiben:

$$(10 - (\quad 1 * (x_1 + x_3 + x_5 + x_7 + x_9 + x_{11}) + \\ 3 * (x_2 + x_4 + x_6 + x_8 + x_{10} + x_{12}) \quad) mod 10 \quad) mod 10$$

Tabelle 2.6: Formel zur Berechnung der EAN-13-Prüfziffer (Lenk, 2000, 2004)

2.5.2 UPC - Universal Product Code

Der UPC war eigentlich der erste standardisierte und genormte Barcode und wurde bereits drei Jahre vor dem EAN eingeführt. Er codiert ebenfalls die Ziffern 0-9, verfügt aber nur über 12 Stellen (siehe Abbildung 2.5). Diese sind wie folgt aufgebaut:(Lenk, 2000; Rosenbaum, 1997)

1. einem Number System Character, welcher angibt, um welche Produktart es sich handelt (siehe Tabelle 2.7)

0, 6, 7	allgemeiner Produktcode
2	abzuwiegende Produkte
3	Produkte aus dem Gesundheitswesen (Medikamente, etc.)
4	interne Codes ohne Spezifikation
5	Kupons
1, 8, 9	nicht definiert

Tabelle 2.7: Number System Character

2. fünf Ziffern, welche den Hersteller kennzeichnen (vergeben von der UCC[13])
3. fünf Ziffern, welche das Produkt kennzeichnen (vom Hersteller verwaltet)
4. einer Prüfziffer

[13] Uniform Code Council

UPC wird in fünf Klassen unterteilt: A, B, C, D und E. Die Klassifikation UPC-A entspricht der gerade beschriebenen und ist am verbreitetsten. B, C und D sind zwar spezifiziert und normiert, werden aber nicht verwendet. Die Klasse UPC-E ist eine Modifikation der Klasse A. Sie beinhaltet eine Unterdrückung von Nullen und komprimiert so die kodierten Daten, verkürzt den Code also.(Lenk, 2000; Rosenbaum, 1997)
Die Berechnung der Prüfziffer erfolgt gleich wie bei EAN. UPC hat zwar eine Stelle weniger, aber kann durch die vielen Gemeinsamkeiten durch ein einfaches Anfügen einer führenden Null in eine gültige EAN Nummer umgewandelt werden. Da UPC vor allem in Amerika stark zu tragen kommt und durch die einfache Konvertierung von UPC zu EAN verwenden viele international agierende Unternehmen den Universal Product Code.

Abbildung 2.5: UPC (http://barcode.tec-it.com/barcode-generator.aspx)

2.5.3 ISBN - International Standard Book Number / ISSN - International Standard Serial Number

Die Internationale Standardbuchnummer (siehe Abbildung 2.6) dient "(...) zur eindeutigen Kennzeichnung von Büchern und anderen selbstständigen Veröffentlichungen mit redaktionellem Anteil, wie beispielsweise Multimedia-Produkte und Software."(Wikipedia, b). Sie ist genormt nach ISO 2108 und bestand ursprünglich aus 10 Ziffern inklusive einer Prüfziffer. Die immer größer werdende Bedeutung von EAN-13 führte schlussendlich zur Einführung der ISBN-13, einer dreizehn-stelligen internationalen Standardbuchnummer welche in das EAN-13-System integriert wurde. Da die ersten zwei bis drei Stellen des EAN für den Länderpräfix stehen (siehe Punkt *EAN - European Article Number*) wurde ein fiktives "Buchland" geschaffen, welches durch die Präfixe 978 und 979 gekennzeichnet wird. Die restliche ISBN-13 ist wie folgt aufgebaut: (Lenk, 2000; Rosenbaum, 1997)

1. Ländernummer
   Diese kennzeichnet ein Land oder einen Sprachraum und hat keine fixe Länge (abhängig vom Sprachraum). Hat ein Land mehrere Sprachräume (zum Beispiel die Schweiz), so werden diesem für jeden Sprachraum eine eigene Nummer zugewiesen.

2. Verlagsnummer
   Dies ist eine dem Verlag von einer ISBN-Behörde eindeutig zugewiesene Nummer. Die Länge ist ebenfalls variabel und abhängig von der Ländernummer (je Land/Sprachraum sind nur gewisse Bereiche gültig; siehe http://www.isbn-international.org/page/ranges).

3. Bandnummer
   Diese Nummer wird vom Verlag selbst vergeben (jeder Verlag hat einen selbstverwalteten Nummernbereich) und ist in der Länge ebenfalls variabel (abhängig von der Länder- und Verlagsnummer und dem zugewiesenen Bereich). In Summe hat jedoch jede ISBN-13 eine dreizehnstellige Ziffernfolge.

4. Prüfziffer
   Diese entspricht der Prüfziffer einer EAN-13.

Abbildung 2.6: ISBN (http://barcode.tec-it.com/barcode-generator.aspx)

Die Internationale Standardseriennummer (siehe Abbildung 2.7) ist das Nummerierungssystem für Zeitschriften und Schriftreihen und ist nach ISO 3297 normiert. Sie besteht aus acht Ziffern (inklusive der Prüfziffer) welche durch einen Bindestrich, der der besseren Lesbarkeit und als Unterscheidungsmerkmal dient, in zwei Gruppen zu je vier Ziffern aufgeteilt ist. Im Gegensatz zur ISBN gliedert sich die ISSN nicht in verschiedene Teile, welche beispielsweise das Land kennzeichnen. Vergeben werden die Nummern vom ISSN-Netzwerk, welches sich aus einzelnen nationalen ISSN-Stellen zusammensetzt.
Die ISSN existiert ebenfalls im EAN-13-System. Dabei wird die Nummer (ähnlich wie bei der ISBN) mit einem Präfix versehen, welches 977 lautet. Die letzten zwei ausstehenden Ziffern (vor der Prüfziffer) werden zur Kennzeichnung von Spezialausgaben verwendet und sind im Normalfall jeweils 0.

2.5.4 Code39

Der Code39 ist ein nach ISO/IEC 16388 genormter Strichcode, welcher es erlaubt alphanumerische Zeichen zu kodieren. Verbreitet ist dieser vor allem im industriellen Bereich und in der Pharmaindustrie. Der Zeichensatz umfasst

Abbildung 2.7: ISSN (http://barcode.tec-it.com/barcode-generator.aspx)

0-9, A-Z und die Sonderzeichen “$“, “%“, “/“, “+“, “.“, “-“, “ “ (Leerzeichen) und “*“ (reserviert für das Stoppzeichen). Die Anzahl der kodierten Zeichen ist hierbei unbeschränkt und der Code lässt sich ebenfalls von beiden Seiten lesen. Die Bezeichnung Code39 ist auf die ursprüngliche Anzahl von 39 kodierten Zeichen zurückzuführen (die Sonderzeichen waren auf “.“, “,“ und “*“ beschränkt). (Lenk, 2000; Rosenbaum, 1997) Weiters gibt es ein optionales Prüfzeichen, auf das später noch näher eingegangen wird.
Der Strichcode hat eine variable Länge, verfügt aber über drei fixe Bereiche: (Lenk, 2000; Rosenbaum, 1997)

1. dem Startzeichen, welches durch ein “*“ symbolisiert wird
2. einer Trennlücke zwischen jedem kodierten Zeichen
3. dem Stoppzeichen, welches durch ein “*“ symbolisiert wird

Jedes Zeichen besteht dabei aus neun Elementen (drei breiten und sechs schmalen), welche insgesamt 5 vertikale Striche und 4 Lücken darstellen und jedes Zeichen mit einem Strich beginnt und mit einem Strich endet. Die Kodierung der verfügbaren Zeichen ist der Tabelle 2.8 zu entnehmen.

Wie bereits erwähnt, kann jedem Code39 Strichcode ein optionales Prüfzeichen zur Korrektheitsprüfung angehängt werden. Dieses wird nach dem letzten Zeichen und vor dem Stoppzeichen eingefügt und wird auf die selbe Weise wie die anderen Zeichen kodiert. Die Berechnung des Prüfzeichens basiert auf einer Modulo 43 Division der Summe aller Zeichenwerte. Hierzu muss zuerst jedem Zeichen ein Wert zugeordnet werden, welche der Tabelle 2.11 zu entnehmen sind. Die Formel für die Berechnung wird in Tabelle 2.9 angeführt.

Dem errechneten Wert wird dann anhand der Tabelle 2.11 ein Zeichen zugeordnet und zusammen mit den restlichen Zeichen kodiert. Zur Veranschaulichung wird in Tabelle 2.10 das Prüfzeichen des Beispiels aus Abbildung 2.8 berechnet.

Zeichen	Kodierung	Zeichen	Kodierung
0	slsLSlSls	M	SlSlslsLs
1	SlsLslslS	N	slslSlsLS
2	slSLslslS	O	SlslSlsLs
3	SlSLslsls	P	slSlSlsLs
4	slsLSlslS	Q	slslslSLS
5	SlsLSlsls	R	SlslslSLs
6	slSLSlsls	S	slSlslSLs
7	slsLslSlS	T	slslSlSLs
8	SlsLslSls	U	SLslslslS
9	slSLslSls	V	sLSlslslS
A	SlslsLslS	W	SLSlslsls
B	slSlsLslS	X	sLslSlslS
C	SlSlsLsls	Y	SLslSlsls
D	slslSLslS	Z	sLSlSlsls
E	SlslSLsls	-	sLslslSlS
F	slSlSLsls	.	SLslslSls
G	slslsLSlS	(Leerzeichen)	sLSlslSls
H	SlslsLSls	*	sLslSlSls
I	slSlsLSls	$	sLsLsLsls
J	slslSLSls	/	sLsLslsLs
K	SlslslsLS	+	sLslsLsLs
L	slSlslsLS	%	slsLsLsLs

Tabelle 2.8: Code39 Kodierung (Lenk, 2000; Rosenbaum, 1997)

(s...dünner Strich, S...dicker Strich, l...dünne Lücke, L...dicke Lücke)

$$\sum_{i=0}^{n} wert(z_i) mod 43$$

Tabelle 2.9: Formel zur Berechnung des Code39-Prüfzeichens

2.5.5 Code128

Der Code128 ist Nachfolger des Code39 und zeichnet sich vor allem durch seine viel höhere Informationsdichte aus, die sich aus der verwendeten Kodierung ergibt. Definiert ist dieser nach ISO/IEC 15417. Jedes Zeichen besteht aus insgesamt 11 Bereichen, welche entweder schwarz (log. 1) oder weiß (log. 0) sein können und maximal vier gleiche Bereiche aufeinander folgen dürfen. Dadurch werden ähnlich wie bei Code39 verschiedene Striche und Lücken geformt und es ergeben sich insgesamt vier Strich- und vier Lückenbreiten. Aneinander gereiht ergibt (fast) jede Kombination die Kodierung eines Zei-

V	O	O	C	H	+	T	U	G	R	A	Z	-	2	0	1	0		
31	24	24	12	17	41	29	30	16	27	10	35	36	2	0	1	0		
																	$\sum$	335
																	mod 43	34
																		Y

Tabelle 2.10: Beispiel zur Berechnung des Code39-Prüfzeichens

Zeichen	Wert	Zeichen	Wert
0	0	M	22
1	1	N	23
2	2	O	24
3	3	P	25
4	4	Q	26
5	5	R	27
6	6	S	28
7	7	T	29
8	8	U	30
9	9	V	31
A	10	W	32
B	11	X	33
C	12	Y	34
D	13	Z	35
E	14	-	36
F	15	.	37
G	16	(Leerzeichen)	38
H	17	$	39
I	18	/	40
J	19	+	41
K	20	%	42
L	21		

Tabelle 2.11: Code39 Prüfziffernwerte (Lenk, 2000; Rosenbaum, 1997)

chens. (Lenk, 2000; Rosenbaum, 1997)
Code128 kodiert beinahe den vollständigen ASCII-127 Zeichensatz. Insgesamt werden 106 verschiedene Zeichen je Zeichensatz codiert, welche sich aus 0-9, A-Z, a-z, Sonderzeichen, ASCII-Steuerzeichen zusammensetzen. Es wird dabei zwischen drei verschiedenen Zeichensätzen unterschieden: (Lenk, 2000; Rosenbaum, 1997)

1. Zeichensatz A
   Dieser kodiert die Ziffern 0-9, die Zeichen A-Z, Sonderzeichen und au-

Abbildung 2.8: Code39 (http://barcode.tec-it.com/barcode-generator.aspx)

ßerdem ASCII-Steuerzeichen

2. Zeichensatz B
   Kodiert werden die Ziffern 0-9, die Zeichen A-Z, a-z und Sonderzeichen

3. Zeichensatz C
   Dieser Zeichensatz ist rein numerisch und kodiert die Zahlen 0-99

Jeder dieser Zeichensätze enthält außerdem Kodierungen für die Steuerzeichen von Code128, welche unter anderem den Zeichensatz definieren und auch einen Wechsel innerhalb des Codes zulassen. Dabei initialisiert das Zeichen "START X" den anfänglichen Zeichensatz auf X und "CODE X" wechselt den Zeichensatz auf X. Die exakte Kodierung ist der Tabelle 2.12 zu entnehmen.

Wie zu erkennen ist, stellt das Zeichen "STOP" einen Sonderfall dar, da es aus 13 anstatt nur 11 Bereichen besteht und ist genauso wie die Zeichen "START A", "START B" und "START C" in allen drei Zeichensätzen gültig. Der Strichcode setzt sich aus folgenden vier Elementen zusammen: (Lenk, 2000; Rosenbaum, 1997)

1. dem Startzeichen
   Dieses kennzeichnet nicht nur den Beginn eines Code128-Strichcodes, sondern legt auch fest, mit welchem Zeichensatz die Kodierung beginnt ("START A", "START B" oder "START C"). Das Startzeichen wird nur im Strichcode kodiert und scheint nicht im Klartext auf.

2. der Zeichenfolge
   Dem Startzeichen folgen die kodierten Zeichen, wobei auch Steuerzeichen zum Zeichensatzwechsel ("CODE A", "CODE B" oder "CODE C") enthalten sein können. Eine Besonderheit gibt es bei den Zeichen des Zeichensatzes C. Diese sind immer zweistellig kodiert (00-99) und werden deshalb immer in Zweiergruppen zusammengefasst (woraus sich auch eine stets gerade Anzahl an Zeichen ergibt). Dies legt auch nahe bei einer Folge von Ziffern auf den Zeichensatz C zu wechseln und so Platz zu sparen.

Wert	Zeichensatz A	B	C	Kodierung	Wert	Zeichensatz A	B	C	Kodierung
00	SPACE		00	11011001100	53	U		53	11011101110
01	!		01	11001101100	54	V		54	11101011000
02	"		02	11001100110	55	W		55	11101000110
03	#		03	10010011000	56	X		56	11100010110
04	$		04	10010001100	57	Y		57	11101101000
05	%		05	10001001100	58	Z		58	11101100010
06	&		06	10011001000	59	[		59	11100011010
07	’		07	10011000100	60	\		60	11101111010
08	(		08	10001100100	61	]		61	11001000010
09	)		09	11001001000	62	^		62	11110001010
10	*		10	11001000100	63	_		63	10100110000
11	+		11	11000100100	64	NUL	‘	64	10100001100
12	,		12	10110011100	65	SOH	a	65	10010110000
13	-		13	10011011100	66	STX	b	66	10010000110
14	.		14	10011001110	67	ETX	c	67	10000101100
15	/		15	10111001100	68	EOT	d	68	10000100110
16	0		16	10011101100	69	ENQ	e	69	10110010000
17	1		17	10011100110	70	ACK	f	70	10110000100
18	2		18	11001110010	71	BEL	g	71	10011010000
19	3		19	11001011100	72	BS	h	72	10011000010
20	4		20	11001001110	73	HT	i	73	10000110100
21	5		21	11011100100	74	LF	j	74	10000110010
22	6		22	11001110100	75	VT	k	75	11000010010
23	7		23	11101101110	76	FF	l	76	11001010000
24	8		24	11101001100	77	CR	m	77	11110111010
25	9		25	11100101100	78	SO	n	78	11000010100
26	:		26	11100100110	79	SI	o	79	10001111010
27	;		27	11101100100	80	DLE	p	80	10100111100
28	<		28	11100110100	81	DC1	q	81	10010111100
29	=		29	11100110010	82	DC2	r	82	10010011110
30	>		30	11011011000	83	DC3	s	83	10111100100
31	?		31	11011000110	84	DC4	t	84	10011110100
32	@		32	11000110110	85	NAK	u	85	10011110010
33	A		33	10100011000	86	SYN	v	86	11110100100
34	B		34	10001011000	87	ETB	w	87	11110010100
35	C		35	10001000110	88	CAN	x	88	11110010010
36	D		36	10110001000	89	EM	y	89	11011011110
37	E		37	10001101000	90	SUB	z	90	11011110110
38	F		38	10001100010	91	ESC	{	91	11110110110
39	G		39	11010001000	92	FS	|	92	10101111000
40	H		40	11000101000	93	GS	}	93	10100011110
41	I		41	11000100010	94	RS	∼	94	10001011110
42	J		42	10110111000	95	US	DEL	95	10111101000
43	K		43	10110001110	96	FUNC3		96	10111100010
44	L		44	10001101110	97	FUNC2		97	11110101000
45	M		45	10111011000	98	SHIFT		98	11110100010
46	N		46	10111000110	99	CODE C		99	10111011110
47	O		47	10001110110	100	CODE B	FNC4	CODE B	10111101110
48	P		48	11101110110	101	FNC4	CODE A	CODE A	11101011110
49	Q		49	11010001110	102	FNC1	FNC1	FNC1	11110101110
50	R		50	11000101110	103	START A			11010000100
51	S		51	11011101000	104	START B			11010010000
52	T		52	11011100010	105	START C			11010011100
						STOP			1100011101011

Tabelle 2.12: Code128 Kodierung (Lenk, 2000; Rosenbaum, 1997)

3. der Prüfsumme
   Diese dient zur Überprüfung einer korrekten Dekodierung und ergibt sich aus einer gewichteten Summierung der Zeichen und einer Modulo-Division der Summe. Dazu jedoch gleich mehr. Die Prüfsumme scheint ebenfalls nicht im Klartext auf.

4. dem Stoppzeichen
   Dieses definiert das Ende des Strichcodes und besteht als einziges Zeichen aus 13 statt 11 Bereichen. Das Stoppzeichen wird gleich wie die anderen Metadaten nur im Strichcode selbst kodiert.

Nach jedem Lesevorgang wird die dekodierte Prüfsumme mit der selbst berechneten Prüfsumme verglichen um zu kontrollieren, ob der Strichcode korrekt dekodiert wurde. Die Berechnung der Prüfsumme basiert auf einer Modulo 103 Division. Hierzu wird der Wert jedes Zeichens (siehe Tabelle 2.12) mit seiner Position gewichtet, aufsummiert und mit dem Wert des Startzeichens addiert. Die Prüfsumme ergibt sich aus der Modulodivision der Summe durch 103. Um die Prüfsumme in den Strichcode zu kodieren, wird das Zeichen verwendet dessen Wert der Prüfsumme entspricht. Wichtig bei der Berechnung der Prüfsumme ist, dass auch alle Code128-Steuerzeichen, wie zum Beispiel ein Zeichensatzwechsel "CODE A/B/C", in die gewichtete Summierung mit einfließen. Die allgemeine Formel der Prüfsumme ist der Tabelle 2.13 zu entnehmen.

$$(wert(< STARTA/B/C >) + \sum_{i=0}^{n} i * wert(z_i)) mod 103$$

Tabelle 2.13: Formel zur Berechnung der Code128-Prüfsumme

Zur Veranschaulichung wird in Tabelle 2.14 das Prüfzeichen des Beispiels aus Abbildung 2.9 berrechnet.

START B	v	o	o	c	h	+	T	U	G	r	a	z	-	2	0	1	0		
104	86	79	79	67	72	11	52	53	39	82	65	90	13	18	16	17	16	*	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17		
																		$\sum$	6238
																		mod 103	58
																			Z

Tabelle 2.14: Beispiel zur Berechnung des Code128-Prüfzeichens

Es errechnet sich das Zeichen "Z" als Prüfzeichen welches zwischen dem letzten Zeichen der Zeichenkette und dem Stoppzeichen in den Strichcode eingefügt wird. Angemerkt sollte noch werden, dass es sich bei der Zahlenfolge "2010" empfehlen würde auf den Zeichensatz C zu wechseln. Dabei würde "20" und "10" als jeweils ein Zeichen kodiert und somit Platz gespart werden. Nicht zu vernachlässigen ist das zusätzlich hinzukommende Zeichen "CODE C" für den Zeichensatzwechsel, womit die effektive Einsparung bei einem Zeichen liegt. Der "Break-Even-Punkt"[14] liegt somit bei drei Zeichen der Zeichensätze A oder B.

[14]Begriff aus der Finanzmathematik, welcher den Schnittpunkt zwischen Kosten und Einnahmen (→ Kostendeckung) bezeichnet

Abbildung 2.9: Code128 (http://barcode.tec-it.com/barcode-generator.aspx)

2.6 2D-Code

Wie auch bei den Strichcodes handelt es sich hierbei um eine etwas ungewöhnlichere Art einen Benutzer über sein Mobiltelefon zu orten. Die Idee bleibt die selbe: durch das Scannen eines eindeutigen 2D-Codes durch die eingebaute Kamera des Endgeräts kann über die darin verschlüsselten Informationen festgestellt werden, an welchem Standort sich der Benutzer befindet. Im folgenden Abschnitt wird auch immer wieder auf die deutlich vervielfachte Speicherkapazität von zweidimensionalen Codes hingewiesen, wodurch die Möglichkeit gegeben ist, viel mehr als nur die Standortinformationen zu verschlüsseln.
2D-Codes gehören auch zur Familie der Strichcodes (siehe Abschnitt 2.5), erweitern die horizontale Ebene[15] aber um eine vertikale Ebene. Das heißt die Daten werden nicht mehr nur in x-Richtung, sondern nun auch in y-Richtung aufgetragen, wenn man den Sachverhalt in einem kartesischen Koordinatensystem betrachtet. Es existieren mittlerweile viele verschiedene Varianten, beginnend mit den einfachen *gestapelten Codes*, über *Matrix Codes* bis hin zu komplexen *Punktcodes*. Aus dieser Fülle von 2D-Codes werden jene ausgewählt und beschrieben, welche zweckdienlich für die Anwendung dieser Arbeit sind oder in Zusammenhang mit vorher bereits ausgewählten Strichcodes stehen.
Jede Codeart hat ihre Vor- und Nachteile und ist zum Teil auf ein gewisses Anwendungsgebiet zugeschnitten. Wichtige Qualitätskriterien sind aber vor allem der Platzbedarf und die damit verbundene Informationsdichte, die Lesbarkeit unter verschiedensten Bedingungen (Licht, Winkel, etc.) und die Fehlerüberprüfungs- und Korrekturmöglichkeiten. Ein Vergleich der Informationsdichte bei verschiedenen 2D-Codes ist der Abbildung 2.10 zu entnehmen.

2.6.1 Stapelcode

Stapelcodes ergeben sich aus der Anordnung mehrerer Strichcodes in Zeilen untereinander. Dabei teilen sich diese meist ein gemeinsames Start- und

[15] Die Bars (dt. Striche) werden ja bei den eindimensionalen Codes in einer Zeile horizontal nebeneinander angeordnet

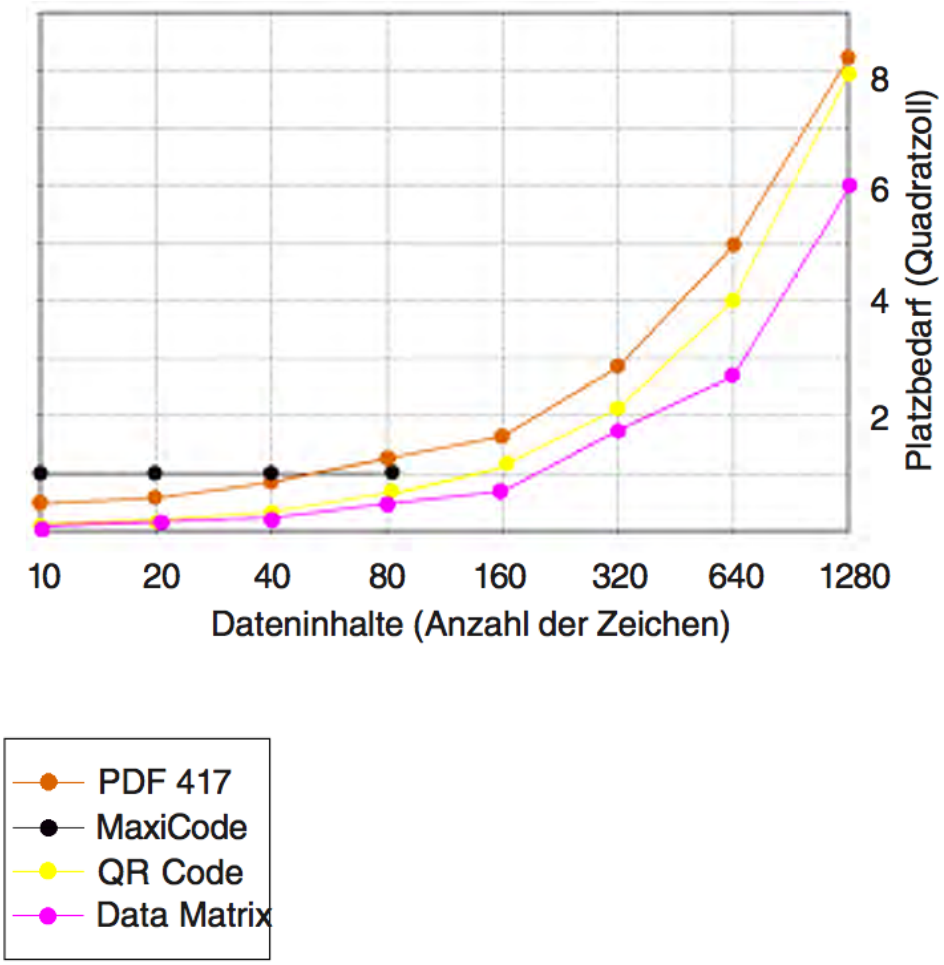


Abbildung 2.10: Informationsdichte bei 2D-Codes (Renn, 2007)

Stoppzeichen. Ein Scanner (CCD[16]- oder Laserscanner) liest dabei die Zeilen einzeln ein, erkennt den Zusammenhang und fügt diese zu einem Gesamtcode zusammen.

- *Codablock* (Lenk, 2000, 2002; Renn, 2007)
  Der Codablock wurde von Dr. Harald Oehlmann entwickelt und basiert je nach Variante auf der Struktur von Code39 oder Code128 (siehe Abschnitt 2.5.4 bzw. 2.5.5). Die Funktionsweise ist recht einfach: ist eine Zeile voll, so wird der Code in der nächsten Zeile fortgesetzt. Zur Orientierung wird jede Zeile mit einer Zeilennummer versehen. Zusätzlich enthält die letzte Zeile die Gesamtanzahl aller Zeilen. Durch die zusätzlichen Informationen enthält der Code zwei Prüfzeichen. Eines

[16] Charge-Coupled Devices: Fotodioden, welche je nach Lichteinstrahlung Ladungen freisetzt

vom Strichcode selbst und eines von der Gesamtnachricht.
Es werden drei Codablock-Varianten unterschieden:

1. Codeblock A
   Codeblock A basiert auf Code39 und erlaubt zwischen zwei und 22 Zeilen, welche zwei bis 61 Zeichen enthalten können. Die Gesamtkapazität beträgt also 1.342 Zeichen.
2. Codeblock F
   Codeblock F basiert auf Code128 und erlaubt zwischen zwei und 44 Zeilen, welche zwei bis 62 Zeichen enthalten können. Die Gesamtkapazität liegt hier bei 2.725 Zeichen.
3. Codeblock 256
   Dieser Codeblock basiert auf Codeblock F, verwendet aber eigene Start- und Stoppzeichen und hat eine zeilenweise Fehlerkorrektur.

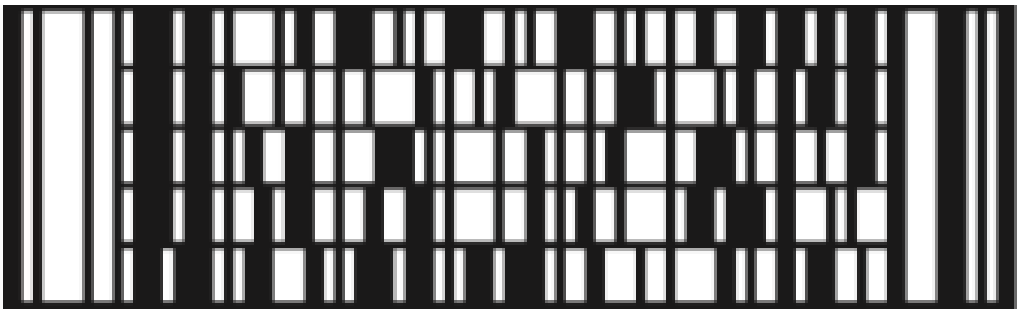


Abbildung 2.11: Codablock (Renn, 2007)

- *PDF417* (Lenk, 2000, 2002; Renn, 2007)
  PDF417[17] wurde 1991 von der Firma Symbol Technologies entwickelt und ist mittlerweile auch nach ISO/IEC spezifiziert. Der große Vorteil ist, dass im Gegensatz zu anderen Stapelcodes eine Zeile nicht vollkommen von der Abtastlinie erfasst werden muss, um ein Zeichen zu erkennen. Dies erhöht die Informationsdichte insgeheim, da die Zeilenhöhe dadurch stark verringert werden kann und Zeilenwechsel auch bei einer Schrägabtastung erkannt und verarbeitet werden können.
  Es werden drei Betriebsmodi standardmäßig unterschieden:

  1. ASCII Modus
     Er erlaubt die Kodierung von zwei alphanumerischen Zeichen in einem Codewort. Es können bis zu maximal 1.850 Zeichen kodiert werden.

[17] PDF...Portable Data File

2. Numerischer Modus
   Ein Codewort kodiert drei Ziffern. Die Maximal Kapazität liegt hier bei 2.710 Ziffern.
3. Binärer Modus

Ein Codewort besteht aus 17 Modulen, welche sich aus vier Strichen und vier Lücken zusammensetzen (daraus ergibt sich auch der Name PDF417). Es sind zwischen drei und maximal 90 Zeilen erlaubt, wobei jede Zeile aus vier fixen Elementen besteht:

1. Startzeichen
2. Zeilenindikator links
3. kodierte Daten, bestehend aus zwischen einem und 30 Modulen
4. Zeilenindikator rechts

Zwei Codewörter dienen als Prüfzeichen und maximal 510 Codewörter zur Fehlerkorrektur. Diese wird in die Stufen 0 bis 9 unterteilt. Stufe 0 ermöglicht lediglich eine Fehlererkennung. Je höher die Stufe ist, umso mehr Fehler können korrigiert werden.

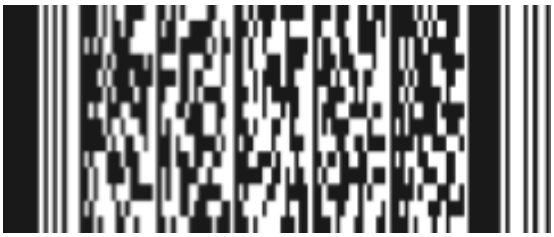


Abbildung 2.12: PDF417 (Renn, 2007)

- *MicroPDF* (Lenk, 2000, 2002; Renn, 2007)
  MicroPDF basiert auf PDF417 und wurde 1997 ebenfalls von der Firma Symbol Technologies entwickelt. Durch seine kompakte Form eignet er sich vor allem für Anwendungsgebiete mit geringen Datenmengen. Startzeichen, Stoppzeichen und die beiden Zeilenindikatoren von PDF417 werden durch so genannte "Row Address Patterns" am Beginn und Ende jeder Zeile ersetzt. Bei drei- und vierspaltigen Zeilen werden diese Patterns in die Mitte jeder Zeile eingefügt. MicroPDF hat eine Datenkapazität von 250 alphanumerischen Zeichen oder 366 Ziffern.

Abbildung 2.13: MicroPDF (Renn, 2007)

2.6.2 Matrixcode

Matrixcodes sind "(...) polygonisch, meist viereckig angeordneten Gruppen von Datenzellen (...)"(Renn, 2007). Um sie voneinander unterscheiden zu können besitzt jede Art von Matrixcode sein eigenes Erkennungssymbol über welches dieser eindeutig identifiziert werden kann.
Die meisten Matrixcodes benutzen aufgrund ihrer polygonischen Eigenschaft das Reed-Solomon-Fehlerkorrekturverfahren. Dabei wird über ein anhand von m Stützstellen errechnetes Polynom an den polygonen Datenstrom der Länge angeglichen, wobei m > n sein muss. Die Daten lassen sich dann bei bis zu maximal (n - m)/2 Fehlern wieder rekonstruieren. Die Hilfsdaten (Stützstellen, etc.) werden an die Daten angehängt und mitkodiert.
Lange Zeit konnten Matrixcodes nur mit CCD-Kameraregeräten gelesen werden. Mittlerweile gibt es aber auch Lasergeräte, welche den Code sowohl waagrecht als auch senkrecht scannen und somit auch für diese Codeart geeignet sind. Viele am Markt befindliche Mobiltelefone verfügen bereits über eine eingebaute Digitalkamera, welche mit einem Code-Scanner ausgestattet ist. Daher eignen sich diese auch als Lesegeräte für Matrixcodes (sofern diese unterstützt werden) und bilden somit gute Voraussetzungen für den Zweck dieser Arbeit. Da die Bilder meist binär weiterverarbeitet werden, ist es wichtig, dass die Codes flächig beleuchtet werden, damit das reflektierte Licht korrekt ausgewertet werden kann.
Die hier nun folgenden Matrixcode-Arten wurden ausgewählt, da sie weit verbreitet sind oder von vielen mobilen Endgeräten unterstützt werden, und aber vor allem, da sie durch die AIM[18] standardisiert sind.

- *Data Matrix* (Lenk, 2000, 2002; Renn, 2007)
  Der Data Matrix Code (siehe Abbildung 2.14) wurde 1989 in den USA entwickelt und ist nach ISO/IEC 16022 standardisiert. Er kommt in sehr vielen Bereichen zur Anwendung, wie zum Beispiel in der Produktion, Automobilindustrie, Medizintechnik, auf Tickets oder auch auf Postsendungen, und ist mittlerweile der gängigste 2D Code (Renn, 2007).
  Sein Erkennungsmerkmal ist die durchgehende Linie an der linken und unteren Kante, welche auch eine Orientierungshilfe darstellt. Bei

[18] Association for Automatic Identification and Mobility

großen Matrizen (mindestens 32 Module in einer Reihe) werden diese durch eine waagrechte und eine senkrechte durchgehende Linie in gleich große Datenfelder aufgeteilt, was nicht nur ein weiteres Erkennungsmerkmal ist, sondern vor allem die Verarbeitung und Auswertung erleichtert. Die Symbole selbst sind quadratisch.
Es gibt verschiedene Entwicklungsstufen zur Fehlerkorrektur: ECC 0 bis ECC 200. Die Stufe gibt an in welchem Ausmaß redundante Daten vorhanden sind. Je höher die Stufe, desto mehr redundante Daten werden gespeichert und desto mehr Nutzdaten können wiederhergestellt werden. ECC 200 ist die bislang sicherste Stufe. Sie verwendet die Reed-Solomon-Fehlerkorrektur und ermöglicht eine Korrektur von bis zu 25% fehlerbehafteter Daten.
Die Kapazität ist hier ganz von der Größe der Datenmatrix abhängig, oder besser gesagt, die Größe der Matrix ergibt sich aus der zu kodierenden Datenmenge.

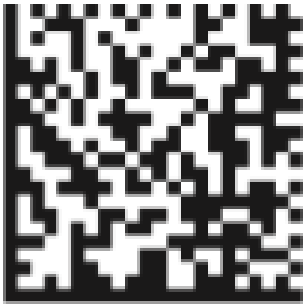


Abbildung 2.14: Data Matrix (Renn, 2007)

- *QR Code* (Lenk, 2000, 2002; Renn, 2007)
  Der Quick Response Code (siehe Abbildung 2.16) wurde 1994 von der japanischen Firma Denso im Auftrag des Autokonzerns Toyota entwickelt und ist nach ISO/IEC 18004 standardisiert. Ursprünglich war er zur Markierung von Teilen in der Produktion von Toyota gedacht, hat sich aber in den letzten Jahren zu einem vielseitigeren Werkzeug entwickelt. Eine breite Verwendung finden diese Codes vor allem im Bereich "Mobile Tagging", indem auf Plakaten, Zeitschriften, Zeitungen und Ähnlichem wichtige Informationen wie URLs, Telefonnummern, Texte, und vieles mehr in QR Codes gespeichert werden. Der Benutzer muss dann lediglich den Code mit seinem Handy fotografieren und ohne mühsames Abtippen öffnet sich dann eine Webseite im Browser oder eine Nummer erscheint am Display.
  Der QR Code besteht immer aus einer quadratischen Matrix (siehe Abbildung 2.15), deren Elemente wiederum kleine schwarze oder weiße Quadrate sind, die die binär kodierten Daten darstellen. Eindeuti-

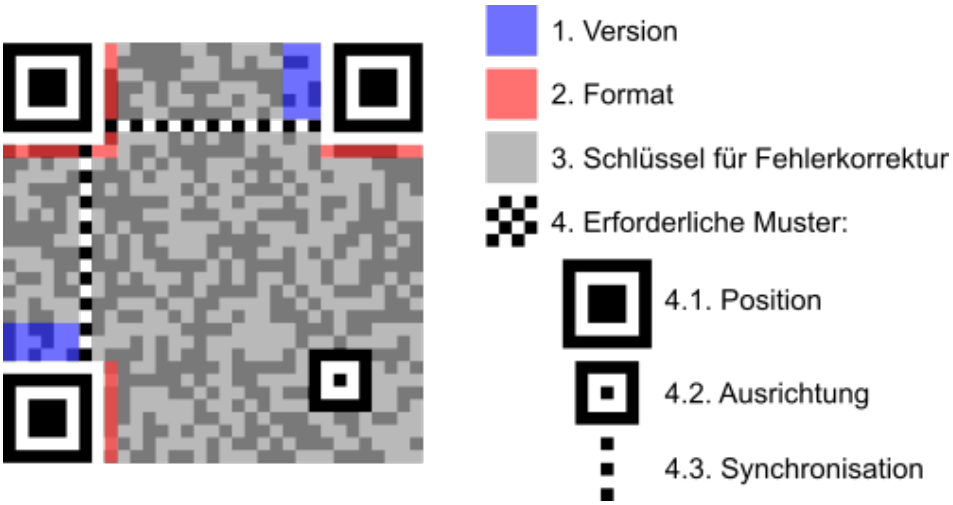


Abbildung 2.15: QR Code Struktur (http://de.wikipedia.org/w/index.php?title=Datei:QR_Code_Struktur_Beispiel.svg&oldid=58295588)

ges Erkennungsmerkmal sind die schwarz-weiß-schwarz ineinander verschachtelten Quadrate in drei der vier Ecken, welche wiederum auch als Orientierungshilfe dienen. Überschreitet das Quadrat eine gewisse Größe werden weitere Orientierungshilfen in der Form von kleineren verschachtelten Quadraten (4.2) in den Code eingefügt. Genauso kann auch ein großer QR Code in bis zu 16 einzelne Codes zerlegt werden, indem entlang der zusätzlich eingefügten Orientierungssymbole aufgespalten wird.
Zur Fehlerkorrektur gibt es vier verschiedene Levels:

1. Level L
   7% fehlerhafte Daten können wiederhergestellt werden
2. Level M
   15% fehlerhafte Daten können wiederhergestellt werden
3. Level Q
   25% fehlerhafte Daten können wiederhergestellt werden
4. Level H
   30% fehlerhafte Daten können wiederhergestellt werden

Bei der Wiederherstellung der Daten wird das Reed-Solomon-Verfahren verwendet. Die redundanten Daten (siehe 3. in Abbildung 2.15) werden zusammen mit den Nutzdaten im Code gespeichert.
QR Codes gibt es in den Größen 21 x 21 (Elemente) bis hin zu 177 x 177 wodurch sich eine Speicherkapazität von 4.296 alphanumerischen Zeichen oder 7.089 Ziffern ergibt.

Abbildung 2.16: QR Code (Renn, 2007)

- *Micro QR Code* (Lenk, 2000, 2002; Renn, 2007)
  Der Micro QR Code (siehe Abbildung 2.17) ist eine spezielle Form des QR Codes und wurde 1999 entwickelt. Er ist speziell für Anwendungen optimiert in denen eine geringe Datenmenge auf einem möglichst kleinem Platz untergebracht werden muss. Die Erkennungssymbole in den drei Ecken des QR Codes werden auf ein Symbol in der linken oberen Ecke reduziert, welches wiederum auch der Orientierung dient.
  Es existieren insgesamt vier verschiedene Größen (M1 - M4). Je nach Größe gibt es bis zu drei Fehlerkorrekturlevels, welche auch die Kapazität beeinflussen, die ihr Maximum bei 21 alphanumerischen Zeichen oder 35 Ziffern erreicht. Details können der Tabelle 2.15 entnommen werden.

Version	Elemente	Korrekturlevel	alphanumerische Zeichen	Ziffern
M1	11 x 11	-	-	5
M2	13 x 13	L	6	10
		M	5	8
M3	15 x 15	L	14	23
		M	11	18
M4	17 x 17	L	21	35
		M	18	30
		Q	13	21

Tabelle 2.15: Micro QR Code Größen

- *Maxi Code* (Lenk, 2000, 2002; Renn, 2007)
  Der Maxi Code (siehe Abbildung 2.18) ist eine Eigenentwicklung des

Abbildung 2.17: Micro QR Code (Renn, 2007)

amerikanischen Unternehmens UPS[19] und ist nach ISO/IEC 16023 standardisiert. Er wurde im Jahr 1989 eingeführt und sollte vor allem die Identifizierung, Verfolgung und Sortierung von Paketen erleichtern und beschleunigen. Als Erkennungszeichen verwendet dieser Matrixcode drei konzentrische Kreise im Mittelpunkt des Symbols.
Im Gegensatz zu anderen Codes werden die Elemente nicht als Quadrat oder Striche sondern als regelmäßiges Hexagon dargestellt. Weiters ist die Größe des Symbols fixiert auf 1x1 Inches[20] und besteht aus 30 Reihen zu je 33 Spalten, insgesamt also 866 Elementen. Damit lassen sich 93 ASCII-Zeichen oder aber 138 Ziffern codieren.
UPS-intern werden folgende Daten codiert:

1. UPS-Kontrollnummer
   Diese dient zur Identifizierung des Paketes.
2. Gewicht
3. Sendungsart
4. Adresse des Absenders
5. Adresse des Empfängers

Das Suchmuster in der Mitte des Symbols erfüllt zweierlei Zwecke:

1. *Verzerrungserkennung*
   Durch die drei konzentrisch angeordneten Kreise können Verzerrungen in jede Richtung erkannt und somit auch in die Decodierung eingerechnet und ausgeglichen werden.
2. *Alternating Pattern*
   Die Linienstärke der drei konzentrischen Kreise wird als das sogenannte "Alternating Pattern" bezeichnet und definiert die Größe der sechseckigen Elemente. Dadurch kann ein virtuelles Gitternetz erstellt werden, welches das Erkennen von Datenelementen erleichtert.

[19] United Parcel Service, http://www.ups.com
[20] entspricht einer metrischen Größe von 25,4 x 25,4 mm

Zur Fehlererkennung und -korrektur verwendet der Maxi Code ebenfalls das Reed-Solomon-Verfahren und unterstützt mehrere Korrekturstufen. Die höchste Stufe erlaubt eine Rekonstruktion des Symbols bei einer maximalen Zerstörungsrate von 25%.

Abbildung 2.18: Maxi Code (Renn, 2007)

- *Aztec Code* (Lenk, 2000, 2002; Renn, 2007)
  Der Aztec Code (siehe Abbildung 2.20) ist eine Entwicklung von Dr. Andy Longacre aus den USA, wurde im Jahr 1995 veröffentlicht und ist nach ISO/IEC 24778 standardisiert. Seinen Namen erhielt dieser Code aufgrund seines Erkennungsmusters, welches aus mehreren abwechselnd schwarz oder weiß ineinander verschachtelten Quadraten besteht und einer vom Himmel aus betrachteten aztekischen Pyramide ähnelt. Die Anzahl der Quadrate ist abhängig von der Größe des Symbols, kann aber in zwei Arten aufgegliedert werden:

  – *kompaktes Erkennungsmuster*
    dargestellt durch fünf verschachtelte Quadrate
  – *volles Erkennungsmuster*
    dargestellt durch sieben verschachtelte Quadrate

  Der Aztec Code besteht insgesamt aus fünf verschiedenen Elementen (siehe Abbildung 2.19), wobei drei davon einen fixen Aufbau haben:

  – *Referenz Gitter (fixer Aufbau; engl. Reference Grid)*
    Dieses Gitter geht durch das komplette Symbol und dient dem Lesegerät als Orientierungshilfe. Handelt es sich um ein Kompakt-Symbol, so entfällt das Referenzgitter.
  – *Suchmuster (fixer Aufbau; engl. Finder Pattern)*
    Das Suchmuster identifiziert das Symbol eindeutig als Aztec Code. Wie bereits vorher erwähnt, wird zwischen einem kompakten und einem vollen Muster unterschieden.

- *Orientierungsmuster (fixer Aufbau; engl. Orientation Pattern)*
  Diese Muster dienen zur Identifizierung der Leserichtung.
- *Modusmeldung (variabler Aufbau; engl. Mode Message)*
  Die Meldung enthält Informationen über die Anzahl der Schichten und die Anzahl der Wörter im Code. Da diese Informationen den Datenbereich nie vollständig füllen, wird der restliche Bereich mit Prüfwörtern befüllt.
- *Datenschichten (variabler Aufbau; engl. Data Layers)*
  Diese enthalten die codierten Daten. Handelt es sich um ein kompaktes Symbol, so gibt es maximal vier Schichten.

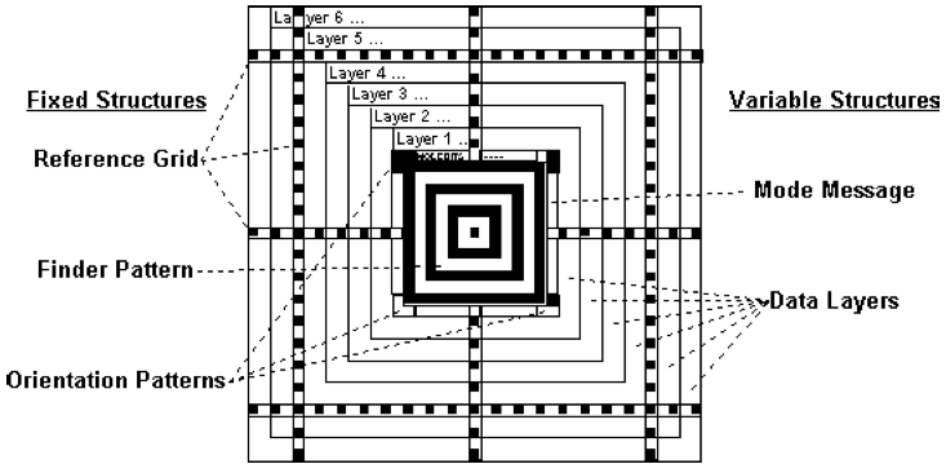


Abbildung 2.19: Aztec Code Struktur (Merki, 2003)

Die einzelnen Symbolelemente bestehen wie bei den anderen Codes aus Quadraten. Die Größe richtet sich hierbei nach der Menge des zu codierenden Inhalts. Insgesamt gibt es 33 verschiedene Größen, welche eine maximale Kapazität von 3067 Zeichen oder 3832 Ziffern haben. Eine grobe Übersicht über das Größenspektrum des Aztec Codes ist der Tabelle 2.16 zu entnehmen.

Ähnlich wie bei einem QR Code kann sich ein großes Symbol aus mehreren kleinen Symbolen zusammensetzen und wird dann vom Lesegerät wieder als einheitliches Symbol erkannt. Da in der Modusmeldung die Anzahl der Datenschichten codiert ist werden im Gegensatz zum QR Code jedoch keine weiteren Orientierungshilfen benötigt. Insgesamt können bis zu 26 Aztec Symbole miteinander verbunden werden.

Erkennungssymbol	Schichten	Elemente	alphanumerische Zeichen	Ziffern
Kompakt	1	15 x 15	12	13
Kompakt	4	27 x 27	89	110
Voll	7	45 x 45	236	294
Voll	11	61 x 61	482	601
Voll	15	79 x 79	808	1008
Voll	20	101 x 101	1324	1653
Voll	26	125 x 125	2107	2632
Voll	32	151 x 151	3067	3832

Tabelle 2.16: Aztec Code Größen (Merki, 2003)

Abbildung 2.20: Aztec Code (Renn, 2007)

2.6.3 Punktcodes

Punktcodes ähneln Matrixcodes, stellen aber eine eigene Art von zweidimensionalen Codes dar. Die Elemente eines Symbols werden durch einen Punkt dargestellt, wobei die An- und Abwesenheit von Punkten einer binären Kodierung entspricht. Die bedeutendsten Vorteile sind der geringe Platzbedarf (beispielsweise Markierung von Mikrochips) und der im Vergleich zu anderen gedruckten Codes für die optische Erkennung nur sehr gering benötigte Kontrast. Weiters können Punktcodes auch direkt auf Materialien gestanzt, gebohrt, gebrannt, oder ähnliches werden, wodurch auf verschmutz- oder beschädigbare Etiketten verzichtet werden kann. Es folgen nun zwei der verbreitetsten Codes:

- *Dot Code A*(Lenk, 2000, 2002; Renn, 2007)
  Der Dot Code A (siehe Abbildung 2.21), auch bekannt als Philips Code, wurde vom Holländer Willibrordus J. Van Gils bei dem Unternehmen US Philips Corporation erfunden und im Jahr 1988 patentiert. Dargestellt wird er durch eine Punkt-Matrix in der Größe von 6 x 6 bis 12 x 12 Punkten, welche es ermöglicht bis zu 42 Milliarden Objekte zu unterscheiden. Als Such- und Orientierungsmuster dienen jeweils die

drei äußersten Punkte in den Ecken, welche durch eine Schwarz/Weiß-Kombination eindeutig identifiziert werden können.
Weiters verwendet der Dot Code A redundante Punkte um einen ge-

Abbildung 2.21: Dot Code A (Renn, 2007)

wissen Grad an Fehlerkorrektur, definiert durch die Korrekturstufen 0 bis 5, zu gewährleisten. In Abbildung 2.22 ist das Beispiel einer 7 x 7 Punktmatrix dargestellt. Dabei sind die mit "p" bezeichneten Punkte redundate Informationen der mit "i" bezeichneten Punkte.

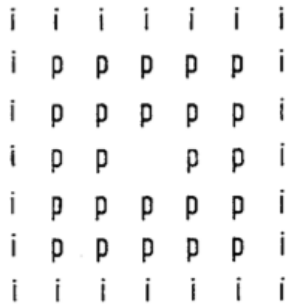


Abbildung 2.22: Dot Code A Kodierung(Patent, 1988)

- *Snowflake Code*(Lenk, 2000, 2002; Renn, 2007)
  Der Snowflake Code (siehe Abbildung 2.24) wurde vom Briten John Paul Chan bei dem Unternehmen Electronic Automation Limited entwickelt, im Jahr 1998 in den USA patentiert und ähnelt dem Dot Code A. Sein Hauptvorteil ist die hohe Informationsdichte, welche es ermöglicht eine Datenmenge von 100 Ziffern auf einer Fläche von nur 25 mm^2 zu codieren. Da dieser Code für Eigenzwecke entwickelt wurde, ist er nie standardisiert worden.
  Als Erkennungsmuster dienen die aus mindestens sechs Punkten bestehenden Ecken 1, 2, 3, 4 (siehe Abbildung 2.23). In Abbildung 2.24 ist ersichtlich, dass die Ecken nur aus 2 Punkten bestehen. Hierbei handelt

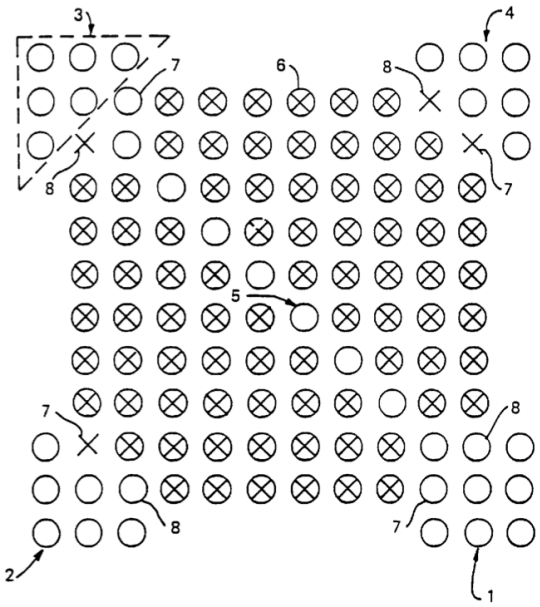


Abbildung 2.23: Snowflake Code Kodierung (Patent, 1998)

es sich um eine alternative Darstellung, welche allerdings in der selben Bedeutung resultiert. Als Orientierungshilfe dienen die an die Ecken angrenzenden Punkte 7 und 8. Durch eine Schwarz/Weiß-Kodierung identifizieren sie jede Ecke eindeutig. Die Diagonale 5 verbindet immer die Ecken 1 und 3 und enthält Informationen über die Punktdichte. Dabei wird diese über die Anzahl der in der Diagonalen enthaltenen Punkte festgelegt.
Der Snowflake Code existiert in den Größen 8 x 8 bis 32 x 32 und verfügt über eine maximale Datenkapazität von 860 bits.

Abbildung 2.24: Snowflake Code (Renn, 2007)

2.7 Bluetooth

Die in diesem Abschnitt beschriebene Lokalisierungsvariante basiert auf der nach Industriestandard IEEE 802.15 spezifizierten Technologie Bluetooth. Hierbei handelt es sich um ein Funknetz, welches es Geräten ermöglicht über kurze Distanzen zu kommunizieren. Bluetooth zählt zur Kategorie der WPANs[21] und hat eine maximale Reichweite von zirka 100 Metern.
In den untersuchten Arbeiten (WPNC, 2004), (Jevring, 2008), (Bargh et al., 2008),(Liu et al., 2010) zum Thema "Indoor-Lokalisierung mittels Bluetooth" werden hauptsächlich Setups beschrieben, in denen Endgeräte innerhalb von Gebäuden in gewissen Räumen geortet werden sollen und die Bewegungspfade nachvollzogen werden können. Dabei werden Techniken wie neuronale Netze und das Hidden Markov Model verwendet, die anhand von "Fingerabdrücken" (= die Antwortzeit zwischen Basisstation und mobilem Gerät), die das Gerät beim Aufenthalt in einem Raum hinterlässt, bestimmen können, in welchem Raum sich dieses befindet. Die Basisstationen sind dabei fix installierte Computer mit einem Bluetooth-Dongle und einer Datenbank, welche ein erlerntes Model von Fingerabdrücken enthält. Verbindet sich nun ein Gerät mit der Basisstation, so kann anhand des Modells die Position des Geräts errechnet werden. Diese Setups behandeln das für diese Arbeit benötigte Thema im Übermaß, da hier lediglich sichergestellt werden muss, dass sich ein Benutzer im Geschäftslokal befindet und nicht genau wo. Die reduzierte Konfiguration besteht also in diesem Szenario aus folgenden Komponenten:

- einer Basistation im Geschäftslokal, bestehend aus einem Computer mit Bluetooth
- einem oder mehreren mobilen Endgeräten, welche auch über Bluetooth verfügen

Der Ablauf zur Lokalisierung bei der Einlösung eines Gutscheines sieht schematisch wie folgt aus:

1. *Konfigurationsabfrage*
   Das Endgerät ermittelt anhand seiner Position die Bluetooth-Konfiguration der Basistation des sich in seiner Nähe befindlichen Geschäftslokals. Diese beinhaltet den Namen oder die Bluetooth-Adresse der Basistation.
2. *Verbindungsaufbau*
   Das Endgerät versucht sich mit der ihm mitgeteilten Basistation zu verbinden.

[21] Wireless Personal Area Network

3. *Geheimnisaustausch*
   Nach erfolgreichem Verbindungsaufbau teilt die Basistation dem Endgerät ein nur ihr bekanntes Geheimnis mit, welches das Geschäftslokal eindeutig identifiziert.

4. *Einlösung*
   Das Endgerät versucht den Gutschein wie bisher einzulösen, teilt dem Server aber zusätzlich das Geheimnis mit, welches es nur innerhalb des Geschäftslokals erhält.

Durch den Austausch der Bluetooth-Konfiguration der Basisstation und des eindeutigen Geheimnisses sollte sichergestellt sein, dass sich der Benutzer im Geschäftslokal befindet. Nachteil dieses Systems ist vor allem der Wartungsaufwand, der beispielsweise durch das Austauschen der Basisstation oder des Bluetooth-Dongles entsteht und den mit der Hardware verbundenen Anschaffungskosten für den Geschäftskunden. Doch bevor die Vor- und Nachteile dieses Systems analysiert werden, folgt zuerst die Untersuchung der Bluetooth-Technologie an sich.

Bluetooth wurde eigentlich mit dem Gedanken entwickelt, den vielen Kabelverwirrungen ein Ende zu setzen und Peripheriegeräten eine kabellose Verbindung zu einem Computer zu ermöglichen. Mittlerweile wurde bereits Version 4.0 spezifiziert, welche aber am Markt noch nicht verfügbar ist und über folgende Kernfunktionen verfügt: (Bluetooth, 2010)

- Enhanced Data Rate (EDR; 2,1 Mbit/sec)
- schneller Verbindungsaufbau ($<$ 5 ms)
- Reichweite bis 100 Meter
- Quality of Service (QoS)
- 128 Bit AES-Verschlüsselung
- WLAN-Unterstützung
- Reduzierung des Stromverbrauches

Es existiert sowohl eine synchrone als eine asynchrone Datenverbindung, wobei erstere hauptsächlich bei der Übertragung von Sprachdaten zur Verwendung kommt, welche durch Nutzung eines Highspeed-Kanals eine maximale (theoretische) Übertragungsgeschwindigkeit von 24 Mbit/sec ermöglichen. Bluetooth arbeitet innerhalb des weltweit freien 2,4-GHz-ISM-Band (2.400 MHz bis 2.483,5 MHz) auf einem Frequenzband von 2.402 MHz bis 2.480 GHz, welches sich unter anderem auch mit dem WLAN-Band überschneidet. Um Störungen zu vermeiden und das Abhören von Datenverbindungen

zu verhindern wird ein so genanntes Frequenz-Hopping verwendet, welches das Frequenzspektrum auf mehrere kleine Frequenzbänder aufteilt. Insgesamt gibt es 79 Bänder/Kanäle zu je 1 MHz. Die einzelnen Bänder werden dann bis zu 1.600 mal pro Sekunde gewechselt.
Bluetooth-Geräte werden anhand ihrer Sendeleistung in drei Klassen unterteilt, in deren direkten Abhängigkeit die Sendereichweite ist. Die Daten sind der Tabelle 2.17 zu entnehmen.
Jeder Bluetooth-Teilnehmer verfügt über einen Namen und über eine eindeu-

Leistungsklasse	maximale Sendeleistung	maximale Reichweite
1	100 mW (20 dBm)	$\sim$ 100 m
2	2,5 mW (4 dBm)	$\sim$ 10 m
3	1 mW (0 dBm)	$\sim$ 1 m

Tabelle 2.17: Bluetooth Geräteklassen (Bluetooth, 2010)

tige 48 bit MAC[22] Adresse, welche sich aus folgenden Teilen zusammensetzt: (Bluetooth, 2010)

- 24 Bit für den Lower Address Part (LAP)
- 8 Bit für den Upper Address Part (UAP)
- 16 Bit für den Non Significant Address Part (NAP)

Weiters werden von jedem Gerät gewisse Dienste, so genannte Profile, zur Verfügung gestellt. Dazu zählen unter anderem Datenaustausch-, Druck- oder Streaming-Dienste. Bei Bluetooth werden folgende Netzwerk-Topologien unterstützt: (Bluetooth, 2010)

- *Punkt-zu-Punkt Verbindung*
  Diese Verbindung findet nur zwischen zwei Endgeräten statt. Dabei werden diese "gepaart", die Verbindung authentifiziert und die Datenpakete ausgetauscht. Die Kommunikation kann sowohl in beide als auch nur in eine Richtung stattfinden.
- *Piconetz*
  Ein Piconetz ist ein Bluetooth-Netzwerk, welches maximal 255 Geräte beherbergen kann. Davon können maximal acht gleichzeitig kommunizieren während sich die restlichen 247 im Parkmodus befinden. Von diesen acht aktiven Geräten übernimmt einer die Funktion des Masters, welcher die Kommunikation untereinander regelt und das Netz verwaltet. Meist ist dies das erste Gerät, welches eine Kommunikation initiiert. Die Slaves werden nach erfolgreicher Verbindung regelmäßig

[22] Media Access Control

in einem Zeitmultiplexverfahren nach zu sendenden Daten abgefragt, welche in weiterer Folge durch den Master weitergeleitet werden.

Bluetooth verwendet zwei verschiedene Techniken um Übertragungsfehler zu erkennen und zu korrigieren:(Bluetooth, 2010)

1. *Forward Error Correction (FEC)*
   Bei der Vorwärtsfehlerkorrektur werden beim Sender die Daten in den Datenstrom redundant eingefügt. Somit kann der Empfänger Fehler erkennen und, ohne mit dem Sender nochmal in Kontakt zu treten, korrigieren. Es werden zwei Varianten der FEC unterstützt:

   - 1/3 FEC
     1 Datenbit wird 3-fach redundant übertragen
   - 2/3 FEC
     Für 2 Datenbit werden insgesamt 3 Bit übertragen

2. *Automatic Repeat Request (ARQ)*
   Diese Technik sendet ein Datenpaket solange, bis es fehlerfrei beim Empfänger ankommt. Zur Fehlerkontrolle wird eine CRC[23]-Prüfsumme beim Sender berechnet und mitübertragen. Der Empfänger berechnet selbst die Prüfsumme und vergleicht sie mit der übertragenen Summe. Stimmen diese überein, wird der Sender über einen erfolgreichen Empfang benachrichtigt. Ansonsten wird das Paket nochmals geschickt, bis die Übertragung erfolgreich war.

Sicherheitstechnisch werden drei verschiedene Modi zur Verfügung gestellt: (Bluetooth, 2010)

- Modus 1 (Non-Secure)
  Es werden keinerlei Sicherheitsmaßnahmen getroffen, weder zur Autorisierung, Authentifizierung noch zur Verschlüsselung der Daten. Dieser Modus ist für den Zweck dieser Arbeit sehr interessant, da der Benutzer, abgesehen von einem möglichen Hinweis Bluetooth bei seinem Endgerät einzuschalten, keinerlei Meldungen erhält oder zu Eingaben aufgefordert wird, somit also nichts von der im Hintergrund ablaufenden Standortvalidierung mitbekommt.

- Modus 2 (Service Level Enforced Security)
  Sicherheitsüberprüfungen werden in diesem Modus auf Applikationsebene vorgenommen. Das heißt, dass sich die Anwendung selbst NACH Herstellung einer Verbindung um die Durchführung etwaiger Autorisierungen, Authentifizierungen und/oder Verschlüsselungen kümmert.

[23] Cyclic Redundancy Check

- Modus 3 (Link Level Enforced Security)
  Dieser Modus unterscheidet sich von Modus 2 dahingehend, dass die Sicherheitsmechanismen bereits auf Verbindungsebene, also VOR Herstellung einer Verbindung ausgelöst werden.

Die Lokalisierung mittels Bluetooth hat also durch ihre geringe Reichweite den Vorteil einer relativ genauen Lokalisierung, ist sehr verbreitet und auf beinahe jedem mobilen Endgerät vorhanden und erlaubt einen möglichst interaktionslosen Verbindungsaufbau und Datenaustausch. Nachteile sind allerdings der relativ hohe Stromverbrauch am Mobiltelefon, die Anschaffungskosten für die Basisstationen und der Verwaltungsaufwand der bei Veränderungen oder Austausch der Basisstation entsteht.

2.8 Wireless Local Area Network (WLAN)

Diese Art der Lokalisierung basiert auf dem nach IEEE 802.11 Standard spezifizierten Wireless LAN. Dabei handelt es sich um ein Funknetzwerk, welches auf dem lizenzfreien 2,4-GHz-ISM-Frequenzband und dem 5-GHz-Band arbeitet.
Ähnlich dem Thema "Bluetoothlokalisierung" aus Abschnitt 2.7 haben die untersuchten Arbeiten (Patmanathan, 2006), (Fang et al., 2009), (Youssef et al.) zum Thema "In-House Lokalisierung mittels WLAN" ihren Schwerpunkt in der Wahrscheinlichkeitsrechnung und Statistik. Es werden Werte wie Antwortzeiten ("Time of arrival" (TOA)) oder Signalstärken ("Received Signal Strength" (RSS)) mit der dazugehörigen Position in ein statistisches Modell eingepflegt, um so die wahrscheinlichste Position anhand von Vergleichswerten bestimmen zu können. Als Referenzstationen dienen Access Points, denen eine fixe Position innerhalb eines Gebäudes/Stockwerkes/Raumes/etc. zugeordnet ist. Kann anhand des Vergleichswertes die Basisstation ermittelt werden, so hat man auch die Position.
Auch in diesem Fall wird eine vereinfachte Variante verwendet, da nur sichergestellt werden muss, dass sich ein Benutzer im Geschäftslokal befindet. Die Konfiguration würde hierfür wie folgt aussehen:

- ein Access Point im Geschäftslokal, mit versteckter[24] Service Set ID (SSID[25]) und optionaler Verschlüsselung über Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA) oder WPA2. Auf die Verschlüsselungsarten wird später noch genauer eingegangen.

[24] Mit "versteckt" ist gemeint, dass der Access Point seine SSID nicht ausstrahlt und somit nicht für jeden sichtbar ist. Die Kenntnis der SSID wird vorausgesetzt um sich mit dem Netzwerk verbinden zu können.

[25] Die SSID ist eine alphanumerische Zeichenkette und kennzeichnet ein Funknetzwerk eindeutig. Mehrere Access Points können die selbe SSID haben und partizipieren somit am selben Netzwerk.

- einem oder mehreren mobilen Endgeräten, welche über WLAN verfügen

Der Ablauf zur Positionsbestimmung bei der Einlösung eines Gutscheines ist wie folgt konzipiert:

1. *Konfigurationsabfrage*
   Das Endgerät ermittelt anhand seiner Position die WLAN Konfiguration des Geschäftslokals. Diese beinhaltet die eindeutige SSID und optional das Geheimnis für die Verschlüsselung.

2. *Verbindungsaufbau*
   Das Endgerät versucht sich mit dem ihm mitgeteilten Funknetzwerk zu verbinden.

3. *Geheimnisermittlung*
   Nach erfolgreichem Verbindungsaufbau ermittelt das Endgerät die eindeutige MAC[26]-Adresse des Access Points, welches in diesem Fall das Geheimnis für die Einlösung darstellt und das Geschäftslokal eindeutig identifiziert.

4. *Einlösung*
   Das Endgerät versucht den Gutschein wie bisher einzulösen, teilt dem Server aber zusätzlich das ermittelte Geheimnis mit, welches es nur innerhalb des Geschäftslokals erhalten sollte.

Durch den Austausch der WLAN Konfiguration des Geschäftslokals zum Einlösezeitpunkt, der versteckten SSID, der optionalen Verschlüsselung und der Verwendung der eindeutigen MAC-Adresse als Geheimnis für die Einlösung sollte sichergestellt sein, dass sich der Benutzer bzw. das Endgerät im Geschäftslokal befindet. Nachteile dieser Variante sind ähnlich wie bei Bluetooth der Wartungsaufwand und die Anschaffungskosten für die Hardware. Hinzu kommt allerdings noch die eventuell zu hohe Reichweite von WLAN, wodurch sich der Benutzer auch eventuell außerhalb des Lokals aufhalten könnte. Näheres dazu ist dem folgenden Abschnitt zu entnehmen, welcher sich mit der WLAN-Technologie auseinander setzt.

WLAN ist ein Funknetzwerk welches nach IEEE 802.11 genormt ist und verfügt im Gegensatz zu WPANs wie Bluetooth (siehe Abschnitt 2.7) sowohl über eine höhere Reichweite als auch über schnellere Übertragungsraten. Im Laufe der Zeit wurden einige Versionen spezifiziert, wovon sich aber nur wenige durchgesetzt haben und Anwendung finden. Diese sind der Tabelle 2.18 zu entnehmen.

[26] Media Access Control

Version	Publikationsjahr	Frequenzband	max. Geschwindigkeit	max. Reichweite
802.11a	1999	2,4 GHz	54 Mbit/sec	120 m
802.11b	1999	5 GHz	11 Mbit/sec	140 m
802.11g	2003	2,4 GHz	54 Mbit/sec	140 m
802.11n	2009	2,4 GHz & 5 GHz	600 Mbit/sec	250 m

Tabelle 2.18: WLAN Spezifikationen (IEEE Computer Society, 1999)

Zur Tabelle 2.18 ist anzumerken, dass es sich bei den angegebenen Geschwindigkeiten und Reichweiten um theoretisch mögliche Werte handelt. Speziell bei der Übertragungsrate ist dies die Bruttodatenrate. Die realitätsgetreue Nettodatenrate liegt meist bei zirka 40 bis 50 Prozent der Bruttorate und ist unter anderem auch darauf zurückzuführen, dass die Bandbreite auf Up- und Downstream aufgeteilt werden muss. Besonders hervor sticht die IEEE 802.11g Norm mit einer Datenrate von 600 Mbit/sec. Solch hohe Geschwindigkeiten werden mit dem verwendeten Multiple Input Multiple Output Verfahren realisiert. Grundlage dieses Verfahrens ist die Verwendung jeweils mehrerer Antennen auf der Sende- und Empfangseinrichtung. Durch die Bündelung der einzelnen Datenströme pro Antenne zu einem gemeinsamen Datenstrom können weitaus höhere Datenraten erzielt werden.
Jedes Funknetzwerk verfügt über eine ID, die sogenannte Service Set ID (SSID), welche ein Netzwerk eindeutig identifiziert und über welche es aufgespürt werden kann. Diese ID kann von einem verantwortlichen Knoten (beispielsweise dem Access Point im Infrastruktur-Modus) ausgestrahlt werden (das Netzwerk wird als "sichtbar" bezeichnet) oder geheim gehalten werden (das Netzwerk ist nicht öffentlich "sichtbar"). Im zweiten Fall können sich nur Geräte in das Netzwerk einhängen, denen dessen SSID bekannt ist. Wireless LAN verfügt über zwei Hauptbetriebsarten, dem Infrastruktur-Modus, die einer Sterntopologie gleich kommt, und dem Ad-Hoc-Modus, in dem alle Teilnehmer gleichberechtigt sind. Diese sind wie folgt beschrieben: (IEEE Computer Society, 1999)

- *Infrastruktur*
  Ein Funknetzwerk im Infrastruktur-Modus ähnelt in seinem Aufbau einer Sternarchitektur. Zentraler Knotenpunkt des Netzwerks ist ein Access Point, welcher die Kommunikation der Clients untereinander regelt. Dieser sendet in zyklischen Intervallen kleine Datenpakete aus, welche unter anderem die Service Set ID und die Art der Verschlüsselung enthält. Durch diese Pakete, auch "Beacons" oder "Leuchtfeuer" genannt, lässt sich ein Funknetzwerk aufspüren und eine Verbindung damit herstellen. Um die Sicherheit des Netzwerks zu erhöhen kann die Ausstrahlung der SSID unterbunden werden und der Client benötigt deren Kenntnis um eine Verbindung herstellen zu können.

Innerhalb eines Infrastruktur-Netzwerks können auch mehrere Access Points gleichzeitig betrieben werden. Dafür werden diese mit den selben Parametern (SSID, Verschlüsselung, ...) konfiguriert. Die SSID wird nun als ESSID[27] bezeichnet, da sie ein erweitertes Netzwerk repräsentiert. Weiters definiert die IEEE 802.11 Norm hierfür auch noch den Begriff Basic Service Set Identifier (BSSID), welcher jeden Access Point im Netzwerk eindeutig identifiziert. Als BSSID wird die MAC Adresse der Basisstation verwendet.
Kurz zusammengefasst gibt es also ein Basic Service Set (BSS), welches ein Funknetzwerk mit einem Access Point bezeichnet, und ein Extended Services Set, welches ein Netzwerk mit mehreren über Ethernet verbundenen Basisstationen bezeichnet, welche sich eine gemeinsame SSID teilen. SSID fungiert hierbei als Überbegriff und steht einerseits für die ID einer Basisstation (BSSID) und andererseits für die Netzwerk-ID (ESSID).

- *Ad-Hoc*
  In einem Ad-Hoc Funknetzwerk gibt es keinen zentralen Knotenpunkt. Jeder Teilnehmer ist mit jedem verbunden, dass heißt sie kommunizieren direkt miteinander. Dies setzt natürlich voraus, dass sich jeder im Sende-/Empfangsbereich des anderen befindet. Da der Ad-Hoc-Modus kein Routing unterstützt, können Datenpakete auch nicht über einen dritten Client weitergeleitet werden. Grundvoraussetzung für das Zustandekommen eines Netzwerks ist ähnlich wie bei einem Extended Service Set die einheitliche Konfiguration aller Teilnehmer.

Neben den zwei eben erwähnten Betriebsmodi existiert noch ein dritter Modus, welcher zur Erweiterung der Reichweite und Signalverstärkung dient und als Wireless Distribution System bezeichnet wird. Hierbei unterscheidet man die Funktion einer Bridge, welche Datenpakete über das Funknetzwerk an eine bestimmte Basisstation weiterleitet, und eines Repeaters, welcher die Datenpakete per Multicast an alle Geräte in seiner Reichweite weiterverteilt. Um die Sicherheit eines WLANs zu erhöhen, kann der komplette Datenverkehr mithilfe verschiedener Verfahren verschlüsselt werden. Der IEEE 802.11 Standard definiert hierfür mehrere Verschlüsselungsmethoden: (IEEE Computer Society, 1999)

- *Wired Equivalent Privacy (WEP)* (Borsc et al., 2005)
  Bei WEP handelt es sich um das mittlerweile veraltete Verschlüsselungsverfahren für Funknetzwerke. Dieser kann innerhalb weniger Sekunden geknackt werden und sollte deshalb nicht mehr verwendet werden.
  Prinzipiell basiert dieses Verfahren auf einem pseudozufällig generier-

[27] Extendend Service Set Identifier

tem Bitstrom, der durch den RC4[28]-Algorithmus erzeugt wird. Die zu verschlüsselnde Nachricht wird dann mittels XOR Operator mit diesem Bitstrom verknüpft (siehe Abbildung 2.25).

Zur Verschlüsselung einer Nachricht (siehe Abbildung 2.26) wird aus

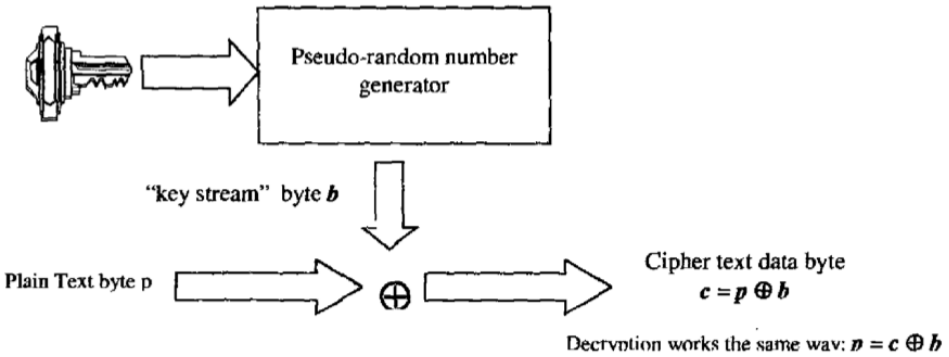


Abbildung 2.25: WEP Übersicht (Borsc et al., 2005)

einem 48 bit langem Initialisierungsvektor (Initialization vector) und einem geheimen Schlüssel (Secret Key) mithilfe des RC4-basierendem Pseudozufallsnummerngenerator (PRNG[29]) ein Bitstrom (Key Sequence) erzeugt. Dieser Schlüssel wird mittels XOR mit dem durch eine Prüfsumme (ICV durch CRC32[30]) ergänzten Klartext (Plaintext) verknüpft und somit verschlüsselt. Die Initialisierungswerte werden der verschlüsselten Nachricht vorangestellt (siehe Abbildung 2.27) und als Gesamtpaket verschickt.

Zur Entschlüsselung der Nachricht wird das Verfahren in umgekehrter

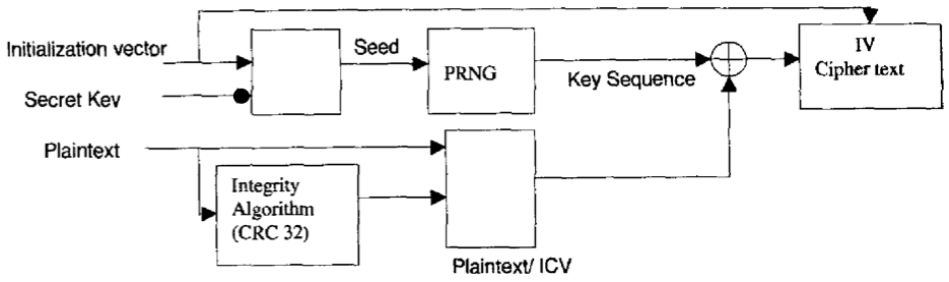


Abbildung 2.26: WEP Verschlüsselung (Borsc et al., 2005)

Reihenfolge auf das WEP-Paket angewendet (siehe Abbildung 2.28). Mit Hilfe des mitgeschickten Initialisierungsvektors und des geheimen

[28] Ronś Code 4 wurde von Ronald Rivest im Jahr 1987 entwickelt.
[29] Pseudo-Random Number Generator
[30] Cyclic Redundancy Check mit 32 Bit

Schlüssels wird der selbe Bitstrom wie beim Sender generiert und mittels XOR mit der verschlüsselten Nachricht verknüpft.

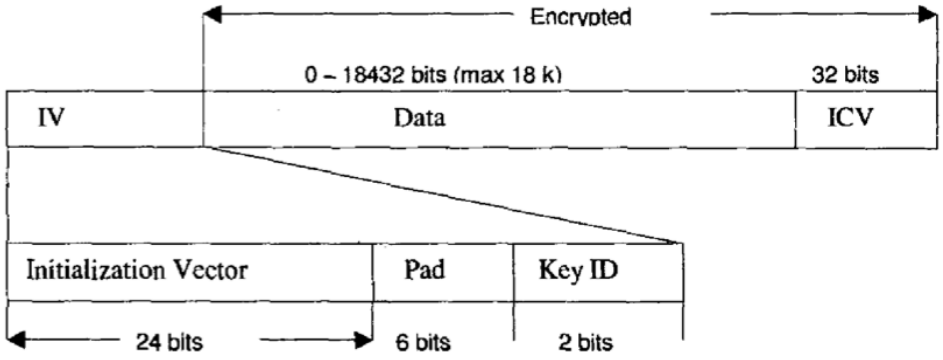


Abbildung 2.27: WEP Datenformat (Borsc et al., 2005)

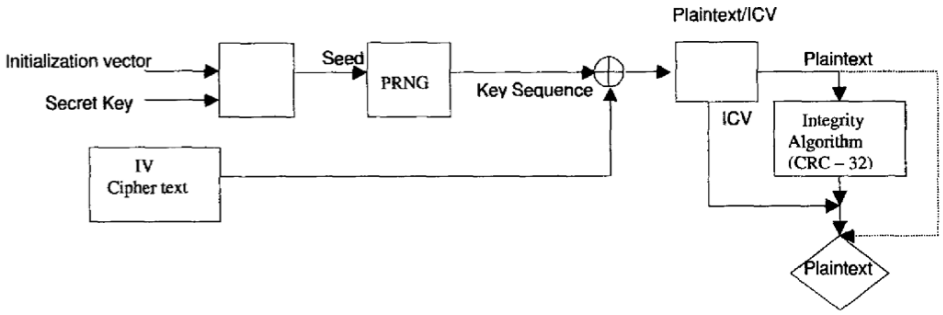


Abbildung 2.28: WEP Entschlüsselung (Borsc et al., 2005)

WEP verfügt außerdem über zwei Betriebsmodi:

- Open System
  Der Netzwerkverkehr wird lediglich über WEP verschlüsselt.
- Shared Key
  Die Netzwerkteilnehmer verfügen über einen gemeinsamen geheimen Schlüssel mithilfe dessen eine Authentifizierung vorgenommen und gleichzeitig der Datenverkehr verschlüsselt wird (wie in dem vorher beschriebenen Verfahren).

- *Wi-Fi Protected Access (WPA)* (Lashkari et al., 2009)
  Wi-Fi Protected Access wurde eingeführt, um die Probleme von WEP auszumerzen und eine komplexere Verschlüsselung zu ermöglichen ohne die Hardware auszutauschen. Es gibt zwei verschiedene Betriebsmodi:

1. Personal WPA
   Dieser Modus, auch bezeichnet als WPA-PSK[31], ist für kleine Firmen- und Heimnetzwerke gedacht und verwendet ähnlich wie WEP einen allen Teilnehmern bekannten alphanumerischen Schlüssel zur Authentifizierung. Dieser wird niemals über das Netzwerk übertragen und wird nur beim Aufbau der Verbindung verwendet. Zur Verschlüsselung des Datenverkehrs können Schlüssel bis zu einer Länge von 256 bit verwendet werden.
2. Enterprise WPA
   Enterprise WPA wird auch als Commercial WPA bezeichnet. Die Authentifizierung basiert auf dem IEEE 802.1X-Protokoll und benötigt einen Authentifizierungsserver (zum Beispiel RADIUS[32]), ist also nur für größere Firmennetzwerke geeignet. Vorteile sind vor allem die Verwendung von EAP[33] für die Authentifizierung und die damit perfekt verbundene Integration in den Microsoft Windows Anmeldeprozess.

WPA baut prinzipiell auf dem Verfahren von WEP auf. Vorteil ist aber die viel komplexere Verschlüsselung mittels TKIP[34]-Verfahren, welches den Initialisierungsvektor IV zweifach in die Schlüsselgenerierung einfließen lässt, wie Abbildung 2.29 zeigt. Weiters wurde auch die Länge des generierten Schlüssels auf 128 bit erhöht.
Sieht man sich WPA noch detaillierter an, steckt noch viel mehr Kom-

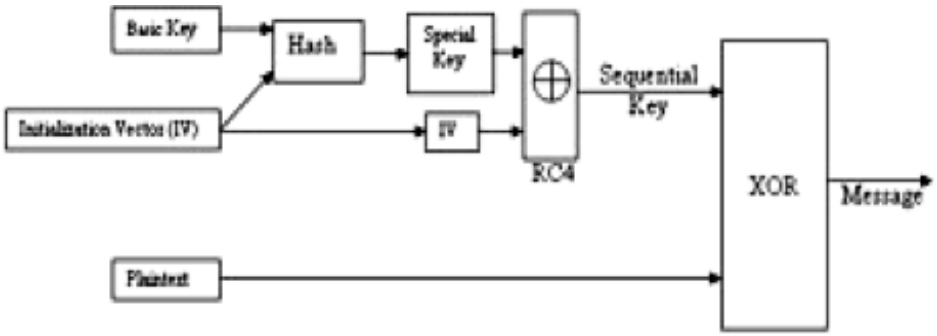


Abbildung 2.29: WPA Übersicht (Lashkari et al., 2009)

plexität in diesem Verfahren (siehe Abbildung 2.30). Zur Integritätsprüfung der Nachricht wird ein Message Integrity Code (MIC) generiert, mit einem eigenen 64 bit Schlüssel verschlüsselt und mitübertra-

[31] Pre-Shared Key
[32] Remote Authentification Dial-In User Service
[33] Extensible Authentication Protocol
[34] Temporal Key Integrity Check

gen. Um so genannten Replay-Attacken[35] vorzubeugen, wird der IV (siehe Abbildung 2.27) als Sequenznummer für Pakete verwendet, und bei jedem neuen TKIP-Schlüssel auf 0 zurückgesetzt. Da dieser in die Schlüsselberechnung mit einfließt, entsteht für jedes Paket ein eigener Schlüssel.
Trotz erhöhter Komplexität wurde das TKIP-Verfahren im November 2003 von Robert Moskowitz geknackt.(Lashkari et al., 2009)

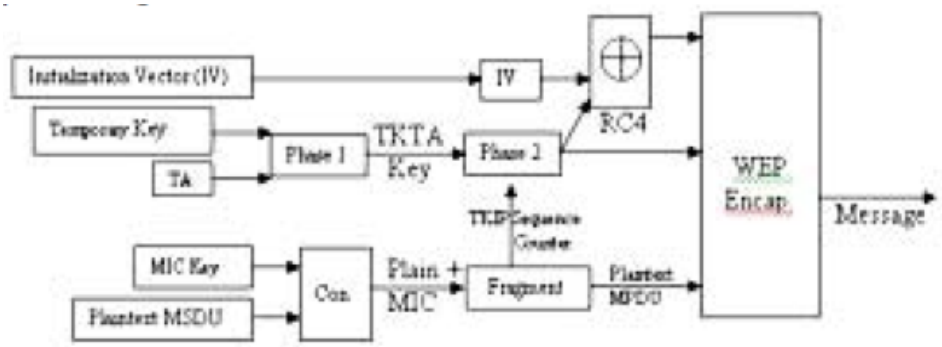


Abbildung 2.30: WPA TKIP Detail (Lashkari et al., 2009)

- *Wi-Fi Protected Access 2 (WPA2)*
  Die zweite Version des WPA-Verfahrens wurde im Jahr 2007 im IEEE 802.11i standardisiert. Es verwendet weiterhin das TKIP-Protokoll, ersetzt aber den RC4-Algorithmus durch den sichereren Advanced Encryption Standard (AES). Weiters wurde auch noch das zu TKIP alternative Verschlüsselungsprotokoll CCMP[36], welches ebenfalls auf AES basiert, verwendet.

Die Lokalisierung mittels WLAN stellt eine Alternative zur Bluetooth-Lokalisierung dar, ist aber nicht so verbreitet und nur bei neueren Smartphones verfügbar. Die höhere Reichweite stellt eher einen Nachteil als einen Vorteil dar, da die Möglichkeit besteht, dass der Benutzer auch außerhalb des Geschäftslokals eine Verbindung zum Access Point herstellen kann. Einen weiteren Nachteil stellen die Anschaffungskosten dar, die für die Basisstation entstehen. Ähnlich wie bei Bluetooth fällt auch hier Verwaltungsaufwand an, welcher beim Austausch des Access Points entsteht.

[35] Replay bedeutet, dass eine Übertragung aufgezeichnet und zu einem späteren Zeitpunkt nochmals übertragen wird.
[36] Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

2.9 Ultraschallortung

Diese Variante der Lokalisierung stammt nicht, wie man vielleicht vermutet, aus der Tierwelt, wo Tiere (wie beispielsweise eine Fledermaus) ein Ultraschallsignal aussenden und durch die reflektierten Wellen ihre Umgebung erkennen, basiert aber dennoch auf der Erkennung von Schallwellen.
Vorreiter auf diesem Gebiet ist die 2009 gegründete amerikanische Firma shopkick[37], über welche gerade erst zuletzt Mitte November wieder im technisch renommierten Online-Blog TechCrunch[38] berichtet wurde (siehe http://techcrunch.com/2010/11/16/target-rolls-out-shopkicks-geo-coupon-system-to-242-stores/). Viele vergleichbare Apps wie Foursquare[39] oder Gowalla[40] basieren auf dem Prinzip von manuellen Check-Ins. Als Check-In wird eine Funktion bezeichnet, die es einem Benutzer ermöglicht, sich an einem Standort (beispielsweise einem Geschäftslokal) anzumelden und über diverse Netzwerke seinen Freundeskreis oder gar die ganze Menschheit darüber zu informieren. Die Benutzer dieser Systeme bewegen sich also zu einem Standort, können sich dann über das Antippen eines Buttons bei diesem einchecken und erhalten dafür auf einem Reward-System basierende Punkte. Vorteil von shopkick gegenüber seinen Konkurrenten ist, dass der Check-In automatisch durchgeführt wird, sobald der Kunde das Geschäft betritt. Dies ermöglicht ein speziell entwickeltes System, bei dem Standorte von Interesse (POI...Point of Interest) von einem Ultraschallsender, welcher sich zum Beispiel an der Decke des Raumes befinden könnte, beschallt wird. Dieser Schall befindet sich in einem vom menschlichen Ohr nicht wahrnehmbaren Frequenzbereich[41], kann aber vom Mikrofon des Mobiltelefons erfasst werden und einem Standort innerhalb des Geschäftslokals zugeordnet werden. Dadurch lässt sich auch einfach durch installieren mehrerer Ultraschallsender eine In-House-Lokalisierung verwirklichen.
Leider ist die genaue Funktionsweise des shopkick-Systems nicht öffentlich bekannt und es können nur Mutmaßungen darüber getroffen werden. Folgende Varianten sind vorstellbar:

- *Frequenzvariation*
  Jedem Ultraschallsender wird eine eindeutige Frequenz und ein Standort zugeordnet. Nimmt das Mikrofon des Endgerätes eine bestimmte Frequenz war, so kann die ungefähre Position im Raum festgestellt werden. Da sich der Schall ausgehend von seiner Quelle symmetrisch in alle Richtungen ausbreitet, kann es aber auch zu Überschneidungen

[37] http://www.shopkick.com
[38] http://www.techcrunch.com
[39] http://www.foursquare.com
[40] http://www.gowalla.com
[41] Das menschliche Ohr kann Frequenzen von 16 Herz bis 20 kHz wahrnehmen, wobei mit zunehmendem Alter der obere Frequenzbereich immer mehr nachlässt. Der Ultraschallbereich befindet sich direkt darüber und reicht von 20 kHz bis 1,6 GHz.

kommen, die sich aber in ihrer Signalstärke unterscheiden würden.

- *Übertragungsmedium*
  Das Hochfrequenzband dient als Übertragungsmedium, über welches beispielsweise Informationen zum Standort übertragen werden. Auch hier kann es zu Überschneidungen von Signalen mehrerer Schallquellen kommen.

- *mathematischer Ansatz*
  Eine komplexere aber dadurch auch genauere Variante ist die mathematische Berechnung der Position. Diese funktioniert sowohl mit einem als auch mit mehreren Signalen. Hierbei gilt, je mehr Quellen verfügbar sind, desto genauer kann der Standort (beispielsweise über Triangulierung) bestimmt werden. Die Berechnungen basieren alle auf der Schallgeschwindigkeit c welche bei normalem Luftdruck (1013 hPa) und Raumtemperatur (20 Grad Celsius) bei 343 m/s liegt und durch die allgemeine Formel $c = \lambda * f$ beschrieben wird. λ repräsentiert dabei die Wellenlänge und f die Frequenz der Schallwelle.

  – Time of Arrival (ToA) / Time of Flight (ToF)
    Der Abstand d kann anhand der Ausbreitungsgeschwindigkeit c und der Zeit t, die zwischen dem Aussenden am Sender bis zum Eintreffen am Empfänger vergangen ist, berechnet werden. Zur Messung der Übertragungszeit wird der genaue Zeitpunkt der Aussendung t0 und der Ankunft t1 benötigt. Dies hat den Nachteil, dass Sender und Empfänger synchronisiert werden müssen. Die Formel für die Abstandsberechnung ist der Tabelle 2.19 zu entnehmen.

$$d = c * (t1 - t0)$$

Tabelle 2.19: Formel zur Berechnung des Abstands anhand der Übertragungszeit (Heinze et al., 2009)

Würde es nun drei Signalquellen A, B und C geben, könnte der Standpunkt trianguliert werden. Der genaue Hintergrund einer Triangulation kann dem Abschnitt 2.1 GPS entnommen werden. Die Rechenschritte zur Positionsbestimmung in einem dreidimensionalen Raum sind der Tabelle 2.20 zu entnehmen, wobei d für den Abstand zwischen der jeweiligen Signalquelle und dem Empfänger steht.

$$
\begin{aligned}
x &= \frac{d_A^2+d_B^2+d_C^2}{2*d_{A,B}} \\
y &= \frac{d_A^2-d_C^2+x_C^2+y_C^2}{2*y_C} - \frac{x_C}{y_C} * x \\
z &= \sqrt{d_A^2 - x^2 - y^2}
\end{aligned}
$$

Tabelle 2.20: Triangulierung im dreidimensionalen Raum (Heinze et al., 2009)

– Time Difference of Arrival (TDoA)
Diese Methode findet Anwendung bei Schwierigkeiten in der Berechnung der Signallaufzeit, beispielsweise durch Unkenntnis des Sendezeitpunktes, und benötigt insgesamt vier Signale. Dazu wird ein Gleichungssystem mit drei Unbekannten (die Koordinaten des Empfängers) und drei Gleichungen aufgestellt, deren Parameter die Empfangszeitpunkte der Signale A, B, C und D sind. Das Gleichungssystem ist der Tabelle 2.21 zu entnehmen.

$$
\begin{aligned}
t_B - t_A &= \tfrac{1}{c} * \sqrt{(x-x_B)^2 + (y-y_B)^2 + (z-z_B)^2} - \sqrt{x^2+y^2+z^2} \\
t_C - t_A &= \tfrac{1}{c} * \sqrt{(x-x_C)^2 + (y-y_C)^2 + (z-z_C)^2} - \sqrt{x^2+y^2+z^2} \\
t_D - t_A &= \tfrac{1}{c} * \sqrt{(x-x_D)^2 + (y-y_D)^2 + (z-z_D)^2} - \sqrt{x^2+y^2+z^2}
\end{aligned}
$$

Tabelle 2.21: Formel zur Positionsbestimmung bei unbekannter Signallaufzeit (Heinze et al., 2009)

– Angle of Arrival (AoA)
Diese Methode erlaubt es anhand einer Signalquelle nicht nur den Abstand d sondern auch den Winkel ψ zwischen Sender und Empfänger zu bestimmen. Die Berechnung basiert auf dem Prinzip der Phasenverschiebung, benötigt aber mehrere Antennen deren Abstand der halben Wellenlänge des Signals entspricht. Befindet sich der Empfänger direkt vor dem Sender (entspricht einem Winkel von 180 Grad), so kommen beide Signale gleichzeitig an und die Phasenverschiebung beträgt 0. Jeder andere Winkel würde eine Phasenverschiebung hervorrufen, welche in die Berechnung des Standortes mit einfließen kann.
Abbildung 2.31 stellt den Zusammenhang grafisch dar. Dabei wird der Sender durch Device i und der Empfänger durch Device j dargestellt. Winkel θ_i definiert die Signalausrichtung, ϕ_{ij} den Winkel der im Raum durch Sender und Empfänger aufgespannt wird und ψ_{ij} den Winkel von Sender zu Empfänger.

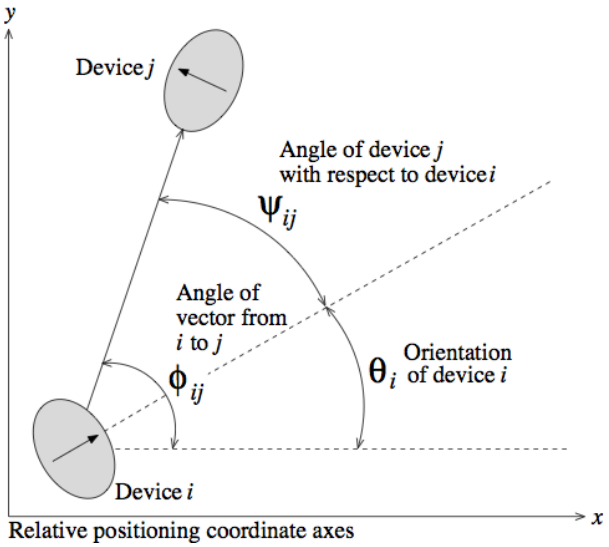


Abbildung 2.31: Angle of Arrival Zusammenhang (Hazas et al., 2005)

Die Rechenschritte sind der Tabelle 2.22 zu entnehmen.

$$d = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$$
$$\psi_{ij} = \phi_{ij}(x_i, y_i, x_j, y_j) - \theta_i$$

Tabelle 2.22: Positionsbestimmung anhand des Angle of Arrival (Hazas et al., 2005)

Anhand der Distanz d und des Winkels ψ_{ij} kann ausgehend von der Position des Senders nun der Standort bestimmt werden. Sind zwei Signale verfügbar, so kann die Position anhand des Winkels α von Signal A und des Winkels β von Signal B noch genauer bestimmt werden (siehe Tabelle 2.23).

$$y = \frac{d * sin(\beta)}{sin(\pi - \alpha - \beta)}$$
$$x = \frac{y}{tan(\alpha)}$$

Tabelle 2.23: Positionsbestimmung anhand des Angle of Arrival mit 2 Signalen (Heinze et al., 2009)

Da Schallwellen nicht unberührt von Störungen[42] bleiben, werden oft spezielle Algorithmen genutzt, die ihre Berechnung nicht auf einen Messwert stützen, sondern beispielsweise den Mittelwert mehrerer Berechnungen heranziehen oder auf einem neuronalen Netzwerk bzw. einem stochastischen Modell aufbauen. Die Behandlung dieser Algorithmen würde den Rahmen dieser Arbeit sprengen, jedoch sollten Schlagwörter wie "Multi Constant At A Time"[43] oder "Single Constant At A Time"[44] mit konkreten Algorithmen wie dem Kalman- oder dem Partikel-Filter genannt werden, deren genauere Bedeutung in weiterführender Literatur[45] nachgeschlagen werden kann.

Die In-House-Lokalisierung über Schallwellen stellt eine interessante, genaue aber auch aufwändige Ergänzung zu den bestehenden Lokalisierungstechnologien dar. Größter Vorteil ist wohl, dass am Mobiltelefon keinerlei zusätzliche Hardware benötigt wird. Lediglich ein Mikrofon ist von Nöten welches aber zur Standardausstattung zählt und in wirklich jedem Handy integriert ist. Ein weiterer Vorteil ist die relativ hohe Genauigkeit, wodurch sogar einzelne Bereiche relativ genau ausgestrahlt werden können. Nachteil ist allerdings der hohe Entwicklungsaufwand und die Anschaffungskosten für die Hardware. Aus diesen Gründen ist das System vor allem für große Indoor-Anwendungen, wie zum Beispiel in Kaufhäusern, geeignet, die in diesem Fall als Entwicklungs- und Finanzierungspartner auftreten sollten und erst im etablierten Zustand bei kleinen Geschäftslokalen umgesetzt werden sollte.

2.10 Near Field Communications (NFC)

Near Field Communications ist eine Technologie, die es Geräten ermöglicht drahtlos über eine kurze Distanz zu kommunizieren. Diese Beschreibung ähnelt der in Abschnitt 2.7 vorgestellten Technologie Bluetooth, welche sich aber in vielen, in diesem Abschnitt behandelten, Punkten unterscheidet. Es wird klar werden, dass Near Field Communications viele Ähnlichkeiten mit den in Abschnitt 2.5 und 2.6 vorgestellten Strich- und 2D-Codes hat. NFC basiert auf der RFID[46]-Technologie, welche es einem der Kommunikationspartner ermöglicht ohne Stromquelle auszukommen. Über ein Magnetfeld wird Strom induziert, wodurch die Kommunikation in einem kleinen Umfeld ermöglicht wird. Dies ermöglicht den Benutzern durch einfache Berührung

[42] Dazu zählen Punkte wie Absorption, Brechung, Streuung, Beugung oder Reflexion, welche aber in abgeschirmten Umgebungen wie Verkaufsräumen und den damit verbundenen kurzen Distanzen kaum zu tragen kommen.

[43] MCAAT; die Berechnung basiert auf dem Mittelwert mehrerer Messungen

[44] SCAAT; die Berechnung basiert auf nur einer Messung. Diese wird dann mit anderen Messungen verglichen und der am nächste Nachbar oder die wahrscheinlichste Messung wird als Referenz herangezogen.

[45] (Hazas et al., 2005), (Heinze et al., 2009)

[46] Radio Frequency Identifier

oder Annäherung Daten auszutauschen oder Geräte zu verbinden.

2.10.1 Radio Frequency Identifier (RFID)

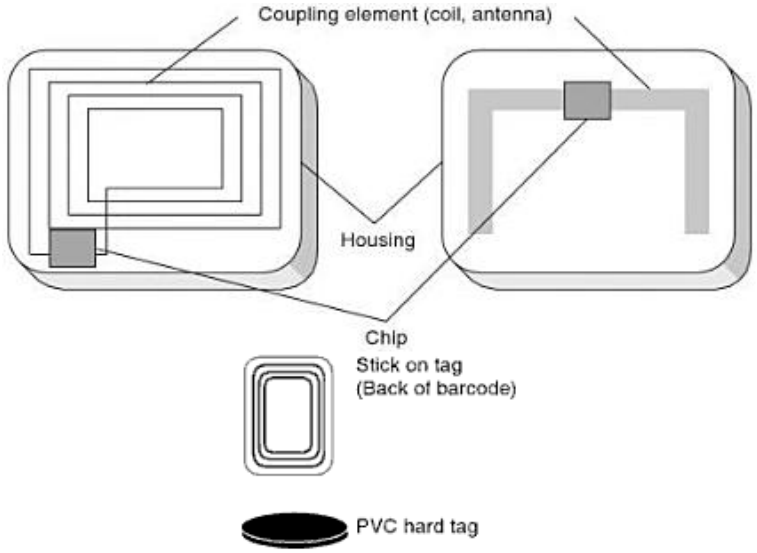


Abbildung 2.32: RFID Tag Aufbau und Designs (Finkenzeller, 2010)

Um NFC besser verstehen zu können, wird die zugrunde liegende RFID-Technologie noch etwas genauer beleuchtet. Das RFID System besteht aus einem Reader/Writer Gerät und einem Tag, welcher die Daten zur Verfügung stellt bzw. speichert. Ein Tag besteht dabei grundsätzlich aus einem Chip und einer Antenne (siehe Abbildung 2.32). Wie bereits erwähnt, ist es möglich, dass ein Kommunikationspartner ohne aktive Stromquelle auskommt. Deshalb werden folgende zwei Betriebsmodi unterschieden: (Finkenzeller, 2010)

- *Aktiver Modus*
  Im aktiven Modus verfügen sowohl der RFID Reader/Writer als auch der RFID Tag über eine eigene Stromquelle.

- *Passiver Modus*
  Im passiven Modus bezieht der RFID Tag seinen Strom aus dem vom RFID Reader/Writer erzeugtem Magnetfeld mittels Induktion (siehe Abbildung 2.33).

Die Daten des RFID Tags werden auf einem Chip gespeichert, dessen Speicherkapazität von einem Byte bis zu mehreren Kilobytes reichen kann. Für spezielle Anwendungsfälle gibt es auch einen Ein-Bit Chip, welcher wie ein

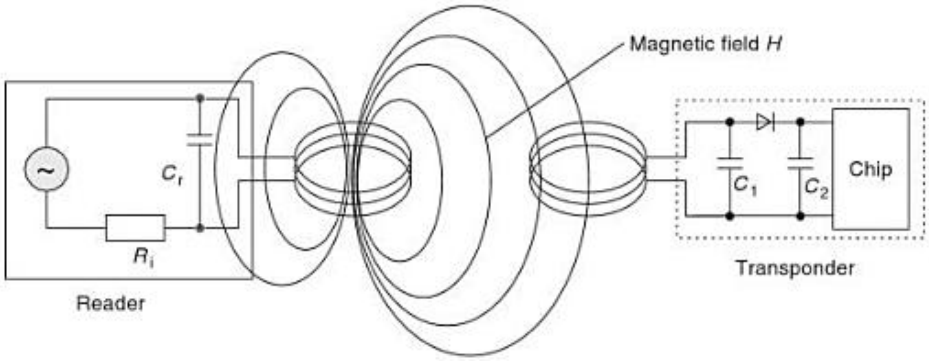


Abbildung 2.33: Induktion durch ein Magnetfeld (Finkenzeller, 2010)

Schalter wirkt. Beispielsweise könnte dieses Bit eine Eintrittskarte als "gültig" oder "bereits entwertet" kennzeichnen. Betritt der Kunde das Areal wird diese Bit gesetzt und kann nicht nochmals entwertet werden. Erst bei einem temporären Verlassen des Geländes (zum Beispiel zum Aufsuchen der Toiletten) wird dieses Bit wieder zurückgesetzt und die Karte kann für das erneute Betreten wieder entwertet werden. Die Chips können weiters schreib- und lesbar oder auch nur lesbar sein. Zweiteres wird für Seriennummern oder im speziellen Fall von Ein-Bit Tags für den Diebstahlschutz in Kaufhäusern eingesetzt. Weiters besteht auch die Möglichkeit einen Mikrocontroller auf dem Tag zu platzieren, welcher es ihm ermöglicht mithilfe eines kleinen Betriebssystems Anwendungen auszuführen oder selbst Berechnungen zu tätigen.
Die von RFID verwendeten Frequenzen zur Datenübertragung lassen sich in drei Frequenzbänder aufteilen: (Finkenzeller, 2010)

- *Low Frequency (LF)*
  Der niederfrequente Bereich reicht von 30 kHZ bis zu 300 kHz.
- *High Frequency (HF)/Radio Frequency (RF)*
  Dieser umfasst die Frequenzen von 3 MHz bis zu 30 MHz.
- *Ultra High Frequency (UHF)*
  Die Frequenzen 300 MHz bis 3 GHz werden dem hochfrequentem Band zugeordnet.

Um Überschneidungen von Übertragungen zu verhindern werden die Signale mittels Amplitudenmodulation[47], Frequenzmodulation[48] und Phasenmodulation[49] übertragen. Das gewählte Frequenzband hat auch Auswirkungen auf

[47] Durch Variation der Amplitude ist es möglich, mehrere Signale auf einer Frequenz zu übertragen.
[48] Die Signale werden auf unterschiedlichen Frequenzen übertragen.
[49] Durch Verschiebung der Phase ist es möglich mehrere Signale auf einer Frequenz mit der selben Amplitude zu übertragen.

die Reichweite bzw. die maximale Distanz zwischen Reader und Tag, deshalb unterscheidet man folgende Typen: (Finkenzeller, 2010)

- Close-Coupling Systeme mit einer Reichweite < 1 cm
- Remote-Coupling Systeme mit einer Reichweite < 1 m
- Long-Range Systeme mit einer Reichweite > 1 m

Ähnlich wie bei vielen anderen Datenübertragungstechnologien existieren auch hier mehrere Übertragungsmodi. RFID verfügt über insgesamt 3 Möglichkeiten, um Daten zwischen einem Reader/Writer Gerät und einem Tag zu übertragen, welche sich hinsichtlich Kommunikationsabfolge und Energieübertragung unterscheiden (siehe Abbildung 2.34) und wie folgt definiert sind: (Finkenzeller, 2010)

- *Full-Duplex Modus (FDX)*
  Der Full-Duplex Modus erlaubt es beiden Teilnehmern gleichzeitig zu kommunizieren. Das heißt, während der Tag noch seine Daten überträgt, kann der Reader/Writer bereits neue Daten anfordern oder auch schreiben. Die Energieversorgung wird während der kompletten Kommunikationszeit vom Reader/Writer sichergestellt. Die beidseitigen Übertragungen können sowohl im selben Frequenzbereich stattfinden, was als subharmonic bezeichnet wird, oder in komplett unabhängigen Frequenzbereichen, was als anharmonic bezeichnet wird. (Finkenzeller, 2010)

- *Half-Duplex Modus (HDX)*
  Im Half-Duplex Modus finden die Übertragungen abwechselnd statt, somit ist entweder der Uplink oder der Downlink aktiv. Das heißt, der Reader/Writer fordert Daten an, darauf folgend werden diese vom Tag übertragen und erst nach vollständiger Übertragung kann der Reader/Writer weitere Operationen ausführen. Gleich wie beim Full-Duplex Modus wird die Energie während der kompletten Kommunikation vom Reader/Writer zur Verfügung gestellt.

- *Sequentieller Modus (SEQ)*
  Der sequentielle Modus entspricht im wesentlichen dem Half-Duplex Modus, da nur entweder der Uplink oder der Downlink aktiv sein kann. Der Unterschied besteht in der Energieversorgung, die nur aufrecht ist während der Reader/Writer aktiv ist, also selbst gerade Operationen ausführt. Hat er diese beendet, wird er inaktiv und damit auch sein Magnetfeld. Das bedeutet für den Tag, dass er schon zuvor die Energie zwischenspeichern muss, um dann selbst aktiv zu werden. Meist werden für die Energiespeicherung kleine Kondensatoren oder Batterien verwendet.

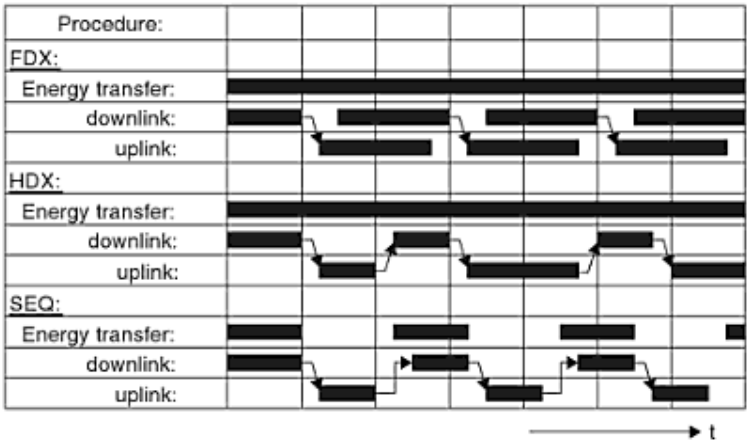


Abbildung 2.34: RFID Übertragungsmodi (Finkenzeller, 2010)

Da es bei RFID keine direkte Adressierung der Teilnehmer gibt, sind Mechanismen von Nöten, welche die Kommunikation überwachen. Wenn der RFID Reader/Writer Daten benötigt, baut dieser sein Magnetfeld auf und sendet eine Anfrage aus. Dies wird als Broadcast bezeichnet, da diese von allen Tags in Reichweite des Readers/Writers empfangen und auch beantwortet wird. Dadurch kommt es zu Überschneidungen, da das Magnetfeld als Übertragungsmedium von allen Teilnehmern gleichzeitig benutzt wird. In der Kommunikationstechnik wird diese Problematik als "Multiple Access" bezeichnet und durch eine der folgenden Methoden behandelt: (Finkenzeller, 2010)

- *Frequency Division/Multiple Access (FDMA)*
  Jedem Teilnehmer wird eine gewisse Frequenz bzw. ein Frequenzband zugeordnet, auf dem nur er überträgt.
- *Time Division/Multiple Access (TDMA)*
  Jedem Teilnehmer werden Zeitschlitze ("Time Slots") zugeordnet, in welchen ihm die Übertragung ermöglicht wird.
- *Space Division/Multiple Access (SDMA)*
  Jedem Teilnehmer wird physisch ein eigener Reader/Writer oder zumindest eine Antenne des Readers/Writers zugeordnet, die nur er benutzt.
- *Code Division/Multiple Access (CDMA)*
  Jedem Teilnehmer wird ein eigener Code zugeordnet, über welchen der Reader/Writer die Daten unterscheiden und korrekt zuordnen kann.

Diese Methoden sind jedoch für RFID meist nicht anwendbar, da sie auf eine längere Kommunikation ausgerichtet sind, wo hingegen bei RFID die

Kommunikationsverbindungen oft nur sehr kurzlebig sind. Aus diesem Grund wurden die obigen Verfahren an die Erfordernisse von RFID angepasst um so Kollisionen zu vermeiden. Unter anderem entstanden diese Verfahren: (Finkenzeller, 2010)

- *ALOHA*
  Dieses sehr einfache Verfahren basiert auf den unterschiedlichen Wartezeiten ("Timeout") der einzelnen Teilnehmer, die im Fall einer fehlgeschlagenen Übertragung zum Einsatz kommen. Es beginnt mit der Anfrage des Readers/Writers, worauf alle Tags gleichzeitig ihre Daten übertragen. Dadurch kommt es zu vielen Kollisionen, die Daten werden zerstört und viele der Tags erhalten keine Bestätigung über eine erfolgreiche Übertragung. Nach einer gewissen Wartezeit, die sich wie bereits erwähnt von Tag zu Tag unterscheidet, werden die Daten nochmals übertragen. Diese Prozedur wiederholt sich, bis die Daten korrekt übertragen wurden. Durch die unterschiedlichen Wartezeiten verursachten unterschiedlichen Sendezeiten wird die Wahrscheinlichkeit erhöht, dass es zu keiner Kollision kommt. Wie sich bereits erahnen lässt, wird durch dieses wirklich einfache Verfahren der Datendurchsatz erheblich geschmälert.

- *Unterteiltes ALOHA*
  Ein verbessertes ALOHA stellt das unterteilte ALOHA ("Slotted ALOHA") dar. Dies soll das gleichzeitige Senden aller Tags verhindern, indem es eine fix vorgegebene Anzahl an Zeitschlitzen verwendet. Ähnlich wie beim einfachen ALOHA sendet der Reader/Writer eine Anfrage an sein Netzwerk, gibt aber gleichzeitig seine Zeitschlitze bekannt. Jeder der Tags wählt für sich einen Schlitz aus und sendet zu diesem Zeitpunkt seine Seriennummer an den Reader/Writer. Dadurch kann es zwar wiederum zu Kollisionen kommen, der Reader/Writer überprüft jedoch all seine Zeitslots und sucht jene ohne Kollision. Mit Hilfe der Seriennummer wird dieser eine Tag selektiert und auf Daten abgefragt. Zwar wird hier wieder ein Broadcast ausgeführt, jedoch antwortet nur der Tag mit der entsprechenden Nummer und die Daten können ohne Kollision übertragen werden. Danach beginnt der Prozess wieder von vorne.
  Da dieses Verfahren mit einer fixierten Anzahl an Zeitschlitzen arbeitet, ist dessen Erfolg abhängig von der sich in Reichweite des Readers/Writers befindlichen Tags. Je mehr Tags es sind, desto unwahrscheinlicher ist eine Übertragung ohne Kollision.

- *Dynamisches ALOHA*
  Um den Problemen einer fixen Zeitschlitzanzahl entgegenzuwirken wurde das dynamische ALOHA ("dynamic ALOHA") eingeführt, welches die Anzahl dynamisch verändern kann. Ähnlich wie beim unterteilten

ALOHA werden die Schlitze bei der Anfrage mitübertragen. Findet sich bei der darauffolgenden Antwort der Tags kein einziger kollisionsfreier Zeitschlitz, so wird deren Anzahl erhöht und die Anfrage erneut geschickt. Diese Prozedur wird so lange wiederholt, bis sich zumindest ein kollisionsfreier Schlitz findet. Ist eine Seriennummer gefunden, wird allen Knoten mitgeteilt, dass sie die Aussendung ihrer Seriennummer beenden können und es wird fortgefahren, wie bisher. Der Tag mit der Seriennummer wird selektiert, nach Daten abgefragt und die Prozedur beginnt wieder von vorne.

Da auch RFID wie jede andere Funktechnologie Störungen unterworfen ist, die die übertragenen Daten beeinflussen können, kann RFID folgende Techniken verwenden, um einen Übertragungsfehler aufzuspüren: (Finkenzeller, 2010)

- *Paritätsprüfung*
  Zu jedem Byte wird zusätzlich ein Bit zur Paritätsangabe übertragen. Dieses Bit gibt an, ob sich in den acht Bit eine gerade Anzahl ("Even") oder eine ungerade Anzahl ("Odd") an 1en befindet. Dadurch können 1-Bit-Fehler in der Datenübertragung erkannt werden.

- *Längssummenprüfung (LRC...Longitudinal Redundancy Check)/XOR-Summe*
  Dieses Verfahren berechnet über einen Datenblock (eine Folge von Datenwörtern) ein Prüfsummenbyte, welches spaltenweiße über mehrere Datenbytes gebildet wird. Dabei wird das erste Bit des ersten Bytes mit dem ersten Bit des zweiten Bytes mittels XOR verknüpft. Das Ergebnis dieser Operation wird dann mit dem ersten Bit des dritten Bytes mittels XOR geknüpft. Nachdem mit allen weiteren ersten Bits der Bytes gleich verfahren wurde, erhält man das erste Bit der Prüfsumme. Nun fährt man mit dem zweiten Bit fort. Es wird also die XOR-Summe über die einzelnen Spalten mehrerer Datenwörter gebildet woraus ein Prüfsummenwort entsteht. Dieses wird mitübertragen und der Empfänger prüft dann den Datenblock inklusive dem Prüfsummenwort mit dem selben Verfahren. Dieses sollte das Ergebnis 0 ergeben, ansonsten war die Übertragung nicht korrekt. Dieses Verfahren erkennt auch nur 1-Bit-Fehler in der Übertragung.

- *Zyklische Redundanzprüfung (CRC...Cyclic Redundancy Check)*
  Bei diesem Verfahren werden die Datenbits durch ein binäres CRC-Polynom dividiert (bitweise mittels XOR). Der dadurch entstehende Rest stellt die CRC Prüfsumme dar. Diese wird mitübertragen und ähnlich wie bei LRC in die Berechnung beim Empfänger miteinbezogen. Die entstehende Prüfsumme sollte wiederum 0 ergeben, ansonsten trat während der Übertragung ein Fehler auf. Zum besseren Verständ-

nis ist der Tabelle 2.24 eine Beispielberechnung zu entnehmen.
Die CRC Prüfung erlaubt es auch Mehr-Bit-Fehler zu erkennen.

10011101	Daten
1010	CRC-Polynom (4 bit)
00111101	Ergebnis
1010	
00010101	
1010	
001	CRC-3 Prüfsumme (3 bit)

Tabelle 2.24: Berechnung einer CRC-3 Prüfsumme

Nachdem die der Near Field Communication zugrunde liegende Technologie RFID genauer betrachtet wurde, kann nun weiter auf Prinzipien und Funktionsweisen von NFC eingegangen werden.

Wie nun erkenntlich gemacht wurde, weisen RFID Tags sehr viel Ähnlichkeiten mit Strich- und 2D-Codes auf. Diese dienen in vielen Anwendungsfällen ebenfalls als Datenspeicher oder um Dinge eindeutig identifizieren zu können, wurden aber in vielerlei Hinsicht erweitert. Die Daten sind weiterhin digitalisiert, werden aber nicht mehr auf einem analogen Medium wie Papier aufgedruckt, sondern werden nun auch digital auf Chips gespeichert. Auch die Datenerfassung ist weiterhin kontaktlos, wurde aber durch die Verwendung einer Funkübertragung modernisiert. Die damit verbundene Integritätsprüfung, um Erfassungs- bzw. nun Übertragungsfehler zu erkennen, blieb weiterhin erhalten und basiert immer noch auf Paritätsprüfungen oder CRC-Prüfsummen. Neu ist allerdings die Selbstständigkeit, die einem Tag durch eine Stromquelle und einen Mikroprozessor gegeben wird, die größere Speicherkapazität und der erweiterte Funktionsumfang, welcher dadurch ermöglicht wird.
Trotz der vielen Erneuerungen bleibt die Idee als Lokalisierungsanwendung die selbe. Die für den Zweck der Gutscheineinlösung bedeutsamen Orte, wie beispielsweise eine Kasse, an der der Gutschein für die Verrechnung verwendet wird, sollen mit Tags versehen werden, welche auf ihrem Chip das Geheimnis enthalten. Der Kunde geht also zur Kasse um seinen Einkauf zu bezahlen und will den am Gutschein angepriesenen Rabatt wahrnehmen. Dazu fährt er mit seinem Mobiltelefon kurz über den Tag, wodurch das Geheimnis ausgelesen und beim Einlösen mitübertragen wird. Durch dieses Geheimnis kann wiederum sichergestellt werden, dass sich der Kunde im Geschäftslokal befindet. Durch die erweiterte Funktionalität eröffnen sich auch neue Möglichkeiten. Beispielsweise könnten Plakate oder Flyer mit Tags versehen werden, welche User beim Vorübergehen über neue Aktionen auf ihrem

Mobiltelefon benachrichtigen oder sie direkt zu dem Gutschein navigieren.

2.10.2 NFC - Anwendung von RFID

NFC wurde von dem aus Philips ausgegliederten Unternehmen Next Experience Semiconductors (NXP) zusammen mit Sony spezifiziert und ist nach ISO/IEC 14443 und ISO/IEC 18092 standardisiert. Großer Vorteil gegenüber Bluetooth ist, dass zwei Geräte ganz spontan ohne besondere Authentifizierung miteinander verbunden werden können, indem sie einfach nah aneinander gehalten werden. Eines der Geräte nimmt dabei die Rolle des NFC Readers/Writers ein, während der andere Kommunikationsteilnehmer als NFC Tag bezeichnet und über die magnetische Induktion betrieben wird. Dieser Tag besteht aus einem Schaltkreis, welcher die gespeicherten Daten enthält und einer Antenne, über welcher der NFC Reader/Writer die Daten auslesen oder auch schreiben kann.
Bei Near Field Communications handelt es sich um eine noch nicht etablierte Technologie. Die Hauptanwendungsbereiche werden aber in folgenden Feldern gesehen: (Innovision Research & Technology plc, 2010a,b)

- *Identifizierung*
  NFC Geräte könnten beispielsweise Ausweiskarten ersetzen, indem die Informationen auf einem Smartphone gespeichert werden. Die NFC Technologie ermöglicht einen einfachen Informationsaustausch.
  In Japan werden Studentenausweise am Handy gespeichert und erlauben dem Student sich mit seinem Telefon für Kurse zu registrieren oder bestimmte Räumlichkeiten zu betreten. (Paus, 2007)

- *Zutrittskontrolle*
  Als Erweiterung der Identifizierung könnten auch Zutrittsberechtigungen auf dem Gerät gespeichert werden. Genauso könnte das Mobiltelefon auch als Haustürschlüssel fungieren.

- *Peer-To-Peer Kommunikation*
  Dies soll ähnlich zu Bluetooth die Kommunikation zwischen zwei Geräten ermöglichen beziehungsweise den Bluetooth-Verbindungsaufbau erleichtern. Handelt es sich um kleine Datenmengen, so kann NFC selbst als Übertragungsmedium dienen. Bei größeren Datenmengen wird allerdings ein leistungsfähigeres Trägermedium wie Bluetooth oder WLAN benötigt, wobei NFC in diesem Fall den Verbindungsaufbau vereinfacht.

- *Zahlungsverkehr und Kartenvertrieb*
  NFC-Geräte sollen beispielsweise als elektronische Geldbörse, Parkticket oder als digitale Eintrittskarte fungieren.

- *Dienstanbindung*
  NFC soll einen nahtlosen Übergang zwischen Dienstanpreisung und Dienstleistung ermöglichen. Ein Beispiel hierfür wären "Smart Posters", welche mit einem NFC Tag versehen sind und einen neuen Film bewerben. Durch Bewegen eines NFC Readers (zum Beispiel einem Mobiltelefon) über den Tag wird der Benutzer zum Kartenservice des nächstgelegenen Kinos weitergeleitet oder erhält weitere Informationen zum angepriesenen Film.

Als Übertragungsmedium nutzen NFC-Geräte das lizenzfreie 13,56 MHz ISM Frequenzband. Sie fallen mit einer Reichweite von bis zu 20 Zentimetern in die Kategorie der "Remote-Coupling Systeme" und unterstützen derzeit folgende Übertragungsraten: (Innovision Research & Technology plc, 2010a)

- 106 kbit pro Sekunde,
- 212 kbit pro Sekunde und
- 424 kbit pro Sekunde.

Ähnlich wie bei RFID (siehe Abschnitt 2.10.1) definiert das NFC Protokoll zwei Betriebsmodi: (Innovision Research & Technology plc, 2010a)

1. *aktiver Modus*
   Beide Geräte arbeiten mit ihrer eigenen Stromquelle und erzeugen jeweils ein magnetisches Feld. Dieser Modus kommt hauptsächlich beim Verbinden zweier Geräte zum Einsatz.

2. *passiver Modus*
   Im passiven Modus nimmt ein Gerät den Status eine Readers/Writers ein und ist somit für die Stromversorgung verantwortlich. Das gegenüberstehende Gerät fungiert als Tag, welcher vom magnetischen Feld des Readers/Writers betrieben wird, und stellt seine Daten zur Verfügung bzw. speichert die empfangenen Daten. Dieser Modus kommt vor allem in Umgebungen zum Einsatz, in denen Geräte mit temporären Stromquellen, wie beispielsweise Akkus, arbeiten. Dazu zählen vor allem mobile Geräte wie Smartphones.

Ein besonderes Augenmerk ist dabei auf die Rollenzuteilung von Kommunikationsinitiator und Kommunikationsziel zu legen. Ein schematischer Ablauf ist der Abbildung 2.35 zu entnehmen. Der Initiator ist jenes Gerät, welches Daten lesen oder schreiben will. Dafür baut dieser sein Magnetfeld auf und schickt eine Anfrage aus, worauf das vermeintliche Ziel antwortet. Da sich auch mehrere Ziele im Bereich des Initiators befinden können, sind diverse Verfahren anzuwenden, um eine Kollision zu vermeiden (siehe Abschnitt 2.10.1). Im Falle einer passiven Kommunikation[50] nimmt das aktive Gerät

[50] Als passive Kommunikation wird die Kommunikation zwischen einem aktiven Gerät und einem passiven Gerät bezeichnet.

immer die Rolle des Initiators und das passive Gerät die Rolle des Ziels ein. Handelt es sich aber um eine aktive Kommunikation[51], so wird jenem Gerät die Initiator-Rolle zugewiesen, welcher die Kommunikation beginnt. Grundsätzlich nehmen alle Geräte die Rolle des Kommunikationszieles an und werden nur zum Initiator, wenn es die Anwendung erfordert.
Die Rolle des Initiators kann allerdings nur von einem aktiven NFC Gerät übernommen werden. Deshalb ist auch die Kommunikation zwischen zwei passiven Geräten nicht möglich (siehe Tabelle 2.25).
Aktive und passive NFC Geräte unterscheiden sich nicht nur in den Rol-

	Initiator	Ziel
Aktiv	Möglich	Möglich
Passiv	Nicht möglich	Möglich

Tabelle 2.25: Mögliche Kommunikationsrollen von NFC Geräten (Paus, 2007)

le, die sie einnehmen können, sondern auch in der Art wie sie ihre Daten übertragen. Es werden zwei Datenkodierungen unterschieden: (Paus, 2007)

- *Manchester Kodierung*
  Die Manchester Kodierung verwendet den Spannungswechsel um die Daten zu kodieren. Dabei stellt ein Spannungsanstieg ("Low-To-High") eine logische 0 und ein Spannungsabfall ("High-To-Low") eine logische 1 dar (siehe Abbildung 2.36).

- *Modifizierte Miller Kodierung*
  Die Miller Kodierung verwendet ebenfalls Spannungswechsel um Daten zu kodieren, jedoch ist die Bedeutung eines Wechsels abhängig von seiner zeitlichen Abfolge. Während die logische 1 immer durch einen Spannungsabfall im dritten und einen neuerlichen Anstieg im vierten Quadranten einer Periode kodiert wird, ist die Kodierung der logischen 0 abhängig von dem vorhergehenden Bit (siehe Abbildung 2.37).

Je nach Geräteart und verwendeter Übertragungsraten wird eines der oben beschriebenen Verfahren in Kombination mit einer ASK[52]-Modulation verwendet. Passive Geräte verwenden immer die Manchester-Kodierung in Verbindung mit einer 10%igen ASK-Modulation, während aktive Geräte hingegen bei einer Übertragungsrate von 106 kBit/sec die modifizierte Miller Kodierung mit einer 100%igen ASK-Modulation anwenden (siehe Tabelle

[51] Als aktive Kommunikation wird die Kommunikation zwischen zwei aktiven Geräten bezeichnet. Hierbei müssen sich beide Geräte mit der Generierung des Funkfeldes abwechseln, wenn sie Daten senden wollen.

[52] Amplitude-Shift Keying moduliert die Daten, indem logische 0 und 1 durch Variation der Amplitude dargestellt werden.

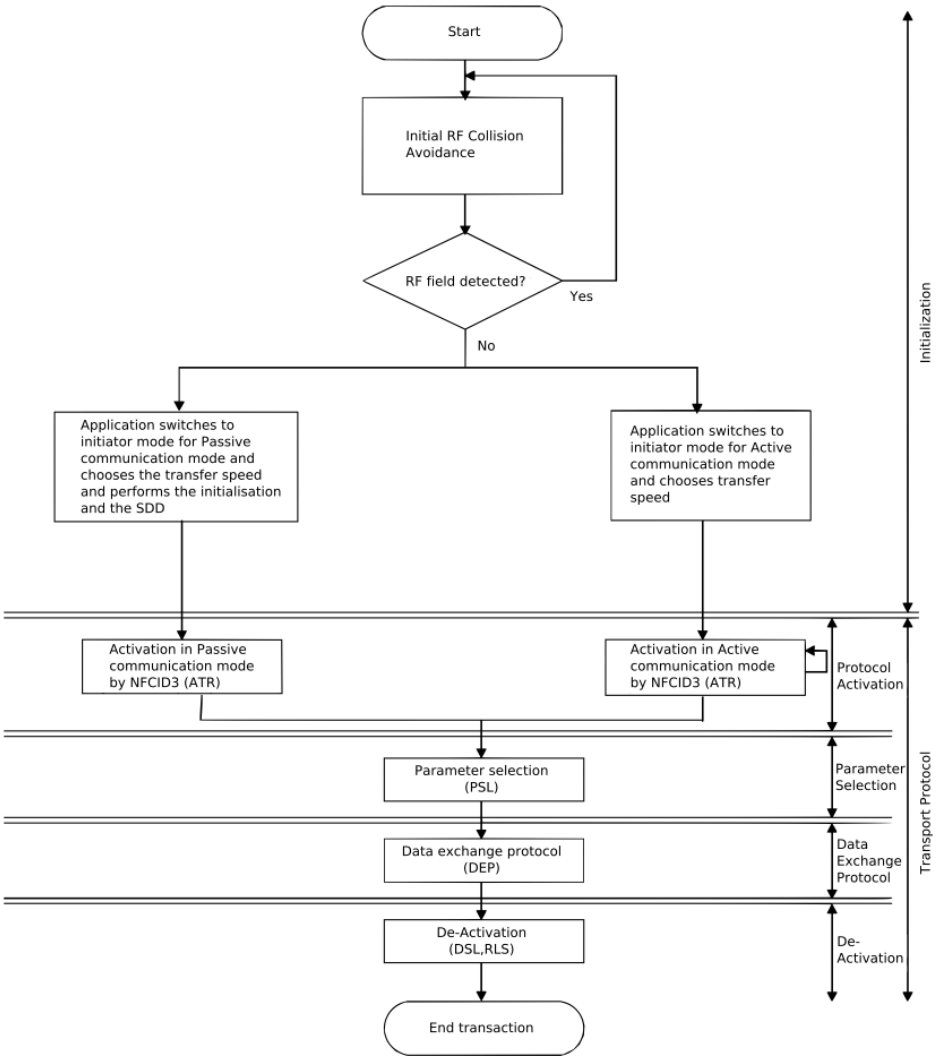


Abbildung 2.35: Schematischer NFC Kommunikationsablauf (Paus, 2007)

2.26).

	Aktiv	Passiv
106 kBit/sec	Modified Miller + 100% ASK	Manchaster + 10% ASK
212 kBit/sec	Manchaster + 10% ASK	Manchaster + 10% ASK
424 kBit/sec	Manchaster + 10% ASK	Manchaster + 10% ASK

Tabelle 2.26: Kodierung und Modulation in Abhängigkeit zur Übertragungsrate (Paus, 2007)

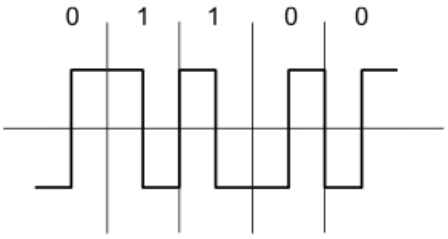


Abbildung 2.36: Manchester Kodierung (Paus, 2007)

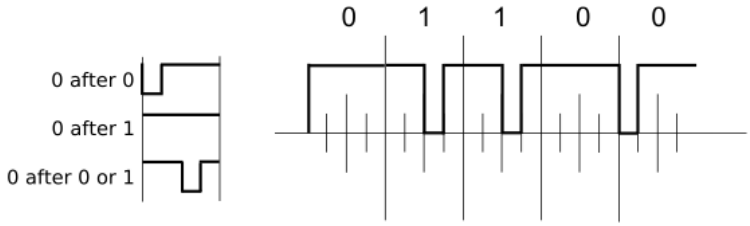


Abbildung 2.37: Modifizierte Miller Kodierung (Paus, 2007)

Um die Kommunikation zwischen NFC Geräten zu vereinheitlichen, wurden vier verschiedene Tag-Formate eingeführt, welche alle auf dem ISO Standard 14443 basieren. Diese unterscheiden sich hauptsächlich anhand folgender Kriterien: (Innovision Research & Technology plc, 2010b)

- Umschaltbar zwischen schreib-/lesbar und nur lesbar
  Geräte, welche sowohl schreib- und lesbar als auch nur lesbar sein können, werden als so genannte "Dual State"-Geräte bezeichnet (siehe Abbildung 2.38). Sind Geräte jedoch nur lesbar, können sie nur ein einziges mal beschrieben werden und behalten dann ihren Status für immer.

- Speicherkapazität
  Die Größe des Speichers ist ein Punkt, welcher vor allem mit den Punkten Sicherheitsmechanismen und Preis eng verbunden ist. Da eine Verschlüsselung oder Signierung einen Overhead an Daten verursacht, steht die Auswahl der Sicherheitsmechanismen in kompletter Abhängigkeit zum verfügbaren Datenspeicher. Dies beeinflusst indirekt den Preis, da mehr Speicherkapazität auf geringem Platz untergebracht werden muss.

- Sicherheitsmechanismen
  Abhängig vom Anwendungsfall sind diverse Mechanismen zur Absicherung der Daten und deren Integrität von Nöten. Beispielsweise ist es

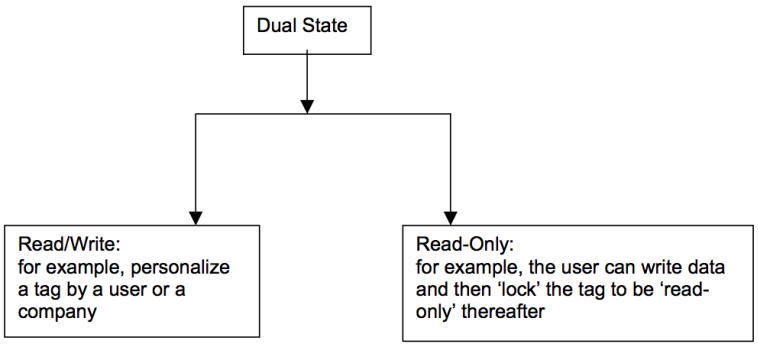


Abbildung 2.38: NFC Dual-State (Innovision Research & Technology plc, 2010b)

bei intelligenten Postern von enormer Wichtigkeit, dass die darin gespeicherten Informationen nicht verändert werden können. Wäre dies möglich, könnten Benutzer in betrügerischer Absicht auf kostenpflichtige Dienste weitergeleitet werden oder ähnliches. Wie bereits erwähnt, beeinflussen die getroffenen Sicherheitsvorkehrungen auch die nötige Speicherkapazität.
NFC benutzt unter anderem das Verfahren "One Time Password" (OTP). Diese soll die Unsicherheit eines benutzergenerierten Passworts, welches meist persönliche Informationen beinhaltet und somit durch Wörterbuchattacken leicht zu knacken ist, eliminieren, indem für jede Verbindung/Session ein eigenes Passwort generiert wird. Damit beide Kommunikationspartner das selbe Passwort generieren, werden synchronisierte Passwortgeneratoren oder Passwortlisten benutzt.

- Preis
  Der Preis ist ein wichtiger wirtschaftlicher Faktor, welcher über die Verwendung einer Technologie entscheidet. Dieser wird von vielen Faktoren wie der Speicherkapazität oder den Zusatzfunktionalitäten eines NFC Tags beeinflusst.

- Größe
  Je nach Anwendungsfall kann es nötig sein, dass ein Chip nur eine gewisse Größe hat. Dies hängt vor allem von den lokalen Gegebenheiten wie der verfügbaren Fläche, auf dem der Tag aufgebracht wird, ab. Der Faktor Größe beeinflusst wiederum den verfügbaren Speicher.

- Lesegeschwindigkeit
  Die Lesegeschwindigkeit beeinflusst vor allem die Verlässlichkeit des Systems und somit die Akzeptanz beim Benutzer. Je schneller die Daten ausgelesen werden können, desto geringer ist die Wahrscheinlichkeit eines Übertragungsfehlers oder einer unvollständigen Übertragung,

wenn die NFC Geräte zu schnell aneinander vorbei bewegt werden. Als spezielles Kommando wird bei Near Field Communication Geräten der Befehl "Read All" verwendet, welcher es ermöglicht, dass die gesamten Daten in nur einer Übertragung gelesen werden können. Dies wird jedoch nicht von allen Tag Formaten unterstützt.

Das NFC Forum, welches als Non-Profit Industrievereinigung von Next Experience Semiconductors gegründet wurde und sich um die Umsetzung und Standardisierung der Near Field Communication kümmert, definiert die vier Tag-Formate wie folgt: (Innovision Research & Technology plc, 2010b)

1. *Typ 1*
   Dieser Tag verfügt über einen 96 Byte großen Speicher und eignet sich vor allem für sehr kleine Anwendungsgebiete oder wenige Daten. Trotz des relativ geringen Speichers ermöglicht er digitale Signaturen bis zu einer Länge von 32 Byte. Aufgrund der geringen Größe und des Funktionsumfangs ist dieser einer der günstigsten Tags. Eine Übersicht der Features von Typ 1 kann der Tabelle 2.27 entnommen werden.

Features	
Dual-State (schreib-/lesbar)	Ja
Speicherkapazität	96 Bytes + 6 Bytes OTP + 2 Byte ROM
Sicherheit	16 oder 32 Byte lange Signatur
Preis	Geringst
Größe	*****
Lesegeschwindigkeit	*** (Read All)

Tabelle 2.27: NFC Tag 1 Features (Innovision Research & Technology plc, 2010b)

*: je mehr *, desto besser

2. *Typ 2*
   Dieser Tag verfügt über nur halb so viel Speicher wie Typ 1 und bietet auch keinerlei Sicherheitsmechanismen, kostet aber mehr als Typ 1. Er eignet sich lediglich für Anwendungsfälle mit geringem Speicherbedarf und keinen Sicherheitsbedürfnissen. Eine Übersicht der Features kann der Tabelle 2.28 entnommen werden.

3. *Typ 3*
   Der Typ 3 Tag sticht vor allem durch seinen viel größeren Speicher (derzeit 2 kByte) und seine höhere Übertragungsrate (212 kbit/sec)

Features	
Dual-State (schreib-/lesbar)	Ja
Speicherkapazität	48 Bytes
Sicherheit	Keine
Preis	Gering
Größe	****
Lesegeschwindigkeit	** (Read All)

Tabelle 2.28: NFC Tag 2 Features (Innovision Research & Technology plc, 2010b)

*: je mehr *, desto besser

hervor. Dadurch eignet sich dieser Tag sehr gut für komplexe Anwendungen. Eine Übersicht der Features kann der Tabelle 2.29 entnommen werden.

Features	
Dual-State (schreib-/lesbar)	Ja
Speicherkapazität	2 kByte
Sicherheit	16 oder 32 Byte lange Signatur
Preis	Hoch
Größe	*
Lesegeschwindigkeit	**

Tabelle 2.29: NFC Tag 3 Features (Innovision Research & Technology plc, 2010b)

*: je mehr *, desto besser

4. *Typ 4*
   Dieser Typ zeichnet sich als Allrounder unter den Tags aus, da er je nach Anwendungsfall variabel gestaltet werden kann. Von der Speicherkapazität bis zur Signaturlänge kann dieser Tag frei konfiguriert werden (innerhalb der technischen Möglichkeiten) und alle Übertragungsraten von 106 kBit/sec bis 424 kBit/sec werden unterstützt. Weitere Features können der Tabelle 2.30 entnommen werden.

Zusammengefasst können die Formate in zwei Gruppen unterteilt werden: den Typen 1 und 2 für Kleinstanwendungen und den Typen 3 und 4 für

Features	
Dual-State (schreib-/lesbar)	Ja
Speicherkapazität	Variabel
Sicherheit	Variabel
Preis	Hoch
Größe	*
Lesegeschwindigkeit	***

Tabelle 2.30: NFC Tag 4 Features (Innovision Research & Technology plc, 2010b)

*: je mehr *, desto besser

komplexere Aufgaben. Diese unterscheiden sich vor allem hinsichtlich Speicherkapazität und Geschwindigkeit.

Die Verwendung der zukunftsträchtigen Near Field Communication Technologie zur Lokalisierung innerhalb von Gebäuden bietet einige Vorteile. Sie ist den in den Abschnitten 2.5 und 2.6 vorgestellten Varianten mit Strichcodes und 2D Codes ähnlich, bietet aber durch Implementierung fortschrittlicher Technologien einen weitaus größeren Informations- und Funktionsgehalt, welche auch das Angebot der vooch GmbH erweitern würde. Durch die geringe Reichweite von 20 Zentimetern lässt sich auch eine hohe Genauigkeit erzielen, wodurch der Aufenthaltsort des Kunden im Geschäftslokal sichergestellt wäre. Auch der im Vergleich zur Anschaffung einer Basisstation (siehe Abschnitte 2.8 WLAN und 2.7 Bluetooth) geringe Preis der NFC Tags (speziell bei der Anschaffung in größeren Mengen) kann als Vorteil gezählt werden. Allerdings ist NFC noch nicht sehr verbreitet und vor allem auf vielen Smartphones noch nicht verfügbar, was den breiten Einsatz dieser Technologie zeitlich in die nahe Zukunft verschiebt. Beobachtet man aktuelle Pressemeldungen (siehe zum Beispiel DerStandard.at über iPhone 5 vom 02. November 2010 [53] oder über Android 2.3 vom 06. Dezember 2010[54]), so ist es relativ wahrscheinlich, dass NFC-fähige Mobiltelefone in den nächsten zwei Jahren in breiter Masse am Markt verfügbar sein werden. Für eine schnelle Lösung eignet sich NFC daher nicht, sollte aber für zukünftige Entwicklungen durchaus in Betracht gezogen werden.

[53] http://derstandard.at/1288659271820/Bericht-iPhone-5-soll-Mac-Nutzung-revolutionieren

[54] http://derstandard.at/1291454222532/Gingerbread-Android-23-Die-naechste-Geruechterunde-sagt-heute

Kapitel 3

Alternativenauswahl

Nachdem im Kapitel 2 nun verschiedenste Technologien zur Ortung definiert, beschrieben und untersucht wurden, befasst sich dieses Kapitel mit der Auswahl einer Variante, um das in Abschnitt 1.2 beschriebene Problem zu lösen bzw. eine Verbesserung zu erzielen. Die derzeit verwendeten Lokalisierungstechnologien GPS (siehe Abschnitt 2.1), Netzwerktriangulierung (siehe Abschnitt 2.2), Assisted GPS (siehe Abschnitt 2.3) und GeoIP (siehe Abschnitt 2.4) haben eine zu hohe Ungenauigkeit um sicherzustellen, dass sich ein Benutzer bei der Einlösung eines Gutscheins wirklich im Geschäftslokal befindet. Diese Ungenauigkeit ist zum Teil auch auf Empfangsschwierigkeiten innerhalb von Gebäuden (wie beispielsweise bei GPS) zurückzuführen. Da der Aufenthalt im Lokal aber ein notwendiges Kriterium ist um eine korrekte Abrechnung den Geschäftskunden gegenüber zu gewährleisten, ist eine Technologie auszuwählen, welche eine genaue Ortung innerhalb von Gebäuden ermöglicht. Da an eine Eliminierung der derzeit verwendeten Ortungstechniken nicht zu denken ist, soll die ausgewählte Variante als Ergänzung hinzugezogen werden.
Gemeinsam mit den Betreuern der vooch GmbH Dr. Tobias Hann und Dipl.-Ing. Michael Meier wurden folgende Kriterien zur Bewertung und Auswahl der Alternativen definiert:

- *Verfügbarkeit der Technologie*
  Da sich vooch auf kein spezielles mobiles Endgerät oder Betriebssystem beschränkt, ist es von enormer Wichtigkeit, dass die Technologie sich bereits am Markt etabliert hat und auf möglichst vielen Mobiltelefonen verfügbar ist. Eine noch nicht etablierte Technologie hätte zur Folge, dass die Problematik nur auf einigen wenigen Endgeräten behandelt würde und somit die Lösung des Problems vom Verbreitungsgrad dieser Variante abhängig wäre.

- *Ortung in Gebäuden*
  GPS verfügt unter den verwendeten Technologien zwar über die höchste Genauigkeit, erlaubt aber keine bzw. nur eine eingeschränkte Ortung

in Gebäuden. Um festzustellen ob sich der Benutzer im Geschäftslokal befindet, sollte zumindest ein Ortung innerhalb des Gebäudes möglich sein. Damit ist keine punktgenaue Ortung innerhalb des Gebäudes gemeint, sondern vielmehr eine Bestimmung, ob sich der Standort nun innerhalb oder außerhalb des Gebäudes befindet.

- *Ortung in Räumen*
  Ähnlich dem vorherigen Punkt wird eine Ortung innerhalb eines Gebäudes benötigt. Da es aber durchaus vorkommen kann, dass sich nicht nur ein im System registriertes Geschäftslokal in einem Gebäude befindet, sondern auch mehrere wie beispielsweise in Einkaufshäusern, wäre ein Ortung innerhalb eines Gebäudes von Vorteil. Damit ist die Beantwortung der Frage, in welchem Raum eines Gebäudes sich der Benutzer befindet, gemeint.

- *Genauigkeit*
  Um dem Problem, welches durch die Ungenauigkeit der verwendeten Technologien entstanden ist, vorzubeugen, wird eine relative hohe Genauigkeit vorausgesetzt. Die Genauigkeit sollte ungefähr im Bereich +/- 50 Meter vom Standort sein.

- *Entwicklungs-/Umsetzungskosten*
  Da es sich bei vooch um ein junges Startup-Unternehmen handelt, sollte sich die Variante relativ kostengünstig umsetzen lassen und im Verhältnis zum Nutzen stehen. Dies schließt unter anderem die Verwendung unausgereifter oder zu umfangreicher Varianten aus, da diese sehr kostenintensiv wären und das Problem in einem Übermaß behandeln.

- *Instandhaltungs- und Wartungskosten/-aufwand*
  Ähnlich dem vorherigen Kriterium sollten sich vor allem die Instandhaltungs- und Wartungskosten in Grenzen halten beziehungsweise im besten Fall entfallen. Auch für die Akzeptanz der Geschäftskunden wäre es von Vorteil, wenn das neue Verfahren ohne Wartungsaufwand betrieben werden kann.

- *Kosten für Geschäftskunden*
  Um das neue Verfahren reibungslos und für das ganze System umsetzten zu können, ist eine Akzeptanz und Teilnahme aller Geschäftskunden erforderlich. Dies wird sich nur erreichen lassen, wenn für den Geschäftskunden keine Kosten entstehen.

- *Verwendbarkeit und Akzeptanz durch den Benutzer*
  Wichtigstes Kriterium für den Erfolg des neuen Verfahrens ist die Akzeptanz durch den Benutzer, der schlussendlich das System benutzt. Wird für ihn der Einlöseprozess zu aufwändig, wird er vooch nicht

mehr benutzen. Deshalb sollte die neue bzw. zusätzliche Ortung möglichst ohne sein Zutun funktionieren. Jeder zusätzliche Schritt, zum Beispiel manuelles Herstellen einer Verbindung, schmälert die Akzeptanz, deshalb sollte sich der Einlöseprozess nach Außen hin möglichst wenig verändern.

- *Zukunftsaussichten der Technologie*
  Um die Funktionsfähigkeit des neuen Verfahrens über längere Zeit zu gewährleisten, sollte es sich um keine veraltete Technologie handeln, welche in naher Zukunft von keinem mobilen Endgerät mehr unterstützt werden wird. Sie sollte außerdem auch Spielraum für zukünftige Anwendungen schaffen, wie beispielsweise für die Thematik personalisierter Werbung.

In den folgenden Abschnitten werden die in Kapitel 2 vorgestellten neuen Technologien anhand dieser Kriterien nochmals beleuchtet und zur leichteren Auswahl bewertet. Zur Bewertung wird das in Tabelle 3.1 dargestellte fünfstufige Punktesystem herangezogen.

Bewertung	Bedeutung
++	Volle Übereinstimmung mit dem Kriterium
+	Größtenteils Übereinstimmung mit dem Kriterium
o	Teilweise Übereinstimmung mit dem Kriterium
–	Kaum Übereinstimmung mit dem Kriterium
– –	Keine Übereinstimmung mit dem Kriterium

Tabelle 3.1: Bewertungssystem zur Alternativenauswahl

3.1 Ortung mittels Strichcode

Die Ortung mittels Strichcode erlaubt ohne großen Aufwand eine punktgenaue Ortung. Dazu wird lediglich ein Strichcode an einem prägnanten Punkt im Geschäftslokal (zum Beispiel an der Kasse) angebracht. Beim Einlösen des Gutscheins wird der Benutzer dazu aufgefordert, den Strichcode vor die Kameralinse des Smartphones zu bringen. Die Anwendung erkennt den Strichcode und kann das darin kodierte Einlösegeheimnis, welches den Standort eindeutig identifiziert, auslesen. Dieses wird gemeinsam mit den anderen Einlösedaten an den Server von vooch geschickt, welcher dann die Korrektheit der Einlösung validieren kann.
Dieses Verfahren erfordert lediglich ein Smartphone mit Kamera und zusätzlich eine kurze Handlung des Benutzer. Für den Geschäftskunden entstehen

keinerlei Kosten. Er muss lediglich einen oder mehrere Strichcodes in seinem Geschäftslokal anbringen. Die Umsetzungskosten sind relativ gering, da sich der Aufwand unter Verwendung einer freien Strichcodedekodierungs-Bibliothek in einem kleinen Rahmen bewegt. Als laufende Kosten fallen lediglich die Druckkosten für die Strichcodes an. Eine Bewertung dieses Verfahrens kann der Tabelle 3.2 entnommen werden.

Kriterium	Bewertung	Bemerkung
Verfügbarkeit	+	Kamera größtenteils verfügbar
Gebäudeortung	++	Identifizierung anhand eindeutigem Code
Raumortung	++	Identifizierung anhand eindeutigem Code
Genauigkeit	++	Benutzer in unmittelbarer Nähe des Codes
Entwicklungskosten	++	geringer Aufwand
Wartungskosten	++	geringe Druckkosten
Kosten für Geschäftskunden	++	keine Kosten
Benutzerakzeptanz	+	Code muss fotografiert werden
Zukunftsaussichten	+	Handykameras nicht wegzudenken
Gesamtbewertung	++	1,67 Pluspunkte

Tabelle 3.2: Bewertung der Ortung mittels Strichcode

3.2 Ortung mittels 2D Code

Die Bewertung des 2D Code Verfahrens ist der des Strichcodeverfahrens ähnlich, mit dem Unterschied der Verwendung von zweidimensionalen Codes und der sich daraus ergebenden höheren Speicherkapazität gegenüber Strichcodes. Dadurch ergeben sich erweiterte Anwendungsmöglichkeiten wie der Kodierung weiterer Informationen für neue Funktionalitäten. Eine Bewertung dieses Verfahrens kann der Tabelle 3.3 entnommen werden.

3.3 Ortung mittels Bluetooth

Die Ortung mittels Bluetooth ist eine sehr fortschrittliche, aber auch komplexe Variante. Einer der Vorteile ist, dass Bluetooth auf mobilen Endgeräten sehr verbreitet ist. Nachteile sind allerdings der hohe Stromverbrauch und der lange Verbindungsaufbau. Bluetooth wird in vielen Fällen zur Indoor-Lokalisierung verwendet, basiert allerdings auf hochwertigen statistischen Modellen und Wahrscheinlichkeitsberechnungen, was vor allem den Entwicklungsaufwand und die damit verbundenen Kosten in die Höhe treibt. Die

Kriterium	Bewertung	Bemerkung
Verfügbarkeit	+	Kamera größtenteils verfügbar
Gebäudeortung	++	Identifizierung anhand eindeutigem Code
Raumortung	++	Identifizierung anhand eindeutigem Code
Genauigkeit	++	Benutzer in unmittelbarer Nähe des Codes
Entwicklungskosten	++	geringer Aufwand
Wartungskosten	++	geringe Druckkosten
Kosten für Geschäftskunden	++	keine Kosten
Benutzerakzeptanz	+	Code muss fotografiert werden
Zukunftsaussichten	++	erweiterter Funktionsumfang
Gesamtbewertung	++	1,78 Pluspunkte

Tabelle 3.3: Bewertung der Ortung mittels 2D Code

Genauigkeit lässt sich über die Qualität und vor allem die Anzahl der Basisstationen steuern, wobei jede weitere Basisstation sich wiederum in Kosten niederschlägt. Aus diesem Grund werden zwei Bluetoothortungs-Varianten betrachtet, welche beide in Abschnitt 2.7 beschrieben wurden. Die komplexe Variante basiert auf einem neuronalen Netzwerk, welches aufgrund der Signalstärke oder den Antwortzeiten zu verschiedenen Basisstationen die Positionsbestimmung des Benutzers innerhalb eines Gebäudes oder Raumes ermöglicht. Die zweite, einfache Variante kommt mit nur einer Basisstation aus, welche ein eindeutiges Einlösegeheimnis bereitstellt oder es selbst ist. Das Mobiltelefon des Benutzers verbindet sich beim Einlösen mit der Basisstation, erhält das Geheimnis und sendet dieses zusammen mit den anderen Daten an den Server, welcher anhand derer feststellen kann, ob sich der Benutzer im Geschäftslokal befindet oder nicht. Bei beiden Varianten wird es erforderlich sein, dass Bluetooth aufgrund des hohen Stromverbrauchs manuell aktiviert und die Verbindung mit der Basisstation bestätigt wird. Die Bewertung des komplexen Verfahrens kann der Tabelle 3.4 und die des einfachen Verfahrens der Tabelle 3.5 entnommen werden.

3.4 Ortung mittels WLAN

Die Ortung mittels WLAN ähnelt jener mittels Bluetooth sehr, es wird lediglich ein anders Funknetz als Trägermedium verwendet. Ebenfalls gibt es hier eine komplexe Variante mit neuronalem Netzwerk, mehreren Basisstationen und der dadurch möglichen Ortung innerhalb eines Gebäudes/Raumes und einer einfachen Variante mit nur einer Basisstation um festzustellen ob sich eine Person im Gebäude/Raum befindet oder nicht. Im Gegensatz zu Bluetooth muss hier die Verbindung zur Basisstation nicht bestätigt werden,

Kriterium	Bewertung	Bemerkung
Verfügbarkeit	++	Bluetooth sehr verbreitet
Gebäudeortung	++	berechnete Position
Raumortung	++	berechnete Position
Genauigkeit	+	abhängig von Basisstationen
Entwicklungskosten	– –	Umsetzung eines neuronalen Netzwerks
Wartungskosten	– –	Wartung der Hardware an Standorten
Kosten für Geschäftskunden	– –	Hardwareanschaffung
Benutzerakzeptanz	–	BT aktivieren u. Verbindung herstellen
Zukunftsaussichten	++	Verwendung für weitere Funktionalitäten
Gesamtbewertung	o	0,22 Pluspunkte

Tabelle 3.4: Bewertung der Ortung mittels Bluetooth (komplex)

Kriterium	Bewertung	Bemerkung
Verfügbarkeit	++	Bluetooth sehr verbreitet
Gebäudeortung	+	im Gebäude: ja/nein
Raumortung	o	abhängig von Größe und Reichweite
Genauigkeit	+	entspricht der Reichweite
Entwicklungskosten	+	Simpler Geheimnisaustausch
Wartungskosten	–	Wartung der Hardware an Standorten
Kosten für Geschäftskunden	–	Hardwareanschaffung
Benutzerakzeptanz	–	BT aktivieren u. Verbindung herstellen
Zukunftsaussichten	++	Verwendung für weitere Funktionalitäten
Gesamtbewertung	o	0,44 Pluspunkte

Tabelle 3.5: Bewertung der Ortung mittels Bluetooth (einfach)

jedoch wird aufgrund des hohen Stromverbrauchs WLAN auf dem Endgerät wiederum manuell aktiviert werden müssen. Eine Bewertung dieser beiden Varianten kann den Tabellen 3.6 und 3.7 entnommen werden.

3.5 Ortung mittels Ultraschall

Dieses Verfahren erlaubt es dem Endgerät des Kunden ohne zusätzliche Hardware auszukommen. Die von einem Sender ausgestrahlten hochfrequenten Schallwellen können vom eingebauten Mikrofon wahrgenommen werden. Anhand von Signallaufzeiten und Phasenverschiebungen kann mit Hilfe von einfachen mathematischen Berechnungen die Position des Endgerätes bestimmt werden. Je nach Bestimmungsverfahren kommt diese Methode mit

Kriterium	Bewertung	Bemerkung
Verfügbarkeit	o	WLAN nur auf moderneren Smartphones
Gebäudeortung	++	berechnete Position
Raumortung	++	berechnete Position
Genauigkeit	+	abhängig von Basisstationen
Entwicklungskosten	– –	Umsetzung eines neuronalen Netzwerks
Wartungskosten	– –	Wartung der Hardware an Standorten
Kosten für Geschäftskunden	– –	Hardwareanschaffung
Benutzerakzeptanz	–	WLAN manuell aktivieren
Zukunftsaussichten	++	Verwendung für weitere Funktionalitäten
Gesamtbewertung	o	0 Pluspunkte

Tabelle 3.6: Bewertung der Ortung mittels WLAN (komplex)

Kriterium	Bewertung	Bemerkung
Verfügbarkeit	o	WLAN nur auf modernen Smartphones
Gebäudeortung	+	im Gebäude: ja/nein
Raumortung	o	abhängig von Größe und Reichweite
Genauigkeit	+	entspricht der Reichweite
Entwicklungskosten	+	simpler Geheimnisaustausch
Wartungskosten	–	Wartung der Hardware an Standorten
Kosten für Geschäftskunden	–	Hardwareanschaffung
Benutzerakzeptanz	–	WLAN manuell aktivieren
Zukunftsaussichten	++	Verwendung für weitere Funktionalitäten
Gesamtbewertung	o	0,22 Pluspunkte

Tabelle 3.7: Bewertung der Ortung mittels WLAN (einfach)

einem oder zwei Signalen, also ein oder zwei Sendestationen aus. Durch dieses relativ einfache Konzept lässt sich das Verfahren auch in größeren Umgebungen, wie beispielsweise Kaufhäusern, gut umsetzen. Da die Berechnungen simpel und die Ultraschallsender günstig sind (speziell in großen Mengen), fallen die Entwicklungskosten gering aus und müssen nicht zum Teil auf den Geschäftskunden abgewälzt werden. Zu den laufenden Kosten zählt nur der Austausch von eventuell defekten Sendern. Eine Bewertung dieses Verfahrens kann der Tabelle 3.8 entnommen werden.

Kriterium	Bewertung	Bemerkung
Verfügbarkeit	++	Mikrofon immer verfügbar
Gebäudeortung	++	berechnete Position
Raumortung	++	berechnete Position
Genauigkeit	+	abhängig von Störungen
Entwicklungskosten	+	günstige Ultraschallsender
Wartungskosten	+	günstige Ultraschallsender
Kosten für Geschäftskunden	++	keine Kosten
Benutzerakzeptanz	++	keinerlei Benutzerinteraktion
Zukunftsaussichten	+	kein erweiterter Funktionsumfang
Gesamtbewertung	++	1,55 Pluspunkte

Tabelle 3.8: Bewertung der Ortung mittels Ultraschall

3.6 Ortung mittels NFC/RFID

Die auf der fortschrittlichen RFID-Technologie basierende Near Field Communication ist der Ortung mittels 2D Code sehr ähnlich. Auf einem NFC Tag wird das Geheimnis für die Einlösung gespeichert. Dieser wird dann an einer prägnanten Stelle im Geschäftslokal (zum Beispiel der Kasse) angebracht. Bei der Einlösung wird der Benutzer dazu aufgefordert, sein NFC-fähiges Smartphone über den Tag zu bewegen um seinen derzeitigen Standort zu bestätigen. Durch das aneinander vorbeiführen von dem NFC Reader und dem Tag kann der Reader das Geheimnis auslesen. Dieses wird gemeinsam mit den anderen Einlösedaten an den Server von vooch geschickt, welcher dann die Korrektheit der Einlösung validieren kann.
Durch die hohe Speicherkapazität und den erweiterten Funktionsumfang eines NFC Tags kann diese Technologie auch für weitere zukünftige Funktionen genutzt werden. Da es sich um eine relativ neuartige Technologie handelt, gibt es am Markt noch kaum NFC-fähige Geräte. Dies schließt NFC für die derzeitige Anwendung aus, sollte aber für spätere Zwecke im Auge behalten werden. Die Entwicklungskosten können niedrig gehalten werden, da der NFC Reader in der Hardware des Smartphones integriert ist und die Funktionalität dem Entwickler direkt zur Verfügung steht. Ähnlich den Ultraschallsendern sind auch die NFC Tags kostengünstig zu erwerben, speziell in größeren Mengen. Eine Bewertung dieses Verfahrens kann der Tabelle 3.9 entnommen werden.

Kriterium	Bewertung	Bemerkung
Verfügbarkeit	-	NFC-fähige Geräte noch nicht verbreitet
Gebäudeortung	++	Identifizierung anhand eindeutigem Geheimnis
Raumortung	++	Identifizierung anhand eindeutigem Geheimnis
Genauigkeit	++	Benutzer in unmittelbarer Nähe des Tags
Entwicklungskosten	++	geringer Aufwand
Wartungskosten	+	geringe Kosten für Tags
Kosten für Geschäftskunden	++	keine Kosten
Benutzerakzeptanz	+	Telefon über Tag bewegen
Zukunftsaussichten	++	erweiterter Funktionsumfang
Gesamtbewertung	+	1,44 Pluspunkte

Tabelle 3.9: Bewertung der Ortung mittels NFC

3.7 Entscheidung

In den letzten Abschnitten wurden die in Kapitel 2 vorgestellten Technologien anhand der gemeinsam mit der vooch GmbH festgelegten Kriterien betrachtet und bewertet. Ziel war es, ein Verfahren auszuwählen, welches den Kriterien am besten entspricht. Die Wahl viel auf die Ortung mittels 2D Code mit einer Bewertung von ++ (1,78 Pluspunkten). Nun wird mit der Entwicklung eines Prototypen begonnen. Dazu wird der bestehenden Android[1] Client erweitert und das Einlöseverfahren um das Scannen eines 2D Codes ergänzt. Dieser Code enthält einen Schlüssel, welcher den Standort eindeutig kodiert. Aufgrund der Verbreitung von QR Codes hat sich die vooch GmbH dazu entschieden, diese Art von 2D Codes zu verwenden. Um die Daten des QR Codes dekodieren zu können, muss eine freie Bibliothek gefunden werden, welche von Android unterstützt wird. Nähers zum Prototypen ist dem folgenden Kapitel 4 zu entnehmen.

[1] Android ist ein mobiles Betriebssystem für Smartphones und wurde von Google entwickelt.

Kapitel 4

Prototyp

Dieses Kapitel befasst sich mit der Umsetzung des in Kapitel 3 ausgewählten Verfahrens. Mit dem daraus entstehenden Prototypen soll ein "Proof of Concept" durchgeführt werden, welcher die Funktionsfähigkeit und die Korrektheit einer genauen Ortsbestimmung mittels QR Codes beweisen soll. Als Basis diente der bereits vorhandene vooch Client in Version 3.0 auf Google's mobiler Plattform Android. Dieser unterstützt alle Android Versionen von 1.5 bis aktuellen 2.2.1 und alle damit verbundenen Displayformate. Entwickelt wurde auf einem Apple iMac mit Mac OS X 10.6.5 "Snow Leopard" mit Eclipse Galileo Entwicklungsumgebung in Version 3.5.2 in Verbindung mit dem Android Development Toolkit in Version 0.9.9.
Zur Dekodierung wurde die Open Source Bibliothek ZXing[1] in Version 1.6 verwendet. Dies ist eine Multi-Format 1D/2D Strichcode Bildverarbeitungsbibliothek. Sie besteht aus einer in Java umgesetzten Kernbibliothek und vielen plattformspezifischen Portierungen, unter anderem auch Android.
Die in vooch integrierte Lösung basiert auf dem ebenfalls zur Verfügung gestellten ZXing Demo Client für Android, aus welchem Teile entnommen und an die Anforderungen angepasst wurden. Die QR Code Validierung wurde als Zwischenschritt zwischen dem Einlösen und der serverbasierten Validierung der Einlösedaten eingefügt. Dabei wird der Benutzer nach dem Tippen auf "Einlösen" dazu aufgefordert, den im Geschäftslokal angebrachten QR Code einzuscannen. Erst nach erfolgreicher Dekodierung des Codes kann der Einlöseprozess abgeschlossen werden. Der restliche Ablauf blieb unberührt. Der Anwendungsfall für die Einlösung eines Gutscheines sieht nun wie folgt aus:

1. Anwendung starten (siehe Abbildung 4.1a)

2. Auswahl eines Gutscheins (siehe Abbildung 4.1b)
   Dem Benutzer stehen in der Anwendung mehrere Möglichkeiten zur

[1] http://code.google.com/p/zxing/

Verfügung einen Gutschein auszuwählen. Diese bestehen alle aus einer Liste mehrerer Gutscheine die anhand gewisser Kriterien selektiert und/oder sortiert wurden. Folgende Möglichkeiten stehen zur Auswahl:

- Highlights
  Diese Liste enthält die neusten, am besten bewerteten und nächstliegendsten Gutscheine. Dabei werden die Gutscheine schon am Server mit einem eigens entwickelten Reihungsverfahren sortiert.
- In der nähe einlösbare Gutscheine
  Dem Benutzer werden Gutscheine präsentiert, welche in seiner unmittelbaren Umgebung eingelöst werden können.
- Kategorien
  Der Benutzer kann die Gutscheine mit vordefinierten Kategorien vorselektieren.
- Suche
  Über ein Textfeld kann der Benutzer selbst Kriterien für die Selektion angeben.
- Gemerkte Gutscheine
  Der Benutzer hat auch die Möglichkeit sich Gutscheine zu merken und sie zu einem späteren Zeitpunkt einzulösen.

3. Einlösen des Gutscheins (siehe Abbildung 4.1c)
   Nachdem der Benutzer einen Gutschein aus einer Liste ausgewählt hat, wird ihm dieser in einer Detailansicht präsentiert, in der er Informationen zur Einlösung erhält, Bewertungen anderer Benutzer lesen oder sich Informationen zum Unternehmen oder zu den Standorten holen kann. Durch das Tippen auf "Einlösen" wird der Einlöseprozess gestartet. Normalerweise werden die Benutzeridentifikation, Koordinaten des Standorts und weiter Daten an den Server geschickt, nun folgt aber zuerst noch das Auslesen des Geheimnisses aus dem QR Code (siehe Punkt 4).

4. Genaue Positionsbestimmung (siehe Abbildung 4.2a und b)
   An dieser Stelle kommt die ZXing Bibliothek zum Einsatz. Dem Benutzer wird ein Kamerafenster präsentiert, in dessen Fokus er den QR Code bringen muss. Die Bibliothek verarbeitet das Farbbild der Kamera laufend in ein Schwarz-/Weiß-Bild und sucht nach den drei Quadraten, dem Erkennungsmuster des QR Codes. Markante Stellen werden am Bildschirm durch gelbe Punkte markiert, wie der Abbildung 4.2a zu entnehmen ist. Konnte ein Muster erkannt und korrekt dekodiert werden, wird das Bild der Kamera angehalten und das erkannte Muster grün markiert (siehe Abbildung 4.2b).

5. Serverbasierte Einlösevalidierung
   Nachdem das im QR Code kodierte Geheimnis ausgelesen werden konn-

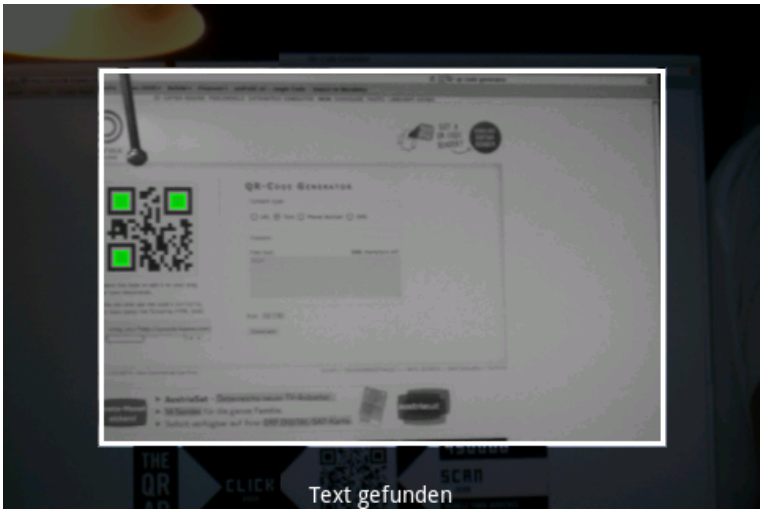
(a) vooch starten (b) Gutschein auswählen (c) Einlösen klicken

Abbildung 4.1: Auswahl eines Gutscheins zur Einlösung

te, wird dieses gemeinsam mit den in Punkt 3 erwähnten Einlösedaten an den Server geschickt. Dieser überprüft nun, ob die Zuordnung vom angegebenen Standort und des Geheimnisses übereinstimmt. Trifft dies zu, wird der Gutschein für den Benutzer freigeschaltet und er erhält ihn in Form eines Bildes mit Sicherheitssiegel und eventueller Gutscheinnummer am Bildschirm präsentiert. Stimmen Standort und Geheimnis nicht überein erhält der Benutzer eine Fehlermeldung und der Einlöseprozess wird abgebrochen.
Zu Testzwecken wurden zwei QR Codes verwendet (siehe Abbildung 4.3a und b). Einer enthält ein falsches, der andere das richtige Geheimnis. Die Einlösung eines Testgutscheins wurde mit beiden getestet und resultierte im ersten Fall in einer Fehlermeldung (siehe Abbildung 4.4a), da nicht das dem Standort eindeutig zugeordnete Geheimnis ausgelesen werden konnte. Im zweiten Fall funktionierte die Einlösung korrekt und es wurde das Gutscheinbild am Display angezeigt.

Wie dem Test zu entnehmen ist, funktioniert das Verfahren mit der QR Code Validierung. Der Gutschein kann nur noch eingelöst werden, sofern der richtige QR Code eingescannt wird. Da dieser nur am jeweiligen Unternehmensstandort verfügbar ist, ist somit sichergestellt, dass sich der Benutzer vor Ort befindet.
Nachdem nun die Funktionsfähigkeit getestet wurde, wird der Prototyp für den Vertrieb freigegeben werden. Mit Hilfe der Vertriebsmitarbeiter können weitere Tests durchgeführt werden. Hauptzweck dieser Freigabe ist allerdings, das System den Geschäftskunden zu präsentieren und deren Akzeptanz zu prüfen. Ist auch dieser Schritt erfolgreich kann eine nahtlose Integration der ZXing Bibliothek in den aktuellen vooch Client durchgeführt werden. Dabei wird eine komplett an die Erfordernisse von vooch angepasste

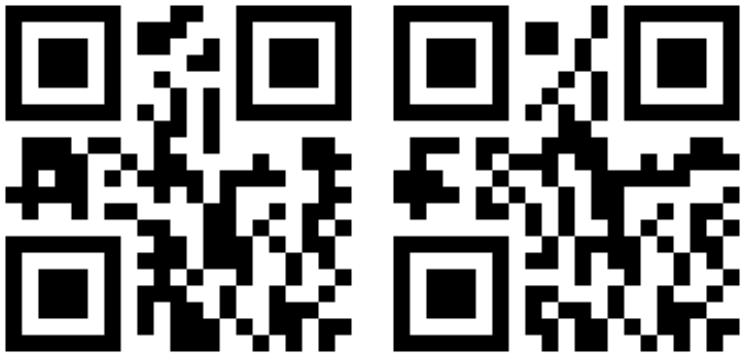
(a) QR Code suchen



(b) QR Code erkannt

Abbildung 4.2: Neue Positionsbestimmung

Lösung entwickelt werden, welche sich perfekt in die bestehende Applikation integriert.



(a) falsches Geheimnis (b) richtiges Geheimnis

Abbildung 4.3: QR Codes mit Einlösegeheimnis (http://qrcode.kaywa.com/)

(a) QR Code falsch (b) Gutschein eingelöst

Abbildung 4.4: Validierung der Einlösedaten

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[WPNC 2004] Bluetooth Indoor Localization System 1st WORKSHOP ON POSITIONING, NAVIGATION AND COMMUNICATION (Veranst.), 2004

[Bargh et al. 2008] Bargh, M. S. ; Groote, R. de: Indoor Localization Based on Response Rate of Bluetooth Inquiries / University of Twente. SEP 2008. – Presentation

[Bauer 2003] Bauer, M.: *Vermessung und Ortung mit Satelliten.* 5. Heidelberg : Wichmann, 2003

[Bluetooth 2010] Bluetooth (Veranst.): *Specification of the Bluetooth System.* 4.0. JUN 2010

[Borsc et al. 2005] Borsc, M. ; Shinde, H.: Wireless security privacy. In: *Personal Wireless Communications, 2005. ICPWC 2005. 2005 IEEE International Conference on*, Januar 2005, p. 424 – 428

[D. Lichtenegger 2009] D. Lichtenegger, BSc.: Standortbezogene Dienste auf der mobilen Plattform Android von Google / Technische Universität Graz. August 2009. – technical report

[Deering et al. 1998] Deering, S. ; Hinden, R.: *RFC 2460: Internet Protocol, Version 6 (IPv6), Specification.* The Internet Society (Veranst.), DEC 1998

[Dijk 2004] Dijk, Esko O.: *Indoor Ultrasonic Position Estimation using a Single Base Station*, Eindhoven University of Technology, dissertation, SEP 2004

[Fang et al. 2009] Fang, Shih-Hau ; Lin, Tsung-Nan: Accurate WLAN indoor localization based on RSS, fluctuations modeling. In: *Intelligent Signal Processing, 2009. WISP 2009. IEEE International Symposium on*, August 2009, p. 27 –30

[Finkenzeller 2010] Finkenzeller, Klaus: *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Iden-*

tification and Near-Field Communication. 3. John Wiley & Sons, Ltd., 2010

[3rd Generation Partnership Project 2008a] Generation Partnership Project 3rd: *Technical Specification Group Core Network and Terminals.* 8th, AUG 2008

[3rd Generation Partnership Project 2008b] Generation Partnership Project 3rd: *Technical Specification Group GSM/EDGE Radio Access Network; Functional stage 2 description of Location Services (LCS) in GERAN.* 8th, DEC 2008

[3rd Generation Partnership Project 2009] Generation Partnership Project 3rd: *Technical Specification Group Core Network and Terminals; Numbering, addressing and identification.* 3rd, SEP 2009

[Hazas et al. 2005] Hazas, Mike ; Kray, Cristian ; Gellersen, Hans ; Agbota, Henoc ; Kortuem, Gerd: A Relative Positioning System for Co-located Mobile Devices / Computing Department, Lancaster University. 2005. – technical report

[Heinze et al. 2009] Heinze, Steffen ; Kaptur, Cristian ; Ilbach, Peter: Ultraschall-Ortung / Institut für Informatik, Humboldt Universität. 2009. – technical report

[IEEE Computer Society 1999] IEEE Computer Society (Veranst.): *802.11 Wireless LAN Specifications.* 1999

[Information Sciences Institute 1981] Information Sciences Institute, University of Southern C.: *RFC 791: Internet Protocol Specification*, SEP 1981

[Innovision Research & Technology plc 2010a] Innovision Research & Technology plc (Veranst.): *Near Field Communication in the real world – part I: Turning the NFC promise into profitable, everyday applications.* 2010

[Innovision Research & Technology plc 2010b] Innovision Research & Technology plc (Veranst.): *Near Field Communication in the real world – part II: Using the right NFC tag type for the right NFC application.* 2010

[Jevring 2008] Jevring, M.: *Automatic Management of Bluetooth Networks for Indoor Localization*, University of Twente, diploma thesis, AUG 2008

[Joeckel et al. 2008] Joeckel, R. ; Stober, M. ; Huep, W.: *Elektronische Entfernungs- und Richtungsmessung und ihre Integration in aktuelle Positionierungsverfahren.* 5th. Heidelberg, 2008

[Kaplan 1996] Kaplan, E. D.: *Understanding GPS. Principles and Applications.* Boston : Artech House, 1996

[Lashkari et al. 2009] Lashkari, A.H. ; Mansoor, M. ; Danesh, A.S.: Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA). In: *2009 International Conference on Signal Processing Systems*, Mai 2009, p. 445 –449

[Lenk 2000] Lenk, B.: *Handbuch der automatischen Identifikation: 1D-Codes, 2D-Codes, 3D-Codes.* Deutschland : Lenk Monika Fachbuchverlag, DEC 2000 (Band 1)

[Lenk 2002] Lenk, B.: *Handbuch der automatischen Identifikation: Stapelcodes, Composite Codes, Dotcodes.* Deutschland : Lenk Monika Fachbuchverlag, SEP 2002 (Band 2)

[Lenk 2004] Lenk, B.: *Handbuch der automatischen Identifikation: Codeprüfung, Etikettierung, Lesegeräte.* Deutschland : Lenk Monika Fachbuchverlag, APR 2004 (Band 3)

[Liu et al. 2010] Liu, Chung-Hsin ; Lo, Chien-Yun: The study for the WLAN with Bluetooth Positioning System. In: *International Conference on Advances in Energy Engineering*, 2010, p. 154 – 157

[Merki 2003] Merki, H. G.: *Informationen zum Aztec Code.* Ruchstuckstraße 19, 8306 Brüttisellen: Ades AG (Veranst.), MAR 2003

[Michahelles et al. 2007] Michahelles, Florian ; Thiesse, Frederic ; Schmidt, Albrecht ; Williams, John R.: Pervasive RFID and Near Field Communication Technology. In: *IEEE Pervasive Computing* 6 (2007), p. 94–96, c3. – ISSN 1536-1268

[NAVSTAR 1995] NAVSTAR: *Global Positioning System Standard Positioning Service Signal Specification.* 2nd, JUN 1995

[Patent 1988] Patent, U. S.: *Dot Code A, Patent No. 4,745,269.* MAY 1988

[Patent 1998] Patent, U. S.: *Snowflake Code, Patent No. 5,825,015.* OCT 1998

[Patmanathan 2006] Patmanathan, V.: *Area Localization using WLAN.* Stockholm, Sweden, KTH Royal Institute of Technology, diploma thesis, 2006

[Paus 2007] Paus, A.: Near Field Communication in Cell Phones / Ruhr-Universität Bochum. 2007. – technical report

[Renn 2007] Renn, U.: 2D-Code-Fibel / BARCODAT GmbH. Robert-Bosch-Straße 13, 72280 Dornstetten, GER, JAN 2007 (Band 5). – technical report. – URL http://www.barcodat-nord.de/fileadmin/images_content/Support/2D-Code-Fibel%202007.pdf [accessed: 26.10.2010]

[Rosenbaum 1997] Rosenbaum, O.: *Das Barcode Lexikon*. 1st. Kaarst, 1997

[Schnabel 2008] Schnabel, P.: *Kommunikationstechnik-Fibel*. 2. Deutschland : Books on Demand GmbH, 2008

[Seifert et al. 2009] Seifert, T. ; Bengelstorff, A. ; Zastiral, S.: Wie das Handy die Welt verändert. In: *Die Presse* (2009), November

[Walke 2001] Walke, B.: *Mobilfunknetze und ihre Protokolle*. 3. Stuttgart, 2001

[Wikipedia a] Wikipedia: *European Article Number*. – URL http://de.wikipedia.org/w/index.php?title=European_Article_Number&oldid=79606038 [accessed: 29.09.2010]

[Wikipedia b] Wikipedia: *Internationale Standardbuchnummer*. – URL http://de.wikipedia.org/w/index.php?title=Internationale_Standardbuchnummer&oldid=79845293 [accessed: 05.10.2010]

[Youssef et al.] Youssef, M. A. ; Agrawala, A. ; Shankar, A. U.: WLAN Location Determination via Clustering and Probability Distributions / University of Maryland. – technical report