Near Field Communication

Potentiale von NFC für Lehr- und Lernunterlagen

Martin Maierhuber

Near Field Communication - Potentiale für Lehr- und Lernunterlagen

Masterarbeit

an der

Technischen Universität Graz

vorgelegt von

Martin Maierhuber

Institut für Informationssysteme und Computer Medien
Technische Universität Graz
A-8010 Graz

Leiter: Kappe, Frank, Univ.-Prof. Dipl.-Ing. Dr.techn.

Begutachter: Ebner, Martin, Dipl.-Ing. Dr.techn. Univ.-Doz.

Graz, im April 2013

Diese Arbeit ist in deutscher Sprache verfasst.

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 entnommenen Stellen als solche kenntlich gemacht habe.

Graz, am …… ……..
(Unterschrift)

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.

Graz, ...

Abstract

NFC is deemed to be a technology with a lot of potential in many areas. Subsequently, the question arises in which areas the technology can be used properly. This question shall be answered using NFC with teaching and learning materials as example.

This thesis deals with potentials NFC offers for teaching and learning materials. First, an overview of similar technologies that share possible use cases is given. Also, technical basics and details about optical recognization methods like QR-Codes will be shown and compared to radio-based technologies like RFID and especially NFC. This will give an overview of possible use cases and applications of above mentioned technologies, as well as their advantages and disadvantages. Also, security aspects are discussed that should point at current flaws and should sensitize the reader about those.

A practical example of NFC will be given based on a prototype that demonstrates basic NFC functions using a digital textbook. This example is used as base to show possible potentials. The prototype runs on Android 4.1 (or newer) systems.

Some ideas and suggestions should motivate the reader to engage further activities regarding the NFC topic. An outlook shows possible future scenarios around NFC. As the technology currently is still in an early stage of development, the reader is given some room for interpretation of some scenarios.

Kurzfassung

NFC gilt als eine Technologie mit sehr viel Potential in vielen Bereichen. Daraus ergibt sich die Fragestellung, in welchen Bereichen die Technologie nutzbar gemacht werden kann. Diese Fragestellung soll in dieser Arbeit insbesondere am Beispiel von Lehr- und Lernunterlagen beantwortet werden.

Diese Masterarbeit beschäftigt sich mit dem Thema NFC und den Potentialen, die diese neue Technologie bietet. Zuerst gibt es aber einen Überblick über Technologien, die mögliche Anwendungsszenarien mit NFC teilen. Es werden Grundlagen und technische Details zu optischen Verfahren wie QR-Codes gezeigt und diese den auf Funktechnologie basierenden Verfahren wie RFID und NFC gegenübergestellt. Dadurch erhält man einen Überblick über mögliche Einsatzgebiete der genannten Technologien, sowie jeweils deren Vor- und Nachteile. Ebenso werden sicherheitsrelevante Aspekte besprochen, die einige aktuell vorhandene Mängel aufzeigen.

Ein praktisches Beispiel zu NFC wird anhand eines Prototypen gezeigt, der die Grundfunktionen anhand eines Lehrbuches demonstriert. Diese sollen als Basis dienen, eventuelle Potentiale zu zeigen. Der Prototyp ist unter Android Version 4.1 (oder höher) lauffähig.

Es werden einige Ideen und Anregungen auch zur weiteren Beschäftigung mit NFC entwickelt. Ein Ausblick zeigt mögliche Zukunftsszenarien mit NFC. Da die Technologie in ihren Einsatzgebieten sich noch in einem recht frühen Stadium befindet, sei einiger Interpretationsspielraum bestimmter Anwendungsfälle gewährt.

Danksagung

Diese Masterarbeit ist am Institut für Informationssysteme und Computer Medien entstanden. Ich möchte mich daher besonders bei meinem Betreuer Univ.-Doz. Dipl.-Ing. Dr.techn. Martin Ebner bedanken, der mich während der Erstellung dieser Arbeit unterstützt hat. Danke!

Desweiteren möchte ich mich bei meinen Studienkollegen bedanken, die mich desöfteren erheitern konnten, wodurch die gemeinsame Zeit bei Gruppenarbeiten nicht nur auf das Fachliche beschränkt war.

Besonderer Dank gilt natürlich meiner Familie, ohne die das nun leider etwas lang geratene Studium nicht möglich gewesen wäre. Während des Studiums gab es viele Rückschläge, die desöfteren in einer Motivationskrise endeten. Doch durch aufmunternde und aufbauende Worte, konnten letztlich alle Krisen überstanden werden, wodurch ich nun die Gelegenheit für diese Zeilen habe: Ich liebe euch, von ganzem Herzen! Ihr seid die Besten!

Martin Maierhuber
Graz, im April 2013

Inhaltsverzeichnis

1 Einleitung 15

2 Strichcodes 16

2.1 Geschichtliches – Vom Barcode zum QR-Code ... 16
2.1.1 Barcode ... 16
2.1.2 PDF417 ... 18
2.1.3 DataMatrix ... 19
2.1.4 QR-Code ... 19

2.2 QR-Code ... 20
2.2.1 Spezifikation ... 20
2.2.2 Anwendungsgebiete ... 22
2.2.3 Weiterentwicklungen ... 29
2.2.4 Sonderformen von QR-Codes ... 32

2.3 Strichcodes und NFC ... 34

2.4 Zusammenfassung ... 35

3 RFID 36

3.1 Geschichte der Entwicklung ... 36

3.2 Technische Spezifikation ... 37
3.2.1 Aufbau 37
3.2.2 Technik 38

3.3 Einsatzgebiete ... 38
3.3.1 Logistik ... 39
3.3.2 Fahrzeugidentifikation ... 39
3.3.3 Personenidentifikation ... 39
3.3.4 Bezahlsysteme ... 40
3.3.5 Textilindustrie ... 40
3.3.6 Landwirtschaft ... 41
3.3.7 Zugangskontrollsysteme ... 41
3.3.8 Bibliotheken ... 42

3.4 Probleme und Bedenken ... 42

3.5 Zusammenfassung ... 43

4 NFC 44

4.1 Geschichtliche Entwicklung von NFC ... 44

4.2 Aktueller Stand der Technik ... 45

4.3 Einsatzgebiete ... 48

4.3.1 Bezahlsysteme ... 48
4.3.2 Zugangskontrollsysteme ... 50
4.3.3 Logistik ... 51
4.3.4 Marketing ... 51
4.3.5 Informationswesen ... 52
4.3.6 NFC als Vermittler anderer Verbindungen ... 52
4.3.7 Steuerung des Gerätes mittels NFC-Tags ... 53
4.4 NFC im Vergleich zu anderen Technologien ... 53
4.4.1 NFC und RFID ... 53
4.4.2 NFC und Strichcodes ... 54
4.5 Probleme, Bedenken und Kritiken ... 54
4.5.1 Abhören ... 54
4.5.2 Übertragungsstörung ... 55
4.5.3 Datenmodifikation ... 55
4.5.4 Einfügen von Daten ... 56
4.5.5 Man in the Middle Angriff ... 56
4.5.6 Relay-Angriffe ... 57
4.5.7 Gerätverlust ... 57
4.5.8 Finanzbetrug durch ungewollte Abbuchungen ... 58
4.6 Zusammenfassung ... 58

5 Praktisches Implementation zu NFC 59

5.1 Motivation ... 59
5.2 Android App ... 59
5.2.1 Aufgabenstellung und Ziele ... 60
5.2.2 Technologien ... 60
5.2.3 Implementierung ... 64

6 Potentiale von NFC für Lehr- und Lernunterlagen 83

6.1 Distribution von Unterlagen ... 84
6.2 Zusatzinformationen zu Unterlagen ... 84
6.3 Teilen von Unterlagen ... 85
6.4 Abgeben von Übungen ... 85
6.5 Integration sozialer Netzwerke ... 85
6.6 Zugangskontrolle von Unterlagen durch NFC ... 86
6.7 Prüfungen ... 86
6.8 Zusammenfassung ... 87

7 Ausblick 88

7.1 Aktuelle Trends ... 88
7.2 Möglichkeiten für zukünftige Forschungsarbeiten ... 89

8 Zusammenfassung und Fazit 91

9 Literaturverzeichnis 94

10 Abbildungsverzeichnis 101

11 Tabellenverzeichnis 103

12 Codelistingverzeichnis 104

1 Einleitung

Diese Masterarbeit behandelt das Thema Near Field Communication (NFC) – Potentiale für Lehr- und Lernunterlagen.

NFC gilt als eine Technologie mit sehr vielen Möglichkeiten in vielen Bereichen. Daraus ergibt sich die Fragestellung, in welchen Bereichen die Technologie nutzbar gemacht werden kann. Diese soll in dieser Arbeit insbesondere am Beispiel von Lehr- und Lernunterlagen beantwortet werden.

Zuerst wird es einen geschichtlichen Überblick über die technischen Entwicklungen geben, in dem auch auf teilverwandte Vorläufertechnologien wie Barcodes und insbesondere QR-Codes eingegangen werden wird. Diese werden in Kapitel 2 beschrieben und anhand einiger Einsatzgebiete auch Vergleiche zu NFC gezogen.

In Kapitel 3 wird die RFID Technologie vorgestellt, die in einigen Anwendungsfällen als Vorläufer zu NFC gilt. Ebenso wird es einige Einsatzbeispiele geben, die den Zusammenhang mit NFC verdeutlichen und einen Übergang zu Kapitel 4 bieten, in welchem NFC genau beschrieben wird. Es wird einen Überblick über die geschichtliche Entwicklung von NFC bis hin zum aktuellen Stand der Technik geben. Dabei wird auch auf die Spezifikation eingegangen, die auch in einem Unterkapitel bei sicherheitskritischen Fragen diskutiert wird.

Anschließend wird der im Rahmen dieser Masterarbeit angefertigte Prototyp einer Smartphone App vorgestellt, die einige Kommunikationsformen mit NFC in Verwendung mit Lehr- und Lernunterlagen zeigt.

Aus dem Prototyp abgeleitet, widmet sich das Kapitel 6 ganz den Potentialen und beschreibt einige Möglichkeiten des Autors, die nach dessen Ansicht in Zukunft mögliche Anwendungsfälle darstellen können. Diese sind jedoch theoretischer Natur, da die derzeitige Entwicklung von NFC für einige dieser Potentiale noch nicht ausreichend ist.

Anhand der in den zuvor beschriebenen Kapiteln wird es in Kapitel 7 eine kurze Übersicht über aktuelle Trends von NFC geben, die als Ausblick der Technologie dienen sollen. Dadurch werden auch ein paar Möglichkeiten für zukünftige Forschungsarbeiten präsentiert.

Abschließend gibt es in Kapitel 8 noch eine Zusammenfassung und ein kurzes persönliches Fazit.

2 Strichcodes

In diesem Kapitel werden die Vor- und Nachteile von zweidimensionalen Barcodes erläutert. Es werden technische Hintergründe, sowie die Entwicklungsgeschichte von QR-Codes beschrieben sowie einige Anwendungsfälle diskutiert. Abschließend wird eine kurze Überleitung zum Kernthema NFC geschaffen, um den Zusammenhang der beiden Technologien näher zu erläutern.

2.1 Geschichtliches – Vom Barcode zum QR-Code

Abbildung 2-1 Einige zweidimensionale Codes im Überblick **(Mobile Tagging, 2007)**

2.1.1 Barcode

Der Barcode, auch Strichcode oder Balkencode genannt, wurde 1949 von Norman Joseph Woodland und Bernard Silver entwickelt und schließlich am 7. Oktober 1952 patentiert (US Patent Office, 2013).

Doch es dauerte über 20 Jahre, bis der Barcode als Universal Product Code (UPC) im Frühling 1973 in Supermärkten der USA eingesetzt wurde. In Europa mussten noch ein paar Jahre vergehen, bis der Barcode als EAN (European Article Number) in den Geschäften Einzug hielt (Heise Online, 2008).

Mittlerweile sind die Strichcodes aus den Geschäften und der automatisierten Warenwirtschaft nicht mehr wegzudenken.

Ein Beispielbild eines EAN8 Barcodes ist in der Abbildung 2-2 **EAN8 Code** zu sehen:

Abbildung 2-2 EAN8 Code **(Strichcode, 2013)**

Es zeigt sich: Die „Kapazität“ an Informationen ist bei eindimensionalen Strichcodes begrenzt. Die Kapazität mag zwar für Produktinformationen in der Warenwirtschaft ausreichend sein, doch um die erhöhte Informationsübertragung in anderen Einsatzgebieten zu ermöglichen, ist die Kapazität nicht mehr ausreichend.

Der Aufbau einer heute weit verbreiteten GTIN (Global Trade Item Number) – bis 2009 EAN – sieht beispielsweise wie in (GTIN (EAN-Code), 2013) beschrieben aus und ist in Abbildung 2-3 GTIN-13 Code dargestellt und erläutert:

Abbildung 2-3 GTIN-13 Code **(GTIN (EAN-Code), 2013)**

Die Basisnummer kann 7, 8 oder 9 Stellen haben

7-stellige Basisnummer (Kapazität: 100.000 GTIN)

8-stellige Basisnummer (Kapazität: 10.000 GTIN)

9-stellige Basisnummer (Kapazität: 1.000 GTIN)

2.1.2 PDF417

Eine Weiterentwicklung der eindimensionalen Strichcodes manifestiert sich in dem als ISO/IEC Norm spezifizierten PDF417 Format.

PDF417 – Portable Data File - wurde von Dr. Ynjiun P. Wang bei Symbol Technologies entwickelt und am 7. September 1993 patentiert (US5243655, 1993).

Die Nummer 417 ist darauf zurückzuführen, dass es 4 Balken und 4 Lücken, sowie 17 Module gibt.

Eine kurze Erklärung der PDF417 Norm sei in folgende Zitat von (PDF417 bar code, 2013) gegeben:

„Die 2D-Codes sind in aller Regel quadratisch aufgebaut und bestehen aus einem zweidimensionalen Bitmuster. Anders ist es mit dem 2D-Code PDF417, der im internationalen Zahlungsverkehr bei den International Payment Instructions (IPI) benutzt wird, aber auch von der Kassenärztlichen Vereinigung für medizinische Formulare und bei der elektronischen Steuererklärung Anwendung findet. Der PDF417 ist ein Stacked-Code oder Codablock, ein mehrfach gestapelter Strichcode, der aus mehreren untereinander angeordneten Strichcodes besteht.“

Abbildung 2-4 zeigt den Aufbau eines PDF417 Codes:

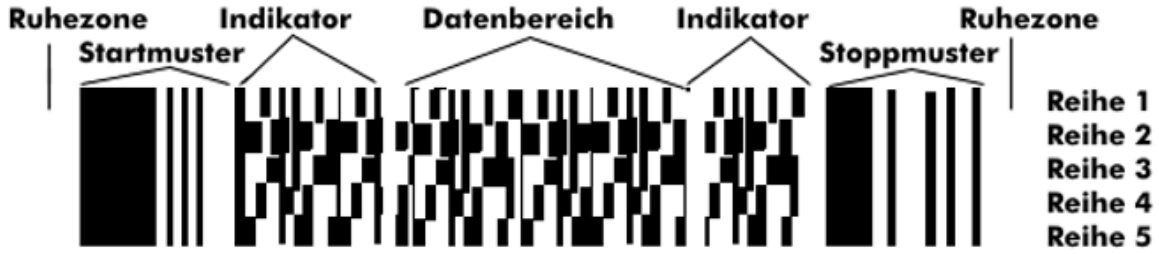

Abbildung 2-4 PDF417 Code Aufbau **(PDF417 bar code, 2013)**

Jeder, der unlängst einen Flug hinter sich hatte, konnte auf seiner Bordkarte einen PDF417 Code erkennen. So befinden sich an den Flughäfen mittlerweile statt der früher üblichen Abrisstickets samt zugehörigem Personal vermehrt automatisierte Durchgangsschranken mit Codescannern. Aber auch Paketdienste wie FedEx verwenden PDF417 auf ihren Verpackungen (Bar Code & Label Layout Specification, 2004). Die maximale Zeichenanzahl ist mit 350 ASCII Zeichen festgelegt, obwohl laut ihren eigenen Aussagen in der Quelle 2725 Zeichen möglich wären, wie aus folgendem Zitat aus (Bar Code & Label Layout Specification, 2004) hervorgeht:

„PDF stands for “Portable Data File” and the symbology can encode up to 2725 characters in a single symbol, however this is reduced by the error correction level and the application. FedEx Ground has set a limit of 350 characters. The complete PDF-417 specification provides many encoding options including data compression options, error detection and correction options, and variable size and aspect ratios.“

2.1.3 DataMatrix

Der DataMatrix-Code wurde von der Firma International Data Matrix, Inc. (ID Matrix) entwickelt und zählt zu den beliebtesten zweidimensionalen Codes. Die DataMatrix-Codes können sowohl quadratisch, als auch rechteckig dargestellt werden. Dadurch sind platzkritische Einsatzgebiete möglich. DataMatrix-Codes halten bis zu 2KB an Daten und sind mit dem in Kapitel 2.2 näher beschriebenen QR-Code vergleichbar. Ebenso wie bei QR-Codes wird bei der Fehlerkorrektur ein Reed-Solomon-Algorithmus eingesetzt, der eine bis zu 25 Prozent Fehleranteil (Schema ECC140) beherrschen kann (Han-soft Corporation, 2013).

In Abbildung 2-5 ist ein Beispiel für einen DataMatrix-Code gezeigt:

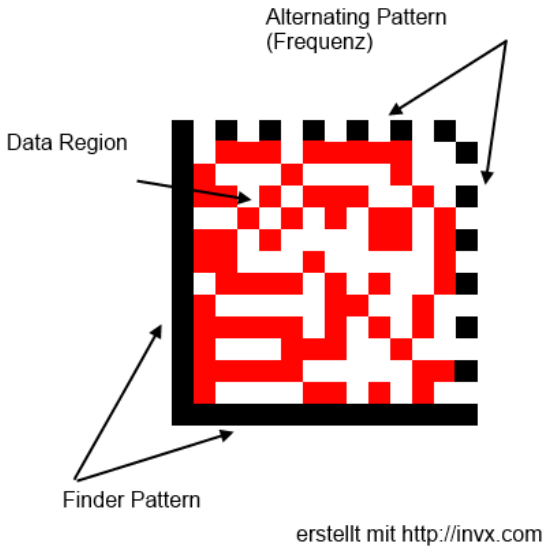

Abbildung 2-5 DataMatrix-Code **(Dipl-Ingo, 2013)**

Die Einsatzgebiete ähneln jenen des QR-Codes, wodurch dieser stellvertretend für zweidimensionale Codes in Kapitel 2.2 näher erläutert wird.

2.1.4 QR-Code

Der QR-Code – von englisch Quick Response – ist wie auch PDF417 ein zweidimensionaler Code.

Entwickelt wurde er im Jahre 1994 von der Firma Denso Wave, die auch das Patent und Markenrecht auf den Namen „QR Code“ hält. Allerdings hat die Firma die Spezifikation öffentlich zugänglich und frei verfügbar gemacht und setzt ihr Patentrecht auf Kostenersatz nicht durch (Denso Wave, 2013).

Durch die weite Verbreitung optischer Scanner in mobilen Geräten wie Smartphones und Tablets, bietet sich ein zweidimensionaler Code zur einfachen Verbreitung von Information an.

Technische Details, sowie Anwendungsfälle und zusätzliche Informationen sind dem Kapitel 2.2.1 zu entnehmen.

2.2 QR-Code

Dieses Unterkapitel widmet sich den technischen Details von QR-Codes, sowie Vergleichen zu Vorläufertechnologien und zeigt einige Anwendungsfälle.

2.2.1 Spezifikation

Der QR-Code ist laut (Denso Wave, 2013) seit Juni 2000 in ISO/IEC18004 standardisiert. Weitere Standardisierungen sind Tabelle 1 zu entnehmen:

October, 1997	Approved as AIM International (Automatic Identification Manufacturers International) standard (ISS - QR Code)
March, 1998	Approved as JEIDA (Japanese Electronic Industry Development Association) standard (JEIDA-55)
January, 1999	Approved as JIS (Japanese Industrial Standards) standard (JIS X 0510)
June, 2000	Approved as ISO international standard (ISO/IEC18004)
November, 2004	Micro QR Code is Approved as JIS (Japanese Industrial Standards) standard (JIS X 0510)
December 2011	Approved by GS1, an international standardization organization, as a standard for mobile phones

Tabelle 1 QR-Code Standards **(Denso Wave, 2013)**

Und die Spezifikation in Tabelle 2:

Symbol size	21 x 21 – 177 x 177 modules (size grows by 4 modules/side)	
Type & Amount of Data (mixed use is possible.)	Numeric	Max. 7,089 characters
	Alphanumeric	Max. 4,296 characters
	8-bit bytes (binary)	Max. 2,953 characters
	Kanji	Max. 1,817 characters
Error correction (data restoration)	Level L	Approx. 7% of codewords can be restored
	Level M	Approx. 15% of codewords can be restored
	Level Q	Approx. 25% of codewords can be restored
	Level H	Approx. 30% of codewords can be restored
Structured append	Max. 16 symbolds (printing in a narrow area etc.)	

Tabelle 2 QR-Code Spezifikation **(Denso Wave, 2013)**

Anhand Tabelle 2 ist schnell ersichtlich, dass QR-Codes deutlich mehr Informationen speichern können als andere 2D-Codes, wie zum Beispiel PDF417. Dabei ist die Fehlerkorrektur bei *Level H* mit 30% schon sehr gut und die effektive Abbildungsgröße des anzuzeigenden QR-Codes im Vergleich zu anderen Methoden verhältnismäßig klein.

Folgende Abbildung zeigt den Größenunterschied derselben Information, die in einem Barcode dargestellt wird:

Abbildung 2-6 Barcode vs. QR-Code **(Denso Wave, 2013)**

Die Fehlerkorrektur verwendet *Reed-Solomon Code* (Denso Wave, 2013), wie auch PDF417 (IDAutomation, 2013).

Durch die beispielsweise 30-prozentige Fehlerkorrektur sind QR-Codes einigermaßen geschützt vor Umwelteinflüssen und Schmutz. Abbildung 2-7 soll die Wiederherstellbarkeit der beinhalteten Information illustrieren:

Abbildung 2-7 QR-Code Fehlerkorrektur **(Denso Wave, 2013)**

QR-Codes können mit Hilfe der Positionierungsmuster von allen Richtungen gelesen werden. Die Positionierungsmuster sind in Abbildung 2-8 markiert:

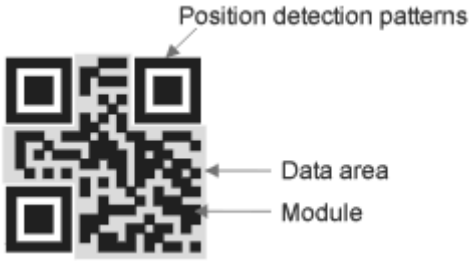

Abbildung 2-8 QR-Code Positionierungsmuster **(Denso Wave, 2013)**

Dadurch entfällt eine zwingende Angabe der Ausrichtung des Lesegerätes beim Lesen des QR-Codes, da die Ausrichtung des QR-Codes anhand der Positionierungsquadrate an den 3 Ecken automatisch erkannt werden kann.

Ein weiterer großer Vorteil von QR-Codes ist die Aufteilung von Information auf mehrere QR-Codes, falls sich die Information beispielsweise nicht in einem QR-Code abbilden lässt. Dies ist in Abbildung 2-9 gezeigt:

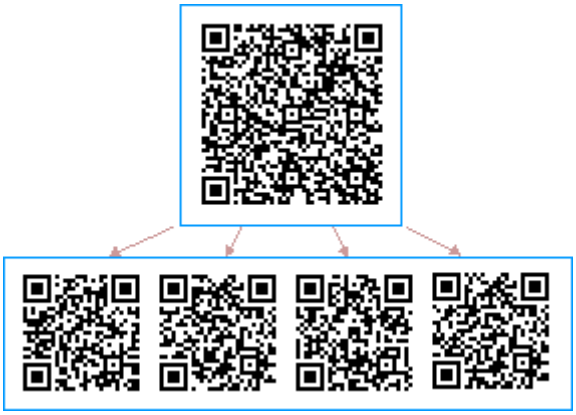

Abbildung 2-9 QR-Code Aufteilung **(Denso Wave, 2013)**

2.2.2 Anwendungsgebiete

QR-Codes haben sich in den letzten Jahren sehr schnell verbreitet. Das liegt nicht zuletzt an den unzählig möglichen Einsatzgebieten und der freien Verfügbarkeit. Durch die mittlerweile sehr weit verbreiteten mobilen Geräte mit integrierter Kamera (Smartphones, Tablets), kann man eine große Anzahl an Benutzerinnen und Benutzern ansprechen.

2.2.2.1 Produktion

Das ursprünglich gedachte Haupteinsatzgebiet ist natürlich die automatisierte Warenwirtschaft, da die Entwicklergesellschaft eine Tochtergesellschaft von Denso ist, welche Teil der Toyota-Gruppe ist. Laut (Denso Wave, 2013) werden einzelne Teile in der Automobilindustrie mit Informationen über Kunden, Transporteur, Produktnummer, Menge und anderen Daten in QR-Codes gespeichert und etikettiert. Dadurch können in einem einzigen Lesevorgang alle relevanten Daten abgerufen werden. So spart man sich die optische Texterkennung mittels Optical Character Recognization (OCR) Verfahren, welche wesentlich aufwendiger sind, wenngleich sie den Vorteil haben, dass der geschriebene Text auch direkt vom Menschen lesbar ist. Dieser Vorteil verschwindet aber immer mehr, weil QR-Code-Scanner in mobilen Geräten schon sehr weit verbreitet sind und daher praktisch jede Mitarbeiterin und jeder Mitarbeiter mit einem Smartphone den entsprechenden Code lesen und überprüfen könnte. Aus Platzgründen kann man dann auf die zusätzliche menschlich lesbare Information, das heisst der im QR-Code enthaltene Text in niedergeschriebener Form, verzichten.

Ein weiteres von Denso Wave erläutertes Einsatzgebiet ist beispielsweise die Prozessleittechnik wie auf (Denso Wave, 2013) angegeben. Auf elektronischen Bauteilen werden auf drei Quadratmillimeter Informationen über Herstellungsdatum, Produktlinie, Seriennummer und anderen Daten gespeichert. Dadurch können die elektronischen Bauteile automatisiert eingesetzt und zusammengefügt werden. Da die vollautomatisierten Vorgänge entsprechend protokolliert werden, erhält man eine komplette Übersicht über die entsprechende Prozesssteuerung.

2.2.2.2 Logistik

Durch den Einsatz von QR-Codes in der Logistik können die automatisierten Warenwirtschaftssysteme auf zusätzliche Parameter reagieren, während weiterhin nur ein Lesesystem nötig bleibt. So können auf Waren erweiterte Metadaten wie beispielsweise Ablaufdatum integriert werden, anhand denen die Auslieferung letztlich ausgerichtet wird. So kann ein FIFO (*First-In-First-Out*) Vorgang gewährleistet werden. Desweiteren ist es dadurch möglich, Produktbewegungen genauer zu verfolgen.

Zusätzlich können Lieferirrtümer vermieden werden, indem für den Menschen offensichtliche Eigenschaften in den QR-Code eingearbeitet werden. So erhält man eine Art der doppelten Produktprüfung, da ein Logistikmitarbeiter mit einem Smartphone diese im QR-Code enthaltenen Daten nachprüfen kann und generell auf alle mit dem jeweiligen Produkt verknüpften spezifischen Daten abfragen kann.

2.2.2.3 Verkauf

Mitarbeiter im Verkauf können zusätzliche Daten per QR-Code abfragen und dem Kunden auf verschiedenste Art präsentieren. Dies können beispielsweise öffentlich verfügbare Daten (z.B. eine URI) zu einem Präsentationsvideo sein, aber auch interne jeweils in Echtzeit abgerufene Daten sein. Durch die auch beim Kunden mittlerweile weit verbreiteten Smartphones, können die erhaltenen Informationen auch am Gerät vom Kunden selbst allerorts gelesen und gegebenenfalls verglichen werden.

Desweiteren können Geschäfte auf die offene Lagerung von Produkten verzichten, wenn sie stattdessen Abbildungen von Produkten mit ihnen zugeordneten QR-Codes ausstellen. Kunden können den QR-Code dann scannen und das Produkt bestellen und liefern lassen. Der Lebensmittelkonzern Tesco hat diese Variante in einer U-Bahnstation in Seoul eingeführt, wie die Abbildung 2-10 zeigt:

Abbildung 2-10 QR-Code shopping **(ORF, 2012)**

2.2.2.4 Elektronische Visitenkarten

QR-Code können auch als Visitenkarten verwendet werden, wie Abbildung 2-11 zeigt:

Abbildung 2-11 QR-Code Visitenkarte **(Ebner, 2008)**

Dabei speichert man die in der elektronischen Visitenkarte enthaltenen vCard Daten als .vcf Datei auf einem öffentlichen Webserver und generiert zur dahinzeigenden URI den QR-Code. In der Beispielgrafik wird zusätzlich noch ein Logo eingebettet. Diese Sonderform des QR-Codes wird in Kapitel 2.2.3 näher erläutert.

2.2.2.5 Terminverwaltung

Ein weiteres Einsatzgebiet für QR-Codes kann die eigene Terminverwaltung sein. So kann man den Termin über den QR-Code in die eigene Kalender-App eintragen lassen. Dies kann zum Beispiel ein Event sein, der auf einer Litfaßsäule ausgehängt ist. Ort und Datum stehen dann bequem in der Kalender-App (Ebner, 2008).

2.2.2.6 m-Learning

Besonders unter jüngeren Benutzerinnen und Benutzern sind Smartphones schon sehr weit verbreitet und elektronische Lernhilfen generell sehr beliebt. So könnte man ein RSS-Feed via QR-Code verteilen (Ebner, 2008), wodurch Studierende zusätzliche, aktuelle Informationen erhalten können. Desweiteren können Links zu Lehrveranstaltungsvideos auf Videoportalen verteilt werden, wodurch beispielsweise die vollständig aufgezeichnete Lehrveranstaltung zum Nachsehen verfügbar ist.

2.2.2.7 Vordefinierte Email, SMS oder Telefonanrufe

Ein eher problematischer Bereich von QR-Code-Anwendungen sind vorgefertigte Emails, SMS oder Telefonanrufe. Diese können mitunter ein Sicherheitsrisiko darstellen, sowie unerwünschte zusätzliche Kosten verursachen.

2.2.2.8 Mobiler Zahlungsverkehr

Ein weiteres mögliches Einsatzgebiet von QR-Codes ist der mobile Zahlungsverkehr. Die eingesetzte Technologie steht in Konkurrenz zu NFC, da die Hardwareanforderungen derzeit nicht von allen mobilen Geräten erfüllt werden. QR-Code Scanner funktionieren hingegen auf einer breiten Masse an Geräten.

Auf QR-Codes basierende Bezahlsysteme befinden sich derzeit (Stand 18.2.2013) noch in einem frühen Stadium. Die Bank of America testet laut (Rothacker, 2012) derzeit so ein System.

Die Kaffeehauskette Starbucks hat Anfang 2012 eine Kampagne gestartet, wo QR-Codes zur Bezahlung in den Kaffeehäusern verwendet werden soll. Dabei wird eine App namens *Square Wallet* verwendet, die auf dem Smartphone des Kunden einen QR-Code generiert, der dann an der Kassa vom Smartphonedisplay abgelesen wird (Squareup, 2013).

In Österreich laufen aktuell (Stand Februar 2013) Vorbereitungen für die Einführung von QR-Codes auf Zahlscheinen für Überweisungen (ORF.at, 2012). Durch die endgültige Einführung von IBAN und BIC Anstelle von Kontonummer und Bankleitzahl, steigt die mögliche Fehlerquote beim Eintippen der deutlich längeren Zeichenfolgen. Eine IBAN ist laut obiger Quelle mit 20 Stellen, bzw. eine BIC mit 8 oder 11 Stellen, spezifiziert. Dadurch wäre die Verwendung von QR-Codes, oder ähnlichen Methoden, eine deutliche Erleichterung und Zeitersparnis.

Abbildung 2-12 illustriert einen Zahlschein mit QR-Code:

Abbildung 2-12 Zahlschein mit QR-Code **(Austrian Payments Council, 2012)**

2.2.2.9 Marketing

In letzter Zeit eines der häufigsten Einsatzgebiete für QR-Code sind Marketingflyer, Broschüren und Werbungen in Druckmedien. Letztlich müssen die Printmedien mit der neuen Zeit mithalten können und eine Brücke zwischen mobilen Benutzern und der Zeitschrift selbst schaffen. Inserate in Zeitschriften können mit Hilfe von QR-Codes sparsam mit dem kostbaren Werbeplatz umgehen und verschaffen dem potentiellen Kunden eine Erleichterung, da er nicht mehr die URI abtippen muss, sondern bequem per mobilem Gerät nachschlagen kann.

Aber auch Zeitschriftenautoren selbst können ihre Quellen oder Artikelzusatzinformationen per QR-Code zugänglich machen, um deren Webseiten zu mehr Zugriffen zu verhelfen.

2.2.2.10 Zugangskontrollsysteme

QR-Codes können auch auf Tickets verwendet werden, wo der Zugang an Lesestellen geprüft wird. Hierbei ist aber zu beachten, dass der Lesevorgang länger dauert als bei gewöhnlichen Barcodes, die für diese Art der Verwendung in den meisten Fällen deutlich besser geeignet sind.

Übersteigt aber die Menge der Information die Grenzen von Barcodes, oder gar PDF417 Codes, greift man gerne auf QR-Codes zurück. Besonders bei Zugangskontrollen zu verschiedenen Zugangsebenen sind QR-Codes deutlich sinnvoller, da sie laut Spezifikation mehr Informationen überliefern können.

QR-Codes mit Verschlüsselung (siehe Kapitel 2.2.3.2) werden beispielsweise von der japanischen Einwanderungsbehörde auf Visa verwendet, wie auch Abbildung 2-13 zeigt:

Abbildung 2-13 Security-QR-Code Visum in Japan **(QR Code Usage In Japan, 2009)**

2.2.2.11 Objektinformationen

QR-Codes können auch dazu verwendet werden, einzelnen Objekten, beispielsweise in einem Labor, eine Kennung zu geben. Das kann besonders bei sehr kleinen Gegenständen sinnvoll sein, zu denen besonders viele Informationen überliefert werden müssen. Oft reicht der Platz für Textzeichen nicht mehr aus, wogegen Micro-QR-Code oder auch iQR-Code für solche Fälle prädestiniert sind.

Weiterführende Informationen zu Micro-QR-Code und iQR-Code sind Kapitel 2.2.3 zu entnehmen.

2.2.2.12 Tourismus

Auch im Tourismus können QR-Codes eingesetzt werden. Beispielsweise bei der Beschreibung von Sehenswürdigkeiten, Bauwerken und Denkmälern, aber auch die Verkehrsbetriebe können die QR-Codes mit der Routing-Funktion verbinden (Strauß, Scholz, Ebner, & Schmidmayr, 2009).

QR-Codes haben also auch im Tourismus ein großes Potential. Hinweistafeln können unter Umständen veraltete Informationen zeigen. Mit einem QR-Code, der auf eine Webseite verweist, könnte man das Problem umgehen, da die Webseite einfacher aktualisiert werden kann. Allerdings muss man darauf achten, dass die zugrundeliegende Struktur nicht geändert wird, da sonst der Link ins Leere zeigen kann.

Anstelle von Broschüren zum Mitnehmen, verwendet der Tourist sein eigenes Endgerät und kann auf diesem die jeweilige Information auch mitnehmen und ist nicht mehr ortsgebunden. Auf (Touristische Anwendungsbeispiele für QR-Codes, 2013) gibt es ein Beispiel, wie das realisiert werden kann:

„Im gesamten Rauristertal werden Informationstafeln aufgestellt, die allgemeine und für Rauris spezifische Informationen über das Wasser vermitteln. Ein in sich geschlossener 2,5 km langer Wasserinformationsweg bietet wissenschaftliche Information, während an den einzelnen Quellen angebrachte Hinweistafeln lokale Gegebenheiten erklären. An bestimmten

besonders interessanten Plätzen (Wasserfälle, große Quellen oder Biotope) werden Erholungsplätze zum Beobachten und Genießen der Naturschönheiten geschaffen. Dazu gibt es eine mehrseitige Informationsbroschüre. Die Broschüre soll neben allgemeinen Informationen zum Thema Wasser, die einzelnen Punkte beschreiben und den Informationsweg in einer aussagekräftigen Karte darstellen.

Die Informationstafeln sind im A3-Format erstellt und werden an den definierten Stellen positioniert. Die Schautafeln beschreiben dann den jeweiligen Ort beschreiben und mit Hilfe eines QR-Codes wird dann auf eine weiterführende Unterseite der www.rauristertal.at verweisen. Dort befinden sich dann detaillierte Informationen zum eben besuchten Ort, eine Routenplanung mit Hilfe von Google Maps, Youtube-Videos über die Entstehung des Ortes, eine Audiodatei in deutscher und englischer Sprache die für sehbehinderte Menschen den besuchten Ort beschreibt uvm.

Die verschiedenen QR-Codes befinden sich dann auch in der oben erwähnten Infobroschüre und können individuell ebenfalls von hier aus aufgerufen werden. Der "Wasserwanderer" erspart sich damit mit dem Smartphone das umständliche Eintippen von URLs und die Navigation auf der Webseite. Dieses Projekt – unter der Leitung von TVB-GF Mag.Alexandra Fankhauser – wird im Frühjahr 2012 abgeschlossen und ist jedenfalls einen Besuch wert – nicht nur der QR-Codes wegen."

Man sieht also, dass das Potential moderner Medien auch in IT-fremden Bereichen vorhanden ist. Die Verknüpfung konventioneller Methoden wie Broschüren, Plakate und Zeitschriften mit der digitalen Welt, bietet für beide Seiten unzählige Möglichkeiten und Vorteile. Allerdings ist die technische Herausforderung nicht zu unterschätzen.

2.2.2.13 Sonstiges

Weitere Möglichkeiten QR-Codes einzusetzen zeigt ein Neulengbacher Internetunternehmen (ORF, 2012): Auf Grabsteinen werden QR-Codes platziert, die zu einem Medienarchiv des Verstorbenen führen. Dabei wird der QR-Code per Sandstrahl in den Grabstein eingraviert, wie Abbildung 2-14 zeigt:

Abbildung 2-14 QR-Code Gräbercodes **(ORF, 2012)**

2.2.3 Weiterentwicklungen

Natürlich existieren schon einige Weiterentwicklungen zu QR-Codes. Einige davon werden in den folgenden Unterkapiteln näher beschrieben.

2.2.3.1 Micro-QR-Code

Der Micro-QR-Code ist eine flächenmäßig stark reduzierte Version des QR-Code. Er besitzt nur mehr ein Positionserkennungsmuster, welches sich in der linken oberen Ecke befindet. Natürlich wird dieser Platzvorteil durch den Verlust an Datenkapazität erreicht. Der größte Micro-QR-Code kann noch immer weniger Daten halten als der kleinste gewöhnliche QR-Code. Lediglich der Platzverlust durch erhöhte Fehlerkorrektur wird optimiert (Denso Wave, 2013).

Obiger Quelle entnommen ist Abbildung 2-15, die den Unterschied von Micro-QR-Codes zu gewöhnlichen QR-Codes zeigt:

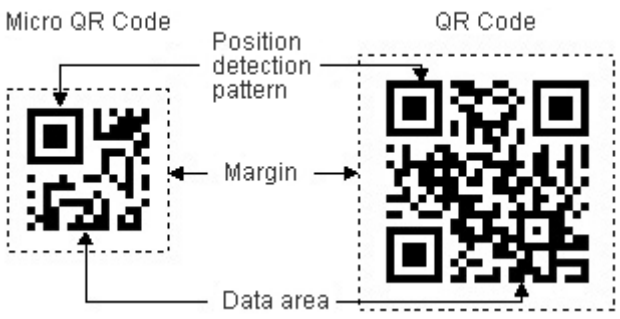

Abbildung 2-15 Micro-QR-Code und QR-Code **(Denso Wave, 2013)**

Der primäre Einsatzzweck dieser Micro-QR-Codes findet sich auf elektronischen Bauteilen, auf denen der vorhandene Platz entsprechend gering ist. Denso Wave hat diese Variante im November 2004 standardisieren lassen (JIS X 0510).

Bei der geringsten Fehlerkorrektur kann der größte Micro-QR-Code beispielsweise 35 numerische Zeichen halten, während der kleinste gewöhnliche QR-Code 41 numerische Zeichen halten kann. Die Modulgröße ist dabei mit 17x17 gegenüber 21x21 jedoch deutlich geringer. Dadurch wird die Nutzung der verwendeten Fläche optimiert.

2.2.3.2 Security-QR-Code (SQRC)

Denso Wave stellte im Jahr 2005 den Secure-QR-Code vor, mit dem sich die Daten entsprechend verschlüsseln lassen. Dabei ist es jedoch möglich, die im QR-Code enthaltenen Daten teilweise verschlüsseln und teilweise öffentlich bereit zu stellen. Ein gewöhnliches QR-Code-Lesegerät kann dann nur die unverschlüsselten Daten lesen. Für den verschlüsselten Teil ist ein spezielles Lesegerät erforderlich. Anders als bei digitalen Verschlüsselungen müssen QR-Codes immer neu generiert werden, wenn sich an der Verschlüsselung etwas ändern soll. Dies hat den Vorteil, dass keine weitere Entschlüsselungssoftware benötigt wird.

Gewöhnlich wird ein 128 bit Schlüssel verwendet, der eine ähnliche Sicherheit wie ein DES-56 Algorithmus bietet, wie (Denso Wave, 2013) berichtet.

2.2.3.3 iQR-Code

Ebenfalls ein von Denso Wave weiterentwickelter QR-Code findet sich als iQR-Code. Hier werden die Vorteile des Micro-QR-Code integriert, indem man ebenfalls auf die Positionierungsmuster verzichtet. Zudem ist die Form nicht mehr zwingend auf ein Quadrat festgelegt, sondern kann auch rechteckig sein. Dies ermöglicht neue Anwendungsbereiche, beispielsweise auf nicht-ebenen Flächen, wo das Lesen quadratischer Codes oft schwierig oder unmöglich war. Durch das Weglassen der zusätzlichen Positionierungsmuster des ursprünglichen QR-Codes, erhält man weiteren Platz für Daten, aber auch für die Fehlerkorrektur (GS1 Japan, 2009).

Laut obengenannter Quelle kann das größte Format eines iQR-Codes ungefähr 40000 alphanumerische Zeichen halten, was gegenüber einem gewöhnlichen QR-Code mit ungefähr 7000 alphanumerischen Zeichen ein doch deutlicher Zuwachs ist. Die effektive Druckgröße eines iQR-Codes im Vergleich zu einem gewöhnlichen QR-Code wurde ebenfalls um bis zu 30% reduziert.

Die rechteckige Variante lässt sich somit auf Oberflächen wie Kabeln, oder Rohren einsetzen, da die Ausrichtung nur mehr entlang einer Achse verifiziert werden muss und die Druckfläche an einer Achse gering gehalten werden kann. So zeigt folgende, obiger Quelle entnommene Abbildung 2-16 einen rechteckigen iQR-Code:

Abbildung 2-16 iQR-Code **(GS1 Japan, 2009)**

Folgende, obiger Quelle entnommene Abbildung 2-17 zeigt die Spezifikation von iQR-Codes und stellt sie QR-Codes und Micro-QR-Codes gegenüber:

	iQR Code	QR Code(Micro QR)
Type	Square, Rectangle	Square
Version	Square : 1(9x9 Cell)~61(422x422 Cell)	QR Code:1(21x21 Cell)~40(177x177 Cell)
	Rectangle : R1(5x19 Cell)~R15(43x131 Cell)	Micro QR:M1(11x11 Cell)~M4(17x17 Cell)
Incorrection Modification	L(7%),M(15%),Q(25%),H(30%), S(50%)	L(7%),M(15%),Q(25%),H(30%)
Character	Numeric,Alphabet, Text(Mode A/B/C), Kanji,Binary	Numeric, Alphabet, Kanji, Binary
Combination	16 Division (Only Square)	16 Division (Only QR Code)
Type	Square, Rectangle	Square
Special Code	Two Sides Inversion, White Black Inversion, Dot Pattern	White Black Inversion,Dot Pattern
Others	GS1 Support , Data Compression	GS1 Support
Margin	2 Cell	4 Cell(Micro QR: 2 Cell)

Abbildung 2-17 iQR vs QR Code **(GS1 Japan, 2009)**

Der iQR-Code ist damit sowohl in der quadratischen, als auch in der rechteckigen Form dem DataMatrix Code (siehe Kapitel 2.1.3) überlegen, wie auch die folgende, ebenfalls obiger Quelle entnommene Abbildung 2-18 zeigt:

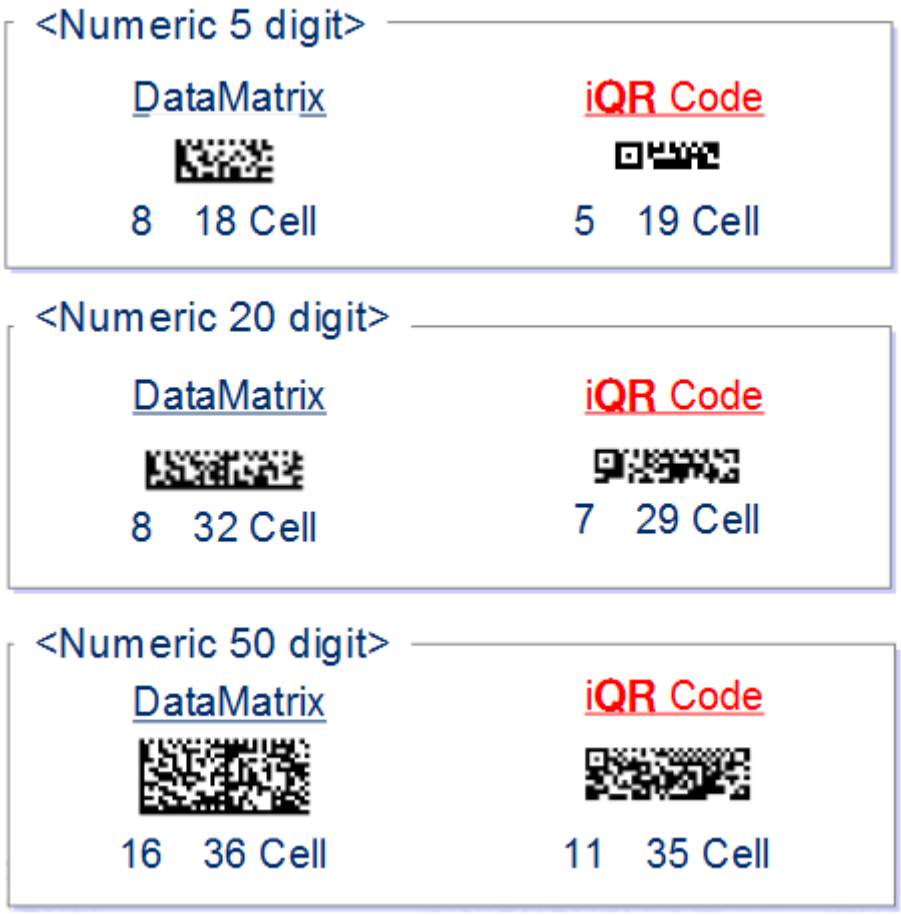

Abbildung 2-18 iQR und DataMatrix **(GS1 Japan, 2009)**

Denso Wave plant (Stand: März 2013) diesen Standard wie auch den ursprünglichen QR-Code frei nutzbar zu machen.

2.2.4 Sonderformen von QR-Codes

In diesem Unterkapitel werden einige Sonderformen von QR-Codes beschrieben, die keine technischen Neuerungen gegenüber herkömmlichen QR-Codes bieten.

2.2.4.1 Custom-QR-Codes

Custom-QR-Codes sind zwar keine offizielle Weiterentwicklung von Denso Wave, sondern nutzen die Fehlerkorrektur von QR-Codes aus, um zum Beispiel Firmenlogos in einen QR-Code zu integrieren. Dies findet auch für spezielle Visitenkarten Anwendung, um den ansonsten optisch eher schlicht aussehenden QR-Codes eine das Auge ansprechende Note zu verleihen. Ein grafisches Beispiel für so eine spezielle QR-Code Visitenkarte ist in Abbildung 2-11 **QR-Code Visitenkarte** gezeigt.

Eine weitere Möglichkeit, QR-Codes einen Wiedererkennungswert zu geben, ist durch ein mathematisches Verfahren möglich, wie ein Projekt namens QArt zeigt: (QArt Codes, 2012) Hier wird der QR-Code mittels spezieller XOR-Masken entsprechend modifiziert. Anschließend muss der QR-Code in einen verständlichen Teil in einen unverständlichen Teil aufgeteilt werden. Somit ergibt sich im Falle einer enkodierten URI ein 8-bit Teil, der lesbar

ist und auch keine optische Veränderung birgt, und einen numerischen Teil, der keine notwendigen Daten besitzt. Im numerischen Teil wird der optisch veränderte Code untergebracht, der dann als zusätzlicher Ankerlink der URI angefügt wird. Da Ankerlinks nicht zwingend gültig sein müssen, ergibt sich für den relevanten Teil der URI kein Problem. Auf obiger Quelle entnommener Abbildung 2-19 ist der nicht veränderbare Teil grau hinterlegt:

Abbildung 2-19 QArt QR-Code **(QArt Codes, 2012)**

Um das Problem des festgelegten veränderbaren Teils zu umgehen, kann man den grau hinterlegten Bereich des QR-Codes auch rotieren, um eventuell horizontal ausgerichtete Grafiken anzeigen zu lassen. Mittels Fehlerkorrektur lassen sich auch die gewöhnlich unveränderbaren Teile verschieben, um einen geeigneten Bildausschnitt im QR-Code möglich zu machen, wie Abbildung 2-20 zeigt:

Abbildung 2-20 QArt QR-Code mit Fehlerkorrektur **(QArt Codes, 2012)**

2.2.4.2 3D-Codes

Ein Händler in Seoul, Emart, ließ aus einem QR-Code eine dreidimensionale Skulptur erschaffen, die durch die Sonneneinstrahlung zu einer bestimmten Uhrzeit mittels geworfener Schatten zu einem dekodierbaren QR-Code wird. Diese Variante entwickelte sich zu einem besonderen Marketingschachzug, da der Händler im dekodierbaren Zeitraum einen Verkaufszuwachs von 25 Prozent verzeichnen konnte. Die speziellen Skulpturen wurden im Großraum Seoul aufgestellt und waren durch die Sonneneinstrahlung nur zwischen 12:00 und 13:00 Uhr dekodierbar (springwise, 2012).

Abbildung 2-21 zeigt die zuvor beschriebene Skulptur:

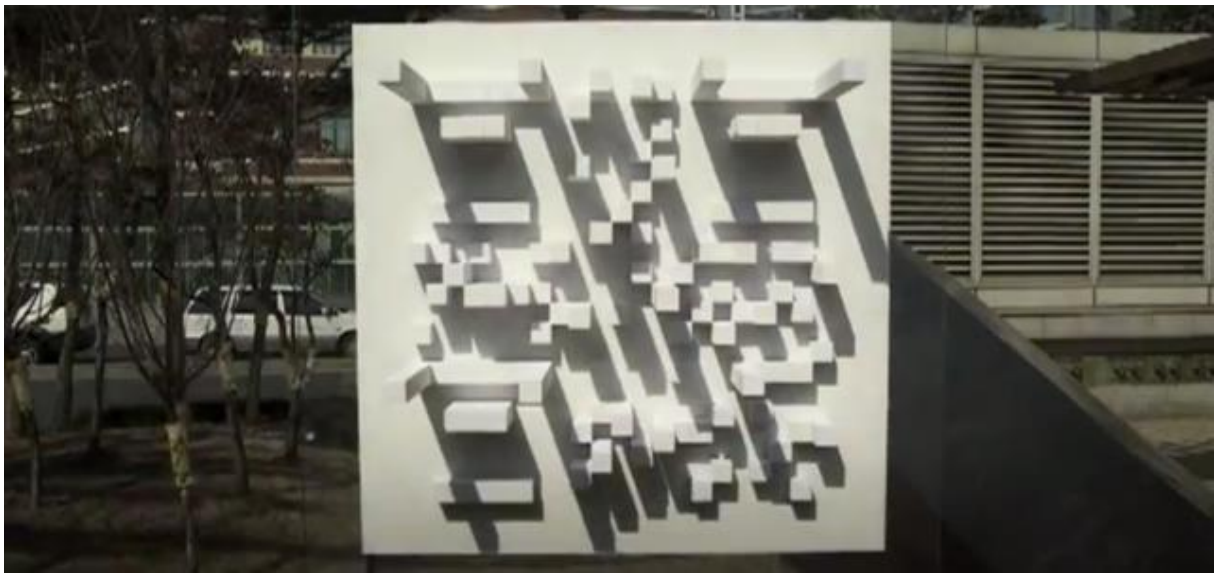

Abbildung 2-21 3D Skulptur QR-Code **(springwise, 2012)**

2.3 Strichcodes und NFC

NFC kann sehr wohl als Konkurrenz zu Barcodes und dessen verwandte Arten wie DataMatrix und QR-Code gesehen werden. Es existieren viele potentielle Einsatzzwecke, wo NFC in Zukunft oft als die plausiblere Methode angesehen werden kann. Auf NFC basierende Systeme (NFC-Tags) sind von den äußeren Bedingungen relativ unabhängig, da keine optische Erkennung stattfindet, sondern nur eine gemäß Spezifikation ausreichende Nähe vom auslesenden Gerät und dem auszulesenden NFC-Tag vorhanden sein muss. Optische Erkennungsverfahren hängen generell von den Lichtbedingungen, sowie Umwelteinflüssen ab. Ein verdreckter QR-Code kann trotz der sehr guten Fehlerkorrektur (siehe Kapitel 2.2.1) oft nicht mehr gelesen werden und ist somit zerstört. In diesem Fall muss ein neuer QR-Code gedruckt und an der notwendigen Stelle angebracht werden.

Das Auslesen von NFC-Tags funktioniert wesentlich einfacher und schneller als bei optischen Codes. Für NFC-Tags wird keine andere Interaktion der Benutzerin oder des Benutzers notwendig, als das annähern des Gerätes an den Tag. Bei optischen Codes muss die Kamera Anwendung gestartet und damit der Code gescannt werden, was je nach Codeart und –größe mehrere Sekunden dauern kann.

NFC-Tags sind auch generell robuster und wesentlich flexibler als optische Codes. Sie können im Gegensatz zu optischen Verfahren auch bei schlechtem Licht ausgelesen werden. Zusätzlich sind sie auch einigermaßen verborgen anbringbar, wodurch beim Einsatz auf Smartpostern die Darstellung des anderen Inhaltes nicht gestört wird. Auf Tags, die in Aufklebern angebracht sind, kann man auch zusätzliche Informationen schreiben, die für die Benutzerin oder den Benutzer hilfreich sein könnten. Bringt man an einer Stelle einen generell wiederbeschreibbaren Tag an, könnte jeder mit einem schreibfähigen Gerät und der nötigen Anwendung den Tag verändern. Um sich davor zu schützen, existieren auch Tags, die eine Authentifizierung verlangen und somit einen Schutz vor Manipulation bieten können. Dadurch ist es einfach möglich, einen bereits angebrachten Tag inhaltlich zu verändern, ohne den Tag selbst ersetzen zu müssen (QR Codes versus NFC Tags).

Allerdings birgt die Verwendung einer auf Funktechniken basierender Technologie Sicherheitsrisiken, die bei optischen Verfahren nicht bestehen. Es ist zwar möglich, einen optischen Code zu manipulieren, allerdings ist es nicht möglich, die ausgelesenen Daten beim Auslesevorgang zu verändern, oder den Auslesevorgang zu stören. Einige dieser NFC-Probleme sind in Kapitel 4.5 beschrieben.

Derzeit (Stand April 2013) ist die Verbreitung NFC-fähiger Geräte verhältnismäßig gering, im Gegensatz zu Geräten mit optischer Hardware (Kamera, teilweise mit Beleuchtungsfunktion). Deswegen ist es noch nicht absehbar, ob und wann NFC beispielsweise QR-Codes verdrängen kann.

2.4 Zusammenfassung

In diesem Kapitel wurde die Entwicklung von Barcode und ähnlichen Systemen erläutert, sowie deren Einsatzgebiete gezeigt. Besonderere Aufmerksamkeit galt den QR-Codes, die eine weite Verbreitung genießen. QR-Codes eignen sich in vielen Bereichen und erfreuen sich einer anhaltenden Beliebtheit.

Weiterentwicklungen versuchen teilweise erfolgreich ursprüngliche Mängel zu beheben und neue Einsatzmöglichkeiten zu erschließen.

Besonders in Printmedien findet man oft QR-Codes, da sie eine gute Schnittstelle zwischen dem ausgedruckten Material und der digitalisierten Welt bilden können. Es bleibt jedoch abzuwarten, inwiefern beispielsweise QR-Codes mit den ständig wachsenden Datengrößen schritthalten wollen, da die Druckgröße mit den derzeit bekannten Methoden nicht mehr entscheidend reduziert werden kann.

3 RFID

Dieses Kapitel behandelt die Geschichte von RFID-Systemen, ihre Spezifikation und zeigt einige Einsatzgebiete. Desweiteren werden Vergleiche zu den anderen in dieser Arbeit erläuterten Technologien gezeigt und deren Vor- und Nachteile verglichen.

3.1 Geschichte der Entwicklung

Die Ursprünge von RFID, kurz für Radio Frequency Identification, reichen bis in den Zweiten Weltkrieg zurück. Damals wurden Vorläufer dieser Technologie zur Freund-Feind-Erkennung verwendet. So waren an offensiven Einheiten wie Panzern und Flugzeugen sekundäre Radargeräte installiert, die die jeweiligen Frequenzen identifizieren und somit feststellen konnten, ob es sich um einen Freund oder Feind handelte. Auf dieser Basis entwickelte Harry Stockman im Rahmen seiner Forschungstätigkeit in der Cambridge Field Station der US Army Air Force 1947-1948 das von ihm so bezeichnete *Number Identification System* und publizierte die Ergebnisse in seiner Forschungsarbeit *Communication by Means of Reflected Power* (Stockman, 1948).

In den 1960er Jahren wurden durch die voranschreitende Wirtschaft neue Lösungen in der Logistik und Fertigungstechnik notwendig. Die *„Siemens Car Identification“*, abgekürzt SICARID, diente zur Identifikation von Autoteilen und Eisenbahnwaggons (Siemens, 2013).

In den 1970er Jahren wurden weitere Vorläufer der RFID-Technik im Bereich der Warensicherung eingesetzt. Auf Waren wird ein solcher Sender angebracht, der dann beim Durchschreiten einer elektronischen Schranke Alarm auslösen kann. Desweiteren wurden Nutztiere in der Landwirtschaft mit elektronischen Kennzeichnungen versehen, die die ständige Identifikation möglich macht.

Das Jahr 1973 markiert den eigentlichen Beginn von RFID. Mario Cardullo erhält das Patent für einen RFID-Tag, der beschrieben und gelesen werden konnte (Violino, 2003).

Folgende zuvorgenannter Quelle entnommene Abbildung 3-1 skizziert den Aufbau des patentierten RFID-Systems:

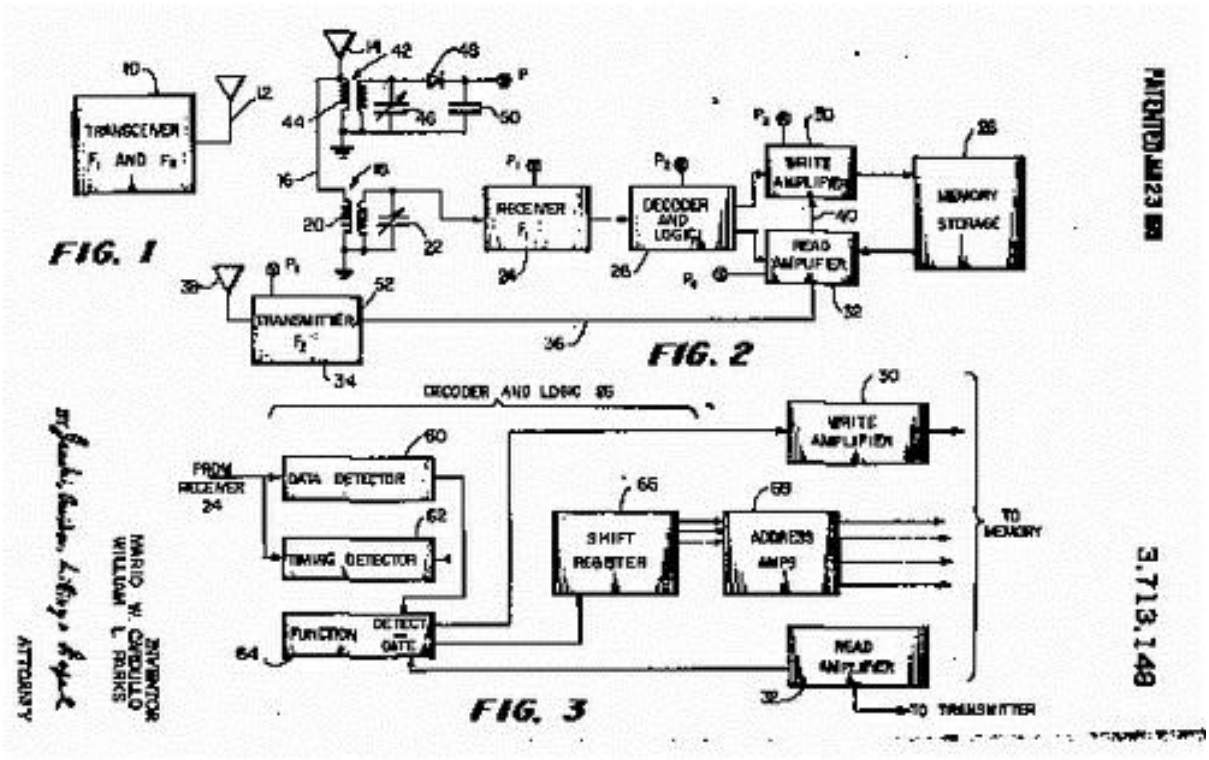

Abbildung 3-1 RFID-Patentskizze **(Violino, 2003)**

3.2 Technische Spezifikation

3.2.1 Aufbau

Ein RFID-Transponder besteht aus einem Tranceiver (Transmitter und Receiver, analoger Schaltkreis), einer Antenne, sowie einem meist permanenten Speicher und einem digitalen Schaltkreis (heute gewöhnlich ein fortgeschrittener Mikrocontroller). Anstelle des permanenten Speichers kann jedoch auch ein mehrfach beschreibbarer Speicher eingesetzt werden. (Siehe Abbildung 3-2)

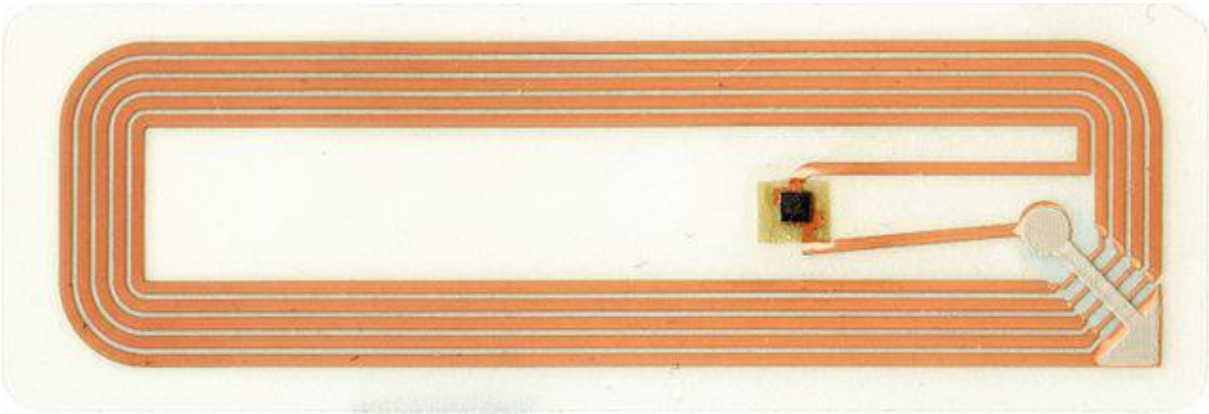

Abbildung 3-2 RFID-Transponder **(Kalinko, 2009)**

3.2.2 Technik

Die technischen Details von RFID-Transpondern unterscheiden sich je nach Einsatzgebiet und Standardisierung.

Die Langwellenfrequenzen liegen im Bereich 125-134kHz, Kurzwelle bei 13.56MHz, UHF *(Ultra High Frequency)* bei 865-869MHz bzw. 950MHz, sowie SHF *(Super High Frequency)* bei 2.45 und 5.8GHz. Dabei ist zu beachten, dass sich die eingesetzten Frequenzen nach Kontinenten unterscheiden. Die Verwaltung der freigegebenen Frequenzen liegt bei der ITU (International Telecommunication Union). Die Signalreichweite hängt von der eingesetzten Frequenz ab und liegt bei Lang- und Kurzwellen bei etwa einem halben Meter, während im UHF-Bereich 3-6 Meter möglich sind. Im SHF-Bereich sind sogar 10 Meter möglich, allerdings mit aktivem anstelle von passivem Transponder.

3.2.2.1 Passive Transponder

Bei passiven Transpondern wird die Empfangsantenne als Energielieferant genutzt. Diese ist dafür in einer Spule angeordnet, wodurch das vom Lesegerät gesendete Signal mittels Induktion in Energie umgewandelt wird. Dies reduziert die Kosten in der Herstellung deutlich und ermöglicht sehr kleine Bauweisen und damit deutlich mehr Einsatzgebiete. Allerdings ist die durch die Energieumwandlung enstehende Verzögerung nicht außer Acht zu lassen und in den technischen Umsetzungen bzw. einzelnen Anwendungsfällen entsprechend zu berücksichtigen. Die Übertragungsreichweite hält sich durch die geringe Sendeleistung ebenfalls in Grenzen.

3.2.2.2 Aktive Transponder

Aktive Transponder besitzen eine eigene Energiequelle und können daher Signale schneller und vor allem stärker senden, wodurch sich eine höhere Reichweite und weniger Verzögerung ergibt. Der Nachteil ist, dass solche Geräte, je nach Einsatzzweck und Konzept, sehr groß und teuer werden können.

3.2.2.3 Semi-passive Transponder

Semi-passive, oder auch semi-aktive Transponder verwenden das physikalische Prinzip der modulierten Rückstreuung (Dobkin, 2007).

Dadurch ist keine eigene Stromversorgung notwendig, wodurch geringere Formgrößen ermöglicht werden als bei aktiven Transpondern, während die Reichweite im Vergleich zu passiven Transpondern deutlich größer ist. Allerdings ist das System auch anfälliger auf Überlagerungen.

3.3 Einsatzgebiete

In diesem Unterkapitel werden einige Einsatzgebiete von RFID erläutert, sowie einige Vergleiche und Zusammenhänge zu auf Barcodes basierenden Techniken erläutert.

3.3.1 Logistik

In der Warenwirtschaft spielt RFID eine bedeutende Rolle (DHL, 2011). Inventuren können in der Lagerlogistik auf Knopfdruck durchgeführt werden. Der große Vorteil gegenüber optischen Erkennungsverfahren über Barcodes liegt darin, dass die Waren ohne „Sichtkontakt“ zum Lesegerät ausgelesen werden können. Es genügt dabei, wenn die Ware in der nötigen Sendereichweite ist, die je nach verwendeter Infrastruktur variieren kann.

Produkte können mittels RFID-Tag überwacht werden. Dabei kann es sich sowohl um die Überwachung zerbrechlicher oder empfindlicher Inhalte handeln, als auch um Produkte, die gekühlt werden müssen. Sollten Produkte ihr Mindesthaltbarkeitsdatum überschreiten oder außerhalb ihrer zulässigen Umgebungsspezifikationen gelagert oder transportiert werden, können die Produkte über ihren RFID-Tag aussortiert werden, bevor sie in der Lieferkette vorwärts gelangen.

Pakete können ihren Weg durch eine Logistikkette „selbst“ steuern, indem sie gemäß der Daten auf dem RFID-Tag verarbeiten lassen.

Allerdings scheitert die weltweite, vollständige Umsetzung derzeit noch an fehlenden, international einheitlichen Standards. Wie in Kapitel 3.2 erwähnt wurde, existieren verschiedene Spezifikationen und Standardisierungen pro Kontinent, sodass im globalen Geschäftsfall keine einheitlichen Systeme verwendet werden können. Dies macht einen großen Vorteil der Technologie zunichte.

3.3.2 Fahrzeugidentifikation

In der Fahrzeugidentifikation kommt bislang zumeist ein Zusatzgerät zum Einsatz, das beispielsweise bei der automatischen Mautkontrolle eingesetzt wird. Derartige *Electronic Road Pricing* Systeme finden mittlerweile (Stand Februar 2013) in einigen Ländern der Welt Einsatz.

In London setzt man bei der Innenstadtmaut gar auf sogenannte e-Plates, wo die RFID-Technologie in das Kfz-Kennzeichen integriert wird. Dadurch wird die durch Umwelteinflüsse beeinträchtigte Kameraerfassung ergänzt (e-Plate, 2013).

Die Technologie kann daher auch auf andere Bereiche ausgedehnt werden, beispielsweise auf Section Control Systeme, aber auch zur automatischen Bezahlung bei Tankstellen. In den USA existiert bereits solch ein automatisches Bezahlsystem bei Tankstellen. Es wurde 1997 von der Mobil Oil Corporation eingeführt und nennt sich *Speedpass* (Speedpass, 2013).

3.3.3 Personenidentifikation

Ein eher umstrittenes, wenngleich manchmal durchaus sinnvolles Einsatzgebiet ist beim Menschen. Sinnvoll eingesetzt, beispielsweise in Patientenarmbändern in Krankenhäusern, können so auf einfache Weise die nötigen Informationen vernetzt werden (heise online, 2006).

Allerdings birgt die Technologie dadurch auch einige Gefahren. Marketingfirmen können RFID-Chips einzelnen Personen aushändigen und durch Positionsfeststellung die einzelnen Wege aufzeichnen und ein Verhaltensmuster ableiten.

Bereits im Jahr 2004 wurden implantierbare RFID-Chips in den USA zugelassen wie Heise (heise online, 2004) bereichtet. Dies wird von Datenschützern sehr kontrovers gesehen, da eine Person mit einem solchen Implantat dem Datenmissbrauch möglicherweise schutzlos ausgeliefert ist und weil sich die Datenübertragung nicht steuern bzw. verhindern lässt. Ein Angreifer braucht sich also nur auf die notwendige Entfernung nähern und hat mit einem entsprechend präparierten Lesegerät Zugriff auf möglicherweise vertrauliche Daten.

In neuen biometrischen Reisepässen ist RFID erstmals seit 1998 in Malaysia im Einsatz. In diesen Reisepässen wurden neben personenbezogenen Daten auch Ein- und Ausreisedaten gespeichert.

Mittlerweile (Stand 2013) haben aber auch EU-Staaten, darunter auch Österreich, sowie nicht-EU-Staaten wie die Schweiz, RFID-Technologie in Reisepässe eingearbeitet. Auf dem Chip werden sowohl personenbezogene, als auch biometrische Daten gespeichert (ARGE DATEN, 2005).

3.3.4 Bezahlsysteme

Ein weiteres Einsatzgebiet von RFID-Technologien findet sich bei Bezahlsystemen wie Kreditkarten. Das Einführen von Chipkarten mit Magnetstreifen in ein Kartenlesegerät entfällt und die notwendigen Daten werden über ein entsprechendes Lesegerät erfasst. Allerdings entfällt die Bestätigung der Übertragung durch den Zahlenden, wodurch hier durch entsprechend präparierte Lesegeräte mehrfache Abbuchungen vorgenommen, beziehungsweise generell Abbuchungen ohne Wissen des Kartenbesitzers durchgeführt werden können.

Dieser Problematik entgegnet man mit niedrig angesetzten Maximalbeträgen. Beispielsweise hat Mastercard mit ihrem *Paypass* so ein System im Umlauf. In der Eurozone ist das Limit bei 25 Euro. Für höhere Beträge ist weiterhin die Eingabe eines PIN notwendig (Mastercard, 2013).

Dies ist die Vorstufe zu einem über NFC abgewickelten Bezahlsystem, da man durch die Chiptechnologie nicht mehr auf das herkömmliche Kartenformat mit Magnetstreifen angewiesen ist und der RFID-Chip auch in anderen Gegenständen mit unterschiedlichen Formen installiert werden kann. Zum Beispiel in Uhren, oder als Sticker am Portemonnaie, Schlüssel und sonstigen Gegenständen, die man ständig dabei hat.

3.3.5 Textilindustrie

RFID-Tags dienen in der Textilindustrie nicht nur der Warensicherung, sondern auch in der zugehörigen Logistik. Somit werden zwei voneinander unabhängige Funktionsweisen in einem System vereint. Die zusätzlich entstehenden Kosten durch die RFID-Chips auf Kleidungsstücken halten sich ob der verhältnismäßig großen Gewinnspannen in Grenzen,

zumal auch durch die Verwendung von RFID-Tags in der Warenwirtschaft Kosten eingespart werden können.

So setzt die Firma *Gerry Weber* RFID-Tags in ihren Textilien ein (Rhea Wessel, 2009).

Laut zuvorgenannter Quelle sind deren AD-827 RFID inlays temperaturbeständig und können bei bis zu 60° Celsius gewaschen werden, ohne beschädigt zu werden. Wäschetrockner stellen ebenfalls keine Bedrohung dar. Insgesamt hält der RFID-Tag bis zu 3 Waschvorgänge aus, wodurch er den Geschäftszyklus bis zum Kunden überstehen sollte.

3.3.6 Landwirtschaft

In der Landwirtschaft kommen RFID-Tags bei Nutztieren zur Verwendung. Dadurch ist es einfach möglich, die Tiere zu überwachen, sowie deren Wege im Geschäftsfall nachvollziehen zu können. Dies geschieht zusätzlich zur herkömmlichen Markierung mit Halsbändern und Ohrmarken. Die Verwendung von RFID-Tags bei Nutztieren geht bereits in die 1970er Jahre zurück und stellt somit einen der längsten Einsatzzwecke der Technologie dar. Die RFID-Tags können dabei sowohl in die bisherige Markierung eingearbeitet werden, als auch im Nutztier implantiert werden.

Abbildung 3-3 RFID-Tag (mit zusätzlich optischem Code) bei einem Rind **(Bob Brewin, 2005)**

3.3.7 Zugangskontrollsysteme

RFID-Transponder werden auch bei elektronischen Schlüsseln verwendet. Beispielsweise wird bei Autoschlüsseln in letzter Zeit vermehrt auf Schlüssel gesetzt, die sich lediglich im Auto befinden müssen, um das Auto zu starten. Auf Zündschlösser mit Steckschlüssel wird hierbei verzichtet. Hierfür wird ein um ein Crypto-Modul erweiterter Transponder eingesetzt werden, der gegen Manipulationen geschützt ist.

Desweiteren kann man mit RFID-Schlüsselkarten Zugänge zu abgesicherten Räumen regeln. Dies kommt häufig zur Anwendung, wenn auf biometrische Zugangserkennungen verzichtet werden muss.

In den meisten Schigebieten werden in den Liftkarten RFID-Chips eingearbeitet, um so den Zugang zu den Schiliften zu kontrollieren, ohne wie früher die Liftkarte in einen dafür vorgesehenen Schlitz stecken zu müssen. Diese mit einem RFID-Chip versehenen Liftkarten können aber auch zusätzlich zur Positionsbestimmung verwendet werden und so eine Integration mit sozialen Netzwerken schaffen. Ein derartiges System mit Integration sozialer Netze wird beispielsweise im Schigebiet Vail/USA eingesetzt (Kinsella, 2010).

Bei der Fußball-Weltmeisterschaft 2006 in Deutschland wurden RFID-Chips auf den Stadiontickets verwendet. Ziel war, den Schwarzhandel einzudämmen. Mittlerweile haben einige Vereine die Technologie bei Spielen der deutschen Bundesliga im Einsatz (Schmidt, 2009).

3.3.8 Bibliotheken

Auch Buchumschläge können mit RFID-Technologie ausgestattet werden. Dabei wird der RFID-Tag sowohl für die interne Logistik, als auch für den Kundennutzen verwendet. Durch die automatische Identifikation des entlehnten Werkes kann ohne zusätzliches Personal eine Übersicht der im Umlauf befindlichen Bücher erstellt werden. In Kombination mit Kundenkarten kann auch eine auch für den Kunden einsehbare Datenbank erstellt werden. Ein derartiges System wird beispielsweise an der TU Graz Hauptibliothek - seit 2005, als erste österreichische Universitätsbibliothek - eingesetzt. RFID-Chips in Büchern dienen hierbei auch zur Buchsicherung. In die Studentenausweise im Scheckkartenformat ist ebenso ein RFID-Chip eingearbeitet (TU Graz, 2012).

3.4 Probleme und Bedenken

Durch die fehlende international einheitliche Standardisierung, sowie oft nur schwache oder weggelassene Verschlüsselung von Daten, können RFID-Tags ohne Gegenwehr und Wissen des Trägers ausgelesen werden. Dies kann auf mehrere Arten zu großen Problemen führen. Einerseits können mit einem unerwünschten Zugriff sensible Daten ausgelesen werden, andererseits kann mittels mehrere Positionsbestimmungen ein Bewegungsprofil des Trägers angelegt werden. Gegen unerwünschte RFID-Chips kann oft nur bedingt vorgegangen werden. Eine Isolation, beispielsweise durch einen Faraday'schen Käfig, ist oft mit einem Aufwand verbunden und nicht auf jedes RFID-Einsatzgebiet anwendbar. Meistens bleibt nur die Zerstörung des RFID-Chips als letzte Konsequenz übrig, wodurch aber auch meistens das Trägermaterial in Mitleidenschaft gezogen wird. So könnte man den RFID-Chip im Reisepass nicht einfach nur in die Mikrowelle legen. Durch die elektromagnetische Feldstärke wird zwar der RFID-Chip zerstört, aber durch die entstehende Hitze auch das umgebende Material beschädigt. Sicherer wäre die Anwendung eines Elektroschockers oder eines Gerätes, das einen elektromagnetischen Impuls aussendet, der den RFID-Chip deaktiviert.

Zur sinnvollen Positionsbestimmung sind RFID-Chips allerdings wegen der verhältnismäßig geringen Sendeleistung unbrauchbar. Hierfür wird gewöhnlich auf andere Positionsbestimmungssysteme wie GPS gesetzt, da im Gegensatz zu RFID auch Daten über Bewegungsgeschwindigkeit, Richtung und Ort geliefert werden. Der Aufwand für eine genaue Positionsbestimmung durch RFID ist durch die geringe Sendeleistung von nur wenigen Metern bei passiven Transpondern zu groß. Man müsste in diesem Anwendungsszenario in geringen Abständen von etwa 10 Metern RFID-Lesestationen

installieren. Damit ließe sich dann allerdings eine sehr präzise Infrastruktur für Navigations- und Verkehrsleitsysteme umsetzen. Dies scheitert aber unter anderem an der schon erwähnten international einheitlichen Standardisierung. Die Kosten für so ein System wären ob der mangelnden Portierbarkeit groß.

Beim Einsatz von RFID auf Konsumgütern besteht ein großes Problem beim Recycling. Da die Technologie oft bei ansonsten nichtmetallischen Gütern eingesetzt wird, gehen bei Müllverbrennungen oder Deponien viele Edelmetalle verloren. Bei einem weitreichendem Einsatz von RFID, kann die Entsorgung durch die teilweise giftigen Metalle wie Blei problematisch werden. Der erhöhte Ressourcenverbrauch bei Edelmetallen dürfte sich irgendwann auch beim Preis bemerkbar machen.

Beim Einsatz von RFID im medizinischen Bereich zur Patientenidentifikation können RFID-Signale eventuell störend auf diagnostische Geräte wirken, wie eine im Jahr 2008 durchgeführte Studie zeigt (van der Togt, van Lieshout, Hensbroek, Beinat, Binnekade, & Bakker, 2008).

So sollen bei den Diagnosegeräten durch die elektromagnetischen Felder abweichende Ergebnisse aufgetreten sein, was in manchen Fällen zu schwerwiegenden Konsequenzen führen könnte, zumal davon auch kritische Geräte wie beispielsweise Beatmungsgeräte betroffen sind. Die relative Häufigkeit von Störungen ist in der Studie mit 27.6% gegeben. Teilweise wurden die Störungen als schwerwiegend klassifiziert, da es unter anderem zu Ausfällen bei Beatmungsgeräten und Infusionspumpen kam. Derartige Störungen sind wiederum auf die fehlende einheitliche Standardisierung von RFID zurückzuführen.

3.5 Zusammenfassung

In diesem Kapitel wurde die Spezifikation von RFID erläutert und einige Einsatzgebiete gezeigt. Es wird ersichtlich, dass die im folgenden Kapitel beschriebene NFC-Technologie eng mit RFID verwandt ist und darauf aufbaut.

RFID bietet eine große Zahl an möglichen Einsatzgebieten, ist jedoch in einigen davon als bedenklich einzustufen. Dies ist darauf zurückzuführen, dass die Reichweite von RFID-Tags verhältnismäßig groß ist und die durch die Auslesevorgänge erhaltenen Daten eventuell Rückschlüsse auf ein Bewegungsmuster einer Person ermöglichen.

Durch den weitreichenden Einsatz von RFID-Tags dürfte sich das Resourcenproblem weiter verschärfen, da diese Tags oft nicht recycled werden können. Derzeit (Stand April 2013) sind die Tags noch verhältnismäßig günstig, doch in Anbetracht einer Ausweitung der Einsatzgebiete könnte sich die Verfügbarkeit der zur Herstellung notwendigen Ressourcen drastisch reduzieren, was einen signifikanten Preisanstieg zur Folge hätte.

Dennoch bietet RFID im Moment eine sehr kostengünstige Anwendung zur Identifikation in vielen Bereichen und wird deshalb wohl noch sehr lange eingesetzt werden.

4 NFC

In diesem Kapitel wird die geschichtliche Entwicklung von NFC erklärt. Es werden Beispiele für Einsatzgebiete der Technologie gezeigt, sowie Vergleiche zu anderen Technologien geboten.

4.1 Geschichtliche Entwicklung von NFC

Die Entwicklung von NFC *(Near Field Communication)* gründet auf der Entwicklung von RFID. Jedoch erst im Jahre 2004 wurde das NFC-Forum von den Firmen Nokia, NXP Semiconductors (Philips) und Sony gegründet (NFC Forum, 2013).

Das NFC-Forum hat sich als Ziel gesetzt, NFC Standards auszuarbeiten, die die Spezifikationen und Handhabung NFC-fähiger Geräte definieren. Dies ist notwendig, um international einheitliche Richtlinien für die Verwendung der NFC-Technologie zu erhalten. Ebenso sollen Anwender für die neue Technologie begeistert werden, indem mit international einheitlichen Anwendungsfällen die Vorteile der neuen Technik bewiesen werden können und dadurch herkömmliche Methoden abgelöst werden können.

Bereits im Juni 2006 konnte eine offizielle Architektur der NFC-Technologie präsentiert werden, wodurch es möglich war, noch im selben Jahr ein mobiles Gerät auf den Markt zu bringen, das diesen neuen Standard umsetzt. Dieses erste NFC-fähige Smartphone war laut der obigen Quelle (NFC Forum, 2013) ein Nokia 6131.

Im Jänner 2009 veröffentlichte das NFC-Forum Peer-to-Peer-Standards für die direkte Übertragung von bestimmten Informationen von einem Endgerät zu einem anderen (NFC Forum, 2009).

Im Dezember 2010 stellt Google das Samsung Nexus S vor, das erste Android Smartphone mit NFC-Fähigkeit, die gleichzeitig mit der Androidversion 2.3 „Gingerbread“ nutzbar gemacht wurde (Hildenbrand, 2010).

Folgend im Frühjahr 2011 zeigt Google die Funktionalität von NFC zum Teilen von Kontakten, Videos, Apps, URLs und anderen Daten in einem einstündigen Video (Pelly & Hamilton, 2011).

Im August 2011 veröffentlicht Nokia eine neue Version ihres Handybetriebssystems Symbian, das die NFC-Funktionalität integriert (Clark, 2011).

BlackBerry Hersteller RIM (Research in Motion) lässt sich im Jahr 2011 als erster Smartphonehersteller bei MasterCards kontaktlosem Bezahlsystem *PayPass* zertifizieren. Dies betrifft die Geräte BlackBerry 9900 und BlackBerry Curve 9360 (Penfold, 2011).

Im Jänner 2012 kündigte Sony ihre „SmartTags“ an, mit denen nicht nur auf dem gleichzeitig veröffentlichten Smartphone Sony Xperia P Einstellungen verändert werden können. Die SmartTags sind dabei selber programmierbar und können dadurch entsprechend angepasst werden. Dies eröffnet der Technologie ein breites Spektrum an Anwendungsmöglichkeiten (MacManus, 2012).

Im März 2012 starten die britische Restaurantkette EAT und der Telekommunikationsbetreiber Orange eine gemeinsame Aktion für NFC-Smartposter. Bei der Aktion erhalten Besucher mit einem NFC-fähigen Smartphone über die App „Quick Tap Treats“ einen kleinen Leckerbissen gratis (Martin, 2012).

Im Oktober 2012 stellt Samsung *TecTile* vor. Das System besteht aus NFC-Stickern des Typs MIFARE. Diese sind über eine ebenfalls von Samsung zur Verfügung gestellten dazugehörigen Android-App les- und beschreibbar (Samsung, 2012).

4.2 Aktueller Stand der Technik

Basierend auf der Ansammlung von Standards durch das NFC Forum, ist die Übertragung auch durch ISO/IEC 18000-3 auf 13.56MHz geregelt. Dadurch ist NFC zu RFID kompatibel. Dies hat zum Vorteil, dass die bestehende RFID-Infrastruktur nicht geändert werden muss. Die verwendete Frequenz ist international durch den mittlerweile sehr langen Einsatz von RFID schon recht weit verbreitet. Dabei kann wie bei RFID ein passiver NFC-Chip verwendet werden, der vom aktiven Gerät mit Strom versorgt wird. Die verwendete Technik ist hierbei mit RFID ident. Mehr Informationen zur Spezifikation von RFID sind dem Kapitel 3.2.2 zu entnehmen.

Ähnlich wie bei RFID gibt es folgende Betriebsmodi (Ortiz, 2008):

- Aktiver Modus: Beide Geräte sind selbst sendeaktiv, besitzen eine eigene Stromversorgung.
- Passiver Modus: Nur ein Gerät sendet aktiv Signale aus und betreibt dadurch das passive Gerät. Wie bei RFID wird der Strom durch Induktion über die Antenne erzeugt. Das passive Gerät agiert hier als Transponder und hat keine eigene Energieversorgung.

Die unterstützten Übertragungsmodi von NFC sind:

- Peer to peer Modus: Dieser Modus verwendet das Logical Link Control Protocol (LLCP) und verbindet auf dessen Basis zwei NFC Geräte für beidseitige Kommunikation.
- Read/Write Modus: Dieser Modus verwendet RTD (Record Type Definition) und NDEF (NFC Data Exchange Format) zur Übertragung. Dieser Paketstandard wurde vom NFC Forum definiert. Dieser Modus ist nicht sicher.
- NFC Card Emulation Modus: Das NFC-Gerät wird praktisch zur Smartcard. Dieser Modus ist sicher.

Abbildung 4-1 illustriert die verwendeten Protokolle und ihre Ebenen:

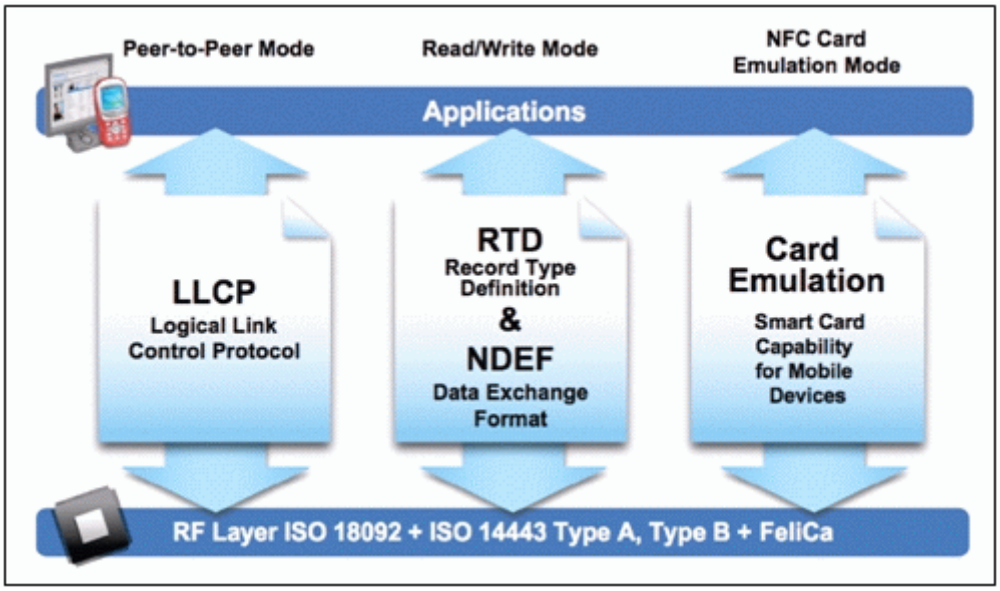

Abbildung 4-1 NFC Übertragungsmodi **(Ortiz, 2008)**

Die Reichweite ist dabei jedoch auf maximal 10cm beschränkt. Üblicherweise übersteigt die Reichweite aber selten 4cm. Dies ist ein Unterschied zu gewöhnlichen RFID-Verfahren, deren Reichweite typischerweise im Meterbereich liegt. Dies hat jedoch auch Vorteile, zumal unerwünschtes Mitlauschen technisch unmöglich gemacht wird.

Die NFC-Chips, auch oft als Tags bezeichnet, halten eine unterschiedliche Anzahl von Bytes an Daten. Die Übertragungsgeschwindigkeiten sind laut Standard mit 106kbit/s, 212kbit/s und 424kbit/s festgesetzt. Dadurch wäre bei einem 4KBytes Chip die größtmögliche Datenmenge in weniger als 0.1 Sekunden übertragen. Da im Vergleich zu anderen Übertragungsarten der Verbindungsaufbau sehr kurz ist, ist der Übertragungsvorgang in sehr kurzer Zeit abgeschlossen.

Gemäß der Spezifikation des NFC Forums (NFC Forum, 2013) existieren vier Tag Typen:

- NFC Forum Type 1 Tag (ISO/IEC 14443A Standard): Wiederbeschreibbare und lesbare Tags zwischen 96 Bytes und 2 KBytes Kapazität. Authentifizierungsfeature nicht vorhanden. Beispielsweise zu finden bei Chips des ursprünglichen Herstellers Innovision Research & Technology PLC (Teil von Broadcom). Installierbarer Schreibschutz kann nicht mehr entfernt werden.
- NFC Forum Type 2 Tag (ISO/IEC 14443A Standard): Wiederbeschreibare und lesbare Tags zwischen 48 Bytes und 2KBytes Kapazität. Manche Chips unterstützen Authentifizierung, wodurch ein Beschreiben nur von autorisierten Geräten bzw. Programmen zulässig ist. Ein Beispiel dafür wäre das System MIFARE Ultralight C.
- NFC Forum Type 3 Tag (JIS X6319-4 Standard): Hauptsächlich in Fernost in Verwendung und basiert auf dem Sony FeliCa System. Authentifizierung und Schreibschutz werden unterstützt. Speichergrößen können gemäß Spezifikation bis zu 1MByte betragen.
- NFC Forum Type 4 Tag (ISO/IEC 14443 Standard): Tags werden bei der Herstellung auf Wiederbeschreibbarkeit konfiguriert. Unterstützt werden Authentifizierung, Verschlüsselung und Schreibschutz. Die Speichergröße beträgt bis zu 32KByte. Diese Tags sind dadurch aber verhältnismäßig größer und mehr schon als Mikrokontroller zu verstehen. Ein Beispiel für solche Chips ist der MIFARE DESFire.

Desweiteren existieren noch jedoch nicht vom NFC-Forum standardisierte, dennoch NFC Data Exchange Format (NDEF) (siehe (NFC Forum, 2006)) unterstützende Tags, die von einigen Geräten unterstützt werden und deshalb in einigen Gebieten weit verbreitet sind, wie folgende Beispiele:

- MIFARE Classic (auf ISO/IEC 14443 basierend): Unterstützt Zugriffskontrolle und Schreibschutz und bietet 1KByte oder 4KByte Speicherkapazität (NXP Semiconductors).
- ICODE SLIX-S (auf ISO/IEC 15693 basierend): Unterstützt Authentifizierung und Schreibschutz, sowie eine gemäß ISO Standard eine höhere Reichweite von etwa 1 Meter (waazaa).

Folgend wird jedoch die vom NFC-Forum standardisierte Spezifikation beschrieben, da die Übertragungsgeschwindigkeiten und Arten der nicht standardisierten Varianten abweichen können.

Gewöhnlich wird Manchester Code mit 10 prozentiger Modulation und mit Amplitudenumtastung abgewickelt. Die einzige Ausnahme ist bei aktiven Geräten mit 106kbit/s Übertragungsgeschwindigkeit. In diesem Fall wird die Digitale Frequenzmodulation mit 100 prozentiger Modulation und ebenfalls Amplitudenumtastung verwendet, wie Tabelle 3 zeigt:

DATA RATE KBPS	ACTIVE DEVICE	PASSIVE DEVICE
106	Modified Miller, 100%, ASK	Manchester, 10%, ASK
212	Manchester, 10%, ASK	Manchester, 10%, ASK
424	Manchester, 10%, ASK	Manchester, 10%, ASK

Tabelle 3 NFC Modulationsmodi **(NFC Modulation & RF Signal)**

Bei Manchester Code wird ein Übergang von „unten nach oben“ als 0 Bit und ein Übergang von „oben nach unten“ als 1 Bit ausgedrückt. Dabei müssen die Übergänge in der Mitte einer Bit-Periode liegen. Die Übertragung nach Manchester Code ist in folgender, ebenfalls letztgenannter Quelle entnommenen Abbildung 4-2 illustriert:

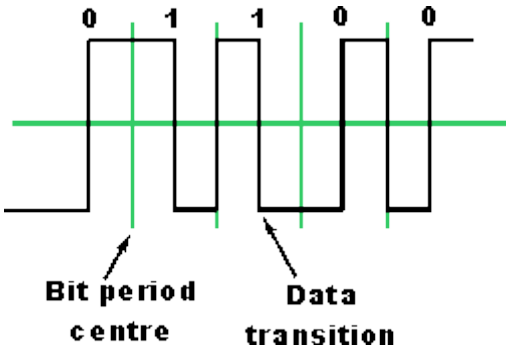

Abbildung 4-2 NFC Manchester Code **(NFC Modulation & RF Signal)**

Demgegenüber verwendet die Digitale Frequenzmodulation einen „dynamischeren“ Weg. Abhängig vom letzten Bitstatus ergibt sich der neue Bitstatus aus der Signalpause in einer Bit-Periode. Die Pause muss nicht zwangsläufig in der Mitte einer Bit-Periode sein. Durch die

Reihenfolge ergibt sich eine unterschiedliche 0 Bit Enkodierung zu Manchester Code. Die 1 Bits werden immer gleich als solche interpretiert. Folgende, ebenfalls obiger Quelle entnommene Abbildung 4-3 zeigt dieses Verhalten und die entsprechende Reihenfolge:

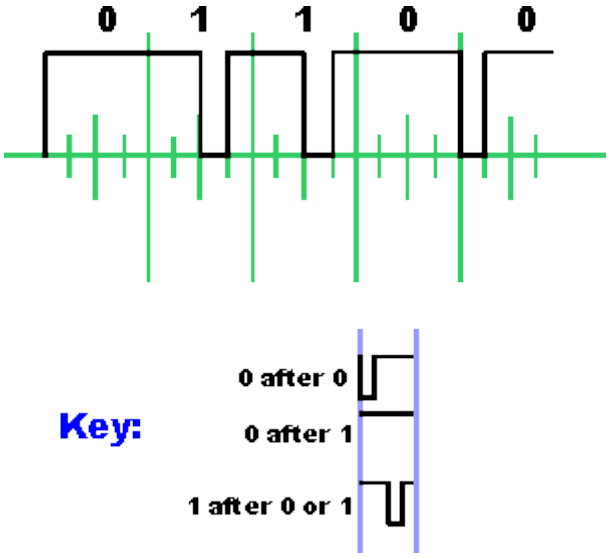

Abbildung 4-3 NFC Digitale Frequenzmodulation **(NFC Modulation & RF Signal)**

4.3 Einsatzgebiete

In diesem Unterkapitel werden einige aktuelle Einsatzgebiete von NFC gezeigt. Einige davon werden sich mit Einsatzgebieten der in anderen Kapitel beschriebenen Technologien decken, sodass ein direkter Vergleich zu RFID und auf Strichcodes basierenden Technologien gezogen werden kann.

4.3.1 Bezahlsysteme

NFC fähige Geräte können als elektronische Geldbörse dienen. Durch die laut Spezifikation sehr kurze Reichweite, gilt die Technologie als sicher vor abhörenden Angriffen. Man-in-the-middle Attacken sind dadurch sehr schwierig, ebenso wie das Mitlesen aus der Entfernung, sowie die Manipulation der übertragenen Daten. Ähnlich wie bei RFID-Bezahlsystemen hat der bezahlende Kunde jedoch keine direkte Kontrolle über mehrfache Abbuchungen bei entsprechend präparierten NFC-Stationen.

Der große Vorteil von NFC gestützten mobilen Bezahlsystemen gegenüber herkömmlichen mobilen Bezahlsystemen liegt in der Unabhängigkeit von der SIM-Karte. Ansonsten wird der Benutzer über die Simkarte beim Provider gemeldet, sowie der Bezahlvorgang selbst über einen Bankbetreiber abgewickelt. Ein Anbieter eines solchen Bezahlsystems muss daher die beiden Schnittstellen vereinen und die Bedürfnisse der beiden Dienstleister Rücksicht nehmen. Der Bankbetreiber stellt gewöhnlich hohe Sicherheitsanforderungen beim verwendeten Bezahlvorgang und der Handynetzbetreiber verlangt entsprechende Flexibilität beim Austausch von SIM-Karten. Diese Kombination kann ein solches System relativ schnell unwirtschaftlich machen. Da jedoch der NFC-Chip fest im Gerät verbaut ist und völlig

unabhängig von der SIM-Karte und dem Netzbetreiber ist, entfällt diese Schnittstelle. Für den Benutzer ergibt sich dadurch ein weiterer Komfort, da eventuelle Zusatzkosten durch SMS an Mehrwertnummern entfallen.

Allerdings gilt auch wie bei Kreditkarten: Verliert man das Smartphone, ist praktisch auch die Kreditkarte weg. Der Gesamtschaden durch den Gerätverlust und die Sperre aller Funktionen beim Betreiber ist dabei nicht außer Acht zu lassen.

4.3.1.1 PayPass, mpass

Etablierte Anbieter wie MasterCard mit ihrem *PayPass* sind oftmals Partner bei solchen Dienstleistern. In Deutschland setzen beispielsweise O2, Vodafone und die Deutsche Telekom auf diese Plattform.

In dieser Kooperation entstand das Bezahlsystem *mpass*. Dieses System ist mittlerweile schon sehr weit verbreitet und wird an sehr vielen Zahlungsstellen akzeptiert. Als Finanzdienstleister wird Bankenlizenzinhaber *Wirecard* eingesetzt. Ohne PIN-Eingabe sind in der Eurozone derzeit allerdings keine Transaktionen mit mehr als 25 Euro erlaubt, was den Bezahlkomfort gegenüber herkömmlichen Bezahlsystemen reduziert (Kuch, 2012).

4.3.1.2 Kreditkarten mit NFC

Auch in Kreditkarten werden mittlerweile NFC-Chips verbaut, der als zusätzliche Schnittstelle zu den immer noch weit verbreiteten Magnetstreifen dienen soll. Die Kreditkarte soll dann wie bei NFC-Verfahren üblich nur mehr an den Bezahlterminal gehalten werden. Allerdings handelt es sich hier um ein rein passives Verfahren. Der Benutzer hat hingegen zum NFC-Einsatz in Smartphones keine Möglichkeit, das Auslesen zu verhindern. Dadurch entsteht ein enormes Sicherheitsrisiko für den Kartenbesitzer. Im Gedränge in öffentlichen Verkehrsmitteln, direkt im Kaufhaus oder an generell stark frequentierten Orten, kann ein Besitzer eines NFC-fähigen Gerätes mit einer entsprechenden Anwendung die Kreditkartendaten auslesen und für seine Zwecke verwenden. Lediglich der dreistellige Sicherheitscode wird nicht über die NFC-Schnittstelle bereitgestellt, was den Angreifer aber nicht daran hindern kann, innerhalb der festgelegten Grenzen ohne diesen Sicherheitscode im Internet einzukaufen (Nöl'Sch, 2012).

Auf Smartphones ist der NFC-Chip hingegen nicht kontaktierbar, wenn das Gerät entweder ganz ausgeschaltet ist oder zumindest die Bildschirmsperre aktiv ist, wie das beispielsweise bei den Testgeräten des Autors der Fall ist.

4.3.1.3 Mobile Ticketing

Die Österreichischen Bundesbahnen und Wiener Linien starteten im Jahr 2007 in Kooperation mit der A1 Mobilkom Austria ihr Ticketbezahlsystem per NFC. An jeder Stelle eines herkömmlichen Fahrkartenentwerters wird ein NFC-Touchpoint installiert, wo bequem per NFC kontaktlos bezahlt werden kann. Damit wurde das bisher bekannte mobile Bezahlen per SMS um eine weitere Möglichkeit ergänzt (derStandard, 2007).

Da jedoch damals die Verbreitung NFC-fähiger Geräte zu gering war, war auch der Andrang zu diesem Bezahlsystem sehr gering. Später veröffentlichte Geräte wie das Nexus S, bei dem

der NFC-Chip besonders beworben wurde, waren vorerst mit den bereits vorhandenen Terminals inkompatibel, wie ein Bericht auf Futurezone.at zeigt (Prenner, 2011).

Abbildung 4-4 Fahrscheinentwerter mit NFC-Touchpoint **(Donau Universität Linz, 2012)**

4.3.1.4 Google Wallet

Mit Google Wallet besitzt auch einer der größten Internetdienstleister weltweit eine Plattform für die einheitliche Bereitstellung von Bezahlsystemen. Dabei kooperiert Google mit mehreren etablierten Kreditkartenbetreibern. Notwendig dafür ist ein Google Wallet Account und die Aktivierung des NFC-Smartphones per PIN-Code. Danach kann an allen unterstützten Terminales per Google Wallet App bezahlt werden. Derzeit (Stand April 2013) steht der Dienst allerdings nur in den USA zur Verfügung (Google, 2013).

4.3.2 Zugangskontrollsysteme

Ähnlich wie bei RFID, können NFC-fähige Geräte auch als Schlüssel zur Zugangskontrolle verwendet werden. Beim Einsatz von primitiven NFC-Tags, die sich im Wesentlichen nicht von RFID-Tags unterscheiden, gibt es durch NFC allerdings einige sicherheitsrelevante Probleme. Durch die Verbreitung von aktiven NFC-Geräten wie Smartphones, lassen sich die NFC-Tags auslesen und entsprechend neu beschreiben. So können auf dem NFC-Tag Daten verändert werden und so ein Zugang erlangt werden, der normalerweise nicht gestattet wäre, wie (Intrepidus Group, 2012) berichtet. Wie in der Quelle angegeben, können so Punktekarten für beispielsweise 10 Zugänge relativ einfach zurückgesetzt werden. Deshalb müssen in solchen Fällen nicht wiederbeschreibbare NFC-Tags verwendet werden, wodurch allerdings wieder zusätzliche Kosten für den Betreiber anfallen.

Sofern die sicherheitskritischen Bedingungen eingehalten werden, kann NFC bei Zugangskontrollsystemen eine wichtige Rolle spielen. Das Smartphone kann so zu einer Art „Schweizer Messer“ werden, mit dem man viele Aktionen durchführen kann. Vom

Autoentriegler, Wohnungsschlüssel bis zur Schiliftkarte, der Betreiber kann im Gegensatz zu QR-Code Anwendungen einfacher und sicherer wissen, wer sich an welchem Zugangskontrollpunkt befindet und darauf entsprechend reagieren. Ebenso lässt die Technologie weitaus größere Möglichkeiten in Bezug auf die per NFC übertragenen Daten zu. Bei optischen Codes wie QR-Codes und DataMatrix, ist der Platz für die zu speichernden Daten durch die Formgröße beschränkt. Riesige QR-Codes können laut Spezifikation (siehe Kapitel 2.2.1) zwar mehr Daten halten als aktuelle NFC-Chips, sind aber ihrer Größe wegen nicht mehr überall einsetzbar. Darüber hinaus ist die optische Erfassung solcher riesigen QR-Codes zu langsam und die mögliche Fehlerquote verhältnismäßig hoch, was ein Auslesen theoretisch unmöglich macht.

So könnte NFC, wie in einem Artikel auf folgender Webseite (Sa, Kein Datum) berichtet, beispielsweise auch in einem Hotel eingesetzt werden. Der Besucher kann den Check-In per NFC durchführen und hat dann auch sein Smartphone als Zimmerschlüssel.

Allerdings gilt auch wie bei Schlüsseln: Wenn man das Smartphone verliert, ist auch der Schlüssel weg und im schlimmsten Fall auch in den falschen Händen. Sofern man das Smartphone allerdings gegen unerlaubte Zugriffe schützen kann, stellt das zumindest kein Sicherheitsrisiko dar, wenn der Dieb keine Rückschlüsse auf den Besitzer ziehen kann und im besten Fall das Smartphone nicht benutzen kann. Allerdings werden ähnlich wie beim Verlust einer Kreditkarte sämtliche Sperrfunktionen durch Anrufe beim Provider ausgelöst werden müssen, um einem finanziellen Schaden vorzubeugen.

4.3.3 Logistik

In der Logistik können Bedienstete in Warenwirtschaftssystemen eventuelle Zusatzinformationen in Echtzeit abrufen. Ähnlich wie bei RFID entfallen dadurch die optischen Erkennungsmethoden und beschleunigen den Lesevorgang erheblich. Durch die beschränkte Reichweite ist jedoch ein Einsatz nicht überall möglich. Außendienstmitarbeiter können beispielsweise aktuelle notwendige Daten sowie das Produkt betreffende Hinweise an den Kunden weitergeben.

Desweiteren kann durch eine entsprechende Signatur in NFC-Tags die Echtheit eines Produktes verifiziert werden, wodurch intensiver gegen Produktfälschungen vorgegangen werden kann.

Gegenüber RFID hat man jedoch den Nachteil, dass beispielsweise keine Inventur auf Knopfdruck durchgeführt werden kann, weil die NFC-Tags gemäß Spezifikation (siehe Kapitel 4.2) innerhalb der sehr geringen Reichweite des Lesegerätes sein müssen.

4.3.4 Marketing

Smartposters haben sich im Marketingbereich zu einer beliebten Methode entwickelt, Kunden zu erreichen. Smartposter sind eine Erweiterung zu gewöhnlichen Postern, die ebenso optisch interessant sein müssen. Jedoch steht die NFC-Funktion im Vordergrund. Benutzer können so über ihr NFC-fähiges Smartphone an Gutscheine kommen, oder auch ihr Smartphone in eine Art Kundenkarte verwandeln. Der Sinn dahinter ist analog dem Einsatz von einem QR-Code zu verstehen. Auf dem NFC-Tag steht gewöhnlich eine URI, auf der der Kunde eine bestimmte Aktion durchführen kann. Ein Vorteil gegenüber optischen Erkennungsmethoden

liegt darin, dass der NFC-Tag auch bei schlechtem Licht ausgelesen werden kann. Ein weiterer Vorteil in der detaillierteren Information über die Benutzerin oder den Benutzer. Zusätzlich können auf NFC-Tags beispielsweise auch Android Application Records gespeichert werden, die ein automatisches Herunterladen einer App ermöglichen, über die dann weitere Features nutzbar sind.

Allerdings ist die Verbreitung von NFC-fähigen Smartphones (Stand April 2013) bei weitem zu gering im Vergleich zu Smartphones mit integrierter Kamera zur Abtastung von beispielsweise QR-Codes, sodass NFC derzeit noch keinesfalls als vollständiger Ersatz von QR-Codes im Marketingsegment gewertet werden kann.

Abbildung 4-5 NFC Smartposter Gewinnspiel, Jamiroquai **(Jamiroquai, 2011)**

4.3.5 Informationswesen

Ein weiteres Einsatzgebiet von NFC findet sich bei der Abfrage und Bereitstellung von Informationen. So setzen beispielsweise die ÖBB Postbusse bei ihren Routen der Vienna AirportLines ein System ein, das den Benutzerinnen und Benutzern ermöglicht, über NFC-fähige Geräte die Abfahrtszeiten der nächsten Busse an den jeweiligen Haltestellen direkt abzufragen, wie auf der ÖBB Postbus Internetseite (ÖBB Postbus) veröffentlicht wurde. Bei einer entsprechenden Verbreitung von NFC-fähigen Geräten kann auf die Installation der beispielsweise auch in Graz an frequentierten Haltestellen vorhandenen großen Terminals in Zukunft verzichtet und somit Kosten eingespart werden.

4.3.6 NFC als Vermittler anderer Verbindungen

Mittels NFC ist es möglich, andere Verbindungen auszuhandeln, über die dann ein Datentransfer ausgeführt wird. Ein beliebter Anwendungsfall dafür ist Bluetooth, da ein

Bluetooth-Pairing zwischen Geräten in manchen Anwendungsfällen verhältnismäßig lange (mehrere Sekunden) dauern kann. In diesem Fall kann man die Verbindungsinformationen über NFC austauschen, wodurch der Initialisierungsschritt bei der Verbindung entfällt. Desweiteren ist NFC energiesparender als Bluetooth in der Standardversion. Seit Bluetooth Version 4.0 existiert jedoch auch eine Erweiterung *Bluetooth low energy*, die diesen Nachteil beheben soll (Bluetooth, 2011).

Bluetooth soll aber keinesfalls als Konkurrenz zu NFC empfunden werden, da die Technologie durch die größere Reichweite ein völlig anderes Konzept verfolgt.

Ein Beispiel wo diese Kombination zum Einsatz kommt, bietet sich bei Bluetooth Lautsprechern. Die Verbindung wird über NFC ausgehandelt, die Daten werden letztlich über Bluetooth zu den Lautsprechern übertragen. Sony nennt diese Funktion One-Touch und setzt diese unter anderem auch zur Verbindung des Smartphones zu Fernsehern ein (Sony, 2013).

4.3.7 Steuerung des Gerätes mittels NFC-Tags

Eine einfache Möglichkeit für die Anwendung von NFC-Tags wäre, damit Gerätaktionen auszuführen. Man verwendet dafür NFC-Tags, die vorgefertigte Aktionen gespeichert haben und die Benutzerinteraktion drastisch verkürzen können. Dies kann besonders bei öfter wiederkehrenden Aktionen nützlich sein. Die auszuführenden Aktionen können verschiedenster Art sein. So können NFC-Tags beispielsweise unter Android auch Einträge über eine zu startende Anwendung halten, wodurch die Benutzerin oder der Benutzer die Anwendung nicht mehr selber starten muss. Zusätzlich dazu kann man auf dem NFC-Tag auch Daten speichern, die die gestartete Anwendung dann verwenden kann.

So ist eine einfache Schnittstelle möglich, beispielsweise für das Senden von Emails an einen bestimmten Empfänger mit einem vorgefertigten Betreff und Text. Ebenso lässt sich mit einem entsprechend konfigurierten Tag zu einem WLAN verbinden, aber auch die Lautstärke verändern. Dadurch können beispielsweise an einer Konferenz teilnehmende Personen am Eingang durch das Überstreifen auf Vibrationsalarm ohne Ton umschalten und beim Verlassen wieder reaktivieren.

4.4 NFC im Vergleich zu anderen Technologien

In diesem Unterkapitel wird auf einige Vor- und Nachteile von NFC zu anderen Technologien eingegangen, aber auch beschrieben, wie die Technologien eventuell vorhandene Synergieeffekte ausnutzen können.

4.4.1 NFC und RFID

NFC ist mit RFID eng verwandt und baut teilweise auf RFID auf. Bei passiven (verbindungslosen) Übertragungen sind gewöhnlich RFID-Transponder im Einsatz. Allerdings können bei NFC die Antennengrößen stark reduziert werden, da die Feldstärke durch die geringere Reichweite niedriger ist als bei klassischen RFID Übertragungen. Das hat zum Vorteil, dass diese NFC-Tags auch auf wesentlich kleineren Gegenständen zum Einsatz kommen kann. Allerdings ist auch das Einsatzspektrum durch die geringe Reichweite

beschränkt. Kann man per RFID noch Daten über einige Meter Entfernung auslesen, ist bei NFC schon nach wenigen Zentimetern Ende.

4.4.2 NFC und Strichcodes

Durch die ähnlich kurze Reichweite der beiden Technologien, sind sie in ihren möglichen Einsatzgebieten vergleichbar. Beinahe überall wo auf Strichcodes basierende Techniken wie die zuvor beschriebenen QR-Codes zum Einsatz kommen können, kann auch über den Einsatz von NFC nachgedacht werden. Der Vorteil von NFC gegenüber optischen Codes liegt in der Unabhängigkeit des Umgebungslichtes. Während in dunklen Umgebungen bei QR-Codes der Code beim Lesevorgang beleuchtet sein muss, funktionieren NFC-Chips trotzdem. Dies ist beispielsweise beim Einsatz von NFC in Smartpostern ein großer Vorteil, da die Information vom jeweiligen Benutzer auch in der Nacht gelesen werden kann.

Ebenso muss auf das stets wachsende Datenvolumen Rücksicht genommen werden. Optische Codes wachsen bis zu ihrer spezifizierten Obergrenze auch in ihrer Fläche mit, was den Einsatz auf sehr kleinen Objekten schwierig oder gar unmöglich macht. Zwar wurde zu diesem Zweck der ebenfalls zuvor beschriebene Micro-QR-Code (siehe Kapitel 2.2.3.1) entwickelt, allerdings sind die technischen Möglichkeiten in der Chip-basierenden Technologie deutlich größer, was sich positiv auf die Menge der zu speichernden Informationen auswirkt.

In vielen Einsatzgebieten wird aber dennoch auf optische Codes zurückgegriffen, da die Verbreitung solcher Lesegeräte, wie Smartphones mit Kamera, deutlich höher ist. NFC-Chips werden immer noch nur in verhältnismäßig wenigen Smartphones eingesetzt. So verzichtet Apple als einer der führenden Smartphonehersteller noch gänzlich auf die Technologie.

4.5 Probleme, Bedenken und Kritiken

In diesem Unterkapitel wird auf einige Probleme, sowie Bedenken und Kritiken von NFC eingegangen und hingewiesen. Es werden einige sicherheitskritische Probleme näher erläutert und gezeigt, wie man sich schützen kann.

4.5.1 Abhören

Wie jede Funkübertragung ist auch die Übertragung über NFC nicht vor dem Abhören sicher. Durch die ständig wachsende Verbreitung NFC-fähiger Geräte kann ein Angreifer einfacher an die notwendige Hardware kommen. Da jedoch die Reichweite von NFC laut Spezifikation auf wenige Zentimeter begrenzt ist, ist ein Abhören im allgemein verstandenen Sinne nur schwer möglich, ohne dabei erkannt zu werden. Allgemeingültige Aussagen über das Abhören von NFC sind daher bislang nicht machbar, da es immer auf die jeweils verwendete Hardware der potentiellen Opfer ankommt, ob Signale außerhalb der üblichen Spezifikation gesendet werden. In diesem Fall kann ein Angreifer mit speziellen Antennen Signale außerhalb der spezifizierten Reichweite auffangen, die jedoch in den wenigsten Fällen verwendbar sind. So sind laut (Haselsteiner & Breitfuß, 2006) folgende Parameter entscheidend für die Entfernung:

- Signalfeldeigenschaften des Sendergerätes (Antennengeometrie, Gehäuseabschirmung, Umgebung)
- Eigenschaften des Empfangsgerätes des Angreifers (Antennengeometrie und –orientierungsmöglichkeit)
- Qualität des Empfangsgerätes des Angreifers
- Qualität des Signaldecoders des Angreifers
- Umfeld des Angriffsortes und Einschränkungen durch Barrieren
- Signalstärke des NFC-Gerätes
- Übertragungsmodus (aktiv oder passiv)

Deswegen muss für jeden Angriff das notwendige „Setup“ stimmen. Da oft mehrere Opfer Ziel einer solchen Attacke werden sollen, hängt ein Angriffsszenario zu sehr vom verwendeten Gerät des Opfers ab. Bei passiven Übertragungen sinkt die mögliche Entfernung durch die deutlich niedrigere Signalstärke deutlich. Laut obiger Quelle können abhängig von den zuvorgenannten Parametern Abhöraktionen in bis zu 10 Meter Entfernung im aktiven Modus und 1 Meter Entfernung im passiven Modus durchgeführt werden.

Einen möglichen Schutz vor dem Abhören bietet eine gesichere Verbindung mittels RSA basierendem Diffie-Hellman Protokoll (Diffie & Hellman, 1976), oder Elliptic-Curve-Cryptography aufzubauen. Über dieses Secret lässt sich dann ein sicherer Kanal mit etablierten Verschlüsselungsalgorithmen aufbauen.

4.5.2 Übertragungsstörung

Ähnlich wie bei Denial-of-Service Attacken kann ein Angreifer im richtigen Zeitpunkt die Übertragung stören, sodass sie nicht korrekt durchgeführt werden kann. Allerdings ist es nicht so einfach, den richtigen Zeitpunkt zu finden. NFC Übertragungen gehen durch die verhältnismäßig hohe Übertragungsrate bei kleinen Datenmengen sehr schnell und das Zeitfenster von der Initialisierung bis zur Übertragung ist gemäß der Spezifikation sehr kurz, allerdings auch abhängig vom verwendeten Gerät.

Sofern der Angreifer über die verwendeten Geräte der Opfer informiert ist, kann er sich den Zeitpunkt ausrechnen. Wichtig sind dabei die verwendeten Frequenzen, Modulation und Kodierung. Auf diese Weise lassen sich die übertragenen Daten jedoch nicht manipulieren, wodurch ein Angreifer nicht immer einen Nutzen von einer Störattacke hat.

Störangriffe können von den aktiven Sendegeräten selbst erkannt werden, indem sie während der Übertragung das Signalfeld überprüfen. Damit ist kann der Störangriff natürlich nicht verhindert werden. Es kann lediglich sichergestellt werden, dass der Empfänger die Daten empfängt. Einen wirksamen Schutz vor Störangriffen gibt es wie bei DoS Attacken nicht (Haselsteiner & Breitfuß, 2006).

4.5.3 Datenmodifikation

Im Gegensatz zur Übertragungsstörung will ein Angreifer gültige Daten übertragen, diese allerdings zu seinen Gunsten modifizieren. Diese Angriffsart ist deutlich komplizierter als die Übertragungsstörung, da in die Modulation eingegriffen werden muss. Wird laut Spezifikation die Miller-Kodierung (106 Kilobit/s 100%, ASK, siehe Kapitel 4.2) verwendet, ist die Modifikation praktisch unmöglich. Der Angreifer müsste ein Pausensignal im richtigen

Zeitpunkt in die Modulation einschleusen und zusätzlich ein Signal aussenden, das im gleichen Zeitpunkt das Signal des Originalsenders überdeckt, um eine 0 in eine 1 umzuwandeln. Die einzige Möglichkeit der Modifikation bietet sich beim Umwandeln der zweiten 1 bei zwei aufeinanderfolgenden 1, da dann lediglich das Pause-Signal überdeckt werden muss. Daher kann man bei einer 100% Modulation nie ein 0 Bit in ein 1 Bit umgewandelt werden, sondern nur 1 Bit in 0 Bit, wenn das vorangegangene Bit auch ein 1 Bit ist. (Siehe Abbildung 4-3 NFC Digitale Frequenzmodulation)

Bei 10% Modulation können beide Bits umgewandelt werden, wenn der Angreifer die Signale analysieren kann. Er vergleicht ein unvollständiges Signal mit dem vollständigen und kann so zum unvollständigen Signal seine veränderten Bits hinzufügen und das Originalsignal wird mit den modifizierten Bits „vervollständigt“. In den meisten Fällen wird das modifizierte Signal zu groß sein, um sinnvolle Modifikationen anzustellen. Laut (Haselsteiner & Breitfuß, 2006) ist das aber nicht auszuschließen.

Will man also eine vor Modifikationen geschützte Übertragung bewerkstelligen, empfiehlt sich die Einstellung auf 106 Kilobit/s mittels Miller-Kodierung und 100% Modulation. Der Nachteil dabei wäre natürlich die langsamere Verbindung. Eine weitere Möglichkeit wäre das Signalfeld ständig zu überprüfen, was jedoch einen erhöhten Energieverbrauch nach sich zieht. Der wirksamste Schutz vor Modifikation ist dennoch der gesicherte Kanal, wie schon beim Abhören beschrieben. (Siehe: Abhören)

4.5.4 Einfügen von Daten

Ein Angreifer könnte versuchen, Daten während der Übertragung einzuschleusen. Die Originaldaten werden dadurch um zusätzliche Daten erweitert. Die Übertragung der einzuschleusenden Daten muss vor der Übertragung der eigentlichen Daten stattfinden. Man kann sich das so vorstellen, dass ein Gerät ein Signal an das andere Schickt und bevor das andere Antworten kann, schickt der Angreifer seine Antwort.

Dabei sind aber einige Dinge zu beachten: Durch die geringere Distanz der Originalgeräte ist auch meist die Antwortzeit kürzer als die eines Angreifers, der möglichst weit weg sein möchte, um unerkannt zu bleiben. Dazu kommt, dass die Übertragung des Angreifers abgeschlossen sein muss, wenn die Übertragung des Opfers beginnt, da die übertragenenen Daten ansonsten korrupt und damit ungültig sind. Sofern das Opfer ein sehr langsames Gerät hat, ist diese Angriffsart also durchaus möglich (Haselsteiner & Breitfuß, 2006).

Diese Angriffsart lässt sich ebenfalls erkennen, indem während der Signalübertragung das Signalfeld überprüft wird, verhindern mittels sicherem Kanal, wie schon beim Abhören beschrieben. (Siehe: Abhören)

4.5.5 Man in the Middle Angriff

Das Prinzip eines Man-in-the-Middle Angriffs ist einfach: Gaukle zwei Opfern vor, dass sie direkt miteinander kommunizieren, während du die Konversation aber ohne deren Wissen vermittelst und durchleitest. Im Grunde ist der Angriff im NFC-Szenario eine Kombination aus Abhören und Modifikation der Daten.

Bei NFC gestaltet sich der Vorgang schwierig. Beim passiven Übertragungsmodus müsste der Angreifer das Signal vom aktiven Sender stören, sodass das passive Gerät das Signal nicht erreicht. Das funktioniert auch, wie zuvor beschrieben. Allerdings nur, wenn der aktive Sender das gestörte Signal nicht mitbekommt. Gleichzeitig muss nun ein Signal an das passive Gerät gesendet werden. Dies ist aber nicht möglich, weil immer noch das originale Signal vom Sender existiert, sowie das Störsignal. Das passive Gerät kann also kein Signal mehr empfangen, auch nicht das des Angreifers. Somit ist diese Angriffsmethode bei einem passiven Gerät praktisch unmöglich.

Anders sieht es bei zwei aktiven NFC-Geräten aus: Theoretisch ist es möglich beiden Kommunikationspartnern Daten zukommen zu lassen, allerdings gewöhnlich nicht ohne deren Wissen. Sobald ein Gerät an das andere gesendet hat, wartet es auf die Antwort dessen. Wie schon zuvor beim Kapitel Datenmodifikation erläutert, ist die Modifikationsmöglichkeit stark eingeschränkt zwar möglich, aber nicht praktikabel. Das Unerkanntbleiben ist für eine echte Man-in-the-Middle Attacke zwingend nötig, da die Opfer ansonsten die Kommunikation abbrechen und anderweitig fortsetzen können.

Sogesehen gilt NFC für Man-in-the-Middle Attacken generell als sicher, sofern die Signalfelder überprüft werden. Ansonsten muss man sich mit „praktischer“ Sicherheit begnügen (Haselsteiner & Breitfuß, 2006).

4.5.6 Relay-Angriffe

Ähnlich wie bei Man-in-the-Middle Angriffen möchte ein Angreifer die Daten weiterleiten. Da dies in Echtzeit geschehen muss, bedarf es in diesem Fall gewöhnlich einer Modifikation zumindest eines Punktes. Ein Relay-Proxy leitet die Daten entsprechend weiter und gaukelt dem jeweiligen Endpunkt vor, dass er mit dem gewünschten Ziel kommuniziert. Dies funktioniert bei nach ISO/IEC 14443 standardisierten Chips, die beispielsweise in Kreditkarten eingesetzt werden, wie in (Hancke, 2005) beschrieben.

Abhilfe gegen diese Art des Angriffs schafft laut obiger Quelle das sogenannte Distance-Bounding Protokoll, was jedoch in praktischer Hinsicht schwierig zu realisieren ist, wenn man den Einsatzort und die damit verbundene Limitierung berücksichtigt.

4.5.7 Gerätverlust

Durch einen Gerätverlust gingen alle möglichen nutzbaren Fähigkeiten verloren oder gar in falsche Hände über. Sollte es möglich sein, Rückschlüsse auf den Besitzer zu schließen, kann der „Finder“ das Gerät und seinen vollen Funktionsumfang für seine Zwecke nutzbar machen. Ähnlich wie bei einer Kreditkarte kann der Besitzer zwar alle möglichen Funktionen sperren lassen, ist aber darauf angewiesen, dass er den Verlust auch rechtzeitig merkt. Dazu kommt noch, dass viele Funktionen auf mehrere Anbieter verteilt sein können, was einen erheblichen Aufwand darstellt, alle zu kontaktieren und die Sperrung zu veranlassen. Das setzt allerdings voraus, dass es eine solche Sperrfunktion überhaupt gibt.

Zusätzlich empfiehlt es sich bei Finanzdienstleistern diverse Limits (Höchstgrenze, Tagesgrenze) festzulegen. Aufgrund der noch verhältnismäßig geringen Verbreitung der Schlüsselfunktion, gibt es (Stand April 2013) noch keine Präzedenzfälle, die ausreichende rechtliche Rahmenbedingungen für Versicherungen im Verlustfall diskutieren.

Sinnvoll ist auch die PIN-Eingabe bei der Geräteaktivierung zu aktivieren.

4.5.8 Finanzbetrug durch ungewollte Abbuchungen

Im Falle ungewollter Abbuchungen liegt die Beweislast bei der Benutzerin oder dem Benutzer. Sofern die verwendeten Anwendungen keine bei Gericht verwenbare Daten speichert, lässt sich nicht feststellen, ob die Abbuchung tatsächlich ungewollt war. Durch die geringe Reichweite wird bei einer Übertragung gemäß Spezifikation davon ausgegangen, dass die Verbindung gewollt ist.

4.6 Zusammenfassung

In diesem Kapitel wurden die Grundlagen von NFC erläutert sowie die Spezifikation näher erklärt. Durch die Gegenüberstellung mit anderen Technologien konnte die Erkenntnis gewonnen werden, dass NFC in vielen Gebieten noch Aufholbedarf hat. Andere etablierte Technologien wie QR-Code versuchen durch Modernisierungen Nachteile auszumerzen beziehungsweise zu reduzieren und gleichzeitig die Vorteile auszubauen. Potential ist bei NFC mehr als nur ausreichend vorhanden. Allerdings muss es auch angenommen und ausgenutzt werden. Vor einigen Jahren wurden von vielen pro-NFC-Firmen mutige Vorhersagen getätigt, dass NFC in mittlerweile vergangenen Daten angesprochene Technologien überholen wird. Allerdings bedarf es wohl noch einiger Jahre, um diese Vorhersagen Wirklichkeit werden zu lassen.

Die steigende Hardwareunterstützung in den jüngst vorgestellten Smartphones lässt jedenfalls darauf hoffen, dass die Technologie in Zukunft noch weiter verbreitet werden wird und weitere potentielle Einsatzgebiete erschlossen werden können.

5 Praktisches Implementation zu NFC

In den bisherigen Kapiteln wurden die theoretischen Grundlagen von NFC und teilweise verwandten oder ähnlichen Technologien erläutert. Es wurden auch einige Anwendungsfälle gezeigt. Um die Funktionalität von NFC näher zu demonstrieren und einen Überblick über die derzeit vorhandenen Möglichkeiten zu geben, wird in diesem Kapitel ein Prototyp einer App vorgestellt. Dieser Android Prototyp ist im Rahmen dieser Masterarbeit entstanden und zeigt einfache NFC Funktionen. Zur Entwicklung wurde eine bereits bei öffentlich verfügbaren Apps im Einsatz befindliche XML Schnittstelle verwendet, die im Rahmen von Projekten anderer Studierender an der Technischen Universität Graz entwickelt wurde.

Grundsätzlich geht es um einen Prototypen um das vorhandene elektronisches Lehrbuch L3T, „Lehrbuch für Lernen und Lehren mit Technologien“. Für weitere Informationen ist die Webseite des L3T Projektes anzusehen (Schön & Ebner, 2013).

Die Implementierung dieses Projektes soll als Basis dienen, um in den folgenden Kapiteln die Potentiale von NFC für Lehr- und Lernunterlagen auszuarbeiten, sowie Schwächen zu beschreiben und Kritiken zu behandeln.

In den folgenden Unterkapiteln werden die einzelnen verwendeten Konzepte beschrieben und näher erläutert.

5.1 Motivation

Da der Autor selbst im Besitz eines Google Nexus S seit dessen Erscheinungsdatum ist und das das erste auf Android basierende Smartphone mit NFC Unterstützung ist, war die gewisse Nähe zur Technologie schon gegeben. Durch diese Masterarbeit enstand auch ein gewisses Umfeld, in dem man den Einsatz von NFC in einem noch eher unbekannten Einsatzgebiet erproben kann.

5.2 Android App

Durch die in den letzten Jahren entwickelten Apps, entstand eine gewisse Affinität des Autors zum Android Betriebssystem. Es bietet gegenüber anderen Betriebssystemen aus der Entwicklersicht einige Vorteile, aber auch einige Nachteile. Die folgenden Unterkapitel sollen einen kurzen Einblick und eine kleine Einführung über die App-Entwicklung unter Android bieten, sowie die zusätzlich verwendeten Bibliotheken beschreiben.

5.2.1 Aufgabenstellung und Ziele

Es sollen die Möglichkeiten von NFC im Rahmen einer bestehenden Umgebung überprüft und implementiert werden. Zu zeigen ist, welchen Nutzen der Einsatz von NFC in diesem speziellen Anwendungsfall des elektronischen Lehrbuches haben kann. Die Anforderungen an den Prototyp sind:

- Einbindung der XML-Schnittstelle zur Übertragung der notwendigen Daten aus dem bereits vorhandenen OpenJournalSystem
- Umsetzung der NFC Funktionalität zum Austausch von Daten von Gerät zu Gerät
- Umsetzung der NFC Funktionalität zum Beschreiben und Auslesen von Daten von NFC-Tags

Ziel ist, die im Lehrbuch vorhandenen Daten auf NFC-Tags schreiben zu können, sodass diese von allen Personen mit NFC-fähigen Geräten ausgelesen werden können. Dadurch soll die Möglichkeit geschaffen werden, ganz oder teilweise Lehrunterlagen über NFC-Tags zu verteilen. Desweiteren sollen die Unterlagen auch von Gerät zu Gerät (Peer-to-Peer) direkt tauschbar sein.

Diese Anforderungen und Ziele waren maßgeblich bei der Wahl der eingesetzten Technologien, Frameworks und Bibliotheken.

5.2.2 Technologien

Anhand der Anforderungen und Ziele wurden die eingesetzten Technologien ausgewählt. Zur ursprünglichen Auswahl standen zum Projektbeginn mehrere Betriebsysteme mit NFC Unterstützung und Verfügbarkeit der Endgeräte, wie in folgender Auswahl aufgelistet:

- Android (ab Version 2.3)
- BlackBerry (Version OS 7 und 10)
- Windows Phone (ab Version 8)
- Symbian (Version „Belle“ und ^3)
- Bada (ab Version 2.0)

Trotz der großen Auswahl an Betriebssystemen, fiel die Wahl auf Android. Es ist von den gelisteten Systemen das am weitesten verbreitete Betriebssystem und besitzt mit der DalvikVM eine mächtige Grundlage für die Entwicklung von Apps. Es ist ein auf dem Linux-Kernel basierendes Betriebssystem, das hauptsächlich auf Smartphones und Tablets zum Einsatz kommt. Android unterstützt seit dem Erscheinen von der Android Version 2.3 NFC (NPP – NDEF Push Protocol) und seit Android 4.0 zusätzlich das SNE-Protokoll (Simple NDEF Exchange Protocol). Android zählt auch (Stand April 2013) zu den weltweit am weitesten verbreiteten mobilen Betriebssystemen. NFC-fähige Geräte sind desweiteren recht günstig zu haben. Deswegen wurde dieses Betriebssystem für diese Aufgabenstellung ausgewählt.

5.2.2.1 Android

Android Applikationen werden in der Programmiersprache Java geschrieben. Applikationen, gewöhnlich kurz Apps genannt, werden durch den Android SDK erstellt. Durch das

Kompilieren und Archivieren der zusätzlich notwendigen Dateien entsteht eine einzelne .apk Datei, die auf den Endgeräten installiert wird. Da Android auf dem Linuxkernel basiert, ist eine Art Sandbox einfach umsetzbar gewesen. Jede einzelne App wird von einem jeweils verschiedenen Benutzerkonto ausgeführt, sodass keine ungewollten Zugriffe auf anwendungsspezifische Dateien stattfinden können. Zusätzlich wird für jede App ein neuer Linuxprozess gestartet. Jede App hat einen ihr direkt zugewiesenen Speicherbereich. Der im Hintergrund weiterlaufende Linuxprozess kann aber vom Betriebssystem freigegeben werden, wenn für andere aktive Prozesse Speicher benötigt wird, oder die Anwendung länger nicht geöffnet wird.

Es ist jedoch auch möglich, mehreren Apps den Zugriff auf einen geteilten Speicherbereich zu geben. Dafür muss man die App mit dem gleichen Schlüssel signieren, sowie im Manifest festlegen, dass sie einen geteilten Speicherbereich verwenden will und mit welcher Anwendung sie den Bereich teilen will. In diesem Fall weist das Betriebssystem den Apps bei der Installation die gleiche UserID zu, sodass die Anwendungen im gleichen Prozess gestartet werden. Die Anweisung dafür ist in **Fehler! Verweisquelle konnte nicht gefunden werden.** ezeigt:

```
<manifest
xmlns:android="http://schemas.android.com/apk/res/android"
      package="com.package.name"
      android:versionCode="1"
      android:versionName="1.0"
      android:sharedUserId="1234"
      android:sharedUserLabel="1234"
>
```

Codelisting 1 Geteilte UserID

Auf systemrelevante Bereiche kann ein Benutzerprozess der Anwendung durch das Sandbox-Prinzip nicht zugreifen. Für gewisse Funktionen stehen aber zusätzliche mögliche Berechtigungen zur Anforderung bereit. Die Entwicklerin oder der Entwickler muss diese Berechtigungen in der Manifest-Datei der Anwendung anfordern. Die Benutzerin oder der Benutzer des Gerätes muss dann bei der Installation die Rechte gewähren. Wird das nicht gemacht, wirft das System eine SecurityException, wenn das Programm dennoch versucht, eine rechteabhängige Aktion auszuführen.

Folgende Rechte können beispielsweise mittels Anforderung in der Manifest-Datei eingeräumt werden:

- Kontakte
- Anrufe
- SMS-Nachrichten
- Externer Speicher (SD-Karten)
- Hardwareelemente steuern (Kamera, Lautsprecher, Mikrofon)
- Netzwerkzugriff (WLAN, Bluetooth, NFC, etc.)
- Standortdienste (GPS, Netzwerkstandort)

- Systemzugriff (Beenden anderer Apps, Systemzeit ändern, etc.)

Man kann allerdings auch selber Berechtigungen definieren. Dazu muss im Manifest festgelegt werden, um welche Permission es sich handelt. Ein Beispiel dafür bietet die in **Fehler! Verweisquelle konnte nicht gefunden werden.** gezeigte Definition:

```
<permission android:name="com.me.app.myapp.permission.DEADLY_ACTIVITY"
        android:label="@string/permlab_deadlyActivity"
        android:description="@string/permdesc_deadlyActivity"
        android:permissionGroup="android.permission-group.COST_MONEY"
        android:protectionLevel="dangerous"
/>
```

Codelisting 2 Android Berechtigungsdefinition **(Android Developers, 2013)**

Android Anwendungen gliedern ihre unterschiedlichen Ansichten in sogenannten Activities. Eine solche Activity behandelt die jeweils zur Ausführungszeit sichtbaren Interfaceelemente und deren zugeordnete Benutzerinteraktionen. Diese Activities können durch sogenannte Intents erstellt werden. Intents dienen generell als Schnittstelle für die Ausführung anderer Aktivitäten. Dabei muss es sich nicht zwangsläufig um Activity-Derivate handeln. Es können auch Aktionen durchgeführt werden, die das Öffnen anderer Anwendungen veranlassen – beispielsweise einen externen Webbrowser.

Das der Androiddokumentation entnommene Zustandsdiagramm in Abbildung 5-1 illustriert den Lebenszyklus einer Activity:

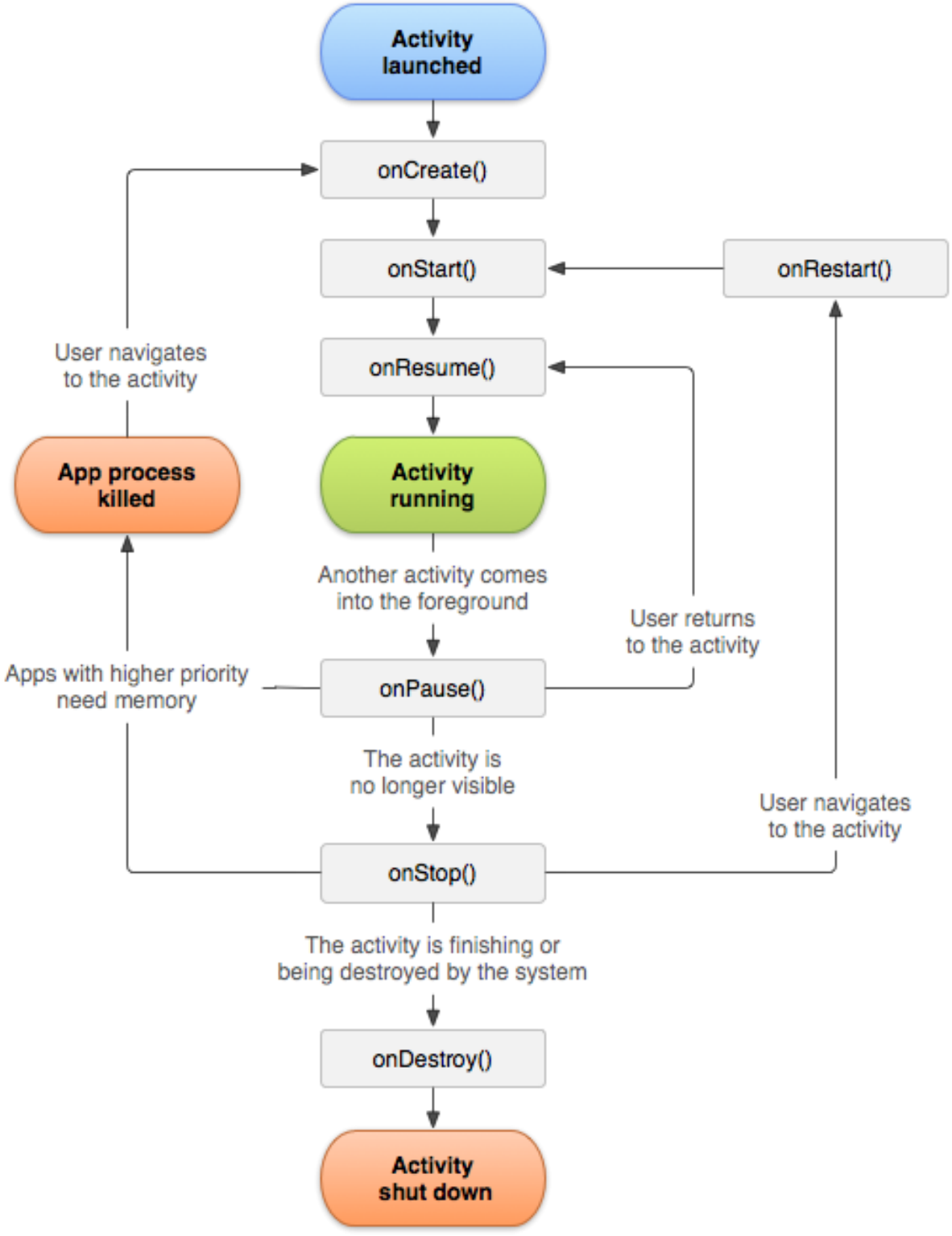

Abbildung 5-1 Android Activity Lifecycle **(Android Developers, 2013)**

Activities werden gewöhnlich durch einen Aufruf von startActivity(Intent) aus einer aktuell laufenden Activity gestartet. Anhand des obigen Diagrammes erkennt man, dass die onCreate Methode zuerst aufgerufen wird. Hier wird das Layout der Activity geladen, sofern eines vorhanden ist. Dafür muss das Layout, das in einer XML-Datei definiert werden muss, mittels

der Methode setContentView gesetzt werden. In der XML-Datei kann man einzelnen Elementen eine ID zuweisen, wodurch man dann in der Activity auf dieses Element zugreifen kann. Eine Definition eines Elementes ist in **Fehler! Verweisquelle konnte nicht gefunden erden.** gegeben:

```
<LinearLayout xmlns:android=http://schemas.android.com/apk/res/android
    android:id="@+id/layout_identifier"
    android:orientation="vertical"
    android:layout_width="match_parent"
    android:layout_height="match_parent"
>
```

Codelisting 3 Android Layout Defnition

Nun kann man in der Activity folgendermaßen darauf zugreifen:

```
LinearLayout layout = (LinearLayout) findViewById(R.id.layout_identifier);
```

Codelisting 4 Android Zugriff auf einen Layoutidentifier

5.2.3 Implementierung

In diesem Unterkapitel wird die Implementierung des Prototypen beschrieben. Der Prototyp wurde für Android 4.1 *Jelly Bean* entwickelt. Als Entwicklungsumgebung wurde ein Windows 7 64-bit System mit NetBeans 7.0.1 verwendet.

5.2.3.1 Setup der Entwicklungsumgebung

Wie im Kapitel 5.2.2 beschrieben, fiel die Wahl auf ein Android-System. Da Android Java verwendet, muss ein Java Development Kit (JDK) auf dem System installiert sein. Eine Java Runtime Environment ist nicht ausreichend. Dieser JDK ist im Internet herunterladbar und installierbar. Mit dem GNU Java Compiler (GCJ) ist Android nicht kompatibel.

Desweiteren benötigt man die Android Development Tools (ADT). Als Buildtool wird Apache Ant verwendet. Für jede benötigte Software gibt es einen einfachen Installer.

Die Wahl der Integrated Development Environment (IDE) ist gewöhnlich Geschmackssache. Viele Androidentwickler verwenden jedoch die Eclipse IDE, die auch auf der offiziellen ADT Downloadseite im Paket angeboten wird. Bei diesem Projekt fiel die Wahl jedoch auf die NetBeans IDE. Die Installation ist unkompliziert, die IDE ist für viele andere Programmiersprachen und Umgebungen geeignet und bietet eine Vielzahl an Plugins. So auch das NBAndroid Plugin, das für die Android Entwicklung mit NetBeans zwingend notwendig ist (Kubacki, 2013).

Um die Entwicklung der NFC-Interaktionen zu vereinfachen, wurde eine externe Bibliothek *ndef-tools* eingebunden (Skjolberg, 2013). Diese stellt Objektrepräsentationen von NDEF-Daten zur Verfügung, die eine bessere Verwaltung und Unterscheidung der verschiedenen übertragenen Daten ermöglicht. Die im Download enthaltene .jar Datei muss in das lib-Verzeichnis des Projektes kopiert bzw. zum Projekt hinzugefügt werden.

Um dieses Setup zu testen und die NDEF-Tools Bibliothek und die NFC-Features generell kennen zu lernen wurde zuerst ein kleines Testprojekt implementiert. Durch dieses Testprojekt konnten die notwendigen Kenntnisse erworben werden, um die L3T-NFC-Applikation zu entwickeln.

Zum Ausführen und Testen des Projektes wurde ein Google Nexus S verwendet. Ein Entwickeln auf dem Simulator ist bei NFC nicht möglich. Für Layouttests empfiehlt es sich jedoch, generell jede App in den verschiedensten verbreiteten Layoutkonfigurationen im Simulator zu testen.

5.2.3.2 Spezifische Anforderungen

Nachdem in Kapitel 5.2.1 die allgemeinen Anforderungen beschrieben wurden, werden in diesem Kapitel die auf den konkreten Anwendungsfall spezifischen Anforderungen beschrieben.

Ausgangsbasis ist die bereits verfügbare App *L3T* (L3T eBook, 2012). Der Prototyp der L3T-NFC App besitzt daher folgende Anforderungen:

- Schnittstelle
    - Implementierung der XML-Schnittstelle des OpenJournalSystem
- Darstellung
    - Darstellung der Artikel in einer nach Sektionen gruppierte Liste
    - Darstellung eines ausgewählten Artikels
- NFC-Komponenten:
    - Umsetzung von Android Beam zur direkten Übertragung zwischen Android Geräten
    - Umsetzung eines Tag-Writers zum Beschreiben von NFC-Tags
    - Umsetzung eines Tag-Readers zum Auslesen von NFC-Tags

Aus obiger Auflistung ergeben sich daher drei Hauptmodule für die App, die jederzeit austauschbar sein sollen.

5.2.3.3 XML Schnittstelle

Es soll eine XML Schnittstelle implementiert werden, die die Daten aus dem OpenJournalSystem einlesen kann. Hierfür werden zwecks objektorientierter Speicherung Beans für jeden XML-Eintrag angelegt.

Um die Schnittstelle einlesen zu können, ist ein XML-Parser notwendig. Folgende XML-Parser kamen für die Implementierung in Frage:

- XML SAX Parser (Simple API for XML)
- XML DOM Parser (Document Object Model)
- XML StAX Parser (Streaming API for XML)

Jeder dieser Parser hat seine Vor- und Nachteile. Gesucht wurde ein Parser, der einfach zu implementieren ist, einigermaßen schonend mit den auf Smartphones sehr begrenzten Resourcen umgeht und trotzdem nicht zu langsam ist.

Vor- und Nachteile eines SAX Parsers gemäß Arbeitsweise:

- Vorteile:
  - Speicherschonend durch sequentielles Einlesen der Elemente
  - Auswertung während des Einlesens möglich
  - Ereignisbasierter Parser ermöglicht akute Fehlererkennung
  - Schneller als DOM
  - Geeignet für schlecht strukturierte XML Daten
- Nachteile:
  - Kein direkter Zugriff auf Elemente
  - Aufwendigere Implementierung
  - Keine Manipulation des Baumes möglich

Vor- und Nachteile eines DOM Parsers gemäß Arbeitsweise:

- Vorteile:
  - Direkter Zugriff auf Elemente möglich
  - Manipulation des Baumes möglich
  - Kombination mit XPath durch Baumstruktur einfach möglich
- Nachteile:
  - Hoher Speicherverbrauch, da gesamtes Dokument als Baumstruktur geladen wird
  - Verhältnismäßig langsam
  - Nicht geeignet für sehr große XML Dokumente wenn wenig Speicher zur Verfügung steht

Vor- und Nachteile eines StAX Parsers gemäß Arbeitsweise:

- Vorteile:
  - Mittelweg zwischen SAX und DOM durch einen Cursor
  - Cursor bewegt sich durch Elemente ähnlich wie bei SAX, ist jedoch nicht ereignisbasiert
  - Iterator-Verfahren objektorientiert
  - Weniger Speicherverbrauch als DOM
  - Höhere Flexibilität als bei SAX
- Nachteile:
  - Iterator-Verfahren langsamer als Cursor
  - Keine akute Fehlererkennung wie bei SAX

Unter Berücksichtigung der eingesetzten Umgebung sind an den XML Parser folgende Anforderungen gestellt:

- Speicherschonend
- Unterstützung für potentiell große XML Daten
- Einfache Implementierung

In Anbetracht der Anforderungen und der Berücksichtigung der Entwicklungsumgebung, ist der Einsatz eines StAX Parsers sinnvoll.

Mit der XmlPullParser Java API steht eine gute Basis für die Entwicklung eines Parsers zur Verfügung. Desweiteren wird diese API von den Android Entwicklern empfohlen (Android Developers, 2013).

Der Parser wird in einem eigenen Thread gestartet. Hierfür wird die Klasse AsyncTask als Basis verwendet, die das Threadhandling auf einer anderen Ebene übernimmt. Zu implementieren ist dann die Methode:

```
protected T doInBackground(T... params);
```

Codelisting 5 Android AsyncTask Hintergrundmethodensignatur

Zusätzlich sinnvoll zu überschreiben:

```
protected void onPreExecute()
protected void onPostExecute(T returnValue);
```

Codelisting 6 Android AsyncTask Hilfsmethodensignatur

Der AsyncTask wird folgendermaßen definiert:

```
class DownloadIndex extends AsyncTask<Void, Void, Boolean>
```

Codelisting 7 Android AsyncTask Klassendefinition

In der onCreate Methode der Activity wird er mittels folgendem Befehl gestartet:

```
new DownloadIndex().execute();
```

Codelisting 8 Android AsyncTask Ausführungsbefehl

In unserem Fall wird in onPreExecute eine Ladeanimation erstellt, die dann in onPostExecute wieder beendet wird. Das Erstellen der Ladeanimation ist recht einfach. Es wurde ein simpler ProgressDialog verwendet, der in unserem Fall keinerlei Informationen über den Fortschritt des Downloads und Parsingvorganges hält. So reicht folgender einfacher Code in Codelisting 9 zum Starten einer solchen Ladeanimation:

```
pd = new ProgressDialog(IndexActivity.this);
pd.setCancelable(false);
pd.setProgressStyle(ProgressDialog.STYLE_SPINNER);
pd.setTitle("Loading...");
pd.setMessage("Please wait...");
pd.show();
```

Codelisting 9 Android AsyncTask ProgressDialog

Der XmlPullParser wird nun auf folgende Weise in der Methode doInBackground(T params) angelegt:

```
URL url = new URL("");
is = url.openStream();
XmlPullParserFactory factory = XmlPullParserFactory.newInstance();
factory.setNamespaceAware(true);
XmlPullParser parser = factory.newPullParser();
parser.setInput(is, null);
```

Codelisting 10 Android XmlPullParser Initialisierung

Anhand der bekannten Struktur wird dann der Parser aufgesetzt. Wichtig bei der Umsetzung eines Parsers mit XmlPullParser ist nun die Abarbeitung des Dokumentes nach der jeweiligen Situation. Der Ablauf ist recht simpel gehalten, indem man bei einem jeweiligen Starttag das zuzuordnende Objekt anlegt und sich die notwendigen Daten (Attribute, Text) holt und beim jeweiligen Endtag die Objekte auf etwaige Listen hinzufügt.

Die Struktur eines Lehrbuchartikels ist in Codelisting 11 definiert:

```
<article id="28">
  <title></title>
  <authors>
    <author>
      <firstName></firstName>
      <middleName></middleName>
      <lastName>
      </lastName>
    </author>
  </authors>
  <language></language>
  <abstract></abstract>
  <subject>
    <topic></topic>
  </subject>
  <files>
    <file id="519">
      <fileUrl</fileUrl>
      <fileSize></fileSize>
      <mimeType>application/x-download</mimeType>
      <originalFileName></orininalFileName>
      <md5checksum></md5checksum>
    </file>
  </files>
  <suppfiles/>
</article>
```

Codelisting 11 XML-Struktur eines Lehrbuchartikels

Daher wurde eine Klasse Article angelegt, um die notwendigen Daten für jedes Article Objekt zu speichern. Dadurch ergibt sich der Codeausschnitt in Codelisting 12 zum Anlegen eines Article Objektes:

```
while (eventType != XmlPullParser.END_DOCUMENT && !done) {
  switch (eventType) {
    case XmlPullParser.START_DOCUMENT:
      sections = new ArrayList<Section>();
      break;
    case XmlPullParser.START_TAG:
      name = parser.getName();
      if (name.equals("article") {
        currentArticle = new Article();
        int articleId = Integer.parseInt(parser.getAttributeValue(null,
"id"))
        currentArticle.setId(articleId);
      }
      break;
    case XmlPullParser.END_TAG:
      name = parser.getName();
      if (name.equals("article") && currentArticle != null &&
currentSection != null) {
        currentArticles.add(currentArticle);
        currentArticle = null;
      }
      break;
    default:
      break;
  }
  eventType = parser.next();
}
```

Codelisting 12 XML-Parser für Article-Objekte

Für jedes gewünschte Element wird dann in START_TAG abgefragt, ob der Tag zur Zeit offen ist, das heißt es existiert bereits ein Element, zu dem die fortan gefundenen Elemente gehören, bis ein END_TAG zu dem bestimmten Element gefunden wurde. Dann wird in diesem Fall das Article Objekt auf eine Liste gespeichert und die Referenz des temporären Objektes gelöscht.

Für jeden zu behandelnden XML-Eintrag muss die Abfrage auf den XML-Tagnamen sowohl in START_TAG, als auch in END_TAG erweitert werden.

5.2.3.4 Darstellung

In diesem bestimmten Anwendungsfall landen die Article Objekte auf einer Liste, die einer Artikelgruppe zugeordnet sind. Diese Gruppen dienen dann zur gruppierten Ansicht der Artikel in einer aufklappbaren Liste. Android stellt dafür eine Klasse ExpandableListView zur Verfügung, die eine Erweiterung der gewöhnlichen ListView ist. Sie benötigt auch einen speziellen Adapter, um die anzuzeigenden Daten zuordnen zu können.

Das Layout für diese Anzeige wurde bewusst simpel gehalten. Rein zur Illustration wie man eine solche aufklappbare Liste anzeigen kann, dient das in Codelisting 13 gezeigte Beispiel:

```
<ExpandableListView
        android:id="@+id/elv_content_listing"
        android:layout_width="match_parent"
        android:layout_height="wrap_content"
/>
```

Codelisting 13 Android ExpandableListView XML-Definition

Es wird hierbei die android:id festgelegt, wodurch auf die Liste im Programm dann zugegriffen werden kann. In diesem Fall sieht das dann wie in Codelisting 14 aus:

```
ExpandableListView listView = (ExpandableListView)
findViewById(R.id.elv_content_listing);
Collections.sort(sections);
IndexActivityListViewAdapter adapter = new
IndexActivityListViewAdapter(IndexActivity.this, sections);
listView.setAdapter(adapter);
```

Codelisting 14 Android ExpandableListView Initialisierung

In Codelisting 14 ist auch zu sehen, wie man der Liste die Daten übergeben kann. Es wird der bestimmte Adapter definiert, der die Zuordnung übernimmt. Der Adapter muss die Basisklasse BaseExpandableListAdapter erweitern und deren bestimmte Methoden implementieren. Besonders relevant für die Zuordnung der Daten zu den angezeigten Interfaceelementen in den jeweiligen Listenabschnitten sind die Methoden:

- public View getGroupView(int position, boolean isExpanded, View convertView, ViewGroup parent)
- public View getChildView(int groupPosition, int childPosition, boolean isLastChild, View convertView, ViewGroup parent)

In diesen Methoden greift man auf die übergebenen Rohdaten zu. In unserem Fall liegen die Daten als Liste von Section Objekten vor, die jeweils eine Liste von ihnen untergeordneten Article Objekten hält.

Der Adapter wird mittels des ViewHolder-Patterns implementiert. Der herkömmliche Weg für jede Position in den getView Methoden wäre jedes Mal direkt über den Resourcen-Identifier R.id.name mit findViewById darauf zuzugreifen. Diese Zugriffe gelten als langsam, besonders wenn man sehr viele Ressourcen hat. Dies reduziert die Arbeit, die vom Thread, der das User Interface behandelt. Das macht sich besonders beim Scrollen langer Listen bemerkbar. Das ViewHolder-Pattern definiert daher eine spezielle Klasse, die die jeweiligen Interfaceelemente hält. Diese werden dort einmal ihren bestimmten Resource-Identifiern zugeordnet. Das ViewHolder-Pattern gilt als allgemein sinnvolle Variante, möglichst resourcenschonend Daten den Listenelementen zuzuweisen (Android Developers, 2013).

Zur Implementierung der getGroupView Methode:

Dem ViewHolder wird in unserem Fall nur der Titel der Section zugewiesen, der dann horizontal zentriert angezeigt wird.

Bei der Implementierung der getChildView Methode ist zusätzlich die Position in der jeweiligen Obergruppe zu berücksichtigen. Wie schon bei der getGroupView Methode greift

man zuerst mit dem Parameter groupPosition als Index auf die Liste der Section Objekte zu und kann damit auf die anzuzeigende Liste der Article Objekte zugreifen. Dort kann man sich mittels des Parameters childPosition das jeweilige Article Objekt holen und mit den darin enthaltenen Daten die Listenelemente befüllen. In unserem Fall haben wir einen Artikeltitel und einen Artikeluntertitel in zwei TextView Komponenten zuzuordnen. Diese sind anhand des ViewHolder-Patterns in einer speziellen Klasse deklariert. Diese ist in Codelisting 15 gezeigt:

```
private static class ChildViewHolder {
    public TextView tvTitle;
    public TextView tvSubTitle;
}
```

Codelisting 15 ChildViewHolder

Der in Codelisting 16 gezeigte Ausschnitt der getChildView Methode definiert dann die Zuordnung der Interfaceelemente:

```
if (convertView == null) {
    convertView = inflater.inflate(R.layout.index_child_row, null);
    holder = new ChildViewHolder();
    holder.tvTitle = (TextView)
convertView.findViewById(R.id.index_tv_child_title);
    holder.tvSubTitle = (TextView)
convertView.findViewById(R.id.index_tv_child_subtitle);
    convertView.setTag(holder);
} else {
    holder = (ChildViewHolder) convertView.getTag();
}
holder.tvTitle.setText(title);
holder.tvSubTitle.setText(subTitle);
```

Codelisting 16 Zuordnung der Interfaceelemente

Abbildung 5-2 illustriert dann das Aussehen dieser aufklappbaren Liste im zusammengeklappten Zustand, Abbildung 5-3 zeigt den auseinandergeklappten Zustand:

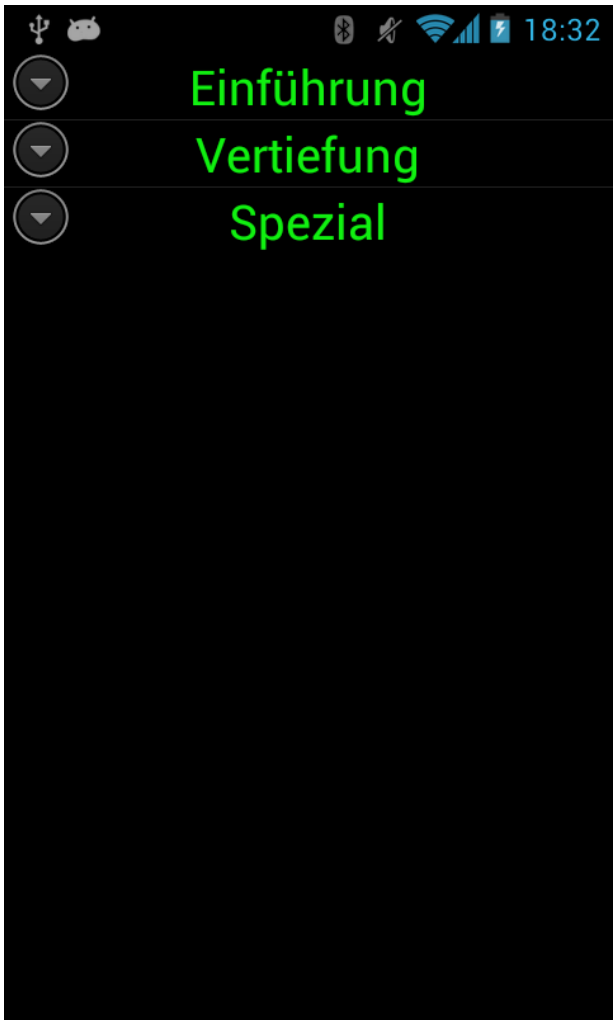

Abbildung 5-2 Sections in ExpandableListView zusammengeklappt

Abbildung 5-3 Sections mit Artikeln in auseinandergeklappter Liste

Zu jedem Artikeleintrag existiert noch eine Detailansicht, die vom Artikel in der Prototypenversion den Titel, die Autoren und den Text aus dem Abstract anzeigt. Die Detailansicht wird mittels onChildClickListener der ExpandableListView aufgerufen. Hierfür muss eine Methode onChildClick implementiert werden, die durch die Position auf die jeweiligen Daten verweist, um diese dann der Detailansicht zugänglich machen zu können. Eine Anwendung dafür ist in Codelisting 17 gezeigt:

```
listView.setOnChildClickListener(new
ExpandableListView.OnChildClickListener() {

    public boolean onChildClick(ExpandableListView listView, View view,
int groupPosition, int childPosition, long id) {
        Section section = sections.get(groupPosition);
        if (section != null) {
            List<Article> articles = section.getArticles();
            if (articles != null) {
                Article article = articles.get(childPosition);
                Intent intent = new Intent(IndexActivity.this,
ArticleActivity.class);
                intent.putExtra("article", article);
                startActivity(intent);
            }
         }
         return true;
    }
});
```

Codelisting 17 ExpandableListView onChildClick-Methode

Es ist ersichtlich, dass das jeweilige Artikelobjekt der neuen Intent zugewiesen wird. Normalerweise akzeptiert die Intent.putExtra Methode nur primitive Datentypen. Für komplexe Datentypen hat man zwei Optionen:

- Serializable
- Parcelable

Nutzt man das Interface Serializable für das jeweilige Objekt, dann übernimmt Java die Serialisierung des Objektes. Das ist unter herkömmlichen Java Anwendungen der einfachste Weg, da hier keine zusätzliche Implementierung mehr notwendig ist. Allerdings führt diese Methode unter ressourcenbegrenzten Systemen wie Android unter Umständen zu starken Performanceeinbußen, sowie möglicherweise zu Speicherproblemen bei größeren Objekten und deren größerer Anzahl. Deshalb gibt es die Möglichkeit, das Parcelable Interface zu implementieren, wodurch die Serialisierung der einzelnen Daten eines Objektes selbst bestimmt werden kann. Allerdings ist diese Parcelable-Variante nicht empfohlen, wenn man die Daten direkt persistieren will, da eine Systemänderung eine Inkompatibilität mit bisherigen Daten verursachen könnte (Android Developers, 2013).

Unter diesen Umständen ist die Verwendung von Parcelable jedoch angebracht und wurde auch umgesetzt. So implementieren alle transferierbaren Objekte, die in einem Article Objekt vorkommen die Methoden von diesem Interface.

5.2.3.5 NFC-Komponenten

Die Umsetzung der NFC-Komponenten bedient sich einer zusätzlichen Bibliothek Ndef-Tools, die die zu übertragenen Daten in eine höhere Abstraktionsebene stellt und daher die einfachere Übertragung von nativen Android NdefMessage ermöglicht. Diese Bibliothek stellt auch abstrakte Basisklassen für die Interaktion mit NFC zur Verfügung, die in diesem Prototypen auch verwendet werden. Der Quellcode für die vier abstrakten Basisklassen kann im Internet auf der Projektseite eingesehen werden: http://code.google.com/p/ndef-tools-for-

android/source/browse/ndeftools-util/src/org/ndeftools/util/activity/ - Zuletzt abgerufen am 24.4.2013

Die NFC-Funktionalität wurde in von obigen Basisklassen abgeleiteten Activities eingebaut, welche per Menütaste aus der Artikelansicht aufgerufen werden können. Implementiert wurden gemäß den Anforderungen drei voneinander unabhängige Funktionen:

- Android Beam
- Tag-Writer
- Tag-Reader

Der Menübildschirm der Artikelansicht zeigt Abbildung 5-4:

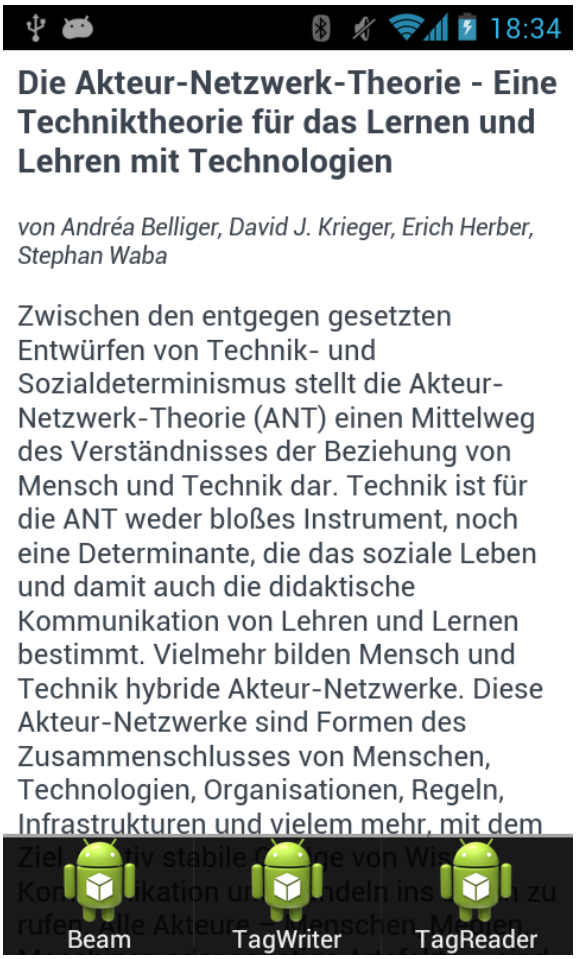

Abbildung 5-4 Artikelansicht mit Optionsmenü

5.2.3.5.1 Android Beam

Android Beam ist seit Version 4.0 für NFC-fähige Geräte verfügbar und dient zur einfachen Übertragung von Daten über NFC zwischen zwei Android Geräten. Sobald ein empfangsfähiges Gerät in Reichweite ist, wird auf beiden eine Vibration und eine Geräuschnotifikation ausgelöst. Der Benutzer wird auf dem Bildschirm angewiesen, diesen zu berühren, damit die Daten per Android Beam auf das andere Gerät transportiert werden. Diese Peer-to-Peer Übertragung wird über das Logical Link Control Protocol (LLCP) abgewickelt.

Grundsätzlich sollte vor dem Starten einer NFC-Aktion überprüft werden, ob das jeweilige Gerät NFC unterstützt. Hierfür kann man sich der Klasse PackageManager bedienen, wie Codelisting 18 zeigt:

```
PackageManager pm = getPackageManager();
if (!pm.hasSystemFeature(PackageManager.FEATURE_NFC)) {
    ...
}
```

Codelisting 18 Android PackageManager Featureüberprüfung

Die Initialisierung der NFC-Funktionalität sieht dann grob wie in Codelisting 19 beschrieben aus:

```
nfcAdapter = NfcAdapter.getDefaultAdapter(this);

nfcPendingIntent = PendingIntent.getActivity(this, 0, new Intent(this,
this.getClass()).addFlags(Intent.FLAG_ACTIVITY_SINGLE_TOP), 0);
IntentFilter tagDetected = new
IntentFilter(NfcAdapter.ACTION_TAG_DISCOVERED);
IntentFilter ndefDetected = new
IntentFilter(NfcAdapter.ACTION_NDEF_DISCOVERED);
IntentFilter techDetected = new
IntentFilter(NfcAdapter.ACTION_TECH_DISCOVERED);
writeTagFilters = new IntentFilter[]{ndefDetected, tagDetected,
techDetected};

nfcAdapter.enableForegroundDispatch(this, nfcPendingIntent,
writeTagFilters, null);

// Register Android Beam callback for creating (dynamic) messages to be
beamed
nfcAdapter.setNdefPushMessageCallback(this, this);

// you could also use the
// nfcAdapter.setNdefPushMessage(..)
// method to set a static message to be beamed

// Register callback to listen for message-sent success
nfcAdapter.setOnNdefPushCompleteCallback(this, this);
```

Codelisting 19 Android NFC-Initialisierung

Erstellt man nun eine Klasse, die bei diesem Prototyp von NfcBeamWriterActivity abgeleitet ist, werden die nötigen Callbacks automatisch eingerichtet, sobald man die startPushing und startDetecting Methoden aufruft. In unserem Fall ist das schon zum Activitystart gewünscht, also in der onCreate Methode. Die zu „beamenden“ Daten sind dann in der Methode createNdefMessage(NfcEvent event) zu erstellen, die dem Callback CreateNdefMessageCallback zugeordnet ist. Eine solche NdefMessage wird über das Ndef-Tools Framework über ein Message Objekt erstellt und sieht beispielsweise wie in Codelisting 20 gezeigt aus:

```
public NdefMessage createNdefMessage(NfcEvent event) {
    Log.i(TAG, "creating NdefMessage");

    Message message = new Message();
    message.add(new TextRecord("L3T recommends you the following
files:"));

    List<ArticleFile> articleFiles = article.getArticleFiles();
    if (articleFiles != null) {
        for (ArticleFile f : articleFiles) {
            message.add(new UriRecord(f.getUrl()));
        }
    }

    return message.getNdefMessage();
}
```

Codelisting 20 Methodendefinition von createNdefMessage

Das Message Objekt ist hier eine modifizierte ArrayList, die aus Objekten vom Typ Record aufgebaut ist. So ist es einfach möglich, aus bestimmten Datentypen bestimmte NdefRecords anzulegen, ohne sich mit unübersichtlichen Bytearrays herumschlagen zu müssen.

Der Prototyp transferiert vorerst nur eine Textmeldung und die URIs zu den im Artikel verlinkten Dateien, die die Empfängerin oder der Empfänger dann herunterladen kann. Generell sind hier noch weitere Datentypen möglich. Ein TextRecord Objekt wird dann in einen primitiven NdefRecord umgewandelt. Dies geschieht wie in Codelisting 21 beschrieben:

```
byte[] textData = text.getBytes(encoding);
byte[] payload = new byte[1 + languageData.length + textData.length];
byte status = (byte)(languageData.length |
(TextRecord.UTF16.equals(encoding) ? 0x80 : 0x00));

payload[0] = status;

System.arraycopy(languageData, 0, payload, 1, languageData.length);
System.arraycopy(textData, 0, payload, 1 + languageData.length,
textData.length);

return new NdefRecord(NdefRecord.TNF_WELL_KNOWN, NdefRecord.RTD_TEXT, id,
payload);
```

Codelisting 21 Umwandlung von TextRecord zu NdefRecord

Die Erstellung von TextRecords wird also durch diese Bibliothek deutlich vereinfacht und übersichtlicher gestaltet.

5.2.3.5.2 Tag-Writer

Der Tag-Writer implementiert die Funktionalität zum Beschreiben von NFC-Tags. Diese sind passiv, wodurch sich das Übertragungsprotokoll von dem bei Android Beam verwendeten LLCP unterscheidet. Es ähnelt zumeist dem RFID-Standard, wie schon in Kapitel 4.2 beschrieben.

Zur implementierung des Tag-Writers wird von der Ndef-Tools Bibliothek die abstrakte Klasse NfcTagWriterActivity zur Verfügung gestellt, die die von der implementierenden Klasse erhaltenen NdefMessage auf den NFC-Tag schreiben versucht, sobald ein NFC-Tag in der Nähe befindlich ist. Der Schreibvorgang kann auf zwei verschiedene Arten ablaufen.

- Formatierbarer NFC-Tag
- Unformatierbarer NFC-Tag

Ist ein Tag per Ndef automatisch formatierbar, kann man sich der in der Android API eingebauten format Methode der NdefFormatable Klasse bedienen. Diese ist aber nicht vom NFC-Forum spezifiziert, wie der Dokumentation der Klasse zu entnehmen ist (Android Developers, 2013).

Dies sieht dann wie in Codelisting 22 beschrieben aus:

```
Tag tag = intent.getParcelableExtra(NfcAdapter.EXTRA_TAG);
NdefFormatable format = NdefFormatable.get(tag);
if (format != null) {
    Log.d(TAG, "Write unformatted tag");
    format.connect();
    format.format(rawMessage);
}
```

Codelisting 22 Schreiben eines unformatierten Tags

Andernfalls muss die NFC-Forum konforme Variante umgesetzt werden, die den vorformatierten Tag erkennt und die NdefMessage auf diesem ersetzt, wenn er beschreibbar ist. Diese Lösung ist in Codelisting 23 gezeigt:

```
Ndef ndef = Ndef.get(tag);
if (ndef != null) {
    Log.d(TAG, "Write formatted tag");
    ndef.connect();
    ndef.writeNdefMessage(rawMessage);
}
```

Codelisting 23 Schreiben eines Ndef-formatierten Tags

Noch zu überprüfen wäre, ob der Tag beschreibbar ist und ob die NdefMessage Größe nicht das Fassungsvermögen des NFC-Tags übersteigt.

5.2.3.5.3 Tag-Reader

Der Tag-Reader implementiert die Funktionalität zum Auslesen passiver NFC-Tags. Hierfür müssen die zu lesenden Tagtypen definiert werden und ein entsprechender IntentFilter angelegt werden. Die Activitydefinition im Manifest ist in Codelisting 24 gezeigt:

```
<activity
    android:name=".ArticleNfcReaderActivity"
    android:label="Article"
    android:theme="@android:style/Theme.NoTitleBar"
    android:screenOrientation="portrait"
>
    <intent-filter>
        <action android:name="android.nfc.action.TECH_DISCOVERED"/>
        <category android:name="android.intent.category.DEFAULT"/>
    </intent-filter>
    <meta-data android:name="android.nfc.action.TECH_DISCOVERED"
android:resource="@xml/techlist" />
</activity>
```

Codelisting 24 Activitydefinition im Manifest

In diesem Fall verweist der Tagfilter auf eine externe XML Datei, die die verstandenen und unterstützten Tagtypen, auch als Techs bezeichnet, auflistet. Da in diesem Prototyp möglichst viele Techs unterstützt werden, ist die Liste verhältnismäßig ausführlich, wie eine beispielhafte Definition in Codelisting 25 zeigt:

```
<resources xmlns:xliff="urn:oasis:names:tc:xliff:document:1.2">
    <tech-list>
        <tech>android.nfc.tech.IsoDep</tech>
        <tech>android.nfc.tech.NfcA</tech>
        <tech>android.nfc.tech.NfcB</tech>
        <tech>android.nfc.tech.NfcF</tech>
        <tech>android.nfc.tech.NfcV</tech>
        <tech>android.nfc.tech.Ndef</tech>
        <tech>android.nfc.tech.NdefFormatable</tech>
        <tech>android.nfc.tech.MifareClassic</tech>
        <tech>android.nfc.tech.MifareUltralight</tech>
    </tech-list>
</resources>
```

Codelisting 25 XML Techliste für unterstützte Tag-Typen

Durch diese Liste an unterstützen Techs ist es möglich, abhängig vom verwendeten Tag gewisse spezifische Methoden anzuwenden. Dies kann unter Umständen sinnvoll sein, wenn man von der NFC-Forum Spezifikation abweichende Tags verwenden möchte, die besondere Funktionalitäten bereitstellen. Besondere Beachtung finden in der Android API die von NXP Semiconductors entwickelten Mifare Typen MifareClassic und MifareUltralight, da auf vielen früheren NFC-fähigen Androidgeräten NFC Chips von NXP Semiconductors verbaut wurden. Mifare Standard Tags in der Größe 1K und 4K weichen jedoch von der vom NFC Forum veröffentlichten Spezifikation für NFC Tags ab, wie Tabelle 4 zeigt:

	NFC Forum Platform			
	Type 1 Tag	Type 2 Tag	Type 3 Tag	Type 4 Tag
Compatible Products	Innovision Topaz	NXP MIFARE Ultralight / NXP MIFARE Ultralight C	Sony FeliCa	NXP DESFire / NXP SmartMX-JCOP
Memory Size	96 Bytes	48 Bytes / 144 Bytes	1, 4, 9 KB	4 KB / 32 KB
Unit Price	Low	Low	High	Medium / High
Data Access	Read/Write or Read-only	Read/Write or Read-only	Read/Write or Read-only	Read/Write or Read-only

Tabelle 4 NFC-Tag Kompatibilitätsliste **(NFC Forum, 2009)**

Die Inkompatibilität bestimmter Gruppen von NFC-Tags der verschiedenen Hersteller zu herstellerfremden Lesegeräten ist offensichtlich ein sehr großes Hindernis bei der Erschließung potentieller Einsatzgebiete für NFC. Diese Frage wird in Kapitel 6 in besonderem Bezug auf Lehr- und Lernunterlagen näher erörtert werden.

Das Auslesen eines NFC-Tags im Ndef-Format funktioniert über den zuvor beschriebenen IntentFilter und wird wie Codelisting 26 zeigt implementiert:

```
Parcelable[] messages =
intent.getParcelableArrayExtra(NfcAdapter.EXTRA_NDEF_MESSAGES);

if (messages != null) {
    NdefMessage[] ndefMessages = new NdefMessage[messages.length];
    for (int i = 0; i < messages.length; i++) {
        ndefMessages[i] = (NdefMessage) messages[i];
    }

    if (ndefMessages.length > 0) {
    // read as much as possible
    Message message = new Message();

    for (int i = 0; i < messages.length; i++) {
        NdefMessage ndefMessage = (NdefMessage) messages[i];

        for (NdefRecord ndefRecord : ndefMessage.getRecords()) {
            try {
                message.add(Record.parse(ndefRecord));
            } catch (FormatException e) {
                // if the record is unsupported or corrupted, keep as
unsupported record

                message.add(UnsupportedRecord.parse(ndefRecord));
            }
        }
    }
    readNdefMessage(message);
}
```

Codelisting 26 Auslesen einer NdefMessage

Dabei wird wieder die Ndef-Tools Bibliothek zum Parsen der NdefRecords verwendet, um eine vernünftige Objektrepräsentation der enthaltenen Daten zu erhalten. Im readNdefMessage Aufruf der implementierenden Klasse werden dann die erhaltenen Daten zur Darstellung übermittelt. Hierfür wird ein spezieller NdefAdapter angelegt, der das erhaltene Message Objekt übernimmt und die erhaltenen NdefRecords zwecks Analyse typisiert in einer Liste darstellt, wie Abbildung 5-5 zeigt:

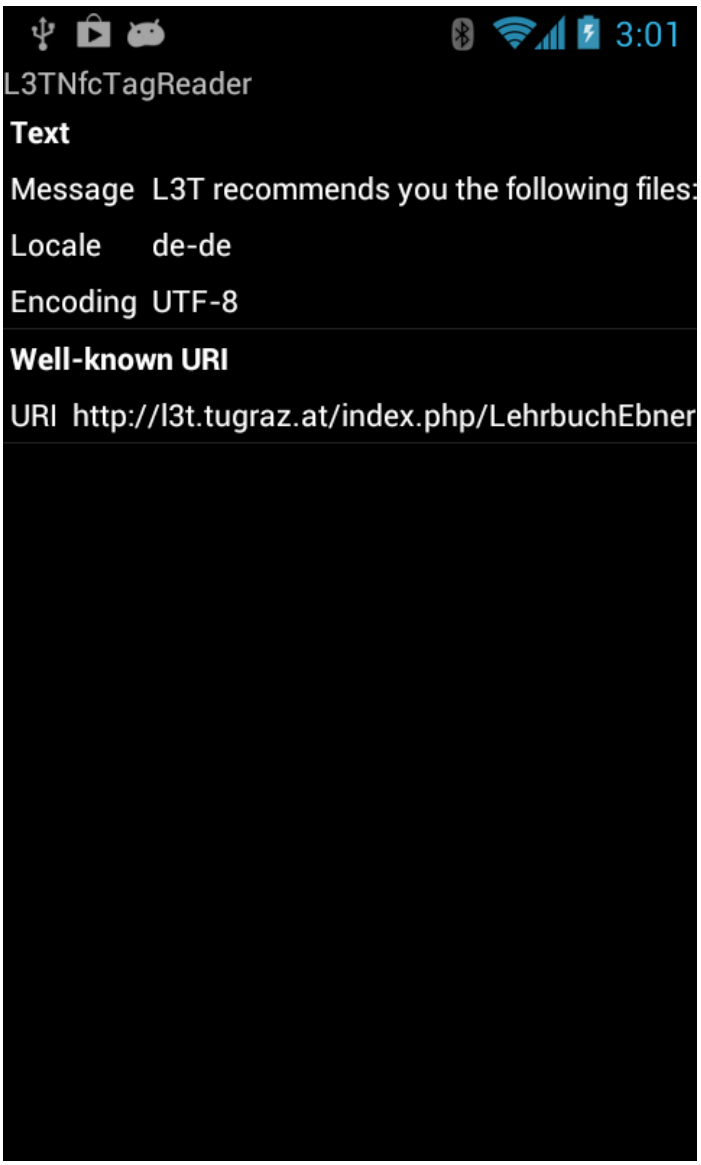

Abbildung 5-5 Tag-Reader Listenansicht mit Ndef Informationen

Durch einen Android spezifischen Application Record, kann man Geräte mit dieser App anweisen, die App zu starten und mit den über NFC erhaltenen Daten arbeiten. Dabei ist jedoch zu beachten, dass diese Android Application Records (AAR) erst mit der Android Version 4 eingeführt wurden. Der Ablauf für einen NFC-Tag mit einem AAR sieht folgende Schritte vor:

1.) Wenn die im AAR enthaltene Anwendung läuft: Ausführung einer Activity durch einen definierten IntentFilter
2.) Läuft die Anwendung nicht: Start der Anwendung des AAR

3.) Ist die im AAR angeforderte Anwendung nicht auf dem Gerät, wird Google Play mit dem Verweis der Anwendung aufgerufen

6 Potentiale von NFC für Lehr- und Lernunterlagen

In diesem Kapitel werden Potentiale von NFC für Lehr- und Lernunterlagen erläutert. Da es sich hierbei um Potentiale handelt, sind viele Einsatzgebiete bislang noch nicht näher erforscht, aber nach der durchgeführten Literaturrecherche und den ersten praktischen Tests höchst vielversprechend. Dennoch ist ihr Einsatz in Zukunft, wenngleich auch in einer etwas anderen Form, möglich.

Mobile Learning wird durch die fortschreitende Verbreitung mobiler Geräte immer wichtiger. Jüngere Generationen lernen meist schon sehr früh damit umzugehen und sehen ihre eigenen Möglichkeiten, wie sie die Geräte zum Lernen verwenden können. Dadurch ergeben sich derzeit größtenteils noch unausgeschöpfte Potentiale, die das m-Learning noch intensivieren und einen deutlichen Mehrwert für alle Beteiligten schaffen können.

Laut (Savill-Smith, Attewell, & Stead, 2006) ergibt sich folgender Mehrwert durch m-Learning:

„The value of mobile learning

Tutors commented on the value of mobile learning as follows.

- *It is important to bring new technology into the classroom.*
- *Mobile learning could be utilised as part of a learning approach which uses different types of activities (or a blended learning approach).*
- *Mobile learning supports the learning process rather than being integral to it.*
- *Mobile learning needs to be used appropriately, according to the groups of students involved.*
- *Mobile learning can be a useful add-on tool for students with special needs. However, for SMS and MMS this might be dependent on the students' specific disabilities or difficulties involved.*
- *Good IT support is needed.*
- *Mobile learning can be used as a 'hook' to re-engage disaffected youth.*
- *It is necessary to have enough devices for classroom use."*

In obiger Studie wurden im m-Learning Kontext Lernspiele entwickelt, die auf SMS basieren. Dabei wird die Bedienbarkeit der Geräte vorausgesetzt. Ebenfalls sind nur SMS und MMS gewisse technologische Einschränkungen gegeben. Ein großes Problem von m-Learning ist die Verbindung von digitalen Unterlagen und gedrucktem Material. Mit NFC bietet sich eine Technologie an, mit der dieser Medienbruch überbrückt werden kann. Diese soll als Schnittstelle dienen und digitale und gedruckte Inhalte sinnvoll miteinander verknüpfen.

Dabei stehen derzeit (Stand April 2013) jedoch noch einige Hindernisse im Weg, wie Inkompatibilität gewisser NFC-Tags und den NFC-Chips. So funktionieren natürlich von NXP Semiconductors hergestellte Tags mit deren hauseigenen Chips prächtig, während andere Chips von denen nicht lesbar sind, obwohl die Daten selbst in einem einheitlichen Format, wie beispielsweise Ndef, gespeichert wurden. So ein Fall tritt aktuell bei MifareClassic Tags (mit Größen von 1K und 4K) auf. In einem Nexus S befindet sich ein NXP Semiconductors NFC-Chip, in einem Nexus 4 allerdings einer des Herstellers Broadcom. Obwohl die Google Nexus Serie als Referenzmodell bei ihren jeweiligen Androidversionen gilt, treten hier Inkompatibilitäten auf. Diese sollen aber nicht hinderlich für die Definition einiger Potentiale sein, da diese vorerst ohnehin nur theoretischer Natur sind.

Die nun folgenden Beispiele gründen auf den gewonnenen ersten Erkenntnissen des Autors, die während dieser Masterarbeit entstanden sind.

6.1 Distribution von Unterlagen

NFC kann dazu verwendet werden, Lehr- und Lernunterlagen zu verteilen. Hierzu folgendes Szenario:

Der Lehrende möchte aktuelle Unterlagen in seinem Raum verteilen, es steht aber kein IP-basierendes Netzwerk zur Verfügung, wodurch es nicht möglich ist, die Unterlagen auf einen Webserver hochzuladen. Anwesend sind 300 Studierende, die die Unterlagen gerne in digitaler Form hätten, um sie für etwaige Übungen verwenden zu können. 300 gedruckte Kopien sind zwar theoretisch schnell verteilbar, aber stellen einen nicht außer Acht zu lassenden Kostenfaktor dar.

Der Lehrende könnte nun bequem seinen NFC-Tag im Vorfeld mit der URL für die gewünschen Unterlagen bespielen und die Studierenden können diese dann durch einfaches Darüberstreifen mit ihrem NFC-fähigen Gerät abrufen. Da NFC-Tags verhältnismäßig oft wiederbeschreibbar sind, wird eine signifikante Kostenreduktion bei der Distribution von Unterlagen erreicht.

Durch die Möglichkeit von Authentifizierungsverfahren sind die NFC-Tags vor unter Umständen auch scherzhaft gemeinten Manipulationen geschützt.

6.2 Zusatzinformationen zu Unterlagen

Aber auch zur Bereitstellung von zusätzlichen Informationen kann NFC verwendet werden. In Zukunft werden Smartphones oder Tablets bzw. deren Nachfolger eine weitaus größere Rolle spielen als bisher. Durch NFC können mehrere Benutzerinteraktionen generell vereinfacht und zu einem simplen Berühren eines Tags zusammengefasst werden. Stellt ein Lehrender beispielsweise ein Video in seiner Lehreinheit vor, ist er auf das Vorhandensein der notwendigen Endgeräte angewiesen, die einen erheblichen Kostenfaktor im Budget darstellen können. Durch die Verfügbarkeit von NFC ist es möglich, direkt einen Videolink aufzurufen und das Video direkt am Benutzergerät abzuspielen und gegebenenfalls auch zu Speichern. Dies gilt natürlich auch für andere externe Informationen, die nicht mit den urspünglichen Unterlagen mitgeliefert werden können.

In diesem Fall bringt der Lehrende an seinen Skripten an den gewünschten Stellen NFC-Tags an, die die Schnittstelle zu den Informationen darstellen. So können die Studierenden bequem ohne eine URL eingeben zu müssen auf die Inhalte zugreifen, indem sie lediglich den Tag berühren.

6.3 Teilen von Unterlagen

Durch Features wie Android Beam ist es bereits ohne zusätzliche Einstellungen möglich, zwischen Geräten unkompliziert Daten über NFC auszutauschen. So könnten beispielsweise Studierende, nachdem sie die Unterlagen, oder auch nur deren URLs, schon auf ihrem Gerät haben, diese mit anderen Studierenden direkt teilen, bzw. weiterleiten. Es ist einfach möglich, einer Anwendung eine solche Fähigkeit hinzuzufügen und die Benutzung jener stellt auch für wenig technisch affine Personen keine Schwierigkeit dar.

Für größere Inhalte empfiehlt sich allerdings über NFC eine andere Verbindung, wie zum Beispiel Bluetooth, aufzubauen, da NFC in der derzeitigen Spezifikation nicht mehr als 424kbit/s Bandbreite nutzen kann, wie aus der Spezifikation in Kapitel 4.2 ersichtlich ist. Durch den Verbindungsaufbau über NFC entfällt eine zusätzliche Wartezeit für die Genehmigung über Bluetooth, was die Gesamtzeit einer Übertragung deutlich reduzieren kann. NFC selbst ist durch die geringe Reichweite nicht für die Übertragung größerer Inhalte konzipiert worden, da dies eine längerfristige physische Nähe der beiden Endgeräte voraussetzt.

6.4 Abgeben von Übungen

Durch NFC-Tags ist es möglich, vorgefertigte Interaktionen auszuführen. Somit könnten Studierende ihre Aufgaben am Ende einer Übungseinheit über ihr NFC-fähiges Gerät „abgeben“. Der NFC-Tag hält die dafür notwendigen Informationen über die Abgabemaske, das Endgerät stellt Informationen über den Studenten bereit (Matrikelnummer, Lehrveranstaltung etc.) und überträgt diese über einen bestimmten Weg, der auf dem NFC-Tag definiert ist. Die Abgabe selbst kann dann beispielsweise über eine Email erfolgen, in die die relevanten Informationen automatisch eingetragen werden. Somit ist es nicht mehr nötig, auf dem Gerät eventuell mühsame und zeitaufwendige Aktionen durchzuführen, da alles mit der Berührung des NFC-Tags erledigt wird.

An der Gegenstelle sind dann durch die NFC-Interaktion zusätzliche Informationen abrufbar, die die Identifikation des Studierenden einfach möglich macht und dadurch eine bessere Zuordnung bei eingehenden Emails ermöglicht.

6.5 Integration sozialer Netzwerke

Eine weitere Möglichkeit wäre die Integration sozialer Netzwerke. In dem Fall ist natürlich nicht ein öffentliches Netz wie Facebook oder Google+ gemeint, sondern ein geschlossenes, lokales Netz, das einen zusätzlichen Kanal zum Austausch von Wissen bei Lernunterlagen bieten kann. Man kann dies als eine Art Verknüpfung mit einem Lesezeichen-System verstehen, das das Teilen einzelner Sätze vereinfachen soll.

Eine Studentin oder ein Student kann auf seinem Gerät einen gewünschten Abschnitt markieren und setzt dafür ein Lesezeichen, das auf diesen Abschnitt verweist. Nun kann ein anderer seine Sammlung von Lesezeichen durch ein einfaches Lesezeichen-Sharing über NFC erweitern und diese Lesezeichensammlung in einem Lern-Netzwerk publizieren. Damit können für Prüfungen besonders relevante Absätze genau markiert werden und eine gesammelte Ausarbeitung erstellt werden. Dies würde einer Lerngruppe von Studierenden ermöglichen, die auszuarbeitenden Kapitel aufzuteilen und gesondert auszuarbeiten. Durch eine simple Berührung der Endgeräte wird dann die zusammengefasste Ausarbeitung erstellt.

6.6 Zugangskontrolle von Unterlagen durch NFC

Durch die Möglichkeit der Zugangskontrolle durch simple Authentifizierungsverfahren über NFC, könnte der ansonsten eingeschränkte Zugang auch zu Teilen von Unterlagen genehmigt werden.

NFC kann dabei hilfreich sein, eine einheitliche Zugangsmethode zu erstellen, die unabhängig vom eingesetzten System im Hintergrund ist. Ein manuelles Einloggen über eine nicht vor Phishing geschützte Loginmaske entfällt, da dies über die sichere Authentifizierung über NFC erfolgt.

Die Grundlage der Berechtigung kann dabei verschiedenste Ursachen haben. Will ein Lehrveranstaltungsleiter seine Unterlagen nur aktuell Anwesenden zugänglich machen, kann er das Auslesen eines NFC-Tags verlangen, der die Zugangsdaten für die weiteren Unterlagen hält und darauf verweist.

Zusätzlich dazu kann die Zugangskontrolle auch über eine etwaige Bezahlung erfolgen, die über NFC durchgeführt werden kann.

Durch eine permanente Zugangskontrolle könnte der Lehrende jederzeit überprüfen, wer wann welche Unterlagen geöffnet hat. Die daraus resultierenden Daten können beispielsweise zur Kontrolle des Lernerfolges verwendet werden, wodurch ein Lehrender die Unterlagen gegebenenfalls entsprechend anpassen kann. Somit wäre eine generelle Aufwandsabschätzung für ein positives Absolvieren der Lehrveranstaltung möglich, was bei der Bemessung im ECTS-Verfahren hilfreich sein könnte.

6.7 Prüfungen

NFC kann den bereits vorhandenen Ausweis ersetzen, bzw. ergänzen. In diesem Fall könnte der Prüfer die Identität über NFC verifizieren und erhält durch die Vernetzung mit dem Verwaltungssystem Informationen, ob der Studierende überhaupt zur Prüfung zugelassen ist und bestätigt gleichzeitig dessen Anwesenheit. Dadurch wäre eine Papierlistenführung nicht mehr notwendig, was die Verwaltung bei Prüfungen mit großer Teilnehmerzahl erheblich erleichtern und beschleunigen kann.

NFC kann auch bei Prüfungen eingesetzt werden, bei denen digitale Unterlagen erlaubt sind. Durch NFC kann ermittelt werden, wer bei der Prüfung auf welchen Abschnitt der Unterlagen zugreift und die in den Unterlagen verbrachte Zeit messen. Diese könnte man dann in

Relation zur Prüfungsantwort stellen und entsprechende Rückschlüsse auf das Verständnis des betreffenden Kapitels ziehen.

Bei der Prüfungsabgabe kann dann ein NFC-Tag beschrieben werden, der obige Informationen speichert, wodurch die Daten längerfristig abrufbar wären. Zusätzlich dazu können beim Abfragen dieser Tags auch Resultate in verwandten Lehrveranstaltungen aufbereitet angezeigt werden, die den Beurteilenden bei der Bewertung hilfreich sein können.

6.8 Zusammenfassung

In diesem Kapitel wurden Potentiale und ihre Umsetzungsmöglichkeiten gezeigt. Einen zusammenfassenden Überblick ist in Tabelle 5 gezeigt:

Potential	Umsetzung
Distribution von Unterlagen	NFC-Tag mit URL zu Unterlagen
Zusatzinformationen zu Unterlagen	NFC-Tag mit URL für Integration externer Medien
Teilen von Unterlagen	Peer-to-Peer Kommunikation zwischen Geräten
Abgeben von Übungen	NFC als Schnittstelle zur automatischen Abgabemaske
Integration sozialer Netzwerke	NFC zur Unterstützung von Lerngruppen durch die direkte Verteilung von Lesezeichen in sozialen Netzen
Zugangskontrolle zu Unterlagen	Verknüpfung von Bezahlfunktion und Sicherungsfunktion zum Zugänglichmachen von Unterlagen
Prüfungen	NFC als Schnittstelle für den Identitätsnachweis, sowie Kontrolle bei Zugriffen auf erlaubte Unterlagen

Tabelle 5 Potentiale und ihre Umsetzungsmöglichkeit

7 Ausblick

Mit NFC wurde eine gute Methode zur Kommunikation zwischen zwei Endpunkten entwickelt, die wegen ihres Konzepts auch als verhältnismäßig sicher gilt, sofern die Spezifikation und Rahmenbedingungen eingehalten werden. Wie auch bei anderen Technologien existieren auch bei NFC, wie in den Unterkapiteln von Kapitel 4.3 beschrieben, noch viele Schwachpunkte, denen in Zukunft mehr Beachtung geschenkt werden muss, um der Technologie zu einem weltweit beliebten Standard zu verhelfen.

NFC gilt keinesfalls als Konkurrenz zu Bluetooth oder auch WLAN, sondern bietet viele Integrationsmöglichkeiten für andere Technologien. Diese Abgrenzung muss noch deutlicher propagiert werden, damit keine Missverständnisse aufkommen können, die zu eventuellen Fehleinsätzen von NFC führen könnten. Nur so kann man die Verbreitung dieser Technologie vorantreiben und dadurch auch neue Einsatzgebiete finden.

7.1 Aktuelle Trends

NFC verbreitet sich derzeit (Stand April 2013) auf vielen Betriebssystemen rasant. Neue Geräte haben mittlerweile meist einen NFC-Chip integriert. Der Smartphone- und Tabletmarkt wächst besonders schnell, wodurch die Fluktuation bei den Geräten auch bei Personen, die bereits ein Smartphone besitzen, groß ist. Dies dürfte wohl in den nächsten Jahren zu einem NFC-Boom führen, der ein großflächiges Einsetzen dieser Technologie auch wirtschaftlich sinnvoll macht.

Derzeit (Stand April 2013) erfährt NFC allerdings auch einigen Widerwillen einiger Gerätehersteller. So sieht beispielsweise Apple keinen großen Nutzen von NFC in ihren Geräten für ihre Kunden, wie derStandard.at berichtet (Schiller, 2012).

Es bleibt abzuwarten, ob sich diese Einstellung noch ändert, oder ob ein vollständig anderer Weg eingeschlagen wird, der möglicherweise eine Eigenentwicklung in Anlehnung an NFC vorsieht.

Besonders im bargeldlosen Zahlungsverkehr kann NFC eine führende Rolle einnehmen, da Smartphones sich immer größerer Beliebtheit erfreuen. Das Smartphone übernimmt dann die Zahlungsvorgänge, die bislang beispielsweise mit Kreditkarten oder Bankomatkarten vorgenommen wurden. Der Vorteil liegt in der elektronischen Signaturmöglichkeit, die eine Identifikation im selben Vorgang möglich macht, wodurch eine gesicherte Transaktion durchgeführt werden kann.

Dennoch bietet NFC weitaus größere Möglichkeiten, die nicht nur auf Bezahlsysteme beschränkt sind. Dabei ist natürlich die Einhaltung und Erweiterung internationaler Standards zwingend notwendig, da ansonsten keine für die Globalisierung geeignete Anwendung durchsetzbar ist.

Soziale Netzwerke erfreuen sich derzeit einer großen Beliebtheit. NFC kann daher als Schnittstelle für Printmedien dienen, um die Barriere zwischen Online- und Offlinemedien zu überwinden. Dadurch kann ein größerer Vernetzungsgrad erreicht werden, der den Anwendern zugute kommen soll.

Allerdings sind in allen Anwendungsfällen die möglichen Risiken nicht zu vernachlässigen. Technische Risiken birgt zwar praktisch jede Technologie, jedoch kommen durch die Verbindung von Online- und Offlinewelten durch NFC weitere Risiken hinzu, wie beispielsweise Datenschutzprobleme.

Mobile Tagging könnte sich durch NFC noch weiter verstärken. Anstelle von QR-Codes könnten zu Marketingzwecken NFC-Tags verwendet werden, die weitaus größere Datenmengen mitliefern können und zusätzlich eine Identifikation des Auslesenden möglich machen.

7.2 Möglichkeiten für zukünftige Forschungsarbeiten

Ein interessanter Forschungsbereich für den Einsatz von NFC bietet sich bei der Verarbeitung und Verwaltung von Personendaten. So zum Beispiel in der Gesundheitstelematik: Es ist zu hinterfragen, wie NFC die Erfassung und Verwaltung von Patientendaten erleichtern oder effizienter gestalten kann. Durch die weitreichenden Fähigkeiten von NFC wäre nicht nur die simple Identifikation eines Patienten möglich, sondern auch dessen Begleitung auf dem Weg durch eine Krankenanstalt, oder auch im extramuralen Bereich. Dabei kann das Smartphone die Funktion der bereits vorhandenen e-Card übernehmen und zusätzlich erweitern. Aber auch auf der medizinisch-technischen Seite gibt es mögliche Anwendungsszenarien, wie beispielsweise die Steuerung der medizinischen Geräte mit gleichzeitiger Übertragung relevanter Daten zur Zentrale.

Der in Kapitel 5 vorgestellte Prototyp bietet derzeit nur die Basisfunktionalität. Er könnte aber als Grundlage für weitere Entwicklungen im Bereich der Lehr- und Lernunterlagen dienen. So könnte die multimediale Vernetzung erprobt werden, indem das Smartphone per NFC Verbindungen anderer Art unterstützt und damit multimediale Geräte steuert. Dabei können auf dem Smartphone spezifische Daten gespeichert sein, mit denen Voreinstellungen auf den anderen Geräten automatisch aktiviert werden können. Somit wäre eine Umschaltung von verschiedenen Betriebsmodi komfortabel möglich. Es ist dabei zu hinterfragen, inwiefern NFC selbst Einfluss auf die Hardwaresteuerung haben kann.

8 Zusammenfassung und Fazit

In dieser Masterarbeit hat man sich eingehend mit der möglichen Verbindung zwischen Offline- und Onlineinhalten beschäftigt. Besonderes Augenmerk galt optischen Erkennungsverfahren wie QR-Code und deren Vorläufer, die in Kapitel 2 beschrieben wurden.

Als „Übergangstechnologie“ mit teilweise ähnlichen Einsatzmöglichkeiten wurde in Kapitel 3 RFID beschrieben, da dies als Basis für die im Kapitel 4 dieser Masterarbeit beschriebene NFC-Technologie dient. Dazu wurden in diesen Kapiteln Anwendungsfälle präsentiert, die die Vor- und Nachteile der jeweiligen Technologien näherbringen und gegenüberstellen.

In Kapitel 5 wurde die Implementierung des Prototypen gezeigt, der die Basisfunktionalität von NFC anhand eines praktischen Beispiels demonstriert. Es wurde dabei auch auf die Grundlagen eingegangen, da es sich bei NFC um eine noch nicht sehr weit verbreitete und bekannte Technologie handelt.

In Kapitel 6 wurde dann auf die Potentiale von NFC für Lehr- und Lernunterlagen eingegangen. Diese Potentiale beruhen auf gewonnenen Erkenntnissen und Ideen, die in Zukunft möglicherweise umgesetzt werden können.

Abschließend wurden in Kapitel 7 noch ein Ausblick für NFC beschrieben und auch einige Anregungen und Ideen für zukünftige Forschungsarbeiten in diesem Bereich gegeben.

Die während dieser Masterarbeit gewonnenen Erkenntnisse sind sehr interessant und regen definitiv zur weiteren Beschäftigung mit NFC an. Die Technologie bietet großes Potential, das jedoch leider derzeit noch nicht ansatzweise ausgeschöpft wird. Auch wenn die Entwicklung vieler Technologien in heutiger Zeit sehr schnell voranschreiten, wird NFC wohl noch mehrere Jahre brauchen, bis die Technologie sich einigermaßen Durchsetzen kann.

Der entstandene Prototyp ist noch in vielerlei Hinsicht weiterentwickelbar, bietet aber ein gutes Grundgerüst. Die NFC Entwicklung unter Android gestaltet sich als angenehm, nicht zuletzt auch durch die verwendete Bibliothek Ndef-Tools (siehe: (Skjolberg, 2013)). Dafür geht ein spezieller Dank an den Entwickler Thomas Rorvik Skjolberg.

Die breitgefächerten Anwendungsbeispiele für NFC verdeutlichen das Potential, aber auch die mit der Technologie verbundenen Risiken und Probleme. Besonders im Zahlungsverkehr müssen definitiv weitreichendere Rahmenbedingungen geschaffen werden, damit die Technologie bereits gewohnte Zahlungsmethoden, wie Kreditkarte oder Bankomat, ablösen kann.

In Bezug auf die Potentiale für Lehr- und Lernunterlagen ist zu sagen, dass die gebrachten Beispiele nur einen Auszug der Möglichkeiten zeigen, aber auch die vorherrschenden Probleme aufzeigen. Das NFC Forum ist zumindest eine gute Basis für die Entwicklung international einheitlicher Standards, um die Verbreitung voranzutreiben. Dabei ist noch zu beachten, dass das „Erbe“ von der RFID-Technologie einigermaßen ausgemistet werden kann, damit die NFC-Technologie in der globalisierten Welt sinnvoll einsetzbar wird. Mit RFID ist das durch die unterschiedlichen Standardisierungen, abhängig vom Kontinent oder Ländergruppe, nur eingeschränkt möglich. Diese Probleme manifestieren sich bei NFC auch in der Kompatibilität von NFC-Tags und den in Smartphones verbauten NFC-Chips. Von NXP Semiconductors hergestellte NFC-Chips, einer davon beispielsweise in meinem Nexus S verbaut, kommen natürlich bestens mit dem MifareClassic System klar. Im Nexus 4 ist aber mittlerweile ein Broadcom NFC-Chip verbaut, der mit dem Mifare-spezifischen System natürlich nicht mehr viel anfängt. Diese Probleme gilt es noch zu beseitigen, bevor NFC sich weiter verbreiten kann.

9 Literaturverzeichnis

US5243655. (7. September 1993). Abgerufen am 14. Jänner 2013 von Espacenet: http://worldwide.espacenet.com/publicationDetails/biblio?CC=US&NR=5243655&KC=&FT=E&locale=en_EP

Bar Code & Label Layout Specification. (Jänner 2004). Abgerufen am 14. Jänner 2013 von Fedex: http://images.fedex.com/us/solutions/ppe/FedEx_Ground_Label_Layout_Specification.pdf

Mobile Tagging. (2007). Abgerufen am 18. April 2013 von Wikipedia: http://en.wikipedia.org/wiki/File:Codes4.png

QR Code Usage In Japan. (18. Mai 2009). Abgerufen am 11. März 2013 von cliffano.com: http://blog.cliffano.com/2009/05/18/qr-code-usage-in-japan/

L3T eBook. (23. Februar 2012). Abgerufen am 29. April 2013 von iTunes Preview: https://itunes.apple.com/at/app/l3t-ebook/id465439895?mt=8

QArt Codes. (12. April 2012). Abgerufen am 17. März 2013 von swtch.com: http://research.swtch.com/qart

e-Plate. (2013). Abgerufen am 26. Februar 2013 von e-Plate.com: http://www.e-plate.com/

GTIN (EAN-Code). (2013). Abgerufen am 14. Jänner 2013 von code-knacker.de: http://www.code-knacker.de/gtin.htm

PDF417 bar code. (2013). Abgerufen am 14. Jänner 2013 von ITWissen: http://www.itwissen.info/definition/lexikon/PDF417-PDF417-bar-code.html

Speedpass. (2013). Abgerufen am 20. April 2013 von speedpass.com: https://www.speedpass.com/

Strichcode. (2013). Abgerufen am 14. Jänner 2013 von Wikipedia: http://commons.wikimedia.org/wiki/File:Barcode_EAN8.svg

Touristische Anwendungsbeispiele für QR-Codes. (13. Jänner 2013). Abgerufen am 19. Februar 2013 von Touristiker.at: http://www.touristiker.at/tourismus-qr-codes/

US Patent Office. (2013). Abgerufen am 20. April 2013 von Google Patents: http://www.google.com/patents?id=vWJoAAAAEBAJ&printsec=abstract&zoom=4&source=gbs_overview_r&cad=0#v=onepage&q&f=false

Android Developers. (2013). *Android Activity Class Reference*. Abgerufen am 15. April 2013 von Android Dokumentation: https://developer.android.com/reference/android/app/Activity.html

Android Developers. (2013). *Android Security Topics*. Abgerufen am 15. April 2013 von Android Dokumentation: https://developer.android.com/guide/topics/security/permissions.html

Android Developers. (2013). *Making ListView Scrolling Smooth*. Abgerufen am 15. April 2013 von Android Developers: http://developer.android.com/training/improving-layouts/smooth-scrolling.html

Android Developers. (2013). *NdefFormatable Class Reference*. Abgerufen am 15. April 2013 von Android Developers: http://developer.android.com/reference/android/nfc/tech/NdefFormatable.html

Android Developers. (2013). *Parcel Class Reference*. Abgerufen am 15. April 2013 von Android Developers: http://developer.android.com/reference/android/os/Parcel.html

Android Developers. (2013). *Parsing XML Data*. Abgerufen am 15. April 2013 von Android Network Ops: http://developer.android.com/training/basics/network-ops/xml.html

ARGE DATEN. (18. Jänner 2005). *Einsatz von Funkchips (RFID) und Biometrie in EU-Reisepässen*. Abgerufen am 20. April 2013 von argedaten.at: http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=89742ati

Austrian Payments Council. (19. November 2012). *Stuzza Zahlschein.* Abgerufen am 18. April 2013 von stuzza.at: www.stuzza.at/11250_DE.pdf?exp=24562515967912&11250

Bluetooth. (2011). *Bluetooth 4.0 with low energy technology paves the way for Bluetooth Smart devices*. Abgerufen am 18. April 2013 von Bluetooth: http://www.bluetooth.com/Pages/low-energy.aspx

Bob Brewin. (2005). *Sidebar: RFID tags key to some cattle ID programs*. Abgerufen am 20. April 2013 von computerworld.com: http://www.computerworld.com/s/article/88687/Sidebar_RFID_tags_key_to_some_cattle_ID_programs

Clark, S. (18. August 2011). *Nokia releases Symbian Anna NFC update*. Abgerufen am 27. Februar 2013 von NFCWorld: http://www.nfcworld.com/2011/08/18/39164/nokia-releases-symbian-anna-nfc-update/

Denso Wave. (2013). *Error Correction Feature*. Abgerufen am 20. April 2013 von qrcode.com: http://www.qrcode.com/en/about/error_correction.html

Denso Wave. (2013). *Micro QR Code*. Abgerufen am 20. April 2013 von qrcode.com: http://www.qrcode.com/en/codes/microqr.html

Denso Wave. (2013). *Patents pertaining to the QR Code.* Abgerufen am 20. April 2013 von qrcode.com: http://www.qrcode.com/en/patent.html

Denso Wave. (2013). *QR Code Standardization*. Abgerufen am 20. April 2013 von qrcode.com: http://www.qrcode.com/en/about/standards.html

Denso Wave. (2013). *SQRC*. Abgerufen am 20. April 2013 von qrcode.com: http://www.qrcode.com/en/codes/sqrc.html

Denso Wave. (2013). *What is a QR Code?* Abgerufen am 20. April 2013 von qrcode.com: http://www.qrcode.com/en/about/

derStandard. (22. Oktober 2007). *Mobilkom startet mit Nahfunk-Handys*. Abgerufen am 8. April 2013 von derStandard.at: http://derstandard.at/3021536

DHL. (29. Dezember 2011). *RFID - so funktioniert's*. Abgerufen am 20. April 2013 von dp-dhl.com: http://www.dp-dhl.com/de/logistik_populaer/trends/rfid.html

Diffie, W., & Hellman, M. E. (22. Juni 1976). New directions in cryptography. *Information Theory, IEEE Transactions*, S. 644-654.

Dipl-Ingo. (8. April 2013). *Wikipedia DataMatrix*. Abgerufen am 29. April 2013 von Wikipedia: http://de.wikipedia.org/wiki/Datei:De-wiki_als_14x14_Data_Matrix_Code.png

Dobkin, D. (2. Oktober 2007). *RFID Basics: Backscatter Radio Links and Link Budgets*. Abgerufen am 26. Februar 2013 von EETimes: http://eetimes.com/design/microwave-rf-design/4018929/RFID-Basics-Backscatter-Radio-Links-and-Link-Budgets

Donau Universität Linz. (15. September 2012). *NFC in aller Munde*. Abgerufen am 8. April 2013 von donau-uni.ac.at: http://imb.donau-uni.ac.at/online-marketing-tools/neue-moglichkeiten-fur-nfc/

Ebner, M. (2008). *QR Code - the Business Card of Tomorrow?* Aachen: Shaker Verlag.

Google. (2013). *Google Wallet*. Abgerufen am 8. April 2013 von Google Wallet: http://www.google.com/wallet/index.html

GS1 Japan. (2009). *QR Code Overview & Progress of QR Code Applications.* Abgerufen am 11. März 2013 von gs1jp: http://www.gs1jp.org/pdf/001.pdf

Hancke, G. (2005). *A practical relay attack on ISO 14443 proximity cards.* Cambridge: University of Cambridge, Computer Laboratory.

Han-soft Corporation. (2013). *TBarcode2D_DataMatrix*. Abgerufen am 29. April 2013 von han-soft.com: http://www.han-soft.com/releases/barcode2d/documents/b_datamatrix.html

Haselsteiner, E., & Breitfuß, K. (Juli 2006). *Security in Near Field Communication (NFC) - Strengths and Weaknesses.* Abgerufen am 18. April 2013 von http://ece.wpi.edu/~dchasaki/papers/Security%20in%20NFC.pdf

heise online. (30. November 2004). *Implantierbare RFID-Chips breiten sich aus*. Abgerufen am 26. Februar 2013 von heise.de: http://heise.de/-118677

heise online. (27. August 2006). *Patientenidentifikation mit RFID-Chips*. Abgerufen am 26. Februar 2013 von heise.de: http://heise.de/-155883

Heise Online. (1. Juni 2008). *35 Jahre Barcode in Supermärkten*. Abgerufen am 14. Jänner 2013 von heise online: http://heise.de/-211487

Hildenbrand, J. (21. Dezember 2010). *Gingerbread feature: Near Field Communication*. Abgerufen am 27. Februar 2013 von Androidcentral: http://www.androidcentral.com/gingerbread-feature-near-field-communication

IDAutomation. (2013). *PDF417 Barcode FAQ & Tutorial*. Abgerufen am 20. April 2013 von IDAutomation.com: http://www.idautomation.com/barcode-faq/2d/pdf417/#Error_Correction_Levels

Intrepidus Group. (21. September 2012). *UltraReset – Bypassing NFC access control with your smartphone*. Abgerufen am 8. April 2013 von Intrepidus Group Mobile Security: http://intrepidusgroup.com/insight/2012/09/ultrareset-bypassing-nfc-access-control-with-your-smartphone/

Jamiroquai. (20. November 2011). *Win a Signed Framed Set List + Merch At The France Gigs*. Abgerufen am 10. April 2013 von Jamiroquai: http://www.jamiroquai.com/?content=133&article_id=10361

Kalinko. (1. August 2009). *RFID*. Abgerufen am 26. Februar 2013 von Wikipedia: http://commons.wikimedia.org/wiki/File:Transponder2.jpg

Kinsella, B. (7. September 2010). *Vail shows that Consumer RFID delivers a better experience*. Abgerufen am 18. März 2013 von odintechnologies.com: http://blog.odintechnologies.com/bid/51179/vail-shows-that-consumer-rfid-delivers-a-better-experience

Kubacki, R. (2013). *NBAndroid Project*. Abgerufen am 15. April 2013 von NBAndroid: http://www.nbandroid.org/

Kuch, A. (27. September 2012). *o2 setzt für kontaktloses Bezahlen auf NFC und Mastercard*. Abgerufen am April. 8 2013 von teltarif.de: http://www.teltarif.de/o2-telefonica-paypass-mpass-nfc-dg-verlag/news/48346.html

MacManus, C. (16. Jänner 2012). *Sony's SmartTags could change phone habits*. Abgerufen am 27. Februar 2013 von CNet News: http://news.cnet.com/8301-17938_105-57359901-1/sonys-smarttags-could-change-phone-habits/

Martin, C. (24. Februar 2012). *Orange pushes NFC with Quick Tap Treats*. Abgerufen am 27. Februar 2013 von The Inquirer: www.theinquirer.net/inquirer/news/2154880/orange-pushes-nfc-quick-tap-treats

Mastercard. (2013). *PayPass*. Abgerufen am 20. April 2013 von mastercard.com: http://www.mastercard.com/at/privatkunden/innovationen_paypass.html

NFC Forum. (24. Juli 2006). *NFC Data Exchange Format.* Abgerufen am 29. April 2013 von NFC Forum: http://www.nfc-forum.org/specs/spec_list/#ndefts

NFC Forum. (19. Mai 2009). *NFC Forum Announces Two New Specifications to Foster Device Interoperability and Peer-to-Peer Device Communication*. Abgerufen am 27.

Februar 2013 von NFC Forum: http://www.nfc-forum.org/news/pr/view?item_key=088d874025e1049cd9c772ea508f4630ebf079b8

NFC Forum. (1. April 2009). *NFC Forum Type Tags.* Abgerufen am 15. April 2013 von NFC Forum: http://www.nfc-forum.org/resources/white_papers/NXP_BV_Type_Tags_White_Paper-Apr_09.pdf

NFC Forum. (2013). *About the NFC Forum*. Abgerufen am 27. Februar 2013 von NFC Forum: http://www.nfc-forum.org/aboutus/

NFC Modulation & RF Signal. (kein Datum). Abgerufen am 19. März 2013 von Radio-Electronics.com: http://www.radio-electronics.com/info/wireless/nfc/near-field-communications-modulation-rf-signal-interface.php

Nöl'Sch. (21. Juni 2012). *Kreditkartenbetrug dank NFC-Technik leichtgemacht*. Abgerufen am 8. April 2013 von Nölsch.de: http://www.nölsch.de/2012/06/21/kreditkartenbetrug-dank-nfc-technik-leichtgemacht/

NXP Semiconductors. (kein Datum). *MIFARE Classic - a pioneer and front runner in contactless smart card ICs* . Abgerufen am 18. April 2013 von NXP Semiconductors: http://www.nxp.com/products/identification_and_security/smart_card_ics/mifare_smart_card_ics/mifare_classic/

ÖBB Postbus. (kein Datum). *NFC-Technologie bei Postbus*. Abgerufen am 10. April 2013 von postbus.at: http://www.postbus.at/de/Hilfe_und_FAQ/NFC/index.jsp

ORF. (30. September 2012). *Gräbercodes halten Erinnerung am Leben*. Abgerufen am 11. März 2013 von ORF.at: http://noe.orf.at/news/stories/2552480/

ORF. (30. Oktober 2012). *Handyshopping kurbelt Onlineumsätze an*. Abgerufen am 18. April 2013 von orf.at: http://orf.at/stories/2144034/2144269/

ORF.at. (2012). *Elektronischer Zahlschein*. Abgerufen am 19. Februar 2013 von ORF.at: http://orf.at/stories/2144034/2144035/

Ortiz, C. E. (Juni 2008). *An Introduction to Near-Field Communication and the Contactless Communication API*. Abgerufen am 27. Februar 2013 von Oracle: http://www.oracle.com/technetwork/articles/javame/nfc-140183.html

Pelly, N., & Hamilton, J. (2011). *How to NFC*. Abgerufen am 27. Februar 2013 von Google I/O: http://www.google.com/events/io/2011/sessions/how-to-nfc.html

Penfold, A. (2011). *RIM Scores MasterCard NFC Certification*. Abgerufen am 27. Februar 2013 von MobileMarketing Magazine: http://mobilemarketingmagazine.com/content/rim-scores-mastercard-nfc-certification

Prenner, T. (21. März 2011). *NFC-Fahrscheine bald auch für Nexus S verfügbar*. Abgerufen am 8. April 2013 von futurezone.at: http://futurezone.at/produkte/2303-nfc-fahrscheine-bald-auch-fuer-nexus-s-verfuegbar.php

QR Codes versus NFC Tags. (kein Datum). Abgerufen am 18. April 2013 von NearFieldCommunication.org: http://www.nearfieldcommunication.org/qr-codes.html

Rhea Wessel. (2. Dezember 2009). *Gerry Weber Sews In RFID's Benefits*. Abgerufen am 26. Februar 2013 von rfidjournal.com: http://www.rfidjournal.com/articles/view?7252

Rothacker, R. (27. September 2012). *Bank of America tests technology to pay with phones*. Abgerufen am 18. Februar 2013 von Reuters: http://www.reuters.com/article/2012/09/27/us-bankofamerica-mobile-idUSBRE88Q04R20120927

Sa, R. (Kein Datum). *Access control with mobile phones: the future with Near Field Communications*. Abgerufen am 8. April 2013 von Source Security: http://www.sourcesecurity.com/news/articles/co-3108-ga.5735.html

Samsung. (24. Oktober 2012). *SAMSUNG Mobile Expands NFC Capabilities with TecTile™ Version 3.0*. Abgerufen am 27. Februar 2013 von Samsung: www.samsung.com/us/news/20301

Savill-Smith, C., Attewell, J., & Stead, G. (2006). *Mobile learning in practice.* London: Learning and Skills Network.

Schiller, P. (13. September 2012). *Warum das iPhone 5 kein NFC-Modul hat*. Abgerufen am 20. April 2013 von derStandard.at: http://derstandard.at/1347492386654/Phil-Schiller-Warum-das-iPhone-5-kein-NFC-Modul-hat

Schmidt, J. (1. Juni 2009). *Fußball: Anpfiff zum RFID-Einsatz*. Abgerufen am 19. März 2013 von rfid-im-blick.de: http://www.rfid-im-blick.de/2009060155/fussball-anpfiff-zum-rfid-einsatz.html

Schön, S., & Ebner, M. (2013). *L3T - Lehrbuch für Lernen und Lehren mit Technologien*. Abgerufen am 10. April 2013 von L3T.eu: http://l3t.eu/homepage/

Siemens. (2013). *Ready For IDentification*. Abgerufen am 26. Februar 2013 von siemens.com: https://www.cee.siemens.com/web/at/de/industry/ia_dt/produkte-loesungen/branchenloesungen/RFID/Pages/Default.aspx

Skjolberg, T. R. (2013). *Ndef Tools for Android*. Abgerufen am 15. April 2013 von Google Code: http://code.google.com/p/ndef-tools-for-android/

Sony. (2013). *Sony Xperia SP Features*. Abgerufen am 18. April 2013 von Sony Mobile: www.sonymobile.com/at/products/phones/xperia-sp/features/

springwise. (18. Mai 2012). *3D QR codes*. Abgerufen am 17. März 2013 von springwise.com: http://webcache.googleusercontent.com/search?q=cache:TonzDw-K1e4J:www.springwise.com/retail/seoul-retailer-3d-qr-codes-sun-deliver-discounts-quiet-times/+&cd=1&hl=de&ct=clnk&gl=at&client=firefox-a

Squareup. (2013). *Using Square Wallet at Starbucks*. Abgerufen am 18. Februar 2013 von squareup.com: https://squareup.com/help/en-us/article/5039-using-square-wallet-at-starbucks

Stockman, H. (Oktober 1948). Communication by Means of Reflected Power. *Proceedings of the IRE*, S. 1196-1204.

Strauß, C., Scholz, J., Ebner, M., & Schmidmayr, P. (2009). Einsatz von Quick Response Codes für ortsbezogene Dienstleistungen. *Konferenzband Geoinformatik 2009*, (S. 57-63). Münster.

TU Graz. (18. Oktober 2012). *TU Graz für Bücherwürmer: Hauptbibliothek präsentiert sich in neuem Glanz.* Abgerufen am 18. März 2013 von tugraz.at: http://www.presse.tugraz.at/pressemitteilungen/2012/18.10.2012.htm

van der Togt, R., van Lieshout, E. J., Hensbroek, R., Beinat, E., Binnekade, J. M., & Bakker, P. J. (2008). *Electromagnetic Interference From Radio Frequency Identification Inducing Potentially Hazardous Incidents in Critical Care Medical Equipment.* Amsterdam: JAMA.

Violino, B. (2003). *Genesis of the Versatile RFID Tag*. Abgerufen am 26. Februar 2013 von rfidjournal.com: http://www.rfidjournal.com/articles/view?392

waazaa. (kein Datum). *ISO/IEC 15693 : Vicinity cards*. Abgerufen am 18. April 2013 von waazaa.org: http://www.waazaa.org/15693/

10 Abbildungsverzeichnis

Abbildung 2-1 Einige zweidimensionale Codes im Überblick (Mobile Tagging, 2007) 16
Abbildung 2-2 EAN8 Code (Strichcode, 2013) 17
Abbildung 2-3 GTIN-13 Code (GTIN (EAN-Code), 2013) 17
Abbildung 2-4 PDF417 Code Aufbau (PDF417 bar code, 2013) 18
Abbildung 2-5 DataMatrix-Code (Dipl-Ingo, 2013) 19
Abbildung 2-6 Barcode vs. QR-Code (Denso Wave, 2013) 21
Abbildung 2-7 QR-Code Fehlerkorrektur (Denso Wave, 2013) 21
Abbildung 2-8 QR-Code Positionierungsmuster (Denso Wave, 2013) 21
Abbildung 2-9 QR-Code Aufteilung (Denso Wave, 2013) 22
Abbildung 2-10 QR-Code shopping (ORF, 2012) 24
Abbildung 2-11 QR-Code Visitenkarte (Ebner, 2008) 24
Abbildung 2-12 Zahlschein mit QR-Code (Austrian Payments Council, 2012) 26
Abbildung 2-13 Security-QR-Code Visum in Japan (QR Code Usage In Japan, 2009) 27
Abbildung 2-14 QR-Code Gräbercodes (ORF, 2012) 29
Abbildung 2-15 Micro-QR-Code und QR-Code (Denso Wave, 2013) 29
Abbildung 2-16 iQR-Code (GS1 Japan, 2009) 30
Abbildung 2-17 iQR vs QR Code (GS1 Japan, 2009) 31
Abbildung 2-18 iQR und DataMatrix (GS1 Japan, 2009) 32
Abbildung 2-19 QArt QR-Code (QArt Codes, 2012) 33
Abbildung 2-20 QArt QR-Code mit Fehlerkorrektur (QArt Codes, 2012) 33
Abbildung 2-21 3D Skulptur QR-Code (springwise, 2012) 34
Abbildung 3-1 RFID-Patentskizze (Violino, 2003) 37

Abbildung 3-2 RFID-Transponder (Kalinko, 2009) 37

Abbildung 3-3 RFID-Tag (mit zusätzlich optischem Code) bei einem Rind (Bob Brewin, 2005)..... 41

Abbildung 4-1 NFC Übertragungsmodi (Ortiz, 2008)..... 46

Abbildung 4-2 NFC Manchester Code (NFC Modulation & RF Signal) 47

Abbildung 4-3 NFC Digitale Frequenzmodulation (NFC Modulation & RF Signal) 48

Abbildung 4-4 Fahrscheinentwerter mit NFC-Touchpoint (Donau Universität Linz, 2012) .. 50

Abbildung 4-5 NFC Smartposter Gewinnspiel, Jamiroquai (Jamiroquai, 2011)..... 52

Abbildung 5-1 Android Activity Lifecycle (Android Developers, 2013)..... 63

Abbildung 5-2 Sections in ExpandableListView zusammengeklappt 72

Abbildung 5-3 Sections mit Artikeln in auseinandergeklappter Liste 73

Abbildung 5-4 Artikelansicht mit Optionsmenü..... 75

Abbildung 5-5 Tag-Reader Listenansicht mit Ndef Informationen 81

11 Tabellenverzeichnis

Tabelle 1 QR-Code Standards (Denso Wave, 2013)..... 20

Tabelle 2 QR-Code Spezifikation (Denso Wave, 2013)..... 21

Tabelle 3 NFC Modulationsmodi (NFC Modulation & RF Signal) 47

Tabelle 4 NFC-Tag Kompatibilitätsliste (NFC Forum, 2009)..... 80

Tabelle 5 Potentiale und ihre Umsetzungsmöglichkeit..... 87

12 Codelistingverzeichnis

Codelisting 1 Geteilte UserID 61
Codelisting 2 Android Berechtigungsdefinition (Android Developers, 2013) 62
Codelisting 3 Android Layout Defnition 64
Codelisting 4 Android Zugriff auf einen Layoutidentifier 64
Codelisting 5 Android AsyncTask Hintergrundmethodensignatur 67
Codelisting 6 Android AsyncTask Hilfsmethodensignatur 67
Codelisting 7 Android AsyncTask Klassendefinition 67
Codelisting 8 Android AsyncTask Ausführungsbefehl 67
Codelisting 9 Android AsyncTask ProgressDialog 67
Codelisting 10 Android XmlPullParser Initialisierung 68
Codelisting 11 XML-Struktur eines Lehrbuchartikels 68
Codelisting 12 XML-Parser für Article-Objekte 69
Codelisting 13 Android ExpandableListView XML-Definition 70
Codelisting 14 Android ExpandableListView Initialisierung 70
Codelisting 15 ChildViewHolder 71
Codelisting 16 Zuordnung der Interfaceelemente 71
Codelisting 17 ExpandableListView onChildClick-Methode 74
Codelisting 18 Android PackageManager Featureüberprüfung 76
Codelisting 19 Android NFC-Initialisierung 76
Codelisting 20 Methodendefinition von createNdefMessage 77
Codelisting 21 Umwandlung von TextRecord zu NdefRecord 77
Codelisting 22 Schreiben eines unformatierten Tags 78
Codelisting 23 Schreiben eines Ndef-formatierten Tags 78
Codelisting 24 Activitydefinition im Manifest 79
Codelisting 25 XML Techliste für unterstützte Tag-Typen 79

Codelisting 26 Auslesen einer NdefMessage 80