Die approbierte Originalversion dieser Diplom-/Masterarbeit ist an der Hauptbibliothek der Technischen Universität Wien aufgestellt (http://www.ub.tuwien.ac.at).

The approved original version of this diploma or master thesis is available at the main library of the Vienna University of Technology (http://www.ub.tuwien.ac.at/englweb/).

MASTERARBEIT

Identifikation und Analyse sicherheitsrelevanter Kriterien für Mobile Contactless Payment-Systeme zur Förderung der Akzeptanz beim Endanwender

zur Erlangung des akademischen Grades

Magister

(Mag. rer. soc. oec.)

ausgeführt am

Institut für Rechnergestützte Automation

Forschungsgruppe Industrial Software

der Technischen Universität Wien

unter der Anleitung von

Univ.-Prof. Dipl.-Ing. Dr. techn. Thomas Grechenig und

Dipl.-Ing. Mag. Andreas Ehringfeld

durch

Yvonne Hren, BSc.

Wien, 27.04.2008

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Wien, am 29. April 2008 ----------

Yvonne Hren

Danksagung

Dank gilt

Univ.-Prof. Dipl.-Ing. Dr. techn. Thomas Grechenig für die Bereitstellung des Themas, Dipl.-Ing. Mag. Andreas Ehringfeld für die umfangreiche Betreuung, Herrn Florian Zauner sowie Frau Mag. Martina Lausmann für die konstruktive Kritik und das Korrekturlesen der Arbeit,

sowie allen, die mir während meines Studiums eine Stütze waren.

Wien, April 2008

Yvonne Hren

Kurzfassung

Das Mobiltelefon dient heutzutage neben seiner primären Funktion als Kommunikationsmedium zur Bereitstellung unterschiedlichster Informationen. Durch die Entwicklung der drahtlosen Near Field Communication (NFC) wurde nun zusätzlich die Nutzung als elektronische Geldbörse für mobile Bezahlung (M-Payment) realisiert.

Die vorliegende Arbeit beschäftigt sich zunächst mit den Grundlagen von Bezahlsystemen im Allgemeinen sowie gängigen Technologien zur Datenübertragung. Kern der Arbeit ist die Identifizierung möglicher Sicherheitsrisiken und die Erarbeitung von Kriterien, die für die Akzeptanz von M-Payment beim Endanwender wichtig sind. Basis für entsprechende Bewertungen waren vor allem Studien und Meinungsumfragen von Endanwendern über die Nutzung oder Ablehnung von M-Payment sowie Erhebungen zum Thema Sicherheitsrisiken im Bereich der Datenübertragung.

Im Rahmen der vorliegenden Arbeit konnte klar aufgezeigt werden, dass derzeit noch zahlreiche Sicherheitsrisiken bei der Nutzung von Mobile Contactless Payment, das ist M-Payment mittels NFC, bestehen. Als kritische sicherheitsrelevante Erfolgsfaktoren bei der Etablierung von Mobile Contactless Payment konnten folgende Parameter identifiziert werden: die sichere Kommunikation der Geräte, die Wahl des Trägermediums, der Einsatz einer geeigneten und ausgereiften Software, Prävention von Anwendungsfehlern, der vertrauliche Umgang mit Daten, die Sicherheit der Smart Card sowie die Einhaltung allgemein gültiger Sicherheitsaspekte.

Zusammenfassend konnte gezeigt werden, dass erst durch die Berücksichtigung dieser identifzierten Sicherheitskriterien die Endanwender-akzeptanz von Mobile Contactless Payment entscheidend erhöht werden kann, woran bisherige Projekte scheiterten.

Abstract

Mobile phones have developed from communication devices to multifunctional information portals. With wireless near field communication (NFC) they can now even be used as electronic purses to conduct mobile payments (m-payment).

The first part of this thesis covers the basics of payment methods and data transfer technologies. The main focus is on the identification of security threats and the development of a criteria catalogue that will help to increase consumer acceptance of mobile contactless payment. This catalogue is built on studies and surveys performed with mobile contactless payment users as well as scientific publications about security issues of data transfers.

This thesis shows that there are several unresolved security issues with mobile contactless payment that need to be addressed before a successful introduction is possible. Some of the major elements are secure communication, functional NFC devices (mobile phone, token, card…), technically mature software, prevention of application errors, protection of confidential information and also the compliance with renowned security standards.

Summarised it is shown, that only by complying with the criteria catalogue the acceptance of mobile contactless payment can be significantly increased.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Das Mobiltelefon ist neben seiner primären Funktion als Kommunikationsmedium mittlerweile auch ein Medium zur Informationsbereitstellung aller Art geworden. Geldgeschäfte oder Einkäufe können mittels mobiler Endgeräte an jedem Ort zu jeder Zeit erledigt werden. Immer mehr Nutzer wollen das Mobiltelefon als Alternative zu Geldbörse, Kreditkarte und Co. nutzen [MOBA04], weshalb M-Payment als eine der wichtigsten Applikationen des Mobile Commerce gesehen wird [UVRV02].

Mittels drahtloser Near Field Communication (NFC), die auf Radio Frequency Identification (RFID) aufbaut, werden neue Möglichkeiten eröffnet [ORTI06]. Diese Technologie ist vielseitig einsetzbar, so z.B. auch in Mobiltelefonen oder Kreditkarten, die zum drahtlosen Zahlungsmittel umfunktioniert werden sollen und als Mobile Contactless Payment bezeichnet wird.

Innerhalb der nächsten fünf Jahre erwarten die großen Kreditkartenfirmen wie MasterCard, Visa oder Amex, dass der weltweite Umsatz aus Mobile Contactless Payment per Mobiltelefon auf 36 Mrd. Dollar steigen wird [PATA06]. Eine wesentliche Voraussetzung für den Erfolg ist die Bereitstellung effizienter und sicherer Abwicklungsformen des Zahlungsvorganges [MOMA02]. Darüber hinaus spielt aber auch das Verhalten der Konsumenten eine wesentliche Rolle bei der Entwicklung und Erschließung des Mobile Contactless Payment Marktes. Selbst wenn die entsprechende Technologie bereits verbreitet ist, könnte es noch einige Zeit dauern, bis Mobile Contactless Payment zur Routine wird. Konsumenten werden noch an traditionellen Zahlungsmethoden festhalten, insbesondere dann, wenn nicht ausreichendes Vertrauen in die Sicherheit bei dem Zahlungsprozess gegeben ist. Dies betrifft vor allem Mobile Contactless Payment, also das Bezahlen mittels Mobiltelefonen und NFC.

Da Endanwender neuen Technologien gerade im Zahlungsverkehr sehr skeptisch gegenüberstehen, ist es besonders wichtig, die Bedürfnisse des Konsumenten genau zu kennen, um neue Lösungen erfolgreich zu etablieren [DAÖÖ07].

Der Trend geht immer mehr weg vom Bargeld in Richtung bargeldloses Bezahlen und der Zahlungsvorgang soll immer einfacher und bequemer werden [BRAN05]. Laut einer Statistik der Internationalen Telekommunikationsunion besitzt mittlerweile jeder fünfte Mensch ein Mobiltelefon und in Westeuropa liegt die Penetration von Mobilfunkgeräten bereits bei über 100 Prozent [INTE08]. Insofern liegt der Gedanke nahe, auch den Zahlungsverkehr über das Mobiltelefon zu ermöglichen. Aus diesem Grund haben renommierte Firmen wie Kreditkartenunternehmen und Mobilfunkanbieter nach neuen Möglichkeiten im bereich M-Payment gesucht.

Mobiltelefone sind heutzutage bereits sehr vielseitig. Man kann damit E-Mails schreiben und abrufen, fotografieren, Videos aufzeichnen u.v.m. Die Bankomat- oder Kreditkarte konnte es bislang allerdings noch nicht ersetzen. NFC ist eine Möglichkeit, durch intuitive Handhabung und drahtlose Datenübertragung, das einfache und rasche Bezahlen vor allem für kleinere Beträge übers Mobiltelefon zu ermöglichen.

Mit dieser Innovation sind jedoch auch viele Risiken verbunden. Sicherheit und einfache Handhabung stehen beim Endanwender an oberster Stelle [KEPO03] und sind neben zahlreichen anderen Faktoren, wie Kosten, Dauer des Zahlungsvorganges, etc. die Schlüsselkonzepte für eine erfolgreiche Reformierung des Zahlungsverkehrs.

Um eine entsprechend hohe Akzeptanz beim Endanwender zu erzielen, müssen potentielle Gefahren von Mobile Contactless Payment Systemen identifiziert, deren Risiken analysiert und anschließend daraus die notwendigen sicherheitstechnischen Kriterien abgeleitet werden. Da es zum einen in der Praxis keine absolute Sicherheit gibt, zum anderen die Kosten zur Höhe des Sicherheitsniveaus exponentiell steigen, darf der Kriterienkatalog nur jene Kriterien beinhaltet, die ein ausgewogenes Kosten - Nutzen Verhältnis darstellen. Da zumindest diese Kriterien für einen sicheren Betrieb von Mobile Contactless Payment Systemen gewährleistet sein müssen, spricht man von der Notwendigkeit der Einhaltung von Mindestkriterien [BSIF08].

1.1 Problemstellung

Forschungsfragen

- Welche nennenswerten M-Payment Systeme gibt es derzeit in Österreich?
- Welche zusätzlichen Gefahren treten beim Mobile Contactless Payment im Vergleich zu den derzeit eingesetzten Varianten auf?
- Fördern die im Rahmen der vorliegenden Arbeit identifizierten Mindestkriterien die Akzeptanz beim Endanwender?

1.2 Aufbau der Arbeit

Die Arbeit gliedert sich in zwei Teile. Im ersten Teil werden die theoretischen Grundlagen erarbeitet bzw. die Begriffe und Technologien erklärt. Im zweiten Teil werden die notwendigen sicherheitstechnischen Mindestkriterien zur Förderung der Akzeptanz des Endanwenders erarbeitet.

In Zuge dieser Arbeit werden nur jene Aspekte des Mobile Contactless Payments behandelt, die kundenseitig relevant sind, d.h. Kriterien, die für die Akzeptanz beim Endanwender wichtig sind, wie Sicherheit, Benutzer-freundlichkeit, u.v.m. Diese sind sehr oft konträr zu den Interessen anderer Parteien, jedoch wird letztendlich der Erfolg einer Technologie durch den Kunden gesteuert.

2 Grundlagen und Begriffsbestimmungen

Die Anfänge des Electronic Commerce (E-Commerce) gehen bis ins Jahr 1997 zurück, wo die US-Regierung ein Framework für Global Electronic Commerce vorstellte [ADOP05]. Es wurden die Hauptziele des Electronic Commerce in einem Dokument festgehalten und bereits wenige Jahre später konnte der Handel mittels Internet auf einem globalen Markt agieren und am Electronic Business (E-Business) teilnehmen.

2.1 Electronic Business

Die Begriffe Electronic Business, Electronic Commerce, Mobile Commerce oder Mobile Business sind Begriffe, die zunehmend häufiger in den verschiedensten Medien und in den unterschiedlichsten Zusammenhängen genannt werden. Der Einsatz mobiler elektronischer Kommunikationstechniken hat in den letzen zehn Jahren wesentlich an Bedeutung gewonnen. Die Mobilfunktechnologie hat ebenso wie das Internet eine rasante Entwicklung hinter sich und durch diese Schlüsseltechnologien entwickelte sich aus dem Electronic Commerce der Mobile Commerce.

Die Folgende Tabelle zeigt einige Definitionen zum Begriff Electronic Business [ADOP05].

Definitionen von **Electronic Business (E-Business)**	
Quelle	**Definition**
Franz-Joachim Kauffels (1999)	*… Unterstützung der Wertschöpfung im Unternehmen durch die Methoden der Verteilten Datenverarbeitung.*
Wolfgang von Kersten (2001)	*Electronic Business ist ein Überbegriff für die strategische Anwendung von computergestützten Informations- und Kommunikationstechnologien zur Erreichung der Unternehmensziele einschließlich der entsprechenden Ausgestaltung und Neuordnung von Geschäftsprozessen.*
Eberhard Holler (2001)	*… alle geschäftlich relevanten Vorgänge, die über Telekommunikationsnetze abgewickelt werden.*
Patrick Stähler (2001)	*E-Business schließt E-Commerce mit ein und integriert mittels neuer Medien sowohl die Austauschverhältnisse zwischen Unternehmen und Kunden bzw. Unternehmen und Geschäftspartnern als auch die internen Koordinationsmechanismen.*
Thomas Schildhauer (2002)	*Electronic Business (EB) umfasst alle Aktivitäten von Marktteilnehmern und Organisationen, deren Ziel es ist, aus digitaler Transaktion und Kommunikation wirtschaftlichen Nutzen zu sichern.*
Electronic Commerce Info Net (ECIN) (2005)	*Die Anbahnung und Abwicklung von geschäftlichen Transaktionen auf elektronischem Wege. Der Begriff E-Business … beschreibt dabei nicht nur die Prozesse, die über das Internet angestoßen werden, sondern bezieht auch alle Produkte und Dienstleistungen die zur Herleitung dieser Prozesse erforderlich sind in die Begriffsbildung mit ein.*
IBM (2005)	*Die Tranksaktion von Geschäftsvorgängen über ein elektronisches Medium wie das Internet.*

Tabelle 1- Definitionen von Electronic Business

Trotz dem die Definitionen sehr unterschiedliche Ansätze verfolgen, sind einige Gemeinsamkeiten festzustellen. Adam Opuchlik [ADOP05] definiert E-Business in Anlehnung an Bernd Wirtz Definition als *"Anbahnung, Unterstützung, Abwicklung und Aufrechterhaltung von Leistungsaustauschprozessen – also der Transfer von materiellen und immateriellen Gütern sowie Dienstleistungen zwischen unterschiedlichen Akteuren zumeist gegen ausgleichende monetäre oder nichtmonetäre Leistungen - durch elektronische Netze und Informations- und Kommunikationstechniken".*

2.2 Electronic Commerce

In der Literatur und im Sprachgebrauch werden die Begriffe E-Business und E-Commerce oft sinnverwandt verwendet. E-Commerce ist jedoch ein Teilbereich aus dem E-Business. Eine Analyse von Definitionen des Begriffes Electronic Commerce beinhaltet Tabelle 2 [ADOP05].

Definitionen von **Electronic Commerce**	
Quelle	**Definition**
Eberhard Holler (2001)	*Electronic Commerce beinhaltet die elektronische Unterstützung von Aktivitäten, die in direktem Zusammenhang mit dem Kauf und Verkauf von Gütern und Dienstleistungen via elektronischer Netze in Verbindung stehen.*
Kersten und Schröder (2002)	*E-Commerce steht für elektronischen Handel oder Einkaufsmöglichkeiten via Internet.*
Michael Merz (2002)	*Die Unterstützung von Handelsaktivitäten über Kommunikationsnetze.*
Rahild Neuburger (2003)	*Elektronische Unterstützung bzw. Abwicklung von Geschäftstransaktionen zwischen Unternehmen und seinen Kunden.*
Electronic Commerce Info Net (ECIN) (2005)	*Der wohl am weitesten verbreitete Begriff für den elektronischen Handel. Im Gegensatz zum E-Business beschreibt der E-Commerce im strengen Sinne nur diejenigen Prozesse bzw. Erträge, die unmittelbar aus oder über das Internet angestoßen werden. Hierzu zählen dann Dienstleistungen ebenso wie die vielschichtigen Transaktionen innerhalb des Zwischenhandels.*
Siemens E-Business Glossar (2005)	*E-Commerce ist ein Teilbereich des E-Business und der Oberbegriff für alle Arten von Transaktionen über elektronische Medien. Das Hauptmedium für E-Commerce ist das Internet, aber auch Standards wie EDI über firmeneigene Netze können für E-Commerce verwendet werden. Kauf-/Verkaufstransaktionen bilden die Hauptbestandteile des E-Commerce. Weitere Transaktionsbereiche umfassen Behörden und Bankgeschäfte.*
Adam Opuchlik (2005)	*Die Möglichkeit, Transaktionen im Absatz- und Beschaffungsbereich über elektronische Kommunikationsnetze zu unterstützen bzw. abzuwickeln.*

Tabelle 2 - Definitionen von Electronic Commerce erweiterte Version

Der Electronic Commerce wird von Bernd Wirtz [BEWI01] definiert als *„…die elektronische Unterstützung von Aktivitäten, die in direktem Zusammenhang mit dem Kauf und Verkauf von Gütern und Dienstleistungen via elektronischer Netze in Verbindung stehen“*. Als Beispiel für E-Commerce Aktivitäten nennt er das elektronische Aushandeln von Preisen oder die Unterzeichnung von Rechnungen mittels digitaler Signatur. Das Electronic Business beinhaltet Prozesse die über den An- und Verkauf von Produkten hinausgehen und stellt somit das umfassendere Konzept dar.

2.3 Mobile Business

Im Zeitalter der rasanten Entwicklung von Übertragungstechnologien und drahtlosen Endgeräten ist Mobile Business (M-Business) entstanden. Viele Wissenschafter schreiben dem M-Business vermehrt ein hohes Marktpotential zu. Ein wesentliches Faktum für die Prognosen ist die schnelle Verbreitung von Mobiltelefonen und PDAs. In Europa gab es bereits 2001 mehr Mobiltelefonbesitzer als Internet-Nutzer [BEWI01], was ein enormes Kundenpotential darstellt und Mobile Business zu einem interessanten Betätigungsfeld macht.

Ebenso wie beim E-Business gibt es keinen Konsens über die Definition des Begriffs M-Business. Allerdings besteht Einigkeit darüber, dass die Nutzung mobiler Endgeräte im Zusammenhang mit wirtschaftlichen Aktivitäten steht. Meist wird die Definition des Begriffs E-Commerce herangezogen und um die Inanspruchnahme mobiler Zugangsgeräte ergänzt, was auch die Unschärfe der Definitionen der Begriffe M-Business und M-Commerce erklärt.

Mobile Business ist ein Teilbereich des Electronic Business, wo eine bestimmte Art von Endgeräten eingesetzt wird, wobei eine Beschränkung lediglich auf die Zugangsgeräte nicht immer ausreichend ist.

Mobile Business ist dem E-Commerce untergeordnet [BSLF02] und beschreibt die Gesamtheit aller Aktivitäten, Prozesse und Anwendungen, die mit mobilen Technologien durchgeführt werden.

Bernd Wirtz [BEWI01] definiert Mobile Business als die *„Anbahnung sowie die teilweise respektive vollständige Unterstützung, Abwicklung und Aufrechterhaltung von Leistungsaustauschprozessen mittels elektronischer Netze und mobiler Zugangsgeräte“.*

2.4 Mobile Commerce

Die folgende Tabelle zeigt einige Definitionen zu dem Begriff Mobile Commerce in Anlehnung an [BEWI01].

Definitionen von **Mobile Commerce**	
Quelle	**Definition**
Durlacher Research (1999)	*The working definition of Mobile Commerce […] is any transaction with a monetary value that is conducted via a mobile telecommunication network.*
Andersen Consulting (2000)	*Mobile Commerce is Electronic Commerce based on mobile telephony, short-range wireless lines, voice recognition and interactive digital TV.*
Kehoe (2000)	*[…] mobile commerce – that is, electronic commerce conducted on mobile phones.*
Rößler (2000)	*[…] Mobile Commerce, also Wirtschaftskontakte über drahtlose Verbindungen an beliebigen Orten […]*
Schmitzer/ Butterwegge (2000)	*MC [Mobile Commerce] bezeichnet die wirtschaftliche Nutzung von mobilen Endgeräten, vor allem von Mobiltelefonen und PDAs.*
Wiedermann/Buxel/ Buckler (2000)	*Die elektronisch gestützte Abwicklung von Online-Geschäftsfällen auf Basis der Nutzung mobiler Endgeräte wird als Mobile Commerce (kurz: M-Commerce) bezeichnet.*
E-Commerce Wissen [XOVE07]	*E-Commerce umfasst somit alles was geschäftsdienend über das Internet gesendet wird. Eine simple E-Mail-Anfrage zählt genauso zum E-Commerce wie die Bestellung eines Artikels in einem Online-Shop.*

Tabelle 3 - Definitionen von Mobile Commerce

Klaus Turowski und Key Pousttchi [KTKP04] definieren Mobile Commerce als *„jede Art von geschäftlichen Transaktionen, bei der die Transaktionspartner im Rahmen von Leistungsanbahnung, Leistungsvereinbarung und Leistungs-*

erbringung mobile elektronische Kommunikationstechniken in Verbindung mit mobilen Endgeräten einsetzen“.

Mobile Commerce kann nach der Art der Geschäftsbeziehung in unterschiedliche Kategorien eingeteilt werden [JÜKU03]. Die wichtigsten sind Beziehungen zwischen Unternehmen also Business to Business (B2B), Beziehungen zwischen Unternehmen und Kunden dem Business to Consumer (B2C) und Beziehungen zwischen Privaten also Peer to Peer (P2P).

Ein wichtiger Faktor für die Marktentwicklung im M-Commerce ist die Durchdringungsrate der Bevölkerung mit mobilen Endgeräten, insbesondere Mobiltelefonen. Weitere Vorteile der mobilen Kommunikation, die zum Wachstum des M-Commerce beigetragen haben, sind laut Mobile Commerce Report 2000 [PDDL00] die permanente Verwendbarkeit von drahtlosen Endgeräten, die Erreichbarkeit an jedem Ort und zu jeder Zeit, die Bedienungsfreundlichkeit, die Personalisierung sowie die Lokalisierbarkeit jedes Benutzers, worauf viele Services basieren.

2.5 Übertragungstechnologien

Elektronische Kommunikationstechniken sind nach Klaus Turowski und Key Pousttchi [KTKP04] Verfahren, mit denen Signale auch über weite Distanzen übertragen werden können. Dies bezeichnet man auch als Telekommunikation. Nach der Definition des European Telekommunications Standards Instituts [ETSI08] ist Telekommunikation „any transmission and/or emission and reception of signals representing signs, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems”. Erfolgt die Übertragung drahtlos, dann bezeichnet man diese Technik als wireless.

Für die drahtlose Kommunikation gibt es verschiedene Technologien, die Jürgen Kuhn [JÜKU03] in Übertragungstechnologien für den Privatbereich (PAN – Private Area Network), den Nahbereich (LAN – Local Area Network) und den Fernbereich (WAN – Wide Area Network) unterteilt.

Die Übertragung von Daten im PAN dient der Vernetzung von Geräten der persönlichen Umgebung wofür Infrarot oder Bluetooth verwendet werden. Übertragungstechnologien im LAN, wie beispielsweise Wireless LAN (WLAN) ermöglichen die Datenübertragung in Gebäuden oder abgegrenzten Geländern. Im Fernbereich kommt die Mobilfunktechnologie zum Einsatz, die eine Übertragung von Daten über sehr weite Distanzen, bis zu 10 Kilometern ermöglicht.

2.5.1 WLAN

WLAN ist eine mobile elektronische Kommunikationstechnik auf lokaler Ebene und wird teilweise als Sammelbegriff für jegliche drahtlose Vernetzung verwendet [KTKO04]. Der Begriff (WLAN) bezeichnet nach IEEE 802.11 [IEEE08] ein drahtloses lokales Netz. Der marktbeherrschende Standard ist IEEE 802.11b aus dem Jahr 1999 der eine maximale Datenrate von 11 MBit/s auf dem 2.4 GHz-Band erlaubt. Seit 2003 gibt es auch den Standard IEEE 802.11g der bei Abwärtskompatibilität wesentlich höhere Datenraten ermöglicht. Die Reichweite vom WLAN ist stark von den räumlichen Verhältnissen abhängig, wobei die typische Reichweite zwischen 30 innerhalb und 300 Metern außerhalb von Gebäuden liegt.

2.5.2 Bluetooth, IrDA

Wenn Endgeräte untereinander oder mit Peripheriegeräten vernetzt werden kommen Bluetooth oder IrDA zum Einsatz, da diese Technologien auf eine geringe Reichweite, von einigen Metern, ausgelegt sind.

Als Schlüsseltechnologie für spontane Vernetzung gilt Bluetooth [BLUE08], wo die Datenübertragung verschlüsselt werden kann und auch der Stromverbrauch relativ gering ist. Jede Bluetooth-Funkverbindung wird im Rahmen eines Piconetzes hergestellt, in dem alle Geräte den gleichen physischen Kanal belegen. Typische Betriebsverfahren und –modi eines Bluetooth-fähigen Gerätes sind die Verbindung mit anderen Bluetooth-fähigen Geräten in einem Piconetz, der Datenaustausch zwischen Bluetooth-fähigen Geräten und die

Bluetooth Wireless-Technologie, die eine drahtlose Ad-hoc-Kommunikations-technologie darstellt.

IrDA DATA [IRDA] ist ein Standard zur Übertragung mittels Infrarotlicht, welcher im Gegensatz zur Funktechnologie immun gegen elektromagnetische Einflüsse ist, jedoch durch andere Lichtquellen gestört werden kann. Es bietet eine hohe Abhörsicherheit, da die Geräte mit einer Sichtverbindung aufeinander ausgerichtet werden müssen. Die Reichweite beträgt etwa 1-2 Meter. Beide Technologien können auch in sehr kleine Endgeräte eingebaut werden.

2.5.3 Mobilfunk

Mobilfunk wird definiert als [KTKP04] „eine Form der Telekommunikation, bei der ein Dienstanbieter die Übertragung von Sprache und Daten von und zu mobilen Endgeräten durch ein drahtloses Zugangsnetz auf Basis elektromagnetischer Wellen ermöglicht“.

Um Mobilfunk betreiben zu können benötigt man ein Mobilfunknetz, das sich aus einem Mobilvermittlungsnetz und einem Zugangsnetz zusammensetzt. Das Mobilvermittlungsnetz ermöglicht die Übertragung und Vermittlung von Signalen zwischen den ortsfesten Einrichtungen des Mobilfunknetzes. Das Zugangsnetz ermöglicht die Übertragung der Signale zwischen einer Mobilfunkantenne und dem mobilen Endgerät. Dies wird auch als Luftschnittstelle bezeichnet und ist in Abbildung 1 dargestellt [KTKP04].

Der größte Teil der Übertragung findet im Mobilvermittlungsnetz im drahtgebundenen Festnetz oder in seltenen Fällen auch über Richtfunkstrecken statt. Das eigentliche Funknetz ist erst das Zugangsnetz.

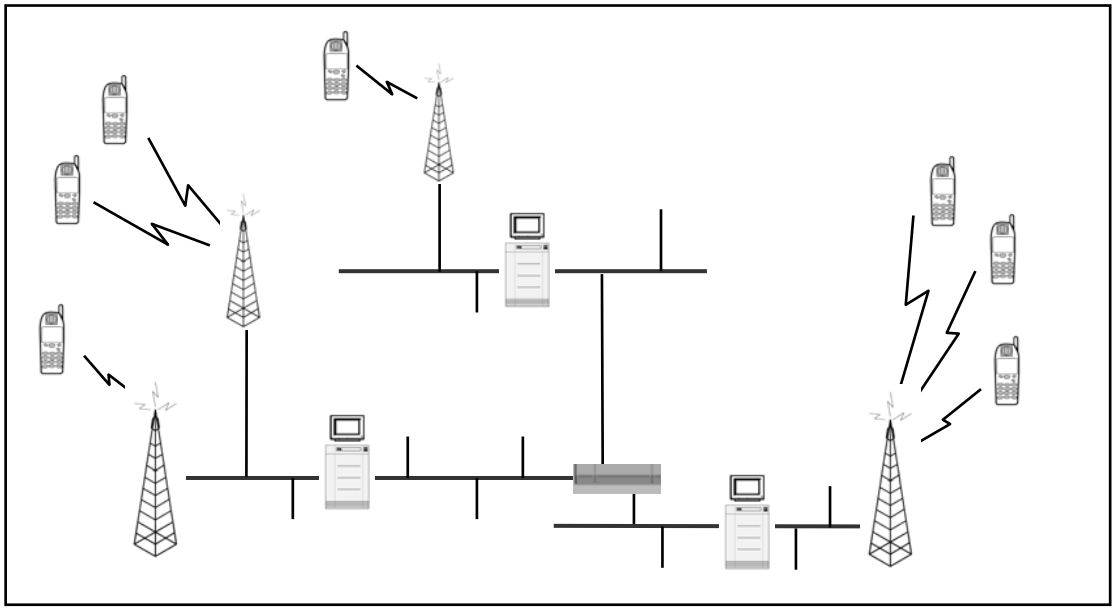


Abbildung 1 - Schematische Darstellung eines Mobilfunknetzes

Der Mobilfunk der ersten Generation (1G) verwendete im Zugangsnetz analoge Übertragungstechniken und ist mittlerweile abgeschaltet [KAWI04]. Für die öffentliche Nutzung gab es von 1958 – 1977 das A-Netz für Autotelefone das seinerzeit das weltgrößte flächendeckende öffentliche Mobilfunknetz war, das B-Netz von 1972 – 1994 für sektororientierte Autotelefone und das C-Netz von 1985 – 2000, das bereits tragbare Telefone auf Basis analoger Funktechnik bot und erstmals Datenübertragung möglich machte.

Beim Mobilfunk der zweiten Generation (2G) wird digitale Übertragungstechnik verwendet und ist bereits datenfähig. Die Fähigkeit ist jedoch nur sehr eingeschränkt nutzbar. Ein Standard dieser Generation ist Terrestrial Trunked Radio (TETRA), ein ETSI-Standard für digitalen Bündelfunk der für sicherheitsrelevante Anwendungen bei Behörden vorgesehen war.

Der weltweit dominierende Standard ist hier jedoch GSM (Global System for Mobile Communications) [GSMW08], der über die verwendeten Frequenzen wie folgt unterschieden wird:

- GSM 900 seit 1991 D-Netz
- GSM 1800 seit 1994 Weiterentwicklung E-Netz
- GSM 1900 USA/Kanada
- GSM 400 Einsatz in einigen Ländern für Eisenbahngesellschafen GSM-Rail. Verfügt über einige Erweiterungen wie Automatic Train Control ATC, Voice Broadcast Service VBS, Voice Group Call Service VGCS, funktionsorientierte und relative Adressierung und einer Priorisierung von Gesprächen innerhalb des Netzes

2.5.4 GSM

In den frühen 80er Jahren wuchsen die analogen Mobilfunknetze in Europa rapide. Jedes Land entwickelte seine nationalen Technologien und es gab eine immer größer werdende Notwendigkeit für einen einheitlichen Mobilfunk-Standard [KTKO04], was auch aus wirtschaftlicher als auch aus EU-politischer Sicht forciert wurde.

1982 wurde auf der Conference of European Posts and Telegraphs (CEPT) die Arbeitsgruppe Groupe Spécial Mobile (GSM) gegründet. 1990 veröffentlichte dann das ETSI - European Telecommunication Standard Institute [ETSI08], dem die Groupe Spécial Mobile im März 1989 unterstellt wurde, Phase I der GSM-Spezifikationen [OSWA96]. Aus der Abkürzung GSM mit der ehemaligen Bedeutung Groupe Spézial Mobile wurde durch den pan-europäischen Gedanken Global System for Mobile Communication.

GSM [GSMW08] ist die Grundlage für die nachfolgenden Standards GPRS und UMTS. Das GSM Netz wird in drei Subsysteme unterteilt:

- **Base Station Subsystems** – Zugangsnetz zur Anbindung der Mobilfunkteilnehmer an das Netz
- **Network and Switching Subsystem** – Mobilvermittlungsnetz zur Vermittlung der Nutzdaten innerhalb des Netzes und zur Bereitstellung der Anbindung an andere Netze
- **Operation and Support Subsystem** – umfasst alle weiteren Elemente für den Betrieb, Administration und Kontrolle des Gesamtnetzes

Es gibt drei Arten von Benutzerdiensten die vom GSM-Netz bereitgestellt werden. Supportdienste legen die Charakteristika des eingerichteten Sendekanals fest, Teledienste stellen die Kernfunktionalität des Netzes dar wie Sprachverbindung, Notruf, Kurznachrichten und Zusatzdienste wie Anruferidentifikation oder Rufumleitung.

Ein Benutzer der am Funkverkehr in einem GSM-Netz teilnehmen möchte benötigt eine Mobile Station, die sich aus einem mobilen Endgerät wie beispielsweise einem Mobiltelefon und dem Subscriber Identity Module (SIM), einer kleinformatigen Prozessorchipkarte, zusammensetzt. Die SIM Karte dient der Authentisierung des Teilnehmers und der Speicherung von statischen und dynamischen Teilnehmerinformationen und wickelt die eigentliche Kommunikation mit dem Netz ab. Gespeichert werden z.B. die Mobilfunkrufnummer oder Mobile Station ISDN Nummer für die externe Identifikation, die International Mobile Subscriber Identifikation, eine netzunabhängige, international eindeutige 15-stellige GSM-Teilnehmernummer für die interne Identifikation, die persönliche Identifikationsnummer (PIN) und die Temporary Mobile Subscriber Identity, die temporär vergeben wird und nach dem Einbuchen in ein Netz die IMSI ersetzt um den Teilnehmer zu anonymisieren.

Die eigentliche Anbindung der Mobile Station an das Netz ist die Aufgabe der Basisstationssysteme, die aus einer Basisstationssteuerung und der Sende- und Empfangsstationen bestehen und den Funkverkehr von ein bis drei Zellen durchführen [KAWI04]. Das Network and Switching Subsystem ist für die Vermittlung der Nutzdaten innerhalb des Netzes und für die Anbindung an andere Netze zuständig. Die eigentliche Kommunikation übernimmt die Mobilvermittlungsstelle. Das Operation und Support Subsystem beinhaltet das Operation and Maintenance Center, welches Systeme für Konfiguration und Wartung des Netzes, Störungs- und Sicherheitsmanagement, Teilnehmerverwaltung und Abrechnungsverwaltung umfasst. Außerdem gehören die Authentifizierungszentrale für Verschlüsselungsinformationen und die Endgerätedatenbank dazu.

Der standardmäßige GSM Datendienst ermöglich eine maximale Übertragungsrate von 14,4 kbit/s. Durch die GSM Softwareerweiterung HSCSD (High Speed Circuit Switched Data) kann die Übertragungsrate durch Kanalbündelung gesteigert werden.

Es gibt grundsätzlich die Möglichkeit Daten verbindungsorientiert oder paketorientiert in einem drahtlosen Netz zu übertragen. Bei der verbindungsorientierten Datenübertragung wird die Übertragungsstrecke für Sprache exklusiv geschaltet. Für die paketorientierte Übertragung werden die Daten in einzelne Pakete zerlegt und adressiert versendet, wodurch eine dynamische Aufteilung der Netzkapazität ermöglicht wird. In 2G Netzen ist die Datenübertragung nur verbindungsorientiert möglich.

Um nun einerseits den Zeitraum bis zur Einführung datenoptimierter Netzte der dritten Generation zu überbrücken und andererseits deren Einführung durch eine schrittweise Vorgehensweise zu erleichtern, wurde eine Zwischen-generation geschaffen, die 2.5G-Netze. Bestehende 2G-Netze werden unter Nutzung dieser Standards um die Fähigkeit zur paketorientierten Daten-übertragung erweitert. Dabei werden die Gespräche und Daten mehrerer zugleich aktiver Benutzer in kleine Datenpakete unterteilt und sequenziell transportiert [MOBI07], wie in Abbildung 2 dargestellt.

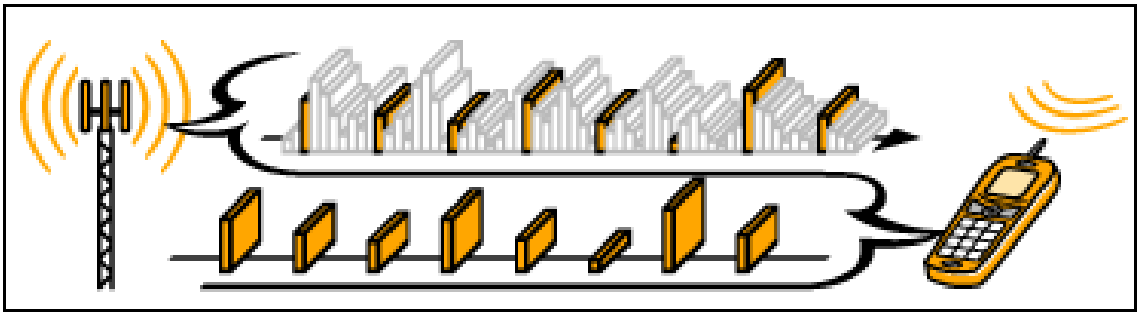


Abbildung 2 - Paketorientiert Datenübertragung

Die Standards in diesem Bereich sind GPRS (General Packet Radio Sevice) und EDGE (Enhanced Data Rates for Global Evolution), die weltweit als Ausbaustufe von GSM-Netzen eingeführt wurden [KTKP04]. Für die Entwicklung der dritten Generation gab es weltweit abgestimmte Ziele, die im

Konzept IMT-2000 (International Mobile Telecommunications 2000) der ITU festgelegt wurden. Die wichtigsten Ziele waren die Unterstützung höherer Datenübertragungsraten, Unterstützung von Multimedia-Anwendungen und erweitertes Roaming. Die daraus resultierenden Standards waren UMTS (Universal Mobile Telecommunications System) und CDMA-2000.

2.5.5 GPRS

GPRS (General Packet Radio Service) ist der nachfolgende Standard von GSM. GPRS ermöglicht eine paketorientierte Datenübertragung durch einen eigenen GPRS-Vermittlungsknoten.

EDGE, ein weiterer Standard, der sich in Europa nicht durchgesetzt hat [KTKO04], versuchte die Leistungsmerkmale eines 3G-Netztes so gut wie möglich zu realisieren ohne der Notwendigkeit ein neues Netz aufzubauen. Es ermöglicht die Nutzung der bestehenden Datendienste mit höherer Bandbreite, leitungs- und paketorientiert. 2003 wurde das erste europäische EDGE-Netz in Ungarn implementiert.

2.5.6 UMTS

Ein weiterer wesentlicher Standard des 3G-Netzes ist UMTS (Universal Mobile Telecommunications System) [UMTS08], das ein vollständig neues Zugangsnetz, das UTRAN (UMTS Terrestrial Radio Access Network) bereitstellt. Die GSM-Mobile Station wird hier durch das User Equipment ersetzt, das aus einem Mobilen Endgerät und des UMTS Subscriber Identity Modul besteht.

Die USIM Karte unterscheidet sich von der SIM Karte vor allem durch die wesentlich höhere Speicherkapazität von mehreren MByte und durch die Präzisierung der Zugriffsbedingungen auf jede einzelne Datei auf der Karte.

Bei der Übertragung von Daten mittels UMTS wird im Gegensatz zu GSM jedem Gespräch ein eigener Code zugewiesen, wie in Abbildung 3 ersichtlich [MOBI07]. Die Mobilfunkanlage kennt alle Codes und kann so die einzelnen

Gespräche zuordnen. Der große Vorteil der dabei entsteht ist, dass jedes Mobiltelefon die gesamte Kapazität nutzen kann.

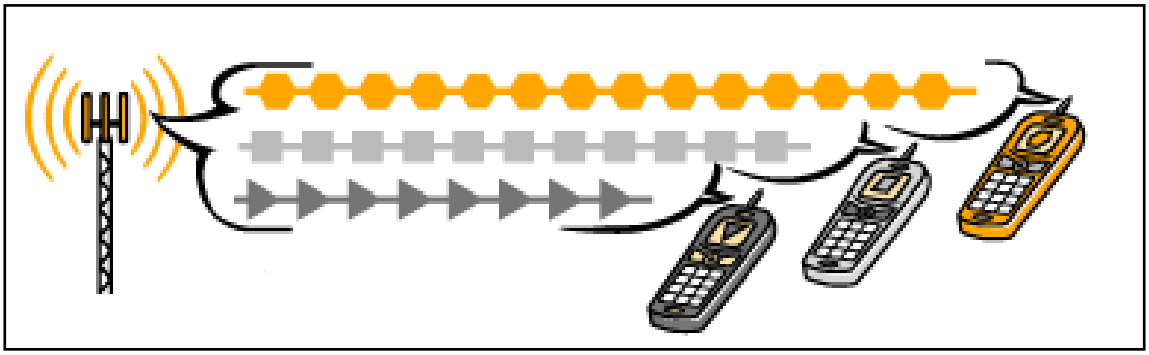


Abbildung 3 – Übertragung mit eigenem Code für jedes Gespräch

Die Schwerpunkte bei der Entwicklung der vierten Generation liegen im Bereich der Integration heterogener drahtloser Netze [KTKP04] sowie der Sicherheit und der effizienten Ausnutzung des Frequenzspektrums.

Ein Grundproblem für die effiziente Nutzung des Mobilfunks sind die knappen Ressourcen [JÜKU03]. Abbildung 4 zeigt die Untergliederung des Mobilfunknetzes ist in Funkzellen [JÜKU03].

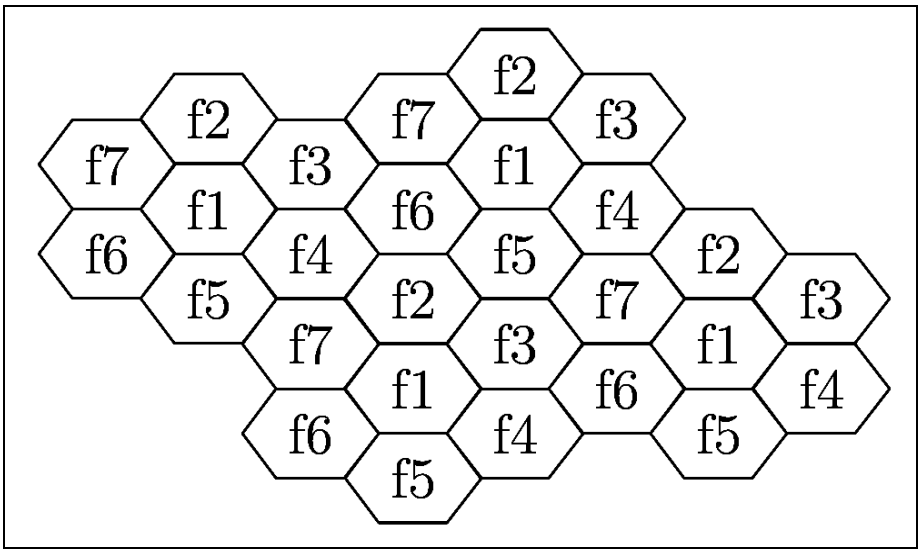


Abbildung 4 – Untergliederung des Mobilfunknetzes in Funkzellen

Mehrere Funkzellen ergeben einen Cluster. Da jede Zelle nur eine geringe Sendeleistung hat, können die gleichen Frequenzen in weit genug auseinander liegenden Zellen wieder verwendet werden.

Je kleiner die Cluster sind, desto mehr Endgeräte können im gleichen Mobilfunknetz das Netz nutzen. Um das begrenze Frequenzspektrum mehrfach nutzen zu können werden Multiplexverfahren eingesetzt. Gängige Verfahren sind Raummultiplex, Frequenzmultiplex, Zeitmultiplex und Codemultiplex.

2.6 NFC – Near Field Communication

Im Jahr 2002 haben Phillips und Sony [NXPC08] begonnen eine neue Funktechnologie, Near Field Communication (NFC) für die Kurzstrecken-kommunikation zu entwickeln. Ziel war es ein weltweit einheitliches Protokoll, für die drahtlose Übertragung von Daten über kurze Distanzen zu schaffen.

Im Jahr 2004 wurde von Phillips, Sony und Nokia das NFC-Forum [NFCF07] gegründet, das vor allem die Entwicklung und Verbreitung der neuen Technologie NFC als Aufgabe hatte. Heute gibt es bereits mehr als 130 Mitglieder wie Microsoft, Visa, AMEX, Siemens usw. Sie arbeiten alle zusammen, um eine weltweit einheitliche Entwicklung von NFC zu ermöglichen und voranzutreiben.

Near Field Communication basiert auf der drahtlosen Radio Frequency Identification (RFID) Technologie und arbeitet im 13,56 MHz Frequenzbereich [MIWE07]. NFC ist daher auch kompatibel zu den bereits weltweit eingesetzten Smart-Card Verfahren Philips-Mifare [MIFA08] und Sony-FeliCa [FELI08], die auf derselben Frequenz arbeiten. Es ist eine für sehr kurze Entfernungen konzipierte Funkkommunikation. Sie ermöglicht eine berührungslose auf Annäherung basierte Interaktion zwischen zwei NFC tauglichen Geräten, wenn man diese sehr nah aneinander heranbringt. NFC hat eine Reichweite von 0 – 20 cm bei vergleichsweise niedrigen Übertragungsraten von max. 424 kbit/s.

Im Vergleich zu anderen Technologien wie Bluetooth scheint die kurze Distanz im Zentimeterbereich auf den ersten Blick eher als Rück- anstatt als Fortschritt.

Wiedmann und Reeh [PWMO06] beschreiben dies jedoch als einzigartige USP (Unique Selling Proposition) und Argumentieren, dass dadurch, das Abhören sehr schwer möglich ist, da ein potentieller Angreifer sehr nah herankommen müsste.

NFC ermöglicht Peering im Vergleich zu herkömmlichen Funksystemen alleine durch Annäherung zweier NFC fähiger Geräte. Ferner ist eine meist lästige manuelle Konfiguration durch den Anwender dabei nicht erforderlich. Der menschliche Kommunikationsmechanismus ist daher leicht auf die NFC Technologie zu übertragen, denn wenn wir uns unterhalten möchten, dann gehen wir aufeinander zu und manchmal flüstern wir sogar, wenn es sich um vertrauliche Inhalte handelt. Dieses Verhalten kann somit intuitiv übernommen werden und muss vom Anwender nicht neu erlernt werden, was einen konzeptionellen Vorteil für die Nutzungsakzeptanz darstellt [PWMO06].

NFC basiert auf einer drahtlosen Verbindung, die aus einem passiven Medium oder Tag und einem aktiven Leser besteht. Laut Tariq Shahab (Manager Philips Semiconductors) [SIOR06] ist die Möglichkeit diese Technologie aktiv und passiv zu verwenden einzigartig gegenüber anderen drahtlosen Kommunikationstechnologien. Der Leser baut ein elektromagnetisches Feld auf. Nähert sich ein NFC Gerät an, dann kann mittels magnetischer Induktion Energie, also Strom in das passive Medium (Tag oder Smartcard) übertragen werden. Sobald die Stromversorgung aufgebaut wurde, können Daten übertragen werden.

Near Field Communication ist mittlerweile nach ISO 18092 [ISO18092], ISO 21481 [ISO21481], ECMA 340 [ECMA340], ECMA 352 [ECMA352] sowie nach ECMA 356 [ECMA356] standardisiert. Abbildung 5 zeigt die Verbindung der Standards und das gesamte NFC Protokoll Arrangement [ECMA].

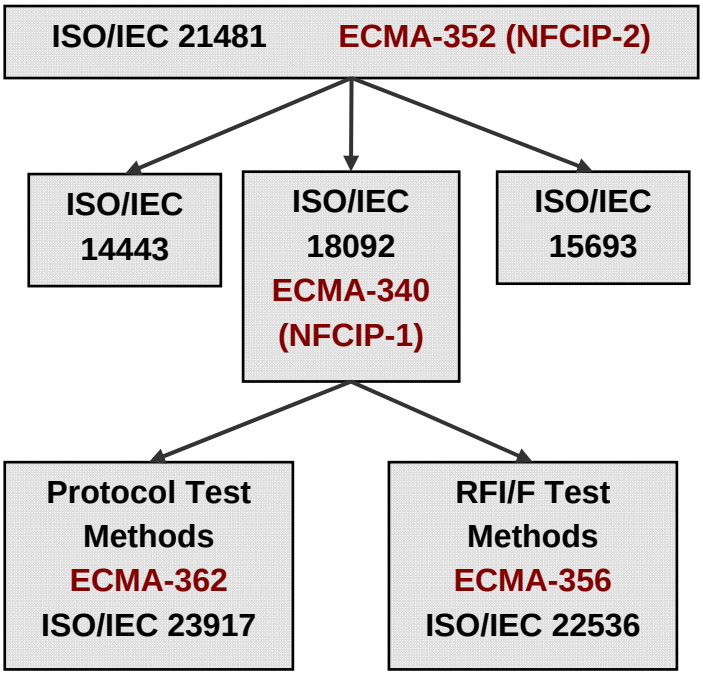


Abbildung 5 - NFC Protokoll Arrangement

Wenn ein NFC Gerät mit einem anderen kommunizieren möchte, gibt es bestimmte Grundregeln die eingehalten werden müssen [AERA08]. Damit eine fehlerfreie Datenübertragung garantiert werden kann, wird das „listen before talk“ Prinzip angewandt. Es können immer nur zwei NFC-Geräte - der „Initiator“, der die Daten versendet und das „Target“ das die Daten empfängt - gleichzeitig miteinander kommunizieren.

Abbildung 6 zeigt einen NFC Protokoll Ablauf [AERA08]. Jedes NFC Gerät befindet sich standardmäßig im Target-Modus und wartet auf einen Befehl von einem Initiator. Je nach Anwendung kann ein NFC Gerät in den Initiator-Modus wechseln und den Übertragungsmodus (aktiv oder passiv) sowie die Übertragungsgeschwindigkeit wählen. Der Initiator überprüft, ob bereits externe NFC Felder aktiv sind. Ist dies der Fall, dann muss der Initiator warten, bis dieses Feld wieder deaktiviert wurde um sein eigenes aufbauen zu können. Der Initiator aktiviert das Feld des Ziels und je nach Einstellung erfolgt die Übertragung von Befehlen im aktiv oder passiv Modus und der gewählten Übertragungsrate und danach empfängt er die Antwort. Anschließend wird das NFC Feld wieder deaktiviert.

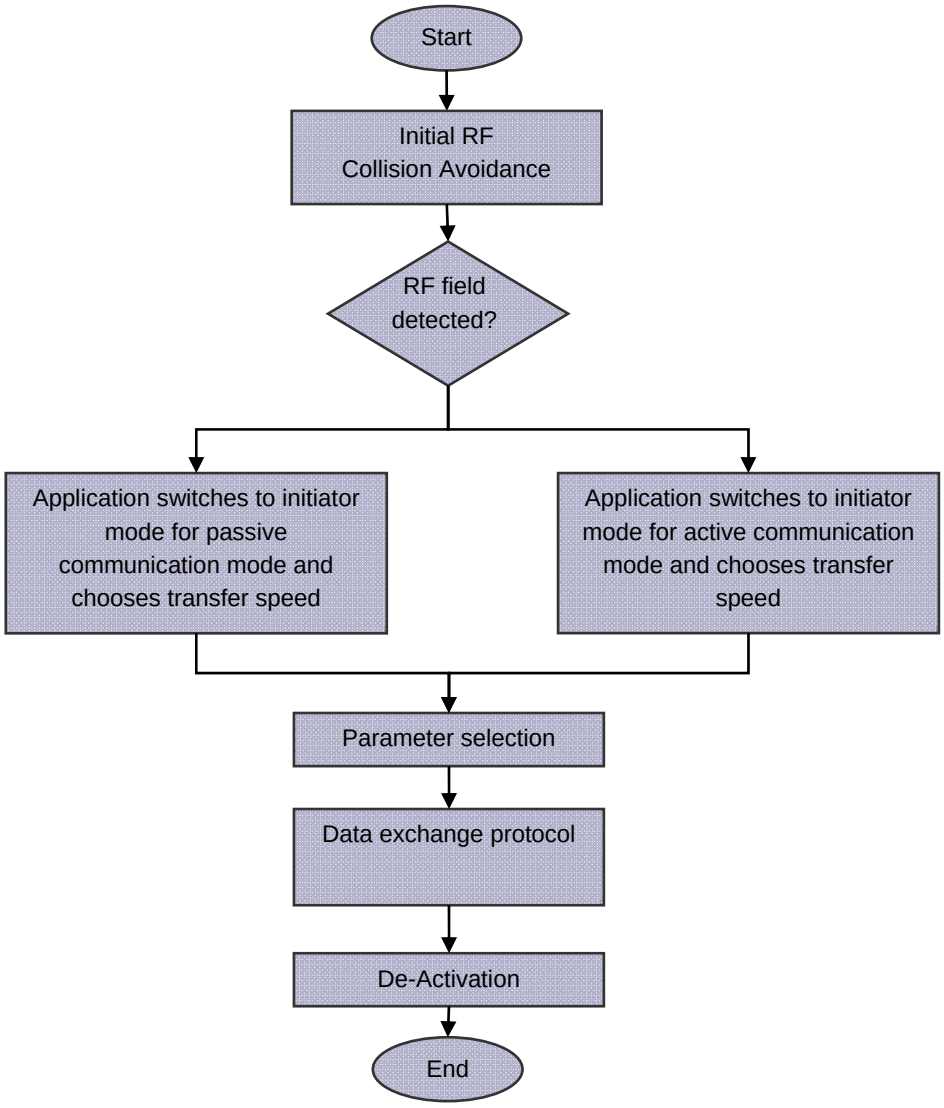


Abbildung 6 - Protokollstack von NFC

2.7 RFID

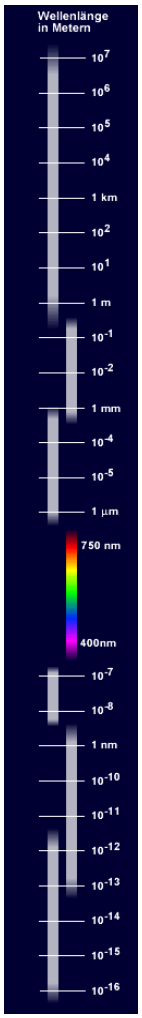
RFID Systeme verwenden viele unterschiedliche Radiofrequenzen sowie andere Technologien. Die Anfänge der RFID Technologie gehen bis ins frühe 20. Jahrhundert zurück.

Das 19. Jahrhundert ist das Zeitalter in dem ein grundlegendes Verständnis für elektromagnetische Energie erlangt wurde. Michael Faraday (1791 - 1867) behauptete [JOTY70], dass Licht eine Form von elektromagnetischer Energie sei. Der Schotte James Clerk Maxwell (1831 - 1879) publizierte 1864 [WELT07]

seine Theorie des Elektromagnetismus, in dem er die wellenartige Ausbreitung elektromagnetischer Kräfte, wie es auch das sichtbare Licht ist, erklärte. Der Physiker Heinrich Hertz (1857 – 1894) erzeugte und empfing 1880 zum ersten Mal Radiowellen und 1896 demonstrierte Guglielmo Marconi (1874 – 1937) die erste erfolgreiche Radiotelegraphie über den Atlantic und gilt somit als Pionier der drahtlosen Kommunikation. 1906 stellte Ernst F.W. Alexanderson (1866 - 1932) den ersten Langwellensender vor und führte die erste Rundfunkübertragung durch [JELA05].

Die Radartechnik wurde Anfang des 20. Jahrhunderts entwickelt und trägt maßgeblich zur Entwicklung von RFID bei. Radarwellen oder Radarstrahlen sind Mikrowellen, also elektromagnetische Wellen mit einer bestimmten Wellenlänge, wie in Abbildung 7 [DRFR07] ersichtlich, die von Gegenständen reflektiert werden.

Die Radiowellen-, und Radartechnik stellen die Grundlage für die RFID Technologie dar [FDSW06]. Durch die Radartechnik können Geschwindigkeit und Position eines Gegenstandes festgestellt werden, indem die Reflexion der ausgesendeten Radiowellen gemessen wird. Im zweiten Weltkrieg haben sich die britischen Streitkräfte diese Technik zu Nutze gemacht um feindliche Flugzeuge von den eigenen bereits beim herannahen zu unterscheiden. Die Entwicklung von RFID Systemen wurde vom Militär weiter vorangetrieben und später überwiegend für Zutritts- und Berechtigungskontrollen eingesetzt. Erst 1977 wurde die RFID Technologie für die zivile Nutzung vom Militär freigegeben.



Hoch, Mittel, Niederfrequente Wechselströme
(U-Boot Kommunikation, Funknavigation)

Radiowellen
Langwelle
Mittelwelle
Kurzwelle
UKW (Ultrakurzwelle)/VHF (Very High Frequency)
(Fernsehen, Hörfunk, Magnetresonanztomografie, Radar)

Mikrowellen
Dezimeter-, Zentimeter-, Millimeterwellen
(Radar, Mobilfunk, Fernsehen,
Mikrowellenherd, WLAN, Bluetooth, Richtfunk)

Infrarotstrahlung (Wärmestrahlung)
Fernes Infrarot
Mittleres Infrarot
Nahes Infrarot

Sichtbares Licht

UV-Strahlung
UV-A, UV-B, UV-C Strahlung
(Desinfektion, UV-Licht, Banknotenprüfung, Schwarzlicht, Fluoreszenz)

Röntgenstrahlen
Weiche-, Harte Röntgenstrahlen
(medizinische Diagnostik, Sicherheitstechnik, Spektroskopie)

Gammastrahlen
(Radioaktivität)

Kosmische Strahlung

Abbildung 7 - Elektromagnetisches Spektrum

RFID steht für Radiofrequenz-Identifikation und diese Technologie ermöglicht es Daten mittels Radiowellen berührungslos und ohne Sichtkontakt zu übertragen. Dazu wird ein Transponder auch Tag genannt, ein Sende-Empfangs Gerät sowie ein IT-System im Hintergrund benötigt. Der Transponder, ein winziger Computerchip mit einer Antenne wie in Abbildung 8 zu sehen ist, der das Herzstück dieser Technik [INRF07] darstellt und nur weniger Quadratmillimeter groß ist, ist in ein Trägerobjekt, wie beispielsweise eine Plastikkarte oder ein Klebeetikett, integriert. Jeder RFID Transponder erhält durch einen Nummerncode der auf dem Chip gespeichert ist eine unverwechselbare Identität.

Abbildung 8 – RFID Inlay mit Schleifenantennen

Das Sende-Empfangs Gerät erzeugt ein elektromagnetisches Feld, das von der Antenne des Transponders empfangen wird und der Transponder sendet daraufhin den Nummercode an das Lesegerät. Abhängig von dem verwendet Frequenzbereich können Daten aus unterschiedlichen Distanzen zwischen wenigen Zentimetern und mehreren Metern gelesen werden.

Funkwellen transportieren bei RFID-Systemen Informationen und Energie und senden auf unterschiedlichen Frequenzen wie es auch das Radio nützt. Dieses verwendet Ultrakurzwellen-, Mittelwellen- und Langwellenfrequenzen.

RFID verwendet den Niedrig-, Hoch- und Ultrahochfrequenzbereich und je nach Art der Anwendung muss entschieden werden, welche Frequenz verwendet wird. Die folgende Tabelle zeigt die typischen Reichweiten und Anwendungsbeispiele der verschiedenen RFID-Frequenzen [INRF07].

RFID-Frequenzen	Anwendungen	Typische Reichweite
LF Niederfrequenz 125 – 135 kHz	➢ Tieridentifikation ➢ Produktionskontrolle ➢ Automatisierung ➢ Zutrittskontrollen ➢ Kfz-Wegfahrsperren	1 - 1,5 Meter Einige Zentimeter
HF Hochfrequenz 13,56 MHz	➢ Handelsgüter (Einzelprodukte) ➢ Bibliotheksmanagement ➢ Ticketing ➢ Zutrittskontrollen ➢ Automatisierung ➢ Near Field Communication	1 – 1,5 Meter 1 – 1,5 Meter 10 Zentimeter 10 Zentimeter
UHF Ultrahochfrequenz 860 – 960 MHz	➢ Palettenidentifikation und Kartonidentifiaktion (Handel)	3 – 4 Meter Europa 7 Meter USA

Abbildung 9 - RFID Frequenzbereiche

Der Chip besteht im Wesentlichen aus drei Komponenten [FGWH06]:

- Hochfrequenzteil, der der Signalverarbeitung und der Energiegewinnung aus dem elektrischen Feld dient
- Kontrolleinheit für die Verarbeitung der empfangenen Kommandos
- Speichereinheit

Wesentlich für den Einsatz des Chips ist die Größe des verfügbaren Speichers, der auch Datenbreite genannt wird und unterschiedliche Funktionen innehaben kann. Die Antenne des RFID Chips nimmt die elektromagnetischen Wellen auf und stellt die Verbindung zum Chip her. Schleifenantennen sind z.B. relativ klein und flach und können einfach auf Trägerfolien gedruckt werden und so können flache Tags sehr preisgünstig produziert werden. Die Wahl von Chip und Antenne sowie die Inlays, die Materialien auf die sie aufgebracht werden, sind von großer Bedeutung für die weitere Funktion bzw. Leserate des Transponders und somit kritische Faktoren bei der Herstellung.

Von einem Inlay spricht man, wenn ein Chip auf das Trägermaterial, wie beispielsweise eine Folie, aufgebracht und mit der Antenne verbunden wird. Erst wenn das Inlay in eine gebrauchsfähige Form gebracht wird, wie zum Beispiel einem Klebeetikett oder einer Smartcard, spricht man vom Tag bzw. Transponder.

Prinzipiell gibt es aktive, passive und semi-aktive RFID Transponder und die Auswahl muss individuell, je nach Einsatzzweck abgestimmt werden [FGWH06]. Aktive RFID Tags können selbst Radiosignale erzeugen und unterschiedlich konfiguriert werden. Sie können auch, um Energie zu sparen, in einen Ruhemodus versetzt und durch bestimmte Ereignisse wieder erweckt werden. Passive Tags kommen ohne Stromversorgung aus und beziehen die benötigte Energie aus dem elektromagnetischen Feld des Readers und haben eine geringere Reichweite. Es gibt nicht-, einmal und mehrfach beschreibbare passive RFID Tags wonach auch die Kosten variieren. Semi-aktiv verhalten sie sich wie passive Tags und werden nur aktiv, wenn sie in ein elektromagnetisches Feld geraten. Sie verfügen über eine Batterie, die das abgegebene Signal verstärken und somit die Reichweite erhöhen soll.

RFID Schreib-/Lesegeräte oder Reader sind entweder mit integrierten oder externen Antennen, die das elektromagnetische Feld aussenden, verbunden. Diese lesen die Daten eines Transponders aus oder beschreiben diesen. Sie beinhalten die Software, die für die Übertragung der empfangenen Daten an die nächst höhere IT Ebene verantwortlich ist. Es gibt stationäre und mobile RFID Reader und sie können anhand von Reichweite, Frequenz, Datenübertragungsprotokollen uns Leistung klassifiziert werden [RFID07]. Mobiltelefone mit RFID bzw. NFC können z.B. so ausgestattet werden, dass sie als RFID Reader ebenso wie als RFID Tag fungieren können.

Die Einsatzmöglichkeiten für RFID sind mittlerweile sehr weitläufig und nahezu unbegrenzt. Diese Technologie wird heutzutage beispielsweise in der Logistik beim Verladen und Abtransport von Waren aller Art verwendet. Bei der Produktionssteuerung hilft RFID bei der Kommunikation von Montageanleitungen und liefert weitere Informationen an die Roboter für die Fertigung.

Ferner wird RFID im Hochsicherheitsbereich, mit dem Ziel nur berechtigten Personen Zutritt zu bestimmten Bereichen zu ermöglichen, eingesetzt. Im Verkehr wird es beispielsweise für die Einhebung der Mautgebühr verwendet, bei der Luftfahrt kommt es bei der Gepäcksabfertigung zum Einsatz, in der Tierzucht und Tierforschung wird die Gesundheit der Tiere mittels RFID überwacht, im Handel wird damit z.B. die Lagerverwaltung automatisiert, bei der Produktsicherheit können mit Hilfe von RFID Plagiate von Originalprodukten unterschieden werden.

Ferner wird RFID im Gesundheitsbereich eingesetzt, um die Patienten besser identifizieren zu können und den Dokumentationsprozess zu automatisieren. Dies sind nur einige Beispiele für den fast unbegrenzten Einsatzbereich von RFID Technologie. [INRF07].

3 Zahlungssysteme

Im Zahlungsverkehr unterscheidet man grundsätzlich zwischen dem Zahlungsverkehr in bar und dem bargeldlosen Zahlungsverkehr [TLKS06]. Beim Zahlungsverkehr in bar handelt es sich um die Verwendung von Banknoten und Münzen, welche die Zentralbank herausgibt und kontrolliert. Zum bargeldlosen Zahlungsverkehr zählt das Buchgeld, wo beispielsweise Schecks oder Überweisungen zum Einsatz kommen.

3.1 Zahlungsverkehr in bar

Der Zahlungsverkehr war von Anfang an ständigen Innovationen unterworfen. In den ersten 33.000 Jahren in der Geschichte des Menschen existierte noch kein Geld [THLA06]. Erst seit rund 7.000 Jahren gibt es Zahlungsmittel, wobei anfangs wertvolle Fundgegenstände, wie Muscheln, Perlen oder auch handwerkliche Produkte und Vieh, als Wertmesser für Güter und Dienstleistungen verwendet wurden. Seit etwa 700 v. Chr. gab es erstmals Bargeld in Form von Münzen. Die ersten Banknoten gab es erst im 18. Jhd. wodurch Käufe und Verkäufe wesentlich einfacher als mit Warengeld wurden.

3.2 Bargeldlose Zahlungsverfahren

Gegenüber dieser Entwicklungsgeschichte folgte im bargeldlosen Zahlungsverkehr auf Basis von Buch- und Giralgeld Innovation auf Innovation. Den bargeldlosen Zahlungsverkehr gibt es erst seit rund 100 Jahren und den Kartenzahlungsverkehr seit rund 50 Jahren. Er hat maßgeblich dazu beigetragen, dass sich die Zahlungsgewohnheiten des Menschen stark verändert haben [THLA06]. Zahlungen von Unternehmen sowie von Privaten an öffentliche Haushalte und umgekehrt sind heutzutage fast ausschließlich bargeldlos. Lediglich Zahlungen von Privaten an Unternehmen am Point of Sale (POS) erfolgen derzeit noch überwiegend in bar.

Es gab drei grundlegende Innovationen, die in der Grundkonzeption bis heute unverändert blieben, jedoch wesentlich dazu beitrugen, dass fast der gesamte

Zahlungsverkehr zwischen Privaten, Unternehmen und öffentlichen Haushalten heutzutage bargeldlos erfolgt.

3.2.1 Scheck

Das erste bargeldlose Zahlungsmittel war der Scheck, der bereits Ende des Mittelalters eingesetzt wurde und die Distanz bei notwendigen Zahlungen von Kaufleuten zwischen den großen Handelsplätzen zu überwinden. In Österreich und Deutschland wurde der Scheck erst Ende des 19. Jhd. zwischen Kaufleuten intensiver verwendet und seine Blütezeit erlangte er als „Eurocheque“ zwischen 1968 und 2001 [EURO07]. Ende der 60er Jahre wurde die Eurocheque Karte erstmals ausgegeben und konnte zur grenzüberschreitenden Bargeldbeschaffung eingesetzt werden. Im angelsächsischen Raum hat der Scheck auch heute noch große Bedeutung.

3.2.2 Überweisung

Der erstmalige Einsatz einer Überweisung wie wir sie heute kennen, war Ende des 19. Jahrhunderts und ihr Zweck war wie beim Scheck die bargeldlose Begleichung von Rechnungen [THLA06]. Durch die sukzessive Ausstattung der Bevölkerung mit Girokonten hat die Überweisung im deutschsprachigen Raum immer mehr an Bedeutung gewonnen.

3.2.3 Lastschrift

Die Lastschrift wurde in den 20er Jahren des 20. Jhd. als „rückläufige Überweisung“ erfunden [THLA06]. Hierbei hat der Zahlungsempfänger die Möglichkeit den offenen Betrag vom Konto des Zahlungspflichtigen, der einen Einziehungsauftrag erteilt hat, einzuziehen.

3.2.4 Kreditkarte

Der Kartenzahlungsverkehr begann mit der Aufnahme des Privatkunden-geschäfts durch die Banken, was in den USA früher als in Europa stattfand. Im Jahr 1924 kamen die ersten Kreditkarten auf den Markt [GEKR04], die als

Metallblättchen von der Western Union, der amerikanischen Telegrafengesellschaft, ausgegeben wurden. Erst seit 50 Jahren gibt es die Plastikkarten wie sie heute im Umlauf sind.

Hinter der Innovation der Kreditkarte stand die Idee, dass Vielreisende mit einer Karte immer liquide sind und bei jeder Vertragsstelle bezahlen konnten. Anfänglich waren die Akzeptanzstellen vor allem Hotellerie und Gastronomie. Es haben sich grundsätzlich drei Arten entwickelt. Die Kreditkarte, die dem Karteninhaber eine Kreditfazilität einräumt und einmal im Monat eine Rechnung abgebucht wird. Die Debitkarte, die im engeren Zusammenhang mit dem Girokonto steht und lediglich die Möglichkeit bietet über das dort vorhandene Kapital zu verfügen. Sowie die Prepaidkarte, bei der ein beliebiger Betrag augebucht wird, über den man anschließend verfügen kann.

1949 gründete Frank McNamara „Diners Club“ [GEKR04] und diese Karte ist bis heute hauptsächlich in den USA eine sehr verbreitete Kreditkarte. Im Jahr 1951 wurde die erste MasterCard in Umlauf gebracht und obwohl Diners Club damals schon sehr viele Mitglieder zählte wurde MasterCard bald auch außerhalb von New York immer beliebter und Ende der 60er Jahre begannen auch Visa und American Express Karten zu emittieren. Gegen Ende der 60er Jahre begann auch der Kreditkartenboom in Europa und Ende 2004 gab es weltweit bereits 2,2 Milliarden emittierte Kreditkarten die einen Umsatz von rund 5,6 Milliarden US-Dollar generierten.

3.2.5 Debitkarten

Debitkarten sind Plastikkarten, die an ein Konto gebunden sind. Im Gegensatz zur Kreditkarte erfolgt unmittelbar nach der Zahlung bzw. Bargeldbehebung, die Abbuchung vom Konto [ATML07].

Da das Privatkundengeschäft in den 60er Jahren immer größer und private Konten immer zahlreicher wurden, musste man eine Lösung finden, um die Bargeldbeschaffung und bargeldlose Zahlungen zu erleichtern. Der erste Vorläufer der Debitkarte war der Eurocheque und die Eurocheque-Karte [EURO07].

Als die Geldausgabeautomaten in den 70er Jahren bekannt wurden, wurden der Eurocheque-Karte weitere Funktionen hinzugefügt, wie die direkte Abbuchung von Bezügen mit Karte und Pin vom Girokonto.

Mitte der 80er Jahre war es möglich mit der Scheckkarte länderübergreifend Geldausgabeautomaten oder ATM (Automated Teller Machine) von kooperierenden Geldinstituten auf Basis des Interchange-Standards zu nutzen, was gleichzeitig zu einem Standard der Eurocheque-Karte wurde. Ein letzter Schritt zur umfassenden Debitkarte erfolgte Ende der 80er Jahre und Anfang der 90er Jahre, mit der Möglichkeit die Eurocheque-Karte bei POS-Terminals zu nutzen. Mit diesem letzten Schritt wurde die Eurocheque-Karte zur weltweit einsetzbaren Debitkarte und 1993 wurden die beiden Funktionen ATM und POS in einer Marke zusammengeführt und sind heute unter dem Namen Maestro bekannt.

3.2.6 Geldausgabeautomat und POS

Der Erfolg der Debit und Kreditkarte ist unter anderem auf die Innovationen POS Terminal und Geldausgabeautomat, der in Österreich Bankomat genannt wird, zurückzuführen. Bereits vor fast 90 Jahren hatte der Armenier Georg Simjian, der in die USA auswanderte, Pläne für eine Geldmaschine. Er konstruierte den ersten Geldausgabeautomaten [WTMS03], den die Citybank 1939 probeweise aufstellte. Dieser Versuch scheiterte allerdings bereits nach kurzer Zeit, wegen zu geringer Nachfrage.

1965 konzipierte der Amerikaner Don Wetzel [THLA06] eine Maschine, die durch Einschieben einer Karte und Eingabe eines Codes automatisiert Bargeld ausgeben sollte und gilt damit heute als einer der Erfinder des Geldausgabeautomaten. Aufgrund der noch nicht ausreichend vorhandenen Sicherheit, der zu geringen Informationskapazität und der mangelnden technischen Konzeption, wurden die ersten Geldausgabeautomaten von Banken nur selten eingesetzt und daher dauerte es eine Weile, bis sich der Erfolg einstellte.

Zeitgleich und unabhängig voneinander konzipierte auch Shepherd-Barron einen Geldautomaten [WOBR07]. Seine Vorlage waren die Automaten bei denen man mit Kleingeld Schokoladeriegel kaufen konnte. Sein Gerät sollte einen Scheck, mit einigen Daten zur Sicherheit für die Auszahlung und Identifizierung der Benutzer, einlesen können und ein Geldpaket mit maximal 10 Pfund ausgeben können. Am 27. Juni 1967 wurde dann der erste Geldausgabeautomat in der Barclay's Bank in London eingesetzt.

Das noch heute übliche Prinzip des Vergleichs eines Codes mit einer auf einer Karte gespeicherten Zahlenkombination geht auf den schottischen Ingenieur James Goodfellow [WTMS03] zurück, der ebenfalls Mitte der 60er Jahre im Auftrag der britischen Midland Bank einen Geldausgabeautomaten entwickeln sollte. Die Prototypen wurden nicht eingesetzt, allerdings meldete James Goodfellow 1966 einige Patente an, die auf seine Arbeit zurückgehen.

Die zweite verbesserte Generation der Geldausgabeautomaten konnte Anfang der 70er Jahre eingesetzt werden, wo bereits genormte Plastikkarten mit Sperrmöglichkeit zum Einsatz kamen. Allerdings erst durch den Fortschritt in der Hard- und Softwarebranche und der Ausstattung der Plastikkarten mit dem einheitlichen Standard des Magnetstreifens sowie der weltweiten Nutzung der Geräte durch Kooperation der Banken weltweit, erreichte die dritte Generation der Geldausgabeautomaten den Durchbruch.

Heute ist bereits die vierte Geldausgabeautomatengeneration im Einsatz [THLA06], die neben dem Magnetstreifen Standard bereits für den weltweit anerkannten EMV (Europay-MasterCard-Visa) Standard gerüstet ist und auch die Funktion der elektronischen Geldbörse übernehmen kann.

Aufgrund des Erfolges der Bankomaten gab es schnell Überlegungen, Bezahlungen bei Handels- und Dienstleistungsunternehmen durch POS (Point of Sale) Terminals, die den Geldtransfer vom Konto des Käufers auf das Konto des Verkäufers vornehmen, zu ersetzen, was bereits Ende der 60er Jahre Dale L. Reistad [THLA06] in seiner Vision der bargeldlosen Gesellschaft publizierte. Die erste Generation dieser Geräte fand wenig Anklang, da sie nur ein

eingegrenztes Gebiet und einen bestimmten Kundenkreis, Kommerz- und Privatkunden, abdeckte.

Der zweite Versuch POS Terminals in Umlauf zu bringen war erfolgreich. Man kam von den bankenbezogenen, lokalen Geräten ab und setzte bankenneutrale, interoperable POS-Systeme ein, die als Universal-POS-Terminals fungierten und Pin-Debitkarten ebenso wie Kreditkartentransaktionen mit Unterschrift abwickeln konnten.

Die POS Terminals der dritten Generation, die heutzutage im Einsatz sind, sind Hybridterminals und können Magnetstreifen ebenso wie EMV basierte Karten lesen. Durch den EMV Chip kann dann auch eine Prüfung der Echtheit der Karte vorgenommen werden, was das Fälschen von Karten schwieriger macht. Mittlerweile gibt es auch mobile POS Terminals, die mit GSM ausgestattet sind und für viele Branchen wie Restaurants, Marktstände etc. notwendig sind.

3.3 Klassifizierung des Zahlungsverkehrs

Der Zahlungsverkehr kann nach dem Zahlungszeitpunkt, der Zahlungsform und dem Transaktionsvolumen eingeteilt werden.

3.3.1 Einteilung nach dem Zahlungszeitpunkt

Am meisten verbreitet und einheitlich in der Literatur ist die Klassifikation nach dem Zahlungszeitpunkt. Es kann eine Einteilung nach dem Zeitpunkt an dem die Zahlung erfolgt getroffen werden [MDAU04].

Abbildung 10 zeigt die Einteilung nach dem Zahlungszeitpunkt in Pre-Paid, Pay-Now und Pay-Later [TLKS06] getroffen werden.

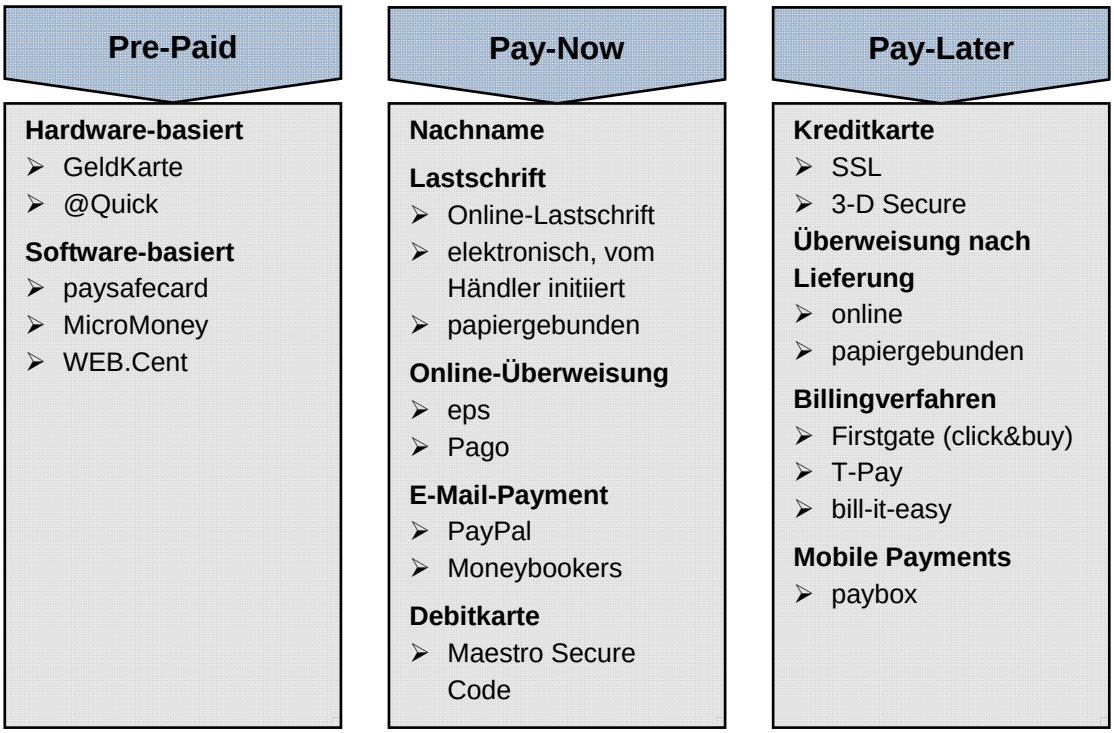


Abbildung 10 - Kategorisierung von Zahlungssystemen im Internet

3.3.1.1 Pre-Paid oder Pay-Before Verfahren

Bei diesem Verfahren erfolgt die Belastung beim Kunden im Vorhinein, also vor der eigentlichen Bezahlung eines Gutes oder Dienstleistung. Ein bestimmter Geldbetrag wird z.B. auf eine Karte aufgeladen und beim Kauf wird der Betrag von dem Guthaben des Kunden abgezogen.

Die Visa Prepaid Karte ist beispielsweise eine solche Karte wo Guthaben aufgeladen werden kann. In Österreich gibt es auch das Quick System, mit dem Bankomatkarten ausgestattet sind. Im Internet gibt es auch Möglichkeiten einen gewissen Betrag auf ein Konto aufzuladen und dann später damit zu bezahlen.

3.3.1.2 Pay-Now Verfahren

Pay-Now bedeutet, dass der fällige Betrag sofort nach Zahlungseinwilligung des Kunden beglichen wird. Dazu zählt neben dem Bargeld auch der Scheck, die Lastschrift und die Maestrokarte bzw. Bankomatkarte. Online gibt es diverse elektronische Lastschriftverfahren oder eine Online-Überweisungen.

3.3.1.3 Pay-Later Verfahren

Bei dieser Methode liegt der Zeitpunkt der Zahlung nach dem Kaufdatum. Klassisches Beispiel dafür sind Kreditkarten, wo eine Abbuchung meist einmal monatlich erfolgt oder auch der Kauf auf Rechnung.

3.3.2 Einteilung nach dem Transaktionsvolumen

Die Einteilung nach der Höhe der Zahlung wird in der Literatur unterschiedlich getroffen und auch die Kategorien die sich dann ergeben sind nicht einheitlich. Viele Autoren sprechen von Micro- und Macropayments [MAHÖ02]. Key Pousttchi [KEPO05] trifft noch eine weitere Unterteilung und spricht auch von Picopayment. Die genauen Betragsgrößen bzw. die Grenzen der einzelnen Kategorien sind nicht einheitlich geregelt und werden von jedem Autor unterschiedlich beziffert.

3.3.2.1 Picopayment

Key Pousttchi spricht bei Picopayment von Beträgen im Cent Bereich etwa 0,10 €, da solche Beträge in der Praxis jedoch kaum eine Rolle spielen ist der Begriff mittlerweile aus der Öffentlichkeit verschwunden. Dies wurde auch durch eine Anhebung der Grenzen für Micro- und Macropayment hervorgerufen.

3.3.2.2 Micropayment

Beim Micropayment zieht man mittlerweile die Grenze bei etwa 12 € [KEPO05] was etwa dem Betrag entspricht, bei dem eine Kreditkartenzahlung kostendeckend abgewickelt werden kann.

3.3.2.3 Macropayment

Von Macropayment spricht man, wenn die Zahlung einem höheren Betrag also über 12 € bis zu ca. 500 € entspricht und einen höheren Sicherheitsstandard erfüllen muss. Meist sind dies Zahlungen in Verbindung mit dem Kauf oder Verkauf von Waren.

3.3.3 Einteilung nach der Art des Transaktionsweges

Dannenberg und Ulrich [MDAU04] unterscheiden in Bezahlverfahren die absender- bzw. empfängerbasiert sind. Bei den absenderbasierten Verfahren betraut der Absender seine Bank mit der Überweisung des Geldbetrages während bei den empfängerbasierten Verfahren der Empfänger den Einzug der Forderung initiiert.

3.3.4 Einteilung nach eingesetzter Hard- oder Softwarekomponente

Es kann eine Systematisierung anhand der eingesetzten Soft- oder Hardwarekomponenten, in Karten- und Netzgeld [KASH99], unterscheiden werden. Es gibt reine softwarebasierte Lösungen bei denen man keine Karte oder Kartenlesegerät benötigt. Bei den hardwarebasierten Verfahren wird eine elektronische Geldbörse in Form von Smartcards benutzt, wie das österreichische Quick System, mit dem jede Bankomatkarte ausgestattet ist oder in Deutschland die Geldkarte. Eine genaue Einteilung ist jedoch schwierig, da fast immer Hard- und Softwarekomponenten genutzt werden.

4 Mobile Payment

Ein Mobilfunkanbieter hat die Aufgabe, Telekommunikationsdienstleistungen bereit zu stellen und erzielt dadurch Erlöse. Es gibt mittlerweile viele Dienste, die über die Telefonrechnung abgerechnet werden. Die Mobilfunkanbieter verfügen über eine komplexe Abrechnungsinfrastruktur, die man für alle Arten von mobilen Diensten nutzen kann. Für die Abrechnung werden einzelne Datensätze mit den Abrechnungsinformationen erstellt und im Rahmen der jeweiligen Abrechnungsbeziehung dem Kunden verrechnet.

Die Benutzung von mobilen Endgeräten für die Bezahlung von Gütern und Dienstleistungen wird von vielen Autoren unterschiedlich definiert. Key Pousttchi [KEYP03] definiert Mobile Payment als *„die Abwicklung von Bezahlvorgängen, bei der im Rahmen eines elektronischen Verfahrens mindestens der Zahlungspflichtige mobile Kommunikationstechniken (in Verbindung mit mobilen Endgeräten) für die Initiierung, Autorisierung oder Realisierung der Zahlung einsetzt“.* Mobile Payment ist somit eine Teilmenge von Mobile Commerce.

Key Pousttchi [KEPO05] definiert noch einen weiteren Begriff, das Mobile Billing, die Abrechnung von Telekommunikationsdienstleistungen durch einen Mobilfunkanbieter. In der Praxis werden mehrheitlich mobile Mehrwertdienste über die Telefonrechnung bzw. bei Prepaid-Kunden über das aufgeladene Guthaben abgerechnet. Wenn ein solcher Dienst über die Mobilfunkanbieter abgerechnet wird, dann bildet dies die Schnittmenge zwischen Mobile Billing und Mobile Payment, dargestellt in Abbildung 11 [KEPO05].

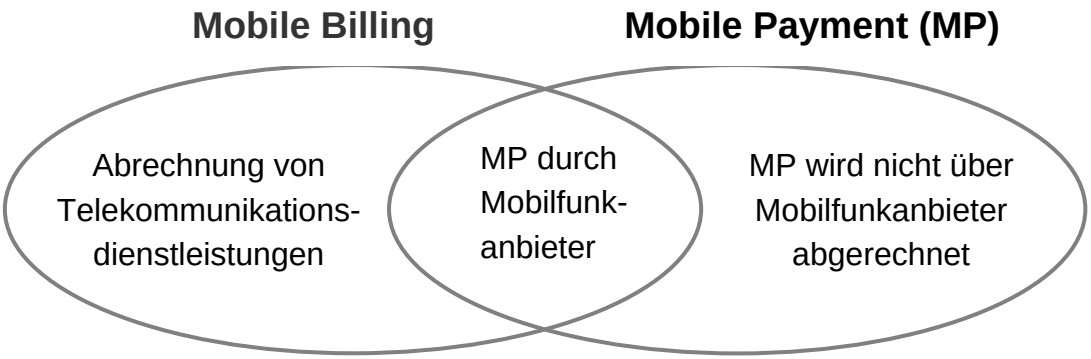


Abbildung 11 - Schnittmenge Mobile Billing und Mobile Payment

4.1 Kategorisierung der Zahlungsmodelle

Im Zuge einer Untersuchung im Rahmen des Projektes „MoMa – Mobiles Marketing“ des Bundesministeriums für Wirtschaft und Arbeit [THSB04], wurden Mobile Payment Zahlungsmodelle untersucht und die folgenden Modelle unterschieden.

4.1.1 Providermodelle

Das zurzeit am häufigsten verwendete Modell für die Zahlungsabwicklung ist das Providermodell, wo die Identifikations- und Abrechnungsmöglichkeiten der Netzanbieter genutzt werden um Zusatzdienste abzurechnen. Die Abrechnung erfolgt dabei über die Telefonrechnung des Kunden. Vorteile für den Kunden sind, dass ihre Kontoinformationen nur dem Provider bekannt sind, der in der Regel als vertrauenswürdig eingestuft wird.

Nachteil dieses Konzeptes für den Kunden ist jedoch, dass damit der Provider viele Informationen über ihn hat, die eventuell ausgewertet werden können. Da die Abhängigkeit für die Serviceanbieter vom Provider relativ hoch ist, ist ein dementsprechender Abstimmungsaufwand zwischen Serviceanbieter und Provider notwendig. Dieser Mehraufwand führt häufig dazu, dass der Provider den Betrieb des Dienstes selbst übernimmt, was die Entwicklung einer unabhängigen mobilen Dienstleistungsbranche hemmt.

4.1.2 Third Party Modell

Third Party Modelle funktionieren meist ohne Beteiligung des Providers, indem vertrauenswürdige Unternehmen in den Zahlungsprozess integriert werden und die finanzielle Abwicklung für den Serviceanbieter übernehmen. Zahlungspartner können Banken oder etablierte Unternehmen im Mobile Payment sein. Einerseits wird dem Kunden ein sicherer Zahlungsablauf, mit Rückverfolgbarkeit gewährleistet. Andererseits wird dem Serviceanbieter die Zahlungsfähigkeit des Kunden garantiert.

4.1.3 0900 Modelle

Bei diesem Modell werden die Dienste vom Dienstleister selbst abgerechnet und kostenpflichtige Telefon- oder SMS-Nummern verwendet. Die Dienstleistungen werden durch Anruf oder SMS einer kostenpflichtigen Nummer in Anspruch genommen, was eine leichte Bedienung von Seiten der Serviceanbieter gewährleistet. Ein großer Nachteil besteht jedoch dadurch, dass der Kunde mit dem Anruf eine Zahlung leisten muss, bevor er die gewünschte Leistung in Anspruch genommen hat. Dies setzt einen Vertrauensvorschuss gegenüber dem Anbieter voraus. Außerdem ist es für den Kunden oft schwer, die Tarife der kostenpflichtigen Nummern zu durchschauen, was die Akzeptanz verschlechtert.

4.1.4 Webkonto Modell

Beim Webkonto Modell muss der Kunde die Dienstleistung im Voraus bezahlen. Das Geld, welches der Kunde dem Anbieter (per Überweisung, Kreditkarte oder aber einer 0900 Nummer) überweist, wird ihm auf einem virtuellen Konto gutgeschrieben. Von diesem Konto werden alle anfallenden Kosten für Dienstleistungen abgezogen. Vorteilhaft hierbei ist, dass keine Kontodaten übertragen werden und die Abrechnung einfach und direkt von Seiten des Anbieters vorgenommen werden kann. Der Kunde hat außerdem eine gute Kostenkontrolle, da er nie mehr verbrauchen kann, als er auf seinem Webkonto aufgeladen hat. Jedoch spielt auch hier Vertrauen eine große Rolle, da das Geld im Voraus bezahlt werden muss. Solche Systeme sind in der Regel nicht interoperabel und daher muss der Kunde für jeden Dienstleister auf ein

getrenntes Konto einbezahlen. Dadurch wird viel Geld gebunden und es fällt schwer den Überblick zu behalten.

4.1.5 Abomodell

Dieses Modell spielt bei Picopayments eine große Rolle, da der Aufwand einer Einzelabrechnung hier zu groß wäre. Solche Dienste werden auch häufig als Abonnements verkauft und entweder über die Zeit der Nutzung oder der Menge kumuliert abgerechnet. Die Bezahlung solcher Abonnements erfordert die Anwendung eines Zahlungssystems. Entweder wird das Geld vom Kunden vorab bezahlt, oder der Anbieter stellt den Dienst erst nach Ablauf des Abonnements in Rechnung. Häufig werden solche Abodienste vom Netzanbieter verwaltet und so über die Telefonrechnung abrechnet.

4.1.6 „Kostenloser“ Dienst

Es kann jedoch auch sein, dass mit der Nutzung eines Dienstes nicht nur ein Nutzen für den Kunden, sondern auch ein Nutzen für den Anbieter verbunden ist. Solche Dienste werden dem Kunden häufig kostenlos zur Verfügung gestellt und die Kosten werden von den Anbietern der Informationen getragen.

4.2 Bezahlsysteme im Internet

Neben den traditionellen Zahlungsmethoden gibt es eine Vielzahl an Bezahlmöglichkeiten, die im Internet angeboten werden und es kommen immer wieder neue hinzu [SHLF04]. In den letzten Jahren ist jedoch ein Rückgang an bestehen Zahlungssystemen zu erkennen, da sie vom Konsumenten nicht akzeptiert wurden.

Die Electronic Payment Systems Observatory [EPSO08] hat bereits über 100 Internetzahlungsmittel nach ihrem technischen Aufbau sowie ihrer Sicherheits- und Datenschutzkriterien untersucht. Demnach kann der österreichische Online-Handel auf ein gutes Dutzend unterschiedlicher Internetzahlungs-systeme zurückgreifen.

Die Akzeptanz elektronischer Zahlungsmittel steigt im Vertrieb digitaler Inhalte insbesondere bei Multimedia-Angeboten (Klingeltöne, Musik, etc.) [ECIN04]. Die Höhe dieser Beträge befindet sich im Micropayment Bereich und wäre mit der Kreditkarte nicht kostendeckend abzuwickeln, was den Einsatz elektronischer Zahlungsmittel begünstigt.

Die Verwendung von Kreditkarten im Internet funktioniert grundsätzlich gleich wie in der realen Welt, jedoch kommt die Tatsache hinzu, dass Händler und Kunde sich nicht kennen und weder die Karte noch der Kunde für den Händler sichtbar sind. Es gibt drei Möglichkeiten für eine Kreditkartentransaktion im Internet, eine unsichere Transaktion, eine Transaktion mittels SSL (Secure Socket Layer) und Transaktionen mittels Secure Payment Applications und Universal Cardholder Authentication Field [SHLF04]. Für das sichere Bezahlen mit Kreditkarten oder Bankomatkarten gibt es Maestro SecureCode, Verified by Visa und MasterCard SecureCode mittels 3-D Secure.

Da Electronic Payment laut Khodawandi, Pousttchi und Wiedemann [DKPW03] als Einstiegsbezahlszenario für M-Payment gesehen wird, gibt dieses Kapitel einen Auszug der derzeit existierenden Bezahlsysteme im Internet.

4.2.1 @Quick

Das @Quick System [QUIC08] zählt zu den Prepaid Zahlungssystemen. Seit 2001 kann die österreichische elektronische Geldbörse Quick, welche sich auf jeder österreichischen Maestrokarte und auch auf einigen Studentenausweisen österreichischer Universitäten befindet, auch für Zahlungen im E-Commerce also Internet eingesetzt werden. Dafür werden ein handelsüblicher Chipkartenleser und eine spezielle, kostenlos verfügbare Software, sowie ein geladener Quick-Chip benötigt. Im Jahr 2005 wurden knapp 8.600 @Quick-Transaktionen mit einem Umsatzvolumen von rund 2,2 Mio. Euro durchgeführt. In Europa existieren unterschiedliche Formen von elektronischen Geldbörsen, jedoch sind diese nicht interoperabel.

4.2.2 Geldkarte

Die Geldkarte [GEKA08] ist auf dem deutschen Markt ebenso wie das Quick System eine auf Smartcard Technologie basierende elektronische Geldbörse, die seit 2002 im Internet verwendet werden kann. Dafür wird ebenfalls ein von der deutschen Kreditwirtschaft zugelassenen Chipkartenleser mit eigener Tastatur und Display benötigt.

4.2.3 Paysafecard

Die Paysafcard [PAYS08] ist in Österreich seit 2000, seit 2001 in Deutschland und in vielen weiteren Ländern erhältlich. Man kann sie in über 90.000 Verkaufsstellen in ganz Europa sowie online erwerben und sie ist in Österreich mit einer Nominale von 10 €, 25 €, 50 € und 100 € erhältlich. Die Paysafecard ist eine nicht aufladbare Einwegkarte. Die Unique Selling Proposition ist die anonyme Zahlung, mittels Eingabe eines Codes (welcher sich auf der Karte befindet), im Internet. Der zu begleichende Betrag wird anschließend vom virtuellen Konto abgebucht.

4.2.4 MicroMoney

MicroMoney [SHLF04] auf dem deutschen Markt ähnelt sehr der Paysafecard, besitzt jedoch einen weiteren Pin Code für die Verwendung als normale Telefonkarte. Die Guthabenverwaltung erfolgt serverbasiert.

4.2.5 WEB.Cent

Bei WEB.Cent [WEBC08] handelt es sich um ein serverbasiertes Konto auf dem deutschen Markt, das mit traditionellen Bezahlmethoden aufgeladen werden kann. Durch das Anklicken des WEB.Cent Logos bei Akzeptanzpartnern kann der Zahlungsvorgang gestartet werden. Durch Eingabe von Username und Passwort werden die Zahlungsdetails angezeigt und durch Bestätigung des Kunden kann der Zahlungsvorgang abgeschlossen werden.

4.2.6 PayPal

PayPal [PAYP08] ist unter E-Mail-Zahlungssystem einzuordnen. Es kommt aus den USA und in Deutschland und Österreich kann es seit 2004 genutzt werden. PayPal ist in zahlreichen Ländern Europas mit länderspezifischen Websites und Anpassung an die jeweiligen Kundenbedürfnissen vertreten.

Bei diesem Zahlungssystem werden keine persönlichen Daten an den Zahlungsempfänger weiter gegeben. Sender und Empfänger müssen bei PayPal registriert sein und für die Bezahlung ist lediglich die E-Mail-Adresse des Empfängers notwendig.

4.2.7 Moneybookers

Moneybookers [MONB08] ist dem System PayPal sehr ähnlich. Moneybookers Limited ist ein weltweites kostenpflichtiges Geldtransfer-Service, bei dem der Empfänger das Geld ebenso wie bei PayPal sofort erhält.

4.2.8 Kreditkartentransaktion über SSL

Laut einer Erhebung von ARGE Daten [AGED08] verwendeten 2005 60 % aller österreichische OnlineShops noch keine SSL Verbindung. Im Gegensatz dazu setzten bereits 70 % aller internationalen OnlineShops auf die Verschlüsselung. Diese Zahlen sind jedoch sehr verwunderlich, da einerseits die Sorge um die Sicherheit der Daten das wichtigste Hindernis der österreichischen Kunden für einen Onlinekauf ist [ZEGE05] und andererseits laut einer EU-Richtlinie aus dem Jahr 2002 die Sicherheit der Übertragung persönlicher Daten [HONC02] gefordert wurde. Der Data Security Standard auf den sich MasterCard, Visa, American Express, Dinersclub, Discover und JCB gemeinsam geeinigt haben, ist seit Juni 2005 verpflichtend und schreibt Mindeststandards für die Übertragung von persönlichen Daten im Internet vor und gewährleistet die Datensicherheit beim Einsatz von Kreditkarten.

SSL wurde von der Firma Netscape und RSA Data Security entwickelt [BSIF08] und gewährleistet, dass Daten während der Übertragung nicht gelesen oder manipuliert werden können und die Verwendung ist durch das „s“, das in der

URL beispielsweise bei „https://....“ erscheint ersichtlich. Bei jedem Aufruf einer sicher Seite mittel SSL prüft der Browser ob der Anbieter ein gültiges SSL-Zertifikat von der Zertifizierungsstelle besitzt. Der Nachfolger von SSL 3.0 ist Transport Layer Security und er erweitert die Palette der einsetzbaren Verschlüsselungsverfahren um den Advanced Encryption Standards und basiert auf einem noch komplexen Verschlüsselungsverfahren wie SSL.

4.2.9 3-D Secure

3-D Secure löst das frühere SET System (Secure Electronic Transaction Protokoll) ab, das aufgrund der langwierigen und für den Kunden umständlichen Handhabung am österreichischen Markt nicht den gewünschten Erfolg eingefahren hat [OENB08]. Anders als beim SET System benötigt der Kunde hier keine zusätzliche Software, lediglich der Händler muss ein 3-D Merchant Plugin installieren. Der große Vorteil dieser Technik ist, dass Händler die das System benutzen von einer Zahlungsgarantie profitieren, da die Kreditkarteninstitute selbst die zusätzliche Authentifizierung des Kunden vornehmen, wodurch eine Abstreitbarkeit der Zahlung seitens des Kunden unmöglich wird. Da dieses Protokoll sehr allgemein entworfen wurde, kann es beispielsweise auch für Debitkarten genutzt werden.

4.2.10 Maestro SecureCode bzw. MasterCard SecureCode

Maestro bzw. MasterCard SecureCode ist ein Verfahren, das MasterCard für sichere Zahlungen im Internet für MasterCard Kreditkarten entwickelt hat [TOWO08]. Seit 2005 gibt es erstmals auch die Möglichkeit mit diesem System mit der Bankomatkarte im Internet sicher zu bezahlen. Für die Bezahlung muss man die 16-stellige Maestro Secure Code Kartennummer, das Ablaufdatum sowie ein selbstgewähltes geheimes Passwort, den SecureCode, eingeben.

4.2.11 Verified by Visa

Verified by Visa [VEVI08] ist eine 3-D Secure basierte Lösung und wurde im Jahr 2003 von Visa eingeführt [TLKS06]. Es gewährleistet einen sicheren Zahlungseingang für Händler bzw. die Echtheit des Händlers für den Kunden.

Um dieses Service nutzen zu können muss der Händler ein Händler Plug-In installieren und es mit seiner existierenden Online-Shop Kreditkarten Zahlungsapplikation verbinden. Der Kunde muss ebenfalls für Verified by Visa angemeldet sein.

Tätigt ein Kunde bei einem registrierten Verified by Visa Händler einen Kauf, wird das Händler Plug-In aufgerufen und der Kunde erhält einen Verified by Visa Screen wo er die Informationen des Händlers überprüfen kann und sein Passwort eingeben muss. Nach korrekter Eingabe des Passworts, wird der Kauf abgeschlossen.

4.2.12 Online-Überweisung

Die Online-Überweisung ist ein Zahlungssystem, das auf das von österreichischen Banken entwickelte Internet-Bankingsystem aufsetzt und unter EPS-Online Überweisung in Online-Shops geführt wird. Wenn ein Käufer diese Zahlungsmöglichkeit auswählt und seine Bank eingibt, dann öffnet sich die bekannte Internet-Banking Maske und mit einem TAN wird die Zahlung bestätigt. Vorraussetzung ist natürlich ein Konto bei einer österreichischen Bank. In Deutschland gibt es ein ähnliches System namens PAGO. [TOWO08]

4.2.13 Click&Buy von Firstgate

Click&Buy von Firstgate [FICB08] fällt unter die Kategorie Billingverfahren. Diese treten typischerweise im Micropayment Bereich auf und werden kumuliert meist einmal monatlich abgerechnet. Dieses System gibt es seit 2000 in Deutschland und seit 2004 wird es auch in Österreich aktiv vermarktet. Für die Verwendung ist eine einmalige Registrierung Vorraussetzung und die Rechnung wird monatlich vom Girokonto oder der Kreditkarte abgebucht.

4.2.14 T-Pay

T-Pay [FICB08] ist das konkurrierende Verfahren zu Click&Buy. Bei diesem System ist eine Registrierung Vorraussetzung. Der Freischaltcode wird

anschließend per Post zugeschickt. Abgerechnet wird dann monatlich entweder per Telefonrechnung, Kreditkarte oder Lastschrift.

4.2.15 bill-it-easy

Bill-it-easy [BIEA08] ist seit 2004 aktiv und wird von Montax Payment Services GmbH, einem Tochterunternehmen von Kapsch und DIMOCO betrieben. Das System ist für den Micropayment Bereich ausgelegt und die Abrechnung erfolgt entweder über den Internet-Provider oder den Mobilfunkanbieter.

4.3 M-Payment Verfahren

Die Wirtschafskammer [WKOB06] sowie Stroborn im Journal of Business Research [SHLF04] listen als einziges richtiges mobiles Zahlungsverfahren in Österreich mittels Mobiltelefon das System Paybox auf. Das Mobiltelefon ist mittlerweile zum ständigen Begleiter geworden die Konsumenten setzen es bereits gerne und regelmäßig zum Bezahlen ein. Viele Autoren zählen auch Bezahlverfahren, die über die Mobiltelefonrechnung abgerechnet werden zu den M-Payment Verfahren.

Paybox

Paybox [PAYB08] ist ein Mobile Payment Verfahren, dass sich vor allem in Österreich etabliert hat und weit verbreitet ist. Es wurde im Jahr 2000 entwickelt und seit 2001 ermöglicht die Paybox Austria AG [JOPU06] das Bezahlen mit dem Mobiltelefon. Seit 2003 ist das Unternehmen eine Tochterfirma der Mobilkom Austria AG.

Die Voraussetzungen um dieses Verfahren nutzen zu können sind der Besitz eines Mobiltelefons, eines österreichischen Bankkontos und die Anmeldung bei Paybox.

Laut einer Studie des Markt- und Meinungsforschungsinstituts FESSL [FESSL04] haben die Österreicher eine große Affinität und ein ständig steigendes Interesse am mobilen Bezahlen.

Paybox bietet verschiedene Produkte mit unterschiedlichen Vorteilen an, die von jedem Mobiltelefonbesitzer jedes Mobilfunkanbieters genutzt werden können. Das Service „Paybox public“ kann kostenlos genutzt werden und bietet nur ein eingeschränktes Service. Das kostenpflichtige Service „Paybox classic“ beinhaltet ein erweitertes Angebot und ermöglicht auch die Abbuchung direkt vom Bankkonto.

Nur Kunden vereinzelter Mobilfunkanbieter können das „Paybox public“ Service ohne Registrierung nutzen. Die Rechnung wird jeweils mit der nächsten Telefonrechnung abgebucht.

Zur Bezahlung gibt man einfach die Mobiltelefonnummer oder eine eigens eingerichtete Wunschnummer bei Paybox weiter und nach wenigen Sekunden erhält man einen automatischen Anruf und hört den Betrag sowie den Zahlungsempfänger. Durch Eingabe eines 4-stelligen Pin Codes wird die Zahlung bestätigt. Im Anschluss erhält der Kunde eine SMS bzw. E-Mail als Zahlungsbestätigung.

5 Mobile Contactless Payment

Wie die Entwicklung des Zahlungsverkehrs zeigt, geht der Trend immer mehr in Richtung bargeldloses Bezahlen und der Zahlungsvorgang soll immer einfacher und bequemer werden [BRAN05].

Laut einer Studie des Marktforschungsunternehmens Informa Telecoms & Media [INTM08] gibt es weltweit 3,3 Milliarden abgeschlossene Mobilfunk-verträge und die Mobiltelefonquote liegt in Europa, Amerika und Asien bei über 100 Prozent. In Entwicklungsländern liegt die Verbreitung von Mobiltelefonen noch unter 10 Prozent.

In Österreich liegt die Rate der aktiven SIM-Karten im Bezug auf die Bevölkerung laut der Rundfunk und Telekom Regulierungs-GmbH [RTRG08] bei 113 % im Jahr 2007, wie in Abbildung 9 ersichtlich ist. Statistisch gesehen besitzt somit jeder Österreicher zumindest ein Mobiltelefon.

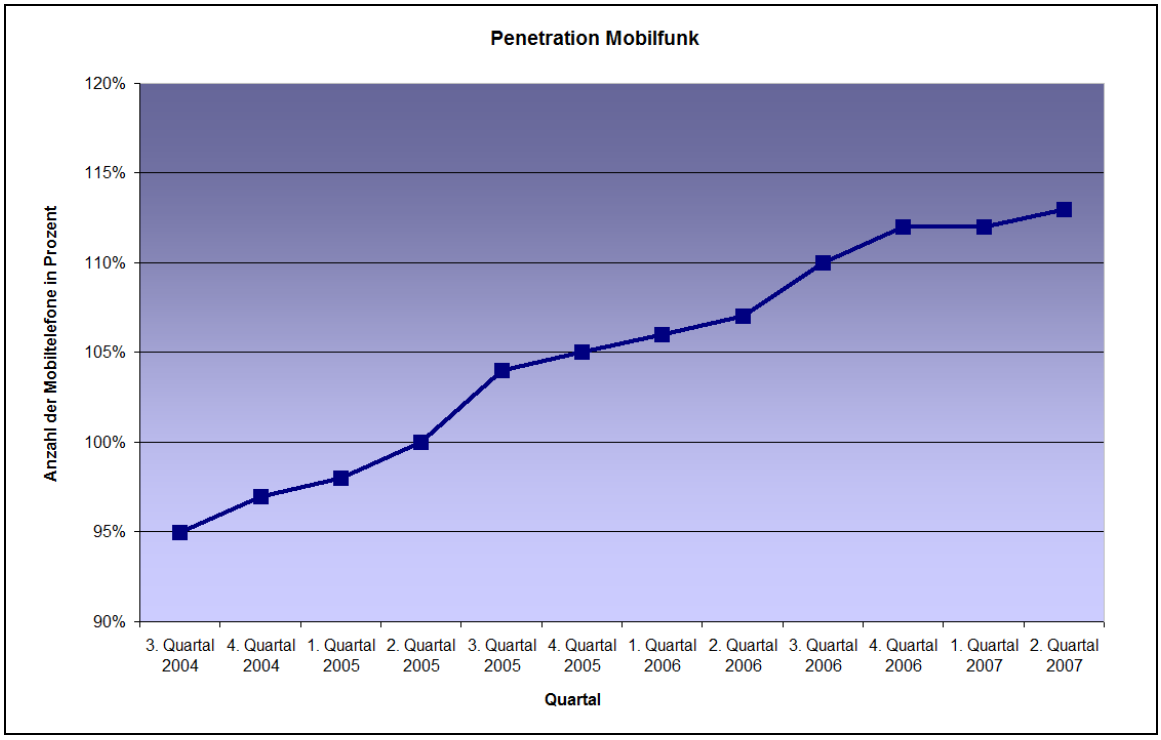


Abbildung 12 - Mobilfunkbesitzer in Österreich

Das Mobiltelefon ersetzt mittlerweile Kalender, Fotoapparat, Mail Clients, MP3-Player, Radio u.v.m. Es hat sich mittlerweile zum ständigen Begleiter entwickelt und ist meistens durchgehend aktiviert. Lediglich die Geldbörse konnte es bisher noch nicht ersetzten.

Durch NFC werden neue Möglichkeiten eröffnet und das Bezahlen mit dem Mobiltelefon soll nun durch diese Technologie in den nächsten Jahren möglich werden [ORTI06]. Durch die Ausstattung eines geeigneten RFID-Chips in ein beliebiges Gerät, kann es zur elektronischen Geldbörse umfunktioniert werden. Das Mobiltelefon wird immer mehr zu einem essentiellen Life Management Werkzeug und die Anwender werden von einer integrierten Zahlungsfunktion profitieren [GSMW08].

Dem Mobile Contactless Payment wird in vielen Studien [PBST02] und von vielen Autoren ein hohes Potential zugesprochen, jedoch wird es dafür auch notwendig sein spezielle Angebote und Geschäftsmodelle auf mobile Endgeräte zu übertragen.

Vor knapp einem Jahr hat die globale Handelsorganisation für Mobilnetzbetreiber, die GSM Association [GSMW08] die Initiative „Pay-Buy Mobile“ gestartet. Dieses Projekt soll den weltweiten Einsatz von Mobiltelefonen für POS Zahlungen mit Contactless NFC-Technologie ermöglichen und vorantreiben.

Eine wesentliche Voraussetzung für den Erfolg von M-Payment ist die Bereitstellung effizienter und sicherer Abwicklungsformen des Zahlungs-vorganges [MOMA02]. Da Endanwender neuen Technologien gerade im Zahlungsverkehr sehr skeptisch gegenüberstehen, ist es besonders wichtig, die Bedürfnisse des Konsumenten genau zu kennen [DAÖÖ07] und Lösungen zu entwickeln, die genau darauf abgestimmt sind.

Versuche im Bereich Contactless Payment Systeme laufen derzeit auf der ganzen Welt. Besonders affine Märkte beim Bezahlen mit dem Mobiltelefon über NFC sind jene in Ostasien oder Nordamerika [ECIN07]. In den europäischen Ländern ist Mobile Contactless Payment jedoch noch kaum

bekannt und Skeptiker [CHHO08] sind derzeit nicht der Ansicht dass man das Mobiltelefone bald als gängiges Zahlungsmittel verwenden können wird.

An der Initiative „Pay-Buy Mobile“ nehmen derzeit vierzehn Mobilfunkbetreiber teil, mit zusammen über 900 Millionen Mobiltelefonkunden und dem Ziel einen gemeinsamen globalen Standard für Zahlungen via Mobiltelefon und nahtlos integrierter systemübergreifender Zahlungsdienste zu entwickeln.

Da Kunden Innovationen gerade im Zahlungsverkehr meistens sehr skeptisch gegenüber stehen, muss der Sicherheit besonderes Augenmerk entgegengebracht werden [KEPO03]. Im Folgenden werden potentielle Gefahren von Mobile Contactless Payment Systemen identifiziert, deren Risiken analysiert und sicherheitstechnische Kriterien abgeleitet. Durch die Einhaltung dieser Kriterien soll die Akzeptanz beim Endanwender erhöht werden.

5.1 M-Payment Systeme

Mobile Payment wird grundsätzlich in vier Bezahlszenarien unterschieden [NKPT02] - Transaktionen im stationären Internet, im klassischen Handel, an Automaten und zwischen Privatpersonen.

Khodawandi, Pousttchi und Wiederman [DKPW03] spezifizieren dieses Modell etwas näher. Die folgende Tabelle stellt die möglichen Bezahlszenarien im Mobile Payment in Anlehnung an [DKPW03] dar.

Szenario	Beschreibung	Konkurrierendes Bezahlsystem
Mobile Commerce Szenario	Mobile Anwendungen und Dienste, z.B. kontextsensitive Information	---
Electronic Commerce Szenario	Alle Arten B2C EC mit Ausnahme von MC, also etwas Kauf von Waren oder Inhalten via Internet	Offline Zahlung Bankomat-/Kreditkarte E-Payment
Stationärer Händler Szenario *(Person)* *(Automat)*	Klassischer Handel am POS mit Transaktion zwischen einer Person (Kunde) und → einer Person (z.B. Kassier) → einem Automaten	Bargeld Bankomat-/Kreditkarte Geldkarte/Quick
C2C Szenario	Geldtransfer zwischen privaten Personen (Kunden)	(Bargeld) (Offline-Zahlung)

Tabelle 4 - Bezahlszenarien im Mobile Payment

Mobile Payment wird, wie im Kapitel 4 angeführt, definiert als *„die Abwicklung von Bezahlvorgängen, bei der im Rahmen eines elektronischen Verfahrens mindestens der Zahlungspflichtige mobile Kommunikationstechniken (in Verbindung mit mobilen Endgeräten) für die Initiierung, Autorisierung oder Realisierung der Zahlung einsetzt“* bezeichnet.

Drahtlos und mobil sind in der Kommunikation grundsätzlich zu Unterscheiden [JÜKU03]. Drahtlos bzw. contactless bedeutet Datenaustausch über Funksignale, ohne physikalische Verbindung. Mobil bedeutet, dass die Portabilität des Kommunikationsgerätes, wie beispielsweise bei einem Mobiltelefon, eine wesentliche Eigenschaft darstellt.

Bei einer herkömmlichen Zahlung mittels Kreditkarte oder Bankomatkarte werden die notwendigen Daten für den Zahlungsvorgang mit speziellen Lesegeräten vom Magnetstreifen oder Chip ausgelesen und über physikalische Verbindungen übertragen.

Beim Mobile Contactless Payment funktioniert die Datenübertragung drahtlos und soll mittels der speziellen NFC Übertragungstechnologie erfolgen. Der Kunde muss also am Point of Sale anwesend sein, um diese Technik nutzen zu können. Daher wird nun für weitere Untersuchungen in dieser Arbeit nur das Szenario stationärer Händler betrachtet.

5.2 Wertschöpfungskette

Die Wertschöpfungskette von Mobile Contactless Payment setzt sich aus acht Kernaktivitäten entsprechend [ROCO02], wie in der folgenden Abbildung dargestellt, zusammen.

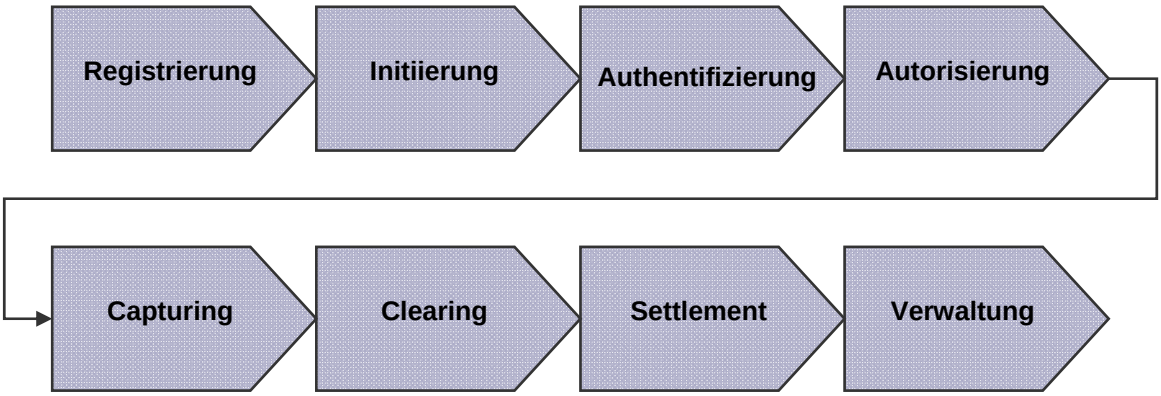


Abbildung 13 - Wertschöpfungskette Mobile Payment

Registrierung ist die Kundengewinnung. Dabei werden gezielte Marketingaktivitäten gesetzt um Händler und Konsumenten als Kunden zu binden. Dies ist einer der wichtigsten Aktivitäten, da ein großer Kundenstamm einer der Haupterfolgsfaktoren für die Einführung eines Zahlungsverfahrens gilt.

Initiierung ist die Herstellung der elektronischen Verbindung zwischen Konsument, Händler und Mobile Contactless Payment Anbieter.

Authentifizierung wird immer vom Mobile Contactless Payment Anbieter durchgeführt und ist die zentrale Aktivität innerhalb der Wertschöpfungskette, da sie grundlegend für die Transaktion ist.

Die **Autorisierung** wird entweder vom Mobile Contactless Payment Anbieter oder von Dritten gemacht. Es ist letztendlich die Freigabe einer Zahlung und hier spielt das Ausfallsrisiko eine große Rolle. Entsprechend der Zahlungsbeträge beim Micro- oder Macro-Payment wird die Autorisation unterschiedlich durchgeführt.

Capturing bezeichnet die systemseitige Erfassung der Transaktion in einer Datenbank.

Die Vermittlung der Zahlungsdaten zwischen Issuer (Kartenausgebende Bank) und Aquirer (vertragsunternehmensabrechnende Bank) wird als **Clearing** bezeichnet. Das ist der Prozess der Übertragung, Abstimmung und teilweise der Bestätigung von Zahlungsanweisungen vor der eigentlichen Ausführung.

Die eigentliche Zahlung, die aus dem Clearing zwischen zwei oder mehreren Parteien entsteht, wird als **Settlement** bezeichnet.

Unter der Aktivität **Verwaltung** werden die Rechnungser- und Zustellung, sowie sämtliche Aktivitäten im Bereich Kundenservice und Zahlungsausfälle zusammengefasst.

Diese Prozesse sind beim Mobile Contactless Payment jedoch die gleichen wie bei den traditionellen Bezahlverfahren.

5.3 Handelnde Personen

Alle Parteien, die beim Mobile Payment beteiligt sind, können in der folgenden Abbildung zusammengefasst werden [RCRM03].

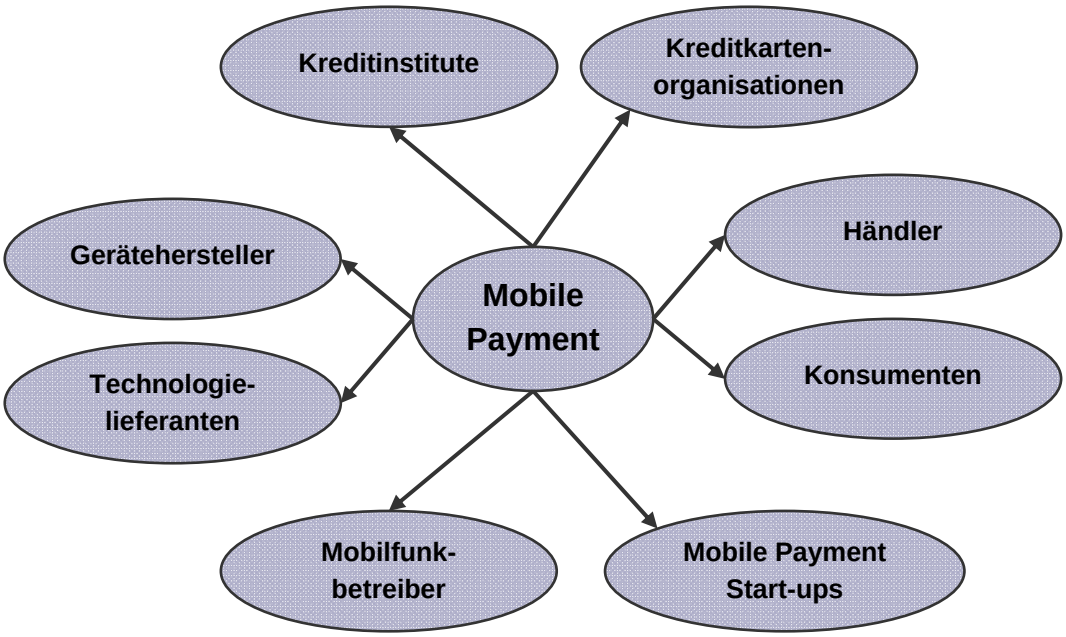


Abbildung 14 - Mobile Payment Marktteilnehmer

An einem Bezahlvorgang sind generell zumindest drei Parteien - der Kunde, der Händler und der Anbieter des Bezahlverfahrens – involviert [PBST02].

Kreditkartenorganisationen und Kreditinstitute treten als Issuer und Acquirer auf, indem sie versuchen, Kunden und Händler zu akquirieren. Der Acquirer stellt dem Händler die notwendige Infrastruktur für die Akzeptanz, meist gegen eine bestimmte Gebühr, zur Verfügung.

Bevor eine Zahlung abgeschlossen werden kann, muss eine Autorisierung vom Issuer erfolgen. Dadurch kann sichergestellt werden, dass der Kunde über das notwendige Kapital für diese Zahlung verfügt und die Karte gültig ist.

Der Händler bietet die Möglichkeit an, die entsprechende Zahlungsmethode zu verwenden. Sein Bestreben ist es, möglichst viel Umsatz zu generieren und dem Kunden dafür die optimalen Bedingungen zu bieten. Er möchte die ihm zustehende Zahlung sichergestellt wissen. Der Händler ist bei der Zahlung dafür verantwortlich, dass alle definierten Bestimmungen, die seitens des Acquirers gefordert werden, eingehalten werden. Durch die Autorisierung der Zahlung und die Einhaltung der Bestimmungen des Acquirers hat der Händler

die Sicherheit, die monetäre Gegenleistung für seine Dienstleistung oder Ware zu erhalten.

Beim Mobile Payment sind die Teilnehmer Gerätehersteller, Technologielieferanten, Mobilfunkbetreiber und Mobile Payment Start-ups neu dazugekommen.

Gerätehersteller liefern zusammen mit den Technologielieferanten die entsprechenden Endgeräte für Mobile Payment. Die verwendeten Geräte für Mobile Payment müssen auf die Bedürfnisse der Kunden ausgerichtet sein, um die Akzeptanz des Kunden zu gewährleisten.

Mobilfunkbetreiber sind für die Infrastruktur zuständig. Sie stellen das Netz, in dem kommuniziert wird, bzw. Daten versendet werden, zur Verfügung.

Mobile Payment Start-ups sind Organisationen, die versuchen, Mobile Contactless Payment zu etablieren. Banken, Kreditkartenorganisationen, Mobilfunkbetreiber und Mobile Payment Start-ups zählen grundsätzlich zu den Marktteilnehmern, die das Potential haben, Mobile Contactless Payment Dienstleistungen anzubieten.

Die Mobilfunkbetreiber gelangen in eine starke Position, wenn das Bezahlen mit dem Mobiltelefon flächendeckend eingesetzt und auf breiter Basis akzeptiert wird [SGJT01]. Mobilfunkanbieter verfügen über eine breite Kundenbasis und bringen Erfahrung in Abrechnungsprozessen mit. Sie haben das Potential, Clearing und Settlement auch für das Mobile Contactless Payment anzubieten. Mobilfunkanbieter sehen ihren Vorteil in der höheren Kundenbindung. Im Gegensatz zu Banken sind Mobilfunkanbieter bis jetzt mit starken Kundenfluktuationen konfrontiert, was zu hohen Kosten führt.

Die Netzbetreiber sind von den Technologielieferanten stark abhängig. Das Potential von Mobile Contactless Payment für Mobilfunkanbieter hängt stark vom Reifegrad der technischen Realisierung ab. Bei den derzeit realisierten Lösungen von Mobile Contactless Payment in Österreich fallen lediglich SMS Gebühren oder normale Gesprächsgebühren für Netzbetreiber an. Bei

Zahlungen die über das Micropayment hinausgehen geht es um wesentlich höhere Summen, womit ein entsprechend höheres Risiko für Netzbetreiber verbunden ist. Zusätzlich nicht zu vernachlässigen ist, dass für ein vollständiges M-Payment eine Banklizenz oder mindestens eine EMI- (Electronic Money Institute) Lizenz notwendig ist.

Banken und Kreditkartenunternehmen haben Erfahrung im Zahlungsverkehr und Risikomanagement. Kreditkartenunternehmen bringen außerdem Know-How bei grenzüberschreitenden Zahlungen mit, da sie international tätig sind. Aus diesem Grund wird diese Branche wahrscheinlich nie komplett aus dem Zahlungsprozess verdrängt werden können.

Auch Gerätehersteller haben ein starkes Interesse an der breiten Akzeptanz von M-Payment, da sich dadurch eine starke Nachfrage an Mobiltelefonen ergeben wird. Sie bringen jedoch im Gegensatz zu Mobilfunkanbietern, Banken und Kreditkartenunternehmen keine Erfahrung im Zahlungsverkehr mit. Daher werden sie im M-Payment Prozess nicht die zentrale Rolle spielen. Sie haben aber sehr großen Einfluss darauf, ob und in welcher Form sich Mobile Contactless Payment durchsetzt. Gerätehersteller bestimmen maßgeblich die Gestalt und Ausstattung der Endgeräte, weshalb sie für andere Interessens-gruppen für Kooperationen von großer Wichtigkeit sind.

Wenn man die geschichtliche Entwicklung von Zahlungssystemen analysiert, so hat sich gezeigt, dass die Entscheidung über die Durchsetzung eines Verfahrens am Markt nicht gleichmäßig zwischen den beteiligten Personen aufgeteilt ist. Es hat sich herausgestellt, dass im Falle eines Zielkonfliktes zwischen den Parteien die Entscheidung allein der Kunde trifft. Diese Tatsache kann an zahlreichen Beispielen belegt werden. So gab es etwa bei der Einführung der Kreditkarte hohen Widerstand seitens der Händler wegen der zu hohen Gebühren. Nichtsdestotrotz war dieser Innovationsschritt aufgrund der Kundenforderung nicht mehr aufzuhalten.

Kunden sind nicht oder kaum bereit, Bezahlverfahren anzunehmen, die nicht ihren Bedürfnissen entsprechen, wie beispielsweise die Geldkarte am Deutschen Markt, das österreichische Quick System oder aus dem E-Commerce Bereich das SET Verfahren, die alle im praktischen Einsatz gescheitert sind.

6 Analyse bestehender Mobile Contactless Payment Systeme

Es gibt mittlerweile viele verschiedene Mobile Contactless Payment Implementierungen im In- und Ausland. Im Folgenden werden die wesentlichen Verfahren von bestehenden Implementierungen analysiert. Die daraus resultierenden Erfahrungen und Schwächen sind sehr wertvoll für zukünftige Lösungen.

6.1 Nationale Mobile Contactless Payment Lösungen

Seit November 2007 kann man in Österreich mittels NFC-fähigen Mobiltelefons bezahlen und es sind bereits etwa 3000 NFC Mobiltelefone im Umlauf [MOBI07]. Derzeit können jedoch nur Kunden eines einzigen Mobilfunk-anbieters in Österreich dieses Service nutzen. Sie können damit ganz einfach lediglich durch Berührung [ANLI07], wie in Abbildung 10 [NFCC08] dargestellt, bezahlen.

Abbildung 15 - Bezahlen mit NFC

Es gibt derzeit nur ein einziges NFC-fähige Mobiltelefon am österreichischen Markt. Dieses Modell ist mit einem RFID Chip ausgestattet. In einem nächsten Schritt wird versucht, NFC auf der SIM Karte zu integrieren, was weitere

Anwendungsszenarien, wie die Simulation von Kreditkarten, ermöglichen wird [ITME07].

6.1.1 Touchpoints der Wiener Linien

Die Touchpoints von den Wiener Linien, bei denen das Bezahlen mittels NFC möglich ist, sind passive NFC Tags, die über das NFC-fähige Mobiltelefon aktiviert werden [NFCC08]. Um den Kontakt zu einem Touchpoint herzustellen, muss das Mobiltelefon sehr nahe an den NFC-Touchpoint herangebracht werden. In den Tags sind alle notwendigen Informationen der U-Bahnstation gespeichert und sobald der Kontakt zwischen Mobiltelefon und NFC Tag hergestellt ist, werden diese Informationen auf das Mobiltelefon übertragen. Es wird eine automatische SMS erstellt, die der Kunde anschließend nur mehr mit einem Tastendruck bestätigen muss. Wenige Sekunden später erhält er den Fahrschein als Bestätigungs-SMS auf sein Mobiltelefon. Diese Dienste werden derzeit entweder über Paybox oder direkt über die Mobiltelefonrechnung abgerechnet.

6.1.2 NFC bei Automaten

Bei der Bezahlung an Automaten stellt oft das fehlende oder nicht passend vorhandene Kleingeld ein Problem dar. Fazit ist, dass dadurch der Kauf des Produktes nicht möglich ist.

Da Getränke- und Naschautomaten normalerweise auch keine Kartenzahlung akzeptieren, ist die bereits implementierte Möglichkeit mit NFC zu bezahlen ein großer Vorteil. Man muss lediglich bei Snack-Automaten das NFC Gerätes an den NFC-Touchpoint halten und die automatische SMS mit der Automaten-kennung verschicken. Nach kurzer Zeit erscheint dann das Guthaben auf dem Display und das Produkt kann ausgewählt werden [NFCC08].

6.1.3 NFC-Karten und Gutscheine

Es gibt die Möglichkeit, verschiedene NFC-Karten zu erwerben, die teilweise mehrmals wieder verwendbar sind. Es gibt beispielsweise eine NFC-Karte, mit

der es möglich ist, einen 30 Minuten Parkschein zu lösen oder andere, mit denen man Lotto spielen kann.

Ebenso können Gutscheine als NFC-Karten ausgegeben werden. Zum Beispiel kann ein bestimmter Betrag als ÖBB-Gutschein in das Mobiltelefon geladen werden. Beim Kauf des nächsten ÖBB-Tickets wird der Betrag vom bestehenden Guthaben abgezogen.

6.2 Internationale Mobile Contactless Payment Lösungen

Es gibt auch zahlreiche internationale Versuche, Mobile Contactless Payment zu etablieren. Die ersten Versuche der Bank of America in den USA scheiterten jedoch [DABA07], obwohl NFC in den USA bereits in einem höheren Stadium ist.

Es wurde ein Versuch gestartet, bei dem die Simulation von Karten erfolgte. Durch speziell angefertigte Applikationen war es möglich z.B. Kreditkarten auf dem Mobiltelefon zu simulieren. Die mobile elektronische Geldbörse wird so Realität.

Die Bank of America verwendete eine Over-The-Air Plattform. Bevor die Kunden diese Simulationen benutzen konnten, mussten sie eine Software downloaden.

Bei der Simulation von Kreditkarten und ähnlichem, ist bei vielen Applikationen die Speicherung von sicheren Elementen notwendig. Bei dem Versuch in den USA wurde das Venyon Secure Chip Management verwendet, das den Upload, die Aktivierung und Speicherung von persönlichen Daten im Mobiltelefon ermöglichte. Daten wie Zahlungs- oder Ticketinformationen, Zutrittskontrollen etc. werden auf einem Smart-Card Chip, wie etwa die SIM-Karte oder einem zusätzlich eingebautem Chip, gespeichert.

Venyon [VENY08] bietet eine Over-The-Air Service-Plattform für NFC Applikationen an, die Unternehmen wie Transportgesellschaften, Banken und andere Serviceanbieter nutzen können. Die Services werden als Business-to-

Business Applikation zur Verfügung gestellt und die Vermarktung und Anpassung an die eigenen Bedürfnisse obliegt dem Serviceanbieter selbst.

Abbildung 11 veranschaulicht den Ablauf, wie eine NFC Applikation von Venyon genutzt werden kann. Zuerst muss die Applikation, wie etwa eine Kreditkarte, sicher auf das NFC-fähige Mobiltelefon übertragen werden. Anschließend kann der Kunde lediglich durch Berührung eines POS-Lesegerätes mit der Kreditkarte über Mobiltelefon bezahlen.

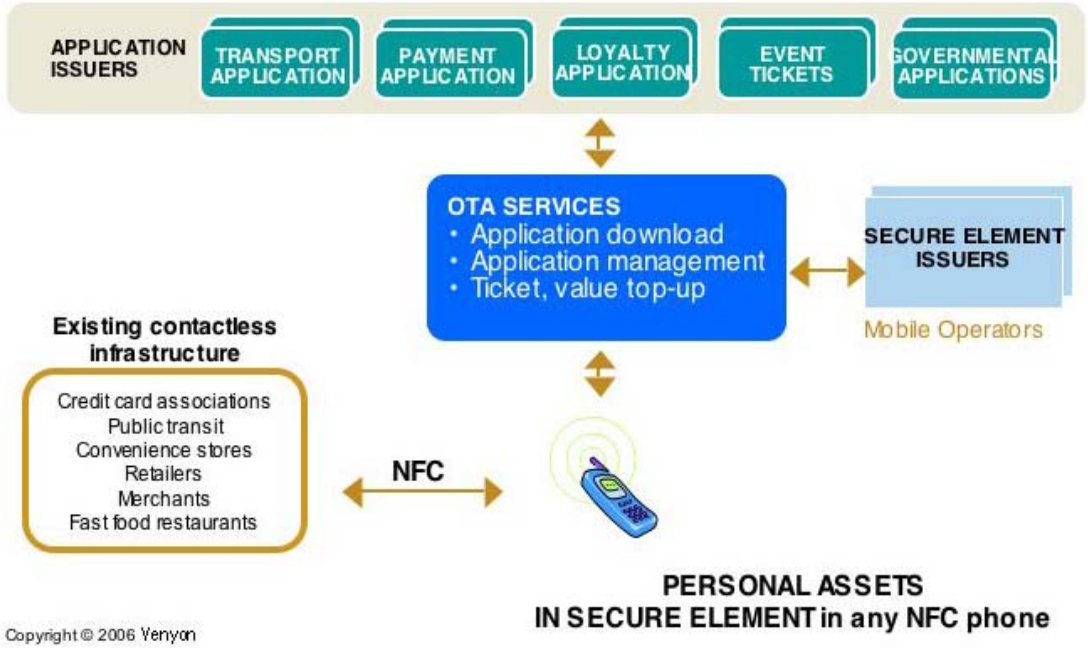


Abbildung 16 - NFC Applikationen von Venyon

Die ersten Versuche der Bank of America scheiterten allerdings aus mehreren Gründen. Das erste am Markt erhältliche NFC-fähige Mobiltelefon wurde von den Usern nicht akzeptiert [DABA07]. Außerdem kann man nicht telefonieren und bezahlen gleichzeitig, was Kunden als nicht akzeptabel erachteten. Ein weiteres Problem stellte der Downloadprozess der Applikationen dar, der für die User verwirrend, zu langsam und generell sehr problematisch war, was ebenfalls zur Ablehnung führte.

Für den Erfolg dieser Technologie muss es jedoch auch die entsprechende Infrastruktur geben. D.h. eine entsprechend große Händlerakzeptanz. Die

fehlende Anzahl an Händlern war auch ein Grund für das Scheitern der Einführung von NFC in den USA. Aufgrund von relativ hohen Händler-Gebühren, die für Contactless Payment entrichtet werden musste, war es für Händler nicht sehr interessant, diese Technologie anzubieten.

Aktuell startet die Bank of Amerika nun einen weiteren Versuch mit einem neuen Mobiltelefon Modell und einer neuen Plattform für den Download von Zahlungsapplikationen. Außerdem wird versucht, die notwendige Infrastruktur so schnell wie möglich aufzubauen.

6.3 Analyse der bestehenden implementierten Systeme

Die NFC Lösungen, die in Österreich derzeit angeboten werden, basieren auf dem SMS Versand. Diese Realisierung schränkt zwar die Möglichkeiten ein, bietet aber eine einfache Handhabung und wenige Sicherheitsrisiken.

Die derzeitige SMS Lösung z.B. der Wiener Linien erfüllt die Anforderung der einfachen Handhabung. Es ist derzeit jedoch nur möglich, über die Telefonrechnung abzurechnen und es gibt viel zu wenig Händler bzw. Möglichkeiten mit NFC zu bezahlen. Andererseits kann jeder, der ein NFC Mobiltelefon besitzt, die derzeitigen Bezahlszenarien sehr leicht erlernen und auch anwenden. Das Zahlen im Ausland ist jedoch noch nicht möglich.

Im Folgenden werden die wichtigsten Gründe für das Scheitern von einzelnen Mobile Contactless Payment Versuchen aufgelistet [DABA07].

- Download von zusätzlicher Software für den Kunden war sehr verwirrend
- Verbindung für den Download war sehr langsam und unzuverlässig
- Telefonieren und Bezahlen funktioniert nicht gleichzeitig
- Das eingesetzte Mobiltelefon wurde von den Kunden aufgrund von schlechter Usability nicht akzeptiert
- Der Zahlungsvorgang, also von Beginn bis zum Abschluss, war für den Kunden nicht genau Nachvollziehbar
- Fehlende Mehrwerte für den Kunden

7 Identifikation von sicherheitsrelevanten Kriterien

Das Potential von Mobile Contactless Payment lässt sich nur dann erfolgreich nutzen, wenn die Kunden diesem System zu einem gewissen Grad vertrauen. Aus diesem Grund muss eine sichere Infrastruktur verwendet werden, welche die Schutzinteressen aller beteiligten Parteien berücksichtigt. Es müssen somit Mechanismen verwendet werden, die Vertraulichkeit, Integrität und Verlässlichkeit gewährleisten.

Thomas Pleil [THPL05] erklärt den Erfolg oder Misserfolg neuer Technologien und Dienstleistungen unter anderem mit den gesellschaftlichen Rahmenbedingungen und die Haltung der Gesellschaft gegenüber Innovationen. Viele Studien und Umfragen [RTRG08] bestätigen immer wieder das grundsätzliche Interesse der Bevölkerung an Innovationen, es stehen jedoch immer weniger Menschen der Technik vollkommen positiv gegenüber. Dies muss bei der Einführung einer neuen Technologie berücksichtigt werden.

Mit der Kommunikation bzw. Vermarktung neuer Technologien oder Dienste wird sehr oft erst spät im Entwicklungsprozess begonnen. Die Menge der Early Adopters, also jener Personen, die von Anfang an der neuen Technologie positiv gegenüber stehen, wird daher immer kleiner. Aus diesem Grund muss so früh als möglich mit der Kommunikation begonnen werden und die neue Technologie sollte sehr rasch eine weite Verbreitung erreichen.

Gerade in der ersten Phase der Einführung einer neuen Technologie besteht jedoch die größte Chance, positive Einstellungen zu prägen. Die Technologie muss den Bedürfnissen und Präferenzen der Kunden entsprechen und darf nicht gegen gesellschaftliche Wertvorstellungen gerichtet sein.

Khodawandi, Pousttchi und Wiedemann [DKPW03] haben eine Studie über das Internet mit 5110 vollständig ausgefüllten Fragebögen durchgeführt, mit dem Ziel die Gründe für die Nutzung oder Ablehnung von M-Payment zu erforschen. Die Auskunftspersonen wurden in MP-Nutzer und MP-Nichtnutzer eingeteilt. Wobei die MP-Nutzer jene Personen waren, die schon zumindest einmal ein MP-Verfahren verwendet haben und die MP-Nichtnutzer jene, die keine

Erfahrung mit M-Payment hatten. Die Fragestellungen wurden dann für die jeweilige Gruppe angepasst. Die Nutzer wurden nach den Nutzungsgründen und die Nichtnutzer nach den Ablehnungsgründen befragt.

Abbildung 14 zeigt das Ergebnis der Studie auf die Fragenstellung „Wie wichtig sind Ihnen folgende Eigenschaften mobiler Bezahlverfahren?“ [DKPW03]. Die Antwortalternativen waren in eine fünf-stufige Rating Skala eingeteilt.

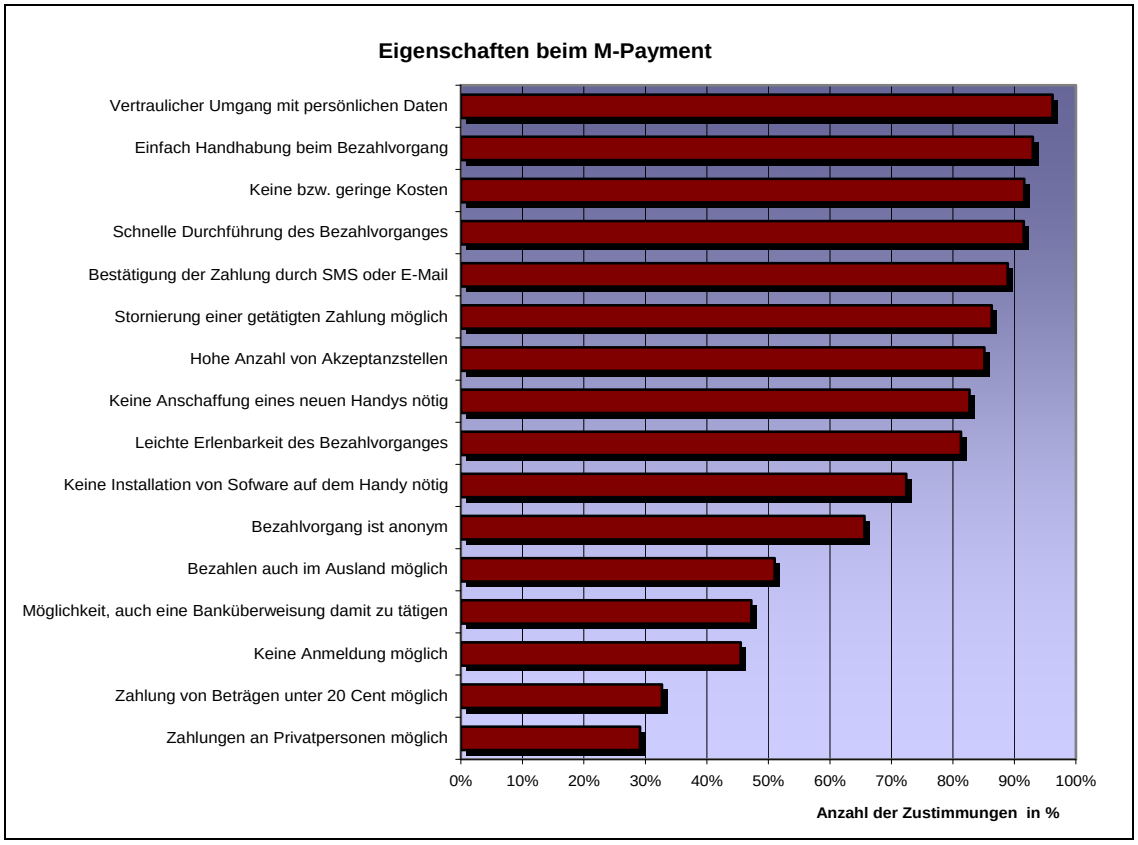


Abbildung 17 - Wichtigkeit von Eigenschaften beim M-Payment

In dieser Grafik ist deutlich erkennbar, dass das Thema Sicherheit in der Prioritätenhierarchie ganz oben angesiedelt ist.

Die folgende Abbildung zeigt eine prozentuelle Aufteilung der Prioritäten Antworten in den jeweiligen Kategorien in Bezug auf die Gesamtantworten [KEPO03].

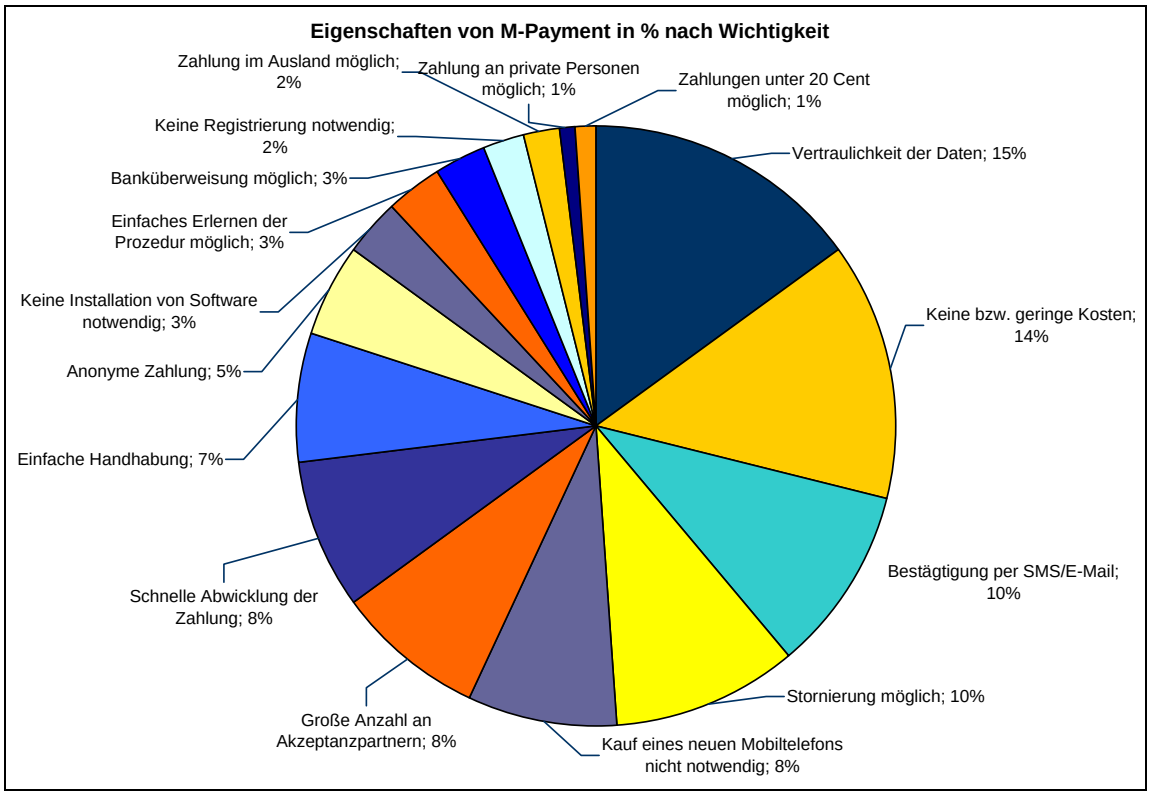


Abbildung 18 - Wichtige Eigenschaften von Mobile Payment

Abbildung 18 widerspiegelt die Prioritäten der verschiedenen Eigenschaften von Mobile Payment aus Sicht des Nutzers. Diese Eigenschaften können grob in Sicherheit, Kosten und Benutzerfreundlichkeit eingeteilt werden.

Das stärkste Kriterium für die Akzeptanz ist die Vertraulichkeit der Daten, sowie weitere sicherheitsrelevante Kriterien, wie Bestätigung durch SMS, Stornierung oder schnelle Abwicklung der Zahlung. Die Anzahl der Akzeptanzpartner, bei denen man mit NFC Technologie bezahlen kann, sollte sehr hoch sein, damit die Attraktion dieser Technologie für den Kunden steigt.

Das Bundesministerium für Wirtschaft und Arbeit beschäftigte sich im Zuge des Projekts MOMA [THSB04] mit dem Thema Sicherheit. Auch das Mobile Payment Forum [MOPA08], eine Organisation, die in Kooperation mit Firmen und Marktforschungsinstituten die Entwicklung mobiler Forschungssysteme forciert, beschäftigt sich verstärkt mit dem Sicherheitsaspekt von mobilen Zahlungssystemen. Es wurden einige Sicherheitslücken für M-Payment identifiziert, die in Anlehnung an [THSB04] und [MOPA08] in dieser Arbeit

diskutiert werden. Um eine weite Verbreitung an Akzeptanz von M-Payment zu forcieren, sollten die folgenden identifizierten Eigenschaften möglichst gut erfüllt werden.

7.1 Geeignetes Trägermedium

NFC kann mit jedem beliebigen Medium betrieben werden. So kann es beispielsweise in Schlüsselanhänger, Kreditkarten oder Mobiltelefone eingebaut werden. Für den Händler und die nachfolgenden Abrechnungsschritte macht die Art des Trägermediums keinen Unterschied. Für den Kunden kann die Wahl des Mediums allerdings entscheidend sein.

Um das große Potential vom Mobile Contactless Payment Verfahren ausschöpfen zu können, ist es erforderlich, dass beim Einsatz Mehrwerte entstehen [PBST02].

In Amerika gibt es seit 2006 Kreditkarten, die mit einem RFID Chip ausgestattet sind. Diese Kreditkarten können mittels NFC, lediglich durch Berührung für den Bezahlvorgang verwendet werden. Die ersten Versuche Contactless Payment dieser Art zu etablieren scheiterten jedoch [DABA07].

Ein essentieller Faktor für das Scheitern war der fehlende Zusatznutzen und Mehrwert. Die Bezahlung mittels Kreditkarte durch Berührung eines Terminals bringt dem Konsumenten keinen Vorteil im Vergleich zur herkömmlichen Methode [DABA07], bei der die Karte durch ein Lesegerät durchgezogen wird. Der Vorgang Karte durchziehen oder Karte auf ein Lesegerät halten dauert etwa gleich lange und der Kunde muss in beiden Fällen das Portemonnaie, sowie die Karte herausnehmen. Da hier der wesentliche Vorteil des Verfahrens für den Kunden fehlt, werden kontaktlose Kreditkarten schwer akzeptiert.

Mehrwerte, die in mobilen Anwendungen realisiert werden können, sind allgemein formuliert [PBST02]:

- Allgegenwärtigkeit (ubiquity)
- Kontextsensitivität (context-sensitivity)
- Identifizierungsfunktionen (identiying functions)

- Telemetriefunktionen (command and control functions).

Erst wenn ein Zahlungsverfahren die wesentlichen Eigenschaften des mobilen Angebotes teilt, insbesondere die Allgegenwärtigkeit, wird sie für den Kunden adäquat sein.

Ein möglicher Mehrwert für Mobile Contactless Payment könnte die richtige Wahl des Trägermediums darstellen. Das Mobiltelefon ist ein geeignetes Trägermedium, um es in Verbindung mit NFC für das Bezahlen zu verwenden. Das Mobiltelefon ist mittlerweile zum ständigen Begleiter geworden und somit allgegenwärtig und daher bringt der Einbau von NFC erhebliche Vorteile mit sich. So wäre man in Zukunft nicht mehr auf eine Geldbörse angewiesen. Wenn das Bezahlen mit NFC in nahezu allen Bereichen, wie Gastronomie, Shopping u.s.w. möglich ist, so ist das Mitführen eines einzigen Geräts ausreichend.

Eine weitere Möglichkeit Mehrwerte mit Mobile Payment zu verbinden, wäre ein bestimmtes Bezahlszenario, welches die Attraktivität der NFC Bezahlfunktion erhöht. Der Einsatz von NFC bei Getränkeautomaten wäre ein solches Szenario, da die Bezahlung mit Kleingeld aus diversen Gründen oft fehlschlägt. Die bereits implementierte Lösung, mit einem NFC-Gerät zu bezahlen, bringt den Vorteil, dass man kein Kleingeld mehr benötigt wird. Da dieses Szenario jedoch nicht so alltäglich ist, ist der Anreiz für den Kauf eines ein NFC Mobiltelefon für den Kunden relativ gering. Insofern müssen diese Szenarien noch weiter ausgebaut werden.

Der Verlust oder Diebstahl des Mobiltelefons stellt ein großes Risiko dar, da es derzeit auch bei dem Verfahren über SMS keinen Schutz vor unrechtmäßiger Verwendung gibt [MOPA08]. In diesem Fall müsste der Kunde vor Missbrauch von dem Zahlungssystemanbieter geschützt werden, ähnlich wie es derzeit auch beim Diebstahl von Kreditkarten der Fall ist. Ein zusätzliches Risiko stellt jedoch auch die Verwendung der Zahlungsfunktion durch die nicht notwendige Bestätigung durch PIN oder Unterschrift dar.

7.2 Prävention von Anwenderfehler

Durch Anwenderfehler kann die Sicherheit des jeweiligen Systems beeinträchtigt werden. Deshalb ist die Benutzerfreundlichkeit für eine breite Akzeptanz in allen Bevölkerungsschichten von großer Bedeutung [PBST02].

Die Benutzerfreundlichkeit wird wie in Tabelle 5 zu sehen ist, in Bedienung und Vorgangsdauer [PBST02] unterschieden. Die Bedienung sollte einfach gestaltet und möglichst selbsterklärend sein, da dies die Anwendung auch weniger technisch versierten Benutzern ermöglicht. Es darf auf keinen Fall durch eine falsche Benutzung eine Sicherheitslücke entstehen.

Benutzer-freundlichkeit	**Bedienung**		**Vorgangsdauer**	
	Einfach	Kompliziert	Kurz	Lang

Tabelle 5 - Akzeptanzkriterium Benutzerfreundlichkeit

In Abbildung 19 sind die Ergebnisse der Umfrage von [DKPW03] auf die Frage „Wie lang darf ein Bezahlvorgang höchstens dauern“ dargestellt. Zum Vergleich wurde die Bezahlung mit der Bankomatkarte, die mit etwa 25 Sekunden vorgegeben war, als Referenzmodell herangezogen.

Man kann in der Abbildung deutlich erkennen, dass die Befragten nicht bereit wären, einen längeren Bezahlvorgang als etwa 25 Sekunden in Kauf zu nehmen.

Ein Bezahlvorgang sollte außerdem schnell abgeschlossen werden können, da durch die Aufrechterhaltung der NFC Verbindung und durch die lange und eventuell mehrmalige Übertragung von Daten die Chance auf Angriffe erheblich erhöht werden.

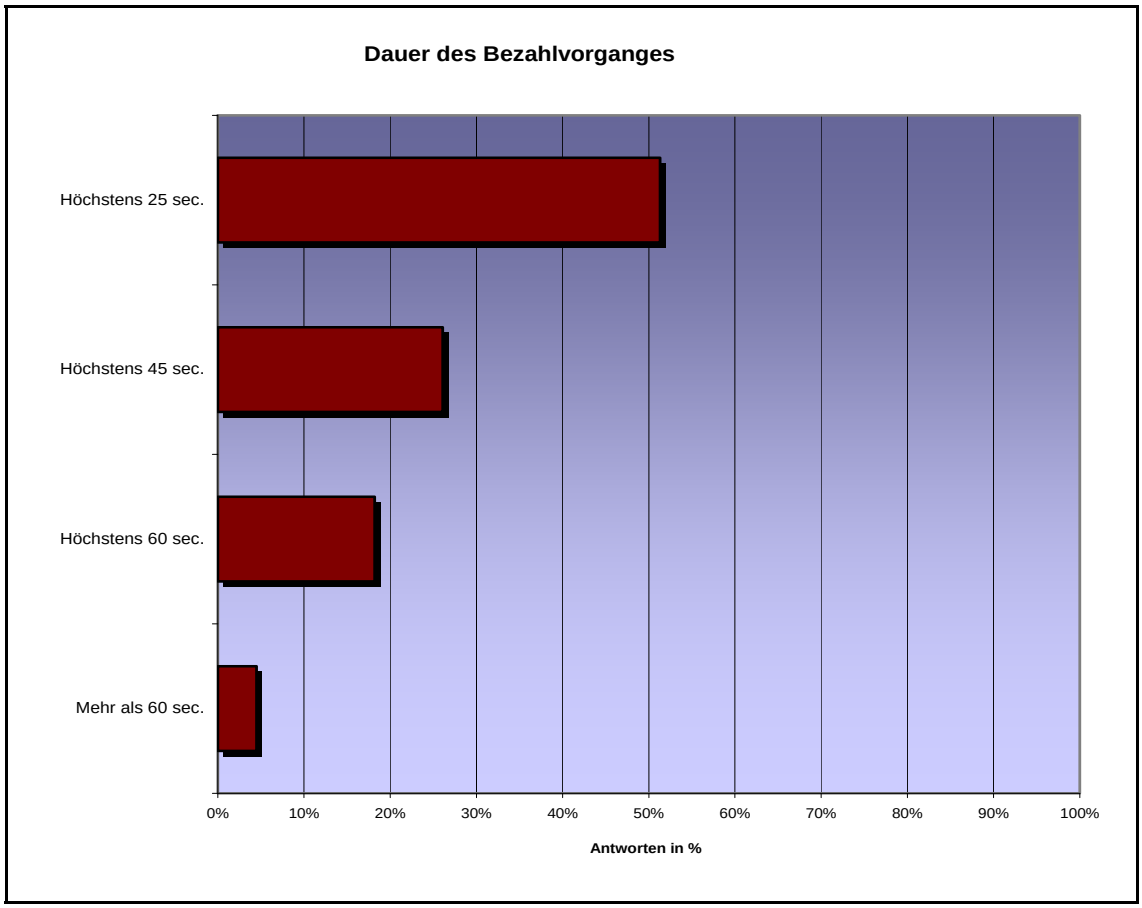


Abbildung 19 - Dauer des Bezahlvorgangs

Die folgende Abbildung zeigt welche Kriterien der Kategorie Benutzerfreundlichkeit aus der Umfrage [DKPW03] den Befragten am Wichtigsten sind.

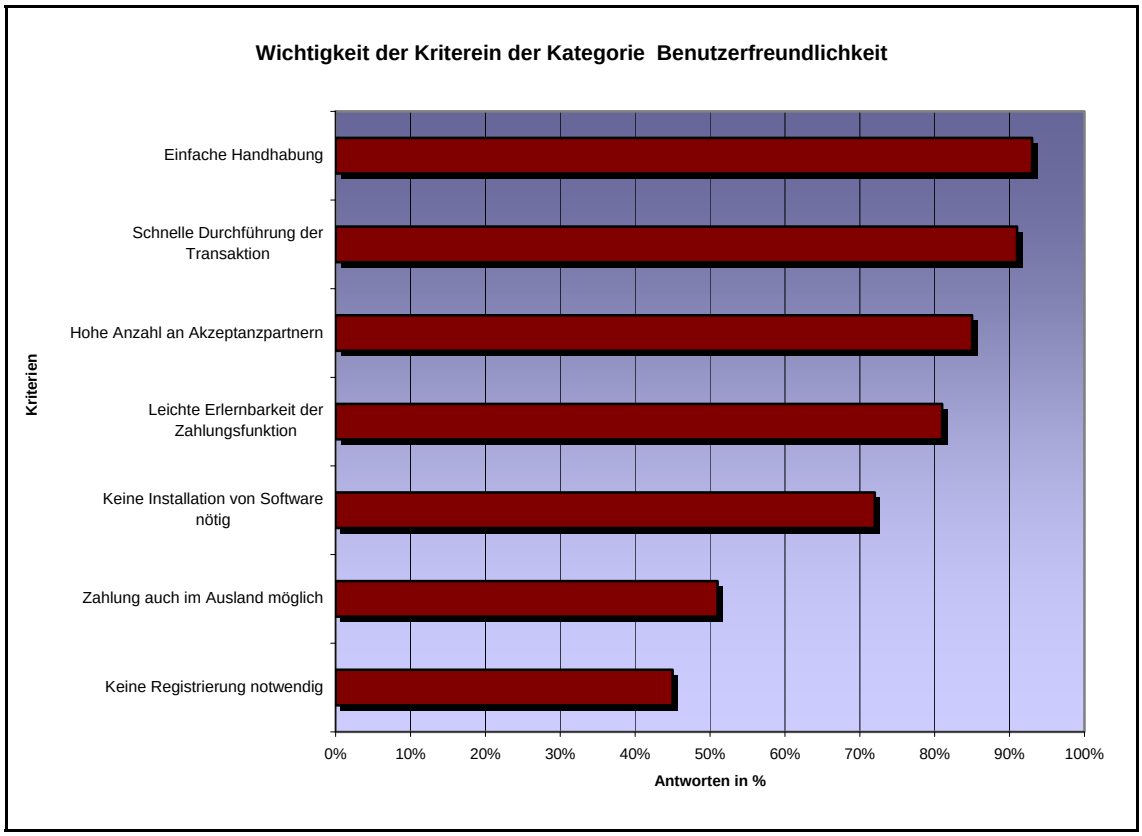


Abbildung 20 - Kriterium Benutzerfreundlichkeit

Man sieht anhand dieser Abbildung, dass fast alle Befragten eine einfache Handhabung gefolgt von schneller Durchführung der Zahlungstransaktion erwarten. Auch die Anzahl an Akzeptanzpartnern, also Händler die diese Art der Zahlung unterstützen, sind für den Kunden und für die Entscheidung für oder gegen die neue Technologie sehr wichtig. Letztendlich erhöht ein durchdachtes Konzept von einem Anbieter im Gegensatz zu vielen Individuallösungen die Bekanntheit und das Gefühl von Sicherheit beim Kunden.

Anwender tendieren sehr häufig dazu, PINs oder Passwörter sehr einfache zu halten, was eines der größten Risiken darstellt [THSB04]. Bisher bestand nur eine relativ geringe Gefahr von Missbrauch bei mobilen Endgeräten und die Sicherheitsvorkehrungen sind dementsprechend dürftig. Allein der vier-stellige PIN, der die SIM-Karte eines Mobiltelefons vor unautorisiertem Zugriff schützen soll, stellt nur einen geringen Schutz dar. Das fehlende Bewusstsein der

Benutzer erhöht diese Gefahr. Die Benutzer müssen sich letztendlich erst daran gewöhnen, dass das Mobiltelefon in Zukunft auch als Zahlungsmittel dienen soll und wichtige Daten auf der SIM-Karte abgespeichert sein werden.

Es stellt eine Herausforderung für die Designer dar, Verfahren zu entwickeln und zu implementieren, die den Anwender davon abhalten, Sicherheits-mechanismen wie Autorisationsüberprüfungen zu deaktivieren oder durch schlecht gewählte Passwörter auszuhebeln, ohne gleichzeitig die Anwenderfreundlichkeit zu gefährden.

Ein weiteres Sicherheitsrisiko kann durch eine Fehlbedienung, die durch falsches Verständnis der Benutzer verursacht wird und dadurch unerwünschte Zahlungen oder das Lesen von sicheren Daten möglich ist, nicht ausgeschlossen werden [MOPA08]. Dieses Problem muss jedoch bei jedem einzelnen Zahlungsverfahren eigens analysiert werden.

Generell gilt, Anwendungen sollen [FSWW03]:

- Intuitiv verständliche Funktionen haben
- Nachvollziehbare Abläufe haben
- Feedback bei Aktionen geben
- Das Widerrufen von Aktionen zulassen
- Übersichtlich sein
- Robust sein
- Zuverlässig sein

Entsprechend [KEPO03] erachten ca. 89% der Befragten eine Bestätigung von Zahlungen als essentielles Sicherheitskriterium. Eine sofortige Bestätigung einer Zahlung per SMS oder E-Mail bietet für den Kunden die Sicherheit, dass nichts Falsches abgebucht wurde. Das wird als fast genauso wichtig wie die Möglichkeit einer Stornierung der Zahlung empfunden.

7.3 Vertraulicher Umgang mit persönlichen Daten

Beim Thema persönliche Daten wollen Kunden den bestmöglichen Schutz erhalten. In Abbildung 17 ist zu sehen, dass das Thema Vertraulichkeit bei der

Umfrage [DKPW03] die meisten Antworten erhalten hat. Das wichtigste Akzeptanzkriterium für die Konsumenten ist somit der vertrauliche Umgang mit persönlichen Daten, um Missbrauch vorzubeugen und das Vertrauen der Kunden zu erhalten.

Die folgende Abbildung betrachtet das Thema Sicherheit noch einmal genauer und zeigt, dass alle Kriterien zu diesem Thema eine sehr hohe Anzahl an Antworten, fast immer über 80 %, erhalten haben [KEPO03].

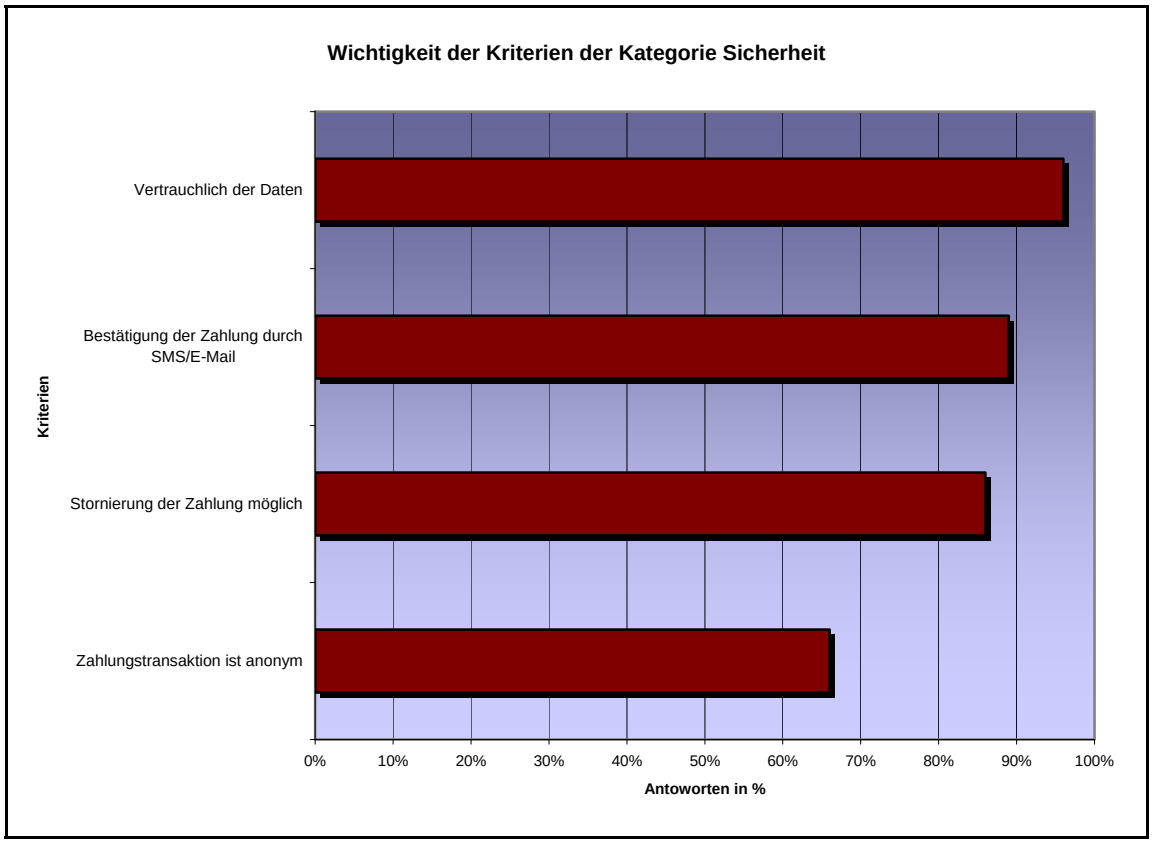


Abbildung 21 - Kriterium Sicherheit

Das Sicherheitsbedürfnis ist allerdings immer subjektiv und variiert von Kunde zu Kunde sowie auch von Kultur zu Kultur. In den USA ist beispielsweise die Akzeptanz persönliche Daten freizugeben wesentlich höher als in Deutschland [DABA07]. Allgemein stößt man auf mehr Akzeptanz je weniger persönliche Daten beim Zahlungsvorgang bekannt gegeben werden müssen.

Entscheidend für den Kunden ist die Vertraulichkeit der Daten, also welche Daten bekannt gegeben werden, wer Zugriff auf diese Daten besitzt und wie groß die Möglichkeit von Missbrauch ist [PBST02]. Ein unautorisierter Zugriff kann entweder das Mitlesen, das Weitergeben oder das Manipulieren sein.

Vertraulichkeit der Daten	Niedrig	Mittel	Hoch

Abbildung 22- Akzeptanzkriterium Vertraulichkeit der Daten

Die Ausprägungsgrade der Vertraulichkeit gliedern sich, wie in Abbildung 22 dargestellt, in niedrig, mittel und hoch [KEPO03]. Die notwendige Sicherheitsstufe ist immer von der jeweiligen Anwendung abhängig. Das Übertragen eines Bildes beispielsweise muss nicht denselben hohen Sicherheitsbestimmungen unterliegen wie etwa ein Bezahlvorgang mit sensiblen Daten. Um eine sehr hohe Vertraulichkeit anzustreben besteht im Idealfall keine Notwendigkeit persönliche Daten für einen Bezahlvorgang bekannt zu geben. Eine hohe Vertraulichkeit impliziert natürlich auch die Sicherstellung des Datenzugriffs ausschließlich von berechtigten Personen.

Im Gegensatz zu einer hohen Vertraulichkeit steht jedoch die unterdrückbare oder nicht verfügbare Anrufer ID [THSB04], die je nach Abrechnungsmodell zu Problemen führen kann. Eine Identifikation wäre dann nicht mehr möglich. Insbesondere wenn die Abrechnung nicht mehr über den Mobilfunkbetreiber erfolgt, müssen neue Konzepte der Authentifizierung gefunden werden.

Wenn das Mobiltelefon in Zukunft auch zum Bezahlen eingesetzt werden kann, dann muss man auch bedenken, dass alle Daten an einer zentralen Stelle gespeichert werden [MOPA08], was zu einer Gefährdung des Datenschutzes führt. Der Mobilfunkbetreiber wüsste dann nicht nur, wo sich der Mobiltelefon Besitzer aufhält, sondern hätte potentiell Einblick in das Zahlungsverhalten des Mobile Contactless Payment Nutzers.

Wenn man von Datenschutz und Sicherheit spricht, muss man auch von Vertrauen in jene Menschen und Institutionen sprechen, die diese

Informationen nicht missbrauchen dürfen. Das Vertrauen in eine Technologie wird durch Transparenz der Funktionen, Interfaces und Prozessstrukturen gestärkt. Das Vertrauen in Menschen ist jedoch ein komplexer sozialer Prozess, in den Designer nur begrenzt eingreifen können [LSCH06]. Die Hauptaufgabe von Designern ist die Technologie und die Anwendungen vertrauenswürdig zu gestalten, d.h. dass sie den größtmöglichen Schutz gegen Missbrauch bieten muss.

7.4 Abhörsicherheit der NFC-Übertragung

Die NFC- Übertragung wird sehr oft als sicher beschrieben, da aufgrund der sehr geringen Distanz das Abhören oder Manipulieren von Daten nur schwer möglich ist.

Ein passives Abhören der NFC ist nach ECMA [ECMA] jedoch mit einfachen Mitteln möglich [BEHA07]. Bedrohungen richten sich fast immer auf die Kommunikationsverbindung zwischen Leser und Tag [TFHK08]. Die Funkschnittstelle nach ISO 14443 Standard, welche die Frequenz 13,56 MHz verwendet, liegt im Kurzwellenband und ist grundsätzlich mit Breit- oder Weltempfängern empfangbar. NFC soll lediglich in 10-15 cm Abstand funktionieren, was laut Thomas Finke und Harald Kelter [TFHK08] lediglich die aktive Kommunikation betrifft und das passive Abhören auch noch in einigen Metern Entfernung funktionieren soll.

Ein Angreifer kann sehr leicht die in der Regel statisch codierte Luftübertragung von GSM entschlüsseln und unbemerkt mithören sowie Nachrichten verändern, was ein hohes Risiko darstellt.

Thomas Finke und Harald Kelter führten einen Versuch in 1m Entfernung, durch, wo in einer Schleife ständig eine bestimmte Adresse auf einer Speicherkarte ausgelesen wurde. Es konnte gezeigt werden, wie in der folgenden Abbildung [TFHK08] zu sehen ist, dass Bitströme zwischen Sender und Empfänger empfangbar sind. Mit zunehmender Entfernung verschlechtert sich das Signal, jedoch konnten auch noch in 3 Meter Entfernung Ströme empfangen werden, ein genaues Mitlesen ist jedoch nicht möglich gewesen.

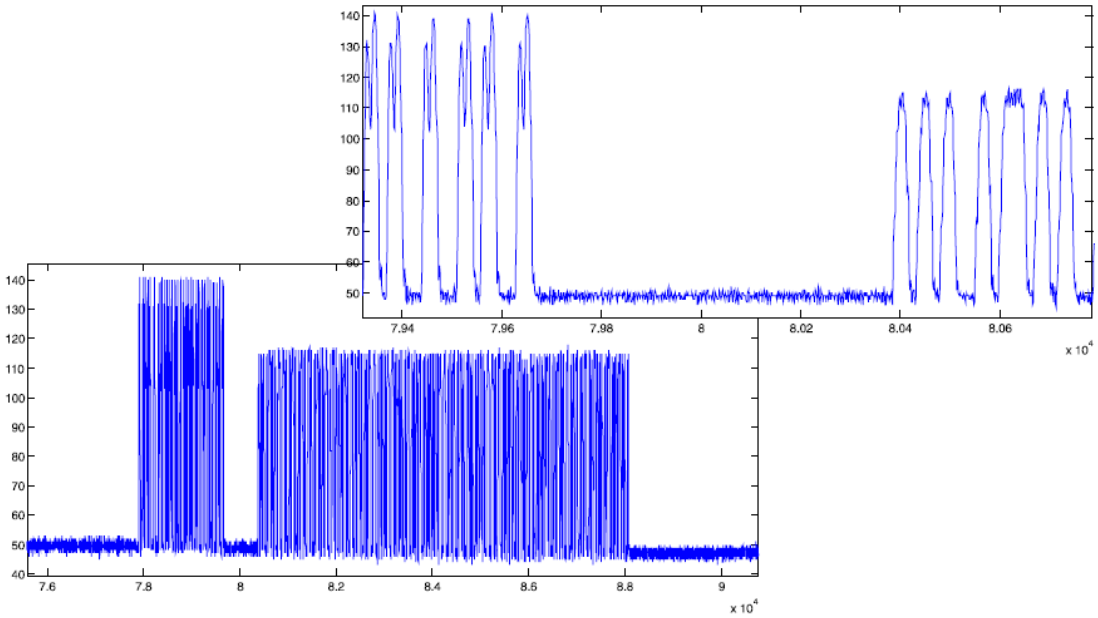


Abbildung 23 - Datentelegramm bei 1m Abstand

Bei einer Zahlungsabwicklung ohne den Netzanbieter kann auch das IP-Spoofing, also das Versenden von IP-Paketen mit gefälschter Quell IP-Adresse, ein großes Problem darstellen [THSB04]. Bei SMS besteht die Möglichkeit, die Absenderadresse beliebig zu ändern und so kann auch ein Angreifer auf fremde Rechnung Dienstleistungen über eine falsche Nummer kaufen. Der Angreifer kann dadurch potentiell erheblichen Schaden anrichten.

Mit entsprechender Hardware ist es auch möglich ein Endgerät auf eine falsche, imitierte Basisstation zu schalten [THSB04] und dabei die Identifikationskennung für ein Zahlungssystem abzuhören.

Möglichen Angriffen auf die NFC- Übertragung muss durch den Einsatz von verschlüsselten Datenprotokollen [NFCF07] und der beidseitigen Autorisation der Kommunikationspartner entgegenwirkt werden.

7.5 Geeignete Software auf dem Trägermedium

Bei der derzeitigen NFC-Lösung in Österreich mittels SMS, muss nicht auf die SIM-Karte zugegriffen werden, da der Betrag über die Telefonrechnung abgerechnet wird und daher sind diese Lösungen leichter zu realisieren.

Wenn das Mobiltelefon jedoch Kreditkarten und ähnliches für die Bezahlung simulieren soll, dann muss für jede Applikation und jedes Mobiltelefon die Software neu geschrieben werden und das ist ein enormer Aufwand. NFC ist derzeit auf dem Stand von Bluetooth vor etwa sieben Jahren [NFCF07] und es ist nicht gewiss, ob sich NFC jemals als Standard etablieren wird.

Das Bezahlen über das Mobiltelefon ist eine sehr komplexe Aufgabe, wenn direkt auf die SIM-Karte zugegriffen werden muss. Das ist eine große Herausforderung für die Software-Entwickler und birgt viele Sicherheitsrisiken für den Anwender.

Eine benutzerfreundliche Anwendung sollte geräteunabhängig betrieben werden können [PBST02]. Das bedeutet einerseits, dass nicht ein bestimmtes Gerät für die Verwendung notwendig ist und andererseits, dass das Gerät unterschiedliche Technologien wie z.B. SMS, WAP oder eine spezielle Payment Software unterstützten muss. Je höher die Anforderungen sind, desto schwieriger wird es jedoch das Verfahren am Markt zu etablieren.

Auf die Gefahr von Softwaremanipulationen, zum Beispiel durch Viren und Trojanern, muss bei der Entwicklung geeigneter Softwarekomponenten besonders Rücksicht genommen werden [THSB04]. Bei der Etablierung von M-Payment Lösungen, die über das Versenden von SMS hinausgehen und die verschiedensten Applikationen verwenden, müssen Lösungen entwickelt werden, um sensible Daten gegen Angriffe zu schützen.

Die Software auf dem Trägermedium muss Robustheits- und Manipulations-sicherheitsansprüchen genügen. Weiters muss sichergestellt werden, dass Softwareupdates zentral verteilt werden können. Der Updatevorgang muss vollautomatisch ablaufen und darf dabei keine Mobiltelefon Besitzer Interaktion bedürfen, da ansonsten die Gefahr von nicht eingespielten sicherheits-

relevanten Updates besteht. Zur Kontrolle sollten sämtliche NFC Kommunikationskomponenten beim Verbindungsaufbau die Aktualität des Softwarestands des Kommunikationspartners überprüfen.

Allgemein kann man NFC Applikationen laut NXP Semiconductors [NXPC08] grundsätzlich in vier Basiskategorien unterteilen.

7.5.1 Touch and Go

Touch and Go sind Applikationen für Zutrittskontrollen, Event Tickets oder auch um diverse Informationen zu speichern wie etwa eine URL von einem Poster. Die Informationen wie Zutrittscodes etc. befinden sich auf dem NFC-fähigen Gerät und werden lediglich durch das Heranbringen an den Leser ausgelesen.

7.5.2 Touch and Confirm

Bei Touch and Confirm handelt es sich um Applikationen wie beispielsweise das Mobile Contactless Payment mit einem NFC-fähigen Gerät. Die User müssen die Transaktion entweder mit oder ohne Passwort bestätigen.

7.5.3 Touch and Connect

Mit Touch and Connect kann man zwei NFC-fähige Geräte verbinden und dann peer to peer Daten, Musik, Bilder u.s.w. downloaden.

7.5.4 Touch and Explore

NFC-fähige Geräte bieten unterschiedliche Kernaktivitäten, die man intuitiv durch Berührung entdecken und erforschen kann.

Ein NFC fähiges Mobiltelefon bietet alle vier Basiskategorien in unterschiedlichen Implementierungen an. Sowohl bei der Funktion Touch and Confirm als auch bei der Funktion Touch and Go sind die Sicherheits-anforderungen als sehr hoch eingestuft. Für die Bezahlszenarien ist die Funktion Touch and Confirm am Wichtigsten.

7.6 Sicherheitsanforderung der Smart Card

SIM Karten gehören zur Familie der Smart Cards. Sie besitzen einen Ein-Chip Mikrocomputer, der aus einer CPU und dem Speicher besteht. Der Speicher teilt sich in ROM, EEPROM und RAM.

Der ROM (Read Only Memory) Speicher wird bei der Produktion hardcodiert und kann daher später nicht mehr verändert werden. Der Vorteil ist, dass die Informationen des ROM dauerhaft ohne Stromversorgung gespeichert werden. Der EEPROM (Electrical Erasable Programmable Read Only Memory) übernimmt grundsätzlich die gleiche Funktion wie der ROM, kann jedoch wiederbeschrieben werden. Die Telefonnummer eines Mobiltelefons wird beispielsweise auf dem EEPROM der SIM Karte gespeichert. Der RAM (Read Only Memory) wird auch als Arbeitsspeicher bezeichnet. Da er Daten nur bei aufrechter Stromversorgung speichert, wird er als Auslagerungsspeicher von Informationen verwendet.

Auf der Smart Card werden Daten verschlüsselt gespeichert und können mittels einer Schnittstelle für geeignete Lese- und Schreibgeräte ausgelesen werden. Je nach Implementierung und Funktionsumfang eines Mobile Contactless Payment Systems, wie Beispielsweise der Simulation von Kreditkarten, kann es notwendig sein, sensible Daten auf der Sim Karte oder einer eigens eingebauten Smart Card zu speichern [NFCF07].

Grundsätzlich gibt es zwei Arten von Angriffen. Einerseits Angriffe von innen, also Personen, die im Zahlungsprozess beteiligt sind (Händler, Kunde, etc.), andererseits Angriffe durch Dritte [BSAS99]. Beim Angriff geht es entweder um finanzielle Anreize oder um Zugang zu bestimmten Systemen und Daten zu erhalten.

- Attacken gegen den Karteninhaber durch gefälschte Terminals, wobei Daten durch die Fälschung eines Lesegerätes bzw. Terminals gestohlen werden können.

- Attacken vom Karteninhaber gegen das Terminal, dabei könnten durch manipulierte Daten auf der SIM Karte, dem Terminal falsche Informationen übermittelt werden
- Attacke vom Karteninhaber gegen den Dateninhaber – von dieser Attacke spricht man, wenn ein Angreifer zum Beispiel bestimmte Algorithmen von einer Karte ausliest. Dieses Wissen kann dann verwendet werden, um weitere Daten von anderen Karten zu stehlen.
- Attacken gegen die Privatsphäre des Karteninhabers, indem der Issuer jede Transaktion des Karteninhabers verfolgt und diese Informationen an Dritte weitergibt oder diese selbst etwa für Werbezwecke oder ähnliches verwendet.
- Angriffe von Dritten mit gestohlenen Karten, sind zu den Attacken des Karteninhabers gegen das Terminal sehr ähnlich, wobei der Unterschied im Wesentlichen darin besteht, dass der Kartenendwender nur einen gewissen Zeitrahmen – bis der rechtmäßige Karteninhaber die Karte sperren lässt - für den Missbrauch zur Verfügung hat.

Neben den potentiellen Angreifern und den verschiedenen Angriffszielen müssen auch Angriffsmethoden genau analysiert werden.

Side Channel Attacks oder Seitenkanalattacken sind durch den US-amerikanischen Kryptologen Paul C. Kocher 1996 [PKJB98] bekannt geworden. Sie bezeichnen eine kryptoanalytische Methode, mit der man Informationen außerhalb des eigentlichen Datenkanals sammelt und analysiert. Mit diesen Attacken ist es möglich die Implementierung eines krypto-graphischen Verfahrens zum Beispiel von einer Smart Card oder einer anderen Software zu knacken [HABE99]. Es wird allerdings nicht das kryptographische Verfahren selbst geknackt, sondern nur eine bestimmte Implementierung angegriffen.

Zu den wichtigsten Side Channel Attacken zählt man die Timing Attack, Power Monitoring Attack sowie die Tempest Attack.

7.6.1 Timing Attacks

Bei der Timing Attack [PCKO96] analysiert ein Angreifer die Rechenzeit des implementierten kryptographischen Verfahrens für verschieden, in der Regel vom Angreifer gewählten, Eingaben. Es werden also die Datenströme der CPU oder des Speichers auf dem Gerät das angegriffen wird analysiert. Lediglich durch die Zeit, die benötigt wird, um die Informationen zu übermitteln, können wichtige Informationen über die Verschlüsselung herausgefunden und ausgewertet werden. Timing Attacken wurden in der Vergangenheit gegen Chipkarten sowie gegen Software gerichtet.

7.6.2 Power Monitoring Attacks

Die Power Monitoring Attack analysiert den Stromverbrauch bei bestimmten Berechnungen. Der Stromverbrauch der Prozessoren und der restlichen Hardware hängt von den durchgeführten Operationen ab [PKJB99]. Durch die Analyse des Stromverbrauches kann man darauf schließen, womit das Gerät gerade beschäftigt ist, also speichern, verschlüsseln, entschlüsseln, etc.

Es gibt 3 verschiedene Formen dieses Angriffs. Die Simple Power Analyse, die Differential Power Analyse und die High-Order Differential Power Analyse.

Die Simple Power Analysis versucht den zeitlichen Verlauf des Stromverbrauches zu analysieren und dadurch auf die durchgeführten Operationen zu schließen.

Die Differential Power Analysis versucht die Unterschiede in der Stromaufnahme für verschiedene Eingaben zu analysieren.

Die High-Order Differential Power Analyse ist eine Kombination aus vielen Differential Power Analyse Attacken. Die High-Order Differential Power Analyse entsteht im Wesentlichen dadurch, dass man die Ergebnisse der einzelnen Attacken komprimiert. Diese Angriffe werden vor allem gegen Chipkarten eingesetzt, wobei diese Art der Attacke wesentlich aufwendiger ist als die Differential Power Analyse und daher kaum angewandt wird.

7.6.3 Tempest

Diese Angriffsmethode misst die elektromagnetische und akustische Strahlung, die von einem Rechner oder Gerät bei Berechnungen erzeugt wird [MAGK04]. Elektromagnetische Felder lassen sich oft noch in einiger Entfernung messen und erlauben ebenfalls Rückschlüsse auf die durchgeführten Operationen. Diese Angriffe sind auch als Van Eck Phreaking bekannt, da Wim van Eck 1985 als erster die Sicherheitsrisiken der Strahlung der Monitore aufzeigte.

Die beschriebenen Angriffe beruhen auf Informationen, die aus elektromagnetischer sowie akustischer Strahlung basieren oder aus der Analyse des Zeit- und Powermanagements abgeleitet werden können. Eine der erfolgreichsten Gegenmaßnahmen ist den Zugang zu diesen Informationen zu erschweren bzw. gar unmöglich zu machen [MKRA98]. Dies kann man beispielsweise durch sehr strahlungsarme Displays erreichen.

Für die Analyse des Zeit- und Powermanagements muss ein Angreifer kleine Programme auf dem Gerät installiert. Zur Prävention sollten Maßnahmen getroffen werden, die Installation solcher Programme zu verhindern.

7.7 Allgemein gültige Sicherheitskriterien

Die folgenden Anforderungen an Zahlungssysteme stellen wichtige Grundeigenschaften eines Systems dar [JOHE01].

In der Literatur sind häufig Anforderungen zu finden, die unter dem Begriff ACID zusammengefasst werden. Das Acronym steht für Atomicity (Totalität), Constistency (Konstistenz), Idependence (Unabhängikeit) und Durability (Dauerhauftigkeit). Joachim Henkel erweitert diese noch mit Reputation und Verlässlichkeit des Zahlungsverfahrens, Internationalität, Fälschungssicherheit, Konvertierbarkeit sowie Umlauffähigkeit.

Atomicity (Totalität) bedeutet, dass eine Transaktion entweder ganz oder gar nicht durchgeführt wird. Wenn eine Transaktion etwa durch ein technisches Gebrechen gestört wird, dürfen keine Daten übertragen werden.

Constistency (Konstistenz) alle Parteien, die an der Zahlungstransaktion beteiligt sind müssen übereinstimmende Informationen haben. Dies betrifft die Höhe des Betrages, das Transaktionsdatum und was bezahlt wurde. Integrität ist die Vorraussetzung dafür, was bedeutet, dass die Zahlungsdaten bei der Übertragung nicht verändert werden dürfen.

Idependence (Unabhängigkeit) steht für die Tatsache, dass sich unterschiedliche Zahlungen gegenseitig nicht beeinflussen dürfen. Es dürfen also die Reihenfolge und der zeitliche Ablauf der Transaktionen keine Rolle spielen.

Durability (Dauerhaftigkeit) bedeutet, dass im Falle eines Defektes das System wieder in den Zustand vor dem Defekt zurückgeführt werden kann. Dies ist besonders für Systeme wichtig, die Daten wie die Höhe eines Guthabens speichern.

Reputation und Verlässlichkeit erwarten sich Kunden sowie Händler. Beide wollen die Sicherheit, dass der Betreiber des Verfahrens sicher und fehlerfrei arbeitet. Bei Debit- oder Prepaid Verfahren ist für Kunden insbesondere wichtig, dass das Guthaben nicht einfach z.B. durch einen Konkurs wertlos wird und Händler wollen die Zahlungsgarantie für offene Forderungen.

Fälschungssicherheit ist eine notwendige Eigenschaft. **Konvertierbarkeit** und **Umlauffähigkeit** wären wünschenswerte Eigenschaften, sind jedoch für die Kernfunktionalität des Contacless Mobile Payments nicht erforderlich. Dies würde bei einem System mit Guthaben zum Einsatz kommen, wenn das Guthaben wieder in normales Geld transferiert werden soll.

Internationalität ist durch den Wegfall nationaler Grenzen ein immer wichtigeres Kriterium. Kunden wollen gewohnte Dienstleistungen auch im Ausland nutzen. Dabei sollte es weder funktionale Einschränkungen geben, noch eine Abstufung auf ein geringeres Sicherheitsniveau passieren.

Die folgende Tabelle stellt eine Zusammenfassung der allgemeinen Anforderungen sowie der Anforderungen des Kunden und der Händler dar [JOHE01].

Allgemein	Kunden	Händler
➢ Atomicity (Totalität) ➢ Consistency (Konsistenz) ➢ Independence (Unabhängigkeit) ➢ Durability (Dauerhaftigkeit) ➢ Reputation und Verlässlichkeit des Verfahrens ➢ Internationalität ➢ Fälschungssicherheit, Konvertierbarkeit, Umlauffähigkeit	➢ Sicherheit ggü. Händlern ➢ Sicherheit ggü. Dritten ➢ Bequeme und einfache Handhabung ➢ Breite Akzeptanz ➢ Niedrige Kosten ➢ Nachvollziehbarkeit ➢ Anonymität ➢ Portabilität ➢ Zusatzleistungen	➢ Zahlungssicherheit ➢ Technische Aspekte ➢ Enge Kunden-beziehungen ➢ Hohe Verbreitung

Tabelle 6- Anforderungen an Zahlungssysteme

Für einen Kunden ist sehr wichtig, die Sicherheit gegenüber dem Händler abschätzen zu können. Dies ist für kleine, spezialisierte Händler oder Gelegenheitshändler wie etwa bei Ebay Auktionen teilweise sehr schwer möglich. Öffentliche Bewertungen können für den Kunden sehr hilfreich sein und es lohnt sich für den Händler einen guten Ruf aufzubauen.

Für einen Händler ist die Zahlungssicherheit ein entscheidender Aspekt für die Akzeptanz eines Zahlungssystems. Dafür ist es essentiell zu wissen, ob ein Kunde überhaupt die Berechtigung für eine Zahlung aufweist. Joachim Henkel charakterisiert sechs verschiedene Konzepte für eine Autorisierung seitens des Kunden [JOHE01]. Diese kann entweder wissensbasiert, zugangsbasiert, durch eine Bestätigung durch Intermediär, durch nachträgliche Überprüfung, besitzbasiert und durch persönliche Identifikation erfolgen.

Eine **wissensbasierte** Autorisation erfolgt durch Eingabe eines PIN Codes oder eines Passworts, das nur dem Kunden selbst bekannt sein darf.

Ein **zugangsbasiertes** Verfahren wird aus einer anderen Autorisierung abgeleitet. D.h. wer beispielsweise Zugang zu einem Telefon hat, der hat damit die Glaubwürdigkeit inne, dass er der rechtmäßige Besitzer ist.

Bei der **Bestätigung durch Intermediär** wird das Vertrauensverhältnis das zwischen einem Kunden und dem Intermediär aufgebaut wurde, auf die Beziehung zwischen dem Kunden und dem Händler übertragen. Es muss jedoch zusätzlich auf ein oben erwähntes Verfahren zurückgegriffen werden.

In manchen Fällen kann eine Autorisierung auch erst **nachträglich** erfolgen, in dem der Kunde die Kontobelastung akzeptiert.

Eine **besitzorientierte** Autorisation bedeutet, dass man lediglich durch den Besitz bezahlen kann. Ähnlich wie bei Bargeld wird der Besitz als Autorisation angesehen.

Eine **persönliche Identifikation** ist durch biometrische Verfahren wie beispielsweise ein Fingerabdruck eine eindeutige Autorisation eines Kunden. Bei dieser Art besteht auch die größte Sicherheit gegen Fälschung oder ähnlichem.

8 Ergebnisse und Ausblick

Das Mobiltelefon ist mittlerweile zu einem essentiellen Life Management Werkzeug geworden und bietet immer mehr Funktionalitäten. Wo vor einiger Zeit noch das unterbrechungsfreie, rauschfreie Telefonieren vermarktet wurde, rücken heute Funktionen wie Organiser, Kalender, Fotoapparat, Radio, MP3 Player u.v.m. nach.

Es gibt weltweit 3,3 Milliarden abgeschlossene Mobilfunkverträge laut einer Studie des Marktforschungsunternehmens Informa Telecoms & Media [INTM08]. In Europa liegt die Mobiltelefonquote bei über 100 Prozent und statistisch gesehen besitzt somit jeder Österreicher zumindest ein Mobiltelefon.

Phillips und Sony [NXPC08] haben im Jahr 2002 begonnen ein weltweit einheitliches Protokoll für die Übertragung von Daten zu entwickeln. Near Field Communication wurde für die Kurzstreckenkommunikation entwickelt und man kann damit das Mobiltelefon in eine elektronische Geldbörse verwandeln.

NFC basiert auf der drahtlosen Radio Frequency Identifikation Technologie und verwendet für die Funkkommunikation den Frequenzbereich von 13,56 MHz. Eine Verbindung zweier NFC fähiger Geräte ist allein durch Annäherung innerhalb einer bestimmten Distanz möglich. NFC hat eine Übertragungsrate von max. 424 kbits/s und eine Reichweite von ca. 0 – 20 cm. Gerade diese kurze Distanz ist einzigartig im Vergleich mit anderen drahtlosen Datenübertragungstechniken. Die Annäherung, wenn man kommunizieren möchte, ist ein intuitives Verhalten und kann vom Anwender einfach übernommen werden.

Mobile Contactless Payment wird immer wieder großes Potential zugesprochen. Es gibt mittlerweile auf der ganzen Welt Versuche mit M-Payment Systemen. Besonders affine Märkte beim Bezahlen mit dem Mobiltelefon über NFC sind die ostasiatischen oder nordamerikanischen. Gleichzeitig gibt es allerdings auch viele Skeptiker, die gerade aufgrund der noch nicht ganz ausgereiften Technologie und der noch vorhandenen Sicherheitsrisiken der Ansicht sind, dass Mobile Contactless Payment sich in

den nächsten Jahren nicht durchsetzen wird und folglich das Mobiltelefon nicht allzu bald unsere Geldbörse ersetzten wird.

Seit knapp einem Jahr gibt es die Initiative „Pay-Buy Mobile“ [GSMW08]. Dieses Projekt soll den weltweiten Einsatz von Mobiltelefonen für POS Zahlungen mit Contactless NFC-Technologie ermöglichen und vorantreiben.

Es gibt viele Risiken, die bei der Etablierung von Mobile Contactless Payment Systeme bedacht werden müssen. Um eine entsprechende Verbreitung der Technologie zu erzielen, müssen die identifizierten Gefahren weitgehend entschärft werden. Endanwender stehen Innovationen gerade im Zahlungsverkehr sehr skeptisch gegenüber, weshalb es besonders wichtig ist, die Bedürfnisse der potentiellen Anwender zu kennen und neue Lösungen darauf auszurichten. Eine wesentliche Voraussetzung für den Erfolg von M-Payment ist die Bereitstellung effizienter und sicherer Abwicklungsformen des Zahlungsvorganges.

Welche nennenswerten Mobile Contactless Payment Systeme gibt es derzeit in Österreich?

Mobile Payment wird von vielen Autoren unterschiedlich definiert. Diese Arbeit stützt sich auf die Definition von Key Pousttchi [KEYP03], der M-Payment definiert als „*die Abwicklung von Bezahlvorgängen, bei der im Rahmen eines elektronischen Verfahrens mindestens der Zahlungspflichtige mobile Kommunikationstechniken (in Verbindung mit mobilen Endgeräten) für die Initiierung, Autorisierung oder Realisierung der Zahlung einsetzt*“.

Häufig werden Bezahlsysteme im Internet als Mobile Payment Systeme bezeichnet. Der Österreichische Online-Handel kann auf ein gutes Dutzend unterschiedlicher Internetzahlungssysteme zurückgreifen [EPSO08] und es kommen immer wieder neue hinzu. Fast alle dieser Zahlungssysteme zählen nach obiger Definition nicht zu den M-Payment Verfahren.

Das „Paybox“ System [PAYB08] kann zum Mobile Payment gezählt werden. Paybox wurde im Jahr 2000 entwickelt und ist seit 2001 aktiv und vor allem am österreichischen Markt verbreitet. Die Daten werden im Gegensatz zur Near Field Communication nicht drahtlos übertragen. Dieses System wird über das Mobilfunknetz abgewickelt indem man seine Mobiltelefonnummer bekannt gibt.

Das Paybox System kann mittlerweile schon in sehr vielen Bereichen genutzt werden. So kann mittels SMS Versand z. B ein Parkschein gelöst werden und bei Automaten und in diversen Online-Shops bezahlt werden.

Seit November 2007 gibt es in Österreich auch die Möglichkeit mittels NFC, in Verbindung mit einem NFC-fähigen Mobiltelefon, zu bezahlen. Am österreichischen Markt gibt es derzeit nur ein einziges Mobiltelefon, das einen eingebauten RFID Chip hat und mit dem man NFC verwenden kann.

Das Bezahlen mittels NFC funktioniert sehr intuitiv, lediglich durch Berührung eines NFC Touchpoints. Nach Berührung und Übertragung von Daten auf das Mobiltelefon wird entweder ein automatisches SMS generiert, das nur mehr versendet werden muss, oder es öffnet sich eine Eingabemaske, wo der Kunde bestimmte Informationen einträgt und per Knopfdruck absendet. Anschließend ist der Kauf auch schon abgeschlossen und der Kunde erhält zur Bestätigung wieder eine SMS auf sein Mobiltelefon.

Der Einsatz von NFC ist derzeit vor allem bei den Wiener Linien und der ÖBB möglich. Außerdem gibt es NFC-Gutscheine oder NFC-Karten, die bestimmte Funktionen erfüllen und immer wieder verwendet werden können.

Die Wiener Linien haben auf sehr vielen Fahrscheinautomaten passive NFC-Touchpoints angebracht, die durch Berührung mit einem NFC-Gerät aktiviert werden und bei denen der Kauf von Fahrscheinen möglich ist. Die notwendigen Informationen der U-Bahnstation sind in den Tags gespeichert und werden automatisch in das SMS geschrieben.

Für den Kauf von ÖBB Fahrkarten über NFC, erscheint nach Berührung des Touchpoints eine Eingabemaske, wo der Kunde die notwendigen Informationen, wie Zielbahnhof, Vorteilskarte, etc. einträgt und abschickt.

Das Angebot für NFC-Karten ist noch relativ gering. Es gibt beispielsweise NFC-Karten, die etwa das Format einer Postkarte haben. Mit diesen NFC-Karten können Parkscheine für eine bestimmte Parkdauer gekauft werden. Diese Karten haben einen eingebauten RFID-Chip. Wird ein Mobiltelefon an diese Karte herangebracht, werden die Daten übertragen und mit Knopfdruck bestätigt.

Welche zusätzlichen Gefahren treten beim Mobile Contactless Payment im Vergleich zu den derzeit eingesetzten Varianten auf?

Der Erfolg von Mobile Contactless Payment hängt in großem Maße von der Sicherheit und dem Sicherheitsempfinden der Konsumenten ab.

Im Bereich Sicherheit entstehen aufgrund der verwendeten Technologie und der Mobiltelefone mehr Risiken als bei bewährten Zahlungsmethoden wie Kreditkarte oder Bankomatkarte. Einerseits entstehen durch die NFC Datenübertragung neue Angriffspunkte. Andererseits ist der Endanwender nicht gewohnt Zahlungsvorgänge über das Mobiltelefon zu tätigen, und dadurch sind die entsprechenden Sicherheitsvorkehrungen sehr dürftig.

Der Verlust des Mobiltelefons stellt ein höheres Risiko als bei bisherigen Zahlungsmitteln dar, da vor allem die Bezahlung ohne Passwort- oder Pin-Eingabe möglich ist und daher die Bezahlfunktion bis zum Zeitpunkt der SIM-Kartensperre verwendet werden kann. Die Sicherheitsvorkehrungen sind sehr dürftig, und das fehlende Bewusstsein der Benutzer erhöht zusätzlich die Gefahr. Die Benutzer müssen sich erst daran gewöhnen, dass das Mobiltelefon nun auch als Zahlungsmittel verwendet werden kann.

Durch unterschiedliche Funktionen und Einsatzbereiche von Mobiltelefonen sind diese technisch teilweise sehr anspruchsvoll. Mangelnde Kenntnisse und

Fehlbedienung können ein Sicherheitsrisiko darstellen, vor allem wenn dadurch ungewünscht Daten versendet werden.

Wenn über das NFC Mobiltelefon diverse Applikationen für die Simulation von Karten verwendet werden, so müssten diese in jedem Fall intuitiv gehalten werden, damit sie leicht erlernt werden können. Für Endanwender sind die Storniermöglichkeit von Zahlungen, die Bestätigungsmeldung von Zahlungen sowie die Nachvollziehbarkeit der Zahlung besonders wichtig.

NFC wird sehr oft als sicher beschrieben, da aufgrund der sehr kurzen Reichweite das Abhören und Manipulieren von Daten nicht möglich sein soll. Die Funkschnittstelle mit der Frequenz von 13,56 MHz ist jedoch grundsätzlich mit Breit- oder Weltempfängern empfangbar. Der Funkabstand von 10 – 20 cm bei der NFC Technologie gilt lediglich für die aktive Kommunikation. Das passive Abhören ist aber auch noch in einigen Metern Entfernung möglich. Es konnte nachgewiesen werden, dass in einem Meter Entfernung Bitströme zwischen Sender und Empfänger sehr gut zu empfangen sind. Die Signale verschlechtern sich mit zunehmender Entfernung, jedoch konnte man auch noch in drei Metern Entfernung Signale empfangen, ein genaues Mitlesen war dann jedoch nicht mehr möglich. Aus diesem Grund muss die NFC Datenübertragung verschlüsselt zwischen authentifizierten Kommunikations-partnern stattfinden.

Das Kriterium Vertraulichkeit impliziert, dass keine Daten von unbefugten Personen gelesen und manipuliert werden können. Im Idealfall werden keine persönlichen Informationen beim Kauf übermittelt. Das gezeigte Risiko durch Abhören der NFC Übertragung ist ein dramatischer Gegensatz für den Datenschutz und die Vertraulichkeit. Das Risiko von Viren oder Manipulation der Absenderadresse von SMS ist ebenfalls ein großes Problem.

Wenn NFC Mobiltelefon Kreditkarten simulieren, dann ist es notwendig, dass bestimmte Informationen auf der Sim Karte oder auf einer eigenen Smart Card gespeichert werden. Vor allem Side Channel Attacks sind gegen die Smart Cards gerichtet. Durch das Auswerten der Rechenzeit oder des Stromverbrauches für bestimmte Operationen können wichtige Informationen

zum Beispiel über das verwendete kryptologische Verfahren herausgefunden werden. Dem kann durch möglichst geringer Abstrahlung (zum Beispiel durch Einsatz strahlungsarmer Komponenten und strahlungsabsorbierender Gehäuse) und durch Prävention der Installation von zusätzlicher Software auf der Smart Card durch den Angreifer entgegengewirkt werden.

Bei der Verwendung von elektronischen Systemen gibt es außerdem gewisse Grundeigenschaften, die erfüllt werden müssen. Einige davon können unter dem Akronym ACID zusammengefasst werden. ACID steht für Atomicity, Consistency, Independence und Durability.

Atomicity bedeutet Totalität. Eine Transaktion soll entweder ganz oder gar nicht durchgeführt werden. Consistency bedeutet, dass alle beteiligten Parteien konsistente also übereinstimmende Informationen haben müssen. Independence heißt Unabhängigkeit und bedeutet, dass sich Zahlungen gegenseitig nicht beeinflussen dürfen. Dauerhaftigkeit oder Durability heißt, dass man den Zustand eines Systems nach einem Defekt wieder herstellen kann.

Außerdem erwarten sowohl Händler als auch der Kunde von einem Zahlungssystem Fälschungssicherheit sowie Verlässlichkeit.

Fördern die entworfenen Mindestkriterien die Akzeptanz beim Endanwender?

Derzeit gibt es noch einige Sicherheitsbedenken, die eine breite Akzeptanz von NFC schwer machen. Wenn das Bezahlen vor allem von großen Beträgen möglich ist, wollen die Kunden die Sicherheit haben, dass diese Funktion nicht missbraucht werden kann.

Für einen Kunden ist es sehr wichtig die Sicherheit gegenüber dem Händler sowie gegenüber Dritten abschätzen zu können. Da dies oft gerade bei kleinen, spezialisierten Händlern oder Privatverkäufern sehr schwer möglich ist, darf das Risiko auch im Ernstfall nicht auf den Kunden abgewälzt werden.

Für die Erarbeitung der sicherheitsrelevanten Kriterien wurden unter anderem Studien über die Ablehnung oder Akzeptanz von Mobile Payment Systeme sowie über Sicherheit und Risiken bei der Datenübertragung von [DKPW03], [DAÖÖ07], [KPDW07], [AKPO04], [CANE02], [KEPO03], [MOMA02] sowie [TFHK08] ausgewertet.

Gelingt es die identifizierten Sicherheitsbedenken des Endanwenders entgegenzuwirken, kann das Vertrauen der Kunden gestärkt werden und dadurch eine hohe Akzeptanz von M-Payment erzielt werden. Gerade bei der Etablierung neuer Technologien ist das Sicherheitsgefühl der Anwender sehr leicht negativ beeinflussbar. Daher ist es erfolgsentscheidend noch vor der Vermarktung einer neuen Technologie, deren Risiken rechtzeitig zu identifizieren und zu minimieren, da publik gewordene Mißbrauchsfälle das Vertrauen der Anwender nachhaltig beeinflussen können (bzw. sogar für das Scheitern einer Technologie verantwortlich sein können).

Genauso wenig ist es förderlich schon lange bevor es eine entsprechende Anwendung geben wird, in der breiten Öffentlichkeit hohe Erwartungen zu wecken. Dabei besteht die Gefahr, dass die Konsumenten schnell gelangweilt sind und die Kommunikation ins Leere läuft. Das Timing der Kommunikation spielt somit eine sehr wichtige Rolle.

Bei jedem Einsatz von Technologie muss jedoch auch bedacht werden, dass es niemals absolute Sicherheit geben kann. Man kann lediglich versuchen, Technologie so sicher wie sinnvoll zu konzipieren.

Die Sicherheit bei M-Payment Verfahren ist das wichtigste Kriterium, jedoch beschränkt sich die Akzeptanz beim Endanwender nicht nur auf dieses Kriterium. Es ist vielmehr ein komplexes Zusammenspiel vieler unterschiedlicher Eigenschaften, die in Abbildung 24 dargestellt sind.

Merkmal	Merkmalsausprägung				
Vertraulichkeit der Daten	Niedrig	Mittel	Hoch		
Kosten	Transaktionskosten				Fixkosten
	Keine	Niedrig	Mittel	Hoch	
Abrechnungs-verfahren	Registrierung erforderlich	Verfahren			
		Prepaid	Lastschrift-verfahren	Kreditkarte	Telefon-rechnung
Belastungs-zeitpunkt	Vor Transaktions-Zeitpunkt	Zum Transaktions-Zeitpunkt	Nach Transaktions-Zeitpunkt		
Akzeptanz-stellen	Anzahl			Verbreitung	
	Niedrig	Mittel	Hoch	National	International
Benutzer-freundlichkeit	Bedienung		Vorgangsdauer		
	Einfach	Kompliziert	Kurz	Lang	
Techn. Voraus-setzungen	SMS	WAP	Dual-Slot/ Dual-Card Mobiltelefon	Payment-Software	
Eignung nach Bezahlszenario	Mobile Commerce	Electronic Commerce	Stationärer Händler	C2C	
Eignung nach Betragshöhe	Picopayment	Micropayment	Makropayment < 50 €	Makropayment > 50 €	
Eignung nach Zielgruppe	Altergruppe		Nutzungshäufigkeit		
	Erwachsene	Jugendliche	Vielnutzer	Wenignutzer	

Abbildung 24- Akzeptanzkriterien für M-Payment

Ein Verfahren, das eine hohe Verbreitung erreichen soll, sollte sehr viele dieser Eigenschaften erfüllen. Abgesehen vom wichtigsten Kriterium der Vertraulichkeit, stellen die Kosten für den Kunden ein essentielles Entscheidungsmerkmal dar. In manchen Ländern wie zum Beispiel Japan, ist die Zahlungsbereitschaft für Gebühren bei M-Payment Verfahren wesentlich höher. Im deutschen Raum können solche Kosten nur teilweise dem Kunden

auferlegt werden. Andererseits akzeptieren auch Händler solche Kosten und Gebühren nur zu einem gewissen Teil, da zu hohe Transaktionskosten eine Verringerung der Gewinnspanne bedeuten.

Die Anzahl der Akzeptanzstellen ist ein wesentliches Kriterium. Je mehr Akzeptanzstellen es für ein Zahlungssystem gibt, desto eher wird ein Kunde dieses nutzen. Es wird sich kaum jemand ein NFC Mobiltelefon anschaffen, wenn die Zahl der Händler zu gering ist. Einher geht damit auch das Marketing. Eine breite Akzeptanz von M-Payment wird nur in Verbindung mit der entsprechenden Menge an Akzeptanzstellen einhergehen.

Vorteilhaft ist, wenn ein Zahlungssystem auf viele Bezahlszenarien wie Mobile Commerce, Electronic Commerce, Stationärer Händler und C2C anwendbar ist. Idealerweise werden mit einem umfassenden M-Payment Verfahren alle Bereiche abgedeckt. Ebenso sollte ein Bezahlsystem nicht auf eine Betragshöhe zugeschnitten und eingeschränkt sein.

Mobile Contactless Payment besitzt sehr viel Potential, jedoch ist derzeit nur jeder zehnte Topmanager der Telekommunikationsunternehmen, laut einer Studie von Steria Mummert Consulting [ECIN07] der Meinung, dass das Mobiltelefon in den nächsten fünf Jahren als Geldbörse den Durchbruch machen wird. Laut dieser Studie gibt es derzeit einfach zu wenig Zuspruch für mobile Zahlungsverfahren und die Skepsis ist bei Geschäfts- und Privatkunden gleichermaßen vertreten. Lediglich acht Prozent glauben, dass sich mobile Zahlungsverfahren durchsetzen werden.

Diese Arbeit hat eine Vielzahl an Kriterien aufgezeigt, die für die Akzeptanz beim Endanwender besonders wichtig sind. Bestehende Implementierungen berücksichtigen diese Kriterien derzeit nur zu einem geringen Teil, was ein Scheitern einzelner Versuche von Mobile Contactless Payment zur Folge hatte. Wie in der Arbeit gezeigt wurde, ist zum Beispiel die Internationale Implementierung von Mobile Contactless Payment in den USA vor allem an einem schlechten Downloadinterface und an fehlender Usability gescheitert.

Da das Mobiltelefon bislang nicht für Zahlungsvorgänge eingesetzt wurde und diese hohe Sicherheitsstufe, wie sie für Zahlungsmethoden notwendig ist noch nicht erfüllt ist, wird es noch ein langer Weg sein, bis alle aufgezeigten Sicherheitsrelevanten Kriterien umgesetzt wurden. Außerdem muss die Gesellschaft ein Bewusstsein dafür entwickeln, dass auf dem Mobiltelefon sensible Daten gespeichert sind und daher auch Sicherheitsmaßnahmen, wie etwa die PIN-Sperre notwendig sind.

9 Zusammenfassung

In dieser Arbeit wurde ein theoretischer Überblick über Zahlungssysteme, M-Commerce, M-Payment sowie drahtlosen Übertragungstechnologien gegeben. Mobile Contactless Payment bezeichnet die Zahlung über NFC mittels eines Mobiltelefons.

Seit etwa einem Jahr gibt es in Österreich die ersten Implementierungen für Mobile Contactless Payment. Für die breite Akzeptanz fehlt jedoch das Vertrauen der Endanwender. Wie in der Arbeit gezeigt werden konnte, sind die Sicherheit des Zahlungssystems und das Vertrauen, das diesem folglich entgegen gebracht werden kann, die entscheidenden Kriterien für die Akzeptanz durch den Kunden.

In der Vergangenheit gab es mehrere Versuche, Mobile Contactless Payment einzuführen. Das nennenswerteste internationale Projekt war die Simulation von Kreditkarten auf dem Mobiltelefon, durchgeführt von der Bank of America in den USA. Dieses scheiterte, wie auch viele andere, aufgrund von fehlender Anwenderakzeptanz, aufgrund von Softwareproblemen, Downloadproblemen sowie schlechter Usability.

Weiters flossen für die Erarbeitung der sicherheitsrelevanten Mindestkriterien Ergebnisse aus nationalen und internationalen Projekten ein, die für eine erfolgreiche Einführung von Mobile Contactless Payment berücksichtigt werden müssen. Betrachtet man die identifizierten Sicherheitskriterien, erkennt man, dass man diese generell einteilen kann in allgemein gültige Aspekte, Anwenderfehler, Anforderungen an Hard- und Softwarekomponenten des Mobiltelefons als auch der Datenübertragung.

Die allgemein gültigen Sicherheitsaspekte sollte jedes System erfüllen. Hier werden Anforderungen klassifiziert, die vor allem für Datenkonsistenz innerhalb eines Systems sorgen. Für die Prävention von Anwenderfehlern spielt die Benutzerfreundlichkeit eine wesentliche Rolle, da ein ausgereiftes Design Fehlern entgegenwirkt.

Das Mobiltelefon ist als Trägermedium sehr gut geeignet, da es allgegenwärtig ist und dadurch Mehrwerte liefert. Wenn es notwendig ist, Daten beispielsweise auf der SIM Karte zu speichern, dann birgt dies viele Sicherheitsrisiken. Es wurden einige Angriffe identifiziert, mit denen das Auslesen von Daten auf einer Smart Card, zu der auch die SIM Karte gehört, möglich ist. Außerdem sind Sofwaremanipulationen durch Viren und Trojanern nicht auszuschließen, wobei dieser Themenbereich stellt für Software-Entwickler eine große Herausforderung dar. Letztendlich konnte gezeigt werden, dass sogar das Abhören von Daten während der NFC-Datenübertragung bis zu einem Meter Entfernung noch sehr gut möglich ist. Dieses Ergebnis ist besonders überraschend, da NFC eigentlich nur eine Reichweite von ca. 20 cm. haben sollte.

Im Rahmen der vorliegenden Arbeit wurden sämtliche relevanten Aspekte des Zahlungsverkehrs mit Mobile Contactless Payment identifiziert. Durch Analyse und Diskussion unterschiedlicher Fallbeispiele konnte deutlich aufgezeigt werden, dass erst bei Berücksichtigung dieser Aspekte die Endanwenderakzeptanz von Mobile Contactless Payment entscheidend erhöht werden kann.

10 Literaturverzeichnis

[ADOP05] Adam Opuchlik
E-Commerce-Strategie
Books on Demand GmbH 2005

[AERA08] AreaMobile AG
http://www.areamobile.de/
Abruf 21.01.2008

[AGED08] ARGE Daten
http://www2.argedaten.at

[ANLI07] Andreas List
NFC: Mobilfunkbranche treibt kontaktloses Bezahlen voran
http://www.pressetext.de/
03.12.2007
Abruf 15.01.2008

[ATML07] ATM Locator
http://www.atmlocator.de/
Abruf 09.12.2007

[AXPO04] Axel Poschmann
Wie sicher ist Mobile Payment?
Lehrstuhl für Kommunikationssicherheit
Universität Bochum
21.Juli 2004

[BBJF99] Frank Braatz, Ulrich Brinker, Hans-Jürgen Friederich
Alles über Zahlungsverkehr mit Karten
Verlag: Luchterhand Hermann
Januar 1999

[BEHA07] Bernhard Hammer
ECMA International Technical Committee 2007
Ecma/TC32/2008/003
Abruf: 12.02.2008

[BEWI01] Bernd W. Wirtz
Electronic Business
Dr. Th. Gabler GmbH
2. Auflage 2001

[BIEA08] bill-it-easy
http://www.billiteasy.com/

[BLUE08] Bluetooth Standard
http://www.bluetooth.com

[BSAS99] Bruce Schneier, Adam Shostack
Breaking Up IS Hard To Do: Modeling Security Threats for Smart Cards
USENIX Association Berkeley, CA, USA
Proceedings of Smartcard Technology
Chicago, Illinois October 1999

[BSIF08] Bundesamt für Sicherheit in der Informationstechnik
http://www.bsi-fuer-buerger.de/
Abruf 06.01.2008

[BSLF02] Berger S., Lehner F.
Mobile B2B Anwendungen
Teilkonferenz der Multikonferenz Wirtschafsinformatik, Nürnberg 2002

[CANE02] Caroline Neufert
Wieviel Sicherheit braucht Mobile Business?
Information Management & Consulting
Fachzeitschrift für Informatik
Information Multimedia Co. Saarbrücken. Nr. 17, 2002

[CHHO08] Christian Horn
Bezahlen per Handy fasst nur langsam Fuß
http://www.teltarif.de/
14.01.2008
Abruf 22.01.2008

[DABA07] Dan Balaban
CardTechnologie
Contactless In America: Some Banks Have Yet To Climb Aboard
Global Magazin of Smard Cards and personal Identification
25.05.2007
Abruf: 16.01.2008

[DAÖÖ07] Tomi Dahlberg, Anssi Öörni
Understanding Changes in Consumer Payment Habits
Proceedings of the 40th Hawaii International Conference on System Sciences - 2007

[DKPW03] Darius Khodawandi, Key Pousttchi, Dietmar G. Wiedemann
Akzeptanz mobiler Bezahlverfahren in Deutschland
3. Workshop Mobiler Commerce
Gesellschaft für Informatik (GI) 2003
Proceedings

[DRFR07] Dr. Reinhard Freund
http://www.drfreund.net/
Abruf 09.12.2007

[ECIN04] ECIN – Electronic Commerce Info Net
ePayments
Zeitgemäße Ergänzung traditioneller Zahlungssysteme (2004)
Abruf: 05.01.2008

[ECIN07] ECIN
Weiterhin warten auf Mobile Payment
http://www.ecin.de/
05.01.2007
Abruf: 28.01.2008

[ECMA] ECMA – Internationale Normungsorganisation
http://www.ecma-international.org/

[ECMA340] ECMA 354
Near Field Communication Interface and Protocol
http://www.ecma-international.org/

[ECMA352] ECMA 352
Interface and Protocol
http://www.ecma-international.org/

[ECMA356] ECMA 356
RF Interface Test Methods
http://www.ecma-international.org/

[EMHB02] Ernst M., Jung M., Madlener F., Huss S., Blümel R.
A Reconfigurable System on Chip Implementation for Elliptic Curve Cryptography
Cryptovision GmbH 2002
Computer Science Department
Darmstadt University of Technology, Germany

[EPSO08] ePayment Systems Observatory
http://epso.intrasoft.lu/
Abruf: 04.01.2008

[ETSI08] European Telecommunication Standard Institute
http://www.etsi.org/

[ETSI102051] ETSI TS 102 051 v1.1.1. (02/2007)
ENUM Administration in Europe
http://www.pts.se/

[EURO07] Eurocheques.de
http://www.eurocheques.de/
Abruf 09.12.2007

[FDSW06] Werner Franke, Wilhelm Danglmaier,
Christian Sprenger, Frank Wecker
RFID Leitfaden für die Logistik
Gabler Verlag 1. Auflage
September 2006

[FELI08] FeliCa Standard
http://www.sony.net/

[FESSL04] Befragung der österreichischen Bevölkerung bez. Handypayment ab 12 Jahren (2003 – 2005)
November 2004
Fessl-GfK – Institut für Markforschung GesmbH

[FGWH06] Dr. Frank Giller, Wolf-Rüdiger Hansen
RFID für die Optimierung von Geschäftsprozessen
Hanser Fachbuchverlag 1.Auflage
Oktober 2006

[FICB08] Firstgate Click&Buy
http://clickandbuy.com/
Abruf 06.01.2008

[FSWW03] Joachim Funke, Michael Stumpf,
Erich Weichselgartner, Friedrich Wilkening
Qualitätssicherung im Bereich neuer Medien durch Einführung von Qualitätskriterien
Universität Heidelberg 2003

[GEKA08] Geldkarte
http://www.geldkarte.de/

[GEKR04] Kreditkarten Vermittlung
http://www.kreditkarten-anbieter.de/
Abruf 25.09.2007

[GSMW08] GSM World
http://www.gsmworld.com/

[HABE99] Hagai Bar-El
Known Attacks Against Smartcards 1998
Technical Report
Advances in Cryptology – Crypto 99 Proceedings

[HONC02] Kommision der Europäischen Gemeinschaften
EU Richtlinie zum Schutz persönlicher Daten 2002
http://www.hon.ch/HONcode/HON_CCE_de.htm

[HSCH08] ABI Research
Studie: Sicherheit ist Erfolgsfaktor für NFC
http://www.abiresearch.com/
23. August 2007
Abruf: 12.02.2008

[IEEE08] IEEE Standard 802.11
http://standards.ieee.org/getieee802/802.11.html

[INRF07] Informationsforum RFID
Basiswissen RFID
www.info-rfid.de
Abruf 11.11.2007

[INTE08] Internationale Telekommunikationsunion
http://www.itu.int/net/home/index.aspx
Abruf: 24.02.2008

[INTM08] Informa Telecoms & Media
Specialist Information for global markets
Statistik: Weltweit 3,3 Milliarden Handy-Verträge
Artikel vom 30.11.2007
http://www.informa.com/

[IRDA] IRDA Data
http://www.irda.org/

[ISO18092] ISO 18092
http://www.ecma-international.org/

[ISO21481] ISO 21481
http://standards.iso.org/

[ITIU04] International Telecommunication Union
Internationale Studie 2004
http://www.itu.int/
Abruf 04.05.2007

[ITME07] Einfacher als SMS-Ticketing
it&t business
10/2007
Abruf 15.01.2008

[JELA05] The history of RFID
Jeremy Landt
IEEE Potentials
Oktober/November 2005

[JOHE01] Joachim Henkel
Anforderungen an Zahlungsverfahren im E-Commerce
E-Commerce und E-Payment
R.Teichmann, M. Nonnenmacher, J. Henkel
GABLER VERLAG 2001

[JOPU06] Jochen Punzet
paybox austria – eine M-Payment Erfolgsgeschichte
Handbuch E-Money, E-Payment & M-Payment
Physika Verlag 2006

[JOTY70] John Tyndall
Faraday und seine Entdeckungen
Braunschweig – Verlag von Friedrich Vieweg und Sohn 1870
Abruf 09.12.2007

[JÜKU03] Jürgen Kuhn
Kommerzielle Nutzung mobiler Anwendungen
Dissertation Universität Regensburg, 2003
Wirtschaftswissenschaftliche Fakultät

[KASH99] Kathrin Schier
Vertrauenswürdige Kommunikation im elektronischen Zahlungsverkehr
Dissertation 1999
Universität Hamburg, Fachbereich Informatik

[KAWI04] Kai Winhoven
Rechen- und Kommunikationszentrum der RWTH Aachen
http://www.rz.rwth-aachen.de/
05.22.2004
Abruf: 10.11.2007

[KEPO03] Key Pousttchi
Conditions for acceptance and usage of mobile payment procedures
mBusiness 2003
The Second International Conference on Mobile Business

[KEPO05] Key Pousttchi
Mobile Payment in Deutschland
Szenarioübergreifendes Referenzmodell für mobile Bezahlvorgänge
DUV – Gabler Edition Wissenschaft, 2005

[KEYP03] Key Pousttchi
Abrechnung mobiler Mehrwertdienste
Proceedings Informatik
Innovative Informatikanwendungen 2003

[KPDW07] What Influences Consumers' Intention to Use Mobile Payments?
Key Pousttchi, Dietmar G. Wiedemann
Mobile Commerce Working Group
Chair of Business Informatics and Systems Engineering
University of Augsburg
Los Angeles Mobility Roundtable 2007

[KTKP04] Klaus Turowski, Key Pousttchi
Mobile Commerce
Springer Verlag Berlin Heidelberg 2004

[LRCL95] Paul Lorrain, Dale R. Corson, Francois Lorrain
Electromagnetische Felder und Wellen
Gruyter Verlag
Auflage 1 1995

[LSCH06] Lutz Schmitt
Konzept für Privatspäre im Ubiquitous Computing
Diplomarbeit
Juni 2006

[MAGK04] Markus G. Kuhn
Electromagnetic Eavesdropping Risks of Flat-Panel Displays
University of Cambridge
Computer Laboratory
4th Workshop on Privacy Enhancing Technologies 2004

[MAHÖ02] Marc Höft
Zahlungssysteme im Electronic Commerce
Books on Demand GmbH
1. Auflage Oktober 2002

[MDAU04] Marius Dannenberg, Anja Ulrich
E-Payment und E-Billing
Elektronische Bezahlsysteme für Mobilfunk und Internet
Gabler 2004

[MIFA08] Philips-MIFARE Standard
http://www.mifare.net/

[MISL05] Mike Slocombe
NFC First, Nokia 3220 Brings Contactless Payment and Ticketing
http://digital-lifestyles.info/
10.02.2005
Abruf 16.01.2008

[MIWE07] Michael Welzel
Was ist Near Field Communication?
Near Field Communication Forum
Jahr 2007

[MKRA98] Markus G. Kuhn, Ross J. Anderson
Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations
University of Cambridge
Computer Laboratory
Information Hiding
Springer Verlag Berlin Heidelberg 1998

[MOBA04] MobilMedia-Barometer, 2. Welle: M-Payment
Befragungszeitraum 11.-14.09.2004
Bundesministerium für Wirtschaft und Arbeit, Deutschland

[MOBI07] Informationen rund um Mobilfunk
http://www.mobilkomaustria.com
Abruf: 12.12.2007

[MOMA02] Marcus Mosen
Mobile Payment – Dienstleistung im Spannungsfeld zwischen Finanzdienstleistern und Telekommunikationsanbietern
Handbuch Mobile-Commerce: technische Grundlagen, Marktchancen und Einsatzmöglichkeiten
Springer-Verlag, Berlin Heidelberg 2002

[MONB08] Moneybookers
http://www.moneybookers.com/app/

[MOPA08] Mobile Payment Forum
http://www.mobilepaymentforum.org/
Abruf 14.02.2008

[NFCC08] NFC – Mobilkom Austria AG
http://www.nfc.at/
Abruf 15.01.2008

[NFCF07] Near Field Communication Forum
http://www.nfc-forum.org
Abruf 20.11.2007

[NKPT02] Nina Kreyer, Key Pousttchi, Klaus Turowski
Characteristics of Mobile Payment
Proceedings of the ISMIS 2002

[NXPC08] NXP
http://www.nxp.com/
Abruf 14.01.08

[OENB08] Österreichische Nationalbank
http://www.oenb.at/
OENB Zahlungsmittelumfrage
Abruf 06.01.2008

[ORTI06] IEEE
Ortiz
Volume 39, Issue 3, March 2006
http://www.ieee.org/portal/site
Abruf: 05.05.2007

[OSWA96] Global System for Mobile Communication
http://oswaldism.de/
GNU General Public Licence
Abruf 03.09.2007

[PATA06] Taylor Patel
Mobile Contactless Payments: Growth on the Horizont (2006)
http://www.strategyanalytics.net/
Abruf: 08.04.2007

[PAYB08] Paybox
http://www.paybox.at/

[PAYP08] PayPal
https://www.paypal.com/
Abruf 05.01.2008

[PAYS08] Paysafecard
http://www.paysafecard.com/
Abruf 05.01.2008

[PAYS08] Paysafecard
http://www.paysafecard.com/at/

[PBST02] Key Pousttchi, Bernhard Selk, Klaus Turowski
Akzeptanzkriterien für mobile Bezahlverfahren
Mobile and Collaborative Business 2002
Nürnberg 2002

[PCKO96] Paul C. Kocher
Timing Attacks on Implementations of Diffie Hellmann, RSA, DSS and Other Systems
Cryptography Research 1996
Lecture Notes in Computer Science
Springer Verlag 1996

[PDDL00] Markus Puchleitner, Wolfgang Dürauer,
Felix Dibelka, Hubert Lindner
Mobile Commerce Report 2000

[PFMC05] Mobile Web Services
P. Farley, M. Capp
BT Technology Journal
Vol. 23 No.2
April 2005

[PKJB99] Paul Kocher, Jushua Jaffe, Benjamin Jun
Differential Power Analysis
Cryptography Research
Lecture Notes in Computer Science
Springer Verlag 1999

[PWMO06] Prof. Dr. Klaus-Peter Wiedmann, Dipl.-Oec. Marc-Oliver Reeh
Positionspapier zu den Erfolgsaussichten von NFC - Der menschliche Kommunikationsmechanismus als Maß aller Dinge!
Institut für Marketing und Management 2006

[QUIC08] @Quick
http://www.quick.at/

[RCRM03] Robin Contius, Robert Martignoni
Mobile Payment im Spannungsfeld vonUngewissheit und Notwendigkeit
3. Workshop Mobile Commerce (2003)
Proceedings

[RFID07] rfid ready Verlag
Informationsportal
http://www.rfid-ready.de/
Abruf 05.12.2007

[ROCO02] Robin Contius
Perspectives of Mobile Payment
Diplomarbeit
2002

[RTRG08] Rundfunk und Telekom Regulierungs-GmbH
http://www.rtr.at/

[RTRT07] RTR Telekom Monitor
Rundfunk und Telekom Regulierungs-GmbH
http://www.rtr.at/
4.Quartal 2007

[SGJT01] Günter Silberer, Jens Wohlfahrt, Thorsten Wilhelm
Mobile Commerce
Grundlagen, Geschäftsmodelle, Erfolgsfaktoren
Gabler Verlag
29. November 2001

[SHLF04] Karsten Stroborn, Annika Heitmann, Kay Leibold, Gerda Frank
Internet payments in Germany: a classificatory framework and empirical evidence
Journal of Business Research 57 (2004)

[SIOR06] Sixto Ortiz Jr.
Is Near Field Communication close to success?
IEEE Comupter Society
März 2006

[TFHK08] Thomas Finke, Harald Kelter
Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO1443 Systems
Bundesamt für Sicherheit der Informationstechnik
Abruf 06.01.2008

[THLA06] Thomas Lammer
Handbuch E-Money, E-Payment & M-Payment
Physica-Verlag Heidelberg 2006

[THPL05] Thomas Pleil
Anmerkungen und strategische Ansätze zur Kommunikation von M-Payment
Proceedings zur 5. Konferenz Mobile Commerce
Technologien und Anwendungen 2005
GI-Edition

[THSB04] Tamara Högler, Gunther Schiefer, Rebecca Bulander
Institut AIFB, Universität Karlsruhe
Bundesministerium für Arbeit und Wirtschaft
Projekt „MoMA - Mobiles Marketing“ (2004)

[TLKS06] Thomas Lammer, Karsten Stroborn
Internet-Zahlungssysteme in Deutschland und Österreich: ein Überblick
Handbuch E-Money, E-Payment & M-Payment
Physika Verlag HD 2006

[TOWO08] mPay24 – Zahlungsplattform für E- und M-Commerce
Tom Wolf
Maestro SecureCode und E-Government Gütesiegel
https://www.mpay24.com/
Abruf 05.01.2008

[UMTS08] UMTS Standard
http://www.umtsworld.com/

[UVRV02] Upkar Varshney, Ron Vetter
Mobile Networks and Applications
Volumne 7, Issue 3 (June 2002)

[VENY08] Venyon
http://www.venyon.com/
Abruf 20.01.2008

[VEVI08] Visa/Cardcomplete
http://www.visa.at

[WEBC08] WEB.Cent
https://www1.webcent.web.de/

[WELT07] Deutsche Physikalische Gesellschaft
http://www.weltderphysik.de/de/
Abruf 09.12.2007

[WKOB06] Wirtschaftskammer
http://wko.at/
Abruf: 04.01.2008

[WOBR07] Wie ich vor 40 Jahren den Geldausgabeautomaten erfand
Wolfgang Braunwieser
SBS Salzburger Banken Software
18. Ausgabe 18. Mai 2007

[WTMS03] Kundenwert in Banken und Sparkassen
Werner E. Thum, Michael Semmler
Gabler Verlag 2003

[XOVE07] XOVER Digital Communication Explored
CrossOVER Thomas Zettelmayr
http://www.x-over.com/
Abruf 05.10.2007

[YCHJ04] Yuntsai Chou, Chiwei Lee and Jianru Chung
Understanding m-commerce payment systems through the analytic hierarchy process
Journal of Business Research 57 (2004)
Yuan Ze University, Taiwan, ROC

[ZEGE05] Hans G. Zeger
Analyse der Einhaltung der E-Commerce rechtlichen Bestimmungen bei Online Shops 2005
ARGE Daten
Abruf 05.01.2008