

Near Field Communication (NFC) als weiterer Baustein des „Pervasive Computing“

Michael Peleschka
michael[at]peleschka.at

24. September 2006

ausgeführt am „Institut für Softwaretechnologie und interaktive Systeme“
der Technischen Universität Wien,
bei Herrn Dipl. Ing. Dr. Alexander Schatten.

Zusammenfassung

Bei der Near Field Communication handelt es sich um eine neue Schnittstelle zum elektronischen Datenaustausch, die auf der RFID- Technologie aufbaut und darüber hinaus noch weitere Vorteile bietet.

Mit dieser ist es möglich die Mensch-Maschinen Interaktion auf ein simples Berühren zu reduzieren. Damit hat die NFC- Technologie das Potential, viele mobile Geschäftsanwendungen radikal zu vereinfachen bzw. neue zu schaffen.

Unter Pervasive Computing versteht man auch das Zusammenspielen vieler kleiner vernetzter digitaler Geräte, die den Menschen auf einfache und intuitive Art und Weise bei zahlreichen Problemstellungen unterstützen.

Somit kann die NFC- Technologie einen weiteren wichtigen Baustein zum sog. Internet der Dinge liefern.

Inhaltsverzeichnis

1	Die Idee des Pervasive Computing	3
1.1	Was versteht man unter dem Begriff „Pervasive Computing“	3
1.2	Voraussetzungen	4
1.2.1	Moorsche Law	4
1.2.2	Hardware	5
1.2.3	Kommunikationstechnologien	7
2	NFC: Technologie	10
2.1	Einleitung	10
2.2	Technische Funktionsweise	13
2.3	Standards	16
2.4	Security	17
2.5	NFC Software Applikationen	18
2.6	Mögliche Einsatzgebiete der NFC- Technologie	21
2.7	Marktchancen	22
3	NFC Anwendungsbeispiele und Pilotprojekte	24
3.1	Echtzeit- Reportingsysteme	24
3.1.1	Anwendungsbeispiel: Strom/Gas Zähler ablesen	24
3.1.2	Anwendungsbeispiel: Nachtwächter	25
3.2	Ticketing	26
3.2.1	Pilotprojekt der Stadt Haunau: Das Handy als Fahrkartenautomat	26
3.3	Unterhaltungselektronik	29
3.4	Pervasive Games und Edutainment	29
3.5	Werbung und Tourismus	30
3.6	Authentifizierungssysteme	31
3.6.1	Smart device statt vieler Plastikkarten und Dokumente	31
3.6.2	Skinplex- Die menschliche Haut als Funksender	32
4	Fazit	33

1 Die Idee des Pervasive Computing

1.1 Was versteht man unter dem Begriff „Pervasive Computing“

„Alle Dinge haben vor allem dem Menschen zu dienen.“ R. H. Tawney [16]

Die rasante Entwicklung in der IT ausgehend vom Mainframe in den 1960er Jahren bis zur Etablierung des Personal Computer in den 80er Jahren des letzten Jahrhundert setzt sich fort, hin zu einem mobilen Informationszugang bzw. sogar zu einer gewissen Art von digitalem kollektiven Bewusstsein.

Heute ist es meist noch so, dass eine einzelne lokale Maschine den Zugang zu den gewünschten Informationssystemen bewerkstelligt. Im Gegensatz dazu geht der Trend bereits in eine andere Richtung. Es zeigt sich, dass der berufliche sowie private Alltag immer mehr von einer Vielzahl von kleinen, intelligenten Geräten mit einem hohen Maß an Kommunikationsfähigkeit durchdrungen ist und wird. Dabei spielt es keine Rolle mehr, ob man sich stationär an einem bestimmten Ort aufhält oder nicht. Der Zugang zu Information ist jederzeit und überall vorhanden.

Der Amerikanische Wissenschaftler Mark Weiser hatte bereits Anfang der 1990er Jahre in seinem Aufsatz „The Computer for the 21st Century“ [23] den Begriff des *Ubiquitous Computing* geprägt. Seiner Meinung nach wird der Personal Computer immer mehr an Bedeutung verlieren und durch das so genannte *Internet der Dinge* ersetzt. Diese soll den Menschen auf intuitive Art und Weise bei einer Vielzahl von Problemen unauffällig unterstützen.

Ein ebenfalls verwandter Begriff ist *Ambient Computing* und stammt aus dem europäischen Forschungsprojekt „Information Society Technologies“. Hierbei geht es ebenfalls um das intelligente Vernetzen der Umgebung. Als Beispiel dafür sei das intelligente Haus genannt. Dabei soll es möglich sein die ganze Infrastruktur (Heizung, Klima, Küche, etc) vollautomatisch auch via mobilen Geräten an die jeweiligen Bedürfnisse der Bewohner automatisch anzupassen.

Pervasive Computing beschäftigt sich im Unterschied zu Ubiquitous Computing bzw. Ambient Computing mit bereits existierenden Technologien und Konzepten um aktuelle Geschäftsprozesse zu optimieren und neue zu schaffen.

Aktuelle Beispiele seien mobile E-Commerce Anwendungen mit Handys bzw. PDA's. Auch in der Transport / Logistik Branche werden immer mehr Güter mit vernetzten Mikrochips (bzw. RFID) ausgestattet um integrierte Echtzeitsysteme realisieren zu können. Viele weitere Anwendungen, zum Beispiel in der Unterhaltungsindustrie, Werbung oder Handel, werden bereits heute eingesetzt oder in absehbarer Zukunft entstehen. Siehe auch Abbildung 1.

Eine wichtige Rolle spielten dabei die vernetzte Hardware wie zum Beispiel *Near Field Communication* (NFC) und *Radio Frequency Identification* (RFID), auch als *smart devices* bezeichnet.

Durch das Zusammenwachsen des Internets mit drahtlosen Kommunikationssystemen, dem Auflösen der klassischen Client-Server Architektur ergeben sich auch völlig neue Herausforderungen für Wirtschaft, Gesellschaft und Politik.

Quelle: [9], [21].

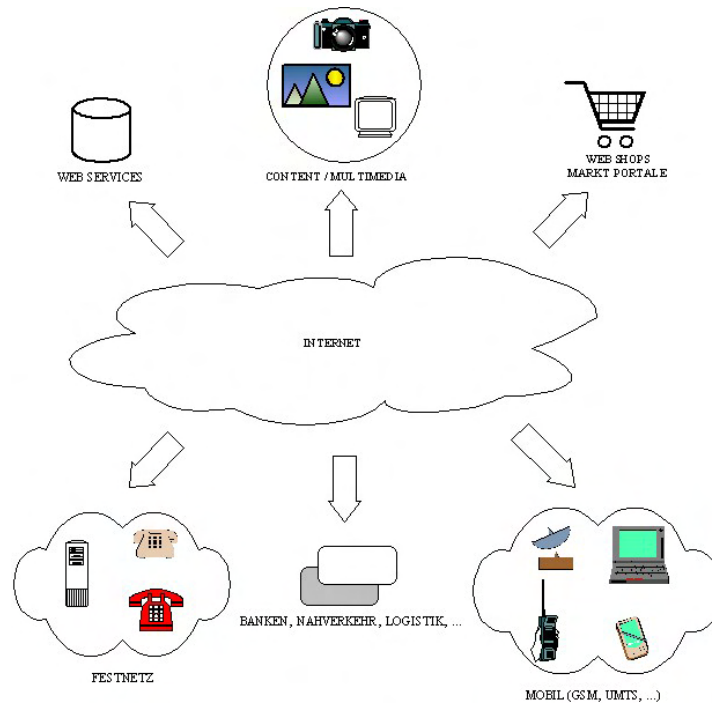


Abbildung 1: Pervasive Computing: Das Internet ist überall.

1.2 Voraussetzungen

Die Tatsache, dass Halbleiterbauteile und Computer immer leistungsfähiger, kleiner und billiger werden verdanken wir der beeindruckenden Entwicklung in der Mikroelektronik. Parallel dazu entstanden immer schnellere drahtlose Netzwerke sowie interoperable Kommunikationsprotokolle für den Datenaustausch über Systemgrenzen hinweg. Ebenso gibt es stetige Verbesserungen und Weiterentwicklung bei der Software.

Diese gleichzeitigen, auf verschiedenen Ebenen stattfindenden Entwicklungen und Errungenschaften, befinden sich bereits heute auf einem Niveau, das *Pervasive Computing* Realität werden kann.

Im Folgenden werden die einzelnen technischen Voraussetzungen kurz beschrieben.

1.2.1 Moorsche Law

Das Moorsche Law ist kein Naturgesetz sondern eine Faustregel und wurde in der amerikanischen Zeitschrift *Electronics* am 19. April 1965 vom Intel- Mitbegründer *Gordon Moore* erstmals publiziert [11]. In diesem beschreibt Moore die Beobachtung, dass sich die Komplexität von „Integrierten Schaltungen“ etwa alle 24 Monate verdoppelt bzw. diese ein exponentielles Wachstum aufweist.

In Abbildung 2 ist ersichtlich, dass sich die Anzahl der Transistoren pro integrierten Schaltkreis tatsächlich seit den 1970er Jahren gemäß dem Moorsche Gesetz zirka alle 2 Jahre verdoppelt. Interessant ist in diesem Zusammenhang auch, dass man dieses Gesetz nicht nur bei integrierten Schaltungen beobachten kann. Es zeigt sich auch im exponentielle Wachstum der Datenübertragungsraten, immer leistungsfähigeren Prozessoren bei gleichen oder billiger wer-

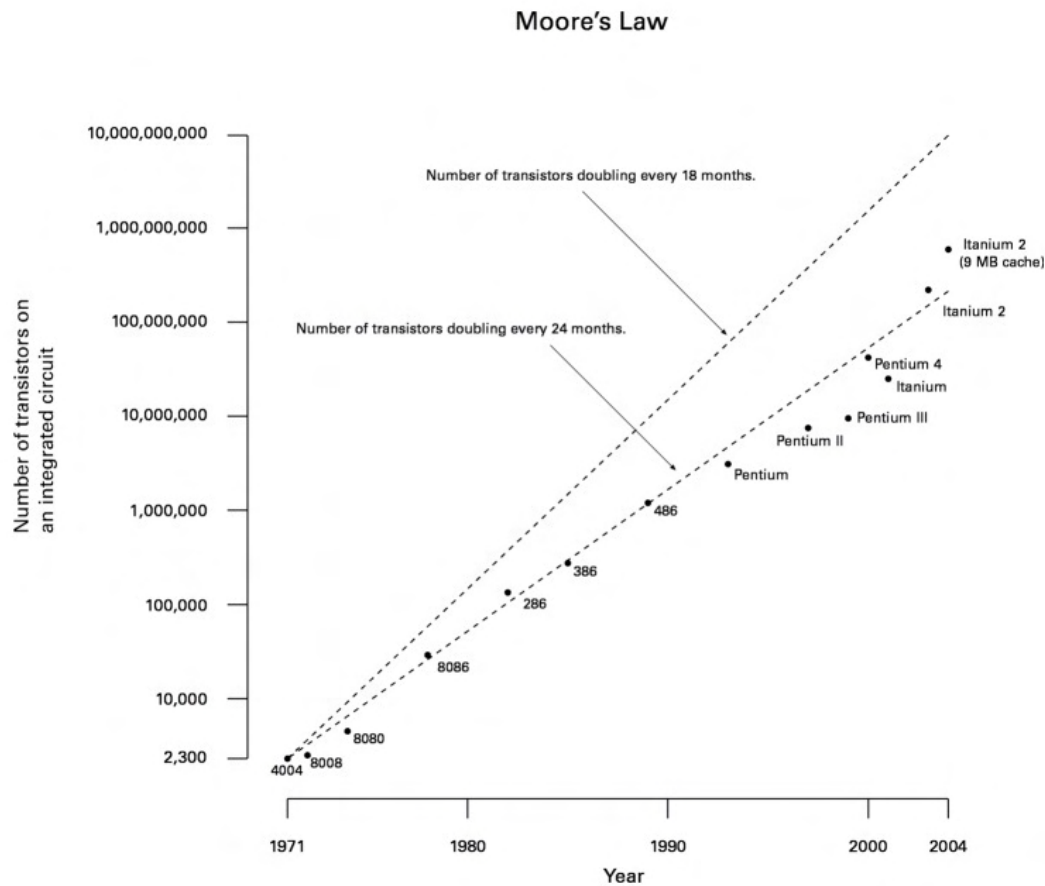


Abbildung 2: Die Anzahl der Transistoren verdoppelt sich ca. alle 24 Monate. Quelle Abbildung: „Wikipedia. Die freie Enzyklopädie“.

denden Preisen sowie im rasanten Wachstum der Speicherkapazitäten.

Im Allgemeinen geht man trotz einzelner Kritiker davon aus, dass das Moorsche Gesetz auch in den nächsten 10 bis 20 Jahren gültig sein wird. Was dies für den technischen Fortschritt bedeutet, lässt sich heute kaum erahnen.

1.2.2 Hardware

Wie bereits oben festgestellt, entwickeln sich Hardwarekomponenten mit rasanter Geschwindigkeit. Ebenfalls steht eine große Anzahl von mobilen Geräten oder Sensoren mit einem immer größeren Horizont an physikalischen Messgrößen zum Sammeln von Daten zur Verfügung. Noch gibt es eine natürliche Mindestgröße von mobile devices, die sich aus der Mensch-Maschinen Schnittstelle ergibt.

In naher Zukunft kann die Dateneingabe nicht mehr über eine Tastatur sondern zum Beispiel via Sprache erfolgen. Bei der Datenausgabe werden neue Materialien (Stichwort: *Polymer-elektronik*) sowie die Miniaturisierung neue optische Anzeigelösungen wie ein *Head-Mounted Display* oder in fernerer Zukunft das *digitale Papier*, bringen [9].

Diese Geräte werden schließlich überhaupt nicht mehr physisch wahrnehmbar sein, da sie im Stoff unserer Kleidung oder in Alltagsgegenständen wie zum Beispiel Brille oder Kugelschreiber eingebaut werden. Natürlich kann man solche *smart Devices* auch im bzw. am Menschen implementieren. Dies wird bereits heute in der Medizin (zum Beispiel Herzschrittmacher) erfolgreich angewandt. Der Begriff des *Cyborg*, welcher Anfang des zwanzigsten Jahrhunderts in science fiction Romanen als Mensch-Maschinen Kreation definiert wurde, nimmt nun bereits konkrete Gestalt an. [18]

Nun wird auf die wichtigsten Hardwarekomponenten wie Stromversorgung, Speicherkapazität kurz eingegangen.

Energieversorgung: Für Pervasive Computing werden hauptsächlich kleine und mobile Geräte eingesetzt. Als wichtigste Energiequelle ist daher die Batterie zu betrachten. Im Gegensatz zur Mikroelektronik hat sich die Batterietechnologie deutlich langsamer weiterentwickelt. Dazu kommt, dass die meisten Fortschritte durch den erhöhten Energieverbrauch von leistungsfähigeren Mikroprozessoren zunichte gemacht wurden.

Aktueller Standard in vielen Mobiltelefonen, Laptops, Digitalkameras ist der *Lithium Ionen* Akku. Er hat den Nickel-Cadmium Akku abgelöst und zeichnet sich durch eine höhere Energiedichte sowie Lebensdauer (kein Memory Effect) aus.

Das Praktische von RFID- Sendern ist die Möglichkeit, dass diese gänzlich ohne eigener Energieversorgung auskommen können. Die zur Datenübertragung notwendige Energie beziehen sie mittels Induktion aus den Funksignalen von der Basisstation. Natürlich sind dann der Reichweite der Datenübertragung physikalische Grenzen gesetzt.

Bei der NFC- Technologie ist ebenfalls ein passiver Betriebsmodus möglich. Weitere Details dazu gibt es im Kapitel 2.2 auf Seite 13.

Speicher: Eine weitere Voraussetzung für Pervasive Computing ist die Möglichkeit, immer mehr Daten in immer kleineren und billigeren Chips zu speichern.

Moore's Law sei Dank, dass dies bereits in der Vergangenheit und wohl auch in der Zukunft erfüllt sein wird. Wichtige Technologietreiber sind die Telekommunikationsanbieter sowie die Unterhaltungsindustrie, die mit Ihren speicherintensiven Inhalten (Multimedia) ein großes Interesse an hohen Speicherkapazitäten zu möglichst günstigen Preisen haben.

Aktuell werden sogenannte *Flash EEPROM* (Electrically Erasable Programmable Read-Only Memory) eingesetzt. Diese Technologie ermöglicht das persistente Speichern von Daten auf minimalem Raum. Weitere Vorteile sind die günstigen Preise der Flash Karten, der geringe Energiebedarf im Betrieb sowie die Resistenz gegenüber mechanischen Erschütterungen.

Die erzielten Speicherkapazitäten reichen zur Zeit je nach Type von einigen Megabyte bis zu 12 Gigabyte bei CF-Karten.

Auch die Festplatten werden immer kleiner. Man spricht dabei von *Microdrives* die bereits die Größe von Compact Flash Karten erreichen. Ihr Vorteil ist der relativ günstigere Preis gegenüber den Flashkarten sowie schnellere Datenübertragungsraten. Nachteile für Pervasive Computing sind der höhere Energiebedarf und Empfindlichkeit gegenüber Erschütterungen. In Abbildung 3 befinden sich unterschiedliche Speichertypen.

Vielversprechend sind Forschungen der Firma IBM, die mit der Speichertechnik *Millipede* die Vorteile von Flashkarten und Microdrives kombinieren und die Nachteile minimieren sollen.



Abbildung 3: Compact Flash Karte (Digitalkamera), Multi Media Card (Handy, PDA), Mini-USB Festplatte.

Die offizielle Projekthomepage finden Sie hier ¹.

Prozessoren/Mikrocontroller: Die Entwicklung von Prozessoren bzw. Mikrocontrollern verlief ähnlich schnell wie die der Speicher.

Verbesserungen der CMOS- Herstellungstechniken führten zu immer kleineren Bauteilen bei gleichzeitiger Steigerung der Dichte von Transistoren. Zusätzlich konnte im Jahr 2000 die Versorgungsspannung von 3,3V auf 1,35V gesenkt werden.

Es gibt bereits eine Vielzahl von Prozessoren, die speziell für den mobilen Bereich (Laptop) optimiert wurden. Diese besitzen unter anderem ein effizientes Power-Management. Damit sind diese Prozessoren in der Lage ihre Taktfrequenz und Kernspannung flexibel an die jeweiligen Gegebenheiten anzupassen. Aktuelle mobile Prozessorvertreter sind zum Beispiel der Intel Core 2 Duo oder die AMD Turion 64 Mobile Technology Familie.

Für Pervasive Computing eignen sich *Mikrocontroller* hervorragend. Denn dazu sind meist keine hohe Taktraten erforderlich.

Auf diesen preiswerten Chips sind sämtliche notwendige Computerkomponenten wie CPU, Arbeitsspeicher, Ein/Ausgabe Schnittstellen integriert. Diese befinden sich bereits heute oft unmerklich in einer Vielzahl von Gebrauchsgegenständen wie zum Beispiel die Heizung, Waschmaschine, das Handy oder im Auto.

1.2.3 Kommunikationstechnologien

Eine wichtige Grundlage für Pervasive Computing ist, dass sich eine Vielzahl von unterschiedlichen stationären sowie mobilen Geräten untereinander drahtlos austauschen können. Dabei spielen Datenübertragungstechniken, Netzwerkprotokolle und Standards wie zum Beispiel

¹<http://www.zurich.ibm.com/st/storage/millipede.html>

XML [10] eine besondere Rolle.

Für die Architektur von solchen Webanwendungen wird aufgrund ihrer Plattformunabhängigkeit häufig die Programmiersprache *JAVA* (*JAVA Server Pages*, *Enterprise JAVA Beans*, *JDBC* etc.) eingesetzt.

Auf weitere wichtige technische Designkriterien für Pervasive Computing wie Transparenz, Skalierbarkeit oder Security kann in diesem Dokument nicht explizit eingegangen werden. Informationen zu diesen Punkten können Sie hier [1] finden.

Es folgt ein Überblick über die wichtigsten Kommunikationstechnologien und Protokolle.

Drahtlose Netzwerke Momentan kann man diese in folgende Kategorien unterteilen:

Mobilfunktechnologien:

Die Einführung der *GSM* (Global System for Mobile Communications) - Erweiterung *GPRS* (General Packet Radio Service) erlaubte zum ersten Mal eine paketorientierte Datenkommunikation sowie variable Bandbreiten bis zu 171 kBit/s.

UMTS (Universal Mobile Telecommunications System) ist der Mobilfunkstandard der dritten Generation (3G) und erfreut sich zunehmender Beliebtheit. Dieser definiert neben der Sprachtelefonie eine Reihe von Services die parallel genutzt werden können.

Die erzielbare Datenübertragungsrate liegt bei 384 kBit/s. Durch zusätzliche Erweiterungen des Standards (*HSDPA*) sollen Übertragungsraten von 10,8 Mbit/s noch im Jahre 2006 möglich sein.

Für Pervasive Computing sind die zusätzlich spezifizierten Dienste für Multimedia, E-Commerce, Informationsdienste oder Navigationssysteme besonders interessant. Der Vorteil von Mobilfunknetzen ist, dass diese beinahe weltweit vorhanden sind.

WLAN:

WLAN (Wireless Local Area Network) steht für eine Funktechnik die hauptsächlich im Nahbereich (30-100 Meter) verwendet wird, um Notebooks einen schnellen mobilen Internetzugang zu ermöglichen.

Neben lokalen Firmennetzen findet man neuerdings *WLAN*-Hotspots auch in öffentlichen Bereichen wie Cafés, Hotels oder Flughäfen. Nach dem neusten *WLAN*-Standard *IEEE 802.11n* werden brutto Datenraten von bis zu 600 Mbps insgesamt für alle Netzteilnehmer möglich sein.

Aufgrund des erhöhten Strombedarfs findet man *WLAN* meist in Notebooks bzw PDAs- jedoch noch kaum in Handys.

Bluetooth:

Der dänische König Harald Blaatand (Harald Blauzahn) einigte im 11. Jahrhundert die skandinavischen Völker und ist Namensgeber der von der Firma Ericsson maßgeblich entwickelten drahtlosen Funktechnologie.

Im Gegensatz zu *WLAN* dient *Bluetooth* der Verbindung von smart devices wie zum Beispiel Handys, MP3-Player, Digitalkameras, PDAs, Laptops etc. im Nahbereich. Je nach Sendeleistung beträgt die maximale Entfernung 10 bis 100 Meter bei Datenübertragungsraten von 732,2 kBit/s bis zu aktuell 2,1MBit/s.

Für unterschiedliche *Bluetooth*- Anwendungen gibt es bestimmte dazupassende Profile. Bei der

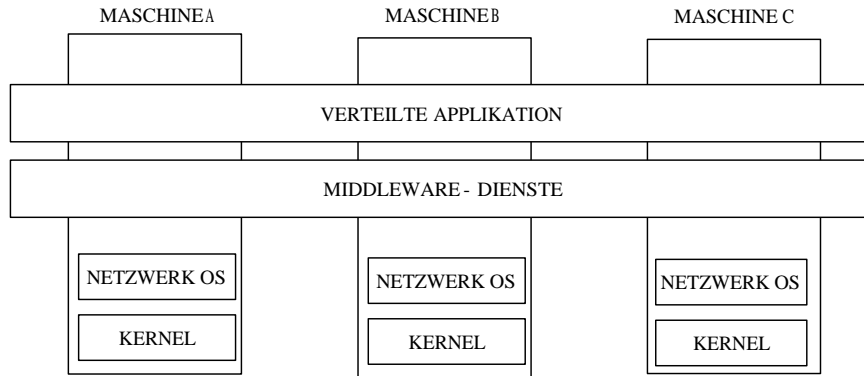


Abbildung 4: Middleware: Transparenz wird durch eine zusätzliche Abstraktionsschicht realisiert.

Freisprecheinrichtung im Auto ist zum Beispiel das *Hands Free Profil (HFP)* zuständig. Dieses verwendet einen Monokanal sowie einfache Befehle zum Steuern der Lautstärke, Gesprächsannahme usw. Fehlt einem Gerät ein bestimmtes Profil, so kann dieses den entsprechenden Dienst nicht nützen. Die Meisten Geräte können oft nur eine Profil gleichzeitig verwenden. Dann ist es nicht möglich ein Handy im Auto an ein Headset sowie gleichzeitig an einen GPS-Empfänger für das Navigationssystem anzuschließen.

Middleware Gerade für Pervasive Computing ist es notwendig, dass unterschiedliche Hardware, Betriebssysteme, Netzwerke und Protokolle in ein für alle Teilnehmer nutzbares System integriert werden können.

Dabei ist zu beachten, dass die Komplexität eines solchen verteilten Systems exponentiell mit der Anzahl der zu integrierenden Systeme steigt. Um diese Komplexität den Applikationsentwicklern zu verbergen, wurde eine zusätzliche Abstraktionsebene -die Middleware konstruiert. Siehe auch Abbildung 4.

Dieser zusätzliche Layer stellt Schnittstellen, Funktionen und Dienste zur interoperablen Kommunikation zur Verfügung. Dies ist eine wichtige Voraussetzung für die weiter unten beschriebenen Anwendungsfälle von Pervasive Computing.

Es gibt mehrere verschiedene Systeme wie zum Beispiel die Programmiersprachen unabhängige CORBA (Common Object Request Broker Architecture), das von SUN Microsystems auf JAVA basierende JINI (Jini Is Not Initials), JAVA RMI oder MICROSOFTS Universal Plug and Play (UPnP). Middleware kann unter anderem auch als Fundament (muss aber nicht) für die im nächsten Punkt beschriebenen *Web-Services* dienen.

Web Services Ermöglichen die Interaktion bzw. den elektronischen Handel zwischen mindestens zwei Computersystemen ohne menschliches Zutun. Zum Beispiel könnte ein Warenbestellsystem einer Firma, automatisch über einen Web-Service einer anderen Firma, Material nachbestellen wenn dieses einen gewissen Grenzwert unterschritten hat. Es ist auch möglich, dass automatisch unterschiedliche Angebote von verschiedenen Lieferanten eingeholt und gemäß den definierten Anforderungen ein neuer Lieferant den Zuschlag erhält. Viele weitere Web Services findet man nicht nur im E- Commerce sondern zusehend auch in der Unterhaltungsindustrie und somit bilden diese ein wichtiges Fundament für Pervasive Com-

puting.

Wichtige Standards sind die Web Service Description Language (*WSDL*) für die Beschreibung der entsprechenden Dienste sowie die Universal Description, Discovery and Integration (*UD-DI*) für das automatische finden bzw. auch für das Registrieren von Web-Services in einer Registry. Beide basieren auf dem plattformunabhängigen XML- Standard.

Genauere Informationen zu diesem Thema finden Sie auch auf der Homepage des *W3C* ².

2 NFC: Technologie

2.1 Einleitung

Near Field Communication ist eine neue drahtlose Funktechnologie für sehr kurze Entfernungen (bis zu maximal 20cm) und wird von den Firmen Sony, Philips und Nokia maßgeblich entwickelt und standardisiert. Zu diesem Zweck haben sie 2004 das *NFC-Forum* ³ gegründet, denen bis heute (Sept. 2006) fast 100 Mitglieder beigetreten sind. Dazu zählen Firmen wie Visa, Microsoft, Sony oder Siemens.

Da sich immer mehr elektronische Geräte hin zu Multifunktionsgeräten entwickeln und diese auch untereinander kommunizieren, ist es wichtig, dem Benutzer die Komplexität des Netzwerkaufbaus zu verbergen. Das ist mittels der NFC- Technologie möglich.

Die Idee ist, dass es auf intuitive Art und Weise möglich sein soll, durch simples „Berühren“ eine *Pear to Pear* Netzwerkverbindung zwischen zwei Geräten herzustellen. Das ermöglicht im Gegensatz zur Bluetooth oder RFID Technologie den einfachen bzw. automatischen Datenaustausch von smart Devices wie Handys, MP3-Player, Smart-Cards, TV oder Laptop.

Near Field Communication bietet daher viele neue Möglichkeiten für die Unterhaltungsindustrie sowie für unterschiedlichste Ticketing- Szenarien. Siehe auch Abbildung 5.

Das NFC Protokoll ist kompatibel mit den bereits existierenden und weltweit sehr verbreiteten Chipkartentechnologien *Mifare* und *Felica* von den Firmen Philips und Sony. Somit ist es möglich, die neue NFC-Technologie mit dieser bereits bestehenden Hardware zu kombinieren.

Mit dieser Technologie kann man der Idee des Pervasive Computing einen großen Schritt näher kommen. Die entsprechenden mobilen Netzwerke und Middlewarekonzepte vorausgesetzt, besteht die Möglichkeit unsere physikalische Umgebung als erweiterte GUI ⁴ wahrzunehmen. Man spricht in diesem Zusammenhang auch von *Smart Spaces* [25]. Durch das Anbringen von kleinen Funksendern (RFID/NFC- Sender bzw. *Tags*) auf physikalische Objekte ist es möglich dort Berechnungen auszuführen oder Informationen zu speichern. Diese *Smart Objects* können durch ein simples Berühren mit einem NFC-Gerät aktiviert werden.

Entwickelt wird der NFC- Mikrochip von der Firma *Philips Semiconductors Styria* im österreichischen Gratkorn. Die NFC- Technologie funkt im 13.56 MHz Frequenzband und ermöglicht je nach Entfernung eine Datenübertragungsrate von bis zu 424 kBit/s zwischen einem *Tag* ⁵ und *Initiator* ⁶. Geschwindigkeiten von 1 Mbit/s sollen bald Realität sein.

²World Wide Web Consortium: <http://www.w3.org/2002/ws/>

³<http://www.nfc-forum.org>

⁴Graphical User Interface.

⁵Sender bzw. Transponder.

⁶Auch Empfänger oder Reader.

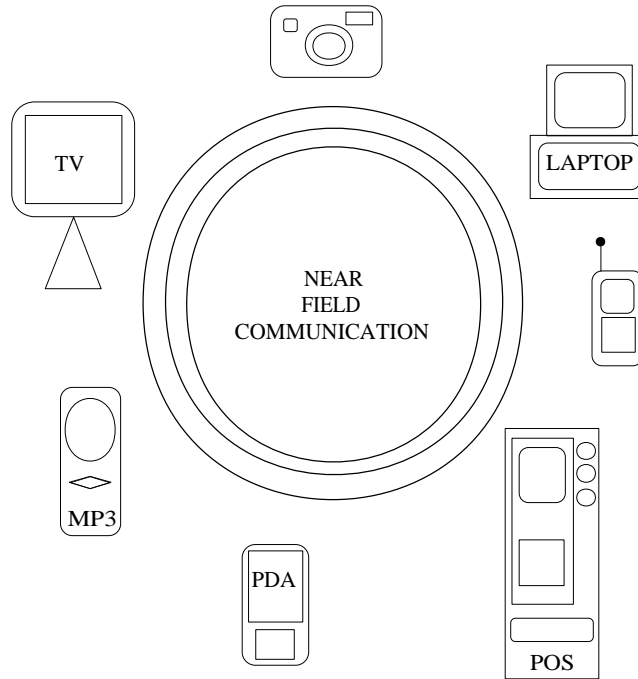


Abbildung 5: NFC: Durch einfaches Berühren wird eine Netzwerkverbindung hergestellt, z.B zwischen Handy und Point of Sale (POS).

Diese neue Technologie erweitert das RFID-Konzept um weitere wichtige Komponenten. So ist zum Beispiel kein „master/slave“ Betrieb vorgesehen. Sender sowie Empfänger können einfach ihre Rollen tauschen. Diese zusätzliche Flexibilität ermöglicht eine Vielzahl von neuen mobilen Anwendungen.

Eine weitere wichtige Funktion von NFC ist die automatische Wahl des optimalen Datenübertragungsprotokolls. Unterstützen beide Geräte zum Beispiel eine schnellere WLAN-Verbindung, so erfolgt die Konfiguration transparent mittels der „langsameren“ NFC-Verbindung. Anschließend werden die Daten mit der viel höheren WLAN-Bandbreite zwischen den Devices übertragen. Dabei ist es nicht notwendig, dass der Benutzer händisch eingreift.

Aufgrund der kurzen möglichen Entfernung von einigen Zentimetern zwischen den Geräten ist auch bei sicherheitskritischen Anwendungen weitgehend für die notwendige Security gesorgt. Ein Abhören oder Manipulieren der Nachricht kann bei diesen Distanzen beinahe ausgeschlossen werden. Zusätzliche Sicherheitsmaßnahmen müssen im Network Protocol Layer und höher implementiert sein. Ausführlicheres zu diesem Thema folgt im Kapitel 2.4 auf Seite 17.

Diese geringen Reichweiten haben auch den Vorteil, dass günstige Funksender verwendet werden können.

Unterschiede zur RFID- Technologie Bei der Near Field Communication handelt es sich um einen Spezialfall des RFID- Konzeptes, jedoch mit einigen wichtigen zusätzlichen Möglichkeiten. Dabei ist zu beachten, dass NFC kein Konkurrenzprodukt zu bestehenden RFID-Systemen ist, sondern dieses um folgende zusätzliche Möglichkeiten erweitert:

- **Betriebsmodi:** NFC- Geräte können sowohl als Sender (Tag) oder Reader (Initiator) betrieben werden. Diese zusätzliche Flexibilität ermöglicht weitere Interaktionsmöglichkeiten sowie zusätzliche Anwendungsszenarien.
- **Standards:** Near Field Communication berücksichtigt viele bereits existierende Standards ⁷ und ist mit diesen voll kompatibel. Daraus ergibt sich, dass bei nachträglicher Integration der NFC-Technologie, die bereits vorhandene Hardware weiter betrieben werden kann.
- **Kommunikationsprotokolle:** Ein weiteres wichtiges Feature von NFC ist, andere Datenübertragungsprotokolle zu beherrschen. Damit besteht die Möglichkeit zum Beispiel eine Bluetooth oder Wlan- Verbindung automatisch zu konfigurieren. Somit wird es für Anwender möglich sein, auf einfachste Art und Weise durch ein simples „Berühren“, schnellere Datenverbindungen transparent herzustellen. Das heute oft noch komplizierte, händische einrichten von Netzwerkverbindungen gehört somit der Vergangenheit an.
- **Security:** Durch die kurzen Datenübertragungsdistanzen von einigen Zentimetern kann eine Vielzahl von Sicherheitsproblemen beinahe ausgeschlossen werden. Zusätzliche Maßnahmen wie *Secure NFC*, können Sicherheitsstandards, wie sie etwa für Bankanwendungen gefordert sind, erfüllen. Weitere Informationen zur Security findet man im Kapitel 2.4 auf Seite 17.

Eine Schlüsseleigenschaft der NFC- Technologie ist sicherlich, eine Vielzahl von Komplexitäten vor den Benutzern zu verbergen. Durch das intuitive „*Touch Me*“- Paradigma ist es möglich, die „Human-Computer Interaction“ (*HCI*) radikal zu vereinfachen. Daraus ergeben sich zahlreiche Möglichkeiten bestehende Geschäftsmodelle zu verbessern bzw. gänzlich neue zu entwickeln.

Prinzipielle Einsatzgebiete von NFC finden Sie im Kapitel 2.6 auf Seite 21.

Es ist schwierig, Anwendungsszenarien der NFC- Technologie gegenüber RFID abzugrenzen. Je nach Situation wird entweder die eine oder die andere Technologie sinnvoller verwendet werden können. Aufgrund der oben aufgelisteten Vorzüge bietet sich NFC für Ticketing, Payment bzw. Anwendungen in der Unterhaltungsindustrie an. Die Domäne von RFID hingegen ist eher der Bereich der Optimierung von unternehmensweiten oder internen Prozessketten. In Tabelle 1 werden wichtige technischen Eigenschaften von NFC und RFID aufgelistet.

⁷Näheres zu diesen Standards finden Sie im Kapitel 2.3 auf der Seite 16.

	NFC	RFID
Frequenzen:	13,56 MHz	125 kHz bis 960 MHz sowie im GHz- Bereich bei Transponder mit eigener Energiequelle.
Reichweite:	bis zu 20 cm	je nach Frequenzbereich von einigen Zentimetern bis zu einigen hundert Metern.
Datenübertragungsrate:	derzeit 424 kbps	derzeit einige Hundert kbps
Security:	Hoch. Kombination mit Secure Card. ^a	Nieder bis moderat. Informationen werden meist in Klartext übertragen.
Betriebsmodi:	Sender und Empfänger können die Rollen tauschen, sowie: Aktiv- Aktiv Aktiv- Passiv ^b	Aktiv- Aktiv Aktiv- Passiv
weitere drahtlose Datenübertragungsprotokolle:	Ja z.B. Bluetooth oder WLAN	Nein
Hardwarekosten:	Aufgrund der kurzen Distanzen sehr preiswert.	Preiswert bis teuer.

Tabelle 1: Gegenüberstellung: NFC - RFID

^aWeitere Informationen zur Security gibt es im Kapitel 2.4 auf Seite 17.

^bSiehe auch im folgenden Kapitel 2.2.

2.2 Technische Funktionsweise

Die Datenübertragung erfolgt mittels eines magnetischen Feldes und basiert auf dem Prinzip der *induktiven Kopplung*. Im Gegensatz zu Hochfrequenztechnologien (RF⁸) wie zum Beispiel der Mobilfunk bietet dies Vorteile wie eine erhöhte Privacy durch die kurzen möglichen Reichweiten. Ein weiterer Vorteil ist, dass magnetische Felder abgeschirmt werden können. Somit kann eine störende Beeinflussung gegenüber anderen elektronischen Geräten vermieden werden.

Eine wichtiges Feature der magnetischen Kopplung ist die Möglichkeit des „passiven Betriebs“.

Passiver Betrieb

Eine für Pervasive Computing sehr wichtige Eigenschaft ist die Möglichkeit des *passiven Betriebs*. Dabei können Geräte, welche selbst keine eigene Energiequelle besitzen, trotzdem Daten senden. Die Funktionsweise erinnert an einen Transformator ⁹. Sowohl der *Initiator* als auch

⁸Radio Frequency

⁹Man spricht dabei auch von transformatorischer Kopplung.

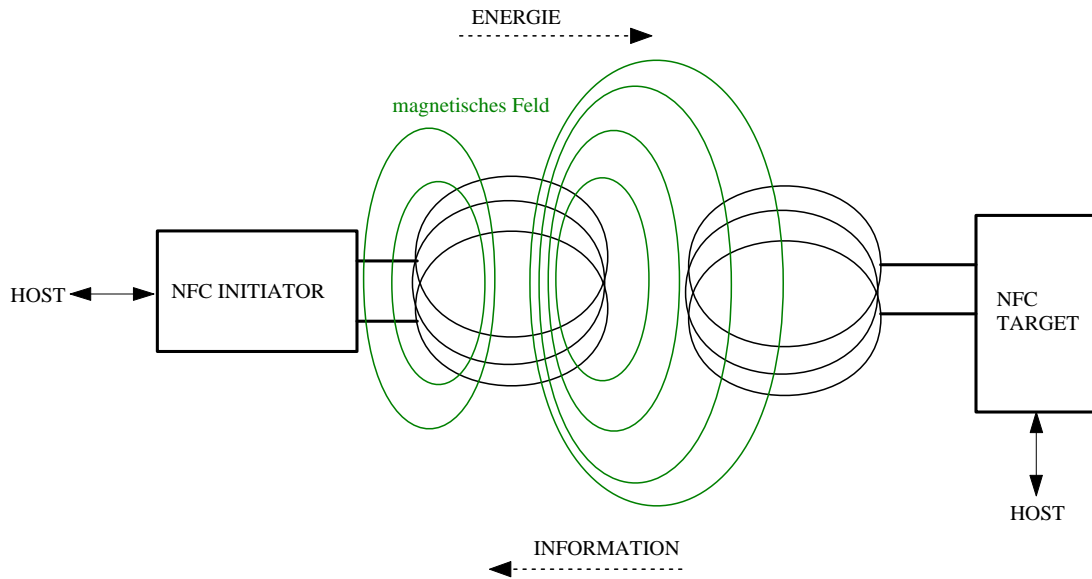


Abbildung 6: Beim passiven Betrieb ist es möglich, dass ein Sender Informationen an den Empfänger übermittelt, ohne eine eigene Energiequelle zu besitzen.

das *Tag* müssen mit einer Antenne (Spule¹⁰) ausgestattet sein. Dabei generiert der *Initiator* ein Magnetfeld. Kommt nun die Spule des *Tags* in die Nähe dieses Feldes, so wird dort eine Spannung induziert. Diese wird nun zur eigenen Energieversorgung des *Tags* verwendet. Der *Initiator* kann nun Informationen mittels Modulation an das *Tag* senden. Dort angekommen werden diese demoduliert und in elektronische Signale umgewandelt. Anschließend können diese Signale dekodiert und vom Gerät entsprechend interpretiert werden. Durch spezielle Schaltungsvorgänge im *Tag* ist es möglich, Informationen an den *Initiator* zu transportieren. Diese Form der Datenübertragung nennt man *Lastmodulation*. Siehe Abbildung 6.

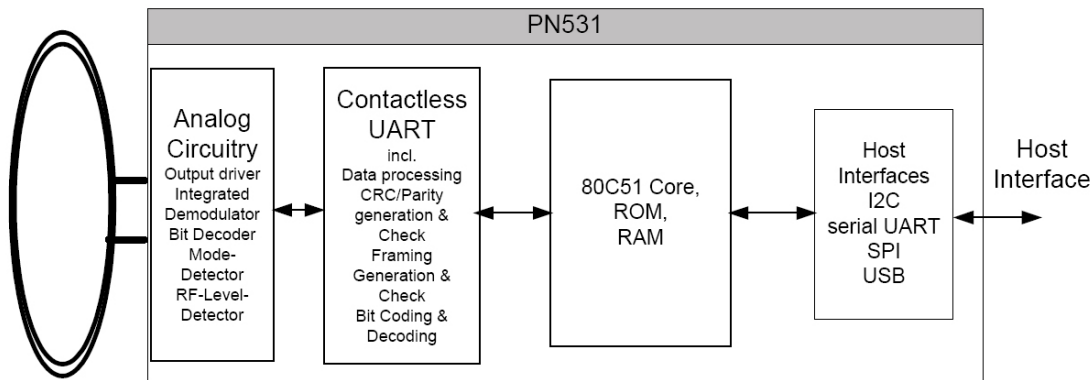
Von einem „aktiven Betrieb“ spricht man, wenn sowohl Initiator als auch Tag über eine eigene Energiequelle verfügen. Wie bereits weiter oben bemerkt, ermöglicht die NFC- Technologie beide Betriebsarten. Quelle: [6].

NFC Transmission Module

Um NFC- Funktionalität in einem elektronischem Gerät integrieren zu können, ist es notwendig, einen entsprechenden Mikrochip einzubauen. Momentan gibt es von Philips zwei Typen der sogenannten „NFC Transmission Module“. Einmal den *PN511* sowie den *PN531*. Diese hochintegrierten ICs sind mit den unterschiedlichsten Schnittstellen ausgestattet, um möglichst viele Standards und Protokolle unterstützen zu können. Der Kommunikationsfluss erfolgt von einem gerätespezifischen internen Mikroprozessor auf der einen Seite, zu den demodulierten Daten von der Antenne auf der anderen Seite bzw. *visa versa*.

Typische Geräte, in denen diese Mikrochips eingebaut werden können, sind Mobiltelefone, PDAs, Personal Computers, Drucker, Scanner sowie Geräte der Unterhaltungsindustrie wie

¹⁰Mit steigender Frequenz nimmt die benötigte Spuleninduktivität und damit die Anzahl der benötigten Windungen ab. Im 13,56 Mhz- Bereich sind 3 bis 10 Windungen typisch.



Source: Philips Semiconductors

Abbildung 7: Blockschaltbild des PN531 Prozessors.

zum Beispiel TV, Digitalkamera oder Videorecorder.

Diese beiden Mikrochips unterscheiden sich in ihrer Bauweise sowie in einigen Details der Spezifikation. Im folgenden werden kurz die wichtigsten Features des „PN531“ [14] vorgestellt:

- Basiert auf einem 80C51 ¹¹ Processor mit 32 Kbytes ROM und 1 Kbytes RAM.
- Die integrierte Firmware unterstützt sowohl den NFC-Standard (NFCIP-1 ¹²) als auch Mifare/FeliCa schreib-/lese Operationen. Auf der „Host-Seite“ stehen eine USB 2.0, serial UART ¹³ sowie SPI - und I2C ¹⁴ Schnittstellen zur Verfügung.
- Integrierte Gerätetreiber für den Anschluss einer Antenne.
- Automatische Erkennung des entsprechenden RF-Levels.
- Integrierte Erkennung des entsprechenden Kartenstandards.
- Flexibles Powermanagement mittels Softwaresteuerung.

In Abbildung 7 ist das Blockdiagramm des von Philips entwickelten NFC- Mikrochips mit der Bezeichnung *PN531* dargestellt:

Analog Circuitry Kümmt sich um die Modulation bzw. Demodulation der analogen Signale entsprechend des gerade eingesetzten Kartensystems.

RF level detector Erkennt die Gegenwart eines externen Magnetfelds im 13,56 MHz Bereich.

Mode Detector Je nach gerade eingesetztem Kartensystems (NFC, Mifare, Felica) wird die entsprechende Kodierung für die Demodulation der empfangenen Signale verwendet.

¹¹Geringer Energieverbrauch. Sehr Preiswert.

¹²NFC Interface and Protocol.

¹³Universal Asynchronous Receiver Transmitter,- ähnlich der bekannteren RS232- Schnittstelle.

¹⁴Sowohl bei Serial Peripheral Interface (SPI) als auch bei Inter-Integrated Circuit (I2C) handelt es sich um ein Bus-System zur seriellen Datenübertragung.

Contactless UART Dieses Modul kümmert sich um die Verwendung der entsprechenden Kommunikationsprotokolle. Ebenso um die Berechnung von Prüfsummen zur Erkennung von fehlerhaften Daten oder Signalen. Die Kodierung bzw. Dekodierung der Informationen wird ebenfalls an dieser Stelle durchgeführt.

80C51 Core Der Prozessorkern ist der zentrale Teil des Mikroprozessors. Dieser ermöglicht mit seiner integrierten Firmware ein autonomes Management der Kommunikation sowohl auf der digitalen „Host- Seite“, als auch auf der analogen „Antennen-Seite“.

Host Interfaces Zahlreiche integrierte Schnittstellen ermöglichen eine Vielzahl von Kommunikationsmöglichkeiten- je nach Anwendungsfall.

2.3 Standards

Wie bereits in der Einleitung bemerkt, ist der aktuelle NFC- Standard (NFCIP-2) zu folgenden Systemen bzw. Normen kompatibel:

- ISO ¹⁵ 18092 (NFC Standard NFCIP-1): Die erste Version des NFC-Standards. Siehe auch weiter unten im Text.
- ISO 14443A (Philips‘Mifare- Technologie): Wird auch als *Proximity Coupling* aufgrund der kurzen Übertragungsdistanzen von ca. 10 bis 15 cm bezeichnet. Datenübertragungsraten bis zu 424 kBit/s sind möglich.
- ISO 14443B (Die weltweit am Meisten verbreitete FeliCa- Technologie von Sony): Ebenfalls Proximity Coupling.
- ISO 15693: Entfernungen bis 1,5 m. Man spricht daher auch von *Vicinity Coupling*. Übertragungsraten bis zu 26,48 kBit/s sind realisierbar. Kann im Gegensatz zu den anderen Standards nicht genug Energie aufbringen um einen IC zu aktivieren. Typische Anwendungen sind daher nur jene mit einer eingebauten starren Logik.

Die einzelnen Standards unterscheiden sich in technischer Hinsicht unter anderem durch unterschiedliche Datenübertragungsprotokolle, mögliche Entfernungen, Schnittstellen oder Prüfsummen zur Erkennung von Fehlern in der Kommunikation.

Die Standardisierung der NFC- Technologie wird von der *ECMA International* ¹⁶ in Genf durchgeführt. Bis heute wurden von der ECMA International im wesentlichen fünf NFC Spezifikationen vorgelegt und von der ISO bzw. IEC ¹⁷ als Standards aufgenommen:

- **ECMA-340** (NFCIP-1) als **ISO/IEC 18092**: Im Dezember 2004 wurde die zweite Version dieser Spezifikation vorgelegt. Dieser NFC-Standard (NFCIP-1) beschreibt die möglichen Betriebsmodi, Schnittstellen sowie Protokolle für die Near Field Communication.
- **ECMA-356** als **ISO/IEC 22536**: Spezielle RF- Testmethoden für NFCIP-1 Geräte.
- **ECMA-362** als **ISO/IEC 23917**: Spezifiziert Protokoll- Testmethoden.

¹⁵International Organization for Standardization

¹⁶European Computer Manufacturers Association

¹⁷International Electrotechnical Commission

- **ECMA-352** (NFCIP-2) als **ISO/IEC 21481**: Diese Version wurde im Dezember 2003 eingereicht und im Jänner 2005 von der ISO/IEC als Standard aufgenommen. Zusätzlich zu den Möglichkeiten, welche NFCIP-1 bereits bietet, wurde dieser um die Möglichkeit der Integration der sehr verbreiteten Chipkartentechnologien (Mifare und Felica) erweitert.
- **ECMA-373** [NFC-WI): Dieser definiert eine Schnittstelle zwischen einem Front-End ¹⁸ und dem Transceiver und wurde am 01. Juli 2006 fertig spezifiziert. Noch kein ISO/IEC Standard.

Die einzelnen Spezifikationen können auf der Homepage der ECMA-International ¹⁹ bzw. die Standards auf der Seite der ISO ²⁰ heruntergeladen werden.

2.4 Security

Eine wichtige Voraussetzung für den zukünftigen Erfolg von NFC- Anwendungen ist, dass diese Technologie hinreichend sicher ist und die Konsumenten den Systemen vertrauen können. Grundsätzlich sollte von Fall zu Fall genau überlegt werden, ob bzw. welche Sicherheitsmaßnahmen gesetzt werden müssen. So wird es einen Unterschied machen, ob ich lediglich ein Photo auf den privaten Fernseher übertrage, oder aber mein NFC- Handy als Kreditkarte verwende.

Oft kann man lesen, dass die NFC- Technologie aufgrund der kurzen Distanzen per se als sicher zu betrachten ist. Diese Annahme kommt daher, dass man es sich schwierig vorstellt, dass jemand eine Kommunikation, welche sich nur über Distanzen von wenigen Zentimetern abspielt, abhören oder manipulieren kann. In vielen Fällen wird dies auch der Fall sein. Aufgrund weiterer technischer Maßnahmen wie Verschlüsselungsalgorithmen oder Authentifizierungsmechanismen, kann ein zusätzlicher Grad an Security erreicht werden. Näheres dazu im nächsten Abschnitt.

Trotzdem wurde gezeigt [19], dass ein „passives Abhören“ ²¹ der drahtlosen RF- Kommunikation auch in größeren Entfernungen als die üblichen 10 -15 cm, mit einfachsten Labormittel (Antenne, Oszilloskop, Testsoftware) problemlos möglich ist. Das Prinzip ist einfach: Die in den Normen genannten Feldstärken der Magnetfelder ermöglichen ein Mithören der Kommunikation bis zu einer Entfernung von drei Metern. Diese Distanz kann möglicherweise durch die Verwendung von abgestimmte Antennen, Vorverstärkern noch deutlich gesteigert werden.

Weitere Angriffsszenarien basierend auf einer *Relay Attack* ²² haben *Ziv Kfir* und *Avishai Wool* in Ihrer Arbeit [24] gezeigt. Im wesentlichen werden dazu zwei speziell modifizierte NFC- Geräte benötigt. Einmal ein sogenannter *Ghost*, der einem Kartenleser (Initiator) einen vermeintlich echten Tag vorspielt und einmal ein sogenannter *Leech*, welcher einem Tag den

¹⁸Auf diesem befindet sich auch die Antenne für die drahtlose Kommunikation mit einem anderem Gerät.

¹⁹<http://www.ecma-international.org/>

²⁰<http://www.iso.org/>

²¹Wird auch als *Eavesdropping* bezeichnet. Dabei geht es darum, dass eine Kommunikation belauscht- jedoch nicht verändert werden kann.

²²Im Gegensatz zu einer *Man in the Middle* Attacke muss dabei der abgehörte Inhalt nicht verstanden, sondern „nur“ entsprechend weitergeleitet werden.

„echten“ Kartenleser vorgaukelt. Somit ist es zum Beispiel bei einem Zahlvorgang theoretisch möglich, dass jemand mit dem speziell adaptierten NFC Handy die Rechnung bezahlt, diese jedoch von einem anderen, fremden NFC-Handy abgebucht wird. Dieser „Trick“ funktioniert selbst bei implementierten Verschlüsselungsalgorithmen. Wird jedoch (wie bei Debit- oder Ticketingsystemen üblich sein sollte!) zur Authentifizierung zusätzlich ein persönliches Wissen (zum Beispiel PIN-Code) verlangt, versagt dieser Angriff.

Secure- NFC

Viele mobile Geschäftsanwendungen und Applikationen erfordern das verschlüsselte Speichern von sensiblen Daten in einem geschützten Adressbereich. Dabei kann es sich um Zugangscodes für Bankanwendungen, Kreditkarten, Tickets oder um kryptographische Schlüssel zum Chiffrieren von Informationen handeln.

Im Handy könnte die bereits implementierte „Subscriber Identity Module (SIM) Karte“ verwendet werden. Möglich sind jedoch auch zusätzliche *Secure IC's*²³, wie zum Beispiel die plattformunabhängige *Java Card*²⁴. Gemeinsam ist diesen Chips, dass diese über einen eigenen Mikroprozessor verfügen. Dieser ermöglicht nur einen Zugriff auf die Daten mittels kryptographische Verfahren. Dabei kommen entweder *asymetrische* oder *symetrische* Schlüsselkonzepte zur Anwendung. Die Wahl nach dem geeigneten Verfahren hängt von der Art der Anwendung ab. Aufgrund des Schlüsselverteilproblems wird für grosse Anwendungen wie zum Beispiel Kreditkartenfunktionalität ein asymmetrisches Schlüsselkonzept gewählt werden. Grundlegende Informationen zur Kryptographie können Sie zum Beispiel hier [3] finden.

Die Kommunikation zwischen dem NFC Transmission Module mit der angeschlossenen Antenne sowie dem Secure IC bzw. der SIM- Karte erfolgt über dem sogenannten „Synchronous Serial Channel (S2C) Interface“. Siehe auch Abbildung 8. Diese synchrone Schnittstelle ermöglicht eine rasche Kommunikation zwischen den einzelnen Modulen und ist daher auch eine wichtige Voraussetzung für die Kundenakzeptanz bei Bezahl- oder Ticketinganwendungen. Weiters ist dieses Interface kompatibel zu bereits existierenden drahtlosen Standards und wurde ebenfalls bereits bei der ECMA-International zur Standardisierung eingereicht. Quellen: [15] [7].

2.5 NFC Software Applikationen

Einleitung

Wie bereits mehrmals festgestellt, kann die Near Field Communication einen wichtigen Beitrag für das *Internet der Dinge* liefern. Durch das intuitive *Touch Me*- Paradigma und die Einbeziehung von physikalischen Objekten in die digitale Welt ergeben sich neue Herausforderungen und Anforderungen an das Softwaredesign [25] [8]. Dies umfasst sowohl die Konzeption von dynamischen Netzwerken oder Middleware, als auch das Design der Mensch- Maschinen Schnittstelle. Einige dieser „neuen“ Kriterien werden kurz aufgelistet:

Automatische Setup Prozeduren: Viele NFC-Geräte können mit einer noch höheren Anzahl von RFID- Tags oder ähnlichen Systemen wie zum Beispiel Transponderkarten kommunizieren. Es wird daher immer wichtiger, dass sich diese smarten Geräte selbst konfigu-

²³ Auch als *Secure Digital Memory Cards* bekannt. Siehe Kapitel 1.2.2

²⁴ Weitere Informationen zur weit verbreiteten Java- Card Architektur kann der interessierte Leser hier finden [22].

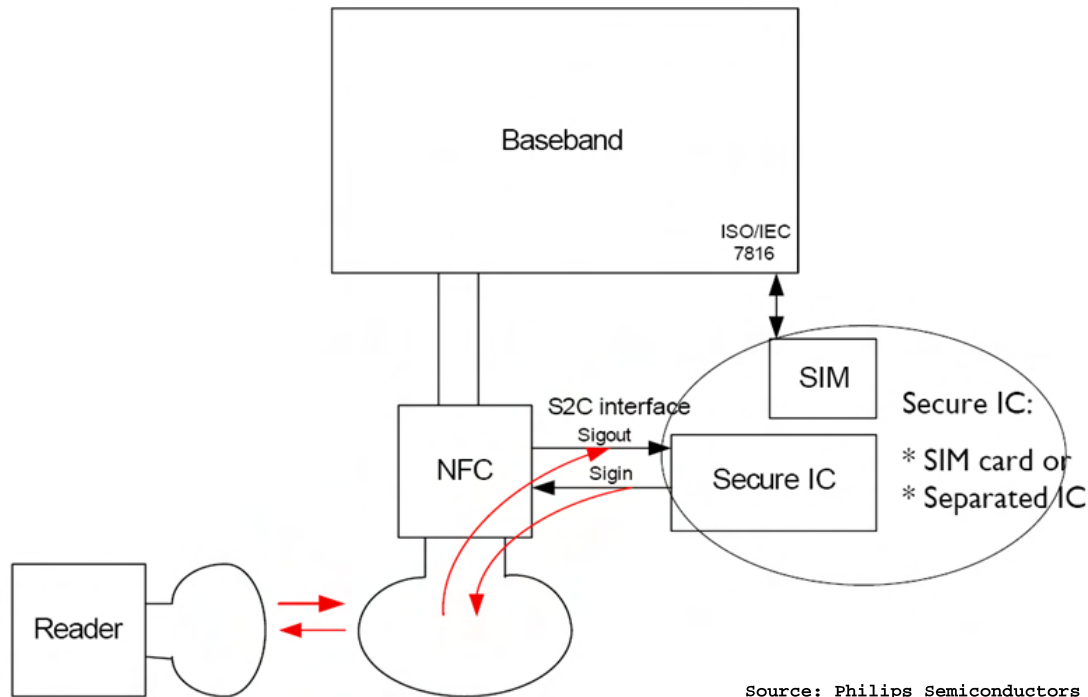


Abbildung 8: Secure NFC ermöglicht das sichere Abspeichern von sensiblen Daten auf einem separaten Sicherheitschip.

rieren, in Netzwerken automatisch an bzw. abmelden sowie ihre „Absichten oder Bedeutungen“ anderen Teilnehmern bekanntgeben. Heutzutage werden für diese Tätigkeiten oft erfahrene Netzwerkadministratoren benötigt. Für das Gelingen von NFC- Lösungen wird auch entscheidend sein, diese unterschiedlichen Komplexitäten (Netzwerke, Hardware, Kommunikation etc.) sowohl vor dem Softwareentwickler als natürlich auch vor dem Kunden zu verbergen.

Gemeinsame API's²⁵: Gerade bei interdisziplinären Anwendungen wie sie die NFC- Technologie ermöglicht, ist es wichtig über eine standardisierte Entwicklungsplattform zu verfügen, damit auch Dritte einfach eingebunden werden können.

Plug and Play: Die Entwicklungszyklen von neuer Software und Hardware werden immer schneller. Daher ist es wichtig, dass es für den Kunden einfach möglich ist, auf die neuesten Versionen zu wechseln.

Derzeit gibt es noch kaum „breite“ Plattformen, um Dienste und Services für die NFC- Technologie einem großem Anwenderpublikum zugänglich zu machen. Das liegt zum einen daran, dass diese Technologie noch sehr jung ist, aber auch weil es bereits historisch gewachsene (aber nicht optimale) Lösungen gibt. Nicht zu vergessen sind natürlich auch mögliche Interessenskonflikte zwischen den beteiligten Firmen und Organisationen.

²⁵ Application Programming Interface. Wird bei der Softwareentwicklung benötigt.

Im folgenden wird ein Softwarekonzept für die NFC bzw. RFID Technologie exemplarisch vorgestellt.

Die NFC- Technologie vereint sowohl eine kontaktlose Smartcard, ein kontaktloses Lesegerät sowie eine drahtlose P2P Funktionalität in einem einzigen Modul. Wird dieses in einem Handy eingebaut, besteht zusätzlich die Möglichkeit zur drahtlosen Interaktion mit einem Server und ermöglicht viele neue Geschäftsmöglichkeiten wie zum Beispiel Reportingsysteme (siehe auch Abschnitt 3.1) oder Ticketing (Abschnitt 3.2) Anwendungen.

Die Firma NOKIA bietet eine Software-Lösung an, die es Firmen erlauben soll, ihre RFID/NFC Reporting bzw. Realtime- Anwendungen einfach selbst zu spezifizieren und in ihre bestehende Firmen-Software zu integrieren. Diese *Nokia Field Force Solution* ²⁶ besteht aus dem *Local Interaction (LI) Client* sowie aus dem *LI-Server*

Local Interaction Client / Server

Damit ist es möglich, lokale Informationen, welche auf einem RFID- Tag vor Ort gespeichert sind, über eine verschlüsselte GPRS oder SMS Verbindung, in die Firma zu übertragen. Genauso können auch Informationen in die andere Richtung von der Zentrale an die Peripherie gesendet werden.

Voraussetzung dafür ist ein spezielles RFID/NFC- Handy, auf dem die J2EE ²⁷ *LI-Client* Software installiert ist.

Mit dem LI-Server ist es einfach möglich, verschiedene Dienste gemäß den speziellen Firmenanforderungen zu definieren. Wird nun das Handy zu einem *Tag* gehalten verbindet sich dieses mit dem LI-Server und die auf XML basierenden Daten werden automatisch an das entsprechende Service weitergeleitet.

Das ermöglicht eine Optimierung und Vereinfachung von Geschäftsprozessen und bietet sich speziell für Problemstellungen von Service-, Wartungs-, Sicherheits- oder Instandhaltungsfirmen bzw. Organisationen an.

Over The Air Plattform

Im 4. Quartal 2006 soll das neu gegründete Joint Venture zwischen Nokia und dem weltweit zweitgrößten Produzenten von Smart Cards, *Giesecke & Devrient (G&D)*, seine operative Tätigkeit aufnehmen. Ziel ist die Entwicklung und das Betreiben einer für alle Mitspieler offenen und sicheren Over The Air (*OTA*) Plattform, die flexible Applikationsmanagementlösungen für NFC- fähige Geräte bereitstellt.

Diese Plattform soll ermöglichen, dass Kreditkartenunternehmen, Banken, Transportunternehmen, Einzelhändler, Content- Anbieter sowie Netzprovider ihre Services den Endkunden, welche mobile NFC- Geräte verwenden, sicher und einfach anbieten können. Siehe auch Abbildung 9.

Es soll also möglich sein, dass sich ein Kunde mit einem NFC- tauglichen Handy oder PDA eine gewünschte Funktionalität wie zum Beispiel eine Kreditkarte, einfach und sicher auf sein mobiles Gerät lädt. Diese Applikation wird dann auf einem separaten Security-Chip (Näheres dazu auch im Kapitel 2.4 auf Seite 18.) am mobilen Gerät verschlüsselt gespeichert. Somit hat

²⁶Weitere Informationen unter: www.nokia.com/fieldforce

²⁷*Java 2 Platform Enterprise Edition*. Homepage: <http://java.sun.com/javaee/>

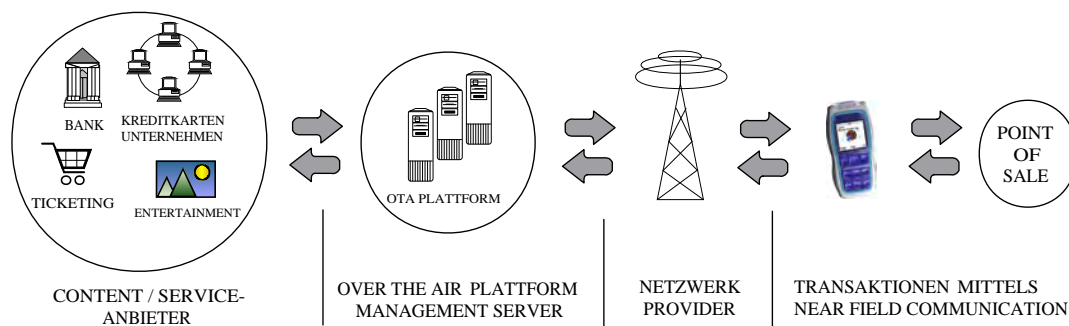


Abbildung 9: OTA Plattform Server: Ermöglicht die Integration von z.B. Debit oder Ticketing Anwendungen von Drittherstellern mit mobilen Geräten basierend auf der NFC-Technologie.

der User die Möglichkeit sein NFC- Handy auch als „ganz normale“ Kreditkarte zu verwenden. Zusätzlich zur „normalen Kreditkarte“ besteht mit einem elektronischen Gerät noch die Möglichkeit der Interaktion und des visuellen Anzeigens der Transaktionen. Auch ganz andere Services wie Online- Ticketing, Event- Management, Zugangskontrollsysteme und viele mehr können mit dieser Plattform dem Kunden transparent angeboten werden. Durch diese neue OTA- Plattform ergeben sich viele Vorteile für alle an diesem System beteiligten Organisationen:

- Der Endkunde kann neue Dienste auf einfache und intuitive Weise nutzen.
- Die Service bzw. Content- Anbieter können Ihre Produkte auf einem neuen Vertriebskanal präsentieren und unkompliziert verteilen.
- Für den Handyproduzenten ergibt sich durch die Implementierung der OTA Plattform bei stetig fallenden Handypreisen eine neue Einnahmequellen mit höheren Deckungsbeiträgen.
- Die Netzbetreiber können neue Dienste anbieten, das Datentransfervolumen steigern sowie die Kundenbindung erhöhen.

2.6 Mögliche Einsatzgebiete der NFC- Technologie

NFC taugliche Geräte können als kontaktlose Smartcard, als lese/schreib -Terminal für Smartcards oder zum direkten Datentransfer zwischen zwei Geräten eingesetzt werden. Daraus ergeben sich grundsätzlich vier unterschiedliche Anwendungsmöglichkeiten. Beispiele zu diesen Kategorien können Sie im Kapitel 3 finden.

1. **Touch and Go:** In diese Kategorie fallen sämtliche Anwendungen wie zum Beispiel Zutrittskontrollsysteme, Reportingsysteme in der Logistik oder Sicherheitstechnik oder zum Beispiel Event- Ticketing. Also all jene Anwendungen, wo der Benutzer einen Zutrittscode oder ein Ticket in seinem NFC- Gerät gespeichert hat. Dieses muss er lediglich in die Nähe eines Terminals halten und die Zutrittsdaten werden von diesem gelesen.

Umgekehrt ist es ebenfalls möglich sich Informationen auf das NFC- Gerät zu laden. Zum Beispiel eine URL bei Berührung eines entsprechenden Tags auf einem Gegenstand wie zum Beispiel einer Plakatwand.

2. ***Touch and Confirm:*** Anwendungen, bei denen eine Userinteraktion notwendig ist. Zum Beispiel das Bestätigen einer Transaktion. Beispiele dazu wären die Eingabe eines Passwortes bei der Bezahlung mit einem NFC- Device. Entsprechende Sicherheitsmechanismen müssen dabei bei dieser Art von Anwendungen berücksichtigt werden.
3. ***Touch and Connect:*** Ist zwischen zwei Geräten möglich. Es wird automatisch die schnellst mögliche P2P- Verbindung transparent konfiguriert. Zum Beispiel zum Austausch von Musik zwischen zwei NFC- Handys oder zur Synchronisation von Adressbüchern oder Terminkalendern.
4. ***Touch and Explore:*** Es sind auch weitere Kombinationen aus obigen Beispielen möglich. Der Kunde hat die Möglichkeit mit seinem NFC- Handy neue Anwendungen intuitiv zu „Entdecken und zu Erforschen“.

2.7 Marktchancen

„During 2006, more NFC trials and data analysis will occur. It will be a critical year for NFC with data determining whether the technology has legs. Negative results of pilot programs could hurt the technology's adoption.“
Alan Goode, Senior Analyst von Juniper Research [13]

Wie man aus obigem Zitat entnehmen kann, ist eine Einschätzung über die zukünftige Verbreitung der NFC- Technologie zum gegenwärtigen Zeitpunkt noch schwierig und mit Unsicherheiten behaftet.

Die im nächsten Kapitel vorgestellten Pilotprojekte, wurden so weit bereits Ergebnisse vorliegen, als sehr positiv beurteilt.

Es zeichnet sich deutlich ab, dass sich das Handy als *das* persönliche NFC- Gerät etablieren wird. Am Ende des Jahres 2005 waren laut Nokia bereits 2 Milliarden Mobiltelefone weltweit im Umlauf. Das entspricht einer globalen Penetration von 28 Prozent. Die jährlichen Wachstumsraten liegen dabei über 20 Prozent. Experten von Philips schätzen, dass bis zum Jahre 2010 die Hälfte aller Mobiltelefone, NFC tauglich sein wird. Betrachtet man dazu die zur NFC- Technologie kompatiblen, kontaktlosen Kartensysteme mit einer weltweiten Anzahl von über 540 Millionen Stück Smart Cards [7], so lässt sich das Potential dieser neuen Technologie bereits erahnen.

Um den zukünftigen NFC- Markt analysieren zu können, ist es notwendig, die wichtigsten ausschlaggebenden Faktoren zu untersuchen [20].

Die Macht der Konsumenten Der Erfolg einer neuen Technologie bzw. eines neuen Services hängt von der Anzahl der beteiligten User und der Anzahl der durchgeführten Transaktionen ab. Dabei ist es wichtig, ob die Bedürfnisse der Kunden erfüllt werden können.

Wie bereits oben bemerkt, könnte die NFC- Technologie aufgrund der hohen weltweiten Anzahl von Mobiltelefonen und Kartensystemen eine große Verbreitung finden. Auch

spricht das intuitive „Touch and Go- Prinzip“ dafür, dass es für die Kunden eine deutliche Erleichterung bei der Bedienung von unterschiedlichen Anwendungen bringt.

Die Macht der Händler Diese ²⁸ spielen eine sehr wichtige Rolle bei der Entwicklung neuer Services. Es ist wichtig, dass alle involvierten Organisationen an der Entwicklung aktiv beteiligt sind um eine möglichst hohe Akzeptanz zu erreichen. Dabei ist zu beobachten, dass es durchaus zu Interessenskonflikten bezüglich der verwendeten Infrastruktur (z.B. welches Netzwerk kommt zum Einsatz?) oder Standards kommt. Aus diesem Grunde wurde im April 2004 von Nokia, Philips und Sony das *NFC- Forum* gegründet, um eine möglichst breite Akzeptanz unter allen Mitspielern herzustellen. Trotzdem gibt es wichtige Hardwareproduzenten, die diesem Forum derzeit noch nicht beigetreten sind [13].

Traditionelle, bestehende Systeme Derzeit sind noch die „konventionellen“ Zahlungsmethoden wie Bargeld, Checks oder Kreditkarten die am häufigsten angetroffen werden. So wird in Europa ²⁹ noch am liebsten in Cash bezahlt,- in den USA werden Kreditkarten bevorzugt. Eine Vorreiterrolle spielt dabei Japan, das neuen Technologien grundsätzlich offener gegenübersteht.

Es ist oft schwierig, gegen traditionelle Systeme anzukämpfen. Es reicht nicht aus, bestehende Möglichkeiten einfach in einen neuem Kanal zu transformieren. Für den Kunden muss sich ein echter „Mehrwert“ ergeben. Untersuchungen haben auch gezeigt, dass zum Beispiel in der Schweiz „Plastikkarten“ gegenüber einem Mobiltelefon für Debit- oder Ticketing Anwendungen bevorzugt werden [20].

Es kann derzeit noch schwer abgeschätzt werden, ob sich die NFC- Technologie gegenüber etablierten Systemen durchsetzen wird. Aufgrund der erweiterten technischen Möglichkeiten, wie zum Beispiel die automatische Konfiguration von unterschiedlichen Netzwerkverbindungen (Bluetooth, Wlan), hat sie aber auf jeden Fall eine sehr gute Ausgangsposition.

Das neue Service Es hat sich gezeigt, dass in der Vergangenheit „neue“ Bezahlmethoden eingeführt wurden, die auf historischen Paradigmen aufgebaut haben. So wird zur Bezahlung von sehr kleinen Beträgen (*micropayments*) im Internet weniger häufig eine Kreditkarte als alternative Systeme wie zum Beispiel PayPal, Paystone oder Peppercoin verwendet, da diese die Anforderungen der Benutzer besser unterstützen.

Aus diesem Blickwinkel hat die NFC- Technologie sicherlich gute Karten, da sie sowohl bestehende Systeme, als auch neue Erweiterungen integriert und in einem einzigen Gerät bündeln kann.

Rivalitäten der Mitspieler Nicht immer setzt sich der beste Standard durch. Oft ist es jener mit der größten Marktmacht. Gerade bei der Entwicklung von neuen Technologien fehlen noch derartige Standards und viele Mitbewerber versuchen ihre eigenen, profitabelsten Lösungen am Markt zu etablieren.

Bei der NFC- Hardware sind diese Spezifikationen zum Großteil bereits abgeschlossen.

²⁸Unter Händler werden alle am System beteiligten Organisationen wie Banken, Netzwerkbetreiber, Kreditkartenunternehmen usw. zusammengefasst.

²⁹Mit Ausnahme der Skandinavischen Länder.

Durch die Gründung des NFC- Forum geht man eine einen sehr offenen und transparenten Weg, damit derartige Probleme verhindert werden können.

Bei der Entwicklung von NFC-Softwareapplikationen besteht bereits eine Vielzahl von Insel-Lösungen. Kreditkartenunternehmen möchten ihre eigenen, bestehenden und kostengünstigen IP- Netzwerke für die jeweilige Debit- Applikationen verwenden. Netzbetreiber haben natürlich ein großes Interesse ihre eigenen Netzwerke mit zusätzlichen Diensten für die Kunden attraktiv zu gestalten.

Für die Zukunft der NFC- Technologie ist es sicherlich von Bedeutung, dass diese Interessenskonflikte im Sinne der Kunden rasch gelöst werden. Die Firma Nokia entwickelt bereits eine Plattform³⁰, bei der alle beteiligten Mitspieler integriert werden können.

Zusammenfassend lässt sich sagen, dass die NFC- Technologie sicherlich ein sehr hohes Marktpotential hat. Aber ob dieses so bedeutend ist, wie uns manche Marketingabteilungen aus der Industrie versprechen, darf bezweifelt werden.

3 NFC Anwendungsbeispiele und Pilotprojekte

Wie bereits im Kapitel 2.6 auf Seite 21 erläutert, gibt es vier grundsätzliche Möglichkeiten die NFC- Technologie einzusetzen. Im folgenden Text werden praktische Anwendungsbeispiele sowie Pilotprojekte zu diesen Punkten vorgestellt. Gemeinsam ist ihnen, dass dem allgegenwärtigen Mobiltelefon eine zentrale Bedeutung zukommt.

3.1 Echtzeit- Reportingsysteme

In der Transport und Logistik Branche gehören Trackingsysteme basierend auf RFID- Chips schon fast zum Alltag. Eine weitere interessante Entwicklung ergibt sich jedoch auch dadurch, dass immer mehr Handys mit RFID/NFC Reader ausgerüstet sind. In Abschnitt 2.5 wurde bereits kurz eine speziell für Echtzeitsysteme entwickelte Client/Server Applikation dargestellt. Es werden nun zwei Beispiele vorgestellt, bei denen Daten in Echtzeit vom Feld in die Applikation mittels mobiler Technologie gespielt werden. Diese Anwendungsfälle können der Kategorie *Touch and Go* zugeteilt werden.

3.1.1 Anwendungsbeispiel: Strom/Gas Zähler ablesen

Mindestens einmal im Jahr schickt das lokale Energieversorgungsunternehmen (EVU) seine Mitarbeiter aus um den Zählerstand von Strom und Gas ihrer Kunden zu erfassen. Meist werden die Daten noch händisch aufgeschrieben und bei Gelegenheit vom Außendienstmitarbeiter entweder persönlich in die Firmenzentrale gebracht oder aber zum Beispiel via Fax oder Email übermittelt. Dort angelangt werden diese dann durch einen anderen Mitarbeiter in das entsprechende Computersystem (ERP³¹) eingegeben. Man kann sich gut vorstellen, dass es aufgrund der großen Anzahl von Haushalten durchaus zu Verwechslungen der Daten oder zu Zahlenstürzen kommen kann. Dies kann zu Inkonsistenzen in der Datenbank führen und verursacht hohe Folgekosten in der Fehlerbehebung.

³⁰Over The Air Plattform. Diese System wurde bereits im Kapitel 2.5 auf Seite 20 vorgestellt.

³¹Enterprise-Resource-Planning

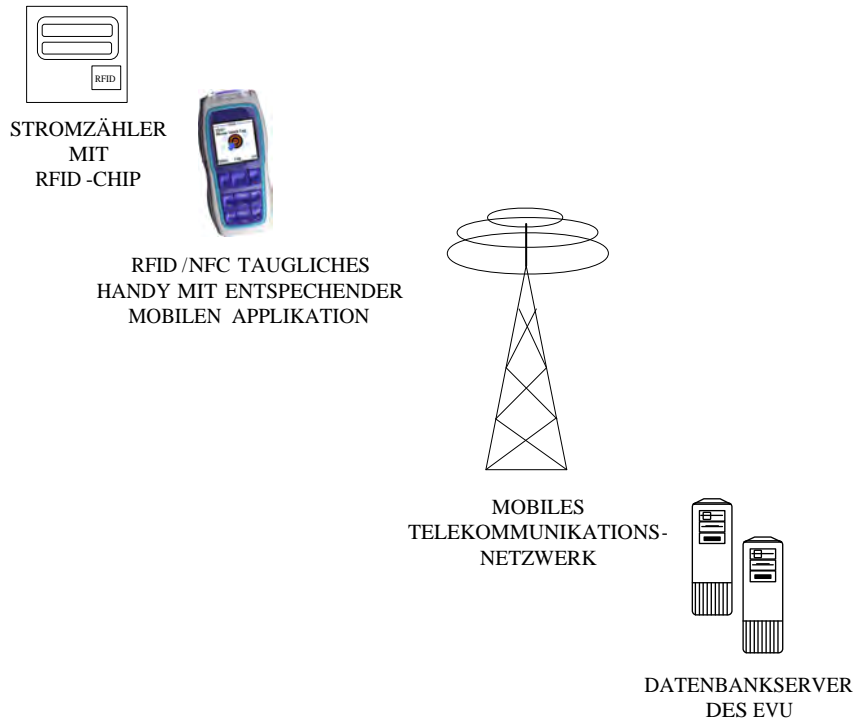


Abbildung 10: Optimierung von Geschäftsprozessen mittels RFID/NFC Technologie.

Eine elegantere Lösung ist, den Prozess von der Datenerfassung beim Kunden bis zum Einspielen in die Datenbank zu automatisieren. Dazu ist es notwendig, dass jeder Zähler mit einem RFID-Tag ausgestattet wird. Auf diesem Chip befindet sich die Seriennummer des Zählers. Je nach Konfiguration des Zählers könnte auch der aktuelle Zählerstand elektronisch am RFID-Tag abgespeichert sein.

Will nun der EVU-Mitarbeiter den Zählerstand ablesen, muss er lediglich sein Handy mit eingebautem RFID-Reader bzw. NFC-Chip zum Zähler halten. Die Daten werden vom RFID-Tag auf das Handy übertragen und von diesem mit der entsprechenden zugehörigen mobilen Applikation (z.B. LI Client/Server) automatisch in den Datenbankserver des Energieversorgungsunternehmens gespielt. Siehe Abbildung 10.

Die Vorteile liegen auf der Hand: Effizientere Bearbeitung, leicht Bedienung, Fehlerminimierung, erhöhte Kundenzufriedenheit, keine Extrakosten mehr.

3.1.2 Anwendungsbeispiel: Nachtwächter

Eine der momentan am schnellst wachsenden Branchen sind die privaten Sicherheitsunternehmen mit über 10 Prozent jährlichem Wirtschaftswachstum. Deren Hauptaufgabe ist der Objektschutz. Gerade in diesem sensiblen Bereich ist es notwendig über verlässliche und aktuelle Daten zu verfügen.

Dank RFID bzw. NFC ist es möglich, zu jedem beliebigen Zeitpunkt einen aktuellen Situationsbericht abzufragen. Siehe Tabelle 2.

Das Prinzip ist einfach: In den zu schützenden Objekten werden an ausgewählten Stellen RFID-

DATUM	ZEIT	OBJEKT ID	NAME	BES.VORK.
31.12.2005	23:58	Bawag	Huber	keine
01.01.2006	00:30	Stefansplatz	Huber	keine
01.01.2006	01:14	Stadtspark	Huber	keine
...

Tabelle 2: So könnte ein Tabelleneintrag in einer Echtzeit-Datenbank eines Sicherheitsunternehmens aussehen.

Tags montiert. Diese können auch direkt im Objekt eingebaut sein und sind daher nach außen hin unsichtbar. Das Sicherheitspersonal muss sich zu definierten Zeitpunkten mit einem RFID- Reader (zum Beispiel RFID/NFC Handy) diesen *Tags* nähern. Sind die Stammdaten des Objekts auf das Gerät übertragen so wird sofort eine gesicherte Onlineverbindung zur Datenbank hergestellt. Somit ist es möglich bei Nichteinhalten des Zeitplans einen vollautomatischen Alarm abzusetzen. Für die Rekonstruktion von Überfällen können diese Daten ebenfalls von großem Wert sein.

Ein wichtiger Punkt in diesem Zusammenhang ist der Datenschutz. Es sind daher entsprechende rechtliche Vereinbarungen zwischen dem Sicherheitspersonal und der Geschäftsführung zu treffen (gläserner Mensch).

3.2 Ticketing

Wie bereits in Abschnitt 1.1 auf Seite 3 beschrieben, spielen mobile Geschäftsmodelle eine wichtige Rolle für die Idee des Pervasive Computing. Dabei zeigt sich, dass das Handy als ständiger Wegbegleiter des Menschen auch hier einen zentralen Platz einnehmen wird.

Wichtige Voraussetzungen für die Akzeptanz von mobilen E- Commerce Applikationen sind:

- ein praktischer Mehrwert
- einfache Bedienbarkeit
- ein sicheres Bezahlungssystem

Dabei kann die NFC- Technologie kombiniert mit einem mobilen Gerät, wie zum Beispiel Handy oder PDA, eine entscheidende Rolle zum Erreichen dieser Vorgaben spielen.

Im Abschnitt 2.5 auf Seite 18 wurden bereits technische Lösungsansätze für den mobilen Handel aufgezeigt.

Im folgenden soll ein konkretes Ticketingprojekt im öffentlichem Nahverkehr vorgestellt werden. Weitere NFC- Ticketing- Anwendungen wären zum Beispiel die Parkraumbewirtschaftung, Veranstaltungs- und Event- Management, Zutritt und Abrechnungssysteme für Skilifte oder Stadien.

Diese Art der Anwendungen fallen in die Kategorie *Touch and Confirm*.

3.2.1 Pilotprojekt der Stadt Haunau: Das Handy als Fahrkartenautomat

Einleitung Im Rhein Main Verkehrsverbund (*RMV*) ist es bereits seit Februar 2002 möglich, flächendeckend sein elektronisches Ticket berührungslos mittels einer Transponderkarte zu

lösen. Ein einfaches Berühren der Karte am entsprechenden Terminal beim Ein-, Aus- oder Umsteigen genügt, um das Ticket zu kaufen.

Der Vorteil für den Kunden besteht neben der bequemeren bargeldlosen Bezahlung auch darin, dass automatisch der günstigste Preis für die Strecke von A nach B berechnet wird. Abgerechnet wird jeweils am Ende des Monats (Post paid, Best price) entweder via Lastschrift oder Kreditkarte. Zusätzlich gibt es unterschiedliche Bonusprogramme, welche die Kundenzufriedenheit weiter erhöhen soll.

Es lag also auf der Hand dieses intelligente Kundenservice mit dem Namen „get>>in“, um die neue NFC- Handy-Technologie zu erweitern. Dank der Kompatibilität zur bereits installierten Mifare- Technologie mussten bei den Terminals keine kostspieligen Adaptierungen vorgenommen werden.

Kurz nachdem der NFC- Standard auf der Cebit 2004 vorgestellt wurde haben sich der *RMV*, die Hanauer Straßenbahn AG (*HSB*) sowie die Firmen Philips und Nokia zusammengeschlossen, um das *NFC- Handy- Ticketing* weltweit als erster in einem Pilotprojekt zu realisieren.

Das NFC- Handy- Ticketing setzt dabei auf dem bereits existierenden „get>>in“ System auf. Funktionelle Erweiterungen, wie die Handy- Client- Applikation für die Kunden, sowie die entsprechende Anwendung für die Kontrolleure musste noch entwickelt und in das existierende System integriert werden.

Es wurden ca. 150 Personen aus dem bestehenden „get>>in“ System ausgewählt. Diese durften nun ihre personalisierten Transponderkarten gegen spezielle NFC- Handys (Nokia 3220), mit zwei zusätzlich integrierten Secure Smart Card, zum sicheren Speichern der „get>>in“- Applikation sowie für die Hanau- Erlebniscard, eintauschen.

Mit dieser Erlebniscard ist es in Hanau möglich, auch andere Services zu nutzen. Zur Erhöhung der Motivation für die Testkunden wurden ebenfalls Bonuspunkte auf das Handy geladen.

Ablauf Um den Kunden einen attraktiven Preis für das notwendige NFC- Handy anbieten zu können, ist der *RMV* eine Kooperation mit dem Netzbetreiber *Vodafone* sowie mit der Stadt Hanau (Erlebnis Card) eingegangen.

Im ersten Schritt ist es notwendig, dass der Kunde mit seinem NFC- fähigen Handy eine Filiale des *RMV* besucht und dieses dort personalisieren lässt. Dabei werden die Stammdaten des Kunden sowie die gewünschte monatliche Bezahlungsart (Lastschrift oder Kreditkarte) registriert. Auch wird die benötigte Software sicher am Handy auf einem separaten Chip verschlüsselt gespeichert.

Mehr ist nicht zu tun. Ab jetzt funktioniert das Handy genauso wie die „get>>in“- Plastikkarte. Bei jedem Check in bzw. Check out muss lediglich das Handy zum entsprechenden Terminal gehalten werden. Siehe Abbildung 11.

Es erfolgt eine automatische Bestätigung am Handy. Technisch ist es auch möglich, sich aktuelle Fahrplaninformationen vom Terminal aufs Handy übertragen zu lassen.

Die Überprüfung durch die Kontrolleure des *RMV* erfolgt ebenso einfach. Diese sind auch mit einem NFC- Handy mit einer speziellen Applikation ausgestattet. Wird man aufgefordert, sein elektronisches Ticket vorzuweisen, so muss man sein Mobiltelefon einfach nahe an das Handy des Kontrollors halten. Die Daten werden über die NFC- Schnittstelle übertragen. Die Software am Handy des Kontrollors überprüft automatisch das Ticket und zeigt dem Kontrollor am Dis-



Abbildung 11: Die bereits bestehenden Terminals können auch für die Bezahlung mit dem NFC-Handy verwendet werden. Quelle Abbildung: Philips



Abbildung 12: Der Kontrolleur sieht auf einen Blick ob das elektronische Ticket gültig ist. Quelle: Rhein Main Verkehrsverbund

play (Midlet) entweder in Rot oder Grün die Gültigkeit des Tickets an. Siehe auch Abbildung 12.

Am Ende des Monats erhält jeder Kunde eine übersichtliche Rechnung mit einer detaillierten Auflistung aller zurückgelegten Fahrten. Die Kosten werden nach dem *Bestprice Prinzip*³² berechnet, sowie diverse Bonuspunktprogramme berücksichtigt.

Weitere Informationen können den jeweiligen Homepages der Projektpartner RMV³³, Philips³⁴ sowie Nokia³⁵ entnommen werden.

Fazit/Ausblick Am Ende des Pilotprojekts wurden die Teilnehmer nach ihrer Zufriedenheit befragt. Dabei zeigte sich, dass die Akzeptanz des neuen Systems sehr gut ist. Hervorgehoben

³²Ein elektronisches System wählt automatisch den günstigsten Tarif unter Berücksichtigung sämtlicher Parameter.

³³<http://www.rmvplus.de>

³⁴<http://www.philips.at>

³⁵<http://www.nokia.com/nfc>

wurde besonders die einfache Bedienbarkeit. Nach dem Schulnotenprinzip wurde von den Teilnehmern die Note 1.7 vergeben.

Auch die Kontrolloren zeigten sich mit der einfachen Überprüfung (Rot/Grün) der elektronischen Tickets begeistert. Einziger Wermutstropfen für alle Beteiligten ist die begrenzte Haltbarkeit der Handy-Akkus.

Aufgrund des großen Erfolgs des Pilotprojektes wurde dieses am 19. April 2006 in den Regelbetrieb überführt.

Der Rein Mein Verkehrsverbund erwartet sich durch die Einführung dieses neuen Informations- und Serviceangebotes neben einer internen Kostenoptimierung eine weitere Erhöhung der Kundenbindung und Zufriedenheit. Weitere Ziele waren der Aufbau eines Portals zur einfachen Einführung neuer Services und Produkte [17].

3.3 Unterhaltungselektronik

Dieser Typus wird dem *Touch and Connect* Prinzip zugeordnet.

In den letzten Jahren verzeichnete man einen wahren Boom an immer kleineren, ausgereifteren und intelligenteren Geräten wie zum Beispiel Video und Digitalkamera, Handy, TV oder MP3-Player. Diese erfreuen sich einer immer größeren Beliebtheit und meist tragen wir auch eines dieser Geräte bei uns am Körper. Sei es um schnell ein Telefonat zu führen, Termine zu checken oder um sich den letzten Podcast der Lieblingsradiostation, zeitversetzt auf dem Weg zur Arbeit in der U-Bahn, anzuhören. Möglicherweise macht man auch noch einen Schnappschuss mit dem im Handy eingebauten Fotoapparat.

Man sieht also, dass wir es mittlerweile mit einer ganzen Menge von *smart devices* zu tun haben. Gemeinsam ist diesen Geräten leider auch, dass sie oft über unterschiedliche Schnittstellen und Speichermedien verfügen. Der kleinste gemeinsame Nenner aller dieser Standards ist heute der Personal Computer. Damit ist es möglich über Umwege die Daten von einem Gerät zum anderen zu transferieren.

Möchte man zum Beispiel Audiofiles, die auf einem USB-Stick gespeichert sind auf einer Stereoanlage abspielen, so ist es zuerst notwendig den Stick am PC anzuschließen. Möglicherweise müssen dann die Files noch auf einer CD gebrannt werden und erst anschließend kann man diese auf der Stereoanlage abspielen. Ähnlich verhält es sich auch mit Bildern, die man am TV-Gerät direkt anzeigen möchte.

Auch für diese Problematiken bietet die NFC-Technologie eine intuitive und praktikable Lösung an. Voraussetzung ist freilich, dass alle diese Geräte mit dem notwendigen NFC-Chip ausgerüstet sind. Quelle: [5].

3.4 Pervasive Games und Edutainment

Gerade die Game Industrie spielte in der Vergangenheit oft eine innovative Vorreiterrolle. Ein relativ neuer Ansatz in diesem Bereich wird mit dem Begriff *Pervasive Games* beschrieben. Darunter versteht man das Einbinden und Mischen der physikalischen Umgebung mit der virtuellen Realität eines Computerspiels.

Im Gegensatz zu herkömmlichen Szenarien, wo sich Spieler stationär hinter einem Computer oder einer Konsole befinden und via Maus oder Joystick interagieren, können sich diese in „Pervasive Games“ frei im Gelände bewegen.

Dabei müssen sie als Einzelpersonen oder in Teams bestimmte Aufgaben lösen, zum Beispiel

das Sammeln von Informationen vor Ort. Die einzelnen Mitspieler können dabei weltweit verstreut sein und müssen auch nicht permanent online sein. Auch ist es technisch möglich die reele Umgebung mit virtuellen Informationen (Augmented Reality) anzureichern.

Zum Beispiel könnten auf einem PDA mit GPS-Empfänger zusätzliche, spielrelevante Informationen angezeigt werden. Möglicherweise verwendet ein anderer Spieler dazu bereits ein Head-Up-Display. Auch könnte es notwendig sein mit einer Videokamera einen Kurzfilm aufzunehmen, um diesen mittels WLAN den Teammitgliedern zukommen zu lassen.

In Abbildung 13 ist ein Bild eines Pervasive Games dargestellt. Dabei handelt es sich um eine neue Version des legendären Videospiele „Pacman“ mit dem Namen *PAC-LAN*³⁶ und spielt am Campus der Lancaster University³⁷. Im Gegensatz zum Original schlüpfen dabei Menschen in die physischen Rollen des *PacMan* oder der *Geister* [12].

Weitere Informationen und Links zu anderen Games kann man auf der IPERG³⁸ Homepage³⁹ finden.

Ähnliches gilt auch für den *Edutainment* Bereich. In Schulen werden immer mehr diese neuen Technologien und Geräte für unterschiedliche Aufgaben und Projekte eingesetzt. Lehrer berichten von einer deutlich höheren Motivation der Schüler, wenn zeitgemäße Tools im Unterricht oder bei Projektarbeiten eingebaut werden.

Es würde daher auch in diesen, laut Marktforschern in Zukunft stark wachsenden Bereichen, Sinn machen die NFC- Technologie als intuitive, integrierende Schnittstelle für die unterschiedlichen Geräte und Komponenten einzusetzen.

Diese Beispiele fallen in die Kategorie *Touch and Explore*.

3.5 Werbung und Tourismus

Auch in diesen Branchen könnte die Near Field Communication viel zu einer einfacheren und direkten mobilen Interaktion zwischen Mensch und Maschine beitragen.

Man denke zum Beispiel an ein Museum: Jedes interessante Objekt sei mit einem RFID-Tag ausgestattet auf dem sämtliche für den Besucher relevante Information gespeichert sind. Hält man nun ein NFC taugliches Gerät in den Nahbereich dieses Tags, so wird automatisch eine vordefinierte Aktion durchgeführt. Es könnte zum Beispiel ein Audio- oder Video- File drahtlos mit einer schnelleren Bluetooth Verbindung auf das Gerät übertragen werden. Oder es öffnet sich eine URL mit weiteren Hintergrundinformationen. Ebenso könnte auch einfach nur eine Textnachricht via SMS geschickt werden.

So ein ähnliches Szenario wird gerade in einem Pilotversuch in der französischen Stadt *Caen* getestet. Hierbei hat die Stadt an öffentlichen Plätzen Terminals installiert, an denen interessierte Personen mit ihrem NFC- Handy via SMS zusätzliche Infos erhalten.

An dem Projekt sind ca. 200 Bürger der Stadt beteiligt und es erstreckt sich über einen Zeitraum von 6 Monaten. Dabei hat man nicht nur die Möglichkeit einfach Informationen abzufragen, sondern man kann auch in zahlreichen Geschäften des Einzelhandels bargeldlos mit dem NFC- Handy bezahlen oder Parktickets lösen. Weitere Informationen zu diesem Projekt kann man

³⁶<http://www.pac-lan.com/>

³⁷<http://www.lancs.ac.uk/>

³⁸ *Integrated Project on Pervasive Gaming*, European Commission's IST Programme.

³⁹<http://iperg.sics.se/>



Abbildung 13: Pervasive Games: Unterwegs mit dem Handy als „PacMan“ am Unicampus.
Quelle Abbildung: Lancaster University

auf der Homepage von Philips finden.

Für Werbe- und Marketing- Fachleute ist es sicherlich interessant, dass man auch auf Plakate oder Poster, RFID- Tags anbringen kann. Damit ist es möglich, seine Zielgruppe auf direkte Art und Weise multimedial anzusprechen. Das Prinzip ist das selbe wie im oben angeführten Beispiel mit dem Museum. Wichtig ist in diesem Zusammenhang auch, dass man die NFC- Funktion am Handy jederzeit deaktivieren kann.

In der Philips Arena in Atlanta (USA) läuft momentan ein NFC- Pilotprojekt, wo neben bargeldlosen Ticketverkauf mit integrierter Zutrittskontrolle, 150 POS Stationen auch noch zirka 60 sogenannte *smart posters* installiert haben. Dort ist es bereits heute möglich, digitale Inhalte wie zum Beispiel Handyklingeltöne, Bildschirmschoner oder Videos mit der jeweils schnellst möglichen Verbindung, berührungslos aufs Handy zu laden.

3.6 Authentifizierungssysteme

3.6.1 Smart device statt vieler Plastikkarten und Dokumente

Seit dem 16. Juni 2006 ist auch in Österreich der *e-pass* Realität. Das bedeutet, dass sich in diesem ein RFID- Tag mit *biometrischen Daten* der entsprechenden Person befindet. Dies ist die Konsequenz des Entschlusses des *Rates der Europäischen Union* im Jahre 2004, welcher unter Druckausübung von Seiten der USA erfolgte. Man drohte mit der generellen Visa Einführung für alle EU- Bürger.

An biometrischen Daten wird im neuen österreichischem *Sicherheitspass* derzeit nur das Passfoto am RFID- Chip gespeichert. Weitere Merkmale wie die Iris oder elektronische Fingerabdrücke könnten in naher Zukunft ebenfalls verpflichtend sein. Durch die Eindeutigkeit, hohe Fälschungssicherheit und das unmögliche Weiterreichen von biometrischen Merkmalen an andere Personen erhofft man sich im Gegensatz zu *Wissens und Besitzelementen* (z.B. Pincode und Passwort) eine erhöhte Authentizität. Weitere Informationen zur Security oder zur den biometrischen Merkmalen im neuen Pass sind hier [2] detailliert beschrieben.

Als Übertragungstechnologie kommt beim e-pass jedoch nicht die NFC- Technologie zum Einsatz, sondern das sogenannte „Golden Reader Tool“, welches spezielle Anforderungen und Standards der ICAO ⁴⁰ erfüllen muss. Rein technisch gesehen wäre NFC ebenfalls dazu in der Lage.

Quellen: [4], BMI ⁴¹

Es zeigt sich generell, dass auch immer mehr Firmen und Organisationen einen immer größeren Wert auf sichere Zutrittskontrollsysteme legen. Man kann davon ausgehen, dass dabei biometrische Daten eine große Rolle spielen werden. Dazu ist es jedoch notwendig, dass diese auf einem Mikrochip elektronisch gespeichert werden. Um die missbräuchliche Verwendung dieser sensiblen Daten zu verhindern, benötigt man eine Sicherheitsstrategie die im Allgemeinen aus vier Mechanismen besteht:

- Verschlüsselung
- Authentifizierung
- Authorisierung
- Auditing

Mittels der NFC- Erweiterung *Secure NFC* lassen sich obige Mechanismen umsetzen. Dabei kommt ein zusätzlicher *Sicherheitschip* zur Anwendung. Auf der Seite 18 im Kapitel 2.4 wurde dieses Konzept bereits vorgestellt.

Somit stehen der NFC- Technologie viele weitere Anwendungsmöglichkeiten im stark wachsenden Markt von biometrischen Identifizierungssystemen offen. Man denke an die elektronische Signatur im Web, an Zutrittsysteme in Hochsicherheitsbereichen wie zum Beispiel Rechenzentren oder auch zum Beispiel der Personalausweis, Führerschein oder E- Card.

All diese Komponenten könnten in einem einzigem Gerät, wie zum Beispiel Handy oder PDA integriert und über die NFC- Schnittstelle, sicher und trotzdem unkompliziert abgefragt werden.

3.6.2 Skinplex- Die menschliche Haut als Funksender

Skinplex ist ein Markenname der deutschen Firma *Ident- Technology AG* ⁴². Diese hält zahlreiche Patente im Bereich der elektrischen Datenübertragung über die menschliche Haut.

Das Funktionsprinzip ist, dass man einen Codegenerator am Körper trägt. Mittels eines schwachen elektrostatischen Feldes werden die Daten von diesem auf die Haut übertragen. Bei Berührung eines Empfängers, wie zum Beispiel einer Türschnalle oder des Lenkrads eines

⁴⁰International Civil Aviation Organization

⁴¹Bundesministerium für Inneres: <http://www.bmi.gv.at/reisepass>

⁴²<http://www.ident-technology.com>



Abbildung 14: Datenübertragung über die menschliche Haut mit der Skinplex Technologie.
Quelle Abbildung: IDENT Technologie AG

Autos, kann diese Information von diesem demoduliert und ausgewertet werden. Siehe auch Abbildung 14.

Dabei entstehenden für den Menschen völlig unbedenkliche Stromstärken, die sich im nano-Ampere Bereich bewegen und nicht wahrgenommen werden.

Mögliche zukünftige bzw. bereits existierende Anwendungsgebiete der Skinplex- Technologie sind:

- Ausschalten einer gefährlichen Maschine bei Detektierung eines Menschen.
- Schlüssellose Zutrittskontrollsysteme für geschlossene Bereiche, sowie unterschiedlichste technische Geräte wie das Auto oder bestimmten Maschinen.
- Warnung bei Verlust von Geräten wie z.B. eines Schlüsselbund oder Schmuck.
- Weitere Möglichkeiten im Bereich des Pervasive Computing bzw. Ambient Intelligence.

Da für viele Skinplex- Anwendungen ein Codegenerator mit den notwendigen Identifikationsinformationen am menschlichen Körper getragen werden muss, bietet sich auch hier das Handy an.

Ein NFC- Mikrochip kann dabei die Aufgabe dieses Generators übernehmen. Auf der Cebit 2006 wurde ein Linux Smartphon der Firma *ImCoSys* ⁴³ vorgestellt, das *Skinplex NFC* unterstützt. Auch wurde eine Kooperation zwischen der Ident AG und ImCoSys eingegangen, um entsprechende Applikationen in diesem Bereich zu entwickeln.

Für diese innovative *Mensch-Maschinen* Schnittstelle kommt der *NFC- Technologie* ebenfalls eine zentrale Bedeutung zu.

4 Fazit

Die Near Field Communication Technologie könnte einen wichtigen Beitrag zur Weiterentwicklung von vielen mobilen Geschäftsanwendungen liefern. Gleichzeitig hilft sie, im Prinzip

⁴³<http://www.imcosys.com>

komplexe Prozesse stark zu vereinfachen. Um beispielsweise eine Bluetooth- Verbindung herzustellen sind durchschnittlich 20 Klicks sowie ein PIN- Austausch notwendig. Um ein Buch im *www* zu bestellen bis zu 100 Mausklicks sowie die Kenntnis der URL. Mittels NFC können dieselben Aufgaben mit einer simplen *Berührung* sowie gegebenenfalls einer Bestätigung auf einfache und intuitive Weise gelöst werden.

Durch den Zusammenschluss von vielen in diesen Bereichen tätigen Firmen und Organisationen im *NFC- Forum* ist die Kompatibilität zu bereits bestehenden Systemen weitgehend gewährleistet. Ebenso ist es wichtig, dass ein neuer Industriestandard von möglichst allen wichtigen Mitspielern mitgetragen wird. Nur dann kann dieser am Markt langfristig erfolgreich sein.

Ein weiterer wichtiger Punkt ist natürlich auch der Preis. Die Firma Philips rechnet damit, dass im Jahre 2010 nur mehr Handys mit NFC Chip produziert werden. Man kann also davon ausgehen, dass sich der Preis für diese Chips über die Stückzahl sehr bald rechnen wird. Diese Entwicklung konnte und kann man auch bei den zur NFC- Technologie kompatiblen RFID- Tags beobachten.

Je nach Ausführungsart und Anzahl kann bei diesen Funketiketten der Preis naturgemäß sehr stark schwanken. Tatsache ist, dass in diesem Bereich in den letzten Jahren viel Entwicklungsarbeit geleistet wurde und man daher in naher Zukunft mit einem starken Preisverfall rechnet. All die oben aufgelisteten Argumente sowie die im Abschnitt 3 ab Seite 24 beschriebenen Anwendungsbeispiele deuten auf das hohe Zukunftspotential dieser Technologie hin.

Neue Technologien bieten nicht nur Chancen, sondern auch Risiken die es abzuschätzen gilt. Laut einer Schätzung von IBM könnten im Jahre 2013 einer Milliarde Menschen bereits eine Billion intelligenter, untereinander vernetzte elektronische Geräte gegenüberstehen. Dies wirft natürlich einige Fragen auf wie zum Beispiel:

- Was kann dies für unsere Umwelt bedeuten?
- Stellt dies ein Gesundheitsrisiko dar?
- Wie sieht es mit dem Energiebedarf all dieser Geräte aus?
- Was passiert mit den Unmengen von Daten die gespeichert und weitergeleitet werden?
- Wer profitiert davon am meisten?
- Was passiert bei Systemausfällen?

Um seriöse Aussagen machen zu können, wäre es notwendig all diese Fragen zu untersuchen und zu beleuchten. Eine solche Technologieabschätzung würde jedoch den Rahmen dieser Arbeit sprengen.

Selbstverständlich spielen bei der Entwicklung und Einführung von neuen Technologien handfeste ökonomische Interessen die Hauptrolle. Das investierte Geld muss letztendlich der Kunde mit Zins zurückzahlen.

Natürlich ist es beabsichtigt das Geldausgeben mittels eines einfachen *touch & pay* Verfahren zu vereinfachen. Die Hemmschwelle wird dadurch minimiert.

Weiters bedürfte es weltweiter Bestimmungen, die regeln, was genau auf einem Mikrochip

gespeichert werden darf und welche Daten an Dritte weitergegeben werden dürfen und welche auf keinen Fall. Ebenso müsste gewährleistet werden, dass man nicht unerwünschte Daten ohne sein Einverständnis auf das NFC- Handy geladen bekommt.

Es muss bewusst sein, dass man sich durch die immer höher werdende Integration gleichzeitig in ein neues Abhängigkeitsverhältnis begibt. Sollte ein System ausfallen, kann es sein, dass eine Vielzahl von eigentlich „simplen“ Anwendungen wie das Starten eines Autos, Bezahlen im Supermarkt, Öffnen der Wohnungstür etc. nicht mehr funktionieren.

Abbildungsverzeichnis

1	Pervasive Computing	4
2	Das Mooresche Gesetz	5
3	Überblick Speicherbausteine	7
4	Middleware	9
5	NFC Übersicht	11
6	Passiver Betriebsmodus	14
7	PN531 NFC-Transmission module	15
8	Secure NFC	19
9	OTA Plattform	21
10	Anwendungsbeispiel Stromzähler	25
11	Terminal ÖPNV	28
12	Handy MIDlet	28
13	Pervasive Games	31
14	Skinplex Technologie	33

Tabellenverzeichnis

1	Gegenüberstellung: NFC - RFID	13
2	So könnte ein Tabelleneintrag in einer Echtzeit-Datenbank eines Sicherheitsunternehmens aussehen.	26

Literatur

- [1] ANDREW S. TANENBAUM, MAARTEN VAN STEEN: *Distributed Systems: Principles and Paradigms*. Prentice Hall, 2002.
- [2] ARI JUELS, DAVID MOLNAR AND DAVID WAGNER: *Security and Privacy Issues in E-passports*. IEEE Computer Society, 2005.
- [3] BEUTELSPACHER, ALBRECHT: *Moderne Verfahren der Kryptographie. Von RSA zu Zero-Knowledge*. Vieweg, 2001.
- [4] DER RAT DER EUROPÄISCHEN UNION: *VERORDNUNG (EG) Nr. 2252/2004 DES RATES vom 13.12.2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten*. Amtsblatt der Europäischen Union, December 2004.
- [5] ECMA INTERNATIONAL: *Near Field Communication*. White Paper TG19, January 2004.
- [6] FINKENZELLER, KLAUS: *RFID- Handbuch*. Carl Hanser Verlag München Wien, Januar 1998.
- [7] JUAN CARLOS LOPEZ CALVET: *The role of RFID in the mobile phone*. Telenor, April 2005.
- [8] LAURI POHJANHEIMO, HEIKKI KERÄNEN und HEIKKI AILISTO: *Implementing Touch-Me Paradigm with a Mobile Phone*. VTT Technical Research Centre of Finland, 2005.
- [9] MATTERN, FRIEDEMANN: *Allgegenwärtige Informationsverarbeitung- Technologietrends und Auswirkungen des Ubiquitous Computing*. To appear, 2006.
- [10] MINTERT, STEFAN: *Man spricht XML*. IX Special, Heise Zeitschriften Verlag, 1/04, January 2004.
- [11] MOORE, GORDAN: *Cramming more components onto integrated circuits*. Electronics, 38(8), April 1965.
- [12] OMER RASHID, PAUL COULTON, REUBEN EDWARDS, WILLIAM BAMFORD: *Utilising RFID for Mixed Reality Mobile Games*. Informatics, Infolab21, Lancaster University, LA1 4WA UK, January 2006.
- [13] ORTIZ JR., SIXTO: *Is near-field communication close to success?* IEEE Computer, 39(3), March 2006.
- [14] PHILIPS SEMICONDUCTORS: *Near Field Communication PN531- μ C based Transmission module*. Datasheet Revision 2.0, February 2004.
- [15] PHILIPS SEMICONDUCTORS: *S2C Interface for NFC. Adding a general purpose interface between NFC and Secure IC to Secure NFC*. Survey V1.0, January 2005.
- [16] RH TAWNEY: *The Acquisitive Society*. Harcourt, Brace and company, 1920.

- [17] SPARMANN, DIPL.-ING. VOLKER: *Elektronisches Ticketing im ÖPNV*. In: 9. Kasseler Nahverkehrstage. Rhein-Main-Verkehrsverbund, Hofheim, 28./29. November 2005.
- [18] STEVE MANN, HAL NIEDZVIECKI: *Cyborg: digital destiny and human possibility in the age of the wearable computer*. Randomhouse Doubleday, October 2001.
- [19] THOMAS FINKE, HARALD KELTER: *Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems*. Bundesamtes für Sicherheit in der Informationstechnik, 2004.
- [20] TOMI DAHLBERG, NIINA MALLAT, JAN ONDRUS, AGNIESZKA ZMIJEWSKA: *Mobile Payment Market and Research- Past, Present and Future*. Helsinki School of Economics, Ecole des HEC- University of Lausanne, University of Technology- Sydney, 2006.
- [21] VASSILIS KOSTAKOS AND EAMONN O'NEILL: *Designing Pervasive Systems for Society*. Department of Computer Science, University of Bath, UK, 2004.
- [22] V.HASSLER, M.MANNINGER, M.GORDEEV, C.MÜLLER: *Java Card for E-Payment Applications*. Artech House computer security series, 2002.
- [23] WEISER, MARK: *The Computer for the 21st Century*. Xerox Palo Alto Research Center, <http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html> 1991.
- [24] ZIV KFIR, AVISHAI WOOL: *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems*. Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005, 2005.
- [25] ZOE ANTONIOU, GOVINDARAJAN KRISHNAMURTHI AND FRANKLIN REYNOLDS: *Intuitive Service Discovery in RFID-enhanced networks*. Nokia Research Center. Burlington, MA, 2006.