Hochschule für Technik und Wirtschaft Berlin
Angewandten Informatik
Forschungsprojekt II

Potentiale von NFC in der Gesundheitswirtschaft

Alexander Miller

Abgabedatum: 30.01.2011

Prof. Dr. Jurgen Sieck

Inhaltsverzeichnis

Abbildungsverzeichnis **II**

Tabellenverzeichnis **III**

1 Einleitung **1**
1.1 Motivation und Problemstellung 1
1.2 Struktur der Arbeit 2

2 Near Field Communication **3**
2.1 Einführung 3
2.2 Entwicklung und Standardisierung 4

3 Potentiale in der Gesundheitswirtschaft **5**
3.1 Marktanalyse und Prognosen 5
3.2 NFC im Gesundheitswesen 8
3.3 Anforderungsanalyse 9

4 Sicherheitsanalyse **11**
4.1 Kryptographie und Kryptoanalyse 11
4.2 Angriffe und Schutzmaßnahmen in NFC 12
4.2.1 Passive Angriffe 13
4.2.2 Aktive Angriffe 14
4.3 Bewertung der Sicherheit 15

5 Entwicklung eines Prototyps **16**
5.1 Anwendungsszenario 16
5.2 Infrastruktur- und Systemanforderungen 20
5.3 Konzeption und Implementierung 21

6 Zusammenfassung **25**

Literaturverzeichnis **27**

Abbildungsverzeichnis

3.1 Entwicklung des RFID-Marktes 6
3.2 Verteilung der RFID-Chips 7
3.3 Marktentwicklung für mobile Geräte 7

4.1 Ver- und Entschlüsselung einer Nachricht 11
4.2 NFC-SEC 13

5.1 Elektronische Gesundheitskarte mit NFC Funktionalität 16
5.2 Ermittlung der Position ohne GPS-Koordinaten 17
5.3 Ermittlung der Position mit GPS-Koordinaten 18
5.4 Erforderliche Systemkomponente 20
5.5 Realisierung mit Smart Poster Record Type 21
5.6 Benutzeroberfläche des Prototyps 23

Tabellenverzeichnis

2.1 Vergleich der Technologien 3

5.1 Notfalldatensatz 19
5.2 Spezifikation der Daten 19

Abkürzungen

Abkürzung	Bedeutung
AES	Advanced Encryption Standard
ECDH	Elliptic Curves Diffie-Hellman
eGk	Elektronische Gesundheitskarte
ISO	International Organization for Standardization
LLCP	Logical Link Control Protocol
MAC	Message Authentification Codes
MITM	Man-in-the-Middle Attacke
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NFCIP	Near Field Communication Interface Protocoll
PDA	Personal Digital Assistant
RFID	Radio-Frequency Identification
SCH	Secure Channel Service
SSE	Shared Secret Service
WLAN	Wireless Local Area Network

1 Einleitung

1.1 Motivation und Problemstellung

Das Gesundheitswesen der Bundesrepublik Deutschland besitzt einen hohen Stellenwert und stellt der Bevölkerung professionelle Gesundheitsversorgung zur Verfügung. Trotz der kontinuierlichen Steigerung der Ausgaben für die Förderung, den Erhalt und die Wiederherstellung der Gesundheit, muss die medizinische Leistungserbringung sowohl eine hohe Qualität als auch einen Forschungsfortschritt aufweisen [Bor02, Seite 1] . Aus diesem Grund ist es erforderlich das Gesundheitswesen, welches alle beteiligten Personen, Organisationen, Einrichtungen und Prozesse umfasst, als ein einheitliches System zu betrachten. Durch eine intensive Analyse können Potentiale zur Verbesserung der angespannten Situation identifiziert werden, so dass durch geeignete Optimierungsmaßnahmen das Ergebnis sowie die Qualität der Medizin signifikant steigen können. Laut [PA02, Seite 129ff.] besteht ein großer Verbesserungsbedarf in den Bereichen Personal, Investitionen, Auslastung, Material und Erlöse. Aus dieser Aussage resultiert, dass rationale Investitionen in neue Software und Gerätetechnik zur Reorganisation der Prozesse führt, die sowohl eine Reduzierung der Personalkosten als auch langfristige Steigerung der Erlöse bewirkt.

Aufgrund von steigenden Anforderungen an die Behandlungsqualität ist es erforderlich moderne Technologien im Gesundheitswesen einzusetzen. Mobilität und Benutzerkomfort, Zeiteinsparungen und Effizienzsteigerungen, verbesserte Kommunikationsfähigkeiten und Reduzierung von Papieraufwand sind die wesentlichen Gründe zur Entwicklung von neuen medizinischen Systemen unter Berücksichtigung neuester Technologien und Standards [BVH06, Seite 115f.]. Trotz einer progressiven informationstechnischen Entwicklung, ist die Nutzung der modernen Technologien im Bereich HealthCare nicht ausreichend, so dass eine Vielzahl von Arbeitsprozessen immer noch nicht automatisiert abläuft. In [LR10, Seite 205ff.], [Fin08, Seite 375] und [BVH06, Seite 123] wird behauptet, dass durch die Konzeption und Entwicklung von NFC basierten Systemen die einzelnen Prozesse systematisch optimiert werden, wobei die Aufnahme der Patienten in medizinischen Einrichtungen oder die Unterstützung bei der stationären Rehabilitation als vorstellbare Anwendungsbereiche genannt werden.

Die Schwerpunkte dieser Forschungsarbeit werden auf die Potentialanalyse von Near Field Communication (NFC) basierten Systemen im Gesund-

heitswesen gelegt. Dabei soll die Frage beantworten werden, ob Near-Field-Communication in diesem Bereich die Erfolgsaussichten bietet, oder nicht. Es wird geprüft, inwieweit die einzelnen medizinischen Bereiche durch NFC verbessert werden können und welche Anforderungen dafür gestellt werden. Für diesen Zweck ist es erforderlich den heutigen Markt hinsichtlich dieser Technologie zu untersuchen sowie von Spezialisten gemachte Prognosen zu analysieren. Die Berücksichtigung von gesellschaftlichen und wirtschaftlichen Trends ermöglicht die Identifikation sowie die Bewertung von einzelnen Chancen und Risiken.

1.2 Struktur der Arbeit

Die vorliegende Forschungsarbeit beschäftigt sich mit dem Thema "Potentialanalyse von NFC in der Gesundheitswirtschaft". Die Schwerpunkte werden auf eine umfangreiche Marktuntersuchung gelegt, wobei es angestrebt wird die Möglichkeiten und Grenzen von Near-Field-Communication speziell im medizinischen Bereich zu erkennen und eine Aussage über die Erfolgsaussichten dieser Technologie zu treffen.

Dazu werden im 2. Kapitel wichtige Entwicklungen und Standards der drahtlosen Datenübertragung vorgestellt. Anschließend erfolgt die Vorstellung der Funktionsweise, wobei das Hauptaugenmerk auf die Unterscheidungsmerkmale der einzelnen Modi sowie deren Sicherheit gelegt wird.

Das 3. Kapitel ermöglicht einen Einblick in die aktuelle Marktsituation im Bereich Gesundheitswesen. Des Weiteren werden verschiedene Marktprognosen diskutiert und in einem Soll-Ist Vergleich dargestellt. Dadurch ergeben sich die einzelnen Chancen und Risiken, die durch die Einführung von NFC basierten Systemen im Bereich mit besonderen Anforderungen entstehen. Darüber hinaus werden die denkbaren Anwendungsbeispiele vorgestellt.

Im Kapitel 4 wird die Funktionalität für das ausgewählte Szenario ausführlich beschrieben bzw. definiert. Um eine prototypische Implementierung zu ermöglichen wird ein grobes Konzept erstellt. Nach der eindeutigen Definition der einzelnen Systemmodule sowie der Auswahl einer Entwicklungsumgebung wird der Prototyp implementiert sowie die resultierten Ergebnisse vorgestellt.

Im letzten Abschnitt erfolgen die Zusammenfassung sowie der Ausblick in die vorstellbare Erweiterung dieser Arbeit.

2 Near Field Communication

In diesem Kapitel wird der Übertragungsstandard Near Field Communication beschrieben. Als erstes erfolgt eine Einführung in die Spezifikationen einzelner Standards und Protokolle, welche in Rahmen einer Normierungsaktivität entstanden sind. Zunächst erfolgt die Beschreibung einzelner Modi, wobei die Schwerpunkte auf Funktionsweise sowie die Sicherheitsaspekte gelegt werden.

2.1 Einführung

Near Field Communication ist ein Übertragungsstandard, welches zum Datenaustausch über kurze Distanzen (bis 10 cm) entwickelt wurde. Diese Funktechnologie basiert auf passiven Radio Frequency Identification (RFID) Systemen [Fin08] und operiert mit einer Frequenz von 13,56 MHz, so dass eine Datenübertragungsrate bis 424 kbit/s erreicht werden kann. Im Gegensatz zu den bereits existierenden RFID-Systemen (Lesen/Schreiben), bietet die NFC-Technologie die Möglichkeit eine bidirektionale Kommunikation zwischen zwei aktiven Geräten aufzubauen. Im Vergleich zu anderen Technologien bietet NFC viele Vorteile, welche der Tabelle 2.1 zu entnehmen sind.

	IrDa	**Bluetooth**	**RFID**	**NFC**
Initialisierung	0.5s	6s	<0.1ms	<0.1ms
Reichweite	<5m	<30m	<3m	<10cm
Usability	mittel	einfach	einfach	einfach
Anwendung	Datentransfer	Headset	AutoID	Zutrittskontrolle

Tabelle 2.1: Vergleich der Technologien

Aufgrund einer einfachen und vor allem sehr schnellen Initialisierung sowie Verbindungsaufnahme, können die Daten in einer sehr kurzen Zeit bidirektional übertragen werden. Durch eine geringe Reichweite wird die Sicherheit dieser Technologie in den Vordergrund gestellt, da die meisten Angriffsmöglichkeiten zur Beeinträchtigung der drahtlosen Übertragung nicht angewendet werden können. Diese Tatsache spricht für die Realisierung von Anwendungen mit hohen Sicherheitsanforderungen [Hen10]. Darüber hinaus zeichnet sich die NFC-Technologie durch die einfache Benutzung in verschiedensten Bereichen, unter Anderem auch im Gesundheitswesen.

2.2 Entwicklung und Standardisierung

Der NFC-Standard wurde 2002 von Sony und NXP Semiconductors entwickelt. Bereits im Jahr 2004 erfolgte ein Zusammenschluss von mehreren Institutionen und Unternehmen mit dem Ziel internationale Normierungsaktivitäten auszuüben und daduch die Nutzung der NFC-Technologie in Bereichen mobile Geräte, Unterhaltungselektronik und Computer zu fördern [NFC11b].

Als Basis für die Standardisierung dienen bereits weit verbreitete RFID-Standards ISO-14443 und ISO-18092, welche die Kompatibilität der NFC mit vielen bestehenden RFID Konmponenten gewährleisten. Auf dieser Grundlage entstand der Near Field Comunication Interface and Protocol Standard (NFCIP-1 nach ISO/IEC 18092), welcher eine einfache drahtlose Vernetzung von eng gekoppelten Geräten im Frequenzbereich von 13,56 MHz vereinheitlicht. Die Definition des Nachrichtenformats für einen Datenaustausch zwischen zwei aktiven NFC Geräten wurde durch NFC Data Exchange Format (NDEF) standardisiert. Laut [NFC06] wird das Logical Link Control Protocol (LLCP) für die Übertragung auf der zweiten OSI-Ebene verwendet. Versendet werden die sogenannten Records, die in NFC Record Type Definition definiert sind.

3 Potentiale in der Gesundheitswirtschaft

Dieses Kapitel bildet den Hauptteil dieser Forschungsarbeit, wobei die Schwerpunkte auf die Markt-, Risiko- und Sicherheitsanalyse gelegt werden. Insbesondere wird auf die Marktentwicklung der NFC Technologie sowie die einzelnen Marktprognosen unterschiedlicher Institutionen, Organisationen und Unternehmen eingegangen. Das Erkennen von Potentialen dieser Technologie insbesondere im Bereich Gesundheitswesen wird als Ziel kontinuierlich verfolgt. Darüber hinaus werden eine Risiko- und anschließend eine Sicherheitsanalyse durchgeführt, um alle Chancen und Risiken neuer Anwendungen, die NFC-Technologie für die Kommunikation verwenden, zu identifizieren. Zuletzt werden unterschiedliche Szenarien vorgestellt und diskutiert, so dass eins davon für die prototypische Implementierung ausgewählt wird.

3.1 Marktanalyse und Prognosen

In den letzten Jahren gewinnen unterschiedliche Funktechnologien wie Bluetooth, ZigBee, WLAN und NFC sowohl in technologischen als auch in betriebswirtschaftlichen Aspekten mehr an Bedeutung. Trotz noch einer relativ geringen Verbreitung, wird NFC in unterschiedlichen Bereichen eingesetzt, so dass eine steigende Tendenz bzw. große Potentiale gekennzeichnet werden [PM11] [BVH06]. Um die Frage zu beantworten, in wieweit NFC in der Gesundheitswirtschaft Perspektiven und Erfolgsaussichten aufweist, muss eine Marktanalyse durchgeführt werden. Dabei muss die Entwicklung mehrerer Marktsegmente wie zum Beispiel der RFID-Tags, Smartphones mit der NFC-Funktionalität beobachtet werden.

Nach der Betrachtung mehrerer Analysen (ABIResearch, Soreon, DBResearch, Frost&Sullivan), stellte sich heraus, dass die Ergebnisse dieser Untersuchungen stark voneinander abweichen. Die Gründe dafür sind die unterschiedlichen Methoden der Datenerhebung sowie die progressive Marktentwicklung der RFID-Technologie. Wie in der Abbildung 3.1 visualisiert, ist die Entwicklung des Marktes bisher mit sehr großem Erfolg verlaufen und weist für die nächsten Jahre optimistische Prognosen für den weiteren Wachstum auf. Das Diagramm entstand bei der Betrachtung von mehreren Aussagen der Forschungsgruppe ABIReseach. Diese Forschungsgruppe veröffentlichte jährlich die ermittelten

bzw. die ”tatsächlich” erzielten Ergebnisse für die vorherigen Jahre. Durch das Zusammentragen von genaueren Jahresbeträgen aus unterschiedlichen Jahresberichten in ein einziges Diagramm, konnte die Entwicklung visualisiert werden. Es muss beachtet werden, dass nicht der Umsatz die wichtige Aussage für diese Forschungsarbeit liefert, sondern die Wachstumsrate und dadurch die resultierende positive Entwicklung von RFID und NFC. Andere Forschungseinrichtungen, wie zum Beispiel DBReseach haben bereits für das Jahr 2010 einen weltweiten Umsatz von 22 Mrd. US-Dollar prognostiziert. Trotz den riesigen Abweichungen sind alle Analysten und Beratungsunternehmen einig, dass der RFID-Markt progressiv wachsen wird.

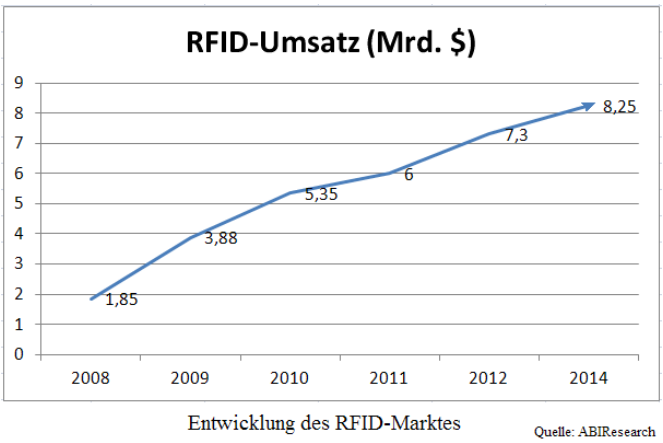

Abbildung 3.1: Entwicklung des RFID-Marktes

Laut einer Studie (siehe Abbildung 3.2) von IDTechEx Ltd., die im Jahr 2005 durchgeführt wurde, gehören die Automobilindustrie, der Finanzsektor sowie der Handel zu den Bereichen mit der größten Nachfrage von RFID-Lösungen. Der Bereich Gesundheitswirtschaft erhielt lediglich 2% der weltweit verkauften RFID-Chips. Es konnte festgestellt werden, dass der Deutsche RFID und NFC Wirtschaft sich proportional zum Weltmarkt entwickelt. Die Verteilung gilt allerdings nur bis zum Jahr 2005. Es muss erwähnt werden, dass genau in diesem Jahr der große Durchbruch kam, so dass es erforderlich ist zu überprüfen in welchen Bereichen im Gesundheitswesen die RFID Technologie verwendet wird und ob der Anteil sich verringert oder vergrößert hat. Eine der größten Einführungen im Gesundheitswesen ist die neue elektronische Gesundheitskarte (eGk). Laut [tel11] wird in die neue Karte ein RFID-Chip für die Gewährleistung eines Signaturvorgangs integriert. Bereits zum 1. Oktober 2011 wurden 7000000 solchen Karte an die Versicherten ausgegeben. Stufenweise werden die Karten für die Bevölkerung in Deutschland ausgegeben. Darüber hinaus gibt es eine Vielzahl von Projekten, die in nachfolgenden Kapiteln näher erläutert werden.

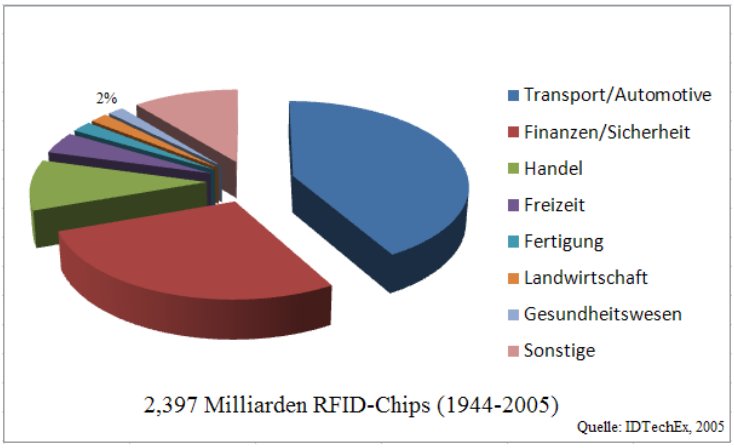

Abbildung 3.2: Verteilung der RFID-Chips

Darüber hinaus ist es ebenfalls sehr wichtig die Entwicklung von NFC fähigen Smartphones zu betrachten. Laut der aktuellen Studie von IHS iSuppli, die in der Abbildung 3.3 dargestellt ist, beträgt die Anzahl der Smartphones im Vergleich zu allen mobilen Telefonen lediglich 22% bzw. 478 Millionen Stück [isu11].

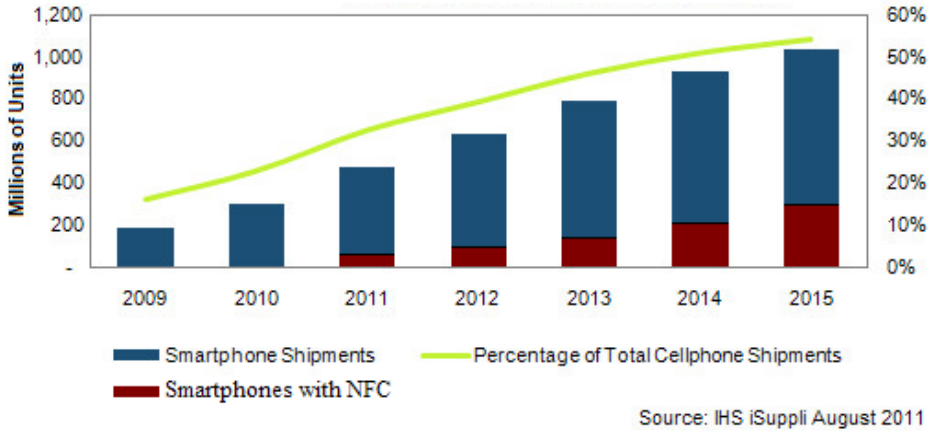

Abbildung 3.3: Marktentwicklung für mobile Geräte

Bei ca. 40 Millionen Smartphones, handelt es sich um NFC-fähige Geräte. Aufgrund der Aussagen von Nokia, dass die kommenden Smartphones zukünftig mit einem NFC-Chip ausgestattet werden, um einen Durchbruch für neue Funktionalitäten zu beschleunigen, machen die Analysten positive Marktprognosen. Darüber hinaus wird von erheblichen wirtschaftlichen Potentialen ausgegangen, da die Verwendung der NFC-Technologie ebenfalls bei marktführenden Unternehmen wie Samsung, BlackBerry und HTC stattfindet [nfc11a]. Basierend auf diesen Aussagen geht IHS iSuppli davon aus, dass im Jahr 2015

die Smartphones mit NFC-Funktionalität einen Marktanteil von 30% (ca. 1,03 Mrd. Stück) betragen wird.

3.2 NFC im Gesundheitswesen

Die Recherche bzw. die Betrachtung der aktuellen Marktsituation sowie der Marktentwicklung weisen in allen Bereichen deutliche Tendenzen auf, so dass weitere hohe jährliche Zuwachsraten zu erwarten sind. Lediglich die Tatsache [RHJ07], dass nur 2% der deutschen Krankenhäuser die NFC-Technologien verwenden und bereits nach einer kurzen Zeit von einem Mehrwert berichten, spricht für eine kommende Nachfrage im Gesundheitssektor. Der weitere Grund ist die Vielfalt der Anwendungsbereiche, die eine Optimierung in folgenden Bereichen ermöglicht:

- **Prozesssteuerung und Dokumentation:** Die städtischen Kliniken Bielefeld haben erkannt, dass durch die Verwendung von NFC sowohl die Prozesssteuerung als auch die Dokumentation optimiert werden kann [RHJ07]. Durch die Einführung eines NFC basierten Systems, die eine effiziente Bettenreinigung nach Bedarf gewährleistet, kann unter der Einsparung von Zeit und speziellen Reinigungsmitteln ein sehr hohes Maß an Sauberkeit und Sterilität erreicht werden. Denn es ist nicht notwendig jedes Bett gleichermaßen zu reinigen, da es unterschieden werden kann, ob der Patient infektiöse Krankheit oder nur Kopfschmerzen hatte. Durch die Verwendung von RFID-Tags können die Informationen mittels NFC-Technologie übertragen werden, so dass abgeleitet werden kann wie hoch der Reinigungsaufwand sein muss. Darüber hinaus erfolgt eine automatische Dokumentation der Prozesse, so dass weitere Prozessoptimierung möglich ist.

- **Lokalisierung:** Laut dem Fachmagazin für kontaktlosen Datentransfer "RFID im Blick", wird die moderne Medizintechnik durch RFID und NFC Einsatz effektiver. Hierzu wird eine Beispielumsetzung für die Unterstützung von Demenzpatienten vorgestellt, die in mehreren Altenpflegeheimen durch die Forschergruppe RI-ComET erprobt wird. Dabei wird es versucht die Aufsicht dementer Personen sowohl für das medizinische Personal zu vereinfachen, als auch dieses Prozess für die Patienten transparenter bzw. nicht bemerkbar zu machen. Die Forscher entwickelten ein Konzept, in dem die Patiente nicht durch die RFID Bänder identifiziert werden, sondern deren Gehhilfen, Rollstühle oder Schuhe getaggt werden. Dadurch ist es möglich die Patienten zu identifizieren und beim Verlassen des Patientenbereichs das Pflegepersonal zu alarmieren.

- **Patientenmedikation:** Eine der führenden Klinik im Bereich RFID/NFC

Technologie ist das Uniklinikum Jena. bereits im Jahr 2006 wird in der Intensivstation eine RFID-gestützte Medikamentennachverfolgung und Patientenmedikation durchgeführt. Dabei werden die Medikamente von der Klinikapotheke bis zur Arzneimittelvergabe verfolgt, so dass eine Fehlmedikation sowie Fälschung von Medikamenten ausgeschlossen werden kann. Das Projekt wird ebenfalls mit RFID-Tags für Medikamente und RFID-Armbänder für die Patienten realisiert. Dabei kann das medizinische Personal mit einem NFC fähigen mobilen Gerät die Daten automatisch abgeglichen und die Medikamente in richtiger Reihenfolge bzw. in korrekter Menge ausgeben. Dadurch werden die Fehlerquellen reduziert, so dass viele Vorteile sowohl für die Kliniken, das Personal als auch für Patienten entstehen.

- **Messdatenüberwachung:** Das Uniklinikum Saarbrücken hat im Jahr 2004 das von Siemens entwickelte System eingeführt, die sowohl für die Identifizierung von Patienten als auch Messdatenüberwachung geeignet ist. Bei der Aufnahme bekommen die Patienten ein RFID-Armband, so dass nach der Identifikation mittels eines PDA auf die wichtige medizinische Werte, Krankengeschichte sowie verabreichte Medikamente zugegriffen werden kann. Darüber hinaus werden die Blutkonserven mit speziellen RFID-Tags (Blutgruppe etc.), die jeweils einen Temperatursensor haben, versehen, um durch die Verwendung von NFC-basierten Systemen die Kühlkette der Blutkonserven immer im Blick zu halten. Mittels eines PDAs werden die Daten abgeglichen, so dass ein Patient bei Bedarf die richtige Blutkonserve bekommt, die stets unter korrekten Bedingungen gelagert wurde.

Die oberen Beispiele zeigen deutlich, dass es tatsächlich möglich ist, durch die Einführung von NFC sowohl bei administrativen als auch bei medizinischen Prozessen einen hohen Optimierungsgrad zu erzielen. Die grundlegende Problematik liegt immer noch bei der Akzeptanz von Innovationen in der Gesundheitswirtschaft. Da es sich nicht nur um reine Profitsteigerung, sondern um die Qualität der medizinischen Patientenbehandlungen handelt, muss eine ausführliche Anforderungsanalyse durchgeführt werden. Dadurch können die Ängste erkannt und durch eine fundierte Untersuchung beseitigt werden. Die resultierenden Ergebnisse könnten für das Aufklärungsgespräch verwendet werden, um die Akzeptanz von NFC zu erhöhen.

3.3 Anforderungsanalyse

Anhand von oben dargestellten Beispielen, kann der tatsächliche Nutzen von der Einführung von NFC bestätigt werden. Allerdings haben nur zwei Prozent der medizinischen Einrichtungen diese Technologie eingeführt. Nun stellt sich

die Frage, welche Anforderungen an diese Technologie gestellt werden und was für die Akzeptanz erforderlich ist.

Es ist selbstverständlich, dass die wichtigste Anforderung der Mehrwert ist. Dabei wird nicht nur die reine Profitsteigerung erwartet, sondern auch solche Nebeneffekte wie die Erhöhung der Kundenzufriedenheit, Optimierung der Prozesse sowie die Qualitätsverbesserung der medizinischen Behandlung. Viele Unternehmen in der Gesundheitswirtschaft, haben bereits NFC-Projekte erfolgreich in das Tagesgeschäft integriert und berichten von einem großen Erfolg.

Ein weiterer Punkt ist das Beeinflussen von medizinischen Geräten. Laut der Studie [BVH06] wurde es tatsächlich festgestellt, dass die medizinischen Geräte durch die NFC Kommunikation negativ beeinflusst werden. Allerdings besteht die Möglichkeit die NFC-Geräte so zu konzipieren, dass diese keine Auswirkung auf die benachbarte Geräte hat. Das heißt, es handelt sich nicht um ein K.O-Kriterium, welches die NFC-Technologie vollständig ausschließt, sondern um ein lösbares Problem.

Weitere Anforderung für die Einführung von NFC-Projekten sind die Kosten für die Anschaffung und die Integration in bereits vorhandene IT-Landschaft. Dieser Punkt muss allerdings zukunftsorientiert betrachtet werden, weil die alleinige Einführung einer Dienstleitung nicht immer rentabel wäre. Allerdings eine Kombination von mehreren Funktionalitäten wie zum Beispiel Patientenidentifikation, Patientenmedikation, Messwerterfassung und Kontrolle, die Prozesssteuerung oder die automatische Dokumentation, werden das Tagesgeschäft erleichtern und die Kosten einer medizinischen Einrichtung reduzieren.

Einer der wichtigsten Punkte ist die Berücksichtigung des Datenschutzes sowie die Gewährleistung der Datensicherheit. Diese Aufgaben, die größtenteils vom Gesetzgeber fest vorgeschrieben sind, müssen zu 100% realisiert werden, da es um sensible bzw. personenbezogene Daten handelt. Aus diesem Grund ist es erforderlich die Daten hinsichtlich des Schutzniveaus zu klassifizieren sowie eine ausführliche Sicherheitsanalyse durchzuführen.

4 Sicherheitsanalyse

In diesem Kapitel werden die Schwerpunkte für die Sicherheitsanalyse in der NFC gelegt, die allgemeingültig ist und somit für alle NFC Anwendungen verwendet werden kann. Durch einen systematischen Ansatz werden die weit verbreiteten Angriffsmöglichkeiten betrachten, wobei das Hauptaugenmerk auf die einzelnen Aspekte hinsichtlich der Datensicherheit sowie der negativen Beeinträchtigung der Kommunikation gelegt wird.

4.1 Kryptographie und Kryptoanalyse

Kryptographie ist eine Wissenschaft, deren ältester Zweig sich mit der Verschlüsselung von Informationen beschäftigt. Das Ziel der modernen Kryptographie ist die Gewährleistung einer sicheren Aufbewahrung oder Übertragung von Nachrichten [KPS02, Seite 41]. Das Grundschema eines kryptographischen Übertragungsprotokolls besteht aus einem Sender, der eine vertrauliche Nachricht an einen Empfänger sicher übermittelt.

Abbildung 4.1: Ver- und Entschlüsselung einer Nachricht

Wie in der Abbildung 4.1 dargestellt, besteht eine Nachricht aus einem Klartext M (engl. *Plaintext*). Um Informationen für Angreifer unverständlich zu machen, wird diese verschlüsselt $E(M)=C$. Eine verschlüsselte Nachricht wird als Chiffretext C (engl. *Ciphertext*) bezeichnet. In dieser Form können beliebige Informationen sicher aufbewahrt oder übertragen werden. Der Prozess der Umwandlung eines chiffrierten Klartextes in lesbare Form wird Entschlüsselung $D(C)=M$ genannt.

Alle Verschlüsselungsverfahren basieren darauf, dass die Umkehrfunktion der Chiffrierung ohne Kenntnis des Schlüssels äußerst aufwendig durchzuführen ist. Daher ist die Sicherheit der Verschlüsselungsverfahren sehr stark vom verwendeten Schlüssel abhängig. Algorithmen, die von der Geheimhaltung ihrer Arbeitsweise abhängen, werden als eingeschränkte Algorithmen bezeichnet und sind nur noch von historischem Interesse [Sch96, Seite 4 ff.].

Kryptoanalytiker untersuchen verschiedene Verschlüsselungsverfahren auf Sicherheit und versuchen die Chiffre aufzubrechen um den Originaltext zu erhalten. So eine versuchte Kryptoanalyse wird als Angriff bezeichnet. Ein häufiger Angriff, bei dem ein Angreifer die Kommunikation zwischen Sender und Empfänger belauscht oder manipuliert, wird als Man-in-the-Middle-Angriff bezeichnet. Es wird davon ausgegangen, dass der Algorithmus dem Angreifer bekannt ist, so dass der Chiffretext mit speziellen Angriffsverfahren gebrochen werden kann. Generell wird zwischen vier folgenden kryptoanalytischen Angriffen unterschieden:

- Ciphertext-only-Angriff,
- Known-plaintext-Angriff,
- Chosen-plaintext-Angriff,
- Adaptive-chosen-plaintext-Angriff.

Eine Verschlüsselungsfunktion ist sicher, wenn sie die oben genannten Angriffe übersteht [Beu06, Seite 6]. Darüber hinaus kann sowohl die Funktionalität als auch die Sicherheit durch weitere Angriffe negativ beeinflusst werden.

4.2 Angriffe und Schutzmaßnahmen in NFC

Wie bei allen anderen Funktechnologien kann die Sicherheit der Datenübertragung mit NFC trotz der geringen Reichweite relativ einfach beeinträchtigt werden. Da die einzelnen NFC-Protokollebenen keine Schutzmaßnahmen gegen Angriffe enthalten, unterliegt die NFC-Technologie folgenden Schwachstellen:

- gezieltes Blockieren einer Datenübertragung durch ein Störsender,
- passive Beeinträchtigung der Kommunikation durch das Belauschen,
- Manipulation der Datenübertragung durch Nachrichtenmodifikation,
- Man-in-the-Middle (MITM) Attacke.

Der Schutz gegen die meisten Angriffsmöglichkeiten lässt sich durch die Anwendung von unterschiedlichen kryptografischen Verfahren wie Verschlüsselung und Message Authentification Codes (MAC) erreichen [**?**]. Für die Durchführung einer Sicherheitsanalyse ist es erforderlich die in NFC integrierten Schutzmaßnahmen zu betrachten. Daraus wird resultieren, ob es Angriffsmöglichkeiten gibt, welche die Kommunikation beinträchtigen können, oder nicht.

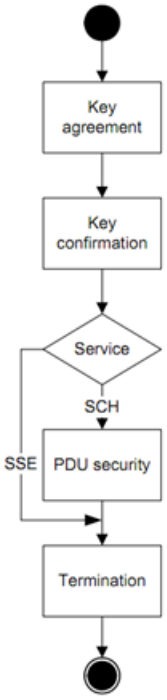

Abbildung 4.2: NFC-SEC

Die einzelnen Schutzmaßnahmen durch kryptografische Verfahren sind in der Norm ECMA-385 definiert. Dieser Standard, der in Form eines Secure Frameworks zur Verfügung steht, agiert zwischen NFCIP-1 und LLCP und gewährleistet eine anwendungsunabhängige Sicherheit.
Mit Shared Secret Service (SSE) erfolgt der Austausch eines gemeinsamen Schlüssels für die unterstützten Verschlüsselungsverfahren. Der Dienst Secure Channel Service (SCH) ermöglicht nicht nur den Schlüsselaustausch, sondern auch den Aufbau eines sicheren Übertragungskanals zur verschlüsselten Datenübertragung. Dabei werden Elliptic Curves Diffie-Hellman (ECDH) und Advanced Encryption Standard (AES) mit einer Schlüssellänge von 128 verwendet [ECM08].

4.2.1 Passive Angriffe

Unter passiven Angriffen, wird das das Abhören eines Kommunikationskanals verstanden. Da es sich bei NFC um eine drahtlose Kommunikation handelt, ist dieser Angriff von essentieller Bedeutung. Für den Kommunikationsaufbau wird ein RF Feld aufgebaut. Somit besteht die Möglichkeit, dass der Angreifer mit einem geeigneten Empfangsgerät den Datenstrom empfangen und daraus die übertragenden Daten extrahieren kann. Der Erfolg dieser Angriffsart, hängt von mehreren Parametern wie zum Beispiel die Qualität bzw. die Charakteristik des Empfangsgeräts sowie der Antenne, dem Übertragungsmodus oder der Signalstärke der NFC-Geräte. Laut [HB06] beträgt die erforderliche Distanz theoretisch ca. 10 m bei einer aktiven Übertragung und ca. 1 m bei der Übertragung in passiven Modus.

Durch den Aufbau eines sicheren Übertragungskanals können die Daten geschützt werden. Hierzu müssen die kryptographischen Verfahren angewendet werden. Da es bei symmetrischen Verfahren die Vereinbarung eines Geheimschlüssels nicht gesichert ist, müssen weitere Verfahren oder Protokolle verwendet werden. Elliptic Curves Diffie-Hellman bietet eine perfekte Möglichkeit für den Aufbau einer sicheren Kommunikation. Im Vergleich zu dem gängigen Diffie-Hellman Protokoll, ermöglicht die Modifizierung durch die el-

liptischen Kurven eine höhere Sicherheit zu erreichen [Paper Diffie Hellman]. Durch die Verschlüsselung der zu übertragenden Daten mit Advanced Encryption Standard (128), können die Daten sicher übertragen werden. Nichtsdestotrotz existieren weitere Angriffsarten: Ciphertext-only-Angriff, Known-plaintext-Angriff, Chosen-plaintext-Angriff, Adaptive-chosen-plaintext-Angriff. Diese Angriffe ermöglichen das Ableiten des Schlüssels, lassen sich allerding durch einfache Maßnahmen vermeiden. Für jede Datenübertragung bzw. für jede Kommunikationsaufbaus soll ein neuer Geheimschlüssel vereinbart werden.

4.2.2 Aktive Angriffe

Da die Kommunikation in NFC gegen passive Angriffe geschützt ist, könnte der Angreifer durch eine Modifikation von Nachrichten die Daten bekommen. Aus diesem Grund ist es erforderlich sowohl eine Möglichkeit der Blockierung der Datenübertragung als auch den Man-in-the-Middle Angriff zu analysieren.

Blockieren der Datenübertragung

Das Blockieren der Datenübertragung kann auf eine unterschiedliche Art und Weise erfolgen. Am einfachsten kann der Angreifer die Kommunikation durch einen ausreichend starken Störsender aus einer Entfernung teilweise oder vollständig beeinträchtigen. Eine weitere Möglichkeit die Übertragung zu blockieren ist die Denial of Service Attacke (DoS). Durch das Verständnis der einzelnen Protokolle der Code-Modulation und Codierung, kann der Angreifer die Pakete in korrekter Reihenfolge zur richtigen Zeit verschicken und somit die Übertragung zwischen zwei Kommunikationspartnern unterbrechen.

Alle NFC-Geräte können gegen diese Angriffe geschützt werden, da diese während der Datenübertragung das RF-Feld überprüfen können. Dadurch kann so ein Angriff erkannt werden, da die Energie bzw. die Signalstärke zur Modifikation der Nachricht viel größer ist als die zur Erkennung eines Gerätes. Dadurch können alle Angriffe dieser Art erkannt werden.

Man-in-the-Middle Attacke

Die oben beschriebenen Angriffe können erfolgreich durch das Verwenden von kryptographischen Verfahren geschützt werden. Es gibt allerdings immer noch keinen Verfahren, welches die Echtheit eines einzelnen NFC-Gerätes verifiziert und somit eine Man-in-the-Middle Attacke verhindert. Aus diesem Grund kann dieser Angriff theoretisch mit einem erheblichen Aufwand umgesetzt werden. Dabei müssen beide Kommunikationspartner in Bezug auf das RF-Feld von einander abgeschirmt sein, um eine gegenseitige Störung zu verhindern. Aufgrund der geringen Reichweite kann die Abschirmung beider Geräte nicht un-

auffällig erfolgen, so dass MITM mit dem Angriff verglichen werden kann bei dem einer der beiden Kommunikationsteilnehmer ausgetauscht wird oder sich unter Kontrolle des Angreifers befindet [LR10, Seite 106].

4.3 Bewertung der Sicherheit

Wie im Kapitel 4.2 belegt wurde, umfasst NFC alle erforderlichen Schutzmechanismen um eine sehr hohe Sicherheit von NFC-Anwendungen zu erreichen. Allerding kann es ebenfalls vorkommen, dass durch eine nicht vollständig durchdachte Planung bzw. eine falsche Konfiguration die Sicherheit negativ beeinflussen können. Daher ist es erforderlich die einzelnen Schutzmaßnahmen korrekt und auch zur richtigen Zeit anzuwenden. Folgende Übersicht, kann als eine Richtlinie für die Verwendung von kryptographischen Verfahren verwendet werden.

1. Intesive Analyse von Sicherheitsanforderungen einer Problemstellung
2. Sicherer Schlüsselaustausch mit Elliptic Curve Diffie Hellman oder Verwendung eines asymmetrisches Kryptosystems
3. Aufbaus eines sicheren Kommunikationskanals, durch die Verschlüsselung der Daten
4. Verwendung von neuen (sicheren) Geheimschlüsseln für jede Kommunikation
5. Authentifikation der Informationsquelle und Signierung von Nachrichten
6. Proximity Check durch die Kontrolle des RF-Felds während der Datenübertragung
7. Verwendung von Verschlüsselungsverfahren und Protokollen, die öffentlich verfügbar sind und als sicher gelten
8. Informative Schulungen und Aufklärungen für das Personal als auch für die Patienten

Falls diese Richtlinie beachtet wird und die einzelnen Maßnahmen korrekt angewendet werden, kann eine NFC-Anwendung als sicher betrachtet werden. Es muss allerding klar sein, dass es in der Kryptographie keine 100% Sicherheit gibt und alle angaben sich auf das aktuelle Zeitpunkt beziehen. Daher ist es erforderlich in regelmäßigen Zeitabständen das Sicherheitsniveau zu kontrollieren und ggf. durch weitere Schutzmaßnahmen zu erhöhen. Der Datenschutz sowie die Sicherheit der Anwendung müssen jederzeit gewährleistet werden, da es im schlimmsten Fall Auswirkungen auf den Gesundheitszustand der Patienten haben kann.

5 Entwicklung eines Prototyps

5.1 Anwendungsszenario

Das Anwendungsszenario basiert auf der neu eingeführten elektronischen Gesundheitskarte. Diese Karte sollte nicht nur zur Unterstützung der ärztlichen Tätigkeit dienen, sondern auch die Möglichkeit geben einen Notruf korrekt abzusetzen, um sowohl die wertvolle Zeit zu sparen als auch so viel wie möglich an Informationen der zuständigen Rettungsstelle zu überreichen. Dadurch wird die Qualität der medizinischen Hilfe verbessert und die Wahrscheinlichkeit einer erfolgreichen Rettung bzw. Behandlung erhöht.

Abbildung 5.1: Elektronische Gesundheitskarte mit NFC Funktionalität

Für die Implementierung eines Prototyps wird eine NFC basierte mobile Applikation konzipiert. Aus Datenschutzgründen kann die mobile Applikation nicht auf den gesamten Speicherbereich zugreifen, da die Informationen verschlüsselt vorliegen und nicht jeder Nutzer berechtigt ist alle personenbezogenen Informationen zu sehen. Aus diesem Grund ist es vorgesehen auf der elektronischen Gesundheitskarte einen separaten unverschlüsselten Speicherbereich zu integrieren, um die Notruf-Funktionalität gewährleisten zu können. Dieser Bereich wird mit erforderlichen Daten beschrieben, die für Ärzte bei der Gewährleistung der Ersten Hilfe von großer Bedeutung sind. Dabei ist es vorgesehen nur die Versicherungsnummer (12 Byte) oder den eindeutigen Zertifikat zu speichern und diese im Notfall an die Notrufzentrale zu übermitteln. Laut [eGk11, Seite 13] ist auf der Gesundheitskarte ein separat angelegter Speicher mit dem Notfalldatensatz vorgesehen, so dass keine Konflikte hinsichtlich des Datenschutzes entstehen können.

Es wird angenommen, dass Herr Sebastian Peters täglich eine wenig befahrene Strecke von Berlin bis Potsdam mit einem Fahrrad fährt. Aufgrund von schlechten Fahrbedingungen stürzte er mit seinem Fahrrad, erlitt einen offenen Bruch am Bein und erleidet eine Ohnmacht bzw. Bewusstlosigkeit. Erst sieben Minuten später findet Herr Mustermann (aus München) eine bewusstlose Person und setzt einen Notruf ab:

Vorher:

Es kommt sehr häufig vor, dass der Anrufer nicht weiß welche Informationen in welcher Reihenfolge mitgeteilt werden müssen. Darüber hinaus ist es nicht immer bekannt wo genau der Betroffene sich befindet, so dass die genaue Ortsangabe mit allen wichtigen Besonderheiten nur nach einer langen Zeit gemacht werden können. Bei einem schweren Unfall spielt allerdings jede Sekunde eine sehr wichtige Rolle.

Es wird angenommen, dass Herr Mustermann das Absetzten eines Notrufs beherrscht und alles richtig macht. Herr Mustermann ruft die Rettungsstelle (112) an und teilt dem Rettungspersonal alle erforderlichen Informationen:

- Wer (Name, Telefonnummer): Max Mustermann, meine Nummer lautet 01743998100
- Wo (Genaue Ortseingabe mit Besonderheiten): Ich befinde mich auf einer Nebenstraße, weiß es allerdings nicht wo genau. Der letzte Ort, welcher ich als letztes durchgefahren bin, war Klein Glinicke. Dann bin ich auf eine Nebenstraße abgebogen. Die Rettungsstelle ermittelt den möglichen Positionspunkt, weiß es allerdings nicht genau wo der verletzte sich befindet.

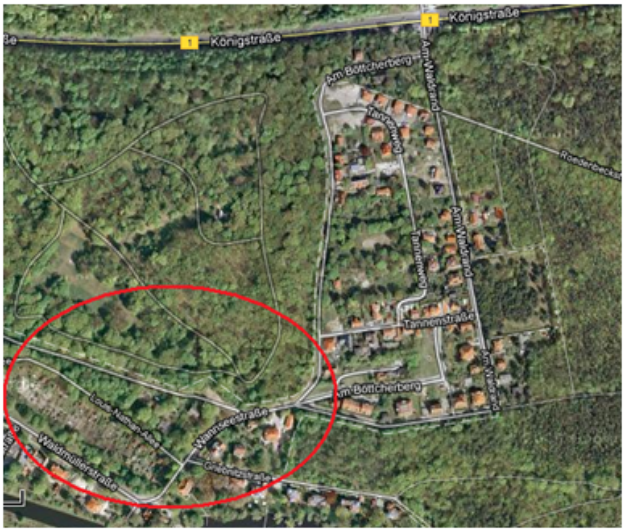

Abbildung 5.2: Ermittlung der Position ohne GPS-Koordinaten

- Was (Was ist passiert): Ich habe vor ca. 4 Minuten eine bewusstlose Person gefunden
- Wie (Anzahl der Verletzte): Es handelt sich um einen Mann, der ca. 30 Jahre alt ist.
- Welche (Art und Schwere der Verletzung): Aufgrund der Position des Körpers sowie viel Blut, gehe ich davon aus, dass es sich um einen offenen Beinbruch handelt. Bin mir allerdings nicht sicher, ob es tatsächlich so ist.
- Warte (Auf die Rückfragen warten): Herr Mustermann wartet auf die Rückfragen

Nachher:
Herr Mustermann startet die mobile Applikation, die bei der Installation vorkonfiguriert wurde und bereits sowohl den Namen als auch die Telefonnummer beinhaltet.

1. Als erstes wird die genaue GPS-Position im Hintergrund automatisch ermittelt und in einer Variablen abgelegt.

Abbildung 5.3: Ermittlung der Position mit GPS-Koordinaten

2. Art des Unfalls wird ausgewählt. Dabei wird zwischen Arbeitsunfall, Fahrzeug-Unfall, Brand, Krankheit, Sonstiges
3. Anzahl der Verletzte wird ausgewählt (1, 2, 3, 4, 5 ... mehr als 5)

4. Nun besteht die Möglichkeit die Art der Verletzung (Offene Wunde, Knochenbruch, Offenes Knochenbruch, Bewusstlosigkeit, Offene Wunde, Schockzustand) zu bestimmen und die Informationen an die Rettungsstelle zu übermitteln oder die elektronische gesundheitskarte (falls vorhanden) Karte einzulesen.

5. Dabei öffnet sich ein weiteres Fenster für die Suche der elektronischen Gesundheitskarte. Es wird angenommen, dass die Karte dabei ist und die Versichertennummer ohne Probleme eingelesen wurde.

Die Rettungsstelle bekommt folgende Mitteilung und nimmt unverzüglich Kontakt mit der Person auf:

Name	Sebastian Peters
Telefon	01743998100
Position	+52° 24’ 36.42”, +13° 6’ 5.54”
Anzahl der Verletzte	1
Art und Schwere der Verletzungen	Offene Wunde Offenes Knochenbruch Bewusstlosigkeit
Versicherungsnummer	A12345678-1

Tabelle 5.1: Notfalldatensatz

Die zuständige Rettungsstelle hat einen Zugriff auf die Datenbank der jeweiligen Krankenversicherung, wobei folgende Informationen automatisch abgerufen und zusätzlich angezeigt werden.

Feld	**Datentyp**	**Beispieldaten**
Versicherungsnummer	String	A12345678-1
Name	String	Peters
Vorname	String	Sebastian
Geburtsdatum	Datum	10.10.1965
Geschlecht	String	Männlich
Blutgruppe	String	AB- (1% in Deutschland)
Behinderungsgrad	Integer	0
Krankheiten	Array[5]	Anämie (Blutarmut)
Implantate	Array[5]	Herzschrittmacher (CRT-D)
Wichtige Informationen	Array[5]	—

Tabelle 5.2: Spezifikation der Daten

Darüber hinaus haben die Ärzte einen Zugriff auf alle Informationen der Gesundheitskarte, während die betroffene Person ins Krankenhaus transportiert wird oder sich im ambulanten Operationssaal befindet.

5.2 Infrastruktur- und Systemanforderungen

Für die Realisierung des oben beschriebenen Anwendungsszenarios ist es notwendig zu analysieren, welche Systemkomponente für die Aufbau der gesamten Infrastruktur erforderlich sind. In der Abbildung 5.4 ist sowohl der grobe Datenablauf als auch die wichtigsten Bestandteile visualisiert.

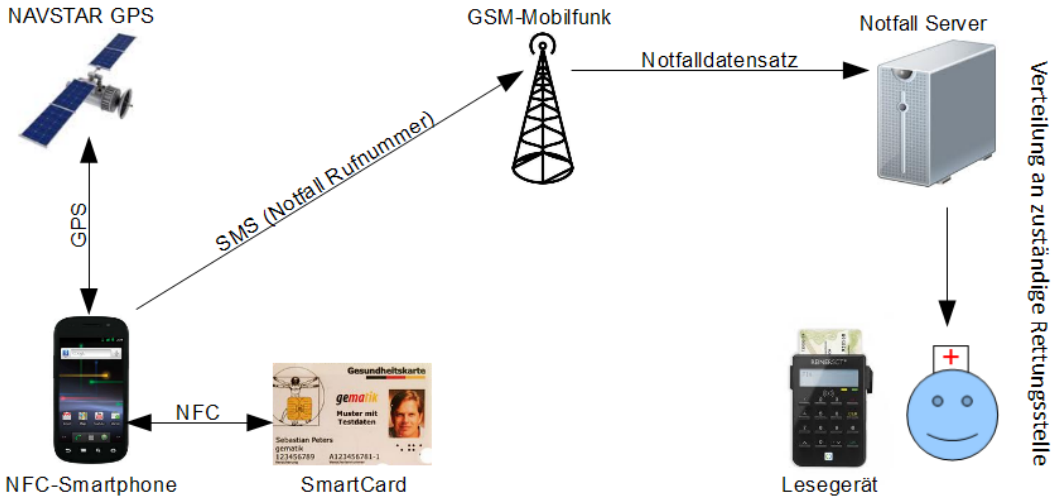

Abbildung 5.4: Erforderliche Systemkomponente

- **SmartCard**: Zu den wichtigsten Komponenten gehört eine SmartCard, die mittel der NFC-Technologie ausgelesen werden kann.
- **Mobiles Gerät**: Das Mobile Gerät muss mehrere Funktionalitäten beinhaltet, um das Szenario umsetzten zu können. Es ist erforderlich, dass das mobile Gerät die NFC-Funktionalität hat und dadurch den Notfalldatensatz auslesen kann. Darüber hinaus muss das Gerät die genauen Koordinaten mittels GPS ermitteln können, um diese an die Rettungsstelle zu übermitteln. Für die Realisierung des Prototyps wird ein Smartphone "Samsung Nexus S" verwendet.
- **GPS-Satteliten**: Wie oben beschrieben, erfolgt die Positionsbestimmung mittels GPS. Es besteht zwar die Möglichkeit die Position mittels Satellitennavigation Galileo zu ermittelt, jedoch ist diese Technologie nicht in den modernen mobilen Geräten integriert.
- **GSM-Mobilfunk**: Die Verwendung des weitverbreiteten GPS-Mobilfunks wird der Notfalldatensatz in Form einer SMS an den Notfallserver versendet. Jedoch muss eine SMS fähige Notfallnummer existieren, um die Meldungen empfangen zu können.

- **Notfall Server** ist sowohl für den SMS-Empfang als auch für die Verteilung an die zuständige Rettungsstelle verantwortlich. Anhand der genauen GPS-Position wird ermittelt welche Rettungsstellen in der Nähe liegen, so dass dadurch die Zeit gespart wird.
- **Medizinisches Personal** entscheidet anhand von gelieferten Daten, welche Medikamente, Geräte, Blutkonserven oder sogar Organe für die erste Hilfe und weiteren stationären Behandlung notwendig sind. Durch das vorhandene Lesegerät, können genauere Daten von der eGesundheitskarte abgerufen werden.

5.3 Konzeption und Implementierung

Die Realisierung dieser Applikation erfolgt durch die Verwendung eines NFC-fähigen mobilen Gerätes (Samsung Nexus S) sowie einer Karte mit einem Smart Poster Record Type. Dabei handelt es sich um eine Kombination von mehreren Records, die die erfassten Informationen vorbereitet an die Rettungsstelle übermitteln. Darüber hinaus ist es sinnvoll die Funktionalität einzubauen, die es ermöglicht verlorene Kinder zu identifizieren und die Eltern unverzüglich zu informieren.

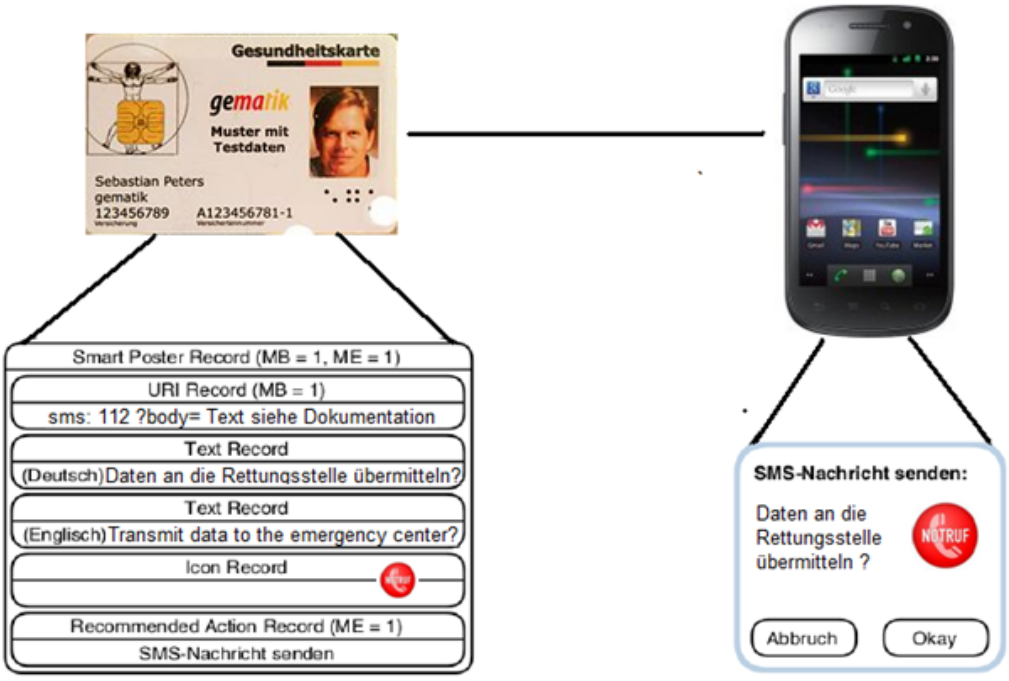

Abbildung 5.5: Realisierung mit Smart Poster Record Type

Eine weitere Möglichkeit der Umsetzung ist die Implementierung einer mo-

bilen Applikation, die den Notfalldatensatz aus der Karte im Textformat ausliest und diese in Kombination von GPS Koordinaten und weiteren Daten an die Rettungsstelle per SMS versendet. Für die praktische Umsetzung des oben aufgeführten Szenarios wurde entschieden ein mobiles Gerät mit dem Android-Betriebssystem zu verwenden. Dabei handelt es sich um ein auf dem Markt weit verbreitetes Betriebssystem von Google, welches auf Linux basierend in der Programmiersprache Java implementiert ist. Das Android Software Development Kit (SDK) ist ein Open Source Entwicklerpacket, welches alle erforderlichen Tools zur Entwicklung von eigenen Anwendungen bereitstellt. Darüber hinaus stellt das SDK einen Emulator zum Testen der implementierten Applikationen zur Verfügung. SDK ist unter allen weitverbreiteten Betriebssystemplattformen wie Windows Systeme, Linux und Mac OS lauffähig. Als Entwicklungsumgebung wird vom Hersteller die Eclipse (Galileo) in der Version 3.5 oder höher empfohlen. Mittels vielfältigen Plug-Ins wird die Entwicklung der Software für mobile Geräte erleichtert. Die einzelnen Systemanforderungen resultieren von den Anforderungen der Entwicklungsumgebung Eclipse [Ecl11] sowie den vom SDK [SDK11].

Folgende Funktionalitäten sind für die Realisierung des Szenarios erforderlich und müssen implementiert werden:

- **Ermittlung der GPS Position**: Die genaue Positionsbestimmung erfolgt durch die Verwendung von GPS. Als erstes muss die Freigabe erfolgen `<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION">` (AndroidManifest.xml), um der Applikation den Zugriff auf die Lokalisierung zu ermöglichen. Durch die Verwendung der `LocationManager` Klasse, kann die Position ermittelt werden. Hierzu wird eine Instanz von `LocationListener` eingesetzt, welche die Koordinaten liefert `mlocManager.requestLocationUpdates( LocationManager.GPS_PROVIDER, 0, 0, mlocListener);`.

- **NFC-Kommunikation mit SmartCard**: Durch den eingebauten NFC Controller von NXP (PN544) ist es möglich auf einer Smart Card bzw. auf den NFC-Tags gespeicherte Daten auszulesen. Um eine Nachricht, die aus mehrere NDEF-Records bestehen kann, auslesen zu können muss die Erlaubnis `<uses-permission android: name="android.permission.NFC"/>` eingetragen werden. Darüber hinaus ist es notwendig die Feature `<uses-feature android:name="android.hardware.nfc"android:required="true"/>` zu bestätigen, damit diese Funktionalität nur bei NFC fähigen mobilen Geräten verwendet werden kann. Für die Realisierung dieser Funktionalität wurde eine Mifare Classic Chipkarte nach ISO/IEC 7810 ID-1 verwendet. Zuerst müssen die benötigten Bibliotheken wie `import android.nfc.tech.MifareClassic;` der Klasse hinzugefügt werden. Durch die unten aufgeführte Methode wird eine SmartCard ausgelesen. Dennoch muss eine zusätzliche Exception-Behandlung erfolgen, um eine absturzfreie Benutzung der Applikation

zu garantieren.

```
1     public static byte[] readTag(Tag tag) {
2         MifareClassic mifare = MifareClassic.get(tag);
3         mifare.connect();
4         mifare.authenticateSectorWithKeyA(2,
              MifareClassic.KEY_DEFAULT);
5         byte[] payload = mifare.readBlock(BLOCK);
6         return payload;
7     }
```

Listing 5.1: NFC

- **Graphische Benutzeroberfläche**: Das graphische Layout wird mittels einer weitverbreiteten Mark-Up Sprache XML definiert und in der Datei main.xml gespeichert. Dabei bilden die Elemente wie TextView, Spinner, CheckBox und Button die für den Benutzer sichtbare Oberfläche und ermöglichen eine komfortable Interaktion sowie eine einfache Nutzung der mobilen Applikation. Dabei besteht die Möglichkeit die Unfallart auszuwählen und die Art der Verletzung zu beschreiben. Die Auswahl wird in Textform an die Rettungsstelle übermittelt.
- **Übermittlung der Daten**: Für die Übermittlung der Daten per SMS muss als erstes eine Freigabe in `AndroidManifest.xml` Datei erfolgen - `SEND_SMS` und `RECEIVE_SMS`. Um eine SMS zu versenden wird die Klasse `SmsManager` verwendet. Es ist nicht notwendig diese Klasse direkt zu instanziieren. Es ist möglich durch den Aufruf der statischen Methode `getDefault()` das SmsManager Objekt zu erhalten. Mittels `sendTextMessage()` wird die SMS versendet.

Abbildung 5.6: Benutzeroberfläche des Prototyps

Die prototypische Implementierung, siehe Abbildung 5.6, wurde im Laufe dieses Projektes zum Teil umgesetzt. Aufgrund der fehlenden Infrastruktur wurde es nicht bestrebt ein laufendes System zu implementieren, sondern die einzelnen Funktionalitäten umzusetzen und zu testen. Dadurch wurde bestätigt, dass im Rahmen eines größeren Projektes diese Applikation ohne weitere Komplikationen umgesetzt werden kann.

6 Zusammenfassung

Die Gesundheitswirtschaft in Deutschland besitzt einen hohen Stellenwert und stellt der Bevölkerung professionelle Gesundheitsversorgung zur Verfügung. Hierzu gehören alle beteiligte Personen, Organisationen, Einrichtungen und Prozesse, so dass ein Zusammenspiel zwischen diesen Akteuren von sehr großer Bedeutung ist. Aus diesem Grund wird es immer wichtiger neue und vor allem zukunftsorientierte Technologien einzusetzen. Das Ziel dieser Arbeit ist die Durchführung einer Potentialanalyse von NFC basierten Systemen in der Gesundheitswirtschaft.

Nach einer Einarbeitung in die Near Field Communication und der anschließenden Betrachtung von Standardisierungen dieser Kommunikationstechnologie, wurde eine intensive Recherche hinsichtlich der Entwicklung und Wachstumsrate in den letzten Jahren durchgeführt. Laut den jährlichen Berichten der Forschungsgruppe ABIReseach entwickelt sich der RFID/NFC Markt sehr positiv. Weitere wichtige Forschungsunternehmen wie DBReseach und IDTechEx Ltd. bestätigen die Aussage. Dabei beträgt der Bereich Gesundheitswesen lediglich 2%, so dass aufgrund von zunehmender Verbreitung von NFC-fähigen mobilen Geräten der Anteil an NFC-Projekten progressiv wachsen wird.

Durch eine intensive Recherche wurde ersichtlich, dass bereits seit dem Jahr 2004 eine Vielzahl von NFC basierten Systemen in der Gesundheitswirtschaft in Bereichen Prozesssteuerung und Dokumentation, Identifikation und Lokalisierung, Patientenmedikation sowie Messdatenüberwachung existieren. Es handelt sich lediglich um die sogenannten Pilot-Projekte, die am häufigsten an Uni-Kliniken erprobt werden. Das heißt dadurch wurde es bereits bewiesen, dass durch die Integration der RFID und NFC Technologie sowohl bei administrativen als auch bei medizinischen Prozessen ein hohes Optimierungsgrad erreicht werden kann.

Da die Akzeptanz von Innovationen, vor allem von neuen Technologien im Bereich Gesundheitswesen zögernd ist, ist es notwendig die Anforderungsanalyse durchzuführen. Dabei wurde festgestellt, dass ein sehr hoher Mehrwert existiert und dieser Projekte nachhaltig bzw. zukunftsorientiert werden könne. Das heißt, eine spätere Erweiterung der Funktionalität würde zu noch besseren Ergebnissen führen und dadurch die Qualität einer medizinischen Einrichtung verbessern. Jedoch muss der Aspekt des Datenschutzes und der Datensicherheit berücksichtigt werden.

Aus diesem Grund wurde eine Sicherheitsanalyse auf der informationstech-

nischen Ebene durchgeführt. Hierzu wurden die einzelnen Angriffe und Schutzmaßnahmen auf NFC untersucht. Durch die Analyse von aktiven und passiven Angriffsszenarien, konnte die Effektivität der Schutzmaßnahmen kontrolliert werden. Als Ergebnis entstand eine allgemeingültige Bewertung der Sicherheit in NFC, die in Form einer Richtlinie bei der Entwicklung von NFC-Projekten verwendet werden kann. Im Allgemeinen wurde die NFC-Technologie als sicher eingestuft, so dass sogar Anwendungen mit kritischen Anforderungen (z.B. personenbezogene Daten) realisiert werden können.

Für die Erkennung weiterer Potentiale und für den Beweis, dass NFC im Bereich Gesundheitswirtschaft an vielen Stellen verwendet werden kann, wurde ein Prototyp konzipiert. Es handelt sich um eine Applikation für mobile Geräte, welche durch die Verwendung einer NFC fähigen elektronischen Gesundheitskarte eine effiziente und vor alle individuelle erste Hilfe gewährleistet. Die Karte besitzt einen Notfalldatensatz, welches im Falle eines Unfalls an die zuständige Stelle per SMS übermittelt wird. Dadurch wird das Rettungspersonal über die Krankheiten, Medikamentenverträglichkeit und weitere wichtigen Gegebenheiten informiert, so dass die Ausstattung eines Krankenwagens und ggf. des Operationssaals rechtzeitig und vor allem vollständig vorbereitet werden kann.

Als Schlussfolgerung folgt, dass Near Field Communication sehr viele Potentiale in allen Bereichen aufweist, insbesondere im Gesundheitswesen. Bei der Betrachtung der Wachstumsrate sowie des Erfolgs in anderen Bereichen, kann es mit Sicherheit behauptet werden, dass NFC sich auch im Gesundheitswesen durchsetzten wird. Angesichts aller Pilot-Projekte, haben bereits die ersten medizinischen Einrichtungen die Umsetzbarkeit dieser Technologie gezeigt. Die Implementierung des oben erwähnten Prototyps zeigt, dass sogar die Verwendung außerhalb der stationären Behandlung erfolgen kann. Die Kritik wie zum Beispiel das beeinflussen anderer medizinischen Geräten sowie der mangelhafte Realisierung des Datenschutzes und der Datensicherheit, konnte mittels der durchgeführten Sicherheitsanalyse beseitigt werden. Für die Realisierung weiterer NFC-Projekte steht lediglich nur die mangelnde Akzeptanz von neuen Technologien im Wege, die allerdings in den späteren Jahren abgeschwächt wird. Eine frühe Integration von NFC-Projekten zur Prozessoptimierung wird sich durch eine erhöhte Kundenzufriedenheit und steigende Behandlungsqualität auszahlen. NFC hat viele Erfolgsaussichten und kann ohne Bedenken für die Realisierung von neuen Projekten verwendet werden.

Literaturverzeichnis

[Beu06] Beutelspacher, Albrecht: *Moderne Verfahren der Kryptographie (German Edition).* Vieweg+Teubner Verlag, 2006

[Bor02] Bornemeier, Olaf: *Benchmarking in der Gesundheitsversorgung.* Autorenverlag Scheriau, 2002

[BVH06] Bärwolff, Hartmut ; Victor, Frank ; Hüsken, Volker: *IT-Systeme in der Medizin: IT-Entscheidungshilfe für den Medizinbereich - Konzepte, Standards und optimierte Prozesse (German Edition).* Vieweg+Teubner Verlag, 2006

[Ecl11] Eclipse - Requirements. In: *Eclipse Foundation* (2011). `http://www.eclipse.org/`. – Zugriffsdatum: 10.09.2011

[ECM08] NFC-SEC - NFCIP-1 Security Services and Protocol. In: *ECMA International* (2008). `http://www.ecma-international.org/activities/Communications/tc47-2008-089.pdf`. – Zugriffsdatum: 06.02.2012

[eGk11] Übersicht Gesundheitskarte. In: *Deutsche Krankenhaus Gesellschaft* (2011). `http://www.nkgev.de/telematik_o/Uebersicht_Gesundheitskarte_3-2011.pdf`. – Zugriffsdatum: 06.02.2012

[Fin08] Finkenzeller, Klaus: *RFID-Handbuch.* Hanser Fachbuchverlag, 2008

[HB06] Haselsteiner, Ernst ; Breitfuss, Klemens: Security in Near Field Communication (NFC) - Strengths and Weaknesses. In: *Philips Semiconductors* (2006)

[Hen10] Henrici, Dirk: *RFID Security and Privacy: Concepts, Protocols, and Architectures (Lecture Notes in Electrical Engineering).* Springer, 2010

[isu11] Smartphones to Account for Majority of Cellphone Shipments by 2015. In: *isuppli.com* (2011). `http://www.isuppli.com/Mobile-and-Wireless-Communications/News/Pages/Smartphones-to-Account-for-Majority-of-Cellphone-Shipments-by-2015.aspx`. – Zugriffsdatum: 06.02.2012

[KPS02] Kaufman, Charlie ; Perlman, Radia ; Speciner, Mike: *Network Security: Private Communication in a Public World (2nd Edition)*. Prentice Hall, 2002

[LR10] Langer, Josef ; Roland, Michael: *Anwendungen und Technik von Near Field Communication (NFC) (German Edition)*. Springer, 2010

[NFC06] NFC Data Exchange Format (NDEF). In: *NFC Forum* (2006)

[nfc11a] A definitive list of NFC phones. In: *NFC-World* (2011). `http://www.nfcworld.com/nfc-phones-list/`. – Zugriffsdatum: 06.02.2012

[NFC11b] Offiziele Webseite. In: *NFC Forum* (2011). `http://www.nfc-forum.org/home/`. – Zugriffsdatum: 06.02.2012

[PA02] Penter, Volker ; Arnold, Christoph: *Zukunft deutsches Krankenhaus - Thesen, Analysen, Potentiale*. Autorenverlag Scheriau, 2002

[PM11] Prinz, Andreas ; Menschner, Philipp: NFC-basiertes Ernährungsmanagement für ältere, pflegebedürftige Menschen. In: *Universität Kassel* (2011)

[RHJ07] Rost-Hein, Manuela ; Japs, Simon: *RFID im Gesundheitswesen*. 2007

[Sch96] Schneier, Bruce: *Angewandte Kryptographie - Der Klassiker. Protokolle, Algorithmen und Sourcecode in C*. 1996

[SDK11] SDK System Requirements. In: *Android Developers* (2011). `http://developer.android.com/sdk/requirements.html`. – Zugriffsdatum: 10.09.2011

[tel11] Zukunftssicher aufgestellt für die elektronische Gesundheitskarte. In: *Telematik-Markt.de* (2011). `http://www.telematik-markt.de/telematik/`. – Zugriffsdatum: 06.02.2012