NFC Tags in der Notfallmedizin

Abruf von Patientendaten in Notfallsituationen

BACHELORARBEIT

zur Erlangung des akademischen Grades

Bachelor of Science

im Rahmen des Studiums

Medizinische Informatik

eingereicht von

Sebastian Bachmann
Matrikelnummer 0925947

ausgeführt am
Institut für Rechnergestützte Automation
Forschungsgruppe Industrial Software
der Fakultät für Informatik der Technischen Universität Wien

Betreuung: Wolfgang Schramm

Wien, 27. November 2013

Kurzfassung

Eine Person bricht auf der Straße zusammen - ein Notfall. Sofort wird der Rettungsdienst kontaktiert und verschiedene Personen beginnen ihre Arbeit mit dem Patienten. Jeder Fehler kann in dieser Situation das Leben des Patienten gefährden, Arzneimittelwechselwirkungen oder eine falsche Behandlung aufgrund chronischer Krankheiten sind nur zwei Komplikationen die auftreten können.

Notfallkarten oder -Ausweise werden meistens aus Papier gefertigt und enthalten nur einen Bruchteil der Informationen, welche möglicherweise notwendig wären. Moderne Technologien wie Near Field Communication (NFC) und Radio Frequency Idenification (RFID) bieten Vorteile gegenüber den konventionellen Ausweisen und könnten in Zukunft diese ablösen. Die Entwicklung eines geeigneten Datenprotokolls sowie einer Benutzerschnittstelle stand bei dieser Arbeit im Vordergrund.

Als Ergebnis wird ein Protokoll spezifiziert, welches die begrenzte Größe der NFC Tags voll ausnutzt und dabei die Kompatibilität verschiedener Versionen von Anwendung und Protokoll sicherstellt. Dabei können Arzneimittel sowie Krankheiten über standardisierte Schnittstellen eingegeben werden und bieten so eine effektive Speicherung der Daten auf dem Tag. Zudem wurde ein Userinterface als Applikation für Android entwickelt, welches die Eingabe der Daten und die anschließende Speicherung ermöglicht. Für das medizinische Personal konnte ein Interface geschaffen werden, welches die Daten strukturiert und gefiltert ausgibt, um etwa für bestimmte Gruppen von Medizinern unnötige Informationen in der jeweiligen Situation auszublenden. Auch wurden der Datenschutz beleuchtet und Möglichkeiten zum Schutz aufgezeigt.

Schlüsselwörter

NFC, RFID, Notfall, Notfallausweis, Android, Notfallmedizin

Abstract

A person breaks down in the middle of the street - an emergency. Immediately emergency services are called and different persons begins their work on the patient. Every little mistake can cost the life of the patient, drug interactions or a wrong treatment because of a chronic disease are just two examples for intricacies in an emergency case.

Emergency cards are mostly made out of paper and contain only a small piece of the information that would be really needed in that case. Modern technologies like Near Field Communication (NFC) and Radio Frequency Idenification (RFID) have the capability to hold the data and provide even more advantages over conventional cards. The design of a data protocol and user interface was the main target of this work.

As result, a protocol is specified which uses the whole limited space on the NFC Tag and contains compatibility for different versions of protocol and using application. The user interface, which was designed for the Android operating system, provides standardized methods to insert medication and diseases, while the protocol provides an effective way to save the data on the tag. The medical personnel uses different interfaces for each group, where information is structured and show in a way that is the most useful for this specific person. Also data privacy and protection was analyzed and security methods are shown.

Keywords

NFC, RFID, emergency, emergency-card, Android, emergency medical aid

Inhaltsverzeichnis

Abkürzungen

.so Shared Object. 8

AES Advanced Encryption Standard. 16

API Application Programming Interface. 8

APK Application Package File. 8, 18

BAC Basic Access Control. 16

CDA Clinical Document Architecture. 5

CRC16 16-bit Cyclic redundancy check. 15

DIDB Metabolism & Transport Drug Interaction Database. 22

DIMDI Deutsches Institut für Medizinische Dokumentation und Information. 5, 6, 19

EHR Electronic Health Record. 6

ELGA Elektronische Gesundheitsakte. 1, 23

FLOPS Floating Point Operations Per Second. 29

HL7 Health Level Seven. 5

ICD10 International Statistical Classification of Diseases and Related Health Problems. 2, 5, 15, 19

IHTSDO International Health Terminology Standards Development Organisation. 6

JAR Java Archive. 8

KIS Krankenhausinformationssystem. 1, 18

NDK Native Development Kit. 7

NFC Near Field Communication. i, ii, 1, 7, 8, 13–16, 18, 24, 25

PKI Public Key Infrastructure. 16, 17, 24

PZN Pharmazentralnummer. 15, 20

RFID Radio Frequency Idenification. i, ii, 1, 7, 16, 17

RFU Reserved for Future Use. 11, 12

SDK Software Development Kit. 7

1 Einleitung

Smartphones gehören mittlerweile zum alltäglichen Leben und haben in vielen Fällen den gleichen oder einen höheren Nutzungsgrad erreicht wie etwa der Computer [1]. Zudem wurden in den letzten Jahren Technologien entwickelt, welche die Vernetzung von mobilen Anwendungen und Geräten noch weiter verbessern. So kann man heutzutage beim Laufen nicht nur Musik von seinem Smartphone lauschen sondern auch gleichzeitig den Puls und Sauerstoffsättigung über ein Bluetooth Gerät ablesen. Zudem können Streckendaten, aktuelle Laufgeschwindigkeit, Temperatur und Luftdruck bequem über integrierte Sensoren sowie das mobile Datennetz geladen werden.

Durch NFC und RFID Techniken, wurde es möglich Daten auf verschiedensten Oberflächen zu speichern und Metadaten direkt auf dem Objekt abzulegen. Dabei kommen so genannte Tags zum Einsatz, auf denen die Daten gespeichert werden.

Auch in der Medizin haben Smartphones und mobile Geräte Anklang gefunden. Nicht zuletzt durch KIS sind auch Tablets in den Krankenhäusern eingezogen und lösen hier die herkömmlichen Papierakten ab. Insbesondere hier scheint der Einsatz von NFC Technologien logisch und sinnvoll, könnte man so Patientendaten live am Tablet ablesen und speichern. Doch bei genauerem Betrachten der utopisch wirkenden Möglichkeiten fallen Nachteile auf, welche insbesondere in Hinblick auf die Sicherheit Fragen offen lassen. Dass es hier Klärungsbedarf gibt, kann auch in der aktuellen Diskussion um die Elektronische Gesundheitsakte (ELGA) beobachtet werden.

1.1 Problemstellung

In dieser Arbeit soll konkret der Frage nachgegangen werden, wie NFC und RFID in der Notfallmedizin eingesetzt werden kann, um die Patientenstammdaten auf strukturierte Art und Weise dem behandelten Arzt zur Verfügung zu stellen. Hierbei ist notwendig zu wissen, dass etwa ein Sanitäter andere Informationen benötigt als der Arzt im Krankenhaus oder sogar später der Chirurg. Hinzu kommt, dass die Informationen zwar allen Personen, die im Notfall an der Behandlung teilhaben, verfügbar sein sollen, aber eben nur in dieser konkreten Situation. Dritte sollen auf die Daten keinen Zugriff erhalten. Dies ist jedoch durch die Funktionsweise von NFC nicht sichergestellt, da für die Übertragung der Daten elektromagnetische Wellen (Funk) verwendet werden und diese prinzipiell nicht abhörsicher gemacht werden können. Somit muss ein Zugriffsschutz auf Ebene der Daten implementiert oder eine andere Möglichkeit des Schutzes gefunden werden.

Ein wichtiger Punkt der Arbeit ist somit auch das Speichern und Auslesen der Daten an sich. So müssen Patienten ihre Daten in einfacher und für sie verständlicher Form eingeben können, ein Mediziner soll sie dann später jedoch in seiner „Sprache" auslesen. Weiters soll Anzahl und Ausführlichkeit der Datensätze nur durch die Speicherkapazität beschränkt sein, so dass verschiedenste Arten von Daten auf dem Chip gespeichert werden können.

1.2 Motivation

Folgendes Szenario könnte sich gerade jetzt abspielen:

> *Person P. ist auf Geschäftsreise in einer fremden Stadt. Auf dem Weg vom Hotel zu seinem Geschäftspartner verliert P. mitten auf der Straße das Bewusstsein, Passanten rufen den Rettungswagen. Als die Sanitäter eintreffen hat auch die Atmung von P. ausgesetzt und er muss reanimiert werden. Die Sanitäter wenden eine akute Maskenbeatmung an, wissen allerdings nicht, dass P. an einer ausgeprägten chronischen, durch sein Diabetes bedingten, Azidose leidet.*

In diesem Fall müsste eine Maskenbeatmung ausgeschlossen werden [2]. Da die Sanitäter jedoch nichts von der chronischen Krankheit wissen, unterläuft ihnen dieser Fehler.

Wie im Szenario beschrieben, gibt es diverse chronische Krankheiten, welche bestimmte Behandlungsmethoden ausschließen.

Auch in späterer Folge können durch Medikamentengabe Allergien ausgelöst werden oder Wechselwirkungen durch regelmäßig eingenommene Präparate entstehen. In vielen Fällen treten Notfälle nicht am Wohnort auf. Auch sind in vielen Fällen weder die behandelnden Ärzte mit dem Patienten vertraut noch gibt es bestehende Aufzeichnungen über die Krankheitsgeschichte. Trotz einer Patientenakte ist es oft schwer eine vollständige Historie des Patienten zu eruieren, wenn der Patient nun bewusstlos ist, in den meisten Fällen gar unmöglich. Auch kommt es durch die Globalisierung vermehrt zu Notfällen außerhalb des Heimatlandes, so dass die Sprachbarriere sowie der Austausch von Daten mit dem Ausland, aufgrund unterschiedlicher Gesetze und Datenprotokolle, die Situation verschärft.

Kommt es nun vor, dass Informationen fehlen, sind diese meistens bereits in irgend einer Form vorhanden, allerdings in anderen Krankenhäusern oder bei unterschiedlichen Ärzten. Würden die akut behandelnden Mediziner von diesen Quellen wissen, könnten sie direkte Rücksprache halten oder weitere Informationen anfordern. Selbes gilt für Personen, welche im Notfall informiert werden sollen, wie etwa Angehörige. Die notwendigen Adressen oder Telefonnummern sind zwar oft im Adressbuch des Patienten vorhanden aber nicht für Außenstehende gekennzeichnet. Somit kann ein Kontakt nicht oder nur schwer hergestellt werden.

1.3 Zielsetzung

Ziel dieser Arbeit ist es, einen Prototypen zu entwickeln, welcher die Schwierigkeiten der Anamnese im Notfall behebt und Risiken bei der Behandlung minimiert.

Dabei sollen verschiedene Sichten auf die Daten den jeweiligen Akteuren die Möglichkeit bieten, unterschiedliche Datensätze anzuzeigen und somit nur für sie relevante Daten zu sehen. Zudem soll es dem Patienten möglich sein, die Daten in einer einfachen und für ihn verständlichen Art und Weise einzugeben, trotzdem aber die semantische Übersetzung auf ein standardisiertes System, etwa ICD10, zu gewährleisten.

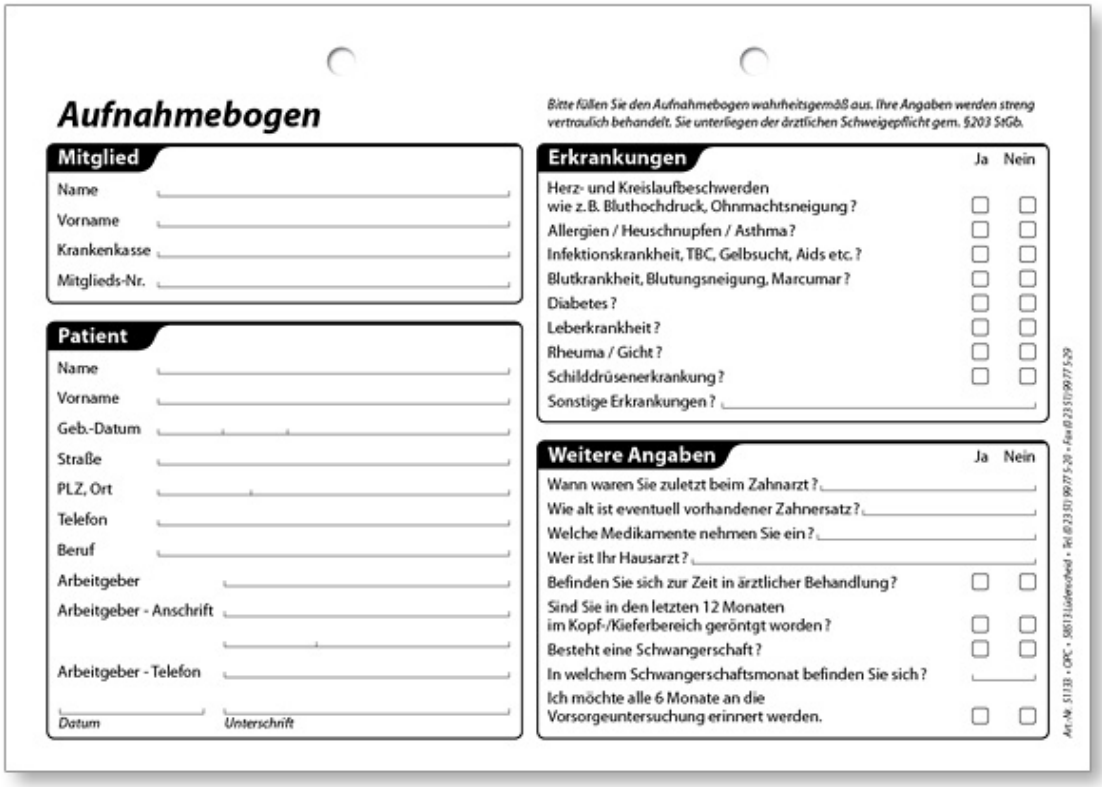
Neben den semantischen und Usability-Problemen sind darüber hinaus Sicherheitsanforderungen an das System zu stellen, welche den Zugriff durch dritte, nicht berechtigte Personen, ausschließen und die Daten trotzdem im Notfall allen beteiligten Personen uneingeschränkt zu Verfügung stellen.

2 Grundlagen

2.1 Notfalldaten

Im Laufe des Lebens sammelt eine Person eine Unmenge an medizinischen Daten an. Doch lediglich ein Bruchteil dieser Daten ist in einem Notfall wichtig, zumal das Lesen und Verstehen der gesamten Patientenakte viel zu viel Zeit in Anspruch nehmen würde.

Bei der Anamnese werden die wichtigsten Daten eines Patienten erfasst und strukturiert abgelegt. Meist werden von Krankenhäusern oder Ärzten Formulare verwendet, um die Anamnesedaten zu speichern und später schnell abrufbereit zu haben. Ein typisches Beispiel für einen solchen Bogen zeigt Abbildung 2.1. Oft werden auch schon vor dem Gespräch mit dem Arzt Kurzanamnesebögen ausgeteilt um die wichtigsten Stammdaten wie Name, Adresse aber auch chronische Krankheiten, Medikamenteneinnahme und Allergien abzufragen.



Aufnahmebogen

Bitte füllen Sie den Aufnahmebogen wahrheitsgemäß aus. Ihre Angaben werden streng vertraulich behandelt. Sie unterliegen der ärztlichen Schweigepflicht gem. §203 StGb.

Mitglied

Name
Vorname
Krankenkasse
Mitglieds-Nr.

Patient

Name
Vorname
Geb.-Datum
Straße
PLZ, Ort
Telefon
Beruf
Arbeitgeber
Arbeitgeber - Anschrift
Arbeitgeber - Telefon
Datum
Unterschrift

Erkrankungen

	Ja	Nein
Herz- und Kreislaufbeschwerden wie z. B. Bluthochdruck, Ohnmachtsneigung?	☐	☐
Allergien / Heuschnupfen / Asthma?	☐	☐
Infektionskrankheit, TBC, Gelbsucht, Aids etc.?	☐	☐
Blutkrankheit, Blutungsneigung, Marcumar?	☐	☐
Diabetes?	☐	☐
Leberkrankheit?	☐	☐
Rheuma / Gicht?	☐	☐
Schilddrüsenerkrankung?	☐	☐
Sonstige Erkrankungen?		

Weitere Angaben

	Ja	Nein
Wann waren Sie zuletzt beim Zahnarzt?		
Wie alt ist eventuell vorhandener Zahnersatz?		
Welche Medikamente nehmen Sie ein?		
Wer ist Ihr Hausarzt?		
Befinden Sie sich zur Zeit in ärztlicher Behandlung?	☐	☐
Sind Sie in den letzten 12 Monaten im Kopf-/Kieferbereich geröntgt worden?	☐	☐
Besteht eine Schwangerschaft?	☐	☐
In welchem Schwangerschaftsmonat befinden Sie sich?		
Ich möchte alle 6 Monate an die Vorsorgeuntersuchung erinnert werden.	☐	☐

Abbildung 2.1: Ein typischer Kurzanamnesebogen, hier für einen Zahnarzt dargestellt

2.1.1 Anamnese im Notfall

In einem Notfall sind für die unterschiedlichen Personen, die an der Behandlung und Versorgung des Patienten beteiligt sind, unterschiedliche Informationen erforderlich. So benötigt ein Ersthelfer kaum Daten, den dazu gerufenen Notarzt könnte allerdings eine Unverträglichkeit gegen ein bestimmtes Medikament oder eine chronische Krankheit interessieren. Bei Kindern sind etwa 75% aller Fälle von anaphylaktischen Schock bei Notfällen durch eine Latexallergie bedingt [3].

In einem Notfall muss die Anamnese auf das Notwendige und Mögliche reduziert werden. Sollte die Person bewusstlos sein, so kann keine Anamnese durchgeführt werden. Ein weiteres Problem kann sein, dass Personen sich im Notfall nicht an alle ihre wichtigen Informationen erinnern oder auch durch Behinderung oder Krankheit nicht in der Lage, sind ihre Informationen zu teilen.

[4] definiert für die Notfallanamnese, dass kurz und symptomorientiert vorgegangen werden soll. Hierbei sollen aktuelle Beschwerden, Therapien, bekannte Symptomatiken sowie Vorerkrankungen und Medikation aufgezählt werden. Im Fall einer Notfallkarte können alle Informationen, mit Ausnahme der aktuellen Beschwerden, abgespeichert werden.

Datensatz	**wird benötigt für**
Name und Anschrift	Identifizierung
Versicherungsnummer	Identifizierung
Alter / Geburtsdatum	Medikamentengabe / Behandlung
Blutgruppe	bei Blutgabe
Chronische Krankheiten	Behandlung, Komplikationsvorbeugung
aktuelle Medikation	Arzeimittelwechselwirkungen
Metallteile im Körper	Radiologie
Organspender	Bei Todesfall
Angehörige / Notfallnummer	zur Verständigung

Tabelle 2.1: Auflistung von verschiedenen Notfalldaten und ihrem Einsatzort

2.1.2 Notfallkarte

Die Idee, die wichtigsten Daten immer dabei zu haben, ist sicherlich so alt wie der Rettungsdienst an sich. Bei der Speicherung dieser Daten wurde auch immer wieder neues entdeckt und umgesetzt, so wurden die ersten Daten einfach nur auf einem Blatt Papier aufgeschrieben, mittlerweile kann dies auch digital geschehen. Eine weit verbreitete Methode zur Kennzeichnung von Personen, welche im Notfall benachrichtigt werden sollen, ist es etwa am Handy-Adressbuch einen Eintrag mit dem Namen „ICE" für „In Case of Emergency" zu speichern. Aber auch Dienstleister bieten Notfalldatenspeicher an, etwa http://www.notfallkarte.at, welche ein kostenpflichtiges Service zur Verfügung stellen um im Notfall auf die Daten zuzugreifen [5]. Ebenso gibt es den Internationalen Notfallausweis, welcher ähnliche Informationen in Papierform speichert [6].

2.1.3 Situation im Katastrophenfall

Neben einem „normalen" Notfall könnte eine solche Karte auch bei einem Großschadensereignis sinnvolle Verwendung finden. Ein solches System kann sehr gut mit einem Triage System kombiniert werden und bietet den Helfern wichtige Daten zur Identifizierung von Opfern und kann helfen bewusstlose Personen besser zu versorgen.

2.2 Semantische Aufbereitung

Patienten und Ärzte reden oft nicht die selbe Sprache. Zwar „sprechen" Ärzte auch Umgangssprache und können verstehen wenn jemand sagt, dass der Blinddarm herausgenommen wurde, allerdings ist die medizinische Terminologie in vielen Fällen besser geeignet um Krankheiten, Verletzungen oder andere Diagnosen exakt zu beschreiben. Allein durch Lageparametern ist es den Ärtzen möglich, etwa Schmerzen besser zu lokalisieren als durch Begriffe wie „daneben" oder „ein bisschen links". Damit ein Patient dennoch sinnvoll seine Daten eintragen kann, sollte dies nach Möglichkeit mit einem Arzt zusammen erfolgen. Ansätze wie eine semantische Aufbereitung der Daten werden allerdings auch schon im klinischen Umfeld erforscht [7]. Allerdings sind auch diese nicht gegen alle umgangssprachlichen Begriffe gefeit und benötigen zudem in vielen Fällen kontextbezogene Daten, ohne die eine genaue Zuordnung zu medizinischen Begriffen nicht möglich ist.

Für medizinische Daten wurden zu dem Zweck einer einheitlichen Sprache Code Systeme eingeführt. Ein Beispiel ist hier etwa ICD10, welches bei Datenverarbeitenden Systemen gute Dienste leistet. Allerdings ist hier auch eine Übersetzung zwischen Volltextnamen der Krankheit sowie dem dazugehörigem Code notwendig. Ein solcher Code bietet jedoch gegenüber dem Volltext die Möglichkeit Namen in anderen Sprachen anzuzeigen.

2.3 Kodierung Medizinischer Daten

Dadurch das Rechnersysteme in den letzten 50 Jahren einen drastischen Wandel vom Mainframe zum Tablet hingelegt haben, ist es nicht verwunderlich dass auch klinische und medizinische Daten statt in Papier- nun auch in digitaler Form abrufbar sein sollen. Dies bringt viele Vorteile mit sich, allerdings auch die Notwendigkeit eine sinnvolle Art und Weise zu haben, diese Daten in den Datenbanken zu speichern. Dabei wurde, etwa wie beim Health Level Seven (HL7) Clinical Document Architecture (CDA) Standard, zunächst nur auf reine Speicherbarkeit geachtet und erst später die Option die Daten auch rechnergestüzt auswerten zu können implementiert.

Generell gibt es bei der speicherung von medizinischen Daten einige Probleme zu lösen, etwa die korrekte Speicherung von behandelden Ärzten, Stammdaten des Patienten, Befunde, Röntgenbilder und die Krankheitsdaten an sich. Für die meisten dieser Arten existieren mittlerweile einige Standards, welche zum Teil in vielen verschiedenen Versionen und Abwandlungen verwendet werden.

2.3.1 International Classification of Diseases

Der Standard wird von der World Health Organisation ausgegeben und befindet sich mittlerweile in der 10. Revision, wobei die 11. Version aktuell in der Entstehungsphase ist. Neben dieser Hauptversion entstehen auch Länderspezifische Abwandlungen, etwa die International Statistical Classification of Diseases and Related Health Problems (ICD10) German Modifications, welche insbesondere in Deutschland verwendet wird sowie ICD10 BMG 2013, welche in Österreich verwendet wird und vom Bundesministerium für Gesundheit herausgegeben wird [8]. Die Deutsche Modifikation des Standards wird von Deutsches Institut für Medizinische Dokumentation und Information (DIMDI) herausgegeben und übersetzt, seit dem 01. Januar 2000 wird in Deutschland der ICD10-GM Standard in Ambulanzen und in Kliniken auch verpflichtend verwendet [9].

Das ICD10 System besteht aus einem Code, welcher mit verschiedenen Namen verknüpft werden kann (siehe Tabelle 5.1 für eine Auflistung von verschiedenen Namen für Diabetes Typ I). Dabei

werden 22 Kapitel von Krankheiten definiert, welche die allgemeine Systematik angeben. Diese Systematiken werden mit einem Großbuchstaben sowie zwei Ziffern beschrieben, etwa E10 bis E14 für verschiedene Arten von Diabetes. Danach kann mit einem Punkt getrennt eine weitere Zahl gestellt werden, welche die Verfeinerung angibt: E10.90 für *Insulinpflichtiger Typ-1 Diabetes mellitus*. Theoretisch ergeben sich dadurch mehr als 250000 Möglichkeiten, dennoch sind nur knapp 13000 davon auch wirklich in Verwendung [10].

Im Codesystem ist es unerheblich wie viele Namen auf einen Code referenzieren, sondern sogar sinnvoll viele verschiedene Namen zu kennen. Die übersetzung in einen Namen in der richtigen Sprache erfolgt dann automatisch. Zu diesem Zweck gibt es etwa vom DIMDI verschieden aufbereitete Tabellen der ICD10-GM, wobei eine Version immer nur den Vorzugsnamen zu einem Code angibt, in einer zweiten Version auch Synonyme (Diagnosentexte) enthalten sind, hierbei enthält diese alphabetische Version mehr als 76000 Einträge [11]. So lässt sich über die Systematik ein Code zu seinem Vorzugsnamen zuordnen und über den alphabetischen Index ein Diagnosentext zu dem dazugehörigen Code.

Hauptnutzen von ICD ist eigentlich die einfache Statistische Auswertung von Diagnosen etwa in der Epidemiologie, kann aber genau so auch für einen Electronic Health Record verwendet werden.

2.3.2 SNOMED Clinical Terms

Neben dem ICD Codesystem existieren noch andere Systeme, eines davon ist SNOMED, welches nicht für die statistische Auswertung konzipiert wurde sondern speziell für den Einsatz in Electronic Health Records. Dabei soll die Genauigkeit der Eingabemöglichkeiten verbessert werden und somit eine detaillierte Informationsweitergabe und -speicherung in einem Electronic Health Record (EHR) möglich sein.

SNOMED wird von der International Health Terminology Standards Development Organisation (IHTSDO) verwaltet und derzeit befinden sich 18 Länder in der Interessensgemeinschaft [12].

SNOMED wird in drei Komponenten unterteilt: *Concepts*, *Descriptions* und *Relationships* [13]. Die *Concepts* beinhalten dabei 300000 verschiedene klinische Begriffe, wobei diese hierachisch angeordnet werden. In den *Descriptions* werden für Menschen sinnvolle Begriffe zu den *Concepts* verknüpft, wobei in der Englischen Version mehr als eine Million Begriffe bekannt sind. Ein *Relationship* verknüpft zwei *Concepts* miteinander, wobei verschiedene Arten von Verbindungen erzeugt werden können, etwa „is a" (ist ein) oder „has" (hat).

Zwischen SNOMED CT und ICD10 existieren Mapping Dokumente, welche SNOMED Queries auf einen ICD10 Code abbilden können.

2.3.3 Pharmazentralnummern

Pharmazentralnummern werden in Deutschland und Österreich verwendet um Medikamente zu kennzeichnen. Die Nummer besteht aus sieben Ziffern, inklusive einer Prüfziffer, und ist für jedes Arzeimittel einzigartig. Dabei wird auch zwischen Packungsgrößen unterschieden [14]. Zwischen dem deutschen und österreichischem PZN System besteht lediglich der Unterschied, dass die Nummern von zwei unabhängigen Instituten vergeben werden und nicht ident sind. In Österreich werden die Nummern etwa von der ARGE Pharma vergeben. Hinzu kommt, dass diese Nummern nur eine gültigkeit von maximal zwei Jahren haben und danach erneut angefordert werden müssen. Dadurch müssen Datenbanken regelmäßig geflegt werden und Updates in die Point-of-Sale Systeme eingespielt werden. Sinn und Zweck der PZN ist die Vereinfachte Abrechnung, Bestel-

lung und Verwaltung von Arzneimitteln etwa in einer Apotheke. Die PZN kann etweder direkt oder im Produkt EAN Barcode auf der Verpackung angebracht werden. Dabei wurden folgende Konventionen entwickelt: Ist nur der PZN im Barcode enthalten, so wird die Nummer selber im Barcode mit einem „-" kodiert, also etwa statt „1234567" nun „-1234567" und der Barcode enthält als Textbezeichner „PZN -123457". Wird hingegen der Produkt EAN verwendet, so setzt sich dieser aus zwei Ziffern für eine Länderkennung, 4 Ziffern für eine Kennung durch die ARGE Pharma und der eigentlichen PZN zusammen [15].

2.4 NFC mittels RFID

Die NFC Technik findet derzeit immer mehr Einzug in viele Bereiche unseres Lebens. Unter NFC versteht man Verfahren, welche in einer kleinen Umgebung kommunikation mit Geräten, aktive oder passive, ermöglichen. Zu diesen Verfahren zählen unter anderem Bluetooth aber auch ein RFID Standard wurde entwickelt. Die NFC Spezifikation für RFID verwendet eine 13.56 MHz Trägerfrequenz und bietet passive sowie aktive Endgeräte an, welche Daten bereit stellen. Konzepte von Kontaktlose Kassen sind bereits Wirklichkeit geworden und viele Smartphones und andere Mobile Geräte unterstützen die Verwendung von NFC.

Die NFC Tags selber sind in verschiedenen Formen erhältlich, etwa als ISO-Karte, Schlüsselanhänger oder Armband und eignen sich daher gut als Datenträger für kurze aber wichtige Nachrichten, welche schnell verfügbar sein sollen. Die Reichweite von NFC Tags beträgt wenige Zentimeter, wobei durch größere Antennen auch bis zu einem Meter möglich ist. Vor dieser Möglichkeit warnt etwa der CCC [16]. Hierbei werden zwar andere RFID Chips verwendet, dennoch tritt die gleiche Gefahr auch bei den NFC Tags auf. Aus diesem Grund entsteht das große Problem mit NFC Tags, dass Daten durch kleine Distanzen hinweg ausgelesen werden können, ohne das der Besitzer dies mitbekommt. Daher sollten auf NFC Tags nur Daten in verschlüsselter Form gespeichert werden oder eben nur solche bei denen ein nicht kontrolliertes Auslesen keinen Sicherheitskritischen Tatbestand darstellt.

NFC Tags werden üblicherweise in den Größen von einem Kilobit (128 Byte) bis zu 64 kB und größer hergestellt wobei ein Großteil der Chips nur mit 128 Byte oder einem kB produziert werden. Typische Einsatzzwecke für die kleinen Chips sind etwa Zugangssysteme, bei denen auf dem Chip nur eine ID gespeichert werden muss. Eine solche ID ist in den meisten Fällen fix und seit der Herstellung auf dem Chip kodiert, so dass sich etwa Zugangs- oder Authentifzierungssysteme besonders einfach umsetzen lassen.

2.5 Android

Android ist ein freies Open Source Betriebsystem, welches auf Linux basiert und von Google im Jahr 2007 veröffentlicht wurde. Die Entwicklung von Applikationen für Android funktioniert über ein eigenes Software Development Kit (SDK), wobei die Entwicklung hauptsächlich in Java geschiet, allerdings auch ein Native Development Kit (NDK) für die Entwicklung in C/C++ bereitgestellt wird. Auf den Android Geräten wird dann allerdings keine Java Runtime verwendet, sondern ein speziell für das Android System entwickelte Bytecode Sprache, nämlich Dalvik, verwendet. Diese unterscheidet sich im Vergleich zu Java Bytecode durch die Verwendung von Registern anstelle von Stacks und dadurch verbesserte Performance auf ARM Systemen. Native Software wird nicht in Dalvik übersetzt sondern als Shared Object (.so) Datei abgespeichert. Durch bestimmte Bindings können native Funktionen in einem Dalvik File aufgerufen werden.

Im Gegensatz zu anderen mobilen Betriebsystemen, etwa iOS, unterstützt Android ein sehr großes Berechtigungsmodell. Hierbei werden Berechtigungen für bestimmte, vom Benutzer zu erlaubende Aktionen gesetzt, welche intern im System auf Unix Gruppen gemapped werden. Bei der Installation werden die Berechtigungen überprüft und die Benutzergruppen gesetzt. Dies funktioniert etwa für die Berechtigung „Internet" so, wo allen Apps, welche diese Berechtigung brauchen, die Benutzergruppe *inet* zugeteilt wird. Diese Gruppe ist dann berechtigungt Sockets zu öffnen. In anderen Fällen wie zum Beispiel den Zugriff auf Benutzerkonten, wird dies durch einen Berechtigungsservice verwaltet. Für jede App wird bei der Erstellung ein Interface geschaffen über das es mit seiner User ID zugreifen kann. Diese User ID wird einzigartig für jede App, mit einigen Außnahmen, bei der Installation generiert.

Applikationen werden als Application Package File (APK) Datei auf das Android Gerät geladen und dort in dieser Form gespeichert. Eine APK Datei hat den selben Aufbau wie eine Java Archive (JAR) Datei, wobei nicht Klassen (.class) abgespeichert werden sondern zumindest eine *classes.dex* (Dalvik Kompilat), *AndroidManifest.xml* (XML Datei mit Metainformationen über das APK) sowie ressources.arsc (Resourcen welche im DEX verwenden werden) Datei vorhanden sein müssen. Um eine APK Datei tatsächlich auf einem Android Gerät zu installieren muss diese noch signiert werden. Die Signatur dient allerdings einzig und allein dem Zweck ein Update für eine App zu erkennen, da der Name einer App prinzipiell öfter vorkommen darf. Auch können über die Signatur spezielle System Berechtigungen angefordert werden, wenn die System Signatur und App Signatur übereinstimmen. Eine Signatur ist hierbei einfach ein öffentlicher DSA oder RSA Schlüssel, sowie eine Datei in dem die Signatur Hashes aller Dateien im APK abgelegt werden (*MANIFEST.MF*).

Das Android System stellt dem Benutzer eine Menge an Application Programming Interface (API) Funktionen zur Verfügung, etwa auch um auf NFC Hardware zuzugreifen. Dabei abstrahiert das Android System diese Dinge so weit, dass die selbe Funktion für unterschiedliche Hardware auf unterschiedlichen Geräten genau so funktioniert. Dies ermöglicht die reibungslose und einfache Verwendung von oft komplizierten Vorgängen auf allen Geräten welche diese Hardware unterstützten und mit Android laufen.

Applikationen können im Vergleich zu iOS nicht nur durch den offiziellen Markt, im Falle von Android „Google Play" auf das Gerät gelangen, sondern prinzipiell über jegliche Kanäle. Dies ermöglicht Anwendern eigene Märkte zu schaffen oder Apps einfach herunterzuladen und das APK direkt von der SD-Karte zu installieren.

Das Android System hat sich in seiner doch erst kurzen Lebenszeit schon als Marktführer etabliert [17].

3 Problemstellung & Umfeld

3.1 Stakeholder

An der Lösung sind zumindest zwei Gruppen von Stakeholder beteiligt, die Patienten, welche ihre Daten sicher, einfach und vor allem in einer für sie verständlichen Form eingeben wollen und auf der anderen Seite die Notfallhelfer, Ärzte und Personen, die bei einem Notfall Daten vom Patienten benötigen. Diese Gruppe möchte die Daten zum richtigen Zeitpunkt in der bestmöglichen für sie aufbereiteten Art bekommen um möglichst keine Wartezeiten zu erzeugen. Wichtig für beide Gruppen ist, dass die Daten sicher gespeichert sind, für den Patienten zählen hier insbesondere der Zugriffsschutz, für den Notfallhelfer, dass die Daten korrekt sind und die sichere Speicherung gewährleistet ist.

3.1.1 Patienten

Der Patient steht im Hauptaugenmerkt der Software. Er muss schließlich seine Daten hier eintragen, welche ihm in einer Notfallsitution vielleicht einmal das Leben retten. Der Patient ist kein Durchschnittsmensch sondern kann aus jeder sozialen Schicht stammen, jeden Alters sein und jegliche Vorerkrankungen, chronischen Leiden oder sonstige Bedürfnisse haben. Daher ist es wichtig, dass auf all diese besonderen Eigenschaften Rücksicht genommen werden kann und alle Bedürfnisse so gut wie möglich erfüllt werden. Wichtig ist dabei zu wissen, dass ein großteil der Bevölkerung nicht sehr technikaffin ist und sich nicht mit Computern, Smartphones oder anderen modernen Technologien auskennt und daher spezielle Konzepte entwickelt werden müssen [18]. Neben der großen Bevölkerungsgruppe der älteren Personen finden sich aber auch die noch größere Gruppe der Nicht-Mediziner. So werden sich nur ein Bruchteil der Bevölkerung ihre Krankheiten mit dem korrekten Vorzugsnamen merken können und auch sonst können sie Befunde eher wenig gut verstehen noch daraus Schlüsse ziehen. Der Patient möchte aber trotzdem verstehen was ihm fehlt oder an welcher Krankheit er leidet, auch wollen ältere Personen in Notfällen die bestmögliche Sicherheit erfahren und sich nicht im Vorhinein Gedanken machen müssen welche Dinge „passieren könnten".

Auch durch die anhaltende Diskussion rund um eHealth und Krankenhausinformationssysteme sowie die Datenspeicherung von Gesundheitsdaten allgemein sind die Patienten verunsichert, was mit ihren Daten geschieht. Dieser inharente Unsicherheitsfaktor bringen aber so gut wie alle Computersysteme mit sich, da nur wenige Menschen wissen und verstehen, was in einem Computer wirklich vor sich geht. Somit möchte der Anwender neben seiner persönlichen Sicherheit im Notfall auch eine Informationssicherheit erfahren - seine Daten sollen sicher vor dritten sein und gleichzeitig zur richtigen Zeit der richtigen Person zur verfügbar stehen.

3.1.2 Medizinisches Personal

Medizinisches Personal und insbesondere Personen welcher in der Notfallbetreuung arbeiten, sind zum Teil einem sehr starken Stress ausgesetzt [19]. Dabei kann sich dieser Stress auch schnell negativ auf die eigene Gesundheit auswirken. Somit gilt es möglichst weiteren Stress in einer Notfallsituation zu vermeiden und sogar zu veringern.

In einer Studie konnte herausgefunden werden, dass sogar langsame Userinterfaces Stress auslösen können [20]. Somit sollte das Userinterface für das Notfallpersonal einfach und schnell funktionieren und die Informationen in einer für den Arzt sinnvollen Art und Weise aufbereitet werden. Dadurch kann die Person die Informationen einfacher erfassen und hat im Endeffekt keinen zusätzlichen Stress. Jedoch muss neben dem Userinterface auch der gesamte Ablauf des Einlesens schnell sein. Denn nur wenn auch die Karte innerhalb von weniger Sekunden gelesen werden kann ist eine sinnvolle Interaktion möglich.

Neben diesen Stressfaktoren sollen die Informationen welche dort angezeigt werden jedoch auch authentisch sein. Denn ebenfalls das Wissen, dass Informationen vielleicht nicht stimmen kann einen Stress auslösen, auch wenn dies nur Unterbewusst geschiet. Ein Anwender soll auf einen Blick feststellen können wann die Daten geändert wurden, also ob diese noch aktuell sind.

Für den Einsatz im Ausland müssen die Daten, welche auf der Notfallkarte gespeichert sind, auch dort auslesbar sein und zwar in einer Form die ein Anwender versteht. Es muss eine Möglichkeit besetehen diesen Anwendern die Daten aufzubereiten, dass sie etwa Krankheiten in ihrer Muttersprache lesen können.

3.2 Umfeld

Das Umfeld in einem Notfall ist nicht vorhersehbar und chaotisch - Notfälle sind Extremsituationen, für den Patienten als auch für den behandelnden Helfer. Obwohl Notfallpersonal extra geschult wird und routiniert im Umgang mit Notfällen ist, sind die wenigsten Fälle gleich und können nicht in der selben Form behandelt werden, da sich Patienten durch physische und psychische Details unterscheiden.

In einem stressigen Umfeld muss die Software mehr denn je den Anwender unterstützen und ihm die Möglichkeit bieten Dinge sehr einfach und ohne große kognitive Last ausführen zu können. Der Anwender soll sich in einer solchen Situation auf seine Aufgabe konzentrieren können und nicht auf die Bedienung einer Software.

3.3 Problemstellung

Bei der Unterstützung von Notfällen durch das Abrufen von personenbezogenen Notfalldaten soll die Behandlung effektivieren und beschleunigen wobei insbesondere Behandlungsfehler durch falsche Medikamentengabe oder Vorhandensein chronischer Krankheiten verringert werden sollen.

Dabei soll die Software in verschiedenen Versionen für unterschiedliche Anwender verfügbar oder konfigurierbar sein, so dass Daten nicht unnötig für eine bestimmte Gruppe angezeigt werden obwohl sie nicht benötigt werden. Weiters soll es möglich sein diese Daten für anderssprachige Systeme lesbar zu machen und so aufzubereiten, dass Personen mit anderen Sprachen die Daten so lesen können, als wären sie in ihrer Muttersprache verfasst. Die Speicherung soll auf möglichst günstiger Hardware erfolgen, so dass die Initialkosten möglichst gering sind und der Einstieg in das System erleichtert wird.

Sicherheitsaspekte des Systems sollen detailliert beleuchtet werden, etwa ob unerwünschtes Auslesen möglich ist und verhindert werden kann.

Auch die Aktualität und Integrität der Daten soll sichergestellt werden.

4 Algorithmen

4.1 NFC Daten Protokoll

Flags	Nachname	Vorname	Adresse	SVNR	Blutgruppe	Extra Count
1 Byte	var	var	var	5 Byte	1 Byte	2 Byte

Daten	Timestamp	CRC16
siehe Tabelle 4.4	8 Byte	2 Byte

Tabelle 4.1: Der Aufbau des NFC Tags

Flags Bit	8	7	6	5	4	3	2	1
	RFU	RFU	RFU	RFU	RFU	RFU	Organspender *0x00* Nein *0x01* Ja	Geschlecht *0x00* Männlich *0x01* Weiblich

Tabelle 4.2: Bit im Flag Feld

Count	String
2 Byte	n Bytes

Tabelle 4.3: Der Aufbau einer var Structure

Identifier	Count	Records
1 Byte	2 Byte	n Bytes

Tabelle 4.4: Der Aufbau der Daten Sektion

Bit	8	7	6	5	4	3	2	1
	RFU	RFU	RFU	RFU	RFU	Disease	Medication	Extra Data

Tabelle 4.5: Bit im Identifier Feld

Bit	8	7	6	5	4	3	2	1
	Blutgruppe				Rhesus		Kell	

Tabelle 4.6: Bit im Blutgruppen Feld

Byte 3	8	7	6	5	4	3	2	1
	RFU			Gruppe A-Z				
Byte 2	8	7	6	5	4	3	2	1
	RFU	Erste Zifferngruppe						
Byte 1	8	7	6	5	4	3	2	1
	RFU	Zweite Zifferngruppe						

Tabelle 4.7: Aufbau eines ICD10 Codes

5 Ergebnisse

5.1 Notfallkarte

Die NFC Tags gibt es beinahe in allen Formen und Ausführungen. Für eine Notfallkarte eignen sich zwei Typen besonders gut: Armbänder und ISO/IEC 7810 Karten der Größe ID-1 („Kreditkartenformat"). Armbänder hat man, solange man sie trägt, bei sich und können im Normalfall leicht gefunden und ausgelesen werden. ISO Karten können in der Geldbörse transportiert werden, ein Gegenstand welcher zur Identifikation von Patienten gesucht wird, da sich hier üblicherweise auch die Personaldokumente befinden.

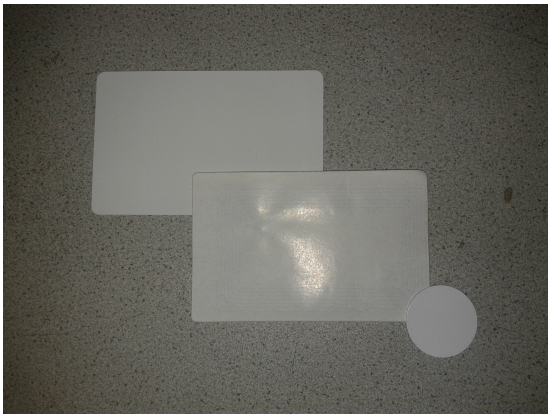


Abbildung 5.1: verschiedene NFC Tags: Karte, Klebetag, Coin-Tag (v.l.n.r.)

Für den Prototypen Test wurden neben den ISO Karten auch aufklebbare NFC Tags im ISO/IEC 7810 Format sowie runde „Coin-Tags" verwendet (siehe Abbildung 5.1). Die NFC Chips selber unterscheiden sich lediglich im Hersteller und sind daher bei allen Typen äquivalent. Im Falle des Prototypen wurde derzeit nur der NFC Type „Vicinity" (NfcV) implementiert. Andere NFC Typen könnten bei Bedarf eingebaut werden um weitere Karten zu unterstüzen.

5.1.1 Verwechselungsschutz

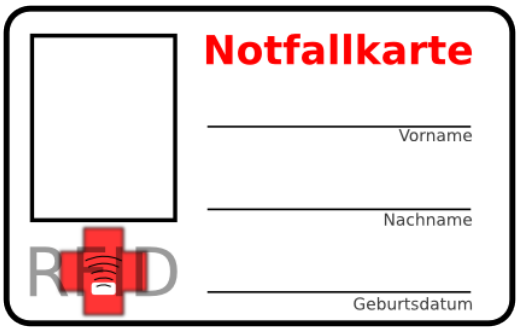


Abbildung 5.2: Prototyp einer Notfallkarte zum Ausdrucken

Da die Notfallkarte prinzipiell jeder eingesteckt haben kann und es Fälle gibt, in denen eine Person mehrere Karten hat, etwa die Eltern für ihre Kinder, muss ein Schutz vor Verwechselung implementiert werden, da sonst die Gefahr einer Fehlbehandlung besteht, welche im schlimmsten Fall mit dem Tod endet.

Ein solcher Verwechselungsschutz wird bei dem Notfalltag mittels eines aufgedruckten Fotos sowie Namen und Versicherungsnummer gelöst. Da ein Foto aufgrund des geringen Speichervolumens der Karte nicht auf dem Tag gespeichert werden kann, ergänzt es die Notfalldaten um ein weiteres wichtiges Merkmal. Name und Versicherungsnummer dienen dem manuellen Abgleich mit den eingelesenen Daten, für den Fall dass mehrere Karten eingelesen werden und so falsche Daten abgelesen werden.

Abbildung 5.3: Die Prototypkarte im Vergleich mit der eCard

Abbildung 5.4: Die Rückseite der Prototypkarte

Die Karte kann dabei immer sehr leicht selbst erstellt werden, da etwa die Front der Karte selber ausgedruckt wird und mittels eines NFC Klebetags vervollständigt wird. Ein Beispiel für eine solche Karte zeigen Abbildungen 5.2, 5.3 und 5.4.

Bei einem Armband können keine Drucksorten aufgebracht werden, daher kann hier kein solcher Schutz verwendet werden. Allerdings sollte ein Armband nur von der Person getragen werden, deren Daten auf dem Tag gespeichert sind. Das mehrere Armbänder gleichzeitig getragen werden, oder die Armbänder zum Beispiel innerhalb der Familie verwechselt werden, kann jedoch nicht ausgeschlossen werden. Hier empfiehlt sich die Verwendung von verschiedenen Armbändern in verschiedenen Farben oder Ausführungen. Da sich die NFC Tags in fast jedes Material integrieren lassen, sollte dies kein schwieriger fertigungstechnischer Vorgang sein.

5.1.2 Implantate

Eine weitere Möglichkeit einen Verwechselungsschutz und gleichzeitig einen Schutz gegen Verlieren der Karte zu implementieren, ist es die Tags zu implantieren. Solche Implantate wurden schon erfolgreich als Bezahlsysteme in Clubs getestet [21] und werden auch für andere Zwecke verwendet. Auch können Do-it-yourself Kits im Internet bestellt werden, um sich selbst die etwa 2x15mm großen Chips zu implantieren [22].

Die Möglichkeiten solcher Implantate sind durchaus sinnvoll, allerdings bietet sich weder ein guter Zugriffsschutz, noch eignen sie sich für die Erforschung von Prototypen. Daher werden sie in dieser Arbeit nicht näher beleuchtet.

Das Protokoll für die Daten ist in Kapitel 4.1 beschrieben. Hierbei wurde versucht so wenig Speicher wie möglich zu verbrauchen, allerdings auch eine gewisse Erweiterbarkeit zu bieten, damit in Zukunft eventuell mehr Daten auf den Tags gespeichert werden können.

Insgesamt können die Basisdaten auf einem 1 Kilobit NFC Tag gespeichert werden, für die kompletten Stammdaten sowie zwei Medikamente und zwei Krankheiten reichen circa 110 Byte. Allerdings könnten multimorbide Personen schnell an die Grenzen eines Tags kommen, da hier unter Umständen viele verschiedene Medikamente eingesetzt werden.

5.1.3 Datenprotokoll

Das NFC Daten Protokoll definiert wie die Daten auf dem NFC Tag gespeichert werden. Dabei wurde insbesondere auf geringen Speicherbedarf geachtet, so dass ein minimales Tag auf einen 1Kbit Tag passt. Der Speicherbedarf eines durchschnittlichen Daten-Tags ist in etwa 80-90 Bytes.

Für den Patienteneintrag werden ICD10 Codes für die Krankheiten verwendet, sowie die Pharmazentralnummer (PZN) für Medikamente.

ICD10 Codes kommen zum Einsatz, da sie sich sehr gut komprimieren lassen und trotzdem recht genaue Angaben über die Krankheit erlauben. Systeme wie SNOMED sind zwar ausführlicher allerdings auch aufwändiger in der Implementation sowie im Betrieb. Auch die Datenbanken würden mehr Speicherbedarf verlangen. Die ICD10 Tabelle, in diesem Falle ICD10 German Modification 2013 Alphabetic Index, verbraucht ca 1.5 Megabyte und beinhaltet mehr als 76000 Einträge. Ein SNOMED System müsste mehrere Millionen an Einträgen verwalten sowie weitere Millionen an Referenzen, was auf einem mobilen Endgerät mit sehr begrenztem Rechenkapazitäten und Speicher unrealistisch ist.

Auch die Pharmazentralnummern bieten gute Komprimierbarkeit und sind zudem in Österreich auf jedem in einer Apotheke verkauften Medikament abgedruckt. Dadurch kann ein Anwender seine Medikamente sehr einfach einscannen und wird in jedem Fall das richtige Medikament in seiner Tabelle speichern. Dadurch werden Fehler durch falsche Medikamentennamen vermieden und durch die einheitliche Nummer könnten Expertensysteme angebunden werden, welche etwa Arzenimittelwechselwirkungen von verschiedenen Wirkstoffen aufzeigen.

Das generelle Layout des NFC Tags wird in Tabelle 4.1 beschrieben. Dabei kommen für alle variablen Felder Strings mit einem Längen-Marker zum Einsatz, welche in Tabelle 4.3 erläutert werden.

Abschließend kommt ein 16-bit Cyclic redundancy check (CRC16) Hash zum Einsatz, welcher über die gesamten gesendeten Daten berechnet wird um Fehler beim Auslesen zu erkennen oder beim Speichern zu vermeiden.

Header

Der Header gibt dabei an, welche der optionalen Felder in der Datensektion angezeigt werden. Anschließend an den Header sind die Flags, welche binär kodierte Informationen speichern.

Data Field

Die Datenstruktur kann verschiedene Daten beinhalten und könnte bei entsprechender Anpassung im Header bis zu 256 verschiedene Datentypen speichern. Derzeit sind drei verschiedene Datentypen implementiert, welche die Medikation als PZN, die Krankheiten als ICD10 (siehe Tabelle 4.7) oder einen Freitext als UTF-8 kodierten Text speichern, ähnlich dem var-Feld (siehe Tabelle 4.3). Das Identifier-Feld (Tabelle 4.5) gibt dabei an, welcher Datenwert gespeichert wird. Das Count-Feld gibt an, wie viele Bytes im Record stehen. Somit ergibt sich aus diesem Wert auch die Anzahl der PZN oder ICD10 Einträge, da jeder PZN Eintrag jeweils 4 Byte und jeder ICD10 Eintrag jeweils 3 Byte hat. Diese Art der Kennzeichnung hat zusätzlichen Nutzen in der Aufwärtskompatibilität. Eine Software, die neue Identifier nicht versteht, kann trotzdem die Länge des danach kommenden Records bestimmen, ihn beim Auslesen überspringen und eine Warnung ausgeben. Somit können Tags auch gelesen werden, wenn sie mit einer neueren Protokollversion erstellt wurden oder die Software am Gerät veraltet ist.

5.1.4 Sicherheit der Daten

Ein wesentlicher Punkt ist die Sicherheit der gespeicherten Daten. Da es sich um sehr sensible Daten handelt ist die Tatsache, dass die Daten kontaktlos ausgelesen werden können, besonders

kritisch. NFC Tags haben zwar nur eine geringe Reichweite, allerdings spielt hier besonders die Antennengröße eine Rolle. Somit wäre es denkbar, dass ein Angreifer mit einer großen Antenne auch Reichweiten von 50cm oder mehr schaffen kann, was zum Auslesen der Karte reicht [23]. Tests mit einem Smartphone (Nexus S) zeigen, dass die Entfernung zur Karte sehr gering, in etwa 4-5cm, sein muss, damit diese ausgelesen werden kann. Zudem ist die Dauer für das Auslesen relativ lang, da die meisten NFC Tags nur wenige Byte pro Sekunde an Datenrate aufbringen können. Dennoch ist das Risiko des unerlaubten Auslesens gegeben und sollte minimiert werden.

5.1.5 Verschlüsselung

Verschlüsselung scheint oftmals der hoffnungsvolle Weg, allerdings erzeugt eine Verschlüsselung wiederum neue Probleme, welche gelöst werden müssen. Der elektronische Reisepass definiert etwa mehrere Zugriffsebenen, welche, je nach Art der Daten, entweder verschlüsselt sind oder nicht [24]. Somit sind die Daten, welche auch in Papierform auslesbar sind, ebenfalls offen per RFID auszulesen. Ähnliche Überlegungen gelten für die Notfallkarte, da eine Notfallkarte in Papierform, sollte sie verloren gehen oder gestohlen werden, ebenfalls komplett ausgelesen werden kann. Der elektronische Reisepass verwendet die Basic Access Control (BAC) um Daten zu sichern, welche nur in Kombination mit dem physischen Ausweis ausgelesen werden sollen. Dabei werden Informationen, welche auf dem Pass aufgedruckt sind, verwendet, um die Daten zu verschlüsseln. Somit muss ein Angreifer über den Chip sowie den physischen Pass verfügen, um die Daten zu erhalten. Diverse Quellen geben allerdings an, dass die Entropie, welche diese Merkmale erzeugen, selbst bei einem elektronischen Pass schon sehr gering ist und zwischen 38 und 53 bit, anstatt der erwarteten 73 bit liegt [25] [26] [27] [28]. Daher ist es unbedingt erforderlich, dass eine solche Verschlüsselung nicht durch Schlüssel beeinträchtigt wird, welche erratbar sind. Ähnliche Probleme hatte auch schon OpenSSL unter Debian [29].

Ein einfaches Verschlüsselungsverfahren bietet der Advanced Encryption Standard (AES). Im einfachsten Fall kommen hier Block- und Schlüsselgrößen von 128 bit zum Einsatz. Im Falle der NFC Tags sollte eine möglichst kleine Blockgröße gewählt werden, damit nicht unnötig viel Platz durch Padding Zeichen verschwendet wird, da die Padding Größe im Worst Case $N_B - 1$ Bit und im Average Case $N_B/2$ beträgt. Ein 128bit Key ergibt in hexadezimaler Darstellung eine 32 Zeichen lange Folge, beziehungsweise bei Verwendung aller alphabetischen Zeichen und Nummern, abzüglich ähnlicher Zeichen wie etwa „0" und „O" 23 Zeichen (siehe Anhang A.1). Ein solch langer Schlüssel birgt jedoch die Gefahr des häufigen fehlerhaften Eingabe und somit eines Zeitverlustes im Notfall. Idealerweise sollte der Schlüssel nur 4 bis 5 Zeichen lang sein, hätte also nur noch 23 bis 28 bit Länge. Ein solcher Code ist wiederum gut geeignet um ihn mittels Brute-Force zu errechnen, Berechnungen sind in Anhang A.2 angeführt.

5.1.6 PKI

Einer der sinnvollsten Wege der Verschlüsselung führt über eine PKI, wobei jeder Teilnehmer einen eigenen Schlüssel erhält und Gruppen von Notfallhelfern, wie Sanitäter oder Ärzte, die Berechtigung erhalten, alle Karten zu entschlüsseln. Dieses System bringt die größtmögliche Sicherheit bei bester Kontrolle der Zugriffe und Berechtigungen. Allerdings sind auch viele Bedingungen an das System geknüpft, etwa ein Internetzugang, um Schlüssel der PKI abzufragen, sowie eine große Anzahl an Schlüssel der Rettungsdienste und Teilnehmer, welche in dieser PKI gespeichert werden. Ein solches System wird in [30] beschrieben, wobei hier der Patient bestimmten Gruppen im Vorhinein den Zugriff erlauben kann. Probleme treten auf, wenn berechtigte Schlüssel gestohlen werden, etwa die eines Rettungsdienstes. Hier könnten Massen an Tags ausgelesen werden. Auch müssten vor Urlauben oder Reisen die im Zielland ansässigen Rettungsdienste und Kran-

kenhäuser authentifiziert werden um im Notfall die Daten auslesen zu können. Dieses System funktioniert nur, wenn im Vorhinein klar ist, wer diese Daten einmal lesen soll.

Generell scheint eine PKI das beste Konzept zu sein, allerdings sind die Einschränkungen für ein Notfallsystem derzeit noch zu hoch.

5.1.7 Physischer Leseschutz

Schon Peter Schaar und Jörg Ziercke [31] schlugen im Zuge der Diskussion um den neuen elektronischen Reisepass vor, ihn einfach in Alufolie zu verpacken. Obwohl seinen Reisepass in Alufolie einpacken eher nach Bastelstunde klingt, ist das Verfahren durchaus sinnvoll. Nachdem der Pass eingepackt wurde, kann man ihn selbst bei direktem Anhalten an den RFID Leser nicht mehr auslesen. Gleiches gilt für die NFC Tags. Ein wie in Abbildung 5.5 eingewickelter elektronischer Reisepass, beziehungsweise ein NFC Tag, lassen sich, auch wenn sie nur teilweise eingewickelt wurden, nicht mehr auslesen.

Dass dieses Problem auch schon von der Wirtschaft erkannt wurde, zeigen RFID sichere Geldbörsen [32] und Reisepasshüllen [33].

Abbildung 5.5: Ein in Alufolie gewickelter Reisepass und NFC Tag

Daher ist ein Verfahren bei dem das Notfalltag in einer lesegeschützten Hülle aufbewahrt wird, besser geeignet als eine Verschlüsselung mittels aufgedrucktem Code. Im Falle des Verlustes einer Karte ist zwar auch nicht gewährleistet, dass die Daten sicher sind, allerdings ist das Verfahren sehr viel einfacher und unkomplizierter in der Anwendung.

Eine solche Hülle lässt sich für den Massenmarkt sehr einfach fertigen und mit der Karte ausliefern.

5.2 Prototyp der Applikation

Zum einfachen Testen wurde die Patienten- und Notfallapp in einem APK, also einer App, zusammengepackt. Im Realbetrieb würde man verschiedene, auf die Kunden zugeschnittene Apps entwickeln, etwa auch um zusätzliche Workflows und Datenanbindungen zu integrieren. Denkbar wäre hier etwa die Anbindung an ein Krankenhausinformationssystem (KIS), um im Notfall die Daten direkt einzuspielen und um die aktuellen Vitalparameter zu ergänzen.

5.3 Patienten App

Die Patienten App bietet ein Interface zum Erstellen der Tags sowie zum Verwalten seiner Notfalldaten. Die App soll dabei ein möglichst einfaches Interface zum Einstellen der Daten haben, allerdings auch alle notwendigen Datensätze speichern können. Dennoch sollte die Eingabe der Daten unter Umständen von einem Arzt begleitet werden, beziehungsweise durch einen Arzt überprüft werden. Die selbe Praktik wird auch bei der Notfallkarte verwendet, um Fehleinträge zu vermeiden.

5.3.1 Workflow

Notfallkarte erstellen

Der Patient gibt zunächst alle seine Stammdaten ein (Abbildung 5.7). Zusätzlich kann ein Freitext angegeben werden, etwa für Notfallnummern oder wichtige Hinweise, welche nicht von dem Standardformular erfasst werden. Zu den Stammdaten gehören:

- Geschlecht
- Vorname
- Nachname
- Sozialversicherungsnummer
- Blutgruppe, Rhesus- und Kellfaktor
- Organspender

Nachdem die Stammdaten eingegeben wurden, können Medikamente und Krankheiten (Abbildung A.1) eingegeben werden. Dazu wird ein neues Fenster geöffnet, in dem die notwendigen Einstellungen vorgenommen werden. Danach kehrt der Anwender wieder zum Hauptbildschirm zurück.

Zum Schluss werden die Daten auf dem NFC Tag gespeichert (Abbildung A.3 und A.4). Dabei können die Daten für später am Smartphone gespeichert werden, etwa um später eine andere Medikation einzustellen oder den Freitext bequem zu ändern. Ein Programmablaufdiagram des Workflows eines Patienten ist in Abbildung 5.6 gezeigt.

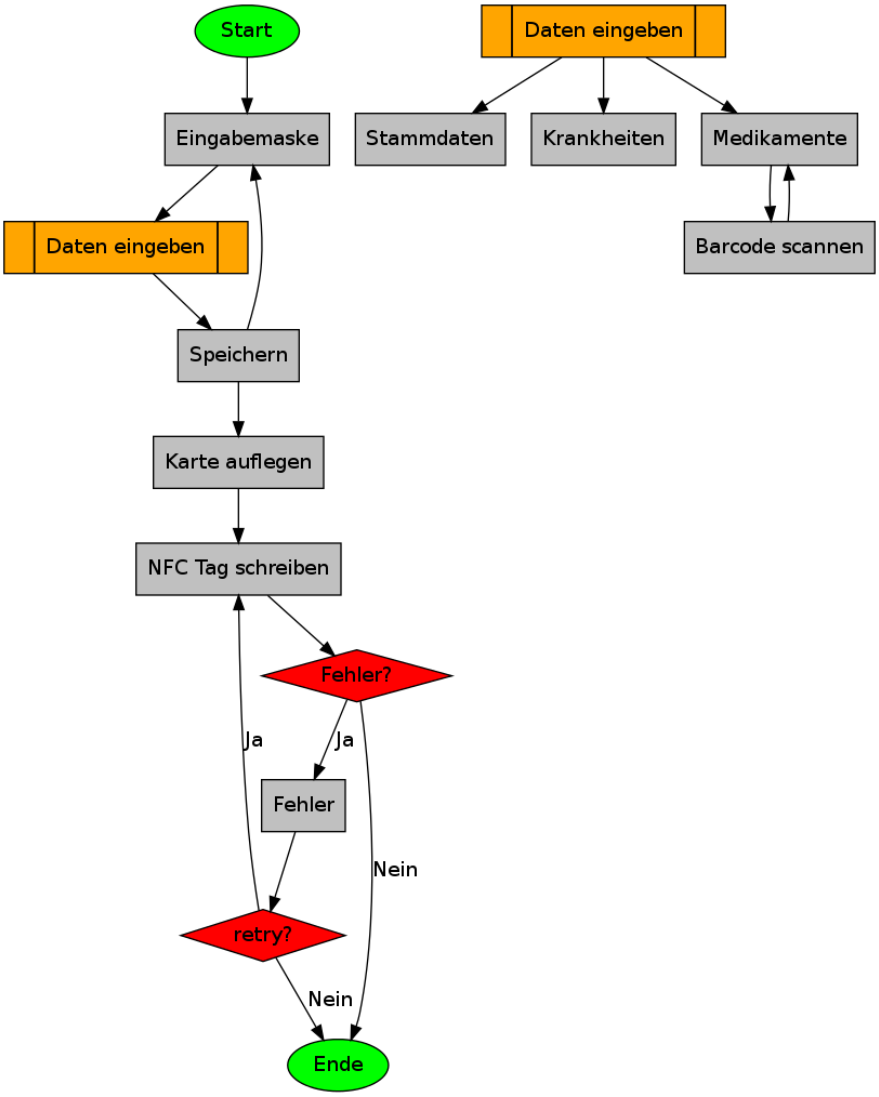


Abbildung 5.6: Workflow für den Patienten

5.3.2 Semantische Übersetzung von Krankheiten

Die ICD10 Liste des DIMDI [34] enthält neben der Zuordnung von ICD Codes auch Einträge, welche rein als Verweis funktionieren. So werden sehr viele verschiedene Namen von Krankheiten erfasst und leiten auf den selben Code weiter.

Ein Beispiel für eine solche Weiterleitung ist der ICD Code *E10.90*, welcher einer Typ-1 Diabetes mellitus entspricht wird in Tabelle 5.1 dargestellt.

Durch diese Mehrfacheinträge ist es möglich, dass auch Personen, welche kein medizinisches Wissen haben, ihre Krankheit finden. Für seltenere Krankheiten existieren jedoch weniger doppelte Einträge, allerdings könnten diese in einer Produktivversion der Software hinzugefügt werden. Alternativ kann die Eingabe auch durch den Hausarzt erfolgen, welcher die genauen Bezeichnungen kennt.

5.3.3 Pharmazentralnummern

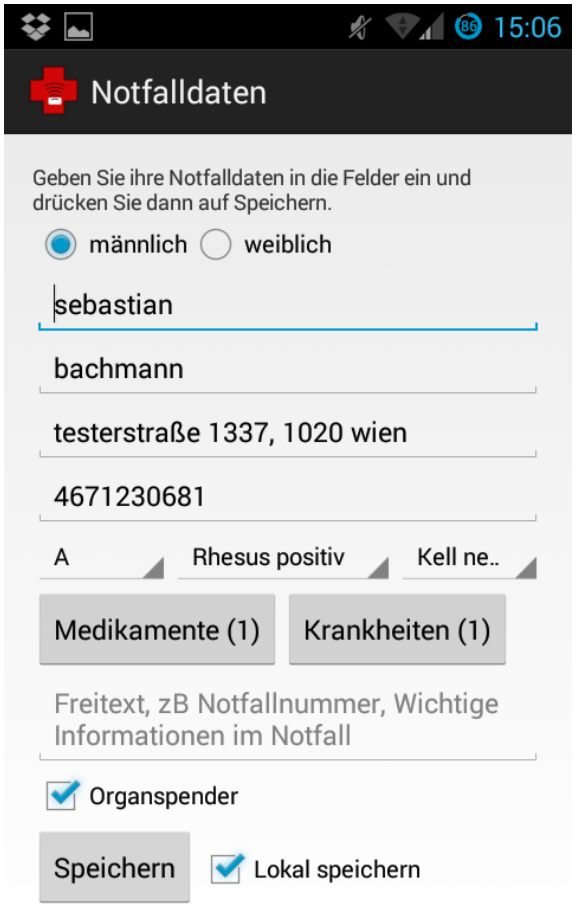


Abbildung 5.7: Eingeben der Stammdaten

Die Pharmazentralnummern ändern sich kontinuierlich und werden in Österreich von der Firma Datacare verwaltet. Diese sendet, etwa bei Apotheken, diese Daten jeden Tag an die Systeme welche die Nummern verwenden verwenden. Für den Falle unserer Software reicht eine Liste aus, welche nicht aktualisiert wird. Für eine produktive Software sollten diese Aktualisierung jedoch nachgerüstet werden.

Abbildung 5.8: Ein PZN Barcode

Da die PZN als Barcode (Abbildung 5.8) auf der Produktpackung angegeben wird, ist die Verwendung eines Barcode Scanners zum schnellen und sicheren Einlesen der Daten angebracht.

5.4 Notfall App

Die Notfall App ist das Interface für das Notfallpersonal um die App auszulesen. Die Ansicht auf die Daten soll für jede Rolle unterschiedlich sein und gefiltert Daten anzeigen.

Für den Prototypen wurden drei verschiedene Ansichtsmodi implementiert, welche sich je nach Einsatzzweck erweitern oder ändern lassen. Die Auswahl der Daten wird in Tabelle 5.2 dargestellt.

ICD10 Code	Name
E10.90	Brittle diabetes
E10.90	Diabetes mellitus Typ 1
E10.90	Diabetes mellitus Typ 1 beim Erwachsenen
E10.90	Diabetes mellitus Typ 1a
E10.90	Diabetes mellitus Typ 1b
E10.90	Diabetes mellitus Typ I
E10.90	IDDM [Insulin dependent diabetes mellitus]
E10.90	Insulinabhängiger Diabetes mellitus Typ 1
E10.90	Insulinbehandelter Typ-1-Diabetes mellitus
E10.90	Insulinbehandelter Typ-1-Diabetes mellitus ohne Komplikation
E10.90	Insulinpflichtiger Typ-1-Diabetes mellitus
E10.90	Juveniler Diabetes mellitus
E10.90	Kongenitaler Diabetes mellitus
E10.90	Labiler Diabetes mellitus
E10.90	LADA (Latent (or late-onset) autoimmune diabetes of adulthood)-Diabetes mellitus
E10.90	Latenter autoimmun-assoziierter Diabetes mellitus
E10.90	Primär insulinabhängiger Diabetes mellitus
E10.90	Primär insulinabhängiger Diabetes mellitus ohne Komplikation
E10.90	Primär insulinpflichtiger Diabetes mellitus
E10.90	Typ-1-Diabetes mellitus - s.a. Diabetes mellitus, Typ-1-
E10.90	Typ-1-Diabetes mellitus ohne Komplikation

Tabelle 5.1: Übersetzung eines ICD Codes

5.4.1 Workflow

Der Workflow für das medizinische Person ist sehr einfach und in Abbildung 5.9 dargestellt. Die Person muss nur seine Rolle auswählen, dies könnte in Zukunft etwa eine eigene NFC Authentifizierungskarte oder ein anderes System gelöst werden. Danach ist das System schon auf das Lesen von NFC Karten eingestellt. Wird eine Karte erkannt, wird diese ausgelesen und der Inhalt angezeigt.

Gruppe	Datensatz	Sanitäter	Arzt	Identifikation
Stammdaten	Name	x	x	x
	Vorname	x	x	x
	Alter	x	x	x
	Freitext	x	x	x
Erweiterte Stammdaten	Adresse		x	x
	SVNR		x	x
	Blutgruppe		x	x
	Organspender		x	x
	Krankheiten	x	x	
	Medikation		x	

Tabelle 5.2: Daten und Ansichten

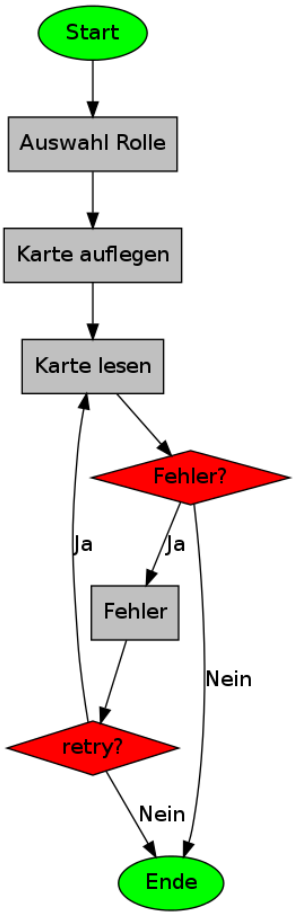


Abbildung 5.9: Workflow für das medizinische Personal

5.4.2 Ansicht: Sanitäter

Der Sanitäter braucht nur wenige Informationen, da sein Handlungsspielraum begrenzt ist. Da er keine Medikamente geben darf, muss er auch nicht über mögliche Wechselwirkungen informiert werden. Daher werden für den Sanitäter nicht die eingenommenen Medikamente angezeigt. Da ein Rettungssanitäter nach §9 des SanG [35] nur Wiederbelebungsmaßnahmen treffen darf, reichen für ihn die Ansicht der chronischen Krankheiten aus, um die bestmögliche Entscheidung zu treffen. Auch wird Name und Alter der Person angezeigt, da diese Informationen im Notfall nützlich sein können.

Notfallsanitäter

Im Gegensatz zum Rettungssanitäter, darf der Notfallsanitäter gewisse Medikamente selbstständig geben [36]. Dies könnte in Verbindung mit der Notfallkarte genutzt werden, um auf typische Wechselwirkungen mit Medikamenten oder spezielle Wirkungen durch Krankheiten in der App hinzuweisen. Solche Expertensysteme könnten bei Bedarf integriert werden.

Eine mögliche Integration stellt die Metabolism & Transport Drug Interaction Database (DIDB) dar, ein System der Universität Washington zur Abfrage von Arzneimittelwechselwirkungen [37].

5.4.3 Ansicht: Arzt

Da ein Arzt oder Notarzt notwendigerweise berechtigt ist Medikamente zu verabreichen, ist es für ihn essentiell zu wissen, ob die Medikation des Patienten nicht gewünschte Nebenwirkungen hervorrufen können. Ein Beispiel für eine solche Wechselwirkung könnte die Gabe von Propofol bei Patienten sein, welche Fentanyl als Schmerzmittel [38] bekommen. Die Folge könnte ein Atemstillstand sein [39], welcher in einer Notsituation zu weiteren Umständen führt.

5.4.4 Ansicht: Identifizierung

Diese Ansicht dient lediglich dazu, die Basisinformation der Karte anzuzeigen. Dies kann nützlich sein, wenn verschiedene Karten ohne Aufdruck zugeordnet werden müssen oder zur Überprüfung des letzten Aktualisierungsdatums der Karte.

Diese Ansicht sollte in einer Produktiven Version in die Patienten Applikation eingebaut werden um seine eigene Karte zu verifizieren.

5.5 Soziale Aspekte

In den letzten Jahren haben sich Diskussionen um Privatsphäre und Datenspeicherung gehäuft. Allein die Einführung des elektronischen Reisepasses hat viele Kritiker und Befürworter auf den Plan gerufen. Auch lässt sich diese Diskussion mit der einer kontaktlosen Notfallkarte am besten vergleichen, da das technische Fundament das gleiche ist. Zudem werden auf beiden Karten persönliche Daten, im Falle des Reisepasses die Fingerabdrücke, gespeichert.

Die ELGA hat zudem in Österreich viel Kritik hinnehmen müssen, da es hier ebenfalls datenschutzrechtliche Bedenken gab.

Besonders wenn persönliche Daten von Dritten, etwa einem Staat, erhoben werden, ist das eigene Empfinden oft anders, als wenn man seine persönlichen Daten etwa an soziale Netze weitergibt. So sind Datenschutzrechtliche Bedenken etwa weit weniger gegen Facebook gerichtet als gegen den Staat, der eine Gesundheitsakte einführen möchte.

Im Falle einer Notfallkarte sind die Datenschutzbedenken von jeder Person selber abzuwägen. Jeder Person ist es freigestellt, so viele Daten wie sie für richtig halten, auf der Karte zu speichern und somit im Notfall einem Helfer zur Verfügung zu stellen. Somit muss auch selbst überlegt werden, ob der Nachteil eine solche Karte zu verlieren, das Risiko dass es zu Komplikationen im Notfall kommt überragt.

6 Zusammenfassung und Ausblick

6.1 Vereinfachte Verfügbarkeit von Patientendaten

Durch den Einsatz von NFC Tags können in Notfällen die Patientendaten schneller und einfacher dem Helfer übermittelt werden. Dadurch werden Fehler minimiert und somit effektiv Leben gerettet.

Vorteile bietet eine solche Karte allerdings nicht nur in Notfällen, sondern auch bei der Vorsorge oder für den privaten Gebrauch, etwa wenn mögliche Wechselwirkungen mit Medikamenten abgefragt werden sollen. Eine solche App ließe sich demnach sehr gut in bestehende Gesundheitsplattformen integrieren.

6.1.1 Evaluierung der NFC Karten

Im Vergleich zu Papierkarten oder Online Systeme stellen sich bei NFC Karten einige wichtige Vorteile heraus. Dabei zeigt sich, dass insbesondere ein Geschwindigkeitsvorteil gegeben ist. Durch die NFC Technik können die Karten nicht nur schneller ausgelesen werden, als dies bei Online Systemen möglich wäre, auch ist kein Online Zugang erforderlich, was insbesondere im ländlichen Raum von Vorteil ist. Auch können Daten so gespeichert werden, dass sie in anderen Ländern ohne große Probleme ausgelesen werden können und dem Mediziner in einer für ihn verständlichen Form dargestellt werden.

Die Sicherheit liegt ungefähr auf dem Niveau einer Papierkarte, da die Daten im Klartext gespeichert werden und somit im Verlustfall für den Finder auslesbar sind. Gegenüber Online Karten, welche Sperrmechanismen anbieten, könnten NFC Karten nur durch PKI Systeme einen Vorteil erzielen. Hier wäre vollständige Kontrolle der Daten gewährleistet. Vor und Nachteile der NFC Technik gegenüber anderen gängigen Techniken sind in Tabelle 6.1 aufgeführt.

	NFC Tag	**Papierkarte**	**Online System**
Geschwindigkeit	Schnell	Mittel	Abhängig von der Internetverbindung
Authentizität	X	X	X
Verlustschutz	mit PKI	-	X
Integrität	X	-	X
Aktualität	X	X	X
Strukturierung	X	-	X
Transitivität	X	-	X

Tabelle 6.1: Vor- und Nachteile von NFC Karten gegenüber gängigen Techniken

6.1.2 Datenprotokoll

Für die Speicherung der Daten auf der Karte wurde ein sehr einfaches und gut erweiterbares Protokoll entwickelt, mit dem es möglich ist, alle Daten, welche in der App eingegeben werden auch auf kleinere (128 Byte) Karten zu spielen. Dies ist wichtig, da NFC Tags für den Endanwender im

Vergleich zur Massenbestellung noch relativ teuer sind und der Markt eher von kleineren Kartengrößen dominiert wird.

Sollten für weitere Einsatzszenarien andere Daten erforderlich sein, können diese auch in das Protokoll eingepflegt werden, ohne dass bei einem Versionswechsel Karten nicht mehr lesbar werden und Smartphones nicht mehr korrekt lesen könnten. Das Protokoll wurde insbesondere auf den Aspekt der Auf- und Abwärtskompatibilität erstellt.

6.1.3 Datensicherheit

Im Zuge der Entwicklung des Datenprotokolls wurden einige Optionen der Datensicherheit evaluiert. Die verschiedenen Verfahren sind in Tabelle 6.2 dargestellt.

Verfahren	**Vorteile**	**Nachteile**
Physischer Ausleseschutz	Einfache Implementierung kann mit Hülle gar nicht gelesen werden Schnelles Auslesen in Notfallsituation	kann bei Verlust ausgelesen werden
Verschlüsselung durch aufgedruckten Schlüssel	Vollständige Verschlüsselung der Karte relativ schnelles Auslesen bei kurzem Schlüssel	Kann bei Verlust ausgelesen werden Fehleranfälligkeit bei langem Schlüssel Kurzer Schlüssel ist leicht errechenbar
Verschlüsselung durch PKI	Sicheres Verfahren Personengenaue Rechtevergabe Karte kann bei Verlust gesperrt werden	Aufwändiges Setup Laufende Kosten für Infrastruktur Funktioniert nicht länderübergreifend

Tabelle 6.2: Gegenüberstellung der Datensicherheitsverfahren

Daraus wird ersichtlich, dass sich ein einfaches Umhüllen der Karte mittels Aluminiumfolie oder ähnlichen Materialien am besten eignet, da die Kosten und Aufwendungen, welche eine PKI mit sich ziehen würde, eine solche nicht rechtfertigen. Eine solche Hülle aus Plastik mit einer leitenden Schicht wäre so dünn, dass die Karte immer noch überall eingesteckt werden kann.

6.1.4 Einsatz einer Android App

Das Android System eignet sich aufgrund der Vielzahl von unterstützten Geräten ideal zur Entwicklung von Applikationen, welche einer breiten Masse zugänglich sein sollen. Die App ist so gestaltet, dass sie in zwei Versionen zur Verfügung steht, jeweils eine für den Endanwender und eine für das Medizinische Personal.

Viele neue Geräte verwenden mittlerweile die NFC Technik, so dass es einem Endanwender durchaus möglich ist, die Karten selber zu beschreiben und auch aktuell zu halten. Zu diesem Zweck werden alle Daten welche auf dem NFC Tag gespeichert werden, auf Wunsch auch am Gerät selber gespeichert, um sie später schneller verändern zu können.

Datensatz	Einsatzzweck
Behandelnde Ärzte und Institute	Zur Abklärung von Behandlungen und Anforderung von Gesundheitsdaten
Aktuelle Gesundheitsdaten	Zur besseren Diagnose
Foto	Zur genauen Identifizierung
In Case of Emergency Kontakte	Zur Verständigung von Angehörigen
Urlaubsdaten	Um im Urlaub verunglückte Personen besser zuordnen zu können (Reisegruppen, Hotels, ...)
Versicherungsdaten	Etwa Alpenvereinszugehörigkeit oder Sonderversicherungen

Tabelle 6.3: Mögliche zusätzliche Datensätze auf der Notfallkarte

Dabei wurde insbesondere Wert auf gute Usability geachtet, damit auch medizinisch nicht gebildete Personen ihre Daten eintragen können. Medikamente werden etwa über einen Barcode Scanner erfasst, somit wird auf der Karte das exakte Medikament gespeichert und nicht nur der Name des Wirkstoffes.

Auch ist es technisch nicht versierten Personen möglich, ihre Medikamente einzulesen, ohne den genauen Wortlaut des Wirkstoffes oder des Medikamentes selber zu kennen.

6.2 Aussicht

Neben dem Haupteinsatzzweck der Applikation und der Notfallkarte lassen sich weitere Gebiete finden, in denen eine sinnvolle Nutzung denkbar ist. Durch die fortschreitende Entwicklung des „pervasive computing" lassen sich insbesondere hier gute Usecases erstellen.

Auch könnten weitere Daten mit der Karte verknüpft werden um bessere Diagnosen stellen zu können. Dies könnte insbesondere über den Einsatz von Körpersensoren geschehen, welche aktuelle Vitalwerte an das Android Device senden. Die Daten könnten später in Verbindung mit der Notfallkarte ausgelesen werden.

6.2.1 Weitere Verwendung der Karte

Neben der Speicherung von Notfalldaten könnte mit größeren Karten auch eine gewisse Krankenakte gespeichert werden. So kann ein behandelnder Arzt auch auf alte Daten zurückgreifen und somit Fehlentscheidungen vorbeugen. Jedoch würde hier die selbe Diskussion um Gesundheitsdaten angefacht werden, wie es mit der ELGA geschah. Fakt ist, dass ganze Krankheitshistorien nicht frei für jeden zugänglich abgespeichert werden dürfen, da das Missbrauchspotential zu hoch ist. Allerdings könnten auf der Karte Referenzen zu anderen behandelnden Ärzten und Instituten gespeichert werden, welche im Notfall kontaktiert werden können. Jedoch werden pro Adresse mit Telefonnummer und E-Mail Adresse gute 100 Byte fällig, so dass dies nur mit einer entsprechend großen NFC Karte möglich ist. Weitere speicherbare Datensätze sind in Tabelle 6.3 dargestellt. Derzeit könnten aber solche Daten schon als Freitext eingegeben werden und müssten nicht in das Datenprotokoll aufgenommen werden.

6.2.2 Weitere Verwendung der App

Neben der physischen Karte lässt sich auch die App in weiterer Folge verwenden um neue Einsatzgebiete zu erschließen.

pervasive computing

Durch den Einsatz von Bluetooth NFC Geräten könnten Sensorinformationen periodisch von der App erfasst werden und schlussendlich auch auf die Notfallkarte gespeichert werden. Als sinnvolle Geräte könnten zum Beispiel Fingerpulsoxymeter, Herzfrequenzmesser, Körpertemperatursensoren und andere Messgeräte genannt werden. Aufgrund der rasanten Entwicklung von Smartwatches oder Datenbrillen, könnten solche Geräte bald schon zur Standardausrüstung gehören und die Lebensweise nachhaltig verändern. Grundlegender Vorteil einer solchen Lösung wäre, dass die Daten von Risikopatientengruppen immer sofort auf der Notfallkarte landen und auch über das Internet behandelnden Ärzten zur Verfügung gestellt werden können.

Notfalldaten am Gerät

Neben der dynamischen Generierung von Daten können aber auch statisch einmalig erfasste Daten einen sinnvollen Nutzen bringen. So könnten die Daten durch die Notfall-Applikation abgerufen werden und nicht nur über die Karte. Dies würde insbesondere Personen mit Smartphones ohne NFC Unterstützung helfen, ihre Daten immer präsent zu haben.

Entscheidender Nachteil wäre das der Akku eines mobilen Endgerätes irgendwann leer ist und die meisten Geräte nicht gegen schwere Erschütterungen oder Wasser abgesichert sind. Bei einem Unfall treten aber solche Dinge durchaus auf und könnten somit das Gerät und die Daten zerstören - eine NFC Karte würde solche Einwirkungen im Normalfall überstehen.

Literatur

Wissenschaftliche Literatur

[2] P. Hien. “Praktische Pneumologie”. In: SpringerLink : Bücher. Springer, 2012. Kap. 45, S. 353–356. ISBN: 9783642102097. URL: http://books.google.at/books?id=NnvOk-jvdlIC.

[3] Jörg Schimpf, Dietmar Craß und Verena Sollmann. “Komplikationen und Notfälle”. German. In: *Kompendium Kinderanästhesie*. Hrsg. von Jörg Schimpf, Dietmar Craß und Verena Sollmann. Springer Berlin Heidelberg, 2012, S. 170–201. ISBN: 978-3-642-16846-8. DOI: 10.1007/978-3-642-16847-5_18. URL: http://dx.doi.org/10.1007/978-3-642-16847-5_18.

[7] M. Kawamoto u. a. “An implementation of a semantic associative search space for medical document databases”. In: *Applications and the Internet Workshops, 2004. SAINT 2004 Workshops. 2004 International Symposium on*. 2004, S. 488–493. DOI: 10.1109/SAINTW.2004.1268678.

[16] 46halbe starbug. “Spaß mit dem ePass”. In: *Die Datenschleuder* 87 (), S. 5–7. URL: http://chaosradio.ccc.de/media/ds/ds087.pdf.

[21] K. Michael und M. G. Michael. “The diffusion of RFID implants for access control and epayments: A case study on Baja Beach Club in Barcelona”. In: *Technology and Society (ISTAS), 2010 IEEE International Symposium on*. 2010, S. 242–252. DOI: 10.1109/ISTAS.2010.5514631.

[23] Z. Kfir und A. Wool. “Picking Virtual Pockets using Relay Attacks on Contactless Smartcard”. In: *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*. 2005, S. 47–58. DOI: 10.1109/SECURECOMM.2005.32.

[24] Harald Welte. “Inside ePassports”. In: *Die Datenschleuder* 87 (), S. 17–19. URL: http://chaosradio.ccc.de/media/ds/ds087.pdf.

[25] A. Juels, D. Molnar und D. Wagner. “Security and Privacy Issues in E-passports”. In: *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*. 2005, S. 74–88. DOI: 10.1109/SECURECOMM.2005.59.

[26] Dario Carluccio u. a. “E-Passport: The Global Traceability Or How to Feel Like a UPS Package”. In: *Information Security Applications*. Hrsg. von JaeKwang Lee, Okyeon Yi und Moti Yung. Bd. 4298. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2007, S. 391–404. ISBN: 978-3-540-71092-9. DOI: 10.1007/978-3-540-71093-6_30. URL: http://dx.doi.org/10.1007/978-3-540-71093-6_30.

[27] Gildas Avoine, Kassem Kalach und Jean-Jacques Quisquater. “ePassport: Securing International Contacts with Contactless Chips”. In: *Financial Cryptography and Data Security*. Hrsg. von Gene Tsudik. Bd. 5143. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2008, S. 141–155. ISBN: 978-3-540-85229-2. DOI: 10.1007/978-3-540-85230-8_11. URL: http://dx.doi.org/10.1007/978-3-540-85230-8_11.

[28] Tom Chothia und Vitaliy Smirnov. “A Traceability Attack against e-Passports”. In: *Financial Cryptography and Data Security*. Hrsg. von Radu Sion. Bd. 6052. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2010, S. 20–34. ISBN: 978-3-642-14576-6. DOI: 10.1007/978-3-642-14577-3_5. URL: http://dx.doi.org/10.1007/978-3-642-14577-3_5.

[30] S. Dünnebeil u. a. “Encrypted NFC Emergency Tags Based on the German Telematics Infrastructure”. In: *Near Field Communication (NFC), 2011 3rd International Workshop on*. 2011, S. 50 –55. DOI: 10.1109/NFC.2011.18.

Online Referenzen

[1] Statistik Austria. *IKT Einsatz in Haushalten 2013*. Nov. 2013. URL: http://www.statistik.at/web_de/statistiken/informationsgesellschaft/ikt-einsatz_in_haushalten/022210.html.

[4] Medizinische Fakultät Universität Düsseldorf-Essen Skillslab. *Anamnese*. März 2013. URL: http://www.uni-due.de/medizinstudium/skillslab/skripte/anamnese.pdf.

[5] MCW Handelsgesellschaft mbH. *Notfallkarte*. Aug. 2103. URL: http://www.notfallkarte.at.

[6] Kirchheim Verlag. *Internationaler Notfallausweiß*. Aug. 2103. URL: http://www.kirchheim-verlag.de/home/news-details-aktuell/article/internationaler-notfallausweis.html.

[8] Bundesministerium für Gesundheit. *ICD10 BMG 2013*. Nov. 2013. URL: http://bmg.gv.at/cms/home/attachments/1/1/2/CH1241/CMS1287572751172/icd-10_bmg_2013_-_systematisches_verzeichnis.pdf.

[9] DIMDI. *ICD10 German Modification*. Nov. 2013. URL: http://www.dimdi.de/static/en/klassi/icd/icd10/index.htm.

[10] Wikipedia. *ICD-10*. Nov. 2013. URL: http://de.wikipedia.org/wiki/ICD-10.

[11] DIMDI. *Downloadcenter ICD10-GM*. Nov. 2013. URL: http://www.dimdi.de/dynamic/de/klassi/downloadcenter/icd-10-gm/version2014/.

[12] IHTSDO. *About SNOMED CT*. Nov. 2013. URL: http://www.ihtsdo.org/snomed-ct/.

[13] IHTSDO. *SNOMED CT Components*. Nov. 2013. URL: http://www.ihtsdo.org/snomed-ct/snomed-ct0/snomed-ct-components/.

[14] Österreichische Apothekerkammer. *Pharmazentralnummer und Strichcode*. Nov. 2013. URL: http://www.apotheker.or.at/internet/oeak/NewsPresse.nsf/print/EE6A2A54CDBCEEC0C1256AB600393F1

[15] Österreichische Apothekerkammer. *Wer vergibt die Pharmazentralnummern in Österreich*. Nov. 2013. URL: http://www.apotheker.or.at/internet/oeak/NewsPresse.nsf/print/6213BA470504C468C1256E8900370485.

[17] Forbes Magazin. *Android Dominates Market Share, But Apple Makes All The Money*. Nov. 2013. URL: http://www.forbes.com/sites/tonybradley/2013/11/15/android-dominates-market-share-but-apple-makes-all-the-money/.

[18] Katrin Claßen. *Zur Psychologie von Technikakzeptanz im höheren Lebensalter: Die Rolle von Technikgenerationen*. Nov. 2013. URL: http://www.ub.uni-heidelberg.de/archiv/14295.

[19] Prof. Dr. Susanne Schäfer-Walkmann. *Stress in der Pflegearbeit: anregend oder aufregend*. Nov. 2013. URL: http://www.stmas.bayern.de/imperia/md/content/stmas/stmas_internet/pflege/dokumentation/ftdw-schaefer.pdf.

[20] CA. *Web Stress*. Nov. 2013. URL: http://www.ca.com/us/~/media/files/supportingpieces/final_webstress_survey_report_229296.aspx.

[22] *RFID Implantats DIY Kits*. Aug. 2013. URL: https://dangerousthings.com/shop/product-category/rfid-nfc/.

[29] *CVE-2008-0166*. Aug. 2013. URL: https://security-tracker.debian.org/tracker/CVE-2008-0166.

[31] Thorsten Denkler. *Der gegrillte Daumen*. Aug. 2013. URL: http://www.sueddeutsche.de/digital/elektronischer-reisepass-der-gegrillte-daumen-1.339537.

[32] *Geldbörsen mit RFID Blocker*. Aug. 2013. URL: http://wwwallets.com/geldboersen/?c=E8&f=g_rfid&t=Geldb%F6rsen+mit+RFID-Blocker.

[33] *RFID-Schutz Reisepass Hülle*. Aug. 2013. URL: http://www.cryptoshop.com/sycamo-cardcare-reisepass-hulle.html.

[34] *Downloadcenter DIMDI*. Aug. 2013. URL: http://www.dimdi.de/dynamic/de/klassi/downloadcenter/icd-10-gm/version2013/.

[35] *§9 Sanitätsgesetz*. Aug. 2013. URL: https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40097367/NOR40097367.html.

[36] *§10 Sanitätsgesetz*. Aug. 2013. URL: https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40027451/NOR40027451.html.

[37] University of Washington School of Pharmacy. *DIDB : The Metabolism & Transport Drug Interaction Database*. Aug. 2013. URL: http://www.druginteractioninfo.org/applications/metabolism-transport-drug-interaction-database/.

[38] *Fentanyl, Wirkstoff*. Aug. 2013. URL: http://medikamente.onmeda.de/Wirkstoffe/Fentanyl.html.

[39] *Propofol, Wechselwirkungen*. Aug. 2013. URL: http://medikamente.onmeda.de/Wirkstoffe/Propofol/wechselwirkungen-medikament-10.html.

[40] Mohit Arora. *How secure is AES against brute force attacks?* Aug. 2013. URL: http://www.eetimes.com/document.asp?doc_id=1279619.

[41] *FLOPS*. Aug. 2013. URL: http://en.wikipedia.org/wiki/FLOPS.

A Anhang

A.1 Schlüssellänge bei verschiedenen Alphabeten

Die Länge des Schlüssels bei Hexadezimaler Ansicht errechnet sich wie in A.1 angegeben.

$$\frac{KeyLength}{ld(16)} = \frac{128}{4} = 32 \tag{A.1}$$

Ein Alphabet mit allen Buchstaben sowie Ziffern hat 62 Zeichen, wobei ähnlich aussehende Zeichen („oO0iIlLjJ1") abgezogen werden, um Verwirrungen zu verhindern. Somit bleiben 52 Zeichen übrig, die Schlüssellänge ist dabei in A.2 angegeben.

$$\frac{KeyLength}{ld(52)} = \frac{128}{ld(52)} \approx 22,5 \tag{A.2}$$

Somit müssten 23 Zeichen verwendet werden um einen 128 bit Key darzustellen.

A.2 Brute Force Attacke auf AES

Laut [40] sind etwa 1000 Floating Point Operations Per Second (FLOPS) notwendig um eine Brute Force Runde zu errechnen. Ein moderner Spiele-PC mit mehreren Grafikkarten und CPUs erreicht etwa $16 * 10^{12}$ FLOPS [41]. Somit errechnet sich die Dauer der Brute Force Attacke für einen 23- beziehungsweise 28 bit Key wie folgt:

$$\frac{2^{23}}{16 \cdot 10^9} = 0{,}000524288\,\text{s} \tag{A.3}$$

$$\frac{2^{28}}{16 \cdot 10^9} = 0{,}016777216\,\text{s} \tag{A.4}$$

Diese Schätzungen sind sehr optimistisch, allerdings zeigen sie, dass diese geringe Anzahl von Schlüssellänge keineswegs ausreichen um ein System sinnvoll zu schützen.

A.3 Screenshots

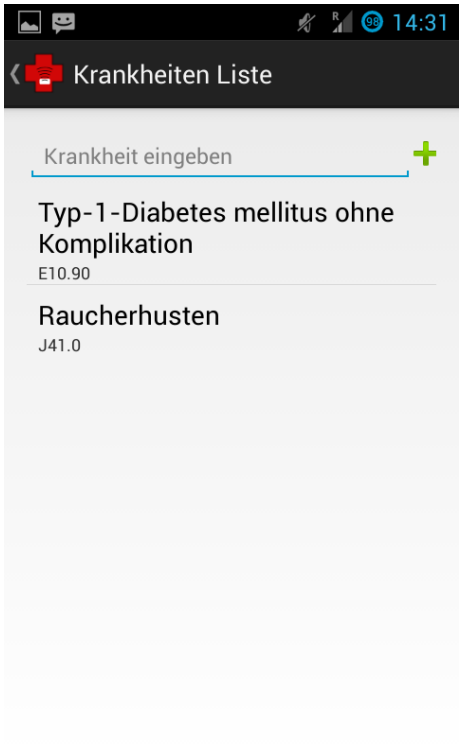


Abbildung A.1: Speichern von Krankheiten

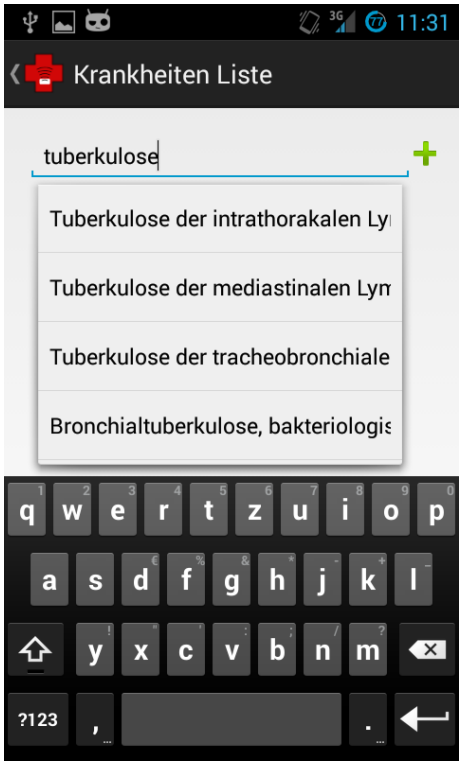


Abbildung A.2: Auswahl einer Krankheit

Abbildung A.3: Speichern auf dem Tag

Abbildung A.4: Das Tag wurde beschrieben

Abbildung A.5: Einscannen eines Arzneimittelcodes

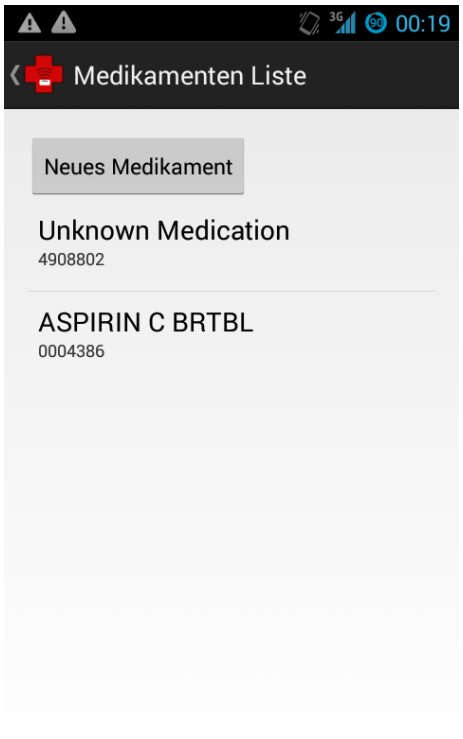


Abbildung A.6: Arzneimittelübersicht aller erfasster Medikamente

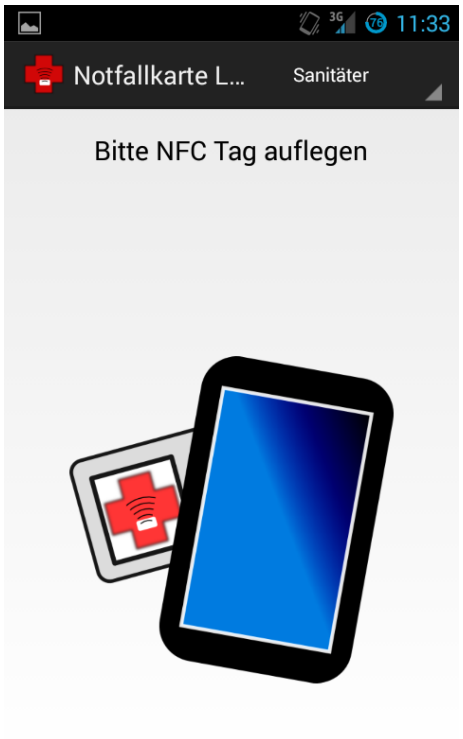


Abbildung A.7: Eine Karte wird eingelesen

Abbildung A.8: Ansicht für den Sanitäter

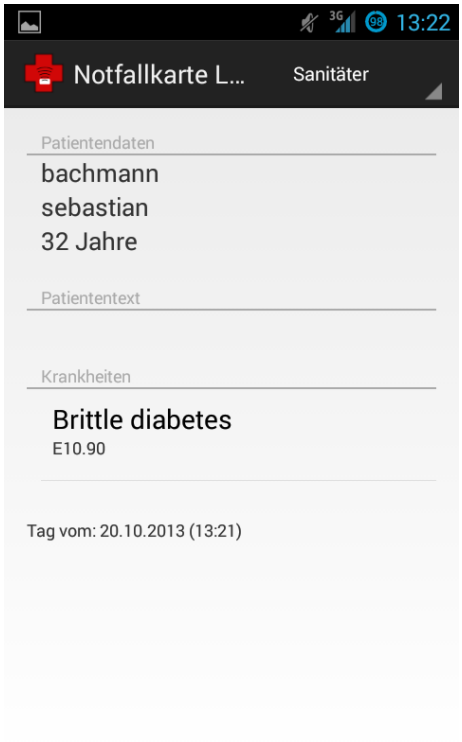


Abbildung A.9: Ansicht für den Sanitäter mit eingetragenen Krankheiten

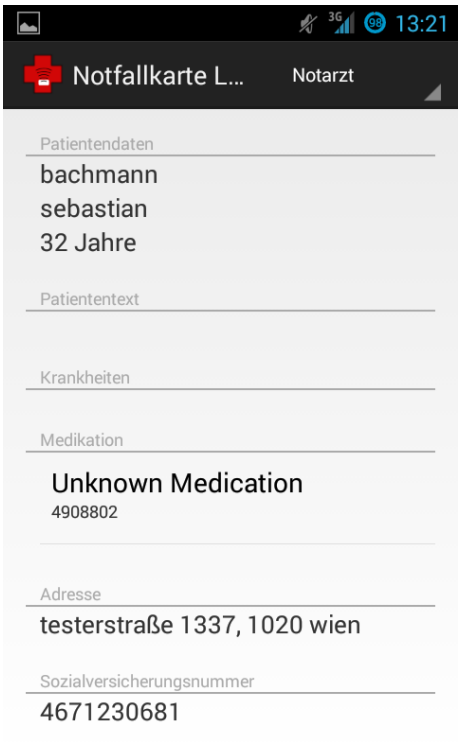


Abbildung A.10: Ansicht für einen Arzt

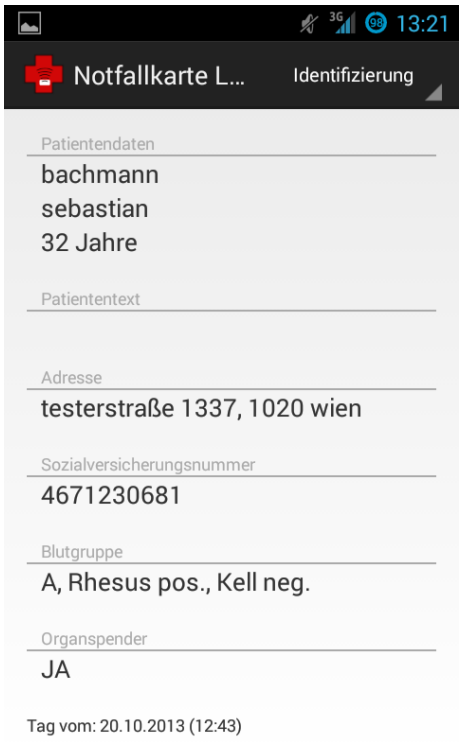


Abbildung A.11: Ansicht zur Identifizierung