



**Thema:**

Smartcards

**Studienarbeit**

Themensteller: Prof. Dr. rer. pol. habil. Hans-Knud Arndt

Betreuer: Prof. Dr. rer. pol. habil. Hans-Knud Arndt

vorgelegt von: Nico Gebauer

Abgabetermin: 20.10.2010

## INHALTSVERZEICHNIS

---

INHALTSVERZEICHNIS.....	II
ABBILDUNGS- / TABELLENVERZEICHNIS.....	III
ABSTRACT.....	IV
1. EINLEITUNG.....	1
1.1 Motivation.....	1
1.2 Begriffsdefinition.....	1
1.3 Anwendungsgebiete.....	2
2. GRUNDLAGEN DER SMARTCARDS.....	3
2.1 Kartentypen.....	5
2.2 Arten von Chipkarten.....	5
2.2.1 Einteilung nach Chiptyp.....	5
2.2.2 Einteilung nach Datenübertragung.....	5
3. AUFBAU VON SMARTCARDS.....	7
3.1 Grundaufbau einer Chipkarte.....	7
3.2 Grundaufbau des Mikrocontrollers.....	7
3.2.1 CPU.....	9
3.2.2 ROM.....	9
3.2.3 RAM.....	9
3.2.4 EEPROM.....	10
3.3 Sonderkomponenten.....	10
4. KONTAKLOSE SMARTCARDS.....	12
4.1 Einsatzgebiete und Anforderungen.....	12
4.2 Energieübertragung.....	12
4.3 Datenübertragung.....	13
4.4 Existierende Normen.....	14
4.5 Die Mifare Card.....	14
5. TICKET PROFILE EDITOR.....	16
5.1 Hintergrund zur Programmstehung .....	16
5.2 Verwendete Techniken.....	16
5.3 Aufbau und Funktion .....	17
6. ABSCHLUSSBETRACHTUNGEN.....	20
LITERATURVERZEICHNIS.....	22

**ABBILDUNGS- / TABELLENVERZEICHNIS**

---

<b>Abb. 1:</b> Anforderungstypen für verschiedene Smartcard-Eigenschaften.....	2
<b>Abb. 2:</b> Klassifizierung der Karten nach Primärmerkmal.....	4
<b>Abb. 3:</b> Grundaufbau einer kontaktbehafteten Smartcard mit Prozessor / Zusammenhänge der verschiedenen Kartenformate.....	7
<b>Abb. 4:</b> Grundaufbau des Mikroprozessors einer Smartcard.....	8
<b>Abb. 5:</b> Größenverhältnis zwischen den einzelnen Speicherzellen.....	10
<b>Abb. 6:</b> Die Charlie Card des MBTA.....	14
<b>Abb. 7:</b> Startbildschirm des Ticket Profile Editors.....	17
<b>Abb. 8:</b> Hauptfenster des Ticket Profile Editors.....	18

---

<b>Tabelle 1:</b> Übersicht über die derzeit existierenden Normen für kontaktlose Smartcards.....	14
---	----

**ABSTRACT**

---

Die Arbeit befasst sich mit der Technologie der Smartcards. Hierfür werden zunächst eine Definition sowie Anwendungsgebiete vorgestellt. Es folgt ein Überblick über die Entwicklung dieser Karten und es wird eine Einteilung der existierenden Chipkarten nach verschiedenen Kriterien vorgenommen. Im weiteren wird es eine Übersicht über den Aufbau der Smartcards und deren Komponenten sowie der Bedeutung und Funktion der einzelnen Bestandteile geben. Als besonderer Vertreter werden die kontaktlosen Smartcards vorgestellt, deren Bedeutung im Alltag immer wichtiger wird und die immer öfter anzutreffen sind. Zum Abschluss erfolgt die Vorstellung eines Programms, das während meines Praktikums entstand. Dort arbeitete ich in der Abteilung eines Betriebes, der sich mit Systemen für Fahrgeldmanagement beschäftigt und somit alltäglichen Umgang mit Smartcards pflegt.

## 1. EINLEITUNG

---

### 1.1 MOTIVATION

Jeder von uns besitzt mindestens ein Paar von Ihnen. Wir benutzen Sie im Alltag wie selbstverständlich, ohne darüber nachzudenken wie Sie überhaupt funktionieren oder welche ausgeklügelte Technik in Ihnen steckt. Die kleinen Helfer aus Plastik erleichtern uns unser alltägliches Leben ungemein und sind auch nicht mehr wegzudenken. Sei es beim Bezahlen des Einkaufs, beim Fahren mit einem öffentlichen Verkehrsmittel oder einem Routinebesuch beim Arzt, ständig kommen wir mit Ihnen in Berührung und genießen Ihre Vorzüge. Sie haben genau die richtige Größe um in das Portmonee zu passen und nicht verloren zu gehen. Sie sind robust, flexibel und halten vielen Strapazen stand. Doch wer oder was sind diese kleinen technischen Meisterwerke die wir überall antreffen können?

Die Rede ist natürlich von Smartcards. Sei es die EC- oder Kreditkarte, die Fahrkarte im öffentlichen Nahverkehr, die Krankenkassenkarte oder einfach der Studentenausweis. Doch handelt es sich bei Smartcards nicht einfach nur um herkömmliche Plastikkarten mit einem bunten Aufdruck, wie Sie es in ihrer Anfangszeit waren, sondern um Technologie auf aller höchstem Niveau. Ausgestattet mit Mikroprozessoren auf dem neuesten Stand, bieten die Smartcards der aktuellen Generation ein breites Spektrum an Einsatzmöglichkeiten, da sie zum einen leistungsfähiger, zum anderen aber auch sicherer gegen Angriffe von außen sind. So benutzen diese Karten hochentwickelte Verschlüsselungsalgorithmen um die auf ihnen gespeicherten und zu verarbeiteten Daten zu schützen und vor Missbrauch zu bewahren.

Doch woher kommen diese Karten eigentlich? Wie genau funktionieren Sie? Wie sind Sie aufgebaut und warum sehen Sie, auch wenn viele die selbe Form haben, doch oft so unterschiedlich aus?

Mit der Beantwortung dieser und weiterer Fragen befasst sich die folgende Arbeit.

### 1.2 BEGRIFFSDEFINITION

Was genau sind Smartcards und wie kann man Sie definieren? Das große Online-Lexikon für Informationstechnologie beschreibt Sie wie folgt:

*„Smartcards, auch als Integrated Circuit Card (ICC) oder Mikroprozessorkarten bezeichnet, sind kontaktbehaftete Plastikkarten mit Speicher in der Größe von 85,6 x 53,58 x 0,76 mm, die als ID1-Karten bezeichnet werden.“ [ 3]*

Eine Smartcard ist also eine Mikroprozessorkarte, die keine willkürliche

Größe und Aufbau besitzt, sondern sich an festen Standards orientiert. So sind die exakten Ausmaße einer Smartcard genau standardisiert und festgelegt. Des Weiteren besitzt sie Kontakte, die als Schnittstelle dienen und externen Geräten den Zugriff auf die Funktionen und Daten der Smartcard gewähren. Diese Schnittstellen sind allerdings nicht immer sichtbar, wie im späteren Verlauf genauer beschrieben wird.

### 1.3 ANWENDUNGSGEBIETE

Wie bereits angesprochen, gibt es eine Vielzahl von Anwendungsgebieten für Smartcards / die Smartcardtechnologie. Jeder dieser Bereiche hat seine eigenen Anforderungen an die Funktionalität der Karten und setzt somit unterschiedliche Schwerpunkte die besonders beachtet werden müssen. So ist es im Öffentlichen-Personen-Nahverkehr (ÖPNV) erwünscht, dass die Karten die hier als Fahrkarten verwendet werden kontaktlos sind, um somit eine schnelle Abwicklung des Verifizierungsprozesses der Gültigkeit der Fahrkarten zu ermöglichen. Im Bereich der Mobilfunkkommunikation oder der Medizin spielt die Datenspeicherung und die Sicherung dieser eine große Rolle.

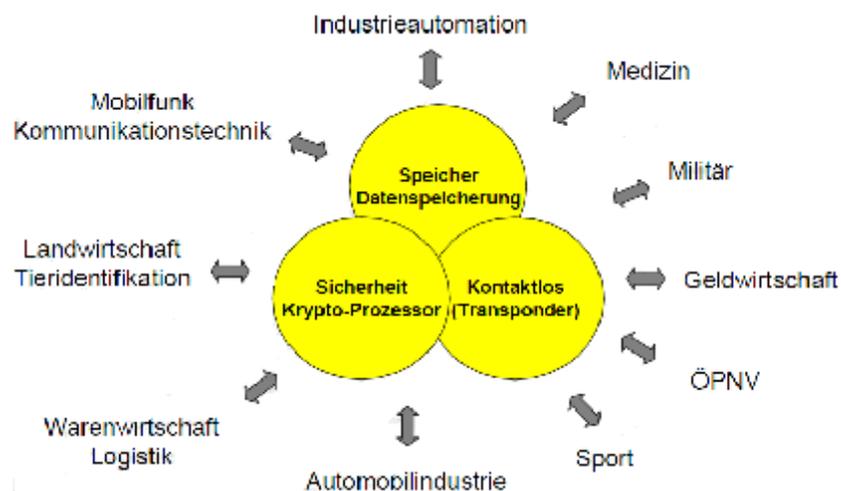


Abbildung 1: Anforderungstypen für verschiedene Smartcard-Eigenschaften. [ 5 ]

## 2. GRUNDLAGEN DER SMARTCARDS

---

### 2.1 KARTENTYPEN

Karten entwickelten sich im Verlauf der Jahre von einfachen Plastikkarten zu hoch entwickelten technischen Geräten. Die ersten Exemplare gab es bereits zu Beginn der 50er Jahre. Sie wurde im Diners-Club verwendet und dienten dort als exklusive Zahlungsart. Diese **hochgeprägten Karten** wiesen nur zwei hauptsächliche Sicherheitsmerkmale auf, die Hochprägung sowie ein Unterschriftsfeld. Bei der Hochprägung handelte es sich meist um den Namen des Karteninhabers sowie um eine Identifikationsnummer. Diese sind speziell in die Karte gestanzt und hervorgehoben. Das zweite Feld diente der Unterschrift des Karteninhabers und somit zur visuellen Kontrolle. Die Art, in der die Hochprägung zu erfolgen hat ist im ISO Standard 7811 festgehalten. Bei der Benutzung der Karte wird mit Hilfe eines einfachen Lesegerätes ein Abdruck der Hochprägung angefertigt und vom Besitzer zur Verifizierung eine Unterschrift geleistet.

Da dieses Verfahren sehr aufwendig war, jeder Kartenabdruck wurde auf Papier angefertigt, entwickelten sich Karten weiter. So entstanden Anfang der 1970er Jahre die **Magnetstreifenkarte**. In diesem Magnetstreifen werden nun die wichtigsten Daten wie Name des Besitzers sowie die Identifikationsnummer gespeichert. Wie auch bei der Hochprägung, sind die genauen Normen für den Magnetstreifen in der ISO Normal 7811 festgehalten. So besitzt der Magnetstreifen bis zu drei verschiedene Spuren, von denen die ersten beiden Spuren lediglich gelesen werden können, auf Ihnen befinden sich also die benutzerspezifischen Daten. Die dritte Spur hingegen bietet die Möglichkeit einen Schreibvorgang vorzunehmen und so weitere Daten über die Karte und Ihre Verwendungschonik ( z.B. Zahlungstransaktionen) zu speichern.

Der Magnetstreifen hat ein Speichervolumen von ungefähr 1.024 Bit. Dieses verteilt sich wie folgt über die drei Spuren:

- Spur 1: 76 Nutzzeichen (alphanumerisch 7 Bit/Zeichen)
- Spur 2: 37 Nutzzeichen (numerisch 5 Bit/Zeichen)
- Spur 3: 104 Nutzzeichen (numerisch 5 Bit/Zeichen)

Leider ist der Vorteil der Magnetstreifenkarten zugleich auch ein Nachteil. So ist es zum Beispiel möglich, mit Hilfe eines Schreib-/Lesegerätes die auf dem Streifen gespeicherten Daten zu manipulieren. Da diese Karten meist maschinell gelesen / verarbeitet werden, gibt es keine weitere Überprüfungsmöglichkeit für die Authentizität der Karte. Zwar gibt es mittlerweile eine Vielzahl von Techniken um die Daten gegen Fälschung und Veränderung zu schützen ( Kodierungen im Kartenkörper), allerdings sind diese Verfahren recht kostspielig. So finden sich reine Magnetstreifenkarten, ohne großartige Sicherung wie PIN (bei EC-Karten) oder andere aufwendige

Sicherheitsverfahren heute meist nur in sicherheitstechnisch unbedenklichen Bereichen, als Karten im Parkhaus, zur Erfassung der Arbeitszeit in Firmen, als Gutscheine und ähnliches. Krankenkassenkarten sowie Bankkarten besaßen in Ihrer Anfangszeit auch nur einen Magnetstreifen, wurden dann aber um einen Chip erweitert.

Dieser angesprochene Chip ist die jüngste und größte Neuerung im Bereich der Karten und erlaubt zum ersten mal den wirklichen Gebrauch des Namens **Smartcard**. Hierbei wird im Kartenkörper eine Schaltung integriert, der es möglich ist, Daten zu speichern und zu verarbeiten. Auch für die Funktionen und Eigenschaften der sogenannten Chipkarten gibt es eine ISO Norm, 7816. Ein Vorteil des Chips gegenüber dem Magnetstreifen wird in Zahlen direkt sichtbar, der Speicherplatz. Während Magnetstreifen lediglich ca. 1.024 Bit an Speicherplatz bieten, kann die Chipkarte bereits heute 256kByte und mehr zur Verfügung stellen. Der zweite große und auch deutlich wichtigere Vorteil ist die von der Chipkarte gebotene Sicherheit. Da der Zugriff auf die Daten über eine serielle Schnittstelle erfolgt ist es möglich Daten auf die Karte (den Chip) zu laden die von außen dann nicht mehr auslesbar sind. So ist dann nur noch das karteninterne Rechenwerk in der Lage die gespeicherten Daten zu lesen und zu verarbeiten. Des Weiteren ist die Lebensdauer von Smartcards (Ø 3 – 10 Jahre, je nach Typ) deutlich höher als die von einfachen Magnetstreifenkarten (Ø 1 – 2 Jahre).

Die bisher genannten Kartentypen kann man nun auch an einem Baumdiagramm darstellen:

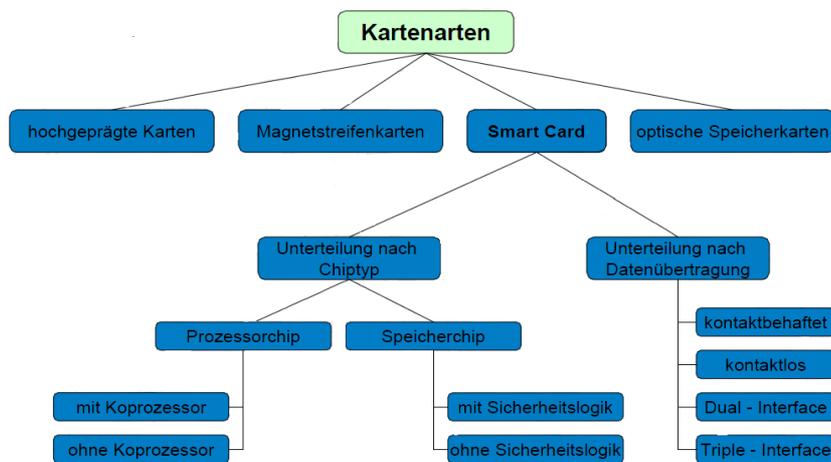


Abbildung 2: Klassifizierung der Karten nach Primärmerkmal. [ 5 ]

Wie aus Abbildung 2 ersichtlich ist, gibt es neben den hochgeprägten Karten, den Magnetstreifenkarten und den Smartcards noch einen weiteren Typen, die optischen Speicherkarten. Diese kommen zum Einsatz, wenn das Speicherangebot einer Smartcard nicht mehr ausreicht. Optische Speicherkarten mit einer Kapazität von mehreren MByte haben allerdings den großen Nachteil, dass Sie nur ein einziges mal beschrieben werden können. Sie finden Ihren Einsatz zum Beispiel im Gesundheitswesen, da diese Karten sogar in der Lage sind, ganze Röntgenbilder zu speichern.

## 2.2 ARTEN VON CHIPKARTEN

Chipkarten haben sich im Laufe der Zeit die unterschiedlichen Anforderungen die an Sie gestellt werden (Abb. 1) bestens erfüllt und sich somit in verschiedene Richtungen weiterentwickelt. Daher ist es notwendig, in der Familie der Chipkarten noch einmal eine extra Unterscheidung vorzunehmen. Hierzu bieten sich zwei Hauptkriterien an:

### 2.2.1 EINTEILUNG NACH CHIPTYP

Unterscheidet man die Karten nach Ihrem Chip, unterscheidet man Sie zugleich nach Ihrer Aufgabe. Als erstes wäre hier die Speicherkarte zu nennen. Diese dürfte jedem von der Telefonkarte oder auch von der Krankenkassenkarte her bekannt sein. Diese Karten besitzen nur eine Adress- und Sicherheitslogik, um auf die gespeicherten Daten zugreifen und diese verwalten zu können. Dabei gibt es noch die Möglichkeit Speicherkarten mit einer Sicherheitslogik auszurüsten, die dann erst die Anfrage überprüft, ob das Gerät oder der User der die Daten von der Karte abrufen möchte überhaupt berechtigt ist diese Daten zu lesen.

Die zweite Art der Karten sind die sogenannten Prozessorkarten. Diese besitzen, wie der Name es schon richtig vermuten lässt, eine eigene Prozessoreinheit. Auch bei diesen Karten gibt es noch ein weiteres Unterscheidungskriterium, besitzen Sie einen Coprozessor oder nicht. Prozessorkarten sind in der Lage, selbstständig Rechenarbeiten auszuführen und sind damit komplexer und vielseitiger einsetzbar als Speicherkarten.

### 2.2.2 EINTEILUNG NACH DATENÜBERTRAGUNG

Die Unterscheidung nach Datenübertragung erfolgt aufgrund des von der Karte angebotenen Input-/ Outputinterfaces. Die erste und zugleich bekannteste Art sind die kontaktbehafteten Karten. Diese haben eine direkte Kontaktstelle, an der das Lesegerät angeschlossen werden muss, um eine Datenübertragung zu ermöglichen. Dieser Kontakt findet sich auf der Karte als „goldenes Plättchen“ wieder und sollte jedem von der EC-Karte oder der Krankenkassenkarte her bekannt sein.

Der zweite Typ von Karten sind die kontaktlosen Karten. Diese haben auf der Oberfläche keine sichtbaren Kontakte mehr, da Sie nicht direkt an ein Gerät angeschlossen werden müssen. Für die Übertragung der Daten gibt es mehrere verschiedene Ansätze, von denen einige im späteren Verlauf noch genauer erörtert werden. Die letzten beiden Typen von Karten die man in dieser Hinsicht unterscheiden kann, sind die Karten mit Dual- bzw. Tripleinterface. Das Dualinterface ist eine Kombination aus kontaktbehafteter und kontaktloser Technologie, das Tripleinterface besitzt noch eine weitere USB Schnittstelle. Solche Interfaces kommen meist dann zustande, wenn ein etwas älteres System, wie zum Beispiel eines

das kontaktbehaftete Karten nutzt, auf kontaktlosen Karten umgestellt werden soll. Während die Hardware umgerüstet wird müssen sowohl die neuen als auch die alten Kartenlesegeräte in der Lage sein die Daten der Karten zu lesen.

### 3. AUFBAU VON SMARTCARDS

#### 3.1 GRUNDAUFBAU EINER CHIPKARTE

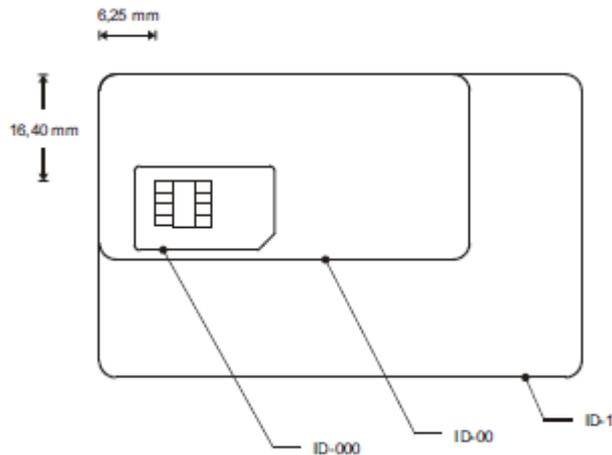


Abbildung 3 : Grundaufbau einer kontaktbehafteten Smartcard mit Prozessor /  
Zusammenhänge der verschiedenen Kartenformate. [ 1 ]

Eine Smartcard besteht Grundsätzlich aus einem Kunststoff auf oder in der an einer normierten Position der Chip implementiert ist. Bei einer kontaktbehafteten Smartcard liegt dieser Punkt bei exakt 6,25mm in der Breite und 16,40 mm in der Tiefe vom oberen linken Kartenrand entfernt. Bei kontaktlosen Karten ist die Chipposition variabel. Die Karte hat eine genormte Größe die im Bereich von 85,46mm – 85,72mm Breite und 53,92mm – 54,03mm Höhe liegen muss. Andernfalls ist die Karte nicht allgemeinen in allen Endgeräten nutzbar und entspräche somit auch nicht der Norm. Die Stärke der Karte beträgt 0,76mm mit einer Abweichtoleranz von  $\pm 0,08$ mm.

Abbildung 3 zeigt ebenfalls noch die anderen existierenden Größen für Smartcards. Zum einen die von den Handy SIM-Karten bekannte Form ID-000, zum anderen die Größe ID-00. Diese beiden Formen liegen eingebettet in der typischen ID-1 Form. Der Hintergrund dafür steckt in der Produktion von Smartcards. So ist es einfacher, die ID-1 Formate zu produzieren und diese dann durch Stanzen in die kleineren Formate zu überführen, als die kleinen Formate extra herzustellen. Zum Anderen unterscheiden sich die Karten auch nur in der Größe, aber meist nicht in ihrem Chipaufbau.

#### 3.2 GRUNDAUFBAU DES MIKROCONTROLLERS

Der Mikrocontroller ist der zentrale Baustein der Smartcard und ist über die Kontakte mit dem Endgerät verbunden, von denen er seine Daten und

Befehle erhält. Es handelt sich hierbei nicht um einen herkömmlichen Mikrocontrollerbaustein, den man auch in anderen Bereichen als der Smartcardtechnologie wiederfinden kann, sondern um speziell für diesen Zweck angefertigte Bausteine. Herkömmliche Mikrocontroller bieten oft Funktionen die für Smartcards nicht benötigt werden und auf dem engen Raum kostbaren Platz verschwenden würden. Zum anderen gestaltet sich die Produktion ohne überflüssige Strukturen und Funktionen auch günstiger.

Die meisten Smartcards werden passiv betrieben, das heißt, sie besitzen keine eigene Stromversorgung, da die Unterbringung einer Batterie auf der kleinen Karte zum einen sehr schwierig, zum anderen eine solche Batterie in der Produktion sehr kostenintensiv ist. Da die Anforderungen an das Batterieelement sehr hoch sind, so müssen diese elastisch sein um beim Biegen der Karte nicht zerstört zu werden, erfolgt die Energieversorgung bei fast allen Smartcards ausschließlich über das Lesegerät.

Der Strom wird dafür bei kontaktbehafteten Karten über den VCC-Pin übertragen, bei kontaktlosen Karten erfolgt die Energieversorgung auf anderem Wege, was später noch genauer erläutert wird. Über den I/O Pin werden die Daten übertragen, die auf der Karte verarbeitet beziehungsweise gespeichert werden sollen.

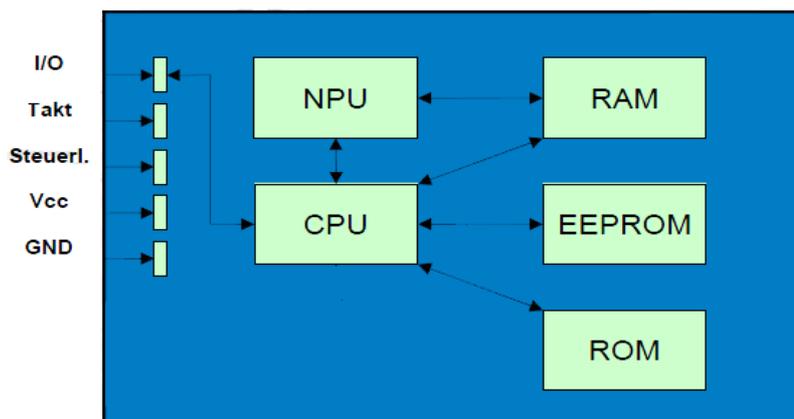


Abbildung 4: Grundaufbau des Mikroprozessors einer Smartcard.

Der Mikrocontroller steuert und überwacht alle Aktivitäten der Smartcard. Er ist auf die speziellen Anforderungen abgestimmt und als vollwertiger Computer zu betrachten. Wie in Abbildung 4 zu erkennen ist, besteht auch ein Smartcard Mikrocontroller aus den typischen Bausteinen:

- **C**entral **P**rocessing Unit ( CPU)
- **N**umeric **P**rocessing Unit ( NPU)  
( variable, heutzutage aber fast fester Bestandteil)
- **R**andom **A**ccess **M**emory ( RAM)
- **R**ead **O**nly **M**emory ( ROM)
- **E**lectronical **E**rasable **P**rogrammable **R**ead **O**nly **M**emory  
( EEPROM)

Die Größe der für die Mikrocontroller eingesetzten Halbleitertechnologie rangiert in einer Ordnung zwischen  $0,25\mu\text{m}$  und  $0,13\mu\text{m}$  und entspricht somit der aktuell kleinsten realisierbaren Strukturbreite. Die Anwendung dieser

kleinsten Strukturen ist wichtig, denn die letztendliche Größe des Chips spielt eine wichtige Rolle. Je größer der Chip wird, um so größer ist auch die Chance, dass der Chip bei Beanspruchung der Karte, wie zum Beispiel dem Biegen oder dergleichen, Schaden nimmt und defekt ist. Hierbei reichen schon kleinste Haarrisse aus, um die Funktionsfähigkeit des Chips komplett zu zerstören. Deswegen setzen sich viele Hersteller von Smartcards eine Obergrenze für die Größe einer quadratischen Chipfläche von ca. 25mm<sup>2</sup>.

### 3.2.1 CPU

Bei den Prozessoren für die Chipkarten handelt es sich nicht um Spezialanfertigungen und das auch aus gutem Grund. Zum einen ist es nicht üblich neue Prozessoren für einen speziellen Anwendungsbereich neu zu entwickeln, zum anderen benötigt man extrem zuverlässige Prozessoren. Daher greift man auf ältere, sich bereits in der Praxis bewährte, Modelle zurück. Somit sind sie zwar nicht auf dem aktuellsten technischen Stand, gewähren aber eine hohe Zuverlässigkeit und somit eine geringe Ausfallquote. Auf der unteren Leistungsskala der Chipkarten-Mikrocontroller werden Prozessoren mit einer Speicherbreite von 8 Bit verwendet, da sich der adressierbare Speicher zwischen 6kByte und 30kByte bewegt. In den oberen Leistungsregionen neigt man aber zur Verwendung von 16 Bit beziehungsweise 32 Bit Prozessoren, da hier die deutlich größeren Speicherbereiche verwaltet werden müssen.

### 3.2.2 ROM

Beim ROM handelt es sich um einen nichtflüchtigen Speicher, was bedeutet, dass der Speicherinhalt auch erhalten bleibt, wenn kein Strom mehr am Speicherbaustein anliegt. ROM steht für „read only memory“ und wie der Name es schon sagt, ist es nicht möglich auf dem ROM zu schreiben, denn dieser bietet auf Grund seiner Bauweise nur Lesezugriffe an. Auf der Smartcard befinden sich im ROM die meisten Betriebssystemroutinen, die während der Produktion der Chips eingebracht werden. So ist ein Einbringen von Daten nach der Halbleiterproduktion nicht mehr möglich und der Baustein kann folglich nur noch gelesen werden.

### 3.2.3 RAM

Der RAM ist der einzige flüchtige Speicherbaustein der auf einem Mikrocontroller Verwendung findet. Der Name steht für „random access memory“ und das bedeutet, dass die in ihm gespeicherten Daten jederzeit gelesen und auch wieder verändert werden können. Allerdings bringt der RAM auch einen großen Nachteil mit sich, so ist er nur in der Lage die in ihm gespeicherten Zustände zu halten, so lange eine Spannungsversorgung gewährleistet ist. Kommt es zu einem Verlust dieser Versorgung sind alle vorher gespeicherten Daten verloren. In einem Mikrocontroller für

Smartcards kommt noch eine besondere Art des RAM's zum Einsatz, der sogenannte statische RAM (SRAM). Dessen Speicherinhalt muss im Gegensatz zum herkömmlichen RAM nicht ständig periodisch aufgefrischt werden und ist somit unabhängig vom äußeren Takt, der an die Smartcard angelegt wird. Der RAM ist nicht geeignet um wichtige Programmroutinen zu speichern sondern findet hier, wie auch im PC, seine Verwendung als Arbeitsspeicher.

### 3.2.4 EEPROM

Bei den EEPROM Speicherbausteinen handelt es sich um die sogenannten „electronic erasable read only memory“. Diese sind in der Herstellung deutlich aufwendiger als RAM oder ROM Bausteine und werden zur Speicherung von veränderlichen Funktionen und Daten verwendet. Wie auch schon beim ROM, so handelt es sich auch beim EEPROM um einen nichtflüchtigen Speicherbaustein. Da er aber im Vergleich zum ROM neu beschrieben werden kann, ist er vergleichbar mit der Festplatte eines PCs. Die Lebensdauer eines solchen EEPROM Bausteines liegt zwischen 100.000 und 1 Million Schreibzyklen. Dies ist der Bauart des EEPROMS geschuldet, bei der sich im Laufe der Beanspruchung die sogenannte Tunnel-Oxidschicht abnutzt. Schon während der Produktion ist diese großen thermischen Belastungen ausgesetzt und somit zugleich die Schwachstelle dieses Speicherbausteins und bestimmt dessen Lebensdauer.

Wie groß der Anteil der einzelnen Speicherbausteine am letztendlichen Chip ist, hängt von seinem späteren Verwendungszweck ab. So wird stets versucht, den Anteil von RAM- und EEPROM-Speicher so klein wie möglich zu halten, da diese Baugruppen deutlich mehr Platz pro Bit verbrauchen als der ROM. So ist der Platzbedarf einer RAM-Speicherzelle ca. 4 mal so groß wie der einer EEPROM-Speicherzelle, der wiederum ca. 4 mal größer ist als der des ROMs, wie in Abbildung 5 gut ersichtlich ist.

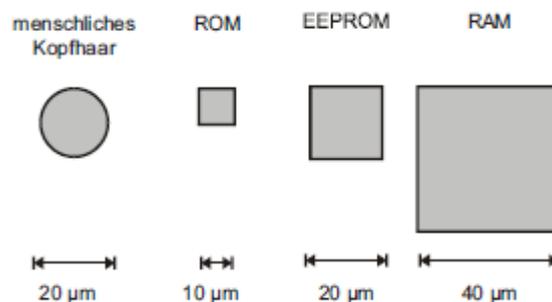


Abbildung 5: Größenverhältnis zwischen den einzelnen Speicherzellen. [ 1 ]

## 3.3 SONDERKOMPONENTEN

Der Aufgabenbereich von Smartcards ist vielseitig und die an sie gestellten

Aufgaben sind teilweise sehr anspruchsvoll und können nicht immer softwaretechnisch gelöst werden. Dies führt dazu, dass diese Funktionen durch weitere Hardwarekomponenten abgedeckt werden müssen. So wäre hier auf jeden Fall die Sicherheit der auf dem Chip verwendeten Daten zu nennen. Diese müssen vor unautorisierten Zugriffen von außen geschützt werden. Da Verschlüsselungen je nach Art sehr aufwendig sind, ist der Prozessor allein damit überlastet und somit kommt oft ein Coprozessor (NCPU) zum Einsatz, der speziell für diese Anforderungen konzipiert ist (symmetrische / asymmetrische Verschlüsselungen).

Auch intern kann es passieren, dass ein später auf den Chip der Smartcard geladenes Programm auf Speicherbereiche zugreift, auf die es nicht zugreifen soll. Um dies zu kontrollieren und die Daten vor unautorisierten Zugriffen von internen Routinen zu schützen, wird häufig eine sogenannte MMU („memory management unit“) verwendet. Dieser Baustein setzt vor der Ausführung einer Routine den erlaubten zu verwendenden Speicherbereich fest. Das verhindert, dass die Routine während ihres Ablaufs auf andere Speicherbereiche Zugriff hat. Dieser durch sogenannte Firewalls eingegrenzte Bereich kann dann von der Routine nicht verlassen werden, sollte trotzdem ein Zugriff auf externe Speicherbereiche erfolgen, wird ein Interrupt ausgelöst und dieser Verstoß detektiert.

Eine weitere Schwachstelle des Chips ist bidirektionale serielle Schnittstelle, deren Geschwindigkeit, insofern sie softwaregesteuert ist, von der Prozessorgeschwindigkeit abhängig ist. So ist ein Prozessor mit einem Takt von 3,5 MHz nur zu einer Datenübertragung von ca. 115kBit/s in der Lage. Um die Übertragungsgeschwindigkeit zu erhöhen, müsste man den Takt des Prozessors erhöhen, was aber zu einem ebenfalls erhöhten Energieverbrauch führt. Da das aber nicht erwünscht ist, kommt auch hier ein weiterer Hardwarebaustein zum Einsatz, ein sogenannter UART („universal asynchronous receiver transmitter“). Dieser übernimmt nun die Datenübertragung auf der untersten Protokollschicht (die oberen Schichten müssen jedoch weiterhin softwaretechnisch im Chip realisiert sein). Der Prozessor muss nun den UART-Baustein nur zeitgerecht beim Senden mit den Daten versorgen und beim Empfangen die Daten rechtzeitig abrufen. Durch Verwendung eines UART sind sogar 1 : 1 Übertragungen möglich, das bedeutet, dass ein 3,5 MHz Chip optimal eine Datenübertragung von 3,5MBit/s theoretisch realisieren könnte.

Ein weiteres Problem für einen Prozessor ist das Erzeugen von Zufallszahlen. Werden sie softwaretechnisch erzeugt, handelt es sich nur um sogenannte Pseudozufallszahlen, die allerdings aufgrund der Sicherheit nicht zur Authentisierung oder zur Generierung von Schlüsseln geeignet sind. Deswegen wird auch hier ein weiterer Hardwarebaustein verwendet, der RND („random number generator“). Dieser erzeugt dann aus verschiedenen Zuständen des Prozessors wie Takt oder Speicherinhalten über mehrere Schritte eine „echte Zufallszahl“.

Natürlich gibt es noch weitere Baugruppen, um die man den Chip erweitern kann und die dem Prozessor die Arbeit erleichtern, allerdings werden diese nicht immer benötigt. Daher wird versucht, die Funktionalität des Chips so genau wie möglich auf die Anforderungen anzupassen und auf überflüssige Funktionen / Baugruppen zu verzichten.

## 4. KONTAKLOSE SMARTCARDS

---

### 4.1 EINSATZGEBIETE UND ANFORDERUNGEN

Besonders im ÖPNV (öffentlichen Personen Nahverkehr), aber auch in der Universität (Unicard) und vielen weiteren Bereichen des alltäglichen Lebens kommen vor allem kontaktlose Smartcards zum Einsatz. Diese haben je nach Ausführung den Vorteil, dass Sie zur Verwendung nicht einmal mehr in die Hand genommen werden müssen, da Sie über Strecken von wenigen Zentimetern bis hin zu einem Meter einsatzfähig sind. Daher ist das Arbeiten beziehungsweise der Umgang mit diesen Smartcards für den Benutzer sehr einfach und bequem. So muss eine Person, die zum Beispiel in Boston mit der U-Bahn fahren möchte lediglich Ihr Ticket vor das Lesegerät halten, um den gebührenpflichtigen Bereich betreten zu können („Charlie Card“). Auch zur Identifikation sowie als Zahlungsmittel sind die kontaktlosen Smartcards besonders geeignet, wie die UniCard der OvGU Magdeburg beweist. Hier ist es möglich, auf den Studentenausweis einen Geldbetrag zu laden. Möchte man nun in der Mensa ein Essen bezahlen, ist es nicht mehr nötig in der Geldbörse nach Kleingeld zu suchen, sondern man hält einfach kurz die Karte vor den Leser, und durch Bestätigung der Kassiererin wird der zu zahlende Betrag direkt von der Karte abgebucht. So vereinfachen und beschleunigen kontaktlose Smartcards die Abläufe von alltäglichen Situationen enorm.

Da diese Smartcards, wie der Name schon sagt, kontaktlos verwendet werden, gibt es zwischen dem Terminal und der Karte auch keine galvanische Kopplung wie bei den kontaktbehafteten Karten. Dies führt aber zu neuen technischen Herausforderungen. So muss die Energieversorgung des integrierten Chips gewährleistet werden, eine Taktsignal sowie die Daten müssen irgendwie zwischen Karte und Terminal übertragen werden. Eine wichtige Rolle spielt hierbei der Abstand der Karte zum Terminal. Je nach erwünschtem Einsatzbereich der Karte gibt es nun verschiedene Lösungsansätze.

### 4.2 ENERGIEÜBERTRAGUNG

Wie bereits angesprochen, müssen Smartcards extern mit Energie versorgt werden, da sie bis auf wenige Ausnahmen passiv betrieben sind. Aus diesem Grund wird die Energie über die Luft vom Terminal zur Karte übertragen. Die am weitesten hierfür verbreitete Technik ist die sogenannte induktive Kopplung. Die für den Kartenbetrieb benötigte Menge an Energie hängt von ihrer Funktion ab. Soll eine Karte zum Beispiel der Erkennung dienen, so benötigt Sie nur wenige  $\mu\text{W}$  an Leistung, da sie hierfür nur gelesen werden muss. Diese Leistungsübertragung kann dann auch über eine größere Strecke von einem Meter erfolgen. Soll allerdings auch auf die Karte geschrieben

werden, erhöht sich der Energiebedarf enorm und die Reichweite der Karte verringert sich. Des Weiteren muss auf die geltenden Funkzulassungsvorschriften geachtet werden, da diese nicht verletzt werden dürfen.

Damit überhaupt Induktion in der Karte stattfinden kann, muss sie bautechnisch ergänzt werden. So wird nun in den Kartenkörper eine Spule integriert, da ohne diese keine Induktion möglich wäre. Die Übertragung der Energie erfolgt nun über das Prinzip des lose gekoppelten Transformators. Auch im Terminal befindet sich eine Spule. Diese erzeugt ein elektromagnetisches Hochfrequenzfeld mit Frequenzen von  $< 135\text{kHz}$  oder  $13,56\text{MHz}$ . Dies führt zu sehr großen Wellenlängen von  $22\text{m}$  beziehungsweise  $2400\text{m}$  und die Karte befindet sich dadurch im Nahfeld der Terminalspeule. Das so erzeugte Magnetfeld durchdringt nun die Karte und induziert somit eine Wechselspannung  $U_i$ . Diese induzierte Spannung ist leider sehr gering und muss deswegen noch weiter verstärkt werden. Dies erreicht man durch den Einsatz von Kondensatoren, die jeweils parallel zu den Spulen im Terminal und der Karte geschaltet sind. Die Kapazität des Terminkondensator ist so gewählt, dass er zusammen mit der Induktivität der Spule einen Schwingkreis bildet, der eine Resonanzfrequenz besitzt die der Übertragungsfrequenz zur Karte entspricht. Auch in der Karte bildet sich ein solcher Schwingkreis aus, der die selbe Resonanzfrequenz besitzt. Durch den Schwingkreis im Terminal fließen dort nun höhere Ströme, was zu einer Verstärkung der Feldstärke des erzeugten Magnetfeldes führt. Da die induzierte Spannung in der Smartcard direkt proportional zur Anzahl der Windungen der Terminalspeule, zu der vom Magnetfeld durchflossenen Fläche und der Übertragungsfrequenz ist, verringert sich mit steigender Übertragungsfrequenz die Anzahl der benötigten Windungen in der Kartenspeule. Während man bei einer Frequenz von  $125\text{kHz}$  zwischen  $100$  und  $1000$  Windungen benötigt, reduziert sich der Bedarf bei  $13,56\text{MHz}$  auf lediglich  $3$  bis  $10$  Windungen.

Der Systemtakt für den Prozessor wird ebenfalls aus der Übertragungsfrequenz gewonnen.

#### 4.3 DATENÜBERTRAGUNG

Auch für die Übertragung der Daten über das Medium Luft gibt es für kontaktlose Smartcards mehrere Lösungsansätze. Ein Ansatz ist die sogenannte „Kapazitive Kopplung“. Hierzu sind sowohl im Terminal als auch in der Smartcard selbst leitende Flächen angebracht. Diese wirken dann beim Einführen der Karte in einen Kartenschlitz oder beim Auflegen auf den Lesebereich als Kondensatorplatten. Wie hoch die erzeugte Kapazität ist, hängt von zwei Faktoren ab, von der Größe und dem Abstand der Kondensatorplatten zueinander. Existiert nun zwischen dem Stromkreis der Karte und des Terminals eine Potentialdifferenz, so entsteht ein elektrisches Feld welches Verschiebungsströme verursacht, die sich dann als Spannungsabfälle in einer dem Nutzsignal überlagerten Störspannung äußern. Da dieses Verfahren aber einen fast direkten Kontakt der Karte mit dem Lesegerät benötigt, hat sich noch ein weiteres Verfahren durchgesetzt, dass es ermöglicht auch Daten über eine größte Distanz zu übertragen. Bei

diesem Verfahren handelt es sich wie bei der Energieübertragung um die induktive Kopplung. Befindet sich die Smartcard im Nahfeld des Terminals, so entzieht diese dem magnetischen Feld Energie. Da sich darauf hin die Stromstärke in der Spule des Terminals erhöht, kommt es zu einem Spannungsabfall im Widerstand  $R_1$  des Terminals. Genau diesen Fakt macht man sich nun zu nutze. Fügt man in der Karte der Spule einen Lastwiderstand  $R_2$  hinzu, kann durch Zu- und Abschalten dieses Widerstandes eine Amplitudenmodulation an der Spannung der Terminalschleife vorgenommen werden. Die auftretenden Spannungsänderungen können nun im Terminal festgestellt und ausgewertet werden. Dieses gefilterte Signal hat leider einen Nachteil, es ist sehr schwach und daher nur sehr aufwendig zu gewinnen. Daher wird bei diesem Verfahren eine Trägerfrequenz verwendet, die dann im Seitenband der Leserfrequenzen auftaucht und unter Verwendung eines Bandpasses problemlos heraus gefiltert werden kann.

#### 4.4 EXISTIERENDE NORMEN

Derzeit existieren insgesamt drei fertiggestellte ISO/IEC-Normen für kontaktlose Smartcards. Bei der ersten handelt es sich um Karten mit einer maximalen Reichweite bis ca. 1cm, den sogenannten „Close Coupling Cards“. Diese müssen zum Lesen in einen Kartenschlitz eingeführt oder auf eine festgelegte Fläche am Terminal aufgelegt werden. Ein Beispiel für diesen Kartentyp ist unter anderem die UniCard der OvGU Magdeburg.

Die andern beiden Normen fast man zusammen unter dem Begriff der „Remote Coupling Cards“. Dies sind Karten die auf einer Entfernung von wenigen Zentimetern bis hin zu etwas einem Meter in der Lage sind, Daten zum Terminal zu übertragen. Diese Karten haben ein breites Spektrum an Anwendungsgebieten und erfreuen sich daher großen Interesses. Als Beispiel zu nennen wären hier zum einen die elektronischen Tickets und Fahrscheine sowie die elektronische Geldbörse.

Kartentyp	Abkürzung	Reichweite	Standards
close coupling	CICC	bis 1 cm	ISO 10536
proximity coupling	PICC	bis 10 cm	ISO 14443
vicinity coupling	VICC	bis 100 cm	ISO 15693

Tabelle 1: Übersicht über die derzeit existierenden Normen für kontaktlose Smartcards.

#### 4.5 DIE MIFARE CARD

Die Mifare ist eine der bekanntesten und am weitesten verbreitetsten Smartcards der Welt. Sie zählt zum Kartentyp der proximity coupling cards. Da man dieser Karte oft begegnet, weil sie in vielen Anwendungsfeldern zum Einsatz kommt, soll sie hier als Beispiel dienen. Sie gehört zu den kontaktlosen Smartcards und ist vielseitig einsetzbar. Auch Witterung und schlechte äußere Bedingungen beeinflussen ihre Funktionsfähigkeit nicht. Bei der Mifare-Technologie handelt es sich um einen offenen Standard der weltweit unterstützt wird. Die wichtigsten technischen Merkmale der

MIFARE 1K aus der Mifare-Kartenfamilie sind:

Material:	PVC
Betriebsfrequenz:	13,56 MHz
Energieversorgung:	passiv
Schreib-/ Leseabstand:	max. 10 cm
Übertragungsrate:	106kBit/s
Datenerhalt:	10 Jahre
Schreibzyklen:	100.000
Temperaturbereich:	-20°C bis + 85°C
Zugriffsmodi:	Schreiben / Lesen oder Schreibschutz/ Schreib- und Leseschutz

Die Mifare kann in einem Abstand von bis zu 10cm problemlos gelesen und geschrieben werden, und strotzt auch sehr starken Temperaturunterschieden, was ihren Einsatz weder im tiefsten Winter noch im heißesten Sommer einschränkt. Der Erhalt der Daten auf der Karte ist mit 10 Jahre sehr hoch und somit sehr zuverlässig. Aus diesem Grund findet die Mifare Card auch großen Anklang als Fahrkarte für den öffentlichen Personen Nahverkehr.

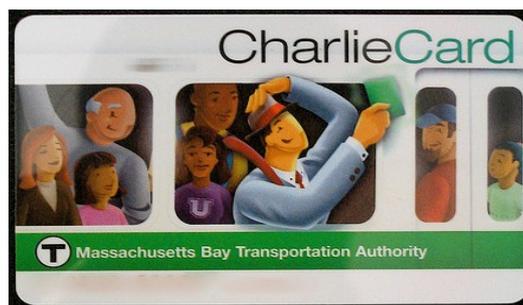


Abbildung 6: Die Charlie Card des MBTA. [ 4 ]

Abbildung 6 zeigt eine der typischen Mifare-Karten wie Sie zum Beispiel in Boston eingesetzt werden, um die Benutzung von Bussen und U-Bahnen zu erleichtern. Die Karte dient zum einen als normale Fahrkarte, zum anderen kann auf die Karte auch ein Geldbetrag geladen werden, der dann nach und nach abgefahren wird. Betritt man mit der Charlie Card eine U-Bahn Station, legt man diese am Eingangstor an, dabei ist es nicht nötig Sie in der Hand zu halten, ein Anlegen der Geldbörse in der sich die Karte befinden reicht vollkommen aus, wird man im System geloggt. Nun kann man frei mit der U-Bahn fahren. Ist man an seiner Zielstation angekommen, hält man hier zum Verlassen des U-Bahnbereiches die Karte an den Leser des Ausgangsgates und loggt sich aus. Dabei wird nun die zurückgelegte Strecke ermittelt, und der zu zahlende Betrag wird von der Karte abgebucht. Das Beispiel der Charlie Card beweist, wie viel einfacher uns Smartcards die Abläufe im alltäglichen Leben machen.

## 5. TICKET PROFILE EDITOR

---

### 5.1 HINTERGRUND ZUR PROGRAMMENTSTEHUNG

Das folgende Programm wurde während des Betriebspraktikums erstellt. Die Arbeit erfolgte in einem Geschäftsbereich der sich mit Systemen für das Fahrgeldmanagement befasste und lieferte einen guten Einblick über die Abläufe der Softwareentwicklung in einer Firma. Wie der Name schon sagt, befasst sich dieser Bereich mit Techniken für Fahrgeldsystem. Dazu zählen vor allem auf Smartcard basierende Lösungen die im öffentlichen Nahverkehr eingesetzt werden. Das Praktikum erfolgte in der Abteilung für Grundsatzentwicklung / Java. Die grundlegenden Aufgaben waren das Einarbeiten in das bereits bestehende und sehr komplexe Smartcard Account Management System sowie:

*„Entwickeln Sie einen Editor zur Pflege und Bearbeitung von Ticketprofilen für Smartcards auf Grundlage der vorhandenen Daten in einer Oracle Datenbank!“*

Bekommt die Firma den Auftrag ein bestehendes Nahverkehrssystem neu zu gestalten und auf Smartcard umzustellen, müssen für dieses System neue kundenspezifische Fahrkarten für die Smartcards erstellt werden. Überschneiden sich die Spezifikationen für neue Fahrkarten mit bereits bestehenden, muss man diese nur von dem alten bereits in der Datenbank existierenden Projekt kopieren und dann in die neue Datenbank einpflegen. Dies geschieht allerdings bisher nur auf dem manuellen Wege, mit Hilfe von sogenannten SQL-Skripten. Diese werden händisch erstellt und dann mittels eines Programms in die Datenbank eingepflegt. Ein Solches Skript besteht aus unzähligen Zeilen von direkten SQL – Skriptbefehlen.

Möchte man hier einen speziellen Datensatz ergänzen oder einen bestehenden Fehler korrigieren, geschieht das nur mühsam per Hand und ist sehr zeitintensiv. Soll ein bestimmter Fahrkartentyp kopiert werden, muss erst der Befehlssatz aus dem Skript gesucht und dann wiederum händisch kopiert und in das neue Skript eingepflegt werden. Das arbeiten mit diesen Skripten ist nicht nur unübersichtlich und sehr fehleranfällig, sondern erfordert auch ein genaues Verständnis über die Erstellung von SQL – Skripten sowie über die einzelnen zu verwendenden Befehle. Aus diesen Gründen entstand der Bedarf an einem Editor der diese und noch viele weitere Aufgaben erledigt und deutlich vereinfacht.

### 5.2 VERWENDETE TECHNIKEN

Wie bereits erwähnt, erfolgte das Praktikum im Bereich der JAVA basierten Softwareentwicklung. Somit stellte sich nicht die Frage, mit welcher

Programmiersprache dieser Editor erstellt werden würde. Zwar wird die Hardware, und damit auch die Smartcardautomaten sowie Smartcardleser mit C beziehungsweise C++ programmiert, jedoch erfolgt die Verarbeitung der durch die C-Programme bereitgestellten Daten in der in JAVA programmierten Leitebene. Da auch dieses Programm mit dieser Leitebene zusammenarbeitet, wurde es in Java erstellt. Bei der für dieses Programm verwendeten Version von Java handelt es sich um 1.5. Der Zugriff auf die Daten in der Datenbank erfolgt über JAVA ODBC. Die zu verwendenden Daten befinden sich in einer Oracle Datenbank auf dem Systemserver. Da die Datenbank mit den echten Ticketprofilen zeitgleich zum Test des Systems sowie von der QS (Qualitätssicherung) verwendet wird, war es nicht möglich, die bestehenden Ticketprofile mit Schreibbefehlen in der Datenbank zu modifizieren, da dies sonst Einfluss auf die laufenden Tests gehabt hätte. Zum Schreiben und Testen der Resultate wurde hierfür eine ebenfalls auf Oracle basierende Testdatenbank zur Verfügung gestellt, die eine Spiegelung der originalen Daten enthielt. Die graphische Oberfläche ist mit Hilfe der JAVA-Swing Bibliotheken erstellt worden, da diese alle für das Programm relevanten Operationen und Funktionen bereit hält. Das Programm wurde in einer Client – Server Architektur erstellt. Um die auf dem Server liegenden Routinen mit Hilfe des Clients ansprechen zu können, kommt hier die sogenannte RMI (remote method invocation) zum Einsatz. Diese gestattet den Aufruf von JAVA Routinen durch den Client, der sich in einer RMI-Registry nach einem Server umschaute, der sich hier registriert hat und die benötigte Routine zur Verfügung stellt. Somit ist der Client in der Lage, Funktionen zu benutzen, die auf einem Server hinterlegt sind.

### 5.3 AUFBAU UND FUNKTION

Bei dem entwickelten Programm handelt es sich wie bereits angesprochen um einen Editor mit graphischer Oberfläche. Wird das Programm das erste mal gestartet, gelangt man auf folgenden Startbildschirm:

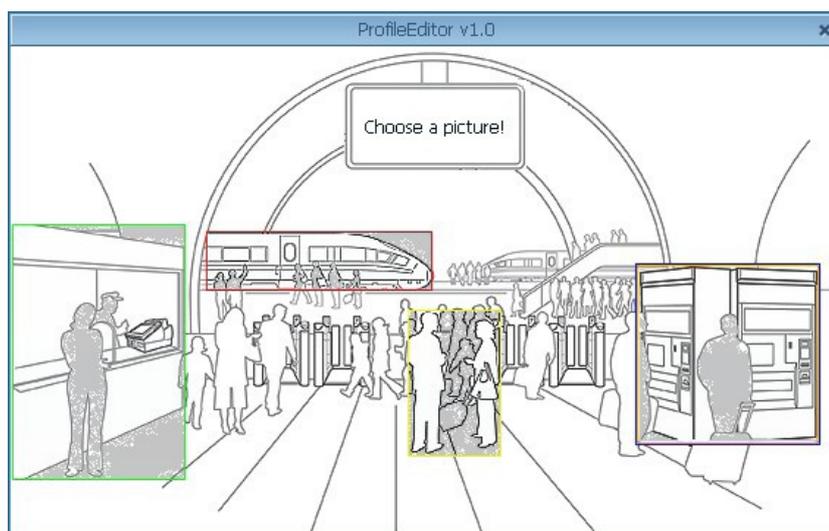


Abbildung 7: Startbildschirm des Ticket Profile Editors.

Der Startbildschirm gliedert sich in 4 Bereiche:

- Ticketschalter (Erstellung eines komplett neuen Tickets)
- Ticketautomat (Arbeiten mit / Modifizieren von bestehenden Ticketprofilen)
- Menschen (Öffnen der Hilfe)
- Zug (sofortiges Verlassen des Programms)

Führt man mit der Maus über einen dieser speziellen Bereiche, hebt sich dieser hervor und die anderen treten automatisch in den Hintergrund. Ein Tooltip informiert den Benutzer dann über die genaue Funktion der aktiven Schaltfläche. Die beiden wichtigsten Funktionen sind hier zum einen die Erstellung eines komplett neuen Tickets, sowie das Arbeiten mit/ beziehungsweise das Modifizieren von bestehenden Ticketprofilen. Entscheidet man sich für die Erstellung eines neuen Tickets, gelangt man in einen Übergangsbildschirm der einem eine Auswahl von möglichen Tickets anbietet. Hier entscheidet der User was für ein Ticket er erstellen möchte. Ob es sich dabei um ein Ticket für den Onlineverkauf, ein Zonenticket oder etwas anderes handelt, spielt für den weiteren Ablauf des Programms keine Rolle. Die Auswahl dieser Ticketeigenschaften spiegelt sich erst in der Datenbankstruktur wieder, in der das neue Ticket dann abgespeichert wird. Möchte man ein bestehendes Ticketprofil bearbeiten, erhält man eine Liste von allen in der Datenbank bereits existierenden Profilen. Wählt man sich eines aus, gelangt man wie auch bei der Erstellung eines neuen Profils, auf das Hauptfenster des Editors.

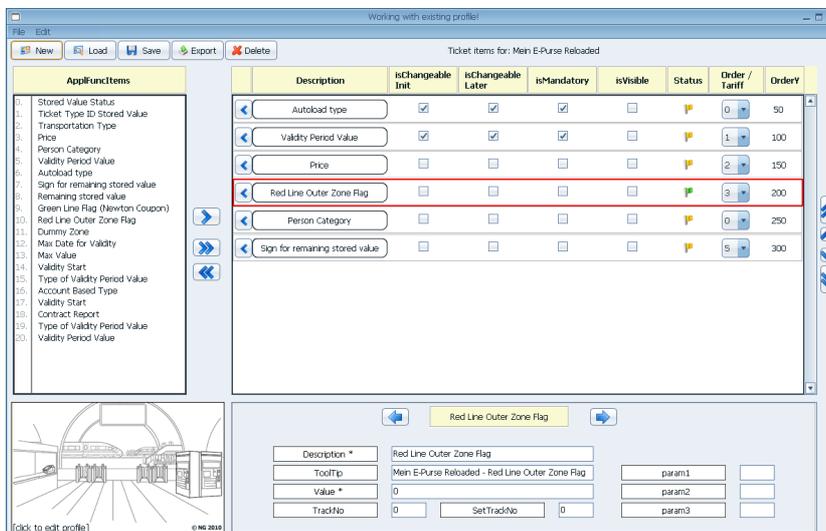


Abbildung 8: Hauptfenster des Ticket Profile Editors.

Das Hauptfenster gliedert sich im Groben in drei Bereiche, in das Fenster der ApplFuncItems am linken Rand, das ItemHolderPanel in der Mitte, das den Großteil des Fensters ausmacht und das Detailfenster im Unteren Teil des Editors. Oben befindet sich wie in jedem Programm eine Menüleiste, in der man nochmals direkt die einzelnen Funktionen des Editors wie zum Beispiel Speichern oder das Erstellen eines weiteren neuen Tickets aufrufen kann.

Wird nun ein neues Ticket erstellt, ist das ItemHolderPanel leer. In diesem befinden sich die sogenannten Items, die ein Ticket genau beschreiben. Zu diesen zählen unter anderem Eigenschaften wie <Preis>, <gültig von>, <gültig bis>, sowie noch viele weitere für die Datenbank und das Managementsystem wichtige Eigenschaften. Möchte man einem Ticket nun neue Eigenschaften in Form von Items hinzufügen, muss man diese aus den sogenannten ApplFuncItems auswählen. Für jeden Tickettypen gibt es einen bestimmten Satz von Items in der Datenbank, die diese Ticket beschreiben. So werden zum Beispiel für ein Onlineticket andere ApplFuncItems angezeigt als für ein Monatsticket. Die entsprechenden Items werden direkt aus der Datenbank geladen und im Editor angeboten. Der dadurch entstehende Vorteil liegt klar auf der Hand. Müsste man so ein Ticket von Hand neu erstellen, bleibt einem nichts anderes über, als in der Datenbank nach den erlaubten Items zu suchen, um keine unzulässigen Items beim Aufbau des Tickets zu benutzen. Hat man nun alle für das Ticket benötigten Items zusammengestellt, werden Sie alle im ItemHolderPanel angezeigt. Die Reihenfolge der Items ( von oben nach unten) spielt für die Anzeige im späteren eine wichtige Rolle. So werden die Items, die oben stehen, auch in der Leitzentrale später an der ersten Stelle angezeigt. Um die Position der Items zu verändern, kann man diese per Drag'n'Drop verschieben. So macht es zum Beispiel keinen Sinn, wenn das Item, dass später den Namen das Karteninhabers symbolisiert, an letzter Stelle steht.

Jedes ausgewählte Item wird noch einmal genauer durch weitere Eigenschaften bestimmt, die im Detailfenster bearbeitet werden können. Da einige dieser Eigenschaften sogenannte „mandatory fields“, also Pflichtfelder sind und ausgefüllt werden müssen, besitzt jedes Items eine Statusanzeige im ItemHolderPanel. Erst wenn alle Items eines Tickets valide sind, kann das Ticket gesichert werden. Diese Pflichtfelder werden durch die Struktur der Datenbank bedingt, so gibt es dort zum Beispiel Spalten, deren Wert „not null“ sein darf, oder einen Zahlenwert erfordern. Somit muss hier unbedingt ein Wert eingetragen werden, da sonst die Integrität der Datenbank verletzt werden würde. Sollte es in der Auswahl ein invalides Items geben, so stehen die Speicheroptionen nicht zur Verfügung.

Ist die Erstellung des Tickets abgeschlossen, stehen zwei Möglichkeiten zur Verfügung dieses zu sichern. Die erste ist das einfache Speichern. Dabei wird das Ticket direkt in der Datenbank gespeichert und alle dafür relevanten Verknüpfungen werden angelegt. Dies erfolgt über einen bereits im Firmenframework existierenden Service, der mittels RMI angesprochen wird. Sollte man das Ticket nicht direkt in der Datenbank speichern wollen, da es zeitgleich auf der Datenbank stattfindende Test beeinflussen könnte, oder zum Beispiel beim Kunden in eine bereits bestehende Datenbank als ergänzendes Ticket eingepflegt werden soll, gibt es die Option, ein SQL-Skript zu erzeugen. Dieses Skript besitzt dann den selben Aufbau wie das früher händisch erstellte und bietet somit die Möglichkeit, es auf eine beliebige Datenbank auszuführen und somit ein Ticket hinzuzufügen, zu modifizieren oder sogar zu löschen.

Die nun in der Datenbank angelegten Ticketprofile werden später als reale Fahrkarten in Form von Smartcards produziert, und sind dann bereit für den Einsatz im Alltag.

## 6. ABSCHLUSSBETRACHTUNGEN

---

Das Ziel dieser Arbeit war es, einen Einblick in die Technologie der Smartcards zu gewinnen. Der Aufbau dieser wurde näher betrachtet und ein breites Spektrum an Einsatzgebieten dargestellt. Es zeigte sich, dass die Einsatzmöglichkeiten der Smartcards nahezu grenzenlos sind. So handelt es sich bei diesen Karten nicht um irgendwelche Exoten, die nur in wissenschaftlichen Einrichtungen zum Einsatz kommen, sondern jeder Mensch besitzt einige dieser cleveren Geräte. Sie erleichtern die täglichen Abläufe und machen den Ablauf dieser Dinge angenehmer. Ohne die Technologie der Smartcards, wäre ein Geldabholen am Automaten nicht möglich. Auch der Besuch beim Arzt würde sich komplizierter gestalten, wenn man keine Krankenkassenkarte besäße. Waren die Karten früher nur ein Aushängeschild für die reichere Bevölkerungsschicht die mit „Ihrem guten Namen“ damit zahlte, so hat heute jeder Zugang zu diesen Karten. Die Entwicklung macht große Schritte und geht ständig voran. So wurden aus den einstigen Magnetstreifenkarten, die noch einige Sicherheitslücken aufwiesen im Verlauf der Zeit technisch ausgereifte und sehr sichere Chipkarten. Je kleiner die für die Smartcards verwendete Chiptechnologie wird, um so leistungsfähiger werden diese Miniaturcomputer. Ein Ende dieser Entwicklung ist noch nicht in Sicht und es bleibt abzuwarten, wo uns in Zukunft Smartcards begegnen und erstaunen werden.

Das während des Praktikums erstellte und in dieser Arbeit vorgestellte Programm erfüllte die vom Praktikumsbetrieb gestellten Anforderungen vollständig und wird dort voraussichtlich bei der Bearbeitung des nächsten Auftrages zum Einsatz kommen. Die Arbeitsprozesse bei der Erstellung und Verwaltung von Ticketprofilen wurden durch das Programm deutlich vereinfacht und es ist nun auch Personen möglich neue Profile zu erstellen, die nicht über ein komplettes Hintergrundwissen über die Datenbankstrukturen verfügen.

In Zukunft wäre es möglich, das Programm weiterhin auszubauen. Derzeit ist es nur an die persönlichen Anforderungen des Betriebes angepasst und dient ausschließlich der innerbetrieblichen Nutzung. Das Programm läuft eigenständig und greift nur über das Firmenframeworks auf Informationen zu. Es ist allerdings denkbar, das Programm dahingehend zu modifizieren, dass es als fester Bestandteil in das bestehende Framework eingeht und somit auch dem Kunden als Editor zur Verfügung steht, um selbst Ticketprofile zu verwalten, zu modifizieren.



## LITERATURVERZEICHNIS

---

- [ 1 ] Wolfgang Rankl und Wolfgang Effing. *Handbuch der Chipkarten*. 4., überarbeitete und aktualisierte Auflage, Carl Hanser Verlag München Wien, ISBN 3-446-22036-4
  
- [ 2 ] Klaus Finkenzeller. *Grundlagen und praktische Anwendungen von Transpondern, kontaktlosen Chipkarten und NFC*. 5., aktualisierte und erw. Auflage, Carl Hanser Verlag München Wien, ISBN: 978-3-446-41200-2
  
- [ 3 ] <http://www.itwissen.info/> . Das große Online-Lexikon für Informationstechnologie.
  
- [ 4 ] <http://mifare.net/> . Homepage über die Mifare Smartcards
  
- [ 5 ] „SmartCard - Was ich schon immer wissen wollte.“  
Firmeninterne Präsentation meines Praktikumsbetriebes zum Thema Smartcards.

## **ABSCHLIEBENDE ERKLÄRUNG**

---

Ich versichere hiermit, dass ich die vorliegende Studienarbeit selbständig, ohne unzulässige Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Weisen, den 20. Oktober 2010

Nico Gebauer