Universität Trier
Fachbereich IV - Wirtschaftsinformatik

Smart Cards

Seminararbeit
im Fach Wirtschaftsinformatik
Sommersemester 2001

Inhaltsverzeichnis

Abbildungsverzeichnis

Seite

Abkürzungsverzeichnis

DES.....	Data Encryption Security
EPROM.....	Electrical Programmable Read Only Memory
EEPROM.....	Electrical Erasable Programmable Read Only Memory
GSM.....	Global System for Mobile Communications
ICC.....	Integrated Circuit Card
ID.....	Identifier
IEC.....	International Electrotechnical Commission
I/O.....	Input / Output
ISO.....	International Organisation for Standardisation
NPU.....	Numeric Processing Unit
PIN.....	Personal Identification Number
RAM.....	Random Access Memory
ROM.....	Read Only Memory
RSA.....	
SIM.....	Subscriber Identity Module

1 Ziel und Aufbau der Arbeit

Im alltäglichen Sprachgebrauch sind ec-Karten, Kreditkarten oder Telefonkarten inzwischen durchaus geläufige Begriffe. Spätestens seitdem das Portemonnaie fast mehr Karten als Münzen beinhaltet, sind die handlichen Plastikkarten in vielen Bereichen nicht mehr wegzudenken. Durch die ständige Verbesserung der Karten- und Chiptechnik wird zudem eine Vielzahl weiterer sinnvoller Anwendungen hinzukommen.

Im Kontext dieser rasanten Entwicklung ist der Begriff der Prozessorkarte zu sehen. Vertraut man der Aussagekraft einer Studie von Forrester Research Deutschland, so steht der *"intelligenten Plastikkarte eine Blütezeit bevor."*[1] Die "Smart Card"[2], wie die Prozessorkarte auch genannt wird, soll u. a. bisherige Bezahlverfahren im e-Business revolutionieren.[3] Trotz des vielfältigen Einsatzes stellen Chipkarten und der Begriff der "Smart Card" für viele Endanwender im wahrsten Sinne des Wortes immer noch Fremdwörter dar.

An diesem Punkt setzt diese Seminararbeit an. Ziel ist es, den Begriff der "Smart Card" in den Kontext der Plastik- und Chipkarten einzuordnen und überwiegend auf wirtschaftliche Aspekte einzugehen.[4] Die Geschichte der Kartentechnik, bestehende Normen und der generelle Kartenaufbau ermöglichen dem Leser einen grundlegenden Einstieg in das Thema. Alle existierenden Kartenarten mit ihren individuellen Funktionalitäten, Eigenschaften und wesentlichen Vor- und Nachteilen werden im Anschluß daran vorgestellt. Da der Erfolg der Plastikkarten auch auf einfach zu realisierende Sicherheitsvorkehrungen zurückzuführen ist, werden die wesentlichen Aspekte erläutert. Einige ausgewählte Beispiele stellen daraufhin die allgemeine Bedeutung der Karten für die Praxis und ihre Anwendungsbereiche heraus. Der Schwerpunkt liegt in dieser Arbeit insbesondere auf den aktuellen Anwendungsmöglichkeiten der "Smart Card". Ein Ausblick auf zukünftige Entwicklungen rundet die Seminararbeit ab.

---

1 Nieman, Frank: Anbieter von Web-Bezahlsystemen entdecken den Konsumenten, in; Computerwoche, Ausgabe Nr. 2, 2001, S. 54.

2 smart card (engl.) = intelligente Karte.

3 Vgl. Nieman, Frank: Anbieter von Web-Bezahlsystemen entdecken den Konsumenten, a. a. O., S. 54 f.

4 Aufgrund des begrenzten Umfanges der Arbeit ist nur ein knapper Einstieg ins Thema möglich. Für einen detaillierteren technischen Einblick wird Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten, Aufbau - Funktionsweise - Einsatz von Smart Cards, 3. Auflage, München: Carl Hanser Verlag 1999 empfohlen.

2 Grundlagen

2.1 Die Geschichte der Plastikkarte

Zu Beginn der 50er Jahre wurden in den USA durch den "Diner's Club" und kurze Zeit später durch VISA und Mastercard erstmals Papierkarten durch Karten aus Plastik ersetzt. Diese Plastikkarten waren reine Identifikationskarten, die den Besitzern einen bargeldlosen Zahlungsverkehr ermöglichten. Zur eindeutigen Identifikation diente eine Hochprägung oder/und die eigene Unterschrift auf der Karte. Da die Kartendaten aufgrund der eingesetzten Techniken schlecht auszuwerten und zu verbuchen waren, wurden wenig später Magnetstreifenkarten eingeführt, die eine leichtere automatische Erfassung ermöglichten. Als im Jahre 1968 die beiden Deutschen Jürgen Detholff und Helmut Grötrupp ein Patent für den Einbau integrierter Schaltflächen in die bis dahin primitiven Identifikationskarten anmeldeten, begann der eigentliche Siegeszug der Chipkarten. Schnell folgten weitere Patente in Japan und Frankreich. Nachdem aus mehreren Pilotversuchen die Chipkarte als eindeutiger Sieger gegenüber den vorherigen Kartentypen hervorgegangen war, wurden die Karten in mehreren Bereichen erfolgreich eingesetzt. So z. B. 1994 bei der bundesweiten Einführung der Krankenversicherungskarte in Deutschland oder 1997 durch den Einsatz der ec-Karte im Banksektor. Im gleichen Jahr waren u. a. bereits mehr als 100 Millionen Telefonkarten im Einsatz.[5]

2.2 Normen und Standards

Die große wirtschaftliche Bedeutung der Chipkarten führte schon frühzeitig dazu, Anstrengungen zu nationalen und internationalen Standardisierungen in die Wege zu leiten. Die wesentlichen Ergebnisse sind heute in den Standards ISO[6] 7810 - 7813 und ISO/IEC 7816 zu finden. Dort werden die physikalischen, elektrischen und anwendungsübergreifenden Eigenschaften aller Kartentypen festgelegt. Jeder, der sich an diesen Normen orientiert, kann dadurch mit standardisierten Vorgaben planen. Die fast

---

5 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten, Aufbau - Funktionsweise - Einsatz von Smart Cards, a. a. O., S. 30 ff.

6 Die ISO (International Organisation for Standardísation) wurde 1946 gegründet. Ihr gehören inzwischen mehr als 90 Normungsgremien an. Vgl. Linke, Marcus; Winkler, Peter: Das M&T Computer Lexikon, München, Heyne Verlag 1999, S. 199.

maßstabsgetreue Abbildung 1 eines ID-1 Kartenformats[7] verdeutlicht exemplarisch einige dieser vordefinierten Merkmale. Z. B. die Kartenabmessungen, die bis auf den Millimeter exakt festgelegt wurden (85,7 x 54 x 0,76 mm ohne Toleranzbereich) oder die Einteilung der Kartenoberfläche, die neben dem heute hauptsächlich verwendeten Chip (siehe grauer Bereich) eine gleichzeitige Integration von Magnetstreifen- und Hochdrucktechnologien ermöglicht.[8]

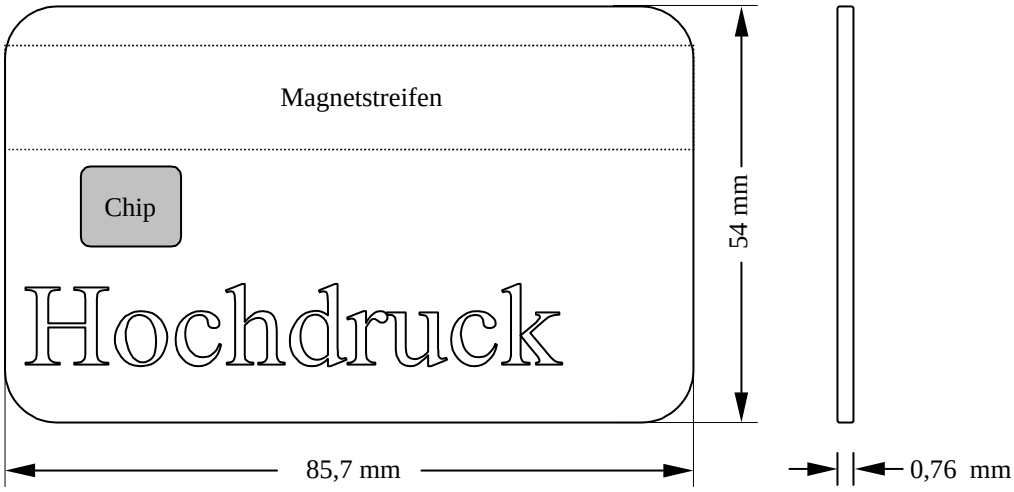

Abb. 1: Format ID-1 und Lage Hochdruck, Chip und Magnetstreifen

Karten, die mehrere Technologien[9] vereinen, werden als Hybridkarten bezeichnet.[10] Hybridkarten finden meist als Übergangslösung Verwendung, die alte Techniken mit Neuen vereinen. Auf diese Weise können Lesegeräte, die zur Auswertung und Stromversorgung bereits älterer Kartengenerationen gedient haben, weiterhin eingesetzt werden. Als Beispiel für Hybridkarten sind die ec-Karten der Banken zu nennen, die außer einem Chip, zudem einen Magnetstreifen aufweisen.

---

7 Neben dem ID-1 Format, welches in der Größe z. B. der bekannten Kreditkarte entspricht, existieren noch die Formate ID-00 (z.B. Dekoderkarte für das Pay-TV) und ID-000 (z. B. SIM-Karte in Handys). Betrachtet man den technischen Aufbau sind alle drei Formate absolut identisch. Vgl. Schütt, Stefan; Kohlgraf, Bert: Chipkarten Technische Merkmale, Normung, Einsatzgebiete, München: Oldenbourg Verlag 1996, S. 19.

8 Vgl. Schütt, Stefan; Kohlgraf, Bert: Chipkarten Technische Merkmale, Normung, Einsatzgebiete, a. a. O., S. 31.

9 Außer den bisher genannten existieren weitere Kartentechnologien, die in Kapitel 3 näher erläutert werden.

10 Vgl. Rankl, Wolfgang / Effing, Wolfgang: Handbuch der Chipkarten, Aufbau - Funktionsweise - Einsatz von Smart Cards, a. a. O., S. 847.

2.3 Definitorische Abgrenzung des Begriffs "Smart Card"

In der Fachliteratur werden unterschiedliche Definitionen für den Begriff der "Smart Card" verwendet. Abbildung 2 gibt einen Überblick über die verschiedenen Kartenarten und erlaubt es, die "Smart Card", so wie sie in dieser Arbeit verstanden wird, einzuordnen. Kapitel 3 beschreibt im Folgenden die einzelnen Kartentypen genauer. Die dort eingehaltene Reihenfolge entspricht in etwa auch der chronologischen Entwicklung.

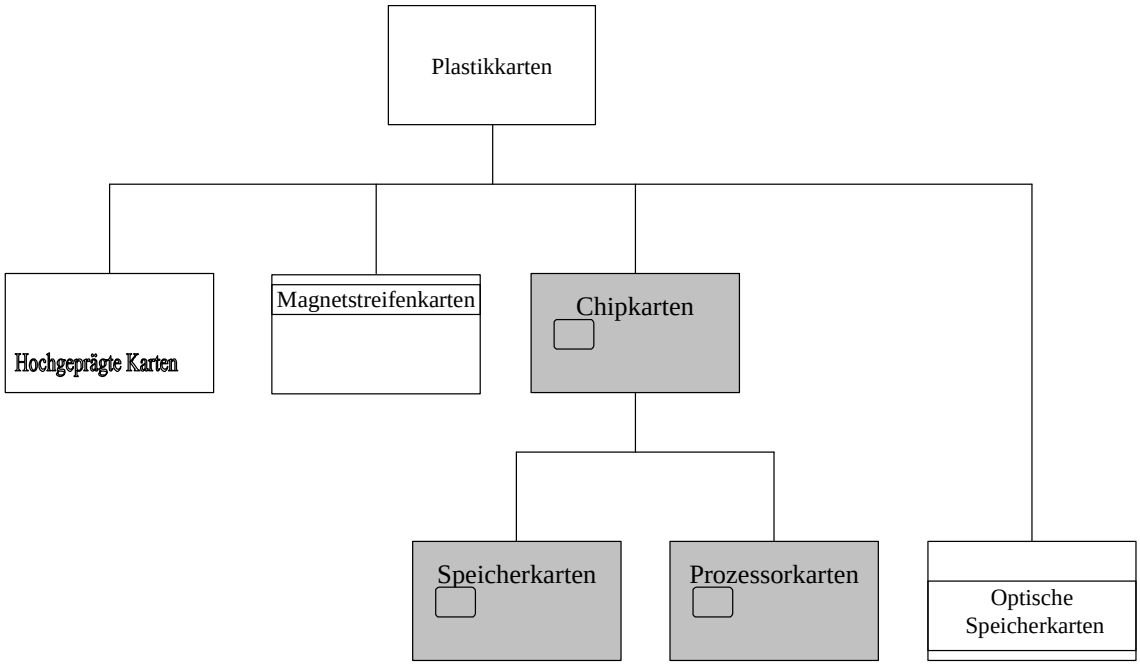

Abb. 2: Kartenarten

In dieser Arbeit wird unter einer "Smart Card" (= Prozessorkarte) eine Chipkarte verstanden, die mit einem (Mikro-) Prozessor und Speicher (RAM, ROM und EE-PROM) und eventuell auch noch einem zusätzlichen (Co-) Prozessor[11] ausgestattet ist[12] (siehe auch 3.3.2). Oftmals wird in der Literatur eine etwas weiter gefasste Definition verwendet, welche die "Smart Card" als Oberbegriff aller Chipkarten versteht.[13] In diesem Fall zählen Speicherkarten ebenfalls zu den Smart Cards. Unabhängig davon, welche der beiden Definition betrachtet wird, werden diese Kartentypen hauptsächlich zum Speichern und Austausch von Daten eingesetzt.

---

11 Dieser Prozessor ist ein sogenannter (Krypto-) Prozessor, der speziell für die schnelle Berechnung von Verschlüsslungsalgorithmen entwickelt wurde.

12 Vgl. http://members.tripod.de/atrtt/faq/faq.htm.

13 Vgl. bspw. http://www.smartcardbasics.com oder http://www.stefan-lenz.ch/glossar/smartcard.htm.

3 Kartenarten

3.1 Hochgeprägte Karten

Die älteste Kartentechnik ist die Hochprägung, auch Embossing genannt. Die Art und Lage der Hochprägung, die sich in zwei Bereiche untergliedert, ist im Standart ISO 7811 (Teil 1 und Teil 3) spezifiziert. Die Hochprägung ist eine sehr einfache Technik, die keine elektrische Energie erfordert. Zudem konnten die hoch gedruckten Zeichen, im Gegensatz zu einer individuellen Unterschrift auf der Karte, durch kostengünstige Geräte, bereits um 1950 maschinell ausgelesen werden. Dies ermöglichte den weltweiten Einsatz dieses Kartentyps, insbesondere auch in unterentwickelten Ländern. Einen entscheidenden Nachteil stellen jedoch die laufenden Kosten für die Auswertung der Daten mittels Papierausdruck dar. Zudem finden nur sehr wenige Informationen auf dem nach ISO-Norm vordefinierten Bereich Platz.[14]

3.2 Magnetstreifenkarten

Mit Hilfe eines auf der (Karten-) Rückseite angebrachten Magnetstreifens können Informationen in digitaler Form, geschrieben, gespeichert und gelesen werden. Der Streifen selbst besteht aus drei Magnetspuren, die in den Teilen 2, 4 und 5 der ISO 7811 festgelegt wurden. Neben einer geringen Speicherkapazität besitzen Magnetstreifenkarten ein hohes Sicherheitsrisiko, da die Daten mit relativ geringem Aufwand gelöscht oder verändert werden können. Heute noch im Einsatz befindliche Magnetstreifenkarten, wie z. B. die ec-Karten, benötigen aus diesem Grund zusätzliche Sicherheitsmechanismen in Form eines unveränderlichen unsichtbaren Codes oder einer PIN, die es bei der Eingabe ermöglicht per Online-Verfahren die Korrektheit einer Transaktion zu überprüfen.[15]

---

14 Online im Internet: http://www.informatik.fh-muenchen.de/~chipcard/vortrag1/seite1.html.

15 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten, Aufbau - Funktionsweise - Einsatz von Smart Cards, a. a. O., S. 45.

3.3 Chipkarten

3.3.1 Speicherkarten

Speicherkarten, die auch als synchrone Chipkarten bezeichnet werden,[16] sind mit einem eingebauten Halbleiterchip versehen (ISO 7813). Wahlweise verfügen diese Speicherchips über sechs oder acht Kontaktflächen, mit denen die Kommunikation (I/O) mit den Kartenlesegeräten stattfindet. Abbildung 3 stellt schematisch den Aufbau eines Speicherchips dar. Alle Speicherkarten sind neben einem Logikteil mit ROM und je nach Baujahr mit dem älteren EPROM- oder dem neueren EEPROM-Speicher[17] ausgestattet. Speicherkarten können im Vergleich zu Magnetstreifenkarten ein Vielfaches an Informationen speichern.[18] Der Logikteil, der den Zugriff auf die Speicherbausteine steuert, setzt sich aus einer Adreß-, Reset- und Programmierlogik zusammen.

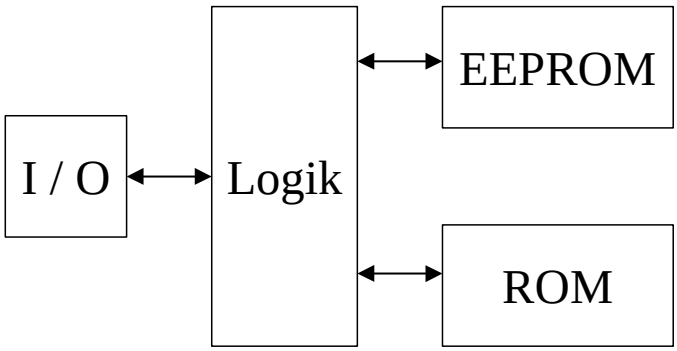

Abb. 3: Schematischer Aufbau eines Speicherchips[19]

Die Kartenlogik kann optional um eine Sicherheitslogik erweitert werden. Anhand dieses Merkmals unterscheidet man zwei Unterarten von Speicherkarten:

- reine Speicherkarten ohne Sicherheitslogik und
- intelligente Speicherkarten mit Sicherheitslogik.

---

16 Bei einer synchronen Übertragung der Daten ist das Signal zwischen Quelle und Ziel gleichgetaktet. Vgl. Linke, Marcus; Winkler, Peter: Das M&T Computer Lexikon, München, Heyne Verlag 1999, S. 199.

17 EPROM kann nur einmal beschrieben und nicht mehr gelöscht werden, während EEPROM mehrfach einsetzbar ist.

18 Aufgrund der nach ISO-Norm restriktierten Größe der Chipfläche (25 x 25 mm), um deren Bruchsicherheit zu gewährleisten, stößt die Speicherkapazität nach heutigem Stand der Technik bei Speicherkarten bei 16 kByte (bei Prozessorkarten bei 32 kByte) an ihre Grenzen. Online im Internet: http://www.smartcardbasics.com, Kapitel 2.

19 In Anlehnung an: Schütt, Stefan; Kohlgraf, Bert: Chipkarten Technische Merkmale, Normung, Einsatzgebiete, a. a. O., S. 23.

Trotz der Sicherheitslogik bieten diese Karten keine ausreichende Garantie, sensible Daten vor Manipulation und Missbrauch zu schützen. Beide Arten sind heute in vielen Bereichen im Einsatz. Vor allem dort, wo preisgünstige Massenanwendungen verlangt sind, die mehr Speicher und Sicherheit als Magnetstreifenkarten bieten müssen, aber nicht unbedingt die Leistungsstärke und Funktionalität einer Prozessorkarte benötigen (siehe 3.3.2). Die Wahl des Kartentyps für die deutsche Krankenversicherung verdeutlicht auf anschauliche Weise die Entscheidung für einen solchen Kompromiss. Zum einen musste genügend Speicher zur Verfügung stehen, um die grundlegenden Patientendaten, wie Name, Strasse, Ort, Name der Krankenkasse, etc. speichern zu können. Zum anderen sollten für eine reibungslose und flächendeckende Einführung die Kosten sowohl für die Karte als auch für die zur Auslesung notwendigen Lesegeräte in den Praxen, Krankenhäusern und Krankenkassen nicht zu teuer sein. Daher die Wahl der Speicherkarte als geeignete Zwischenlösung, die dennoch Optionen für den Ausbau des Systems offen lässt. Zum jetzigen Stand stellt die Krankenversicherungskarte aufgrund der Wahl einer Speicherkarte nur einen digitalen Ersatz für den Krankenschein dar.[20] Die Speicherung sensibler Daten, wie die Krankheitsgeschichte oder Medikamentenlisten, sind aufgrund der unzureichenden Sicherheitsvorkehrungen der eingesetzten Speicherkarten nach dem Datenschutzgesetz nicht erlaubt.[21]

3.3.2 Prozessorkarten

Anstelle des in Speicherkarten verwendeten Logikteils wird in Prozessorkarten (asynchrone Chipkarten[22]), ein Mikroprozessor (CPU) verwendet. Neben dem für interne Berechnungen notwendigen Arbeitsspeicher (RAM) wird häufig zudem ein zweiter Prozessor (NPU[23]) eingesetzt, der speziell für die schnelle Berechnung numerischer Verschlüsselungsalgorithmen entwickelt wurde. Dieser greift auf denselben RAM wie die CPU zurück. Alle anderen Komponenten und die Datenflüsse sind, wie auch Abbildung 4 verdeutlicht, mit denen einer Speicherkarte identisch.

---

20 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten, Aufbau - Funktionsweise - Einsatz von Smart Cards, a. a. O., S. 671.

21 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten, Aufbau - Funktionsweise - Einsatz von Smart Cards, a. a. O., S. 49, 97.

22 Bei einer asynchronen Übertragung der Daten muss das Signal zwischen Quelle und Ziel nicht gleichgetaktet sein. Vgl. Linke, Marcus; Winkler, Peter: Das M&T Computer Lexikon, a. a. O., S. 199.

23 NPU = Numeric Processing Unit.

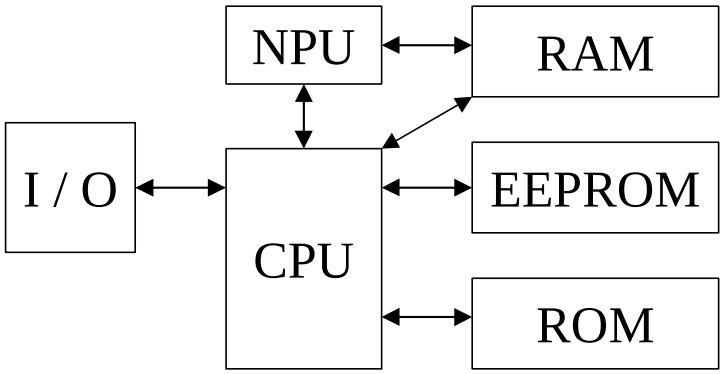

Abb. 4: Schematischer Aufbau eines Prozessorchips[24]

Durch den (Mikro-) Prozessor, der von der Leistung in etwa mit dem Modell eines Personalcomputer 80286 zu vergleichen ist,[25] stehen dem Anwender potentiell viele neue Einsatzmöglichkeiten zur Verfügung. Das Betriebssystem und eine Kartenprogrammiersprache wie z. B. Java 2.0[26] ermöglicht es im nachhinein neue Anwendungen auf den Chip zu laden und/oder alte Software zu löschen. Generell können auch mehrere Anwendungen (Multifunktionalität) zur gleichen Zeit auf der Karte gespeichert und nacheinander abgerufen werden. Prozessorkarten besitzen gegenüber den bisher vorgestellten Kartentypen zudem den entscheidenden Vorteil, dass durch die Verwendung eines Zweitprozessors, die Sicherheit und der Schutz sensibler Daten erheblich verbessert werden kann (siehe Kapitel 4).[27]

Aufgrund ihrer Bauweise und Funktionalität sind "Smart Cards", im Gegensatz zu anderen Kartenarten, die nach dem Gebrauch meistens wertlos werden, für einen längeren oder sogar dauerhaften Einsatz geeignet. Lediglich die Kontaktflächen (I/O) des Chip, welche die Verbindung zu den Lesegeräten herstellen um Daten mit der Aussenwelt auszutauschen, unterliegen bei hoher Belastung noch einem starken Verschleiss. Aus diesem Grund wurden in den letzten Jahren kontaktlose Prozessorkarten entwickelt, die die Haltbarkeitsdauer der Karte insgesamt erheblich erhöhen. Dank dieser neuen Übertragungsmöglichkeit[28] sind zusätzliche Einsatzfelder entstanden. So

---

24 In Anlehnung an: Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten, Aufbau - Funktionsweise - Einsatz von Smart Cards, a. a. O., S. 50.

25 Wo steht dieses scheißß zitat!!!!!!!!!!!!!!!!!

26 Quelle zu Internetseite fehlt!!!!!!!!!!!!!!!!!!!!!

27 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten, Aufbau - Funktionsweise - Einsatz von Smart Cards, a. a. O., S. 50.

28 Die Verbindung des Lesegerätes mit der Karte erfolgt über induktive oder kapazitive Kopplung per Funk.

können Anwendungen "praktisch im Vorbeigehen" automatisch aktiviert und durchgeführt werden, ohne die Karte dafür explizit benutzen zu müssen. Nach dem für eine erfolgreiche Transaktion erforderlichen Abstand der Karte zur Empfangsstation unterscheidet man zwei Typen von kontaktlosen Karten, die genauer in der ISO / IEC 10536 beschrieben werden:

- "close coupling card" (für den Datenaustausch in unmittelbarer Nähe) und
- "remote coupling card" (für den Datenaustausch bis zu Satellitenentfernungen).[29]

In einigen Pilotversuchen werden die Karten im Personennahverkehr und an Flughäfen derzeit als Ticketersatz getestet. Die Technik ermöglicht eine schnellere Abwicklung an den Kassenschaltern. Jedoch befinden sich die Tests noch in einem Anfangsstadium, in dem Probleme, wie z. B. die gleichzeitige Aktivierung mehrerer, im Empfangsbereich des Lesegerätes befindliche Karten mittels Kollisionsbeseitigung gelöst werden müssen. Zudem sind die Kosten, nicht nur für diesen Kartentyp, sondern auch für die dafür notwendigen Empfangsgeräte noch sehr hoch.[30]

3.4 Optische Speicherkarten

Wird für spezielle Anwendungen mehr Speicherplatz benötigt, als herkömmliche Chipkarten aufgrund ihres begrenzten Platzes auf dem Chip zur Verfügung stellen, können optische Speicherkarten eingesetzt werden. Optische Speicherkarten, die in der ISO / IEC 11693 und 11694 näher spezifiziert sind, erlauben in Kombination mit dem zusätzlichen Einsatz eines Chips eine optimale Ausnutzung von Speicherkapazität im Megabyte-Bereich sowie optionaler Sicherheitsmöglichkeiten. Einziger Nachteil ist, dass optische Speicher nur ein einziges Mal beschrieben werden können. Das Löschen oder Verändern von Daten ist somit nicht möglich. Anwendung findet diese Art von Hybridkarte vorwiegend in Krankenhäusern, um bspw. Röntgenbilder zu speichern.[31]

---

29 Vgl. Schütt, Stefan; Kohlgraf, Bert: Chipkarten Technische Merkmale, Normung, Einsatzgebiete, a. a. O., S. 125.

30 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten, Aufbau - Funktionsweise - Einsatz von Smart Cards, a. a. O., S. 51 ff.

31 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten, Aufbau - Funktionsweise - Einsatz von Smart Cards, a. a. O., S. 54 f.

4 Kartensicherheit

4.1 Generelle Sicherheitsaspekte von Plastikkarten

Der Aspekt, Daten sicher vor Manipulation und Mißbrauch zu schützen, steht bei Chipkarten, die heute fast ausschließlich zur Verwahrung und Übertragung sensibler Daten des Trägers verwendet werden, im Vordergrund. Ansonsten würden sich Karten nicht wesentlich von anderen Datenträgern wie z. B. Disketten unterscheiden. Neben den bereits in Kapitel 3 genannten, vom Kartentyp abhängigen Sicherheitsmerkmalen sind im Laufe der Entwicklung eine Vielzahl weiterer Eigenschaften und Komponenten hinzu gekommen, die Unbefugten und sogar den Kartenträgern selbst den Mißbrauch erschweren sollen. Diese lassen sich in die vier Kategorien (1) Kartenkörper, (2) Hardware, (3) Software und (4) Anwendung einteilen (vergleiche Abbildung 4).

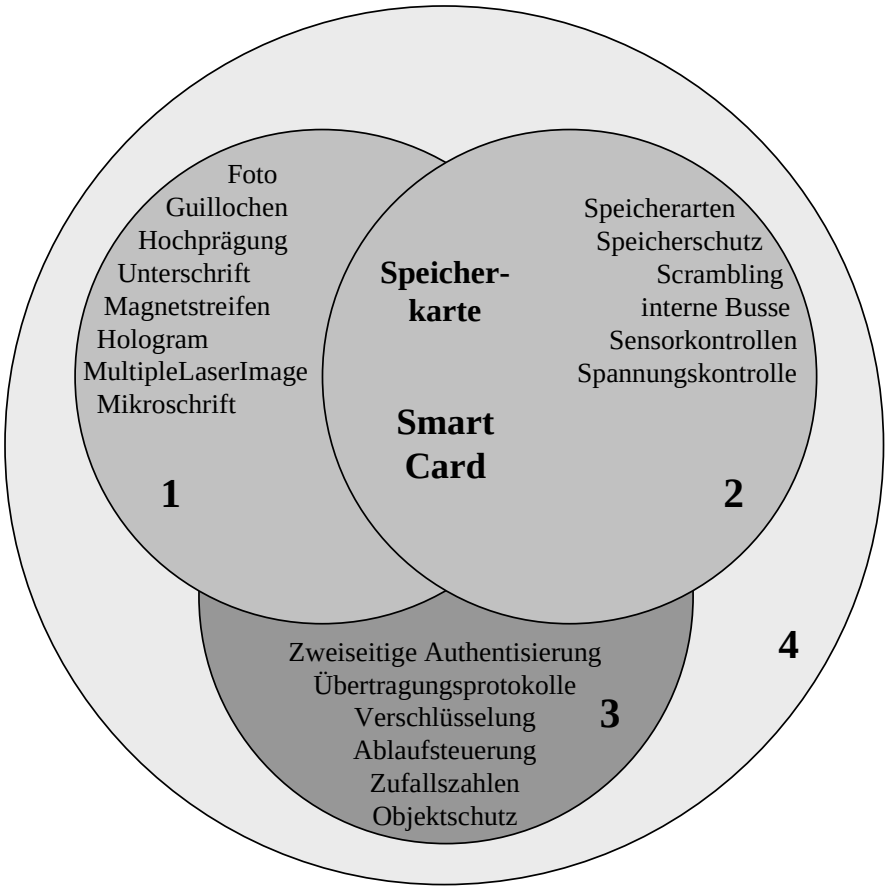

Abb. 5: Sicherheitsmöglichkeiten für Chip- oder Prozessorkarten[32]

[32] In Anlehnung an: Online im Internet: http://www.informatik.uni-trier.de/~damm/Lehre/E-Money/Augustin/semina~1.htm, S. 22.

Viele Sicherheitskomponenten des ersten Bereiches stammen aus den Anfängen der Kartengeschichte. Persönliche Unterschrift oder der in Hochdruck geschriebene eigenen Namen waren gleichzeitig Sicherheitsmerkmal und aufzubewahrende Identifikationsdaten. Noch bis heute dienen diese beiden Elemente, ebenso wie die anderen aufgelisteten Merkmale rund um den Kartenkörper (1) der visuellen Kontrollmöglichkeit durch den Menschen. Diese Komponenten sind jedoch relativ leicht zu fälschen.[33]

Dem gegenüber stehen die Sicherheitsvorkehrungen des zweiten Bereiches, die speziell für den Chip entwickelt wurden. Diese bleiben dem menschlichen Auge ohne Zuhilfenahme technischer Instrumente verborgen. Im Bereich der Hardware (2) werden die dargestellten Sicherheitsoptionen, wie z. B. das Scrambling[34], während der Produktion unter hoher Geheimhaltung auf und in den miniaturisierten Chip integriert. Das Ausspionieren der Architektur des Chipinneren ist daher für Dritte mit einem hohen Zeit- und Kostenaufwand verbunden. Nachteil ist, dass auch dem Betreiber vergleichbare Aufwände entstehen, wenn die Korrektheit einer im Einsatz befindlichen Karte mittels teurer Terminals überprüfen werden muss.

4.2 Spezifische Sicherheitsaspekte einer "Smart Card"

Für Computern existieren seit langem eine Vielzahl von diversen Sicherheitsmechanismen. Seitdem Mikroprozessoren auch auf einem Kartenchip Platz finden, konnten aus diesem Umfeld verschiedene Verfahren einfach übernommen werden. So z. B. die Verfahren der gegenseitige Authentifizierung oder der Datenverschlüsselung, mit deren Hilfe zwei wesentliche Schwachstellen einer Karte nahezu ausgeschlossen werden können;[35] dies ist zum einen das unbefugte Lesen von Informationen und zum anderen die unbefugte Nutzung einer fremden Karte oder eines Terminals.

---

33 Alle Sicherheitskomponenten, die aufgrund des begrenzten Seitenumfanges nicht explizit beschrieben werden, sind auf der folgenden Internetseite http://www.informatik.fh-muenchen.de/~chipcard/vortrag1/birgit/chip_sec2.html anschaulich dargestellt und erläutert.

34 Scrambling = Vermischtes Anordnen interner Busse auf dem Chip eines Mikrocontroller, so dass die Funktionszuordnung ohne Hintergrundinformationen nicht mehr möglich ist. Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten, Aufbau - Funktionsweise - Einsatz von Smart Cards, a. a. O., S. 757.

35 Statistisch gesehen, ist es trotz des Einsatzes modernster Techniken momentan nicht möglich, die korrekte Entschlüsselung von Algorithmen mit exponentieller Komplexität in akzeptabler Zeit (d. h. nicht unter mehreren hundert Jahren) durchzuführen. Vgl. Schütt, Stefan; Kohlgraf, Bert: Chipkarten Technische Merkmale, Normung, Einsatzgebiete, a. a. O., S. 194 f.

Während herkömmliche Chipkarten aufgrund mangelhafter Sicherungsmöglichkeiten überwiegend mit einer in der Karte hinterlegten PIN online authentifiziert werden müssen, ist durch die Verwendung einer Verschlüsselungssoftware auch eine Offline Nutzung möglich.[36] Denn interne Sicherheitsmechanismen der "Smart Card" gewährleisten nicht nur die sichere Speicherung der Daten, sondern auch die sichere Aufbewahrung möglicher Passwörter und Geheimschlüssel.[37] Zudem können sensible Daten bereits vor der Datenübertragung in der Karte sicher verschlüsselt werden. Dazu werden verschiedene Verschlüsselungsverfahren[38] eingesetzt, um aus den in Klartext vorliegenden digitalen Karteninformationen unverständlichen Geheimtext zu generieren, der erst durch die zugelassene Gegenseite wieder korrekt entschlüsselt werden kann.

Die einzelnen (Software-) Verfahren (3) sind dabei in unmittelbarem Zusammenhang mit dem jeweiligen Anwendungsgebiet (4) zu betrachten. Denn nur eine lückenlose Implementierung, sowohl von Seiten der Karte, als auch von Seiten der Kartenautomaten, ermöglicht optimale Sicherheit, die z. B. für den Bereich des e-Payments von immenser Bedeutung ist.[39] Um sicher zu stellen, dass die Karte vom richtigen Besitzer verwendet wird oder der Kartenterminal nicht manipuliert wurde, wird zum einen eine PIN verwendet oder/und zum anderen eine zweiseitige Authentifizierung durchgeführt. Dabei wird zuerst die Kartennummer angefordert, mit welcher ein individueller Authentifizierungschlüssel angelegt wird. Anschließend erhalten beide Seiten eine Zufallszahl und können so ermitteln, ob beide Seiten den geheimen Schlüssel besitzen. Dieses Verfahren wird auch Challenge-Response-Verfahren genannt. Es handelt sich dabei, um die Verflechtung zweier einseitiger Authentifizierungsverfahren.[40]

---

36 Online im Internet: http://members.tripod.de/atrott/apss.htm, S. 3.

37 Vgl. Lepschies, Gunter: E-Commerce und Hackerschutz - Leitfaden für die Sicherheit elektronischer Zahlungssysteme, 2. Auflage, vieweg Verlag: Wiesbaden 2000, S. 29 f.

38 Es existieren symmetrische (z. B. der Data Encryption Standard, DES) und asymmetrische Verschlüsselungstechniken (z. B: der Rivest, Shamir and Adleman Kryptoalgorithmus, RSA). Vgl. Lepschies, Gunter: E-Commerce und Hackerschutz - Leitfaden für die Sicherheit elektronischer Zahlungssysteme, a. a. O., S. 15 ff.

39 Aufgrund des begrenzten Seitenumfanges wird auf e-Payment nicht näher eingegangen, da bisher kein Standard existiert, der in der Praxis angenommen wird. Die Möglichkeiten, die durch den Einsatz einer Prozessorkarten entstehen, sind in folgenden Vortrag dargestellt. Online im Internet: http://www.ti.fhg.de/smartvortraege/weikmann/sld010.htm, Folie 10.

40 Online im Internet: http://www.informatik.fh-muenchen.de/~chipcard/vortrag1/birgit/chip_sec2.html, S. 11 f.

Trotz des Leistungspotentials eines Prozessors gewährleistet erst eine Kombination verschiedener Komponenten aus den vier Bereichen eine umfassende Sicherheit für die gespeicherten Daten.[41] Parallel zur "Smart Card" wird an der Entwicklung und Integration weiterer Bauteile eines herkömmlichen Computersystems in den Kartenkörper gearbeitet. So werden Anstrengungen unternommen, eine Tastatur und ein Display in die Karte zu integrieren und ein vollständiges "stand alone System"[42] zu erstellen. Diese Karten werden als "Super Smart Card" bezeichnet und sollen u. a. auch biometrische Erkennung[43] ermöglichen, welche die Sicherheit weiter erhöhen würde. Bisher besitzen diese komplexen Hardware Komponenten jedoch keine ISO-konforme Größe.[44]

5 "Smart Card" - Anwendungen

5.1 Vorteile, Einsatzmöglichkeiten und Probleme

Neben den im letzten Kapitel angesprochenen Sicherheitsmaßnahmen ist die einfache Handhabbarkeit ein weiteres Kriterium, warum Chipkarten seit Jahren immer stärker an Bedeutung gewinnen. Kaum ein anderes Medium ermöglicht es, in vergleichbarer Weise sensible Daten sicher zu verwahren, sowie jederzeit und vielerorts multifunktional einsetzen zu können. Abbildung 6 stellt einige Anwendungsmöglichkeiten verschiedener Kartentypen gegenüber. Die Einsatzgebiete sind in der Graphik nach Speicherkapazität und Leistungsfähigkeit angeordnet. In vielen Bereichen wird auf die Verwendung großer Speicher oder hoher Leistungsfähigkeit verzichtet. Dies ist vor allem bei älteren Anwendungen (weiße Kästchen) zu beobachten und überwiegend auf Kostenargumente zurückzuführen. Denn je größer der Speicher und der Leistungsumfang des Chips, desto teurer sind nicht nur die Karten, sondern auch die dafür benötigten Lesegeräte.[45] Andererseits ist der Umstieg oder Einstieg in die "Smart Card" Technologie für viele Unternehmen, insbesondere bei Massenanwendungen, ökonomisch nicht

---

41 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten, Aufbau - Funktionsweise - Einsatz von Smart Cards, a. a. O., S. 450.

42 Jede Art von Computer, die in kein Netzwerk eingebunden ist. Vgl. Linke, Marcus; Winkler, Peter: Das M&T Computer Lexikon, a. a. O., S. 691.

43 Individuelle Merkmale des Menschen, wie z. B. der Fingerabdruck oder die Netzhaut.

44 Online im Internet: http://www.fernuni-hagen.de/NT/kurse/seminar_1998/7wagner.htm.

45 Die notwenigen Hardwarekomponenten kosten zur Zeit zwischen 70 - 100 DM. Vgl. Brehm, Bernd: Geldkarte im Internet, in 11. Rundbrief 2/2000 von Gesellschaft für Informatik e. V., S. 15.

effektiv. In solchen Fällen eröffnen intelligente Speicherkarten eine sinnvolle Alternative im Vergleich zu neueren Prozessorkarten, bei der geringere Sicherheit und eingeschränkte Funktionalität in Kauf genommen werden.

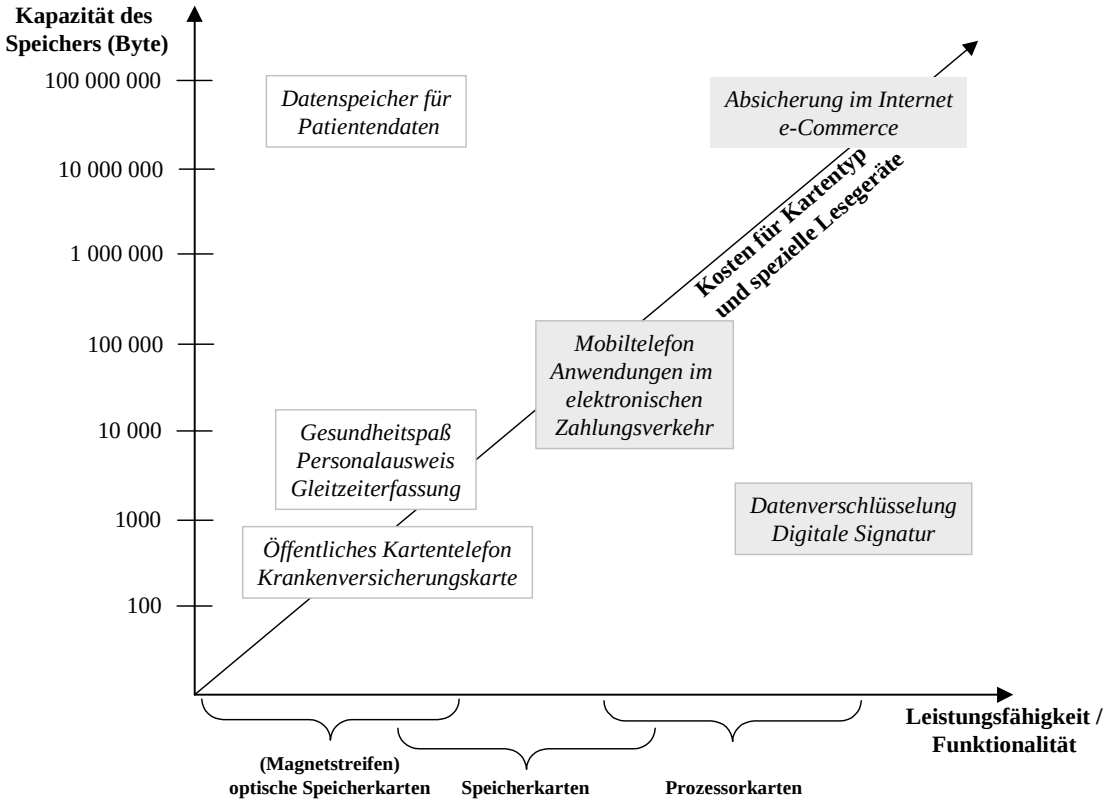

Abb. 6: Verschiedene Anwendungsbereiche von Karten[46]

"Smart Cards" werden bisher fast ausschließlich für unterschiedliche Tests, die von Zugangskontrollen über sichere Bezahlverfahren bis hin zu multifunktionalen Einsätzen reichen, eingesetzt. Standardisierter Anwendungen sind in der Praxis hingegen selten. Daher beschränkt sich dieses Kapitel auf die Beschreibung eines einzigen Beispiels, welches jedoch die Leistungsfähigkeit und das Potential einer "Smart Card" aufzeigt.

5.2 Beipsiel: SIM-Karte für Handys

Vorreiter und inzwischen das weltweit führende Einsatzgebiet für Prozessorkarten stellt das digitale Mobiltelefonsystem GSM dar.[47] Das GSM Netz besteht grob aus einem

---

46 In Anlehnung an: Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten, Aufbau - Funktionsweise - Einsatz von Smart Cards, a. a. O., S. 36.

47 GSM = Global System for Mobile Communications. Anfang 2000 benutzeten ca. xxx Teilnehmer in über 120 Ländern die GSM Norm.

Hintergrundsystem und den einzelnen Mobiltelefonen.[48] Ein Mobiltelefon besteht wiederum aus zwei Komponenten, dem Radio- und Verschlüsselungsteil und dem SIM-Modul. Das Modul ist eine GSM spezifische Chipkarte entweder im ID-1 oder im ID-000 Format, die über eine asynchrone Schnittstelle mit dem Radio- und Verschlüsselungsteil kommuniziert. Das SIM hat zum einen die Aufgaben, personenbezogene Daten wie z. B. eine eindeutige Kartennummer, die Rufnummer, den geheimen Teilnehmerschlüssel, etc. zu speichern und zu schützen. Zum anderen generiert die Prozessorkarte einen temporären Schlüssel, den der Verschlüsselungsteil als Grundlage für die Authentifizierung und die Datenverschlüsselung verwendet. So kann jedes Mobiltelefon durch den Netzbetreiber über eine Luftschnittstelle mittels einseitiger Authentifizierung eindeutig identifizieren werden und anschließend mittels eines kartenindividuellen Schlüssels in Echtzeit Sprachdaten ver- und entschlüsseln. Die für die Übertragung durchzuführende vollständige Verschlüsselung der Daten wird nicht mehr von der Prozessorkarte, sondern durch einen leistungsfähigeren Verschlüsselungsteil durchgeführt. Während die (GSM-) Karte ursprünglich nur zur Identifizierung und zur Speicherung von Abrechnungsdaten dienen sollte, sollten im Laufe der Zeit weitere Funktionen nachgerüstet werden. Dazu wurde die GSM, um die Spezifikation 11.14 (SIM Application Toolkit), erweitert. Dieser Application Toolkit ermöglicht es, beliebige Anwendungen sogar über eine Luftschnittstelle auf die Karte nach zu laden.

Die Spezifikation 11.14 stellt in vielerlei Hinsicht die Basis für zukünftige multifunktionale Anwendungen dar. Vorreiter wird aber auch in dieser Beziehung vorerst das Mobiltelefon bleiben. Denn das Handy, welches Hardware- (z. B. die Tastatur) und Softwarekomponenten in sich vereint, stellt inzwischen ein vertrauenswürdiges, von aussen schwer zu manipulierendes Gerät dar. Ein weiterer Vorteil stellt die weltweite Verbreitung und der international anerkannte GSM-Standard dar. Zukünftige Anwendungen wie z. B. e-Payment oder die digitale Unterschrift[49] sind hier unter bedeutend geringeren Kosten zu implementieren und einzuführen.[50]

---

48 Auf technische Aspekte oder eine detaillierte Ausarbeitung muss aus Platzgründen verzichtet werden. Im Folgenden werden die Eigenschaften der im Mobiltelefon verwendeten Prozessorkarte skizziert.

49 Bisher kein einheitlicher Standard oder praxistaugliche Anwendung vorhanden. Die Anfänge können nachgelesen werden in: Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten, Aufbau - Funktionsweise - Einsatz von Smart Cards, a. a. O., S. 692 ff.

50 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten, Aufbau - Funktionsweise - Einsatz von Smart Cards, a. a. O., S. 683-688.

6 Quo vadis Smart Cards?

Die Miniaturisierung ermöglichte es im Laufe der Jahre, Plastikkarten, um Speicherbausteine und Mikroprozessoren zu erweitern. Die Verbreitung dieses jüngsten leistungsstarken Kartentyps befindet sich noch in der Anfangsphase. Hindernis für den Durchbruch dieser Technologie sind zum einen die Kosten und zum anderen der Umstand, dass viele Bereiche ein so umfassendes Leistungsspektrum nicht benötigen. Interessant erscheint die Zusammenlegung vieler kleinen Anwendungen zu einer multifunktionalen Karte, hier fehlen aber noch internationale Standards. Dennoch ist die steigende Bedeutung der "Smart Card" für die Wirtschaft schon heute nicht zu übersehen. Wie die letzten Kapiteln verdeutlichen, weist die Prozessorkarte aufgrund der leichten Handhabbarkeit und der hochwertigen Sicherheitsmöglichkeiten Eigenschaften auf, welche vor allem neuen Anwendungsbereichen wie z. B. der digitalen Signatur zu Gute kommen. Es ist nur eine Frage der Zeit bis die Prozessorkarte das *"Endstück einer informationstechnischen Kette"*[51] darstellt. Denn die "Smart Card", die im Endeffekt nichts anderes als einen transportablen (Mini-) Computer ist, kann theoretisch mit allen bestehenden Computersystemen der Welt integriert und vernetzt werden. Notwendige Voraussetzung bleibt die Schaffung einheitlicher Standards insbesondere für den multifunktionalen Einsatz.

Unabhängig davon stellt sich die Frage, ob die Karte als solche erhalten bleibt. Denn der Kartenkörper aus Plastik, ist inzwischen nicht mehr als ein einfaches Trägermedium, für ein "intelligentes Innere". Und ob diese zukunftsweisende Technologie nun in der Kleidung, in der Brille oder sogar in der menschlichen Haut untergebracht wird, ist letztendlich für die meisten Anwendungsbereiche irrelevant. Zum jetzigen Zeitpunkt stellt jedoch die "Smart Card" noch die cleverste Alternative dar.

---

[51] Sietmann, Richard: Das Kreuz mit den Karten, http://www.heise.de/ct/01/03/036/ in: c't 3/2001, S. 36.

Literaturverzeichnis

1. **Lepschies, Gunter:** E-Commerce und Kackerschutz - Leitfaden für die Sicherheit elektronischer Zahlungssysteme, 2. Auflage, Wiesbaden: vieweg Verlag 2000.

2. **Linke, Marcus; Winkler, Peter:** Das M&T-Computer-Lexikon, München: Heyne Verlag 1999.

3. **Rankl, Wolfgang / Effing, Wolfgang:** Handbuch der Chipkarten, Aufbau - Funktionsweise - Einsatz von Smart Cards, 3.Auflage, München: Carl Hanser Verlag 1999.

4. **Schütt, Stefan / Kohlgraf, Bert:** Chipkarten Technische Merkmale, Normung, Einsatzgebiete, München: Oldenbourg Verlag 1996.

5. **Brehm, Bernd:** Geldkarte im Internet, in 11.Rundbrief 2/2000 von Gesellschaft für Informatik e. V.

6. **Nieman, Frank:** Anbieter von Web-Bezahlsystemen entdecken den Konsumenten, in; Computerwoche, Ausgabe Nr. 2, 2001.

7. **Sietmann, Richard:** Das Kreuz mit den Karten, URL; **http://www.heise.de/ct/01/03/036/** in: c't 3/2001.

8. **Damm:** Seminar Electronic Money Thema: Smart-Cards, URL; **http://www.informatik.uni-trier.de/~damm/Lehre/E-Money/Augustin/semina~1.htm**.

9. O. A.: URL; **http://www.informatik.fh-muenchen.de/~chipcard/vortrag1/seite1.html**.

10. O. A.: URL; **http://www.ti.fhg.de/smartvortraege/weikmann/sld010.htm.**

11. **http://members.tripod.de/atrtt/faq/faq.htm**.

12. **http://members.tripod.de/atrott/apss.htm**.

13. **http://www.stefan-lenz.ch/glossar/smartcrad.htm.**

14. **http://www.smartcardbasic.com.**

15. **http://www.fernuni-hagen.de/NT//kurse/seminar_1998/7wagner.htm.**

16. **http://www.ti.fhg.de/smartvortraege/weikmann/sld010.htm.**