Fakultät für Elektro- und Informationstechnik
Lehrstuhl für Kommunikationssicherheit
Prof. Dr. Christof Paar
SS 2002

Die Geldkarte

Eine „sichere“ elektronische Geldbörse?!

Marcel Selhorst

Sicherheit in der Informationstechnik
Matrikel-Nummer: 108 099 210 313
Fachsemester: 6

Huestr. 8
44787 Bochum
0234 / 640 82 62

marcel.selhorst@ruhr-uni-bochum.de

Inhaltsverzeichnis:

I. Einleitung

Im März 1996 startete der erste Feldversuch zur Einführung einer elektronischen Börse in der Region Ravensburg. Erstmals wurden an Kunden von Sparkassen „ec-Karten mit Chip“ ausgeliefert, mit der Absicht, kleinere Geldbeträge einfach und unkompliziert auf elektronischem Wege bezahlen zu können, und zwar kostengünstig ohne Online-Verifikation und ohne die Eingabe einer Personal Identification Number (PIN). Um dieses neue System zu realisieren, führte die deutsche Kreditwirtschaft das Zahlungssystem „Geldkarte“ ein, und die Banken und Sparkassen begannen damit, die von ihnen ausgelieferten Kunden-, Giro- und ec-Karten mit einem Mikrochip auszustatten. Entgegen dem allgemeinen Sprachgebrauch ist die Geldkarte kein eigenes Chipkarten-System, sondern eine Applikation, die auf dem Betriebssystem des Mikrocontrollers ausgeführt wird.

Die Geldkarte entstand unter Leitung des „Zentralen Kreditausschusses“ (ZKA), dem die Spitzenverbände des deutschen Kreditgewerbes angehören, also die Dachverbände der deutschen Bankindustrie. Nach der erfolgreichen Erprobungsphase in Ravensburg wurde nach Beseitigung letzter Fehler damit begonnen, die bisher einfachen Magnetstreifenkarten der Banken standardmäßig um den Mikrochip mit integrierter Geldkartenapplikation zu erweitern. Somit entstanden die Hybrid-Karten als neue Generation von ec-Karten.

Das System „Geldkarte“ wurde noch vor der deutschlandweiten Einführung 1997 im Rahmen der weltgrößten Fachkonferenz für Chipkarten und Sicherheitsanwendungen CardTech / SecurTech in Las Vegas im Juni 1997 von der amerikanischen Smart Card Industry Association mit dem „Outstanding Smart Card Application Award“, einem internationalen Innovationspreis, ausgezeichnet. Die Geldkarte wurde hierbei als weltweit herausragende Chipkartenanwendung gewürdigt. Sie diente in den Folgejahren als Vorbild für ähnliche elektronischen Geldbörsen in Luxemburg (MiniCash, Dez. 1998) und Frankreich (Moneo, Okt. 1999).

II. Das System „Geldkarte“

II.1. Funktionsweise und Einsatzgebiete der Geldkarte

Grundsätzlich existieren im Geldkartensystem zwei verschiedene Kartentypen:

1. Die unter dem Namen „Geldkarte“ laufende Karte für Kunden. Mit dieser Karte kann ein Kunde in Geschäften mit entsprechenden Geldkarten-Terminals Bezahlvorgänge verrichten.
2. Für Händler, die in ihrem Geschäft ein Geldkarten-Terminal aufstellen, existiert eine sog. Händlerkarte, über die sich der Händler gegenüber dem Kunden ausweist und der Kundenkarte als Kommunikationspartner dient. Die Händlerkarte ist entweder im Geldkarten-Terminal integriert oder in Form von Software auf einem entsprechenden Computer installiert.

Die Geldkarten von Kunden werden nochmals in zwei Bereiche unterteilt:

1. die kontogebundene Geldkarte
2. die kontoungebundene Geldkarte, die auch als „White Card“ bzw. „Weiße Karte“ bezeichnet wird.

Bei der kontogebundenen Geldkarte wird der Mikrochip auf eine Kunden- bzw. ec-Karte einer Bank oder Sparkasse eingebettet. Der Chip enthält Informationen über die ausstellende Bank, den Kontoinhaber, das dazugehörige Konto und eine Log-Datei mit den zuletzt durchgeführten Transaktionen und Ladevorgängen. Möchte man die Funktionen der Geldkarte nutzen, muss die Chipkarte erst einmal aufgeladen werden. Hierzu wird auf den im Mikrochip integrierten Speicher einer Variable das aktuelle Guthaben zugeordnet und der reelle Gegenwert vom zugehörigen Konto abgebucht. Dies erfolgt in extra dafür vorgesehenen Ladeterminals, die über eine Online-Verbindung mit dem Autorisierungssystem der Kundenbank verbunden sind. Die Terminals lesen die notwendigen Informationen über den Inhaber und das zu belastende Konto aus der Karte aus und fordern vom Besitzer der Karte die Autorisierung mittels PIN-Eingabe. Nach erfolgreicher Autorisierung prüft das Terminal die Gültigkeit der Karte und zeigt im Display den maximal verfügbaren Ladebetrag an, worauf der Kunde den gewünschten Ladebetrag eingeben kann. Dieser wird dann mitsamt den dazugehörigen Daten an die Ladezentrale übermittelt, welche sie an die Kundenbank und die Kartenevidenzzentrale (siehe II.2.) weiterleitet. Nachdem die Kundenbank die

Abbuchung autorisiert hat, wird der Chip mit dem gewünschten Betrag aufgeladen und im Gegenzug das dazugehörige Konto belastet.

Neuerdings besteht auch die Möglichkeit, seine kontogebundene Geldkarte vom heimischen PC aus über das Internet zu laden, bzw. Beträge über das Internet mit der Geldkarte zu bezahlen. Hierzu benötigt man einen Klasse-3-Chipkartenleser (mit integriertem Display und Zifferntastatur zur sicheren Eingabe der PIN am Gerät), der über die serielle bzw. die USB-Schnittstelle mit dem Computer verbunden wird, sowie ein Online-Banking-Konto, welches nach Aufladen der Geldkarte belastet wird. Der PC übernimmt beim Aufladen der Karte lediglich die Rolle der Verbindungsstelle zur Bankzentrale. Sämtliche sicherheitsrelevanten Vorgänge wie die Eingabe einer PIN bzw. das Auslesen der Karteninformationen finden in dem Chipkartenterminal statt und werden verschlüsselt zum PC übertragen, der diese dann weiterleitet. Somit ist ein Ausspionieren der Daten durch Dritte ausgeschlossen.

Bei der kontoungebundenen Variante handelt es sich ebenfalls um eine Smartcard mit integriertem Mikrocontroller und identischem Betriebssystem wie bei der kontogebundenen Karte. Auch hier läuft eine Geldkarten-Applikation, die allerdings so modifiziert wurde, dass sich die Karte nicht in Ladeterminals aufladen lässt, da kein Bezug zu einem Girokonto hergestellt werden kann. Die Aufladung erfolgt daher gegen Bargeld in einer Bank an sogenannten Banken-Sonderfunktions-Terminals (BSFT). Hierbei ist die Eingabe einer PIN nicht erforderlich.

Möchte man nun einen Kauf mit der Geldkarte tätigen, so führt man die Geldkarte in ein entsprechendes Terminal ein, bestätigt den zu zahlenden Betrag, und das Guthaben wird von der Geldkarte abgebucht und der Geldkarte des Händlers gutgeschrieben. Da keine weitere Autorisierung durchgeführt wird (wie z.B. die Eingabe einer PIN), ist im eventuellen Verlust der Karte das noch gespeicherte Guthaben verloren, da jeder mit der Geldkarte bezahlen kann. Wird die Geldkarte verloren, das Guthaben aber nicht aufgebraucht, so besteht nach Ablauf der Gültigkeit der Geldkarte durch Nachprüfung der Schattensalden die Möglichkeit, das Restguthaben zurückzubekommen. Um den Schaden bei Verlust zu minimieren, ist der Verfügungsrahmen der Geldkarte auf maximal 200,- € limitiert. Dieser Ladebetrag kann auf Wunsch gesenkt, allerdings nicht erhöht werden. In Abbildung 1 werden die Lade- und Bezahlvorgänge mit der Geldkarte schematisch dargestellt.

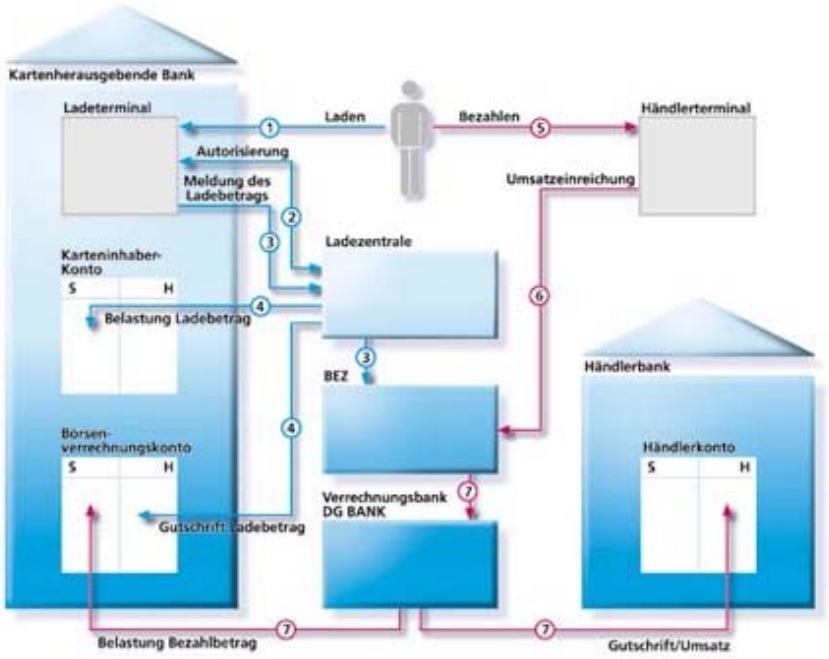

Abbildung 1: Lade- und Bezahlvorgang mit der Geldkarte

Die Haupteinsatzgebiete der Geldkarte liegen im gewerblichen Einzelhandel. In einigen Städten bestehen bereits Kooperationen mit dem öffentlichen Nahverkehr, Taxizentralen und Parkhäusern, so dass die dort anfallenden Beträge ebenfalls mit der Geldkarte bezahlt werden können. Weitere Akzeptanten der Geldkarte sind Gastronomien, Kino-Zentren, Theater, Tankstellen und Automaten jeglicher Art.

Als besonders praktisch erweist sich die Geldkarte aufgrund ihrer unkomplizierten Bedienung und Anwenderfreundlichkeit. Durch den geringen Maximalbetrag ist die Karte vorwiegend für Zahlungen zwischen einigen Cent und wenigen Euro ausgelegt, da kein Kleingeld mehr benötigt wird. Dies spart sowohl den Kunden als auch den Händlern Zeit und erleichtert die Gewöhnung an elektronische Zahlungsmethoden. Für Händler ergibt sich weiterhin der Vorteil, dass Kunden „liquider“ sind und eher zu Spontankäufen angeregt werden als bei normalem Bargeld, da man beim Einsatz der Geldkarte das Geld nicht direkt aus der Hand gibt (psychologischer Ansatz der Geldkartenpolitik).

Durch das spezielle Sicherheitskonzept der Geldkarte ist bei einem Zahlungswunsch keine Online-Autorisierung nötig, was dem Händler Kosten von bis zu 80% spart. Allerdings bringt der Einsatz der Geldkarte für den Händler auch Nachteile. Er muss erst eine Abrechnung mit der Evidenzzentrale machen, um über das erhaltene elektronische Geld verfügen zu können. Weiterhin liegen die anfallenden Gebühren der

Banken für jeden getätigten Geldkartenkauf beim Händler und werden direkt bei der Abrechnung einbehalten. Diese belaufen sich auf 0,3 % des getätigten Umsatzes, mindestens aber 0,01 €.

II.2. Evidenzzentralen im Zahlungssystem

Wird eine Geldkarte mit einem Guthaben geladen, so wird das entsprechende Girokonto mit dem gebuchten Betrag belastet. Dabei stellt sich die Frage, was mit dem Geld passiert, das auf die Karte geladen wird. In diesem Zuge kommen Evidenzzentralen ins Spiel. Evidenzzentralen spielen eine wichtige Rolle im Zahlungssystem der Geldkarte, denn sie gewährleisten die Systemsicherheit und sorgen für eine reibungslose Abwicklung der getätigten Transaktionen.

Es gibt zwei unterschiedliche Evidenzzentralen (EZ):

1. Händler-Evidenzzentralen (HEZ)
2. Karten-Evidenzzentralen (KEZ)

Evidenzzentralen können sowohl HEZ als auch KEZ sein. Dies hängt davon ab, für welchen Kartentyp die beauftragende Bank der EZ die Verwaltung überträgt.
Händler-Evidenzzentralen sind EZs, die von der Bank des Händlers beauftragt wurden, die Umsätze der Händlerkarte zu betreuen und die Prüfung der Daten zu übernehmen. Jede Händlerkarte muss genau einer HEZ zugeordnet sein. Nur diese HEZ kann die Umsätze der Händlerkarte prüfen und darf die Gutschriften auf das entsprechende Händlerkonto veranlassen. Karten-Evidenzzentralen sind für die Betreuung der Geldkarten von Kunden zuständig. Jede Geldkarte ist genau einer KEZ zugeordnet und nur diese KEZ darf über die Karte ein sogenanntes Schattenkonto führen und nur diese KEZ darf Geld von dem zugehörigen Verrechnungskonto abbuchen. Bei erfolgreicher Aufladung einer Geldkarte wird das Geld von dem zu belastenden Konto durch die Kartenevidenzzentrale abgebucht und auf ein Schattenkonto der Evidenzzentrale überwiesen. Lässt man seine Geldkarte gegen Bargeld aufladen, z.B. weil es sich um eine „White Card“ handelt, so wird das Geld ebenfalls auf das Schattenkonto bei der KEZ eingezahlt. Diese führt darüber Buch, wann welche Karte mit wie viel Geld geladen bzw. entladen wurde, und welche Umsätze damit wo und mit welcher

Händlerkarte getätigt wurden. Das geladene Geld wird auf der Geldkarte als ein in einer Variablen gespeicherter numerischer Wert repräsentiert.
Im Zahlungssystem Geldkarte werden die in allen technischen Systemen immensen Sicherheitsrisiken durch spezielle Sicherungsverfahren minimiert. Hierzu werden die Einzelumsätze beim Händler erfasst und individuell gesichert. Die Prüfung und Verarbeitung der Einzelumsätze nimmt die Evidenzzentrale vor.
Hauptvorteil und Hauptanreiz für Banken, die Rolle einer Evidenzzentrale zu übernehmen, liegt an dem finanziellen Gewinn. Der Kunde, der seine Geldkarte auflädt, gewährt der Bank ein „zinsfreies Darlehen“, da das Geld auf einem Schattenkonto lagert und die Bank somit darüber verfügen kann.

II.3. Anonymität

Die Evidenzzentralen speichern Informationen über sämtliche Lade-, Entlade- und Bezahlvorgänge. Daher kann man an Hand der Geldkartendaten alle getätigten Einkäufe zurückverfolgen. Da bei jedem Kauf die Nummer der Händlerkarte, mit der der Kauf getätigt wurde, mitprotokolliert wird, kann man sogar exakt den Zeitpunkt und den Ort bzw. die Art des Kaufes bestimmen. Die Speicherung solcher Informationen ermöglicht den Evidenzzentralen, Missbrauch schnell zu erkennen und durch sequentielles Abspeichern der eingereichten Daten eine Doppelauszahlung an Händler zu verhindern. Weiterhin werden die letzten 15 getätigten Einkäufe in einer bestimmten Log-Datei auf der Geldkarte gespeichert, ebenso wie die letzten drei Aufladevorgänge. In beiden Fällen werden die Händlerkartennummer bzw. die Ladeterminal-ID zzgl. Uhrzeit, Datum und Betrag protokolliert. Diese Informationen können mittels einfacher Taschenkartenlesegeräte ausgelesen werden, um dem Benutzer die Möglichkeit zu bieten, seine Ausgaben zu beobachten (und natürlich jedem anderen, der eine Geldkarte in die Hand bekommt).
Trotz Beteuerung des Zentralen Kreditausschusses (ZKA) kann ein Kauf mit der Geldkarte im Vergleich zum Bargeld nicht anonym sein. Vor allem bei den kontogebundenen Geldkarten lässt sich aufgrund der gespeicherten Kontoinformationen sogar ein Rückschluss auf die wirkliche Identität durchführen. Beim Nutzen einer „White Card“ lässt sich zwar die Identität des Karteninhabers nicht feststellen, da der Bezug zu einem Konto nicht hergestellt werden kann. Es lässt jedoch die Erstellung

eines Kauf-Profils zu, da sich das Kaufverhalten aufgrund der Pseudonymität der Geldkarte nachvollziehen lässt. Jede Geldkarten-ID ist eindeutig. Um dieses Problem zu relativieren, werden die Informationen an unterschiedlichen Stellen unabhängig voneinander abgespeichert. Eine Auswertung ist nur mit gerichtlicher Anordnung bzw. bei einem Rückerstattungswunsch möglich. Obwohl die Evidenzzentralen und die Händler, die das Geldkartensystem nutzen, gesetzlich dazu verpflichtet sind, nach Abschluss der Verrechnung sämtliche gespeicherte Umsatzdaten zu löschen bzw. zu anonymisieren (Clearing), lässt sich eine vollständige Anonymisierung nicht realisieren. Problematisch beim Geldkartensystem ist, dass den Kunden fälschlicherweise eine Anonymität suggeriert wird, die nicht existiert, und nur wenige Banken ihre Kunden überhaupt über die Existenz eines Schattenkontos bei den Evidenzzentralen aufklären. In den USA existiert ebenfalls ein ähnliches Geldkartensystem, welches auch Schattenkonten zu den einzelnen Geldkarten führt. Einem Nutzer dieses Systems wurde ein Kredit verweigert, weil er als nicht kreditwürdig eingestuft wurde. Die Bank hat seine Daten überprüfen lassen und festgestellt, dass mit seiner Geldkarte des öfteren Alkoholika und Spirituosen bezahlt worden sind. Um so einen Missbrauch von Kundendaten zu verhindern, wurde auf der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder ein Entschluss gefasst, der die Kartenherausgeber und die Kreditwirtschaft erneut dazu auffordert, das System so zu erweitern, dass die Privatsphäre gewährleistet wird. Weiterhin werden sie aufgefordert, sicherzustellen, dass die Möglichkeit der Anonymität im wirtschaftlichen Leben im gleichen Umfang gewährleistet ist, wie dies momentan beim Bargeld der Fall ist. Allerdings bringt die Führung von sog. Schattensalden den Vorteil, dass bei verloren gegangenen Geldkarten nach Ablauf der Gültigkeit die Möglichkeit auf eine Geldrückerstattung besteht.

III. Der Aufbau der Geldkarte

Die Geldkarte besteht aus einem Kartenkörper mit der Dicke von 0,76mm und der Kartengröße von 85mm x 54mm gemäß ISO-Norm 7816. Auf diesem Kartenkörper ist bei kontogebundenen Geldkarten auf der einen Seite ein Mikrochip implementiert und auf der anderen Seite ein Magnetstreifen aufgebracht. Diese Doppelfunktionalität aus ec- bzw. Kundenkarte und Mikrochip gibt der Geldkarte den Namen „Hybridkarte“. Bei kontoungebundenen Geldkarten entfällt die Aufprägung eines Magnetstreifens. Bei 87,5% der weltweit hergestellten Karten wird PVC für die Produktion von Chipkartenkörpern benutzt. Für die Herstellung der Kartenkörper werden zwei unterschiedliche Verfahren angewandt: Entweder entsteht dieser durch Heißverklebung mehrerer Folien unter hohem Druck (Laminierung), oder er wird im Spritzgussverfahren hergestellt. Bei kontogebundenen Geldkarten nutzt man fast ausschließlich das Laminierungsverfahren, da somit Layout und persönliche Informationen unter einer transparenten Folie direkt mit eingeschweißt werden können und länger halten. Bei zeitlich begrenzten „White Cards“, beispielsweise für Touristen nutzt man die günstigere Variante des Spritzgussverfahrens. Für die Aufnahme des Chipmoduls muss eine Aussparung ausgefräst werden, in welche das Chipmodul eingebettet und mittels Kleber befestigt wird.

III.1. Hardware

Die in Geldkarten eingebetteten Mikrochips sind speziell im Auftrag des Zentralen Kreditausschusses (ZKA) gefertigt worden. Die am häufigsten verwendeten Mikrochips werden von der Firma Siemens hergestellt (bzw. der Firma Infineon, die die Chipproduktion von Siemens durch Zusammenschluss übernommen hat). Dabei handelt es sich vorwiegend um den Cryptocontroller SLECX160S mit 32 kB ROM, 8 bzw. 16 kB EEPROM und 512 Byte RAM. Die Chips mit 8kB EEPROM werden bei Geldkarten für Kunden eingesetzt, während die mit 16 kB EEPROM ausschließlich für Händlerkarten genutzt werden. Bei einigen „White Cards“ der CashGroup (eine Vereinigung privater Banken) findet der Cryptocontroller Siemens SLE 66C80S Verwendung. Detailliertere Informationen über den eigentlichen Mikrochip-Aufbau bzw. Schaltpläne sind aus Sicherheitsgründen nicht öffentlich zugänglich. Lediglich Chiphersteller und Grossbanken dürfen Einsicht in die konkreten Chip-Spezifikationen

nehmen. Man weiß aber, dass die Architektur des Controllers der der 8051-Controller-Familie ähnelt und der Controller mit 8-Bit-Befehlen und einem 16-Bit breiten Datenbus arbeitet, mit dem 2^{16} = 65536 Bytes adressiert werden können. Gerüchten zufolge sollen durch Hacker Details der Chiphardware aufgedeckt und detaillierte Informationen über das eingebaute BIOS veröffentlicht worden sein. Allerdings stellte sich bereits am Tag nach der Veröffentlichung heraus, dass es sich bei den Informationen um selbstprogrammierbare Controller der Firma Siemens vom Typ SLC 44/66 handelte und diese Informationen frei zugänglich waren, da nie einer dieser Chips auf Geldkarten implementiert worden ist. Die Ansteuerung des Mikrochips erfolgt bei allen Kartenvarianten über 8 Kontakte auf der Geldkartenoberfläche. Abbildung 2 beschreibt die Belegung dieser Kontakte.

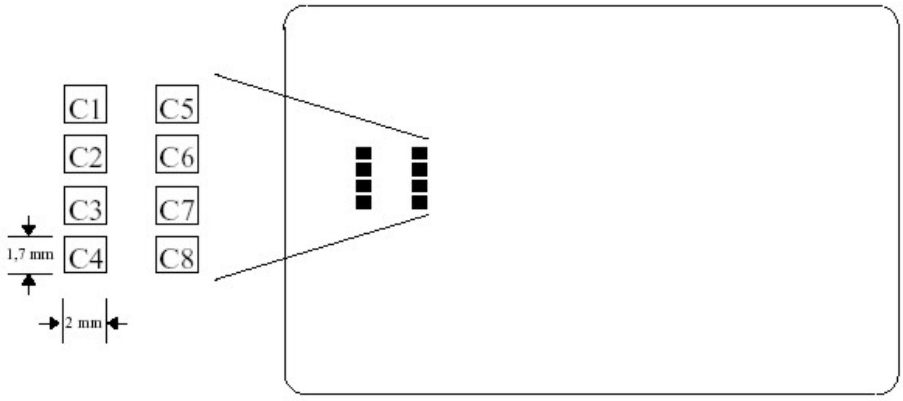

Abbildung 2: Kontakte bei Chipkarten

Kontakt	Signal	Anmerkung
C1	V_{CC}	Versorgungsspannung
C2	RST	Reset-Signal
C3	CLK	Taktsignal
C4	RFU	Reserviert für zukünftige Anwendungen
C5	GND	Masse
C6	V_{PP}	Programmierspannung
C7	I/O	Dateneingang / -ausgang
C8	RFU	Reserviert für zukünftige Anwendungen

Nachfolgend werden die einzelnen Kontakte beschrieben.

C1 – Versorgungsspannung

Die Versorgungsspannung der Geldkarte liegt bei 5 Volt. Standardmäßig ist aber eine Toleranz von 10 % möglich, so dass die Ansteuerung des Chips zwischen 4,5 und 5,5 Volt liegt. Neuere Chipkarten kommen aber auch mit weitaus weniger Versorgungsspannung aus (bis 1,8 Volt).

C2 – Reset-Signal

Über die Reset-Leitung wird der Mikrocontroller zurückgesetzt. Das RST-Signal kann während des Betriebes (Warmstart) oder beim Initialisieren gesetzt werden. Dabei wird der Adresszähler zurückgesetzt und der Speicher gelöscht.

C3 – Taktversorgung

Da Chipkartenprozessoren selbst keinen Takt erzeugen, muss dieser von außen angelegt werden. Normalerweise werden Chipkarten mit 3,5712 MHz bzw. 4,9152 MHz betrieben.

C4 / C8 – RFU

RFU steht für „reserved for future use“ - diese beiden Kontakte werden daher momentan noch nicht verwendet. Um Produktionskosten zu sparen werden deshalb einige Chips mit nur 6 Goldkontakten ausgeliefert.

C5 – Masse

Die Masseverbindung muss nach ISO 7816-3 vor der Versorgungsspannung an die Chipkarte angelegt werden.

C6 – Programmierspannung

Bei älteren Chipkartenmodellen wurde dieser Kontakt zur Versorgung des EEPROMs mit Spannung genutzt, um es zu programmieren oder zu löschen. Mittlerweile hat dieser Kontakt aus Sicherheitsgründen keine Funktion mehr. Um das EEPROM zu programmieren, erzeugt der Chip selber die Spannung durch sogenannte Ladungspumpen aus der Versorgungsspannung.

C7 – Dateneingang / -ausgang

Dieser Kontakt ist allein für die Datenübertragung zuständig. Daher findet die Übertragung halbduplex statt, d.h. es kann immer nur eine Seite senden. In zukünftigen Chipkarten ist eine Vollduplex-Übertragung geplant. Hierfür soll einer der nicht genutzten Kontakte C4 / C8 genutzt werden.

Die Lebensdauer des Chips wird insbesondere durch das EEPROM beeinflusst. Im EEPROM werden die Daten gespeichert, die veränderbar sein sollen. Die Lebensdauer wird durch Schreibzyklen verkürzt, die Hersteller garantieren aber für 1.000.000 Schreib- bzw. Löschzyklen, so dass der Datenerhalt für mindestens 10 Jahre garantiert wird. Allerdings kann die Funktionsfähigkeit der vergoldeten Kontakte nach ca. 10.000 Steckvorgängen eingeschränkt sein, da durch Verkratzen der Kontakte Schmutz und Fett haften bleiben, oder durch die fehlende Goldschicht eine Oxidation eintritt. Bei der Produktion wird jede Karte speziellen Tests unterzogen, um mögliche Produktionsfehler ausschließen zu können. Dazu zählen unter anderem Speichertests, Funktionskontrollen der Software, Biegetests usw.

Die momentane Generation von Geldkarten besteht aus einem eingebauten Mikrocontroller. Dieser wiederum besteht aus einem Mikroprozessor (CPU), ein ROM (Read Only Memory) in dem das Betriebssystem installiert ist, RAM (Random Access Memory) als Arbeitsspeicher und einem EEPROM (Electrical Erasable and Programmable Read Only Memory) als Datenspeicher. Abbildung 3 veranschaulicht den Aufbau eines Microcontrollers.

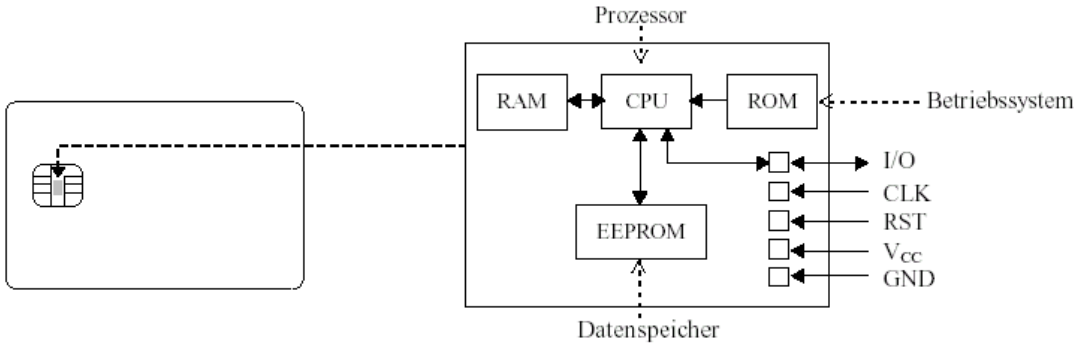

Abbildung 3: Aufbau des Mikrocontrollers

Geldkarten werden auch als asynchrone Karten bezeichnet, da der integrierte Mikrocontroller für die Datenübertragung ein asynchrones Übertragungsprotokoll verwendet. Während die kryptographischen Operationen bei der heutigen Smartcard-Generation noch durch das Betriebssystem – also per Softwarelösung – ausgeführt werden, enthalten zukünftige Versionen der Geldkarte spezielle Coprozessoren, die Exponential- und Modulooperationen mit Ganzzahlen hardwaremäßig ausführen.

Dazu zählen unter anderem:

- DES - Beschleuniger für DES und Triple-DES
- EC2 – Beschleuniger für den GF(2^n)
- ACE (Advanced Crypto Engine) mit Unterstützung für RSA bis zu einer Schlüssellänge von 1024 Bit und einer Beschleunigung für den GF(p)
- Hash-Funktion-Beschleuniger für SHA-1 und MD5

III.2. Software

Das im ROM der Geldkarte untergebrachte Betriebssystem war bis Ende 2000 ein Derivat des von IBM in Kooperation mit Siemens Nixdorf und der Telekom entwickelten Smartcard-Betriebssystems MFC („MultiFunctionCard“). Dieses verfügte über 14 Kommandos zur Steuerung der Karte. Seit dem 1. Oktober 2000 wurden allerdings im Zuge der Euro-Umstellung die Geldkarten mit einem neuen Betriebssystem ausgeliefert. Alle bis dahin im Umlauf befindlichen Karten liefen zum 31.12.2000 ab und wurden mit Ablauf des Datums ungültig. Dies hängt damit zusammen, dass ältere Versionen nur mit DM-Beträgen arbeiten konnten und durch die Euro-Umstellung unbrauchbar wurden. Einige Karten sollten nach offiziellen Angaben mit beiden Währungen umgehen können, allerdings stellte sich in der Praxis heraus, dass bei Bezahlvorgängen Rundungsfehler auftraten, die bis zu einigen Pfennigen hoch sein konnten. Die Banken haben dann diese Karten kostenlos durch neue ersetzt. Durch technische Innovationen und den Zusammenschluss mehrerer Staaten für ein gemeinsames, europäisches, elektronisches Geldbörsen-Projekt musste bei der Konzeption der Software komplett von vorne angefangen werden. Aus diesem Grunde zogen sich die einstigen Hersteller des MFC-Betriebssystems aus der Entwicklung zurück und überließen den führenden Chipkartenspezialisten „Gemplus“, „Giesecke & Devrient“ und „Orga Kartensysteme“ die Entwicklung des neuen Betriebssystems. Mit der neuen Version 4.1 wurde die Anzahl der Kommandos, die die Geldkarte steuern, auf 21 erhöht, um die Sicherheit zu verbessern. Die implementierten Kommandos sind aus einzelnen Befehlen eines Befehlssatzes zusammengesetzt. Das Betriebssystem selbst ist in Assembler geschrieben, da höhere Sprachen zu speicherintensiv sind.
Die wichtigsten Aufgaben des Betriebssystems bestehen aus der Ablaufsteuerung, der Datenübertragung, der Dateiverwaltung und der Ausführung von kryptographischen

Algorithmen. An dieser Stelle sei noch einmal erwähnt, dass das Geldkarten-System lediglich ein Programm für das Chipkarten-Betriebssystems ist.

Die durch die I/O-Schnittstelle empfangenen Befehle werden nach folgendem Schema abgearbeitet:

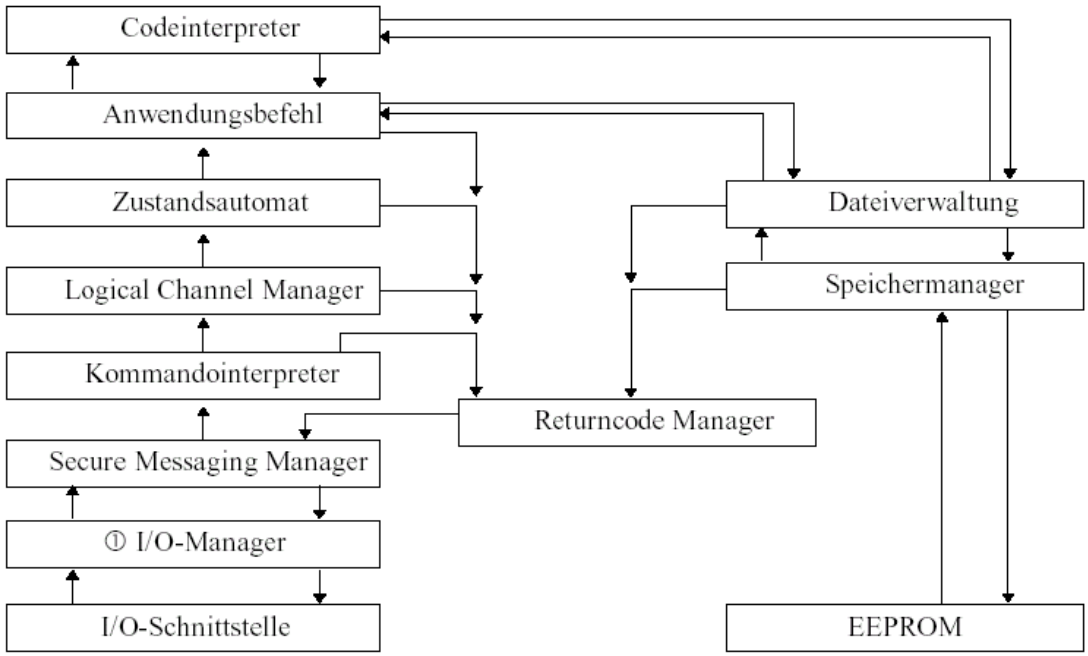

Abbildung 4: Ablauf der Befehlsabarbeitung innerhalb eines Chipkarten-Betriebssystems

Zuerst führt der I/O-Manager bei Bedarf Fehlererkennungs- und Fehlerkorrekturmaßnahmen durch. Wurde der Befehl durch eine gesicherte Datenübertragung verschlüsselt, so wird der Befehl vom Secure Messaging Manager entschlüsselt bzw. auf Integrität geprüft. Dann wird der Befehl vom Kommandointerpreter decodiert, vom Logical Channel Manager der angewählte Kanal ermittelt und der gewählte Kanal vom Zustandsautomaten auf Zulässigkeit überprüft. Erst jetzt wird der zugrunde liegende Programmcode ausgeführt und ggf. vom Codeinterpreter überwacht. Bei Zugriff auf Dateien wandelt die Dateiverwaltung die für die Umsetzung nötigen logischen Adressen in physikalische um. Der Speichermanager verwaltet die physikalischen Adressen des EEPROM. Der Returncode-Manager sorgt für die Erzeugung von Antworten. Dieser kann von allen Schichten im Fehlerfall aufgerufen werden, um den Programmablauf zu unterbrechen und eine Fehlermeldung auszugeben. Das Betriebssystem regelt unter anderem die Kommunikation der Geldkarte mit den Geldkartenterminals. Zwischen den

Terminals und der Smartcard besteht ein Master-Slave-Verhältnis, wobei das Terminal die Master-Rolle übernimmt und die Geldkarte die Slave-Rolle. Hauptaufgabe dieser Rollenvergabe besteht darin, dass die Geldkarte keinerlei Informationen von sich aus über sich preisgibt. Erst wenn der Master mit korrekten Kommandos die Karte dazu auffordert, stellt das Betriebssystem die nötigen Informationen zur Verfügung.
Dies beginnt bereits beim Einführen der Karte in das Terminal. Hierbei setzt das Terminal das RST-Signal, um die Karte zu initialisieren. Diese antwortet dann mit einem ATR (Answer-to-Reset) und übermittelt die notwendigen Kartenparameter. Muss das Terminal aufgrund von Sicherheitsupdates der Geldkartensoftware einige Parameter auf der Karte ändern, so folgt direkt auf das ATR die Anforderung an die Geldkarte, seine Zustimmung hierzu zu geben. Dies erfolgt mittels PTS (Protocol Type Selection).
Ist dies nicht notwendig, kann das Terminal direkt Befehle an die Chipkarte senden, die diese abarbeitet und beantwortet. Der erste Befehl, den das Terminal an die Chipkarte sendet, beinhaltet den Aufruf der Geldkartenapplikation. Nachfolgend ist der Ablauf dieser Kommunikation dargestellt:

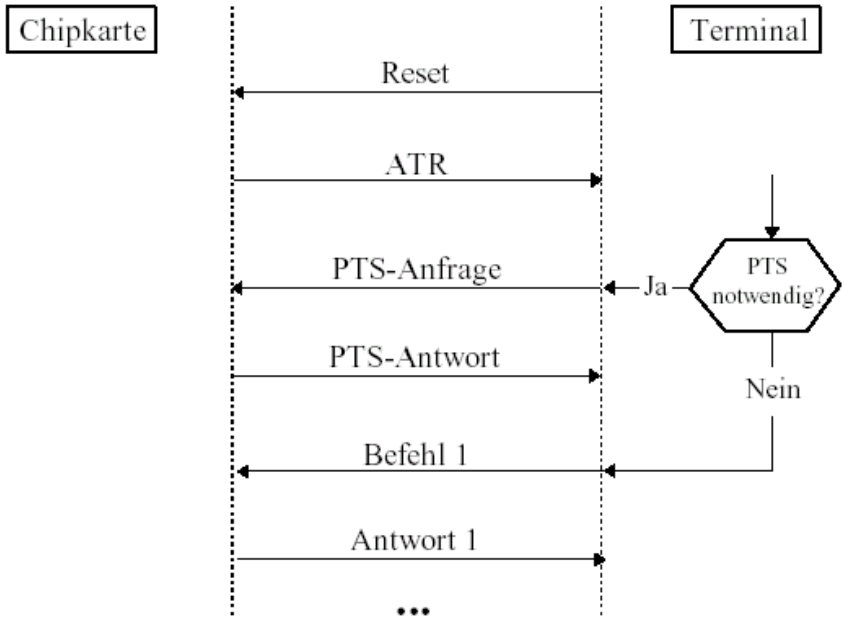

Abbildung 5: Kommunikation zwischen Geldkarte und Terminal

Die Befehle an die Chipkarte werden als Befehls-APDU bezeichnet, die dazugehörigen Antworten als Antwort-APDU (APDU = Application Protocol Data Unit).

Struktur einer Befehls-APDU

Die Struktur einer Befehls-APDU geht aus Abbildung 6 hervor. Im Header einer Befehls-APDU werden die Klasse (CLA), die jeweiligen Einzelbefehle (INS) und zwei Parameter (P1, P2) festgelegt. Im Body ist ein Längenfeld für die nachfolgenden Daten (L_c: length command) und ein Feld für die Länge der erwarteten Antwort (L_e: length expected) vorgesehen.

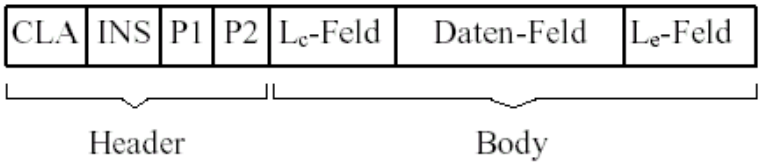

Abbildung 6: Struktur einer Befehls-APDU

Struktur einer Antwort-APDU

Die Antwort-APDU besteht nur aus einem Body und einem Trailer. Der Body enthält die Daten, die angefordert wurden. Der Trailer setzt sich aus zwei Status-Worten (SW1, SW2) zusammen, die den Returncode bzw. die Antwort auf das Kommando enthalten. Die beiden Felder sind in Abbildung 7 dargestellt.

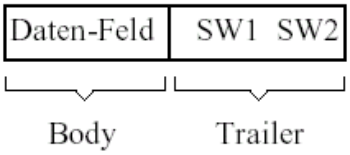

Abbildung 7: Struktur einer Antwort-APDU

Um Daten oder Befehle mit einer Smartcard auszutauschen, bedarf es bestimmter Übertragungsprotokolle, die sich an der Funktion der Smartcard orientieren. Man unterscheidet bei den Übertragungsprotokollen zwischen synchronen und asyonchronen Protokollen. Synchrone Varianten wie „2-wire“, „3-wire“ oder „IIC“ finden bei Smartcards mit Geldkartenapplikation keinerlei Verwendung. Die wichtigsten asynchronen Übertragungsprotokolle sind T=0, T=14 und T=1.

T=0 findet vor allem beim Mobilfunksystem GSM Verwendung, da es schnell und einfach ist und wenig Speicher benötigt. Das Protokoll T=14 ist für nationale Anwendungen reserviert und wurde von der Telekom für das C-Netz und bei Telefonkarten für öffentliche Telefonzellen verwendet. Hierbei handelt es sich um ein blockorientiertes Protokoll, das großen Einfluss auf das später genormte Protokoll T=1 hatte, welches in der Geldkarte Verwendung findet.
Das Übertragungsprotokoll T=1 ist ein asynchrones Halbduplexprotokoll, dass blockorientiert funktioniert. Diese Blöcke werden in drei verschiedene Blockarten unterteilt:

1) Informationsblöcke dienen der Übertragung von Daten der Anwendungsschicht
2) Empfangsbestätigungsblöcke geben eine positive bzw. negative Rückmeldung bzgl. Übertragungsfehlern
3) Systemblöcke beinhalten Steuerinformationen

Jedem dieser Blöcke ist ein Prologfeld vorangestellt, welches Steuerungs- und Anzeigeinformationen des betreffenden Blocks enthält. Weiterhin wird im Prologfeld die Länge des folgenden Informationsfeldes vermerkt, welches wiederum die Befehls- oder Antwort-APDU enthält. Handelt es sich bei dem zu übertragenen Block um einen Systemblock, so enthält das Informationsfeld keine Daten. Bei einem Empfangsbestätigungsblock befinden sich darin die nötigen Informationen für das Protokoll. Jedem Übertragungsblock wird ein Epilogfeld angehängt, welches der Fehlererkennung dient. Hierzu werden Längsprüfungscodes (LRC – Longitudinal Redundancy Check) gebildet. Sowohl die Befehls- als auch die Antwort-APDU werden im Informationsfeld untergebracht.
Tritt bei der Übertragung ein Fehler auf, so fordert der Empfänger durch Senden eines negativen Empfangsbestätigungsblocks zum erneuten Senden des Blocks auf. Enthält der nachfolgende Block nochmals Fehler, so wird die Verbindung zwischen den Kommunikationspartnern getrennt und neu aufgebaut. Ist auch dann keine erfolgreiche Kommunikation möglich, so markiert das Terminal die Chipkarte als defekt und deaktiviert sie. Abbildung 8 beschreibt den Aufbau des Übertragungsprotokolls T=1.

Prologfeld			Informationsfeld	Epilogfeld
Knotenadresse NAD	Protokoll-kontrollbyte PCB	Länge LEN	APDU	EDC
1 Byte	1 Byte	1 Byte	0 ... 254 Byte	1 .. 2 Byte

Abbildung 8: Aufbau eines Übertragungsblocks bei T=1

Das Übertragungsprotokoll T=1 ist das einzige Übertragungsprotokoll, dass für die Geldkarte Verwendung finden kann, da eine strenge Schichtentrennung nach dem OSI-Referenzmodell realisiert wurde. Dies ist für die transparente Übertragung von Anwendungsdaten nötig und die wichtigste Voraussetzung für die Übertragung verschlüsselter Daten.

IV. Die Sicherheit der Geldkarte

Eine Smartcard, auf der eine Geldkartenapplikation laufen soll, muss verschiedene Sicherheitsanforderungen erfüllen.

1) Vertraulichkeit: die Geheimhaltung der gespeicherten Daten
2) Integrität: die gespeicherten Daten dürfen weder absichtlich noch unabsichtlich geändert werden
3) Verfügbarkeit: die auf der Smartcard gespeicherten Informationen dürfen nicht unbeabsichtigt verloren gehen.

Gerade bei dieser Anwendung einer Chipkarte könnte die Verletzung einer der o.g. Sicherheitsanforderungen einen Schaden für eine der beteiligten Parteien des Geldkartensystems bedeuten. Obwohl die Chipkarte nur ein Teil des Geldkartensystems ist und daher nur einen Teil der Gesamtsicherheit ausmacht, müssen die Anforderungen an die Chipkarte besonders hoch sein, da der Kartenherausgeber keinerlei Einfluss auf Manipulationsversuche durch den Karteninhaber hat. Daher ist das Hauptziel des Kartenherausgebers bzw. des Kartenherstellers, den Aufwand für die erfolgreiche Manipulation einer Geldkarte so hoch zu setzen, dass der zu betreibende Aufwand den möglichen Nutzen übersteigt. Um die Sicherheitsanforderungen an die Chipkarte zu realisieren, müssen verschiedene Sicherheitsaspekte gewährleistet sein, die im folgenden beschrieben werden.

IV.1. Physikalische Sicherheit

Die physikalischen Sicherheitsmaßnahmen sollen durch Sensoren die Funktions- und Speicherelemente überwachen und vor Manipulation und Analyse schützen. Um die Analyse des eingebauten Mikrocontrollers zu erschweren, wird der Aufbau des Chips durch eine sehr hohe Transistordichte realisiert, welche den Gewinn von Informationen über die Struktur nahezu unmöglich macht. Die Busse, die zur Verbindung des Prozessors mit den Speichern benötigt werden, dürfen nicht von außen kontaktierbar sein. Die Leistungsaufnahme des Prozessors muss bei allen Befehlen näherungsweise die gleiche Stromaufnahme haben, um das Erkennen von Programmabläufen oder das

Ausspähen von kryptographischen Schlüsseln zu verhindern. Weiterhin werden die Adress- und Datenleitungen ungeordnet und „wild durcheinander“ verlegt, um die Zuordnung zu einzelnen Funktionselementen zu erschweren. Bei der Produktion der Chipkarte wird nach der Personalisierung (dem Aufbringen der persönlichen Informationen des Karteninhabers) eine Sicherung im Inneren des Chips durchgebrannt. Weiterhin wird in einem bestimmten Bereich im EEPROM vermerkt, dass die Karte nicht mehr in einen Test-Modus gebracht werden kann. Dieser Test-Modus ist bei der Produktion wichtig, da hierbei auf alle Speicherbereiche frei zugegriffen werden kann.
Um die Karte vor externen Manipulationen zu schützen, wird weiterhin eine Passivierungsschicht auf den Chip aufgetragen, die ihn vor chemischen Angriffen schützt. Durch Widerstands- bzw. Kapazitätsmessung wird das Fehlen dieser Schicht festgestellt und der Chip deaktiviert. Weiterhin wird die angelegte Spannung gemessen um sicherzustellen, dass der Chip in einem für ihn vorgesehenen Spannungsbereich betrieben wird, um nicht unerwünscht Informationen preiszugeben. Eine weitere Schutzmassnahme besteht darin, die angelegte Taktfrequenz zu überwachen. Unterschreitet diese einen gewissen Minimalwert, so wird die Karte deaktiviert, um den Gewinn von Informationen durch einen Einzelschrittbetrieb zu verhindern.

IV.2. Logische Sicherheit

Um die logischen Sicherheitsanforderungen an die Chipkarte zu realisieren, müssen eine sichere Datenspeicherung und eine sichere Kommunikation gewährleistet sein, wobei die sichere Kommunikation durch Kryptographie gewährleistet wird, welche in den nachfolgenden Kapiteln genauer beschrieben wird. Um die sichere Datenspeicherung zu gewährleisten, überprüft das Betriebssystem bei der Initialisierung den Arbeitsspeicher und berechnet für wichtige Teile des EEPROMs Prüfsummen. Weiterhin werden die Inhalte des Speichers vor allem dadurch geschützt, dass nur über die vom Betriebssystem zur Verfügung gestellte Ein- / Ausgabeschnittstelle auf den Speicherbereich zugegriffen werden kann. Ein externer Zugriff wird dadurch verhindert. Ein weiterer Sicherheitsaspekt besteht darin, das Betriebssystem nicht vollständig im ROM des Controllers unterzubringen, sondern lediglich große Teile. Beim Initialisieren der Karte werden die fehlenden Informationen durch die sogenannte Komplettierung aus Tabellen und Konfigurationsdateien ergänzt und durch einen im EEPROM

untergebrachten Code vervollständigt. Somit müssen Chiphersteller nicht das gesamte Wissen über die Software preisgeben. Dieses Schichtenmodell sorgt ebenfalls für weniger Programmier- bzw. Konzeptionsfehler.
Ein weiterer wichtiger Aspekt der logischen Sicherheit besteht darin, die Karte jederzeit deaktivieren zu können. Zum einen wird dies bei defekten Karten benötigt, zum anderen bei Ablauf der Gültigkeitsdauer, um die Analyse abgelaufener Karten zu verhindern. Hierzu löscht das Betriebssystem der Karte sämtliche im Speicher befindlichen Daten.

IV.3. Aufbau des Dateisystems

Ein großer Bestandteil der Sicherheit in Geldkarten besteht in der Verwaltung und Struktur des Dateisystems, da in eben diesen Dateien bspw. der noch geladene Wert der Geldkarte enthalten ist. Sämtliche Dateien, die sich auf der Geldkarte befinden, sind im EEPROM gespeichert. Auf diese Dateien kann nur das Betriebssystem der Chipkarte zugreifen. Zur Verwaltung dieser Dateien gibt es unterschiedliche Typen:

1) **Masterfile (MF)**
   Das Masterfile ist das Wurzelverzeichnis oder Root-Verzeichnis der Dateistruktur. Es muss auf jeder Geldkarte vorhanden sein und darf nur genau einmal existieren. In einem Masterfile können mehrere Dedicated Files (DFs) und Elementary Files (EFs) enthalten sein, die zu einer besseren Strukturierung der Daten führen. Diese Einteilung wird auch Baumstruktur genannt.

2) **Dedicated File (DF)**
   Ein Dedicated File ist ein Verzeichnis, in dem Dateien zusammengefasst werden können. Ein Dedicated File kann sowohl weitere DFs als auch EFs enthalten.

3) **Elementary File (EF)**
   Ein Elementary File entspricht einer Datei, in deren Inhalt Nutzdaten gespeichert werden. Ein EF kann keine weiteren EFs oder DFs enthalten. Die Struktur eines EF kann für jede Datei separat festgelegt werden. Abbildung 9 zeigt die möglichen Strukturen.

Bezeichnung	Beschreibung	Zugriff	Befehle (Beispiele)
transparent (binär, amorph)	keine innere Struktur	byteweise oder blockweise	READ BINARY WRITE BINARY UPDATE BINARY
linear fixed	Verkettung von Records gleicher Länge	wahlfrei	READ RECORD WRITE RECORD UPDATE RECORD
linear variable	Verkettung von Records unterschiedlicher Länge; Längenfeld notwendig	wahlfrei	READ RECORD WRITE RECORD UPDATE RECORD
cyclic	auf linear fixed basierend; enthält zusätzlich Zeiger für zuletzt geschriebenen Satz	wahlfrei	READ RECORD WRITE RECORD UPDATE RECORD
Execute	Speicherung von ausführbarem Programmcode		

Abbildung 9: Mögliche Dateistrukturen

Um die Dateistruktur auf der Chipkarte verwalten zu können, besitzt jedes DF oder EF einen eigenen Namen. Dieser Name ermöglicht eine eindeutige Identifizierung aller Dateien und Verzeichnisse, wird als File Identifier (FID) bezeichnet und als hexadezimale Zahl realisiert.
Das Masterfile hat ebenfalls einen FID, der standardmäßig mit „3F00“ vorgegeben ist.
Zusammengehörende Dateien (EFs) werden in DFs zusammengefasst. Laut den Geldkartenspezifikationen muss die zugrunde liegende Baumstruktur mindestens drei Verzeichnisebenen unterstützen. Änderungen an der Baumstruktur dürfen nur durch Entfernen oder Hinzufügen von Dateien erfolgen, die in der Struktur eine Ebene tiefer liegen. Um eine Anwendung auf einer Chipkarte unterzubringen, wird ein DF erstellt und die zur Anwendung nötigen Dateien (EFs) in diesem DF organisiert. Handelt es sich um eine ausführbare Anwendung, so bekommt das dazugehörige DF einen Application Identifier (AID) zugeordnet, über den die Applikation angesprochen werden kann.
Um nun auf ein DF oder ein EF zuzugreifen, muss dieses durch einen speziellen Befehl selektiert werden. Standardmäßig ist nach der Initialisierung das MF selektiert.

In der nachfolgenden Grafik ist ein Verzeichnisbaum aufgeführt, mit allen notwendigen DFs und EFs, die für die Nutzung einer kontogebundenen Geldkarte notwendig sind.

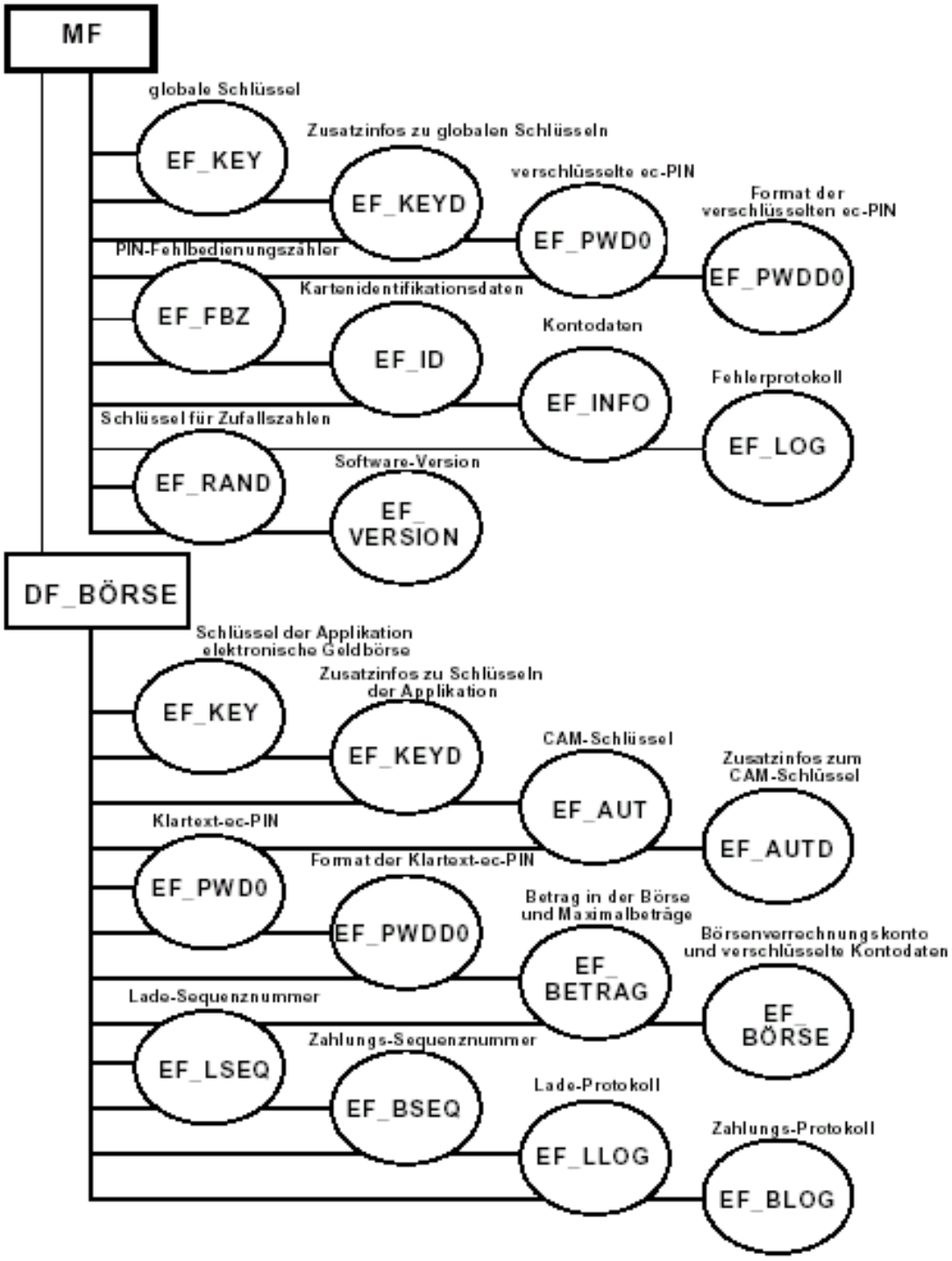

Abbildung 10: Aufbau der Baumstruktur einer kontogebundenen Geldkarte

IV.4. Zugriffsrechte

Beim Erstellen von Dateien oder Verzeichnissen lassen sich explizit Zugriffsrechte festlegen. Diese Access Conditions (AC) hängen vom jeweiligen Datentyp ab und regeln die Steuerung und den Zugriff auf die Daten. Beim Wurzelverzeichnis (Masterfile) und Verzeichnissen (DFs) werden die Möglichkeiten zur Erzeugung von Dateien und Unterverzeichnissen geregelt, bei Dateien (EFs) sind Schreib- und Leserechte gespeichert. Das Betriebssystem steuert den Zugriff auf Dateien und Verzeichnisse anhand dieser Zugriffsrechte. Diese werden bei Erzeugung von EFs bzw. DFs explizit für den jeweiligen Datentyp festgelegt und in einer Zugriffstabelle gespeichert. Access Conditions unterscheiden sich in globale ACs und DF-spezifische ACs. Globale ACs erfordern die Verwendung eines globalen Passwortes oder eines globalen Schlüssels, welcher für den Hauptzugriff auf die Karte zuständig ist. DF-spezifische ACs erfordern ein DF-spezifisches Passwort bzw. einen DF-spezifischen Schlüssel. Laufen auf einer Karte mehrere Applikationen, so gibt es einen globalen Schlüssel, der den Zugriff auf die Karte regelt und für jedes DF kann es mehrere eigene Schlüssel bzw. Passwörter geben. Nachfolgend werden die am häufigsten gebrauchten Zugriffsrechte aufgelistet und erläutert:

AC	Erklärung
ALW (Always)	Der Zugriff auf die Datei ist immer erlaubt
NEV (Never)	Der Zugriff des Kommandos auf die Datei ist nie erlaubt
PWD (Password)	Durch eine AC vom Typ PWD wird festgelegt, dass der Zugriff des Kommandos auf die Datei nur erlaubt ist, wenn zuvor eine Authentikation der externen Welt, wie z.B. das Terminal, durch Angabe eines Passwortes mittels des Kommandos VERIFY stattgefunden hat. Das AC vom Typ PWD legt detailliert fest, ob das zu verwendende Passwort global oder DF-spezifisch ist.
PRO (Protection)	Das AC vom Typ PRO erfordert für den Zugriff des Kommandos auf die Datei eine MAC-Bildung (Message-Authentication-Code)

	zum Nachweis der Integrität. Es handelt sich im eigentlichen Sinne nur dann um ein Zugriffsrecht, wenn sich das AC auf die Kommandonachricht zum Dateizugriff bezieht und durch die externe Welt ausgeführt wird. In diesem Fall ist die Ausführung des Kommandos von dem kommandospezifischen Sicherheits-zustand abhängig.
ENC (Encryption)	Das AC vom Typ ENC erfordert für den Zugriff des Kommandos auf die Datei eine MAC-Bildung zum Nachweis der Integrität und eine Verschlüsselung der Daten zum Nachweis der Vertraulichkeit. Ebenso wie beim AC vom Typ PRO handelt es sich bei der Ausführung um einen kommandospezifischen Sicherheitszustand.
Sowohl beim Typ PRO als auch beim Typ ENC wird bei der Erzeugung eine Referenz auf den zu verwendenden Schlüssel gesetzt.	
AUT (Authenticate)	Durch ein AC vom Typ AUT wird festgelegt, dass der Zugriff des Kommandos auf die Datei nur erlaubt ist, wenn zuvor eine Authentikation der externen Welt mittels des Kommandos EXTERNAL AUTHENTICATE unter Verwendung eines bei der Erzeugung referenzierten Schlüssels stattgefunden hat.

Diese Zugriffsrechte lassen sich auch kombinieren, um beispielsweise Standardkommandos mit der AC „NEV“ zu belegen, aber speziellen Administrationskommandos den Zugriff durch die ACs „ENC+AUT“ zu erlauben. Diese speziellen Administrationskommandos können nur durch spezielle Authentifikation mit separaten Schlüsseln genutzt werden. Zu jeder Datei existiert eine explizite AC für die Gruppe ADMIN, die die Zugriffskontrolle solcher Kommandos festlegt. Gültige Administrationskommandos sind:

- CREATE FILE
- DELETE FILE
- INCLUDE bzw. EXCLUDE (bezieht sich auf Verzeichnisse, um Dateien auszuschliessen oder einzufügen)
- APPEND RECORD (bezieht sich auf Dateien)

IV.5. Kryptographische Protokolle

Um die Vertraulichkeit sowie die Integrität der Daten innerhalb der Geldkarte zu gewährleisten, werden verschiedene kryptographische Algorithmen verwendet. In der momentanen Generation von Geldkarten finden die symmetrischen Verschlüsselungs-algorithmen „Data Encryption Standard“ (DES) und Triple-DES Verwendung. Weiterhin werden „Message Authentication Codes“ zur Sicherung der Integrität gebildet.

Der DES arbeitet mit Blöcken à 64 Bit. Der Schlüssel, der zur Ver- und Entschlüsselung verwendet wird, hat eine Länge von 56 Bit. Somit stehen für die Verschlüsselung 2^{56} Schlüssel zur Auswahl, die bis auf sog. 16 semischwache und 4 schwache Schlüssel alle genutzt werden können. Die Verschlüsselung ist in 16 Runden unterteilt, für die jeweils ein 48 Bit langer Rundenschlüssel generiert wird.
Der DES ist ein sehr schneller Verschlüsselungsalgorithmus, der aber aufgrund der niedrigen Schlüssellänge nicht die gewünschte Sicherheit bringt. Um die Schlüssellänge effektiv zu verlängern, wird der Triple-DES benutzt. Dabei werden drei Verschlüsselungs- und Entschlüsselungsoperationen durchgeführt. Die Schlüssellänge wird beim Triple-DES verdoppelt, da man zwei 56-Bit-lange Schlüssel hintereinander hängt und die 1. und die 3. Operation mit dem gleichen Schlüssel durchführt. Somit erhöht sich die Schlüssellänge von 56 Bit auf 112 Bit. Der erste Teil dieses Schlüssels wird für die 1. und 3. Verschlüsselungs-Operation genutzt, während der zweite Teil des Schlüssels für die in Schritt 2 genutzte Entschlüsselungsoperation verwendet wird.

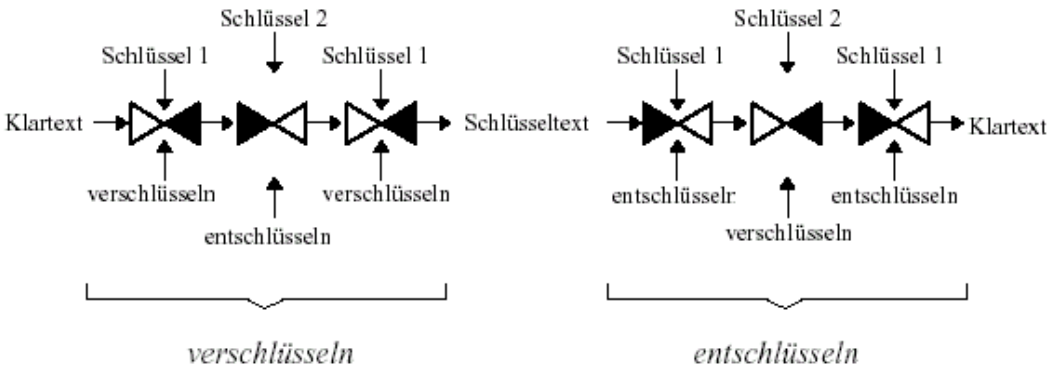

Abbildung 11: Funktionsweise des Triple-DES

Der Vorteil von Triple-DES ist neben der erhöhten Sicherheit, dass bis auf die erhöhte Berechnungszeit kein zusätzlicher Aufwand erforderlich ist. In der momentanen Generation von Geldkarten existiert noch kein implementiertes Hardware-Modul für die Berechnung des DES, der Algorithmus wird daher noch vom Betriebssystem ausgeführt. In der aktuellen Betriebssystemversion der Geldkarte befindet sich eine neue Implementierung des DES-Algorithmus, der besonders sicher gegen „Differential Power Analysis“ und „Differential Fault Analysis“ ist und im Vergleich zu älteren Versionen schneller abläuft. So dauert eine Ver- oder Entschlüsselung von 64 Bit bei 4,9 MHz weniger als 7,5 ms, und ein Triple-DES mit einem 112-Bit-Schlüssel gelingt in weniger als 25 ms. Die genauen Spezifikationen des „Data Encryption Standard“ werden in „Federal Information Processing Standards Publications (FIPS PUBS)“ 46-2 vom „National Institute of Standards and Technologies“ (NIST) beschrieben.
Werden kryptographische Operationen mit dem DES oder dem Triple-DES ausgeführt, so findet in der Geldkarte der spezielle CBC-Modus des DES Verwendung. CBC steht für „Cipher-Block-Chaining“-Modus und stellt sicher, dass jeder verschlüsselte Block vom vorherigen abhängt, um so einen gezielten Austausch einzelner Blöcke zu verhindern. Dem verschlüsselten Block wird der vorherige Ciüher-Block mit einer XOR-Operation aufaddiert:

Verschlüsselung: $Y_i = eK(Y_{i-1})$ XOR (X_i) für i = 1, ... , n

Entschlüsselung: $X_i = dK(Y_i)$ XOR (Y_{i-1}) für i = 1, ... , n

In beiden Fällen gilt für den ersten Block ein 64 Bit langer Initialisierungsvektor Y_0, der als ICV (Initial Chaining Value) bezeichnet wird und explizit festgelegt wird.

Die zweite wichtige kryptographische Operation zur Sicherung der Geldkarte ist die Bildung von „Message Authentication Codes“ (MACs). Diese werden zu einer Nachricht unter Verwendung eines kryptographischen Schlüssels gebildet und mit der Nachricht versandt, damit der Empfänger die Integrität der Nachricht überprüfen kann. Je nach Länge des verwendeten Schlüssels werden in der Chipkarte zwei verschiedene, auf dem DES beruhenden Algorithmen zur MAC-Bildung realisiert, die beide einen 64 Bit langen MAC erzeugen. Das erste Verfahren verwendet einen 56-Bit-Schlüssel und wird als „einfacher MAC“ bezeichnet, während das zweite Verfahren einen 112-Bit-

Schlüssel verwendet und als „Retail MAC“ bezeichnet wird. Beide Verfahren können sowohl im „Cipher-Block-Chaining“-Modus (CBC) als auch im „Cipher-Block-Feedback“-Modus (CFB) betrieben werden. Die genauen Spezifikationen der MAC-Bildung mit dem DES werden in „Federal Information Processing Standards Publications (FIPS PUBS)“ 113 vom „National Institute of Standards and Technology“ (NIST) beschrieben.

Die Schlüssel, die zur Berechnung von MACs bzw. zur Verschlüsselung und Entschlüsselung von Daten benutzt werden, sind je nach Verwendungsart 56 Bit oder 112 Bit lang und leiten sich von einem Hauptschlüssel, auch Masterkey genannt, ab. Dieser Masterkey wurde einmalig vom Zentralen Kreditausschuss erstellt und in zwei Teile aufgespalten, welche in unterschiedlichen Hochsicherheitssafes liegen. Diese beiden Teilschlüssel XOR aufaddiert ergeben den Hauptschlüssel des Geldkartensystems. Um bei kryptographischen Operationen nicht auf den Hauptschlüssel zugreifen zu müssen, wurden zwei reduzierte Schlüssel aus dem Masterkey erzeugt, einen für Händlerkarten und einen für Kundenkarten. Diese „Reduced-Masterkeys“ lassen keine Rückschlüsse auf den Hauptschlüssel zu. Im Geldkartensystem besitzen die verschiedenen Geldkarten nicht die gleichen Schlüssel, sondern jede Karte besitzt ihren eigenen kartenindividuellen Schlüssel, der bei der Personalisierung auf die Karte geschrieben wird. Dieser kartenindividuelle Schlüssel wird von dem entsprechenden Reduced-Masterkey in Abhängigkeit von einem eindeutigen Merkmal wie z.B. der Seriennummer der Geldkarte berechnet. Dieser Reduced-Masterkey wird aus Sicherheitsgründen nicht auf der Geldkarte gespeichert, da bei einer eventueller Aufdeckung des Schlüssels die Sicherheit des Geldkartensystems gefährdet wäre. Der Reduced-Masterkey für die Kundenkarten ist in sichere Hardware-Module eingebaut, die sich in den Händlerterminals befinden und organisatorisch und physisch geschützt sind. Daher ist eine Analyse bzw. eine Manipulation nur schwer möglich. Durch das Fehlen der geheimen Information kann selbst bei Aufdeckung des „Reduced-Masterkey“ nicht auf den Hauptschlüssel geschlossen werden.

Abbildung 12 verdeutlicht die Berechnung des kartenindividuellen Schlüssels.

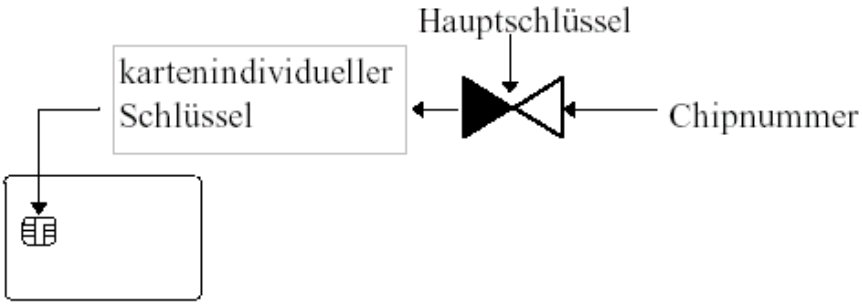

Abbildung 12: Berechnung und Abspeicherung des kartenindividuellen Schlüssels als Geheimnis in der Chipkarte

Soll nun eine verschlüsselte Kommunikation zwischen der Geldkarte und dem Geldkartenterminal stattfinden, um z.B. den Betrag der gespeicherten Karte zu erhöhen oder eine Ware mit dem auf der Karte gespeicherten Guthaben zu bezahlen, so müssen sich Karte und Terminal erst einmal gegenseitig authentifizieren. Hierzu erhält das Terminal auf Anforderung an die Chipkarte die nicht geheime Seriennummer und berechnet nun mit dem in dem Sicherheitsmodul gespeicherten reduzierten Hauptschlüssel den kartenindividuellen Schlüssel der Geldkarte (s. Abbildung 13).

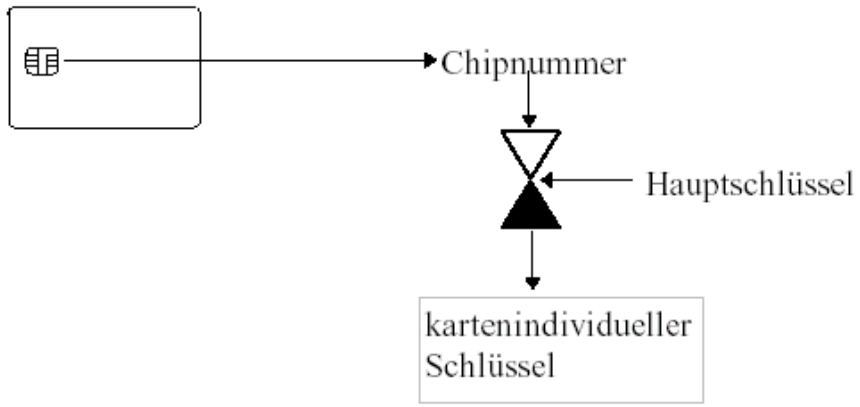

Abbildung 13: Berechnung des kartenindividuellen Schlüssels durch das Terminal

Für die anschließende Authentifizierung besitzen sowohl Karte als auch Terminal denselben Schlüssel und können sicher kommunizieren. Damit sich aber Chipkarte und Terminal beweisen können, dass beide im Besitz der geheimen Information sind, wird eine Authentifizierung nach dem Challenge–Response-Verfahren durchgeführt. Um sowohl Terminal als auch die Geldkarte zu authentifizieren wird ein gegenseitiges symmetrisches Verfahren benutzt, das auf DES beruht. Die gegenseitige

Authentifizierung ist insofern wichtig, dass ein Kunde dem Terminal auch trauen kann, bevor er seine PIN eingibt.

Zuerst verlangt das Terminal von der Chipkarte eine zufällige Zahl. Hat es diese erhalten, so produziert das Terminal ebenfalls eine Zufallszahl und verschlüsselt mit dem gemeinsamen kartenindividuellen Schlüssel die Zufallszahl vom Terminal und die Zufallszahl, die ihm von der Chipkarte zugesandt wurde. Hierzu ist nur eine Verschlüsselung notwendig, da die beiden Zahlen hintereinander geschrieben werden. Das Terminal übermittelt nun diese Nachricht an die Chipkarte, welche sie entschlüsselt, um zunächst die ursprünglich von der Chipkarte erstellte und vom Terminal zurückgesandte Zufallszahl zu überprüfen. Ist die Verifikation erfolgreich verlaufen, so verschlüsselt die Chipkarte die eigene Zufallszahl und die des Terminals, und sendet diese an das Terminal zurück. Durch Umdrehung der Reihenfolge der Verschlüsselung wird die Sicherheit der Authentifikation sichergestellt, da ansonsten durch die Verwendung symmetrischer kryptographischer Verfahren die gleiche Nachricht erzeugt würde. Das Terminal verifiziert die erhaltenen Zahlen, und bei Erfolg sind Karte und Terminal gegeneinander authentifiziert.

Somit ergibt sich folgendes Ablaufdiagramm

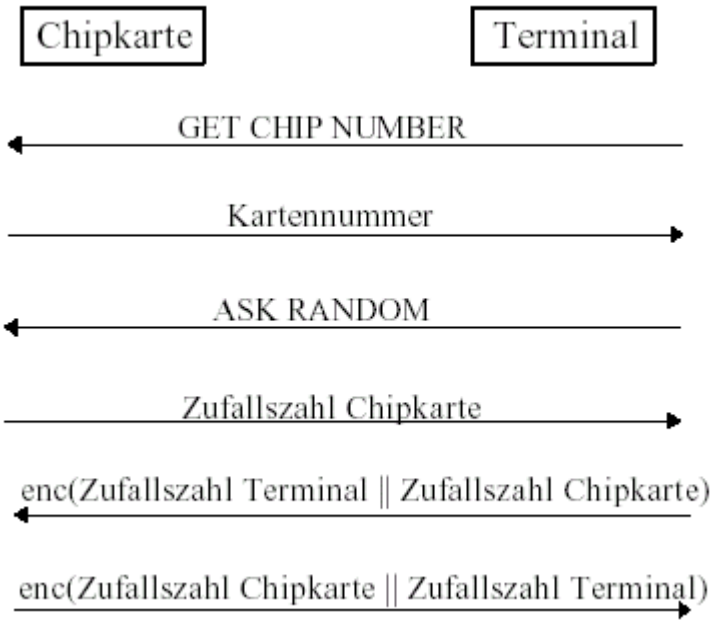

Abbildung 14: Gegenseitige symmetrische Authentifizierung

Die von der Chipkarte erzeugten Zufallszahlen werden für die aktuelle Sitzung gespeichert, um die Generierung einer zufällig gleichen Zufallszahl zu verhindern. Einmal generierte Zufallszahlen werden mit einem Statusbit „ungültig“ versehen und in einem speziell dafür vorgesehenen Elementary File auf der Chipkarte gespeichert, auch wenn sie nicht benutzt wurden. Um einen Pseudo-Zufallszahlengenerator auf einer Smartcard zu implementieren wird der DES im CBC-Modus verwendet, dessen ICV immer mit der zuvor erzeugten Zufallszahl überschrieben wird. Der erste Initialisierungsvektor wird in einem speziell dafür vorgesehenen Elementary File gespeichert und ist auf jeder Karte unterschiedlich.

Sollen am Abschluss eines Geschäftstages die gebuchten Umsätze aus den Händlerkarten an die Evidenzzentralen übermittelt werden, so wird über eine Wählverbindung die Kommunikation zwischen den Händlerterminals und der Zentrale hergestellt. Da in einer Händlerkarte ebenfalls ein händlerkartenspezifischer Schlüssel ist, funktioniert die Authentifikation nach dem gleichem Schema wie bei den Kunden-Geldkarten. Die Zentrale berechnet aus der Händler-ID und dem Reduced-Masterkey für Händlerkarten den händlerkartenspezifischen Schlüssel, mit dem eine sichere Verbindung hergestellt wird. Anschließend werden die Daten verschlüsselt übertragen und vom Händlerterminal gelöscht.

IV.6. Angriffsmöglichkeiten

Betrachtet man die verschiedenen Angriffsmöglichkeiten des Geldkartensystems, so liegt das Hauptaugenmerk in erster Linie auf den Geldkarten selbst. Ein Großteil der Sicherheit im Geldkartensystem besteht aus der Echtheit der Ladeterminals. Diese sind online mit den Bankzentralen verbunden. Nur diese können Geldkarten aufladen, was für die Banken den größten Sicherheitsnutzen bringt. Jedoch basiert die gesamte Kommunikation auf kryptographischen Protokollen bzw. der Geheimhaltung der zugehörigen Schlüssel. Die beste Angriffsmöglichkeit bestünde darin, zu versuchen, an den geheimen Masterkey des Geldkartensystems zu gelangen, sei es durch Einbruch, Bestechung oder Social Engineering. Einbruch fällt bei den verwendeten Hochsicherheitssafes ebenso weg wie Bestechung. Die zu bezahlenden Summen würden den zu erzielenden Gewinn bei weitem übersteigen. Durch spezielle psychologische Schulung und Aufklärung über die Notwendigkeit der Geheimhaltung dieser Schlüssel dürfte auch das Social Engineering wegfallen.

Die Möglichkeiten, an einen geldkartenspezifischen Schlüssel zu gelangen, sind sehr gering, da diese in speziell gesicherten Bereichen auf der Geldkarte gespeichert und physikalisch geschützt sind. Durch die speziellen Zugriffsrechte und die einzige Möglichkeit, über das Betriebssystem an sensible Daten zu gelangen, ist ein Auffinden verwendeter Schlüssel nahezu auszuschließen. Würde man es schaffen, die nach der Personalisierung der Geldkarte durchgebrannte Sicherung wiederherzustellen, so kann man die Karte in einen Test-Modus schalten und somit auf alle Speicherbereiche frei zugreifen. Ross Anderson beschreibt in seinem Buch „Security Engineering“, dass so etwas möglich sei. Allerdings wäre der Aufwand im Vergleich zum Nutzen zu groß.

Bei den verwendeten kryptographischen Schlüsseln und Algorithmen besteht durch langjährige Erfahrung und Verbesserung der Implementierung kaum noch die Chance, Schwachstellen im Algorithmus zu finden. Lediglich die „Brute-Force“-Suche nach passenden Schlüsseln durch Ausprobieren wäre möglich, allerdings nur bei Verwendung des DES, da die dort verwendete Schlüssellänge zu kurz ist. Da die wichtigsten Bereiche der Geldkarte mit einem Triple-DES verschlüsselt sind, welcher eine doppelt so lange Schlüssellänge aufweist wie der DES, ist der Aufwand einer „Brute-Force“-Suche nicht mehr realisierbar.

Um die „Brute-Force“-Suche nach Schlüsseln zusätzlich zu erschweren, ist das Betriebssystem an gewisse Latenzzeiten gebunden. Dauert eine Operation zu lange oder werden zu viele falsche Eingaben gemacht, wird die Karte deaktiviert.

Wäre man im Besitz des Betriebssystemquellcodes, so könnte man nach Schwachstellen im implementierten System suchen und sich eventuell vorhandene Schwächen zu Nutze machen. Diese Annahme ist aber rein hypothetisch, da der Quellcode des Betriebssystems geheim ist und es sich dabei nur um einen Teil der gesamten Software handelt. Bei der Initialisierung der Geldkarte wird das Betriebssystem aus Tabellen und Dateien aus dem EEPROM ergänzt und komplettiert.

Im Falle der Kompromittierung eines geldkartenspezifischen Schlüssels und einer demzufolge erfolgreichen Authentifikation z.B. durch Aufsetzen eines falschen Ladeterminals, könnte man die Geldkarte zwar mit Guthaben aufladen, allerdings wäre der erzielte Erfolg nur von kurzer Dauer. Aufgrund der Führung spezieller Schattenkonten ist eine Aufdeckung des Missbrauchs innerhalb kürzester Zeit möglich. Bei kontogebundenen Geldkarten ist damit ein Zusammenhang zur wahren Identität des Geldkarteneigentümers sofort herzustellen. Erfolgversprechender scheint da die Verwendung von „White Cards“ zu sein, da nicht sofort ein direkter Bezug zu einer realen Person hergestellt werden kann. Ist man einmal im Besitz eines geldkartenspezifischen Schlüssels, so gibt es einige interessante Angriffsmöglichkeiten. Zum Beispiel sind die zu verwendenden kryptographischen Algorithmen für bestimmte Dateien in Tabellen realisiert. Darin wird detailliert definiert, wann der DES und wann der Triple-DES verwendet werden muss. Schafft man es, die Tabelle insofern zu ändern, dass bei allen Operationen DES verwendet wird, oder erreicht man sogar, die Verschlüsselung komplett auszuschalten, so steht einer Manipulation der Geldkarte nichts mehr im Wege.
Die zu verwendenden Schlüssel stehen in speziellen Elementary Files im Dateisystem der Geldkarte. Eine Änderung dieser Schlüssel ist aber aus praktischen Gründen nicht möglich, da diese bei einem möglichen Bezahlvorgang identisch mit dem vom Terminal errechneten Schlüssel sein müssen.

Um das auf der Geldkarte gespeicherte Guthaben dennoch zu erhöhen, ohne die Geldkarte manuell aufzuladen, gibt es in einer speziellen Datei (EF_ID) einen 22 Byte langen Record, bei dem das 21.igste Byte die Wertigkeit der Währung enthält. Dieser Multiplikator steht standardmäßig auf „10^{-2}“, um zu definieren, dass der gespeicherte Betrag in EuroCent auf der Karte gespeichert ist. Schafft man es, diese Variable zu ändern (z.B. auf „10^{0}“) so enthält die Karte z.B. bei einem gespeicherten Guthaben von 0,40 € nach der Änderung ein Guthaben von 40,-- €. Man muss dabei jedoch den maximalen Verfügungsrahmen der Karte beachten. Allerdings wird diese Variante spätestens dann aufgedeckt, wenn das Schattenkonto überzogen wurde.

Ein lohnenswerteres Ziel scheint jedoch die virtuelle Händlerkarte in Softwareform zu sein. Durch Einsatz von speziellen Disassemblern ließe sich der „Reduced-Masterkey“ gewinnen, mit dem man gültige Geldkarte-ID - Geldkarte-Secret – Tupel generieren könnte. Im nächste Schritt könnte man Smartcards fertigen, die mit dem Reduced-Masterkey bei jedem Kaufvorgang eine neue ID und ein neues, dazu passendes Secret berechnen. Mit der so erstellten Geldkarte kann man zwar Waren einkaufen, jedoch wird der Betrug in jedem Falle aufgedeckt, da die Geldkarten-ID wahrscheinlich nicht existiert und, falls doch, fällt es spätestens dann auf, wenn der rechtmäßige Besitzer sein Guthaben verbaucht.

Das Klonen von Geldkarten scheidet komplett aus, da man Schwierigkeiten haben dürfte, an die nötige Hardware zu gelangen bzw. die dazu notwendigen Smartcard-Rohlinge zu bekommen. Selbst bei Erfolg könnte man nicht doppelt bezahlen, da der Missbrauch wiederum bei der Prüfung der Schattenkonten auffallen würde.

V. Zukunftsvisionen – Die Geldkarte als „All-Round“-Karte

Obwohl die Geldkarte mit weit über 55 Millionen im Umlauf befindlicher Karten das weltweit am weit verbreitetste elektronische Geldbörsensystem ist, konnte sich das System bislang nicht durchsetzen. Anfängliche Schwierigkeiten der Akzeptanz durch Kunden und Händler beruhten hauptsächlich auf Unwissenheit. Über 1/3 aller Bundesbürger, die im Besitz einer Geldkarte sind, sind sich darüber nicht bewusst bzw. wissen nicht um die Funktion des goldenen Chips auf ihrer ec-Karte. Weitere Startschwierigkeiten ergaben sich durch die anfänglich geringe Verbreitung von Ladeterminals und Akzeptanzstellen. Mittlerweile gibt es in der BRD zwar über 22.000 Ladeterminals und weit über 70.000 Händlerterminals, die Zahl der durchgeführten Transaktionen lag 1999 jedoch immer noch bei durchschnittlich einer halben Transaktion pro Karte und Jahr.
Die notwendige deutschlandweite Umstellung aller Automaten auf den Euro führte zu einer Erhöhung der Akzeptanz, da viele Automaten mittlerweile standardmäßig die Nutzung der Geldkarte unterstützen, was das „lästige“ Kleingeldzählen überflüssig macht, sei es an Park-, Zigaretten- oder Süßwarenautomaten.

Da die Geldkarte kein nennenswertes Konkurrenzprodukt hat, wird sie sich langfristig durchsetzen, spätestens jedoch, wenn die Kunden gemerkt haben, wie zugänglich, unkompliziert und effektiv die Handhabung der Geldkarte eigentlich ist. Durch kleine Taschenlesegeräte ist jederzeit eine Kontrolle des noch vorhandenen Guthabens möglich, ebenso wie ein Überblick über die 15 letzten getätigten Käufe.

Durch die Implementierung und Umstellung des neuen Betriebssystems ist der erste Schritt zu einer einheitlichen europäischen elektronischen Geldbörse getan. Ein erster Schritt ist die Einführung der "Purse Application for Cross Border Use in Euro" (PACE). Die Systembetreiber Cetrel (miniCash, Luxemburg), Cartes Bancaires (moneo, Frankreich) und der ZKA (Geldkarte, Deutschland) haben sich zusammengetan, um sicherzustellen, dass die Systeme der Partner ab 2001 alle ihre Karten akzeptieren. Die Tatsache, dass die französischen und luxemburgischen Systeme auf der Geldkarte aufbauen, erleichtert dabei die Implementierung.
Eine Kompatibilität zu anderen als den genannten Geldbörsen ist jedoch weitaus komplexer und kann mit der aktuellen Betriebssystem-Variante nicht erreicht werden.

Deshalb arbeiten die Chipkartenunternehmen mit eigenen Entwicklungsabteilungen bereits an der nächsten Fassung, dem so genannten "erweiterten" Betriebssystem, das auch als SECCOS 5.0 bezeichnet wird. Dieses nächste Betriebssystem soll asymmetrische Verschlüsselungen und digitale Signaturen unterstützen. Basieren bisher noch alle kryptographischen Geldkarten-Algorithmen auf DES, beziehungsweise Triple-DES, so will man künftig auf das RSA-Verfahren zurückgreifen. Eine Signatur-Anwendung in der ec-Chipkarte wird dem deutschen Signatur-Gesetz (SigG) entsprechen müssen und erfordert die Einführung einer landesweiten PKI. Hier spielt auch die Schlüsselgenerierung eine wesentliche Rolle: SigG-konforme Schlüssel müssen in einer gesicherten Umgebung erstellt werden. Hier bietet sich der Chip selbst an und wird daher vermutlich nicht nur zur Speicherung der RSA-Schlüssel, sondern auch zu deren Generierung dienen. An Konzepten zur Verwaltung der Vielzahl an "Geldkarten-Schlüsseln" wird bereits gearbeitet.
Der RSA-Algorithmus ist auch für den internationalen Gebrauch der Karte wichtig: Die im vergangenen Jahr verabschiedeten „Common Electronic Purse Specifications“ (CEPS) definieren die Schnittstellen für ein weltweites Geldbörsen-System und benutzen RSA.
Da der Nutzer einer Geldbörse nicht mehrere Guthaben unterschiedlicher Börsen-Systeme auf seiner Karte haben sollte, sieht CEPS ein einziges Guthaben vor, auf das man über unterschiedliche Schnittstellen zugreifen kann. So würde die Geldkarte in Deutschland über die Geldkarten-Schnittstelle geladen, eine Transaktion etwa in Paris oder Rom jedoch über die CEPS-Schnittstelle abgebucht. Der GSM-Standard für Mobiltelefone hat gezeigt, dass eine solche Standardisierung zu einer weltweiten Akzeptanz führen kann und eine essenzielle Voraussetzung für internationalen Erfolg darstellt.

Durch das offene Betriebssystem des Geldkartenchips ist eine Erweiterung der Funktionalität sehr einfach realisierbar. In einigen Pilotprojekten werden bereits auf Geldkartenchips elektronische Fahrausweise, Studentenausweise oder elektronische Zutrittskontrollen implementiert. Der erste Eindruck ist durchaus positiv.
Einige Anbieter nutzen die Geldkarte für Bonusprogramme wie z.B. günstigeres Parken in Parkhäusern, wobei die Geldkarte selbst als Parkausweis genutzt wird, günstigere Eintrittspreise in Freizeitparks oder Museen bzw. Rabatte beim Entleihen eines Mietwagens.

Der VfB Stuttgart hat seine ClubCard um die Geldkartenfunktion erweitert und reguliert so den Zutritt zu VIP-Bereichen und wickelt sämtliche Transaktionen in Gastronomien und Fan-Shops darüber ab.

Weitere Möglichkeiten bieten sich mit der Einführung der UMTS-Handy-Netze und der Einführung neuer Technologien. Durch sogenannte Dual-Slot-Handys soll es dann möglich sein, seine Geldkarte direkt über das Handy zu laden, bzw. Zahlvorgänge übers Handy mit Hilfe der Geldkarte abzuwickeln. Momentane mobile Bezahlvorgänge erfordern die Anmeldung bei Diensten wie PayBox, die nicht anonym sind.

Durch die zukünftige Generation von Geldkartenhardware mit integriertem RSA-Chip steht auch dem Einsatz von HBCI (Home Banking Computer Interface) in Verbindung mit der Geldkarte nichts mehr im Wege.

VI. Fazit

Die Entwicklung des Geldkartensystems als elektronische Geldbörse ist ein sehr guter Bargeldersatz für kleine Geldbeträge. Sowohl der Einsatz im täglichen Leben als auch bei spezielleren Einsatzgebieten wie z.B. Bezahlungen im Internet sind mit der Geldkarte gut und einfach realisierbar. Der technische Fortschritt und die innovativen Entwicklungen der zugrundeliegenden Smartcard, ebenso wie die implementierten kryptographischen Algorithmen und die Sicherheitsmechanismen des Betriebssystems, machen die Geldkarte zu einer äußerst sicheren und vor Manipulation geschützten Lösung für elektronisches Kleingeld.

Durch den beschränkten Verfügungsrahmen, den das Geldkartensystem mit sich bringt, ist der Aufwand für die erfolgreiche Brechung der Sicherheitsmechanismen nicht lukrativ. Daher bietet die Geldkarte (noch) nicht den Anreiz für derartigen Zeit- und Geldaufwand.

Mit zunehmender Akzeptanz und Fortschritten in der Entwicklung sowohl der Hardware als auch zusätzlicher Anwendungen ist mit der Geldkarte eine gute Plattform für die Zukunft geschaffen. Die erfolgreiche Umstellung des Geldkartensystems auf den Euro und die Minimierung der Fehler, die bei der Handhabung mit der Geldkarte auftreten können, machen sie zu einem attraktiven Werkzeug im Alltag eines Käufers. Allerdings bietet die Geldkarte nicht nur dem Kunden Vorteile. Der Händler profitiert ebenfalls von dem Geldkartensystem, da die Kundschaft eher zu Spontankäufen angeregt wird, wenn sie das Geld nicht „direkt aus der Hand“ geben muss. Weiterhin werden die Kosten für eventuell anfallende Online-Kosten zur Authorisierung von ec-Karten oder Standleitungen zu Banknetzwerken gesenkt, da Bezahl-Transaktionen offline stattfinden.

Die günstigen Produktionskosten ermöglichen eine schnelle und effiziente Verbreitung, nicht nur für Banken und Sparkassen, sondern auch in anderen Bereichen.

Universitäten können die offenen Spezifikationen des Geldkarten-Betriebssystems ebenso nutzen, wie Fan-Clubs oder Bibliotheken und so mit eigenen Applikationen den Kunden Dienste anbieten, ohne dass diese gleich mehrere Karten mit sich führen müssen. Dadurch, dass die Geldkarte fast alle Eigenschaften von natürlichem Bargeld erfüllt, wie z.B. Sicherheit, Offline-Bezahlung und Übertragbarkeit, könnte in einigen Jahren das normale Bargeld der Vergangenheit angehören. Lediglich die Anonymität des Geldkartensystems lässt noch zu wünschen übrig.

VII. Abkürzungsverzeichnis

Abkürzung	Bedeutung
AC	Access Condition
ACE	Advanced Crypto Engine
AID	Application Identifier
APDU	Application Protocol Data Unit
ATR	Answer-to-Reset
BIOS	Basic-Input-Output-System
BRD	Bundesrepublik Deutschland
BSFT	Banken-Sonderfunktions-Terminal
CBC	Cipher-Block-Chaining
CEPS	Common Electronic Purse Specifications
CFB	Cipher-Block-Feedback
CPU	Central Processing Unit
DES	Data Encryption Standard
DF	Dedicated File
EC	Electronic Cash
EEPROM	Electric Erasable Programmable Read Only Memory
EF	Elementary File
ENC	Encryption
EZ	Evidenzzentrale
FID	File Identifier
FIPS PUBS	Federal Information Processing Standards Publications
GF	Galois Field
GSM	Global System for Mobile Communication

HBCI	Home Banking Computer Interface
HEZ	Händlerevidenzzentrale
I/O	Input / Output
ICV	Initial Chaining Value
KEZ	Kartenevidenzzentrale
KID	Key ID
LRC	Longitudinal Redundancy Check
MAC	Message Authentication Code
MF	Master File
MFC	MultiFunctionCard
NIST	National Institute of Standards and Technologies
PACE	Purse Application for Cross Border Use in Euro
PC	Personal Computer
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PTS	Protocol Type Selection
RAM	Random Access Memory
ROM	Read Only Memory
RSA	Rivest Shamir Adleman
SECCOS	Secure Card Operating System
SIGG	Signatur Gesetz
SW	Status Word
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
VFB	Verein für Bewegungsspiele
ZKA	Zentraler Kreditausschuss

VIII. Bildnachweis

Abbildung	Quelle	Seite
1	Bartsch, C., Geldkarte, *http://www.zahlungsverkehrsfragen.de/Geldkarte.html, 2000*	5
2	Schütt, S. / Kohlgraf, B., Chipkarten, 1996, S.21	12
3	Rankl, W. / Effing, W., Chipkarten, 1996, S. 32	14
4	Rankl, W. / Effing, W., Chipkarten, 1996, S. 124	16
5	Rankl, W. / Effing, W., Chipkarten, 1996, S. 155	17
6	Rankl, W. / Effing, W., Chipkarten, 1996, S. 202	18
7	Rankl, W. / Effing, W., Chipkarten, 1996, S. 204	18
8	Rankl, W. / Effing, W., Chipkarten, 1996, S. 175	19
9	Gentz, W., Die elektronische Geldbörse, 1997, S. 24	23
10	Schnittstellenspezifikation für die ec-Karte mit Chip, Version 2.2, 1997, S. 191	24
11	Rankl, W. / Effing, W., Chipkarten, 1996, S. 94	27
12	Rankl, W. / Effing, W., Chipkarten, 1996, S. 271	29
13	Rankl, W. / Effing, W., Chipkarten, 1996, S. 271	30
14	Rankl, W. / Effing, W., Chipkarten, 1996, S. 272	31

IX. Literaturverzeichnis

Beykirch, H.-B., Anonymität und Reklamation – ein Widerspruch?, iX, Verlag Heinz Heise, 12/1998,
http://www.heise.de/ix/artikel/1998/12/148/02.shtml

Beykirch, H.-B., Chipgeld, iX, Verlag Heinz Heise, 12/1998,
http://www.heise.de/ix/artikel/1998/12/148

Beykirch, H.-B., Geldkarten-Latein, iX, Verlag Heinz Heise, 12/1998,
http://www.heise.de/ix/artikel/1998/12/148/01.shtml

Ferrari, J. / Poh, S., Smartcards, A Case Study, IBM, 1998,
http://www.redbooks.ibm.com

Fiesel, Stefan, Elektronische Geldbörsen – Das Konzept der Geldkarte, Hauptseminar Elektronische Zahlungssysteme, Universität Stuttgart, Fakultät für Informatik, SS 2001

Focus Online, Geldkarte, Archiv Focus, 2002,
http://www.focus.de

Gentz, Wolfgang, Die elektronische Geldbörse, Fachhochschule München, Fachbereich Informatik, 1997

Giesecke & Devrient GmbH, Geldkarte – das weltgrößte elektronische Geldbörsensystem, 2001,
http://www.gdm.de/ger/products/03/index.php4?product_id=137

Giesecke & Devrient GmbH, Geldkarte System Description, 2000,
http://www.gieseckedevrient.com

Giesecke & Devrient GmbH, Modernste Technologie für elektronische Geldbörsen, 2001,
http://www.gdm.de/ger/products/03/index.php4?product_id=136

Giesecke & Devrient GmbH, Smart Payment Cards, Security by G&D, 1999,
http://www.gieseckedevrient.com

Greiersen, A., Neue Geldkarte – Versionen und Visionen, Secu-Media Verlags GmbH, Ingelheim, KES 6/2000

Kölbe, Generationen von Chipkartenlesern, Archiv ZDF-Online, 26.07.2001,
http://heute.t-online.de

LDA Brandenburg, Datenschutzprobleme der Geldkarte, 3/1998,
http://www.brandenburg.de/land/lfdbbg/dsk/dsk55/dsk5502.htm

Müller, D., Geldkarte gehackt?, 12/1999,
http://news.zdnet.de/zdnetde/news/story/0,,s2049735,00.html

Müller, D., Geldkartenhack: Entwarnung, 12/1999,
http://news.zdnet.de/zdnetde/news/story/0,,s2049745,00.html

National Institute of Standards and Technologies (NIST), Federal Information Processing Standards Publications (FIPS PUBS)“ 46-2
(http://www.itl.nist.gov/fipspubs/fip46-2.htm)

National Institute of Standards and Technologies (NIST), Federal Information Processing Standards Publications (FIPS PUBS)“ 113
(http://www.itl.nist.gov/fipspubs/fip113.htm)

Rankl, W. / Effing, W., Chipkarten, 1996

Rolle, M., Zahlung mittels Geldkarte, Lehrstuhl für Bürgerliches Recht, Prof. Dr. Franz Häuser, Universität Leipzig, 2000

Schnittstellenspezifikation für die ec-Karte mit Chip, Version 2.2, 1997,
http://www.ccc.de

vera@verbrauchernews.de, Das Ende der Geldkarte?, Der Verbraucher-Newsletter vom 01.10.1999,
http://www.verbrauchernews.de/finanzen/drucken.html?article=0000003733

Verlag Heinz Heise, Banken einig – Geldkarte zum Bezahlen im Internet, 5/1999,
http://www.heise.de/newsticker/data/cp-31.05.99-001

Verlag Heinz Heise, Geldkarte und der Euro, 1/2000,
http://www.heise.de/newsticker/data/hod-03.01.02-000

Verlag Heinz Heise, Geldkarten-Leser fürs Internet zugelassen, 11/2000,
http://www.heise.de/newsticker/data/ad-09.11.00-000

Verlag Heinz Heise, Wenig Vertrauen in Geldkarte, ecash & Co, 3/2000,
http://www.heise.de/newsticker/data/ad-07.03.00-000

VÖB-ZVD GmbH, Übersicht zum Zahlungssystem Geldkarte,
http://www.voeb-zvd.de/Geldkarte.htm