Diplomarbeit

Vergleichende Analyse von elektronischen Geldtransfer-Systemen

Arbeitsgruppe Rechnernetze und Verteilte Systeme

Prof. Dr. Peter Ladkin

Andreas Kaiser

Abgabe: 5. August 1998

Danksagung

An dieser Stelle möchte ich mich bei all denen bedanken, die mich in der Zeit dieser Arbeit unterstützt haben.
Besonderer Dank gilt hier meinem Betreuer Peter Ladkin, der mir während der Arbeit mit vielen Ideen und Ratschlägen zur Seite stand. Herzlicher Dank geht ebenso an meine Eltern und Schwestern, die mich liebevoll unterstützt haben, sowie an Markus, Susanne, Milan, Martin, Nancy und Michael, die an der Erstellung mit Anregungen und eifrigem Korrekturlesen beteiligt waren.

Inhaltsverzeichnis

1 Einleitung **2**

2 Das Phänomen *Geld* **7**

2.1 Der Weg zum abstrakten, elektronischen Geld 7

2.2 Institutionelle Tatsachen 11

2.3 Das Artefakt Geld 12

3 Die herkömmlichen Instrumente des bargeldlosen Zahlungsverkehrs **14**

3.1 Scheck 15

3.2 Überweisung 18

3.3 Lastschrift 18

4 Kommunikation **21**

4.1 Kryptographie 24

4.1.1 Symmetrische Verschlüsselung 25

4.1.2 Asymmetrische Verschlüsselung 25

4.2 Zertifikate 26

4.3 Secure Socket Layer (SSL) 26

4.4 Secure Electronic Transactions (SET) 27

5 Kommunikation im Internet **31**

5.1 Internet-Protokolle 31

5.1.1 IP 32

5.1.2 ICMP 34

5.1.3 TCP 34

5.1.4 UDP 35

5.2 Das Domain Name System (DNS) 36

5.3 Zusammenfassung 38

6 Zahlungssysteme für das Internet **39**
6.1 eCash 39
6.2 CyberCoin 45

7 Kartenbasierte Systeme **50**
7.1 Debitkarte 50
7.2 Kreditkarte (Bankkreditkarte) 55
7.3 GeldKarte 59

8 Simuliert die GeldKarte Geld ? **65**

9 Schlußbetrachtung und Ausblick **73**

A Das System *Geld* in TLA+ **78**

B Das System *GeldKarte* in TLA+ **83**

C Verwendete Module **90**
C.1 Modul SemaphoreBin 90
C.2 Modul Sequences 91

Literaturverzeichnis **91**

„... in ... Zeiten ..., wo die Römer, anstatt des abgebildeten Ochsen auf ihren Ledermünzen, das Rindvieh selber vorführten.“

[Jean Paul]

Kapitel 1

Einleitung

In der vorliegenden Arbeit wird ein Ausschnitt aus der gesellschaftlichen Realität mit Mitteln der Informatik beschrieben und untersucht. Gegenstand der Betrachtung ist der Zahlungsvorgang mit Geld aus der Sicht der Informatik.

Ziel der Arbeit ist die Beschreibung und der tentative Vergleich verschiedener Systeme, die den Zweck dieses sozialen Algorithmus erfüllen, um darauf aufbauend der Fragestellung nachzugehen, ob die Zweckdienlichkeit eines Systems dem eigentlichen Zweck aus Benutzer-Perspektive entspricht. Oder anders formuliert: Leistet ein System den Dienst für seine Benutzer, den es leisten sollte?

Die Hauptgesichtspunkte bei der Beschreibung der Systeme sind hierbei:

Beteiligte Die in die Durchführung eines Zahlungsvorgangs involvierten Parteien in minimaler Umgebung, wobei minimale Umgebung bedeutet, daß die Beschreibung allein die minimalen Voraussetzungen und notwendigen Aktionen zur Leistung einer Wertübertragung von einer Person auf eine andere enthält. Gefragt ist im Zusammenhang mit dem Ziel der Arbeit das grundlegende Prinzip eines Zahlungsvorgangs, nicht der Umfang der Möglichkeiten, die ein System bzw. Verfahren bietet.

Zuordnung Die Relation eines werttragenden Objektes bzw. Zahlungsmittels zu der Person des Benutzers. Der Begriff der *Person* wird in der Arbeit durchgehend synonym für die juristische Definition *„natürliche oder juristische Person“* verwendet. Es wird keine explizite Unterscheidung zwischen Person, Unternehmen oder Organisation vorgenommen.

Aktionen Die erforderlichen Aktionen zur finalen Durchführung eines Zahlungsvorgangs und deren zeitliche Abfolge.

Aufbauend hierauf wird exemplarisch an einem ausgewählten System die Herangehensweise skizziert, wie mit formalen Mitteln der Informatik der Aspekt der *Zweckdienlichkeit im Kontext von sozialen Algorithmen* untersucht werden kann. Die konkrete Fragestellung ist, ob die Spezifikation eines elektronischen Zahlungssystems die Spezifikation des sozialen Algorithmus von *Geld* aus Benutzersicht erfüllt. Hierbei wird nicht die Wertübertragungs-Funktion untersucht, die vom Emittenten des Zahlungsmittels in beiden Fällen allgemein garantiert ist, sondern es geht um den Vergleich der Rahmenbedingungen und Eigenschaften des Zahlungsvorgangs zweier Systeme. Untersuchungsgegenstand ist somit die *Benutzeroberfläche* der Systeme.

Grundlegende Annahme dieser Ausarbeitung ist, daß ein Zahlungsvorgang mit Hilfe eines Zahlungssystems final durchgeführt ist, wenn ein bezifferter *Wert* von einem Zahlungssender auf einen Zahlungsempfänger übertragen ist. Zur Beschreibung des Prinzips dieses Vorgangs werden die oben erwähnten Gesichtspunkte 'Beteiligte', 'Zuordnung' und 'Aktionen' herangezogen. Wichtig ist außerdem, wann ein Zahlungsvorgang abgeschlossen ist, also zu welchem Zeitpunkt bzw. im Zuge welcher Aktionen der eigentliche Geldtransfer erfolgt. Wo befindet sich der *Wert* und somit das *Geld* in einem bestimmten Zustand eines Zahlungsvorgangs, der aus mehreren unabhängigen Aktionen besteht?
Zur Klärung dieser Sachverhalte der einzelnen Systeme wurden, da jedes der betrachteten Systeme an Geschäftsbanken[1] geknüpft ist, zuerst mehrere, größtenteils telefonische Interviews mit Mitarbeitern von Kreditinstiuten geführt. Ein wichtiger Punkt dieser Gespräche bestand weiterhin in der Erörterung des benutzten Zahlungsmittels. Der Begriff des *Zahlungsmittels* findet in der gesamten Ausarbeitung Anwendung, ohne aussagen zu wollen, daß es sich bei dem Zahlungsmittel eines Systems immer um wirkliches Geld handelt.
Dies geschieht entgegen der ökonomischen Definition in [Jarchow, 1984], in der die beiden Begriffe Zahlungsmittel und Geld gleichgesetzt werden: „Ganz allgemein kann man unter *Geld* oder *Zahlungsmittel* alles verstehen, was im Rahmen des nationalen Zahlungsverkehrs einer Volkswirtschaft generell zur Bezahlung von Gütern und Dienstleistungen oder zur Abdeckung anderer wirtschaftlicher Verpflichtungen akzeptiert wird." Dieses Zitat benennt außerdem das Fehlen einer präzisen Definition von *Geld*, auf die sich die folgenden Betrachtungen stützen könnte.

Die Problematik ist also, welche Definition von Geld dieser Ausarbeitung zu Grunde liegen kann, wenn es keine präzise ökonomische Begriffsdefinition gibt. Desweiteren problematisch ist: Was wird von einer Zahl bzw. einem Token[2] repräsentiert, das zum Zwecke der Durchführung eines Zahlungsvorgangs zwischen beteiligten Personen transferiert wird? Wird ein konkreter Wert transportiert?

[1] Es wird kein Unterschied zwischen Bank und Sparkasse gemacht, in der Arbeit werden durchgehend die Begriffe *Bank* und *Kreditinstitut* synonym verwendet.

[2] Zeichen

Wichtig ist im Zuge dieser Arbeit der Gesichtspunkt, daß das den finanziellen Wert repräsentierende *Zahlungsmittel* getrennt vom Begriff des in sich Wert tragenden *Tauschmittels* verwendet wird. Dieser wesentliche Unterschied bezieht sich auf die Möglichkeit des frei in einer Gesellschaft zirkulierenden, an ein Objekt geknüpften *Wertes* und wird eingehend behandelt, wenn es im Schlußteil um die besonderen Eigenschaften von elektronischem Geld gehen wird.

Vorweggenommen werden muß an dieser Stelle, daß sich als ein wesentlicher Punkt bei der Durchführung eines Zahlungsvorgangs die notwendige bankeninterne Buchungstransaktion darstellt. In allen der folgenden Systeme handelt es sich bei dem eigentlichen Geldtransfer im Verlauf eines Zahlungsvorgangs um Bewegungen zwischen Konten. Die sogenannten *Buchungsschnitte*, die Zeitpunkte, an denen alle im letzten Intervall vorgemerkten Buchungstransaktionen beim Kreditinstitut durchgeführt werden, erfolgen in bestimmter Periodik, in der Regel einmal am Tag. Ein über Banken abgewickelter Geldtransfer geschieht somit immer mit einer bestimmten zeitlichen Verzögerung und nie in Echtzeit.

„Konten fungieren als klassisches Hilfsmittel jeder Bankentätigkeit. [...] Jede Geschäftsverbindung, die auf Geldbewegungen abzielt, beginnt mit der Errichtung eines oder mehrerer Konten [...]“ [SANDKÜHLER, 1992, S. 92]

Das wesentliche Prinzip des kontobasierten Geldtransfers ist die atomare Buchungs-*Transaktion* auf Grundlage einer doppelten Buchführung. Die vier wesentlichen Eigenschaften einer atomaren Transaktion sind

- Unteilbarkeit des Vorgangs, er erfolgt ganz oder gar nicht
- Konsistenz, die beidseitige Übereinstimmung
- Isoliertheit, somit Tranaktionen untereinander völlig unabhängig
- Stabilität, es muß zu jedem Zeitpunkt die Möglichkeit zur Wiederherstellung des letzten konsistenten System-Zustandes geben

Ein entscheidender Gesichtspunkt jedes Systems ist somit der der Zuordnung von Person zu Konto. Im Gesetzestext heißt es dazu: „§163 AO[3] bestimmt, daß niemand auf einen falschen oder erdichteten Namen für sich oder einen anderen ein Konto errichten oder Buchungen vornehmen lassen [...] darf. [...] [Eine] genaue Bezeichnung des Kontoinhabers mit Adressenangabe ist unerläßlich. [...] Als Legitimation genügt der mit Lichtbild versehene amtliche Personalausweis[...].“ [LEXIKON, 1968, Band II, S.1028]

[3] Abgabenordnung

Die Auswahl der Systeme für diese Arbeit hat sich an das Kriterium der weiten Verbreitung gehalten. Da keine Statistik über die Nutzung elektronischer Geldtransfer- bzw. Zahlungssysteme vorliegt, beruht die Wahl vorwiegend auf eigenem Ermessen. Bei den beiden in Kapitel 6 behandelten Internet-Zahlungssytemen war ausschlaggebender Faktor der bei beiden Systemen in Deutschland laufende Pilotversuch, somit der praktische Einsatz der Systeme. Im Verlauf dieser Arbeit konnten viele andere Internet-Zahlungssysteme aufgrund der ausschließlich theoretischen Grundlage nicht auf sinnvolle Weise in die Betrachtung mit einbezogen werden. Vielfach blieb die Frage nach der eigentlichen Realisierung eines Zahlungsvorgangs offen, das theoretische System blieb die Antwort nach der konkreten Realisierung schuldig. Außerdem stellte sich im Fall von MilliCent[4] beispielsweise die Betrachtung in *minimaler Umgebung* als besonders nachteilig und wenig sinnvoll heraus, da die Konzeption des Systems gerade auf einen großen Benutzerkreis mit einem hierarchisch aufgebauten Systemanbieter-Kreis zielt. Ähnliches gilt für NetCash[5].

In dieser Arbeit werden die einzelnen Systeme in minimaler Umgebung beschrieben, so daß der Gesichtspunkt des sogenannten *Abrechnungsverkehrs*[6] der Banken untereinander, der von den Landeszentralbanken und Girozentralen abgewickelt wird, keine Beachtung findet. Alle Beschreibungen von Zahlungsvorgängen gehen davon aus, daß nur eine Bank beteiligt ist und, falls notwendig, stehen Zahlungssender und Zahlungsempfänger mit dieser einen Bank in Verbindung.

Eine Unterscheidung zwischen *Geldtransfer* und *Zahlung* wird bei den einzelnen Systemen nicht konsequent vorgenommen. Intuitiv bringt man oft den Begriff der Zahlung in Verbindung mit dem Begriff des Handels und den Begriff des *Geldtransfers* mit einer Wertübertragung getrennt von der Erbringung einer Gegenleistung. Diese Eingrenzungen werden allerdings im folgenden nicht gemacht.

Überblick und Herangehensweise Im einleitenden Kapitel über Historie und Wesen des Geldes wird deutlich, daß es sich bei *Geld* eben nicht um ein technisches Objekt, sondern um ein psychologisches Phänomen, ein von Menschen geschaffenes Artefakt handelt. Der wichtigste Aspekt in diesem Zusammenhang, der des allgemeinen Vertrauens und der Übereinkunft der System-Benutzer untereinander, wird besonders in Abschnitt 2.2, der *Theorie der institutionellen Tatsachen* hervorgehoben.
In diesem Kapitel wird nicht zuletzt die Bedeutung des bereits oft verwendeten,

[4]nähere Informationen zu diesem System finden sich unter [MilliCent, 1998] und [Glassmann *et al.*, 1995]

[5]siehe [Medvinsky u. Neumann, 1995]

[6]die Erfüllung fälliger Verbindlichkeiten

aber nie näher erläuterten *Wert*-Begriffes deutlich.

Im Kapitel 3 werden die drei herkömmlichen Instrumente des bargeldlosen Zahlungsverkehrs beschrieben. Die Notwendigkeit dieser Beschreibung ergibt sich aus der Tatsache, daß diese Instrumente in vielen Fällen die grundlegende Realisierung des eigentlichen Geldtransfers für die im weiteren Verlauf der Arbeit behandelten Systeme bilden.

Das vierte Kapitel beschäftigt sich mit den wesentlichen Eigenschaften der Kommunikation zwischen zwei sich gegenüberstehenden Personen zum Zweck der Durchführung einer Wertübertragung. Diese Eigenschaften müssen ebenso in einer Umgebung vorhanden sein, in der die Kommunikationspartner räumlich voneinander entfernt nur mittels Daten-Fern-Übertragung (DFÜ) miteinander verbunden sind.

Das folgende Kapitel geht als Grundlage der beiden in Kapitel 6 behandelten Internet-Zahlungssysteme *eCash* und *CyberCoin* der Frage nach, inwiefern der aktuelle Stand der Internet-Technologien die in dem vorausgegangenen Kapitel erläuterten Eigenschaften der Kommunikation erfüllen.

Kapitel 7 beschreibt das Prinzip eines Zahlungsvorgangs mit den drei kartenbasierten Zahlungssystemen *Point of Sale* (in Verbindung mit der *Debitkarte*), *Kreditkarte* und *GeldKarte*.

In Kapitel 8 wird, aufbauend auf der Beschreibung des *GeldKarten-Systems* im vorangegangenen Kapitel, exemplarisch skizziert, mit formalen Methoden der Informatik eine Beantwortung der Frage 'Simuliert das GeldKarten-System *Geld* ?' herbeizuführen. Als Beschreibungsmittel wird die *Temporale Logik der Aktionen*, auf deren formaler Grundlage die Anwendung eines logisch-mathematischen Beweisverfahren erfolgen kann, herangezogen. Ein Beweis wird im Rahmen dieser Arbeit allerdings nicht geführt, da er den Umfang der Arbeit übersteigt. Es wird die Herangehensweise veranschaulicht.

In der Schlußbetrachtung wird im Anschluß an die Zusammenfassung die Besonderheit von sogenanntem 'elektronischen Geld', wie es in Abschnitt 6.1 über des Internet-Zahlungssystems *eCash* genannt wird, behandelt. Ferner wird Stellung zu den in Abschnitt 2.2 beschriebenen Gedanken zur *Institution Geld* in Bezug auf einige der behandelten elektronischen Zahlungssysteme genommen.

Kapitel 2

Das Phänomen *Geld*

Als Einleitung in das Thema *Geld* soll im folgenden kurz die Entstehungsgeschichte des Phänomens *Geld* dargelegt werden[1], ohne allerdings einen Anspruch auf Vollständigkeit erheben zu wollen. Es geht vordergründig um die Frage: Wie ist die Vorgeschichte des elektronischen Geldes, welches heutzutage im Volumen das materielle Geld weit überwiegt?
Der Abschnitt 2.1 macht deutlich, daß der Geldbegriff nicht nur aus ökonomischer Sicht, sondern auch aus historischer Sicht schwer zu fassen ist. Im den darauffolgenden beiden Abschnitten wird die *Theorie der institutionellen Tatsachen* von John R. Searle und deren Anwendung auf das Thema Geld zusammengefaßt.

2.1 Der Weg zum abstrakten, elektronischen Geld

Seit mehreren Tausend Jahren gibt es zwischen zwei Personen den Mechanismus des direkten Tausches von Gütern und damit verbunden den Begriff des *Handels*. Eine frühe Theorie der Geldgeschichte geht von der Vorstellung aus, daß zur Vereinfachung der Verfahrensweise des Handels die Idee von einem Universal-Pfand entstanden ist und so der Begriff des *Geldes* geboren wurde. In der heute gängigen Theorie der Geldentstehung nimmt man allerdings an, daß das menschliche Bedürfnis nach einem Wert- und Rangordnungsmittel uns somit nach einem Wertaufbewahrungsmittel und einem Wertmaßstab unabhängig von den Anfängen der Tauschwirtschaft in der menschlichen Gesellschaft zur Schaffung der ersten *Geld-Objekte* führte. Die Tauschmittelfunktion und Wertübertragungsfunktion von Geld hat später die Möglichkeiten der gesellschaftlichen Institution Geld durch zusätzliche Funktionen/Algorithmen

[1] Grundlage dieses Abschnitts ist das Kapitel 'Begriff und Aufgaben des Geldes' aus [Bundesbank, 1997]

erweitert. In [Lexikon, 1968, S.588] heißt es dazu: „Sieht man im Geld [...] ein Substrat der zwischenmenschlichen Kommunikation, die zur Natur des Menschen gehört, so ist der Ursprung des Geldes älter als die arbeitsteilige Volkswirtschaft [...]“. Die Sichtweise vom „Geld [als] ein[em] zweckvoll geschaffene[n] Werkzeug zur Erleichterung des Tausches“ entspricht somit nicht ganz dem historischen Wissensstand. In den folgenden Ausführungen wird allerdings der Tausch-Mechanismus als der in dieser Arbeit interessante Gesichtspunkt des *Geldes* im Vordergrund stehen.

Mit dem Vorhandensein eines Tauschmittels entfällt die Notwendigkeit, daß jemand einen Gegenstand von einer Person nur durch Tausch gegen einen konkreten anderen Gegenstand erwerben kann. Mit *Geld* steht als *Universal-Pfand/Zwischentauschgut* ein Tauschmittel zur Verfügung, welches einen abstrakten Gegenwert repräsentiert. Das *Wertmaß* hierzu gründet auf der Arithmetik der Mathematik.

Die Erscheinungform des Geldes hat sich im Laufe der Zeit stetig geändert. In den Anfängen des Tauschhandels gibt es nur das *Warengeld*, meist knappe, begehrte Güter wie z.B. Muscheln oder Gewürze. Mit der Entdeckung von Metallen geht die Erfindung von Münzen als Zahlungsmittel einher[2]. Zuerst wird nur mit uneinheitlichen Metallstücken gehandelt, die zur Wertbemessung abgewogen werden müssen, später dann auf genormte Münzen der entsprechende Wert aufgedruckt (das sogenannte *'Zeichengeld'*). Es ist schnell klar, daß einheitliche Metallmünzen wesentliche Vorteile gegenüber verderblichem, schlecht teilbarem Warengeld haben. Von nationalen Regierungen wird schließlich das allgemeine Tauschmittel zum gesetzlichen Zahlungsmittel erklärt. So werden Kurantmünzen zum ersten definitionsgemäßen *Geld*. Die vier wesentlichen Funktionen, die Geld erfüllt, sind Tauschmittel, Maßstab zur Wertbemessung, Wertübertragungsmittel und Wertaufbewahrungsmittel. Der aufgeprägte Wert entspricht dem Metall-Wert der Münze selbst. Goldschmiede sind zu dieser Zeit *Geld-Emittenten*, sie prägen aus Edelmetallen Münzen und tauschen sie gegen Warengeld ein.
Mit der Idee, Edelmetalle bzw. die Münzen u.a. aus Sicherheitsgründen bei den Goldschmieden in Verwahrung zu geben und dafür Quittungen (also private Schuldversprechen der Goldschiede) zu bekommen, ist die erste *Bank* und das erste (abstrakte) *Papiergeld* geboren[3]. Papiergeld ist also ursprünglich die

[2]Die so vereinfachend formulierte *Warentheorie des Geldes*, die allein den Geldstoff als Wesens- und Wertmerkmal ansieht, beachtet nicht die zentrale Rolle der allgemeinen, gesellschaftlichen Anerkennung der Institution *Geld* (siehe Abschnitt 2.2.)

[3]Im Rahmen der britischen Geldverfassung ist später gestritten worden, ob Banknoten nur Stellvertreter der bei der Zentralbank lagernden Münzen oder als selbständige *Geldzeichen* anzusehen seien. In diesem Zusammenhang kam die Meinung auf, daß nur diejenigen Tauschmittel als *Geld* zu bezeichnen wären, die nicht nach kurzzeitigem Umlauf automatisch

„Verbriefung einer Forderung auf Metallgeld“ [Harlandt, 1989, S.179]. Papiergeld hat große Vorteile gegenüber Metallmünzen, die zur allgemeinen Verbreitung der Geldform beitragen. Der Transport ist einfacher und die Herstellungskosten niedriger.

Der Schritt zum *Kreditgeld* und somit zum Mechanismus der *Geldschöpfung* ist nicht mehr weit, wenn man sich vorstellt, daß das Vertrauen in die ausgegebenen Hinterlegungsscheine in der Gesellschaft wächst und schließlich mehr Scheine ausgegeben werden als Werte hinterlegt worden sind. Diese Scheine kann man vielleicht in dieser Situation als *ungedeckte Banknoten* ansehen. Um das Vertrauen der Bevölkerung in die nationale Währung zu sichern, wird bald ein der Menge des umlaufenden Geldes entsprechender Wert in Waren, meist Edelmetalle wir Gold oder Silber, bei einer zentralen Institution hinterlegt, der *Zentralbank*.

Das umlaufende (materielle) Geld in Gestalt der Banknoten und Münzen hat die im folgenden aufgelisteten wesentlichen Eigenschaften.

- Es ist allgemein akzeptiertes Zahlungsmittel; die Geldeinheiten besitzen nur die *Geld-Funktion*, sind z.B nicht gleichzeitig Genußmittel wie Zigaretten.
- Ein Transfer von Geld hinterläßt keine weitere Forderung gegenüber dem Zahlungssender, eine Zahlung ist *final*.
- Der Wert ist inhärent in den Geldeinheiten enthalten, es gibt keine weiteren Erfordernisse zum Geldtransfer als die Übergabe der Einheiten an den Zahlungsempfänger.
- Es gibt keine Beziehung oder es kann keine Beziehung hergestellt werden zwischen den aufeinanderfolgenden Besitzern einer Geldeinheit. In der Geldeinheit ist keine Information für eine Zuordnung zu einer Person enthalten bzw. speicherbar.[4]

Neben dem materiellen Geld in Form der Münzen und Scheine ist Anfang des 16. Jahrhundert eine andere abstrakte, aber nicht-physikalische Geldform entstanden, das *Buchgeld*, Geld was nur als Zahlen in den Büchern von Banken existiert. Die ersten Girobanken werden in dieser Zeit gegründet und es gibt anfänglich für die Kunden die Geldtransfer-Instrumente *Scheck* und *Überweisung*[5]. Der Geldtransfer erfolgt in diesem System ausschließlich zwischen

wieder zum Verschwinden kämen. Dieser Gesichtspunkt wird noch an anderer Stelle, wenn es um die Eigenschaften des *elektronischen Geldes* geht, wichtig sein (siehe hierzu Kapitel 9).

[4] Dieser Punkt ist allerdings nur für Münzen gegeben, Banknoten besitzen Sereinnummern zur Identifizierung.

[5] das *Lastschriftverfahren* kommt zu einem späteren Zeitpunkt hinzu

Girokonten (Gutschrift auf der einen Seite und Belastung auf der anderen). Der Übergang vom Warengeld zum stoffwertlosen bzw. immateriellen Geld wird durch entsprechend der Gesamt-Geldmenge hinterlegte Warenwerte beim Geld-Emittenten gesichert.

Die Entwicklung geht also weg vom reinen Warengeld mit *inhärentem Wert* hin zu einem „[...] im Gelde verkörperten [und dokumentierten] Wertversprechen [...]“[LEXIKON, 1968, Band I, S.601].

Die in Deutschland bis zum Jahre 1914 bestehende *Golddeckung* der Währung und damit verbundene durch staatliche Autorität garantierte unmittelbare *Goldeinlösung* von Banknoten ist einer Währung ohne konkrete Deckung gewichen. Der hinterlegte materielle Waren-Gold-Wert ist zuerst einer teilweisen Deckung durch eine entsprechende Goldmenge und schließlich durch die abstrakte offizielle Repräsentation bzw. Dokumentation eines Anteils am nationalen Sozialprodukt durch die Nominalwerte von Banknoten ersetzt worden.

Dieser Wandel ändert auch die Wertschätzung des Geldes. Nun ist nicht der Warenwert entscheidend sondern die Menge des Geldes. Das Geldsystem basiert auf dem Prinzip Wert aus Knappheit. Wichtig wird, daß kein großes Mißverhältnis zwischen umlaufender Geldmenge und Gütermenge entsteht. Es gibt nun anstatt des hinterlegten Edelmetalls den abstrakten Gegenwert der gesamten volkswirtschaflichen Gütermenge. Eine zentrale Kontroll-Instanz, die *Zentralbank*, sorgt national für eine möglichst konstante Geldmenge.

Wie besonders noch im nächsten Abschnitt erläutert wird, basiert das Wesen des Geldes auf dem allgemeinen Vertrauen der Benutzer bzw. der ganzen Gesellschaft in das Zahlungsmittel. Voraussetzung für die Funktionalität von *Geld* ist das Geldwertbewußtsein in der Gesellschaft. Jeder muß sich sicher sein, daß er den nahezu gleichen Warenwert, den er für einen bestimmten Geldbetrag eingetauscht hat, zu einem späteren Zeitpunkt zurückbekommt.

F. Knapp beschreibt in seiner *Staatlichen Theorie des Geldes* (1905) Geld primär als Träger von Rechtsbeziehungen zwischen Personen. Dieser juristische Aspekt wird in späteren Kapiteln bei der Beschreibung von elektronischen Zahlungssystemen von Bedeutung sein, wenn ein elektronisches Zahlungssystem vielfältige vertragliche Bindungen zwischen beteiligten Personen erfordert.

Heutzutage ist das damals auf Seiten von Büchern verzeichnete *Buchgeld* in die elektronische Datenverarbeitung (EDV) übergegangen. Ohne den Einsatz von EDV wäre der bargeldlose Zahlungsverkehr im aktuellen Umfang sonst nicht realisierbar.

Banknoten sind zwar einziges *unbeschränktes gesetzliches Zahlungsmittel*[6], aber Bankenguthaben in Form von Sichteinlagen (= täglich fällige Einlagen) werden ebenso zum Geld gerechnet, sie sind *allgemein akzeptiertes Zahlungsmittel.* Die Umwandlung von Giralgeld in Bargeld (und somit in gesetzliches Zahlungsmittel) ist jederzeit möglich. Damit das nur als numerischer Saldo gespeicherte Giralgeld die Funktion als Zahlungsmittel erfüllt, müssen Banken für dessen Umlauf sorgen und Instrumente zum Giral-Geldtransfer zur Verfügung stellen. Auf diese Instrumente wird im nächsten Kapitel eingegangen.

2.2 Institutionelle Tatsachen

In diesem Abschnitt wird die *Theorie institutioneller Tatsachen* von JOHN R. SEARLE im Zusammenhang mit dem Phänomen Geld erläutert. Searle führt in seinem Buch [SEARLE, 1995][7] als klassisches Beispiel eines menschlichen Artefakts das Geld an.

Grundlegender Gedanke seiner Theorie ist, daß viele objektive Fakten unabhängig von ihrer Erscheinung allein auf der Basis von menschlichen, mentalen Zuständen existieren. *Manche Dinge existieren, weil wir glauben, daß sie existieren.*[8]

Eine kollektive Ziel- und Zweckgerichtetheit einer Personengruppe legt einem bestimmten Phänomen einen speziellen, neuen Status auf. Dieser Status ist in den meisten Fällenverbunden mit einem oder mehreren sogenannten *Status-Funktionen.* Sowohl der Status als auch die auferlegten Status-Funktionen ergeben sich nicht aus den intrinsischen Eigenschaften des Phänomens selbst. Sie existieren nur auf der Grundlage von kollektiver, kontinuierlicher Übereinkunft bzw. Akzeptanz im Denken der beteiligten Personen. Die Existenz eines solchen Artefakts kann nur relativ zur Intention der Benutzer oder Betrachter erfaßt werden, sie fußt allein auf mentalen Zuständen beteiligter Personen.

Die Status-Auferlegung ist bei allen institutionellen Formen in einer menschlicher Kultur bzw. Gesellschaft beschreibbar als

X zählt als Y im Kontext C.[9]

Das Objekt (der X-Term) der Institution repräsentiert nicht nur den Status (den Y-Term), sondern es eröffnet in Verbindung mit den Status-Funktionen

[6]Münzen sind lediglich beschränktes gesetzliches Zahlungsmittel

[7]vergleiche zu diesem Abschnitt [SEARLE, 1995, S. 1-124]

[8]„[...] there are things that exist only because we believe them to exist." [SEARLE, 1995, S. 1]

[9]vergl. [SEARLE, 1995, S. 27f,43f]

dem Benutzer bzw. Betrachter die Möglichkeit von *Aktivität*. Eine institutionelle Tatsache ist allgemein gesprochen eine *Ermächtigung zum Handeln*.

Es sind drei Aspekte *in der Evolution* institutioneller Tatsachen zu unterscheiden, die Erzeugung, die Existenz und die Repräsentation einer Institution.

- Die **Erzeugung** ist den Beteiligten unbewußt, sie geschieht im allgemeinen als ein sozialer Prozeß.
- Die **Existenz** einer Institution basiert auf der kontinuierlichen Akzeptanz des Artefakts. Geht die Übereinkunft verloren, hört die Institution auf zu existieren. Die konstitutiven Regeln einer Institution sind meist explizit in *Gesetzen* verankert. So garantiert der Staat (selbst Institution) mit Hilfe von *Erlassen* für die Existenz anderer Institutionen, z.B. der Institution *Geld*. Ein Indikator der Akzeptanz ist der kontinuierliche *Gebrauch* der institutionellen Status-Objekte.
- Als Grundbedingung für die Existenz muß die Institution als solche erkennbar sein. Es ist eine aussagekräftige Dokumentation erforderlich, eine **Repräsentation**.

2.3 Das Artefakt Geld

Eine Definition des Begriffs Geld kann nach Searle nur in Verbindung mit der Aussage *Geld ist institutionelles Faktum* erfolgen. Geld ist klassisches Beispiel für eine Tatsache, die offenkundig objektiver Art ist, aber sich im Rahmen eines naturwissenschaftlichen Weltbildes, allein im Rahmen der natürlichen, *begreifbaren* Fakten, nicht hinreichend beschreiben läßt[10].

Geld benennt analog zu den Überlegungen des letzten Abschnitts einen neuen Status und gleichzeitig eine Menge von Status-Funktionen. Ein System konstitutiver Regeln ist Grundlage der Existenz der *Institution Geld*. Einerseits müssen die Geld-Objekte gewissen minimalen Bedingungen des X-Terms genügen. Sie müssen im Hinblick auf die zu erfüllenden Funktionen bestimmte Eigenschaften wie Beständigkeit, Seltenheit, Fälschungssicherheit, offizielle Dokumentation einer Wert-Garantie durch Autorität u.a. besitzen, ohne die eine allgemeine Akzeptanz nicht denkbar wäre. Andererseits haben alle Objekte, die die Bedingungen erfüllen, eine Menge auferlegter Status-Funktionen (z.B.: *Gesetzliches Zahlungsmittel für alle öffentlichen und privaten Verpflichtungen* oder *Wertaufbewahrungsmittel*) (Y-Term). Sie *zählen als Geld*. Dieses kollektive, intentionale Verhalten der Benutzer, das Auferlegen des *'Zählen-als'*, ebenso

[10]dieser Abschnitt gibt, bis auf die Anmerkungen zu *elektronischem Geld*, die Gedanken des Autors wieder (vergl. [Searle, 1995, S. 1-124])

wie das allgemeine Einvernehmen aller Mitglieder der Gesellschaft, in der die Institution existiert, *erzeugt* erst die institutionelle Tatsache *Geld*.

Da die Zweckdienlichkeit der Institution *Geld* im Vordergrund steht, ist das konkrete Objekt (der X-Term) nur im Hinblick auf die praktische Ausübung der Status-Funktion interessant. Die Geld-Objekte werden von den Benutzern ignoriert, bewußt ist nur die den Objekten zugeschriebene kontinuierliche Möglichkeit der Aktivität. Im Falle von Geld betrifft die Hauptfunktion die Zahlungs- bzw. Tauschmöglichkeit auf der Basis des allgemein anerkannten *Wertes*, einer weiteren gesellschaftlichen Institution. Das Objekt selbst dient allein der Repräsentation des Bündels von auferlegten Status-Funktionen.

Der Prozeß der Erzeugung der Institution Geld wurde im Abschnitt 2.1 deutlich, in dem kurz auf die Evolution des Geldes eingegangen wurde. Dabei wurden ebenfalls staatliche Maßnahmen zur Garantie der Existenz der Institution Geld erwähnt als Grundlage für die heutige Situation, in der Geld ein Objekt mit einem abstrakten Gegenwert in Form des national erwirtschafteten Wertes ohne gleichzeitig hinterlegte Wertgegenstände darstellt. Auf elektronisches Geld[11] trifft nicht der Aspekt einer gesellschaftlichen Evolution zu, es handelt sich um im Zuge der Konzeption von technischen Systemen entwickelten *Hilfsmitteln zur Duchführung einer Wertübertragung*.

Es handelt sich bei den in dieser Arbeit behandelten elektronischen Zahlungssystemen insgesamt um *Werkzeuge* zur Handhabung von einer bereits existierenden Geldform, dem Buchgeld. Es wird keine neue Geldform geschaffen. Aus diesem Grund ist die Anwendung der Theorie von SEARLE in diesem Zusammenhang nicht möglich. Der Autor bezieht sich in seinen Überlegungen auf die traditionelle, nationale Währung, die in historischem Zusammenhang entstanden ist.

Die teilweise bei den im folgenden behandelten Zahlungssystemen benutzten Token bzw. gespeicherten Zählerständen auf transportablen Karten sind nicht im Sinne von SEARLES Überlegungen als Geldeinheiten anzusehen, sondern als Hilfsmittel zur Durchführung einer Zahlung, als Repräsentanten für den beim Emittenten der Token (einer Bank) verbleibenden tatsächlichen Geldwert in Form von Kontosalden. Sie tragen keinen Wert in sich, sondern stellen - wie in der Einleitung bereits erwähnt - die *Verpflichtung des Zahlungsmittel-Emittenten zur Zahlung des repräsentierten Wertes an den Inhaber dar.* Dieser Punkt muß natürlich national aufgrund des geltenden Monopols der Zentralbank zur Emission von Geld sichergestellt sein.

[11] Diese Bezeichnung bezieht sich hier auf die bei den in dieser Arbeit behandelten Zahlungssystemen benutzen Zahlungsmittel, die im Gegensatz zu Banknoten und Münzen in sich keinen Wert tragen.

Kapitel 3

Die herkömmlichen Instrumente des bargeldlosen Zahlungsverkehrs

In diesem Kapitel werden die von der Kreditwirtschaft in Deutschland angebotenen konventionellen Mittel des bargeldlosen Zahlungsverkehrs *Überweisung*, *Lastschrift* und *Scheck* beschrieben. Mit ihnen wird gegenwärtig der weitaus größte Teil des Zahlungsverkehrs in Deutschland abgewickelt. Im Mittelpunkt der Betrachtung steht der Aspekt des Zahlungsvorgangs, wobei die Rahmenbedingungen und Eigenschaften der Verfahrensweise im einzelnen erläutert werden.

Die Notwendigkeit der Ausführungen in diesem Kapitel ergibt sich aus der Tatsache, daß einzelne Instrumente bei mehreren der nachfolgend betrachteten Systeme als Grundlage des Geldtransfers zwischen zwei Personen benutzt werden.

Bei allen drei Verfahren[1] wird Buchgeld auf dem Wege von Buchungstransaktionen zwischen zwei Girokonten bewegt.
Beteiligt an einem Zahlungsvorgang in Annahme einer minimalen Umgebung[2] sind bei allen Verfahren des bargeldlosen Zahlungsverkehrs jeweils Zahlungsempfänger, Zahlungssender und eine Bank als vermittelnde Instanz.

Voraussetzung für einen Zahlungsvorgang unter Nutzung der Instrumente ist jeweils eine vertragliche Bindung des Zahlungssenders mit der Bank. Es muß zwischen Zahlungssender und Bank ein *Girovertrag* bestehen. Mit Ausnahme des Schecks ist bei Überweisung und Lastschrift zusätzlich eine vertragliche Bindung zwischen Zahlungsempfänger und Bank erforderlich.

[1] mit Ausnahme des Orderschecks ohne Verrechnungsvermerk (s. Abschnitt 3.1)

[2] wie in der Einleitung bereits erwähnt, wird von *einem* Kreditinstitut bei der Beschreibung eines Zahlungsvorgangs ausgegangen

Bei einem Zahlungsvorgang mit den Zahlungsinstrumenten wird zwischen Zahlungssender und Zahlungsempfänger Buchgeld anstatt Bargeld bewegt. Der eigentliche Geldtransfer erfolgt innerhalb der Bank auf dem Wege einer Buchungstransaktion.

Aus Gründen der Zuordbarkeit gibt es wie bereits erwähnt in Deutschland keine anonyme Kontoführung. Die Authentifizierung des Kontoinhabers geschieht bei den drei Verfahren jeweils auf Basis des nationalen Rechtssystems mittels handschriftlicher Unterschrift. Die Authentifizierung eines *rechtmäßigen Benutzers* mit Hilfe einer physikalischen Karte bzw. eines Personalausweises wird nicht durchgeführt.

Das Prinzip eines Zahlungsvorgangs mittels der Instrumente ist, daß ein Kontobesitzer bzw. eine von ihm für definierte Aktionen autorisierte Person als Zahlungssender eine der beiden anderen Parteien zur Belastung des eigenen Girokontos ermächtigt oder beauftragt. Dies kann entweder einmalig in definierter Höhe oder als *Sammelauftrag* für mehrere Zahlungsvorgänge gleichzeitig in vom Zahlungsempfänger definierter Höhe geschehen. Daraufhin führt entweder die Bank die Anweisung zur Ausführung des Geldtransfers direkt aus oder der Zahlungsempfänger muß mit einer separaten Aktion die Bank zum Einzug des Zahlungsbetrages beauftragen.

3.1 Scheck

> „[..] eine gegen eine Bank (oder anderes Geldinstitut) gerichtete *täglich* fällige Forderung auf Bargeld [wird] an ein (drittes) Rechtssubjekt abgetreten [...]" [Harlandt, 1989, S.113]

Ein Scheck ist ein sogenanntes *Zahlungspapier* mit beliebigem Betrag als Instrument des bargeldlosen Zahlungsverkehrs. Mit einem Scheck weist der Zahlungssender seine Bank zur Zahlung des angegebenen Betrages an den Überbringer an. Gleichzeitig ist der Scheck die Anweisung an die Bank zur Belastung des Girokontos des Zahlungssenders. In juristischer Terminologie ist ein Scheck ein *Wertpapier*, das die rechtliche Relation zwischen dem Zahlungssender, dem Zahlungsempfänger und der Bank festschreibt. Zentraler Punkt ist also die *Rechtsbeziehung*, die zwischen den zwei Personen Zahlungssender und Zahlungsempfänger besteht. Zwischen Zahlungssender und Bank muß ein sogenannter Scheckvertrag bestehen, in dem die Bank den Zahlungssender autorisiert zur Ausstellung von Schecks mittels bankspezifischer Formulare (s.u.).

Der Scheckvertrag berechtigt den Zahlungssender generell zum Ausstellen von Schecks und verpflichtet die Bank zum Einlösen von auf ihren Vordrucken ausgestellten Schecks, falls das Girokonto des Zahlungssenders gedeckt ist. Der Scheckvertrag beinhaltet somit die zwei Bedingungen eines Zahlungsvorgangs

- Verwendung von Scheckformularen des betreffenden Kreditinstitutes und
- aureichende Deckung des Girokontos des Zahlungssenders.

Die Gültigkeit eines Schecks bedarf einer bestimmten Form mit fünf Erfordernissen (vergl. [HUECK, 1986, S. 180]). Nur eine Urkunde, die diese Voraussetzungen erfüllt, ist definitionsgemäß ein Scheck im Sinne des deutschen Scheckgesetzes von 1933. Die Erfordernisse sind:

- Bezeichnung als Scheck
- unbedingte Anweisung zur Zahlung einer bestimmten Geldsumme
- Name des Bezogenen
- Angabe über Tag und Ort der Ausstellung
- Unterschrift des Austellers

Das Recht ist direkt durch das Wertpapier verkörpert, das beurkundete Recht ist allein abhängig vom *Besitz* der Urkunde[3]. Eine Übertragung des verbrieften Rechts, und damit eine *Zahlung*, geschieht durch eine Übertragung des Papiers auf eine andere Person[4]. Der Aussteller eines Schecks haftet in jedem Fall für dessen Einlösung, auch im Falle eines nicht bestehenden Scheckvertrages. Auch ein ungedeckter Scheck ist rechtlich gesehen *vollgültig* und hat somit eine Funktion als Nachweis der Pflicht des Austellers zum *Schadensersatz*.

Einem Scheck ist ausschließlich die Zahlungsmittelfunktion auferlegt, er ist konzeptioniert als Mittel des Zahlungsverkehrs und hat aus diesem Grund eine eingeschränkte zeitliche Gültigkeit. Der Inhaber wird durch die Frist zur *baldigen Vorlegung* veranlaßt. Wenn ein Scheck innerhalb dieses definierten Zeitraums ab Ausstellungstag nicht eingelöst wird, so ist er *ungültig* und verliert seine Funktion.

Es gibt den Scheck in zwei Formen, die sich in der Dokumentation des Zahlungsempfängers und somit der Art der Übertragung unterscheiden: zum einen den *Orderscheck* und zum anderen den *Inhaberscheck*. Ein Orderscheck ist definiert als zahlbar an eine in der Dokumentation namentlich genannte Person. Der Scheck darf in diesem Fall den Zusatz *'oder Überbringer'* nicht enthalten. In allen anderen Fällen handelt es sich um einen Inhaberscheck ohne dokumentierte Referenz zur Person des Zahlungsempfängers.

Falls ein Scheck den *Verrechnungsvermerk* enthält, ist damit der Bank verboten, den Scheck bar einzulösen. Der Scheck darf nur auf dem Wege der

[3] Im Gegensatz zu den rechtlichen Bestimmungen eines *Schuldscheins* z.B.

[4] Beim Order-Scheck ist die Person des Zahlungsempfängers festgelegt im Dokument

Gutschrift eingelöst werden. Der Zahlungsempfänger muß in diesem Fall notwendigerweise ein Girokonto bei der Bank führen. Der Mechanismus des Verrechnungsvermerks dient der Minderung des Risikos in Bezug auf Veruntreuung bzw. Fälschung eines Inhaberschecks, da die eindeutige Identifizierbarkeit des Inhabers (des Zahlungsempfängers) gewährleistet ist durch die eindeutige Zuordbarkeit des Kontos zur Person. Ohne den Verrechnungsvermerk geschieht die Einlösung in Form von Bargeld und der Zahlungsempfänger bleibt der Bank gegenüber anonym. Die Identität des Einlösenden wird nicht überprüft.

Das Zahlungsrisiko trägt bei einem Zahlungsvorgang mittels Scheck ohne Verwendung einer Scheckkarte der Zahlungsempfänger. In Verbindung mit einer Scheckkarte (meist der *ec-Karte*) und einem eurocheque-Vordruck geht eine Garantie-Haftung der Bank in Höhe von derzeit 400,00 DM einher. Dies dient der erhöhten Akzeptanz des Schecks als Zahlungsmittel. Im Falle eines Zahlungsvorgangs in Verbindung mit der Scheckkarte enthält der Scheck nicht nur den Anspruch des Zahlungsempfängers (dem Schecknehmer) gegenüber dem Zahlungssender (Aussteller der Schecks), sondern auch die explizite Zahlungsgarantie für den Zahlungsempfänger.

Die Bank sagt mit dem Verfahren zu, einen Scheck bis zu dem Maximalbetrag einzulösen. Die angewandte Verfahrensweise ist die Authentifizierung des Zahlungssenders durch den Besitz der Scheckkarte und der eigenhändigen Unterschrift zum Zeitpunkt der Scheckübergabe. Die eindeutige Nummer der Scheckkarte wird auf der Rückseite des Schecks notiert. Die auf der Karte dokumentierte Kontonummer und die im Formular eingetragene Kontonummer müssen übereinstimmen. Dies wird durch den Zahlungsempfänger überprüft. Letztendlich muß noch die Gültigkeit der Scheckkarte zum Zeitpunkt der Scheckausstellung gegeben sein.
Der eigentliche Geldtransfer zwischen Zahlungssender und Zahlungsempfänger durch den separaten Prozeß des *Einlösens* muß wiederum innerhalb einer bestimmten Frist durch den Zahlungsempfänger erfolgen.

Der Scheck repräsentiert eine Instruktion an eine Bank, die mit dem Vorgang des Einlösens erst den Wert auf den Überbringer überträgt. Das gültige Formular hat also nicht die Funktion eines Zahlungsmittels. „Ein Scheck ist kein Geld, sondern *Hilfsmittel, über Geld, nämlich Buchgeld, zu verfügen.*“ [Harlandt, 1989, S. 115].

Allein die Person des Kontoinhabers kann der Aussteller eines Schecks und somit Zahlungssender mittels dieses Zahlungsinstrumentes sein. Ein Scheck benötigt im Gegensatz zu einem (anonymen) Token wie etwa einer physikalischen Banknote eine Referenz zum namentlich definierten Zahlungssender mit Angabe der Kontoverbindung. Im Gegensatz zur nachfolgend beschriebenen Überweisung muß der Zahlungsempfänger die unabhängige Aktion des Einreichens eines Schecks durchführen, um einen Zahlungsvorgang abzuschließen.

3.2 Überweisung

Überweisung „Buchmäßige Übertragung einer Geldsumme von einem Konto auf ein anderes Konto auf der Basis eines entsprechenden Auftrages [des Zahlungssenders][...]“ [Finanzlexikon, 1996]

Die Überweisung ist zahlenmäßig das herausragende Mittel des bargeldlosen Zahlungsverkehrs in Deutschland. Voraussetzung für einen Zahlungsvorgang sind vertragliche Vereinbarungen, zwei *Giroverträge*, zwischen der Bank und dem Zahlungssender einerseits und der Bank und dem Zahlungsempfänger andererseits. Der Girovertrag beinhaltet die Verpflichtung der Bank, auf dem entsprechenden Girokonto laufende Einzelüberweisungsaufträge des Kunden auszuführen sowie für ihn auf dem Konto eingehende Zahlungen in Form von Giralgeld entgegenzunehmen.

Ein Überweisungsauftrag ist eine Weisung des Kontoinhabers an die Bank.

Im Gegensatz zum Scheck muß auch der Zahlungsempfänger ein Konto bei einem Geldinstitut haben. Dem Zahlungssender muß das Geldinstitut, die Kontonummer und der Name des Empfängers bekannt sein.

Die *finale* Zahlung ist die mit zeitlicher Verzögerung erfolgende Buchungstransaktion bzw. Gutschrift auf dem Girokonto des Zahlungsempfängers. Der Zahlungsempfänger muß keine zusätzliche Aktion ausführen, um den Zahlungsvorgang abzuschließen.

Die Person des Kontoinhabers kann allein mit Hilfe der Überweisung eine Buchungstransaktion zwischen seinem und dem Girokonto des Zahlungsempfängers initiieren. Die Authentifizierung des Auftraggebers erfolgt durch eigenhändige Unterschrift auf dem Überweisungsformular.

3.3 Lastschrift

Lastschrift: „Einzugspapier, mit dem ein Zahlungsempfänger durch Vermittlung eines Kreditinstitutes vom Konto des Zahlungspflichtigen einen Betrag abbuchen läßt. Ausgelöst wird die Zahlung nicht wie beim Dauerauftrag vom Zahlungspflichtigen, sondern vom Zahlungsempfänger, der die Lastschrift bei seiner Bank (erste Inkassostelle) einreicht, die den Lastschriftbetrag gutschreibt und bei der Bank des Zahlungspflichtigen (Zahlstelle) belastet. Grundlage einer Lastschrift ist entweder ein Abbuchungsauftrag oder eine Einzugsermächtigung. Das Lastschriftverfahren ist besonders geeignet für ständig wiederkehrende Zahlungen über unterschiedliche Beträge.“ [Finanzlexikon, 1996]

Der Unterschied zum oben beschriebenen Überweisungsverfahren besteht darin, daß die (*finale*) Zahlung nicht vom Zahlungssender, sondern vom Zahlungsempfänger ausgelöst wird[5]. Der Zahlungssender unterschreibt eine Berechtigung zur Verfügung über das eigene Girokonto. Erst in einem zweiten Prozeß, den der Zahlungsempfänger zu einem vom System nicht vorgegebenem späteren Zeitpunkt ausführt, geschieht der Geldtransfer. Der Zahlungsempfänger reicht bei der Bank die entsprechende Lastschrift ein und beim nächsten Buchungsschnitt erfolgt die Buchungstransaktion, die Giralgeld-Bewegung zwischen dem Konto des Zahlungssenders und dem Konto des Zahlungsempfängers.

Voraussetzung für einen Zahlungsvorgang ist neben dem notwendigen Girovertrag jeweils zwischen Zahlungssender und der Bank und zwischen Zahlungsempfänger und der Bank eine ergänzende vertragliche Vereinbarung zwischen Zahlungsempfänger und Bank, die sogenannte *Zulassung zum Lastschriftverkehr*.

Innerhalb des Lastschriftverfahres wird unterschieden zwischen *Abbuchungsauftragsverfahren* und *Einzugsermächtigungsverfahren.*

Im ersten Fall weist der Zahlungssender die Bank an, die vom Zahlungsempfänger vorgelegten Lastschriften vom (eigenen) Girokonto abzubuchen. Die Bank (des Zahlungssenders) ist bei aureichender Deckung des Kontos berechtigt und verpflichtet zur Einlösung von durch den Zahlungsempfänger vorgelegten Lastschriften (in vom Zahlungssender nicht definierter Höhe). Es existiert kein Widerspruchsrecht, der Zahlungssender kann aber jederzeit den Auftrag zurückziehen. Die (unterschriebene) *Weisung* befindet sich in den Händen der Bank. Eine Überweisung ist eine ähnliche *Weisung*, beinhaltet aber nur einen *einzelnen* Geldtransfer.

Beim Einzugsermächtigungsverfahren autorisiert der Zahlungssender den Zahlungsempfänger, den zu zahlenden Betrag (die fällige Forderung ihm gegenüber) von seinem Girokonto einzuziehen. Es stellt keine Anweisung an eine Bank dar. Der Zahlungsempfänger löst in einem zweiten Schritt den Geldtransfer aus, in dem er die Ermächtigung bei der Bank vorlegt und der angegebene Betrag schließlich per Buchungstransaktion seinem Girokonto gutgeschrieben und dem Girokonto des Zahlunngssenders belastet wird. Die Autorisierung in Form eines vom Zahlungssender unterschriebenen Beleges liegt in diesem Fall in den Händen des Zahlungsempfängers.

Fehlt zum Zeitpunkt der Durchführung der Buchungstransaktion (zum

[5] Aus diesem Grund wird die Lastschrift auch *rückläufige Überweisung* genannt

Zeitpunkt des nächsten Buchungsschnitts bei der Bank) eine ausreichende Deckung des Girokontos des Zahlungssenders, so wird der Zahlungssender von der Bank benachrichtigt, für die nötige Deckung seines Kontos zu sorgen. Gelingt ihm dieses nicht, so gibt die Bank die Lastschrift zurück und storniert die Gutschrift.

Das Einzugsermächtigungsverfahren beinhaltet die Möglichkeit, einen Zahlungsvorgang rückgängig zu machen. Eine entsprechende Lastschrift kann sowohl vom einlösenden Kreditinstitut aufgrund von mangelnder Deckung des Girokontos des Zahlungssenders zurückgegeben werden, als auch vom Zahlungssender innerhalb eines rechtlich definierten Zeitrahmens widerrufen werden durch Vorgang des *Widerspruchs*.

Das Zahlungsrisiko trägt bei Widerruf des gutgeschriebenen Betrages seitens des Zahlungssenders die Bank.

Kapitel 4

Kommunikation

Allgemein ausgedrückt ist Kommunikation die „Verständigung durch die Verwendung von Zeichen und Sprache.“([DUDEN, 1970]). Im Zusammenhang mit einer kooperativen Handlung eines Geldtransfers bzw. Zahlungsvorgangs zwischen zwei Personen (Zahlungssender und Zahlungsempfänger) kommen weitere wichtige Aspekte hinzu, die Gegenstand dieses Kapitels sind.
Die Situationen eines Zahlungsvorgangs zwischen zwei sich gegenüberstehenden Personen besitzt Eigenschaften, die ebenso für einen Zahlungsvorgang, vermittelt durch ein elektronisches System, z.B. in einer verteilten Computer-Netzwerk-Umgebung, gegeben sein müssen.

Wenn ein elektronisches System[1] die Vermittlung eines derartigen *Handelsvorgangs* übernimmt, so verläuft die Kommunikation in einem durch das System in Form von System- und Datenstrukturen definierten Funktionsumfang mit dem Ziel eines Geldtransfers (bzw. der Durchführung einer Zahlung). Nachrichten werden zwischen den Beteiligten auf der Basis der Einhaltung von Vereinbarungen über Nachrichtenformate und Regeln des Kommunikations-Verfahrens, den sogenannten *Protokollen*, ausgetauscht.

Welches sind die wesentlichen im elektronischen Medium zu simulierenden Eigenschaften einer Kommunikation zwischen zwei sich gegenüberstehenden Personen?

Authentizität einer Person Die beiden beteiligten Kommunikationspartner müssen sich jeweils sicher sein, daß der Gegenüber derjenige ist, für den er sich ausgibt. Eine Person muß anhand von Merkmalen, die nur dieser einen Person eigen sind, in einem System zuverlässig identifizierbar, d.h. von allen anderen unterscheidbar sein. Die eindeutige Identifizierung einer Person kann anhand des Wissens um ein Geheimnis, welches nur diese eine Person hat, oder

[1] als Zusammenstellung von Komponenten, die in ihrer Gesamtheit einen bestimmten Dienst leisten

anhand eines Gegenstandes, den die Person als einzige besitzt, erfolgen.

Charakteristische biologische Eigenschaften einer Person wie Gesichtszug, Fingerabdruck oder Stimme, die zur alltäglichen Identifizierung zwischen einander gegenüberstehenden Personen benutzt werden, sind weniger gut geeignet in einem verteilten elektronischen System aufgrund der Komplexität der Aufgabenstellung. Wesentlich einfacher zu realisieren sind *kryptographische Verfahren.*

Die im folgenden beschriebenen kryptographischen Methoden zur Personen-Authentifizierung, die bei den betrachteten Zahlungssystemen zum Einsatz kommen, beruhen auf geheimem Wissen und zum Teil zusätzlich auf dem Besitz eines physikalischen Gegenstandes in Gestalt einer Plastikkarte mit einem Mikroprozessor, der das Geheimnis sicher speichern und zusätzlich eigene Verarbeitungsschritte durchführen kann.

In der Situation, in der sich *eine Person gegenüber einem System* als rechtmäßiger Benutzer identifizieren muß, ist die am häufigsten angewandte Methode die der Passwort-Abfrage. Das System vergleicht die Eingabe einer Person mit einer nur für das System einsehbaren Referenzliste gültiger Name-Passwort-Relationen. Alphabet und Wortlänge sind dabei so gewählt, daß die Wahrscheinlichkeit des Erratens eines Passworts seitens eines unautorisierten Dritten sehr gering ist. Die Passwort-Methode birgt das Sicherheitsrisiko, daß das Geheimnis (das Passwort) bei jedem Autorisierungsvorgang zwischen den beiden beteiligten Personen kommuniziert (z.B. eingetippt) werden muß[2]. Jemand der den Kommunikations-Kanal abhört und in den Besitz des (mitunter verschlüsselten) Passworts gelangt, kann die erhaltene Nachricht selbst erneut versenden, um eine falsche Identität vorzutäuschen.

Die Challenge-and-Response Methode, die beim später beschriebenen Geld-Karten-System zur gegenseitigen Authentifizierung von Karte und Terminal benutzt wird, umgeht dieses Risiko, in dem bei jedem Authentifizierungsvorgang eine Zufallszahl von der einen Person geschickt wird, diese von der anderen Person mit Hilfe des gemeinsamen Geheimnisses verschlüsselt wird und als Schlüsseltext zurückgesendet zum Beweis dient, daß die andere Person das Wissen um den (gemeinsamen) geheimen Schlüssel besitzt.
Mechanismen der Authentifizierung können demnach eingeteilt werden in solche, bei denen die eine Seite die Identität der anderen Seite anhand des übermittelten Geheimnisses verifiziert und solche, bei denen hierzu das Geheimnis nicht kommuniziert werden braucht.

[2] falls nicht die Methode der *Einmal-Passworte* verwendet wird

Authentizität und Integrität einer Nachricht In [WELSH, 1991, S. 257] wird die Aufgabenstellung des Beweises der Echtheit einer Nachricht als *Authentifizierungproblem* bezeichnet. Es muß sowohl der Ursprung einer Nachricht zweifelsfrei nachweisbar sein als auch eine Veränderung an einer Nachricht erkennbar sein. Sowohl Sender als auch Empfänger besitzen hierzu ein nur ihnen beiden bekanntes Geheimnis. Der Sender authentisiert die zu verschickende Nachricht, indem er mit Hilfe des Geheimnisses erzeugte Information der Nachricht hinzufügt und so das Geheimnis mit dem Dokument verbindet. Der Empfänger kann mit Hilfe eines öffentlichen Algorithmus zusammen mit dem ihm bekannten Geheimnis überprüfen, ob die zusätzliche Information unter der Nachricht mit dem selber berechneten Wert übereinstimmt. Eine Übereinstimmung beweist gleichzeitig dem Empfänger die Echtheit der Nachricht als auch die Integrität der erhaltenen Nachricht.

Als ergänzende Anforderung wird in [WELSH, 1991, S. 257] das *Signaturproblem* genannt, bei dem die Beweisbarkeit des Ursprungs einer Nachricht gegenüber einem außenstehenden Dritten möglich sein muß. Wenn zwei Personen bei ihrer Kommunikation die gegenseitige Nachrichten-Authentifizierung mittels eines symmetrischen Verfahrens (beide haben das Wissen um *ein* Geheimnis) durchführen, sind die Nachrichten dieser beiden Personen ihrer Herkunft nach nicht unterscheidbar.

Eine *digitale Signatur* ermöglicht demgegenüber den eindeutigen Nachweis des Ursprungs einer Nachricht. Eine Person A ergänzt mit Hilfe eines nur ihr bekannten geheimen Schlüssels die zu verschickende Nachricht um Information und 'signiert' sie so. Jede andere Person im System kann nun die Authentizität der Nachricht anhand dieser Information überprüfen. Der Empfänger einer Nachricht benötigt zur Verifikation kein Geheimnis, er kann den Nachweis allein anhand von öffentlich verfügbarer Information führen.
Voraussetzung ist, daß niemand sonst die (eindeutige) Signatur fälschen bzw. generieren kann. Weder ein mithöhrender Dritter noch der Empfänger darf mit Hilfe der in einer Nachricht enthaltenen Information (der Klartext zusammen mit der dazu gehörenden Signatur) die Identität des Senders vortäuschen können.

Dies entspricht den beiden wesentlichen Eigenschaften einer herkömmlichen *handschriftlichen* Unterschrift, der *Echtheits-* und der *Identitätseigenschaft*[3]. Zum einen muß ein enger Zusammenhang zwischen Dokument und Unterschrift bestehen, das Dokument muß wirklich vom Unterschreibenden stammen, zum anderen ist es eine *persönliche* Unterschrift, die nur von einem einzigen Menschen ausgestellt werden kann.

In der praktischen Anwendung sind diese Forderungen erfüllt bei einem *asymmetrischen Verschlüsselungsverfahren* (siehe Abschnitt 4.1.2), bei dem die beiden einer Person zugeordneten Schlüssel (das *Schlüsselpaar*) für Ver-

[3] vergl. hierzu [BEUTELSPACHER *et al.*, 1995, S. 16]

schlüsselungs- und Entschlüsselungsfunktion vertauschbar sind.

Vertraulichkeit Als weitere Eigenschaft muß die Vertraulichkeit der Datenübermittlung bei der Kommunikation über einen unsicheren Kanal wie ein offenes Netzwerk gegeben sein. Niemand sonst außer den an der Kommunikation Beteiligten darf die Möglichkeit des Mithörens bzw. Mitlesens von Information haben (und z.B. in den Besitz des Wissens um eine Kreditkartennummer kommen). Um den Inhalt einer Nachricht zu verheimlichen[4] werden in der Praxis bei im Einsatz befindlichen elektronischen Zahlungssystemen die beiden in Abschnitt 4.1 beschriebenen Verschlüsselungsprinzipien verwendet. Der Sender verschlüsselt vor dem Abschicken seine Nachricht und sendet anstatt des Klartextes den Schlüsseltext, der auf der Seite des Empfängers entschlüsselt wird, um den Inhalt der Nachricht sichtbar zu machen.

Anonymität Schließlich kann noch die Eigenschaft der Anonymität als Eigenschaft eines Zahlungsvorgangs zwischen zwei sich gegenüberstehenden Personen genannt werden. Es kann die Forderung gestellt werden, daß der Zahlungsempfänger zum einen nicht direkt die Identität des Zahlungssenders erfährt und zum anderen mit Erhalt des benutzten Zahlungsmittels keine Informationen bekommt, die auf die Identität des Zahlungssenders schließen lassen. Gerade physikalische Münzen erfüllen diese zweite Forderung, da keinerlei Registrierung und somit Nachvollziehbarkeit von Zahlungsvorgängen möglich ist. Die Anonymität des Zahlungssenders ist durch die Eigenschaft des Zahlungsmittels gewährleistet.

Allerdings ist hier ein Widerspruch zur oben genannten Forderung der Authentizität von Personen gegeben. Falls sich beide in ausschließlich elektronischer Verbindung stehende Kommunikations-Partner sicher sein wollen, daß sie mit der 'richtigen' Person kommunizieren, ist eine Realisierung von Anonymität nicht möglich.

4.1 Kryptographie

Das universelle Werkzeug für die Realisierung der oben erwähnten Eigenschaften in einem elektronischen Medium ist die Kryptographie. Es existieren zwei grundlegend verschiedene Prinzipien der Verschlüsselung von Nachrichten.

[4]Eine andere Methode zur Wahrung der Vertraulichkeit wäre das Verheimlichen der Existenz einer Nachricht bzw. des gesamten Kommunikations-Kanals.

4.1.1 Symmetrische Verschlüsselung

Bei einem symmetrischen Verschlüsselungsverfahren vereinbaren Sender und Empfänger vor der eigentlichen Datenübermittlung einen nur ihnen beiden bekannten Schlüssel. Der Sender verschlüsselt die Nachricht mit Hilfe des Schlüssels und einem öffentlich zugänglichem Algorithmus, übermittelt den Schlüsseltext dem Empfänger und dieser kann als einziger mit dem Wissen um den geheimen Schüssel die Nachricht entschlüsseln und so die beinhalteten Informationen sichtbar machen. Auf beiden Seiten wird dieselbe Prozedur mit denselben Parametern ausgeführt.

Problematisch ist hierbei das Austauschen des geheimen Schlüssels vor dem eigentlichen Nachrichtenaustausch. Außerdem muß es jeweils zwischen zwei Personen (Sender und Empfänger) einen geheimen Schlüssel geben, den niemand sonst kennen darf. Somit wächst die Anzahl der Schlüssel quadratisch zur Anzahl beteiligter Personen im System. Ein Schlüsselmanagment für ein großes Systems mit vielen Beteiligten ist schwierig zu realisieren.

4.1.2 Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung besitzt jede Person ein einmaliges Schlüsselpaar bestehend aus öffentlichem und geheimem Schlüssel. Wichtige Eigenschaft ist, daß aus dem einen nicht auf den anderen geschlossen werden kann. Vor allem ist wichtig, daß der geheime nicht aus dem öffentlichen ableitbar ist. Der Ablauf einer gesicherten Datenübermittlung beginnt damit, daß der Sender sich den frei zugänglichen öffentlichen Schlüssel des Empfängers besorgt. Mit diesem verschlüsselt er mit ebenfalls öffentlich zugänglichem Verschlüsselungs-Algorithmus die Nachricht, schickt den resultierenden Schlüsseltext dem Empfänger zu und dieser kann als einziger mit seinem zugehörigen geheimen Schlüssel die Nachricht entschlüsseln und so die im Schlüsseltext enthaltene Information sichtbar machen. Es finden pro Übermittlungsvorgang nur die beiden Schlüssel des Empfänger-Schlüsselpaares Verwendung. Im Gegensatz zur symmetrischen Verschlüsselung, bei dem jedem *Kanal* zwischen zwei Beteiligten ein Schlüssel zugeordnet ist, gibt es hierbei pro beteiligter Person ein Schlüsselpaar.

Ein geheimer Schlüssel wird im Gegensatz zur symmetrischen Methode in diesem System zu keinem Zeitpunkt auf potentiell abhörunsicherem Wege kommuniziert. Es muß allerdings sichergestellt sein, daß alle öffentlichen, z.B. bei einer zentral zugänglicher Instanz hinterlegten Schlüssel authentisch sind, d.h. tatsächlich derjenigen Personen *gehören*, der sie zugeordnet sind. Dieser Gesichtspunkt ist Inhalt des nächsten Abschnitts.

4.2 Zertifikate

Die große Problematik bei der Personen-Identifizierung mit Hilfe elektronischer Schlüssel und asymmetrischem Verschlüsselungsverfahren ist die vertrauenswürdige Zuordnung von Schlüsselpaaren zu Personen wie auch die vertrauenswürdige Verbreitung der Informationen über öffentliche Schlüssel mit den dazugehörigen Personendaten. In einem kleinen Personenkreis kann der notwendige Informationsaustausch in vertrauenswürdiger Umgebung untereinander stattfinden. Bei großer Personenzahl ist eine zentrale Instanz eine Lösung des Problems. Diese Instanz, eine sogenannte *Certification Authority (CA)*[5], vergibt an Personen eindeutige Schlüsselpaare und sorgt für die notwendige freie Zugänglichkeit der öffentlichen Informationen.

In der Praxis werden zu diesem Zweck *Zertifikate* von der *CA* ausgegeben. Ein Zertifikat enthält (mindestens) den Namen der Person und den öffentlichen Schlüssel des zugeordneten Schlüsselpaares. Diese Informationen über eine Person werden zusammen mit entsprechendem geheimen Schlüssel der *CA* signiert und so die Beweisbarkeit erbracht, daß ein bestimmter öffentlicher Schlüssel zu einer bestimmten Person gehört[6].

4.3 Secure Socket Layer (SSL)

Als Beispiel eines kompletten Paketes, das die wichtigsten Anforderungen an eine Kommunikation über ein offenes Netzwerk erfüllt, sei an dieser Stelle das von NETSCAPE COMMUNICATIONS CORPORATION für das Internet konzipierte Protokoll *Secure Socket Layer (SSL)* angeführt. *SSL* ist ein universell einsetzbares, kryptographisches Netzwerk-Protokoll. Es umfaßt die gegenseitige Authentifizierung der beiden beteiligten Kommunikationspartner, Integrität und Vertaulichkeit der Datenübertragung sowie Beweisbarkeit des Ursprungs einer Nachricht (die Unleugbarkeit des Ursprungs einer Nachricht)[7]. Unabhängig von der Anwendungs-Software wird transparent auf der Ebene der Transport-Schicht[8] eine sogenannte *Socket-Library* implementiert, die die gesamte Kommunikation des bidirektionalen Kanals verschlüsselt. *SSL* kann somit als Erweiterung der Basis-Internet-Technologien um Eigenschaften, die eine *sichere* Kommunikation zwischen zwei Kommunikationspartnern gewährleisten, verstanden werden.

[5] in Verbindung mit der Schlüsselgenerierung und -ausgabe auch *Trustcenter* genannt

[6] In [GARFINKEL U. SPAFFORD, 1997, Kap. 6] wird allerdings argumentiert, daß Zertifikate in der realen Welt zu wenig Informationen über eine Person enthalten und daher keine ausreichende Zuordbarkeit zur Person zulassen. Die Maßnahme, aus diesem Grund umfassendere Informationen in Zertifikate aufzunehmen, wird allerdings durch Forderungen nach Anonymität und Privatsphäre verhindert.

[7] vergl. [GARFINKEL U. SPAFFORD, 1997, S. 234f]

[8] gemäß dem TCP/IP-Schichtenmodell

Für die einzelnen zu realisierenden Eigenschaften und Aufgaben werden unterschiedliche Verschlüsselungs-Verfahren mit jeweils verschiedenen Schlüsseln eingesetzt. Vertraulichkeit der Datenübermittlung wird durch die Verwendung von verschiedenen kryptographischen Algorithmen realisiert, Datenintegrität durch die Verwendung von verschiedenen Hash-Funktionen, gegenseitige Authentifizierung mittels Public-Key-Zertifikaten und Beweisbarkeit des Ursprungs einer Nachricht durch digitale Signaturen.

Am Anfang eines Verbindungsaufbaus mit *SSL* werden zwischen den zwei Kommunikationspartnern die bei der anstehenden Kommunikations-Sitzung zum Einsatz kommenden Verschlüsselungs-Verfahren und die jeweiligen Schlüssellängen vereinbart.

4.4 Secure Electronic Transactions (SET)

Das *SET*-System[9] ist eine Internet-Lösung für die jeweils durch Verschlüsselungs-Methoden realisierte Sicherung der Datenübertragung, die Anonymisierung der Zahlungsdaten gegenüber dem Zahlungsempfänger und gegenseitige Authentifizierung der beiden beteiligten Kommunikationspartner. *SET* betrifft nicht die Funktion eines Zahlungsinstrumentes, nur Aspekte der Kommunikation in einem offenen Netzwerk zum Zweck einer Kreditkarten-Zahlung. Der Zahlungsvorgang geschieht demnach nach dem Prinzip der in Abschnitt 7.2 veranschaulichten Kreditkarten-Zahlung. Analog sind die vertraglichen Vereinbarungen zwischen den beteiligten Parteien Voraussetzung für einen Zahlungsvorgang.

Das SET-System sichert einen bidirektionalen Kommunikations-Kanal für spezifische Informationen bei Kreditkarten-Zahlungen im Internet. Der Funktionsumfang von *SET* ist ein Paket von Diensten, die die sichere Übertragung der Zahlungsinformationen realisieren. Die vertrauliche Datenübertragung wird gewährleistet durch asymmetrische kryptographische Verfahren, gegenseitige Authentifizierung der beteiligten Parteien ist enthalten unter Verwendung von Digitalen Signaturen. Schließlich ist die Daten-Integrität bei der Übermittlung über das Internet gegeben.

SET benutzt zur Identitätsprüfung (Authentifizierung) aller an einem Zahlungsvorgang beteiligten Parteien (Zahlungsempfänger, Zahlungssender und Bank) Zertifikate, ausgestellt von einer zentralen Institution[10].

Das Prinzip der *Dual Signatures* wird verwendet, um einerseits vertrauliche

[9] siehe [SET, 1998]
[10] siehe hierzu Abschnitt 4.2

Informationen zwischen Kunde und Händler (Zahlungssender und Zahlungsempfänger) und andererseits zwischen Händler und Bank zu gewährleisten. Eine Nachricht vom Zahlungssender (zum Zweck des Kaufs einer vom Zahlungsempfänger angebotenen Ware oder Dienstleistung) besteht aus zwei Feldern. Das eine ist ausschließlich bestimmt für den Zahlungsempfänger (den Händler), das andere ausschließlich für die Bank. Hierzu sind die Felder jeweils verschlüsselt mit dem öffentlichen Schlüssel der entsprechenden Partei und somit nur jeweils für die eine Partei (den Adressaten) lesbar. So erfährt beispielsweise der Zahlungsempfänger nicht die Kreditkarten-Nummer des Zahlungssenders.

Das Verfahren eines Zahlungsvorgangs mittels *SET* umfaßt die im folgenden aufgeführten Verfahrensschritte[11]. Die Beschreibung benennt zur Veranschaulichung die einzelnen Schritte als von der jeweiligen Partei einzeln ausgeführte Aktionen, obwohl der Vorgang ab dem zweiten Schritt tatsächlich als eine streng sequentielle Prozeß von den auf beiden Seiten vorhandenen Software-Komponenten[12] des Systems automatisch ausgeführt wird. Da es sich bei einem Zahlungsvorgang mit dem SET-System in jedem Fall um einen Handel und nicht bloß um die Durchführung einer Wertübertragung zwischen zwei Privatpersonen handelt, werden die Begriffe *Kunde* und *Händler* anstatt *Zahlungssender* und *Zahlungsempfänger* benutzt.

Der Vorgang beginnt, in dem der Kunde den Händler informiert, daß er an einem Kreditkarten-Kauf eines seiner Angebote interessiert ist.

1. Daraufhin generiert der Händler eine Rechnung und schickt sie an den Kunden. (Dieser Schritt ist innerhalb des Standards nicht näher spezifiziert.)

2. Der Kunde wählt eine seiner Kreditkarten für den Zahlungsvorgang aus und initiiert die Zahlung durch eine Anfrage an den Händler um Preisgabe seines öffentlichen Schlüssels und den des Acquirer-Gateways (beide Schlüssel sind notwendige Voraussetzung für die weiteren Schritte). Diese Anfrage enthält Informationen über den beim Zahlungsvorgang verwendeten Kreditkarten-Typ des Kunden.

3. Der Händler schickt als Antwort eine Nachricht mit dem Inhalt: eindeutige Transaktions-ID, Zertifikat des öffentlichen Schlüssels des Händlers und Zertifikat des öffentlichen Schlüssels des Gateway. (Die Zertifikate sind jeweils authentisierte Versionen der öffentlichen Schlüssel).

4. Der Kunde überprüft anhand der Zertifikate die Authentizität von Händler und Acquirer.

[11] vergleiche [Lamond, 1996]

[12] Sowohl Zahlungssender als auch Zahlungsempfänger benötigen spezielle Software.

5. Der Kunde generiert separat zwei Pakete, die er zusammen an den Händler schickt,

   - zum einen das *Order Information Packet (OI)* und
   - zum anderen das *Purchase Instructions Packet (PI)*,

   jeweils verschlüsselt mit dem öffentlichen Schlüssel des Adressaten (das *PI* wird mit dem öffentlichem Schlüssel des Gateways und das *OI* mit dem öffentlichem Schlüssel des Händlers verschlüsselt).
   Das *OI*, das allein für den Händler bestimmt ist, enthält eine Transaktions-ID, den Kreditkarten-Typ und das Transaktions-Datum.
   Das *PI* ist allein für den Acquirer-Gateway bestimmt zur Abwicklung der Kreditkarten-Zahlung und wird dementsprechend vom Händler unverändert (und unlesbar) weitergeleitet. Die enthaltenen Informationen sind: Kreditkartennummer des Kunden mit Verfallsdatum, vereinbarter Zahlbetrag und eine Beschreibung der Gegenleistung des Händlers.

6. Der Kunde schickt das *PI* und das *OI* zusammen zum Händler.

7. Es folgt eine Integritätsprüfung des gesamten Paketes durch den Händler.

8. Der Händler schickt eine (verschlüsselte) Authorisierungs-Anfrage für die Kreditkartenzahlung an den Acquirer-Gateway, die Information um Authorisierungs-Anfrage, *PI*-Paket des Kunden und Händler-Zertifikat mit enthaltenem öffentlichem Schlüssel beinhaltet.

9. Der Gateway entschlüsselt mit Hilfe seines geheimen Schlüssels die Nachricht und prüft, ob die eindeutige Transaktionskennung in der Authorisierung mit derjenigen im *PI*-Paket des Kunden übereinstimmt und ob Daten-Integrität des *PI*-Paketes gegeben ist.

10. Der Gateway schickt die Anfrage auf Authorisierung der Zahlung an die entsprechende Kreditkarten-Organisation (des Kunden) weiter[13].

11. Die Kreditkarten-Organisation antwortet dem Gateway mit Informationen zur Authorisierung der Zahlung.

12. Der Gateway generiert und verschickt eine verschlüsselte, authentifizierte Nachricht an den Händler, die Information über die Authorisierung der Zahlung enthält.

13. Der Händler entschlüsselt die Nachricht und speichert sie für die spätere Abrechnung der Umsätze.

[13] Diese Datenübertragung erfolgt über Banken-Infrastruktur, nicht über den Internet-Weg.

14. Es wird außerdem eine Bestätigung an den Kunden geschickt („Zahlung ist erfolgt, die Gegenleistung wird geliefert.“).

Im weiteren Verlauf des an dieser Stelle noch nicht abgeschlossenen Zahlungsvorgangs generiert der Händler zu einem nicht definierten Zeitpunkt einen Rechnungsabschluß über alle bei ihm gespeicherten Einzel-Transaktions-Daten und schickt sie gesammelt an den Acquirer-Gateway zur Gutschrift auf dem beim Aquirer geführten Händler-Girokonto.

Die nun folgenden Prozesse zur Vervollständigung des Zahlungsvorgangs entsprechen der in Abschnitt 7.2 behandelten herkömmlichen Kreditkarten-Zahlung.

Kapitel 5

Kommunikation im Internet

In diesem Kapitel wird als Grundlage des nächsten Kapitels der Frage nachgegangen, ob die geforderten generellen Eigenschaften einer Kommunikation im Hinblick auf eine Geldtransfer-Situation zwischen zwei beteiligten Kommunikations-Partnern, wie sie am Anfang des vorangegangenen Kapitel 4 beschrieben wurden, durch die grundlegenden Internet-Technologien erfüllt werden.

Kann sich eine Person sicher sein, daß sie mit demjenigen kommuniziert, mit dem sie glaubt zu kommunizieren und ist Vertraulichkeit und Integrität der Daten-Übertragung gewährleistet?

Hierzu wird im folgenden das Prinzip der Kommunikation im Internet zwischen vernetzten Rechnern basierend auf dem status quo der eingesetzten Technologien erläutert.

Das Ziel des Benennens einiger konkreter Sicherheitsrisiken in den einzelnen Abschnitten ist nicht die Wiedergabe des aktuellen Standes der Spezifikationen oder Implementierungen, sondern das Aufzeigen prinzipieller Eigenschaften und Problematiken im Zusammenhang mit dem Thema *Kommunikation im Internet*. Bezugnehmend auf Quellen, die zum Teil schon einige Jahre alt sind, können diese 'Sicherheitslöcher' inzwischen schon behoben sein[1]. Dieser Punkt wird im Rahmen der Arbeit nicht überprüft.

5.1 Internet-Protokolle

Die *TCP/IP Internet Protokol Suite (TCP/IP)*[2] ist als Protokoll-Schichten-Modell und -Implementierung die Basis der Kommunikation zwischen vernetzten Rechnern im *Internet*. Aufsetzend auf der physikalischen Netzwerk-

[1]dieses ist z.B. bei der *DNS-Server-Software* der Fall, siehe hierzu die neuste Version des unter *Unix* meistgenutzten Paketes *BIND* unter der URL `http://www.isc.org/bind.html`

[2]vergl. hierzu [Holtkamp, 1998] und [?]

Schicht mit verschiedenen eigenen Protokollen und unabhängigen Technologien (wie z.B. ETHERNET oder X.25) besteht *TCP/IP* aus drei hierarchisch aufgebauten logischen Protokoll-Ebenen, der Internet-, Transport- und Anwendungsschicht. Im Rahmen der folgenden Betrachtung werden Internet- und Transport-Schicht im Vordergrund stehen, sie enhalten die grundlegenden *Internet-Kommunikations-Technologien* in Gestalt der einzelnen Protokolle *IP*, *ICMP*, *TCP* und *UDP*.

Die Grundlage der Kommunuikation im Internet ist die Paketvermittelung auf Basis numerischer 32Bit-Rechner-Nummern, den *IP-Nummern*. Die Übertragungseinheit ist das einheitliche *IP-Datagramm*. Weder der Sender noch der Empfänger einer Nachricht kann den Verlust eines IP-Datagramms detektieren, es gibt keine Garantie für die Zustellung eines Paketes. Annahme und Praxis ist die gute statistische Chance, daß ein Paket dem Zielrechner und somit dem Empfänger zugestellt wird. Praktikabel ist diese Idee auf der Grundlage der erwähnten hierarchisch gestaffelten Kommunikations-Protokolle. Die Unzuverlässigkeit der unteren Internet-Schicht in Gestalt von *IP*[3] wird (falls notwendig) ausgeglichen durch das zuverlässige, darauf aufsetzende Transport-Protokoll der nächsthöheren Schicht in Gestalt von *TCP*[4]. Dieses benutzt das unzuverlässige Prinzip der unteren Schicht, bietet aber insgesamt den übergeordneten Schichten einen zuverlässigen Transport-Dienst.

Zur Realisierung der Paket-vermittelten Kommunikation wird von jedem Protokoll die zu verschickende Information in einheitliche Pakete gekapselt und jedes einzelne Paket mit angehängter *Header*-Information versehen.

5.1.1 IP

Das Internet-Protokoll (*IP*) ist das universelle und einzige Protokoll, das für die Paketzustellung im Internet sorgt, das sogenannte *Packet Routing*[5]. Die Paketzustellung geschieht nach dem Prinzip des *packet switching* in einer hierarchisch aufgebauten Adress-Struktur der vernetzten Systeme. Der Weg eines Paketes führt meistens über mehrere Netzknoten bzw. -rechner, die jeweils nach *'bestem Wissen'* den nächsten Knoten des Weges auswählen und das Paket dorthin weiterschicken. Auf diese Art gelangt schließlich das Paket vom Absender zum Zielrechner.
IP spezifiziert, wie ankommende Pakete aus der physikalischen Schicht an die darüberliegende Transport-Schicht weitergereicht und andersherum in entgegengesetzter Richtung zu verschickende Pakete aus der Transport-Schicht versehen mit Kontrollinformationen an die physikalische Schicht übergeben wer-

[3] siehe Abschnitt 5.1.1
[4] siehe Abschnitt 5.1.3
[5] vergl. [SCHUBA, 1993, S. 7]

den. Die Aufgabe von IP ist die Adressierung der zu verschickenden Pakete mit den eindeutigen 32Bit-IP-Nummern, die Fragmentierung bzw. Zusammensetzung von Paketen und die Behandlung von Timeouts[6].

IP ist als unzuverlässiges Protokoll zu bezeichnen, da keine Bestätigung von am Zielort eingetroffenen Paketen zur Detektion von Übertragungsfehlern beinhaltet ist. Der Verlust eines IP-Paketes kann nicht erkannt werden. Außerdem wird weder die sequentielle Reihenfolge der Pakete beachtet noch eine Prüfsumme zum Zweck der Daten-Integrität berechnet und verglichen.

Eine zusätzliche Integritätsprüfung zur Sicherung der Datenübermittlung wird auf IP-Ebene nicht umgesetzt. Das im IP-Header enthaltene Prüfsummenfeld bezieht sich allein auf die Header-Daten, nicht auf die Nutzdaten eines Paketes[7].
Pakete können auf dem Weg zum Empfänger abgefangen werden ohne Möglichkeit, den Verlust zu detektieren. Außerdem kann ein Paket kopiert oder verändert werden ohne daß die Möglichkeit zur Detektion gegeben ist. Die nach Veränderung eines Paketinhalts falsche Prüfsumme der IP-Header-Daten kann hierzu leicht entsprechend dem Inhalt des veränderten Paketes neu berechnet und ersetzt werden.

Das Manko der unzuverlässigen Zustellung der Übertragungseinheiten wird, wie oben erwähnt, aufgefangen durch das Prinzip der Protokoll-Hierarchie. Die Internet-Schicht (in Gestalt von *IP*) mit darüberliegender Transportschicht (*TCP*) bilden zusammen einen zuverlässigen, bidirektionalen Kommunikationskanal zwischen zwei vernetzten Rechnern.

Als Beispiel einer vorhandenen Schwachstelle im Zusammenhang mit der allein auf Grundlage von Rechner-IP-Nummern realisierten Authentifizierung sei die in einem lokalen Netzwerk bestehende Angriffsmöglichkeit der *Adress-Maskierung* erwähnt (vergl. [Bellovin, 1989]).
Im Fall des weit verbreiteten *Network File Systems (NFS)* der Firma Sun basiert die Authentifizierung von anfragenden Hosts[8] nur auf der Rechner-IP-Adresse. Ist ein Host im lokalen Netz abgeschaltet bzw. nicht erreichbar, so kann jemand einem zweiten lokalen Host dessen IP-Adresse zuweisen. Dieser Host erbt automatisch alle Befugnisse des inaktiven Rechners in Bezug auf den Zugriff auf exportierte Teile von Dateisystemen lokaler Rechner.

[6] Der IP-Header enthält das Feld *Time to live*, nach dessen Wert der Zustellungsversuch eines Paketes beendet wird und der Absender über den nicht erfolgreichen Versuch informiert wird.

[7] siehe [Holtkamp, 1998]

[8] Ein Host ist ein vernetzter Rechner.

5.1.2 ICMP

Das *Internet Control Message Protocol (ICMP)* ist zur Kontrolle der Paketzustellung im Internet zuständig. Es umfaßt die Fehlerbehandlung und verschiedene Kontrollfunktionen in Bezug auf das oben genannte *IP*-Protokoll. *ICMP* beinhaltet

- Meldungen über Netzwerkfehler,
- Meldungen über Netzwerküberlastung,
- Maßnahmen zur Fehlerbehandlung und
- Meldungen über Timeouts von IP-Paketen.

5.1.3 TCP

Das *Transmission Control Protocol (TCP)* ist eines der beiden Protokolle der *TCP/IP*-Transport-Schicht, deren Dienste direkt von den verschiedenen Netzwerk-Applikationen benutzt werden. Es ist im Gegensatz zum zweiten Protokoll dieser Schicht (*UDP*, s.u.) verbindungsorientiert und zuverlässig im Hinblick auf eine fehlerfreie und gesicherte Zustellung von Paketen. Der Mechanismus der zuverlässigen Kommunikation zwischen zwei Rechnern (Client *C* und Server *S*) mittels *TCP* beginnt mit einem Verbindungsaufbau nach folgendem Verfahren, dem sogenannten *three-way handshake*[9]:

- C sendet S ein Paket mit *initialer Sequenznummer (cISN)* im Header, um den Wunsch nach einem Verbindungsaufbau zu signalisieren.
- S antwortet daraufhin mit einer Bestätigung der Anfrage (*cISN+1*) und einer eigenen ISN (*sISN*).
- Die Verbindung ist aufgebaut, wenn C diese Nachricht von S mit einer Nachricht C→S {sISN+1} bestätigt.

Die hergestellte Verbindung ist durch das Quadrupel (Client-IP-Nummer, Client-Port-Nummer, Server-IP-Nummer, Server-Port-Nummer) zusammen mit der Information über das verwendete Protokoll eindeutig definiert. Der TCP-Header enthält als Kontrollinformation die beiden Port-Nummern, die IP-Nummern der beiden beteiligten Rechner werden von *IP*[10] spezifiziert.

Die weitere, zuverlässige Kommunikation zwischen den beiden Kommunikationspartnern erfolgt nach dem Prinzip des *Positive Acknowledgement with*

[9]vergleiche [HOLTKAMP, 1998]
[10]siehe 5.1.1

Re-Transmission (PAR). Der Sender wiederholt das Verschicken eines Paketes solange, bis vom Empfänger der Erhalt des anhand einer Prüfsumme auf Daten-Integrität hin geprüften Paketes bestätigt wird. Jedes einzelne Paket wird mit einer Sequenznummer versehen, die eine Einordnung von Paketen in den Kommunikationsvorgang ermöglicht.

Eine Sequenznummer ist im TCP/IP-Standard gegen das *Erraten* seitens eines Dritten, der am Kanal lauscht, nicht abgesichert. Ein Zähler wird einfach in bestimmter, konstanter Frequenz inkrementiert. Der einzige Zweck der Sequenznummern ist der des Zuordnungskriteriums für mehrere parallel laufende Kommunikations-Kanäle. Zwei Verbindungen müssen unterscheidbar sein zur Verhinderung von Seiteneffekten.
Eine Sequenznummer ist aufgrund des einfachen Generierungsprinzips leicht annäherungsweise vorausberechenbar. Vereinfacht formuliert können zwei Antworten eines Zielrechners auf ein Initialpaket und ein weiteres Paket ausgewertet werden, um den ungefähren aktuellen Sequenznummern-Stand und die ungefähre Frequenz der Inkrementierung herauszufinden. Ein Angreifer schickt im weiteren Verlauf des Angriffs mehrere Pakete mit gefälschter IP-Absender-Adresse und mit jeweils variierenden, um die Vorausberechnung gestreuten Sequenznummern und hat eine gute Chance, daß eines der Pakete vom Zielrechner des Angriffs für echt befunden und akzeptiert wird.
Eine konkretes Risiko beschreibt die folgende Situation aus [Bellovin, 1989]:

- Host S vertraut generell Host C in einem lokalen Netz, von außen (*remote*) bestimmte Befehle ohne vorherige Identitätsprüfung des Benutzers auszuführen.
- Es besteht eine TCP-Verbindung zwischen Host S und Host C.
- Ein Angreifer an einem Rechner mit Verbindung zum Internet konstruiert ein IP-Paket mit Absender-Adresse von Host C und *erratener* TCP-Sequenz-Nummer der Verbindung.
- Die Authentisierung erfolgt aufgrund richtiger IP-Absender-Adresse und der gültigen Sequenznummer und der im Paket enthaltene Befehl wird auf Rechner S ausgeführt.

5.1.4 UDP

Das *User Datagram Protocol (UDP)* ist das zweite Protokoll der *TCP/IP*-Transport-Schicht. Konzeptioniert zur schnellen, effizienten Übertragung von kleinen Datenmengen ist der Header eines UDP-Paketes mit nur wenigen Kontrollinformationen ausgestattet. *UDP* spezifiziert im Gegensatz zu *TCP* eine unzuverlässige, verbindungslose Kommunikation. Es gibt keine Bestätigungs-Information über am Ziel-Rechner angekommene Pakete. Falls der Anfragende keine Antwort auf sein abgeschicktes UDP-Paket erhält, wird die Anfrage nach einer gewissen Zeit erneut geschickt. Sequenznummern wie bei *TCP* gibt es nicht, die über *UDP* versendeten Nachrichten umfassen immer nur ein Paket. Der Inhalt eines UDP-Headers besteht aus

- Portnummer des Quellrechners,
- Portnummer des Zielrechners,
- Größe des gesamten Paketes und
- Prüfsumme[11].

5.2 Das Domain Name System (DNS)

Im Internet sind die einzelnen teilhabenden Rechner unabhängig von der darunterliegenden Netzwerk-Topologie mit eindeutigen alphanumerischen Namen eines baumartig strukturierten Namensraumes (siehe [SCHUBA, 1993, S. 12]) benannt.[12] Der gesamte Namensraum des Internets ist unterteilt in *Zonen*, für die jeweils verschiedene *Nameserver* die Umsetzung der logischen Namen in die IP-Nummern[13], die für die Kommunikation der vernetzten Rechner untereinander notwendig sind[14], bereitstellen. Das *DNS* als verteiltes, dezentrales Datenbank-System innerhalb des Internets hat hierfür zu jedem Rechnernamen neben anderen Informationen eine eindeutige 32Bit-Internet-Nummer gespeichert.

Das *DNS* spezifiziert die beiden möglichen Aktionen des *Lookups* und des *Zonentransfers*. Lookups sind (iterative oder rekursive) Anfragen von Clients an einen Nameserver zur Namensauflösung, die aus Effizienzgründen mittels eines einzelnen UDP-Paketes erfolgen. Auf die Zuverlässigkeit der Paketzustellung wird hierbei verzichtet, da eine Anfrage bei ausbleibender Antwort des Servers auf effizientere Weise nochmals verschickt wird anstatt eines komplexeren Verbindungsaufbaus mit *TCP*.
Ein Zonentransfer erfolgt von Zeit zu Zeit zum Abgleich der Datenbank-Einträge von zwei Nameservern untereinander. Zonentransfers werden mittels zuverlässigem *TCP* durchgeführt.

Die Problematik von *DNS* besteht darin, daß eine falsche Zuordnung von Name zu IP-Adresse eine Zuordnung zu einer falschen Rechner-Identität bedeutet. Falls jemand im World-wide-Web beispielsweise die Homepage von

[11] Dieser Feldeintrag ist optional.

[12] vergleiche zu diesem Abschnitt [SCHUBA, 1993] und [MRAZ U. WEIDNER, 1997]

[13] Das *DNS* bietet unter anderem ebenfalls den umgekehrten Dienst, die Auflösung von IP-Nummern in Rechner-Namen.

[14] siehe Abschnitt 5

einer *Bank XY* besuchen will und beim Verbindungsaufbau eine Zuordnung zu einer falschen IP-Adresse geschieht, landet seine Anfrage bei einem falschen Rechner. Im allgemeinen wird der Besucher an den zurückgesendeten Antwort-Daten (der HTML-Seite) erkennen, daß er falsch verbunden wurde. Falls jedoch ein böswilliger Dritter die falsche Zuordnung herbeigeführt hat und unbemerkt das Erscheinungsbild der BANK XY annimmt, kann er so die Identität der BANK XY vortäuschen.
Eine besonders trickreiche Variante des Vortäuschens einer falschen Identität läßt sich mit Hilfe der von Web-Browsern direkt ausgeführten *JavaScript*-Befehle erzielen, das sogenannte *Web-Spoofing*[15].

Implementierungen zum Generieren und Abschicken eines *UDP-Lookups*, sogenannte *Resolver*, benutzen als einziges Authentifizierungsmerkmal einer (zurückkommenden) DNS-Antwort eine 16Bit-Sequenznummer, die sogenannte *Query-ID*. Ursprünglich einziger Zweck dieser ID-Nummer ist die Zuordnung von Paketen zu möglicherweise mehreren parallel laufenden Anfragen. Der anfragende Resolver wählt hierzu eine Query-ID für das *Lookup*-Paket und ein daraufhin eintreffendes Antwort-Paket mit derselben Query-ID (am richtigen Port) wird als authentisch akzeptiert. Da die meisten Resolver für aufeinanderfolgende DNS-Anfragen einfach inkrementierte ID-Nummern wählen, ist das Herausfinden bzw. Erraten einer nächsten Query-ID und somit die Fälschung einer entsprechenden (vermeintlichen Nameserver-) Antwort möglich.

Eine konkretes Risiko des *DNS* ist der Mechanismus des *Cache pollution*[16]. Es beruht auf der Tatsache, daß einige Nameserver bei rekursiven Anfragen untereinander alle empfangenen Daten aufgrund von Performanz-Vorteilen ohne Überprüfung eine definierte Zeit lang im Speicher halten. Eine Authentifizierung zwischen Nameservern ist im aktuellen *DNS* nicht realisiert. Ein Angreifer kann versuchen, die Namensumsetzung eines bestimmten Namens zu beeinflussen, in dem er eine Anfrage mit dem aufzulösenden Namen an einen Nameserver, von dem er weiß, daß dieser Nameserver den Namen nicht selber auflösen kann, schickt. Der Nameserver sendet daraufhin eine rekursive Anfrage an andere Nameserver. Zu diesem Zeitpunkt sendet der Angreifer eine große Anzahl gefälschter DNS-Antworten, die die falsche Antwort-IP-Nummer beinhalten, an den ursprünglichen Nameserver. Wenn der Nameserver eine dieser gefälschten Antworten akzeptiert, speichert er die Zuordnung des Namens zur falschen Nummer für eine gewisse Zeit ab und alle in diesem Zeitraum ankommenden Anfragen bezüglich des Namens werden mit der falschen Nummer beantwortet.

---

[15] Für ausführliche Informationen zu diesem Thema siehe [FELTEN *et al.*, 1997].
Die Problematik in Verbindung mit der von allen gängigen Web-Browsern interpretierten, weit verbreiteten Sprache *JAVA* werden umfassend in [DEAN *et al.*, 1997] behandelt.

[16] siehe [SCHUBA, 1993, S. 42]

5.3 Zusammenfassung

Zusammenfassend läßt sich sagen, daß die in Kapitel 4 aufgezeigten Erfordernisse für die Simulation einer Zwei-Parteien-Kommunikation, in der sich die beiden Kommunikationpartner gegenüberstehen, mittels der grundlegenden Internet-Technologien nicht erfüllt werden. Die Authentizität von Nachrichten und Personen ist ebensowenig realisiert wie umfassende Daten-Integrität oder die Vertraulichkeit kommunizierter Informationen.
Diese Eigenschaften müssen explizit durch die auf dieser grundlegenden Kommunikations-Funktionalität des Internets aufsetzenden Anwendungs-Software realisiert werden.

Zur Sicherung der Kommunikation werden lediglich einfache mathematische Verfahren zur Prüfung auf Übertragungsfehler verwendet[17]. Es ist hiermit sichergestellt, daß auf Empfängerseite erkannt werden kann, ob in Folge eines Übertragungsfehlers der Inhalt eines Paketes verfälscht wurde. Die Prüfsummen dienen nicht der Authentifizierung von Nachrichten bzw. einzelnen Paketen, sondern lediglich der einfachen Integritäts-Prüfung. Die bei *TCP* im Header der Pakete verwendeten 'Seriennummern' sind ausschließliches Kriterium der Zuordnung für mehrere parallel laufende Verbindungen und erfüllen keine weitere Funktion im Hinblick auf die Kommunikation.

Vertraulichkeit der Datenübertragung ist in den beschriebenen Internet-Technologien nicht berücksichtigt; es werden weder Verfahren zur Verheimlichung der Übertragung noch zur Verheimlichung des Inhalts der Pakete angewendet.

Eine Authentifizierung von Personen ist mit den erläuterten Mechanismen nicht möglich, da die beschriebenen Protokolle allein die Kommunikation zwischen vernetzten Rechnern spezifizieren bzw. realisieren. Eine Zuordnung der eindeutig mittels IP-Nummern identifizierbaren Rechner des Netzwerks zu Personen ist nicht enthalten. Es gibt dementsprechend keine Authentifizierungs-Mechanismen für Personen. Wie bereits erwähnt, müssen die hierauf aufsetzenden Programme der Anwendungsschicht letztendlich dafür sorgen, daß eine der Anwendung genügende Realisierung einer Personen-Authentifizierung implementiert wird, ohne zu diesem Zweck zurückgreifen zu können auf Protokoll-Informationen der TCP/IP-Schichten.

Das Prinzip des *DNS* ist ein zusätzlicher Unsicherheitsfaktor in Bezug auf die Kommunikation zwischen zwei vernetzten Rechnern. Falls bei einer durch das *DNS* vermittelten Zuordnung der alphanumerischen Rechnernamen zu den IP-Rechnernummern ein Fehler auftritt, wird ein vom Benutzer ungewollter Verbindungsaufbau mit einem (falschen) Rechner auf der anderen Seite unternommen.

---

[17] „Der Algorithmus für die Bildung der Prüfsumme ist einfach: alle 16-Bit Wörter werden im 1er-Komplement addiert und die Summe ermittelt.“ [Holtkamp, 1998]

Kapitel 6

Zahlungssysteme für das Internet

In diesem Kapitel werden die beiden speziell für das Internet konzipierten Zahlungssysteme *eCash* und *CyberCoin* behandelt. Die Wahl der Darstellung dieser beiden Systeme wurde getroffen, da sie zum Zeitpunkt der Ausarbeitung die einzigen eigenständigen Internet-Zahlungssysteme in Deutschland darstellten. Beide Systeme werden in der Praxis von Geschäftsbanken angeboten. Einige andere Systeme, wie beispielsweise *MilliCent* und *NetCash*[1] konnten im Rahmen der Darstellung nicht sinnvoll eingebunden werden, da sie als theoretische Modelle[2] die Frage nach dem eigentlichen Geldtransfer offen lassen. Die Beschreibung eines vollständigen Zahlungsvorgangs war aus diesem Grund nicht möglich.

Ebenso wird auf die Darstellung von Systemen verzichtet, die allein die Realisierung eines anderen, herkömmlichen Systems, wie etwa die *Kreditkartenzahlung* in einer Netzwerk-Umgebung bilden. Dies ist bei den zwei neben *CyberCoin* im CyberCash-System enthaltenen Zahlungsverfahren der Fall.

Der Umstand, daß es sich sowohl bei *eCash* als auch bei *CyberCoin* um explizite Zahlungssysteme im *Niedrigwertbereich* handelt, hat die Auswahl in diesem Kapitel nicht beeinflußt. Das Prinzip des Zahlungsvorgangs ist hiervon nicht betroffen.

6.1 eCash

Die folgenden Angaben beziehen sich auf den von der Deutschen Bank unternommenen, Ende 1997 gestarteten Pilotversuch mit dem von der Firma

[1] in [Medvinsky u. Neumann, 1995]

[2] *MilliCent* existiert lediglich als Demonstrations-Version mit Token, die die Funktion von *Spielgeld* besitzen, siehe [MilliCent, 1998] und [Glassmann *et al.*, 1995].

DigiCash Inc. entwickelten Internet-Zahlungssystem *eCash*[3].

Das Prinzip von *eCash* ist, daß von einer Bank sogenannte *elektronische Münzen* in Form von mittels eindeutiger Seriennummer identifizierbaren Bitfolgen (Token) mit jeweils bestimmtem Nominalwert an Benutzer ausgegeben werden. Diese Token repräsentieren ein Zahlungsversprechen des emittierenden Institutes (der Bank) gegenüber dem Inhaber der elektronischen Münze. Die Bank garantiert für die Einlösung der von ihr ausgegebenen Token. Jedes Token ist hierzu mit Hilfe des in Abschnitt 4.1 beschriebenen asymmetrischen Kryptoverfahrens signiert. Die einzelnen Token beinhalten jeweils ein Verfallsdatum der ihnen auferlegten Nachweis-Funktion, ähnlich einem herkömmlichen Scheck. Analog zum System der *GeldKarte* und zu *CyberCoin* (siehe Abschnitt 6.2) existiert bei der Bank als ausgebendem Institut ein sogenanntes *eCash-Poolkonto*[4], in dessen Saldo der Wert aller emittierten Token des Systems gespeichert ist. Die Token selber tragen inhärent keinen Wert, sie dokumentieren lediglich eine Verpflichtung des Token-Emittenten gegenüber dem Inhaber. Sie stellen ein dokumentiertes Zahlungsversprechen auf Zahlung des betreffenden Betrages dar.

Beteiligt an einem Zahlungsvorgang mit *eCash* sind die drei Parteien Zahlungssender und Zahlungsempfänger (zwei *Benutzer* des Systems) und die Bank. *eCash* ist nicht wie *CyberCoin* oder *GeldKarte* auf eine ausschließliche Kunden-Händler-Beziehung beschränkt. Es können digitale Münzen zwischen zwei beliebigen System-Benutzern transferiert werden.

Voraussetzung eines Zahlungsvorgangs ist, daß Zahlungssender und Zahlungsempfänger jeweils ein Girokonto bei der dritten Partei, der *eCash*-emittierenden Bank, führen. Es müssen jeweils spezielle vertragliche Vereinbarungen über die Nutzung des *eCash*-Systems bestehen. Jeder System-Benutzer nimmt bei der Bank persönlich die *eCash*-Software in Empfang und erhält zusammen mit einem Initialisierungspasswort eine eindeutige Kontokennung für ein seiner Person zugeordnetes, bei der Bank geführtes *virtuelles eCash-Konto*. Vor einem Zahlungsvorgang müssen sowohl Zahlungssender als auch Zahlungsempfänger die *eCash*-Software lokal auf ihrem PC installieren und außerdem Zugang zum Internet haben. Bei der Installation werden nach Eingabe des Initialisierungs-Passworts ein Börsen-Passwort und ein Konto-Passwort[5] generiert für die Authentifizierung des Kontoinhabers als einzigem rechtmäßigen Benutzer der lokal installierten *eCash*-Software, mit der allein der Zugang zum *eCash*-System möglich ist. Diese durch Passwort realisierte Zugangskontrolle bezieht sich sowohl auf den Zugriff auf die auf dem Benutzer-PC lokal gespeicherten Informationen als auch auf das Girokonto und *eCash*-Konto bei

[3] Die Informationen hierzu stammen aus [eCash-Pilotprojekt, 1998]

[4] siehe hierzu die Veranschaulichung des Systems in Abb. 6.1

[5] Börsen-Passwort und Konto-Passwort können identisch sein.

der Bank. Bei Ausführung der lokalen *eCash*-Software wird vom Benutzer das Börsen-Passwort als Authentifizierungs-Beweis abgefragt.

Es gibt zwei verschiedene Versionen der *eCash*-Benutzer-Software. Die eine Version ist eine Implementierung speziell für *Händler*, die andere für alle sonstigen Benutzer des Systems. Die Händler-Version beinhaltet die automatische Erstellung von Zahlungsaufforderungen. Bei Anbindung der *eCash*-Software an einen Web-Server und Aufruf einer entsprechenden URL wird eine Zahlungsaufforderung an den die Seite aufrufenden Kunden verschickt. Die zweite Version mit ausschließlicher Kunden-Funktionalität bearbeitet automatisch ankommende, von einer Händler-Software generierte und verschickte Zahlungsaufforderungen.

Zahlungsaufforderungen können von der *Kunden-Software* nicht generiert werden, eine Zahlungssendung ohne spezielle Händler-Software an einen anderen Benutzer im System kann nur per *email* geschehen.

Eine Einschränkung des Systems besteht darin, daß die Funktionalität des Systems Zahlungen bzw. Geldtransfers im Niedrigwertbereich von bis zu 400,00 DM liegt. Der Saldo eines *eCash*-Kontos kann diesen Betrag nicht überschreiten.

Ein **Zahlungsvorgang** mit dem *eCash*-System verläuft in vier bzw. fünf[6] voneinander unabhängigen, einzeln zu initiierenden Prozessen.
Der erste Prozeß ist eine vom Zahlungssender initiierte konventionelle **Überweisung**[7]. Die Bank wird vom Zahlungssender zur Buchungstransaktion eines bestimmten Betrages vom Girokonto auf das *eCash*-Poolkonto des Zahlungssenders angewiesen. Die aus dieser Anweisung resultierende Vormerkung der Buchungstransaktion wird beim nächsten Buchungsschnitt von der Bank ausgeführt. Gleichzeitig wird der Betrag dem virtuellen *eCash*-Konto des Benutzers gutgeschrieben. Der eigentliche *Geld-Wert* ist nur durch den Saldo des Poolkontos repräsentiert, nicht durch den Saldo des *eCash*-Kontos.
Der Saldo des *eCash*-Kontos wird dem Zahlungssender als *maximaler Verfügungsrahmen* über einen Anteil des Poolkontos durch seine lokale *eCash*-Software angezeigt. Der Zahlungsvorgang kann somit im Gegensatz zum *CyberCoin*-System solange nicht fortgesetzt werden, wie die Überweisung durch die Bank nicht ausgeführt ist.

Danach kann vom Zahlungssender der zweite Prozeß des **Abhebens** ausgelöst werden. Hierbei werden vom *eCash*-Konto sogenannte elektronischen Münzen in den lokalen Speicher des Zahlungssenders, in die sogenannte *eCash*-Wallet der lokalen *eCash*-Software, überführt. Für diesen Vorgang ist zur Authentifizierung gegenüber der lokalen *eCash*-Software die Eingabe des Konto-

[6] abhängig von der *eCash*-Software-Komponente des Zahlungssenders
[7] wie in Abschnitt 3.2 ab Seite 18 beschrieben

Passworts durch den Zahlungssender notwendig. Die Ausgabe der elektronischen Münzen seitens der Bank geschieht unter Verwendung des Verfahrens der *Blinden Signatur*[8]. Der Zahlungssender, bzw. seine *eCash*-Software, generiert eine zur Wahrung der Einmaligkeit ausreichend große Zufallszahl als Seriennummer der elektronischen Münze. Diese Seriennummer wird vor dem Verschicken an die *eCash*-emittierende Bank *ausgeblendet*. Die mit der *Ausblendung* realisierte Verheimlichung des Nachrichteninhalts gegenüber der Bank mit gleichzeitiger Möglichkeit des digitalen Signierens seitens der Bank ist mit Hilfe des bankeigenen öffentlichen Schlüssels und einer weiteren vom Zahlungssender generierten Zufallszahl möglich. Die so erhaltene *'rohe'* elektronische Münze mit der *unlesbaren* Seriennummer wird an die Bank geschickt. Die Bank signiert die Bitfolge mit ihrem den Nominalwert der elektronischen Münze repräsentierenden, geheimen Schlüssel. Da die Bank nicht in Kenntnis der Serienummer der ausgegebenen Münze kommen kann, ist eine Zuordnung des Tokens zu Personen nicht möglich. Die Bank *weiß* nicht, an wen sie bestimmte Token ausgegeben hat, da die Bank nicht die notwendige Information zur Identifizierung der Token besitzt. Diese Eigenschaft der *eCash*-Token entspricht der von (*echten*) physikalischen Münzen.

Die Anonymität des Zahlungssenders ist in diesem Systems durch das Prinzip der *Blinden Signatur* gewährleistet. Mehrere Zahlungen können nicht mittels Informationen, die im Zahlungsmittel selbst enthalten sind oder die dem Zahlungsmittel-Emittenten bekannt sind, in Beziehung gesetzt werden.

Das *eCash*-Konto des Zahlungssenders wird entsprechend dem Betrag der ausgegebenen Münzen belastet und die elektronischen Münzen dann zurück an den Zahlungssender geschickt. Die *eCash*-Software des Zahlungssenders dividiert daraufhin automatisch den *Ausblendfaktor* wieder aus der Seriennummer jeder einzelnen elektronischen Münze heraus.
Der verfügbare Gesamtbetrag an lokal vorrätigen elektronischen Münzen wird dem Zahlungssender mittels Anzeige durch die *eCash*-Software mitgeteilt.

Mit Hilfe der in einer elektronischen Münze enthaltenen digitalen Signatur und dem frei zugänglichen öffentlichen Schlüssel der Bank ist die Echtheit einer Münze für jede Person im System überprüfbar.

Es folgt der Prozeß der **Zahlung**, der abhängig von der Version der *eCash*-Software des Zahlungsempfängers Mit Hilfe zweier, voneinander verschiedener Methoden abläuft.
Mit der ersten Methode erfolgt sie als Reaktion auf eine *Zahlungsaufforderung eines Händlers*, bzw. dessen *eCash*-Händler-Software.

Der Zahlungssender signalisiert durch Aufruf einer mit der Händler-*eCash*-Software verbundenen *URL*[9] eines Händlers den Kaufwunsch eines angebotenen Produktes bzw. Dienstes. Die *eCash*-Software des Händlers schickt darauf-

[8]genaueres hierzu findet sich in [Chaum, 1983]

[9]Spezifizierung eines Objektes im Internet durch Angabe von Protokoll, Host und Pfad

hin automatisch der *eCash*-Software des Zahlungssenders eine Zahlungsaufforderung zu, in der Kontokennung des Händlers und Rechnungsbetrag enthalten sind. Falls der Benutzer diese Aufforderung gegenüber seiner lokalen *eCash*-Software bestätigt, werden elektronische Münzen in ausreichender Menge vom Zahlungssender zur Bank geschickt und gleichzeitig lokal beim Zahlungssender gelöscht. Die Münzen landen also nicht in der *eCash*-Wallet des Zahlungsempfängers, sondern werden direkt zur Bank geschickt. Nach Prüfung der Gültigkeit der eingegangenen elektronischen Münzen seitens der Bank wird der Betrag gemäß der enthaltenen Information über die (eindeutige) Kontokennung dem betreffenden Händler-*eCash*-Konto gutgeschrieben. Die Prüfung umfaßt zum einen die Authentifizierung der Token mittels enthaltener Bank-Signatur und zum anderen den Vergleich der Seriennummern mit in zentraler Datenhaltung erfaßten bereits eingelösten Token-Seriennummern. Falls eine Münze schon einmal eingereicht wurde, ist ihre Funktion verfallen, sie ist als Mittel der Zahlung ungültig.

Die zweite Methode (im folgenden *email-Verfahren* genannt) ist die der Zahlung zwischen zwei System-Benutzern, die nicht im Besitz der speziellen Händler-Software sind. Diese Methode sieht zur Kommunikation der nötigen Information den *email*-Dienst des Internets vor. Der Zahlungssender schickt per *email* die elektronischen Münzen an den Zahlungsempfänger. In der email ist wiederum die eindeutige Kontokennung des Zahlungsempfängers enthalten. Auf diese Art erhaltene Token können nur der *eCash*-Wallet mit der entsprechenden Kontokennung gutgeschrieben werden. Die per *email* und ebenso die in der oben genannten Methode auf Zahlungsaufforderung hin transferierten Token sind somit ihrer Eigenschaft nach mit *Orderschecks* (siehe Abschnitt 3.1) vergleichbar, die nur der namentlich genannte Zahlungsempfänger einlösen kann und nicht generell der *Inhaber* des (in diesem Fall elektronischen) Dokumentes.
Eine Zahlungsaufforderung der erstgenannten Händler-Methode ist nur durch die spezielle Händler-*eCash*-Software generierbar. Der reine Transfer von Token zwischen sonstigen System-Benutzern ist ausschließlich per *email* möglich.

Falls beim Zahlungsvorgang die zweite *email-Methode* benutzt wurde, müssen vom Zahlungsempfänger an dieser Stelle noch *zwei* weitere, voneinander unabhängige Prozesse initiiert werden, um einen Zahlungsvorgang abzuschließen. Nach der ersten *Händler*-Methode folgt hier nur noch *ein* Prozeß.

Die *email*-Methode erfordert zuerst den Prozeß des **Einreichens** der während des Zahlungsvorgangs erhalten und nun lokal auf dem PC des Zahlungsempfängers gespeicherten Token bei der Bank. Der Zahlungssender schickt die Token zum Emittenten (die Bank) und diese überprüft, bevor der Betrag auf dem entsprechenden *eCash*-Konto gutgeschrieben wird, in zwei Schritten jede

eingereichte *elektronischen Münze*. Die Überprüfung erfolgt analog zu einem Token-Transfer auf Zahlungsaufforderung hin (s.o.). Einmal wird überprüft, ob die Signatur einer Münze mit der individuellen Signatur der Bank übereinstimmt. Zum anderen wird die Seriennummer eines Tokens mit allen innerhalb eines bestimmten Zeitraums[10] eingereichten Token verglichen, um das mehrmalige Einreichen der identifizierbaren Token durch System-Benutzer zu verhindern. Die Einmalbenutzung der leicht kopierbaren Token muß sichergestellt sein. Daraufhin wird der Betrag der eingereichten Token dem definierten *eCash*-Konto gutgeschrieben, die jeweilige Seriennummer in die zentrale Datenhaltung aufgenommen und *die elektronische Münze gelöscht*.
Im zweiten Prozeß muß noch der Saldo des *eCash*-Kontos vom *eCash-Poolkonto* der Bank auf das Girokonto des Zahlungsempfängers überwiesen werden, um den Zahlungsvorgang abzuschließen. Der Zahlungsempfänger beauftragt hierzu mit Hilfe seiner *eCash*-Software die Bank zu einer herkömmlichen Überweisung analog zum oben erwähnten ersten Prozeß des Zahlungsvorgangs. Beim nächsten Buchungsschnitts wird so zeitverzögert die vorgemerkte Buchungstransaktion von der Bank ausgeführt und der Zahlungsvorgang ist abgeschlossen. Der *Wert* ist vom Zahlungssender zum Zahlungsempfänger transferiert.

Bei der *Händler-Methode* sind die Token in dem Zustand nach dem *Zahlungsvorgang* bereits bei der Bank eingereicht. Sie werden als Reaktion auf die vom Händler verschickten Zahlungsaufforderung direkt vom Zahlungssender zur Bank gesendet. Der Zahlungssender (Händler) muß somit nur noch eine Überweisung des auf seinem *eCash*-Konto verzeichneten Betrages auf sein Girokonto initiieren und die Bank daraufhin bei nächstem Buchungsschnitt die entsprechende Buchungstransaktion ausführen.

Die Kommunikation über den unsicheren Weg des Internets ist im *eCash*-System mit Hilfe des asymmetrischen Verschlüsselungsverfahrens gesichert. Jede Partei (jeder Benutzer und jede Bank[11]) hat ein eigenes Schlüsselpaar (einen privaten und einen öffentlichen Schlüssel). Zwischen zwei Kommunikations-Partnern wird jede Nachrichten mit dem öffentlichen Schlüssel der jeweils anderen Partei verschlüsselt. So ist Vertraulichkeit der gesamten Datenübertragung und gegenseitige Überprüfbarkeit der Authentizität einer Nachricht gewährleistet.

Die drei Aktionen, die zur Durchführung des Zahlungsvorgangs vom *Zahlungssender* initiiert werden, können nicht von einer anderen Person ausgeführt werden. Die Passwörter zur jeweiligen Authentifizierung sind laut den vertrag-

[10] die *elektronischen Münzen* besitzen eine zeitlich eingeschränkte Gültigkeit

[11] der Digicash-Entwurf sieht die Möglichkeit vor, daß mehrere Banken jeweils ihr *eigenes eCash* herausgeben und *Abrechnungen* zwischen den Banken erfolgen

lichen Vereinbarungen nicht übertragbar und somit hat niemand anders als der Inhaber des Giro– und *eCash*-Kontos Zugriff zum System.

Ebenso kann als Zahlungsempfänger nur die Person des Kontoinhabers die Token bei der Bank einreichen und den Zahlungsvorgang so abschließen. In den Token ist jeweils als eindeutige Zuordnung die Kontokennung enthalten.

6.2 CyberCoin

Aktuell besteht das Angebot der CyberCash GmbH[12] in Deutschland aus einem Internet-Zahlungssystem mit drei verschiedenen Zahlungsverfahren[13], von denen in diesem Abschnitt nur auf das *CyberCoin-System*[14] eingegangen wird. *CyberCoin* stellt als einziges der drei Verfahren ein eigenes Konzept eines Zahlungsverfahrens dar, während die beiden anderen auf den bereits beschriebenen Zahlungssystemen Lastschriftverfahren (siehe Abschnitt 3.3) und Kreditkarten-Zahlung (siehe Abschnitt 7.2) aufsetzen und lediglich deren Realisierung für eine Umgebung von innerhalb des Internets vernetzten Computern darstellen. *CyberCoin* ist als eigenständiges System genauso wie *eCash* ein auf Niedrigwertbeträge eingeschränktes Zahlungssystem.

Das *CyberCash-System* besteht aus den drei Software-Komponenten *Kunden-Wallet*, *Händler-Wallet* und *Gateway-Server* mit den virtuellen Konten[15]. Zahlungssender und Zahlungsempfänger müssen die für sie erforderlichen Software-Komponenten des Systems persönlich bei der an das System angebunden Bank entgegennehmen (mit Prüfung ihrer Identität durch Vorlage des Personalausweises) und lokal bei sich installieren. Ähnlich des in Abschnitt 7.3 beschriebenen GeldKarten-Systems sind für Zahlungssender und Zahlungsempfänger unterschiedliche Komponenten vorgesehen, allerdings hier im Gegensatz zum GeldKarten-System in Form von Software. Das *CyberCoin*-System bezieht sich in seiner Funktionalität allein auf die Zahlungsfunktion in einer Kunde-Händler-Situation. Die Realisierung der separaten Wertübertragungsfunktion von Geld zwischen zwei beliebigen System-Benutzern ist nicht enthalten. Im folgenden wird aus diesem Grund vorwiegend der Begriff *Kunde* anstatt *Zahlungssender* und *Händler* anstatt *Zahlungsempfänger* verwendet.

[12] bestehend aus der Firma CyberCash Inc. zusammen mit mehreren deutschen Kreditinstituten

[13] in [CyberCash-Pilotprojkt, 1998] wird zwar die Formulierung der „möglichen Verknüpfung des CyberCash-Software-Paketes mit den drei verschiedenen *Zahlungsmitteln oder -methoden*“ verwendet, im weiteren wird aber weiterhin der Begriff des *Zahlungsverfahrens* verwendet, da der Zahlungs*vorgang* in dieser Betrachtung im Vordergrund steht.

[14] Dieser Abschnitt ist mit Hilfe von Informationen aus [CyberCash-Pilotprojkt, 1998] und der zusätzlichen Befragung eines Mitarbeiters der Dresdner Bank entstanden.

[15] siehe die Veranschaulichung hierzu in Abb. 6.1 auf Seite 49

Beteiligt an einem Zahlungsvorgang sind in minimaler Umgebung der Kunde, der Händler, der vermittelnde, bankeigene sogenannte *CyberCash-Gateway-Server* und eine Bank der *CyberCash GmbH*. Mit der Bank muß sowohl der Kunde als auch der Händler vertragliche Vereinbarungen (einen Girokonto-Vertrag und einen speziellen Teilnahmevertrag am *CyberCash-System*) halten.

Seitens des Zahlungssenders ist Voraussetzung eines *CyberCoin*-Zahlungsvorgangs die Generierung einer Wallet-ID[16] zusammen mit einem Passwort. Die Wallet-ID wird in die vertraglichen Vereinbarungen zwischen Benutzer und Bank aufgenommen. Mit ihr wird die eindeutige Zuordnung von Wallet zu Konto hergestellt. Hiermit ist sichergestellt, daß der Zugriff auf ein Konto nur mit einer individuellen Software-Komponente möglich ist und ein Mißbrauch mit dem Wissen um eine Kontonummer ausgeschlossen ist.

Mit dem Passwort muß sich der Kunde bei jedem System-Zugang gegenüber seiner lokal installierten Wallet-Software authentifizieren.

Das Konzept des *CyberCoin*-System realisiert nicht die separate Wertübertragungsfunktion von *Geld* zwischen beliebigen System-Benutzern. Jeder Zahlungsvorgang ist direkt gekoppelt an die Zustellung der Gegenleistung vom Händler (dem Zahlungsempfänger). Bei dieser Gegenleistung kann es sich definitionsgemäß nur um ein 'Gut' in elektronischer Form handeln, das *CyberCoin*-Zahlungssystem ist festgelegt auf den *Handel von im Internet zustellbaren Soft-Goods*. Das Verfahren eines *CyberCoin*-Kaufvorgangs gewährleistet, daß sowohl der Händler *sein Geld* als auch der Kunde die mit dem Geld gekaufte Gegenleistung erhält.

Die nun folgende Beschreibung erläutert die in sich streng sequentiell ablaufenden *vier* Prozesse eines Zahlungsvorgangs in minimaler Umgebung.

Der Ladevorgang Es handelt sich im folgenden um einen *nicht-initialen* Ladevorgang, bei dem im Gegesatz zum allerersten *CyberCoin*-Ladevorgang mit der *CyberCash*-Software der Ladebetrag dem Kunden zur Verfügung steht *bevor* die Bank-interne Buchungs-Transaktion (zwischen Girokonto des Zahlungssenders und Sammelkonto) ausgeführt ist.

Der Zahlungssender authentifiziert sich mittels Passwort-Eingabe gegenüber seiner lokalen *CyberCash*-Software. Er schickt mit Hilfe der Wallet-Software eine Anfrage mit dem Ladewunsch über einen bestimmten Ladebetrag an den *CyberCash-Gateway*. Dieses erstellt eine technische Lastschriftdatei[17] für den Einzug des Betrages zum Zeitpunkt des anschließenden Buchungsschnitts

[16] Identifikations-Nummer

[17] diese Bezeichnung hat nicht die rechtlichen Konsequenzen des Lastschriftverfahrens wie es in Abschnitt 3.3 beschrieben wird, es liegen andere vertraglich vereinbarte Bedingungen

bei der Bank. Daraufhin erfolgt zeitverzögert die entsprechende Buchungs-Transaktion zwischen Girokonto des Zahlungssenders und *CyberCoin*-Sammelkonto. Die hierfür notwendigen Informationen der technischen Lastschrift werden über Banken-eigene Infrastruktur zur Bank gesendet. Der *CyberCash-Gateway* erhöht den Saldo des virtuellen Kontos (des *CashContainers* des Zahlungssenders) und der Zahlungssender kann sofort über den durch seine Wallet-Software angezeigten Saldo seines CashContainers verfügen.

Der Kaufvorgang Wie beim Ladevorgang authentifiziert sich die Person des Zahlungssenders (der Kunde) mit dem laut vertraglichen Konditionen nicht übertragbaren Passwort.

- Der Kunde teilt dem Händler seinen Kaufwunsch mit und bekommt daraufhin das gewünschte 'Soft-Good' in verschlüsselter, unbrauchbarer Form zugesendet. Dieses erfolgt mit Hilfe eines Web-Browsers, der so konfiguriert ist, daß er direkt die Wallet-Software des Kunden aufrufen kann.
- Die Wallet-Software startet automatisch lokal beim Kunde und das persönliche Passwort des Kunden muß eingegeben werden.
- Der Kunde bestätigt die ihm angezeigte Zahlungsaufforderung.
- Die Zahlungsinformationen der Kunden werden verschlüsselt an den Händler übertragen.
- Der Händler fügt eigene Zahlungsinformationen hinzu und schickt diese an den *CyberCash-Gateway*.
- Der *CyberCash-Gateway* entschlüsselt das bei ihm eingetroffene Paket, prüft die Daten auf Integrität und auf übereinstimmende Angaben von Kunde und Händler.
- Falls die Prüfung ein positives Ergebnis liefert, werden die virtuellen *CyberCash*-Konten entsprechend den Daten aktualisiert: Der Kunden-CashContainer wird mit dem übermittelten Betrag belastet und der Betrag dem Händler-CashContainer gutgeschrieben.
- Es folgt die Bestätigung der erfolgten Zahlung vom *CyberCash-Gateway* an den Händler, der wiederum den Kunden hiervon in Kenntnis setzt.
- Schließlich wird der zur Entschlüsselung des noch unbrauchbaren Soft-Goods benötigte Schlüssel vom Händler an den Kunden geschickt. Der Kaufvorgang ist abgeschlossen.

---

zwischen Zahlungssender und Bank zu Grunde.

Im Gegensatz zum *GeldKarten-System* ist somit die Person des Benutzers über den gesamten Zahlungsvorgang hinweg invariant, genauso wie beim *eCash-System*.

Der Kassenabschluß-Vorgang Zu einem vom Zahlungsempfänger gewählten (vom System nicht vorgegebenem) Zeitpunkt wird ein sogenannter *Kassenabschluß* durchgeführt. Der Zahlungsempfänger schickt zur Initiierung eine Nachricht an das *CyberCash-Gateway*, das daraufhin die nötigen Daten für den Einzug des Betrages vom Sammelkonto an die Bank sendet. Der Betrag des Überweisungsauftrages ist der Saldo des CashContainers des Zahlungssenders. Der Überweisungsauftrag wird von der Bank im folgenden Buchungsvorgang ausgeführt. Der CashContainer-Saldo des Zahlungsempfängers wird am Ende des Kassenabschluß-Vorgangs gelöscht.
Wie beim *eCash*-System endet der Zahlungsvorgang mit der zeitverzögerten Buchungs-Transaktion innerhalb der Bank, die den eigentlichen Geldtransfer darstellt. Zum Zeitpunkt des nächsten Buchungsschnitts wird das Sammelkonto um den Betrag der eingegangenen Transaktions-Daten belastet und dem Girokonto des Zahlungsempfängers der entsprechende Betrag gutgeschrieben. Zu diesem Zeitpunkt sind die aus dem Ladevorgang hervorgegangenen Buchungs-Daten entweder schon bearbeitet (Girokonto-Belastung des Zahlungssenders und Sammelkonto-Gutschrift) oder die Bearbeitung erfolgt im Buchungsvorgang der Kassenabschluß-Daten.

Vergleich von *eCash* und *CyberCoin* Im abschließenden Vergleich dieser beiden Internet-Systeme sind drei wesentliche Punkte zu nennen.

- Bei *CyberCoin* handelt es sich, ähnlich wie beim *GeldKarten*-System, um ein ausschließliches Zahlungssystem ohne Realisierung der Wertübertragungsfunktionalität. *eCash* dagegen legt mit den für die Benutzer erforderlichen Software-Komponenten nicht fest, wer die ausschließliche Möglichkeit zum Zahlungssenden und zum Zahlungsempfangen besitzt.

- Die Dokumentation des Nachweises wird während des Zahlungsvorgangs bei eCash in Form der Token *direkt* beim Benutzer gespeichert, bei *CyberCoin* erfüllen die an zentraler Stelle (beim Gateway) gespeicherten CashContainer-Salden diese Funktion.

- eCash-Token sind nach dem Vorbild von physikalischen Münzen *anonym*, bei *CyberCoin* ist jede Aktion eines Benutzers vollständig protokollierbar mittels Informationen, die dem Gateway vorliegen. Es ist ein rein kontobasiertes System im Gegensatz zu eCash.

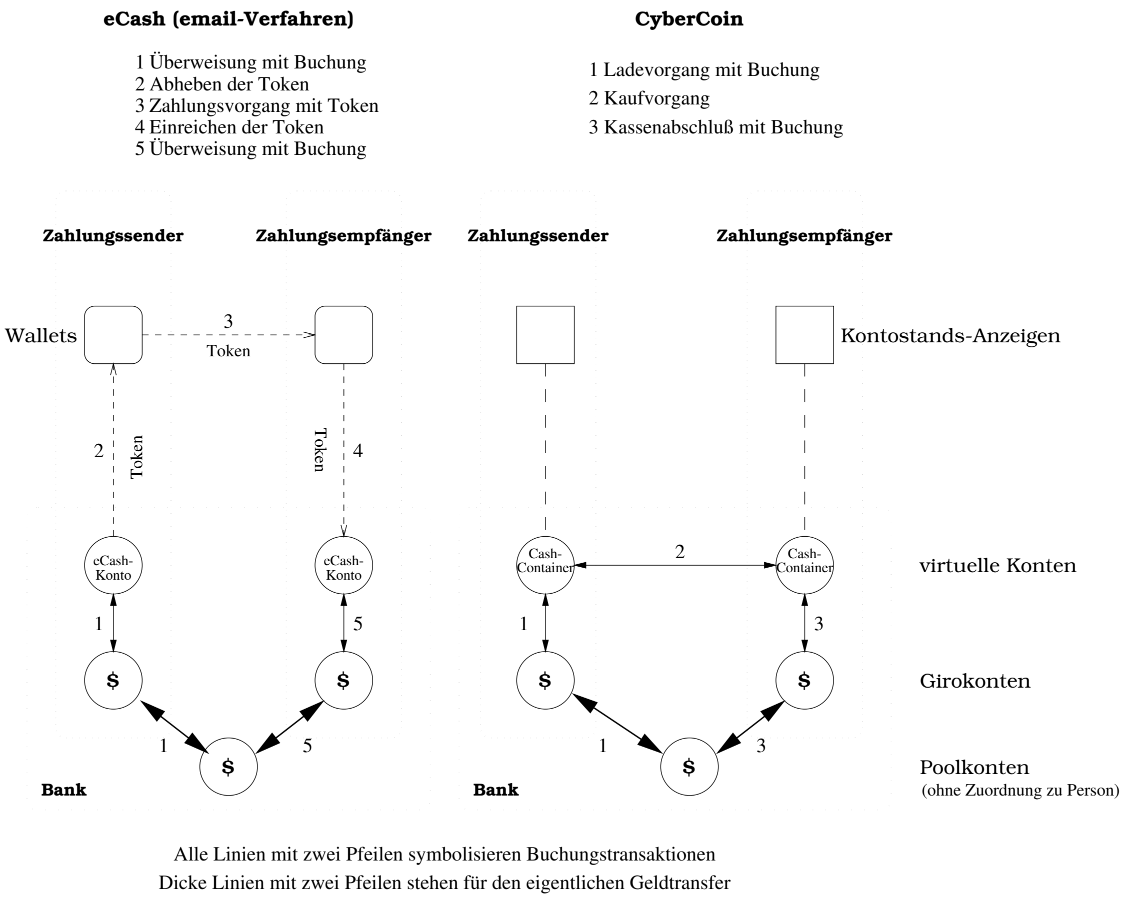

Abbildung 6.1: *eCash* und *CyberCoin* im Vergleich

Kapitel 7

Kartenbasierte Systeme

Betrachtet werden in diesem Kapitel drei weit verbreitete hardwarebasierte Zahlungssysteme, die an den Besitz einer physischen *Karte* gebunden sind. Bei allen drei Systemen werden zur Automatisierung von Zahlungsvorgängen elektronisch Informationen auf der Karte gespeichert. Gleichzeitig dient der Besitz der Karte (meistens zusammen mit einem anderen Merkmal) der Authentifizierung eines rechtmäßigen Benutzers.

Als erstes wird das Debitkarten-Zahlungssystem, das *POS-System* mit den drei verschiedenen Verfahrensweisen *electronic cash*, *POZ* und *ELV* beschrieben, danach die Zahlungsmöglichkeit mit einer Bankkreditkarte behandelt. Schließlich wird die *GeldKarte* der deutschen Kreditwirtschaft als national in Verbindung mit Kunden- bzw. ec-Karten von Kreditinstituten am weitesten verbreitetes sogenanntes *stored value card system* analysiert. Exemplarisch wird dieses System im nächsten Kapitel Untersuchungsobjekt zur Beantwortung der Frage sein: Simuliert ein bestimmtes Zahlungssystem *Geld*.

Auf die Tatsache, daß sich gebündelt mehrere Zahlungssysteme an eine einzige physikalische Karte gebunden sein können, wie es bei der deutschen ec-Karte der Fall ist[1], wird in der folgenden Betrachtung nicht eingegangen.

7.1 Debitkarte

Das Charakteristikum der Debitkarte ist die Eigenschaft, daß jede einzelne Transaktion, also jeder einzelne mit der Karte durchgeführte Zahlungsvorgang,

[1] Es ist möglich, in Verbindung mit der PIN weltweit Bargeld an ATM-Automaten abzuheben; das POS-System ist in der Karten-Funktionalität enthalten und ebenso der Zugang zum GeldKarten-System.

unmittelbar[2] zur Belastung des der Karte zugeordneten Girokontos führt. Im Gegesatz dazu werden beispielsweise bei der *Kreditkarte*[3] Transaktions-Daten über einzelne Zahlungsvorgänge auf einem Zwischenkonto zusammengefaßt und zu einem späteren Zeitpunkt gesammelt abgewickelt.

Eine Debitkarte wird im Gegensatz zur später behandelten *Kreditkarte* ausschließlich von Banken ausgegeben. Die Zitate in diesem Abschnitt beziehen sich exemplarisch auf die *ec-Karte* als der in Deutschland am weitesten verbreiteten Form der Debitkarte.

Eine Debitkarte ist eine Magnetstreifenkarte; sie ist eine passive Speicherkarte, die keine Logik enthält. Auf alle Daten kann direkt lesend zugegriffen werden, es kommt kein Verschlüsselungs-Verfahren zum Einsatz. Die auf dem Magnetstreifen gespeicherten Daten umfassen Kontonummer, Gültigkeitsdatum, Länderschlüssel, Daten des Kartenherausgebers, Bankleitzahl, Währungsschlüssel und Hinweise auf Zugriffsrestriktionen bezüglich des zugeordneten Kontos. Es sind keine Informationen enthalten, die direkt einen Wert oder Kontostand repräsentieren (wie etwa auf der später beschriebenen *GeldKarte*). Außerdem sind keine Informationen über die Person des der Karte eindeutig zugeordneten Kontoinhabers gespeichert[4], sondern ausschließlich Informationen über die Kontoverbindung.

Eine Debitkarte wird bei der Aushändigung durch das kartenausgebende Institut an die Person des Kontoinhabers gebunden. „[Der] Kontoinhaber unterschreibt die ec-Karte und Empfangsbescheinigung in Anwesenheit eines Mitarbeiters des Kreditinstitutes [...]. Unterschrift auf der Empfangsbescheinigung und der ec-Karte müssen übereinstimmen.“ [Bülow, 1991, S. 754]. Die Karte ist eindeutig dem auf ihr angegebenen Konto zugeordnet. „Die ec-Karte gilt [bis zum Ende des auf ihr vermerkten Kalenderjahres] ausschließlich für das auf ihr angegebene Konto. Sie kann nur auf den Namen des Kontoinhabers oder eines Bevollmächtigten ausgestellt werden.“ [Bülow, 1991, S. 753]. Da es, wie bereits erwähnt, keine *anonymen* Konten in Deutschland gibt, ist hiermit eine eindeutige Zuordnung von Karte zu Person gegeben.

Jede Debitkarte wird mit einer *Persönlichen Identifikationsnummer (PIN)* ausgegeben. Das Wissen um die *PIN* in Verbindung mit dem Besitz der Karte sind zusammen Identifizierungsmerkmal eines rechtmäßigen Benutzers. Die vierstellige PIN erlaubt 9999 verschiedene Variationen (Passworte), es ist also keine eigentliche Identifizierung des Benutzers damit möglich. Eine Identifi-

[2] aber nicht sofort; die Buchungstransaktion wird erst bei nächstem Buchungsschnitt ausgeführt

[3] siehe nächster Abschnitt

[4] der Name des Kontoinhabers ist der Plastikkarte aufgeprägt

zierung wäre gegeben, wenn jeder System-Benutzer ein eindeutiges Geheimnis besitzen würde. Der zusätzliche System-Mechanismus bei dem folgenden *electronic cash*-Verfahren ist die zwischen Systemanbieter und Benutzer vertraglich vereinbarte Geheimhaltungspflicht der *PIN* seitens des Benutzers.

Zusätzlich erfolgt zur Sicherheit des Benutzers die Sperrung des System-Zugangs mit einer Karte, wenn dreimal die der Karte zugeordnete *PIN* falsch eingegeben wurde.

Das institutsübergreifende System zur bargeldlosen Zahlung an automatisierten Kassen (POS-System)

Die Grundlage des an die Debitkarte gekoppelten Zahlungssystems *Point of Sale (POS)* mit den drei unterschiedlichen Verfahren *electronic cash*, *Point of Sale ohne Zahlungsgarantie (POZ)* und *Elektronisches Lastschriftverfahren (ELV)* sind vertragliche Vereinbarungen zwischen Zahlungssender und kartenausgebendem Institut einerseits und Zahlungsempfänger und kartenausgebendem Institut andererseits. Der Zahlungssender muß beim kartenausgebenden Institut ein Girokonto führen (also einen *Girovertrag* mit dem Institut haben). Dieser Vertrag beinhaltet die Authorisierung der Bank zur automatischen, elektronischen Kontobelastung ohne explizite Austellung einer Rechnung. Der Zahlungsempfänger muß sich mit der Unterzeichnung eines besonderen *Händlervertrages*[5] dem *POS-System* anschließen. Dieser Vertrag ist seitens des Zahlungsempfängers zusätzlich zu einem Girovertrag erforderlich. Außerdem ist ein besonderes *Kassenterminal* mit Anschluß an eine DFÜ-Leitung beim Zahlungsempfänger Voraussetzung für die Funktion des Systems.

Ein Zahlungsvorgang erfolgt mit den drei verschieden POS-Verfahren jeweils in zwei unabhängigen Prozessen. Zum einen werden die Transaktionsdaten an einer automatisierten Kasse erfaßt und gespeichert, zum anderen muß der Zahlungsempfänger die Abwicklung der innerhalb der Bank stattfindenden Buchungstransaktion einleiten.

electronic cash Bei *electronic cash* handelt es sich unabhängig von den herkömmlichen Instrumenten des bargeldlosen Zahlungsverkehrs (s. Kap. 3) um ein eigenständiges Zahlungsverfahren der (deutschen) Kreditwirtschaft.
Ein Zahlungsvorgang beginnt, in dem der Zahlungssender dem Zahlungsempfänger[6] die Karte aushändigt. Die Karte wird in das Leseterminal gesteckt und es folgt die Abfrage und Eingabe der *PIN* durch den Karteninhaber. Der Karteninhaber ist gemäß den dem System zu Grunde liegenden vertraglichen Vereinbarungen die Person des Kontoinhabers. Mit Erhalt der Karte hat er

[5] diesen Vertrag schließt er stellvertretend für das kartenausgebende Institut mit der *Gesellschaft für Zahlungssysteme* ab

[6] bzw. dem Bedienungspersonal der automatisierten Kasse

sich verpflichtet, daß „[...] ein Dritter keine Kenntnis von der persönlichen Geheimzahl [der *PIN*] erlangt, insbesondere darf sie Dritten nicht mitgeteilt und nicht auf der ec-Karte vermerkt werden.“ [Bülow, 1991, S. 760]. Die automatisierte Kasse ist über DFÜ-Leitung mit einem sogenannten *Netzbetreiber* verbunden, der eine vermittelnde Funktion bei dem Zahlungsvorgang übernimmt. Mit Hilfe der Online-Verbindung über den Netzbetreiber zum kartenausgebenden Institut wird eine Authorisierung der Zahlung durch das kartenausgebende Institut eingeholt.

Hierbei wird die PIN überprüft, das Nicht-Vorhandensein der Kartensperre, eine eventuelle Überschreitung des zwischen Zahlungssender und Bank im Girovertrag festgeschriebenen maximalen Verfügungsrahmens sowie die Bonität des Zahlungssenders sichergestellt. Mit der positiven Bestätigung dieser Überprüfung wird der Zahlungsvorgang fortgesetzt und die entsprechenden Transaktionsdaten (u.a. Zahlungsbetrag und die zwei Kontoverbindungen) zum Netzbetreiber geschickt und dort zwischengespeichert.

In einem zweiten Prozeß gibt der Zahlungsempfänger mit der Übermittlung einer Nachricht dem Netzbetreiber das Signal zur Erstellung eines *Kassenabschlusses*. Der Netzbetreiber faßt alle seit dem letzten Kassenabschluß eingegangenen Transaktions-Daten zusammen und schickt sie über bankeneigenes Netzwerk zur Bank des Zahlungsempfängers. Dort wird zum Zeitpunkt des nächsten Buchungsschnitts der Zahlungsvorgang abgeschlossen. Es erfolgt der Einzug des Zahlungsbetrages vom Girokonto des Zahlungssenders und die Gutschrift des Zahlungsbetrages auf dem Girokonto des Zahlungsempfängers. In diesem System gibt es keine Möglichkeit des *Rückgängigmachens eines Zahlungsvorganges* in Form einer *Lastschriftrückgabe*, wie es bei den beiden folgenden Systemen der Fall ist. Bei *electronic cash* handelt es sich nicht um das allgemeine Lastschriftverfahren, wie es in Kap. 3.3 beschrieben ist.

Die Identifizierung des Kontoinhabers als einzig rechmäßigem Benutzer der Karte in einem *electronic cash*-Zahlungsvorgang beruht nicht allein auf den automatisierten Mechanismen des Systems, sondern gründet sich auf der Einhaltung der von der Person des Kontoinhabers unterzeichneten oben genannten Vertragbedingungen. Man kann sagen, daß die Personen-Authentifizierung des Systems nur in Verbindung mit den zusätzlichen Allgemeinen Geschäftbedingungen (AGB) des kartenausgebenden Instituts gegeben ist. Wie im Kapitel *Kommunikation* auf Seite 21 bereits erläutert, ist sowohl die Karte als auch die PIN prinzipiell (leicht) übertragbar auf eine andere Person. Dieser Punkt wird allerdings unterbunden, indem rechtlich den Benutzern bestimmte Aktionen verboten werden (nämlich die Weitergabe des Wissen um die PIN) und so die Eigenschaft gewährleistet, daß nur die Person des Kontoinhabers direkten Zugriff auf das ihr zugeordnete Konto hat.

Es sind somit vier Parteien an einem Zahlungsvorgang mittels *electronic cash* beteiligt: der Zahlungssender (Karteninhaber und Kontobesitzer), der Zahlungsempfänger, die vermittelnde Dienstleistungs-Instanz des Netzbetreibers und letztendlich die Bank, die den eigentlichen Geldtransfer in Form der Buchungstransaktion zwischen den beiden Girokonten (dem das Zahlungssenders und dem des Zahlungsempfängers) ausführt.

electronic cash beinhaltet als einziges der drei Verfahren die Service-Leistung der Kreditwirtschaft einer *offiziellen Zahlungsgarantie*, ist allerdings aus diesem Grund auch das System mit den höchsten Gebühren.

POZ Bei dem System des *Point of Sale ohne Zahlungsgarantie (POZ)* wird analog zum *electronic cash*-System die Karte dem Zahlungsempfänger bzw. dem Bedienungspersonal ausgehändigt und in das Kassenterminal eingeführt. Abhängig von der Höhe des Zahlungsbetrages wird wiederum mittels DFÜ eine Anfrage über den zwischengeschalteten Netzbetreiber an das kartenaugebende Institut geschickt. Diese Anfrage beinhaltet allerdings im Unterschied zum vorher geschilderten *electronic cash*-System ausschließlich die Überprüfung, ob die Karte in einer bankeneigenen Kartensperr-Datei enthalten ist. Auf diese Überprüfung wird derzeit generell bei Zahlungsbeträgen unter 60,00 DM seitens des Zahlungsempfängers verzichtet. Daraufhin werden die auf der Karte gespeicherten Daten zur automatischen Erstellung einer Einzugsermächtigung im herkömmlichen Lastschriftverfahrens benutzt. Der ausgedruckte Beleg muß vom Karteninhaber unterschrieben werden und die geleistete Unterschrift muß mit derjenigen auf der Rückseite der Karte übereinstimmen. Es ist folglich ebenso wie bei *electronic cash* nur der Kontoinhaber berechtigt zur Ausführung eines Zahlungsvorgangs mit dem POZ-Verfahren. Eine Übertragung dieser Zahlungs-Funktionalität der Karte (der Zugang zum POZ-Verfahren) auf eine andere Person ist nicht möglich.
Ein Zahlungsvorgang mittels POZ-Verfahren beinhaltet analog zu *electronic cash* den weiteren Prozeß der Auslösung eines Kassenabschlusses durch den Zahlungsempfänger. Wiederum wird eine Nachricht vom Zahlungsempfänger an den zwischengeschalteten Partei des Netzbetreiber gesendet und dieser schickt daraufhin die aufbereiteten Transaktionsdaten über die bankeneigene Infrastruktur zur Bank des Zahlungsempfängers. Dort wird zum Zeitpunkt des nächsten Buchungsschnitts die entsprechende Buchungstransaktion ausgeführt und der Zahlungsvorgang ist damit abgeschlossen.
Da es sich um das Lastschriftverfahren handelt, ist keine (offizielle) Zahlungsgarantie der Bank enthalten wie bei *electronic cash*. Der Zahlungsempfänger trägt das volle Zahlungsrisiko bei einer möglichen Lastschriftrückgabe. Zur Sicherheit beinhaltet die Unterschrift des Zahlungssenders nicht nur die Au-

thorisierung zum Einzug des Zahlungsbetrages, sondern gleichzeitig das Einverständnis des Zahlungsempfängers zur Preisgabe seiner Identität durch die Bank[7] bei Nicht-Einlösung der Lastschrift.

Genauso wie bei *electronic cash* sind vier Parteien an einem Zahlungsvorgang beteiligt: Zahlungssender, Zahlungsempfänger, Netzbetreiber und Bank.

ELV Das *Elektronische Lastschriftverfahren (ELV)* entspricht bis auf wenige Unterschiede dem POZ-System. Bei einem Zahlungsvorgang sind jeweils nur drei Parteien beteiligt: eine Zahlungssender, ein Zahlungsempfänger und die Bank. Die vermittelnde Partei des Netzbetreibers entfällt. Beim ELV gibt es keine Authorisierung oder Überprüfung von Zahlungsdaten durch die Bank. Die einzige (gängige) Vorsichtsmaßnahme ist das Führen und Prüfen einer eigenen Sperrdatei seitens des Zahlungsempfängers.
Auch das ELV-System erfordert bei einem Zahlungsvorgang einen durch den Zahlungsempfänger explizit ausgelösten zweiten Prozeß: den Vorgang des *Kassenabschlusses*. Im Unterschied zu den beiden anderen Systemen werden die lokal gesammelten Transaktionsdaten direkt bei der Bank eingereicht. Der Zwischenschritt über den Netzbetreiber entfällt.
Bei nächstem Buchungsschnitt der Bank wird wiederum der Zahlungsvorgang mit Ausführung der Buchungstransaktion abgeschlossen.

7.2 Kreditkarte (Bankkreditkarte)

> „*Kredit* im Sinne der Nationalökonomie ist ein *Auseinanderfallen von Leistung und Gegenleisung* [...], ein Tauschgeschäft kommt zustande, in dem ein gegenwärtiges gegen ein zukünftiges Gut getauscht wird.“ [Weisensee, 1970, S. 13].

In diesem Abschnitt über das Zahlungsmittel *Kreditkarte* wird kein Unterschied zwischen einer sogenannten *Charge-Card* und einer klassischen *Kreditkarte* gemacht, das Prinzip eines Zahlungsvorgangs ist im wesentlichen identisch, unterschiedlich sind lediglich die zu Grunde liegenden vertraglichen Konditionen, welche die Abrechnung zwischen Kunde (Zahlungssender) und Kreditkarten-Organisation betreffen (z.B. Abrechnungszeitraum, Kreditrahmen, etc.). Einige *Kreditkarten* können in Verbindung mit einer PIN auch zur POS-Zahlung an automatisierten Kassen verwendet werden, dieser Sachverhalt wird allerdings ebefalls nicht gesondert behandelt (das *POS-System* wird allgemein in Kapitel 7.1 auf Seite 50 behandelt).

[7] Die Bank hat die Informationen über die Zuordnung von Konto zu Person.

Ein Zahlungsvorgang mit *Kreditkarte* führt im Unterschied zur im letzten Abschnitt behandelten Debitkarte nicht zur *unmittelbaren* Belastung des Zahlungssender-Kontos. Die einzelnen Transaktionen werden gesammelt (gleichzeitig stellvertretend bezahlt) und zu einem späteren Zeitpunkt abgewickelt. Zwischen das Konto des Zahlungssenders und das Konto des Zahlungsempfängers ist ein *Zwischenkonto* geschaltet.

Basis eines Zahlungsvorgangs mit einer *Kreditkarte* sind vertragliche Vereinbarungen zwischen Zahlungssender und Kreditkarten-Organisation einerseits und Zahlungsempfänger und Kreditkarten-Organisation andererseits auf der Grundlage des nationalen Rechtssystems. Der Zahlungsempfänger (Händler) verpflichtet sich in einem solchen Vertrag, eine Kreditkartenzahlung (mit der entsprechenden Karte) *an Zahlungs statt* anzunehmen.

Beteiligt an einem Zahlungsvorgang sind die folgenden vier Parteien:

- die Kreditkarten-Organisation als Herausgeber/Anbieter des Systems
- das Vertragsunternehmen (i.A. ein Händler) als Zahlungsempfänger
- der Acquirer[8] als Vermittler zwischen Kreditkarten-Organisation und Händler und gleichzeitig kontoführendes Institut des Händlers
- der Kreditkarteninhaber als Zahlungssender

Eine Kreditkarten-Organisation ist in den allermeisten Fällen keine Bank, der Karteninhaber führt somit kein Guthaben-Konto bei ihr. In bestimmter Frequenz[9] erfolgt die Abrechnung aller mit der Karte getätigten Käufe zwischen Karteninhaber und Kreditkarten-Organisation. Dieser Abrechnungsvorgang erfolgt üblicherweise mit dem Lastschriftverfahren (aus Kapitel 3). Im Rahmen der vertraglichen Vereinbarungen ist die Kreditkarten-Organisation vom Karteninhaber zum Einzug des geschuldeten Betrages von einem seiner bei einer Bank geführten Girokonten autorisiert.

Eine Kreditkarten-Organisation tritt als Dienstleister (gegen Gebühr) bei einem Zahlungsvorgang stellvertretend für den Käufer in einem Zahlungsvorgang als Zahlungssender ein. Der Karteninhaber ist (laut Vertrag) berechtigt, Waren oder Dienstleistungen eines Vertragsunternehmens bargeldlos

[8] Ein Acquirer ist ein Unternehmen, das Akzeptanzstellen für Kreditkartenzahlungen akquiriert: es benötigt für seine Tätigkeit von entsprechender Kreditkarten-Organisation eine Lizenz.

[9] i.d.R. einmal monatlich

durch Unterzeichnung eines Rechnungsbeleges[10] zu beziehen. Durch die Unterschrift (bzw. durch Bekanntgabe der Kartennummer) verweist den Vertragsunternehmer auf die Zahlung durch den Kreditkarten-Herausgeber. Gleichzeitig ermächtigt der Karteninahaber unwiderruflich die Kreditkarten-Organisation die in dem Zahlungsvorgang entstandene Forderung des Zahlungsempfängers gegenüber dem Zahlungssender zu *erwerben*. Diese erworbene Forderung der Kreditkarten-Organisation (über alle mit der Karte in einem bestimmten Zeitraum getätigten Käufe) wird gegenüber dem Käufer in Form einer Rechnung geltend gemacht.

Die Besonderheit des Systems ist der verspätete Zeitpunkt (nämlich der zwischen Zahlungssender und Kreditkarten-Organisation vereinbarte Abrechnungstag), der (strenggenommen) den Zahlungsvorgang erst abschließt, d.h. den Wert letztendlich vom Zahlungssender auf den Zahlungsempfänger überträgt.

Das **Zahlungsrisiko** bei einer Kreditkarten-Zahlung trägt bei Einhaltung der vertraglichen Bedingungen seitens des Karteninhaber die Kreditkarten--Organisation. Die *Allgemeinen Mitgliedschaftsbedingungen* der Karten-Emittenten sehen eine Verpflichtung zum Ersatz der dem Vertragsunternehmen (d.h. dem Zahlungsempfänger) geleisteten Zahlungen nur dann vor, wenn die Unterschrift auf dem vom Vertragsunternehmen vorgelegten Beleg mit der Unterschrift auf der Karte übereinstimmt. Erfolgt der Karteneinsatz unterschriftslos, liegt die Beweislast beim Karteninhaber, daß die Karte von ihm nicht benutzt wurde.

Kreditkarten besitzen eine eingeschränkte Verbreitung, da sie nur an bestimmte Personen mit der von der Kreditkarten-Organisation gewünschten *Kreditwürdigkeit* vergeben werden (bekannter Werbeslogan: *'Bezahlen Sie mit Ihrem guten Namen'*). Ebenso akzeptiert nur ein Teil der Händler als Zahlungsempfänger die Kreditkarten-Zahlungsmöglichkeit. Ein Händler muß sogenanntes *Vertragsunternehemen* der entsprechenden Kreditkarten-Organisation auf Grundlage einer vertraglichen Übereinkunft sein. Des weiteren ist ein *Händlerterminal* analog zu einer automatisierten Kasse beim *POS-System* auf der Seite des Zahlungsempfängers erforderlich. Die Zahlungsmittel-Funktion ist somit eingeschränkt. Zentraler Aspekt bei diesen Systemen ist die zusätzliche, explizite Kreditfunktion.

[10] In Abstimmung mit dem Vertragsunternehmen kann der Vorgang auch unterschriftslos allein mit Bekanntgabe der Kartennummer als einzigem Authentifizierungsmerkmal erfolgen. Beweislast (und damit das Zahlungsrisiko) trägt in diesem Fall allerdings das Vertragsunternehmen. Es muß bei Widerruf der Zahlung nachweisen, daß der Karteninhaber als alleiniger rechtmäßiger Benutzer der Karte den Vorgang ausgeführt hat.

Das generelle Verfahren einer Kreditkarten-Zahlung mit üblicher Online-Autorisierung der Zahlung durch die Kreditkarten-Organisation ist im folgenden aufgelistet:

- Der Karteninhaber händigt dem Zahlungsempfänger (Händler) seine Karte aus.
- Der Händler bringt die Karte mit seinem Händlerterminal in Verbindung und gibt zusätzlich den vereinbarten Betrag ins Terminal ein.
- Die Kreditkartendaten und der Betrag werden vom Terminal zur Vertragsbank des Händlers (Acquirer) als Anfrage zur Autorisierung der Zahlung (Autorisierung somit zum Zeitpunkt des Kaufs) transferiert.
- Der Acquirer sendet die Anfrage-Daten weiter zum kartenausgebenden Institut (Kreditkarten-Organisation des Zahlungssenders).
  Die übermittelte Kartennummer enthält Informationen über den Typ der Karte, über die Kreditkarten-Oganisation und über das Kartenkonto (und somit die Zuordnung zum Karteninhaber).
- Wenn das kartenausgebende Institut Kredit für den zu zahlenden Betrag gewährt, generiert es zur Autorisierung der Zahlung einen Autorisierungs-Code und sendet diesen zurück an den Acquirer des Händlers. Das kartenausgebende Institut speichert auf dem entsprechenden Kartenkonto den Betrag (dieser wird aber erst zu einem späteren Zeitpunkt automatisch von dem Bankkonto des Kartenbesitzers auf dem Wege des Lastschriftverfahrens eingezogen).
- Der Acquirer bestätigt dem Händler die Autorisierung (bzw. nicht erfolgte Autorisierung) des Zahlungsvorgangs dem Händlerterminal (dieses hat eindeutige Terminal-ID, mit dessen Hilfe die *Zustellung* der Nachricht möglich ist).
- Falls die Autorisierung vorliegt, wird ein Zahlungsbeleg vom Händler-Terminal ausgedruckt und vom Käufer unterschrieben[11]. Die Unterschrift weist das Karten-emittierende Institut zur stellvertretenden Zahlung des Betrages an den Händler an.
- Zu einem späteren Zeitpunkt vergleicht der Händler alle im Terminal gespeicherten Autorisierungs-Codes mit den unterschriebenen Zahlungsbelegen und transferiert die einzelnen, übereinstimmenden Transaktions-Daten zum Acquirer zur Gutschrift. Dieser elektronische Weg entspricht dem (manuellen) Einreichen der unterschriebenen Belege beim Acquirer.

[11] ...oder in Vereinbarung mit dem Händler nicht unterschrieben wird, falls er den zusätzliche Authentifizierungs-Nachweis des Karteninhabers nicht für erforderlich hält

- Der Acquirer vollzieht einen sogenannten *Interchange* für jede Einzelzahlung mit dem jeweiligen Karten-emittierenden Institut. Es wird jeweils zum Acquirer einer der (Einzel-)Zahlung entsprechender Geld-Bertag transferiert (abzüglich einer Gebühr).

- Der Acquirer schreibt daraufhin dem Händlerkonto die Summe aller Zahlungsbeträge abzüglich einer Gebühr (*discount fee*) gut. Der Zahlungsempfänger hat zu diesem Zeitpunkt *sein Geld* aus dem Zahlungsvorgang erhalten.

- Die Forderung des Karten-emittierenden Instituts gegenüber dem Karteninhaber als dem eigentlichen Zahlungssender über die in dem vereinbarten Zeitraum mit der Karte getätigten Käufe wird üblicherweise mittels Lastschriftverfahren (s. Kap. 3) ausgeglichen. Mit diesem letzten Prozeß sind alle durch den Zahlungsvorgang entstandenen Forderungen beteiligter Parteien erfüllt; der Geldtransfer zwischen Zahlungssender und Zahlungsempfänger ist beendet.

7.3 GeldKarte

Im Gegensatz zur Telefon-(Chip-)Karte, bei der Kartenemittent und Zahlungsempfänger identisch sind[12], handelt es sich bei der *GeldKarte* um ein multifunktionales *stored value card*-Zahlungssystem.
Geldtransfers zwischen Privatpersonen bietet das System nicht, es ist ausschließlich auf Kunde-Händler-Situationen beschränkt. Zahlungssender und Zahlungsempfänger haben jeweils unterschiedliche Systemkomponenten, auf der einen Seite die *'aufladbare' Kundenkarte* und auf der anderen das *Händlerterminal*. Die *Kundenkarte* trägt zur Identifizierung eine eindeutige Kartennummer in elektronisch gespeicherter Form, allerdings keine Information über die Person des Karteninhabers. Der Name des Inhabers des der Karte zugeordneten Kontos ist sichtbar auf der Oberfläche der Karte vermerkt. Das Händlerterminal enthält hingegen alle Informationen über die Kontoverbindung der Person des Händlers. Alle in Empfang genommenen Zahlungsbeträge werden auf diesem definierten Girokonto gutgeschrieben.
Bei einem Zahlungsvorgang in minimaler Umgebung sind die drei Parteien Zahlungssender (Kunde), Zahlungsempfänger (Händler) und die Bank zusammen mit mehreren zwischengeschalteten Organisations- und Kontrollinstanzen[13] beteiligt.

Voraussetzung für die Funktionalität des GeldKarten-Systems sind jeweils

[12] Eine Telefonkarte als klassische *single-purpose-card* repräsentiert eine bestimmte Anzahl im eigentlichen Sinn mit Erwerb der Karte *vorausbezahlter* Telefoneinheiten.

[13] Börsenevidenz- und Ladezentrale sowie ein Netzbetreiber zum Zweck der DFÜ

vertragliche Bindungen zwischen Zahlungssender und Bank sowie Zahlungsempfänger und Bank. Beide Parteien müssen ein Girokonto bei der Bank führen.
Ein Zahlungsvorgang geschieht in vier voneinander unabhängigen, asynchronen Prozessen, die *in sich* streng sequentiell ablaufen. Am Anfang steht der vom Zahlungssender ausgelöste *Ladevorgang* über den für den anschließenden *Bezahlvorgang* ausreichend hohen Zahlbetrag[14], es folgt der *Abrechnungsvorgang*, das Einreichen der Zahlungsdaten seitens des Zahlungsempfängers bei der Bank und schließlich der eigentliche Geldtransfer bei der Bank, der *Buchungsvorgang* in Form einer Buchungstransaktion zwischen den beiden Girokonten.
Im folgenden sind die Prozesse einzeln aufgeführt.

Der Ladevorgang Der Zahlungssender authentifiziert sich an einem bankeigenen *Ladeterminal* als rechtmäßiger Benutzer der in seinem Besitz befindlichen Karte (und gleichzeitig als Inhaber des der Karte eindeutig zugeordneten Girokontos), indem er die zu der Karte gehörende PIN eingibt (und somit das geheime Wissen des Kontoinhabers als einzig legitimer Person für den Ladevorgang nachweist). Genauso wie beim POS-System handelt es sich bei der PIN lediglich um eine vierstellige Dezimalzahl, also keiner wirklichen *Identifizierung* des Kontoinhabers. Die eindeutige Zuordnung der Karte zur Person des Kontoinhabers geschieht wie beim *POS-System* durch die vertraglich festgehaltene Geheimhaltungspflicht der *PIN* seitens das Zahlungssenders. Der Ladevorgang ist somit ausschließlich von der Person des Kontoinhabers ausführbar. Beim Ladevorgang wird parallel zur Erhöhung des Karten-Zählerstandes der Ladebetrag vom Girokonto des Zahlungssenders auf ein Sammelkonto bei der Bank, das *Börsenverrechnungskonto (BVK)*, gebucht.

Die im folgenden aufgeführte Darstellung der Abfolge der Verfahrensschritte bei einem Karten-Ladevorgang mit einer kontogebundenen *GeldKarte*[15] bezieht sich aufgrund fehlender Informationen über das konkrete *GeldKarten-System* auf die Darstellung eines allgemeinen Chipkarten-Ladevorgangs, dargestellt in dem Buch [Rankl u. Effing, 1996]. Es geht somit um das dem *GeldKarten-System* ähnliche *Prinzip* eines Ladevorgangs mit Online-Verbindung zu einer *Ladezentrale*.

- Die Karte wird in das Ladeterminal eingegeben und ein elektrischer Ver-

[14] Die Betrachtung berücksichtigt nicht die Tatsache, daß dieser Prozeß bei der Durchführung von mehreren Zahlungsvorgängen nicht notwendigerweise jedesmal ausgeführt werden muß. Falls der Kundenkarten-Zählerstand für einen weiteren Bezahlvorgang mit bestimmtem Betrag ausreicht, so entfällt der Aufladevorgang.

[15] Es existiert auch eine eigenständige *GeldKarte* in kontoungebundener Form, allerdings wird diese hier aufgrund geringer Verbreitung nicht näher betrachtet.

bindungsaufbau zwischen Karte und Terminal wird hergestellt.

- Als Antwort auf ein Reset-Signal des Terminals sendet die Karte Informationen für den nachfolgenden Kommunikationsablauf.
- Der Karteninhaber bekommt die Aufforderung zur Eingabe der PIN und des Ladebetrages vom Terminal.
- Die eingegebenen Daten werden an die Ladezentrale übermittelt und Ladebetrag und PIN hin überprüft.
- Die Ladezentrale sendet das Ergebnis der Überprüfung an das Terminal zurück.
- Das Terminal sendet die von der Ladezentrale erhaltenen Daten zusammen mit dem zu ladenden Betrag und einem speziellen *Initialisierungsbefehl* an die Karte.
- Die Karte prüft auf eine mögliche Überschreitung des Karten-Maximal-Saldos durch den zu ladenden Betrag. Falls dies nicht der Fall ist, sendet sie einen (selbst errechneten) Sitzungsschlüssel, eine (selbst errechnete) Signatur, den Stand des Transaktionszählers und verschiedene andere Daten an das Terminal.
- Das Terminal leitet die Daten weiter an die Ladezentrale.
- Die Ladezentrale überprüft die erhaltenen Daten auf gültigen Wertebereich und erzeugt kartenindividuellen Schlüssel und Sitzungsschlüssel. Ein übereinstimmender Vergleich der übermittelten Kartensignatur und des kartenindividuellen Schlüssels authentisieren die Karte gegenüber der Ladezentrale (bzw. Terminal). Somit erfolgt die Authentifizierung der Karte mit dem Wissen um den (geheimen) Kartenschlüssel.
- Die Ladezentrale erzeugt daraufhin eine eigene Signatur, die über das Terminal, welches das Auflade-Kommando hinzufügt, zur Karte gesendet wird.
- Die Karte benutzt zur Authentitätsprüfung des Terminals die erhaltene Signatur und erhöht bei positivem Ergebnis den Karten-Saldo um den vom Karteninhaber gewünschten Betrag.
- Die Karte erzeugt eine weitere Signatur, die übermittelt ans Terminal und weiter an die Ladezentrale die erfolgreiche Aufladung bestätigt. Die Ladezentrale schickt eine Nachricht an die Bank (das Karten-emittierende Institut) mit den Informationen des Ladevorgangs, so daß die entsprechenden Buchungstransaktionen zwischen Girokonto des Zahlungssenders und Börsenverrechnungskonto (BVK) der Bank *vorgemerkt* und

beim nächsten Buchungsschnitt ausgeführt werden (dem BVK wird der Ladebetrag gutgeschrieben und gleichzeitig das Girokonto des Zahlungssenders mit demselben Betrag belastet).

Die Ladezentrale benachrichtigt daraufhin die zuständige Börsenevidenzzentrale über den abgeschlossenen Ladevorgang und diese aktualisiert entsprechend bei der Börsenevidenzzentrale das kundenkartenindividuelle Schattenkonto sowie das BVK-Schattenkonto für die Bank. Dieser letzte Schritt dient System-Kontroll-Zwecken[16], wird aber auch benötigt zur Wiederherstellung von defekten Hardware-Komponenten im System (vor allem der *Kundenkarten*) zur Erstattung des Karten-Restguthabens. Sonst wäre allein im Speicher der *Kundenkarte* die Ladesumme dokumentiert und es müßte für die Benutzer zur Wahrung des Vertrauens in das System die Ausfallsicherheit dieser Komponente garantiert sein.

Wie bereits erwähnt wird beim Ladevorgang keine im Sinne von *Geld* in sich Wert tragende Information auf die Karte übertragen, sondern ein vom Kartenemittenten einzulösendes *Zahlungsversprechen* in definierter Höhe. Der *Gegenwert* dieses Zahlungsversprechens verbleibt beim Kartenemittenten (der Bank) als erhöhter Saldo des BVK.

Der Bezahlvorgang Im Unterschied zum ersten Prozeß des GeldKarten-Ladevorgangs erfolgt beim zweiten die Authentifizierung eines rechtmäßigen Benutzers allein durch den Besitz der physikalischen Karte; der Benutzer kann folglich während eines Zahlungsvorgangs an dieser Stelle zwischen Lade- und Bezahlvorgang wechseln. Beteiligt am Bezahlvorgang sind ausschließlich der Karten-Benutzer und der Händler (mitsamt Händler-Terminal).

Das prinzipielle Verfahren des Zahlungsvorgang zwischen Karte und Terminal (zwischen Käufer und Händler) wird im folgenden aufgelistet[17]. Das Terminal beinhaltet ein sogenanntes Sicherheitsmodul, in dem das General-Kartengeheimnis und das eigene Terminal-Geheimnis für die gegenseitige Authentifizierung der System-Komponenten gespeichert ist.

- Die *Kundenkarte* wird mit dem Händlerterminal in Verbindung gebracht: Einschieben der Karte in Schacht und Herstellung einer Verbindung zwischen elektrischen Kontakten der Karte und des Terminals.
- Das Terminal sendet einen speziellen Initialisierungsbefehl für die Bezahlprozedur an die Karte.

[16] z.B. unautorisierte Systemaktivitäten wie das Erhöhen von Kundenkarten-Zählerständen

[17] Die Angaben beziehen sich wie beim ersten Prozeß des *Ladens* auf die in [Rankl u. Effing, 1996] beschriebene prinzipielle Verfahrensweise.

- Die Karte erhöht daraufhin einen Transaktionszähler und erzeugt eine digitale Signatur über verschiedene Datenelemente und sendet diese an das Termial.
- Das Terminal überprüft die Daten (Ablaufdatum der Karte, verwendeter kryptographischer Algorithmus) und erhöht bei positivem Ergebnis den übermittelten Transaktionszähler. Der kartenindividuelle Schlüssel wird mit dem eigenen Karten-*Generalschlüssel* errechnet und die Authentizität der Karte durch Vergleich mit der erhaltenen Sigantur geprüft. Bei einer Übereinstimmung sind sowohl übergebene Daten als auch Karte gegenüber dem Terminal (bzw. dem Hintergrundsystem) für echt befunden.
- Es folgen die Eingabe des zu transferierenden Zahlungs-Betrages ins Terminal und eine eventuelle Bestätigung des Betrages durch den Karten-Benutzer.
- Das Terminal sendet DEBIT-Kommando zusammen mit eigener Signatur und Zahlbetrag an die Karte.
- Die Karte prüft, ob der aktuelle Zählerstand zum Bezahlen des gewünschten Betrages ausreicht. Falls ja, wird die Signatur des Terminals (bzw. des Hintergrundsystems) geprüft. Bei positivem Ergebnis ist die Daten-Integrität gewährleistet und das Terminal gegenüber der Karte authentisiert.
- Im Speicher der Karte wird der Betrag vom aktuellen Zählerstand subtrahiert.
- Eine weitere Signatur wird erzeugt und zusammen mit Zahlbetrag, Kartennummer und Transaktions-ID zum Terminal gesendet zur Bestätigung der erfolgreichen Kartenkonto-Belastung.
- Ist die Signatur der übermittelten Transaktionsdaten korrekt, so werden sie im Terminal gespeichert.
- Der Terminal-Zählerstand wird um den Betrag erhöht.
- Der Bezahlvorgang ist beendet; die Karte wird dem Terminal entnommen.

Der Abrechnungsvorgang Der Händler leitet zu einem durch das System nicht vorgegebenen Zeitpunkt[18] einen sogenannten *Kassenabschluß* ein und die

[18] Üblich ist, daß der Händler jeweils abends diesen Vorgang auslöst oder der Vorgang immer nach 10 erfolgten Zahlungsvorgängen vom Terminal automatisch eingeleitet wird.

hieraus resultierende Zahlungsdatei mit den zusammengefaßten Transaktions-Informationen wird über die vermittelnde Instanz einer *Buchungszentrale* an die Bank gesendet. Bevor die Daten bei der Bank eintreffen und anschließend bei nächstem Buchungsschnitt der Buchungsvorgang zwischen den Konten erfolgen kann (der eigentliche Geldtransfer), werden die Daten bei der Buchungszentrale mit Hilfe kryptographischer Verfahren auf gefälschte bzw. verfälschte Beträge und auf Mehrfacheinreichung derselben Daten geprüft. Außerdem werden die Börsenevidenzzentrale von den einzelnen Zahlungsvorgängen in Kenntnis gesetzt und die betreffenden Schattenkonten entsprechend aktualisiert.
Bei nächstem *Buchungsschnitt* werden bei der Bank alle im letzten Intervall eingegangenen Transaktions-Daten verarbeitet und so der aus dem Abrechnungsvorgang *vorgemerkte* Zahlungsbetrag dem Händler-Girokonto gutgeschrieben sowie das BVK um denselben Betrag belastet.

Das BVK dient im System als ein keiner (Einzel-)Person zugeordnetes Sammelkonto mit der Dokumentation der Summe aller Kundenkarten- und Händlerterminal-Zählerstände. Im GeldKarten-Zahlungssystem ist zu jedem Zeitpunkt die verwendete Gesamt-Geldmenge in den Händen der Bank: Es fließt keine Liquidität von der Bank ab. Die Verbindlichkeiten der Bank gegenüber den Benutzern des GeldKarten-Systems wechseln lediglich in ihrer *Dokumentation*. Sind vor dem Zahlungsvorgang alle Verbindlichkeiten in den Salden der beiden beteiligten Girokonten repräsentiert, so sind sie während eines Zahlungsvorgangs in Form der einzelnen Kundenkarten- und Händlerterminal-Zählerstände dokumentiert[19].
Die Karten mit den auf ihnen gespeicherten Zählerständen erfüllen ausschließlich eine Nachweisfunktion im System, der einzige Zweck ist die Repräsentation eines *Verfügungs-Höchstbetrages*[20] über einen Teil des im Saldo des BVK gespeicherten Geldbetrages. Der eigentliche Geldtransfer geschieht im System nicht beim Übertragen elektronischer Daten zwischen Zahlungssender und Zahlungsempfänger, dem *Bezahlvorgang* (s.o.), sondern bei der vom vermittelnden Geldinstitut realisierten Buchungstransaktion zwischen den Konten der beiden Parteien.

Ein wesentlicher Unterschied zwischen den Systemkomponenten *Kundenkarte* und *Händlerterminal* ist, daß die im Zählerstand der *Kundenkarte* dokumentierte Verbindlichkeit keiner Person zugeordnet ist. Ein Händlerterminal steht dagegen in direkter Verbindung zum Girokonto des Händlers und folglich zur Person des Händlers als Kontoinhaber.

[19]Die Schattenkonten bei der Börsenevidenzzentrale dienen nur der Systemkontrolle und zur Sicherheit der Benutzer bei defekten Karten.

[20]Eigene Formulierung, denn es gibt seitens der Kreditwirtschaft keine Bezeichnung für die Variable im Speicher der Karte.

Kapitel 8

Simuliert die GeldKarte Geld ?

Aufbauend auf der Beschreibung des *GeldKarten*-Systems im letzten Abschnitt 7.3 soll nun der Frage der Zweckdienlichkeit des Systems nachgegangen werden.

Die Fragestellung, ob die Zweckdienlichkeit dieses komplexen, technischen Systems gegeben ist, hat in dieser theoretischen Betrachtungsweise als Vergleichsobjekt das Bargeld in Form in sich Wert tragender Token. Banknoten und Münzen wechseln in einer Gesellschaft zwischen System-Benutzern ihren Besitzer zum Zwecke der Wertübertragung. Die Forderung an das *GeldKarten*-System ist hierbei, daß es die Rahmenbedingungen und Eigenschaften des herkömmlichen Geldes und somit seinen eigentlichen Zweck erfüllt.

Die folgende theoretische Betrachtungsweise bedient sich des klassischen Informatik-Modells der virtuellen Maschine. Innerhalb des abstrakten Modells einer virtuellen Maschine wird ein System vereinfachend innerhalb von Datenstrukturen und auf ihnen definierten Instruktionen formal beschrieben. Es werden alle im betreffenden Welt-Ausschnitt relevanten variablen und konstanten Objekte erfaßt zusammen mit den auf ihnen möglichen Aktionen.

Dementsprechend wird nicht das *Phänomen Geld* formalisiert[1], wie es sich vor allen Dingen in Kapitel 2.1 dargestellt hat, sondern ausschließlich die mit dem Untersuchungsgegenstand des Zahlungsvorgangs verbundene formalisierbare *soziale Aktivität*. Allein das Verfahren einer Wertübertragung wird formal beschrieben. Sowohl ein technisches Zahlungssystem als auch Geld an sich besitzen fest vorgegebene Handlungs-Möglichkeiten, Aktionen, die von Benutzern, die das Ziel einer Wertübertragung auf eine andere Person haben, ausgeführt werden müssen.

[1] das wäre ein sehr anspruchsvolles Ziel für eine andere Ausarbeitung

Das *Zahlungssystem GeldKarte* kann man sich in drei aufeinander aufsetzenden Abstraktionsebenen vorstellen, als drei hierarchisch geordnete virtuelle Maschinen. Auf der untersten Ebene befindet sich die konkrete Implementierung des Systems in Form von Datenstrukturen und Instruktionen einer Programmiersprache. Die Ausführung dieser Programme ist die Realisierung des aus einer Menge von miteinander kommunizierenden Komponenten bestehenden Gesamtsystems. Zu dieser Ebene gehören unter anderem die Programme der Rechenzentren der Banken und die Protokolle eines Auflade- bzw. Bezahlvorgangs, der sich zwischen Kundenkarte und Aufladeterminal bzw. Kundenkarte und Händlerterminal abspielt[2]. Für den Benutzer ist diese Ebene vollständig verborgen.
Die darüberliegende virtuelle Maschine ist das GeldKarten-*System, wie es sich Benutzern und Bankangestellten präsentiert.* Ein Benutzer ist bei einem Zahlungsvorgang im Besitz der *Kundenkarte* und kann hiermit bestimmte Aktionen ausführen, deren Effekt am Terminal-Display oder Kontoauszug wahrnehmbar ist. Ein zweiter System-Benutzer kann mit der in seinem Besitz befindlichen Systemkomponente 'Händler-Terminal' Zahlungen in Empfang nehmen. Zu dieser Benutzeroberfläche des *GeldKarten*-Systems zählen außerdem Informationen aus der Öffentlichkeitsarbeit bzw. Werbung der Kreditwirtschaft als Anbieter des Systems.

Die höchste der drei Abstraktionsstufen ist in dieser Sichtweise das System *Geld* an sich. Wie bereits erwähnt, wird als Referenzobjekt das herkömmliche Bargeld gewählt. Die Eigenschaften von Bargeld im Hinblick auf seine Wertübertragungsfunktion sollten auf das System *GeldKarte* ebenfalls zutreffen.

Aus dieser Perspektive besitzt die virtuelle Maschine *Geld* eine festgelegte Prozeßhaftigkeit, die sie den Benutzers in Form von möglichen Aktionen zum Zweck einer Wertübertragung bietet. Ein *System-Benutzer* besitzt als wesentliche Möglichkeit die Aktion des *Zahlens*. Er kann einen abstrakten *Wert* auf eine andere Person im System übertragen. Die Voraussetzung hierfür ist die Durchführung der Aktion *Geld-Abheben* bei dem (zentralen) Emittenten, der gleichzeitig die Funktion des Geldemittenten als auch die Verwahrungsfunktion für die im System befindlichen hinterlegten Werte erfüllt.

Die Frage ist, ob das *System GeldKarte* aus Benutzersicht, also der zweiten der oben erwähnten Abstraktionsebenen, das *System Geld* simuliert. Präziser formuliert geht es um die Frage, *ob das gesellschaftliche Verfahren eines Bargeld-Zahlungsvorgangs durch das - technische - GeldKarten-System simuliert wird.*
Eine Beantwortung dieser Frage läßt sich auf der Grundlage der bereits erwähnten virtuellen Maschinen mit Hilfe von formalen Beschreibungsmitteln der In-

[2]Hierauf wird in Kapitel 7.3 näher eingegangen.

formatik herbeiführen. Die Hierarchie von zwei formal definierten Abstraktionsebenen in Form der virtuellen Maschinen ist die Basis der Überprüfbarkeit der Fragestellung in diesem Abschnitt. An diesem Punkt setzt die Möglichkeit eines mathematischen Beweisverfahrens an.

Anfangs wird jeweils eine formal-logische Spezifikation für jedes der beiden Systeme erstellt. Auf Basis dieser beiden formalen Beschreibungen läßt sich mathematisch beweisen, ob in der oben genannten Sichtweise die konkretere der beiden Spezifikationen[3] (die Spezifikation des Systems *GeldKarte*) die abstraktere[4] (die Spezifikation des Systems *Geld*) impliziert. Die bewiesene logische Implikation ist gleichbedeutend mit der Aussage, daß die konkrete Maschine die abstrakte *simuliert*. Die beiden Spezifikationen beinhalten ausschließlich die Beschreibung der beiden Systeme im Hinblick auf das Verfahren eines bzw. mehrerer Zahlungsvorgänge in einer minimalen Umgebung. Beteiligt ist jeweils ein Zahlungssender, ein Zahlungsempfänger und das Geldinstitut, das im Anfangszustand im Besitz der gesamten hinterlegten Geldmittel ist. Ein Zahlungsvorgang ist abgeschlossen, wenn der zu transferierende Wert, also *das reale Geld*) in den Besitz des Zahlungsempfängers übergegangen ist.

Als formales Beschreibungsmittel der Systeme bietet sich die *Temporale Logik der Aktionen (TLA)*[5] zusammen mit der auf ihr aufsetzenden Spracherweiterung *TLA+* an. Die formale Logik TLA ist hierbei die mathematische Basis für die formale Logik-*Sprache* TLA+. Mit Hilfe der in ihrem Sprachumfang enthaltenen Operatormenge und einer Modulstruktur (siehe [Lamport, 1996] und [Lamport, 1997]) können die in der Betrachtung relevanten Eigenschaften der beiden Systeme *GeldKarte* und *Geld* programmiersprachennah exakt beschrieben werden.
Die beiden Spezifikationen befinden sich im Anhang dieser Arbeit ab Seite 78.

Spezifikationen in TLA+ beschreiben ein System als *Zustands-Machine*. Es wird eine logische Aussage über alle möglichen zukünftigen Zustände des Systems macht. Eine Spezifikation beginnt mit der Definition aller Variablen und Konstanten und deren Initialisierung. Die Definition der Aktionen legt für das System alle möglichen Zustandsübergänge fest. Eine Aktion spezifiziert die Relation zwischen einem Zustand und seinem Nachfolgezustand mit der Angabe über Wert-Änderungen aller in der Spezifikation enthaltenen Variablen. So ist gewährleistet, daß keine undefinierten Bereiche in einer System-Spezifikation existieren.

[3] im folgenden 'die konkrete Spezifikation' genannt
[4] im folgenden 'die abstrakte Spezifikation' genannt
[5] siehe [Lamport, 1994]

In den beiden Spezifikationen der Systeme *Geld* und *GeldKarte* sind alle relevanten Variablen und Konstanten enthalten, sowie die Definition der den Benutzern gebotenen Aktionen zur Durchführung einer Wertübertragung. Außerdem wird eine Aussage über die *notwendigen* Aktionen zur finalen Durchführung eines Zahlungsvorgangs in Form von sogenannten Liveness-Eigenschaften des Systems getroffen. Es wird definiert, welche Aktionen ausgeführt werden müssen, um das Ziel einer Wertübertragung zu erreichen.

Da es sich bei TLA+ um eine formale Logik-Sprache handelt, beinhaltet TLA+ automatisch die Möglichkeit eines mathematischen Beweises. Mit Anwendung der in [LADKIN, 1997] beschriebenen Regelmenge zusammen mit einem Beweisverfahren kann daraufhin der mathematische Beweis geführt werden. Er betrifft die logische Implikation der beiden Spezifikationen. Das Überprüfen der oben genannten Fragestellung besteht darin, mit den beiden aufgestellten Spezifikationen einen mathematischen Beweis der logischen Implikation durchzuführen. Zentrale Frage ist, ob alle abstrakten Datenstrukturen und Aktionen der einen Spezifikation durch die konkreten Datenstrukturen und Aktionen der anderen Spezifikation definiert sind.

Das Beweisverfahren benutzt hierzu die Methode des sogenannten *refinement mappings*. Alle Variablen der Spezifikation der abstrakten Maschine werden durch Terme von freien Variablen der Spezifikation der konkreten Maschine ersetzt als rein syntaktischer Vorgang. Daraufhin wird der Beweis der logischen Folgerung geführt. Falls im obigen Fall von *Geld* und *GeldKarte* gilt, daß die konkrete Spezifikation des Systems *GeldKarte* die abstrakte Spezifikation des Systems *Geld* impliziert, also

$$\mathrm{GeldKarte(Vars).Spec} \Rightarrow \mathrm{F(Geld(Vars).Spec)}$$

gilt, so *simuliert die GeldKarte Geld*. Die Funktion F ist hierbei die Abbildung der Variablen der abstrakten Spezifikation auf Terme von Variablen der konkreten Spezifikation.

Die Durchführung des Beweises übersteigt allerdings den Rahmen dieser Ausarbeitung. Der Beweis kann an anderer Stelle mit einem automatischen Beweiser durchgeführt werden, den es zur Zeit für TLA noch nicht gibt.

Die formalen System-Spezifikationen von *Geld* und *GeldKarte* enthalten einige **Vereinfachungen**, die den tatsächlichen Gegebenheiten *in der realen Welt* nicht entsprechen. Der Grund für die vorgenommenen Vereinfachungen ist, daß die Formulierung der exakten Sachverhalte die Spezifikation erheblich komplizierter machen würde, ohne am angestrebten Ziel der Beschreibung des jeweiligen System-Prinzips etwas zu ändern bzw. etwas dazu beizutragen. In den folgenden Beschreibungen der beiden System-Spezifikationen wird auf diesen Aspekt für jede Spezifikation einzeln eingegangen. Annahme in beiden

Spezifikationen ist, daß die Gesamt-Geldmenge im Systems konstant ist[6]

Das System GeldKarte Als erster Unterschied zum *realen GeldKarten-System* werden in der Spezifikation[7] keine Schattenkonten[8] berücksichtigt, da sie nur Kontrollfunktion im System erfüllen und das Prinzip eines Zahlungsvorgangs nicht betreffen.
Eine zweite, wichtige Vereinfachung geht einher mit der Beschreibung der *Zeit* innerhalb der Spezifikation. Alle Aktionen außer *Bank.Batch* sind so spezifiziert, als ob sie *augenblicklich* geschehen würden. In der realen Welt sind dagegen in einem bestimmten Zeitraum (ein Tag beispielsweise) nicht unendlich viele Aktionen möglich, jede Aktion nimmt eine bestimmte - wenn auch kurze - Zeitdauer in Anspruch. Die im Modul *Time* spezifizierte Zeit fließt in der System-Spezifikation nur in das Modul *Bank* mit ein, da die strenge Periodik des Abarbeitens der gesammelten Buchungstransaktionen (des sogenannten Buchungsschnitts) wesentlich für das Prinzip eines Zahlungsvorgangs ist. Ein Zahlungsvorgang ist erst abgeschlossen, wenn die entsprechenden bei der Bank eingegangenen Transaktionsinformationen zum Zeitpunkt des nächsten Buchungsschnitts abgewickelt wurden und der Zahlungsempfänger den Zahlungsbetrag auf seinem Girokonto gutgeschrieben bekommen hat.
Die entsprechende Aktion *Bank.Batch* berücksichtigt nicht die Implementierung der bei der Rechenzentrale der Bank tatsächlich ausgeführten Aktionen zu diesem Zweck. Die Spezifikation beschreibt den Buchungsschnitt so, als würden alle im letzten Intervall (dem Zeitraum zwischen zwei Buchungsschnitten) bei der Bank eingegangenen Transaktionsdaten innerhalb eines Zustandsüberganges abgewickelt (mittels der Aktion *Bank.AllTransaktions*). Der Frage, wie dieser Vorgang genau bei den Rechenzentren erfolgt, wurde im Rahmen dieser Arbeit nicht nachgegangen, da das Ziel die Spezifikation der Benutzeroberfläche des Systems ist.
Zur Modellierung des periodischen Buchungsschnitts enthält die Variable *buffer* eine Liste von Tupeln. Jedes Tupel enthält alle zur Durchführung einer Buchungstransaktion nötigen Informationen (Annahme in der Spezifikation ist: die drei Komponenten Quelle, Ziel und Betrag der Buchung). Wie bereits erwähnt, wird in der zeitabhängigen Aktion *Bank.Batch* diese Liste der gesammelten Transaktionsinformationen in *einem* Zustandsübergang vollzogen.

Die Beschreibung des Moduls *Bank* als einziges zeitabhängiges Modul stimmt außer in dem genannten Punkt noch in anderer Hinbsicht nicht überein mit den realen Gegebenheiten. Da es sich beim *GeldKarten*-System um ein reines Kunde-Händler-Zahlungssystem handelt, ist nach *Ladenschluß* keine Bezahl-

[6] Daß dies in der realen Welt nicht so ist, wird in [Blaug *et al.*, 1995] eingehend behandelt.

[7] siehe Anhang A

[8] Schattenkonten werden bei der Börsenevidenzzentrale geführt (Abschnitt 7.3).

Aktion (*Sender.Trans*) mehr möglich. *Sender.Load* und *Recipient.Clear* können demgegenüber sowohl in der Spezifikation als auch im realen System 24 Stunden am Tag stattfinden.

Die Aktion *GeldKarte.ChangeUser* beschreibt die im System enthaltene Möglichkeit der Übertragung der *Kundenkarte* zwischen zwei Personen während eines Zahlungsvorgangs. Es kann zwar nur der Kontobesitzer als einzige Person, die laut der Allgemeinen Geschäftsbedingungen (AGB) des Kartenemittenten das Wissen um die *PIN* hat, die Aktion *Sender.Load* durchführen, aber die darauffolgende Bezahl-Aktion *Sender.Trans* kann durch eine andere Person ausgelöst werden. Für die Bezahl-Aktion ist nur der Besitz der Karte erforderlich; es findet keine zusätzliche Authentifizierung des Benutzers statt. In der TLA+-Spezifikation spiegelt sich dieser Sachverhalt wider in der möglichen *GeldKarte.ChangeUser*-Aktion (nachdem die Karte aufgeladen wurde), bei der die Variable *user* eventuell ihren Wert ändert. Der Wertebereich ist vereinfacht definiert durch vier verschiedene Buchstaben, die exemplarisch vier mögliche Benutzer mit Zugriff auf die Karte (also etwa der Bekanntenkreis des Karteninhabers) repräsentieren. Genauso gut kann aber auch der Finder einer verlorenen Karte innerhalb des auf der Karte gespeicherten Verfügungsrahmens Käufe tätigen. Diese Eigenschaft des Systems ist analog zum Bargeld und somit analog zur Spezifikation des Systems *Geld* im nächsten Abschnitt.

In das System *GeldKarte* sind drei binäre Semaphore eingebunden, um den wechselseitigen Ausschluß verschiedener Aktionen im System zu steuern. Zum einen schließen sich Lade- und Bezahl-Aktion gegenseitig aus. Es kann entweder die Karte aufgeladen werden oder mit ihr an anderer Stelle eingekauft werden. Des weiteren erfolgen Bezahl- und Clearing-Aktion sowie Clearing und Buchungsschnitt niemals parallel. Die Aktion *GeldKarte.ChangeUser* kann nur im wechselseitigen Auschluß-Prinzip mit den beiden Aktionen *Sender.Load* und *Sender.Trans* erfolgen.

Gerade im *Artefakt GeldKarte* – und somit gleichzeitig in der Spezifikation des Systems *GeldKarte* – verdient die *Zweckdienlichkeit* der einzelnen Variablen eine besondere Beachtung. Dieser Punkt betrifft vor allem die in der Einleitung bereits erwähnte zentrale Frage, wo sich zu einem bestimmten Zeitpunkt das *reale* Geld im System befindet. In der Spezifikation sind die Variablen, die einen *Geldwert* repräsentieren, nicht extra kenntlich zu machen. In Analogie zum realen System haben die drei Variablen *giroSend*, *giroRecip* und *bvk* in der Spezifikation die ausschließliche *Geldwert-Bedeutung*; sie repräsentieren die bei der Bank geführten Konto-Salden. Alle anderen Variablen haben den Zweck von Hilfsvariablen zur Durchführung eines Zahlungsvorgangs im System.

Das System Geld Die Spezifikation[9] beschreibt die vereinfachte Situation eines Zahlungsvorgangs bzw. Geldtransfers zwischen zwei Benutzern mit Beteiligung eines Geldinstitutes, welches das im System vorhandene Geld verwahrt und gleichzeitig emittiert. Der Zahlungssender hebt Geld von seinem Konto bei der Bank ab, bekommt Banknoten bzw. Münzen ausgehändigt und transferiert diese zur Person des Zahlungsempfängers. An dieser Stelle ist ein Zahlungsvorgang abgeschlossen, der zu transferierende *Wert* ist in den Besitz des Zahlungsempfängers übergegangen.

Bei der Initialisierung des Systems wird mittels *CHOOSE*-Operator festgelegt, wer im Zahlungsvorgang die Rolle des Zahlungssenders und wer die Rolle des Zahlungsempfängers hat. Davon abhängig sind die möglichen Aktionen der beiden Benutzer des Systems. Der Zahlungssender kann zum Zweck einer Zahlung bzw. eines Geldtransfers eine *Get*- und eine *Pay*-Aktion ausführen, dem Zahlungsempfänger wird mit Ausführung von *Pay* der *Wert* direkt übertragen.

Es gibt in der Spezifikation des Systems *Geld* einen binären Semaphore, die benutzt wird, um den wechselseitigen Ausschluß einer *Abhebe*-Aktion (*GetA* oder *GetB*) und einer Transfer-Aktion (*PayAtoB* oder *PayBtoA*) zu erreichen. Entweder hebt jemand bei der Bank Geld ab oder er zahlt an anderer Stelle damit. Die Reihenfolge zweier dieser Prozesse ist nicht streng abwechselnd. Der Zahlungssender kann beispielsweise einmal Geld abheben und mehrmals damit zahlen oder mehrmals Geld abheben und einmal damit zahlen. Diese Eigenschaft ist durch das wechselseitige Ausschluß-Prinzip der binären Semaphore gegeben.

Analog zum System *GeldKarte* beschreibt die Aktion *cash.ChangeUser* das eventuelle Wechseln des Benutzers während eines Zahlungsvorgangs. Wiederum sind exemplarisch vier verschiedene Personen definiert, auf welche die Person des Kontobesitzers das Zahlungsmittel (die *Kundenkarte*) übertragen kann nachdem der erste Prozeß des Geld-Abhebens von ihm ausgeführt wurde. Die Person des Geld-Abhebenden muß folglich nicht mit der Person des Zahlenden identisch sein.

Vergleich Im Vorgriff auf einen möglichen Beweis der logischen Implikation der beiden System-Spezifikationen lassen sich anhand des Vergleichs der beiden Spezifikationen schon wesentliche Unterschiede zwischen den Systemen festmachen.

- Da ein Zahlungsvorgang beendet ist, wenn das *reale Geld* in den Händen des Zahlungsempfängers angekommen ist, ist vom Zahlungsempfänger bei dem System *Geld* keine weitere Aktion in einem Zahlungsvorgang auszuführen. Der Zahlungssender hält mit den Banknoten und Münzen den eigentlichen Wert in den Händen. Ein Zahlungsempfänger im *Geld*-

[9] in Anhang B

Karten-System muß hingegen die erhaltenen, in seiner System-Komponente gespeicherten 'Transaktionsinformationen' bei der Bank einreichen, um den Zahlungsvorgang abzuschließen.

- Ein Zahlungsvorgang mit dem *GeldKarten*-System ist zeitabhängig, da die finale Zahlung erst mit der Buchungstransaktion erfolgt und diese nicht in Echtzeit von der Bank (bzw. dem Rechenzentrum der Bank) ausgeführt wird.

- Beim System *GeldKarte* ist zu jedem Zeitpunkt die Gesamt-Geldmenge bei der Bank; es fließt bei einem Zahlungsvorgang mit dem System keine Liquidität von der Partei der Bank ab. Dieser Punkt entspricht nicht dem System Geld, wo der Wert durch die Aktion des *Abhebens (GetA oder GetB)* direkt auf den Zahlungssender übertragen wird.

- Das System Geld legt nicht fest, wer Zahlungssender und wer Zahlungsempfänger bei einem Zahlungsvorgang ist, das System *GeldKarte* bestimmt durch die unterschiedlichen Komponenten *Kundenkarte* und *Händlerterminal* die möglichen Aktionen und so die Festlegung der Rollen.

- Die konzeptionsbedingte Beschränkung des *GeldKarten*-System auf Niedrigwertbeträge ist bei Geld nicht gegeben.

Eine wesentliche Übereinstimmung zwischen den beiden betrachteten Systemen ist die des möglichen Wechsels des Benutzers während eines Zahlungsvorgangs. Diese Eigenschaft existiert bei keinem anderen der in dieser Arbeit behandelten Systeme.

Kapitel 9

Schlußbetrachtung und Ausblick

Im vorangegangenen Kapitel 8 wurde untersucht, ob die Rahmenbedingungen und Eigenschaften von Geld in Bezug auf das Verfahren eines Zahlungsvorgangs im *GeldKarten-System* gegeben sind.
Als Ergebnis läßt sich zusammenfassen, daß der Umfang der Eigenschaften des Systems *Geld* im System *GeldKarte* nicht gegeben ist. Gerade die wichtige Eigenschaft des frei in einer Gesellschaft zirkulierenden 'Tauschmittels' ist nicht erfüllt. Ein Zahlungsempfänger im System *GeldKarte* erhält keinen Wert im Zuge eines Transfers von Token, sondern lediglich einen 'Bon', den er beim Emittenten einlösen muß, um den *Wert* zu erhalten. Dies ist die einzig mögliche Aktion für den Zahlungsempfänger. Im System *Geld* ist der Wert durch die Token verkörpert. Der Besitz eines Token beinhaltet die erneute Möglichkeit der Wertübertragung an einen (beliebigen) Benutzer im System.
Außerdem geschieht im *GeldKarten-System* die Wertübertragung im Anschluß an die Aktion des Einreichens zeitabhängig. Erst bei dem nächsten Buchungsschnitt der Bank wird der Giralgeld-Transfer zwischen Zahlungssender und Zahlungsempfänger ausgeführt und der Zahlungsvorgang ist beendet. *Geld* besitzt demgegenüber keine zeitabhängige Komponente.
In dem Vergleich von *Geld* und *GeldKarte* ist deutlich geworden, daß die Zweckdienlichkeit des technischen Systems nicht den eigentlichen Zweck von *Geld* erfüllt. Das *GeldKarten-System* ist reines Zahlungsinstrument und besitzt nur einen Teil der Eigenschaften des Systems *Geld*.

Bei den beiden in Kapitel 6 behandelten Internet-Zahlungssystemen *eCash* und *CyberCoin* liegt das vorrangige Ziel in der Simulation einer Situation, in der sich zwei Personen direkt gegenüberstehen und miteinander zum Zweck einer Wertübertragung kommunizieren. Auch bei diesen Systemen, ebenso wie bei den anderen in dieser Ausarbeitung beschriebenen Systemen, kann die Benutzer-Oberfläche analog zu den Überlegungen beim *GeldKarten-System* untersucht werden. Dieses bietet Raum für weitergehende Untersuchungen an anderer Stelle.

Allgemein ist die in dieser Arbeit vorgeführte Herangehensweise auf alle technischen Systeme übertragbar, die geschaffen wurden, um (soziale) Aktivitäten bzw. Handlungsabläufe zu vereinfachen oder auf effiziente Weise abzubilden. Bei vielen dieser Systeme kann analog einer Beantwortung der Frage nachgegangen werden, ob die Zweckdienlichkeit des Systems tatsächlich dem eigentlichen Zweck aus Benutzersicht entspricht.

Im Vergleich der einzelnen Systeme hat sich herausgestellt, daß sich anhand der Kriterien 'Beteiligte', 'Zuordnung' und 'notwendige Aktionen' nur bedingt ein aussagekräftiges Resultat erzielen läßt. Im Verlauf der Arbeit ist deutlich geworden, daß sich die Konzepte der Systeme in vielen Fällen grundlegend voneinander unterscheiden. Dies soll an zwei Beispielen verdeutlicht werden.

Bei der herkömmlichen *Überweisung* und *Lastschrift* sowie des in Verbindung mit der *Debitkarte* behandelten *POS-Systems* wird die Wertübertragung realisiert mit Hilfe einer von einem Benutzer ausgeführten *Anweisung* an die vermittelnde Bank[1]. Diese Anweisung kann sowohl durch den Zahlungssender im Fall der *Überweisung* als auch durch den Zahlungsempfänger bei der *Lastschrift* und dem *POS-System* erfolgen. Im Anschluß an die erfolgte Anweisung wird von der Bank mittels Buchungstransaktion der entsprechende Wert zwischen den Girokonten von Zahlungssender und Zahlungsempfänger bewegt.

Bei der *Kreditkarte* kommt als charakteristische Eigenschaft eines Zahlungsvorgangs ein 'Zwischenkonto' hinzu. Einzelne Zahlungsvorgänge werden bei einer Kreditkartenzahlung prinzipiell *nicht unmittelbar* ausgeführt, sondern die Informationen über auszuführende Wertübertragungen werden gespeichert und zu einem späteren Zeitpunkt gesammelt abgewickelt.

Ein übereinstimmendes Prinzip weisen demgegenüber *GeldKarte*, *eCash* und *CyberCoin* auf. Es wird jeweils eine Nachweis-Dokumentation das Anspruchs auf einen hinterlegten Wert transferiert. Das technische Prinzip der Realisierung der Dokumentation unterscheidet sich allerdings bei den drei Systemen. Während bei der *GeldKarte* ein portabler, hardwaregesicherter Zählerstand die Funktion erfüllt, sind es bei *eCash* diskrete *elektronische Münzen* und bei *CyberCoin virtuelle Konten*. Die *virtuellen Konten* bei *CyberCoin* haben im Unterschied zu den beiden anderen Systemen die Eigenschaft, daß sie sich nicht im unmittelbaren Besitz des System-Benutzers befinden. Die Zuordnung erfolgt hierbei mittels Personen-Authentifizierung durch die notwendige Software seitens des Benutzers und darauffolgendem Zugriff auf das bei der Bank gespeicherte *virtuelle Konto*. Der für den Benutzer verfügbare hinterlegte Wert wird bei allen drei Systemen in Form des Kontosaldos eines bankeigenen *Pool-Kontos* gespeichert. Ein *Pool-Konto* hat im Gegensatz zu herkömmlichen, in eindeutiger Weise Personen zugeordneten Girokonten das Charakteristikum

[1]Bei der Bank wird das Geld von Zahlungssender und Zahlungsempfänger personenbezogen verwahrt.

eines ‘Kontos für viele’.

Das Zahlungsinstrument der *Überweisung* ist die einzige Ausnahme bei der im Hinblick auf das Verfahren eines Zahlungsvorgangs wichtigen Feststellung, daß alle Systeme expliziter Aktionen des Zahlungsempfängers bedürfen, damit der Geldwert in dessen Besitz übergeht.

Ausgangspunkt für diese Arbeit war die Untersuchung verschiedener Systeme im Hinblick auf die Eigenschaften des den Benutzern gebotenen Geldtransfers. Im Laufe der Bearbeitung des Themas hat sich herausgestellt, daß die Bezeichnung des *Zahlungssystems* die Verhältnisse bei den behandelten Systemen generell korrekter wiedergibt. Die zum Beispiel Bargeld innewohnende Wertübertragungsfunktion[2] ist oft separat nicht gegeben. Die Systeme beinhalten für Zahlungssender und Zahlungsempfänger spezifische Hardware- bzw. Software-Komponenten, welche die möglichen Aktivitäten für die Benutzer definieren. Die Konzeption der Systeme ist mit Ausnahme von *eCash* und den in Kapitel 3 beschriebenen ‘Instrumenten des bargeldlosen Zahlungsverkehrs’ auf eine ausschließliche Käufer-Händler-Situation ausgelegt.

Es hat sich gezeigt, daß viele Aspekte aus unterschiedlichen Fachgebieten im Zusammenhang mit dem Thema der Arbeit wichtig sind. Neben einer psychologischen und ökonomischen Sichtweise (Was ist Geld? Ist die Geldmenge im System konstant?) kommt als ein wesentlicher Aspekt von Zahlungssystemen das zugrungeliegende nationale Rechtssystem hinzu. Es läßt sich feststellen, daß bei allen Systemen in unterschiedlicher Form auf vertragliche Vereinbarungen zwischen beteiligten Parteien zurückgegriffen wird.

Alle betrachteten Systeme beinhalten dem Systemanbieter gegenüber rechtsverbindliche Zustimmungen zu vertraglichen Vereinbarungen der Benutzer.
In bestimmten Fällen stellen die Systeme Aktionen zum Zwecke eines einer Wertübertragung zur Verfügung, untersagen den Benutzern aber gleichzeitig andere Aktionen, um die Funktionalität bzw. die Spezifikation des betreffenden Systems zu erfüllen. Ein anschauliches Beispiel bietet das *POS-System* mit dem *electronic cash-Verfahren*. Zur Authentifizierung eines Benutzers ist neben dem Besitz einer physikalischen Karte die *Persönliche Identifikations-Nummer (PIN)* Teil des Konzepts[3], die der Identifizierung des rechtmäßigen Benutzers (des Kontoinhabers) dient. Prinzipiell ist das Wissen um die vierstellige Dezimalzahl leicht übertragbar. Dieses Problem lösen die im System festgelegten vertraglichen Bestimmungen zwischen System-Anbieter und Benutzer; der System-Benutzer verpflichtet sich bei Vertragsabschluß zur Geheimhaltung der *PIN*.

[2]im Sinne von keiner ausschließlichen Kunde-Händler-Situation; die Rollen Zahlungssender und Zahlungsempfänger sind frei wählbar und werden vom System nicht festgelegt

[3]siehe Kapitel 7.1

Diese Methode der zu den Mechanismen des Systems hinzukommenden vertraglichen Vereinbarungen gewährleistet die Bedingung, daß nur die Person des Kontobesitzers Zugriff auf das entsprechende Girokonto hat.

Im Sinne der Überlegungen von [SEARLE, 1995][4] kann man sagen, daß das Artefakt des *GeldKarten*-Systems und ebenso der beiden Internet-Zahlungssysteme *eCash* und *CyberCoin* von der abstrakten, gesellschaftlichen Institution *Geld* in Form der inhärent werttragenden Banknoten und Münzen noch weiter abstrahiert. Der Zählerstand der *Kundenkarte* repräsentiert genauso wie eine *elektronische Münze* oder ein *virtuelles Konto* einen entsprechenden bei der Bank hinterlegten Geldwert ohne selbst 'in sich' einen Wert zu tragen. Es geht bei *Kundenkarte*, *elektronischen Münzen* und *virtuellen Konten* allein um die auferlegte Funktion des Nachweises. Es wird die maximale Verfügungshöhe über einen Anteil des im Saldo eines Pool-Kontos bei der Bank gespeicherten Wertes dokumentiert. Diese Dokumentation erfolgt beim *GeldKarten-System* im Gegensatz zum *eCash*-System, das identifizierbare Bitfolgen zu diesem Zweck benutzt, in hardwaregesicherter, nicht fälsch- oder duplizierbarer Form eines Variablenwertes im Chip-Speicher der Karte. Ein Benutzer des *CyberCoin*-Systems hat Zugriff auf das bei der Bank geführtes *virtuelles Konto*.

Über den in Kapitel 2.2 zentralen Aspekt der allgemeinen und kontinuierlichen Akzeptanz eines Zahlungsmittels kann an dieser Stelle wenig Konkretes über die einzelnen Systeme ausgesagt werden. Bei den zwei Internet-Zahlungssystemen handelt es sich um Pilotprojekte mit einer sehr kleinen Benutzerzahl im Vergleich zu *traditionellen* Zahlungsmitteln wie z.B. den Instrumenten des bargeldlosen Zahlungsverkehrs. Das in dieser Arbeit eingehend dargestellte *GeldKarten*-System hat zwar eine große Verbreitung in Deutschland, da die Zahlungssender-Komponente des Systems automatisch in Bankkunden- und ec-Karten integriert ist. Die Nutzung dieser Funktionalität ist demgegenüber noch sehr gering. Wie in Nr. 15 des Newsletters [EZI-N, 1998] vom 12.06.1998 in Anlehnung an eine Statistik des Zentralen Kreditausschusses (ZKA) berichtet wird, ist zwar die Akzeptanz auf Händlerseite aufgrund sehr geringer System-Kosten[5] gegeben; die Nutzung durch die Kunden ist zum jetzigen Zeitpunkt allerdings (noch) anteilsmäßig sehr gering. „Bezogen auf die etwa 44 Mio. ausgegebenen Geldkarten [Kundenkarten] ist davon nur etwa 1 Prozent auch aktiv[6]." [EZI-N, 1998, Nr. 15]

---

[4] in Abschnitt 2.2 auf S. 11

[5] Es fallen nur die im Vergleich zum POS- oder Kreditkarten-System geringen Gebühren für die durchgeführten Zahlungsvorgänge an; die Händler-Komponente des Systems wird durch den Anbieter größtenteils kostenlos zur Verfügung gestellt. Die geringen Kosten sind nach einer kleinen Umfrage unter Einzelhändlern der Hauptgrund, das GeldKarten-System im Ladengeschäft zu nutzen und den Kunden bereitzustellen.

[6] bezogen auf die Nutzung zu einem Ladevorgang oder Bezahlvorgang im Zeitraum eines

In Abschnitt 6.1 über das Internet-Zahlungssystem *eCash* wird deutlich, welches der grundlegende Unterschied zwischen physikalischen und elektronischen Token ist, die zum Zweck einer Wertübertragung benutzt werden.

Bei software-basierten Systemen ist eine Bitfolge, die als Entität eine elektronische Geldeinheit repräsentiert, sehr leicht kopierbar. Um die Konsistenz in einem Software-System mit elektronischen Token zu gewährleisten, muß der Emittent als dritte Partei bei jedem Zahlungsvorgang eingeschaltet werden und dafür Sorge tragen, daß jede emittierte Geldeinheit nur einmal benutzt wird. „[...] electronic money requires the intervention of a third party for each flow of electronic money [...]“ [Piffaretti, 1998, S. 7].

Nach Empfang der elektronischen Geldeinheiten hat ein Zahlungsempfänger noch keinen *Wert* erhalten, die endgültige Bezahlung erfolgt nach dem Einreichen der elektronischen Geldeinheiten durch den Emittenten. Dieser führt die Zahlung (und somit den eigentlichen Geldtransfer) aus, indem er dem Konto des Zahlungsempfängers den entsprechenden Betrag gutschreibt bzw. ihm entsprechende neue elektronische Geldeinheiten oder gesetzliches Zahlungsmittel ausgibt. („Therefore, there is no direct transfer of funds [...], funds are kept at the bank“ [Piffaretti, 1998, S.10]). Die vom Zahlungsempfänger beim Emittenten eingereichte elektronische Geldeinheit wird vernichtet, ihre Existenz beschränkt sich auf einen einzelnen Zahlungsvorgang.

Da sich die Existenz einer Geldeinheit auf eine einzelne Zahlungsaktion beschränkt, kann elektronisches Geld nicht zwischen Beteiligten zirkulieren. Die Sicherheitseigenschaften von Papier- oder Münzgeld erlauben demgegenüber einen offenen Geldkreislauf in einer Gesellschaft. Hier sind bei einem Zahlungsvorgang jeweils nur die zwei Parteien Zahlungssender und Zahlungsempfänger beteiligt. Die Notwendigkeit einer dritten Partei für einen Zahlungsvorgang entfällt. “Thus electronic money issued in closed circulation systems is issued [...] exclusively in order to make a payment.“ [Piffaretti, 1998, S. 8]

In [Piffaretti, 1998] wird die Konsequenz aus diesem kleinen Kreislauf, in dem elektronisches Geld existiert, als Unterschied in der Funktion des Geldmittels zwischen *Zahlungsmittel* und *Tauschmitel* benannt. Banknoten fungieren als vollwertiges Tauschmittel, da sie nach dem Zahlungsvorgang beim Zahlungsempfänger keinen Anspruch gegenüber dem Zahlungssender hinterlassen. Elektronisches Geld erfordert demgegenüber prinzipiell einen abschließenden Zahlungsschritt, das Einreichen der Geldeinheit beim Emittenten.

Monats des ersten Quartals 1998

Anhang A

Das System *Geld* in TLA+

Das verwendete Modul *SemaphoreBin* findet sich in Anhang C.1.

module *Geld*

import *Naturals*

---

parameters

$amount$: CONSTANT
$select$: CONSTANT

$user$: VARIABLE
$bank$: VARIABLE
$purse_A, purse_B, giro_A, giro_B$: VARIABLES
$price, load$: VARIABLES
sem, pc : VARIABLES

$SenderA \triangleq$ **instance** $User$ **with** $purse \leftarrow purse_A, giro \leftarrow giro_A$
$SenderB \triangleq$ **instance** $User$ **with** $purse \leftarrow purse_B, giro \leftarrow giro_B$

$Semaphore \triangleq$ **instance** $SemaphoreBin$ **with** $semVar \leftarrow sem$

---

predicates

$$\begin{aligned} \mathit{Init} \triangleq\ & \land\ \mathit{giro}_A, \mathit{giro}_B = \{a \in \mathit{Nat}\} \\ & \land\ \mathit{purse}_A, \mathit{purse}_B = 0 \\ & \land\ \mathit{bank} = (\mathit{giro}_A + \mathit{giro}_B) \\ & \land\ \mathit{amount} = (\mathit{giro}_A + \mathit{giro}_B) \\ & \land\ \mathit{select} = \textsc{choose}\ x : x \in \{\text{“A”}, \text{“B”}\} \\ & \land\ \mathit{user} = \mathit{select} \\ & \land\ \mathit{pc}, \mathit{sem} = 0 \end{aligned}$$

---

definitions

$$\begin{aligned} \mathit{Vars} &\triangleq \langle \mathit{purse}_A, \mathit{purse}_B, \mathit{giro}_A, \mathit{giro}_B, \mathit{bank}, \mathit{price}, \mathit{load}, \mathit{user} \rangle \\ \mathit{People} &\triangleq \{\text{“A”}, \text{“B”}, \text{“C”}, \text{“D”}\} \end{aligned}$$

---

actions

$$\begin{aligned} \mathit{PayAtoB} \triangleq\ & \lor\ \land\ \mathit{pc} = 0 \\ & \quad \land\ \mathit{select} = \text{“A”} \\ & \quad \land\ \mathit{price} = \{p \in \mathit{Nat} : (p > 0) \land (p \leq \mathit{purse}_A)\} \\ & \quad \land\ \mathit{Semaphore.P} \\ & \quad \land\ \mathit{pc}' = 1 \\ & \quad \land\ \textsc{unchanged}\ \mathit{giro}_A, \mathit{giro}_B, \mathit{purse}_A, \mathit{purse}_B, \mathit{bank}, \mathit{load}, \mathit{user} \\ & \lor\ \land\ \mathit{pc} = 1 \\ & \quad \land\ \mathit{purse}'_A = (\mathit{purse}_A - \mathit{price}) \\ & \quad \land\ \mathit{purse}'_B = (\mathit{purse}_B + \mathit{price}) \\ & \quad \land\ \mathit{pc}' = 2 \\ & \quad \land\ \textsc{unchanged}\ \mathit{giro}_A, \mathit{giro}_B, \mathit{bank}, \mathit{load}, \mathit{price}, \mathit{user}, \mathit{sem} \\ & \lor\ \land\ \mathit{pc} = 2 \\ & \quad \land\ \mathit{Semaphore.V} \\ & \quad \land\ \mathit{pc}' = 0 \\ & \quad \land\ \textsc{unchanged}\ \mathit{Vars} \end{aligned}$$

$$
\begin{array}{lll}
PayBtoA & \triangleq & \lor \land pc = 0 \\
& & \quad \land select = \text{"B"} \\
& & \quad \land price = \{p \in Nat : (p > 0) \land (p \leq purse_B)\} \\
& & \quad \land Semaphore.P \\
& & \quad \land pc' = 1 \\
& & \quad \land \text{UNCHANGED } giro_A, giro_B, purse_A, purse_B, bank, load, user \\
& & \lor \land pc = 1 \\
& & \quad \land purse'_B = (purse_B - price) \\
& & \quad \land purse'_A = (purse_A + price) \\
& & \quad \land pc' = 2 \\
& & \quad \land \text{UNCHANGED } giro_A, giro_B, bank, load, price, user, sem \\
& & \lor \land pc = 2 \\
& & \quad \land Semaphore.V \\
& & \quad \land pc' = 0 \\
& & \quad \land \text{UNCHANGED } Vars
\end{array}
$$

$$
\begin{array}{lll}
GetA & \triangleq & \lor \land pc = 0 \\
& & \quad \land select = \text{"A"} \\
& & \quad \land Semaphore.P \\
& & \quad \land pc' = 1 \\
& & \quad \land \text{UNCHANGED } Vars \\
& & \lor \land pc = 1 \\
& & \quad \land SenderA.Withdraw \\
& & \quad \land bank' = bank - load \\
& & \quad \land pc' = 2 \\
& & \quad \land \text{UNCHANGED } giro_B, purse_B, price, sem, user \\
& & \lor \land pc = 2 \\
& & \quad \land Semaphore.V \\
& & \quad \land pc' = 0 \\
& & \quad \land \text{UNCHANGED } Vars
\end{array}
$$

$$
\begin{array}{lll}
GetB & \triangleq & \lor \land pc = 0 \\
& & \quad \land select = \text{"B"} \\
& & \quad \land Semaphore.P \\
& & \quad \land pc' = 1 \\
& & \quad \land \text{UNCHANGED } Vars \\
& & \lor \land pc = 1 \\
& & \quad \land SenderB.Withdraw \\
& & \quad \land bank' = bank - load \\
& & \quad \land pc' = 2 \\
& & \quad \land \text{UNCHANGED } giro_B, purse_B, price, sem, user \\
& & \lor \land pc = 2 \\
& & \quad \land Semaphore.V \\
& & \quad \land pc' = 0 \\
& & \quad \land \text{UNCHANGED } Vars
\end{array}
$$

$$
\begin{array}{lcl}
\mathit{ChangeUser} & \triangleq & \lor \land pc = 0 \\
 & & \quad \land ((\mathit{purse}_A > 0) \lor (\mathit{purse}_B > 0)) \\
 & & \quad \land \mathit{Semaphore.P} \\
 & & \quad \land pc' = 1 \\
 & & \quad \land \textsc{unchanged}\ \mathit{Vars} \\
 & & \lor \land pc = 1 \\
 & & \quad \land \mathit{user}' = \{x : x \in \mathit{People}\} \\
 & & \quad \land pc' = 2 \\
 & & \quad \land \textsc{unchanged}\ \mathit{giro}_A, \mathit{giro}_B, \mathit{purse}_A, \mathit{purse}_B, \mathit{bank}, \mathit{price}, \mathit{load}, \mathit{sem} \\
 & & \lor \land pc = 2 \\
 & & \quad \land \mathit{Semaphore.V} \\
 & & \quad \land pc' = 0 \\
 & & \quad \land \textsc{unchanged}\ \mathit{Vars}
\end{array}
$$

temporal

$$
\begin{array}{lcl}
\mathit{Spec} & \triangleq & \land \mathit{Init} \\
 & & \land \Box[\lor \mathit{PayAtoB} \\
 & & \qquad \lor \mathit{PayBtoA} \\
 & & \qquad \lor \mathit{GetA} \\
 & & \qquad \lor \mathit{GetB}]_{\mathit{Vars},\mathit{sem}} \\
 & & \land \Diamond[\mathit{ChangeUser}]_{\mathit{Vars},\mathit{sem}} \\
 & & \land \Box \mathit{amount} = (\mathit{giro}_A + \mathit{giro}_B + \mathit{purse}_A + \mathit{purse}_B) \\
 & & \land \mathit{WF}_{\mathit{Vars},\mathit{sem}}(\mathit{PayAtoB})\ \textbf{if}\ \mathit{select} = \text{“A”} \\
 & & \land \mathit{WF}_{\mathit{Vars},\mathit{sem}}(\mathit{PayBtoA})\ \textbf{if}\ \mathit{select} = \text{“B”}
\end{array}
$$

module *User*

parameters

$purse$: VARIABLE
$giro$: VARIABLE
$load$: VARIABLE

actions

$$Withdraw \triangleq \begin{array}{l} \land\ load = \{l \in Nat : (l > 0) \land (l < giro)\} \\ \land\ purse' = purse + load \\ \land\ giro' = giro - load \end{array}$$

temporal

$$Spec \triangleq \Box[Withdraw]_{load,purse,giro}$$

Anhang B

Das System *GeldKarte* in TLA+

Die in das Hauptmodul *GeldKarte* eingebundenen Module *Sequences* und *SemaphoreBin* befinden sich im Anhang C.

module *GeldKarte*

import *Naturals, Sequences*

---

parameters

$amount$: CONSTANT

$bank$: CONSTANT
$buffer$: VARIABLE
$giroSend, giroRecip, cardSend, cardRecip$: VARIABLES
bvk : VARIABLE
$user$: VARIABLE
$load, price$: VARIABLES
$pc, time$: VARIABLE

$SemLoadTrans \triangleq$ **instance** $SemaphoreBin$ **with** $semVar \leftarrow semLT$
$SemTransClear \triangleq$ **instance** $SemaphoreBin$ **with** $semVar \leftarrow semTC$
$SemClearBatch \triangleq$ **instance** $SemaphoreBin$ **with** $semVar \leftarrow semCB$

$S \triangleq$ **instance** $Sender$
$R \triangleq$ **instance** $Recipient$
$B \triangleq$ **instance** $Bank$

predicates

$$
\begin{aligned}
\mathit{Init} \triangleq\ & \land\ S.\mathit{Init}\\
& \land\ B.\mathit{Init}\\
& \land\ \mathit{cardSend}, \mathit{cardRecip} = 0\\
& \land\ \mathit{giroSend} = \{\mathit{giroSend}_0 \in \mathit{Nat} : \mathit{giroSend}_0 > 0\}\\
& \land\ \mathit{giroRecip} = \{\mathit{giroRecip}_0 \in \mathit{Nat}\}\\
& \land\ \mathit{bvk} = 0\\
& \land\ \mathit{buffer} = \langle\, \rangle\\
& \land\ \mathit{amount} = (\mathit{giroSend} + \mathit{giroRecip})\\
& \land\ \mathit{bank} = \mathit{amount}\\
& \land\ \mathit{user} = \text{“A”}\\
& \land\ \mathit{semLT}, \mathit{semTC}, \mathit{semCB} = 0\\
& \land\ \mathit{pc} = \alpha
\end{aligned}
$$

definitions

$$
\begin{aligned}
\mathit{Vars} &\triangleq \langle \mathit{giroSend}, \mathit{giroRecip}, \mathit{cardSend}, \mathit{cardRecip}, \mathit{bvk}, \mathit{buffer}, \mathit{load}, \mathit{price}, \mathit{time} \rangle\\
\mathit{Sem}123 &\triangleq \langle \mathit{semLT}, \mathit{semTC}, \mathit{semCB} \rangle\\
\mathit{People} &\triangleq \{\text{“A”}, \text{“B”}, \text{“C”}, \text{“D”}\}
\end{aligned}
$$

actions

$$
\begin{aligned}
\mathit{Load} \triangleq\ & \lor \land\ \mathit{pc} = \alpha\\
& \land\ \mathit{user} = \text{“A”}\\
& \land\ \mathit{SemLoadTrans}.P\\
& \land\ \mathit{pc}' = \beta\\
& \land\ \text{UNCHANGED } \mathit{Vars}, \mathit{semTC}, \mathit{semCB}, \mathit{user}\\
& \lor \land\ \mathit{pc} = \beta\\
& \land\ S.\mathit{Load}\\
& \land\ \mathit{time}' = \mathit{time} + 1\\
& \land\ \mathit{pc}' = \gamma\\
& \land\ \text{UNCHANGED } \mathit{cardRecip}, \mathit{giroRecip}, \mathit{bvk}, \mathit{price}, \mathit{load}, \mathit{Sem}123, \mathit{user}\\
& \lor \land\ \mathit{pc} = \gamma\\
& \land\ \mathit{SemLoadTrans}.V\\
& \land\ \mathit{pc}' = \alpha\\
& \land\ \text{UNCHANGED } \mathit{Vars}, \mathit{semTC}, \mathit{semCB}, \mathit{user}
\end{aligned}
$$

$$
\begin{array}{lcl}
Trans & \triangleq & \lor \land pc = \alpha \\
& & \quad \land SemLoadTrans.P \\
& & \quad \land SemTransClear.P \\
& & \quad \land pc' = \beta \\
& & \quad \land \text{UNCHANGED } Vars, semCB, user \\
& & \lor \land pc = \beta \\
& & \quad \land S.Trans \\
& & \quad \land time' = time + 1 \\
& & \quad \land pc' = \gamma \\
& & \quad \land \text{UNCHANGED } giroSend, giroRecip, bvk, load, price, buffer, Sem123, user \\
& & \lor \land pc = \gamma \\
& & \quad \land SemLoadTrans.V \\
& & \quad \land SemTrasnClear.V \\
& & \quad \land pc' = \alpha \\
& & \quad \land \text{UNCHANGED } Vars, semCB, user \\
Clear & \triangleq & \lor \land pc = \alpha \\
& & \quad \land SemTransClear.P \\
& & \quad \land SemClearBatch.P \\
& & \quad \land pc' = \beta \\
& & \quad \land \text{UNCHANGED } Vars, semLT, user \\
& & \lor \land pc = \beta \\
& & \quad \land R.Clear \\
& & \quad \land time' = time + 1 \\
& & \quad \land pc' = \gamma \\
& & \quad \land \text{UNCHANGED } cardSend, giroSend, giroRecip, bvk, load, price, Sem123, user \\
& & \lor \land pc = \gamma \\
& & \quad \land SemTransClear.V \\
& & \quad \land SemClearBatch.V \\
& & \quad \land pc' = \alpha \\
& & \quad \land \text{UNCHANGED } Vars, semLT, user \\
Batch & \triangleq & \lor \land pc = \alpha \\
& & \quad \land SemClearBatch.P \\
& & \quad \land pc' = \beta \\
& & \quad \land \text{UNCHANGED } Vars, semLT, semTC, user \\
& & \lor \land pc = \beta \\
& & \quad \land B.Actions \\
& & \quad \land pc' = \gamma \\
& & \quad \land \text{UNCHANGED } cardSend, cardRecip, load, price, Sem123, user \\
& & \lor \land pc = \gamma \\
& & \quad \land SemClearBatch.V \\
& & \quad \land pc' = \alpha \\
& & \quad \land \text{UNCHANGED } Vars, semLT, semTC, user
\end{array}
$$

$$
\begin{array}{lcl}
\mathit{ChangeUser} & \triangleq & \lor \land\ pc = \alpha \\
 & & \quad \land\ \mathit{SemLoadTrans.P} \\
 & & \quad \land\ pc' = \beta \\
 & & \quad \land\ \textsc{unchanged}\ \mathit{Vars}, \mathit{semCB}, \mathit{semTC}, \mathit{user} \\
 & & \lor \land\ pc = \beta \\
 & & \quad \land\ \mathit{user}' = \{x : x \in \mathit{People}\} \\
 & & \quad \land\ pc' = \gamma \\
 & & \quad \land\ \textsc{unchanged}\ \mathit{Vars}, \mathit{Sem}123 \\
 & & \lor \land\ pc = \gamma \\
 & & \quad \land\ \mathit{SemLoadTrans.V} \\
 & & \quad \land\ pc' = \alpha \\
 & & \quad \land\ \textsc{unchanged}\ \mathit{Vars}, \mathit{semCB}, \mathit{semTC}, \mathit{user}
\end{array}
$$

temporal

$$
\begin{array}{lcl}
\mathit{Spec} & \triangleq & \land\ \mathit{Init} \\
 & & \land\ \Box[\lor\ \mathit{Load} \\
 & & \qquad \lor\ \mathit{Trans} \\
 & & \qquad \lor\ \mathit{Clear} \\
 & & \qquad \lor\ \mathit{Batch}]_{\mathit{Vars},\mathit{Sem}123} \\
 & & \land\ \Box \mathit{amount} = \mathit{bank} = (\mathit{bvk} + \mathit{giroSend} + \mathit{giroRecip}) \\
 & & \land\ \Diamond[\mathit{ChangeUser}]_{\mathit{Vars},\mathit{Sem}123} \\
 & & \land\ \Box\, \mathit{WF}_{\mathit{Vars},\mathit{Sem}123}(\mathit{R.Clear}) \\
 & & \land\ \Box\, \mathit{WF}_{\mathit{Vars},\mathit{Sem}123}(\mathit{B.Batch})
\end{array}
$$

module *Recipient*

parameters

$buffer, cardRecip \ : \ \text{VARIABLES}$

actions

$$Clear \triangleq \begin{array}{l} \land\ cardRecip > 0 \\ \land\ buffer' = buffer \circ \langle \text{“bvk”}, \text{“giroRecip”}, cardRecip \rangle \\ \land\ cardRecip' = 0 \end{array}$$

temporal

$$Spec \triangleq \Box[Clear]_{cardRecip, buffer}$$

module *Sender*

parameters

$\text{LOCAL}\ max \ : \ \text{CONSTANT}$

$load, price \ : \ \text{VARIABLE}$
$buffer, cardSend, cardRecip \ : \ \text{VARIABLES}$

predicates

$$Init \triangleq \land\ max = 40000$$

definitions

$$Vars \triangleq \langle load, price, cardSend, cardRecip, buffer \rangle$$

actions

$$Load \triangleq \begin{array}{l} \land\ load = \{l \in Nat \ : \ (l > 0) \land (l \leq (max - cardSend)) \land (l \ mod \ 100 = 0)\} \\ \land\ buffer' = buffer \circ \langle \text{“giroSend”}, \text{“bvk”}, load \rangle \\ \land\ cardSend' = (cardSend + load) \\ \land\ \text{UNCHANGED}\ cardRecip, price, load \end{array}$$

$$Trans \triangleq \begin{array}{l} \land\ price = \{p \in Nat \ : \ (p > 0) \land (p \leq cardSend)\} \\ \land\ cardRecip' = (cardRecip + price) \\ \land\ cardSend' = (cardSend - price) \\ \land\ \text{UNCHANGED}\ load, price, buffer \end{array}$$

temporal

$$Spec \triangleq \land\ Init$$
$$\qquad\qquad \land\ \Box[\lor\ Load$$
$$\qquad\qquad\qquad \lor\ Trans]_{Vars}$$

---

module *Bank*

import *Naturals, Sequences*

---

parameters

$maxsteps$: CONSTANT
$buffer, bvk$: VARIABLES
$giroSend, giroRecip$: VARIABLES
$time$: VARIABLE

include *Time*

---

predicates

$$Init \triangleq \land\ Time.Init$$
$$\qquad\qquad \land\ maxsteps = \phi$$

---

definitions

$$Vars \triangleq \langle giroSend, giroRecip, bvk, buffer, time \rangle$$

---

actions

$$Batch \triangleq \land\ time\ mod\ maxsteps = 0$$
$$\qquad\qquad \land\ \mathbf{AllTransactions}(\mathbf{buffer})$$
$$\qquad\qquad \land\ buffer' = \langle\,\rangle$$
$$\qquad\qquad \land\ Time.Step$$

$$Sleep \triangleq \land\ time\ mod\ maxsteps > 0$$
$$\qquad\qquad \land\ Time.Step$$
$$\qquad\qquad \land\ \text{UNCHANGED}\ giroSend, giroRecip, bvk, buffer$$

---

temporal

$$Actions \triangleq \lor\ Batch$$
$$\qquad\qquad \lor\ Sleep$$

$$Spec \triangleq \land\ Init$$
$$\qquad\qquad \land\ \Box[Actions]_{Vars}$$

---

module *Time*

import Naturals

parameters

$time \; : \; \text{VARIABLE}$

predicates

$Init \;\triangleq\; time = 1$

actions

$Step \;\triangleq\; \land\ time' = time + 1$

temporal

$$Spec \;\triangleq\; \begin{array}{l} \land\ Init \\ \land\ \Box[Step]_{time} \end{array}$$

Anhang C

Verwendete Module

C.1 Modul SemaphoreBin

Das Modul ist [BLUME, 1998] entnommen.

module *SemaphoreBin*

parameters

$semVar \ : \ \text{VARIABLE}$

predicate

$$Init \ \triangleq \ semVar = 1$$

actions

$$P \ \triangleq \ (semVar > 0) \land (semVar' = semVar - 1)$$
$$V \ \triangleq \ (semVar = 0) \land (semVar' = semVar + 1)$$

temporal

$$spec \ \triangleq \ \begin{array}{l} \land\ Init \\ \land\ \Box[P \lor V]_{semVar} \end{array}$$

C.2 Modul Sequences

Dieses Modul stammt aus [LADKIN *et al.*, 1996, S. 11].

module *Sequences*

import *Naturals*

$$\begin{array}{lll}
mn & \triangleq & \{i \in Nat : (m \leq i) \land (i \leq n)\} \\
Len(s) & \triangleq & \text{CHOOSE } n : (n \in Nat) \land ((\text{DOMAIN } s) = (1n)) \\
Head(s) & \triangleq & s[1] \\
Tail(s) & \triangleq & [i \in 1(Len(s) - 1) \mapsto s[i+1]] \\
s \o t & \triangleq & [i \in 1(Len(s) + Len(t)) \mapsto \textbf{if } i \leq Len(s) \textbf{ then } s[i] \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad\quad \textbf{else } t[i - Len(s)]] \\
Seq(S) & \triangleq & \text{UNION } \{[(1n) \to S] : n \in Nat\}
\end{array}$$

$$\begin{array}{lll}
SelectSeq(s, test()) & \triangleq & \textbf{let } F[\, t : Seq(\{s[i] : i \in 1Len(s)\})\,] \triangleq \\
 & & \qquad \textbf{if } t = \langle\,\rangle \textbf{ then } \langle\,\rangle \\
 & & \qquad\qquad \textbf{else if } test(Head(t)) \\
 & & \qquad\qquad\qquad \textbf{then } \langle Head(t)\rangle \o F[\,Tail(t)] \\
 & & \qquad\qquad\qquad \textbf{else } F[\,Tail(t)] \\
 & & \textbf{in } F[s] \\
SubSeq(s, m, n) & \triangleq & [i \in 1(1 + n - m) \mapsto s[i + m - 1]]
\end{array}$$

Literaturverzeichnis

[ACHERMANN, 1997] ERIC ACHERMANN. *Worte und Werte.* Geld und Sprache bei Gottfried Wilhelm Leibniz, Johann Georg Hamann und Adam Müller. Max Niemeyer Verlag, Tübingen. 1997

[AX *et al.*, 1997] R. AX, T. GROSSE, J. CÄMMERER. *Abgabenordnung und Finanzgerichtsordnung.* Schäffer-Poeschel Verlag Stuttgart. 15. Aufl. 1997

[BELLOVIN, 1989] STEVEN BELLOVIN. *Security Problems in the TCP/IP protocol suite.* Computer Communications Review. April 1989

[BEUTELSPACHER, 1993] A. BEUTELSPACHER. *Kryptologie.* Vieweg, Braunschweig/Wiesbaden, 1993

[BEUTELSPACHER *et al.*, 1995] A. BEUTELSPACHER, J. SCHWENK, K.-D. WOLFENSTETTER. *Moderne Verfahren der Kryptographie.* Vieweg, Braunschweig/Wiesbaden. 1995

[BLAUG *et al.*, 1995] M. BLAUG, W. ELTIS, D. O'BRIEN, D. PATINKIN, R. SKIDESKY, G. E. WOOD. *The Quantity Theory of Money.* From Locke to Keynes and Friedman. Elgar, 1995

[BLUME, 1998] MICHAEL BLUME. *Kleine Einfhrung in die Spezifikationssprache TLA+.* `http://www.rvs.uni-bielefeld.de/m̃blume/`. Stand: 15. Juli 1998

[BÜLOW, 1991] PETER BÜLOW. *Wechselgesetz Scheckgesetz Allgemeine Geschäftsbedingungen.* C. F. Müller Juristischer Verlag Heidelberg. 1991

[BUNDESBANK, 1997] DEUTSCHE BUNDESBANK. *GELD & GELDPOLITIK.* Sekundarstufe 2. `http://www.bundesbank.de/`. 1997

[CAMP *et al.*, 1995] J. CAMP, M. SIRBU, J.D. TYGAR. *Token and National Money in Electronic Commerce.* Carnegie Mellon University. http://www.ksg.harvard.edu/people/jcamp/usenix/usenix.html. Stand: 15. Juli 1998

[Chaum, 1983] David Chaum. *Blind signatures for untraceable payments.* Advances in Cryptology - Crypto '82. Springer-Verlag. 1983

[CyberCash, 1998] CyberCash, Inc.
http://www.cybercash.com/. Stand: 15. Juli 1998

[CyberCash-Pilotprojkt, 1998] Dresdner Bank.
http://www.dresdner-bank.de/f_firmen/b_office/c_cash/-home.htm. Stand: 15. Juli 1998

[Dean *et al.*, 1997] Edward W. Felten, Dirk Balfanz, Drew Dean, Dan S. Wallach. *Java Security: Web Browsers and Beyond.* Department of Computer Science, Princeton University. http://www.cs.princeton.edu/sip/pub/internet-beseiged.html. Febr. 1997

[Deider, 1989] G. Deider. *Mißbrauch von Scheck- und Kreditkarte durch den berechtigten Karteninhaber.* Freie Universität Berlin, Diss.. 1989

[DigiCash, 1998] DigiCash Ltd. http://www.digicash.com/. Stand: 15. Juli 1998

[Dresen u. Dunne, 1998] Stepfan Dresen, Thomas Dunne. *Fürs Netz geprägt.* Wie CyberCash funktioniert. Artikel in der Zeitschrift iX, Heinz Heise Verlag. April 1998

[DUDEN, 1970] Bibliographisches Institut.
DUDEN Bedeutungswörterbuch. Dudenverlag. 1970

[eCash-Pilotprojekt, 1998] Deutsche Bank.
http://info.deutsche-bank.de/ui/index.htm.
Stand: 15. Juli 1998

[Escher, 1997] Dr. Markus Escher. *Bankrechtsfragen des Elektronischen Geldes im Internet.* aus WERTPAPIER-MITTEILUNGEN. Juni 1997

[EZI-N, 1998] Projektleiter: Knud Böhle. EZI-N Elektronische Zahlungssysteme im Internet - Newsletter. Herausgegeben im Rahmen des Projekts Elektronische Zahlungssysteme (PEZ). http://www.itas.fzk.de/deu/projekt/pez.htm.

[Felten *et al.*, 1997] Edward W. Felten, Dirk Balfanz, Drew Dean, Dan S. Wallach. *Web spoofing: An Internet Con Game.* Technical Report 540-96.
Department of Computer Science, Princeton University.

http://www.cs.princeton.edu/sip/pub/spoofing.html. Febr. 1997

[FINANZLEXIKON, 1996] DEUTSCHE BANK. *Finanzlexikon 1996.* http://www.deutsche-bank.de/online_d/finlex_d/. Stand: 15. Juli 1998

[FURCHE U. WRIGHTSON, 1997] ANDREAS FURCHE, GRAHAM WRIGHTSON. *Zahlungssysteme im Internet.* dpunkt.verlag. 1997

[GARFINKEL U. SPAFFORD, 1997] S. GARFINKEL, G. SPAFFORD. *Web Security & Commerce.* O'Reilly. Juni 1997

[GLASSMANN *et al.*, 1995] S. GLASSMANN, M. MANASSE, M. ABADI, P. GAULTHIER, P. SOBALVARRO. *The Millicent Protocol for Inexpensive Electronic Commerce.* http://www.research.digital.com/SRC/personal/Martin_Abadi/-Papers/millicent.html. 1995

[HARLANDT, 1989] HANS HARLANDT. *Die Evolution des Geldes.* I.H. Sauer-Verlag Heidelberg. 1989

[HOLTKAMP, 1998] HEIKO HOLTKAMP. *Einführung in TCP/IP.* AG Rechnernetze & Verteilte Systeme, Technische Fakultät der Universität Bielefeld. http://www.rvs.uni-bielefeld.de/. Mai 1998

[HUECK, 1986] A. HUECK, C.-W. CANARIS. *Recht der Wertpapiere.* 12. Aufl.. Verlag Franz Vahlen, München. 1986

[HUNT, 1997] C. HUNT. TCP/IP Network Administration. 2nd Edition. O'Reilly. 1997

[JANSON U. WAIDNER, 1995] P. JANSON, M. WAIDNER. *Electronic Payment over Open Networks.* http://www.zurich.ibm.com/Technology/Security/-publications/1995/JaWa95.dir/JaWa95e.html. April 1995

[JARCHOW, 1984] H.-J. JARCHOW. *Theorie und Politik des Geldes.* Vandenhoeck & Ruprecht, Göttingen. 1984

[LADKIN *et al.*, 1996] PETER B. LADKIN, LESLIE LAMPORT, DENIS ROEGEL, BRYAN OLIVIER. Lazy Caching in TLA. http://www.research.digital.com/SRC/tla/papers.html. Jan. 1996

[LADKIN, 1997] PETER B. LADKIN. *Using The Teporal Logic of Actions: A Tutorial on TLA Verification.* Universität Bielefeld. http://www.rvs.uni-bielefeld.de/. Juni 1997

[LAMOND, 1996] KEITH LAMOND. *Credit Card Transactions.* `http://rembrandt.erols.com/mon/ElectronicProperty/-klamond/CCard.htm`. Real World and Online. 1996

[LAMPORT, 1994] LESLIE LAMPORT. *The Temporal Logic of Actions.* DEC SRC Research Report 79. `http://www.research.digital.com/SRC/tla/papers.html`. April 1994

[LAMPORT, 1996] LESLIE LAMPORT. *The Module Structure of TLA+.* DEC SRC Technical Note 1996 - 002. `http://www.research.digital.com/SRC/tla/`. Sept. 1996

[LAMPORT, 1997] LESLIE LAMPORT. *The Operators of TLA+.* DEC SRC Technical Note 1997 - 006. `http://www.research.digital.com/SRC/tla/`. April 1997

[LEXIKON, 1968] *Enzyklopädisches Lexikon für das Geld- Bank- und Börsenwesen.* 3.Auflage. Fritz Knapp Verlag Frankfurt a. M.. 1967/68

[MEDVINSKY U. NEUMANN, 1995] GENNADY MEDVINSKY, B. CLIFFORD NEUMANN. *NetCash: A design for practical electronic currency on the Internet.* University of Southern California. `http://gost.isi.edu/info/NetCash/`. 1995

[MILLICENT, 1998] DIGITAL EQUIPMENT CORPORATION. `http://www.millicent.digital.com/`. Stand: 15. Juli 1998

[MRAZ U. WEIDNER, 1997] VIKTOR MRAZ, KLAUS WEIDNER. *Falsch verbunden.* Gefahr durch DNS-Spoofing. Artikel in der Zeitschrift c't, Heft 10, Heinz Heise Verlag. 1997

[NEUMAN *et al.*, 1995] B. CLIFFORD NEUMAN, GENNADY MEDVINSKY. *Requirements for Network Payment: The NetCheque Perspective.* `http://nii.isi.edu/info/netcheque/documentation.html`. Mar. 1995

[PEIRCE U. O'MAHONY, 1995] MICHAEL PEIRCE, DONALD O'MAHONY. *Scaleable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set.* 1995

[PIFFARETTI, 1998] NADIA PIFFARETTI. *A Theoretical Approach To Electronic Money.* Working Paper N.302. http://www.unifr.ch/macroeco/papers.html. Febr. 1998

[RANKL U. EFFING, 1996] W. RANKL, W. EFFING. *Handbuch der Chipkarten.* 2.Aufl. Carl Hanser Verlag München Wien. 1996

[SANDKÜHLER, 1992] G. SANDKÜHLER. *Bankrecht.* Carl Heymanns Verlag KG. 1992

[SET, 1998] SECURE ELECTRONIC TRANSACTION LLC. http://www.setco.org/. Stand: 15. Juli 1998

[SCHUBA, 1993] CHRISTOPH L. SCHUBA. *Addressing Weaknesses in the Domain Name System Protocol.* COAST Laboratory, Department of Computer Science, Purdue University. August 1993

[SEARLE, 1991] JOHN R. SEARLE. *Intentionalität.* Suhrkamp Verlag Frankfurt a. M.. 1991

[SEARLE, 1995] JOHN R. SEARLE. *The Construction of Social Reality.* Penguin Books. 1995

[SCHÖTER, WILLMER, 1997] ANDREAS SCHÖTER, RACHEL WILLMER. *Digital Money Online.* A Review of Some Existing Technologies. http://www.intertrader.com/library/DigitalMoneyOnline/-dmo/dmo.htm. Stand: 15. Juli 1998

[TANENBAUM, 1994] ANDREW S. TANENBAUM. Moderne Betriebssysteme. Hanser Studienbücher der Informatik. 1994.

[WEISENSEE, 1970] G. J. WEISENSEE. *Die Kreditkarte - ein amerikanisches Phänomen.* Verlag Paul Haupt, Bern u. Stuttgart. 1970

[WELSH, 1991] D. WELSH. *Codes und Kryptographie.* VCH Weinheim, 1991

Erklärung

Hiermit versichere ich, daß ich die vorliegende Diplomarbeit, „Vergleichende Analyse von elektronischen Geldtransfer-Systemen“, selbstständig bearbeitet und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie Zitate kenntlich gemacht habe.

Bielefeld, den 5. August 1998