Seminar der Arbeitsgruppe

Datenbanken und Informationssysteme

im Sommersemester 2001

DB-Aspekte des E-Commerce, Schwerpunkt: Techniken

Elektronische Bezahlverfahren

Alexander Hilliger von Thile

Elektronische Bezahlverfahren

Elektronische Bezahlverfahren

Einführung

„Bezahlen sie einfach mit ihrem guten Namen“ – so heißt es im Werbeslogan eines großen Kreditkartenherstellers. Aber funktioniert Bezahlen in der Realität wirklich so einfach?

Durch fallende Preise von Mobiltelefonen und mobilen Personal Digital Assistents (PDA), wie z.B. dem Palm Pilot oder PocketPC, entwickelt sich zur Zeit ein Trend zum „everything goes everywhere online“ wodurch Konsumenten in die Lage versetzt werden, ortsunabhängig weltweit Waren und Dienstleistungen erwerben zu können. Doch das sog. M-Commerce (Mobile Commerce) zeichnet sich zur Zeit noch durch eine große Schwäche aus, da es zwar zahlreiche Möglichkeiten gibt, Waren vom Anbieter zum Kunden zu transportieren, aber sich die Bezahlung dieser häufig als kompliziert oder unsicher erweist.
Somit entscheidet sich der Erfolg des M-Commerce nicht nur vom Angebot, sondern auch maßgeblich davon, wie Käufer diese bezahlen können.

Diese Ausarbeitung stellt die grundlegenden Anforderungen an elektronische Bezahlverfahren vor und verdeutlicht die Rolle von modernen Datenbanksystemen im Bezahlvorgang. Da es zur Zeit kein Bezahlverfahren gibt, das alle Anforderungen hinreichend erfüllt, werden die vorgestellten Bezahlverfahren klassifiziert und bewertet.

KAPITEL 1

Bezahlen: Was ist das?

Bevor die Eignung von elektronischen Bezahlverfahren untersucht werden kann, ist zu definieren, was unter „Bezahlen“ zu verstehen ist.

1.1 Traditionelle Sicht

Die ersten Bezahlvorgänge finden sich bereits in den frühen Anfängen der menschlichen Evolution und wurden durch Tausch realisiert. Zwei Personen, in der Volkswirtschaftslehre auch als Wirstschaftssubjekte [MAN99] bezeichnet, tauschten dabei eine Form von Gütern gegen eine gewisse Anzahl anderer Güter ein, wobei beide Teilnehmer durch diese Transaktion keine Nachteile erleiden, da der Wert des Eingetauschten für sie gleich oder mehr Wert hat als das ursprüngliche Gut. Dieser Vorgang (siehe Abb. 1.1) wird als unmittelbare Transaktion bezeichnet und beschreibt die einfachste Form eines Bezahlvorganges.

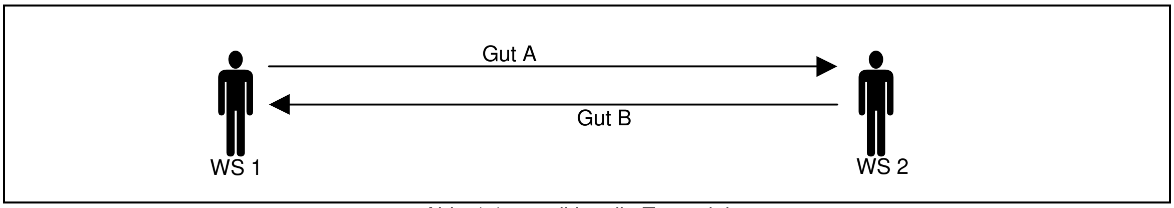

Abb. 1.1 – traditionelle Transaktion

Seit der Einführung von Geld lassen sich alle Güter miteinander vergleichen, weil jedes Gut einen gewissen Wert hat, der in Geldeinheiten ausgedrückt werden kann. Dies ändert jedoch nichts an den Grundeigenschaften des oben genannten Tauschgeschäftes, denn eine Person, die ein Gut einer anderen gegen Geld überläßt, erwartet von diesem Geld, daß es den Wert des Gutes repräsentiert und später gegen ein anderes Gut diesen Wertes wieder eingetauscht werden kann. Während Geld noch vor wenigen Jahrhunderten selbst einen hohen materiellen Wert hatte, z.B. Goldmünzen, ist das heutige Geld keineswegs mehr materiell das wert, was es repräsentiert. Es läßt sich feststellen, daß nicht das Geld selbst wertvoll ist, sondern der Glaube, daß der Wert, den das Geld repräsentiert, zum Tausch gegen ein Gut gleichen Wertes ermächtigt.

1.2 Abstrakte Sicht

Im folgenden soll eine abstrakte Sicht auf das oben genannte traditionelle Bezahlverfahren vorgestellt werden.

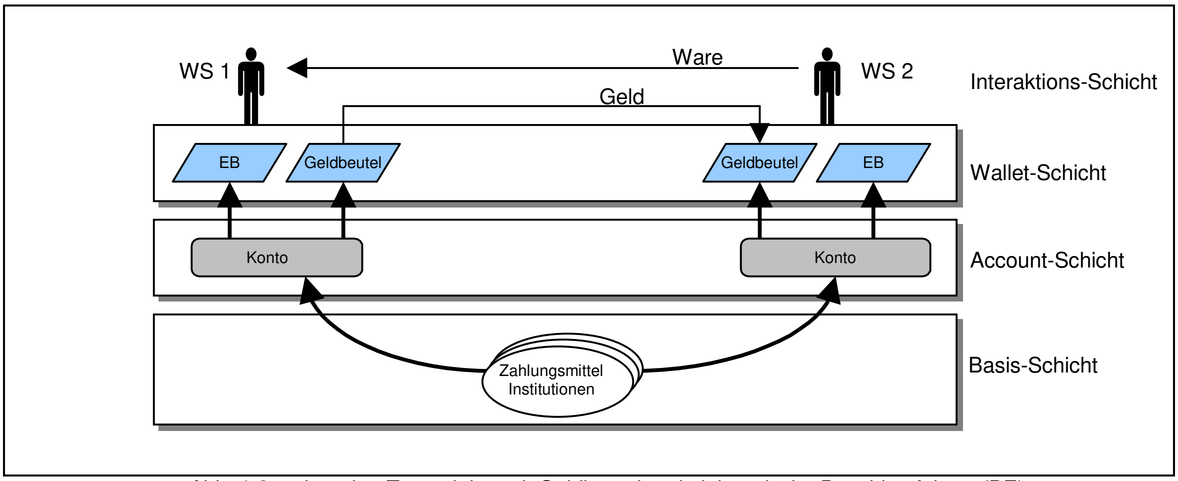

Abb. 1.2 – abstrakte Transaktion mit Geldbeutel und elektronische Bezahlverfahren (BE)

Hierzu werden verschiedene Schichten betrachtet (siehe Abb. 1.2). Auf der untersten Schicht befinden sich die Zahlungsmittel-Institutionen. Diese sind z.B. von staatlicher Seite ermächtigt, gültige Zahlungsmittel in Umlauf zu bringen. Als Beispiel sei hier die europäische Zentralbank genannt, die den Euro zur Verfügung stellt.

Auf der darüberliegenden Account-Schicht befinden sich die Banken und Sparkassen. Diese verwalten die Zahlungsmittel für ihre Kunden, betreiben Handel mit Zahlungsmitteln (z.B. über Kredite) und stellen Konten zur Verfügung. Diese Konten speichern einen einfachen Zahlenwert, der die Höhe des in dem Konto niedergelegten Zahlungsmittelbestandes repräsentiert. Es ist an dieser Stelle wichtig zu verstehen, daß die Zahlungsmittel nicht im Konto hinterlegt sind, sondern lediglich ihr Wert dort gespeichert wird. Konten stellen in der heutigen Zeit den wichtigsten Aufbewahrungsort für Zahlungsmittel dar, da größere Beträge, wie z.B. Löhne und Gehälter nicht mehr bar ausgezahlt, sondern überwiesen werden. Der Hauptvorteil bei Konten besteht darin, daß Standard-Transaktionen, wie z.B. regelmäßige Zahlungen mit einer Person abgewickelt werden können, obwohl diese dabei nicht anwesend zu sein braucht. Die Bank nimmt somit eine Stellvertreterrolle ein.

Die darüberliegende Wallet-Schicht stellt das Portemonnaie einer Person dar. Dieses enthält einen kleinen Betrag, den die Person mit sich führt, um kleinere Einkäufe zu erledigen. Zu dieser Schicht zählen ebenfalls Kredit- und Geldkarten sowie alle Zahlungsmöglichkeiten, die eine Person mit sich führt. Markant an dieser Schicht ist die enge Bindung zur darunterliegenden Account-Schicht. Das Wallet wird z.B. durch den Besuch am Geldautomaten aufgefüllt. Die bei der Wallet-Schicht dargestellten Zahlungsmöglichkeiten bringen unterschiedliche Vor- und Nachteile mit sich. So lassen sich zwar mit einem Portemonnaie problemlos Beträge bezahlen, diese müssen sich jedoch zuvor in diesem befinden, was einen vorhergegangenen Aufwand unterstellt. Kreditkarten, die mit dem Konto „verbunden" sind, haben diesen Nachteil nicht, bieten dafür aber keine Anonymität beim Einkauf, da anhand der Kassenbelege und Kreditkartenrechnung nachvollziehbar ist, wer zu welchem Zeitpunkt was gekauft hat.
Diese Schicht ist für diese Ausarbeitung die wichtigste, da die elektronischen Bezahlverfahren hier aufsetzen.

Auf der obersten Schicht interagieren die Personen und kaufen Waren und Dienstleistungen voneinander durch den Austausch von Zahlungsmitteln. Es gibt zwei grundlegende Voraussetzung für eine erfolgreiche Abwicklung:

1. Beide Personen akzeptieren das Zahlungsmittel. Dies bedeutet, daß sie das Zahlungsmittel als gültig anerkennen.
2. Beide Personen verfügen über kompatible Zahlungsmöglichkeiten auf der Wallet-Schicht, das bedeutet, daß der Verkäufer die Zahlung des Käufers annehmen kann. Als einfache Beispiele sei hier Wechselgeld aufgeführt oder ein Kreditkartenlesegerät.

1.3 Probleme von traditionellen Zahlungsmitteln

Eine berechtigte Frage wäre nun, warum man beim M-Commerce nicht auf die traditionellen Bezahlverfahren zurückgreift, sondern Neue, Elektronische, einführt.
Betrachtet man die Abbildungen 1.1 und 1.2 so fällt auf, daß in beiden Darstellungen für einen Geldbetrag Ware eingetauscht wird. Geht man davon aus, daß beide Personen direkt interagieren und sich gegenüberstehen, geht die Ware des Verkäufers in den Besitz des Käufer über, nachdem diese bezahlt wurde.

Diese Konstellation bildet beim M-Commerce aber eher eine Ausnahmesituation. In den seltensten Fällen werden sich Käufer und Verkäufer in unmittelbarer Nähe befinden. Während beim E-Commerce, bereits Käufer und Verkäufer (weit) voneinander entfernt sind, muß die Ware noch zum Kunden transportiert werden. Der Bezahlvorgang läßt sich hierbei auf den Ort verlagern, an dem der Kunde seine Ware entgegen nimmt. In diesem Fall wurde zwischen Verkäufer und Käufer ein Mittelsmann gestellt, der die Ware ausliefert und den Bezahlvorgang übernimmt. Hier sind traditionelle Bezahlverfahren zwar noch ausreichend, verursachen jedoch zusätzlichen Aufwand, da der Zahlvorgang über einen Mittelsmann vorgenommen wird (z.B. Nachnahme), vorweg durch eine Überweisung geleistet werden muß (Risiko für den Käufer) oder nach Erhalt der Ware durchgeführt wird (Risiko für den Verkäufer).

1.4 Moderne Zahlungsmittel – Eine Neue Sicht

Wie in 1.1 beschrieben, drückt sich der Wert des Geldes nicht in seinem materiellen Wert aus. Die Frage ist nun, ob Geld überhaupt noch materiellen Wert haben muß, bzw. ob Geld in Zukunft noch anfaßbar sein muß.
Des weiteren wurde festgestellt, daß nicht das Geld selbst wertvoll ist, sondern der Glaube, daß der Wert, den das Geld repräsentiert, zum Tausch gegen ein Gut gleichen Wertes ermächtigt. Somit würde als Geld auch *etwas*, dies kann z.B. eine Zahlenfolge sein, ausreichen, das diesen Glauben vermittelt.

Hierauf setzen nun neue elektronische Bezahlverfahren auf, wodurch sich ein neues Anwendungsgebiet für Datenbanken eröffnet, da sie nicht mehr nur zur Speicherung von Geldwerten, wie z.B. Kontoständen dienen, sondern Datenbanken in Zukunft „Geld“ speichern.

Bevor dies jedoch möglich ist, müssen sowohl elektronische Bezahlverfahren, als auch Datenbanken eine Reihe von Voraussetzungen erfüllen, die im folgenden erläutert werden.

KAPITEL 2

2.1 Anforderungen an elektronische Bezahlverfahren

Untersuchungen in Einkaufszentren haben ergeben, daß beim Kauf von non-convenience-goods[1], z.B. Luxusartikeln, 65 % der Einkäufe direkt vor der Kasse abgebrochen werden. Der häufigste Grund ist der Preis des Artikels. In einem online-Shop kommen nun noch weitere Faktoren hinzu, die den Käufer zurückhalten. Sicherheitsaspekte bei der Übermittlung von Kreditkarteninformation oder auch Vorkasse per Überweisung hemmen den Käufer.
Wichtig bei den Anforderungen an elektronische Bezahlverfahren ist also, daß sie Vorteile gegenüber den traditionellen Verfahren bringen, nach Möglichkeit die Vorteile dieser aber ebenfalls erhalten.

2.1.1 Essentielle Anforderungen

Die essentiellen Anforderungen, die ein elektronisches Bezahlverfahren erfüllen sollte sind:

Vertraulichkeit

Kein Dritter darf die Möglichkeit haben die zu übertragenden Daten ausspähen zu können. Nur die Geschäftspartner haben Einblick in die Transaktion.

Integrität

Auf dem Weg vom Absender zum Empfänger dürfen die übermittelten Daten nicht manipuliert oder gelöscht werden.

Identität / Anonymität

Die Identitäten der Geschäftspartner müssen zweifelsfrei feststellbar sein es sei denn, ein Partner (in der Regel der Kunde) wünscht explizit anonym zu bleiben. Die elektronischen Bezahlverfahren müssen in diesem Fall sicherstellen, daß die Anonymität gewahrt bleibt, jedoch die Gültigkeit des Zahlungsmittels zweifelsfrei festgestellt werden kann und dem anderen Geschäftspartner garantiert wird.

Authentizität

Die Korrektheit der Absenderdaten darf nicht in Frage stehen. Hierzu ist eine Legitimierung (z.B. durch digitale Signaturen) notwendig bei der alle Beteiligten zweifelsfrei identifiziert werden können.

Die oben genannten Anforderungen bilden die Grundlage für Vertrauen beim Käufer als auch beim Verkäufer. Sie sind Voraussetzung für ein Vertragsrecht, das Nichtabstreitbarkeit, Beweisbarkeit und Einklagbarkeit garantiert.

2.1.2 Weitere Anforderungen

Das ideale elektronisches Bezahlverfahren erfüllt zusätzlich noch folgende Anforderungen:

Nachvollziehbarkeit

Alle Geschäftspartner müssen in der Lage sein sich über ihren aktuellen Bestand an Zahlungsmitteln zu informieren und ihre Transaktionen nachvollziehen zu können. Dies muß ähnlich dem Bargeld zeitgleich möglich sein und darf nicht, wie z.B. bei Kreditkarten nur zum Monatsende vorgesehen sein.

Keine Unterbrechung des Einkaufsvorganges

Die Bezahlung muß integriert stattfinden können. Dies bedeutet, daß die Zahlung zeitgleich zum Einkauf erfolgt.

Kein Medienbruch

Das ideale elektronisches Bezahlverfahren funktioniert medienunabhängig, kann also sowohl im Internet als auch am Telefon und dem WAP fähigen Mobiltelefon genutzt werden ohne zwischen verschiedenen Medien zu wechseln.

Minimale Zusatzausrüstung

Sowohl dem Käufer als auch dem Verkäufer müssen die für die Bezahlung notwendigen technischen Einrichtungen kostengünstig zur Verfügung stehen. Sie sollten für den Käufer klein und transportabel auf einer Chipkarte oder in elektronische Geräte, wie z.B. ein Handy integriert sein. Für den Verkäufer ist eine einheitliche Schnittstelle sinnvoll, die möglichst viele verschiedene Bezahlverfahren in einem Gerät verarbeiten kann.

Minimale Vorbereitung

Nutzer von elektronischen Bezahlverfahren sollten diese nach Möglichkeit mit minimaler Vorbereitung einsetzen können (z.B. vorheriger Besuch am Geldautomaten, etc.).

In kürzester Zeit

Eine elektronische Bezahlung darf nicht wesentlich mehr Zeit in Anspruch nehmen, als eine Bezahlung mit Bargeld. Dies ist das größte Problem der neuen Verfahren, denn jedes neue System verliert die Akzeptanz, wenn sich in einer Kassenschlange die Bezahlung dadurch verzögert.

Im Kapiteln 3-9 werden elektronische Bezahlverfahren vorgestellt und anhand der oben genannten Anforderungen bewertet.

2.2 Anforderungen an Datenbanken

```
create row type konto (
  id integer,
  guthaben money,
);
```

Abb. 2.2.1

In Abschnitt 1.1 wurde festgestellt, daß Geld nicht notwendigerweise einen materiellen Wert haben und auch nicht anfassbar sein muß. Geld kann demnach auch eine Ziffernfolge sein, die in einer Datenbank gespeichert wird.

[1] Conveniece Goods bezeichnen Alltagswaren, wie z.B. Nahrungsmittel

Die Anforderungen an moderne Datenbanksysteme gehen deshalb über das einfache Verwalten von Zahlungsmittelhöhen, wie z.B. Kontoständen, hinaus (vgl. Abb. 2.2.1). Vielmehr werden Datenbanken in Zukunft „Geld" speichern.

```
create row type coin (
  id varchar(100)
);
create row type wallet (
  one_cent_coins set(coin),
  two_cent_coins set(coin),
  five_cent_coins set(coin),...
);
```

Abb. 2.2.2

Bereits heute existieren Verfahren, die auf der Wallet-Schicht aufsetzen und dort ein virtuelles Portemonnaie durch virtuelle Münzen realisieren. Diese sind eine Menge langer Ziffernfolgen, die einen festen Betrag darstellen. Die Echtheit dieser virtuelle Münzen kann nicht allein durch mathematische Algorithmen überprüft werden, sonder muß durch Datenbanken gewährleistet werden, die kontrollieren, daß virtuelle Münzen nicht mehrfach existieren (in diesem Falle bedeutet dies, daß eine Ziffernfolge nicht einfach kopiert werden kann).

Somit lassen sich neben den bekannten Anforderungen an Datenbanken, wie z.B. die ACID-Eigenschaften folgende weitere festhalten:

Föderierte DB

Es wird keine zentrale Datenbank für alle Formen von elektronischen Bezahlvorgängen geben, da unter den Zahlungsmittelorganisationen sowie der Banken ein Wettbewerb existiert. Stattdessen ist eine föderierte Datenbank, die aus heterogenen Subsystemen besteht, zu erwarten. Damit diese untereinander kommunizieren können ist ein einheitliches Protokoll notwendig. Hierzu wurden Protokolle, wie das beispielsweise das Online Transaction Protocol [OTP] entwickelt.

Hohe Anforderungen an Verfügbarkeit

Um eine hohe Verfügbarkeit sicherzustellen, kann bei Datenbanken, die elektronische Bezahlvorgänge abbilden, Redundanz eingeführt werden. Ein Ausfall einer Datenbank oder auch nur ein Netzausfall zwischen ihnen darf Bezahlvorgänge nicht verzögern oder verhindern, muß aber ebenfalls die Gesamtkonsistenz (eine digitale Münze darf nur einmal existieren) erhalten.

Verschlüsselung

Datenbanken müssen um Verschlüsselungstechniken erweitert werden. Dies ist auf der einen Seite wichtig, um den Anforderungen aus Abschnitt 2.1.1 zu genügen, auf der anderen Seite erfordern einige elektronische Bezahlverfahren spezielle Verschlüsselungsverfahren, wie z.B. Blinding (genauer beschrieben in Abschnitt 7.2), die die Anonymität des Besitzers und die Authentizität des Geldes sicherstellen.

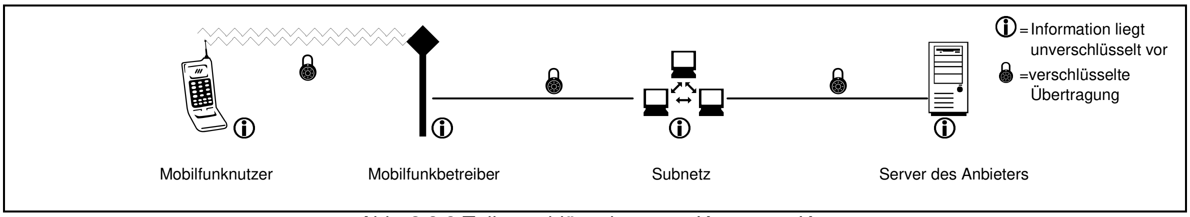

Abb. 2.2.3 Teilverschlüsselung von Knoten zu Knoten

In Zukunft muß diese Verschlüsselung durchgängig sein.

KAPITEL 3

In den folgenden Kapiteln soll ein Überblick über die existierenden elektronischen Bezahlverfahren gegeben werden. Obwohl es eine große Zahl von Bezahlungsmöglichkeiten gibt, lassen sich diese in fünf Kategorien einteilen aus denen jeweils die am meisten verbreiteten elektronischen Bezahlverfahren im folgenden detailliert vorgestellt werden.
Anschliessend werden diese Verfahren auf ihren Nutzen hin untersucht wobei als Bewertungskriterium die in Abschnitt 2.1.1 und 2.1.2 angegeben Punkte gelten.

3.1 Klassifikation

Elektronischen Bezahlverfahren lassen sich primär in zwei Klassen einteilen:

3.1.1 Macropayment: bezeichnet Zahlungen von höheren Beträgen (z.B. ab 10•), die sporadisch oder regelmäßig, aber selten, beispielsweise pro Benutzer ein mal täglich, anfallen. Die Kosten die durch die elektronische Verarbeitung entstehen werden dabei durch den bezahlten Betrag (von dem ein gewisser Prozentsatz abgezogen wird) vollständig gedeckt. Klassische Kreditkarten decken z.B. dieses Einsatzfeld ab.

3.1.2 Micropayment: bezeichnet Zahlungen von Kleinstbeträgen, die z.B. unterhalb eines Cents liegen und die sporadisch oder regelmäßig aber häufig anfallen. Die Kosten die durch die elektronische Verarbeitung entstehen, werden dabei durch den bezahlten Betrag mit zur Zeit existierenden Lösungen in der Regel noch nicht gedeckt.

Macro- und Micropayment sind keine disjunkten Klassen, da der Übergang von Kleinstbetrag und höherem Betrag nicht allgemein definiert, sondern anbieterspezifisch ist. Des weiteren lassen sich elektronische Bezahlverfahren noch nach der Art der „Währung“ die über sie abgerechnet werden klassifizieren:

3.1.3 Kontotransaktion: Hierzu zählen beispielsweise Girokontoüberweisungen. Eine Bezahlung entsteht dadurch, daß ein Betrag vom Konto des Käufers abgebucht und beim Käufer gutgeschrieben wird. Kontotransaktionen finden entweder vor dem Kauf (Vorkasse) oder nach dem Kauf (Lastschrift, Rechnung), nie aber während des Kaufes statt. Auch neuere Verfahren, wie beispielsweise Paybox, ändern diese Prinzip nicht, da sie dem Verkäufer lediglich garantieren, daß der Käufer seinerseits die Transaktion (Geldüberweisung) angestoßen hat, die eigentliche Gutschrift findet aber nach wie vor verzögert statt.

3.1.4 Transaktion über Trusted Third Party: Eine Trusted Third Party ist ein Unternehmen oder eine Institution, denen Käufer und Verkäufer „vertrauen”. Bei einem Online-Einkauf, der prinzipiell ein Risiko darstellt, trägt die Trusted Third Party dieses Risiko und sichert dem Verkäufer zu, daß er sein Geld und dem Käufer, daß er seine Ware erhält. Diese Bezahlform ist an Kontotransaktionen gebunden.

3.1.5 Telefonrechnungsbasiert: Hierbei wird der für eine Dienstleistung zu entrichtende Betrag über die Telefonrechnung vergolten. Der Käufer ruft eine Telefonnummer an, bei der die Kosten für die Gesprächseinheit nicht nur an die Telefongesellschaft sondern auch an den Anschlußinhaber entrichtet werden.
BTX und DatexJ von der Telekom waren Onlinedienste, bei denen kostenpflichtige Angebote ausgewählt werden konnten und diese nach unterschiedlichen Minutenpreisen abgerechnet wurden.

3.1.6 Virtuelle Währung: Diese setzen als Adapter auf der Wallet-Schicht auf vgl. Abbildung 1.2 und stellen virtuelles Geld dar, welches zuvor mit herkömmlichen Geld erworben wurde. Als Beispiel seien hier virtuelle Münzen genannt (siehe Kapitel 7) oder Mensaessensmarken.

In der Praxis finden sich fünf Kategorien, die aus Kombinationen der oben genannten Klassen hervorgehen.

Macropayment Kreditkartenbasiert:	Kreditkartenzahlung mit SSL, SET
Macropayment über Trusted Third Party:	eTrustco, paybox, click&buy
Micropayment mit virtueller Währung:	eCash, Geldkarte ZKA, CyberCoins
Micropayment Telefonrechnungsbasiert:	net900, infin, webcoinbox, dtms @ cash
Kombinationen der Verfahren:	PowerCash21

3.2 Kontotransaktionen

Da alle im folgenden vorgestellten elektronischen Bezahlverfahren eine Mitgliedschaft bei den jeweiligen Anbietern voraussetzen, die häufig mit einem Konto verbunden sind, werden in diesem Abschnitt Möglichkeiten vorgestellt, mit denen Zahlungsmittel per herkömmlicher Überweisung mobil vom persönlichen Girokonto (oder etwas vergleichbarem) zum Konto des Anbieters transferiert werden können.

- **Proprietäre Homebanking Lösungen**
  Die ersten Homebankinglösungen wurden bereits kurz nach der Einführung der ersten PCs vorgestellt. Homebanking bedeutet orts- und zeitunabhängigen Zugriff auf häufig genutzte Geschäftsvorfälle, wie z.B. Kontostandsabfragen, Überweisungen und Daueraufträge ohne dabei persönlich bei der Bank anwesend sein zu müssen. Da diese Lösungen bereits vor dem

WWW existierten und in der Regel von den Banken selbst entwickelt wurden, stellte man dem Kunden spezielle Software zur Verfügung, die per Modemeinwahl eine Verbindung zur Bank herstellte. Durch DatexJ und BTX wurde in Deutschland durch die Post/Deutsche Telekom erstmals ein Standard etabliert und die gesonderte Einwahl zur Bank, sowie die proprietären Softwarelösungen entfielen.

- **HBCI**
  Als einheitlicher Standard wurde HBCI (Home-Banking-Computer-Interface) auf Initiative des Zentralen Kreditausschusses (ZKA) der deutschen Kreditwirtschaft für das sichere und anwenderfreundliche Homebanking entwickelt. Dieser Standard ermöglicht das Homebanking über das Internet (siehe Abb. 3.2). Durch ein allgemein zugängliches API (Application Programming Interface) können zu HBCI kompatible Homebanking Programme für den Endanwender auf allen Platformen entwickelt werden, die nicht mehr nur zur Verwaltung von Konten bei einer Bank dienen. Viele der renommierten Banken sind bereits zu HBCI kompatibel. Durch die Verwendung von anerkannten und leistungsstarken Verschlüsselungsverfahren wie RSA wird eine sichere Abwicklung der Bankgeschäfte garantiert. Ein weiteres Hauptmerkmal von HBCI ist seine Erweiterbarkeit. Sowohl die Integration neuer Gerätegenerationen, wie Mobiltelefonen und Online-Terminals als auch die Kommunikation zu unterschiedlichen Banknetzwerken (z.B. international) stellen laut Hersteller keine Probleme dar.

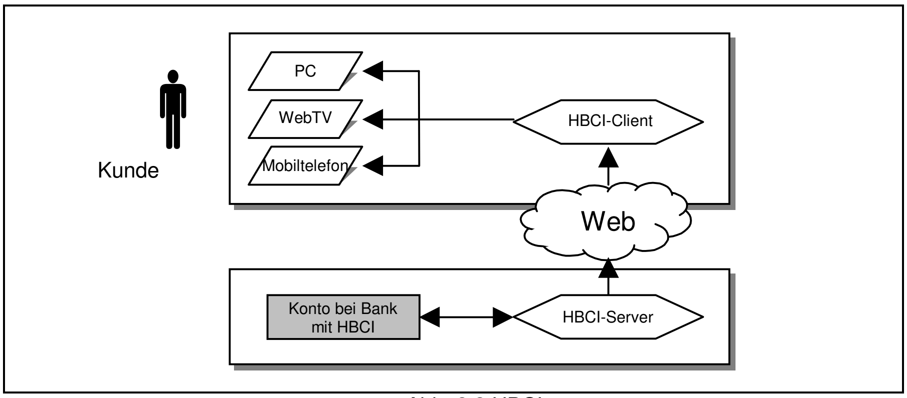

Abb. 3.2 HBCI

Es existieren noch weitere Verfahren, Geld von Girokonto zum Konto beim Anbieter von elektronischen Bezahlverfahren zu transferieren. Die einfachste (gemessen nach Aufwand für den Kunden) besteht in einer sog. Einzugsermächtigung. Hierbei erteilt der Kunde dem Anbieter eine Berechtigung, anfallende Kosten von seinem Girokonto abzuheben. Obwohl dieses Verfahren im Gegensatz zur Überweisung, die „von Hand“ stattfinden muß, Vorteile bietet, wird sie aus Mißtrauen nur von wenigen Kunden akzeptiert.

KAPITEL 4 KREDITKARTENZAHLUNG

Kreditkarten stellen eine der ältesten Formen des bargeldlosen Bezahlens dar. Sie etablierten sich auf Grund ihrer einfachen Handhabung innerhalb kürzester Zeit. Zu den größten Anbietern von Kreditkarten zählen zur Zeit Mastercard/Eurocard, Visa und American Express. Kreditkarten sind einfache Plastikkarten mit zwei grundlegenden Merkmalen:

Abb. 4.1 Bild einer Kreditkarte
Die obere 16 stellige Nummer dient der Identifikation des Herausgebers der Karte
(ersten 4 Stellen),der Identifkation des Besitzers sowie einer Prüfsumme, die die Fälschungssicherheit erhöht.

1. Auf die Karte werden allgemeine Daten, wie Identifikationsnummer, Gültigkeitsbereich und Besitzername eingestanzt (siehe Abb. 4.1). Dies dient primär nicht der Fälschungssicherheit, sondern dazu, die Karte für alte Geräte lesbar zu machen. In diesem Fall wird die Karte als Stempel benutzt, und die eingestanzten Daten werden direkt auf den Beleg (Kassenbon) übertragen.
2. Auf der Rückseite der Karte befindet sich ein Magnetstreifen für elektronische Lesegeräte, der ebenfalls alle oben genannten Daten speichert. Durch ein spezielles Verfahren bei der Beschreibung des Magnetstreifens ist eine spätere Änderung nicht mehr möglich, was die Sicherheit erhöhen soll.

4.1 Funktionsweise/Eingliederung ins Modell

Kreditkarten werden entweder von einer Bank, bei der man ein Girokonto besitzt oder direkt vom Herausgeber von Kreditkarten, wie beispielsweise Visa, ausgegeben. Eine Kreditkarte ist mit einem separaten Konto gekoppelt, das bis zu einem gewissen Betrag überzogen werden darf (hierher stammt der Name „Kredit"-Karte). Bezahlungen, die mit der Karte vorgenommen wurden, werden auf dem Kreditkartenkonto nicht sofort, sondern in der Regel erst zum Monatsende berücksichtigt. Salden auf dem Kreditkartenkonto werden dann per Überweisung (vgl. Abschnitt 3.3) vom Girokonto entweder selbst oder per Einzugsermächtigung gedeckt.

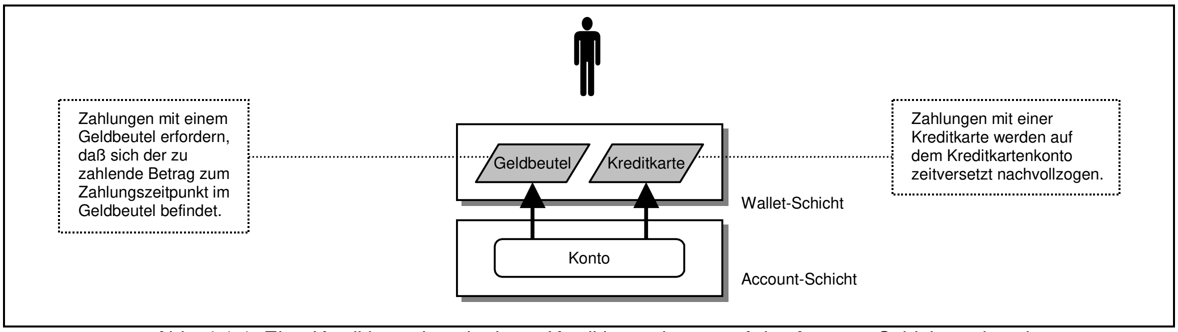

Abb. 4.1.1 Eine Kreditkarte ist mit einem Kreditkartenkonto auf der Account-Schicht verbunden. Über die Kreditkartendaten kann auf der Wallet-Schicht auf dieses Konto zugegriffen werden.

Die Bezahlung mit einer Kreditkarte ist medienunabhängig, d.h. sie kann sowohl von Telefon, mit dem PC oder im Geschäft mit der Karte selbst ausgeführt werden. Die klassische Form der Kreditkartenbezahlung funktioniert derart, daß ein Kunde dem Händler seine Kreditkartendaten (Nummer, Gültigkeitsdatum und eigenen Namen) mitteilt, entweder verbal bei telefonischer Bestellung oder durch vorlegen seiner Kreditkarte. Der Verkäufer hat nun zwei Möglichkeiten, die Gültigkeit der Karte zu überprüfen:

1. **Offline**: Die Identifikationssnummer der Karte enthält eine Prüfsumme. Somit kann sichergestellt werden, daß der Käufer die Nummer nicht manipuliert hat.
2. **Online**: Der Verkäufer läßt die Daten von einer Bank bestätigen. Diese Möglichkeit ist wesentlich sicherer, da somit gesperrte und gefälschte Karten besser erkannt werden können.

Nach erfolgreicher Validation der Daten bestätigt der Käufer die Bezahlung mit seiner Unterschrift.

Kreditkarten eignen sich durch ihre Medienunabhängigkeit auch zur Bezahlung im Internet. Hierbei gibt der Käufer seine Kreditkartendaten in eine Webmaske ein. Sowohl für Käufer, als auch für Verkäufer entstehen hierbei hohe Risiken, da der Käufer seine Kreditkartendaten an jemanden preisgibt, dessen Identität er nicht überprüfen kann und der Verkäufer lediglich die Gültigkeit der Karte validieren kann, nicht aber die Identität des Käufers.

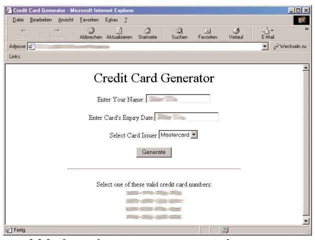

Abb. 4.2 Abbildung einer Webseite zum generieren von Kreditkartennummern

4.2 Sicherheit

Sicherheitsaspekte wurden bei Kreditkarten lange Zeit vernachlässigt, obwohl es jedes Jahr steigende Zahlen von Mißbrauch (z.B. Fälschung) gibt (siehe obige Abbildung). Um das Bezahlen über das Internet sicherer zu machen, wurden in den letzten Jahren verschiedene Sicherheitsverfahren eingeführt:

4.3 Erweiterung SSL

Secure Socket Layer (SSL) ist ein verbindungsorientiertes Verschlüsselungsprotokoll, das die Übertragung von Kreditkarteninformationen gegen Manipulation und Abhören sichern soll. Es wurde von Netscape entwickelt und avancierte durch die kostenlose Bereitstellung über den Netscape-Navigator zum Defakto-Standard. SSL erlaubt sowohl die Verschlüsselung von Daten, als auch die Authentifikation von Servern (ab Version SSL-2) und Clients (ab Version SSL-3) mit Hilfe digitaler Zertifikate. Die Identität von Käufer und Verkäufer läßt sich somit eindeutig bestimmen. Problematisch ist hierbei jedoch, daß der Verkäufer immer noch alle Kreditkartendaten des Kunden erhält, was prinzipiell ein hohes Sicherheitsrisiko darstellt, da sich in jüngster Vergangenheit Einbrüche auf Servern großer Anbieter häuften.

4.4 Erweiterung SET

Secure Electronic Transaction (SET) ist ein offener Standard von Mastercard und Visa. Dieser schließt die Sicherheitslücke von SSL dadurch, daß Kredikarteninformationen vom Kunden mit Hilfe einer digitalen Signatur unterschrieben werden und vom Verkäufer weder geändert noch eingesehen werden können.
Dieses Verfahren stellt zur Zeit die sicherste Form der Kreditkartenzahlung über das Internet dar.

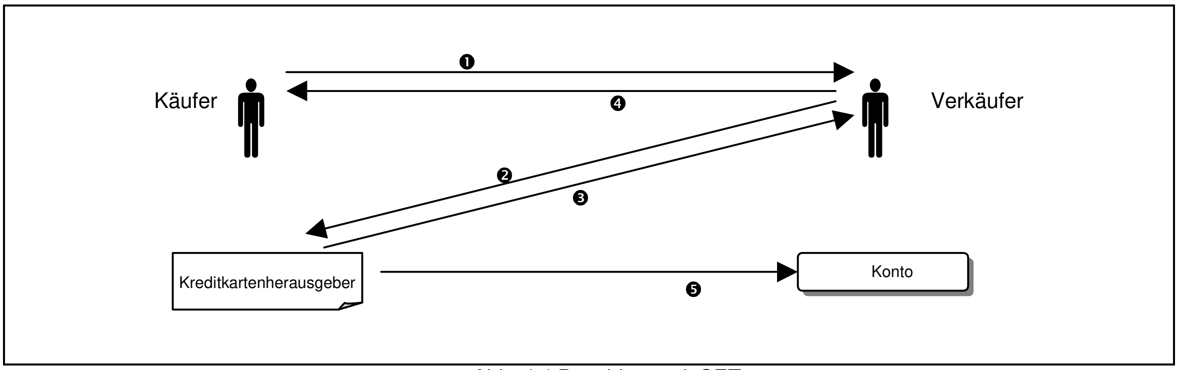

Abb. 4.4 Bezahlung mit SET

1. Kunde bestellt mit seinem Zertifikat
2. Verkäufer schickt Autorisierungsanfrage (Benutzerdaten, sein Zertifikat) an Kreditkartenorganisation
3. Verkäufer erhält Bestätigung (Karte ist gültig, nicht gesperrt,...)
4. Ware wird versandt
5. Kontobewegungen

4.5 Bewertung

- Kreditkarten dienen nur dem Bezahlen, man kann kein Geld per Kreditkarte einzahlen (dies ist nur über den Umweg über das Kreditkartenkonto möglich).
- Hohe Akzeptanz weltweit aber nur für Macropayment (vgl 3.1.1) geeignet
- **Vertraulichkeit**, **Integrität**, **Identität** und **Authentizität** (vgl. 2.1.1) werden mit Hilfe von SET sichergestellt. **Anonymität** ist bei Keditkartenzahlungen nicht möglich.
- **Nachvollziehbarkeit** ist über die Kreditkartenrechnung erst am Monatsende möglich.

- **Unterbrechung des Einkaufsvorganges** findet nicht statt, da die Bezahlung innerhalb weniger Sekunden ohne größeren Aufwand (für Käufer und Verkäufer) durchgeführt wird.

- **Medienbruch** ist durch die Medienunabhängigkeit nicht gegeben.

- **Minimale Zusatzausrüstung**: diese muß nur vom Verkäufer erworben werden und ist günstig in der Anschaffung.

4.6 Neue Formen von Kreditkarten

Obwohl Kreditkarten medienunabhängig sind und somit auch die Bezahlung im Internet ermöglichen sind sie in der Praxis hierfür ungeeignet, da:

- Der Käufer die Daten der Karte in Web-Formularen manuell eintragen muß
- Die Daten auch unverschlüsselt übertragen werden können (z.B. bei Onlineshops, die weder SSL noch SET unterstützen).

Diese Mängel sollen durch neuere Formen von Kreditkarten ersetzt werden. Hierbei werden die Kreditkarten durch sog. Smartcards ersetzt. Diese enthalten einen Chip, ähnlich wie bei Telefonkarten, der über ein an den PC anschließbares Lesegerät ausgewertet werden kann. Somit entfällt die manuelle Eingabe der Kreditkartendaten. Durch eine Sicherheitsfunktion auf dem Chip, werden die Kreditkartendaten nie unverschlüsselt übertragen, womit eine versehentliche Preisgabe der Informationen ausgeschlossen werden kann.
Als Beispiel sei hier *Blue* von American Express genannt. Diese Kreditkarte verwendet einen JavaCard Chip, der die oben beschriebenen Sicherheitsfunktionen zur Verfügung stellt. Des weiteren ist es möglich, kleine Applets aus dem Internet auf den Chip zu übertragen, womit Zusatzfunktionen, wie Bonuspunkte oder Fahrkartenfunktionen möglich werden.

Kapitel 5 Geldkarte

Eine Geldkarte ist vergleichbar mit einer Smartcard-Kreditkarte. Sie ist jedoch für die Bezahlung von Micropayments entwickelt worden. Geldkarten sind zur Zeit nur in Deutschland bei Sparkassen und vereinzelten Banken erhältlich.

5.1 Funktionsweise/Eingliederung ins Modell

Der Hauptunterschied zur Kreditkarte besteht darin, daß eine Geldkarte nicht mit einem Konto gekoppelt sein muß. Vielmehr wird eine Geldkarte „aufgeladen“. Dies bedeutet, daß ein gewisser Betrag von einem Girokonto auf eine Geldkarte übertragen wird. Hierbei werden allerdings keine Zahlungsmittel vergleichbar mit CyberCoins auf die Karte übertragen, sondern lediglich das aktuelle Guthaben auf der Karte vermerkt. Dieses Guthaben, das nicht mehr als 400 DM (ab 1.1.2002 200 •) betragen darf, ist ebenfalls beim Herausgeber der Karte gespeichert, so daß eine Manipulation des Betrages ausgeschlossen ist. Bezahlungen, die mit der Karte vorgenommen wurden, wirken sich direkt auf das Guthaben auf der Karte aus, der zu zahlende Betrag wird also wie bei Bargeld sofort fällig. Eine gesonderte Abrechnung in Form einer Rechnung findet nicht statt, wodurch die Nachvollziehbarkeit von Zahlungen erschwert wird. Geldkarten bieten neben dem Bezahlen noch

weitere Funktionen, wie z.B. Rabattvermerke und elektronische Fahrscheine, die auf die Karte übertragen werden können.
Die Bezahlung mit einer Geldkarte ist nicht medienunabhängig und kann nur mit einem speziellen Lesegerät (Abb. 5.1.1) erfolgen. Bezahlungen im Internet erfordern somit zusätzliche Hardware.

Abb. 5.1.1 Bild des Cash Mouse™ Geldkartenlesegerätes von Giesecke&Devrient ***[GMSE]***

Eine Bezahlung mit Geldkarte funktioniert folgendermaßen:

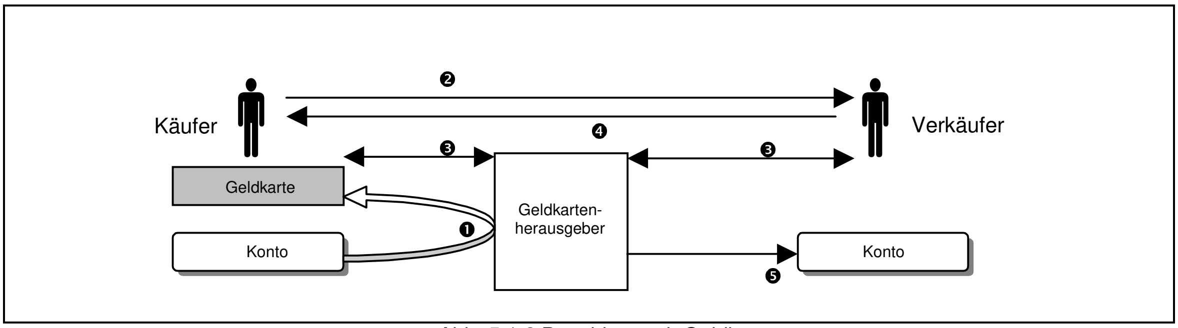

Abb. 5.1.2 Bezahlung mit Geldkarte

1. Unterschreitet das Kartenguthaben den Kaufpreis, muß der Kunde seine Geldkarte zuerst aufladen. Dies ist bei einem Geldautomaten oder auch per PC von zu Hause aus möglich.
2. Der Kunde gibt seine Bestellung auf und wählt als Bezahlmöglichkeit „Geldkarte“
3. Ein Java-Applet wird vom Geldkartenherausgeber übertragen, das die Geldkarte im Lesegerät sowie den Käufer anhand einer PIN validiert und den Kaufpreis von der Karte abbucht. Der Chip auf der Geldkarte signiert den abgebuchten Betrag und stellt somit eine digitale Unterschrift dar. Die erfolgreiche Abbuchung wird dem Verkäufer mitgeteilt
4. Es erfolgt die Lieferung
5. Der Geldkartenherausgeber überweist den Betrag auf das Konto des Verkäufers

Die Übertragung aller Kartendaten ist gegen unerlaubte Einsicht und Manipulation durch SSL (siehe Abschnitt 4.3) und DES Verschlüsselung (hier nicht weiter vertieft) gesichert.

5.2 Verbreitung

Die Geldkarte ist zur Zeit nur in Deutschland, in Kürze auch in Frankreich, erhältlich und ihre Akzeptanz ist gerade im Internet noch sehr eingeschränkt. Sie eignet sich durch die extra anzuschaffenden Lesegeräte daher zur Zeit eher zur Bezahlung ohne Bargeld in herkömmlichen Geschäften und neuerdings auch Park-, Fahrkarten- und Getränkeautomaten.
Anfang 2001 befanden sich ca. 50 Mio. Geldkarten in Umlauf, die bei ca. 60.000 realen und ca. 50 virtuellen Akzeptanzstellen genutzt werden konnten. Im Jahr 2000 wurden mit Geldkarten ca. 15 Mio. Transaktionen mit einem Gesamtwert von 175 Mio. DM vorgenommen.

5.3 Bewertung

Geldkarten können wie ein Portemonnaie auf- und entladen werden. Der „intelligente“ Chip auf der Karte speichert das auf der Karte befindliche Guthaben, das mit handlichen Lesegeräten (Kaufpreis ab 2•) ausgelesen werden kann. Des weiteren signiert der Chip Zahlungen, die mit der Geldkarte vorgenommen werden, womit eine Manipulation ausgeschlossen werden kann und ein Kaufvertrag, ähnlich wie bei einer herkömmlichen Unterschrift zu Stande kommt.

- Weltweit nur geringe Akzeptanz, exponentielles Wachstum in Deutschland
- Für Micropayment (vgl. Abschnitt 3.1.2) geeignet
- **Vertraulichkeit**, **Integrität**, **Identität** und **Authentizität** (vgl. Abschnitt 2.1.1) werden standardmäßig sichergestellt.
- **Anonymität** ist technisch möglich
- **Nachvollziehbarkeit** ist auf Grund fehlender Abrechnung nur begrenzt möglich
- **Unterbrechung des Einkaufsvorganges** findet nicht statt, da die Bezahlung innerhalb weniger Sekunden ohne größeren Aufwand (für Käufer und Verkäufer) durchgeführt werden kann.
- **Medienbruch** ist durch die fehlende Medienunabhängigkeit gegeben. Bei einer telefonische Bestellung müsste der Bezahlvorgang separat durchgeführt werden.
- **Zusatzausrüstung**: ein Lesegerät muß vom beim Einkauf im Internet vom Käufer erworben werden

KAPITEL 6 TRUSTED THIRD PARTY PAYMENT

Die folgenden wird die Klasse der Trusted Third Party Payment-Verfahren anhand von E-Trustco, Paybox und Click&Buy vorgestellt.

6.1 E-Trustco

E-Trustco ist ein neues elektronisches Bezahlverfahren, das zur Zeit noch keine nennenswerte Akzeptanz gefunden hat. Einziger Anbieter und Hersteller ist die E-Trustco AG. E-Trustco wird in dieser Auswertung lediglich exemplarisch für die Klasse von Trusted-Third-Party-Payment-Verfahren (siehe 3.1.4) vorgestellt auf dem viele elektronische Bezahlverfahren aufsetzen.

Bei allen Trusted-Third-Party-Payment-Verfahren müssen sich Käufer und Verkäufer bei der Trusted-Third-Party unter Angabe ihrer Personen- und Kontodaten anmelden und erhalten danach eine Identifikation. Im Falle von E-Trustco ist dies ein digitales Zertifikat mit dem sie sich gegenüber der Trusted-Third-Party, hier der E-Trustco AG, ausweisen können.

E-Trustco ist nicht medienunabhängig und nur für Bezahlungen über das Internet geeignet. Es sind sowohl Micro- als auch Macropaymentzahlungen (siehe Abschnitt 3.1) möglich.

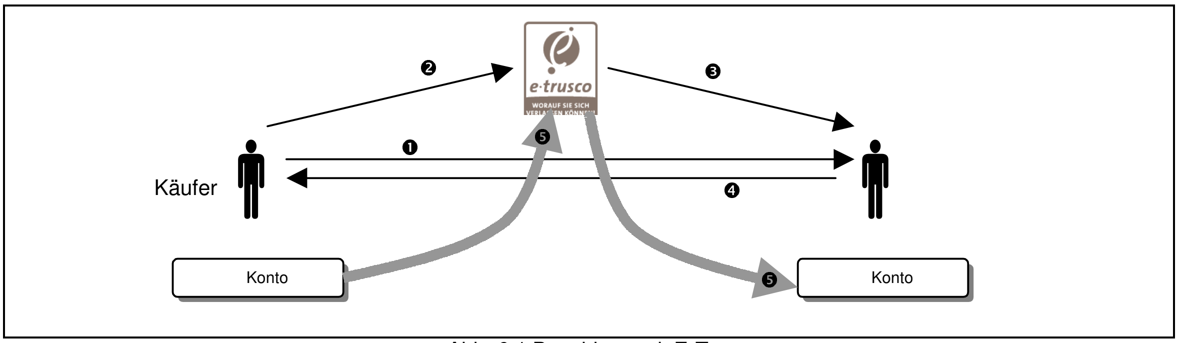

Abb. 6.1 Bezahlung mit E-Trustco

6.1.1 Funktionsweise/Eingliederung ins Modell

Ein typischer Bezahlvorgang über eTrustco verläuft folgendermaßen:

1. Der Kunde gibt seine Bestellung auf und wählt als Bezahlmöglichkeit „E-Trustco“
2. Der Kunde übermittelt den zu zahlenden Betrag, den Empfänger und sein Zertifikat per SSL an E-Trustco
3. Die erfolgreiche Validation der Kundendaten wird dem Verkäufer mitgeteilt
4. Es erfolgt die Lieferung
5. E-Trustco überweist den Betrag auf das Konto des Verkäufers und stellt ihn dem Käufer in Rechnung

Die Überweisung des Geldes vom Käufer zum Verkäufer nimmt E-Trustco mit zweiwöchiger Verzögerung vor, da in dieser Zeit der Käufer nach Fernabsatzgesetz dazu berechtigt ist, den Kauf rückgängig zu machen. Sollte der Käufer vom Kauf zurücktreten, löscht E-Trustco die Überweisung, sobald die Ware wieder beim Verkäufer eingegangen ist.

6.1.2 Bewertung

Größtes Problem bei Trusted-Third-Party-Payment Anbietern ist, daß sie zuerst das Vertrauen der Kunden gewinnen müssen. Der Slogan „E-Trustco – *Worauf Sie sich verlassen können*“ ist sicherlich nicht hinreichend überzeugend. Für Kunden fehlt zur Zeit noch eine objektive Bewertung der Trusted-Third-Parties.

6.2 Paybox

Paybox [PBX], [BMS20] ist zur Zeit das populärste elektronische Bezahlverfahren für M-Commerce, das Trusted-Third-Party basiert ist. Einziger Hersteller und Anbieter ist die Paybox.net AG. Paybox ist nur für Macropayment geeignet und ist speziell für das mobile Bezahlen entwickelt worden und setzt daher ein Mobiltelefon voraus. Paybox unterscheidet nicht prinzipiell zwischen Käufer und Verkäufer, d.h. jeder Payboxteilnehmer kann mit Paybox sowohl bezahlen als auch Geld empfangen.

6.2.1 Funktionsweise/Eingliederung ins Modell

Der Hauptunterschied zu anderen Trusted-Third-Party-Payment Verfahren besteht darin, daß Paybox zwingend ein Mobiltelefon beim Käufer voraussetzt. Dieses wird benötigt um den sicherheitskritischen Bezahlvorgang vom „unsicheren“ Medium Internet zum „sicheren“ Mobilfunknetz, bei dem es u.a. Teilnehmeridentifikation und standardmäßig Verschlüsselung gibt, zu transferieren.

Paybox stellt seinen Teilnehmern kein eigenes Konto zur Verfügung, sondern koppelt ein existierendes Girokonto mit der Payboxmitgliedschaft. Empfängt ein Payboxmitglied einen Betrag, so wird ihm dieser von Paybox überwiesen, tätigt er eine Zahlung, so wird der Betrag von seinem Girokonto per Lastschrift abgebucht.

Die Bezahlung mit Paybox ist auf Grund der Mobilfunkbindung nicht medienunabhängig. Der Bezahlvorgang findet immer vom Einkaufsvorgang entkoppelt auf einem „sicheren" Medium statt. Bezahlungen im Internet erfordern somit, sofern ein Mobiltelefon vorhanden ist, keine zusätzliche Hardware. Paybox funktioniert mit jedem Mobiltelefon, da außer Sprach- und Tastentonübertragung keine Anforderungen gestellt werden.

Eine Bezahlung verläuft folgendermaßen:

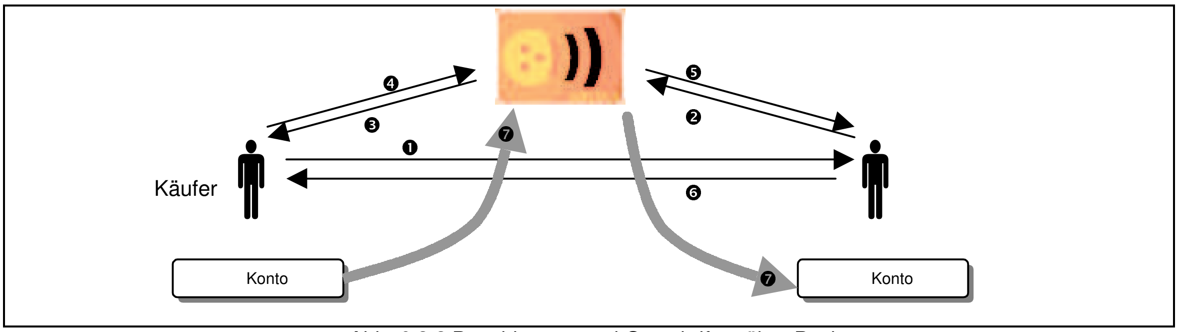

Abb. 6.2.2 Bezahlungen und Gutschriften über Paybox
werden auf dem Girokonto zeitversetzt nachvollzogen

1. Der Kunde gibt seine Bestellung auf, wählt als Bezahlmöglichkeit „Paybox" und gibt seine Payboxnummer an
2. Der Verkäufer sendet eine Autorisierungsanfrage an Paybox. Diese enthält die Payboxnummern von Käufer und Verkäufer, sowie den zu Zahlenden Betrag. Diese Datenübermittlung ist noch nicht auf das Mobilfunknetz beschränkt.
3. Paybox ermittelt validiert die Nummern von Käufer und Verkäufer und ruft die Mobilfunknummer des Käufers an.
4. Der Käufer nimmt den Anruf von Paybox entgegen, ihm werden der Empfänger sowie der zu zahlende Betrag genannt.
5. Der Käufer stimmt der Abbuchung zu und autorisiert sie durch Eingabe seiner PIN.
6. Der Verkäufer erhält eine Autorisierungsbestätigung
7. Es erfolgt die Auslieferung der Ware
8. Dem Käufer wird der gezahlte Betrag per Lastschrift abgebucht und dem Verkäufer nach wahlweise zwei oder vier Wochen gutgeschrieben.

6.2.2 Verbreitung

Paybox ist zur Zeit nur in Deutschland erhältlich und seine Akzeptanz ist gerade im Internet noch sehr eingeschränkt. Ein Modellversuch, mit Paybox Taxirechnungen zu bezahlen, wurde bisher nur mäßig angenommen. Der anhaltende „Boom" im Mobilfunksektor, sowie die Möglichkeit Geld von Person zu Person zu überweisen stellen jedoch gute Wachstumschancen in Aussicht.

6.2.3 Bewertung

Paybox bietet durch seine Entkopplung von Einkaufs- und Bezahlvorgang eine hohe Sicherheit beim mobilen Einkauf. Durch die hohe Verbreitung und geringen Anforderungen an Mobiltelefone ist eine gesonderte Anschaffung von Hardware somit in der Regel nicht notwendig.
Besonders hinderlich bei der Bezahlung ist die durch den Autorisierungsanruf entstehende Verzögerung, die eine Bezahlung an der Supermarktkasse ausschließen.

- Weltweit nur geringe Akzeptanz, gute Wachstumschancen in Deutschland
- Nur für Macropayment (vgl. Abschnitt 3.1.1) geeignet, wegen hoher Kosten für Autorisierungsanruf
- **Vertraulichkeit**, **Integrität**, **Identität** und **Authentizität** (vgl. Abschnitt 2.1.1) werden standardmäßig sichergestellt.
- **Anonymität** ist gegenüber dem Verkäufer möglich, nicht jedoch gegenüber Paybox
- **Nachvollziehbarkeit** ist auf Grund verzögerter Abbuchung erschwert
- **Unterbrechung des Einkaufsvorganges** findet statt, da die Bezahlung auf Grund des Autorisierungsanrufes mehrere Sekunden bis hin zu Minuten in Anspruch nehmen kann.
- **Medienbruch** ist durch die fehlende Medienunabhängigkeit gegeben. Jeder Bezahlvorgang muß separat über das Mobiltelefon autorisiert werden.

6.3 Andere Formen des Bezahlens mit Mobiltelefonen

In Frankreich läuft zur Zeit ein Modellversuch, bei dem Smartcards in Mobiltelefone integriert werden, die Zahlungsfuntionen übernehmen können. Der Bezahlvorgang ist vergleichbar mit dem von Geldkarten, lediglich die Datenübertragung findet hierbei per Übermittlung über das Mobilfunknetz statt. Die Autorisierung findet wie bei Paybox auf dem Mobiltelefon des Käufers statt, ein Sprachanruf ist jedoch wegen der Zusatzausstattung des Mobiltelefons nicht notwendig. Statt dessen erscheinen alle Daten zur aktuellen Bezahlung auf dem Display des jeweiligen Gerätes.

6.4 Click&buy

click&buy wird von der Firma Firstgate Internet AG vertrieben. Es ist ein Trusted-Third-Party Payment Verfahren, das speziell für Micropayments im Internet entwickelt wurde. Click&buy ist zur Zeit nur in Deutschland erhältlich und wird von Firmen, wie ePost, Stiftung Warentest und Verlagen eingesetzt.

6.4.1 Funktionsweise/Eingliederung ins Modell

Käufer und Verkäufer müssen mit Personen- und Kontodaten bei der Firstgate Internet AG angemeldet sein. Ähnlich wie bei Paybox, ist eine Mitgliedschaft bei click&buy mit einem existierenden Girokonto gekoppelt. Möchte ein Anbieter kostenpflichtige Informationen auf seinen Internetseiten anbieten, so stellt der diese auf einen nicht öffentlich zugänglichen Bereich seines Servers und richtet einen Link auf den click&buy-Server ein.

Abb. 6.4.1 Beispiel eines click&buy Links

Möchte ein Käufer dieses Angebot nutzen, klickt er auf den eingerichteten Link (Abb. 6.4.1) und wird zum click&buy Server weitergeleitet. Hier wird er über die Höhe der anfallenden Kosten (einmalig oder pro Zeiteinheit) informiert und kann, wenn er einverstanden ist, dies durch Eingabe seiner Mitgliedsdaten und einer PIN bestätigen. Nach erfolgreicher Autorisierung durch den click&buy Server wird dem Käufer der Zugang zum nicht öffentlichen Bereich des Anbieters gewährt. Verläßt der Käufer das Angebot, werden die Kosten für die Nutzung dem Käufer in Rechnung gestellt und dem Verkäufer gutgeschrieben.

Die Bezahlung mit click&buy ist prinzipiell medienunabhängig, wird aber nur zur Bezahlung im Internet verwendet.

6.4.2 Verbreitung

Click&buy ist zur Zeit nur in Deutschland erhältlich, hat aber im deutschen Internet bereits eine beachtliche Akzeptanz gefunden. Im Jahre 2000 gab es bereits über 1000 Angebote.

6.4.3 Bewertung

- Weltweit nur geringe Akzeptanz, exponentielles Wachstum in Deutschland
- Ausschließlich für Micropayment (vgl. Abschnitt 3.1.2) im Internet geeignet
- **Vertraulichkeit** und **Integrität** werden durch Verschlüsselung sichergestellt
- **Identität** und **Authentizität** (vgl. Abschnitt 2.1.2) werden durch digitale Zertifikate ermöglicht
- **Anonymität** ist nicht garantierbar
- **Nachvollziehbarkeit** ist auf Grund einer Online-Abrechnung verzögert möglich
- **Unterbrechung des Einkaufsvorganges** findet im Internet für angemeldete Benutzer nicht statt, da die Autorisierung innerhalb weniger Sekunden ohne größeren Aufwand durchgeführt werden kann.
- **Medienbruch** ist nicht gegeben.
- **Zusatzausrüstung**: muß weder vom Käufer noch vom Verkäufer erworben werden

KAPITEL 7 ECASH

eCash stellt ein völlig neues Konzept beim bargeldlosen elektronischen Bezahlen dar. Es wurde von der Firma eCash Inc. USA entwickelt und wird als Pilotprojekt in Deutschland von der Deutschen Bank 24 betrieben. Es wurde speziell für Micropayment über das Internet entwickelt und garantiert im Gegensatz zu den bisher vorgestellten Verfahren absolute Anonymität beim Einkauf sowohl vor dem Verkäufer als auch vor der Bank. eCash verwendet sog. „ecoins“ oder auch „cyberBucks“ (vgl. Abschnitt 2.2.2), die aus Ziffernkombinationen bestehen und virtuelles Geld repräsentieren. Dieses virtuelle Geld kann der Besitzer beliebig weitergeben, z.B. per eMail versenden, wodurch es sich von realem Geld in Münzform kaum unterscheidet.

7.1 Funktionsweise/Eingliederung ins Modell

Käufer und Verkäufer benötigen einen eCash Account. In Deutschland kann man diesen zur Zeit nur über die Deutsche Bank 24 erhalten. eCash Accounts sind mit einem Girokonto gekoppelt. Ein Käufer benötigt eine spezielle Wallet-Software, die auf einem PC installiert werden muß.

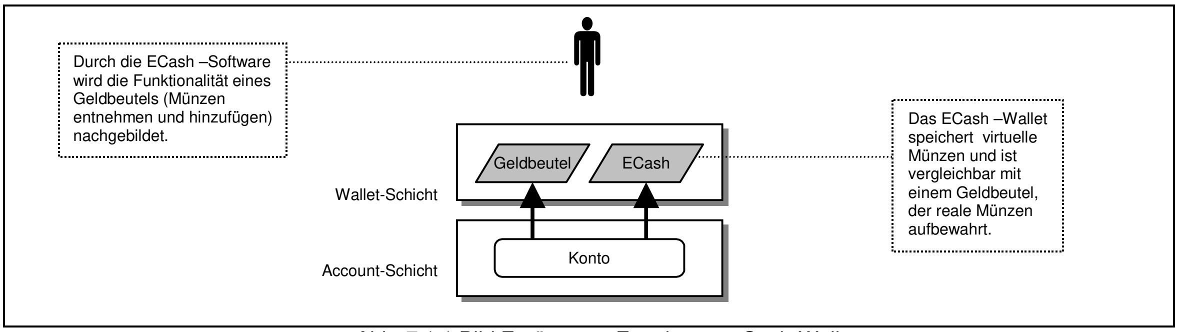

Abb. 7.1.1 Bild:Ergänzung: Extrakonto, eCash-Wallet
Das eCash-Wallet stellt ein Portemonnaie für virtuelles Geld dar. Es ist mit einem Girokonto auf der Account-Schicht verbunden.

Wie bei einer Geldkarte (siehe Kapitel 5) müssen Zahlungsmittel von dem gekoppelten Girokonto ins eCash-Wallet übertragen werden. In diesem werden die elektronischen Münzen verschlüsselt gespeichert und durch mehrere Passwörter vor fremdem Zugriff gesichert. Bezahlungen, die mit den virtuellen Münzen vorgenommen wurden, werden im Wallet sofort berücksichtigt. Enthält das Wallet nicht ausreichend Münzen, kann eine Zahlung nicht durchgeführt werden.

Die Bezahlung mit eCash ist nicht medienunabhängig und wird nur für die Bezahlung im Internet angeboten.

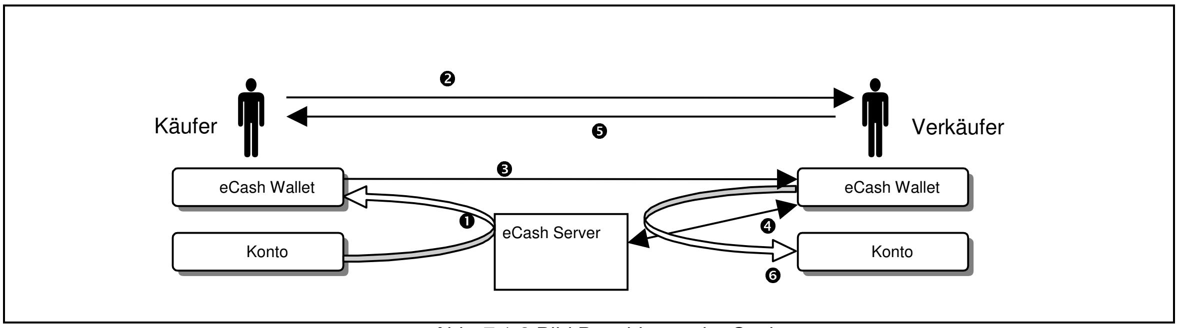

Abb. 7.1.2 Bild Bezahlung mit eCash

1. Überschreitet der Kaufpreis das aktuelle Guthaben im eCash-Wallet, muß der Käufer zuerst virtuelle Münzen von eCash herunterladen. Hierzu startet er die eCash-Wallet-Software, gibt den zu herunterladenden Betrag ein und identifiziert sich durch Eingabe seines Passwortes. Die Software stellt eine Verbindung zum eCash-Server (sog. Mintserver) her und überträgt die virtuellen Münzen bei erfolgreicher Autorisierung. Der Transfer der virtuellen Münzen vom Server zum Wallet läuft transaktionsgeschützt ab, so daß entweder alle oder keine Münzen übertragen werden.
2. Der Kunde gibt seine Bestellung auf und wählt als Bezahlmöglichkeit eCash.
3. Die benötigte Menge an virtuellen Münzen wird vom Wallet des Käufers zum Verkäufer transaktionsgeschützt und verschlüsselt übertragen.
4. Der Verkäufer kann sich die Echtheit der virtuellen Münzen vom eCash-Server bestätigen lassen.

5. Es erfolgt die Auslieferung der Ware
6. Die virtuellen Münzen, die der Verkäufer erhalten hat, können zu weiteren Einkäufen genutzt werden oder an eCash geschickt werden, die dann per Überweisung gutgeschrieben werden.

7.2 Sicherheit

Beim Entwurf von eCash, bei dem „Geld" über das Internet übertragen wird, wurde besonderer Wert auf die Sicherheit gelegt. Das Wallet des Käufers ist durch zwei Passwörter gesichert, alle Daten werden per RSA Verschlüsselung mit 768 Bit, Triple DES und SHA-1 (hier nicht weiter vertieft) gesichert, was zur Zeit ein Höchstmaß an Sicherheit bietet und einen Diebstahl der virtuellen Münzen ausschließen soll.
Besondere Probleme entstehen jedoch durch die geforderten Eigenschaften der Anonymität und der gleichzeitigen Garantie, daß auch bei einem Festplattenfehler kein Münzverlust zu Stande kommen kann.

Dies wird durch ein spezielles kryptographisches Verfahren, das sog. Blinding sichergestellt.

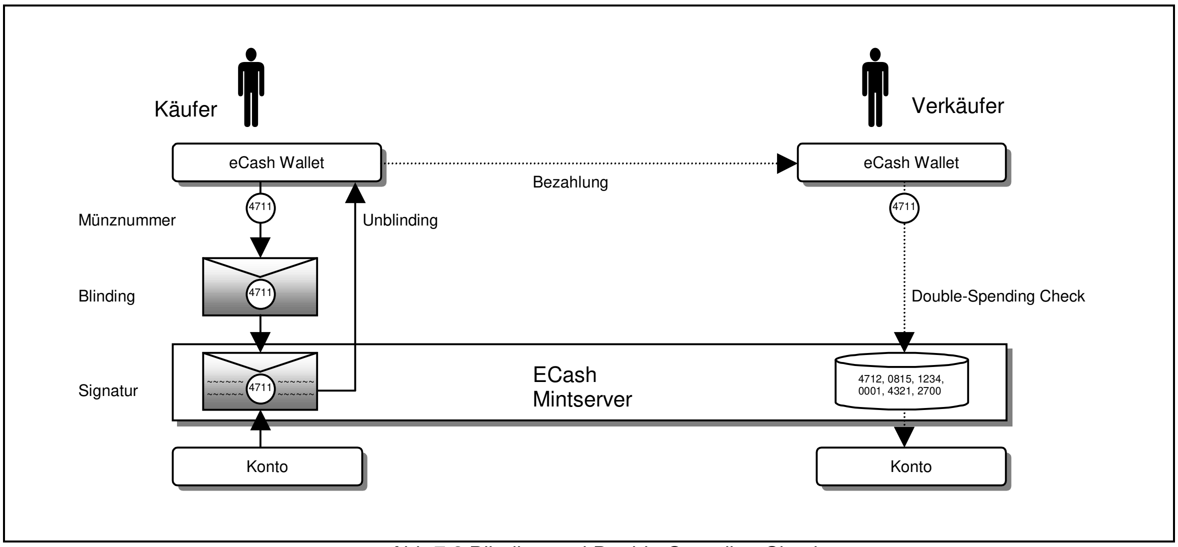

Abb 7.2 Blinding und Double-Spending Check

Der Käufer verpackt Münznummern in einen digitalen Umschlag (siehe Abb. 7.2), der durch den Blinding-Algorithmus erzeugt wird und den die Bank nicht einsehen kann. Die Bank signiert den Umschlag und sendet ihn an der Käufer zurück, der damit im Besitz von gültigen Münzen ist. Da diese Münzen nur einfache Ziffernfolgen darstellen und somit problemlos kopiert werden können, wird bei jeder Zahlung ein sog. „double spending check" durchgeführt, der sicherstellt, daß jeder Münze nur einmalig existiert.

7.3 Bewertung

- Die Bezahlung mit eCash kommt der Bezahlung mit herkömmlichen Bargeld sehr nahe.
- Geringe Akzeptanz weltweit, aber gute Wachstumschancen
- nur für Micropayment (vgl. Abschnitt 3.1.2) geeignet

- **Vertraulichkeit**, **Integrität**, **Identität** und **Authentizität** (vgl. Abschnitt 2.1.2) werden sichergestellt. **Anonymität** wird garantiert.
- **Nachvollziehbarkeit** ist über die Wallet-Software jederzeit möglich.
- **Unterbrechung des Einkaufsvorganges** findet nicht statt, da die Bezahlung im Internet innerhalb weniger Sekunden ohne größeren Aufwand (für Käufer und Verkäufer) durchgeführt wird.
- **Medienbruch** ist durch die fehlende Medienunabhängigkeit gegeben.
- **Minimale Zusatzausrüstung**: es ist lediglich die Installation von Software notwendig

KAPITEL 8 CYBERCOINS

CyberCoins stellen ein vergleichbares Verfahren wie eCash dar. In Deutschland wird es als Pilotprojekt der Dresdner Bank betrieben. Da der Bezahlvorgang mit CyberCoins nahezu identisch mit dem von eCash ist, wird im weiteren darauf nicht eingegangen.

CyberCoins sind im Gegensatz zu eCash viel stärker verbreitet. Sie werden von ca. 20.000 Händlern weltweit akzeptiert, in Deutschland sind es 37. eCash hat lediglich 500 Händler. In den USA unterstützen bereits 80% der Banken CyberCoin-Transaktionen. Im Jahr 2000 wurden 1 Mio. Transaktionen weltweit ausgeführt.

KAPITEL 9 TELEFONRECHNUNGSBASIERTES MICROPAYMENT

Dieses Kapitel stellt das telefonrechnungsbasierte Micropayment am Beispiel von net900 vor.

9.1 net900

Hersteller von net900 ist die Firma „in medias res“. Es wird zur Zeit von Net Pay, TeleCash und der Deutschen Telekom angeboten und wurde speziell für das Micropayment im Internet entwickelt. Beträge, die über net900 anfallen, werden direkt über die Telefonrechnung abgerechnet.
Net900 setzt voraus, daß die Internetverbindung modembasiert ist. Des weiteren muß die Net900 Software bei einem Käufer installiert sein.

9.2 Funktionsweise

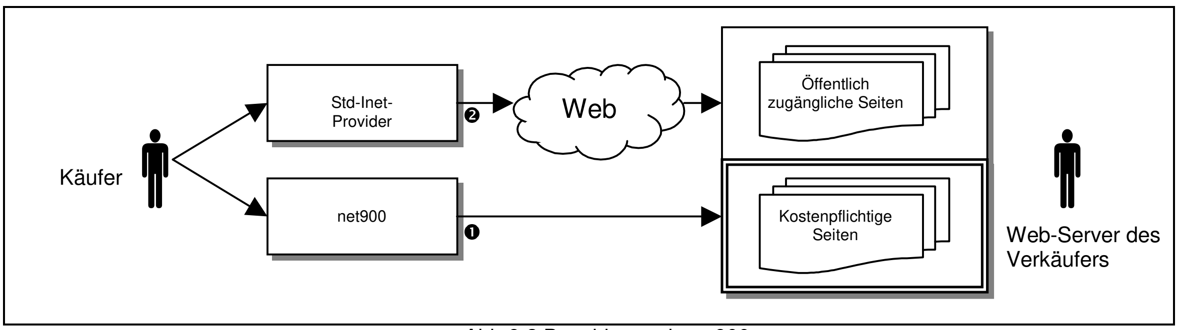

Abb 9.2 Bezahlung mit net900

1. Ruft ein Käufer ein kostenpflichtiges Angebot im Internet auf, das über net900 tarifiert ist, unterbricht die net900 Software die aktuelle Internetverbindung und ruft eine höher tarifierte 0192xx Nummer an und verbindet sich anschließend mit dem kostenpflichtigen Angebot.
2. Nach der Nutzung wird die Verbindung zum net900 beendet und die Internetverbindung über den Standard-Provider wird wieder hergestellt.

9.3 Sicherheit

Als einzige Sicherheitsmaßnahme sieht Net900 eine Bestätigung vor, bevor die Verbindung zur höher tarifierten 0192xx Nummer aufgebaut wird.

9.4 Vergleichbare Verfahren

Ein vergleichbares Verfahren zu net900 stellt „dtms @ cash“ dar, das von der AASP GmbH entwickelt wurde. Hierbei wird eine frei tarifierte 01900 Verbindung aufgebaut.

Das von der Firma BeLingua Systems entwickelte Verfahren „WebCoinBox“ und „infin“, das von der Ingenieurgesellschaft für Informationstechnologien entwickelt wurden, nutzen den Anruf bei einer 01900-Nummer, um für ein kostenpflichtiges Angebot im Internet dem Nutzer einen Zugangscode mitzuteilen. Dieser erlaubt die zeitlich begrenzte Nutzung des Angebotes, nachdem der Zugangscode auf der Webseite eingeben wurde. Nach Ablauf dieser Zeitspanne muß erneut ein Anruf getätigt werden.

9.5 Bewertung von telefonrechungsbasierten Zahlungsverfahren

- nur für Micropayment (vgl. Abschnitt 3.1.2) geeignet
- **Vertraulichkeit**, **Integrität**, **Identität** und **Authentizität** (vgl. Abschnitt 2.1.2) werden im Rahmen der Sicherheitseinrichtungen der Telefongesellschaft sichergestellt. **Anonymität** kann gegenüber dem Anbieter garantiert werden.
- **Nachvollziehbarkeit** ist nur über eine Telefonrechnung mit Einzelverbindungsnachweis möglich. Während die Verbindung zum Anbieter besteht, lassen sich die anfallenden Kosten nur abschätzen oder mit Hilfe von spezieller Software berechnen.
- **Unterbrechung des Einkaufsvorganges** findet immer statt, da die Bezahlung im Internet wegen des **Medienbruches**, der durch die fehlende Medienunabhängigkeit entsteht, gegeben ist.
- **Minimale Zusatzausrüstung**: es ist lediglich die Installation von Software notwendig

KAPITEL 10 MULTIZAHLUNGSVERFAHREN

Multizahlungsverfahren stellen Kombinationen der verschiedenen Klassen von elektronischen Bezahlverfahren dar (vgl. Abschnitt 3.2). Da es zur Zeit noch kein elektronisches Bezahlverfahren gibt, das sowohl für Micro- als auch für Macropayment geeignet ist und gleichzeitig eine hohe Akzeptanz findet, stellen Multizahlungsverfahren zur Zeit die einzige Möglichkeit dar, sicherzustellen, in nahezu jedem Onlineshop bezahlen zu können.

10.1 Powercash 21

Powercash 21 wurde von den deutschen Sparkassen entwickelt und stellt eine Kombination von Kreditkarte für Macropayments und CyberCash für Micropayments dar. Durch SSL (siehe Abschnitt 4.3) und SET (siehe Abschnitt 4.4) soll der Bezahlvorgang im Internet abgesichert werden. Eine zusätzliche Zahlungsgarantie wir über eTrustco (siehe Abschnitt 6.1) sichergestellt.

KAPITEL 11

In diesem Kapitel soll ein Überblick über die existierenden elektronischen Bezahlverfahren gegeben werden.

	Spezielle Hardware	Spezielle Software	Anmeldung erforderlich	Spezielle separate Verbindung erforderlich	Trusted Third Party	Spezielle Zertifikate erforderlich	Für Micropayment geeignet	Für Macropayment geeignet	Vertraulichkeit	Integrität	Identität	Authentizität	Anonymität (garantiert)	Unterbrechung des Einkaufsvorganges	Rolle des Datenbanksystems
Kreditkarte klassisch			X					X							Nur Speicherung von Transaktionen
Kreditkarte mit SET			X			X		X	X	X	X	X			Nur Speicherung von Transaktionen
Geldkarte	X	X	X				X		X	X	X	X			Nur Speicherung von Transaktionen
E-Trustco		X	X		X	X	X	X	X	X	X	X			Speicherung von Transaktionen und Zertifikaten
Paybox	X		X	X	X			X	X	X	X	X		X	Nur Speicherung von Transaktionen
Click&buy			X		X		X		X	X	X	X			Nur Speicherung von Transaktionen
ECash		X	X				X		X	X	X	X	X		Speicherung von virtuellen Münzen
CyberCoins		X	X				X		X	X	X	X	X		Speicherung von virtuellen Münzen
Net900		X		X			X		X		X	X		X	Speicherung von Verrechnungsinformationen
Dtms @ cash		X		X			X		X		X	X		X	Speicherung von Verrechnungsinformationen
Infin				X			X		X		X	X		X	Speicherung von Verrechnungsinformationen
WebCoinBox				X			X		X		X	X		X	Speicherung von Verrechnungsinformationen
PowerCash21		X	X				X	X	X	X	X	X			Speicherung von Transaktionen und Zertifikaten und virtuellen Münzen

KAPITEL 12

Ausblick

Nachdem nun ein Teil der zur Zeit existierenden elektronischen Bezhalverfahren vorgestellt wurde ist deutlich geworden, daß sich außer der Kreditkarte kein Zahlungsmittel bisher weltweit etabliert hat. Die Vielzahl der kleinen Anbieter, deren Zahlungsmittel in der Regel untereinander nicht ausgetauscht werden können und nur für die Bezahlung bei wenigen Akzeptanzstellen dienen, erklärt sich an den hohen Umsatzerwartungen, die für elektronische Bezahlverfahren existieren und somit einen attraktiven Markt bieten.

Doch die Unbequemlichkeit für den Verbraucher, für unterschiedliche Anbieter jeweils andere Bezahlverfahren anzuschaffen, wird auf Dauer keine Akzeptanz finden, weshalb Lösungen, bei denen der Verbraucher nur einen Anbieter von elektronischen Bezahlverfahren benötigt, vorzuziehen sind. American Express etabliert z.B. zur Zeit „Blue" eine neue Smartcard-Kreditkarte auf der Basis von Sun Microsystems JavaCard. Hierbei kann der Benutzer aus dem Internet JavaCard-Applets auf der Karte installieren, die elektronische Bezahlverfahren abbilden, womit das Ziel der „eine Karte für Alles" näher rückt.

QUELLEN

[MAN99] N. Gregory Mankiw, „Grundzüge der Volkswirtschaftslehre“, Schäfer-Poeschel Verlag 1999
[KRS20] J. Krause , „E-Commerce und Online Marketing“, 2.Auflage, Hanser Verlag 2000
[PRA99] Brigitte Preißl, Hansjörg Haas, „E-Commerce – Erfolgsfaktoren von Online-Shopping in den USA und Deutschland“, Duncker & Humbolt; 1999

[BMS20] Prof. Dr. Dieter Baums, „Internet Payment SK Online“, Vortragszusammenfassung 1.12.2000

[HBCI] http://public.deutsche-bank.de/global/ui/home_ec.nsf/doc/OEBE-4NWGPX?OpenDocument
[OTP] http://www.mastercard.com → Suche nach OTP
[WEBDB] http://www.deutsche-bank.de
[WEBDR] http://www.dresdner-bank.de

[MCRD] http://www.mastercard.de, http://www.mastercard.com/ourcards/smartcard
[VISA] http://www.visa.de
[AMEX] http://home3.americanexpress.com/germany/personal_main.asp

[SSL] vgl. [HBCI] → SLL
[SET] vgl. [HBCI] → SET

[GKTE] http://www.sparkasse.de/artikel/0,4705,621,00.html
[GMSE] http://www.cashmouse.de/

[ETR] http://www.e-trusco.de/a2_leistungen/index.html
[PBX] http://www.Paybox.de
[FGT] http://www.Firstgate.de

[ECSH] http://www.e-cash.com
[CCNE] http://www.cybershops.de/infos/bezahlverfahren.html

[NET9] http://www.in-medias-res.com/

[JCRD] http://java.sun.com/products/javacard

Weitere Links zum Thema:

[MCMS] http://www.mobilecommerceworld.com
[EPAY] http://www.epaynews.com

Stand der Internetlinks 1.6.2001