Technische Universität München

Forschungs- und Lehreinheit Informatik III
Prof. R. Bayer Ph.D., Prof. Dr. D. Kossmann

Hauptseminar Informatik im Sommersemester 2003

Web Services

Zahlungssysteme und Sicherheit

Referentin: Katy Kirsche

Betreuer: Prof. R. Bayer Ph.D

Abgabetermin: 28. Mai 2003

Vortragstermin: 5. Juni 2003

Inhaltsverzeichnis

1. Einleitung

Das Internet stellt aufgrund seiner weiten Verbreitung und seines enormen Wachstums ein großes Potential für den Ecommerce dar, d.h. für das Kaufen und Verkaufen von Produkten, Informationen und Dienstleistungen über elektronische Netze. Händler können ohne viel Aufwand ihre Produkte im Internet anbieten und eine Kundschaft in der ganzen Welt erreichen. Um dieses Kundenpotential nutzen zu können, sind sichere und effiziente Zahlungssysteme erforderlich.
Die konventionellen Zahlungsverfahren wie Nachnahme, Lastschrift, Scheck und Überweisung finden nach wie vor für Bezahlvorgänge im Internet ihre Verwendung. Bei diesen Verfahren wird das Internet aber nur als Bestellmedium genutzt und nicht für die Zahlungen selbst. Es wurden deshalb in letzter Zeit mehr oder weniger erfolgreiche Versuche unternommen, elektronische Zahlungssysteme, die das Internet tatsächlich für die Zahlungsvorgänge benutzen, zu entwickeln und am Markt zu etablieren.
Das Internet ist ein sehr unsicheres Übertragungsmedium. Einen Einkauf könnte man sich folgendermaßen vorstellen: Auf einem Marktplatz rufen sich alle Händler gleichzeitig ihre Angebote zu. Man ruft dem Händler, für dessen Angebot man sich interessiert, das Gegengebot zu, wobei jeder andere zuhören kann. Ist man sich einig, wirft der Käufer dem Händler das Geld und der Händler dem Käufer die Ware zu. Ware wie Geld können also ohne weiteres in falsche Hände geraten oder gegen Falschgeld und minderwertigere Ware ausgetauscht werden.
Dieses Szenario verdeutlicht, daß die Sicherheit bei Zahlungssystemen eine große Rolle spielt. Der Zahlungsvorgang muß wohl organisiert sein, damit das Bezahlen im Internet sicher, effizient und bequem ist.

Zunächst sollte man sich allgemein den Einkaufs- und Bezahlvorgang und die daran beteiligten Akteure genauer betrachten (Kapitel 2).
Zum weiteren besseren Verständnis ist es nötig, die elektronischen Zahlungssysteme zu klassifizieren, um einen Überblick über die unterschiedlichen Grundkonzepte zu bekommen (Kapitel 3).
Die Schwierigkeiten bei elektronischen Zahlungssystemen lassen sich besser verstehen, wenn man sich die mannigfaltigen Anforderungen an ein solches System betrachtet (Kapitel 4).
In diesem Zusammenhang ist es ebenso hilfreich, sich die zahlreichen Angriffs- und Betrugsmöglichkeiten bei Zahlungssystemen vor Augen zu führen (Kapitel 5).
Diese rechtfertigen den vermehrten Einsatz verschiedenster komplexer kryptographischer Verfahren und Sicherungsmechanismen (Kapitel 6).
Wie diesen zahlreichen Anforderungen nachgekommen wird, zeigt die Beschreibung verschiedener Zahlungssysteme (Kapitel 7).
Abschließend stellt sich die Frage über Erfolg und Mißerfolg der Zahlungssysteme im Internet, und soviel sei vorab schon verraten, dies ist meistens eine Frage des Mißerfolgs. Deshalb wird der Schwerpunkt dieser Arbeit auf Erklärungen und Darstellungen grundsätzlicher Art gelegt. Es soll damit ein Einblick in die Schwierigkeiten, die mit der Entwicklung und Implementierung elektronischer Zahlungssysteme einhergehen, gegeben werden.

2. Einkaufs- und Zahlungsszenario im Internet

Jede Bezahlung im Internet setzt zunächst den Einkauf oder Konsum eines Produktes oder einer Dienstleistung voraus. Zunächst wird also in diesem Kapitel ein Einkaufsvorgang im Internet beschrieben, dann werden die an einem Zahlungsvorgang beteiligten Akteure vorgestellt und schließlich die Basisarchitektur eines jeden elektronischen Zahlungssystems erklärt.

2.1. Einkaufsvorgang im Internet

Kaufvorgänge im Internet erfolgen in fünf Schritten:

1. Der Händler bietet seine Waren oder Dienste über einen WWW-Server an. Der Kunde findet auf der WWW-Seite alle Informationen über das Produkt und eine Auflistung der Zahlungsmöglichkeiten.
2. Der Kunde meldet nun beim Händler Kaufinteresse an. Dazu gibt er auch Auskunft über die gewünschte Zahlungsart.
3. Der Händler sendet den zu zahlenden Preis in der jeweiligen Währung.
4. Der Kunde antwortet mit der gleichen Preis- und Währungsangabe und einem sogenannten Zahlungsobjekt. Dieses Zahlungsobjekt kann von unterschiedlichen Herausgebern (Banken) stammen und unterschiedliche Zahlungsarten repräsentieren. Es kann einen bestimmten Geldwert darstellen (anonymes, digitales Bargeld) oder Informationen zum Bankkonto des Kunden enthalten (Einzugsermächtigung, Kreditkarteninformationen).
5. Nachdem der Händler die Zahlung erhalten hat, stellt er dem Kunden eine digitale Quittung aus und sendet die gewünschte Ware an den Kunden.

2.2. Akteure bei einem Zahlungsvorgang

Der **Kunde** möchte gerne bequem und sicher über das Internet bezahlen können, um rund um die Uhr Waren oder auch Dienstleistungen einkaufen und sofort beziehen zu können. Dazu sollten ihm kundenfreundliche, sichere und effiziente Zahlungssysteme zur Verfügung stehen.

Das Internet bietet für den **Händler** ein großes Kundenpotential, daß er durch die Repräsentation und die Verkaufsmöglichkeit im Internet nutzen kann. In der Regel hat er die Kosten des bargeldlosen Zahlungsverkehrs zu tragen, die aber mit dem zusätzlichen Umsatz leicht ausgeglichen werden können. Außerdem hat der Händler die Möglichkeit, basierend auf, natürlich freiwillig gegebenen, Kundeninformationen, Kundenprofile zu erstellen, die ihm bei Strategie- und Marketingentscheidungen nützlich sein können.

Der **Systemarchitekt** entwickelt ein Zahlungssystem und prägt den Produktnamen seines Systems (branding). Er kann kostenpflichtige Lizenzen an die Systembetreiber vergeben, oder seinen Nutzen aus der weiteren Verbreitung seines Brandings ziehen (z.B. VISA und MasterCard mit dem SET Standard).
Der Systemarchitekt muß das Zahlungssystem gemäß den sich ständig ändernden technischen Standards laufend weiterentwickeln.

Der **Systembetreiber** vermittelt zwischen Händler und Banken. Er leitet alle Händlereinnahmen an die entsprechenden Banken weiter und wickelt für den Händler das Clearing, also den Kontenausgleich zwischen den beteiligten Banken, ab. Er ist für die Installation und die Wartung des Systems bei Kunden und Händlern verantwortlich. Er finanziert sich durch

Gebühren, Umsatzbeteiligungen und Dienstleistungen. Oftmals fungieren die Banken selbst als Systembetreiber.

Die **Banken** führen die Konten der Kunden und der Händler und stellen ihre Infrastruktur für die Zahlungsvorgänge zur Verfügung.
Es empfiehlt sich, Banken als Herausgeber von elektronischen Zahlungssystemen zuzulassen, da somit die rechtlichen Anforderungen am besten erfüllt werden können. Die Öffentlichkeit vertraut diesen Institutionen, und die Kunden können gegen die Folgen eines Konkurses geschützt werden. Bei kreditkartenbasierten Zahlungssystemen sind außerdem die **Kreditkartenfirmen** beteiligt.

Neben diesen Hauptakteuren spielen sogenannte **dritte Parteien** je nach Implementierung eine mehr oder weniger große Rolle beim Bezahlvorgang. Es kann z.B. ein **Prüfungsstelle** für bestimmte Überprüfungsvorgänge beteiligt sein (Payment-Gateway beim SET-Standard). **Zertifizierungsstellen** (**Trust Center**) erfüllen die wichtige Aufgabe des Schlüssel-managements. Sie sorgen als staatlich zertifizierte Instanzen für die sichere Verteilung der Schlüssel an die beteiligten Akteure und garantieren somit deren Identität.
Sicherheit der Zahlungssysteme hängt also in hohem Maße von der vertrauenswürdigen Infrastruktur der Trust Center ab. Diese Infrastruktur ist zumeist hierarchisch aufgebaut (chain of trust) und es gibt verschiedene Konzepte, wie sich die Trust Center untereinander austauschen und die Zertifikate und Schlüssel überprüfen können [ibis03]. Die Anbieter von Trust-Center-Diensten müssen strenge gesetzliche Vorgaben erfüllen. Diese gewährleistete Sicherheit wird von den Kunden, Händlern, Systembetreibern und Banken finanziert.

2.3. Zahlungsszenario im Internet

Der **Zahlende** (Payer) ist in diesem Szenario der Kunde (Customer). Er zahlt an den **Zahlungsempfänger** (Payee), d.h. den Händler (Merchant). Synonym verwendet man auch die Bezeichnungen Käufer oder Nutzer für den Kunden, bzw. Verkäufer oder Provider (Internetprovider) für den Händler.
Diese beiden Parteien stehen jeweils mit ihrer Bank in Verbindung. Für den Kunden ist dies die **Kundenbank** (Issuer), für den Händler die **Händlerbank** (Acquirer). Kunde und Händler müssen nicht notwendigerweise bei derselben Bank ihre Konten haben. Die Banken stehen durch das Bankennetzwerk in Verbindung zueinander, um das sogenannte Clearing, die Überprüfung der Zahlungsfähigkeit und der Abgleich der Konten, vornehmen zu können.
Manche Zahlungssysteme sehen die Rolle eines Brokers vor. Ein **Broker** ist eine Kombination von Issuer und Acquirer, der von Kunden und Händlern gleichermaßen genutzt wird.
Zusätzlich können **dritte Parteien** involviert werden, wie z.B. Trust Center oder spezielle, vom Systembetreiber eingerichtete, Prüfungsstellen. Die Beteiligung dieser Akteure hängt von der Implementierung des Zahlungssystems ab.

Käufer, Händler und die Banken müssen über spezielle **Soft- und Hardware** verfügen. Der Käufer muß eine digitale Geldbörse (wallet) auf seinem Rechner installieren. Zusätzlich bedarf es bei manchen Systemen noch eines Chipkarten-Lesegerätes, das mit der installierten Software zusammenarbeitet. Der Kunde ist der einzige Beteiligte, der selbst aktiv wird und den Zahlungsvorgang manuell auslösen muß, z.B. durch Anklicken eines entsprechenden Buttons.
Die Software des Händlers und der Banken bearbeitet die Zahlungsvorgänge automatisch. Dabei benötigt der Händler eine digitale Kasse (till) und die Banken digitale Schalter (counters), um die Interaktion mit den Kunden effizient und sicher abwickeln zu können.

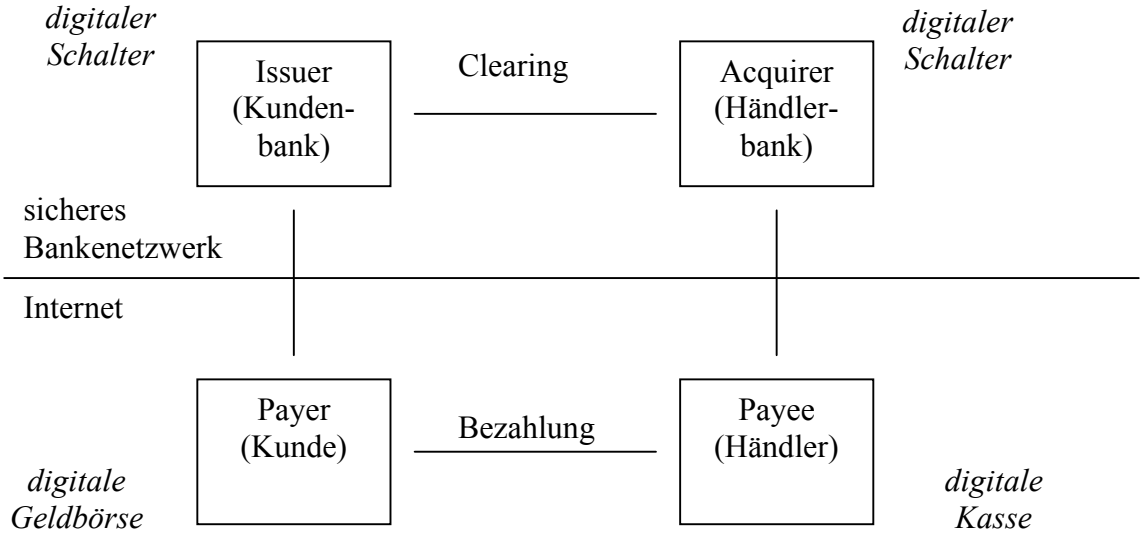

Abbildung 2.3.: Szenario eines elektronischen Zahlungsvorgangs

3. Anforderungen an ein Zahlungssystem

Ein sicheres, effizientes und vor allem benutzerfreundliches elektronisches Zahlungssystem stellt eine Fülle von Anforderungen, die sich in die Kategorien Sicherheit, Funktionalität und Wirtschaftlichkeit einordnen lassen.

3.1. Sicherheitsanforderungen

Vertraulichkeit: Bei einer Zahlung über ein elektronisches Zahlungssystem gibt der Kunde vertrauliche Daten preis. Da das Internet allein aber keine Vertraulichkeit gewährleistet, können diese Daten leicht in die Hände von Betrügern gelangen. Deshalb sind die Authentisierung der Teilnehmer und Verschlüsselungsmaßnahmen bei der Nachrichtenübermittlung ebenso wichtig wie der gewissenhafte Umgang mit diesen Daten auf Seiten des System-Betreibers (z.B. Zugangs- und Zutrittkontrolle zu den Kundendatenbanken, Verschlüsselung der Daten). Ein weiterer Aspekt ist der Schutz vor Beobachtung und Auswertung von Dauer, Häufigkeit, Quelle und Zielpunkt der Datenübertragung.
Authentisierung: Die Identität der Teilnehmer sollte immer auf Korrektheit überprüft werden, damit jeder Empfänger von Daten auch gewiß sein kann, die Daten von dem Sender zu bekommen, der er vorgibt zu sein, und damit jeder Sender gewiß sein kann, daß er seine Daten an den Empfänger sendet, der er vorgibt zu sein.
Autorisierung: Es muß gewährleistet sein, daß nur berechtigte Mitarbeiter Zugriff auf die kundenspezifischen Daten haben.
Integrität: Die Inhalte einer Zahlung sollen unverändert übertragen werden. Diese Sicherheit vor Manipulation der Daten gewährleistet Betrugssicherheit aber auch Fehlerrobustheit. Digitales Geld sollte fälschungssicher sein und nicht doppelt ausgegeben werden können.
Anonymität: Die Anonymität der Nutzer oder auch der anderen beteiligten Akteure sollte bewahrt werden. Es sollte nicht möglich sein, die individuellen Zahlungsmuster zu überwachen oder auch die Quellen des Einkommens bestimmen zu können. Die Anforderung der Anonymität stellt sich insbesondere für Zahlungssysteme, die mit elektronischem Geld arbeiten, da sie denselben Komfort versprechen, wie ihn richtiges Bargeld bietet. Grundsätzlich sollte gelten, daß die Kosten zur Verfolgung von Zahlungsvorgängen den Nutzen der damit gewonnen Information übersteigen sollten.
Pseudonymität: Schwache Anonymität kann durch die Verwendung von Pseudonymen erreicht werden. Die Teilnehmer verwenden eine andere Benennung als ihren Namen.
Unverkettbarkeit: Es sollte unmöglich sein, aus den einzelnen Bezahlvorgängen z.B. Profile über die Kaufgewohnheiten der Teilnehmer zu erstellen.
Nichtortbarkeit: Diese Anforderung wird an mobile Zahlungssysteme gestellt. Es sollte weder den Teilnehmern noch Dritten möglich sein, den momentanen Aufenthaltsort des Kunden ausfindig machen zu können, sonst besteht u.a. die Gefahr der Erstellung von Bewegungsprofilen.
Verfügbarkeit: Ein Zahlungssystem sollte für den Benutzer jederzeit zugänglich und verfügbar sein. Die Zahlungssystemserver sollten deshalb ständig betriebsbereit und zugreifbar sein. Kommt es dennoch zu einem Systemabsturz, z.B. durch einen Angriff von außen, so sollte eine schnelle Rückkehr zum geordneten Betrieb möglich sein. Robuste Systeme können den Betrieb auch beim Ausfall von Komponenten zumindest in Teilen aufrecht halten.
Zuverlässigkeit: Ein Zahlungssystem sollte zuverlässige, d.h. fehlertolerante und betriebsichere Soft- und Hardware einsetzen. Bei einem Systemausfall sollte der letzte konsistente Zustand einer Transaktion, bzw. eines Kontos wieder hergestellt werden, damit keine Geldwerte verloren gehen. Der störungsfreie Betrieb hat absolute Priorität.
Zurechenbarkeit: Es sollte stets möglich sein, zu einzelnen Zahlungshandlungen den

Urheber bzw. Verantwortlichen ermitteln zu können. Somit kann Betrug aufgedeckt werden. Diese Forderung widerspricht allerdings der Forderung nach Anonymität. Es liegt am Zahlungssystembetreiber in diesem Spannungsfeld abzuwiegen.
Nichtrückweisbarkeit/Verbindlichkeit: Sender und Empfänger müssen vor der Abstreitung einer Nachrichtenübertragung geschützt werden. Wenn eine Nachricht geschickt wurde, kann der Empfänger beweisen, daß der angebliche Absender diese Nachricht auch wirklich geschickt hat. Umgekehrt kann der Empfänger den tatsächlichen Erhalt einer Nachricht nicht leugnen. Ein Kunde kann somit eine Zahlungsanweisung nicht abstreiten.
Hardware: Manche Zahlungssysteme setzen Hardware zur Speicherung der Geldwerte und/oder der kryptographischen Schlüssel ein. Dabei muß gewährleistet werden, daß diese Hardware tatsächlich sicher gegenüber Manipulationsversuchen ist und auch mit neuester Technologie nicht geknackt werden kann.

3.2. Funktionalitätsanforderungen

Transaktionalität: Durch Störungen im Internet können Zahlungstransaktionen unterbrochen werden, was zu Geldverlust führen kann. Ein Zahlungssystem sollte solche Störungen ausgleichen, indem die Transaktionen entweder vollständig ausgeführt oder zurückgesetzt werden. Um dies gewährleisten zu können, sollten die Transaktionen atomar, konsistent und isoliert voneinander ablaufen.
Bidirektionalität: Es sollte dem Kunden eines Zahlungssystems möglich sein, selbst Zahlungen empfangen zu können, so daß z.B. auch Geldrückerstattungen möglich sind. So kann auch ein Handel zwischen Privatpersonen stattfinden.
Mehrwährungsfähigkeit: Um einen weltweiten Handel im Internet zu ermöglichen und die Akzeptanz eines Zahlungssystems zu erhöhen, sollte es dem Nutzer möglich sein, mit verschiedenen Währungen zahlen zu können.
Rücktauschbarkeit: Der Nutzer sollte jederzeit sein elektronisches Geld in konventionelles Geld zurücktauschen können.
Flexibilität: Ein Zahlungssystem sollte verschiedene Zahlungsmöglichkeiten anbieten, die in einem gemeinsamen Framework integriert werden sollten, wie z.B. Zahlung mit Kreditkarte, mit Scheck oder mit digitalen Bargeld.
Konvertierbarkeit: Der Kunde sollte die elektronischen Zahlungsmittel eines Zahlungssystems in die Zahlungsmittel eines anderen System konvertieren können. Dies gilt ebenfalls für Zahlungsmittel in einer bestimmten Währung. Schließlich soll er je nach Situation das am besten geeignete Zahlungsmittel nutzen können, ohne dabei Verluste hinnehmen zu müssen.
Portabilität: Das Zahlungssystem sollte plattformunabhängig sein.
Skalierbarkeit: Ein elektronisches Zahlungssystem sollte einen Zuwachs an Benutzern und Händlern ohne große Schwierigkeiten und Leistungsverluste kompensieren können. Ein Problem beim Ausbau von Zahlungssystemen sind vor allem zentrale Server, die bei erhöhten Nutzer- und Händleraufkommen einen Engpaß darstellen können. Mit der Nutzung von mehreren Servern, die über das Land verteilt sind, könnte dieser Schwachstelle Abhilfe geleistet werden.
Ebenso vermindern die Verfahren, mit denen man der Mehrfachausgabe von digitalem Geld Einhalt gebieten will, die Erweiterbarkeit von Zahlungssystemen. Je mehr Nutzer mit digitalem Geld bezahlen, desto mehr Münzen müssen in einer zentralen Datenbank zur Prüfung von Zahlungen gespeichert werden, um den Betrug durch Mehrfachausgabe und Kopieren des digitalen Geldes aufzudecken. Diese Datenbanken werden immer größer und bereiten große Probleme durch die damit verursachten Kosten.
Durchgängigkeit der IT-Mittel: Ein Zahlungssystem sollte Medienbrüche vermeiden. Wenn der Kunde eine Zahlungstransaktion über das Internet erledigt, möchte er nicht, daß er z.B. seine Kreditkartennummer per Telefon angeben muß. Medienbrüche verringern die

Akzeptanz eines Systems.
leichte Bedienbarkeit: Benutzer sollten nicht immer während des Zahlvorganges aufgehalten werden, indem sie vom Zahlungssystem nach Informationen gefragt werden. Es wäre also besser, wenn die Zahlungen weitestgehend automatisch ablaufen.
Aber dem Nutzer sollte es dennoch möglich sein, seine Ausgaben zu limitieren. Zahlungen, die einen bestimmten Betrag übersteigen, sollten eine explizite Bestätigung erfordern. Der Nutzer sollte ohne viel Aufwand seine Ausgaben kontrollieren können. Das Auslösen der Zahlungstransaktion sollte eindeutig angezeigt werden.
leichte Inbetriebnahme und Installierbarkeit: Ein elektronisches Zahlungssystem sollte einfach und ohne spezielle (PC-)Systemkenntnisse zu installieren und in vertretbarer Zeit in Betrieb zu nehmen sein.

3.3. Wirtschaftlichkeitsanforderungen

Effizienz: Gerade im Micropayment-Bereich sind häufige Zahlungen von Kleinstbeträgen die Regel. Das Zahlungssystem muß in der Lage sein, diese vielen Zahlungsvorgänge ohne Verringerung der Leistung zu bewältigen. Die Kosten pro Transaktion sollten niedrig gehalten werden, so daß sie selbst bei häufigen Microzahlungen nicht ins Gewicht fallen.
geringe Fixkosten: Zu den Fixkosten zählen die Ausgaben für manipulationssichere Benutzerendgeräte wie etwa Chipkartenleser sowie die Grundgebühren für die Zulassung des Kunden als Nutzer eines Zahlungssystems und für den Internetzugang. Die Fixkosten hängen von der Anzahl der insgesamt mit einem Zahlungssystem durchgeführten Zahlungen ab.
geringe Transaktionskosten: Die wirtschaftlichen Transaktionskosten sind die Gebühren, die bei der Durchführung einer Transaktion erhoben werden. Die technischen Transaktionskosten sind die Kosten für die notwendigen Kommunikationsvorgänge, wie z.B. Telefonkosten, und die Kosten für die technischen Geräte des Kunden, z.B. den Rechner. Je schneller eine Transaktion über das Internet abgewickelt werden kann, desto niedriger fallen diese Kosten aus. Wird dem Händler als Zahlungsempfänger vom Zahlungssystembetreiber ein Abgeld berechnet, so wirkt sich das indirekt in der Preisgestaltung des Händlers für den Kunden aus.
Integrationsfähigkeit: Ziel ist die Abwicklung von Transaktionen ohne Methoden-, Medien und Verfahrensbruch. Zum einen sei hier die technische Integrationsfähigkeit der Zahlungssysteme genannt, die definierte Schnittstellen für die Kommunikation des Zahlungssystems mit dem Gesamtsystem voraussetzt, zum anderen die Integrationsfähigkeit in anwenderinterne Applikationen, wie z.B. Buchhaltungssysteme.
Akzeptanz: Die Akzeptanz hängt für die **Kunden** davon ab, wie viele Händler das Zahlungssystem unterstützen, d.h. welche Einkaufsmöglichkeiten sie haben. Arbeitet ein Zahlungssystem mit mehreren Banken zusammen, so erhöht das die Akzeptanz erheblich, da der Kunde nicht an eine Bank gebunden ist und es ihm möglich ist, mit Kunden anderer Banken Geschäfte abzuwickeln. Die Mehrwährungsfähigkeit erhöht ebenfalls die Akzeptanz.
Der Wert eines Zahlungssystem hängt für den **Händler** von der Größe der Teilnehmerzahl ab, da er möglichst viele neue potentielle Kunden erreichen will. Je größer die Nutzerzahl ist, desto größer ist die Bereitschaft eines Händlers, dieses Zahlungssystem zu unterstützen.
Diese zwei Akzeptanzanforderungen bedingen sich gegenseitig, wodurch sich für die Betreiber von Zahlungssystemen ein großes Problem ergibt: Sie können keine Kunden gewinnen, wenn sie nicht mit vielen registrierten Händlern werben können. Und sie können keine Händler gewinnen, wenn sie nicht mit vielen registrierten Kunden werben können. Es handelt sich also um ein klassisches **Henn-and-Egg-Problem**, was sich nur schwer lösen läßt und sicherlich ein Hauptproblem bei der Etablierung von Zahlungssystemen darstellt.

4. Klassifikation elektronischer Zahlungssysteme

Es gibt unterschiedliche Kriterien, nach denen man Zahlungssysteme einordnen und in verschiedene Klassen einteilen kann. Die Zahlungssysteme, die jeweils als Beispiel für eine Kategorie angegeben werden, werden in Kapitel 7 genauer vorgestellt:

4.1. Zeitpunkt der Zahlung

- „**Prepaid**"-Zahlungssysteme
  Der Kunde muß, bevor er die Zahlung ausführt, ein Guthaben auf ein Zahlungsmedium einzahlen. (z.B. Ecash, Geldkarte)
- „**Pay now**"-Zahlungssysteme
  Mit den Auslösen einer Zahlung wird sofort das Bankkonto des Kunden mit dem entsprechenden Betrag belastet (z.B. ec-Karte).
- „**Postpaid**" – Zahlungssysteme
  Die Zahlung ist genaugenommen eine Zahlungsanweisung. Die Abbuchung der Beträge erfolgt erst einige Zeit nach dem Kauf (z.B. Kreditkartenzahlung mit SET).

4.2. Geldmodel

- „**Noational Money"- oder Kontobasierte Zahlungssysteme**
  Geld existiert nur auf Konten. Es wird durch Verfügung des Zahlenden oder des Zahlungsempfängers vom Konto des Zahlenden auf das Konto des Zahlungsempfängers transferiert (z.B. Kreditkartenzahlung mit SET). Diese Systeme entsprechen den „**Postpaid**" – Zahlungssystemen, da der Konsum vor der Abbuchung vom Bankkonto erfolgt. **Scheckbasierte Zahlungssysteme** lassen sich ebenfalls hier zuordnen. Elektronische Schecks stellen digitale Forderungen dar, zu deren Verrechnung eine dritte Partei benötigt wird.
- **„Token Money" – oder „Cash-like (bargeldähnliche)"-Zahlungssysteme**
  Geld existiert in Form von digitalen Werteinheiten (Tokens), die in Form von Dateien auf dem PC (z.B. Ecash) oder auf Smart Cards (z.B. Geldkarte) gespeichert werden. Der PC oder die Smart Card fungieren dabei als elektronische Geldbörse. Die digitalen Münzen können wie echtes Bargeld weitergegeben werden, ohne das eine Kontoübertragung damit direkt verbunden ist. Diese Systeme entsprechen den „**Prepaid**" –Zahlungssystemen, da man das elektronische Geld erst gegen Bezahlung mit herkömmlichen Geld erhält.

4.3. Zahlungssystemmodelle

Die Zahlungssystemmodelle kann man in direkte oder indirekte Modelle einteilen. Dabei orientiert man sich an der **Zahlungskommunikation**, d.h. ob der Zahlende direkt oder indirekt während des Zahlvorgangs mit dem Zahlungsempfänger in Verbindung tritt.

Direkte Zahlungssysteme: Bei den direkten Zahlungssystemen, also den Systemen, in denen Zahlender und Zahlungsempfänger direkt in Verbindung zueinander treten, unterscheidet man nach dem **Geldmodel**:

- direkte „**Cash-like**" Zahlungssysteme
- direkte **kontobasierte** Zahlungssysteme

Indirekte Zahlungssysteme: Bei den indirekten Zahlungssystemen, also bei den Systemen, bei denen Zahlender und Zahlungsempfänger nicht in direkte Verbindung zueinander treten, unterscheidet man nach der **Initiierung des Zahlungsvorganges:**

- indirekte „**Push-like**“ – Zahlungssysteme
  Der Zahlende initiiert den Zahlungsvorgang, indem er seine Bank anweist, von seinem Konto einen bestimmten Betrag auf das Konto des Zahlungsempfängers zu überweisen (z.B. Online-Banking mit Überweisungsauftrag).

- indirekte „**Pull-like**“ – Zahlungssysteme
  Der Zahlungsempfänger initiiert den Zahlungsvorgang, indem er seine Bank anweist, den vereinbarten Betrag über die Bank des Zahlenden vom Konto des Zahlenden einzuziehen (z.B. elektronisches Lastschriftverfahren).

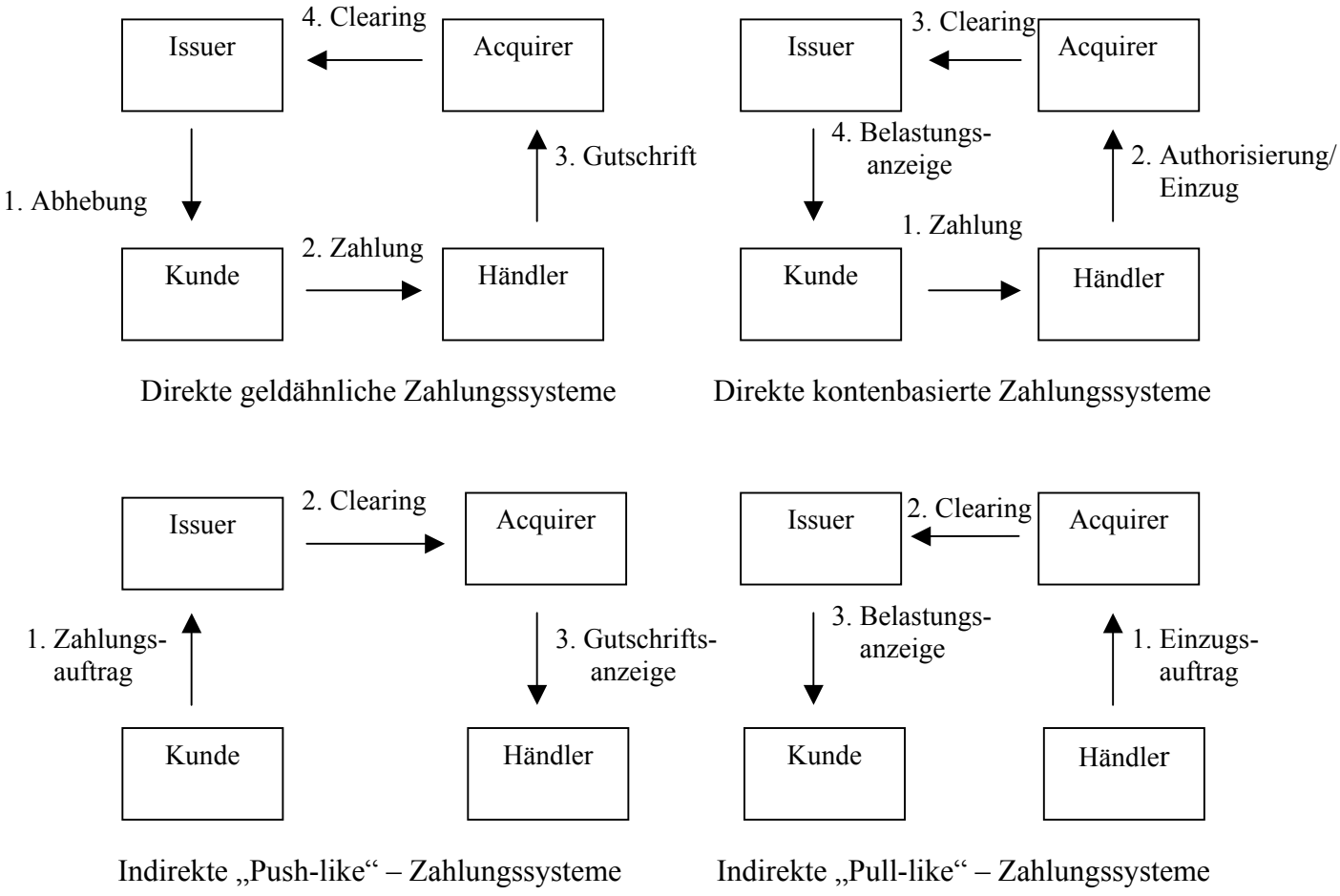

Abbildung 4.3.: Zahlungssystemmodelle

4.4. Art der Gültigkeitsprüfung

Kriterium für diese Einteilung ist, ob Zahlender oder Zahlungsempfänger beim Zahlungsvorgang in direkter **Verbindung** mit **dritten Parteien** (die Zahlung durchführende Organisationen bzw. Kreditinstitute, Issuer und/oder Acquirer) stehen muß.

- „**Online**"-Zahlungssysteme
  Zahlender oder Zahlungsempfänger treten beim Zahlungsvorgang direkt (online) mit dritten Parteien in Verbindung.
- „**Offline**"-Zahlungssysteme
  Zahlender oder Zahlungsempfänger treten beim Zahlungsvorgang nicht direkt (online) mit dritten Parteien in Verbindung.
- „**Semi-online**" – Zahlungssysteme
  Zahlender und Zahlungsempfänger müssen zwar mit dritten Parteien in Verbindung treten, aber nicht zu jedem Zahlungsvorgang. Z.B. genügt eine Online-Verbindung beim ersten Zahlungsvorgang.

4.5. Zahlungsgröße

Zusätzlich zu den eben vorgestellten Klassen, ist es üblich, Zahlungssysteme gemäß der Zahlungsgröße zu klassifizieren. Man unterscheidet 3 Kategorien:

- **Makrozahlungen**: Unter Makrozahlungen versteht man Zahlungen, für die der Einsatz von Kreditkarten wirtschaftlich rentabel ist, also schätzungsweise ein Mindestbetrag von 10 Euro.
- **Kleinzahlungen**: Beträge, für deren Zahlung der Einsatz von Kreditkarten unrentabel ist, die aber noch nicht in den Microzahlungsbereich reichen, werden den Kleinzahlungen zugeordnet. Die Höhe der Beträge von Kleinzahlungen richtet sich also nach der Definition der Makro- und Mikrozahlungen.
- **Microzahlungen**: Die Zeiten, in denen sämtliche Informations- und Unterhaltungsangebote im Internet kostenlos waren, sind vorbei. Für die Nutzung von Angeboten wie der Download von Videoclips, Liedern, digitalen Zeitungsartikeln oder anderen Dokumenten, Software und dergleichen mehr werden Gebühren erhoben, die den Bruchteil eines Cents betragen können. Für die Zahlung dieser Kleinstbeträge sind Kreditkarten-Zahlungssysteme aufgrund der hohen Gebühren ungeeignet. Es bedarf neuer Systeme, die die Zahlung von Kleinstbeträgen effizient und kostengünstig abwickeln können.

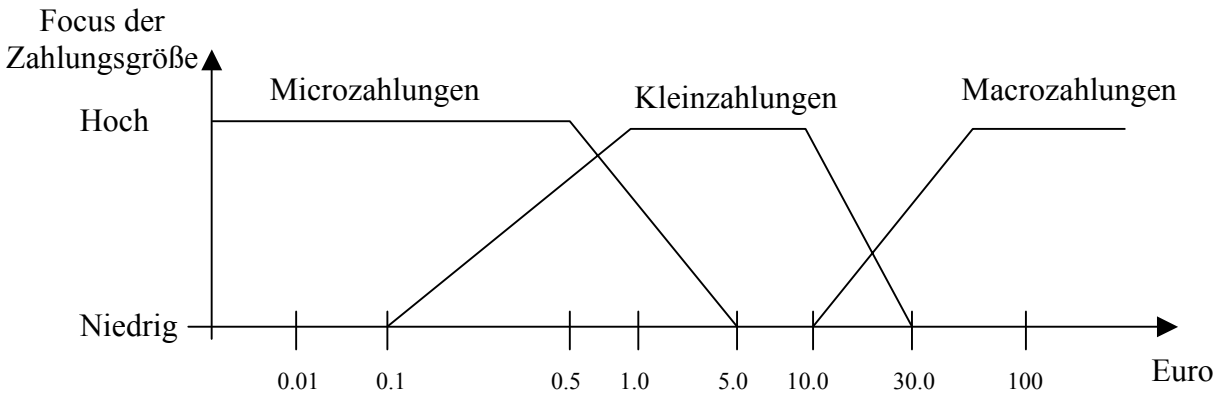

Abbildung 4.5.: Typische Zahlungsgrößen

5. Angriffs- und Betrugsszenarien bei Zahlungssystemen

Elektronische Zahlungsvorgänge werden über das Internet abgewickelt. Bei diesen Zahlungsvorgängen werden vertrauliche Daten der Kunden über das sehr unsichere Medium Internet übermittelt.
Dies stellt ein großes Problem für die Zahlungssystem-Betreiber dar, denn der Erfolg eines Zahlungssystems hängt im Wesentlichen von dem **Vertrauen der Kunden** ab. Sie müssen sicher sein, bei der Nutzung des Zahlungssystems nicht Betrügereien zum Opfer zu fallen.

Es gibt die Möglichkeit, ein Zahlungssystem von außen anzugreifen (**externer Angriff**). Aber auch die Mitarbeiter eines Zahlungssystems können Betrügereien begehen (**interner Angriff**). Und ebenso kann Betrug durch den **Kunden** wie durch den **Händler** begangen werden.

Bei der **Nachrichtenübermittlung**, z.B. Übermittlung von Kreditkarteninformationen, hat der Angreifer folgende Ansatzpunkte. Man unterscheidet passive und aktive Attacken:

Passive Attacken: Der Angreifer kann die **Nachricht abhören** und gelangt somit in den Besitz vertraulicher Informationen, die er zum Betrug mißbrauchen kann, z.B. im Namen des Kunden einkaufen kann. Um dies zu verhindern, müssen **Nachrichten verschlüsselt** werden, so daß sie nur von den tatsächlich vorgesehenen Empfängern gelesen werden können. Dabei werden Mechanismen verwendet, die in der Verschlüsselungswissenschaft, der Kryptographie, entwickelt wurden. Eine Attacke kann aber schon durch die alleinige Feststellung geschehen, daß eine Nachricht übertragen wurde. Unberechtigte erhalten somit die Möglichkeit, Analysen bezüglich Häufigkeit und Länge des Nachrichtenaustausches anzufertigen.

Aktive Attacken: Der Angreifer kann die **Nachricht manipulieren** oder verändern, z.B. den Betrag einer Zahlung verändern. Als Gegenmaßnahme dazu werden die Nachrichten mit eindeutigen Prüfsummen (elektronischer **Fingerabdruck**) versehen, die der Angreifer nicht erzeugen kann und somit seine Manipulation nicht unentdeckt bleibt.
Der Angreifer kann die **Nachricht unterbrechen**. Dies geschieht meist bei Angriffen auf die Hardware. Die Verfügbarkeit des Zahlungssystems muß deshalb gewährleistet werden.
Der Angreifer kann die **Nachricht wiedereinspielen**. Man denke z.B. an die Mehrfachausgabe von digitalem Geld. Zur Verhinderung bedient man sich **Zeitstempeln** und anderer Integritätssicherungsverfahren.
Der Angreifer kann eine andere **Identität vortäuschen** und somit in den Besitz von Informationen kommen, die nicht für ihn bestimmt sind, oder er kann sich als Empfänger einer Zahlung ausgeben. Schutz davor bietet die **eindeutige Authentisierung** der Nachrichtenempfänger und -sender z.B. durch Eigenschaften (Fingerabdruck, Stimme), Besitz (Schlüssel) oder spezielles Wissen (Paßwort). Bei einer Man-in-the-Middle-Attacke stellt sich der Betrüger zwischen zwei Verhandlungspartner und täuscht beiden vor, jeweils der andere Partner zu sein.

Auch bei der **Speicherung der Zahlungsinformationen** ist besondere Vorsicht geboten. So sollten diese Daten nicht unverschlüsselt in einer Datenbank gespeichert werden, die überdies auch noch auf einem über das Internet zugänglichen Rechner liegt. Zur Lösung dieses Problems wurden verschiedene Systemarchitekturen entwickelt [ISEC02].
Ein großes Risiko für den Kunden stellt die **Schlüsselaufbewahrung** dar. Eine Möglichkeit ist die Speicherung der Schlüssel auf einem Sicherheitsmodul (z.B. Chipkarte). Allerdings besteht dann wieder das Risiko eines Diebstahls der Chipkarte oder einer unsicheren

Übertragung von Chipkarte zum PC oder Kassenterminal. Auf der Festplatte sollten Schlüssel nur verschlüsselt aufbewahrt werden.

Die Sicherungsmechanismen schützen nicht nur Kunden und Händler vor Angreifern von außen, sondern verhindern ebenfalls **Betrugsversuche von Kunden und Händlern**. Ein Kunde könnte z.B. die Preisangabe ändern und somit ein Gut zu niedrigeren Preisen beziehen. Ein Händler könnte dem Kunden einen höheren Betrag in Rechnung stellen, als der Kunde ursprünglich angenommen hat. Die Anwendung von Verschlüsselungs- und Authentisierungstechniken minimieren diese Manipulationsmöglichkeiten.

Einen weiteren Angriffspunkt stellen die **Zahlungssystemserver** dar. Durch einen Distributed Denial of Service-Angriff können sie wegen Überlastung ausfallen und dem Zahlungssystembetreiber wird durch den Geschäftsausfall beträchtlicher Schaden zugefügt.
Betrug ist natürlich auch durch einen **Mitarbeiter eines Zahlungssystembetreibers** möglich. Wenn dieser Zugang zu der Datenbank mit den kundenspezifischen Daten (Kreditkarteninformationen, Paßwörter, etc.) hat, oder diese knacken kann, dann kann er mit Hilfe dieser Informationen dem Kunden Schaden zufügen. Deshalb sollten diese Datenbanken zutritts- und zugriffsbeschränkt sein.

Zahlungssysteme, die mit **digitalem Geld** arbeiten, bieten dem potentiellen Betrüger **zusätzliche Angriffspunkte**, die weitere Abwehrmechanismen erfordern. Digitales Geld wird durch Bytes auf einem Speichermedium des Nutzers repräsentiert, die natürlich beliebig oft kopiert und verändert werden können. Zum einen ist damit die Gefahr der unkontrollierten **Geldvermehrung** und der **Fälschung** der Werte verbunden, was Konsequenzen für die gesamte Geldwirtschaft hat, zum anderen besteht auch die Möglichkeit der Mehrfachausgabe (**double spending**) von digitalen Geld. Um dies zu verhindern, arbeiten die Systembetreiber mit Datenbanken zur Überprüfung der digitalen Münzen (-> Kapitel 7, Ecash). Diese Datenbanken werden je nach Anzahl der ausgegeben Münzen sehr groß und somit auch sehr teuer. Die Registrierung der Münzen stellt also ein großes Problem für bargeldähnliche Zahlungssysteme dar.
Manche Systeme verwenden **Hardware** wie z.B. Chipkarten und Smart Cards, um die Sicherheitsanforderungen zu erfüllen. Diese Hardware muß natürlich vor Manipulation sicher sein. Chipkarten als elektronische Zahlungsmittel können festhalten, wer was wo und bei wem gekauft hat. Dadurch stellen sie ein großes Gefahrenpotential dar, wenn sie in fremde Hände gelangen. Der **Diebstahl** von Chipkarten ist gleichzusetzen mit dem Diebstahl von Bargeld. Durch die Führung von **Schattenkonten** kann unautorisierten Geldausgaben auf die Spur gekommen werden.

Zahlungssysteme können auch indirekt für kriminelle Handlungen benutzt werden. Zum einen seien Straftaten wie z.B. Steuerhinterziehung, Geldwäsche und illegales Glücksspiel genannt. Es ist schon in der traditionellen Geldwirtschaft sehr schwer möglich, diesen kriminellen Handlungen Einhalt zu gebieten. Man kann sich also leicht ausmalen, daß sich kriminelle Gruppierungen die sich mit der neuen Form der Geldwirtschaft bietenden Möglichkeiten nur allzu gerne zu eigen machen werden.
Eine weitere Möglichkeit des **indirekten Betrugs** mit Zahlungssystemen besteht im Sammeln von kundenspezifischen Informationen ohne Kenntnis der Kunden. Diese Informationen können z.B. zu Marketingzwecken verwendet werden oder weiter verkauft werden. Deshalb müssen z.B. Kundendatenbanken vor Angriffen besonders geschützt werden. In diesem Zusammenhang sei noch die Erpressung von Kunden mit Informationen über den Kauf verfänglicher Artikel erwähnt.

6. technische und kryptographische Grundlagen

Die in Kapitel 5 beschriebenen Angriffs- und Betrugsszenarien zeigen, daß Verschlüsselungs- und Sicherungsmechanismen dringend erforderlich sind bei der Implementierung von elektronischen Zahlungssystemen. In diesem Kapitel werden die grundlegenden Sicherungsverfahren vorgestellt. Dies erfolgt allgemein und unabhängig von speziellen Implementierungen einzelner Zahlungssysteme, da die verschiedenen Systeme im wesentlichen auf den gleichen Verfahren basieren (-> Kapitel 7).

6.1. Sichere Nachrichtenübertragung

Bei einer **sicheren Nachrichtenübertragung** sollen die übertragenen Daten nicht eingesehen werden können. Deshalb werden die Nachrichten verschlüsselt. Der Empfänger kann die Nachricht nur lesen, wenn er sie mit einem ihm bekannten Schlüssel entschlüsseln kann. Für einen Angreifer ist eine verschlüsselte Nachricht ohne Wert, da er sie ohne Kenntnis des Schlüssels nicht oder nur unter sehr großem Aufwand lesen kann.
Für die Qualität eines Verschlüsselungsverfahrens ist die Generierung und die Anzahl der möglichen Schlüssel von wesentlicher Bedeutung. Denn grundsätzlich gilt, daß der Erfolg bei einem Angriff in keinem Verhältnis zum Aufwand stehen darf, d.h. es ist kein Algorithmus bekannt, um den Schlüssel direkt zu berechnen, und dem Angreifer bleibt nur das Durchprobieren aller möglichen Schlüssel. Die Anzahl der möglichen Schlüssel ist aber so groß, daß das systematische Durchprobieren in angemessener Zeit nicht möglich ist. Wobei ständig wachsende Rechnerleistungen und –kapazitäten die Verlängerung der Schlüssel notwendig machen, was aber wiederum die Effizienz der Verschlüsselungsverfahren herabsetzt. Man unterscheidet symmetrische und asymmetrische Verschlüsselung.

6.1.1. Symmetrische Verschlüsselung

Bei symmetrischen Verfahren (private-Key-Verfahren) gibt es einen einzigen Schlüssel, mit dem die Nachricht ver- und entschlüsselt wird und der Absender und Empfänger bekannt sein muß.
Ein großes Problem stellt deshalb die Verteilung der Schlüssel an die Kommunikationspartner dar, d.h. der Schlüssel muß zunächst auf sicherem Weg ausgetauscht werden, z.B. durch persönliche Treffen oder Kuriere. Ein spontaner und gesicherter Datenaustausch ist somit nicht möglich. Ebenfalls problematisch ist die aufwendige Verwaltung der geheimen Schlüssel bei vielen Kommunikationspartnern. Hingegen sind symmetrische Verfahren für die Sicherung von Datenbeständen (z.B. digitalen Münzen) auf der Festplatte durch Speicherung in verschlüsselter Form gut geeignet. Ein Vorteil der symmetrischen Verfahren ist die relativ geringe benötigte Rechenleistung.
Am häufigsten wird das 1975 von IBM entwickelte DES-Verfahren zur symmetrischen Verschlüsselung verwendet. Weitere Kryptosysteme sind IDEA, RC2, RC4 oder RC5.

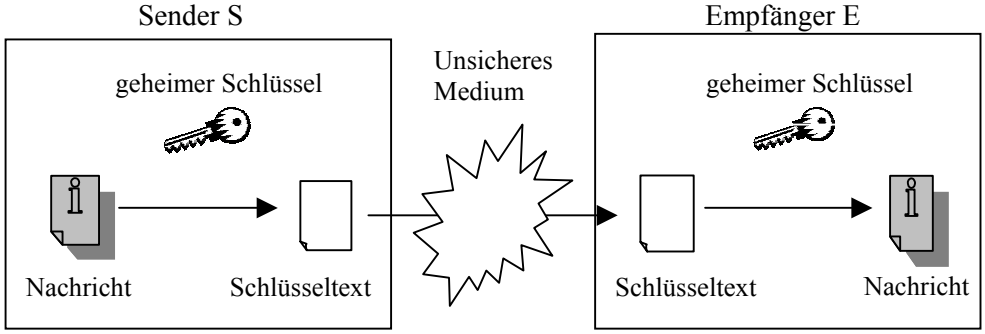

Abbildung 6.1.1.: Nachrichtenübertragung mit symmetrischer Verschlüsselung

6.1.2. Asymmetrische Verschlüsselung

Asymmetrische Verfahren (Public-Key-Verfahren) verwenden Schlüsselpaare für die Ver- und Entschlüsselung. Nachrichten, die mit dem einen Schlüssel verschlüsselt wurden, können nur mit dem zweiten Schlüssel des Paares entschlüsselt werden. Diese Schlüsselpaare bestehen aus einem privaten und einem öffentlichen Schlüssel. Der private Schlüssel wird geheim gehalten und der öffentliche Schlüssel wird bekannt gegeben.
Der Absender A verschlüsselt nun seine Nachricht an den Empfänger E mit dessen öffentlichen Schlüssel. Der Empfänger E benutzt seinen privaten Schlüssel, um die Nachricht zu entschlüsseln. Das asymmetrische Verfahren löst somit das Problem der sicheren Schlüsselverteilung, eine spontane und sichere Kommunikation ist nun möglich. Der Nachteil gegenüber der symmetrischen Verfahren ist der erhöhte Bedarf an Rechenleistung.
Das klassische asymmetrische Verfahren ist das RSA-Verfahren [Eck01].

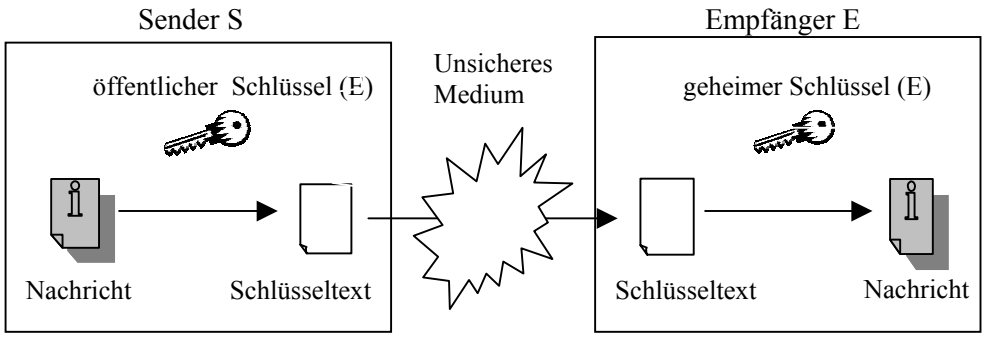

Abbildung 6.1.2.: Nachrichtenübertragung mit asymmetrischer Verschlüsselung

6.1.3. Hybride Verfahren

Hybride Verfahren kombinieren die Vorteile der symmetrischen und asymmetrischen Verfahren. Die eigentliche Nachricht wird mit einem symmetrischen Schlüssel (Sitzungsschlüssel) verschlüsselt (wenig Rechenleistung). Der Sitzungsschlüssel wird dann mit Hilfe der asymmetrischen Verschlüsselung an den Empfänger übertragen (kein Schlüsselaustausch notwendig). Der Empfänger entschlüsselt den Sitzungsschlüssel mit seinem privaten Schlüssel und dann mit dem somit erhaltenen Sitzungsschlüssel die eigentliche Nachricht. Dieses Verfahren wird auch **digitaler Umschlag** genannt.

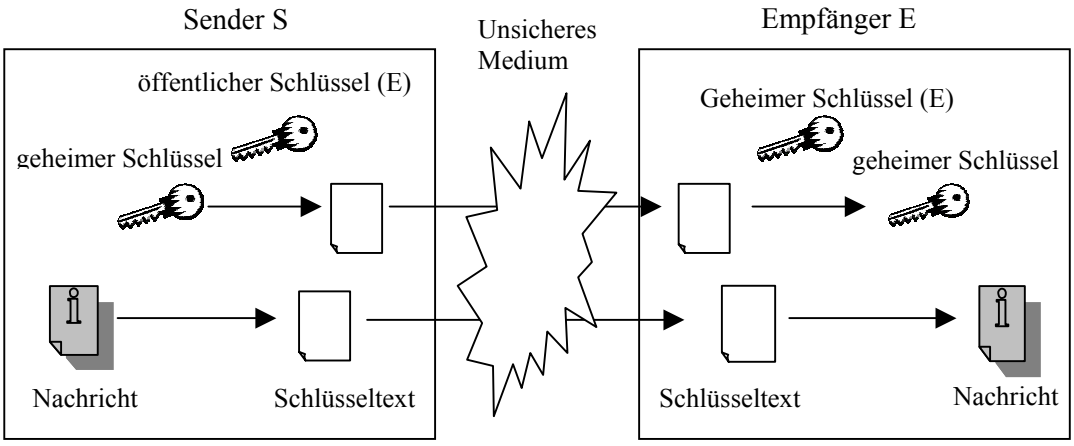

Abbildung 6.1.3.: Nachrichtenübertragung mit digitalem Umschlag

6.2. Authentische Nachrichtenübertragung

Neben der sicheren Übertragung einer Nachricht, ist es ebenfalls wichtig zu gewährleisten, daß die übertragene **Nachricht authentisch** ist, d.h. daß sie während der Übertragung nicht verändert wurde und daß ihr Absender auch wirklich der ist, der er vorgibt zu sein. Um die Authentizität einer Nachricht zu gewährleisten, gibt es verschiedene Verfahren.

6.2.1 Asymmetrische Verschlüsselung

Mit der unter 6.1.2. beschrieben asymmetrischen Verschlüsselung lassen sich Nachrichten sicher übertragen. Wendet man die asymmetrische Verschlüsselung „andersherum" an, so läßt sich auch eine authentische Nachrichtenübertragung realisieren. Der Absender A verschlüsselt die Nachricht mit seinem privaten Schlüssel. Jeder kann die Nachricht von A nun mit dem öffentlichen Schlüssel von A lesen, aber es ist sichergestellt, daß die Nachricht von A ist. Durch die Verwendung beider Versionen der asymmetrischen Verschlüsselung läßt sich eine sichere und authentische Nachrichtenübertragung bewerkstelligen. Dieses Verfahren ist allerdings sehr zeitaufwendig, da rechenintensiv.

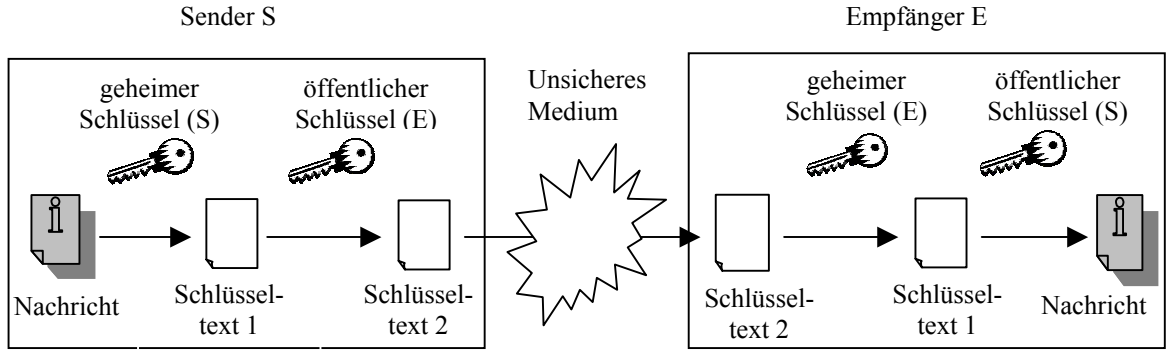

Abbildung 6.2.1.: gesicherte und authentische Nachrichtenübertragung mit asymmetrischer Verschlüsselung

6.2.2. Digitaler Fingerabdruck

Wenn eine Nachricht nicht unbedingt geheim gehalten werden muß, aber dennoch sicher gestellt werden soll, daß sie unverändert übermittelt wurde, kann sie mit einem digitalen Fingerabdruck (Message Digest) versehen werden. Dieser Fingerabdruck ist das Ergebnis einer Einweg-Hash-Funktion, die auf ein beliebig langes Dokument angewendet wird und einen Hashwert fester Länge liefert. Eine Hash-Funktion ist nicht umkehrbar, aus dem Hashwert kann das Dokument nicht wieder reproduziert werden. Der Empfänger der Nachricht berechnet ebenfalls den Hashwert der Nachricht, indem er die gleiche Hash-Funktion auf die Nachricht anwendet wie der Sender, und vergleicht den berechneten Wert mit dem übermittelten Wert. Stimmen beide Werte überein, so wurde die Nachricht nicht verändert. Eine manipulierte Nachricht würde nicht denselben Hash-Wert liefern.

6.2.3. Digitale Signatur

Mit der digitalen Signatur kann die Authentizität eines Absenders A gewährleistet werden, da sie nur von einer einzigen Person korrekt erzeugt werden kann, aber von allen Empfängern der Nachricht überprüft werden kann. Um die Authentizität von A zu gewährleisten, wird nicht die gesamte Nachricht mit dem privaten Schlüssel von A verschlüsselt (siehe 6.2.1, zu lange Rechenzeit), sondern nur der Fingerabdruck. Absender A hängt den mit seinem privaten Schlüssel verschlüsselten Fingerabdruck an die Nachricht an. Der Empfänger E überprüft den

entschlüsselten Fingerabdruck. Stimmen die Fingerabdrücke überein, so kann E von einer sicheren und authentischen Nachrichtenübertragung ausgehen.
Die digitale Signatur wird oft als das elektronische Äquivalent zur handschriftlichen Unterschrift bezeichnet und unterliegt als solchem strengen gesetzlichen Auflagen.

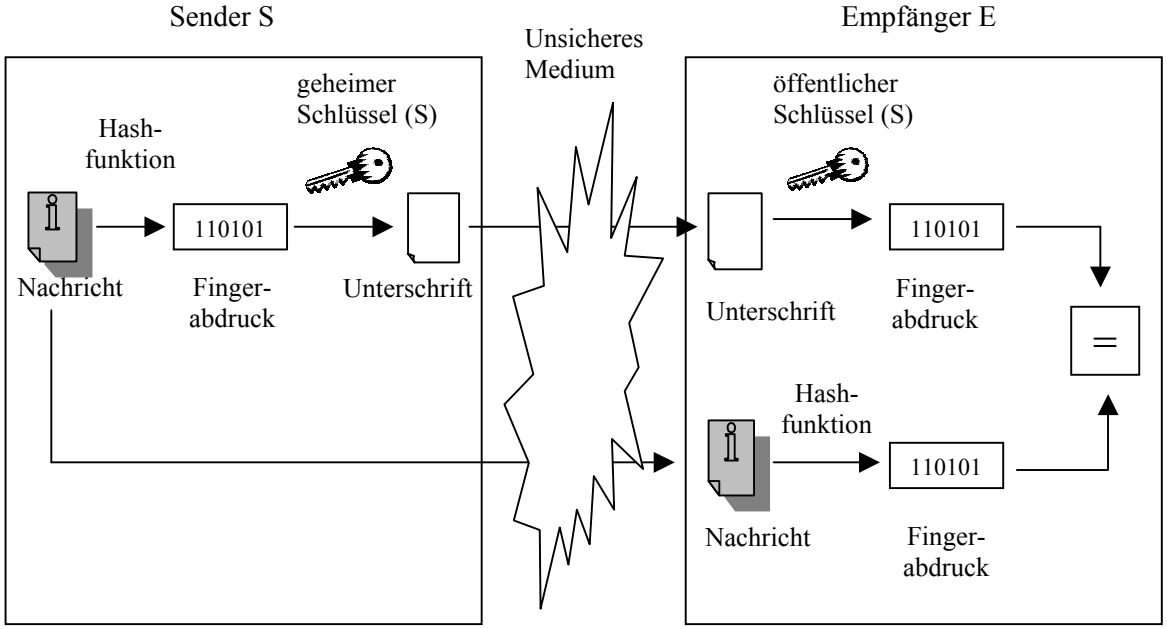

Abbildung 6.2.3.: Grundkonzept der digitalen Signatur

6.2.4. Duale Signatur

Der SET-Standard (-> Kapitel 7) sieht eine Abwandlung der digitalen Signatur vor. Die Duale Signatur erlaubt es, zwei getrennte Nachrichten mit einer gemeinsamen Unterschrift so zu verbinden, daß sie nicht aus dem Zusammenhang gerissen und mißbraucht werden können. Beide Nachrichten können dennoch getrennt versendet werden und durch ihre Doppelunterschrift verifiziert werden.
Zur Erstellung der dualen Signatur wird von beiden Nachrichten ein Fingerabdruck berechnet. Die beiden Fingerabdrücke werden aneinander gehängt. Davon wird wiederum ein Fingerabdruck erzeugt und schließlich mit dem privaten Schlüssel des Absenders verschlüsselt. Der Empfänger kann nun mit Hilfe einer der beiden Nachrichten, den Fingerabdruck der anderen Nachricht und den gemeinsamen Fingerabdruck zweifelsfrei feststellen, daß die Nachricht zum Fingerabdruck, bzw. zum Sender gehört. Dazu bildet er einfach den Fingerabdruck der Nachricht, hängt ihn an den bereits vorhandenen zweiten Fingerabdruck und berechnet daraus wiederum den Fingerabdruck. Stimmt dieser Wert mit dem ihm zugesandten Wert überein, kann der Empfänger von einer authentischen Nachrichtenübertragung ausgehen, ohne beide Nachrichten eingesehen zu haben.
Die Duale Signatur wird im SET-Standard zum Schutz des Kunden und zur Absicherung des Händlers eingesetzt. Dabei werden Bestellung und Zahlungsanweisung miteinander verknüpft, ohne das der Händler die Zahlungsinformation und die Bank die Bestellinformation lesen kann. Denn der Kunde verschlüsselt seine Kreditkarteninformationen mit einem Bankschlüssel und die Bestellung mit dem Schlüssel des Händlers.
Der Händler bekommt also eine Nachricht vom Kunden, die aus der Bestellung und den Kreditinformationen des Kunden besteht und mit einer dualen Signatur unterschrieben ist. Um sicherzustellen, daß diese Nachricht authentisch ist, überprüft der Händler die duale Signatur. Er kann dabei die Nachricht mit den Kreditkarteninformationen nicht lesen, von ihr hat er nur

den Fingerabdruck. Wenn der Händler sichergestellt hat, daß die Bestellung und die Kreditkarteninformationen tatsächlich vom Kunden sind, verschlüsselt er die Bestellung und sendet die gesamte Nachricht zwecks Zahlungsanweisung an die Bank weiter. Die Bank überprüft ebenfalls die duale Signatur. Sie kann die Kreditinformationen des Kunden einsehen, aber nicht seine Bestellung beim Händler.
Hat der Kunde falsche Kreditkarteninformationen angegeben, so kann ihm das mit Hilfe der Signatur nachgewiesen werden. Der Händler ist somit vor Betrug abgesichert. Der Kunde kann den Preis anhand der Bestellung nachweisen und ist somit vor Betrug des Händlers abgesichert.

6.2.5. Challenge Response

Mit Challenge Response werden Verfahren bezeichnet, die eine Authentisierung ohne Informationspreisgabe erlauben.
Eine solche Authentisierung wird durch eine Frage und eine Antwort (challenge und response) realisiert. Teilnehmer A sendet eine zufällige Zahl an Teilnehmer B, und erhält von Teilnehmer B eine mit Hilfe des gemeinsamen Schlüssels berechnete Antwortzahl. Stimmt diese mit der von Teilnehmer A selbst berechneten Antwortzahl überein, so ist Teilnehmer B im Besitz des geheimen Schlüssels und somit authentisch. Der geheime Schlüssel muß beim Authentifizierungsvorgang nicht übertragen werden.
Dieses Verfahren wird vor allem bei Chipkarten verwendet, die sich gegenüber den Kartenlesegeräten verifizieren müssen. Teilnehmer A wäre somit das Kartenlesegerät (Terminal) und Teilnehmer B die Chipkarte. Es muß geprüft werden, ob die Chipkarte im Besitz eines ordnungsgemäßen Sitzungsschlüssel ist, ohne daß der Sitzungsschlüssel übertragen wird, sondern lediglich eine durch ihn erzeugte Unterschrift (Antwortzahl).

6.2.6. Secure Socket Layer Protocol

Das von Netscape Communications Corporation entwickelte Protokoll ermöglicht durch eine verschlüsselte Netzwerkverbindung die sichere und authentische Nachrichtenübertragung zwischen einem Client und einem Server, bzw. einem Kunden und einem Händler. Bei SSL wird die Authentisierung der Kommunikationspartner durch Verwendung von asymmetrischen Verschlüsselungsverfahren und Zertifikaten, die vertrauliche Datenübertragung durch Nutzung eines gemeinsamen symmetrischen Sitzungs-Schlüssel und schließlich die Integrität der übermittelten Nachrichten durch spezielle Fingerabdrücke gewährleistet. Das SSL-Protokoll besteht u.a. aus dem Handshake-Protokoll, das die Sicherung und Authentisierung realisiert: Auf Anfrage des Clients schickt der Server sein Zertifikat und einen öffentlichen Schlüssel an den Client. Der Client generiert nun einen symmetrischen Schlüssel (Master Key) für den nachfolgenden Datenaustausch und schickt diesen, verschlüsselt mit dem öffentlichen Schlüssel des Servers, an diesen zurück. Falls erforderlich schickt der Client zusätzlich noch sein Zertifikat. Der Server generiert aus dem entschlüsselten Master Key mit zuvor ausgetauschten Zufallszahlen die Sitzungsschlüssel für die Kommunikation.
Zur ausführlichen Beschreibung des SSL-Protokolls siehe [SSL96].

6.3. Schlüsselmanagement

Mit den oben beschriebenen Verfahren zur sicheren und authentischen Nachrichtenübertragung stellt sich nun das Problem der sicheren und zuverlässigen Verteilung der Schlüssel an die Kommunikationspartner, das man z.B. mit Zertifikaten lösen kann.

6.3.1. Zertifikate

Um die Authentizität der öffentlichen Schlüssel zu gewährleisten, stellen offizielle, allgemein anerkannte und bekannte Zertifizierungsstellen Zertifikate aus. Die Zertifizierungsstelle (Trust Center) versichert sich der wahren Identität einer Person, z.B. durch Vorlage des Personalausweises. Dann erstellt das Trust Center das Zertifikat, indem es den öffentlichen Schlüssel der Person zusammen mit Angaben zur Person mit dem geheimen Schlüssel des Trust Centers verschlüsselt. Eine Person B erhält den öffentlichen Schlüssel einer Person A durch die Entschlüsselung des Zertifikates mit dem bekannten öffentlichen Schlüssel des Trust Centers. B kann bei Erhalt des Zertifikates sicher sein, den öffentlichen Schlüssel von A zu erhalten, da das Zertifikat nur vom Trust Center erstellt worden sein kann.

6.4. Sicherungsverfahren für digitales Bargeld

Für Zahlungssysteme, die mit digitalen Geld arbeiten, gelten neben einer sicheren und authentischen Nachrichtenübertragung und einem sicheren Schlüsselmanagement zusätzlich die Anforderung der **Anonymität**, um annährend die Vorteile richtigen Bargeldes erreichen zu können. Zudem muß der **Kopierschutz und die Registrierung digitalen Bargeldes** gewährleistet werden, um ungewünschte Geldvermehrung, Fälschung und Mehrfachausgaben zu verhindern. Außerdem bedarf es Recovery-Mechanismen, um dem **Verlust von digitalen Münzen** verhindern zu können.

6.4.1. Blinding

Gibt die Bank digitale Münzen aus, so kann sie die Transaktionen der Kunden z.B. anhand von Seriennummern auf den Münzen, verfolgen und hat somit die Möglichkeit, Kundenprofile zu erstellen. Andererseits müssen die Münzen aber von einer Bank verifiziert werden, um einen geordneten Geldverkehr zu gewährleisten und Betrug zu verhindern. Der Kryptographie-Experte David Chaum, Gründer der Firma Digicash B.V. (-> Kapitel 7), hat dieses Problem mit dem von ihm entwickelten und patentierten Blinding-Verfahren gelöst.
Will der Kunde eine elektronische Münze von seinem Konto abheben, so generiert er selbst in seiner Softwarebörse die gewünschte Münze mit einer zufälligen Seriennummer und multipliziert diese mit einem bestimmten Faktor (blinding factor). Die Münze steckt nun in einem sogenannten digitalen Umschlag. Der Kunde sendet den Umschlag mit der Münze an die Bank. Die Bank versieht die Münze mit ihrer digitalen Unterschrift und weist dadurch den Seriennummern einen bestimmten Betrag zu. Sie kann aber die Seriennummer der Münze nicht lesen und somit auch nicht aufzeichnen, weil die Münze im digitalen Umschlag steckt. Diesen Vorgang kann man sich bildlich vorstellen: Die Bank drückt ihren Stempel auf den Umschlag. Durch Blaupapier im Umschlag bekommt die Münze im Umschlag ebenfalls den Stempelabdruck. Die Bank stempelt also die Münze, ohne sie sehen zu können. Nachdem der entsprechende Betrag vom Konto des Kunden abgebucht wurde, schickt die Bank den Umschlag mit der Münze zurück. Der Kunde holt die Münze aus dem Umschlag, indem er durch den blinding factor dividiert. Die Unterschrift der Bank bleibt dabei gültig. Somit ist der Kunde im Besitz einer anonymisierten digitalen Geldmünze.

6.4.2. Secret Sharing

Um Kopierschutz bei digitalem Geld gewährleisten zu können, müßten Rückschlüsse auf den ehemaligen Besitzer der Münzen geschlossen werden können, um ihn für den Betrug verantwortlich machen zu können. Das Zahlungssystem wäre dann aber nicht mehr anonym. Mit Secret Sharing, oder auch Secret Splitting, kann den gegensätzlichen Forderungen nach Anonymität und Kopierschutz nachgekommen werden. Den Münzen werden Teilinformationen über die Identität des Besitzers hinzugefügt. Beim einmaligen Bezahlen mit der Münze werden nicht genügend Informationen bekannt gegeben, um den ehemaligen Besitzer der

Münze feststellen zu können. Erst bei unrechtmäßiger mehrmaliger Verwendung ein und derselben Münze kann die Bank verschiedene Teilinformationen des ehemaligen Besitzer sammeln und mit Hilfe der sich ergänzenden Informationen den Betrüger identifizieren.

6.4.3. Recovery digitaler Münzen

Digitale Münzen können verloren gehen, z.B. durch versehentliches Löschen. Das Ecash-System der Firma DigiCash B.V. (-> Kapitel 7) beinhaltet durch seine Implementierung einen Recovery-Mechanismus, der eine erneute Generierung der noch nicht ausgegeben Münzen erlaubt. Hierzu muß die Abhebung neuer Münzen mit derselben zufällig gewählten Zeichenkette wie bei der vorherigen Abhebung erfolgen (Recovery-Button in der Softwarebörse). Dann werden dieselben Seriennummern und derselbe blinding factor generiert. Die Bank erkennt dies und sendet die bereits abgehobenen, aber noch nicht ausgegebenen Münzen dem Kunden erneut zu.

6.5. Sicherungsverfahren mit Hardware

Sicherheit kann man auch mit spezieller Hardware erreichen, wie z.B. **Chipkarten** oder **Smart Cards**. Um z.B. die Schlüssel zu sichern, werden sie oftmals nicht auf der Festplatte hinterlegt, wo sie bei Angriffen auf den Rechner leicht in falsche Hände geraten können, sondern auf Chipkarten gespeichert. Dies erfordert natürlich den Gebrauch von speziellen Chipkartenlesegeräten, die mit der wallet-Software zusammenarbeiten. Diese Lesegeräte müssen ebenfalls manipulationssicher sein (**tamper-resistant Hardware**).
Zusätzlich werden bei Smart Card-basierten Zahlungssystemen oft sogenannte **Schattenkonten** geführt. Auf diesen Konten werden die Zu- und Abgänge auf der Smart Card automatisch mitprotokolliert. Bei Mißbrauch der Karte kann der verlorengegangene Betrag somit genau ermittelt und dem Kunden rückerstattet werden. Diese gewährleistete Sicherheit geht allerdings auf Kosten der Anonymität der Kunden.

7. Übersicht über Zahlungssysteme im Internet

Im Folgenden werden verschiedene Zahlungssysteme vorgestellt und auf ihre Besonderheiten hingewiesen. Dabei soll ein Überblick über die unterschiedlichen Ansätze gegeben werden.

7.1. Kontobasierte Zahlungssysteme

SET: Secure Electronic Transaction (SET) [SET03] ist ein offener Standard für den sicheren Einsatz von Kreditkarten als Zahlungsmittel im Internet. SET entstand aus 2 Entwicklungen: SEPP (Secure Electronic Payment Protocol) von MasterCard, IBM, Netscape u.a. und STT (Secure Transaction Technology) von VISA und Microsoft.
SET erfaßt die sichere Abwicklung des kompletten Kaufvorgangs von der Bestellung bis zur Quittung. Die Verwendung von Kryptographie garantiert eine sichere und authentische Nachrichtenübertragung. Es werden alle Nachrichten und Protokolle definiert und die kryptographischen Algorithmen festgelegt, wie z.B. SHA-1 für die Hash-Verfahren und DES und RSA für die Verschlüsselung. Um einen Ausgleich zwischen Geschwindigkeit und optimaler Sicherheit zu erlangen, verwendet SET eine Kombination von DES- und RSA-Verschlüsselung. Außerdem werden digitale Signaturen (-> 6.2.2.), Zertifikate (-> 6.3.1.) und Duale Signaturen (-> 6.2.3.) verwendet, um die Integrität der Nachrichten und die Authentisierung von Händler und Kunden zu gewährleisten. Alle SET-Nachrichten werden signiert, aber nicht verschlüsselt. Die vertraulichen Kreditkarteninformationen werden ebenfalls signiert, mit dem RSA-Verfahren verschlüsselt und den Nachrichten separat in einen digitalen Umschlag beigelegt.
Eine wichtige Rolle spielen Zertifikate, die bei jeder Nachrichtenübermittlung überprüft werden und die in ihrer Funktion dem Präsentieren der Plastikkreditkarte gleichkommen. Kundenzertifikate sind optional. Für Händler setzt SET Zertifikate zwingend voraus, vergleichbar mit dem Aufkleber: „Wir akzeptieren MasterCard."
SET sieht eine zwischengeschaltete Instanz vor, das Payment Gateway, das zwischen Händler und Banken vermittelt sowie eine sichere Verbindung zwischen Händler und Kunden ermöglicht.
Zentrale Idee von SET ist die Duale Signatur (-> 6.2.3.), mit der Bestelldaten und Kreditkarteninformationen aneinander gebunden werden, der Händler aber nur die Bestelldaten und die Bank nur die Kreditkartendaten einsehen kann.
Der Zahlungsablauf sieht folgendermaßen aus: (1) Der Kunde klickt den Bestellbutton und bekommt daraufhin die Bestellinformationen und den Preis vom Händler zugeschickt. Der Kunde wählt die Kreditkarte, mit der er zahlen möchte. (2) Dann fertigt er eine Bestellung und eine Zahlungsanweisung an und unterzeichnet sie mit einer Dualen Signatur (-> 6.2.2.). (3) Der Händler fragt beim Payment Gateway nach, ob die Zahlungsanweisung des Kunden akzeptiert wird und schickt ihm dazu die verschlüsselte Zahlungsanweisung des Kunden. (4) Das Payment Gateway überprüft die Übereinstimmung der Zahlungsanweisung mit den Angaben des Händlers und befragt über das Bankennetzwerk die Kundenbank. (5) Die Kundenbank akzeptiert oder verweigert die Zahlungsanweisung des Kunden. (6) Das Payment Gateway erstellt ein Capture Token und schickt dieses an den Händler zurück. Das Capture Token ist verschlüsselt und kann nur vom Payment Gateway gelesen werden. Der Händler braucht es später für die Abrechnung. (7) Der Händler speichert das Capture Token und liefert die Waren an den Kunden aus, bzw. erbringt seine Dienstleistung. (8) Zu einem späteren Zeitpunkt rechnet der Händler mit Hilfe des Capture Token mit seiner Bank ab. Dafür sendet der Händler eine Anfrage an das Payment Gateway. Diese Nachricht enthält u.a. den zu zahlenden Betrag und das Capture Token. (9) Der Payment Gateway wertet das Capture Token aus und sendet die Anfrage des Händlers an die Kundenbank weiter. (10) Die Kundenbank prüft die Zahlungsanweisung und schickt dem Payment Gateway die entsprechende

Antwort zurück. (11) Das Payment Gateway teilt dem Händler die Antwort der Kundenbank mit. (12) Die Kundenbank überweist den vom Kunden zu zahlenden Betrag an die Händlerbank.
Obwohl SET eine elegante und äußerst sichere Lösung ist, hat sich der SET-Standard nicht durchsetzen können. Gründe gibt es viele: fehlende Kundenbasis, geringe Händlerbasis, hohe Teilnahmehürden, die einen spontanen Einkauf unmöglich machen, juristische Schwierigkeiten, z.B. mit dem Signaturgesetz, aufwendiges Zertifikatemanagement, etc. Die Frage nach dem Scheitern kann dennoch nicht abschließend beantwortet werden.

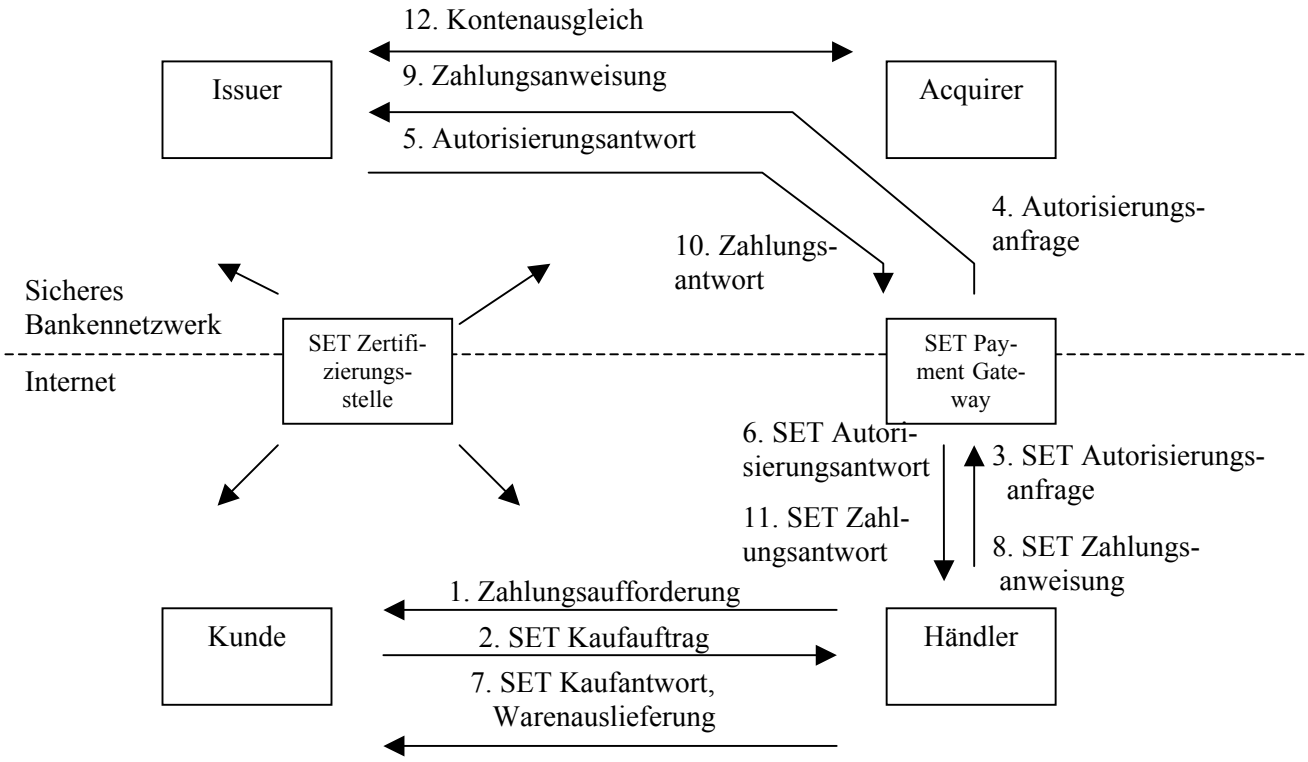

Abbildung 7.1.: Zahlungsablauf bei SET

CyberCash: Die Firma CyberCash Inc. entwickelt seit 1994 komplette Zahlungsdienste für das Internet. So wurde, neben einem System zur gesicherten Übertragung von Kreditkarteninformationen, ein Aggregationskonten-basiertes System für Kleinzahlungen (CyberCoin) und ein lastschriftbasiertes Zahlungsverfahren (EDD) für den US-amerikanischen Markt entwickelt. Ziel war die Integration unterschiedlichster Zahlungsmittel in eine Benutzeroberfläche.
Die Kreditkartenzahlung von CyberCash setzt auf den SET-Standard. Das CyberCash-System besteht im Wesentlichen aus drei Komponenten: der CyberCash-Geldbörse für den Kunden, der CyberCash-Kasse für den Händler und dem CyberCash-Gateway, das die Funktion des Payment Gateways von SET übernimmt. Die Aufgaben des Gateways können auch von einer der CyberCash-Lizenzbanken übernommen werden.
CyberCoin arbeitet mit Schattenkonten für Kunden und Händler, die vom CyberCash Gateway verwaltet werden. Der Kunde muß seine digitale Geldbörse zunächst mit dem gewünschten Betrag aufladen. Dazu wird das Geld vom Girokonto des Kunden auf sein Schattenkonto (Aggregationskonto) transferiert. In der Geldbörse des Kunden befindet sich kein Geld, es wird ihm nur sein aktueller Kontostand angezeigt. Die Zahlung erfolgt durch Buchung auf den Schattenkonten, die Banken müssen dabei nicht involviert werden.

CyberCash Inc. hat sich vom amerikanischen Markt zurückgezogen und entwickelt nun Systeme für den europäischen und asiatischen Markt. So bietet die 1997 gegründete CyberCash GmbH [Cyb03] aktuell das Point-of-Sale-Händlerterminal (POSH) an. Dieses virtuelle Terminal integriert der Händler in seine Web-Seite. Er kann nun über den POSH Kreditkartenzahlungen seiner Kunden entgegennehmen und effizient bearbeiten. Weder Kunde noch Händler müssen spezielle Software installieren. Der Händler kann die Funktionalität des POSH-Service über seinen Web-Browser nutzen oder fest in seine Applikation integrieren. Für die sichere und authentische Abwicklung der Zahlung wird zusätzlich ein SSL-Formularservice angeboten. Der POSH-Service selbst übernimmt die eigentliche Kreditkartenzahlung.

7.2. bargeldähnliche Zahlungssysteme

Ecash: Die niederländisch amerikanische Firma Digicash B.V., gegründet von dem Kryptographie-Experten David Chaum, stellte mit ihrem Ecash-System ein anonymes, bargeldähnliches Kleinzahlungsverfahren zur Verfügung.
Für die Nutzung von Ecash braucht der Kunde ebenso wie der Händler eine digitale Geldbörse (Software mit graphischer Bedienoberfläche, bzw. mit Kommandozeile). Beide Seiten können Zahlungen tätigen und empfangen. Sie benötigen dazu ein Konto bei einer Bank, die Ecash anbietet, oder bei einem sogenannten Ecash Broker, der mit den Banken zusammenarbeitet.
Bei Ecash werden alle ausgegebenen Münzen in einer Datenbank registriert, um Mehrfachausgaben aufdecken zu können. Wird bei einer Überprüfung festgestellt, daß die Münze bereits registriert wurde, so kann man von einer versuchten Mehrfachausgabe ausgehen und die Münze wird für ungültig erklärt. Die Münzen sind mit einem Zeitstempel versehen. Nach einer bestimmten Zeit werden die Münzen ungültig und können vom Kunden bei der Bank eingetauscht werden. Die zeitliche Beschränkung der Gültigkeit begrenzt die Anzahl der ausgegebenen Münzen, die in der Datenbank registriert sind. Aber je mehr Kunden Ecash benutzen, desto mehr Münzen sind im Umlauf, und die ständig wachsende Datenbank wird somit zum Schwachpunkt im Ecash System. Eine Zahlungstransaktion kann bis zu einer Minute dauern.
Der Ecash Zahlungsvorgang läßt sich folgendermaßen darstellen: Zunächst muß der Kunde digitale Münzen in seine Geldbörse abheben. Dies geschieht mit dem Blinding-Verfahren (-> 6.4.1.). (a) Die „blinden“ Münzen (Token) werden an die Bank geschickt. (b) Diese schickt sie signiert zurück. (c) Der Kunde ist nun im Besitz signierter anonymisierter Münzen, die er ausgeben kann. (1) Der Kunde klickt auf „Bezahlen mit Ecash“. Der Händler stellt eine Zahlungsauforderung mit dem zu zahlenden Betrag. (2) Der Kunde transferiert die Münzen zum Händler. Wenn er die Münzen nicht passend hat, so muß er sie bei der Bank umtauschen. (3) Der Händler schickt die Münzen sofort an die Bank zur Überprüfung der Gültigkeit (-> 4.4. online Zahlungssysteme). Ist die Münze gültig, so wird der entsprechende Betrag vom Broker-Konto auf das Händler-Konto gebucht. (4) Der Händler bekommt eine Bestätigung über die erfolgreiche Prüfung. (5) Der Händler schickt dem Kunden eine Quittung und liefert die Waren aus.
Digicash B.V. erklärte 1998 Bankrott. Die Ecash-Technologie wurde 1999 von eCash Technologies, Inc aufgekauft. Zahlreiche Banken haben die Technologie lizenziert und geben eigenes Ecash-Geld in nationalen Währungen heraus. Hierzu gehört u.a. die amerikanische Mark Twain Bank, die ihren Ecash-Betrieb 1998 einstellte und die Deutsche Bank, die ihren Ecash-Betrieb 2000 ebenfalls einstellte.

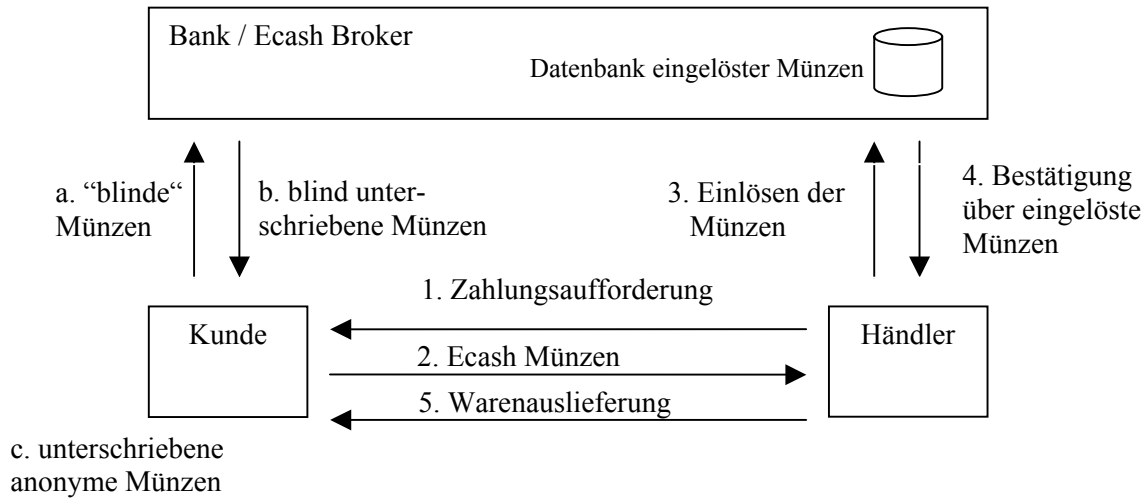

Abbildung 7.2.: Zahlungsablauf bei Ecash

MilliCent: Bei MilliCent handelt es sich um ein gutscheinbasiertes elektronisches Zahlungssystem für Microzahlungen entwickelt von Digital Equipment. Millicent verwendet händlerspezifische Gutscheine, sogenannte Scrips, die bei einem Broker erworben werden. Ein Scrip ist nur bei einem bestimmten Händler gültig und ist zeitlich limitiert. Der Händler tauscht die vom Kunden erhaltenen Scrips einmal im Monat in echtes Geld um.
MilliCent ist über den Status des Feldversuchs nicht hinausgekommen.

IBM MicroPayments: IBM Haifa hat MicroPayments als Lösung für Mikrozahlungen entwickelt [IBM03]. Das System basiert auf einem Mikro-Scheck-Konzept mit Aggregationskonten. Kunden erhalten täglich von ihrem MicroPayments-Provider ein Zertifikat, das sie zur Ausstellung von Mikro-Schecks bis zu einem gewissen Geldbetrag autorisiert. Händler sammeln diese Mikro-Schecks und reichen sie täglich bei ihren eigenen MicroPayments-Providern ein. Diese kooperieren zum Clearing untereinander.
Das MicroPayments-System hat sich am Markt nicht etablieren können.

Geldkarte: Die Geldkarte ist ein Smart Card-basiertes Kleinzahlungssystem [Geldk03], das als Bargeldersatz konzipiert wurde. Die Geldkarte auch für die Nutzung im Internet bereitzustellen [Geldon03] ist u.a. eine Initiative von [G&D03].
Der Bezahlvorgang im Internet ist im wesentlichen so organisiert wie der konventionelle Bezahlvorgang in Geschäften. Der Kunde muß im Besitz einer Geldkarte und eines Geldkartenlesegerätes (z.B. die Cashmouse von Giesecke & Devrient) und entsprechender Software sein. Der Händler benötigt ebenfalls Software, die die Funktion des Terminals übernimmt. Die Karte des Kunden und das "Terminal" des Händlers authentisieren sich gegenseitig über Zertifikate, z.B. über eine sichere Verbindung mit SSL (-> 6.1.4.). Der Zahlungsvorgang verläuft folgendermaßen: (1) Der Kunde klickt auf „Bezahlen mit Geldkarte". Der Händler schickt ihm eine Zahlungsaufforderung mit dem zu zahlenden Betrag. (2) Der Kunde schiebt die Geldkarte in das Kartenlesegerät. Die Geldkarte stellt eine Zahlungsanweisung aus und schickt sie an den Händler. (3) Der Händler hat somit eine Zahlungsgarantie und speichert diese ab. (4) Er kann die Waren ausliefern, bzw. die Dienstleistung erstellen. (5) Später schickt der Händler die gesammelten Zahlungsanweisungen zu seiner Bank. (6) Die Händlerbank führt mit der Kundenbank einen Kontenausgleich durch. Die Banken sind verpflichtet, bei Mißbrauch der Geldkarte, den Händler zu entschädigen. Kunden

bekommen ihre verlorengegangene Geldkarte nicht erstattet. Mit Hilfe von Schattenkonten (-> 6.5.) wird der Kunde aber vor Betrug geschützt.
Der durchschlagende Erfolg der Geldkarte ist beim Einsatz im Internet bis heute ausgeblieben. Es stellt sich wieder die Frage nach den Gründen, wobei die Anschaffung eines Kartenlesegerätes und die fehlenden Einkaufsmöglichkeiten mit der Geldkarte als Hauptgründe anzuführen sind. Da die Geldkarte auch beim Einsatz im realen Leben immer noch ihre Anlaufschwierigkeiten hat, was auf unzureichendes Marketing zurückgeführt wird, startet im Mai 2003 in München eine Kampagne, die den Kunden die Geldkarte näherbringen soll. Dabei ist Geldkarte keine separate Plastikkarte, sondern als Chip in die EC-Karte integriert. Damit sind Kleinzahlungen z.B. an vielen Automaten möglich [SüdZ03].

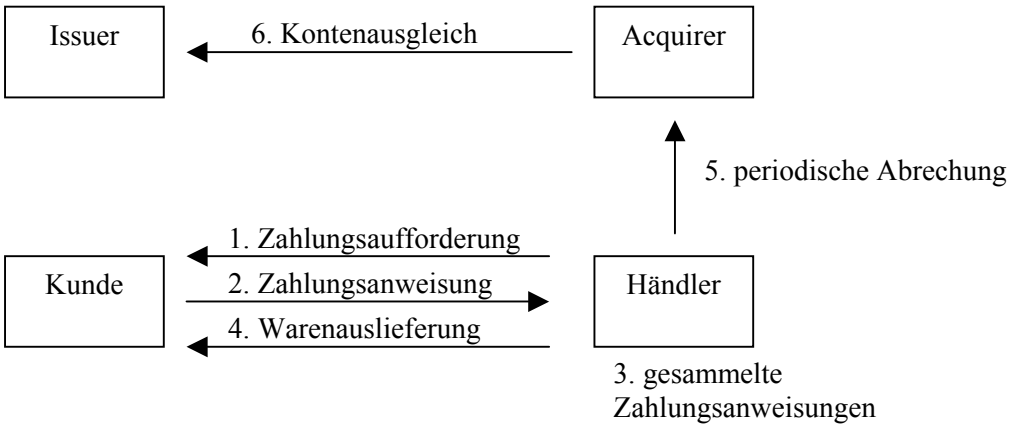

Abbildung 7.3.: Zahlungsablauf bei Geldkarte im Internet

7.3. aktuelle Entwicklungen

PayBox: PayBox wurde im Juli 1999 von Mathias Entenmann gegründet und entwickelt mobile Zahlungsverfahren [paybox03]. PayBox ist aber kein mobiles Zahlungssystem in dem Sinne, daß der Zahlende von überall aus mit dem Handy bezahlen kann, sondern PayBox benutzt das Handy lediglich zur Autorisierung einer Zahlung im Internet. Im Jahr 2000 haben sich die Deutsche Bank mit 50 Prozent und der Stuttgarter Mobilfunkdienstleister Debitel mit weiteren 4,8 Prozent an dem Unternehmen beteiligt.
Kunde wie Händler müssen einen Account bei PayBox haben. Bei der Bezahlung gibt der Kunde seine Handynummer an und klickt den „Call me!"-Button. Der Server des Händlers überträgt die Nummer mit dem zu zahlenden Betrag an die PayBox-Zentrale. Diese ruft automatisch auf dem Handy des Kunden an und fragt ihn, ob er mit der Abbuchung einverstanden ist. Der Kunde bestätigt dies mit seiner PayBox-PIN. Daraufhin wird der zu zahlende Betrag vom Kundenkonto abgebucht und auf dem Händlerkonto gutgeschrieben. Der Kunde bekommt eine SMS, die seine Zahlung bestätigt. Der Händler bekommt ebenfalls eine Bestätigung von PayBox und kann seine Leistung erbringen. Der Kunde muß für die Inanspruchnahme des Dienstes eine prozentuale Gebühr an PayBox abtreten.
Vorteilhaft bei PayBox ist die sichere Authentisierung des Kunden durch den Rückruf von PayBox und die weite Verbreitung von Handys, die einen zunehmenden Gebrauch des PayBox-Systems verspricht. Allerdings ist das Authentisierungsprozedere mit dem Rückruf von PayBox umständlich und zeitintensiv. Außerdem hat der Händler die Möglichkeit, in Besitz der Mobilfunknummer des Kunden zu kommen. Der Kunde ist dann vor penetranter Werbung über das Handy nicht mehr sicher.

Im Herbst 2002 hat die Deutsche Bank AG ihre Anteile an das PayBox-Management veräußert. Daraufhin hat Paybox seinen mobilen Zahlungsservice in Deutschland zwecks einer kompletten Umstrukturierung vorläufig unterbrochen. Als Gründe dafür werden die sehr langsame Entwicklung des mobile-payment-Marktes sowie das anhaltend schlechte Investitionsklima und die mangelnde Kooperationsbereitschaft insbesondere bei Banken und Telekommunikationsanbietern angeführt.

Sich ebenfalls am Markt etablieren konnte sich die 2000 in Köln gegründete **Firstgate Internet AG** mit ihrem Micropayment-System **Click&Buy** [First03] zum einfachen und sicheren Tarifieren und Abrechnen von Internet-Inhalten und –Diensten. Der Content-Anbieter muß sich gegen Gebühr bei Firstgate registrieren und integriert den Click&Buy-Button auf seiner Web-Seite oder auf der besucherstarken Web-Seite eines Partners. Für die Gestaltung der Umsatzprovisionen für Firstgate gibt es unterschiedliche Modelle. Der Kunde muß sich ebenfalls bei Firstgate registrieren. Als Zahlungsmöglichkeit bietet Firstgate alle bekannten Kreditkarten oder Bankeinzug an. Nach der Registrierung kann der Kunde sofort mit dem System bezahlen. Die Nutzung ist kostenlos für ihn und er bleibt gegenüber dem Content-Anbieter anonym. Einmal im Monat bucht Firstgate das Geld vom Girokonto oder der Kreditkarte des Kunden ab und teilt es unter den Content-Anbietern auf.
Click&Buy ist sehr kundenfreundlich, da es nicht der Installation spezieller Software bedarf. Allerdings ist Click&Buy nur als Dienst für Content-Anbieter gedacht, und nicht für die Abrechnung physikalischer Güter. Somit stellt Click&Buy kein umfassendes elektronisches Zahlungssystem dar.
Die **Deutsche Telekom** bietet seit November 2002 mit der Plattform **T-Pay** [tpay03] Kunden und Händlern gleich vier Abrechnungsarten an: Kreditkarte, Einzug per Telefonrechnung, Lastschriftverfahren und die MicroMoney-Karte. Der Kunde braucht keine spezielle Software, er kann Zahlungen aller Größenordnungen vornehmen. Der Konkurrenz ist vor allem die Abrechnung **über die Telefonrechnung** ein Dorn im Auge. Dabei kann T-Pay auf den vorhandenen Datenstamm der Telekom zurückgreifen und sich somit einen monopolistischer Vorteil verschaffen. Mit T-Pay können Güter aller Art bezahlt werden.
Die **Paysafecard.com GmbH** hat zusammen mit IBM **paysafecard** [pay03] als neues Zahlungsmittel für das Internet entwickelt. Die Funktionsweise des seit März 2001 verfügbaren Systems ist dabei mit Prepaid-Karten im Mobilfunkbereich zu vergleichen. Auf den Karten, die von Tankstellen, Kiosken und Einzelhändlern vertrieben werden, befindet sich eine sechzehnstellige Geheimzahl, die freigerubbelt werden muß. Beim Einkauf gibt der Käufer diese Nummer an und der zu zahlende Betrag wird vom Kartenguthaben abgebucht und dem Verkäufer gutgeschrieben. Diese anonyme Zahlungsart ist für den Kunden kostenfrei und bedarf nicht der Installation von Software.

8. Abschluß

Die meisten Zahlungssysteme, die in den 90er Jahren entwickelt wurden, haben ihren Dienst wegen fehlenden Geschäftserfolgs eingestellt. Verschiedene Gründe sind bei der Vorstellung der Zahlungssysteme (-> Kapitel 7) zum Teil schon genannt worden. Aber die Diskussion über das Scheitern der zum Teil wirklich vielversprechenden Ansätze, wie z.B. Ecash, gestaltet sich schwierig. Niemand weiß eine zufriedenstellende Antwort, alles ist mehr Spekulation denn Wissen.

Zum einen wird argumentiert, daß der Kunde von dem Wirrwarr der verschiedenen Zahlungssystemen abgeschreckt wird. Um das für ihn günstige System wählen zu können, muß er sich erst über die Vor- und Nachteile der jeweiligen Systeme kundig machen. Entschließt er sich für ein System, kann er nicht sofort damit bezahlen, sondern muß sich zunächst (umständlich) registrieren, Software installieren oder sich gar ein teures Chipkartenlesegerät anschaffen. Und all dieser Aufwand gewährleistet ihm nicht einmal, daß er überall im Internet bezahlen kann. Den Zahlungssystemen gehen somit die Kunden verloren, was wiederum die Händler abschreckt. Neben diesem klassischen Henn-and-Egg-Problem sollte man aber ebenfalls bedenken, daß gerade völlig neuartige innovative Systeme, wie z.B. Ecash, technisch, wirtschaftlich, juristisch, politisch, sozial und kulturell hochgradig komplexe Ansätze sind. Sie läuten eine neue Ära in der Geldwirtschaft und in den Gewohnheiten der Menschen ein. Vielleicht ist der Internet-User doch nicht so aufgeschlossen und flexibel, wie er immer beschrieben wird. Wenn es um das eigene Geld geht, ist er wohl vorsichtiger und konservativer als allgemein angenommen wurde.

Der Kreditkarte gerät zum Nachteil, daß die Banken keine Zahlungsgarantie geben, so daß der Händler Kunden ausgeliefert ist, die behaupten, nie eine Lieferung bekommen zu haben, und umgekehrt die Kunden Anbietern ausgeliefert sind, deren Leistung sie nie oder nicht ordnungsgemäß erhalten haben. Solange die Banken nicht die Beweislast in diesen Angelegenheiten übernehmen und Kunden und Händler somit abgesichert sind, wird es die Kreditkarte schwer haben. Zumal die Zahlung mit Kreditkarte auch nicht als unbedingt sicher gelten muß, da auf vielen Webseiten die Verschlüsselung mit zu kurzen Schlüsseln erfolgt und folglich die Daten leicht zu knacken sind. Der SET-Standard sollte da Abhilfe schaffen. In Europa mangelt es aber am Engagement der Banken. Die waren zunächst mit dem Jahr-2000-Problem beschäftigt und sehen sich heute aufgrund der allgemeinen schlechten wirtschaftlichen Lage mit weitaus wichtigeren Problemen konfrontiert als der Entwicklung und Standardisierung von elektronischen Zahlungssystemen. Von den einst angekündigten Großinitiativen ist nichts mehr zu hören. Die Banken sind sich uneins über die zukünftige Entwicklung, es gibt keinen gemeinsamen Ansatz für einen möglichen Standard. Daher werden den klassischen Zahlungsarten Rechnung und Lastschrift weiterhin Erfolgschancen eingeräumt.

Im Zuge der Kommerzialisierung des Internets, wo laut Prognosen bald alles nur noch gegen Bezahlung zu haben sein wird, konzentrieren sich die Systemanbieter auf Micropayment-Systeme, mit denen sie sich große Gewinnchancen ausrechnen. Die Bereitschaft für bestimmte Online-Inhalte und –Dienste zu zahlen, ist bei den Nutzern so hoch wie noch nie. Die Betreiber von Zahlungssystemen setzen dabei hauptsächlich auf zwei Verfahren: Die monatliche Sammelabrechnung, wie z.B. bei Firstgate, und die Bezahlung über eine Art Telefonkarten-System, wie z.B. bei Paysafecard. Die Telekom setzt mit ihre T-Pay-Plattform dennoch auf einen umfassenden Ansatz für Micro-, Klein- und Makrozahlungen. Die Akzeptanz für das erst seit kurzem verfügbare System wird sich zeigen.

Schlußendlich werden sich nur wenige Anbieter elektronischer Zahlungssysteme durchsetzen, so sie sich denn einen Marktanteil von mindestens 30% erarbeiten können. Hilfreich dabei ist die Zusammenarbeit mit Großunternehmen, wie z.B. bei der Paysafecard.com GmbH mit IBM, die durch ihre finanziellen Ressourcen den notwendigen langen Atem haben, um eine neue Technologie am Markt zu etablieren

Wie sich die Entwicklung der Zahlungssysteme in Zukunft gestaltet, kann absolut nicht vorausgesagt werden. Es fehlen die Standards und die dauerhaften Erfolgsrezepte. Das der Marktführer PayBox seinen Zahlungsdienst im Herbst 2002 eingestellt hat, zeigt, welche unvorhergesehene Wendungen das Geschäft mit den Zahlungssystemen im Internet haben kann, und wer sich langfristig am Markt behaupten kann, wird die Zukunft zeigen.

9. Literaturverzeichnis

[Eck01] Claudia Eckert: IT-Sicherheit. Konzepte-Verfahren-Protokolle, München, Oldenbourg Wissenschaftsverlag GmbH, 2001

[com03] http://www.computerwoche.de

[Cyb03] http://www.cybercash.de/

[First03] http://www.firstgate.de/

[G&D03] Giesecke & Devrient, http://www.gdm.de/

[Geldk03] http://www.geldkarte.de

[Geldon03] http://www.geldkarte-online.de

[ECC03] E-Commerce-Center Handel: http://www.ecc-hanel.de/

[gentz99] Ortwin Gentz: Integration der digitalen Zahlungsysteme CyberCash und Ecash in den elektronischen Aufsatzdienst Elektra. Diplomarbeit, TU München, Februar 1999

[heise03] http://www.heise.de

[ibis03] Vorlesung Internetbasierte Geschäftssysteme: Sichere Protokolle, TUM, SS 23.04.2003, http://ibis.in.tum.de/teaching/VO.htm

[IBM03] http://www.alphaworks.ibm.com/tech/micropayments

[ISEC02] The Third International Symposium on Electronic Commerce: Alan Liu, Vincent Y. Shen, Jogesh K. Muppala. Security Issues on Server-Side Credit-based Electronic Payment System http://ecommerce.ncsu.edu/ISEC/papers.html

[pay03] http://www.paysafecard.com

[paybox03] http://www.paybox.de

[reich01] Martin Reichenbach: Individuelle Risikohandhabung elektronischer Zahlungssysteme, Deutscher Universitäts-Verlag GmbH Wiesbaden, Betriebswirtschaftlicher Verlag Gabler GmbH Wiesbaden, 2001

[ruf96] Christine Ruf: Sicherheitsaspekte beim elektronischen Zahlungsverkehr im World Wide Web. Diplomarbeit, TU München, August 1996

[SET03] http://www.setco.org/

[SFE97] Rolf Schuster, Johannes Färber, Markus Eberl: Digital Cash. Zahlungssysteme im Internet, Springer-Verlag Berlin Heidelberg, 1997

[SSL96] http://wp.netscape.com/eng/ssl3/ssl-toc.html

[SüdZ03] Süddeutsche Zeitung vom 2. April 2003, Rubrik: München, Seite N1, gefunden bei www.GeldKarte.de

[tpay03] http://www.telekom.de/dtag/ipl2/cda/mr2/ 0,15187,0140129435111 00003166 2811,00.html

[Web00] Ricarda Weber: Accounting and Payment Concepts for Fee-Based Scientific Digital Libraries. Dissertation, TU München, Juni 2000