Universität Kaiserslautern

Seminararbeit zum Thema:

Sicherheitsaspekte beim Electronic Commerce

Melanie Ruhe
m_ruhe@informatik.uni-kl.de

Arbeitsgruppe Datenbanken und Informationssysteme

Seminar Anwendungsentwicklung
im Wintersemester 1999/2000

Inhaltsverzeichnis

1 Einleitung

Im Laufe der letzten Jahre und Jahrzehnte hat der Umgang mit elektronischen Medien immer mehr Einzug in des berufliche, aber auch das private Leben gehalten. Die rasante Entwicklung des Internet und dessen hohe Akzeptanz haben vor allem zu dieser Entwicklung beigetragen, was an folgenden Zahlen verdeutlicht werden soll: Der Computer-Almanach prognostiziert weltweit 300 Mio. Internetnutzer im Jahr 2000, allein in Deutschland wird mit 23 Mio. Nutzern des Internet gerechnet [www: cia]. Gleichzeitig haben sich über das Internet elektronische Vertriebswege als neue Wirtschaftskomponente etabliert.

Electronic Commerce ist das neue Stichwort, mit dem Firmen versuchen, sich den neuen wirtschaftlichen Herausforderungen zu stellen. Unter Electronic Commerce wird die automatische Durchführung von Handelstransaktionen über Kommunikationsnetze verstanden [Merz, Tu, Lamersdorf 99]. Es verspricht sowohl dem Kunden als auch dem Anbieter viele Vorteile und erfährt so innerhalb den letzten Jahren eine immer höhere Popularität [www: tuwien]:

Als Vorteile für die Kunden sind der höhere Komfort und ein hohes Maß an Bequemlichkeit zu nennen. Man muss keine Ladenöffnungszeiten beachten, spart sich die Anfahrtswege, insbesondere dann wenn es sich um Produkte aus anderen Länder oder Kontinenten handelt, und man kann völlig zwanglos durch die Angebote blättern. Den Anbietern hingegen steht, völlig unabhängig von der Größe des Unternehmens, der weltweite Markt offen. Als weiterer Vorteil ist die Einsparung an Kosten zu nennen, da weder ein “reales” Geschäft noch Verkäufer benötigt werden, um als Anbieter am Markt teilzunehmen. Dies kann sich in günstigeren Preisen für den Kunden niederschlagen.

Auch die Einführung des Euro treibt die Entwicklung des Electronic Commerce voran, da somit lästige Umrechnungen in Europa wegfallen. Bei der europäischen Kommission in Brüssel geht man davon aus, dass im Jahr 2000 schon nahezu 50% aller Geschäfte im Business-to-Business-Bereich in den EU-Ländern über das Internet abgewickelt werden. Das Marktvolumen wird auf 200 Milliarden Euro geschätzt [EITO 99]. Die Zahl der weltweiten Online-Nutzer, die über das Internet einkaufen, soll von 31 Millionen im Jahr 1998 auf 183 Millionen im Jahr 2003 ansteigen, was etwa 36 % der prognostizierten Zahl an Internetnutzern ausmacht [www: brokat].

Nichtsdestotrotz stehen diesen positiven Entwicklungen der letzten Jahre auch Probleme und Risiken gegenüber. Eine der technischen Herausforderung ist die an die Datenbanken. Zum einen müssen oft heterogene und global verteilte Datenbestände integriert werden, zum anderen sind die Anbindung ans Web und ein hohes Maß an Performance unumgänglich. Dabei spielen Zugriffsgeschwindigkeit, Aktualität und die einfache Nutzung des Datenbestandes eine große Rolle [Merz 99].

Eine weitere wichtige Rolle im Zusammenhang mit Electronic Commerce nimmt die Gewährung von Sicherheit, vor allem innerhalb von der Zahlungsvorgänge, ein. Das Internet wurde ursprünglich unter dem Paradigma der Offenheit für Forschungszwecke entwickelt und weist deshalb keine ausreichenden Sicherheitsprinzipien vor [www: isoc]. Wenn jedoch kein Vertrauen in die Technologie und deren Sicherheit vorhanden ist, werden sich die positiven Prognosen nicht erfüllen können. Die vorliegende Arbeit soll einen Überblick über die bisher entwickelten Lösungsansätze bieten, indem zum einem näher auf die entstehenden Probleme und Risiken eingegangen wird. Zum anderen werden verschiedene Entwicklungen von Zahlungsverfahren vorgestellt, die versuchen die aufgezeigten Probleme zu beantworten.

Die Arbeit ist wie folgt gegliedert: Zunächst wird der grundsätzliche Ablauf des Electronic Commerce vorgestellt und anhand dessen die verschiedenen Sicherheitsrisiken herausgearbeitet. Im dritten Abschnitt werden Anforderungen an die Transaktionen beim Electronic Com-

merce erläutert. Kapitel 4 dient der Aufbereitung der Lösungsansätze, es werden allgemeine Verschlüsselungsalgorithmen und Zahlungsverfahren präsentiert. Im letzten Kapitel wird kurz auf die praktische Umsetzung eingegangen und ein Ausblick gegeben, der ungelöste Probleme anspricht und eine Frage über die zukünftige Entwicklung aufwirft.

2 Motivation

Im folgenden Abschnitt wird die Funktionsweise des Electronic Commerce vorgestellt und anhand dessen werden die sicherheitskritische Stellen aufgezeigt. Herkömmlichen Verfahren zum Austausch von Informationen werden dazu noch einmal kurz vorgestellt, um deren Vor- und Nachteile aufzuzeigen.

In der realen Welt werden Informationen und Waren in physikalischer Form ausgetauscht und es ist eine Sicherheitsinfrastruktur vorhanden, die sich über Jahrhunderte aufgebaut hat und selbstverständlich ist. Man spricht vom Vertrauen in die Sicherheit dieser Aktionen. Das Beispiel Postverkehr soll dies verdeutlichen [www: brokat]:

Wenn Nachrichten von einem Ort in der Welt zu einem anderen vertraulich versendet werden sollen, wurde dies bis vor ein paar Jahren mit Hilfe des Postverkehrs vollzogen. Die Nachrichten wurden in einem Umschlag verborgen und ggf. versiegelt und gegebenenfalls per Einschreiben versendet. Somit konnte sichergestellt werden, dass die Nachricht zugestellt wird und nur der beabsichtigte Empfänger die Nachricht lesen kann. Eine Empfangsquittung diente dem Sender dazu, sich über den Empfang der Nachricht zu vergewissern. Heutzutage wird für diese Art des Nachrichtenaustausches oft das Internet genutzt. Eine Art neuer Postdienst (E-mail) wurde entwickelt, der viel schneller arbeitet und zudem auch kostengünstiger ist. Allerdings hat dieser neue Postdienst einige Schwächen: es gibt weder eine Garantie dafür, dass allein der Empfänger die Nachricht lesen kann, noch dafür, dass die Nachricht überhaupt ankommt. Es wird geschätzt, dass 20% des Datenverkehrs im Internet irgendwo kopiert und gespeichert wird [www: brokat]. Dies stellt eines der Risiken beim Electronic Commerce dar.

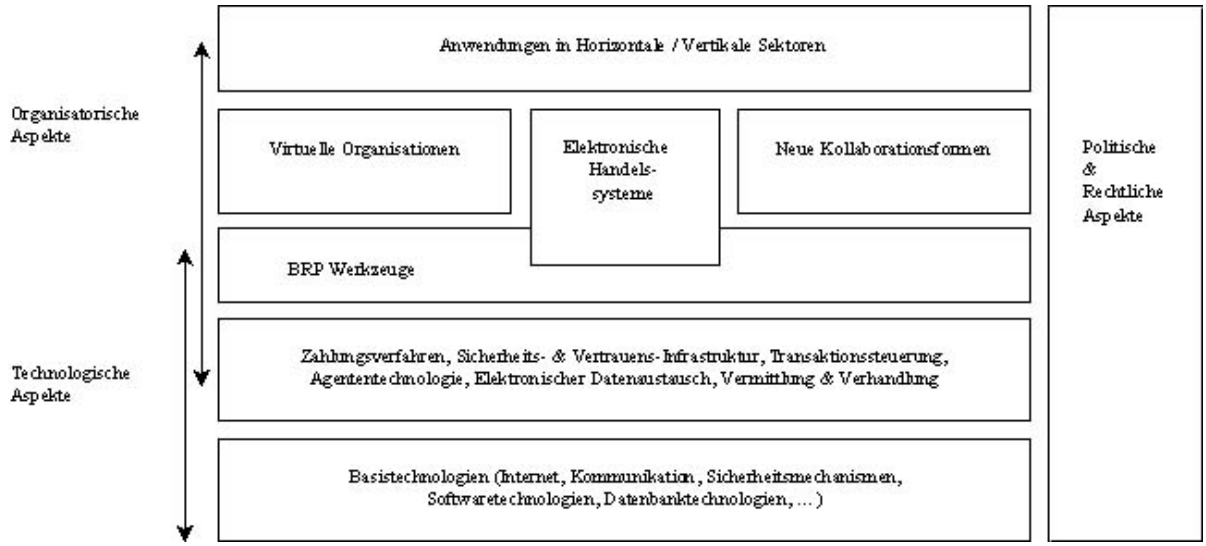

Abb. 1: Referenzmodell zum Electronic Commerce nach [Merz, Lamersdorf, Tu 99]

Vertrauen in die neuen Technologien muss zunächst gewonnen werden. Merz [99] formuliert das Problem wie folgt: “Sicherheit kann technisch realisiert werden – Vertrauen nicht.” Dazu sind technische und organisatorische Maßnahmen und deren Integration notwendig (siehe Abb. 1). Der Schwerpunkt dieser Arbeit liegt auf den technischen Maßnahmen. Grundlage für vertrauenswürdige Zahlungsmechanismen ist zunächst einmal die Sicherheit auf der Ebene der Basistechnologien [Merz 99].

Das Zahlungsmittel beim Postverkehr ist die Briefmarke. Im Internet werden andere Mittel eingesetzt, die in Kapitel 4 näher vorgestellt werden. Das normalerweise eingesetzte physische Geld ist dazu nicht geeignet. Stattdessen führt man digitales Geld ein, das schon seit Jahren in Form von Geld-, Kredit- und Magnetstreifenkarten in Benutzung ist [www: tuwien]. Fast jeder kennt sie und weiß deren Vorteile zu schätzen. Diese Form der Bezahlung wirft jedoch neue Probleme und Sicherheitsrisiken auf, da elektronisches Geld im Grunde nur eine Bitfolge ist, die man möglicherweise manipulieren oder kopieren kann.

An den Handelstransaktionen im Electronic Commerce sind in der Regel drei Rollen beteiligt (siehe Abb. 2): der Kunde, der Händler und die Bank, wobei durchaus weitere Instanzen beteiligt sein können (z. B. mehrere Banken). Zur Abwicklung eines Zahlungsgeschäftes gibt es zum einen die Möglichkeit Geld zwischen den Parteien zu transferieren, z. B. über die Geldkarte, und zum anderen kann der Käufer dem Händler auch eine Erlaubnis erteilen, bei seiner Bank Geld abzuheben, z. B. mit der Kreditkarte. Sowohl beim Transfer des Geldes oder der entsprechenden Erlaubnis kann durch Kopieren oder Fälschen Missbrauch entstehen.

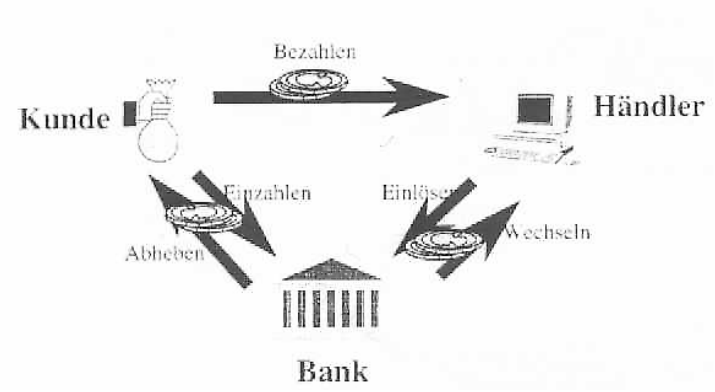

Abb. 2: Grundschema einer elektronischen Bezahlung [Merz, Tu, Lamersdorf 99]

Die wesentlichen Betrugsmöglichkeiten sind deshalb folgende [Merz, Tu, Lamersdorf 99]:

- *Double spending:* Elektronische Zahlungseinheiten werden mehrfach benutzt.
- *Stehlen von Daten:* Ein Kunde hat beispielsweise Kreditkarteninformationen gestohlen und gibt vor, Besitzer dieser Karte zu sein.
- *Händlerseitiger Betrug:* Ein Kunde bezahlt die Forderungen des Händlers, der jedoch den Empfang des Geldes abstreitet. Ebenso könnte es sein, dass ein Kunde bezahlt, dafür jedoch keine Waren übermittelt werden.
- *Käuferseitiger Betrug:* Ein Kunde bestellt Ware, streitet jedoch ab die richtigen Güter erhalten zu haben, d. h., es wurden eventuell nicht die richtigen Waren gesendet. Eine andere Möglichkeit besteht darin, dass der Kunde den Erhalt der Güter abstreitet.

Im folgenden werden deshalb Anforderungen an die Transaktionen definiert, die sowohl jenen Betrugsmöglichkeiten vorbeugen als auch Vertrauen bei den potentiellen Nutzern des Electronic Commerce aufbauen sollen.

3 Anforderungen an die Transaktionssteuerung

3.1 Atomarität

Eine Transaktion soll atomar und isoliert ausgeführt werden. Das Kriterium der Atomarität ist eines der vier Kriterien an Transaktionen in Datenbanken und ist auch im Bereich des Electronic Commerce unerlässlich. Es gewährleistet, dass eine Transaktion, die in der Regel aus

mehreren Aktionen besteht, entweder vollständig oder gar nicht ausgeführt wird, d. h., der Zustand des Systems ist der gleiche wie zu Beginn der Transaktion. Beim Scheitern einer Aktion der Transaktion zwischen Kunde und Händler muss vermieden werden, dass beispielsweise die Zahlung bereits erfolgt ist, die Warenabsendung jedoch nicht initialisiert wurde. Tygar [98] unterscheidet drei Grade von Atomarität:

1. *Geld-Atomarität:* Der Transfer der Zahlungsmittel ist atomar, d. h., das Geld kann weder zerstört noch kann neues Geld erzeugt werden.
2. *Güter-Atomarität:* Güter-atomare Protokolle sind gleichzeitig geld-atomar und beinhalten den exakten Austausch von Gütern basierend auf dem transferierten Geld. Man erhält genau dann Güter, wenn auch bezahlt wurde. Das ist beispielsweise dann wichtig, wenn man für das Herunterladen von Software Geld bezahlt, beim Datentransfer jedoch eine Unterbrechung stattfindet. Ein Beispiel aus dem Post-Liefer-Dienst ist das Paket per Nachnahme, das nur dann ausgehändigt wird, wenn die Rechnung an den Boten bezahlt wird.
3. *Zertifizierte Lieferung:* Zertifizierte Lieferung schließt Geld- und Güter-Atomarität ein, und zusätzlich erlaubt es den beteiligten Parteien genau zu prüfen, welche Güter geliefert wurden. Erhält ein Käufer die falsche Ware, so kann er sofort reklamieren und Ersatz einfordern.

3.2 Authentisierung

Die Authentisierung trägt ebenfalls zur Vertrauenswürdigkeit von Transaktionen bei. Auch hier ist im Internetprotokoll TCP/IP kein Verfahren implementiert, das es ermöglicht, den Absender einer Nachricht eindeutig zu bestimmen [Denning 98]. Emails können durch dritte Parteien manipuliert werden, z. B. können Inhalte und der Name des Senders verändert werden. Wenn gleiches mit den Kreditkarteninformationen geschehen würde, gäbe es zwischen Banken und Kunden häufig Auseinandersetzungen. Mit Hilfe der Authentisierung kann nachgewiesen werden, dass eine Nachricht von dem Absender kommt, der vorgibt es zu sein. Dies kann mit Zertifikaten oder Signaturverfahren (siehe Kapitel 4) erfolgen [Merz 99]. Zertifikate werden von Zertifizierungsautoritäten, sogenannten Trust-Zentren, vergeben, die als unabhängige, vertrauensvolle, dritte Partei fungieren. Außerdem gibt es die Möglichkeit, sich über ein Passwort zu authentisieren.

3.3 Integrität und Autorisierung

Im Internet besteht, wie in der realen Welt auch, nicht das Recht, auf beliebige Ressourcen zugreifen zu können. Deshalb müssen Rechte vergeben werden, die eine Person für bestimmte Aktionen autorisieren. Diese Berechtigungsnachweise müssen wiederum vertrauensvoll verwaltet werden, was beispielsweise durch jene Trust-Zentren erfolgen kann. Zertifikate können zusätzlich zur Authentisierung auch die Aufgabe der Autorisierung übernehmen. Im Falle von Zahlungen im Internet darf kein Geldtransfer auf ein Konto ohne Autorisierung des Inhabers erfolgen. Da nicht jeder Privatkunde über ein Zertifikat verfügt, gibt es weitere Methoden zur Autorisierung, wie z. B. Rückfragen, die auf eine Bestätigung für die Ausführung der Transaktion warten, nachdem über diese informiert wurde. Über Zugangskontrolllisten kann nach der Authentisierung festgestellt werden, wer für welche Transaktion autorisiert ist [Merz 99].

Um außerdem sicher zu gehen, dass die übertragenen Daten nicht manipuliert worden sind, gibt es Verfahren zur Prüfung der Unversehrtheit von Nachrichten. Zu diesem Zweck werden Hash-Algorithmen eingesetzt [Merz 99]. Dabei wird der auf der Basis der vorliegenden Nachricht mit bestimmten Algorithmen ein Hash-Wert berechnet, der vom Empfänger basierend auf der erhaltenen Nachricht verifiziert werden kann.

3.4 Anonymität

Kunden können den Wunsch haben, ihre getätigten Transaktionen geheim zu halten. Dritte Parteien, d. h., unbefugte Personen, sollen also nichts über die möglicherweise fragwürdigen Produkte, deren Preis o. ä. wissen, die eine Person erworben hat. Die Registrierung der Banknoten macht es beispielsweise möglich, den Weg zu verfolgen, den bestimmte Geldscheine "gehen" und verletzt somit dieses Kriterium. In diesem Fall würde man von Anonymität bezüglich der ausstellenden Bank sprechen. Eine weitere Form der Anonymität ist die des Kunden gegenüber dem Händler, d. h. der Händler erfährt nichts über die Identität des Kunden. In manchen Ländern sind vollkommen anonyme Transaktionen jedoch illegal. Generell ist das Kriterium der Anonymität als weniger wichtig einzustufen [Tygar 98].

3.5 Weitere Kriterien

Als weitere wichtige Kriterien sind zu nennen:

- *Verfügbarkeit:* Ein Zahlungssystem sollte 24 Stunden, 7 Tage pro Woche ohne Ausfall zur Verfügung stehen [www: tuwien].
- *Transaktionsgröße:* Das System sollte unabhängig von der Transaktionsgröße arbeiten, d. h., auch sogenannte Mikrotransaktionen (weniger als $1) bearbeiten [Tygar 98].
- *Mehrbenutzerbetrieb:* Das System muss von mehreren Personen gleichzeitig nutzbar sein.

Ein Zahlungssystem muss demzufolge zum einen den klassischen Datenbankanforderungen (ACID) genügen, und weiterhin müssen Kriterien zur Autorisierung erfüllt sein, um Vertraulichkeit zu gewährleisten. Beim Electronic Commerce sind nur selten all diese Kriterien erfüllt. Im folgenden werden nun verschiedene Verfahren zur Verschlüsselung und zur Bezahlung im Internet vorgestellt, die, falls möglich, anhand der oben genannten Kriterien bewertet werden.

4 Zahlungsverfahren

Das elektronische Bezahlen hat seine Anfänge in den 90er Jahren. Es galt zunächst als Mysterium, Produkte im Internet zu erwerben. Es wurden jedoch bald verschiedene Prototypen entwickelt, die diese Handelstransaktionen unterstützen sollten. Außerdem wurden Standards eingeführt, mit deren Hilfe man im Internet mit den klassischen Verfahren, wie Scheck, Kreditkarte oder Lastschriftverfahren, bezahlen konnte. Im Laufe der Zeit wurden zwar sehr viele Zahlungssysteme entwickelt, Schätzungen gehen auf etwa 100 Systeme, aber deren Qualität bzw. Sicherheit war mehr als fragwürdig [Merz 99]. Vor allem unter den potentiellen Käufern kann auf diese Weise kein Vertrauen aufgebaut werden. Nur wenige Systeme haben letztendlich Einsatz bei Banken und Firmen gefunden. In den folgenden Abschnitten werden diese Systeme klassifiziert und vorgestellt. Zunächst werden Verschlüsselungsalgorithmen erläutert, die bei Handelstransaktionen zur sicheren Übermittlung von Zahlungsinformationen benutzt werden.

4.1 Verschlüsselungsalgorithmen

Die Verschlüsselung ist eine der ältesten Maßnahmen, um Nachrichten gegenüber Dritten zu verbergen. Dazu verwendet man Schlüssel zum Ver- und Entschlüsseln. Ersterer überführt das Dokument in eine Form, die für Dritte ohne Schlüssel nicht rekonstruierbar ist. Zum Entschlüsseln wird wiederum ein Schlüssel benötigt (siehe Abb. 3).

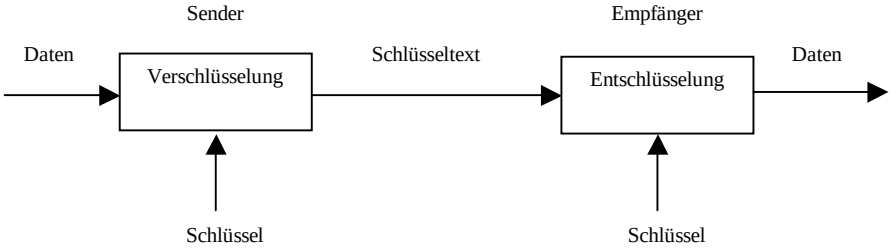

Abb. 3: Prinzip von Verschlüsselungsverfahren

Je nachdem, ob es sich bei dem Schlüssel zum Entschlüsseln um den gleichen oder einen anderen Schlüssel handelt, unterscheidet man symmetrische und asymmetrische Verfahren. Im ersten Fall besteht die Gefahr, dass der Schlüssel von Fremden kopiert und zum Entschlüsseln der Daten benutzt werden kann. Deshalb muss darauf geachtet werden, dass der Schlüssel über einen sicheren Kanal übermittelt wird, womit das Problem der sicheren Verteilung jedoch nur verlagert wird [Merz 99].

Im Internet haben sich aus diesem Grund die asymmetrischen Verfahren durchgesetzt. In diesem Fall werden zwei verschiedene Schlüssel benutzt, ein öffentlicher und ein privater Schlüssel. Der private Schlüssel darf nicht an Dritte weitergegeben werden, wohingegen der öffentliche Schlüssel bewusst öffentlich verteilt wird, um von jedermann zum Verschlüsseln benutzt werden zu können. Der Empfänger verwendet dann den privaten Schlüssel zum Entschlüsseln. Dabei ist zu beachten, dass der private Schlüssel nicht von Fremden kopiert werden kann. Von Nachteil bei diesen Verfahren ist der hohe Zeitaufwand beim Entschlüsseln. Deshalb werden oft symmetrische und asymmetrische Verfahren kombiniert, um sich deren beider Vorteile zu Nutzen zu machen [Merz 99].

Im folgenden werden einige Verfahren vorgestellt, die auch im Rahmen des Electronic Commerce Anwendung finden. Die praktische Umsetzung kann dabei sowohl hardware- als auch softwaremäßig (RSA bzw. Diffie-Hellmann) erfolgen.

4.1.1 DES

Der Data Encryption Standard (DES) ist ein symmetrisches Verfahren, das 1975 erstmals veröffentlicht wurde. Es werden jeweils Blöcke von 64 Bit verschlüsselt. Dies erfolgt mit einem 64 Bit langen Schlüssel, der auch zum Entschlüsseln dient und die Transformation der Daten steuert. Es werden mehrere Transpositionen und Substitutionen hintereinander ausgeführt, die von den Schlüsselbits gesteuert werden. Der Nachteil dieses Verfahrens liegt in der geringen Schlüssellänge und damit der Möglichkeit der Entschlüsselung durch Dritte. Als Erweiterung wurde deshalb Triple-DES eingeführt, das DES dreimal hintereinander ausführt [Merz 99].

4.1.2 RSA

Dieses sehr bekannte Verschlüsselungsverfahren ist nach seinen Entwicklern Rivest, Shamir und Adleman benannt und wurde 1978 erstmals veröffentlicht. Die Schlüssel haben eine Länge von bis zu 2048 Bit, wobei man bereits ab einer Länge von 1024 Bit von einer sicheren Länge spricht [Merz 99]. Man verwendet hier Schlüsselpaare und nutzt die Schwierigkeit aus, große Zahlen in Primfaktoren zu zerlegen. RSA gilt als sehr sicheres Verfahren gilt, da es für dieses Problem kein Verfahren mit vertretbarem Zeitaufwand zur Lösung gibt [www: tuwien]. Beim Entschlüsseln entsteht deshalb auch ein relativ hoher Rechenaufwand, was zur Folge hat, dass RSA häufig nur zum sicheren Austausch von Schlüsseln und zur Authentisierung

benutzt wird. Dieses Verfahren findet im Bereich des Electronic Commerce häufig Anwendung. Der Algorithmus selbst kann bei Merz [99] nachgelesen werden.

4.1.3 Diffie-Hellmann

Auch dieses Verfahren wurde nach seinen Erfindern Diffie und Hellmann benannt und wurde 1976 erstmals veröffentlicht. Dabei wird von den beiden Kommunikationspartnern ohne Vorwissen ein Sitzungsschlüssel vereinbart. Beide Partner müssen sich auf zwei Zahlen *g* und *n* einigen, welche die Bedingungen erfüllen, dass *n* Primzahl ist, und *g* modulo *n* prim zu *n* ist. Mit diesen Zahlen werden folgende Berechnungen durchgeführt [Merz 99]:

1. Partner A wählt eine beliebig große Zahl *x* und sendet an Partner B die Zahl $X=g^x \bmod n$
2. Partner B wählt eine beliebig große Zahl *y* und sendet an Partner A die Zahl $Y=g^y \bmod n$
3. A berechnet seinen Schlüssel $k=Y^x \bmod n$
4. B berechnet seinen Schlüssel $k'= X^y \bmod n$
5. Es gilt nun für beide Schlüssel $k=k'= g^{xy} \bmod n$

Somit sind die Schlüssel *k* und *k'* vereinbart, ohne dass es für Außenstehende nachvollziehbar ist, auch wenn *g*, *n*, *X* und *Y* öffentlich bekannt sind. Deshalb zählt dieses Verfahren ebenso wie RSA zu den Public-Key-Verfahren [Merz 99].

4.2 Kreditkartenbasierte Verfahren

Kreditkarten sind generell, insbesondere in den USA, ein sehr beliebtes Zahlungsmittel (etwa 1 Milliarde Karten weltweit). Außerdem ist diese Zahlungsart relativ einfach auf das Internet übertragbar und auf internationaler Ebene die einzige Zahlungsmöglichkeit im Business-to-Consumer-Bereich [Merz 99]. Im folgenden werden das Protokoll SSL, das die Übertragung von vertraulichen Informationen über das Internet sicherer gestaltet, und einige Kreditkartenbasierte Zahlungsverfahren vorgestellt.

4.2.1 SSL

Das Internet-Protokoll TCP/IP wird um die Secure Socket Layer (SSL) erweitert, um zwischen zwei Kommunikationspartnern im Internet (z. B. Client und Server) eine sichere Verbindung (sicherer Kanal) aufzubauen. Das Diffie-Hellmann-Verfahren ist dazu sehr geeignet, da es zwischen zwei "fremden" Kommunikationspartner im Internet ohne Vorwissen einen Sitzungsschlüssel generieren kann. Dies wird z. B. bei der Kreditkarten-Bezahlung eingesetzt, um die Kreditkarteninformationen vertraulich übertragen zu können. Allerdings bleibt das Risiko aufrecht erhalten, dass der Empfänger der Informationen diese missbraucht oder aber der Sender eine gestohlene Karte benutzt. Man spricht dann von händler- bzw. käuferseitigem Betrug [Merz 99]. Dennoch genießt das Verfahren weite Verbreitung als Vorstufe der installationsaufwendigeren Zahlungssysteme; die einzige Vorraussetzung auf der Server-Seite ist ein Zertifikat, das die Autorität des Händlers zertifiziert. Sehr bekannte Anwender von SSL sind "Amazon", die weltweit größte Online-Buchhandlung [www: tuwien], und der FCK (www.fck.de).

4.2.2 FirstVirtual

Hinter dem im Oktober 1994 in den USA eingeführten Internet-Zahlungssystem FirstVirtual steckt ein sehr einfaches Prinzip: Jede einzelne Aktion einer Handelstransaktion muss vom Kunden via Email bestätigt werden. Zunächst muss jedoch ein Konto bei FirstVirtual via E-mail eröffnet werden, worauf dem Kunden eine Telefonnummer über Email übermittelt wird. Auf telefonischem Weg, der als weitaus sicherer als das Internet gilt, werden dann die Kreditkarteninformationen übermittelt. Bei Kaufwünschen muss der Kunde dann nur die entsprechenden Produkte und seine Kontonummer bei FirstVirtual nennen. Daraufhin wird dem an diese Kontonummer gekoppelten Kunden eine Email zur Rückfrage geschickt. Als Antwort-

möglichkeiten kommen nur “ja”, “nein” oder “Betrug” in Frage. Im letzten Fall wurde der Kaufwunsch nicht vom Kontobesitzer, an den die Email gerichtet ist, geäußert, d. h. eine dritte Person ist im Besitz der Kontonummer. Daraufhin wird das Kundenkonto gesperrt und auf diese Weise dem käuferseitigem Betrug vorgebeugt. Bei der Antwort “ja” wird der entsprechende Betrag dem Kundenkonto bzw. später der Kreditkarte belastet [Merz 99, www: tuwien].

Aufgrund dieses Vorgehens kann FirstVirtual als geld-atomar, jedoch nicht als güter-atomar eingestuft werden [Tygar 98]. Ein weiterer Kritikpunkt ist, das FirstVirtual keine vollkommene Anonymität wahrt, da für jeden Kauf eine Zuordnung zwischen Kunde und Produkt(en) beim Händler gespeichert werden muss. Außerdem eignet sich das Verfahren weder für Mikrotransaktionen noch für Kunden, die kein Konto in den USA haben [Merz 99]. Als positiv einzuschätzen sind die geringen technischen Vorraussetzungen bei Händlern und Kunden und die Tatsache, dass Kreditkarteninformationen nicht über das Internet übertragen werden [www: tuwien].

4.2.3 Kreditkartenzahlung mit Vermeidung von Händlerbetrug (CyberCash)

CyberCash ist ein software-basiertes Zahlungssystem, das verschiedene Zahlungsmittel zulässt. Dazu muss sich der Kunde die kostenlose “CyberCash Wallet”-Software auf seinen Rechner laden. Bevor man das Wallet nutzen kann, müssen beim Installieren die Kreditkarteninformationen eingegeben werden Die Verschlüsselung der Informationen erfolgt auf der Client-Seite mit RSA und DES. Der geheime Schlüssel für RSA ist im Wallet gespeichert, der öffentliche Schlüssel für DES ist der vom Händler, der vom Wallet zu Beginn der Transaktion abgefragt wird. Auf Seiten der Händler ist das Programm “SMPS” notwendig. Das Zahlungsprotokoll wird vom Kunden auf den Webseiten des Händlers gestartet, indem das CyberCash Wallet eine Anfrage an den Händler sendet. Daraufhin laufen folgende Schritte ab (siehe Abb. 4):

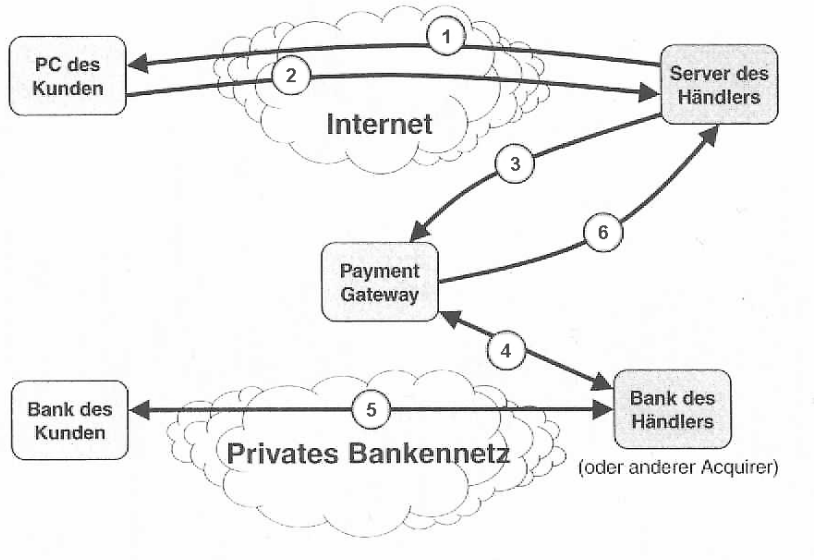

Abb. 4: Zahlungsprotokoll bei CyberCash [Merz 99]

1. Der Händler sendet nähere Informationen, wie z. B. den Preis, und fragt den Kunden nach der Zahlungsart.
2. Der Kunde wählt eine Zahlungsart aus und bestätigt die Anfrage. Dabei werden die Zahlungsinformationen verschlüsselt an den Händler geschickt.

3. Der Händler kann auf diese Informationen nicht zugreifen. Stattdessen versieht er die Daten mit einer elektronischen Signatur und sendet die Informationen weiter an den CyberCash Server (Payment Gateway).
4. Die Daten werden vom CyberCash-Server dekodiert und weitergeleitet.
5. Die Kreditkarteninformationen werden von der entsprechenden Bank verifiziert.
6. Im positiven Fall wird das Konto des Kunden belastet und eine Bestätigung an den Händler verschickt, der daraufhin dem Kunden die Waren zukommen lässt.

Neben der Bezahlung mit Kreditkarte können in Zukunft auch das Lastschriftverfahren und elektronisches Geld (siehe 4.4.) benutzt werden. Letzteres ermöglicht Mikrotransaktionen, also Zahlungen von weniger als US$10. Als Nachteile sind zu nennen, dass der Kunde in jedem Falle das CyberCash Wallet installieren muss. Bevor es zu Handelstransaktionen kommen kann, können mehrere Tage vergehen. Anonymität des Kunden gegenüber dem Händler jedoch nicht gegenüber der Bank gewährleistet. Im Falle von zahlreichen Kundenanfragen kann es zu Engpässen beim CyberCash Server kommen, da alle Autorisierungsvorgänge über ihn geregelt sind. Außerdem liegt die Software nur in Versionen für Windows und Macintosh vor [www: tuwien]. Von Vorteil ist, dass Händlerbetrug vermieden wird, der käuferseitige Betrug kann jedoch nicht ausgeschlossen werden [Merz 99]. Das im folgenden vorgestellte Protokoll SET versucht dies mit Hilfe von Zertifikaten zur Authentisierung des Kunden zu umgehen.

4.2.4 Kreditkartenzahlung mit Zertifikat (SET)

Visa und Mastercard haben gemeinsam das sehr komplexe Protokoll SET (Secure Electronic Transaction) entwickelt. Auch dies ist ein Zahlungsprotokoll zur Übermittlung von Kreditkarteninformationen, das jedoch versucht diese Transaktionen zu standardisieren. SET arbeitet mit digitalen Zertifikaten und einem asymmetrischen Public-Key-Verfahren, um die Transaktionsteilnehmer authentisieren und Bezahlung und Auslieferung garantieren zu können.

Um SET einzusetzen, sind auf der Kundenseite das relativ komplexe SET-Wallet zu installieren, auf der Seite des Händlers ein SET-Server auf dessen Web-Server und seitens der Bank des Händlers ein SET Payment Server [Merz 99]. Diese technischen Komponenten sind denen von CyberCash sehr ähnlich (vgl. mit Abb. 4). Zusätzlich werden Zertifikate für Kunde, Händler und Payment Server verwendet. Bei der Installation des Wallets werden wiederum die Kreditkarteninformationen verschlüsselt auf dem Rechner des Kunden gespeichert. Möchte der Kunde nun eine Zahlung vornehmen, geschieht folgendes [www: tuwien]:

1. Der Kunde sendet seinen Kaufwunsch zusammen mit den verschlüsselten Zahlungsinformationen an den Händler.
2. Der Händler übermittelt dem Kunden sein Händlerzertifikat, das Zertifikat des Payment Gateways und eine Transaktionsnummer.
3. Der Kunde sendet dem Händler sein Zertifikat, das er zuvor bei einer Zertifizierungsautorität erworben hat, die mit DES verschlüsselte unterschriebene Bestellinformation und die Kreditkarteninformationen, die mit RSA so verschlüsselt sind, dass nur die Bank des Händlers diese entschlüsseln kann (siehe Abb. 5)
4. Der Händler prüft das Kundenzertifikat (beim entsprechenden Trust-Center) und die digitale Unterschrift und schickt die Zahlungsinformationen weiter an seine Bank, nachdem sie vom ihm signiert wurden.
5. Die Bank des Händlers entschlüsselt und verifiziert diese Daten bei der Bank des Kunden. Das Ergebnis wird zusammen mit einer Autorisierungsnummer verschlüsselt an den Händler weitergeleitet, der bei positiver Nachricht eine beglaubigte Rechnung an den Kunden sendet.

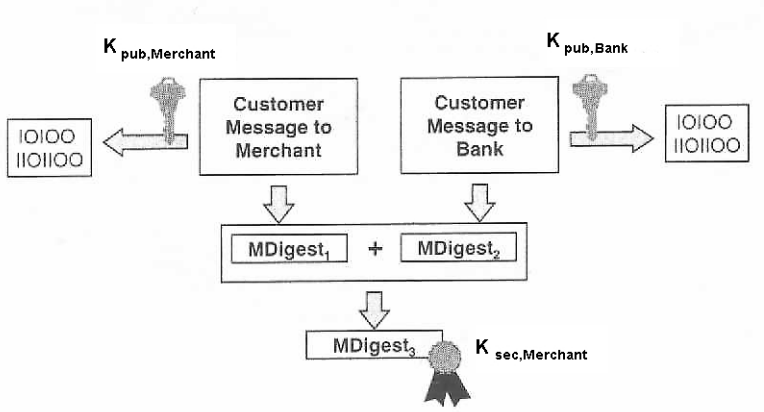

Abb. 5: Das dual-signature-Verfahren von SET [Merz 99]

Beim dual-signature-Verfahren werden die Bestell (OI)- und die Kreditkarteninformationen (PI) mit dem öffentlichen Schlüssel des Kunden bzw. der Bank verschlüsselt. Außerdem werden Hash-Werte für diese Komponenten ermittelt und miteinander verknüpft ($MDigest_1$, $MDigest_2$). Für diese Größe wird wiederum ein Hash-Wert ermittelt ($MDigest_3$), der dann im letzten Schritt mit dem geheimen Schlüssel der Bank signiert wird.

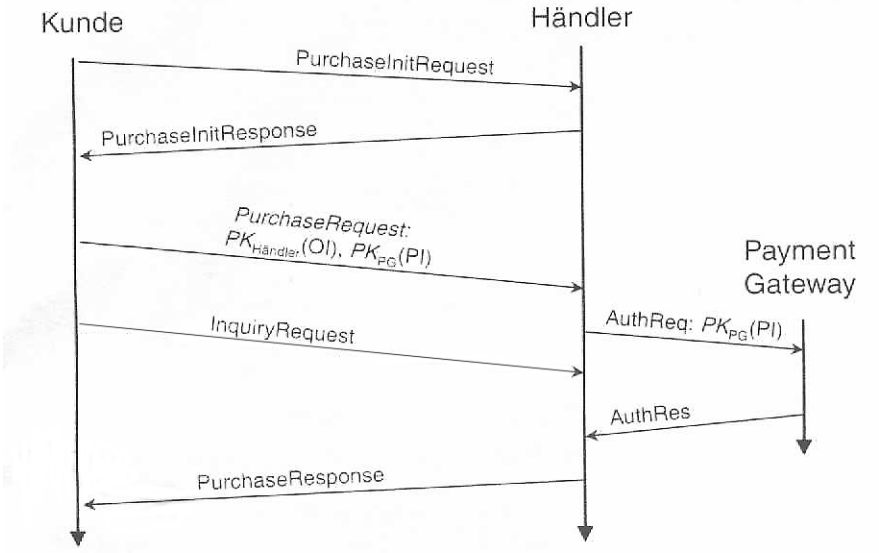

Abb. 6: Nachrichtenfluss bei SET [Merz 99]

Abb. 6 soll den Nachrichtenfluss bei SET verdeutlichen. SET bietet somit dem Käufer Vertrauen darüber, dass die Kreditkarteninformationen nicht missbraucht werden können. Dem Händler hingegen wird mit Hilfe des Zertifikates die Zahlungsfähigkeit des Kunden zugesichert. Auch die Höhe des zu zahlenden Betrages wird bei SET durch Verifikation der Daten des Kunden und des Händlers durch die Bank überprüft und festgelegt. Als Nachteil erweisen sich die komplexen Autorisierungsprozess sowohl beim Kunden als auch beim Händler und die fehlende Anonymität. Tygar [98] kritisiert weiterhin, dass SET zwar geld-atomar jedoch nicht güter-atomar ist. Dennoch ist diese Verfahren für Zahlungen über das Internet als das momentan sicherste Verfahren einzustufen [computerzeitung 99].

4.3 Kartenbasierte Verfahren

Diese Systeme basieren auf einer Karte mit einem Chip, auf dem Daten, wie z. B. Geldbeträge gespeichert werden können. Diese Guthabenkarten sind nicht nur für Electronic Commerce nutzbar, sondern finden im "realen" Leben häufig Einsatz. Die Systeme sind hardwareorientiert und gehen von der kritischen Annahme aus, dass diese Hardware fälschungssicher ist. Neben der Karte sind Kartenlesegeräte notwendig, die Beträge von der Karte abbuchen bzw. auf die Karte buchen können [Merz 99].

4.3.1 Smart Card

"Smart Cards entsprechen der Leistungsfähigkeit eines Heimcomputers der 80er Jahre" [Merz 99]. Sie verfügen neben einer CPU, RAM, ROM und weiteren Modulen über ein eigenes Betriebssystem, das die Kommunikation mit der Außenwelt über eine serielle Schnittstelle regelt und Daten verwaltet. Damit unterscheiden sie sich von Chip- und Magnetkarten vor allem in der höheren Sicherheit und Funktionalität. Jede Karte besitzt eine eigene ID und einen privaten Schlüssel, auf den Dritte nicht zugreifen können. Ein kryptographischer Koprozessor erzeugt RSA-Schlüssel von bis zu 1024 Bit Länge, die es ermöglichen Daten zu verschlüsseln bzw. zu signieren. Damit sind Smart Cards vielfältig einsetzbar: zum Authentisieren, Bezahlen, als Träger von Kundeninformationen usw. Eine weitere Alternative zur Authentisierung bilden biometrische Verfahren, die den Fingerabdruck prüfen. Diese Technologie ist jedoch noch nicht voll entwickelt, stellt aber ein weiteres Potential der Smart Card dar, da somit persönliche Daten weitaus sicherer als über PIN-Nummern oder Passwörter gespeichert sind.

Die Lesegeräte für Smart Cards können dementsprechend verschieden sein. Als einfachste Form sind Lesegeräte zu nennen, die nur den Ladezustand der Karte anzeigen. Um diese Karten auch für den Electronic Commerce einsetzen zu können, sind jedoch Lesegeräte notwendig, die im Rechner integriert sind. Folgende Möglichkeiten werden bisher angeboten [Merz 99]:

- Integration des Lesegerätes in das Diskettenlaufwerk mit einer entsprechenden Hülle im Diskettenformat, in die man die Smart Card einlegt.
- Externe Lesegeräte über serielle Schnittstellen.
- Integration des Lesegerätes in die Tastatur.
- Lesegeräte in Mobiltelefonen u. ä. Geräten.

Die Smart Card hat ein großes Potential vorzuweisen und kann auch bei entsprechender Entwicklung die Bezahlung beim Electronic Commerce sicherer und einfacher gestalten. Bis dahin muss jedoch noch an der sicheren Implementierung gearbeitet werden, um sowohl physikalische Angriffe als auch Angriffen auf Software-Ebene entgegnen zu können.

Geldkarte

Die Geld- bzw. Guthabenkarte stellt eine Form der Smart Card dar, die in Deutschland sehr beliebt und verbreitet ist, um Zahlungen auf elektronischem Wege vorzunehmen. Diese Smart Card kann mit einem Betrag von bis zu 400,- DM aufgeladen und schrittweise zur Bezahlung genutzt werden kann. Somit können auch Mikrotransaktionen vorgenommen werden. Von Nachteil ist, dass Daten wie z. B. der Betrag und die Kartennummer über Jahre hinweg gespeichert und somit keinerlei Anonymität gewahrt wird. Das Konzept wurde vom Zentralen Kreditinstitut entwickelt, das jedoch die Freigabe der Geldkarte für das Internet verweigert. Somit ist diese Verfahren für Electronic Commerce momentan noch nicht nutzbar, stellt jedoch für Nutzer in Deutschland und speziell für kleinere Geldbeträge ein großes Potential dar [Merz, Tu, Lamersdorf 99].

4.3.2 Mondex

Mondex ist ein in Großbritannien entwickeltes System, das erstmals 1995 eingesetzt wurde. Es wurde für den internationalen Gebrauch entworfen. Auf die Mondex-Karte kann über einen Code zugegriffen und sowohl über Bankterminals als auch speziell ausgestattete Telefone aufgeladen werden. Zusätzlich zur Karte besitzt man ein Mondex-Wallet als Lesegerät. Händler und Kunden verfügen über die gleichen Geräte. Sie ermöglichen es, zwischen zwei Kartenbesitzern Geld von einer Karte auf die andere Karte zu transferieren. Die Offline-Geldübertragung ist derzeit nur über diese Smart Cards möglich. Im Vergleich zur Geldkarte gewährt dieses Verfahren etwas mehr Anonymität; die letzten zehn Transaktionen werden jedoch auf der Karte gespeichert und sind über die Lesegeräte einsehbar [www: tuwien].

4.4 Elektronisches Bargeld (eCash)

Unter elektronischem Geld versteht man jene Zahlungssysteme, die dem Bargeldcharakter sehr nahe kommen, d. h. man kann grundsätzlich überall damit bezahlen. Es handelt sich um Münzen in elektronischer Form, die dem Kunden vollkommene Anonymität gewährt [Merz, Tu, Lamersdorf 99]. David Chaum hat diese Währung in Bit-Format 1994 in Zusammenarbeit mit der Firma DigiCash entwickelt. Der Herausgeber dieser eCash-Währung muss immer einen festen Wechselkurs einhalten, was zur Folge hat, das eCash nicht beim Handel auf länderübergreifender Ebene eingesetzt werden kann. Die Stückelung der Münzen entspricht 2er-Potenzen von 0.01, da dies von Vorteil für die Speicherung der Geldbeträge ist.

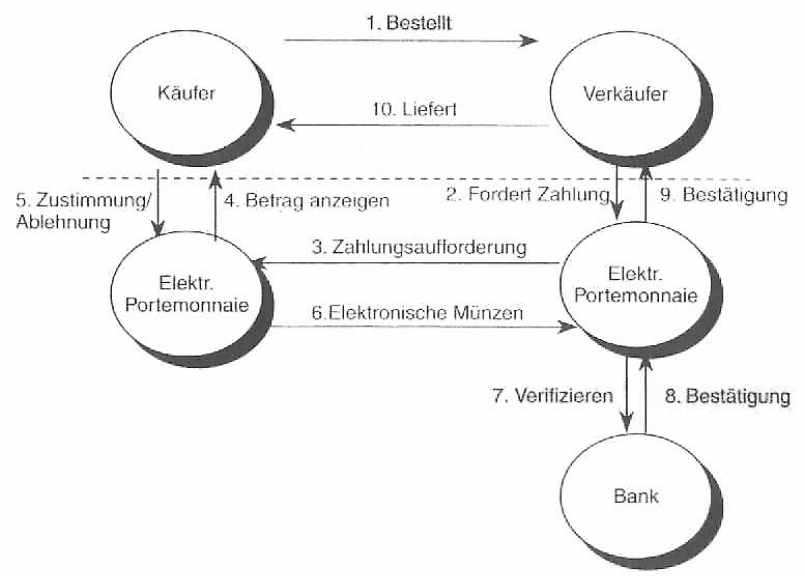

Abb. 7: Zahlungsprotokoll bei eCash [Merz 99]

Die einzelnen Schritte bei der Bezahlung mit eCash werden in Abb. 7 dargestellt. Kunde und Händler müssen dazu eine Software - eine Art elektronisches Portemonnaie - installieren, welches die Verwaltung des Geldes übernimmt. Abhebungen und Einzahlungen, die auch in geringen Höhen (Mikrotransaktionen) vorgenommen werden können, werden RSA-verschlüsselt übertragen und in einem Log-Buch der Bank festgehalten [www: tuwien]. Der Erwerb von Münzen erfolgt mit blinden Signaturen, die zum einen die Anonymität des Kunden gewährleisten und zum anderen der Bank die Möglichkeit der Kontrolle über das double spending bietet [Merz 99]. Von großem Nachteil ist, dass eCash keines der Atomaritätskriterien erfüllt [Tygar 98]. Da das Geld nur auf der Festplatte des Kunden gespeichert ist, besteht die Gefahr des Betruges durch Dritte und des Verlustes von „Geld“. Der Bargeldcharakter zwingt die Bundesbank aus wirtschaftlichen und rechtlichen Gründen, die Geldmenge zu kon-

trollieren und zu limitieren. Deshalb wird diese Form der Bezahlung bisher nur von Banken genutzt [Merz 99].

4.5 Billing-Verfahren

Der Ansatz von Billing-Verfahren unterscheidet sich von den bisher vorgestellten Verfahren. Das Prinzip teilt die Bezahlung in zwei Ebenen [Merz 99]: Auf der Ebene des Buchungssystems führt eine Bezahlung zur Kontenbuchung beim Betreiber. Auf der Ebene der Bezahlung gleicht der Betreiber die Konten aller Teilnehmer aus, indem er eine Abbuchung vornimmt bzw. eine Rechnung stellt. Dieses Prinzip wird seit langem von Telekommunikationsanbietern verwendet. Die Telefoneinheiten werden über einen bestimmten Zeitraum auf dem Kundenkonto verbucht und dem Kunden später in Rechnung gestellt. Dabei handelt es sich bei den einzelnen Transaktionen teilweise um sehr geringe Beträge, d. h., Billing-Systeme sind mikrotransaktionsfähig.

4.5.1 MilliCent

MilliCent wurde 1995 von der Digital Equipment Corporation (DEC) als Multikunden-Inkassosystem vorgestellt, das tokenbasiert arbeitet [Merz 99]. Es gilt als das wichtigste Mikrotransaktionssystem. Grundlage sind Token, sogenannte Scrips, die zu Beginn bei einem Broker erworben werden. Der Broker ist eine Art Zwischenhändler, der Scrips beim Händler zum Großhandelspreis erwirbt und im Wert von 0,1 Cent bis $5 an die Kunden weiterverkauft. Der Händler verkauft seine Scrips wiederum an den Broker. Die Scrips sind jedoch, anders als es bei eCash der Fall ist, nur bei einem Händler gültig und enthalten neben dem Namen des Händlers auch eine Seriennummer, ein Ablaufdatum, den Wert des Scrips und eine digitale Signatur des Händlers zur Authentisierung. Es können noch weitere Informationen auf den Token gespeichert werden.

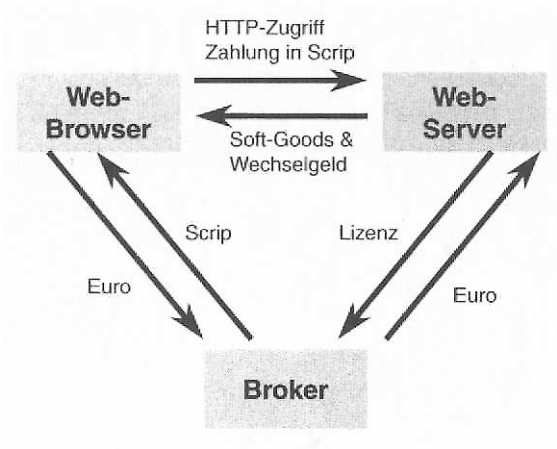

Abb. 8: Bezahlung mit Scrip bei MilliCent [Merz 99]

Abb. 8 verdeutlicht den Zahlungsvorgang bei MilliCent. Die Datenübertragung wird aus Gründen der Geschwindigkeit nur symmetrisch verschlüsselt. Dennoch sind die Token aufgrund kryptographischer Maßnahmen vor double spending geschützt. Der Händler besitzt eine Liste der Seriennummern und kann somit verifizieren, ob das Token bereits von einem Kunden zur Bezahlung benutzt wurde [www: tuwien]. Dies hat den Nachteil zur Folge, dass keinerlei Anonymität gewährleistet ist. Ein Vorteil von MilliCent gegenüber eCash ist, dass es von den Notenbanken nicht mengenmäßig begrenzt wird, da es nicht universell einsetzbar ist. MilliCent ist sehr geeignet für Soft-Goods von geringem Preis [Merz 99].

4.5.2 eCharge

Das Unternehmen eCharge nutzt die Telefon-Provider zur Abrechnung von im Internet getätigten Käufen. Will der Kunde im Internet etwas erwerben, müssen zunächst die Wallet-Software geladen und Fragen zur Person und dem Telefonanschluß beantwortet werden. Daraufhin werden Informationen zu den gewünschten Produkten verschlüsselt an den Kunden übermittelt und die Verbindung zum Internet durch das Wallet abgebrochen, um sich über Telefon beim eCharge Server einzuwählen. Über diesen Kanal wird der Kauf vollzogen und ein Schlüssel zum Entschlüsseln der Informationen gesendet. Die Verbindung zum Internet kann dann wieder hergestellt werden. Die Kosten der Produkte werden monatlich der normalen Telefonrechnung angefügt. Die Beträge sind dabei auf $300 begrenzt [www: echarge]. eCharge kann in das Microsoft Wallet integriert werden [Merz 99].

4.5.3 NetBill

Netbill ist ein Mikrotransaktionssystem für Informationsgüter, das 1994 von Studenten der University Carnegie Mellon, USA entwickelt wurde [www: tuwien]. Dieses Verfahren unterscheidet sich von allen anderen darin, dass sowohl das Geld als auch die Güter über das Internet transferiert werden. Netbill basiert auf einem Protokoll zwischen Händler, Kunde und dem NetBill-Server. Händler und Kunde müssen ein Konto auf dem Netbill-Server besitzen, auf dem das elektronische Geld, das zuvor vom Kunden eingezahlt werden muss, gespeichert ist. Somit wird sichergestellt, dass der Kunde sein Geld weder verlieren noch fälschen kann. Von Nachteil ist jedoch, dass der Server an jeder Transaktion teilnimmt und es dadurch zu Engpässen kommen kann.

Eine Zahlungstransaktion beinhaltet folgende Schritte [www: tuwien]:

1. Der Kunde sendet zusammen mit seinem öffentlichen Schlüssel seine Anfrage bezüglich der gewünschten Informationsgüter.
2. Der Händler beantwortet die Anfrage und sendet die Informationen zusammen mit einem symmetrischen Sitzungsschlüssel verschlüsselt an den Kunden.
3. Der Kunde bestätigt die Anfrage.
4. Der Händler übermittelt in verschlüsselter Form die gewünschten Informationsgüter zusammen mit einer Prüfsumme und dem Preis an den Kunden.
5. Die Software des Kunden signiert mit seinem privaten Schlüssel die Prüfsumme und den Preis und sendet die Daten an den Händler.
6. Der Händler prüft die Daten (Prüfsumme) auf deren Identität und signiert sie ebenfalls bevor er sie an den Server weiterleitet.
7. Der Server prüft die Identität der beiden Prüfsummen und Preise und ob der Kunde noch genügend Geld auf dem Konto hat. Ist dies der Fall, wird das Geld vom Kunden- auf das Händlerkonto übertragen und der Schlüssel für die verschlüsselten Informationsgüter an den Kunden verschickt.

Tygar [98] beweist, dass dieses Protokoll alle drei Atomaritätskriterien erfüllt und sich damit von vielen anderen Protokollen unterscheidet.

4.6 Zusammenfassung

Nachdem nun verschiedene Zahlungssysteme diskutiert wurden, werden deren wesentliche Eigenschaften in Tabelle 1 noch einmal zusammengefasst.

Tabelle 1: Eigenschaften der Zahlungsverfahren

System	Atomarität	Anonymität	Authentifizierung	Transaktionsgröße	Voraussetzungen auf der Kundenseite
FirstVirtual	Geld-atomar	Nein	Konto-Nr.	medium-macro	Kunde benötigt Konto in den USA; Email
CyberCash	Geld-atomar	Nein	Cyber Cash Wallet	medium-macro	CyberCash-Wallet
SET	Geld-atomar	Nein	Zertifikate	medium-macro	Zertifikat; SET-Wallet
Geldkarte	Geld-atomar	Nein	Karte, PIN	micro-medium	Karte
Mondex	k. A.	Nein	Karte	micro-medium	Karte & Lesegerät
eCash	keine	Ja	Seriennr. der Münzen	micro-medium	Software zur Verwaltung der Münzen
MilliCent	Geld-atomar	Nein	Seriennr. der Münzen	micro-medium	k. A.
eCharge	Geld-atomar	Nein	Telefon-Nr.	micro-medium	Telefonanschluss
NetBill	Zertifizierte Lieferung	Nein	Konto-Nr.	micro-medium	NetBill-Konto

5 Ausblick

Diese Arbeit untersucht die Sicherheitsaspekte beim Electronic Commerce. Nach der Erläuterung der Prinzipien im Electronic Commerce wurden verschiedene Verfahren vorgestellt, die zur Erhöhung der Sicherheit in diesem Bereich beitragen sollen. Die Vorstellung dieser Verfahren kann jedoch nur einen Ausschnitt dessen bieten, was momentan im Bereich des Electronic Commerce angewendet und entwickelt wird. Da dieser Zweig der Informatik bzw. Wirtschaft noch sehr jung ist, ist die Entwicklung von Dynamik geprägt und es kann an dieser Stelle nicht auf alle Möglichkeiten eingegangen werden.

Zusammenfassend kann festgestellt werden, dass sich die traditionellen Systeme wie die Kreditkarte, das Lastschriftverfahren bzw. die Geldkarte am ehesten durchsetzen werden. Dies ist vor allem darin begründet, dass deren Umsetzung und Anwendung im Internet sehr einfach ist und die Kunden bereits Vertrauen in diese Verfahren in der realen Welt aufgebaut haben. Ein weiterer Grund besteht in der Wirtschaftlichkeit der einzelnen Systeme. Dazu sind jedoch bisher keine genauen Zahlen veröffentlicht worden [Merz 99].

Um als Händler im Internet seine Produkte anbieten zu können, benötigt man Software, die neben der Realisierung des Zahlungsverkehrs z. B. auch Produkte präsentieren, Bestellungen aufnehmen und Datenbanken verwalten kann. Bei der Umsetzung dieser Anforderungen gibt es erneut eine Vielzahl von Ideen bzw. Anbietern von Software. Diese Anbieter müssen sich aber neben der sicheren Abwicklung der Handelstransaktionen vor allem auch um ihre Wirtschaftlichkeit kümmern. Die “Computer Zeitung” [computerzeitung 99] warnt in diesem Zusammenhang mit folgender Schlagzeile: “Sicheres Bezahlen im Web spielt keine müde Mark ein.” Viele Verfahren sind bisher an ihrer mangelnden Wirtschaftlichkeit gescheitert. Es ist demnach nicht klar, inwieweit die vorgestellten Verfahren auch tatsächlich genutzt werden.

Die Frage, ob sich Electronic Commerce letztendlich durchsetzen wird, kann noch nicht beantwortet werden. Technologisch gesehen sind die Grundlagen für Handelstransaktionen über

das Internet geschaffen worden. Außerdem ist aber auch eine organisatorische und rechtliche Vertrauensinfrastruktur notwendig. Das Kundenrisiko muss so weit wie möglich reduziert und geschützt werden, so dass Kunden ohne Bedenken auf diese Alternative zurückgreifen können. Vertrauen muss der Händler jedoch nicht nur gegenüber dem Kunden sondern auch gegenüber den beteiligten Banken aufbauen. Bisher haben sich Banken ihr Vertrauen von den Händlern bezahlen lassen [Merz, Tu, Lamersdorf 99]. Wie und ob das Vertrauen längerfristig auch ohne finanzielle Mittel erworben werden kann, bleibt eine offene Frage.

Ein weiterer kritischer Aspekt in diesem Zusammenhang ist, inwieweit Entwicklungen wie das Internet und Electronic Commerce die Gesellschaft verändern können. Folgende Fragen sind beispielsweise zu überdenken: „Wird die Arbeitslosigkeit durch die Entwicklung des Electronic Commerce ansteigen?“, „Inwieweit wird sich die zwischenmenschlichen Kommunikation verringern bzw. verändern?“ oder „Welche rechtlichen Konsequenzen wird diese Entwicklung mit sich bringen?“

6 Literaturverzeichnis

[computerzeitung 99]	Computer Zeitung, Sicheres Bezahlen im Web spielt keine müde Mark ein, Jahrgang 10, Ausgabe 47, 25.11.1999
[Denning 98]	D. E. Denning, P. J. Denning, Internet Besieged, Addison-Wesley, 1998, Part IV, pp. 373-435
[EITO 99]	European Information Technology Observatory - EITO Jahresbuch 1999, ISBN 3-8163-0378-1
[Merz 99]	Michael Merz, Electronic Commerce, dpunkt-Verlag, 1999
[Merz, Tu, Lamersdorf 99]	Michael Merz, Tuan Tu, Winfried Lamersdorf, Electronic Commerce, Informatik Spektrum, Band 22, Heft 5, S. 328ff.
[Tygar 98]	J. D. Tygar, Atomicity versus Anonymity: Distributed Transactions in Electronic Commerce, Proceedings VLDB’98, New York, 1998, S.1-12
[www: brokat]	http://www.brokat.de/netnews/archive-ecommerce.html
[www: cia]	http://www.c-i-a.com
[www: echarge]	http://www.echarge.com
[www: epays]	http://www.epaynews.com
[www: isoc]	http://www.isoc.org/internet-history/
[www: tuwien]	http://stud1.tuwien.ac.at/~e8525020/preecash.html