Analyse unterschiedlicher Zahlungssysteme im Internet

STUDIENARBEIT
Prüfung zum
Diplom – Wirtschaftsinformatiker
(Berufsakademie)

im Ausbildungsbereich Wirtschaft
in der Fachrichtung Wirtschaftsinformatik

an der
BERUFSAKADEMIE
-Staatliche Studienakademie-
RAVENSBURG

Name:	Marc Grieser
Kurs:	WI 98
Betreuer:	Prof. Dr. Michael Bächle
Abgabedatum:	02. Januar 2001

INHALTSVERZEICHNIS

1 EINLEITUNG 1

2 ANFORDERUNGEN AN EIN ZAHLUNGSSYSTEM IM INTERNET 2

3 EIGENSCHAFTEN UND BESONDERHEITEN DES B2C – BEREICHES 3

3.1 ÜBERBLICK 3
3.2 TRANSAKTIONSVOLUMEN UND DEREN ABGRENZUNG 3
3.3 STATISTIK 5

4 SICHERHEIT UND VERTRAUEN 5

4.1 ALLGEMEINES 5
4.2 AUTORISIERUNG 6
4.3 VERSCHLÜSSELUNG 6
4.3.1 Überblick 6
4.3.2 DES – Data Encryption Standard 8
4.3.3 RSA – Rivest-Shamir-Adleman 8
4.3.4 IDEA – International Data Encryption Standard 9
4.4 DATENINTEGRITÄT 9
4.5 AUTHENTISIERUNG 10
4.6 ZERTIFIKATE 11

5 ZAHLUNGSSYSTEME IM INTERNET 12

5.1 0190ER NUMMERN 12
5.2 KREDITKARTENZAHLUNGEN 12
5.2.1 Allgemeines 12
5.2.2 SSL – Secure Socket Layer 13
5.2.3 Cyber Cash 13
5.2.4 SET – Secure Electronic Transaction 14
5.3 ELEKTRONISCHES GELD 16
5.4 BILLING VERFAHREN 20
5.4.1 Allgemeines 20
5.4.2 MilliCent 20
5.4.3 Net900 21
5.4.4 Variable Internet Billing System - Vibsy 21
5.5 PAYBOX 22

6 BEWERTUNG 24

Quellenverzeichnis

Ehrenwörtliche Erklärung

1 Einleitung

Das Internet ist zu einem nicht mehr wegzudenkenden Medium unserer Gesellschaft geworden. Dienste, wie z.B. das World Wide Web (WWW), e-mail oder File-Transfer (FTP) ließen die Anzahl der Nutzer schlagartig in die Höhe schnellen, wie Abb.1 verdeutlicht.

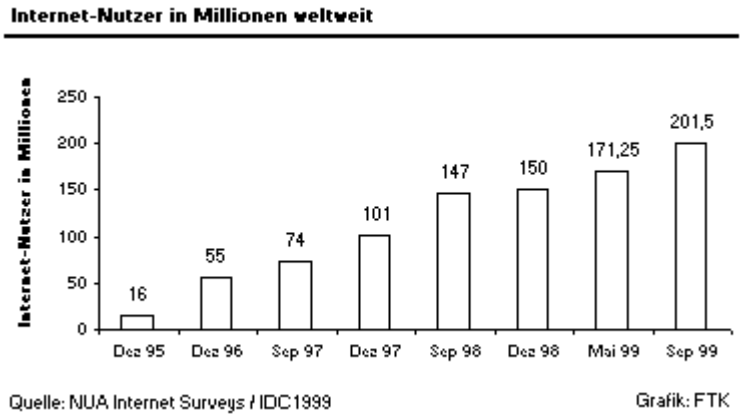

Abbildung 1: Internet-Nutzer in Millionen weltweit

Quelle: [Eci300]

Ein weiter Trend ist der sogenannte Electronic Commerce oder eCommerce (EC). [nach: KöBe98, S. 7] definiert eCommerce folgendermaßen:

„eCommerce ermöglicht die umfassende, digitale Abwicklung der Geschäftsprozesse zwischen Unternehmen und deren Kunden über öffentliche und private Netze (Internet).“

Eine wichtige Voraussetzung für diese Art der Internetnutzung ist die Möglichkeit des Bezahlens der gekauften Waren oder Dienstleistungen auf elektronischem Wege.

Diese Problematik möchte ich in meiner Studienarbeit näher betrachten und die wichtigsten bereits bestehenden elektronischen Zahlungssysteme analysieren. Besonders eingehen möchte ich hierbei auf den Business-To-Consumer (B2C) Bereich.

Betrachten wir zunächst die unterschiedlichen Anforderungen, die an ein Zahlungssystem im Internet gestellt werden.

2 Anforderungen an ein Zahlungssystem im Internet

Elektronisches Geld weißt nicht mehr die gewohnten Charakteristika von Banknoten und Münzen auf. Es schöpft seinen Wert nur noch aus der Funktion und nicht mehr aus dem Materialwert. Es ist nur noch digitale Information [KöBe98]. Deshalb werden an elektronische Zahlungssysteme besondere Anforderungen gestellt: [Bäch00]

Sicherheit

Einer der wichtigsten Aspekte beim Bezahlen im Internet ist wohl die sichere Abwicklung der Zahlungstransaktion. Es soll verhindert werden, daß Dritte, z.B. an persönliche PIN-Nummern, Kreditkartennummern oder sonstige Schlüssel, gelangen können. Ebenso dürfen beim Bestellvorgang keine Daten durch Dritte geändert werden können.

Skalierbarkeit

Jeder Internetnutzer hat die Möglichkeit, ein elektronisches Zahlungssystem zu nutzen. Deshalb sollten solche Systeme nicht an die Grenzen ihrer Leistungsfähigkeit (Teilnehmerzahl, etc.) stoßen. Die Erweiterbarkeit der Systeme spielt hierbei eine nicht unbedeutende Rolle.

Micropayments

Jedes Zahlungssystem sollte effizient und wirtschaftlich arbeiten. Das heißt auch im Bereich kleiner Beträge (< 5 Euro) sollten die Transaktionskosten (Buchungskosten, Systemkosten, etc.) in einer wirtschaftlichen Relation zum getätigten Umsatz stehen.

Bedienbarkeit

Das Zahlungsmittel muß für den durchschnittlichen Benutzer einfach zu bedienen sein. Das heißt die Systeme sollten überschaubar und transparent sein, sowie für jeden Schritt des Zahlungsvorganges bis hin zum bewußten Einleiten der eigentlichen Zahlung nachvollziehbar sein.

Anonymität

Für den Käufer muß es möglich sein, anonym zu bleiben, d.h. Zahlungen ohne Preisgabe seiner Identität durchzuführen. So ist es dem Händler nicht möglich, Kundenprofile des Kunden anzulegen. Andererseits sollte Kriminalität wie z.B. Geldwäsche vorgebeugt werden.

Akzeptanz

Als äußerst wichtig erscheint es mir auch, daß ein Zahlungssystem sowohl vom Händler als auch vom Kunden bereitwillig akzeptiert wird, um ein möglichst einheitliches Zahlungssystem im Internet vorzufinden und nicht bei jedem anderen Händler jeweils auf unterschiedliche Zahlungsmethoden zurückgreifen muß.

Konvertierbarkeit der Währungen

Das Internet kennt keine Grenzen. Ich kann meine Ware oder Dienstleistung in Amerika, Asien, Afrika, Australien oder Europa beziehen. Deshalb ist es auch wichtig, daß das elektronische Zahlungssystem nicht nur in einem geschlossenen Zahlungsraum eingesetzt werden kann.

Doch mit den Anforderungen allein ist es noch nicht getan. Im B2C – Bereich gibt es noch einige Besonderheiten, die es zu beachten gilt.

3 Eigenschaften und Besonderheiten des B2C – Bereiches

3.1 Überblick

Beim B2C – Commerce spricht man von dem Handel zwischen einem Anbieter und einer großen, wechselnden Zahl an Kunden. Das Transaktionsvolumen ist in aller Regel aber ziemlich gering. Wir sprechen von Zahlungen im Bereich von einigen wenigen bis zu einigen hundert Euro. Der wesentlichste Unterschied zum Business – To – Business (B2B) Commerce aber, ist das Fehlen entsprechender Anwendungssoftware auf der Kundenseite, ausgenommen des Web-Browsers mit eventuell installiertem Wallet.

3.2 Transaktionsvolumen und deren Abgrenzung

[Merz99] gliedert die unterschiedlichen Transaktionsvolumenbereiche anhand der dadurch unterschiedlichen zugrundeliegenden Geschäftsmodelle. Je nach Transaktionsvolumen unterscheidet man bei den technischen Verfahren der Zahlungsabwicklung.

Macropayments (>= 1.000 Euro)

Macropayments kommen eher im B2B Commerce zum Tragen. Es besteht bereits eine Beziehung zwischen den beiden Transaktionspartnern. Aufgrund der hohen Transaktionskosten und des benötigten Vertrauens in den Geschäftspartner kommen hier Internet-Zahlungsverfahren nur sehr schwer zum tragen.

Medium Payments (5 – 1.000 Euro)

Medium Payments liegen in dem Bereich, die mit Kreditkartenzahlungen abgedeckt werden können. Ich muß hierbei kein besonderes Vertrauensverhältnis zu meinem Geschäftspartner aufbauen, da dies meist durch Dritte, wie z.B. Banken oder Kreditkartengesellschaften übernommen wird. Dieser Bereich ist bis heute auch am interessantesten für Online Transaktionen und Internet Bezahlung.

Micropayments (0,1 – 5 Euro)

Bei den Micropayments kommt in der „Offline-Welt“ nur Bargeld als Zahlungsmittel in Frage. Die positiven Eigenschaften des Bargeldes in diesem Bereich, wie z.B. vollkommene Anonymität, oder keine Bank zur Verifikation notwendig, lassen sich nur sehr schwer auf Online-Zahlungssysteme abbilden. Aber gerade in diesem Marktsegment stecken interessante Geschäftspotentiale im B2C oder Consumer – To – Consumer (C2C) Bereich (z.B. Online-Auktionen).

Nanopayments (0,001 – 0,1 Euro)

Der Begriff Nanopayments wurde lediglich eingeführt, um diesen Bereich benennen zu können. Das Transaktionsvolumen ist so gering, daß sich der Aufwand für Micropayment Verfahren für niemanden rechnen würde. Die Transaktionspartner sollten in diesem Bereich sogar akzeptieren, daß Zahlungsmittel mangels transaktionaler Unterstützung hin und wieder verloren gehen.

3.3 Statistik

Die neuen Möglichkeiten, im Internet zu bezahlen, werden noch nicht so genutzt, wie angenommen. Es werden nach wie vor die „Offline“ Verfahren, wie Rechnung, oder Bankeinzug bevorzugt, wie Abb. 2 zeigt. *„Verschiedene Arten des elektronischen Geldes sind mittlerweile technisch ausgereift, so dass in Zukunft der Anteil dieser Zahlungssysteme steigen dürfte“.* [Eci400]

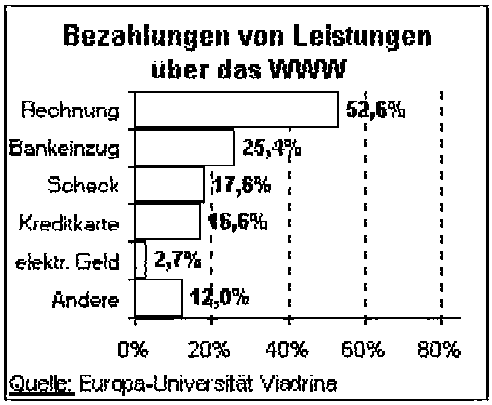

Abbildung 2: Bezahlungen von Leistungen über das WWW

Quelle: [Eci400]

4 Sicherheit und Vertrauen

4.1 Allgemeines

Eine der wichtigsten Voraussetzungen für ein Zahlungssystem, dies gilt sowohl für Offline-, als auch für Onlinezahlungssysteme, ist, daß es von den Nutzern akzeptiert wird. Dies wiederum setzt voraus, daß ich als Nutzer Vertrauen in dieses habe. Vertrauen habe ich, wenn ich mich in der Umgebung sicher fühle.

Sicherheit kann technisch realisiert werden, jedoch das Vertrauen nicht. Aber Sicherheit ist ein wichtiger Grundstein dafür.

Doch was versteht der Nutzer unter Sicherheit?

Zum einen ist es der Schutz der Privatspähre, zum anderen aber auch die Sicherung von Werten in Form von Geld, oder anderen handelbaren Gütern. [Merz99]

Nachfolgend will ich einige Punkte aufführen, die diese Sicherheit ermöglichen sollen.

4.2 Autorisierung

Wer darf was? Dies ist die zentrale Frage, welche die Autorisierung zu beantworten versucht. Nur der Hinweis darauf, daß ein bestimmter Bereich nicht betreten werden darf, würde nicht ausreichen. Deshalb müssen spezielle Barrieren errichtet werden, die den Zugriff auf bestimmte Ressourcen nicht für jede Person freigeben.

Moderne Betriebssysteme verwalten deshalb verschiedene Benutzer, die unterschiedliche Rechte über z.B. Dateien, Verzeichnisse, Kommunikationsports, Geräte oder sogar ausführbare Software haben.

Schwieriger wird die Autorisierung aber im Internet. Hier werden durch zertifizierte Kontrollinstanzen, Zertifikate vergeben, die zu bestimmten Handlungen berechtigen. Auf diesen Bereich gehe ich weiter unten in meiner Arbeit nochmals speziell ein.

4.3 Verschlüsselung

4.3.1 Überblick

Beim eCommerce werden meist sensible Daten und Dokumente zwischen Kunde und Händler auf elektronischem Wege ausgetauscht. Durch Verschlüsselung dieser Dokumente soll verhindert werden, daß potentielle Angreifer diese einsehen oder ändern können. Hierzu werden spezielle Schlüssel eingesetzt, die verhindern sollen, daß Dritte das Originaldokument rekonstruieren können.

Es gibt zwei Verfahren, seine Dokumente zu ver- bzw. entschlüsseln. Die symmetrische und die asymmetrische Verschlüsselung. In der Praxis des eCommerce werden diese Verfahren oftmals gekoppelt. Auf bekannte Algorithmen, welche die asymmetrischen bzw. symmetrischen Verfahren nutzen, wird weiter unten noch eingegangen.

Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung besitzen Sender und Empfänger den identischen Schlüssel. Man spricht von einem Private Key. Dieser wird sowohl zur Chiffrierung, als auch zur Dechiffrierung der Daten eingesetzt. Der generelle Nachteil dieses Algorithmus ist der direkte Austausch des geheimen Schlüssel, welcher seine Anwendung in einer Kunde-Händler Beziehung erschwert. In der

Praxis wird oft ein sicherer Übertragungskanal gewählt, wie z.B. ein Diskettentausch der Partner, auf dem sich der Schlüssel befindet. Der Schlüssel darf jedoch niemals in unberechtigte Hände geraten. Deshalb auch der Name, Private-Key Verfahren. Der Vorteil besteht in der relativ geringen benötigten Rechenleistung. [Ding97] Abb. 3 verdeutlicht den Vorgang nochmals.

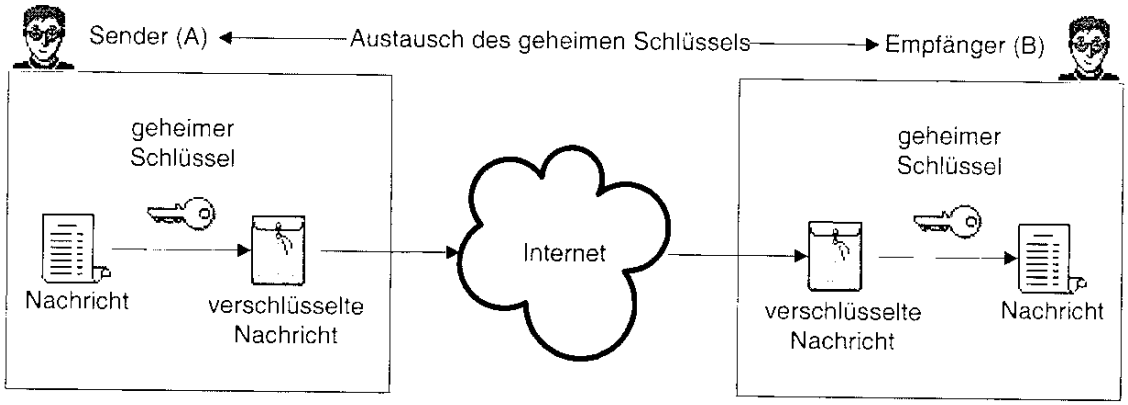

Abbildung 3: Symmetrische Verschlüsselung

Asymmetrische Verschlüsselung

Die Gefahr, die sich beim Austausch der Private-Keys beim symmetrischen Verfahren ergibt, wurde schnell erkannt. Aus diesem Grund haben sich im Internet zum größten Teil auch die asymmetrischen Verfahren durchgesetzt. Hier besitzt der Anwender zwei Schlüssel. Ebenfalls einen privaten Schlüssel (Private-Key), der wiederum geheim gehalten werden sollte und nicht mal dem Kommunikationspartner mitgeteilt werden darf, als auch einen öffentlichen Schlüssel (Public-Key). Dieser Public-Key sollte bewußt verbreitet werden. Jede beliebige Person darf den öffentlichen Schlüssel besitzen.

Will der Sender mir nun eine Nachricht übermitteln, deren Inhalt für potentielle Angreifer verborgen bleiben sollte, verschlüsselt er sie mit meinem allgemein bekannten öffentlichen Schlüssel. Nachrichten, die mit meinem Public-Key verschlüsselt wurden, können auch nur wieder durch meinen Private-Key entschlüsselt werden. Da dieser private Schlüssel nie von einer Person außer mir

gesehen wurde, kann auch nur ich diese Nachricht wieder dechiffrieren. Siehe auch Abb. 4.

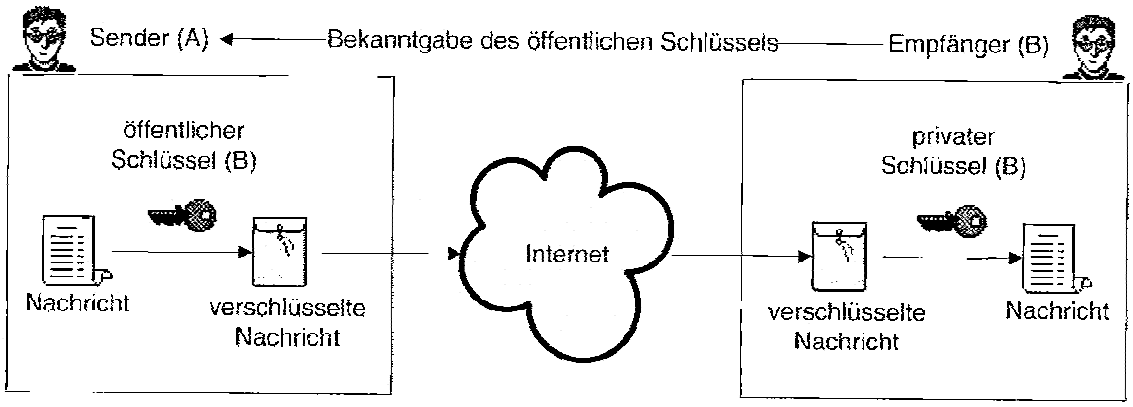

Abbildung 4: Asymmetrische Verschlüsselung

Die umgekehrte Reihenfolge entspricht der Digitalen Signatur, welche weiter unten noch näher erläutert wird.

4.3.2 DES – Data Encryption Standard

DES ist ein symmetrisches Verschlüsselungsverfahren, das 1975 von IBM entwickelt wurde. Aufgrund der Begrenzung der Schlüssellänge der amerikanischen Regierung auf 56 Bit, gilt das Verfahren als relativ unsicher. Es findet aber immer noch Anwendung in der Industrie und auch in Geldautomaten.

Als Weiterentwicklung des DES – Algorithmus gilt das Verfahren Triple-DES. Hier wird die Verschlüsselung dreimal angewandt und somit ergibt sich eine Schlüssellänge von 168 Bit. [Ding97]

Der DES Algorithmus wird oftmals zum Aufbau einer SSL (Secure Socket Layer) Verbindung benutzt, welche ich weiter unten noch erläutere.

4.3.3 RSA – Rivest-Shamir-Adleman

RSA ist ein asymmetrisches Verschlüsselungsverfahren, das 1978 veröffentlicht wurde. Der Algorithmus kann ebenfalls zur digitalen Signatur verwendet werden. Eine mit RSA verschlüsselte Nachricht mit angemessenem Aufwand zu entschlüsseln, gilt als so unwahrscheinlich, daß die US-Sicherheitsbehörde (National Security Agency - NSA) erhebliche Exportrestriktionen für den Algorithmus festlegte. Außerhalb der USA darf er lediglich zum signieren von

Daten oder im Finanzsektor eingesetzt werden. Je nach Sicherheitsbedürfnis kann man Schlüssellängen bis zu 2048 Bit verwenden. [Merz99]

Jedoch haben wir bei den asymmetrischen Verfahren das Problem der Geschwindigkeit. Die Softwareimplementierung von DES gilt als um den Faktor 100 schneller als RSA. [Ding97]

RSA findet z.B. bei eCash und SET Anwendung. Auf beide Bereiche gehe ich später noch ein.

4.3.4 IDEA – International Data Encryption Standard

IDEA ist ein symmetrisches Verfahren, welches in den 90er Jahren in Europa entwickelt wurde. Es gilt als sehr stark, da es aus diesem Grund nicht den US-Exportbestimmungen unterliegt. Der Algorithmus verwendet 128 Bit Schlüssel und arbeitet noch schneller als das DES Verfahren.

4.4 Datenintegrität

Es soll sichergestellt sein, daß meine gesendeten Daten unversehrt und auch unverändert beim Empfänger eintreffen. Bei der Online-Bestellung müssen z.B. Preis, Name und Kontonummer richtig und nicht manipuliert beim Händler ankommen. Um die Daten auf Korrektheit zu überprüfen werden Hash-Algorithmen eingesetzt.

Aus den Daten, die gesendet werden, wird ein Hashwert errechnet. Dieser ist in aller Regel wesentlicher kürzer (<= 200 Bit) als der Ausgangsstring. Es ist allerdings auch möglich, daß mehrere verschiedene Ausgangsdokumente den gleichen Hashwert erzeugen. Man spricht dann von einer Kollision, die aber in der Praxis als eher unwahrscheinlich gilt. Es ist allerdings nicht möglich, von dem Hashwert zurück auf das Originaldokument zu schließen. Deshalb wird es auch als Einweg-Hash-Funktion bezeichnet.

Das Originaldaten und der Hashwert werden getrennt voneinander an den Empfänger übermittelt. Wird das Originaldokument nun auf dem Weg zu seinem Bestimmungsort von Dritten verändert oder manipuliert, kann dies der Empfänger feststellen, indem er von dem erhaltenen Dokument wieder einen Hashwert bildet und mit dem ihm vorhin übermittelten vergleicht. Allerdings sollte der Hashwert auf sicherer Weise zum Empfänger gelangen. Dies kann durch Einsatz der oben genannten Verfahren geschehen.

4.5 Authentisierung

„Allgemein bedeutet Authentisierung nachzuweisen, daß eine Nachricht von dem Sender kommt, von dem sie zu sein vorgibt.“ [Merz99]

Im Internet haben sich hierfür die elektronischen Signaturen durchgesetzt. Diese sollten im Allgemeinen folgende Eigenschaften aufweisen: [Ding97]

- Authenzität – Dem Empfänger wird bestätigt, daß das Dokument von dem Sender stammt.
- Fälschungssicherheit – Nur der Sender darf die Möglichkeit besitzen seine Dokumente zu unterzeichnen.
- Die Signatur darf nicht auf ein anderes Dokument übertragen werden können.
- Nach der Unterzeichnung darf ein Dokument nicht mehr geändert werden können.
- Die Unterschrift darf nicht mehr zurückgenommen werden können, d. h. der Unterzeichner darf im Nachhinein seine Unterschrift nicht leugnen können.

Mit asymmetrischen Verschlüsselungsverfahren, wie z. B. RSA, können all diese Bedingungen erfüllt werden. Sie arbeiten folgendermaßen. Der Sender berechnet den Hashwert aus seinem Dokument und verschlüsselt diesen mit seinem Private Key, den ja nur er kennt. Sobald der Empfänger das Dokument und den verschlüsselten Hashwert erhält, errechnet auch dieser den Hashwert aus dem Dokument. Nun braucht er nur noch mit dem Public Key des Empfängers den Hashwert zu entschlüsseln und mit seinem berechneten zu vergleichen. Sind sie identisch, so stammt die Unterschrift eindeutig vom Sender. Vorausgesetzt ist natürlich, daß der öffentliche Schlüssel des Senders auch wirklich von ihm stammt. Dies wird aber von Vermittlern zertifiziert. Vergleiche Abb.5.

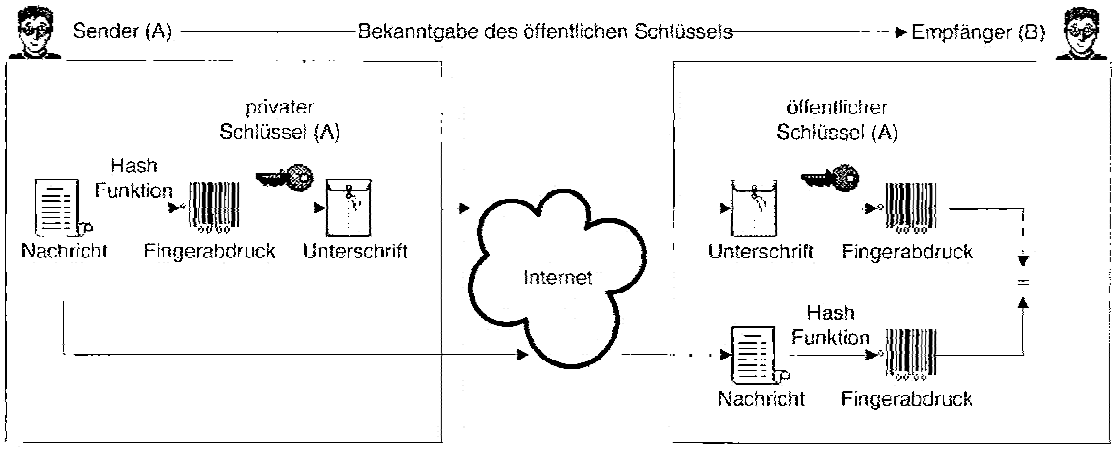

Abbildung 5: digitale Signatur

4.6 Zertifikate

So sicher die oben genannten Verschlüsselungsverfahren auch sind, so funktionieren sie nur richtig, wenn die Schlüssel eindeutig einer Person zugeordnet werden können. Hierzu werden Zertifikate verwendet. Eine zentrale Institution, die Zertifizierungsstelle, überzeugt sich von der Identität und vom öffentlichen Schlüssel einer Person. Aus diesen Daten wird ein Zertifikat erstellt, das mit dem Private Key der Zertifizierungsstelle verschlüsselt wird. Der Public Key der Institution ist ja allgemein bekannt, und somit kann auch das Zertifikat wie der entschlüsselt werden und der Public Key des eigentlichen Senders entnommen werden. Abb.6 erläutert das Verfahren der Zertifizierung näher.

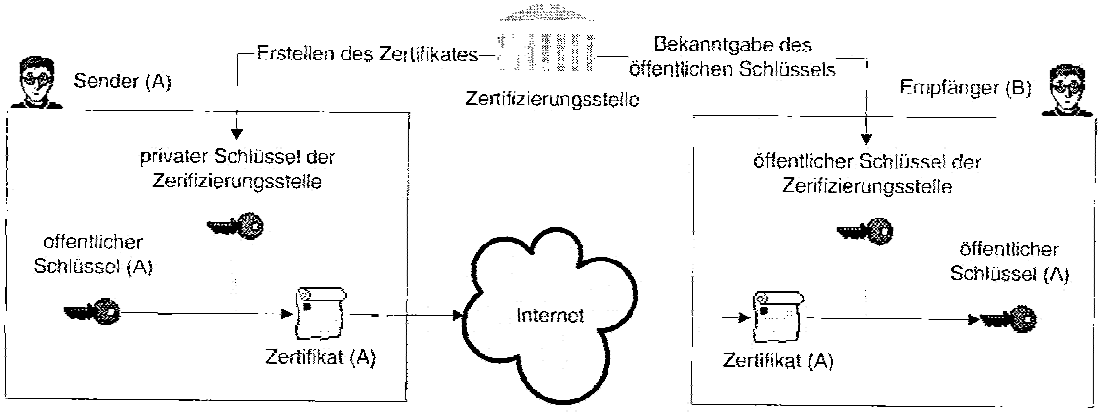

Abbildung 6: Zertifikate

5 Zahlungssysteme im Internet

5.1 0190er Nummern

Die wohl einfachste Art und Weise, Beträge im Micropayment Bereich zu begleichen, sind die 0190er Nummern. Das Prinzip ist einfach. Nachdem der Kunde sich für ein Produkt oder eine Dienstleistung bei einem Anbieter entschieden hat, gibt dieser ihm eine kostenpflichtige (z.B. 50 Cent pro Minute) 0190er Nummer an. Der Kunde muß diese nun eine bestimmte Zeit lang anrufen und sich z.B. mit Werbung des Händlers berieseln lassen. Nachdem die Zeit abgelaufen ist, wird ihm über das Telefon ein bestimmter Schlüssel mitgeteilt, mit dem er das Produkt bestellen, oder die Dienstleistung nutzen kann. Dieses Verfahren findet häufig Anwendung bei Seiten, die schlüpfrige Fotos oder Videoclips anbieten.

Ein gravierender Nachteil dieses Verfahrens sind aber die horrenden Gebühren, welche die Telekom auf diese Nummern berechnet. Es sind derzeit noch 50% des Umsatzes, was abzuführen ist. Jedoch durch die gebrochene Monopolstellung der Telekom, dürfte auch hier bald Besserung in Sicht sein. Wenn diese Gebühren sinken, sind diese Nummern ernst zu nehmende Gegner anderer weit aus mehr ausgeklügelter Micropayment Verfahren.

5.2 Kreditkartenzahlungen

5.2.1 Allgemeines

Die Kreditkartenzahlung ist die am meisten genutzte Möglichkeit, Waren im Internet zu bezahlen. Dem Händler muß einfach der Name und die geheime Kreditkartennummer übermittelt werden. Für den tatsächlichen Zahlungsverkehr ist jedoch noch eine Kooperation mit einem sog. Acquirer, *„einer Organisation, die die Zahlungsaufforderung entgegennimmt und den Geldtransfer zwischen den Banknoten von Kunde und Händler initiiert“* [Merz99 S.165], von Nöten. Diese Rolle wird oft von bestimmten Serviceunternehmen oder direkt von den Kreditkartenunternehmen übernommen. Die Kosten einer solchen Zahlung belaufen sich beim Händler auf 3% des Zahlungsbetrages. Im Micropaymentbereich sind Kreditkartenzahlungen jedoch uneffizient, da die Transaktionskosten zu hoch sind. Ich möchte nun 3 Verfahren zur Übermittlung der sensiblen Kreditkartendaten vorstellen.

5.2.2 SSL – Secure Socket Layer

Bei diesem Verfahren werden die Daten direkt in ein HTML-Formular eingetragen und bei der Übermittlung mit SSL, dem meist ein symmetrisches Verschlüsselungsverfahren zu Grunde liegt, verschlüsselt. SSL ist ein sehr einfaches Verfahren, welches verhindert, daß vermeintliche Angreifer die Daten bei der Übertragung einsehen können. Die sichere Übertragung der Daten ist in dem jeweiligen Web-Link daran zu erkennen, daß er mit https:// beginnt.

Jedoch kann der kunden- oder händlerseitige Betrug nicht ausgeschlossen werden. Mit diesem Verfahren kann nicht garantiert werden, daß der Händler vertraulich mit den Kreditkartendaten umgeht und diese nicht mißbraucht. Ebenfalls kann nicht ausgeschlossen werden, daß der Kunde über fremde Kreditkarteninformationen verfügt, oder eine Bestellung im Nachhinein leugnet.

Um zumindest den händlerseitigen Betrug auszuschließen wurde Cyber Cash entwickelt.

5.2.3 Cyber Cash

Cyber Cash war ein sehr bekanntes Verfahren, welches den händlerseitigen Betrug nicht zuließ. Der Kunde verschlüsselte seine Kreditkartendaten so, daß der Händler diese nicht einsehen konnte. Nur ein sogenannter Cyber Cash Server war dazu in der Lage und bestätigte dem Händler die Zahlung. [Merz99]

Cyber Cash sollte zumindest mal erwähnt sein, jedoch möchte ich nicht näher darauf eingehen, da dieses Verfahren wegen mangelnder Akzeptanz eingestellt wurde. Die Cyber Cash GmbH schreibt [Cybe00]:

„CyberCash GmbH wird die Wallet-basierten Bezahlverfahren nicht weiter unterstützen. Dies sieht ein Beschluß ihrer Gesellschafter vor. Die mangelnde Akzeptanz der elektronischen Geldbörse seitens der Endkunden ist einer der wesentlichen Gründe für diese Entscheidung.“

Ein Verfahren, welches sowohl den händler-, als auch den käuferseitigen Betrug ausschließt, ist das SET Verfahren.

5.2.4 SET – Secure Electronic Transaction

Beim SET Zahlungsprotokoll ist sowohl der händler- als auch der käuferseitige Betrug ausgeschlossen. Deshalb bietet dieses Verfahren einen optimalen Schutz bei elektronischen Transaktionen. Es ist sowohl eine Authentifikation des Karteninhabers, als auch des Händlers gegenüber dem Kreditkartenunternehmen möglich. Dies wird dadurch realisiert, indem beide Teilnehmer Zertifikate ihrer Banken benötigen.

Um SET als Kunde benutzen zu können, ist sowohl ein sogenanntes Wallet, als auch ein SET-Zertifikat notwendig. Beides erhält man von seinem Kreditkartenunternehmen, sofern dieses die SET Technologie unterstützt. Ein Wallet ist eine Software, welche der Kunde auf seinem Rechner installieren muß. Das Programm speichert sowohl einige kundenspezifische Daten, als auch die Kreditkarteninformationen verschlüsselt auf der Festplatte. Zusätzlich generiert es ein Schlüsselpaar, um später die Daten mit einem asymmetrischen Verschlüsselungsverfahren (RSA mit 1024 Bit) übertragen zu können.

Abb. 7 soll den Ablauf einer Bestellung unter Einsatz der SET Technologie verdeutlichen. In Anlehnung an [Merz99, S.178]:

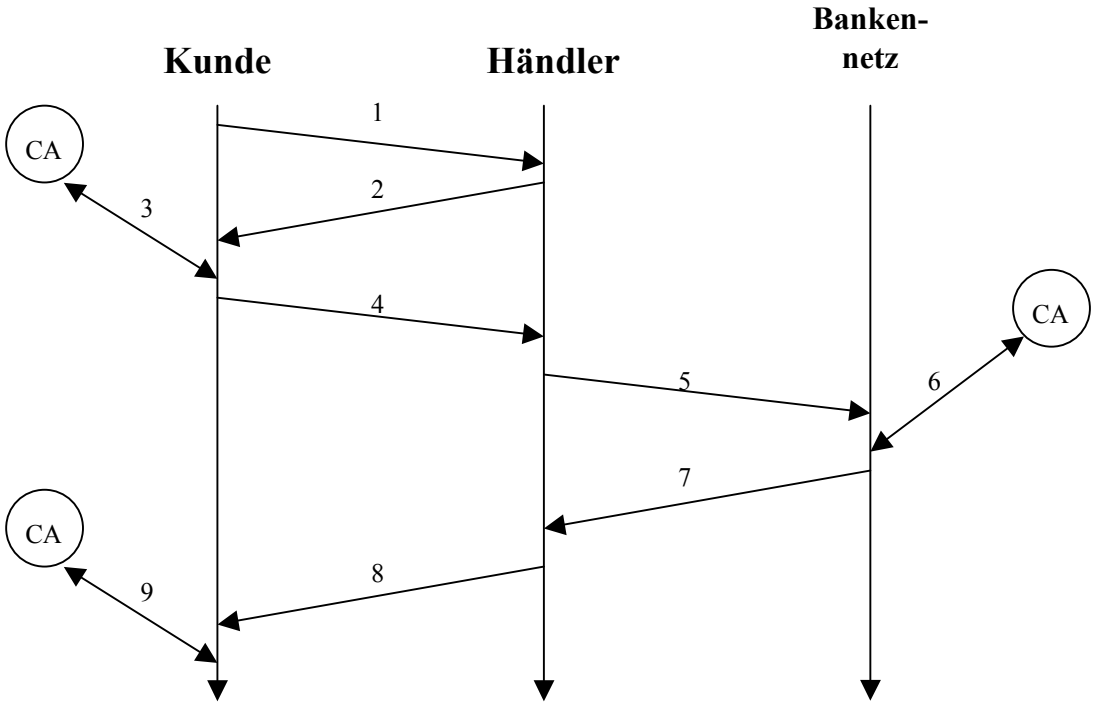

Abbildung 7: Funktionsweise von SET

Die Bestellung (Punkte 1 – 4)

Der Kunde eröffnet die vorgesehene Transaktion mit einer ersten Kontaktaufnahme zum Händler (1). Dieser sendet eine unterschriebene Antwort, sowie sein eigenes Zertifikat, als auch jenes der Händlerbank, zurück an den Kunden (2). Der Kunde überprüft die beiden Zertifikate bei einer Zertifizierungsstelle (Certification Authority – CA). Dies wird für den Anwender transparent durch das installierte Wallet übernommen (3). Nun macht der Kunde seine Bestellung und eine Zahlungsanweisung. Beides zusammen wird als sogenannte Dual Signature Nachricht an den Händler übermittelt. Die Bestellung selbst wird mit dem öffentlichen Schlüssel des Händlers, die Zahlungsanweisung mit dem der Händlerbank verschlüsselt. Somit ist der händlerseitige Betrug ausgeschlossen, da er die Kreditkartendaten, die in der Zahlungsanweisung vorhanden sind, nicht wieder entschlüsseln kann. Er kann lediglich die Bestelldaten lesen. Die Daten der Zahlungsanweisung können somit nur durch den privaten Schlüssel der Händlerbank wieder entschlüsselt werden. An die Dual Signature Nachricht wird auch noch das Zertifikat des Kunden mit angehängt (4).

Akzeptieren der Zahlungsanweisung (Punkte 5 – 9)

Der Händler verfügt nun über die Bestelldaten des Kunden, da er diesen Teil der Nachricht mit seinem privaten Schlüssel lesen konnte. Um den Betrug von der Seite des Kunden aus ausschließen zu können, übermittelt er den Rest der Nachricht, ergänzt mit seinem eigenen Zertifikat, an die Händlerbank (5). Diese überprüft beide Zertifikate bei einer Zertifizierungsstelle und stellt somit die Echtheit des Kunden und des Händlers sicher (6). Ebenfalls kann sie mit ihrem privaten Schlüssel die Zahlungsanweisung des Kunden entschlüsseln und eine entsprechende Anfrage über das bankeninterne Netz an das Kreditkartenunternehmen des Kunden stellen. Die Bestätigung der Zahlungsanweisung wird nun zurück an den Händler gesandt (7). Die Bestätigung des Bestellvorganges wird mit dem Zertifikat des Händlers verschlüsselt und an den Kunden übermittelt (8). Dieser braucht nun nur noch das Händlerzertifikat zu überprüfen (9), und die Transaktion ist abgeschlossen.

Die Hauptvorteile von SET liegen darin, daß sowohl der kunden-, als auch der händlerseitige Betrug ausgeschlossen werden. Durch die Vermeidung dieser beiden Gefahrenquellen ist auch zu erwarten, daß die kriminalitätsbedingten Transaktionskosten erheblich sinken werden. Ein weiterer Vorteil ist, daß SET theoretisch weltweit eingesetzt werden kann. Jedoch unterstützen bislang nur ein ca. 50 Händler die Technologie, auch deswegen, weil diese einen sogenannten Payment-Server einrichten müssen. Und auch auf der Kundenseite wird die Installation des Wallets und die Zertifizierung noch nicht so akzeptiert, als dies erwartet wurde.

[Merz99, Visa00, Kore00, Com100, Com200, Net100]

5.3 Elektronisches Geld

Als elektronisches Geld wird virtuelles Geld bezeichnet, welches dem Kunden auf seinem Rechner zur Verfügung steht. Durch Eigenschaften wie totale Anonymität, oder Stückelung des Geldes in Werteinheiten, ist dieses elektronische Geld den Charakteren von Münzen und Scheinen sehr ähnlich. Die wohl bekanntesten Verfahren sind zum einen CyberCoin der Cyber Cash GmbH und zum anderen eCash der Firma DigiCash. Wie weiter oben schon beschrieben hat die Cyber Cash GmbH alle Wallet basierten Verfahren – und somit auch CyberCoin - eingestellt [Cybe00]. Ein weiteres Verfahren ist noch MilliCent, auf das ich aber weiter unten bei den Billing Verfahren zu sprechen komme. Aus diesem Grund beschränke ich mich hier auf das eCash Protokoll.

Nachdem die Firma DigiCash im Sommer 1998 Konkurs anmelden mußte, wird eCash heute von unterschiedlichen Banken angeboten. Die Deutsche Bank betreibt z.B. einen Feldtest in DM. Das Protokoll unterstützt lediglich einen geschlossenen Währungsraum, *„d.h. weder zwischen zwei eCash-Währungsräumen, die an die gleiche reale Währung gekoppelt sind, noch zwischen unterschiedlichen Realwährungen sind eCash-Münzen automatisch konvertierbar“* [Merz99, S191].

Zunächst muß der Kunde bei der eCash unterstützenden Bank – im DM Währungsraum ist dies die Deutsche Bank 24 – ein kostenloses eCash Konto einrichten, auf welches er von seinem Girokonto einen gewissen Geldbetrag überweist. Zusätzlich muß er noch die eCash Wallet Software auf seinem Rechner installieren.

Generierung der Münzen

Der Kunde generiert seinen Münzvorrat selbst, – möglich sind alle Beträge, die sich aus 2er Potenzen (z.B. 2, 4 oder 128 Cent) bilden lassen - und die Wallet Software versieht diese Münzen mit einer eindeutigen Seriennummer. Sie werden nun mit dem privaten Schlüssel des Kunden signiert und an den Bankserver weitergeleitet. Dieser kann mit dem zugehörigen, bekannten öffentlichen Schlüssel den Kunden eindeutig identifizieren. Die Seriennummer wird jedoch anders verschlüsselt, so daß der Bankserver diese nicht einlesen kann. Die Bank signiert diese Münze und kann somit bei späterem Einlösen ihre Echtheit bestätigen. Das signierte Geldstück wird an den Kunden zurückgesandt. Die Bank weiß nun lediglich, daß der Kunde ein Münze abgehoben hat und belastet sein eCash Konto mit dem entsprechenden Betrag. Sie weiß aber nicht, welche Münze dies war. Nachdem der Kunde die Münze wieder zurückerhalten hat, transformiert er sie wieder in seine ursprüngliche Form, so daß die Seriennummer sichtbar ist.

Der Bezahlvorgang

Abb. 8 verdeutlicht den Ablauf einer Bestellung mit eCash. In Anlehnung an [Merz99, S.193]:

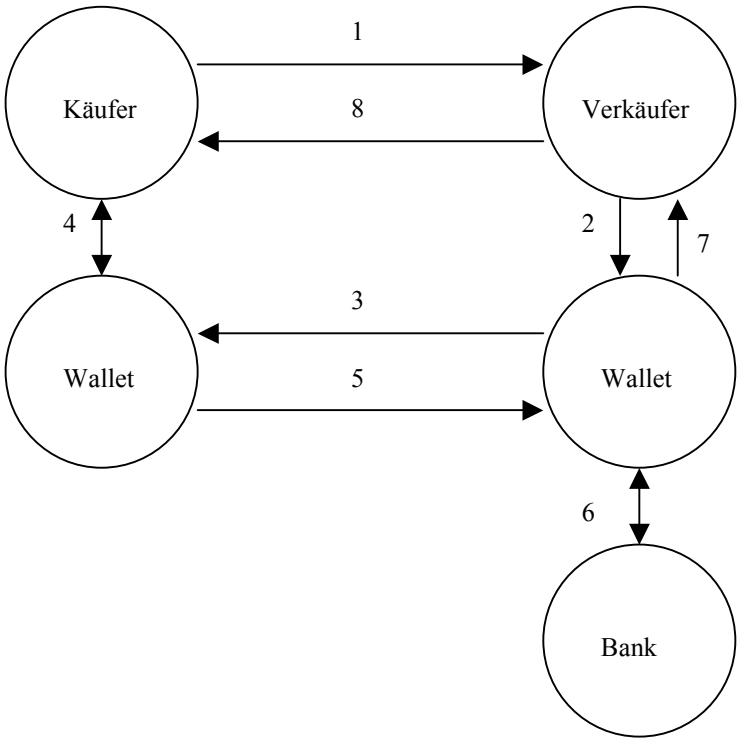

Abbildung 8: Ablauf einer Bestellung bei eCash

Der Käufer bestellt eine Ware oder Dienstleistung beim Verkäufer und wählt als Zahlungsform die Option eCash (1). Nun schaltet sich das Wallet des Händlers (2) in die Transaktion mit ein. Es kommuniziert mit dem des Käufers und fordert dieses zur Zahlung des Rechnungsbetrages auf (3). Das Wallet des Käufers verlangt von diesem eine Bestätigung für den Kaufvorgang und die genannte Höhe des Betrages (4). Sobald der Käufer den Angaben zugestimmt hat, übermittelt das Wallet die elektronischen Münzen zum Wallet des Verkäufers (5). Dieses wiederum läßt sich die Echtheit des virtuellen Geldes von der eCash Bank bestätigen (6). Die Bank überprüft dabei, ob die Signatur der Münze von ihr stammt und ob mit der Münze dieser Seriennummer nicht schon einmal bezahlt wurde. Auf diese Problematik werde ich allerdings weiter unten noch eingehen. Nachdem die Bank die Echtheit bestätigt hat, teilt das Wallet dies dem Verkäufer mit, und er kann die Ware ausliefern (7 + 8).

Double Spending

Die totale Anonymität des Kunden ist wohl der größte Vorteil dieses Verfahrens. Aber dieser bringt auch ein grundsätzliches Problem mit sich. Das Problem bei diesen münzbasierten Verfahren ist, daß das elektronische Geld eigentlich Daten sind, die beliebig oft kopiert werden können. Aus sicherungstechnischen Gründen sollte dies auch möglich sein, da z.B. nach einem Festplattenabsturz das ganze Geld verloren sein kann. Deshalb sollten z.B. Sicherungskopien des Geldes auf Disketten vorliegen. Bei eCash wird auch der doppelte Einsatz einer Münze, das sogenannte Double Spending, ausgeschlossen. Mit dem Algorithmus von eCash kann sogar festgestellt werden, wer – Kunde oder Händler - eine Münze fälschlicherweise mißbraucht hat.

Bevor der Kunde dem Händler eine Münze übermittelt, wird noch eine zusätzliche Information mit angehängt. Es wird ein String generiert, der den Kunden eindeutig identifizieren kann (z.B. Personalausweisnummer). Dieser String wird nun n mal kopiert und jeweils in einen linken und einen rechten Teilstring unterteilt. Mit nur einem Teilstring kann nicht mehr auf die ursprüngliche Information geschlossen werden. Jeder der Teilstrings der Stringpaare wird nun getrennt verschlüsselt, so daß 2n Schlüssel entstehen.

Wenn der Kunde nun dem Händler eine Münze übermittelt, übermittelt er z.B. die Schlüssel aller linken Teilstrings mit. Somit kann jeweils nur ein Teil der eigentlichen Information entschlüsselt werden. Es kann damit allein auch noch nicht auf die Identität des Kunden geschlossen werden.

Die Bank überprüft nun die Signatur der Münze, ob sie überhaupt von ihr stammt, und die Seriennummer. Taucht die Nummer zum erstenmal auf, ist alles in Ordnung, und der Händler bekommt die Echtheit der Münze bestätigt. Trifft dies jedoch nicht zu, muß die Münze doppelt ausgegeben worden sein, denn ansonsten könnte die Bank ja noch nicht über die Seriennummer verfügen. Es gibt nun 2 Möglichkeiten. Entweder der Händler hat die Münze doppelt eingereicht, oder der Kunde.

Im ersten Fall wären die Schlüssel der Stringpaare beider Einreichungen genau gleich verteilt. Es ist davon auszugehen, daß der Händler betrogen hat, weil es als extrem unwahrscheinlich gilt, daß der Kunde zweimal dieselben Schlüssel beim Double Spending herausgeben würde.

Im zweiten Fall sind die Schlüssel beider Einreichungen nicht identisch. Hier kann der Händler nicht betrogen haben, da er, wenn der Kunde die Münze nur einmalig eingesetzt hat, niemals über beide Schlüssel eines Stringpaares verfügen könnte. Nun kann auch der Kunde eindeutig identifiziert werden, weil es ja jetzt mindestens ein Stringpaar gibt, von dem beide Teile entschlüsselt werden können.

ECash eignet sich auch hervorragend für Transaktionen im Micropayment Bereich, da keine speziellen Gebühren, nur die Kontoführungsgebühren anfallen. Als Nachteil wäre jedoch noch zu sehen, daß sich das elektronische Portemonnaie mit maximal 400 DM auffüllen läßt und somit für größere Zahlungen nicht in Frage kommt.

[Merz99, Eci200, DeBa00, Net100]

5.4 Billing Verfahren

5.4.1 Allgemeines

Die Billing Verfahren wurden von den verschiedenen Firmen speziell für Transaktionen im Micropayment Bereich entwickelt. Das Verfahren ist eigentlich nichts neues und von den Telekommunikationsprovidern seit jeher bekannt: Meine Telefoneinheiten werden nach jedem Gespräch auf meinem Kundenkonto mitgezählt, und einmal am Ende des Monats in Rechnung gestellt. So entsteht ein minimaler Transaktionsaufwand und ist damit ein *„perfektes System zur Abrechnung von Microtransaktionen“*. [Merz99, S.199]

Es gibt eine Vielzahl unterschiedlicher Billing Systeme, von denen ich hier nur die wichtigsten näher erläutern werde.

5.4.2 MilliCent

MilliCent wurde von der Firma Digital speziell für Micropayment Transaktionen entwickelt. Es befindet sich derzeit nur auf dem japanischen Markt im Einsatz, soll aber laut [Mill00] in kürze auch auf dem nordamerikanischen und europäischen Markt zur Verfügung stehen.

Das Verfahren ist denkbar einfach. Der Kunde kauft sich bei MilliCent (Broker) für einen bestimmten Betrag Wertmarken, sogenannte Scrip. Mit diesen Scrip kann er bei den Händlern, die dieses Verfahren unterstützen, auch im Bereich der Kleinstbeträge – MilliCent hat in einem Rechenmodell nachgewiesen, daß auch bei Beträgen um die 0,5 Cent, noch ein wirtschaftlicher Betrieb möglich ist - einkaufen. Hat sich beim Händler eine bestimmte Menge an Scrip angesammelt, kann er diese bei MilliCent wieder in Euro umtauschen. Somit werden die hohen Transaktionskosten einer Zahlung umgangen, indem man mehrere Geldtransfers zusammenfaßt. Der Scrip selbst ist durch kryptographische Maßnahmen gesichert, so daß er nicht doppelt ausgegeben, gefälscht oder gestohlen werden kann. Da er nur eine Verechnungseinheit darstellt, braucht MilliCent auch nicht den Druck der Notenbank, wie z.B. bei eCash, zu fürchten.

5.4.3 Net900

Net900 ist von dem Unternehmen In Media Res und ist als Ablösung für das bekannte T-Online-Billing, welches wegen den hohen Stornierungskosten 1999 eingestellt wurde, gedacht. Hierbei erfolgt die Abrechnung der Transaktionen über die Telefonrechnung. Der Kunde muß hierfür einmalig die net900 Software auf seinem Rechner installieren. Betritt er nun einen kostenpflichtigen Bereich eines Angebotes, wird nach Bestätigung die aktuelle Modemverbindung unterbrochen und mit einer 0190er Nummer verbunden. Anschließend wird die alte Verbindung wieder aufgebaut. Hier zeigt sich ein Vorteil für ISDN Benutzer auf, bei denen die bestehende Verbindung nicht unterbrochen werden muß, weil mehrere parallel aufgebaut werden können. Laut [Inmr00] soll net900 jetzt auch im LAN, oder via DSL möglich sein. Die Gebührenabrechnug funktioniert auch bei sogenannten Call-by-Call Providern.

Es gibt 2 unterschiedliche Tarifvarianten für net900. Beim sogenannten Pay-per-Minute, bleibt die 0190er Verbindung eine bestimmt Zeit lang geöffnet – z.B. solange ein bestimmtes Web-Angebot in Anspruch genommen wird – und rechnet diesen ab. Beim Pay-per-Click, wird nur ganz kurzfristig die Verbindung zur 0190er Nummer hergestellt, und es wird die vorher vereinbarte Gebühr sofort berechnet.

Die Kosten des Händlers belaufen sich, ähnlich zu dem reinen 0190er Nummern Verfahren, auf die Gebühren der Deutschen Telekom, die ca. 31-63% des Umsatzes kassieren. Darüber hinaus fallen für die Einrichtung einmalig ca. 250 Euro an, sowie weitere 50 Euro pro Monat.

[Merz99, Robb00]

5.4.4 Variable Internet Billing System - Vibsy

KDD Conos hat ein weiteres Verfahren, das ähnlich wie Net900 arbeitet, das Variable Internet Billing System, kurz Vibsy, entwickelt. Hierbei wird eine Punkt-zu-Punkt Verbindung zwischen händler- und kunden PC hergestellt. Somit könnte mit einer speziellen Kommunikationssoftware der Händler Kontakt zum Kunden aufnehmen und dies damit eventuell zur Beratung, oder Beantwortung bestimmter Fragen nutzen.

[Com300]

5.5 Paybox

Paybox ist eine der neueren Methoden, im Internet zu bezahlen. Das Verfahren wurde im Mai 2000 von der paybox.net AG, die eng mit der Deutschen Bank AG zusammenarbeitet, vorgestellt. [Gatz00] Bei diesem Verfahren muß lediglich die Mobiltelefonnummer, und sogar diese kann durch eine Aliasnummer [Ente00] ersetzt werden, des Käufers übertragen werden. Sowohl die Autorisierung als auch die Identifizierung erfolgt über das *„in hohem Maße für Sicherheit“* [Eci100] bürgende GSM Handynetz. Paybox nutzt somit den derzeitigen Handy Boom in Deutschland und macht quasi über Nacht rund 25 Millionen Handys zu einsetzbaren Zahlungsmitteln im Internet, und nicht nur da. Auch im Mobile Commerce, auf den ich hier allerdings nicht näher eingehen werde, kann paybox eingesetzt werden. Und die Zahl der Handynutzer ist stark ansteigend, wie Abb. 9 zeigt. [Pay100]

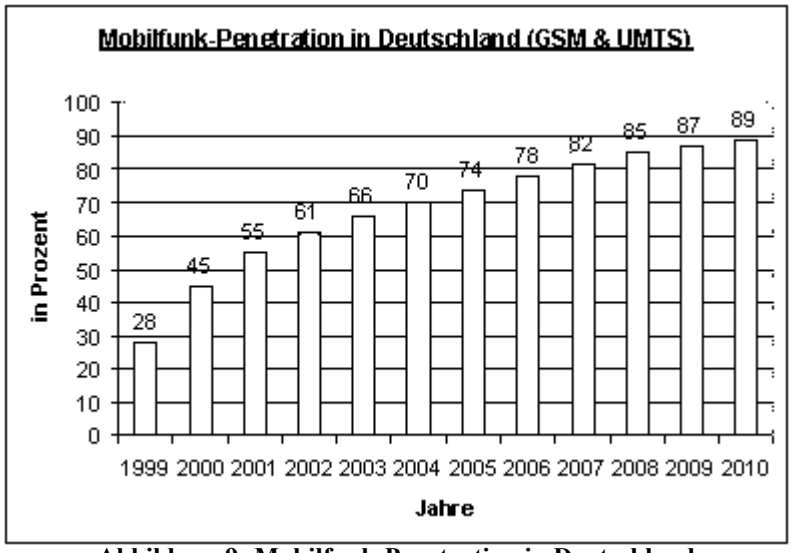

Abbildung 9: Mobilfunk-Penetration in Deutschland

Quelle: [Pay100]

Der Privatkunde, der paybox als Zahlungsmethode einsetzen will, muß lediglich über ein Handy und ein Girokonto verfügen. Zusätzlich muß er sich bei paybox registrieren lassen. Die Registrierung kann sowohl online bei der Paybox.net AG, als auch bei einigen Handyvertragsanbietern durchgeführt werden. Die Kosten für den Kunden belaufen sich jährlich auf 5 Euro. Nach seiner Registrierung erhält er seine persönliche paybox-PIN. Auch der Händler muß sich bei paybox registrieren lassen und eine Software installieren, deren Lizenzgebühren sich auf ca. 250 Euro

belaufen. Pro Transaktion werden dann Gebühren in Höhe von 3% des Zahlungsbetrages fällig [Pay100].

Der Zahlungsvorgang ist denkbar einfach. Nachdem sich der Kunde eine bestimmte Ware ausgesucht hat, entscheidet er sich mit dem paybox-Button (siehe in Abb. 10) für die Bezahlung per Handy. Er wird nun aufgefordert, seine Mobiltelefonnummer, oder alternativ eine ihm bei der Registrierung zugeteilte Alias-Nummer, anzugeben.

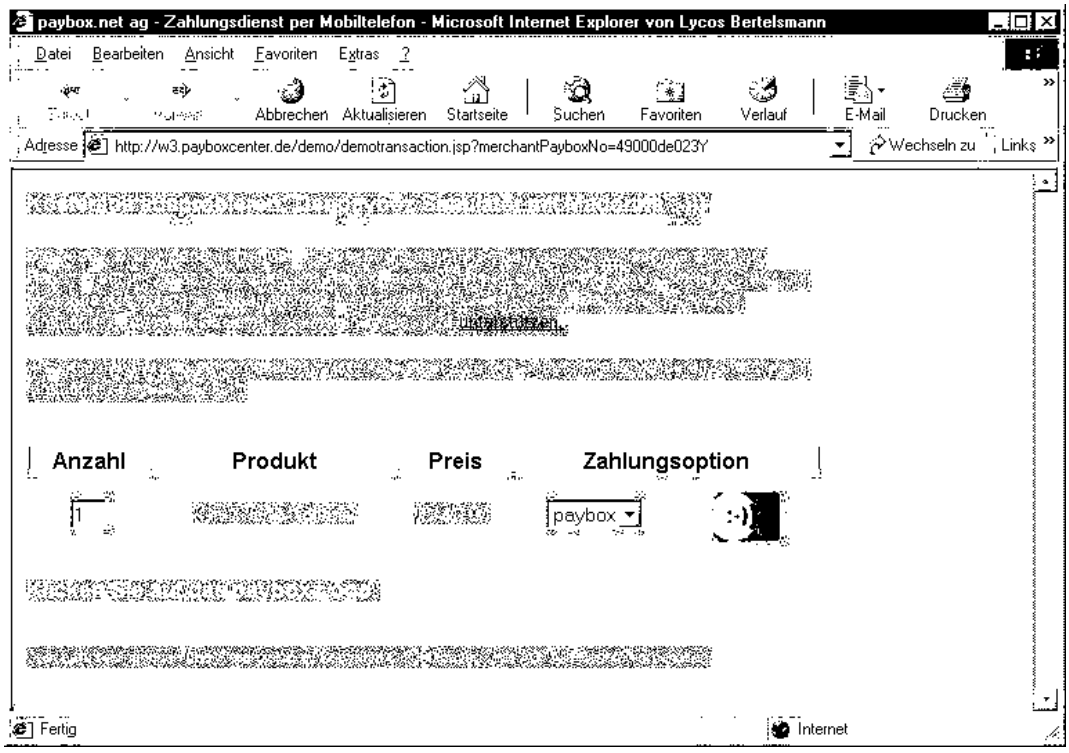

Abbildung 10: Beispiel für Paybox

Quelle: [Pay300]

Diese Nummer wird über eine sichere Datenleitung an die paybox.net AG weitergeleitet, die kurz darauf auf dem Handy des Kunden anruft und ihm den zu zahlenden Betrag und den Zahlungsempfänger nennt. Mit seiner persönlichen paybox-PIN bestätigt der Kunde die Richtigkeit der gemachten Angaben und erlaubt damit paybox.net AG den Betrag an den Händler zu übergeben. Laut [Gatz00] soll der gesamte Vorgang nicht mehr als 30 Sekunden in Anspruch nehmen. Allerdings gibt es ein Tageslimit für den paybox Kunden, so daß ein Tagestransaktionsvolumen von 300 Euro bis 1.000 Euro nicht überschritten

werden kann. Dieses Limit paßt sich aber, ähnlich zur Kreditkarte, dem Kundenverhalten an. [Ente00]

Die positive Entwicklung des Verfahrens wird auch dadurch bestätigt, daß das Ziel der paybox.net AG, bis zum Jahresende 2000 300 Händler zu gewinnen, die das Zahlungssystem unterstützen, bei weitem übertroffen wurde. [Eci100] Bereits jetzt gibt es mehr als 500 Online Shops, die dieses System als Zahlungsvariante anbieten. [Pay200]

6 Bewertung

Am Schluß meiner Arbeit möchte ich noch eine Gegenüberstellung und Bewertung der einzelnen Zahlungssysteme vornehmen:

Zahlungs-methode	Funktionsweise	Vorteile	Nachteile
0190er Nummern	Der Kunde ruft eine kostenpflichtige Nummer an und muß die Verbindung eine bestimmte Zeit lang aufrecht erhalten. Nach Ablauf dieser Zeit wird ihm ein Schlüssel mitgeteilt, der ihn berechtigt, ein Angebot in Anspruch zu nehmen.	Das Verfahren ist sehr einfach handzuhaben und es ist keine Installation von Zusatzsoftware erforderlich. Es kann eine sehr genaue Abrechnung erfolgen.	Der Hauptnachteil sind die horrenden Gebühren, welche die Telekom derzeit noch verlangt. Sie belaufen sich auf ca. 50% des Umsatzes. Auch aus diesem Grund kann dieses Verfahren nur im Micropayment Bereich eingesetzt werden.

Zahlungs-methode	Funktionsweise	Vorteile	Nachteile
Kreditkarte mit SSL	Bei der Übertragung mit dem SSL Protokoll werden die Daten durch Sitzungsschlüssel effektiv verschlüsselt.	Das Verfahren ist relativ rasch einsetzbar und auch international nutzbar. Es ist sehr weit verbreitet und je nach zugrundeliegendem Verschlüsselungsverfahren sind Angriffe Dritter so gut wie ausgeschlossen.	Bei diesem Verfahren werden nur die Daten auf dem Weg vom Kunden zum Händler verschlüsselt. Wie der Händler weiterhin mit den Kreditkartendaten umgeht kann nicht gesagt werden. Sowohl der händler-, als auch der kundenseitige Betrug kann nicht ausgeschlossen werden. Aufgrund der Transaktionskosten, sind Kreditkartenzahlungen nicht im Micropayment Bereich einsetzbar.
Kreditkarte mit SET	Bei der Datenverschlüsselung mit dem SET Protokoll müssen Händler und Kunden zertifiziert sein. Die Kreditkartendaten werden verschlüsselt gesendet und der Händler kann diese nicht einsehen. Nur seine Bank ist über das Bankennetz dazu in der Lage. Auf beiden Seiten ist ein SET-Wallet erforderlich.	Das System ist weltweit einsetzbar. Bei diesem Verfahren ist sowohl der händler-, als auch der kundenseitige Betrug ausgeschlossen. Das Verfahren ist sehr einfach handzuhaben, da die Wallet Software für den Anwender transparent arbeitet.	SET wird bislang nur von ca. 50 Händlern unterstützt. Auch die Installation der Software und die Registrierung bei einer Zertifizierungsstelle sind Hemmschwellen für den Kunden. Aufgrund der Transaktionskosten, sind Kreditkartenzahlungen nicht im Micropayment Bereich einsetzbar.

Zahlungs-methode	Funktionsweise	Vorteile	Nachteile
eCash	Der Kunde legt ein eCash Konto bei der Deutschen Bank 24 an. Auf seinem Rechner hat er eine Wallet Software installiert, in das er von seinem Konto elektronisches Geld transferieren kann. Mit diesen Geldeinheiten kann bei Händlern wie mit "echtem" Geld bezahlt werden.	eCash ist hervorragend für Transaktionen im Micropayment Bereich geeignet, da keine Gebühren anfallen. Es ist auch kein Mißbrauch der virtuellen Geldeinheiten möglich. Der größte Vorteil jedoch ist, daß dieses Verfahren dem Kunden absolute Anonymität gewährleistet.	Sowohl der Kunde als auch der Händler müssen sich ein Wallet installieren, was oft eine Hemmschwelle bedeutet. Das elektronische Portemonnaie läßt sich nur bis 400 DM auffüllen. eCash funktioniert auch nur in einem geschlossenen Währungsraum.
MilliCent	MilliCent wurde von der Firma Digital entwickelt. Der Kunde kauft sich bei MilliCent für einen bestimmten Betrag eine virtuelle Währung namens Scrip. Mit diesen Scrip kann er bei Händlern im Micropayment Bereich einkaufen. Dieser tauscht sie, nachdem sich ein gewisser Betrag angesammelt hat, um Transaktionskosten zu sparen, bei MilliCent wieder in Euro um.	MilliCent ist sehr einfach handzuhaben und arbeitet auch noch im Bereich der Kleinstbeträge wirtschaftlich effektiv. Um Transaktionskosten zu sparen, kann der Händler seine Scrips, sobald sich ein bestimmter Betrag angesammelt hat, wieder in Euro umtauschen.	Der Scrip ist zwar kryptographisch gesichert, so daß er nicht doppelt ausgegeben werden kann, aber nur soviel, daß er sich lediglich für den Micropayment Bereich eignet. Der Kunde muß schon eine Zahlung an MilliCent tätigen, um umzutauschen, bevor er überhaupt etwas gekauft hat. MilliCent befindet sich derzeit nur auf dem japanischen Markt im Einsatz.

Zahlungs-methode	Funktionsweise	Vorteile	Nachteile
Net900	Der Kunde installiert eine net900 Software auf seinem Rechner. Sobald der Kunde eine Dienstleistung, oder eine Ware bezahlen muß, baut das Modem eine kostenpflichtige Verbindung zum Anbieter auf. Die Abrechnung erfolgt dann einmal monatlich mit der Telefonrechnung.	Net900 ist sehr einfach handzuhaben, da der Verbindungsaufbau für den Anwender transparent abläuft. Durch die Abrechnung über die Telefonrechnung fallen für den Kunden geringe Transaktionskosten an und ist deshalb für den Micropayment Bereich geeignet.	Durch die benötigte Installation der net900 Software, ist wiederum eine Hemmschwelle auf Kundenseite vorhanden. Das Verfahren ist nur für Micropayment Transaktionen sinnvoll, da sich die Gebühren, wie bei den 0190er Nummern, zwischen 30 und 60% des Umsatzes bewegen. Zusätzlich fallen noch einmalige Einrichtungsgebühren von 250 Euro an, und laufende gebühren mit 50 Euro pro Monat.
Paybox	Paybox ist ein Verfahren, welches das Bezahlen mit dem Handy ermöglicht. Der Kunde muß sich bei Paybox registrieren lassen. Nachdem sich der Kunde für das Bezahlen mit Paybox entschieden hat, wird er auf dem Handy angerufen und dazu aufgefordert, den Betrag zu bestätigen und eine persönliche PIN einzugeben. Er begleicht den Betrag dann mit seiner monatlichen Handyrechnung.	Es ist keine zusätzlich Software erforderlich. Der Kunde benötigt nur sein Handy. Und auch die jährliche Gebühr von 5 Euro ist erschwinglich. Das Handynetz gilt gegenüber Angriffen Dritter als sehr sicher.	Anonymität ist nicht voll gewährleistet. Derzeit unterstützen nur ca. 500 Händler das System. Es ist ein maximales Transaktionsvolumen von bisher 1.000 Euro vorgesehen. Aufgrund der Gebühren, die für den Händler anfallen, ist Paybox für den Micropayment Bereich nicht geeignet. Paybox ist bisher auf den deutschen Markt beschränkt.

QUELLENVERZEICHNIS

[Bäch00] Prof. Dr. M. Bächle: Im Rahmen seines WI Net Vortrags an der Berufsakademie Ravensburg im November 2000.

[Com100] gfh: „*Uneinige Banken blockieren Internet-Zahlungssysteme*“, Computerwoche Nr. 02 (2000) vom 14.01.2000, S. 17-20

[Com200] F. Niemann: *„Web-Bezahlsysteme treten gegen Papierrechnung an“*, Computerwoche Nr. 16 (2000) vom 21.04.2000, S. 25-26

[Com300] fn: *„Surfer zahlen über die Telefonrechnung – Bezahlsystem für das Web“*, Computerwoche Nr. 47 (2000) vom 24.11.2000, S.45

[Cybe00] Cyber Cash GmbH: *„Aktuelle Informationen“.*
Online im Internet: URL:
http://www.cybercash.de/news/index.html
(Download: 18.12.2000)

[DeBa00] Deutsche Bank: *„Zahlung mit eCash“.* Online im Internet: URL: http://public.deutsche-bank.de/deuba/ui/ec/nav_ec.nsf/Frameset/JWID-45WJT7?OpenDocument
(Download: 25.12.2000)

[Ding97] G. Dingler: Vorlesungsskript: *„Informationssicherheit & Computerkriminalität“*, Berufsakademie Ravensburg 1997

[Eci100] Electronic Commerce InfoNet: *„paybox – Wunsch und Wirklichkeit“,* 14.09.2000. Online im Internet: URL:
http://www.ecin.de/zahlungssysteme/allgemein/paybox2.html
(Download: 18.12.2000)

[Eci200] Electronic Commerce InfoNet: *„Ecash in der Praxis“*.
Online im Internet: URL:
http://www.ecin.de/zahlungssysteme/geld/ecash.html
(Download: 22.12.2000)

[Eci300] Electronic Commerce InfoNet: *paybox – „Nutzerzahlen – Wie hoch ist die Reichweite des Internets“,* 10.02.2000. Online im Internet: URL: http://www.ecin.de/marktbarometer/daten/nutzer.html (Download: 30.11.2000)

[Eci400] Electronic Commerce InfoNet: *„paybox – Unternehmen im Internet – Bezahlen von Leistungen über das WWW“*. Online im Internet: URL: http://www.ecin.de/marktbarometer/daten/2-unternehmen-archiv.html (Download: 22.12.2000)

[Ente00] M. Entenmann: *„debitel und paybox – bezahlen Sie mit Ihrem Handy“,* AIRTime – Das Magazin für debitel Kunden Jahrgang 7 Heft 4 Winter 2000 S. 6 - 8

[Gatz00] M. Gatzke: *„paybox - Revolution im Zahlungsverkehr“,* Electronic Commerce InfoNet, 18.05.2000. Online im Internet: URL: http://www.ecin.de/zahlungssysteme/allgemein/paybox.html (Download: 18.12.2000)

[Inmr00] In-Medias-Res: *„NET900 jetzt auch im LAN und via DSL“*. Online im Internet: URL: http://www.in-medias-res.de (Download: 24.12.2000)

[KöBe98] T. Köhler, R.B. Best: *„Electronic Commerce – Konzipierung, Realisierung und Nutzung in Unternehmen“*, Addison Wesley 1998

[Kore00] T. Korell: *„SET – Sicheres Bezahlen mit der Kreditkarte im Internet“,* Electronic Commerce InfoNet. Online im Internet: URL: http://www.ecin.de/zahlungssysteme/kreditset/set1.html (Download: 22.12.2000)

[Merz99] M. Merz: *„Electronic Commerce – Marktmodelle, Anwendungen und Technologien“*, dpunkt: München 1999

[Mill00] Digital: *„MilliCent Frequently Asked Questions´s“*. Online im Internet: URL: http://www.millicent.com/faq/index.html (Download: 24.12.2000)

[Net100] S. Buckl: *„Gesucht: Die passende Geldbörse fürs Internet“*, Net-Business vom 07.08.2000, S.17

[Pay100] paybox.net AG: *„Daten und Fakten über e-Commerce in Deutschland“, Online im Internet: URL*: http://www.paybox.net/index.php3
(Download: 19.12.2000)

[Pay200] paybox.net AG: *„Zahlungsdienst per Handy“*.
Online im Internet: URL:
http://www.paybox.de
(Download: 19.12.2000)

[Pay300] paybox.net AG: *„Zahlungsdienst per Mobiltelefon“.*
Online im Internet: URL:
http://w3.payboxcenter.de/demo/demotransaction.jsp?merchantPayboxNo=49000de023Y
(Download: 19.12.2000)

[Robb00] M. Robben: *„Micropayment: Wer den Pfennig nicht ehrt...“*, Electronic Commerce InfoNet, 24.08.2000. Online im Internet: URL:
http://www.ecin.de/zahlungssysteme/micropayment/index.html
(Download: 24.12.2000)

[Visa00] VISA: *„SET (Secure Electronic Transaction)“.*
Online im Internet: URL:
http://www.visa.de/technologie/technologie_set_funktion.htm
(Download: 22.12.2000)

Ehrenwörtliche Erklärung

Ich versichere hiermit, dass ich meine Studienarbeit mit dem Thema

Analyse unterschiedlicher Zahlungssysteme im Internet

selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

.....

Ort

....

Datum Unterschrift