

Universität Trier

Fachbereich IV

Electronic Payment Systems (EPS) im Web

Seminararbeit

im Fach Wirtschaftsinformatik

Sommersemester 2001

Inhaltsverzeichnis

	Seite
Abbildungsverzeichnis.....	II
Abkürzungsverzeichnis	III
1. New Economy, New Money?	1
2. Anforderung an elektronische Zahlungssysteme	2
2.1 Anforderung an (elektronische) Zahlungsmittel	2
2.2 Anforderung an elektronische Zahlungsmethoden	3
3. Klassifizierung elektronischer Zahlungssysteme	5
3.1 Klassifizierung nach Zahlungsbetrag	5
3.2 Klassifizierung nach Zahlungsmodus	6
3.3 Zusammenfassende Bemerkungen.....	7
4. Funktionsweise ausgewählter Beispiele	7
4.1 eCash.....	7
4.2 Secure Electronic Transaction (SET).....	9
4.3 Paybox.....	12
5. Probleme und Grenzen	15
6. Zusammenfassung und Ausblick.....	16
Literaturverzeichnis	IV

Abbildungsverzeichnis

	Seite
Abb. 1: Nachrichtenfluss bei Bezahlung mittels eCash.....	8
Abb. 2: Nachrichtenfluss bei Bezahlung mittels SET.....	11
Abb. 3: Nachrichtenfluss bei Bezahlung mittels Paybox.....	13

Abkürzungsverzeichnis

EPS..... Electronic-Payment-System

GfK..... Gesellschaft für Konsumforschung

PIN Personal Identification Number

PKI Public Key Infrastructure

SET..... Secure Electronic Transaction

SIM..... Subscriber Identity Module

SMS..... Short Message Service

TAN Transaction Number

1 New Economy, New Money?

Die rasante Entwicklung der elektronischen Netze, darunter vor allem die des Internet, ist nicht zu übersehen. Das Internet ist derzeit mit mehr als 260¹ Millionen angeschlossenen Computern das größte Rechnernetzwerk der Welt, mit ständig steigenden Anschlusszahlen. So ist es nicht verwunderlich, dass das Internet nicht ausschließlich als Informations- und Werbeträger genutzt wird, sondern dass in zunehmendem Maße auch Online-Shopping-Angebote frequentiert werden. Einer rasanten Entwicklung des Online-Shopping steht jedoch als Haupthindernis eine mangelnde Akzeptanz, bzw. ein „Mangel an adäquaten elektronischen Zahlungssystemen“² im Wege. Dies kann man auch in einer Studie der GfK erkennen, welche zeigt, dass 90% der User Online-Einkäufe vor allem aus Sicherheitsbedenken bezüglich der Zahlungsdaten vorzeitig abbrechen.³ Andere Untersuchungen zeigen, dass das beliebteste Zahlungsmittel bei Online-Käufern das Bezahlen per Rechnung, gefolgt von Lastschriftverfahren und Nachnahme, ist.⁴ Dieser Medienbruch zwischen Online einkaufen und Offline bezahlen führt zu erhöhten Transaktionskosten und ist daher aus betriebswirtschaftlicher Sicht nicht sinnvoll. Um die Entwicklung des eCommerce nicht zu bremsen und um das wirtschaftliche Potential auszunutzen, ist es daher notwendig, sichere elektronische Zahlungssysteme zu entwickeln und einzuführen.⁵

Ziel der vorliegenden Seminararbeit ist es, einen Überblick über elektronische Zahlungssysteme zu geben. Dazu werden zunächst die Anforderungen an elektronische Zahlungssysteme diskutiert und versucht, eine Klassifizierung der Vielzahl an Zahlungssystemen vorzunehmen. Des weiteren werden die Funktionsweisen ausgewählter Beispiele offengelegt und die Probleme und Grenzen der jeweiligen Systeme aufgezeigt.

1 Vgl. Computer Industry Almanac Inc.: Internet Users, Online im Internet: <http://www.c-i-a.com/199911iu.htm>, 4.11.1999.

2 Pernul, Günther; Röhm, Alexander W.: Neuer Markt, Neues Geld, in: Wirtschaftsinformatik, Ausgabe 4/1997, S. 345.

3 Vgl. Niemann, Frank: Anbieter von Web-Bezahlsystemen entdecken den Konsumenten, in: Computerwoche, Young Professional, Ausgabe 2/2001, S. 54.

4 Vgl. Institut für Wirtschaftspolitik und Wirtschaftsforschung: Umfrage zu Zahlungsmitteln im Internet, Online im Internet: <http://www.iww.uni-karlsruhe.de/IZV4/auswertung/showalle.html>, 20.3.2001.

5 Vgl. Schwickert, Axel C.: Electronic-Payment-Systeme im Internet, in: IM Informationsmanagement, Ausgabe 4/1996, S. 24.

Volkswirtschaftliche Fragen, wie z.B. das Emittieren von elektronischem Geld, und rechtliche Fragen, die bei Abschluss eines Kaufvertrages zwischen Händler und Käufer auftreten, sind ein gesondertes Thema und werden daher im Rahmen dieser Seminararbeit nur am Rande angesprochen.

2 Anforderung an elektronische Zahlungssysteme

Anforderungen an elektronische Zahlungssysteme werden in der Literatur häufig differenziert betrachtet. So sprechen einige Autoren von allgemeinen Anforderungen und Sicherheitsanforderungen⁶, andere Autoren unterscheiden zwischen Anforderungen an das Zahlungsmittel und Anforderungen an die Zahlungsmethode.⁷ Im weiteren wird die Unterscheidung zwischen Anforderungen an Zahlungsmittel und Anforderungen an die Zahlungsmethode zu Grunde gelegt, wobei anzumerken ist, dass die Grenzen zwischen Zahlungsmittel und Zahlungsmethode, wie auch zwischen Allgemein- und Sicherheitsanforderungen, häufig verwischen und eine Zuordnung zu beiden Kategorien möglich wäre.

2.1 Anforderung an (elektronische) Zahlungsmittel

Anforderungen an elektronische Zahlungsmittel entsprechen weitestgehend den Anforderungen an reales Geld.⁸ Eine erste Anforderung an elektronische Zahlungsmittel ist die Erfüllung einer Tauschmittelfunktion. Voraussetzung hierfür ist eine gewisse Akzeptanz sowohl bei Kunden, als auch bei Shop-Anbietern, aber auch Knappheit des vorliegenden Zahlungsmittels. Eine weitere Anforderung stellt die Wertaufbewahrungsfunktion dar.⁹ Elektronisches Geld muss problemlos gespeichert werden können und auch nach einer längeren Zeitperiode seinen Wert behalten. Außerdem muss elektronisches Geld unkompliziert in nationale Währungen konvertiert und zwischen verschiedenen Personen übertragen werden können - Interpersonelle Übertragbarkeit - ebenso muss es über die Ländergrenzen eines Landes hinaus

6 Vgl. Rothhaas, Frank: Fundamentals of Electronic Business, Online im Internet: http://www.bwl.uni-mannheim.de/Niedereichholz/Fundamentals_of_E-Business_II.pdf, 16.10.2000.

7 Vgl. Schwickert, Axel C.: Electronic-Payment-Systeme im Internet, a. a. O., S. 25 f.

8 Vgl. Schwickert, Axel C.: Electronic-Payment-Systeme im Internet, a. a. O., S. 25.

9 Vgl. Merz, Michael: Elektronische Märkte im Internet, Bonn et al.: International Thomson Publishing 1996, S. 67.

akzeptiert werden.¹⁰ Die Forderung nach Konvertibilität stellt eine logische Konsequenz des globalen Rechnernetzwerkes Internet dar. Weiterhin kann die Rechenmittelfunktion des Geldes zu den Anforderungen an elektronische Zahlungsmittel gezählt werden. Das Zahlungsmittel selbst unterliegt Sicherheitsanforderungen, es muss sicher gegenüber Fälschungen, Mehrfachverwendung, Manipulation des Wertes, Diebstahl und Verlust sein. Anonymität, welche verhindern soll, dass Kundenprofile angelegt werden können, stellt eine letzte Anforderung an elektronische Zahlungsmittel dar.¹¹

2.2 Anforderung an elektronische Zahlungsmethoden

Unabhängig von der methodischen Umsetzung eines Zahlungssystems muss ein solches prinzipielle Anforderungen erfüllen. Die wohl wichtigste Eigenschaft eines EPS ist das Gewährleisten von Sicherheit. Betrachtet man die an einem Zahlungsvorgang beteiligten Parteien, erkennt man, wo Sicherheitslücken vorhanden sein können. Stolpmann unterscheidet fünf verschiedene Angriffspunkte, die sich ein potentieller Angreifer zu Nutze machen kann. Diese verschiedenen Angriffspunkte lassen sich in Sicherheitsaspekte bezüglich der Datenhaltung, der Datenübertragung und fahrlässiges Verhalten der an einer Transaktion beteiligten Akteure einteilen. Datenhaltung stellt nach Stolpmann vor allem auf den PCs der Kunden ein großes Problem dar, da diese Systeme bekanntlich meistens weder durch eine Firewall, noch durch aktuelle Antiviren-Programme ausreichend gesichert sind. Trojanische Pferde und andere Hackerprogramme können hier meist problemlos TANs, PINs, Kreditkartennummern oder sonstige vertrauliche Daten ausspähen. Die Möglichkeit eines Angriffs bei Banken oder sonstigen Institutionen, die als „Anbieter“ an den Zahlungsvorgängen beteiligt sind und daher auch kritische Daten in ihren Systemen gespeichert haben, wird von Stolpmann als weitaus geringer eingeschätzt, da der Aufwand des Datenklau und der Datenmanipulation wesentlich größer ist. Der Grund hierfür liegt im Einsatz von Firewalls, die den Angriff in ein Netzwerk von außerhalb dieses Netzes verhindern sollen. Sicherheitsbedenken treten hier jedoch auf, falls der Angriff eines Hackers aus dem Internen dieses Netzes erfolgt. Das Problem der Datenhaltung stellt neben den

10 Vgl. Schwickert, Axel C.: Electronic-Payment-Systeme im Internet, a. a. O., S. 25 f. Vgl. dazu auch Stolpmann, Markus: Elektronisches Geld im Internet. Grundlagen, Konzepte, Perspektiven, Köln: O'Reilly 1997, S. 50 ff.

11 Vgl. Pernul, Günther; Röhm, Alexander W.: Neuer Markt, Neues Geld, in: Wirtschaftsinformatik, Ausgabe 4/1997, S. 350 f.

Kundenrechnern und den Bankrechnern auch dann ein Problem dar, falls Händler die kritischen Daten zwischenspeichern und diese meist, "aus Mangel an Wissen"¹², nicht ausreichend schützen.¹³

Sichere Datenübertragung wird häufig mit Transaktionssicherheit gleichgesetzt. Die Datenübertragung bietet für Hacker ein großes Angriffsfeld. Der Angriff auf eine Nachricht, die vom Kunden zur Bank, eventuell über einen Händler, geschickt wird, kann zum einen passiver, zum anderen aktiver Natur sein. Passive Angriffe beschränken sich auf das Abhören der sensiblen Daten, aktive Angriffe hingegen versuchen sich direkt in die Kommunikation einzumischen, indem versucht wird, die Nachrichtenverbindung aufzutrennen. Aktive Angriffe führen dazu, dass beispielsweise Nachrichten verändert oder häufiger eingespielt werden und es dabei zu Vertrauensverlust, aber auch zu finanziellem Schaden sowohl für den Verkäufer als auch den Käufer kommen kann.¹⁴ Mit Hilfe von Verschlüsselungsverfahren, digitaler Zertifikate und Signaturen kann versucht werden die Datenübertragung sicherer zu gestalten.¹⁵ In der Literatur werden mehrere Aspekte einer sicheren Datenübertragung genannt, die ein Zahlungssystem erfüllen muss. Diese Aspekte sind Integrität, d.h. dass eine Transaktion nicht unbefugt manipulierbar ist, Vertraulichkeit, Identifikation (Authentizität), Nicht-Abstreitbarkeit (Verbindlichkeit) und eine ausreichende Verschlüsselung. Abschließend ist anzumerken, dass eine vollkommene Sicherheit jedoch von keinem System zu gewährleisten ist, da beispielsweise durch Austesten aller möglichen Schlüssel jede Verschlüsselung entschlüsselbar ist. Als sicher gelten daher jene Systeme, die in angemessener Zeit bzw. Aufwand nicht zu entschlüsseln sind.¹⁶ Neben der Anforderung an Sicherheit sind Skalierbarkeit, Transaktionskosten,

12 Stolpmann, Markus: Elektronisches Geld im Internet. Grundlagen, Konzepte, Perspektiven, a. a. O., 1997, S. 109.

13 Vgl. Stolpmann, Markus: Elektronisches Geld im Internet. Grundlagen, Konzepte, Perspektiven, a. a. O., S. 108 ff.

14 Vgl. Lepschies, Gunter: E-Commerce und Hackerschutz. Leitfaden für die Sicherheit elektronischer Zahlungssysteme, 2. überarbeitete Auflage, Braunschweig et al.: vieweg Verlag 2000, S. 8 ff.

15 Auf die verschiedenen Verschlüsselungsverfahren, PKI, Signaturen wird in dieser Arbeit nicht weiter eingegangen.

16 Vgl. Stolpmann, Markus: Elektronisches Geld im Internet. Grundlagen, Konzepte, Perspektiven, a. a. O., S. 111 f. Vgl. dazu auch Lepschies, Gunter: E-Commerce und Hackerschutz. Leitfaden für die Sicherheit elektronischer Zahlungssysteme, a. a. O., S. 98 ff.

Anonymität, Benutzerfreundlichkeit und Plattformunabhängigkeit weitere Anforderungen, die elektronische Zahlungsmethoden erfüllen sollten.¹⁷

3 Klassifizierung elektronischer Zahlungssysteme

Es gibt eine Vielzahl verschiedenartiger Zahlungssysteme, die sich nur in der konkreten Realisierung unterscheiden, im Kern jedoch die gleichen Funktionsweisen aufweisen, so dass man sie in wenige Klassen aufteilen kann. Eine Klassifikation der verschiedenen Systeme lässt sich zum einen über die damit abgewickelten Zahlungsbeträge, zum anderen über den Zahlungsmodus erreichen. Im weiteren werden die beiden Kategorisierungsansätze kurz vorgestellt.

3.1 Klassifizierung nach Zahlungsbetrag

Die Klassifikation verschiedener Zahlungssysteme mittels der Höhe einer Zahlung begründet sich in der Eigenschaft, dass einige Systeme besser für niedrige, andere Systeme besser für höhere Zahlungsbeträge geeignet sind. Dies hängt mit den für den Zahlungsvorgang anfallenden Transaktionskosten zusammen. Unter Transaktionskosten versteht man in diesem Zusammenhang „die Zeit, die eine Transaktion benötigt, aber auch die finanziellen Ausgaben, die für die weitere Verarbeitung, Hardwarekosten und anderen Aufwendungen anfallen“¹⁸. Kreditkartenzahlungen sind beispielsweise auf Grund der hohen Transaktionskosten, Furche spricht von bis zu 2,40 DM pro Transaktion, kaum für Zahlungen im Pfennigsbereich geeignet.¹⁹ Andere Methoden bieten sich hingegen nur in diesem Bereich an und weisen im Bereich hoher Beträge Schwächen auf. Generell unterscheidet man daher Systeme, die sich auf Grund der anfallenden Transaktionskosten für Micropayments eignen und Systeme, die sich für Macropayments eignen (manchmal auch noch Smallpayments)²⁰, wobei Schuster unter

17 Vgl. Schwickert, Axel C.: Electronic-Payment-Systeme im Internet, a. a. O., S. 25 f. Vgl. dazu auch Stolpmann, Markus: Elektronisches Geld im Internet. Grundlagen, Konzepte, Perspektiven, a. a. O., S. 50 ff.

18 Furche, Andreas; Wrightson, Graham: Computer Money. Zahlungssysteme im Internet, Heidelberg: dpunkt, Verlag für digitale Technologie, 1997, S. 16.

19 Vgl. Furche, Andreas; Wrightson, Graham: Computer Money. Zahlungssysteme im Internet, a. a. O., S. 17.

20 Vgl. Kuhlen, R; Semar, W.: Zahlungssysteme im Internet. Allgemeine Einführung, Online im Internet: <http://www.inf-wiss.uni-konstanz.de/CURR/summer98/imk/Internet-Zahlungssysteme/zahlungssysteme.html>, 4.5.2001.

Micropayments Zahlungen unter DM 5, und Macropayments Zahlungen über DM 5 versteht (Smallpayments ab \$ 0,1 bis \$ 10)²¹ .²²

3.2 Klassifizierung nach Zahlungsmodus

Neben der aufgezeigten Klassifizierung nach Zahlungsbeträgen unterscheidet man Zahlungssysteme auch nach dem Zahlungsmodus. Dabei rückt die Funktionsweise der Zahlung in den Vordergrund. Dies führt dazu, dass man EPS in die Klassen Kreditkartenzahlungen, Kundenkonto-Zahlungen (Account-Zahlungen) und elektronisches Geld (digitale Münzen) unterteilt. Kreditkartensysteme bauen auf der Infrastruktur der bereits etablierten Kreditkarten auf und versuchen die Übertragung der Kreditkartennummern über das Medium Internet sicher zu gestalten. Kundenkonten basieren zum einen auf einem Debit-, zum anderen auf einem Credit-System. Credit-Systeme erinnern stark an Girokonten, auf denen im voraus ein Betrag eingezahlt wurde, über welchen verfügt werden kann. Für Zahlungen im Netz ist nun nicht ein Girokonto bei der Hausbank, sondern ein Guthabenkonto bei einem der zahlreichen EPS-Service-Anbietern vonnöten. Debit-Systeme funktionieren ähnlich wie die Credit-Systeme, mit dem Unterschied, dass die bei Transaktionen anfallenden Kosten von dem jeweiligen EPS-Service-Provider vorgestreckt und zu einem späteren Zeitpunkt eingefordert werden. Elektronisches Geld ist eine Übertragung realen Geldes auf die Welt der Computer. Es existiert also nicht in materieller Form, sondern wird auf dem Computer in Form von Bitfolgen auf der Festplatte des Eigentümers codiert abgespeichert. Um elektronisches Geld zu erhalten, muss man im voraus reales Geld umtauschen. (Eine genauere Abhandlung dieses Vorganges wird im Abschnitt 4.2 eCash vorgenommen.) Die hier aufgezeigten Unterscheidungen sind nicht trennscharf, der Übergang zwischen den einzelnen Systemen ist fließend.²³

21 Vgl. Stumpf, Martin; Schöpf Thomas: Digitale Zahlungssysteme, Online im Internet: <http://chablis.informatik.tu-muenchen.de/fohlen/zahlungssysteme.pdf>, 22.11.2000.

22 Vgl. Schuster, Rolf; Färber, Johannes; Eberl, Markus: Digital Cash - Zahlungssysteme im Internet, Berlin et al.: Springer, 1997, S. 33.

23 Vgl. Schuster, Rolf; Färber, Johannes; Eberl, Markus: Digital Cash - Zahlungssysteme im Internet, a. a. O., S. 31 ff. Vgl. dazu auch Stolpmann, Markus: Elektronisches Geld im Internet. Grundlagen, Konzepte, Perspektiven, a. a. O., S. 53 f.

3.3 Zusammenfassende Bemerkungen

Die zwei aufgezeigten Kategorisierungen stehen nicht im Gegensatz zueinander, sondern weisen Zusammenhänge auf. Kreditkartenzahlungen eignen sich, wie bereits erwähnt, kaum für Microzahlungen und werden bevorzugt für Macrozahlungen eingesetzt. Elektronisches Geld hingegen eignet sich auf Grund der im folgenden genannten Eigenschaften nur begrenzt für Macrozahlungen, sehr wohl aber für Microzahlungen und Smallpayments.²⁴

4 Funktionsweise ausgewählter Beispiele

Die Anzahl verschiedener Zahlungssysteme, die es zur Zeit gibt, ist enorm. Dennoch fristen die meisten Anbieter ein Schattendasein. Einige Anbieter von EPS sind bereits wieder aus dem Markt ausgetreten bzw. fusionieren, um eine lohnende Verbreitung und Akzeptanz zu erlangen.²⁵ In den folgenden Abschnitten wird versucht die Funktionsweise einiger EPS offen zu legen und deren Stärken bzw. Schwächen aufzuzeigen.

4.1 eCash

Obwohl eCash zum 25. Mai 2001 von der Bank24 eingestellt wird, soll an dieser Stelle ein Überblick über eCash gegeben werden, um die Funktionsweise münzbasierter Systeme aufzuzeigen.²⁶ eCash ist ein rein auf Software basiertes Zahlungssystem. Um eCash benutzen zu können, muss auf Seiten des Kunden und auf Seiten des Händlers ein sogenanntes Cyberwallet installiert sein, über welches die weiteren Transaktionen, wie z.B. der Zahlungsvorgang, aber auch das Erstellen digitaler Münzen, abgewickelt werden können. Des weiteren benötigt man ein Konto bei einer Bank, welche eCash ausgibt. Kryptographische Grundlage von eCash stellen die sogenannten Blind Signatures dar, welche auf dem Public-Key-Verfahren aufbauen. Mit Hilfe der Blind Signatures wird eine anonyme Zahlung im Internet ermöglicht. Das Verfahren beruht

24 Vgl. Schuster, Rolf; Färber, Johannes; Eberl, Markus: Digital Cash - Zahlungssysteme im Internet, a. a. O., S. 33.

25 Vgl. u.a. Heise Online: Cybercash: Aus für Elektronisches Geld, Online im Internet: <http://www.heise.de/newsticker/data/ad-19.12.00-000/>, 19.12.2000.

26 Vgl. Heise Online: Deutsche Bank 24 stellt eCash ein, Online im Internet: <http://www.heise.de/newsticker/data/js-08.04.01-000/>, 8.4.2001.

darauf, dass die Seriennummer einer Münze auf dem Rechner des Kunden festgelegt, diese mit einer Blinding Number verschlüsselt und anschließend an die Bank gesendet wird. Die Bank versieht die jeweilige Münze mit ihrer digitalen Signatur und sendet sie dann wieder an den User zurück. Dieser muss nur noch die Blinding-Number entfernen und hat damit eine gültige, mit der Unterschrift der Bank versehene digitale Münze mit einer der Bank unbekanntem Seriennummer. Damit weiß die Bank zwar, dass sie eine Münze „geprägt“ hat, sie kann aber keine Protokollierung der Zahlungsvorgänge durchführen, da sie die Seriennummer der Münzen keinem Benutzer zuordnen kann. Mit Hilfe dieser Münzen kann der jeweilige Benutzer in den eCash akzeptierenden Shops bezahlen. Der Zahlungsablauf ist in der folgenden Graphik dargestellt und wird im weiteren erläutert.²⁷

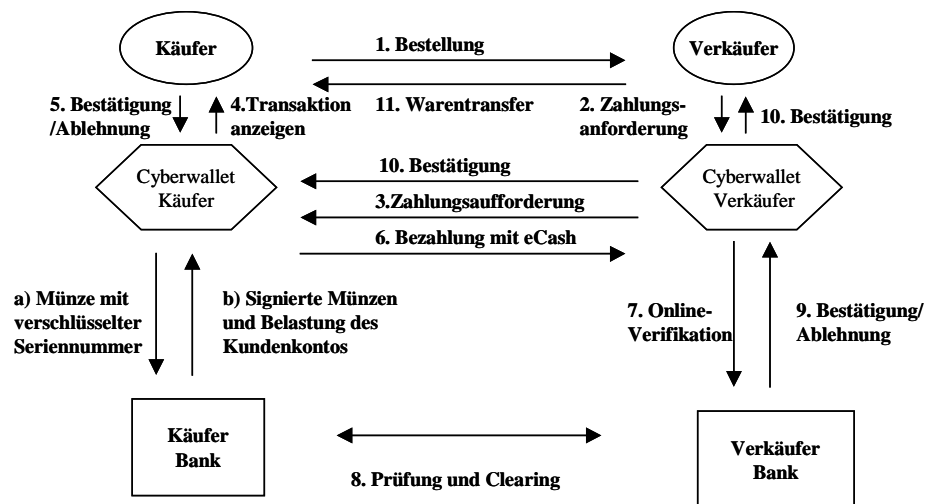


Abb. 1: Nachrichtenfluss bei Bezahlung mittels eCash²⁸

Bestellt der Kunde eine Ware über das Internet und wählt als Zahlungssystem das eCash System, wird eine Zahlungsanforderung an das Cyberwallet des Shophändlers gesendet (1-2). Das Cyberwallet des Händlers leitet daraufhin eine Zahlungsaufforderung an das Cyberwallet des Kunden weiter, welches veranlasst, dass beim Kunden die Transaktionsdaten des Zahlungsvorgangs angezeigt werden (3-4). Bestätigt der Kunde diese, so wird auch die Bezahlung bestätigt und die Münzen an das Cyberwallet des Händlers übertragen (5-6). Das Cyberwallet des Händlers leitet die Münzen wiederum

²⁷ Vgl. Schuster, Rolf; Färber, Johannes; Eberl, Markus: Digital Cash - Zahlungssysteme im Internet, a. a. O., S. 60 ff. Vgl. dazu auch Stolpmann, Markus: Elektronisches Geld im Internet. Grundlagen, Konzepte, Perspektiven, a. a. O., S. 56 f.

²⁸ In Anlehnung an: Merz, Michael: Elektronische Märkte im Internet, a. a. O., S. 73.

zur Bank, wo sie einer Online-Verifikation unterzogen werden. Dabei wird zum einen geprüft, ob die Münzen echt sind, zum anderen, ob eine Münze mit der entsprechenden Seriennummer bereits ausgegeben wurde (double spending problem) (7). Für diesen Vorgang ist eventuell eine Kommunikation zwischen den verschiedenen Banken vonnöten (8). Sind die Münzen „echt“, und wurden sie bisher nicht ausgegeben, wird eine Bestätigung an das Cyberwallet des Händlers geschickt, welches wiederum dem Cyberwallet des Kunden und dem Händler selbst die Zahlung bestätigt (9-10). Abschließend sollte der Transfer der Waren an den Kunden erfolgen (11).

eCash erfüllt die meisten der in Kapitel 2 genannten Anforderungen an Zahlungssysteme. Die Stärke des eCash-Systems liegt in der gewährleisteten Anonymität. Eine Zurückverfolgung von Zahlungen ist de facto nicht möglich. Außerdem wird durch die Online-Verifikation der Münzen dem Händler eine Zahlungssicherheit gegeben. Mit der Online-Verifikation ist jedoch ein Skalierbarkeits-Problem verbunden, da jede bereits eingelöste Münze auf einem zentralen Server hinterlegt werden muss. Ein weiteres Manko des eCash Systems ist die fehlende Transaktionalität. Kommt es während eines Zahlungsvorganges zu einer Störung, kann dies zu unwiderruflichem Verlust der Münzen führen. Die nötige Softwareinstallation und der Registrierungsprozess bei einer eCash anbietenden Bank ist ein weiterer Nachteil des Systems. Sicherheit bei der Datenübertragung wird durch das Public-Key-Verfahren gewährleistet. Die Datenhaltung der Münzen hingegen ist nach Stolpmann unzureichend gegen Missbrauch geschützt.²⁹ Die aufgelisteten Negativ-Aspekte und die damit verbundene mangelnde Akzeptanz sind Gründe dafür, dass das Verfahren von einigen Anbietern nicht mehr zur Verfügung gestellt werden wird.³⁰

4.2 Secure Electronic Transaction (SET)

Bei SET handelt es sich nicht um ein Zahlungssystem im engeren Sinne, sondern um ein Übertragungsprotokoll, das eine sichere Übertragung von Kreditkartendaten garantieren soll. SET wurde in Zusammenarbeit von Visa und MasterCard entwickelt, mit der Zielsetzung, einen offenen Standard für die Übertragung von

29 Vgl. Merz, Michael: Elektronische Märkte im Internet, a. a. O., S. 72 ff. Vgl. dazu auch Stolpmann, Markus: Elektronisches Geld im Internet. Grundlagen, Konzepte, Perspektiven, a. a. O., S. 54 ff.

30 Vgl. Heise Online: E-Payment: Praxistaugliche Verfahren vor dem Durchbruch, Online im Internet: <http://www.heise.de/newsticker/data/js-16.02.01-000/>, 16.2.2001.

Kreditkarteninformationen zu schaffen. SET bietet die Verschlüsselung der zu übertragenden Nachrichten, die Integrität von Transaktions- und Bestelldaten und die Identität des Karteninhabers und des Händlers.³¹ Dies wird durch eine Kombination von verschiedenen Verschlüsselungsverfahren, digitalen Unterschriften (digital signatures) und Zertifikaten erreicht.³² An einer Transaktion über das SET-Protokoll sind verschiedene Parteien - Kunde, Händler, Händlerbank und Zertifizierungsinstanzen - beteiligt. Der Kunde benötigt zur Verwaltung seiner Kreditkarten ein sogenanntes Cyberwallet, welches die virtuellen Kreditkartendaten aufnehmen kann. Die Kreditkarten werden durch digitale Zertifikate abgebildet, die an die Kartenummer sowie das Ablaufdatum der jeweiligen Kreditkarte gekoppelt sind. Das Zertifikat erhält der Kunde von einer Zertifizierungsinstanz, in der Regel ist dies die kartenausgebende Bank. Die zweite Partei, die an dem Zahlungsvorgang teilnimmt, ist der Händler. Dieser muss neben seinem Shopsystem einen SET-Server (Payment Server) betreiben und sich von einer Zertifizierungsstelle zertifizieren lassen. Der SET-Server dient dazu, die Kommunikation zwischen dem Cyberwallet des Kunden, dem eigentlichen Shopsystem und dem Payment-Gateway der Händlerbank zu steuern. Die Händlerzertifikate dienen einer sicheren Kommunikation mit Kunden und Payment Gateway. Die Händlerbank betreibt das Payment Gateway, welches die Schnittstelle zwischen Internet und den Kreditkartennetzwerken darstellt. Außerdem verwaltet das Payment Gateway die eigenen Zertifikate und die Certification Revocation Lists (CRL), mit deren Hilfe festgestellt werden kann, ob die bei der Transaktion benutzte Karte Gültigkeit besitzt. Wie man erkennt, müssen alle an einer SET-Transaktion beteiligten Partner ein gültiges Zertifikat besitzen. Diese Zertifikate werden von hierarchisch angeordneten Zertifizierungsstellen ausgegeben. Der Zahlungsvorgang einer SET-Transaktion ist in der folgenden Graphik dargestellt.

-
- 31 Vgl. Stolpmann, Markus: Elektronisches Geld im Internet. Grundlagen, Konzepte, Perspektiven, a. a. O., S. 73.
- 32 Vgl. Lepschies, Gunter: E-Commerce und Hackerschutz. Leitfaden für die Sicherheit elektronischer Zahlungssysteme, a. a. O., S. 114 ff.

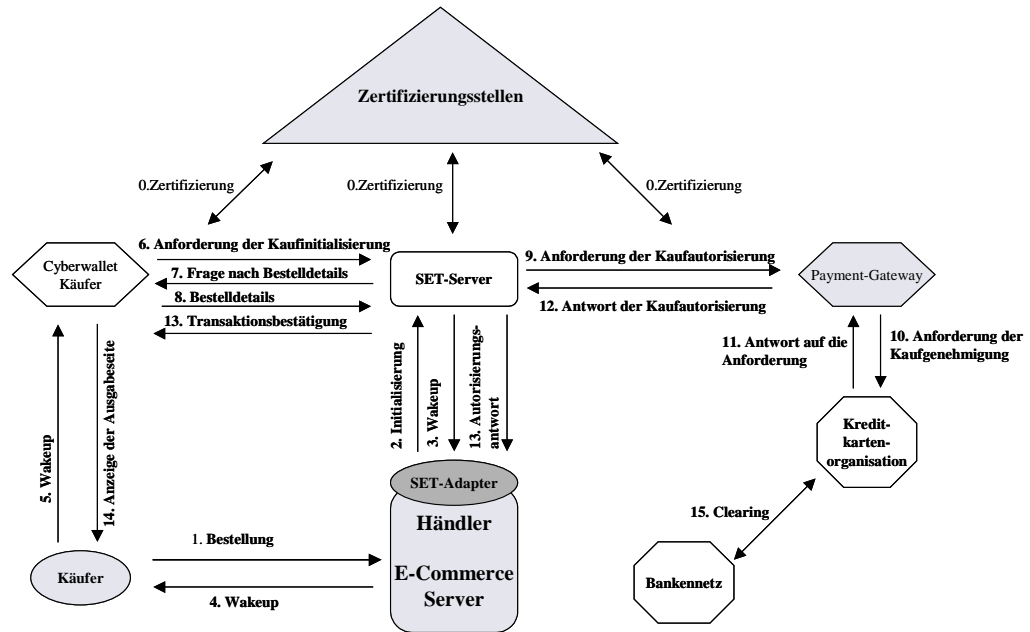


Abb. 2: Nachrichtenfluss bei Bezahlung mittels SET³³

Hat der Kunde die gewünschte Ware ausgesucht und wählt an der Kasse des Web-Shops die Bezahlung über SET (1), so initialisiert der Shopperserver den SET-Server (2). Dieser schickt daraufhin eine Wake-Up Nachricht an den Shopperserver, welche über den Browser des Kunden an dessen Cyberwallet weitergeleitet wird (3-5). Daraufhin wählt der Kunde die gewünschte Kreditkarte aus und sendet danach die Kaufinitialisierung an den SET-Server. Der SET-Server identifiziert sich darauf bei dem Cyberwallet des Kunden Käufer und wartet auf die Bestelldetails (6-7). Signiert der Kunde den Einkauf (8), leitet der SET-Server die Zahlungsinformationen an das Payment Gateway weiter (9). Innerhalb des Kreditkartennetzes werden nun die Zahlungsinformationen überprüft und eine Antwort an das Payment Gateway weitergegeben (10-11), welches die Nachricht wiederum an das Shoppersystem und über den SET-Server an das Cyberwallet weiterleitet (12-13). Abschließend wird der Kunde abhängig vom Erfolg der Transaktion auf eine HTML Seite weitergeleitet, die ihm den Status der Transaktion anzeigt (14).³⁴

Das SET Protokoll hat Stärken im Bereich der Datenübertragung aufzuweisen, da Bestell- und Bezahlinformationen verschlüsselt und getrennt voneinander über das Netz transportiert werden. Des weiteren bietet die Zertifizierungshierarchie weitere

33 In Anlehnung an: Computop Wirtschaftsinformatik GmbH: So funktioniert SET, Online im Internet: <http://www.computop.de/set2.htm>, 5.5.2001.

34 Vgl. Boden, Klaus-Peter: Sicherheitsaspekte in internetbasierten Zahlungssystemen und deren Integration in Online-Shops, HMD - Praxis der Wirtschaftsinformatik, Heft 216 12/2000, S. 36 ff.

Sicherheitsvorteile. Andererseits werden durch SET Angriffsszenarien, z.B. das automatische Generieren von Kreditkartennummern und deren Missbrauch durch Händler, nicht ausgeschaltet.³⁵ Bei der Datenhaltung, speziell auf Seiten des Kunden, können ebenfalls Sicherheitsprobleme auftauchen. Die Frage nach der Skalierbarkeit stellt für Zahlungssysteme auf SET basierend kein Problem dar, da es für den weltweiten Einsatz konzipiert wurde und auf bestehende Infrastruktur zurückgreifen kann. Auf Grund der hohen Transaktionskosten, die durch die Kreditkartennutzung anfallen, eignet sich SET nicht für Micropayments. Die nicht gewährleistete Anonymität stellt einen weiteren Nachteil von SET dar. Fraglich ist auch, ob die Kosten, die den Banken durch die Zertifizierung der Kreditkarten entstehen, die Banken nicht von der Teilnahme an SET abschrecken. SET hat nur dann eine Zukunft, wenn alle Kreditkarten herausgebenden Banken daran teilnehmen, da diese die Kreditkarten zertifizieren. Die weitere Entwicklung des SET-Protokolls und darauf basierender Zahlungssysteme wird daher auch von politischen Fragen abhängen.³⁶

4.3 Paybox

Paybox ist ein account-basiertes Zahlungssystem. Die Funktion des EPS-Provider übernimmt dabei die paybox.net AG, bei der sich sowohl Kunde als auch Händler registrieren müssen. Das Paybox-Verfahren ist kein neues Bezahlverfahren, sondern eine Methode mittels Mobiltelefon eine Genehmigung zum Lastschriftinzug zu geben. Dazu benötigen weder Kunde noch Händler, außer einem Giro-Konto bei Ihrer Hausbank, besondere bankliche Voraussetzungen. Software Installation auf Seiten des Kunden sind nicht vonnöten. Dieser muss sich lediglich, unter Angabe seiner Handynummer, Bankverbindung und persönlichen Daten, bei der paybox.net AG registrieren. Im Gegenzug erhält er von der paybox.net AG über einen sicheren Kanal (Postweg) eine Paybox-PIN zugesendet, mit der er während eines Einkaufes die Zahlung genehmigt. Für die Nutzung von Paybox wird dem Kunden eine jährliche Grundgebühr von € 5 in Rechnung gestellt.

35 Vgl. Lepschies, Gunter: E-Commerce und Hackerschutz. Leitfaden für die Sicherheit elektronischer Zahlungssysteme, a. a. O., S. 121.

36 Vgl. Furche, Andreas; Wrightson, Graham: Computer Money. Zahlungssysteme im Internet, a. a. O., S. 53.

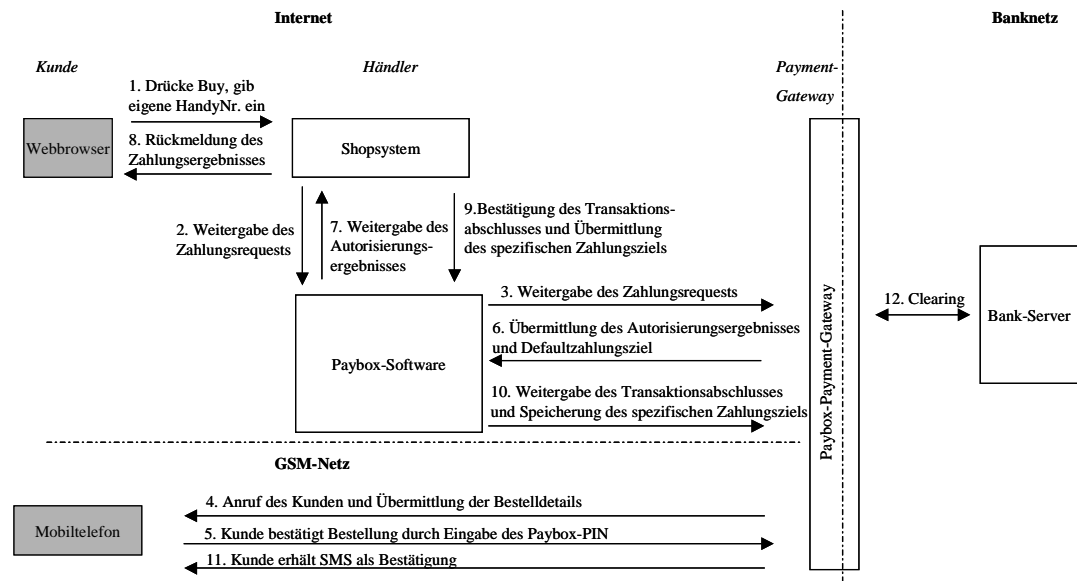


Abb. 3: Nachrichtenfluss bei Bezahlung mittels Paybox³⁷

Der Händler muss außer seinem Webshop noch eine kostenpflichtige Software einsetzen, welche die Kommunikation zwischen Shop-System und dem Paybox-Gateway aufbaut. Außerdem verpflichtet er sich mit der Registrierung bei paybox.net AG einen prozentualen Anteil des Transaktionsvolumen an die paybox.net AG abzutreten. Diese übernimmt im Gegenzug den Lastschrifteinzug vom Kundenkonto und die Überweisung auf das Konto des Händlers. Die paybox.net AG gibt hierbei jedoch keine Zahlungsgarantie, sichert in Fällen des Missbrauchs dem Händler Leistungen, wie z.B. die Herausgabe der Kundendaten oder Einschaltung eines Inkassounternehmens, zu. Abbildung 3 zeigt die bei der Transaktion beteiligten Parteien und den Kommunikationsfluss, der im weiteren erläutert wird.

Möchte ein Kunde im Internet mittels Paybox bezahlen, so muss dieser nach Auswahl des entsprechenden Verfahrens an der Shop-Kasse seine Handynummer eintragen (1) und startet damit eine Zahlungsanfrage. Diese Zahlungsanfrage leitet der Web-Shop über die Paybox-Software an das Paybox-Payment-Gateway weiter (2-3). Das Payment-Gateway ruft daraufhin die angegebene Mobilfunknummer an und übermittelt die Bestelldetails (4). Danach bestätigt der Kunde den Anruf durch Eingabe seines Paybox-PIN (5). Das Payment-Gateway übermittelt das Autorisierungsergebnis und ein Default-

37 In Anlehnung an: Boden, Klaus-Peter: Sicherheitsaspekte in internetbasierten Zahlungssystemen und deren Integration in Online-Shops, HMD - Praxis der Wirtschaftsinformatik, Heft 216 12/2000, S. 42. und Paybox.net AG: Integration von Paybox in ihr Shopsystem, Online im Internet: http://www.paybox.de/registrierung/paybox_Whitepaper_V1.pdf, 7/2000.

Zahlungsziel an die Paybox-Software, welche die Nachricht an das Shopsystem weiterleitet (6-7). Das Shopsystem veranlasst darauf, dass eine Rückmeldung auf die Zahlungsanforderung des Kunden an diesen gesendet wird. Gleichzeitig bestätigt der Web-Shop der Paybox-Software den Transaktionsabschluss und übermittelt das transaktionsspezifische Zahlungsziel. Die Informationen werden an das Paybox-Payment-Gateway weitergeleitet und gespeichert (8-10). Der Zahlungsabschluss wird dem Kunden zusätzlich via SMS auf die angegebene Handynummer bestätigt (11). Nach Abschluss der Transaktion veranlasst die paybox.net AG das Clearing (12).³⁸

Die Stärken des Paybox-Verfahrens liegen in der Einfachheit des Zahlungsvorgangs. Der Kunde muss lediglich seine Handynummer an der Shopfront eingeben, warten bis er angerufen wird und die Transaktion mit der ihm zugeteilten PIN bestätigen. Eine Software-Installation entfällt gänzlich. Dennoch ist das Verfahren dreifach gegen Missbrauch geschützt. Ein Hacker müsste zum einen die SIM-Karte des Handys und die zugehörige PIN besitzen, zum anderen müsste er Kenntnis über die Paybox-PIN haben. Anonymität ist bei Bezahlung mittels Paybox nicht gewährleistet, da die paybox.net AG die Transaktionen eines Kunden problemlos nachvollziehen kann. Paybox eignet sich kaum für Microzahlungen, sondern zielt auf Macrozahlungen ab.³⁹ Paybox ist, sowohl für den Kunden als auch für den Händler, ein kostenpflichtiges Zahlungssystem. Mit bisher 200.000 registrierten Kunden und 800 Internetshops haben sich dennoch bereits sehr viele User registriert.⁴⁰ Die große Anzahl an registrierten Handys bietet Paybox ein großes Wachstumspotential. Paybox eignet sich nicht nur für das Bezahlen im Internet, sondern auch im Alltag. Überweisungen zwischen Paybox-Kunden sind kostenpflichtig, aber möglich, Pilotprojekte, wie das Bezahlen in Taxen, oder Supermärkten⁴¹ werden bereits durchgeführt.⁴²

38 Vgl. Boden, Klaus-Peter: Sicherheitsaspekte in internetbasierten Zahlungssystemen und deren Integration in Online-Shops, HMD - Praxis der Wirtschaftsinformatik, Heft 216 12/2000, S.42.

39 Vgl. Seeger, Jürgen: Zahlungssysteme für E-Commerce – Frischer Wind, in: Ix, Magazin für professionelle Informationstechnik, CeBIT Special, 3/2001, S. 40.

40 Vgl. Schmidt, Holger: Deutsche Bank und Paybox bieten Handy-Überweisungen an, in: FAZ, Online im Internet: <http://presse.paybox.de/pressemeldung/index.php3?kat=Pressespiegel>, 26.3.2001.

41 Vgl. o.V.: Paybox Übersicht, Online im Internet: <http://www.wattline.de/Produkte/Paybox/Paybox.htm>, 15.5.2001.

42 Vgl.: Boden, Klaus-Peter: Sicherheitsaspekte in internetbasierten Zahlungssystemen und deren Integration in Online-Shops, HMD - Praxis der Wirtschaftsinformatik, Heft 216 12/2000, S. 40 ff.

5 Probleme und Grenzen

Die langsame Verbreitung der Zahlungssysteme beruht auf einem „Henne-Ei-Syndrom“. Ist die Anzahl der bisher registrierten Nutzer eines Zahlungssystems zu gering, werden sich kaum Händler finden, die das Zahlungsmittel anbieten. Auf der anderen Seite sind die Kunden nicht dazu bereit Software zu installieren oder langwierige Registrierungsverfahren durchzuführen, wenn nur wenige Anbieter das in Betracht kommende Zahlungsverfahren zur Verfügung stellen.⁴³ Diese Tatsache führt dazu, dass eine Vielzahl verschiedener Anbieter von Zahlungsmitteln am Markt existieren, deren Produkte sich jedoch kaum für alle Transaktionen eignen. Ein Kunde muss daher neben den bisherigen Zahlungsmitteln, wie z.B. EC-Karte und Bargeld, auch für den elektronischen Handel Zahlungssysteme bei verschiedenen Anbietern registrieren. Dieses Fehlen einer universellen Zahlungslösung und damit eines Standards stellt nach Stolpmann ein weiteres Problem dar.⁴⁴ Weiterhin werden durch die verschiedenen Zahlungsverfahren zwar teilweise Anonymität und sichere Übertragung der Transaktionsdaten gewährleistet, jedoch bleiben die Bedenken der Kunden, dass versteckte Schattenkontenführung oder Missbrauch der Benutzerdaten erfolgt, bestehen. Um dem entgegenzuwirken müssten staatliche bzw. freiwillige Kontrollmechanismen eingesetzt werden, die ein Vertrauensverhältnis schaffen.⁴⁵ Neben den aufgezeigten technischen und personenbezogenen Problemen sind mit der Einführung von elektronischen Zahlungssystemen auch volkswirtschaftliche, politische und gesetzliche Fragestellungen verbunden. Volkswirtschaftliche Folgen können u.a. eine sinkende Bargeldnachfrage, Verlust von Seignorage⁴⁶, Verlust des Einflusses der Zentralbank und ein Anstieg der Umlaufgeschwindigkeit, die zu verstärkter Inflation führen könnte, sein. Politische und gesetzliche Fragen können im Gewährleisten des Datenschutzes, der Verhinderung von elektronischer Geldwäsche, Steuerflucht,

43 Vgl. Niemann, Frank: Anbieter von Web-Bezahlssystemen entdecken den Konsumenten, a. a. O., S. 54.

44 Vgl. Stolpmann, Markus: Elektronisches Geld im Internet. Grundlagen, Konzepte, Perspektiven, a. a. O., S. 136.

45 Vgl. Schuster, Rolf; Färber, Johannes; Eberl, Markus: Digital Cash - Zahlungssysteme im Internet, a. a. O., S. 80.

46 Seignorage ist der Gewinn, den die Zentralbank aus der Bargeldemission schöpft.

Festlegen von Wechselkursen und dem Gewährleisten sicherer Zertifizierungsmechanismen bestehen.⁴⁷

6 Zusammenfassung und Ausblick

Wie man in den vorigen Kapiteln erkennen kann, gibt es eine Reihe von verschiedenen Lösungsansätzen im Bereich des elektronischen Bezahls. Dennoch existiert keine Lösung, die alle in Kapitel 2 angegebenen Anforderungen erfüllt. Die Nichterfüllung aller Anforderungen ist jedoch nicht das Hauptproblem, welches sich den verschiedenen Zahlungssystemen stellt. Vielmehr ist die mangelnde Akzeptanz bzw. Verbreitung, die vor allem aus dem oben erwähnten Teufelskreis resultiert, ein Haupthindernis in der Entwicklung von elektronischen Zahlungssystemen. Die weitere Entwicklung von EPS ist nicht vorauszusehen. Es ist jedoch zu erwarten, dass durch Werbekampagnen und Fusionen verschiedene EPS-Anbieter versuchen ihren Kundenstamm zu vergrößern, aber auch neue Verfahren an Bedeutung gewinnen werden. Als ein solches modernes Verfahren werden nach einer Studie von Forrester Research intelligente Smartcards angesehen, die heutzutage aufgrund teurer Lesegeräte noch sehr kostenintensiv sind und daher bisher nur eine marginale Verbreitung aufweisen.⁴⁸

Abschließend ist festzustellen, dass es, wie in Kapitel 5 gezeigt, noch viele Probleme und offene Fragen gibt, die es zu klären gilt, bevor ein Durchbruch in der Verbreitung und Nutzung elektronischer Zahlungssysteme erfolgen kann.

47 Vgl. Furche, Andreas; Wrightson, Graham: Computer Money. Zahlungssysteme im Internet, a. a. O., S. 94 ff.

48 Vgl. Niemann, Frank: Anbieter von Web-Bezahlssystemen entdecken den Konsumenten, a. a. O., S. 54.

Literaturverzeichnis

1. **Boden, Klaus-Peter:** Sicherheitsaspekte in internetbasierten Zahlungssystemen und deren Integration in Online-Shops, HMD - Praxis der Wirtschaftsinformatik, Heft 216 12/2000.
2. **Computer Industry Almanac Inc.:** Internet Users, Online im Internet: <http://www.c-i-a.com/199911iu.htm>, 4.11.1999.
3. **Computop Wirtschaftsinformatik GmbH:** So funktioniert SET, Online im Internet: <http://www.computop.de/set2.htm>, 5.5.2001.
4. **Furche, Andreas; Wrightson, Graham:** Computer Money. Zahlungssysteme im Internet, Heidelberg: dpunkt, Verlag für digitale Technologie, 1997.
5. **Heise Online:** Cybercash: Aus für Elektronisches Geld, Online im Internet: <http://www.heise.de/newsticker/data/ad-19.12.00-000/>, 19.12.2000.
6. **Heise Online:** Deutsche Bank 24 stellt eCash ein, Online im Internet: <http://www.heise.de/newsticker/data/js-08.04.01-000/>, 8.4.2001
7. **Heise Online:** E-Payment: Praxistaugliche Verfahren vor dem Durchbruch, Online im Internet: <http://www.heise.de/newsticker/data/js-16.02.01-000/>, 16.2.2001.
8. **Institut für Wirtschaftspolitik und Wirtschaftsforschung:** Umfrage zu Zahlungsmitteln im Internet, Online im Internet: <http://www.iww.uni-karlsruhe.de/IZV4/auswertung/showalle.html>, 20.3.2001.
9. **Kuhlen, R; Semar, W.:** Zahlungssysteme im Internet. Allgemeine Einführung, Online im Internet: <http://www.inf-wiss.uni-konstanz.de/CURR/summer98/imk/Internet-Zahlungssysteme/zahlungssysteme.html>, 4.5.2001.
10. **Lepschies, Gunter:** E-Commerce und Hackerschutz. Leitfaden für die Sicherheit elektronischer Zahlungssysteme, 2. überarbeitete Auflage, Braunschweig et al.: vieweg Verlag 2000.
11. **Merz, Michael:** Elektronische Märkte im Internet, Bonn et al.: International Thomson Publishing 1996.

12. **Niemann, Frank:** Anbieter von Web-Bezahlssystemen entdecken den Konsumenten, in: Computerwoche, Young Professional, Ausgabe 2/2001, S. 54-56.
13. **o.V.:** Paybox Übersicht, Online im Internet: <http://www.wattline.de/Produkte/Paybox/Paybox.htm>, 15.5.2001.
14. **Paybox.net AG:** Integration von Paybox in ihr Shopsystem, Online im Internet: http://www.paybox.de/registrierung/paybox_Whitepaper_V1.pdf, 7/2000.
15. **Pernul, Günther; Röhm, Alexander W.:** Neuer Markt, Neues Geld, in: Wirtschaftsinformatik, Ausgabe 4/1997, S. 345-364.
16. **Rothhaas, Frank:** Fundamentals of Electronic Business, Online im Internet: http://www.bwl.uni-mannheim.de/Niedereichholz/Fundamentals_of_E-Business_II.pdf, 16.10.2000.
17. **Schmidt Holger:** Deutsche Bank und Paybox bieten Handy-Überweisungen an in: FAZ, Online im Internet: <http://presse.paybox.de/pressemeldung/index.php3?kat=Pressespiegel>, 26.3.2001.
18. **Schuster, Rolf; Färber, Johannes; Eberl, Markus:** Digital Cash - Zahlungssysteme im Internet, Berlin et al.: Springer, 1997.
19. **Schwickert, Axel C.:** Electronic-Payment-Systeme im Internet, in: IM Informationsmanagement, Ausgabe 4/1996, S. 24-30.
20. **Seeger, Jürgen:** Zahlungssysteme für E-Commerce – Frischer Wind, in: Ix, Magazin für professionelle Informationstechnik, CeBIT Special, 3/2001, S. 40.
21. **Stolpmann, Markus:** Elektronisches Geld im Internet. Grundlagen, Konzepte, Perspektiven, Köln: O'Reilly 1997.
22. **Stumpf, Martin; Schöpf Thomas:** Digitale Zahlungssysteme, Online im Internet: <http://chablis.informatik.tu-muenchen.de/folien/zahlungssysteme.pdf>, 22.11.2000.