

Ein agentenbasiertes Micropaymentsystem

Der Fakultät für Ingenieurwissenschaften,
Abteilung Maschinenbau der
Universität Duisburg-Essen
Standort Duisburg

zur Erlangung des akademischen Grades

DOKTOR-INGENIEUR

genehmigte Dissertation

von

Matthias Lenord

aus

Oberhausen

Referent: Prof. Dr.-Ing. Hans-Dieter Kochs
Korreferent: Prof. Dr.-Ing. Walter Geisselhardt
Tag der mündlichen Prüfung: 16. Mai 2003

Vorwort

Die vorliegende Dissertation entstand während meiner Arbeit als wissenschaftlicher Mitarbeiter im Rahmen des Sonderforschungsbereiches 291 an der Universität Duisburg-Essen. Wichtige Stationen meiner Tätigkeit waren die Lehrstühle Technische Informatik und Datenverarbeitung am Institut für Informationstechnik und der Lehrstuhl Mechatronik am Institut für Mechatronik und Systemdynamik. Ich möchte mich bei den Lehrstuhlinhabern Prof. Dr.-Ing. H.-D. Kochs, Prof. Dr.-Ing. W. Geisselhardt und Prof. Dr.-Ing. habil. M. Hiller für alle wertvollen Anregungen, die großzügige Förderung und die hilfreiche Begleitung bedanken. Herr Prof. Kochs und Herr Prof. Geisselhardt haben durch ihr Engagement als Referent und Korreferent die Fertigstellung der Arbeit erst möglich gemacht.

Bei meinen Kollegen bedanke ich mich für die vielen interessanten Diskussionen, die Hilfsbereitschaft und das gute Arbeitsklima. Herr Dr.-Ing. Jörg Petersen hat mir durch seine guten Ratschläge über die formalen Hürden des Promotionsverfahrens hinweggeholfen. Weiterhin danke ich auch den Studenten, die im Rahmen von Studien- und Diplomarbeiten sowie ihrer Tätigkeit als studentische Hilfskraft, einzelne Aspekte zum Thema „Internet-Technologien für Ingenieure“ beleuchtet haben. Hervorheben möchte ich die hervorragende Diplomarbeit von Herrn Dipl.-Ing. Moritz Königsbüscher zum Thema Micropayments, der mir dadurch die Anregung zu einer Vertiefung dieser Thematik gegeben hat.

Von meinem langjährigen Freund Thomas Nisbach habe ich neben der persönlichen Unterstützung wesentliche Anstöße für meine Arbeit erhalten. Durch seine Kreativität und sein tiefes Fachwissen auf dem Gebiet der Kommunikations- und Softwaretechnik habe ich viel für die praktische Implementierung des Konzeptes gelernt. Mein Dank gilt auch der Firma Allcash GmbH mit ihrem technischen Leiter Herrn Thomas Pieper, der eine prototypische Umsetzung des Micropaymentsystems ermöglicht hat.

Ganz besonders bedanken möchte ich mich schließlich bei meiner Frau Diana und meinen Kindern Samuel und Silas. Sie haben die Belastungen des Promotionsverfahrens mit großer Geduld getragen. Ohne ihr Verständnis und ihre Unterstützung wäre die Arbeit sicherlich nicht zustande gekommen. Dem anschließen möchte ich den Dank an meine Eltern, die mich immer ermutigt und gefördert haben.

Last but not least möchte ich mich als Christ bei Jesus bedanken, den ich in meinem Leben als tägliche Kraftquelle und Richtungsweisung erlebe.

Duisburg, im Juni 2003

Matthias Lenord

Inhaltsverzeichnis

VORWORT	III
INHALTSVERZEICHNIS	V
ABSTRACT	VI
1 EINLEITUNG	1
2 GRUNDLAGEN	4
2.1.1 <i>Prinzipien</i>	4
2.1.2 <i>Stand der Wissenschaft</i>	5
3 KONZEPTION EINES MICROPAYMENTSYSTEMS	8
3.1 ANWENDUNG VON PREPAIDKARTEN IM INTERNET	8
3.2 ARCHITEKTUR ZUR EINZELTRANSAKTIONSABWICKLUNG	9
3.2.1 <i>Problemlösung mit Softwareagenten</i>	9
3.2.2 <i>Agentenbasierte Architektur</i>	9
3.3 KONZEPT FÜR EINE DYNAMISCHE PREISBESTIMMUNG	11
4 ZUSAMMENFASSUNG UND AUSBLICK	15
5 LITERATURVERZEICHNIS	18
5.1 MONOGRAFIEN	18
5.2 KONFERENZBÄNDE, ZEITSCHRIFTEN	19
5.3 HOCHSCHULSCHRIFTEN	21
5.4 FIRMENSCHRIFTEN	22
5.5 NORMEN, INTERNETSTANDARDS UND PATENTE	23
LEBENS LAUF DES VERFASSERS	25

Abstract

Das Internet hat sich besonders in den letzten Jahren vom wissenschaftlich-militärischen Informationsmedium zu einer kommerziellen Dienstleistungsplattform entwickelt. Im Zentrum der Betrachtungen bei der Erschließung des Marktsegmentes „e-Commerce“ stehen Mechanismen zur sicheren Abwicklung von Finanztransaktionen. Während sich bereits Verfahren zur Abwicklung von Zahlungen im mittleren Preissegment etabliert haben, steckt insbesondere die Technologie für den Handel mit elektronischen, klein-preisigen Gütern, die unmittelbar online ausgeliefert werden, noch im Forschungs- und Entwicklungsstadium. Aufgrund des Transfers von sehr kleinen Geldsummen wurde hierfür der Begriff „Micropayments“ geprägt.

Micropayments spielen seit den Arbeiten von David Chaum zu eCash im Jahre 1983 eine Rolle. Seitdem wurden immer wieder Ansätze entworfen, die im wissenschaftlichen Bereich ihre Bedeutung hatten, sich aber im kommerziellen, praktischen Umfeld nicht durchsetzen konnten. Grund dafür war, dass die mathematische Lösung von kryptografischen Problemen im Fokus der Betrachtungen stand, während technologische und finanzrechtliche Aspekte in den Hintergrund gerückt wurden.

In dieser Arbeit werden Micropaymentssysteme in ihrem Gesamtkontext betrachtet und ein Vorschlag für ein Konzept vorgestellt, das neben kryptografischen Methoden auch die Aspekte der realen Geldflüsse und ergonomischen Technologie einbezieht. So wird in dieser Arbeit eine neuartige Methode zur einfachen und anonymen Bereitstellung von Geldbeträgen mittels einer kartenbasierten Zertifikatserzeugung vorgestellt, die auf die Anforderungen von Micropaymentssystemen zugeschnitten ist. Weiterhin wird ein Konzept für ein adaptives und intelligentes System zur Abwicklung der kostenpflichtigen Einzeltransaktionen erarbeitet, das sich auf das Kaufverhalten der Nutzer einstellt und eine autonome Preisermittlung vornimmt. Die Basistechnologie bilden kooperierende Softwareagenten. Damit stellt die Konzeption im Bereich der Micropaymentssysteme eine wissenschaftliche Neuerung dar und knüpft an die nächste Entwicklungsstufe des Internets an, ein intelligentes Netz zu werden.

1 Einleitung

Das Internet entwickelt sich zum Alltagsmedium. In Deutschland nutzen mittlerweile über 50 Prozent (ca. 30 Mio) der Bundesbürger zwischen 14 und 69 Jahren das weltumspannende Computernetz. Die Zahl der Nutzer versechsfachte sich in den letzten 4 Jahren (vgl. **Bild 1.1**).

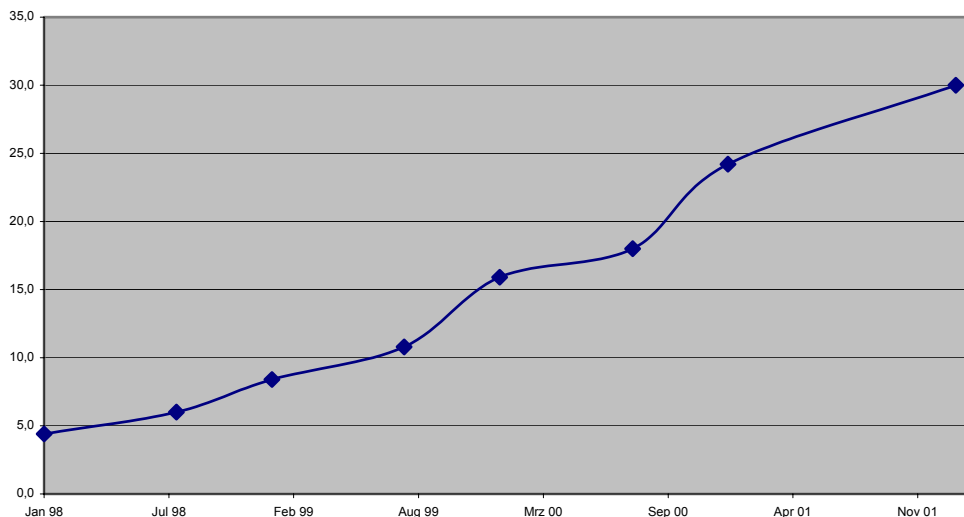


Bild 1.1: Anzahl der Internetnutzer in Deutschland in Mio¹

Obwohl das Internet erst in den letzten Jahren den Marktdurchbruch vollzogen hat, wurde bereits 1966 die erste Idee geboren. Seitdem hat es verschiedene Entwicklungsstufen durchlaufen (Hafner und Lyon 2000). Bis zum Jahre 1989 wurde es in erster Linie vom Militär und von Forschungseinrichtungen zum Austausch von wissenschaftlichen Daten und zur Ressourcenteilung genutzt. Erst mit der Einführung des Hypertextsystems ist das heute bekannte WWW (World Wide Web) geboren worden. Das Internet bietet seitdem eine durchdachte Bedieneroberfläche, die auch unerfahrenen Nutzern den Zugriff auf weltweite Daten ermöglicht. Es entsteht ein breiter Markt für Online-Dienste und ISPs (Internet Service Provider), während die Werbewirtschaft das WWW als zugeschnittene Marketingplattform entdeckt. Mit der Einführung der ersten Online-Zahlungssysteme im Jahr 1996, unterstützt von großen Kreditkartenherausgebern und Banken, wird es möglich, Geschäfte über das Internet abzuwickeln (Sandig 1999). Marketingfachleute prägen die Begriffe „eCommerce“ und „eBusiness“, um das neue Geschäftsfeld griffig zu vermarkten. Viele Unternehmen bieten Infrastrukturen, Produkte und Dienstleistungen rund um den elektronischen Handel an. Beispiele sind PSPs (Payment Service Provider), die Dienstleistungen für die Zahlungsabwicklung im Internet anbieten.

¹ 7. Studie der GFK-Medienforschung (GFK 2001) und Studie der BITKOM (BITKOM 2002)

Trotz der rasanten Entwicklung steckt das Internet noch immer in den Kinderschuhen. Insbesondere die Technologie für den Handel mit elektronischen, kleinspreisigen Gütern (intangibles), die unmittelbar online ausgeliefert werden, ist im Forschungs- und Entwicklungsstadium steckengeblieben. So schätzt der Erfurter Forscher Dr. K. Beck² ein: „Die Entwicklung dürfte etwa so weit fortgeschritten sein wie die des Radios im Jahr 1928. Wenn es möglich wäre, auch winzigste Informationsschnipsel unmittelbar abzurechnen, würde dies das Medium stark wandeln.“ Systeme, die eine derartige Zahlungsabwicklung ermöglichen, werden als „Micropaymentsysteme“ bezeichnet.

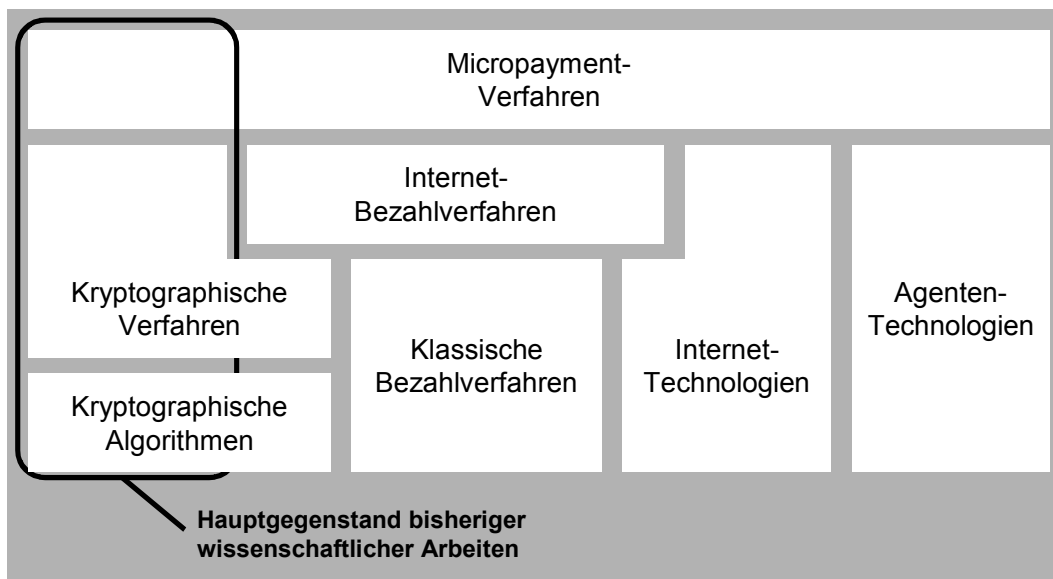


Bild 1.2: Bausteine für Micropaymentverfahren

Micropaymentverfahren basieren auf den in **Bild 1.2** dargestellten Technologien. *Kryptografische Algorithmen* stellen die mathematischen Grundlagen bereit, um Daten effizient zu verschlüsseln und eindeutig zu identifizieren. *Kryptografische Verfahren* nutzen diese Algorithmen, um anwendungsorientierte Ziele zu erreichen. Dazu zählen u.a. Techniken für digitale Unterschriften, elektronische Zertifikate und digitale Münzen. Diese beiden Bausteine bilden ein Kernelement bei der Betrachtung von Micropaymentverfahren und waren damit auch Hauptgegenstand der wissenschaftlichen Arbeiten in der Vergangenheit. Die vorgeschlagenen Systeme haben in fast allen Fällen das Forschungsstadium nie verlassen, weil sie nur eine Teillösung bei der Konzeption von Micropaymentsystemen darstellen und nur selten in der Kombination mit den weiteren Bausteinen betrachtet wurden.

In dieser Arbeit werden Micropaymentsysteme in ihrem Gesamtkontext betrachtet und ein Vorschlag für ein Konzept vorgestellt, das auch die folgenden Bausteine einbezieht. *Klassische Bezahlverfahren* bilden das Rückgrad der Zahlungsabwicklung, da alle e-

² Kommunikationswissenschaftler von der Universität Erfurt in einem dpa-Gespräch am 30.12.2000 (<http://www.heise.de/newsticker/data/jk-30.12.00-000/>)

elektronischen Verfahren letztendlich einen realen Geldtransfer (z.B. Kreditkarte, Lastschrifteinzug) auslösen. Hier wird die gerade für Micropaymentverfahren besonders entscheidende Frage des Risikos – Zahlungsgarantie versus Stornierungsmöglichkeit – bei der Geschäftsabwicklung beantwortet. Diese klassischen Bezahlverfahren werden durch *Internet-Bezahlverfahren* für größere Geldbeträge sog. „Macropayments“ ins Internet abgebildet und greifen dabei auf kryptografische Verfahren und *Internet-Technologien* zurück. Für diesen Bereich wird in dieser Arbeit eine neuartige Technologie zur einfachen und anonymen Bereitstellung von Geldbeträgen mittels einer kartenbasierten Identifikationsnummer integriert (vgl. Kapitel 3.1), die auf die Anforderungen von Micropaymentsystemen zugeschnitten ist.

Weiterhin wird das System als adaptives und intelligentes System konzipiert, das sich auf das Kaufverhalten der Nutzer einstellt und eine autonome Preisermittlung vornimmt (vgl. Kapitel 3.3). Damit stellt es im Bereich der Micropaymentsysteme eine weitere Neuerung dar und knüpft an die nächste Entwicklungsstufe des Internets an, ein intelligentes Netz zu werden. Zur Zeit sieht sich der Nutzer vor einem unüberschaubaren Angebot an Informationen und Diensten. Er muss Mittel und Wege finden, diese zu durchdringen. Ein intelligentes Internet würde sich auf den Nutzer einstellen und autonom Aufträge ausführen. Systeme, die in der Lage sind, ihre Umgebung zu erfassen und sich an diese anzupassen, fallen in die Klasse der adaptiven Systeme. Diese sind zur Zeit Gegenstand der wissenschaftlichen Arbeit in vielen Bereichen. Eine Liste des amerikanischen Verteidigungsministeriums (DoD, Department of Defense) mit Forschungsschwerpunkten der Zukunft³ bezog sich in sieben von 15 Punkten auf adaptive Systeme. Softwarekomponenten, die diese Ansätze im Internet umsetzen, werden als intelligente Agenten bezeichnet. Das hier vorgestellte Micropaymentsystem wird als verteiltes Agentensystem konzipiert (vgl. Kapitel 3.2.1).

³ Prof. Michalewicz auf der internationalen Konferenz für "Intelligent Agents Web Technologies and Internet Commerce" im Juli 2001

2 Grundlagen

2.1.1 Prinzipien

Um den genannten Anforderungen gerecht zu werden, muss die Abwicklung und Bezahlung der Einzeltransaktionen losgelöst werden von dem realen, gebührenpflichtigen Geldfluss. Dies wird von einem Zahlungsdienstleister mit dem Prinzip der Aggregation realisiert (vgl. **Bild 2.1**).

1. Der Käufer erwirbt einen Geldbetrag, den er für Micropaymentzahlungen verwenden möchte. Dieser wird bei tokenbasierten Verfahren durch eine Wallet-Software auf dem Rechner des Käufers gespeichert. Bei notationellen Verfahren erfolgt eine zentrale Erfassung auf „Schattenkonten“. An dieser Stelle werden Macropayment-Verfahren eingesetzt.
2. Mit dem reservierten Betrag führt der Käufer Micropaymentzahlungen durch. Bei tokenbasierten Mechanismen werden die entsprechenden Münzen transferiert und bei notationellen Verfahren erfolgt eine Umbuchung zwischen den Schattenkonten.
3. Nachdem der einzelne Händler eine lohnenswerte Summe an Einzeltransaktionen gesammelt (Aggregation) hat, stößt er den realen Geldtransfer an. Hier werden wiederum Macropayment-Verfahren eingesetzt.

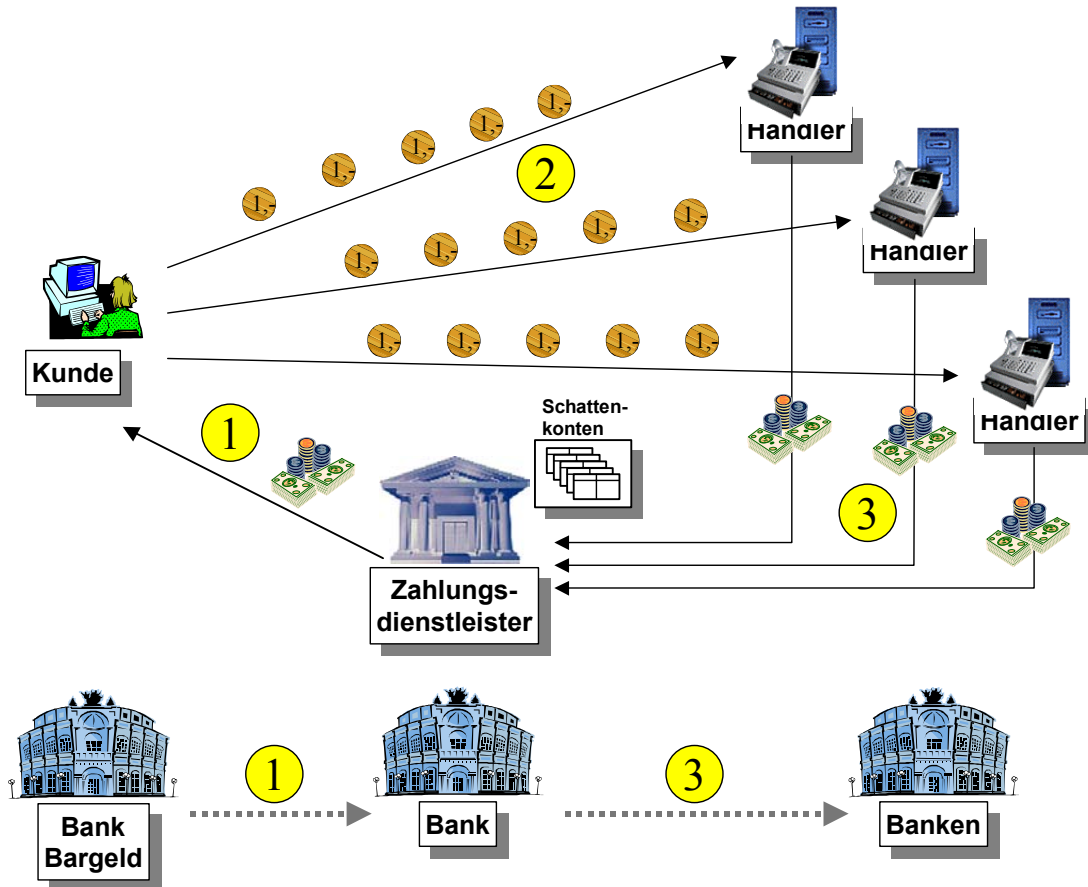


Bild 2.1: Prinzip von Micropayments

2.1.2 Stand der Wissenschaft

Zunächst wird ein kurzer Überblick über die Entwicklungen der letzten 10 Jahre gegeben, bevor auf die technischen Hintergründe der einzelnen Systeme eingegangen wird.

Tabelle 2.1: Bedeutende Schritte in der Entwicklung von Micropaymentsystemen⁴

Jahr	Micropaymentsystem	Ereignis
1993	NetCash	Vorstellung des Prototyps von Neumann und Medvinsky
1994	eCash MilliCent NetCash	Demonstration von eCash, Beginn der Pilotversuche im Internet Beginn der Forschungsarbeiten bzgl. Micropayments Testversuch auf dem Campus der University of Southern California
1995	eCash MilliCent NetCash PayMe PayWord PhoneTicks	Einführung von eCash durch die Mark Twain Bank mit US Dollar Fertigstellung der Version 1.0 Vorschlag einer überarbeiteten Version von Neumann und Medvinsky Vorschlag von Michael Pierce vom Department of Computer Science des Trinity Colleges Dublin Vorschlag von Rivest und Shamir Vorschlag von Pedersen
1996	CyberCoin Geldkarte MicroMint SubScrip	Vorstellung und Beginn von Testversuchen Erste Feldversuche in Ravensburg und Weingarten Vorschlag von Rivest und Shamir Vorschlag von Furche und Wrightson
1997	MilliCent CyberCoin	Beginn von internen Testversuchen bei Digital Equipment Corp. Markteinführung

⁴ Vgl. Sandig 1999

	IBM Micropayments Geldkarte eCash Polling	Fertigstellung der ersten Version unter dem Titel „MiniPay“ am Haifa Research Laboratory Bundesweite Markteinführung und Demonstration auf der CeBit Pilotbetrieb durch die Deutsche Bank Vorschlag von Odlyzko und Jarecki
1998	eCash MilliCent IBM Micropayments Geldkarte	Kooperation mit Banken in Österreich und der Schweiz, Ende der Zusammenarbeit mit der Mark Twain Bank Beginn des Pilotbetriebs Ausweitung des Pilotbetriebs von „MiniPay“ unter dem neuen Titel IBM Micropayments Kooperation mit VISA und dem ZKA
1999	MilliCent PayCash	Entscheidung für die Markteinführung, Lifeschaltung in Japan Öffentliche Testphase und geplante Markteinführung
2000	NET900 click&buy	Angebot eines Inkasso-Systems durch die Firma „in medias res“ in Kooperation mit der Deutschen Telekom Einführung von click&buy durch die Firma Firstgate
2001	CyberCoin eCash	Einstellung des Betriebs der Wallet-basierten Bezahlverfahren ⁵ Endgültige Einstellung des Betriebs durch die Deutsche Bank ⁶

⁵ <http://www.heise.de/newsticker/data/ad-19.12.00-000/>

⁶ <http://www.heise.de/newsticker/data/js-08.04.01-000/>

3 Konzeption eines Micropaymentsystems

3.1 Anwendung von Prepaidkarten im Internet

Der Forderung nach einer echten Zahlungsgarantie werden vorausbezahlte Systeme am besten gerecht. Der Kunde entrichtet einen Betrag im Vorhinein, der entweder tokenbasiert auf einer Chipkarte oder notationell auf einem virtuellen Konto gespeichert wird. Die Zahlungsabwicklung wird von einem vertrauenswürdigen Dritten, z.B. einer Bank oder einem Zahlungsdienstleister überwacht und durchgeführt. Die Geldflüsse werden nach einer Bestätigung durch den Kunden als endgültig betrachtet und können ohne Einwilligung des Zahlungsempfängers nicht wieder rückgängig gemacht werden. Da für die eigentlichen Zahlungstransaktionen kein Interbanken-Geldfluss angestoßen wird, beschränken sich die Kosten auf ein Minimum. Hier fällt nur die Bereitstellung der Netzwerkverbindung und Rechnerleistung ins Gewicht. Prepaid-Beträge sind entweder an Token oder nicht-namentliche Konten gebunden, so dass der Kunde vollkommen anonym bleiben kann. Prepaid-Systeme sind damit auf die Anforderungen von Micropaymentsystemen zugeschnitten.

Da tokenbasierte Prepaid-Verfahren in naher Zukunft wegen des hohen technischen Aufwandes keine große Marktdurchdringung erreichen werden, sind in dieser Arbeit nur Konzepte für notationelle Verfahren Gegenstand der Betrachtung. Kernfrage dabei ist die eindeutige Identifikation eines Schattenkontos und die anonyme Autorisierung des Zugriffs. Ein solches Konto wird mit einer eindeutigen Kontonummer identifiziert und mit einem festen Startbetrag bereitgestellt. Der Kunde erwirbt gegen Barzahlung Zugriff auf diese Kontonummer und kann über den Betrag verfügen. Verschiedene Mechanismen erlauben eine Autorisierung für einen Zugriff auf das Konto:

- Autorisierung über die Kontonummer
- Autorisierung über User-ID und Passwort
- Autorisierung über die Uhrzeit und einen privaten Schlüssel
- Autorisierung mit sicherer Verschlüsselung des Abbuchungsbetrages

3.2 Architektur zur Einzeltransaktionsabwicklung

3.2.1 Problemlösung mit Softwareagenten

Bei der Transaktionsabwicklung von Micropaymentsystemen muss ein Kompromiss zwischen den folgenden divergierenden Forderungen gefunden werden:

- Es wird eine hohe *Effizienz* gefordert, die den Kommunikationsaufwand pro Einzeltransaktion möglichst begrenzt. Ziel ist, den Aufwand auf die Kommunikation zwischen Kunde und Händler zu beschränken, ohne den Zahlungsdienstleister zu kontaktieren.
- Es wird eine hohe *Zahlungssicherheit* gefordert, die wiederum verlangt, dass der Zahlungsdienstleister als Verwalter der Schattenkonten einbezogen wird.

Gelöst werden kann dieses Problem, indem der Zahlungsdienstleister einen Softwareagenten bereitstellt, der in seinem Auftrag die Zahlungsabwicklung beim Händler vornimmt. So wird der Transaktionsaufwand minimiert und trotzdem verbleibt die Kontrolle über die Zahlungsabwicklung beim Dienstleister als vertrauenswürdigen Dritten.

3.2.2 Agentenbasierte Architektur

Bild 3.1 stellt dar, wie die dargestellten Komponenten um ein System von kooperierenden Agenten erweitert werden. Auf der Seite des Kunden ist dabei keinerlei zusätzliche Installation notwendig. Das Micropaymentsystem ist damit von jedem beliebigen Browser nutzbar.

Auf der Seite des Händlers werden fünf Agenten eingerichtet, die in keiner Weise in die bestehende Webserver-Architektur eingreifen, sondern einfach in den Kommunikationsweg zwischen Kundenbrowser und Webserver gelegt werden (Proxyfunktionalität). Die Migration ist damit für den Händler unkompliziert.

- **Proxy-Agent**
- **Authentication- und Billing-Agent**
- **Pricing-Agent**
- **Configuration-Agent**
- **Security-Agent**

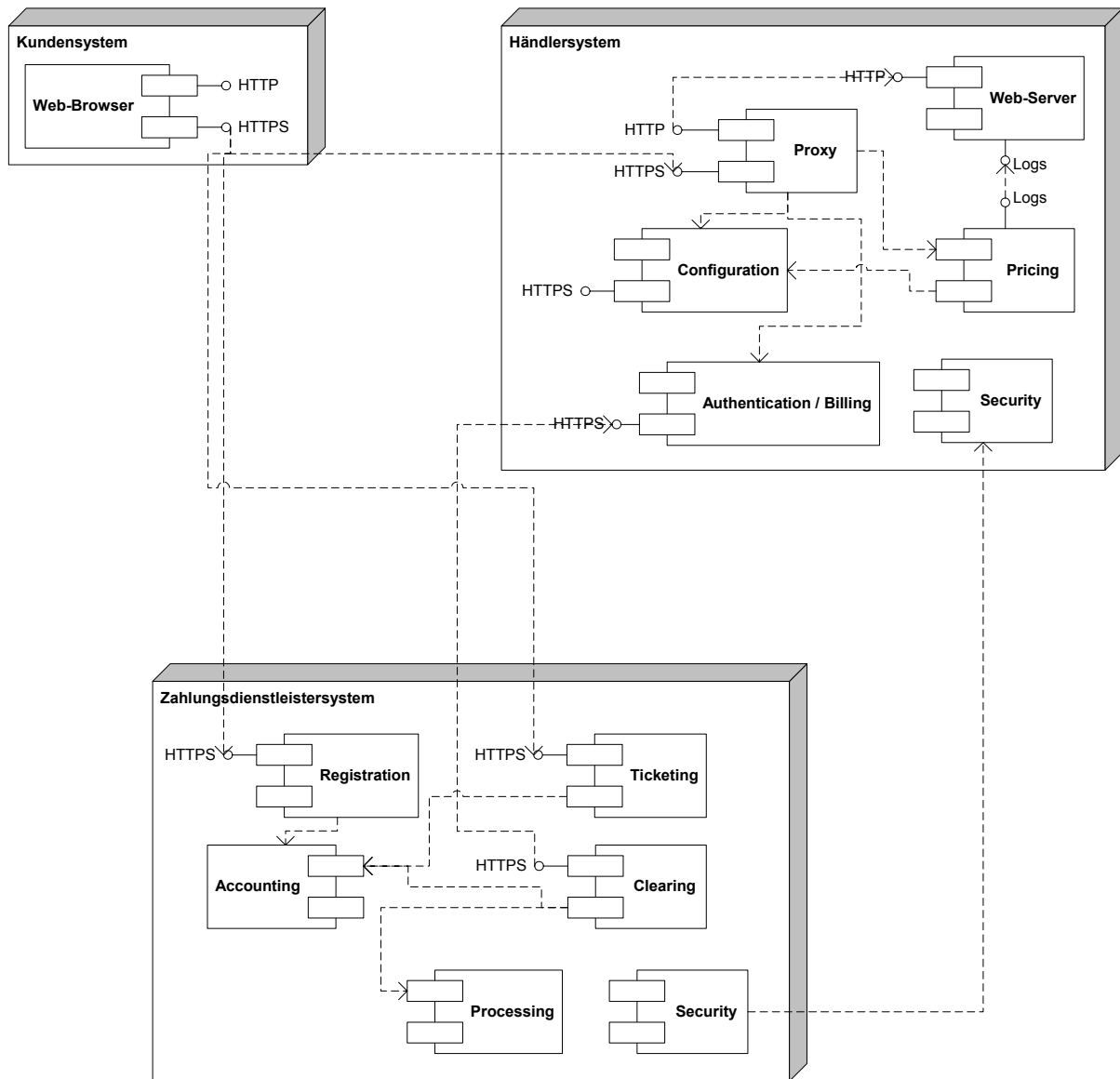


Bild 3.1: Struktur von kooperativen Agenten

Der Zahlungsdienstleister stellt serverbasierte Agenten bereit, die zwischen Kunde und Händler vermitteln und die eigentliche Zahlungsabwicklung vornehmen.

- **Accounting-Agent**
- **Registration-Agent**
- **Ticketing-Agent**
- **Clearing-Agent**
- **Processing-Agent**
- **Security-Agent**

3.3 Konzept für eine dynamische Preisbestimmung

Während bei den bisher vorgestellten Agenten der Aspekt der Kooperation im Vordergrund steht, ist der Pricing-Agent ein intelligenter Agent (vgl. Kapitel 3.2.1). Er gehört nicht zu den Kernkomponenten (vgl. **Bild 3.2**), d.h. er ist nicht notwendig für die Abwicklung des eigentlichen Micropaymentprozesses oder die Bedienung des Systems. Auch der sichere Betrieb ist ohne ihn möglich. Er stellt vielmehr einen Mehrwertdienst bereit, der dem Händler einen deutlichen Vorteil bei der Vermarktung seiner Inhalte ermöglicht.

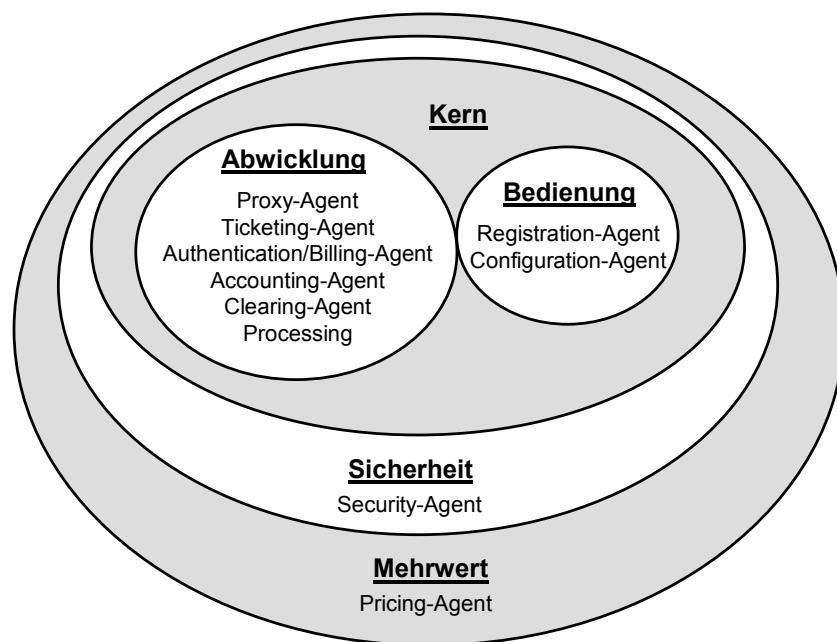


Bild 3.2: Kategorisierung der eingesetzten Agenten

Das Geschäftsziel des Händlers ist, seine Inhalte (content) an möglichst viele Kunden zu verkaufen und dabei seinen Umsatz (U) zu optimieren. Darauf haben die Anzahl der Verkaufstransaktionen (v) und der Preis (P) Einfluss. Wird der Preis statisch festgelegt ($P=const$), ist der Umsatz einzig von der Anzahl an Verkäufen abhängig:

$$U(v) = P \cdot v \quad (3.1)$$

Außer seinem Marketing hat der Händler in diesem Fall keine Instrumente zur Optimierung des Umsatzes. An diesem Punkt setzt die dynamische Festlegung des Preises (P_i) an, die autonom vom Pricing-Agent vorgenommen wird. Der Händler erhält ein Instrument zur Beeinflussung seines Umsatzes.

$$U(P_1, \dots, P_v) = \sum_{i=1}^v P_i \quad (3.2)$$

Der Preis wird in der realen Welt, insbesondere beim Rohstoffhandel, durch das Zusammenspiel von „Angebot und Nachfrage“ bestimmt. Die Menge der angebotenen Güter im Verhältnis zur Menge der Nachfrage führt zu einem sich dynamisch anpassenden Preis (vgl. **Bild 3.3**). Bei virtuellen Gütern ist die Menge des Angebots aufgrund der Möglichkeit zur beliebigen Vervielfältigung unbegrenzt. Aufgrund der fehlenden Knappheit spricht man auch von der „Umkehr der Marktlogik“. Die Angebotsmenge ist nicht mehr entscheidend für die Preisentwicklung, sondern die Qualität des Produktes. Diese wird gerade im „Content-Business“ durch den Hauptfaktor „Aktualität des Inhaltes“ (vgl. **Bild 3.4**) bestimmt. Beispiele sind: Börseninformationen, Nachrichten, Downloads, Warentests, Online-Bücher usw. Allen ist gemeinsam, dass mit dem Alter des Inhaltes auch der Wert sinkt. Bei statischen Preisen wird schnell der Zeitpunkt erreicht, an dem der Wert des Inhalts unter dem angebotenen Preis liegt und die Nachfrage abbricht. Eine adaptive Preisermittlung kann die Nachfrage über einen längeren Zeitraum aufrecht erhalten.

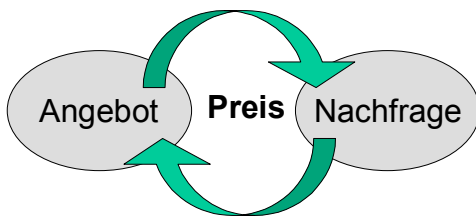


Bild 3.3: Preisbestimmung bei realen Produkten

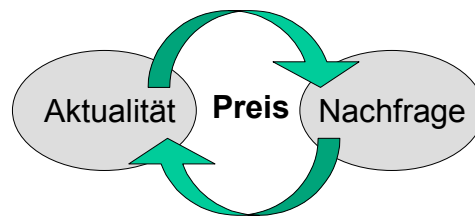


Bild 3.4: Preisbestimmung bei virtuellen Produkten

Der Pricing-Agent hat damit die folgenden Ein- und Ausgangsgrößen (vgl. **Bild 3.5**):

- Das **Alter des Inhalts** wird aus der Differenz zwischen dem Bereitstellungszeitpunkt und der aktuellen Zeit ermittelt. Der Betrachtungszeitraum ist dabei abhängig von der Produktgruppe. Bei Börseninformationen ist dieser z.B. kürzer als bei Warentests.
- Die **Nachfrage** nach einem bestimmten Inhalt kann zum einen unmittelbar von dem Proxy-Agent ermittelt werden. Da er alle Anfragen vermittelt, stehen ihm die

Daten zur Verfügung. Zum anderen ist es auch möglich, die Daten aus den Logfiles des Händlerwebserverns zu generieren. Hier werden die Zugriffe auf jede einzelne Datei inklusive der Zeitpunkte erfasst. Nachfrage (*Nfr*) heißt in diesem Fall: Anzahl Zugriff (*N*) pro Zeitraum (Δt).

$$Nfr = \frac{N}{\Delta t} \quad (3.3)$$

Auch hier ist der Zeitraum von der Produktgruppe abhängig und korreliert mit dem Betrachtungszeitraum für das Alter des Inhaltes.

Die Nachfrageprofile und Regeln des Händlers werden in den folgenden Kapiteln vorgestellt.

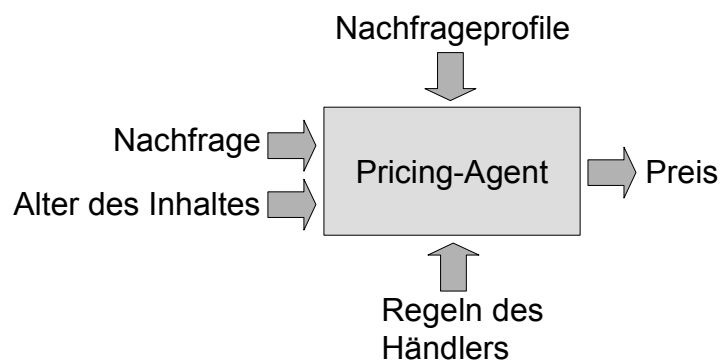


Bild 3.5: Ein- und Ausgangsgrößen des Pricing-Agent

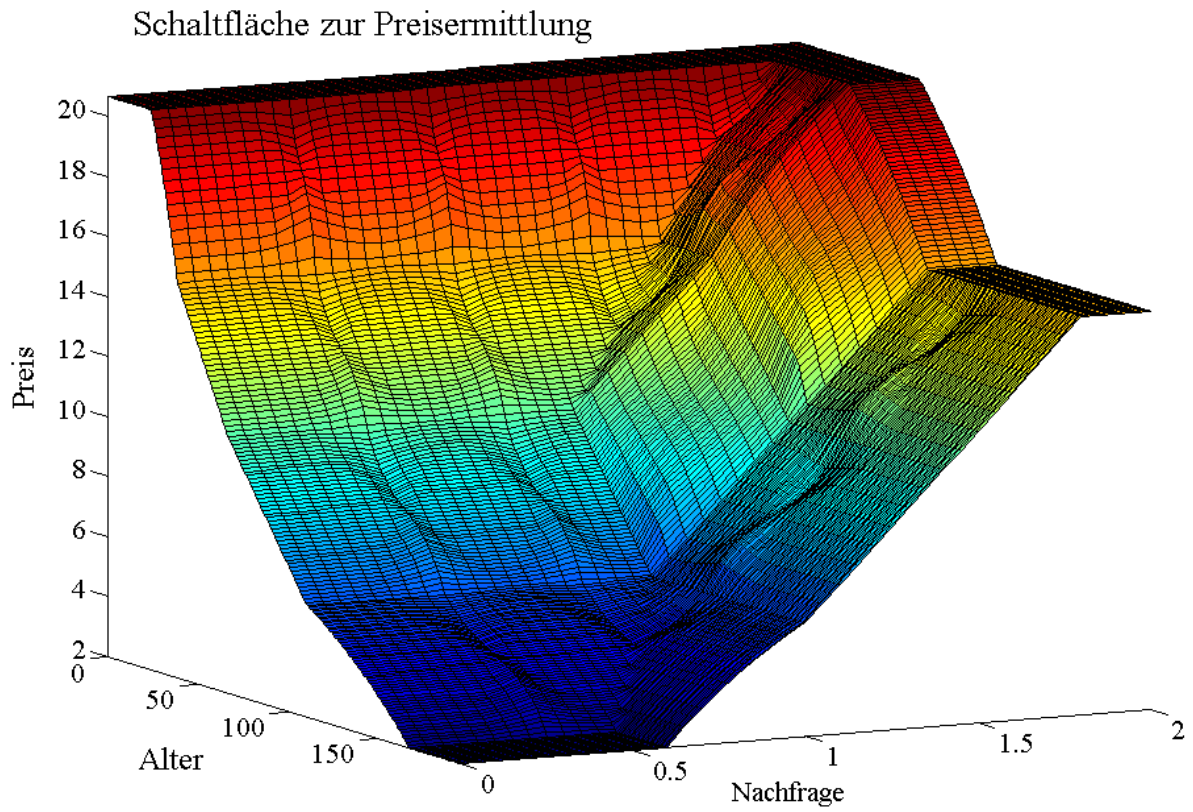


Bild 3.6: Schaltfläche zur Ermittlung des Preises

4 Zusammenfassung und Ausblick

Die Bedeutung des Internets als Plattform für die internationale Geschäftsabwicklung ist in den letzten Jahren stark gestiegen. Es wird erwartet, dass hier in Zukunft ein weiteres erhebliches Entwicklungspotential besteht. Damit steigen auch die Anforderungen an die Online-Zahlungsabwicklung als integrativer Bestandteil eines Geschäftsprozesses. Bisher eingesetzte Technologien basieren im Wesentlichen auf „klassischen“ Bezahlverfahren. Bekannte und erprobte Zahlungsmechanismen werden aus der realen Welt in die virtuelle Welt transferiert. Insbesondere Kredit- und Debittransaktionen haben neben der reinen Rechnungsstellung einen hohen Marktanteil. Wegen der relativ hohen Transaktionsgebühren sind diese Verfahren für Güter im mittleren Preissegment geeignet. In den meisten Fällen handelt es sich bei dem Handelsgegenstand um Waren, die über Lieferanten zugestellt werden.

Das Internet hat einen weiteren Markt geschaffen, der kein vergleichbares Ebenbild in der realen Welt hat. Die Nachfrage nach hochwertigen Informationen und elektronischen Dienstleistungen gewinnt in der wachsenden Flut an Daten eine immer größere Bedeutung. Da die kostendeckende Finanzierung des Angebots über Werbeeinnahmen nur zum Teil möglich ist, werden Mechanismen zur Bezahlung von niedrigpreisigen virtuellen Gütern gefordert. Es muss eine Technologie bereitgestellt werden, um eine große Anzahl an Einzeltransaktionen im Centbereich oder darunter abzuwickeln. Das Kernkonzept zur Vermeidung von kostenintensiven Banktransaktionen besteht darin, Transaktionen zu aggregieren, die dann in Summe profitabel abgerechnet werden. Die verschiedenen Ansätze aus dem wissenschaftlichen und kommerziellen Bereich wurden in dieser Arbeit diskutiert.

Die vorgestellten tokenbasierten Verfahren basieren auf kryptografisch sehr ausgefeilten Ideen und lassen sich effizient umsetzen. Sie haben jedoch nicht den Sprung aus dem wissenschaftlichen Umfeld heraus in den kommerziellen Einsatz geschafft. eCash wurde von einigen Banken angeboten, ist aber wegen der mangelnden Akzeptanz wieder vom Markt genommen worden. Gründe dafür sind, dass der Einsatz eine spezielle Software beim Nutzer erfordert und die Speicherung von Geldwerten auf dem Rechner Unbehagen erzeugt.

Notationelle Ansätze sind hier vielversprechender, da die Verwaltung der Geldwerte auf virtuellen Konten zentral beim Zahlungsdienstleister erfolgt. IBM hat ein ausgereiftes System entwickelt, das aber technologisch noch zu aufwändig ist, um vom Markt akzeptiert zu werden. Das einzige produktiv erfolgreiche System wird in Deutschland von Firstgate bereitgestellt. Inkassosysteme nutzen mit der Telefonrechnung zwar einen bekannten Zahlungsweg, schränken aber mit der Bindung an einen Telefonanschluss die Mobilität des Nutzers ein.

In dieser Arbeit wurde ein Konzept vorgestellt, das auf einer ganzheitlichen Betrachtung basiert. Neben der technischen Abwicklung der Einzeltransaktionen, wurden auch neuartige Konzepte zur Durchführung der Macropaymentzahlung zum Aufladen der virtuellen Konten vorgestellt. Es wurde ein skalierbares Modell zur Zahlungsabwicklung über Prepaidkarten entworfen. Der Zugriff auf das virtuelle Prepaidkartenkonto kann in vier Stufen autorisiert werden. Hier bietet besonders die Autorisierung mit sicherer Verschlüsselung des Abbuchungsbetrags eine hohe transparente Sicherheit. Dieses Verfahren ist in der Form neu.

Grundlage für die Durchführung der Einzeltransaktionen sind bekannte kryptografische Verfahren, die in geeigneter Weise kombiniert werden. Die Authentifikation des Kunden erfolgt über virtuelle Tickets, die über Standard-HTTP-Mechanismen übergeben werden. So kann dieses Konzept vom Kunden ohne jeglichen technischen Aufwand eingesetzt werden und bietet trotzdem eine hohe Sicherheit. Der neuartige agentenbasierte Ansatz mit Proxy-Technologie fordert vom Händler einen sehr geringen Implementierungsaufwand. Das System arbeitet autonom losgelöst vom Webserver. Die Preisermittlung über einen intelligenten Agenten stellt eine weitere Besonderheit des vorgestellten Konzepts dar und gibt dem Händler ein Instrument in die Hand, um den Umsatz mit seinem Online-Angebot zu optimieren.

Das Kernsystem wurde zunächst an einem Prototypen validiert. Der nächste Schritt ist die Implementierung bei einem realen Content-Provider, um Detailprobleme zu erkennen und zu beheben. Insbesondere ist interessant, das Modell zur Preisbestimmung über die Simulation hinaus anhand von realen Nachfrageverläufen zu verfeinern. Die gesammelten Daten würden die Grundlage bilden, um das Kaufverhalten für Micropayment-Geschäftsprozesse zu modellieren. Dies ist bisher nicht möglich, da die vorgestellte Architektur in der Praxis nicht existiert und keine Datenbestände vorliegen.

Nach einer erfolgreichen Markteinführung des Prepaidkartensystems ist der nächste Schritt, Mechanismen zum Aufladen von vorhandenen Prepaid-Konten zu entwickeln. Dabei kommen nur Varianten in Frage, die den Hauptvorteil der Prepaidkarte die Zahlungsgarantie nicht untergraben.

- Die einzige Möglichkeit, um auch die Anonymität zu wahren, ist eine Bareinzahlung bei einer Bank auf das virtuelle Konto. Dem Kunden entstehen dabei allerdings unnötige Bareinzahlungsgebühren, so dass kein Vorteil gegenüber dem Kauf einer neuen Prepaidkarte entsteht.

- Die direkte Überweisung würde die Anonymität einschränken, könnte aber internetbasiert über HBCI (Homebanking Connection Interface) oder PIN/TAN-Mechanismen erfolgen. Mit HomePay⁷ und Stackbox⁸ sind weiterhin Produkte auf dem Markt, um Überweisungen direkt vom Paymentprovider zu inszenieren. Die Zahlungsgarantie bliebe erhalten und beim Kunden erfolgt kein Medienbruch, um einen weiteren Betrag auf dem Prepaid-Konto bereitzustellen.

Wie sieht die Zukunft von Micropaymentsystemen aus? Das Wachstumspotential ist groß und ein Durchbruch wird mittelfristig erfolgen. Immer mehr Content-Provider bieten hochwertige Dienste mit einem Alleinstellungsmerkmal an. Vorsichtige Prognosen⁹ gehen davon aus, dass in Zukunft Internetangebote neben der Werbefinanzierung zu einem Anteil von 10%-30% durch den Nutzer bezahlt werden. Während rein journalistische Anbieter wie z.B. „Der Spiegel“ noch Probleme haben, eine große Benutzergruppe mit ihren kostenpflichtigen Inhalten zu erreichen, haben andere Anbieter wie z.B. Stiftung Warentest¹⁰ mit ihrer elektronischen Dienstleistung bereits Umsätze von mehreren 10.000 € pro Monat erreicht. Weitere Beispiele für Anbieter sind FUNCARD¹¹, Börseninformationen¹² und Schwacke¹³. Mit steigender Qualität der Online-Angebote wird ein echter Markt für Micropaymentsysteme entstehen. Die Güte muss für den Nutzer bereits vor dem Kauf ersichtlich sein. Er sieht sich zur Zeit vielfach einem „markt of lemons“ gegenüber. Erst beim Kauf des Inhalts wird die Qualität ersichtlich. Hier wird von den Content-Providern immer mehr Transparenz geschaffen, so dass zwar kein boomartiges, aber ein stetiges Wachstum zu erwarten ist.

⁷ <http://www.fun.de/deutsch/produkte/internetpayment/homepay.htm>

⁸ <http://www.stackbox.com/>

⁹ Fachtagung am 14.5.2002 von New Media Sales in Hamburg

¹⁰ <http://www.warentest.de/>

¹¹ <http://www.funcard.de/>

¹² <http://onvista.imbp.de/ovsm/>

¹³ <http://www.schwacke.com/>

5 Literaturverzeichnis

5.1 Monografien

- BARTHOLOMÉ, A.; RUNG, J.; KERN, H.: *Zahlentheorie für Einsteiger*. Braunschweig: Vieweg-Verlag, 2001 – ISBN: 3-528-36680-X
- BOGER, M.: *Java in verteilten Systemen*. Heidelberg: dpunkt-Verlag, 1999 – ISBN: 3-932-58832-0
- BUCHMANN, J. : *Einführung in die Kryptographie*, Berlin: Springer-Verlag, 2001 – ISBN: 3-540-41283-2
- CONALLEN, J.: *Building Web Applications with UML*. München: Addison-Wesley, 1999 – ISBN: 0201730383
- DAEMEN, J.; RIJMEN, V.: *The Design of Rijndael. The Wide Trail Strategy*. Berlin: Springer, 2001 – ISBN: 3540425802
- FUMY, W.; RIEß, H.-P.: *Kryptographie - Entwurf, Einsatz und Analyse symmetrischer Kryptoverfahren*. Oldenbourg: München, 1994 – ISBN: 3486222139
- HAFNER, K.; LYON, M.: *ARPA Kadabra oder Die Geschichte des Internet*. Heidelberg: dpunkt-Verlag, 2000 – ISBN: 3932588592
- KAHLERT, J.; FRANK, H.: *Fuzzy-Logic und Fuzzy-Control*. Braunschweig: Vieweg-Verlag, 1993 – ISBN: 3-528-15304-0
- KNUDSEN, J.: *JAVA Cryptography*. O'Reilly, 1998 – ISBN: 1565924029
- MENEZES, A.: *Elliptic Curve Public Key Cryptosystems*, Boston: Kluwer, 1993 – ISBN: 0792393686
- MÜLLER, G.; REICHENBACH, M.: *Sicherheitskonzepte für das Internet*. Berlin: Springer-Verlag, 2001 – ISBN: 3540417036
- O'MAHONY, D.; PEIRCE, M.; TEWARI, H.: *Electronic Payment Systems for E-Commerce*, London: Artech House, 2001 – ISBN: 1580532683
- OESTEREICH, B.: *Objektorientierte Softwareentwicklung*. Wien: Oldenbourg, 1999 – ISBN: 3486255738
- ROSCOE, B.; LOWE, G.; GOLDSMITH, M.; RYAN, P.; SCHNEIDER, S.: *Modelling and Analysis of Security Protocols*. Addison-Wesley, 2000 – ISBN: 0201674718
- SCHMEH, KLAUS: *Kryptografie und Public- Key Infrastrukturen im Internet*. Heidelberg: dpunkt-Verlag, 2001 – ISBN: 3932588908

- SCHNEIER, B.: *Angewandte Kryptographie*. Bonn: Addison-Wesley, 1996 – ISBN: 3893198547
- SCHNEIER, B.: *The Twofish Encryption Algorithm*. John Wiley & Sons, 1999 – ISBN: 0471353817
- STALLINGS, W.: *Cryptography and Network Security*, Upper Saddle River: Prentice Hall, 1999 – ISBN: 0130914290

5.2 Konferenzbände, Zeitschriften

- BRAND, J.: Zero-Knowledge Authentication Scheme with Secret Key Exchange. In: *Journal of Cryptology*, No. 11 (1998). Berlin: Springer Verlag – ISSN: 0933-2790
- BUCHMANN, J.: Faktorisierung großer Zahlen. In: *Spektrum der Wissenschaft*, No. 9 (1996). Heidelberg: Verlagsgesellschaft Spektrum der Wissenschaft – ISSN: 0170-2971
- CHAUM, D.: Blind Signatures for Untraceable Payments. In: *Advances in Cryptology* (1982). New York, London: Plenum Press – ISBN: 3540650695
- DAEMEN, J.; RIJMEN, V.: The Block Cipher Rijndael. In: *Smart Card Research and Applications* (2000), Quisquater, J.-J. (Hrsg.); Schneier, B. (Hrsg.). Heidelberg: Springer-Verlag – ISBN: 3540679235
- DOBBERTIN, H.: The First Two Rounds of MD4 are Not One-Way. In: *Fast Software Encryption*, Lecture Notes in Computer Science, Vol. 1372, Springer, 1998 – ISBN: 3-540-64265-X
- FRANK, G.; HEITMANN, A.: Internet Payments in Germany: A Classification. In: *Conference on Telecommunications and Information Markets* (2001). Karlsruhe – ISBN: 0-965440-2-6
- FRANKLIN, S.; GRAESSER, A.: Is it an agent or just a program? A taxonomy for autonomous agents. In: *Third International Workshop on Agent Theories, Architectures and Languages* (1996), Berlin: Springer – ISBN: 3-540-62507-0
- FURCHE, A.; WRIGHTSON, G.: SubScrip - An efficient protocol for pay-per-view payments on the internet. In: *Proc. 5th international Conference on Computer Communications and Networks* (1996). IEEE – ISBN: 0818677228 Rockville
- GABBER, E.; SILBERSCHATZ, A.: Agora: A Minimal Distributed Protocol for Electronic Commerce. In: *Proceedings of the Second USENIX Workshop on Electronic Commerce* (1996). Oakland, CA – ISBN: 1-88044-683-9

- GOLDWASSER, S.; MICALI, S.; RACKO, C.: The Knowledge Complexity of Interactive Proof Systems. In: *17th Annual Symposium on Theory of Computing* (1985). Providence, USA – ISBN: 0897911512
- HERZBERG, A.; SARIG, A.; YOCHAI, H.: Secure Payments in Java: MiniPay and JECF. In: *International Workshop on Security and Efficiency Aspects of Java* (1997). Eilat, Israel – ISBN: 0818677589
- HERZBERG, A.; YOCHAI, H.: Mini-Pay Charging per Click on the Web. In: *Sixth World Wide Web Conference* (1997). Santa Clara, California – ISBN: 0-9657614-0-1
- JUTLA, C.; YUNG, M.: PayTree: Amortized-Signature for Flexible Micropayments. In: *2nd USENIX Workshop on Electronic Commerce* (1996). Oakland – ISBN: 1-88044-683-9
- KOBLITZ, N.: The State of Elliptic Curve Cryptography. In: *Designs, Codes and Cryptography, No. 19* (2000). Boston: Kluwer Academic Publishers – ISSN: 0925-1022
- KOLBERG, B.; SCHARMACHER, T.: *Logistik- und Payment-Dienstleistungen für Online-Handelsunternehmen*. Köln: Institut für Handelsforschung der Universität Köln, 2001 – ISBN: 3-935546-07-6
- LAI, X.; MASSEY, J.; MURPHY, S.: Markov Ciphers and Differential Cryptanalysis. In: *Advances in Cryptology--EUROCRYPT '91 Proceedings* (1991), Berlin: Springer-Verlag – ISBN: 3-540-54620-0
- LEIBOLD, K.; STROBORN, K.: The Customers' Acceptance of Internet Payment Systems in Germany - An Empirical Analysis. In: *Conference on Telecommunications and Information Markets* (2001). Karlsruhe – ISBN: 0-965440-2-6
- LENORD, M.; NISBACH, T.: Allcash Internet Payment System. In: *E-Commerce und E-Payment. Rahmenbedingungen, Infrastruktur, Perspektiven* (2001). Teichmann (Hrsg.), Wiesbaden: Gabler – ISBN: 3-40911-805-5
- LENORD, M.; NISBACH, T.: Internet-Zahlungssysteme aus Sicht des Dienstleisters. In: *Handbuch ePayment - Zahlungsverkehr im Internet: Systeme, Trends und Perspektiven* (2001). Ketterer (Hrsg.), Stroborn (Hrsg.), Fachverlag Deutscher Wirtschaftsdienst – ISBN: 3-87156-463-X
- LENORD, M.; NISBACH, T.: Prepaid-Payment-Solutions for Micropayments from a Technical Point of View. In: *International Conference on Intelligent Agents, Web Technologies and Internet Commerce* (2001). Las Vegas – ISBN: 0-858-89848-9

- LENORD, M.; NISBACH, T.: Prepaid-Payment-Solutions for Micropayments. In: *Conference on Telecommunications and Information Markets* (2001). Karlsruhe – ISBN: 0-965440-2-6
- MEDVINSKY, M.; NEUMAN, C.B.: NetCash: A design for practical electronic currency on the Internet. In: *ACM Conference on Computer and Communication Security* (1993). Fairfax, VA – ISBN: 0-89791-629-8
- NWANA, H.-S.: Software agents: An overview. In: *The Knowledge Engineering Review 11 No 3* (1996). Cambridge University Press – ISSN: 0269-8889
- PAYBOX.NET: Mobile Payments - From e-commerce to m-commerce. In: *Conference on Telecommunications and Information Markets* (2001). Karlsruhe – ISBN: 0-965440-2-6
- PEIRCE, M.; O'MAHONY, D.: PayMe. In: *4th International World Wide Web Conference* (1995). Boston – ISSN: 1085-2301
- PENG, Y.; HOLDING, D.J.; BLOW, K.J.: A Possible Secure Solution for Mobile Agents. In: *International Conference on Intelligent Agents, Web Technologies and Internet Commerce* (2001). Las Vegas – ISBN: 0-858-89848-9
- SANDIG, KAI: Die Geschichte des virtuellen Geldes. In: *Bezahlsysteme im Internet*. Frankfurt: Verlag Fritz Knapp, 1999 – ISBN: 3781906426
- TYGAR, D.; CAMP, L.; SIRBU, M.: Token and notational money in electronic commerce. In: *Proceedings of the 1st USENIX Workshop on Electronic Commerce* (1995). New York – ISBN: 188044674X
- WOOLDRIDGE, J.; JENNINGS, N.-R.: Intelligent agents. In: *The Knowledge Engineering Review 10 (2)* (1995) – ISSN: 0269-8889
- YEN, S.; HO, L.; HUANG, C.: Internet Micropayment Based on Unbalanced One-Way Binary Tree. In: *International Workshop on Cryptographic Techniques and E-Commerce* (1999). Hong Kong – ISBN: 962-937-049-2
- ZADEH, L.-A.: Toward an Enlargement of the Role of Natural Languages in Information Processing, Decision and Control. In: *International Conference on Intelligent Agents, Web Technologies and Internet Commerce* (2001). Las Vegas – ISBN: 0-858-89848-9

5.3 Hochschulschriften

- DIPPEL, A.-K.: *Authentication of Computer Communications*. Indiana University, Department of Computer Science, 1996 – URL: <http://www.cs.indiana.edu/>

- JARECKI, S.; ODLYZKO, A.: *An efficient micropayment system based on probabilistic polling*. MIT Laboratory for Computer Science, 1997 – URL: <http://www.lcs.mit.edu/>
- KÖNIGSBÜSCHER, M.: *Bestimmung des Status-Quo und Einschätzung der zukünftigen Entwicklung von Zahlungssystemen für Kleinbeträge (Micropayments) im Internet*. Diplomarbeit an der Gerhard-Mercator-Universität Duisburg am Institut für Informationstechnik, 2000 – URL: <http://iit.uni-duisburg.de/>
- WHEELER, D.: *Transactions using Bets*. England, University of Cambridge, Computer Laboratory, 1996 – URL: <http://www.cl.cam.ac.uk/>

5.4 Firmenschriften

- BITKOM. *Bericht zum Jahr 2002 des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V.* – URL: <http://www.bitkom.net/>
- CYBERCASH. *Das CyberCash-System im Überblick*. CyberCash GmbH, 1999 – White Paper, URL: <http://www.cybercash.de/>
- EUROPEAN MONETARY INSTITUTE: *Report of the Working Group on EU Payment Systems*, Frankfurt, 1993 – URL: <http://www.ecb.int/emi/emi01.htm>
- FIRSTGATE: *FIRSTGATE click&buy Das Payment System für das stationäre und mobile Internet*. Firstgate GmbH, 2001 – White Paper, Version 1.0, URL: <http://www.firstgate.de/>
- GFK MEDIENFORSCHUNG: *7. GFK Studien: GFK-Online-Monitor 2001* – URL <http://www.gfk.de/>
- GLASSMAN, S.; MANASSE, M.; ABADI, M.; GAUTHIER, P.; SOBALVARRO, P.: *The MilliCent Protocol for Inexpensive Electronic Commerce*. Digital Equipment Corporation, Systems Research Center, 1995 – Firmenschrift, URL: <http://www.digital.com/>
- IN MEDIAS RES: *NET900 - Technische Erläuterung*. IN MEDIAS RES Gesellschaft für Kommunikationstechnologien mbH, 2001 – Firmenschrift, URL: <http://www.in-medias-res.de/>
- INFIN: *Infin-Micropayments*. Ingenieurgesellschaft für Informationstechnologien mbH & Co. KG, 2001 – Firmenschrift, URL: <http://www.infin.de/>
- KOCKER, P.; FREIER, A.; KARLTON, P.: *The SSL Protocol Version 3.0*. Netscape Communications Corporation, 1996 – Firmenschrift, URL: <http://www.netscape.de/>
- KPN: *SwitchPoint*. KPN Multimedia Services Den Haag, 2001 – White Paper, URL: <http://www.kpn.com/>

- MASTERCARD AND VISA COOPERATIONS: *Secure Electronic Transaction Specification - Book3: Formal Protocol Definition*. Mastercard und VISA 1997 – Firmenschrift, URL: <http://www.setco.org/>
- PEDERSEN, T.: *Electronic Payments of Small Amounts*. Cryptomathic A/S, Dänemark, 1997 – Firmenschrift, URL: <http://www.cryptomathic.com/>
- RIVEST, R.; SHAMIR, A.: PayWord and MicroMint: Two simple micropayment schemes. In: *CryptoBytes, volume 2, number 1* (1996) – Technical newsletter of RSA laboratories, URL: <http://www.rsasecurity.com/>
- SETCo: *SET Secure Electronic Transaction Specification - Formal Protocol Definition*. SETCo 1997 – URL: <http://www.setco.org/>
- SYMPOSION PUBLISHING: *Internetshopping Report 2001. Käufer, Produkte, Zukunftsaussichten, Studie*. Düsseldorf, 2001 – URL: <http://www.symposion.de/>
- WAYNER, P.: Digital Cash. In: *Byte, Vol. 19, No. 10* (1994) – URL: <http://www.byte.com/>

5.5 Normen, Internetstandards und Patente

- AMERICAN NATIONAL STANDARDS INSTITUTE X3.92: *Triple-DES*
- FEDERAL INFORMATION PROCESSING STANDARD 180: *Secure Hash Standard*
- FEDERAL INFORMATION PROCESSING STANDARD 180-2: *Secure Hash Standard*
- FEDERAL INFORMATION PROCESSING STANDARD 46-2: *Data Encryption Standard*
- ISO/IEC IS 9594-2: *Information Technology - Open System Interconnection - The Directory: The Models*
- RFC 1320: *The MD4 Message Digest Algorithm*
- RFC 1321: *The MD5 Message Digest Algorithm*
- RFC 1898: *CyberCash Credit Card Protocol Version 0.8*
- RFC 2068: *Hypertext Transfer Protocol – HTTP/1.1*
- RFC 2246: *The TLS Protocol Version 1.0*
- RFC 2396: *Uniform Resource Identifiers*
- RFC 2459: *Internet X.509 Public Key Infrastructure - Certificate and CRL Profile*
- RFC 2617: *HTTP Authentication: Basic and Digest Access Authentication*
- U.S. PATENT 5,214,703: *Device for the Conversion of a Digital Block and Use of Same*. Massey, J.-L.; Lai. X., 25 May 1993

W3C. *Micro Payment Transfer Protocol (MPTP) Version 0.1*. World Wide Web Consortium Working Draft, 1995

Lebenslauf des Verfassers

Matthias Lenord

mti@lenord.net

<http://www.lenord.net/>



Okt. 89 - Feb. 95	Studium der Elektrotechnik an der Gerhard-Mercator-Universität Duisburg mit dem Abschluss Diplom-Ingenieur, Auszeichnung mit dem VDE-Blumenbecker-Preis
Okt. 93 - Dez. 94	studentische Hilfskraft im Fachgebiet Nachrichtentechnik an der Universität Duisburg, Softwareentwicklung für Parallelrechner
Apr. 95 - Sep. 96	Tätigkeit im selbstgegründeten Ingenieurbüro "Nisbach + Lenord", Design und Entwicklung von Software für die Automatisierungs- und Kommunikationstechnik
Okt. 96 - Dez. 97	wissenschaftlicher Mitarbeiter im Fachgebiet Datenverarbeitung an der Universität Duisburg mit dem Thema: „Sichere Kommunikationsabwicklung in komplexen, mechatronischen Systemen“
Jan. 98 - Dez. 00	Systemingenieur im Sonderforschungsbereich 291 der Universität Duisburg in den Fachgebieten Technische Informatik und Mechatronik in den Arbeitsbereichen Schwerlastrobotik und Internet-Technologien für Ingenieure
Jan. 01 - Okt. 02	Projektleiter bei der Firma Allcash GmbH auf dem Gebiet des eCommerce und der elektronischen Zahlungsabwicklung
seit Nov. 02	Projektleiter bei der Firma Siemens AG, Automation & Drives, Motion Control im Bereich der Antriebskommunikation