Elektronische Zahlungsmechanismen im Überblick

Andreas Hitzbleck[1] · Detlef Hühnlein[2]

[1]Mühlbergstraße 1, 82319 Starnberg,
andreas@hitzbleck.com

[2]secunet AG, Sudetenstraße 16, 96247 Michelau,
huehnlein@secunet.de

Zusammenfassung

Diese Arbeit liefert einen aktuellen Überblick über die zur Zeit, bzw. möglicherweise in Zukunft, im deutschsprachigen Raum eingesetzten elektronischen Zahlungsmechanismen. Neben wirtschaftlichen Überlegungen werden insbesondere auch die Sicherheitsaspekte der einzelnen Verfahren beleuchtet.

1 Einleitung

Beim immer populärer werdenden elektronischen Handel von Waren und Dienstleistungen – z.B. im Internet – ist es nötig, Mechanismen für die elektronische Abwicklung der Zahlungsvorgänge zur Verfgung zu stellen. Eine besondere Herausforderung stellen hierbei Zahlungen zwischen Endkunden und Händlern dar, da hier oft keine etablierte Geschäftsbeziehung – und somit kein inhärentes Vertrauensverhältnis – existiert. Deshalb spielt, neben wirtschaftlichen und ergonomischen Aspekten, die Sicherheit dieser Zahlungsmechanismen eine besondere Rolle.

In diesem Beitrag soll ein aktueller Überblick über die zur Zeit, bzw. möglicherweise in Zukunft, eingesetzten Verfahren vermittelt werden. Während das Hauptaugenmerk den aktuellen Entwicklungen im deutschsprachigen Raum gilt, so werden auch weitere – subjektiv für interessant erachtete – Verfahren gestreift und ein Ausblick auf zukünftige Entwicklungen gewagt.

Diese Arbeit ist folgendermaßen gegliedert: In Abschnitt 2 sind aktuelle Marktanalysen und -prognosen für den elektronischen Handel und insbesondere die damit verbundenen Zahlungsgewohnheiten zusammengetragen. In den beiden folgenden Abschnitten werden die verschiedene Zahlungsmechanismen ausführlich behandelt. Für eine grobe Einteilung der Verfahren, wurde die Höhe des Zahlbetrages herangezogen. Bei den – in Abschnitt 4 diskutierten – Verfahren für *Macropayments* wird unterstellt, dass der Zahlbetrag keinenfalls weniger als 1,– DM beträgt. Da sich das World Wide Web insbesondere auch für das Anbieten von kostenpflichtigen Informationen und Dienstleistungen eignet, deren Transaktionswert diese Grenze unterschreitet, ist es wichtig neben diesen – mittlerwei-

le etablierten – Verfahren auch Mechanismen zur Abwicklung von *Micropayments* zu entwickeln, mit denen auch Zahlungstransaktionen durchgeführt werden können, deren Wert nur wenige Pfennige, oder sogar nur Bruchteile von Pfennigen, beträgt. Hierbei ist natürlich nicht die technische Machbarkeit solcher Transaktionen, sondern vielmehr deren Wirtschaftlichkeit das entscheidende Kriterium. Solche Verfahren werden in Abschnitt 5 ausführlich erläutert. Wir beschließen diese Arbeit – in Abschnitt 6 – mit einem kurzen Fazit.

2 Der elektronische Marktplatz

Während in den letzten Monaten erste spektakuläre Firmenpleiten im Business-to-Consumer - Umfeld (B2C), wie z.B. `www.boo.com`, publik wurden, so sind sich dennoch alle Analysten einig, dass sich das grundsätzliche Wachstum im E-Commerce-Umfeld auch in den nächsten Jahren fortsetzen wird.

So beziffert beispielsweise eine KPMG-Studie [KPM00] das globale, jährliche Umsatzwachstum in den nächsten Jahren mit etwa 100%. In Europa soll demzufolge der Gesamtumsatz im E-Commerce, d.h. B2B und B2C zusammen, von knapp 300 Milliarden Euro (ca. 4%) im Jahre 1999 bis zum Jahr 2002 auf etwa 2 Billionen Euro (ca. 14%) anwachsen.

Verglichen mit der globalen Entwicklung wird dem B2C-Markt in Europa gar ein etwas stärkeres Wachstum vorausgesagt. Einer Forrester-Studie [For00b] zufolge soll der Umsatz in diesem Bereich gar um etwa 140% wachsen und die Zahl der Online-Konsumenten bis zum Jahr 2004 bei etwa 100 Millionen liegen. Nach dieser Studie betrug der B2C-Umsatz im Jahr 1999 in Europa etwa 36 Milliarden, wobei in England etwa 10 und in Deutschland etwa 7 Milliarden umgesetzt wurden.

Betrachtet man nun die aktuellen Zahlungsgewohnheiten in Deutschland, so zeigt eine Foris [For00a] - Umfrage, dass – neben den klassischen „Zahlungsmechanismen“ (Überweisung 26%, Lastschrift 22% und Nachnahme 13%) – heute praktisch[1] nur per Kreditkarte (30%) bezahlt wird. Bis zum Jahr 2004 soll sich das dahingehend ändern, dass etwa 22% mit SmartCards, was wohl in Deutschland der GeldKarte gleichkommen dürfte, 20% mit elektronischer Rechnung, 19% per Kreditkarte, 18% durch Rechnung/Überweisung, 16% Lastschrift und 5% durch andere Verfahren bezahlt werden würde.

Wenngleich nur 154 Kunden und 35 Anbieter an dieser Umfrage teilnahmen, so scheinen diese Zahlen ein gewisses Gefühl für die aktuelle Stimmung und möglicherweise die zukünftige Entwicklung zu vermitteln.

3 Münz- und Kontenbasierte Verfahren

Da es sehr viele – teilweise inzwischen wieder eingestellte[2] – Systeme und vor allem Systementwürfe für elektronische Zahlungsmechanismen gibt, wird im Folgenden lediglich eine Auswahl vorgestellt. Für eine ausführlichere Betrachtung und Bewertung verschiedener (Micropayment-) Verfahren sei auf [Hit00] verwiesen. Hier wurden die Kategorien „Münzbasierte Verfahren“ und „Kontenbasierte Verfahren“ gewählt. Da die Begriffe *münzbasiert*

[1] Alle sonstigen Zahlungsmechanismen machten weniger als 1% aus.

[2] Ein prominentes Beispiel in diesem Zusammenhang ist die Einstellung der walletbasierten, in den Abschnitten 4.2.3 und 4.3.1 näher erläuterten, Cybercash-Systeme im Dezember 2000.

und *kontenbasiert* bei näherer Betrachtung nicht eindeutig sind[3], vorab eine kurze Definition:

Münzbasierte Verfahren
In einem münzbasierten Verfahren wird eine Bezahlung durch die Übertragung eines elektronischen Tokens geleistet. Ein Token ist dadurch gekennzeichnet, dass es mit einem Wert behaftet ist und demzufolge ein Verlust des Tokens den Verlust des Wertes impliziert.

Kontenbasiertes Verfahren
Ein kontenbasiertes Verfahren zeichnet sich durch die (sofortige) Buchung einer Zahlung auf dem entsprechenden Konto aus. Die Zahlung wird dabei ebenfalls durch die Übertragung einer elektronischen Nachricht initiiert, ein Verlust dieser Nachricht hat jedoch keinen Geldverlust zur Folge.

4 Verfahren für Macropayments

In diesem Abschnitt wollen wir einen groben Überblick über elektronische Zahlungsmechanismen geben, die – im Gegensatz zu den in Abschnitt 5 diskutierten Verfahren – sinnvollerweise nur zur Zahlung von Gütern und Dienstleistungen mit einem Wert von (deutlich) mehr als 1,– DM eingesetzt werden.

Wie bereits angedeutet, unterscheiden wir zwischen münz- und kontenbasierten Verfahren. Bei den kontenbasierten Verfahren unterscheiden wir weiterhin zwischen kredit- und debitartigen Verfahren.

4.1 Münzbasierte Macropayment-Verfahren

4.1.1 eCash

eCash ist „der Klassiker“ unter den münzbasierten Bezahlverfahren und basiert auf der richtungsweisenden Arbeit [Cha83] von David Chaum. Nach dem Konkurs der Firma Digicash im Jahr 1998, wurde die Technologie von einem neuen Unternehmen Ecash Technologies Inc. übernommen. eCash wurde in Deutschland insbesondere durch die Kooperation mit der Deutschen Bank bekannt.

Der Ablauf im System läßt sich in grober Art und Weise folgendermaßen beschreiben:

In der Initialisierungsphase erzeugt sich die eCash-Bank einen RSA-Modul $n = pq$ und für jeden Münzwert jeweils ein RSA-Schlüsselpaar (e_i, d_i), wobei $(n, e_1, e_2, \cdots)$ veröffentlicht wird. Nun erzeugt sich ein registrierter Kunde eine „rohe“ eCash-Münze m sowie eine Zufallszahl r und schickt den Wert $w \equiv r^{e_i} \cdot m \pmod{n}$ zur eCash-Bank. Diese veranlasst die entsprechende Verbuchungen mit dem Giro-Konto des Kunden und signiert die maskierte Münze w. D.h. sie berechnet $s' \equiv w^{d_i} \equiv (r^{e_i} \cdot m)^{d_i} \equiv r \cdot m^{d_i} \pmod{n}$ und schickt dem Kunden diesen Wert zurück. Dieser kennt r und kann deshalb durch Berechnung von $s \equiv s' r^{-1} \pmod{n}$ die Signatur $s \equiv m^{d_i} \pmod{n}$ der eCash-Bank für die Münze m extrahieren. Beim Bezahlen schickt der Kunde die Münze (m, s) zum Händler,

[3] Eine Münze ist ein ein Datenpaket, das durch ein Netz übertragen wird. Doch auch kontenbasierte Systeme setzen einer Buchung die Übertragung elektronischer Nachrichten voraus. Im Gegenzug müssen bei tokenbasierten Verfahren auch „Konten“ existieren, in denen die Münzen bis zur Einlösung gesammelt werden.

der sie wiederum online bei der Bank einlöst. Die Bank speichert die Seriennummer der Münze in einer Datenbank und veranlasst die Buchung auf das Giro-Konto des Händlers. Double-spending würde beim Eintrag der Seriennummer in der Datenbank entdeckt.

Bei diesem Verfahren ist es auch möglich Bezahlungen zwischen Privatpersonen durchzuführen, indem die so erstellte Münze z.B. als Email-Anhang verschickt wird. Vor der Benutzung muss der neue Besitzer jedoch diese Münze wieder bei der Bank gegen eigene Münzen tauschen. Steht der gewünschte Bezahlbetrag nicht passend zur Verfügung, so müssen die Münzen vorher bei der Bank gewechselt werden.

Die herausragende Eigenschaft dieses Verfahrens ist, dass selbst die Bank nicht herausfinden kann, bei welchen Händlern welcher Kunde wann, wieviel bezahlt. Der Kunde agiert also – auch für die Bank – anonym.

4.1.2 SuperCash

Bei SuperCash [NTT00] handelt es sich um ein von NTT entwickeltes Bezahlungsverfahren, das sich der Arbeit [Oka95] von Tatsuaki Okamoto bedient. Während nicht zu erwarten ist, dass SuperCash auf dem deutschen Markt Relevanz erlangen wird, so scheint dieses Verfahren nach heutigem Kenntnisstand das leistungsfähigste Bezahlverfahren zu sein.

Neben der Anonymität des Kunden – wie bei eCash – besteht hier ausserdem die Möglichkeit eine Münze – ohne Zutun einer Bank – zu teilen. Deshalb ist es hier wichtig, dass die Münze selbst versteckte Informationen über die Identität des Kunden trägt, die jedoch nur ermittelt werden kann, sobald eine Münze ein zweites Mal ausgegeben wurde.

4.2 Kreditartige Verfahren

In diesem Abschnitt beschäftigen wir uns mit kreditkartenbasierten Verfahren. Durch die relativ hohen Gebühren ist es klar, dass sich mit diesen Verfahren nur recht hohe Beträge – in sinnvoller Art und Weise – abrechnen lassen.

4.2.1 MoTo / SSL

Die einfachste Art und Weise eine Bezahlung im Internet durchzuführen ist, dass der Händler die Kreditkartennummer des Kunden erfragt und – nach einer entsprechenden Autorisierungsanfrage – die Abrechnung, wie bei einer Bestellung per Brief, Fax oder Telefon (Mailorder/Telephoneorder, MoTo), abwickelt. Um zu verhindern, dass die sensiblen Kreditkartennummern ungeschützt über das Internet verschickt werden, scheint es mittlerweile (gottlob) üblich zu sein, die Kommunikationsverbindung zwischen Händler und Kunde mit SSL abzusichern.

Wie die bekanntgewordenen Betrugsfälle belegen, ist dieses Vorgehen – aus Perspektive der Sicherheit – alles andere als unbedenklich. So konnte beispielsweise der Hacker „Maxus“ im Januar 2000 etwa 300.000 Kreditkarten-Nummern vom Web-Server der Firma CD-Universe stehlen. Beim jüngsten und wohl spektakulärsten Kreditkarten-Betrugsfall [Egg00] wurden im Dezember 2000 vom Egghead.com-Server mehr als 3 Millionen Karten-Nummern gestohlen. Mit diesen Kreditkarten-Nummern wäre es nun leicht selbst beliebige Waren per MoTo zu kaufen. Deshalb ist es nicht verwunderlich, dass der Händler hierbei keine Zahlungsgarantie zugesichert bekommt.

Auf der anderen Seite könnte ein betrügerischer Händler mit den übermittelten Kreditkartendaten selbst beliebige Zahlungen anstoßen. Dass dies nicht nur ein potentielles Risiko ist, belegt der im Mai 1999 bekannt gewordene Fall: H. Taves – ein kalifornischer Internet-Erotik-Unternehmer – verbuchte im Jahr 1998 einen Umsatz von etwa 49 Millionen US$, die er durch Kreditkarten-„Zahlungen“ einnahm. Problematisch war hierbei, dass von diesem Betrag lediglich knapp vier Millionen US$ legitimierte Bezahlungen waren.

Die einfachste – und vermutlich die weitaus verbreitetste – Möglichkeit an fremde Kreditkartennummern zu gelangen ist die sorgfältige Inspektion von Mülleimern – z.B. an Tankstellen. Um den Effekt dieses „Trashings“ einzudämmen, wird es bei den künftigen Kreditkarten – neben der auf jedem Beleg vorhandenen Kreditkartennummer – einen zusätzlichen dreistelligen „Autorisierungscode“ geben.

Dass dies wohl eher als kurzfristiger Versuch den Kreditkartenbetrug einzudämmen, denn als langfristige Lösung, zu beurteilen ist, liegt auf der Hand.

4.2.2 SET

Secure Electronic Transaction (SET) ist eine von VISA und Mastercard – zusammen mit IBM und Microsoft – entwickelte Sicherheits-Infrastruktur für die Abwicklung elektronischer Transaktionen im B2C - Bereich. Ein wichtiges – aber langfristig möglicherweise nicht das einzige – Einsatzgebiet von SET ist die sichere Kreditkartenzahlung.

Die drei beteiligten Parteien (Cardholder, Merchant und Payment-Gateway) erhalten von ihrer jeweiligen Zertifizierungsinstanz Zertifikate, die die Erstellung digitaler Signaturen und die asymmetrische Verschlüsselung erlauben. Diese Zertifizierungsinstanzen erhalten – nach einer entsprechenden Sicherheitüberprüfung durch VISA bzw. Mastercard – wiederum ein Zertifikat von der Brand-Level-CA, die direkt unter der globalen Wurzelinstanz hängt.

Der entscheidende Vorteil gegenüber der naiven MoTo/SSL-Variante ist, dass der Händler die Kreditkartennummer nicht zu Gesicht bekommt, aber trotzdem – was aufgrund der durch die Public Key Infrastruktur induzierten Sicherheit gerechtfertigt ist – eine Zahlungsgarantie erhält.

4.2.3 Cybercash - Kreditkartenzahlung

Bei diesem – bis Dezember 2000 u.a. von der Dresdner Bank, der Commerzbank und der Hypo-Vereinsbank unterstützten Verfahren [Cyb00] existierte neben der MoTo/SSL-Lösung, bei der der Kunde nicht registriert sein muss, auch die Möglichkeit, dass beim Kunden ein Cybercash-Wallet installiert wurde, welches die Kreditkarteninformation für das Cybercash Payment Gateway verschlüsselte. Deshalb war es hierbei nicht möglich, dass der Händler die übertragenen Karteninformationen mißbraucht.

Aus mangelnder Kundenakzeptanz wurde dieses Verfahren, wie auch die anderen walletbasierten Cybercash-Verfahren (EDD und Cybercoin), mittlerweile jedoch eingestellt.

4.3 Debitartige Verfahren

In diesem Abschnitt werden einige Verfahren vorgestellt, bei denen die Bezahlung durch Abbuchung von einem (vorausbezahlten) Konto erfolgt.

4.3.1 Cybercash – Electronic Direct Debit und Cybercoin

Beim Electronic Direct Debit (EDD) Verfahren der Firma Cybercash GmbH [Cyb00] handelte es sich um einen lastschriftartigen Mechanismus. Das heisst, dass bei der intitalen Registrierung der als Vermittler zwischen Kunden und Händler fungierenden Cybercash GmbH die Erlaubnis erteilt wurde die im Rahmen von EDD umgesetzten Beträge vom Girokonto des Kunden abzubuchen.

Bei Cybercoin bestand die Möglichkeit Geldbeträge in das Cybercoin-Wallet zu laden, mit dem elektronische Zahlungen – vorzugsweise für niedrigpreisige, elektronische Güter – durchgeführt werden konnten. Für jedes Cybercoin-Wallet existierten bei der Cybercash GmbH entsprechende Schattenkonten, über die die Buchungen abgewickelt wurden.

Aus mangelnder Kundenakzeptanz wurden beide Systeme im Dezember 2000 eingestellt. Die Cybercash GmbH bietet nunmehr lediglich Systeme für die MoTo/SSL-Kreditkartenzahlung an.

4.3.2 Lastschrift mit elektronischer Signatur

Bei diesem – z.B. von der Deutschen Post AG / SignTrust angebotenen – Verfahren handelt es sich um eine elektronische Version des Bezahlens per Lastschrift. Hierbei wird die Abbuchungserlaubnis nicht wie üblich manuell, sondern – unter Verwendung SigG-konformer Chipkarten und Zertifikate – elektronisch signiert.

Während der Händler, durch die Verbindlichkeit der SigG-konformen elektronischen Signatur, die Durchführung der Transaktion leicht, ggf. vor Gericht, nachweisen kann, so muss beim Kunden bereits die entsprechende Infrastruktur mit Chipkarte und Leser vorhanden sein.

4.3.3 GeldKarte

Neben der Zahlung mit der GeldKarte am Point of Sale ist es seit kurzem auch möglich mit der GeldKarte im Internet zu bezahlen [Zit99]. Der wesentliche Unterschied zwischen diesen beiden Zahlungsvarianten ist, dass die Identität des Händlers bei der Bezahlung im Internet keineswegs klar ist. Deshalb wurde vom ZKA, abgesehen von (sparkasseninitiierten) Pilotprojekten, die Verwendung von sog. Klasse 3 Lesern vorgeschrieben. Dieser, z.B. von Kobil angebotene, Leser ist in der Lage den Händler durch Überprüfen einer digitalen Signatur zuverlässig zu authentifizieren und die Händleridentität sowie den Zahlbetrag auf dem Display des Lesers anzuzeigen.

Durch die weite grundsätzliche Verbreitung der GeldKarte, die wachsende Verfügbarkeit von Akzeptanzstellen an Verkaufsautomaten, die im Rahmen von HBCI 3.0 geplante Möglichkeit des Ladevorganges im Internet [Zit99] und insbesondere die moderaten Gebühren von derzeit 0,3 % des Warenwertes, bzw. mindestens 0,02 DM, erscheint die GeldKarte – abgesehen von der benötigten Kartenleserinfrastruktur – als ein sehr vielversprechendes elektronisches Zahlungsverfahren für den deutschen Markt. Inwieweit sich das GeldKarten-System – im Zuge von CEPS – auch auf europäischem Boden durchzusetzen vermag muss die Zukunft zeigen.

4.3.4 Paybox

Beim Paybox-System [Pay00a] handelt es sich um ein Bezahlverfahren, bei dem die Paybox AG das Clearing zwischen Kunden und Händlern durchführt. Hierbei zahlt der Kunde

eine jährliche Grundgebühr von 5 Euro und der Händler, bzw. bei Peer-to-peer-Zahlungen der Zahlende, eine umsatzabhängige Gebühr.

Das Alleinstellungs-Merkmal von Paybox ist, dass die Zahlung durch die Eingabe einer PIN mit einem gewöhnlichen Mobiltelefon autorisiert wird. Der Kunde teilt dem Händler – z.B. einem Taxifahrer direkt oder im Internet mit SSL geschützt – zur Zahlung seine Mobiltelefon-Nummer, bzw. eine Paybox-Alias-Nummer, mit. Nachdem der Händler die Daten an die Paybox AG geschickt hat, initiiert diese einen Anruf zum registrierten Mobiltelefon des Kunden. Nachdem dem Kunden die Zahlungsdaten von einem Sprachcomputer „vorgelesen“ wurden, kann er die Zahlung durch Eingabe seiner Paybox-PIN freigeben.

Während dieses Verfahren durch seine Flexibilität und Einfachheit besticht, so verlässt sich Paybox auf die in GSM implementierten Sicherheitsmechanismen. Diese lassen sich bekanntlich, durch den Einsatz von – in Österreich übrigens legal erwerbbaren – IMSI-Catchern – wie in [Fed] beschrieben – aushebeln. Somit könnte beispielsweise die im Sprachkanal übertragene Paybox-PIN eines Kunden ausgeforscht, und die Telefon-Nummer im Netz auf das Gerät eines Angreifers umgeleitet werden. Ob diese grundsätzliche Schwäche mehr als ein theoretisches Angriffspotential bildet, muss die Zukunft zeigen.

4.3.5 Prepaid-Papierkarten

Bei der Paysafecard [Pay00b] in Deutschland und internetCASH [InC00] in den USA können z.B. an Tankstellen, Kiosken, ..., Papierkarten erworben werden, mit deren Seriennummer und einer durch Rubbeln sichtbaren PIN auf ein beim Anbieter vorhandenes Konto mit dem entsprechenden Wert zugegriffen werden. Diese Verfahren arbeiten somit analog zu den in den USA üblichen Prepaid Telefon-Karten, wobei die Übertragung der Zugangsdaten (Konto-Nummer und PIN) im Internet durch SSL geschützt wird.

5 Verfahren für Micropayments

Wie bereits angedeutet, zielen Verfahren für Micropayments darauf ab, Transaktionen im Wert von unter 1,– DM abzurechnen. Die Entwicklung des Internet hin zu einem breitbandigen Medium, welches in naher Zukunft die gewohnte Form von Radio, Musik und sogar Fernsehen ablösen könnte und die gegenwärtig weite Verbreitung werbefinanzierter Seiten im Internet macht die Dimensionen des vorhandenen Marktes für Micropaymentsysteme deutlich.

Bei dem Entwurf eines Systems, das kleine und kleinste Transaktionen abrechnen soll, ist es wichtig darauf zu achten, alle eventuell anfallenden Kosten zu minimieren. Wird diese Anforderung nicht konsequent umgesetzt, so besteht die Gefahr, dass die bei der Abrechnung anfallenden Kosten den Wert der jeweiligen Transaktion übersteigen. Auch die Effizienz ist ein wichtiges Kriterium, da selbst bei kostendeckender Abrechnung von Transaktionen die Gewinnmarge so gering ist, dass eine sog. kritische Masse von Kunden benötigt wird, um durch das System einen lohnenden Betrag einzunehmen.

Analysiert man ein übliches Szenario, in dem neben Händler und Kunde immer ein Broker als Vermittler zu den finanziellen Netzwerken existiert, so stellt man fest, dass neben der zur Abwicklung einer Transaktion benötigten Rechenleistung – deren Minimierung

wichtig für die Effizienz des Systems ist – die Art der Autorisierung einer Zahlung eine entscheidende Rolle für die Wirtschaftlichkeit des Systems spielt. Jede Prüfung einer digitalen Münze auf Gültigkeit und jeder Datenbankzugriff, z.B. zur Prüfung eines Kontostandes, erhöht die Kosten und senkt die Gewinnmarge des Systems. Zusätzlich zu diesen wirtschaftlichen Anforderungen sind auch technische Anforderungen wie Sicherheit und Integrationsfähigkeit sowie soziale Anforderungen wie Funktionalität und einfache Bedienbarkeit zu berücksichtigen. Für weitere Anforderungen an Micropaymentsysteme verweisen wir auf [HR 96, Hit00].

5.1 Münzbasierte Verfahren

In einem grundlegenden Szenario kauft ein Kunde zunächst Münzen von einem Broker, oder generiert diese selbst. Im zweiten Fall muss sichergestellt werden, dass er auch den entsprechenden Gegenwert in realer Währung besitzt. Diese „Kreditlinie“ kann durch einen Broker anhand eines digitalen Zertifikates zugesichert werden. Die so erhaltenen Münzen werden in der Regel in einer elektronischen Geldbörse auf dem Rechner des Kunden gespeichert. Optional eingesetzte Techniken können es ermöglichen, dieses „Geld“ bei Verlust wieder herzustellen.

Bei münzbasierten Verfahren muss zum Einen verhindert werden, dass mit einer Münze mehrfach bezahlt werden kann (double spendig), und zum Anderen überprüft werden, ob eine Münze gültig ist. Dies geht meistens mit aufwendigen Datenbankabfragen einher, welche ein Micropaymentsystem schnell unwirtschaftlich machen können.

5.1.1 MicroMint

Bei MicroMint [RS96] handelt es sich um den eher akademischen Entwurf eines Micropaymentsystems von Ronald L. Rivest und Adi Shamir. Ziel bei dem Entwurf des Systems war es, langsame Public-Key Operationen und gleichzeitig Datenbankabfragen zu vermeiden und ein schnelles, effizientes System zu entwickeln.

Diese Ziele werden erreicht, indem als Münzen sog. k-fach Kollisionen von Hashfunktionen verwendet werden. Die Erzeugung solcher Kollisionen ist mit hohem Rechenaufwand verbunden und lohnt sich erst, wenn sie in großen Mengen durchgeführt wird. Im Gegenzug ist die Überprüfung einer Münze auf Gültigkeit sehr einfach durch die Rechnung

$$h(x_1) \stackrel{?}{=} h(x_2) \stackrel{?}{=} ... \stackrel{?}{=} h(x_k) \stackrel{?}{=} y$$

möglich, wobei $x_1, \cdots, x_n$ beliebige Zeichenfolgen sind. Münzen werden von einem Broker jeweils für eine Periode generiert und zusammen mit der verwendeten Hashfunktion ausgegeben. Nach Ablauf dieser Periode verfallen die Münzen und werden durch neue ersetzt. Eine Fälschung der Münzen ist sehr schwer, da diese erst nach Veröffentlichung der Hashfunktion möglich und dann mit sehr hohem Zeit- und Rechenaufwand verbunden ist.

Da dieses System nie implementiert wurde, können keine Aussagen über die Bedienbarkeit oder Akzeptanz getroffen werden. Die Vorteile des Systems liegen jedoch in der Effizienz, der Anonymität, der einfachen Überprüfbarkeit einer Münze auf Gültigkeit und der damit verbundenen Möglichkeit von *peer-to-peer* Zahlungen. Die Nachteile liegen in dem extrem

hohen Rechenaufwand bei der Generierung der Münzen, der allein durch den Broker getragen werden muss und der trotz hoher Unwahrscheinlichkeit vorhandenen Möglichkeit, Münzen zu fälschen.

5.1.2 Millicent

Das System Millicent der Firma Digital [Man97] setzt auf eine Beziehung zwischen Broker, Händler und Kunde. Der Kunde kann von einem Broker digitales Geld kaufen, sog. „Broker-Scrip". Dieses kann er dann bei einem Händler in dessen Währung eintauschen („Händler-Scrip").

Die Bezahlung erfolgt durch das Senden von Scrip an den Händler, der dessen Gültigkeit anhand einer Überprüfung eingebetteter Hashwerte sicherstellen kann. Daraufhin sendet der Händler die Ware und das „Wechselgeld" zurück. Der Kunde kann jederzeit Händler-Scrip in Broker-Scrip umtauschen und umgekehrt.

Das System bietet dem Kunden wenig Schutz. Jeder Händler wäre in der Lage, das empfangene Geld zu behalten, ohne die gewünschte Ware auszuliefern. Es werden auch keine digitalen Signaturen verwendet, anhand derer die Nicht-Abstreitbarkeit von Nachrichten erreicht werden könnten. Als Begründung für die fehlende Sicherheit wird die Größe der Beträge angeführt.

5.1.3 PayWord

Der Ansatz PayWord [RS96] wurde zusammen mit MicroMint veröffentlicht. Er basiert auf verketteten Hashwerten, die als elektronische Münzen verwendet werden.

Ein Kunde erhält durch ein – regelmäßig durch einen Broker erneuertes Zertifikat – das „Recht", selber Münzen zu generieren. Klickt eine Kunde bei einem Händler das erste Mal auf einen kostenpflichtigen Link, so wird der Vorgang der Münzerzeugung, z.B. durch eine elektronische Geldbörse auf dem Rechner des Kunden, in Gang gesetzt. Der Kunde muss sich entscheiden, wie viel „Geld" er generieren möchte, da es nur bei diesem Händler gilt. Der Ausgangspunkt ist die Erzeugung einer Zufallszahl w_0. Diese Zufallszahl wird sodann mehrmals mittels der Hashfunktion $h()$ gehasht:

$$w_1 = h(w_0), w_2 = h(w_1), \cdots, w_n = h(w_{n-1})$$

Der zuletzt generierte Hash wird digital signiert und zusammen mit dem gewünschten Wert pro Hash (z.B. 1 Pfennig) und der Länge der Hashkette an den Händler übertragen. Der davor generierte Hash ist der erste, der zur Bezahlung verwendet werden kann. Der Händler ist nun in der Lage, anhand einer einzigen Hash-Operation zu überprüfen, ob die Münze gültig ist.

Ähnlich wie bei MicroMint liegt der Vorteil dieses Verfahrens in der einfachen Überprüfung der elektronischen Münzen. Als Nachteile sind jedoch die fehlende Anonymität, die Voraussetzung korrelierte Zahlungen bei einem Händler durchführen zu müssen und der damit verbundene Aufwand der initialen Zahlung zu nennen.

Als Verfahren, die ebenfalls Hashketten zur Bezahlung verwenden, sind PhoneTicks [Ped95], MPTP [H 95] und Mykro-iKP [HSW96] zu nennen. NetCard [Net96] und MicPay [PM 00] arbeiten auch auf Basis von Hashketten, jedoch unter Verwendung von Smart-Cards.

5.2 Kontenbasierte Verfahren

Kontenbasierte Verfahren buchen jede Zahlung direkt auf ein Konto. Bei sehr vielen kontenbasierten Verfahren handelt es sich um Dienste zur Abrechnung von Zahlungen, die über das Internet angeboten werden.

5.2.1 CyBank, Firstgate, ...

CyBank [Cyb] und Firstgate [Fir00] bieten Händlern die Verwaltung von vorausbezahlten Kundenkonten bzw. Kundenkonten mit Einzugsermächtigung an. Sobald ein Kunde auf einen kostenpflichtigen Link klickt, wird er beispielsweise zu einem Server von Firstgate weitergeleitet und muss durch Eingabe seines Benutzernamens und seines Passwortes die Zahlung bestätigen. Daraufhin wird der Betrag von seinem Konto abgebucht und dem Konto des Händlers gutgeschrieben. Nach diesem Vorgang wird er zurück auf die Seite geleitet, die er eigentlich betrachten wollte.

Der Vorteil dieses Verfahrens liegt auf der Hand. Weder auf Händler- noch auf Kundenseite muss Software installiert werden und deshalb ist die Integration in bestehende Infrastrukturen sehr einfach. Entscheidende Nachteile sind jedoch die fehlende Anonymität und das benötigte Vertrauen in einen zentralen Dienstleister. Zusätzlich stellt der Dienstleister einen „Single-Point-Of-Failure“ dar, d.h. wenn dessen Systeme einmal ausfallen sollten, können weder angeschlossenen Händler noch Kunden Zahlungen abwickeln. Bemerkenswert ist hierbei, dass die Gebühren z.B. bei Firstgate – abhängig vom Umsatz – bis zu 40% betragen können.

Dienste dieser Art gibt es sehr viele im Internet. Sie alle aufzuzählen würde an dieser Stelle zu weit führen.

5.2.2 Net900

Net900 [Net00] ist ein Inkasso-System, bei dem die DFÜ Verbindung des Kunden bei Klick auf einen kostenpflichtigen Link getrennt und zu Net900 neu aufgebaut wird. Dabei handelt es sich um eine 0190er Nummer, welche die Abrechnungsarten pay-per-use und pay-per-time ermöglicht. Nach Ablauf der gewünschten Zeit oder Abrechnung des gewünschten Artikels wird die ursprüngliche Verbindung wieder aufgebaut.

Der Vorteil bei diesem System liegt wiederum bei der einfachen Integration in bestehende Infrastrukturen. Nachteile sind das benötigte Vertrauen in eine zentrale Einrichtung, fehlende Anonymität und Probleme bei der Nutzung einer Standleitung. Zusätzlich liegt die minimal abzurechnende Einheit bei 0,27 DM - eine Grenze die für ein Micropaymentsystem sehr hoch ist und das Bezahlen von Pfennigen oder Teilen davon von vornherein ausschließt.

6 Fazit

In dieser Arbeit wurde ein grober Überblick über verschiedene elektronische Zahlungssysteme geliefert, die für den deutschen Markt eine gewisse Relevanz zu besitzen scheinen. Schenkt man den entsprechenden Studien Glauben, so dürfte das GeldKarten-System in Deutschland mittel- und langfristig, d.h. insbesondere sobald entsprechende Klasse 3 Kartenleser zur PC-Standardausstattung gehören, sowie Kreditkartenzahlungen – unter

Berücksichtigung der ständig wiederkehrenden Mißbrauchsfälle wohl auf (möglicherweise chipkartengestützter) SET-Basis – großes Potential besitzen.

Betrachtet man sich die Vielzahl der existierenden, untereinander inkompatiblen, Systeme, so ist die jüngste Cybercash-Meldung, d.h. dass keine proprietären, Wallet-basierten Verfahren mehr unterstützt werden, in der Tat wenig verwunderlich. Der Markt für Systeme zur Abwicklung von Macropayments befindet sich bereits in einer Phase der Konsolidierung, wobei eher Bedienbarkeits- als Sicherheitsaspekte im Vordergrund zu stehen scheinen.

Etwas anders stellt sich die Situation bei Micropayment-Systemen dar. Auch wenn die grundsätzlich verfügbaren Verfahren – aus wissenschaftlicher Sicht – noch recht unbefriedigend sind, so sprießen immer neue Micropayment-Dienstleister aus dem Boden. Bei Gebühren bis zu 40% des Umsatzes, wie bei Firstgate, ist dies auch kaum verwunderlich. In diesem Segment scheint die technologische und wirtschaftliche Entwicklung alles andere als abgeschlossen.

Literatur

[Cha83] Chaum, David: Blind signatures for untraceable payments. **In:** *Proceedings of CRYPTO 82*, Plenum Press, 1983, S. 199–203

[Cyb] CyBank Homepage. Internet. – http://www.cybank.net

[Cyb00] Cybercash Homepage. Internet. 2000. – http://www.cybercash.de

[Egg00] Massive credit heist, fraud reported - Hackers crack Egghead.com; Russian fraud rampant. Internet. Dezember 2000. – http://www.msnbc.com/news/506714.asp

[Fed] Federrath, Hannes: Sicherheit mobiler Kommunikation - Schutz in GSM-Netzen. **In:** *Mobilitätsmanagement und mehrseitige Sicherheit*, Vieweg

[Fir00] Firstgate Homepage. Internet. 2000. – http://www.firstgate.de

[For00a] Foris Homepage. Internet. 2000. – http://www.foris.de

[For00b] Forrester Homepage. Internet. 2000. – http://www.forrester.com

[H 95] Hallam-Baker, Phillip [u. a.] : W3C micro payment transfer protocol / W3C. 1995 (WD-mptp-951122). – Working Draft http://www.w3.org/TR/WD-mptp

[Hit00] Hitzbleck, Andreas: *Ermittlung und Bewertung des State of the Art im Bereich der Micropaymentsysteme*, Universität Gesamthochschule Essen, Diplomarbeit, Dezember 2000

[HR 96] Himmelspach, A. ; Runge, A. [u. a.] : Anforderungen an elektronische Zahlungssysteme / Universität St. Gallen. Schweiz, 1996 (BusinessMedia/51, Version: 1.0). – Forschungsbericht http://www.netacademy.org

[HSW96] Hauser, R. ; Steiner, M. ; Waidner, M.: Micro-Payments based in ikp / IBM Research Laboratiory. Zürich, 1996 (RZ 2791). – Forschungsbericht http://www.zurich.ibm.com/Technology/Security/publications/1996/HSW96.ps.gz

[InC00] internetCASH Homepage. Internet. 2000. – http://www.internetcash.com

[KPM00] KPMG Homepage. Internet. 2000. – http://www.kpmg.com

[Man97] Manasse, Mark: The Millicent Microcommerce System / Digital Systems Research Center. Palo Alto, 1997. – Forschungsbericht

[Net96] NetCard Homepage. Internet. 1996. – http://www.cl.cam.ac.uk/ftp/users/rja14/netcard.ps.Z

[Net00] Net900 Homepage. Internet. 2000. – http://www.in-medias-res.com/net900.htm

[NTT00] SuperCash Homepage. Internet. 2000. – http://supercash.ntt.com/en/

[Oka95] Okamoto, Tatsuaki: An efficient divisible electronic cash scheme. **In:** Coppersmith, D. (Hrsg.): *Proceedings of CRYPTO '95* Bd. 963. Bd. 963, Springer, 1995, S. 438–451

[Pay00a] Paybox Homepage. Internet. 2000. – http://www.paybox.de

[Pay00b] Paysafecard Homepage. Internet. 2000. – http://www.paysafecard.com

[Ped95] Pedersen, T.: Electronic Payments of small amounts / Aarhus University, Institut für Informatik. Denmark, August 1995 (DAIMI PB-495). – Forschungsbericht

[PM 00] Petersen, Holger ; Michels, Markus [u. a.] : MicPay - Micropayments for correlated payments. **In:** *Informatik/Informatique* (2000), Nr. No. 1

[RS96] Rivest, Ronald L. ; Shamir, Adi: PayWord and MicroMint: Two simple micropayment schemes / MIT Laboratory. 1996. – Forschungsbericht

[Zit99] Zitzelsberger, R.: Die GeldKarte der deutschen Kreditwirtschaft. **In:** Thiessen, F. (Hrsg.): *Bezahlsysteme im Internet*. Frankfurt am Main : Fritz Knapp Verlag, 1999, Kapitel Systemalternativen, S. 143–153