Anforderungen an elektronische Zahlungssysteme

Andrea Himmelspach, Alexander Runge,
Petra Schubert, Hans-Dieter Zimmermann

Bericht-Nr.: BusinessMedia/51
Version: 1.0
Datum: Oktober 1996

**Universität St. Gallen -
Hochschule für Wirtschafts-,
Rechts- und Sozialwissenschaften (HSG)**

Institut für Wirtschaftsinformatik
Dufourstrasse 50
CH-9000 St. Gallen
Tel. +41 71 224 2297
Fax +41 71 224 2771

Inhaltsverzeichnis

EUREKA

EUREKA Projekt Nr. 1483
KTI-Projekt Nr. 3245.2

PAYSYST
Entwicklung generischer Zahlungssysteme für elektronische Marktplätze durch Adaption und Integration von bestehenden, elektronischen Zahlungssystem-Komponenten

Vorwort

Das PAYSYST-Projekt ist ein EUREKA-Projekt und wird durch nationale Fördergremien unterstützt. In der Schweiz wird PAYSYST durch die KTI (Kommission für Technologie und Innovation) gefördert.

Der vorliegende Bericht dokumentiert die Ergebnisse des Arbeitspakets Nr. 1 gemäss Projektplan.

Die folgende Tabelle enthält die Projektpartner und deren Repräsentanten:

Organisation	Vertreter
AGI, St. Gallen	Jürg Padrutt
Electronic Mall Bodensee (EMB)	Hans Meli
FirmNet GmbH / Electronic Mall Zentralschweiz (EMZ), Luzern	Guido Auchli
Institut für Wirtschaftsinformatik an der Universität St. Gallen (HSG), St. Gallen	Andrea Himmelspach, Alexander Runge, Petra Schubert, Hans-Dieter Zimmermann
Schweizerischer Bankverein, Basel	Boris Brunner, Patrick Hafner
Ubis AG, Berlin	Ansgar Kückes
Ubis Schweiz GmbH, Tägerwilen	Knut Jessen
VRZ Informatik, Dornbirn	Gerd Burtscher, Roland Hilbrand

Das administrative Projektmanagement wird von Herrn Thomas Schumann, TEMAS AG, Frasnacht, durchgeführt. Wir danken allen Vertretern für ihre konstruktive Mitarbeit in den Workshops und der Bearbeitung der Arbeitspakete.

1 Einführung

Das Internet bzw. der darauf aufsetzende multimediale Mehrwertdienst World Wide Web (WWW) wird heute von den meisten Teilen der Wirtschaft als die „enabling technology“ für Anwendungen der elektronischen Geschäftsabwicklung, den „Electronic Commerce“, betrachtet. Die globalen und heute allgemein verfügbaren Telematikinfrastrukturen auf der Basis des Internet bilden die Grundlage für das Entstehen offener, elektronischer Märkte (EM) [Schmid95a S. 18ff.].

Elektronische Zahlungssysteme sind ein entscheidender Faktor für den Erfolg der elektronischen Geschäftsabwicklung und damit elektronischer Marktplätze. Digitale Zahlungsmittel bilden - analog zu traditionellen Marktplätzen - das *Schmiermittel* der elektronischen Marktplätze, dem *Marketspace*. Wirtschaft und Wissenschaft arbeiten heute mit Hochdruck an innovativen Lösungen für die komfortable, sicherere und ökonomische Zahlungsabwicklung in offenen Netzen wie dem Internet. Wichtige Voraussetzung für die Akzeptanz elektronischer Zahlungssysteme ist die Berücksichtigung der Anforderungen möglichst aller Teilnehmer.

Im Rahmen des EUREKA-Projektes PAYSYST („Entwicklung generischer Zahlungssysteme für elektronische Marktplätze durch Adaption und Integration von bestehenden, elektronischen Zahlungssystem-Komponenten“) wurden in der Phase 1 die Anforderungen an elektronische Zahlungssysteme analysiert. Der vorliegende Bericht dokumentiert die Ergebnisse. Die Analyse wurde im Sommer 1996 begonnen und im Herbst 1996 abgeschlossen.

Der Bericht gliedert sich in die folgenden Hauptkapitel: Es werden Überblicke über die Anforderungen an elektronische Zahlungssysteme aus technischer (Abschnitt 2), betriebswirtschaftlicher (Abschnitt 3) und nutzerbezogener Sicht (Abschnitt 4) gegeben. Eine Zusammenfassung der Anforderungen (Abschnitt 5) rundet den Bericht ab. Hervorgegangen sind die Anforderungen sowohl aus der zitierten Fachliteratur als auch aus Diskussionen im Rahmen des Projektes PAYSYST.

Die folgende Graphik gibt einen Überblick über den Aufbau und Inhalt des vorliegenden Berichts:

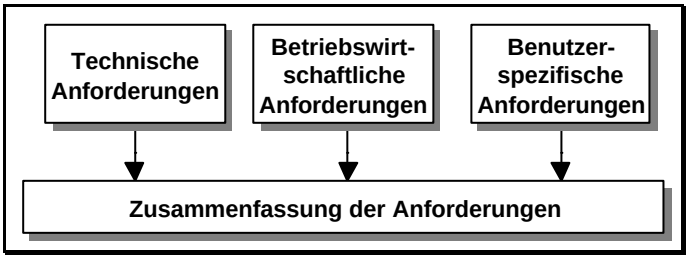

Abbildung 1.1: Aufbau des Arbeitsberichtes

2 Technische Anforderungen

Bei den technischen Anforderungen werden Sicherheitsanforderungen, Integrationsaspekte und Anforderungen an die Realisierung beschrieben.

2.1 Sicherheitsanforderungen

Verfügbarkeit und Zuverlässigkeit

Verfügbarkeit. Alle teilnehmenden Parteien möchten jederzeit in der Lage sein, Zahlungen auszuführen oder zu erhalten [Janson/Waidner96a]. Deshalb müssen:

(a) der Anbieter-/Electronic Commerce-Server,
(b) der Zahlungsserver des Zahlungssystem-Anbieters und
(c) das Banken-Informationssystem
ständig online sein und
(d) der Internet-Zugang für den Konsumenten immer gewährleistet sein.

Zuverlässigkeit. Zahlungstransaktionen müssen atomar (vollständig oder überhaupt nicht) ausgeführt werden und dürfen sich nie in einem unbekannten oder inkonsistenten Zustand befinden. Kein Teilnehmer akzeptiert einen Geldverlust, der durch Netzwerk-Absturz oder Server-Absturz verursacht wird [Janson/Waidner96a].

Verfügbarkeit und Zuverlässigkeitkeit setzen voraus, daß die darunterliegenden Netzwerk Dienstleistungen, Software- und Hardware-Komponenten in hohem Maße zuverlässig, fehlertolerant und betriebssicher sind. Zum Zurücksetzen von unterbrochenen Transaktionen aufgrund von Systemausfällen werden bei allen Parteien sichere Speicher und spezielle Resynchronisations-Protokolle benötigt [Janson/Waidner96a].

Vertraulichkeit

Bestimmte Einzelheiten der Transaktion, wie z.B. Käufer-, Verkäuferidentität, das gekaufte Produkt und der Preis sind nur den beteiligten Parteien bekannt. Die Informationenen bleiben gegenüber Unbeteiligten vertraulich und geheim. Die Vertraulichkeit kann sich auch nur auf einzelne Teilnehmer beschränken und findet dann Anwendung, wenn Anonymität oder Geheimhaltung gefordert wird [Janson/ Waidner96b].

Vertraulichkeit wird besonders von Konsumenten gefordert, da sie durch ihre getätigten Einkäufe im Internet nicht zum „gläsernen Menschen“ werden möchten.

Integrität

Unter Integrität versteht man Nachrichtenunversehrtheit, d.h. daß die gesendete Nachricht mit der empfangenen Nachricht identisch ist. Besonders im Hinblick auf Zahlungstransaktionen muß die Unversehrtheit der übertragenen Daten gewährleistet werden, um zu verhindern, daß Dritte:

(a) Nachrichten duplizieren,
(b) Nachrichten abändern,
(c) Nachrichten einfügen,
(d) Nachrichten zerstören und/oder
(e) Nachrichten umordnen können.

Der Nachrichtenempfänger muß bei Zahlungssystemen überprüfen können, ob die erhaltenen Daten genau in dieser Form abgeschickt wurden, oder ob auf dem Übertragungsweg die erwähnten Modifikationen vorgenommen wurden [Fumy94, 18]. Die Integrität kann mit digitalen Signaturen gewährleistet werden.

[Janson/Waidner96b] verstehen unter Integrität in Bezug auf Zahlungssysteme, daß kein Teilnehmer ohne vorherige Zahlungsautorisierung Geld hergeben muß, und - um passive Bestechung zu verhindern - keine Partei Geld ohne ihre Zustimmung erhalten soll. Diese Art der Integrität wird durch besondere Gestaltung der Zahlungsabläufe und Autorisierungsverfahren erreicht[1].

Im folgenden wird Integrität im Sinne der Nachrichtenunversehrtheit verwendet.

Authentisierung

Das Internet läßt als offenes Netzwerk jeden Teilnehmer unabhängig von Ort, Alter, Vorstrafen, u.a. zu. Durch Modifikationen von E-Mail-Adressen oder durch WWW-Publikationen kann in diesem Netz eine beliebige Identität vorgetäuscht werden. Bei Geschäftstransaktionen müssen die Geschäftspartner jedoch darauf vertrauen können, daß die Vortäuschung einer falschen Identität unmöglich ist [Schonhardt95].

Um seine Identität zu beweisen, besitzt jeder Netzteilnehmer eine Teilnehmer-Identifikation, welche aus einer Zahl, Zeichenfolge, einem Algorithmus oder einer anderen Art von Information besteht, und die ihn eindeutig identifiziert [Muftic92, 12f.]. Der Verifikationsprozeß dieser Teilnehmer-Identitäten wird als Authentifizierung bezeichnet.

Der am weitverbreiteste, aber auf geringem Sicherheitsniveau basierende Mechanismus der Authentifizierung ist die Eingabe eines Paßwortes durch den Benutzer. Eine höhere Sicherheit bei der Identifizierung bieten Sicherheitsmechanismen wie digitale Signaturen und Zertifikate, deren Erstellung, Anwendung und Verifizierung allerdings im Vergleich zur Paßwort-Handhabung mit mehr Aufwand verbunden ist. Bei der Authentifizierung ist keine Wahrung der Anonymität möglich. Es handelt sich um ein Spannungsfeld unvereinbarer Zahlungssystem-Anforderungen.

Autorisierung/Zugriffskontrolle

Eine bedeutende Rolle in Client-Server-Architekturen und somit auch im Internet ist der Schutz gegen unberechtigten Zugriff auf Ressourcen. Um einen unberechtigten Zugriff auf Daten, Programme und andere Ressourcen zu vermeiden, muß anhand der Autorisierung festgestellt werden, *wer* auf eine Ressource *wie* zugreifen darf.

[1] Diese Art der Integrität wurde bei dem System Ecash realisiert.

Aussagen, *wer* auf ein Objekt *wie* zugreifen darf versteht man unter Zugriffskontrolle. Dabei können mehrere Zugreifende auf ein Objekt existieren, die gleichzeitig mehrere Rechte beim Zugriff auf ein Objekt besitzen. Die Entscheidung, ob ein gewünschter Zugriff zugelassen werden darf ist die Zugriffsentscheidung. Eine Autorisierung ist im Gegensatz zur Zugriffskontrolle die z.T. dynamische Zuweisung eines bestimmten Rechte-Satzes an Anwender, die durch Identifier dargestellt werden. Die Autorisationsentscheidung ist demnach die Entscheidung, ob bestimmte Rechte zugeteilt werden können.

Eine Autorität verwaltet die Zugriffsrechte auf Ressourcen bzw. Funktionen i.d.R. in Form von Lese-, Schreib- und Ausführungsrechten in einer Datenbank. Um Autorisierungsentscheidungen auszuführen braucht die Autorität sicheres Wissen über die Personenidentität [Schonhardt95]. Bei elektronischen Zahlungssystemen bedeutet dies die Autorisierung z.B. Berechtigung zur Scheckausstellung oder Zugriff auf das elektronische Münzkonto bei der Bank. So ist bei Ecash der Münztransfer vom elektronischen Münzkonto auf den lokalen Rechner mit einem Paßwort geschützt.

Non-Repudiation

[Meli-Isch95, 100] unterscheidet zwischen drei Arten der Non-Repudiation:

⇒ Mit der *Non-Repudiation of Origin* wird der Nachrichtenempfänger gegenüber dem Nachrichtensender geschützt, der die Nachricht bzw. deren Inhalt leugnen will.

⇒ Die *Non-Repudiation of Delivery* ermöglicht den Schutz des Nachrichtensenders gegenüber dem Empfänger, der den Empfang der Nachricht bzw. deren Inhalt leugnen will.

⇒ Die *Non-Repudiation of Submission* schützt den Nachrichtensender gegen den Leugnungsversuch eines Message Transfer Systems, daß eine Nachricht zur Versendung an einen bestimmten Empfänger vorgelegen hat.

Keiner der Teilnehmer soll demnach bestreiten können, daß er eine Willenserklärung abgegeben oder erhalten hat. Non-Repudiation wird mit Hilfe von digitalen Signaturen und zertifizierten öffentlichen Schlüsseln erreicht.

Vermeidung von Attacken

Schlecht konfigurierte Systeme, nachlässig geschriebene Software, schlechte Systemverwaltung und Benutzernachlässigkeit sind nach [Bhimani96] die Gründe für erfolgreiche Attacken. Bei der Vermeidung von Attacken spielen der Schutz des Rechners *und* die verschlüsselte Datenübertragung über das Internet eine maßgebliche Rolle. Zum Zeitpunkt der Erstellung dieser Arbeit bestehen im Bereich der Datenübertragung sichere Kryptographiemethoden. Der empfindlichste Teil des Gesamtsystems ist der (private) Rechner, auf dem das Geld bzw. die Kontoinformationen gespeichert sind. Ihn gilt es besonders zu schützen, d.h. es soll kein freier Zugang zu dem Rechner bestehen (z.B. durch abschließbaren Raum oder Rechner) und der Zugriff sollte nur mit Paßwort (sinnvolle Paßwortwahl, keine Geburtsdaten, Vornamen, usw.) geschehen. Von seiten des Netzwerks können Firewalls zum Schutz des Rechners eingesetzt werden.

Das Zahlungssystem sollte so konzipiert sein, daß niemand außer dem Besitzer Veränderungen vornehmen kann, z.B. in Form von Wertetransfers und Modifikationen von Daten. Attacken werden erleichtert, wenn Authentifizierungen, Autorisierungen und Verschlüsselung der Transaktionsdaten fehlen.

2.2 Integrationsanforderungen

Technische Integrationsfähigkeit

Technische Integration des Zahlungssystems wird von allen Teilnehmern gefordert. Hierzu sind definierte Schnittstellen erforderlich, die das Zahlungssystem mit dem Gesamtsystem kommunizieren lassen.

Integration in anwenderinterne Applikationen

Voraussetzung der Integration von Zahlungssystemen in die internen Applikationen ist die technische Integrationsfähigkeit. Sie beinhaltet, daß das Zahlungssystem beispielsweise an das Buchhaltungs-System des Konsumenten die Zahlungstransaktionsdaten in einem definierten Format übergibt, so daß dieser eine Verarbeitung ohne weiteren Aufwand vornehmen kann.

Besonders Anbieter sind an der automatischen Übernahme der elektronischen Zahlungstransaktionsdaten interessiert um Fehler durch Neueingaben zu verhindern. Im „klassischen" elektronischen Zahlungsverkehr mittels EDI ist diese Art der Integration schon seit mehreren Jahren gegeben.

Durchgängigkeit der IT-Mittel

Die Durchgängigkeit sollte über alle Phasen der Markttransaktion reichen. Auch innerhalb der Abwicklung ist deshalb ein einheitliches IT-Mittel gefordert[2]. Der Internet-Benutzer möchte die Zahlungstransaktion, begonnen mit der Konteneröffnung, Geldtransfer auf das Konto und die Zahlungen selbst durchgängig über das Internet erledigen. Medienbrüche wie z.B. die Übermittlung der Kreditkartennummer per Telefon oder die Versendung von Bankkonto-Informationen auf dem klassischen Postweg werden als negativ empfunden.

[2] siehe o.V. *Ohne Medienbruch einkaufen - vom Ordern bis zum Zahlen*, Computer Zeitung Nr. 28, 11.07.96

2.3 Anforderungen an die Realisierung

Auswahl der Zahlungs-Kommunikation

Bei der Zahlungs-Kommunikation wird zwischen online- und offline-Kommunikation (synchrone und asynchrone Kommunikation) unterschieden.

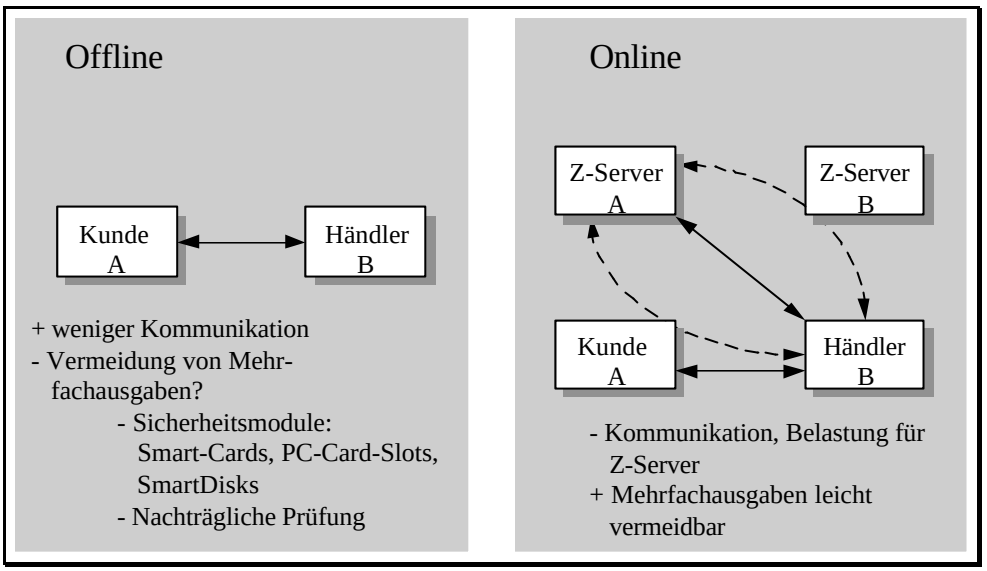

Abbildung 2.2: Kommunikation bei der Zahlung [Pfitzmann95]

Online-Betrieb. Während des Zahlungsprozesses sind alle Beteiligten verbunden und können miteinander kommunizieren. In der Regel wird die Hilfe eines entfernten Rechners benötigt, der die Kontrolle bzw. Steuerung des Dialogs übernimmt. Als Resultat ergibt sich eine hohe Belastung für den Zahlungsserver, es entstehen Verbindungskosten für die Leitung, jedoch ist die Prüfung des elektronischen Geldes sofort möglich. Mehrfachausgaben können verhindert werden (z.B. Zahlung mit kopierten Münzen). Die hohe Beanspruchung von Kommunikationsressourcen ist oft ein Grund für die Verwendung von Offline-Systemen [Wayner96, 75f].

Offline-Betrieb. Der Zahlungsprozeß findet ohne Teilnahme einer Bank/Clearingstelle direkt vom Kunden zum Verkäufer statt (siehe Abbildung 1.2). Wayner ist der Ansicht, daß es kein echtes Offline-Cash gibt. Diese Systeme sind in gewisser Hinsicht auch online, die Interaktion zur Bank verschiebt sich nur um einige Zeit [Wayner96, 76]. Vorteil des Offline-Betriebs ist die geringe Kommunikation, was eine Reduktion der Kommunikationskosten mit sich bringt. Nachteil ist die Frage der Mehrfachausgaben, die jedoch bei SmartCards z.B. mit Sicherheitsmodulen, PC-Card-Slots oder SmartDisks gelöst werden, welche die Authentisierung der Münzen bzw. Karten ermöglichen. Bei anderen Zahlungssystemen kann die Prüfung des Geldes bzw. die Berechtigung der Kontobelastung auch rückwirkend erfolgen.

Zusätzliche Hardware

Wird für ein Zahlungssystem zusätzliche Hardware benötigt, stellt dies eine Hemmschwelle dar. Bei allen SmartCards wird ein separater oder in der Tastatur integrierter Kartenleser benötigt. Das Bun-

desamt für Sicherheit in der Informationtechnik (BSI) publiziert regelmäßig zertifizierte Produkte im Bereich IT-Sicherheit, worunter sich auch eine große Anzahl zertifizierter Kartenleser befindet. Nachfolgend ein Auszug aus der BSI Publikation (Stand: Oktober 1996).

Siemens AG
Produkt: **KV-CKT (J31032-K0108-L012-A1)** **Produkt-Typ**: Chipkartenlesegerät **Status**: Zertifiziert unter BSI-ITSEC-0055-1993 am 24.11.1994 **Ergebnis**: **E2/niedrig, Funktionalität gemäß technischer Spezifikation der KBV vom 23.07.1993**
IBM Deutschland Entwicklung GmbH
Produkt: **Kartenleser IBM 5937-B04, ab Seriennummer S/N 00231** **Produkt-Typ**: Chipkartenlesegerät **Status**: Zertifiziert unter BSI-ITSEC-0066-1994 am 18.01.1995 **Ergebnis:** **E2/niedrig, Funktionalität gemäß technischer Spezifikation der KBV vom 22.11.1993**

Abbildung 2.3: Beispiele von zertifizierten Chipkartenlesern [BSI-Zertifikate96]

Portabilität

Eine weitere technische Anforderung an Zahlungssysteme ist die Portabilität [Weiler96]. Dies bedeutet, daß das System unabhängig von einem Rechner lauffähig ist, folglich also plattformunabhängig ist.

Ein weiteres Merkmal der Portabilität ist die Unabhängigkeit eines bestimmten Rechners, auf der die Zahlungs-Software läuft. Die meisten Zahlungssysteme erfüllen diese Anforderungen nicht, da die Zahlungs-Software benutzerbezogen installiert werden muß und die Host-Adresse des Internet-Rechners bei dem jeweiligen Zahlungssystem-Anbieter gespeichert wird.

Gewährung der Durchsatzgeschwindigkeit

Um die Kommunikationskosten nicht in die Höhe zu treiben, sollte eine definierte Durchsatzgeschwindigkeit von Zahlungstransaktionen gewährleistet sein. Die Durchsatzgeschwindigkeit ist abhängig von der Anzahl der Zahlungs-Server, die der Zahlungssystem-Anbieter installiert hat, und der weiten Verbreitung des Zahlungssystems (Anzahl der Nutzer).

Die Gewährung der Durchsatzgeschwindigkeit spielt bei Online-Zahlungssystemen eine große Rolle. Vernachlässigt werden kann diese Anforderung bei Offline-Zahlungssystemen.

Nutzung per ftp, E-Mail und/oder WWW

Die Realisierungsanforderungen bezüglich der Nutzung von Zahlungssystemen sind sehr individuell und hängen implizit mit der Auswahl der Zahlungskommunikation und der Durchgängigkeit der IT-Mittel zusammen. Steht der Komfort eines Zahlungssystems beim Benutzer an erster Stelle, wird er ein System das ausschließlich per WWW bedient wird, gegenüber einem E-Mail System mit Offline-Funktionalität vorziehen.

3 Betriebswirtschaftliche Anforderungen

In diesem Kapitel werden betriebswirtschaftliche (Abschnitt 21.), organisatorische (Abschnitt 2.2) und funktionale (Abschnit 2.3) Anforderungen untersucht. Im Anschluß daran wird besonders ausführlich wird auf die Anforderungen im Kosten/Nutzen-Verhältnis (Abschnitt 2.4) eingegangen. Da die Aufwendungen eine besondere Rolle für alle Beteiligten spielen, werden einerseits die Bestandteile der Transaktionskosten an einem Berechnungsbeispiel aufgezeigt. Weiterhin werden anhand konkreter Systeme Berechnungsbeispiele durchgeführt, welche die tatsächlichen Transaktions- und Initialkosten verdeutlichen.

3.1 Grundlegende betriebswirtschaftliche Anforderungen

Hohes Entwicklungspotential

Entwicklung des Systems. Das Entwicklungspotential ist abhängig von den Firmen, Universitäten und Institutionen, die das System entwickelt haben. Handelt es sich um namenhafte Entwickler, so ist die Systemakzeptanz größer. Mit Hilfe von Fachzeitschriften und Publikationen im Internet kann der Bekanntheitsgrad dieser Zahlungssysteme zusätzlich erweitert werden. Als Beispiel sei hier SET mit den Entwicklern VISA und MasterCard aufgeführt.

Nutzung des Systems. Ausschlaggebend ist, welche Teilnehmer das System aktiv nutzen; so hat sich z.B. das Entwicklungspotential des Systems Ecash durch den angekündigten Pilotversuch der Deutschen Bank enorm verbessert. Das hohe Entwicklungspotential äußert sich in der weiten Verbreitung und der Akzeptanz des Zahlungssystems und ist eine der wichtigsten betriebswirtschaftlichen Anforderungen.

Geographische Anwendbarkeit

Die zunehmende Internationalisierung wirtschaftlicher Aktivitäten zieht die Forderung der internationalen Anwendbarkeit von Zahlungssystemen nach sich. Bisher ist für den Retailkunden lediglich die Kreditkarte als internationales Zahlungssystem ökonomisch sinnvoll anwendbar [Himmelspach/Zimmermann96].

Auch in regionalen Märkten, wie z.B. der EMB, die Web-Applikationen von Unternehmen aus der Schweiz, Österreich, Deutschland und Liechtenstein zur Verfügung stellt, spielt eine grenzüberschreitende Anwendbarkeit von Zahlungssystemen eine wichtige Rolle. Die geographische Anwendbarkeit ist somit ein Indikator für das hohe Entwicklungspotential.

Betriebswirtschaftliche Integration

Zahlungen sind Bestandteile der Abwicklungphase von Markttransaktionen, wie sie bereits in den Phasen der Wertschöpfungskette elektronischer Märkte erläutert wurden. Sie werden aus der vorangegangenen Vereinbarungsphase initiert und dienen somit der Abwicklung der jeweiligen Geschäftstransaktion.

Die Integration von Finanzdienstleistern in die Abwicklungsphase einer Transaktion innerhalb der Wertschöpfungskette beinhaltet bisher nicht ausgeschöpfte Potentiale von EM.

Zeitpunkt der Zahlung

Anhand des Kriteriums „Zeitpunkt der Zahlung“ können laut [Janson/Waidner96a] drei unterschiedliche Arten von Zahlungssystemen definiert werden. Der Zahlungszeitpunkt bezieht sich auf die Zeit, die zwischen dem Auslösen einer Zahlungstransaktion und der tatsächlichen Belastung auf dem Kundenkonto liegt.

Pre-paid System. Bei Pre-paid Systemen muß der Kunde bevor er eine Zahlung ausführt, ein Guthaben auf seine Karte einbezahlen, d.h. es entsteht eine gewisse Zeitspanne zwischen dem Einzahlen des Geldes und der Ausgabe (z.B. Telefonkarten, Electronic Cash). Das Geld wird zuerst von einem zinsgünstigen Bankkonto abgebucht und in eine zahlungsgeeignete Form gebracht. Das so vorbereitete Geld wird später zum Konsum verwendet.

Pay-now System. Mit dem Auslösen einer Zahlung wird sofort die Belastung auf dem Bankkonto des Kunden ausgeführt, d.h. es ist keine „Zwischenlagerung“ des Geldes nötig. Ein Beispiel für ein pay-now System ist EC-Direct als POS/EFT System. Konsum und Abbuchung vom Konto erfolgen (im Prinzip) zum selben Zeitpunkt.

Pay-later System. Die Zahlung ist genau gesehen ein Zahlungsanweisung, da erst nach einem bestimmten Zeitintervall, oder nach Kumulierung von Beträgen die Abbuchung auf dem Bankkonto des Kunden erfolgt. Hier erfolgt der Konsum vor der Abbuchung vom Konto, es entsteht ein Kredit, der durch den Verkäufer oder den Mittler finanziert wird. Kreditkarten- und Schecksysteme sind typische pay-later Systeme.

Für pre-paid Systeme wird in vorliegender Arbeit auch der Ausdruck „bargeld-ähnlich“ verwendet. Pay-now und pay-later Systeme sind „kontenbasierende“ Systeme.

Die Anforderungen der Markteilnehmer in Bezug auf den Zeitpunkt der Zahlung sind unterschiedlich. So werden beispielsweise pay-later Systeme von Kunden bevorzugt, da das Geld aufgrund des Darlehenscharakters erst im Nachhinein vom Bankkonto abgebucht wird. Anbieter präferieren pre-paid Systeme, da man sich keine Gedanken über die Kreditwürdigkeit machen muss.

3.2 Organisatorische Anforderungen

Systemoffenheit

Das System soll betriebswirtschaftlich gesehen offen sein, indem neue Markteilnehmer einfach integriert werden können. Auch in technischer Hinsicht soll es sich um ein offenes System handeln und sich durch Plattform- und Browserunabhängigkeit auszeichnen.

Datenschutz/Safety

Da elektronische Münzen in Form von Dateien im Rechner gespeichert sind, bietet es sich an, Kopien von diesen Dateien zu erstellen, falls sie „versehentlich“ gelöscht werden. Durch die Speicherung des Geldes auf einer SmartCard, die spezielle Mechanismen auf dem Chip integriert hat, wird ein besonders hoher Schutz geboten.

Datenschutz/Security

Kreditkarteninformationen. Die Kreditkartennummern sollten bei Dienstleistungsmittlern und Finanzintermediären keinesfalls unverschlüsselt in einer Datenbank abgespeichert werden. Eine Sicherheitsvorkehrung bei First Virtual ist die Speicherung auf einem separaten Rechner, der nicht am Internet angeschlossen ist.

Kryptographieschlüssel. Hier gilt wie bei elektronischen Münzen: die sicherste Speicherung erfolgt auf einer SmartCard. Zukünftig werden (öffentliche) Kryptographieschlüssel bei Zertifizierungsstellen (Trusted Third Parties) gespeichert werden, um zu gewährleisten, dass vertrauenswürdige und korrekte öffentliche Schlüssel im Umlauf sind. Das Vertrauen in diese Stellen spielt dabei eine entscheidende Rolle.

Transaktionsdaten. Aus Kundensicht ist die bevorzugte Lösung, daß Transaktionsdaten nur auf dem eigenen Rechner vorhanden sind. Eine Speicherung bei Händlern oder gar bei Finanzinstituten zieht die bereits erwähnte Gefahr des „gläsernen Menschen“ nach sich, da mit elektronisch gespeicherten Daten einfach und schnell ein Benutzerprofil erstellt werden kann. Andererseits bietet die Speicherung der Transaktionsdaten den Teilnehmern einen gewissen Schutz im Hinblick auf die Nichteinhaltung von Zahlungen und Produktlieferungen. Bei der Aufbewahrung der Transaktionsdaten spielt der Aufbewahrungsort, die jeweiligen Sicherheitseinrichtungen und auch die Zugriffsrechte innerhalb des Systems eine bedeutende Rolle.

Vermeidung von Geldverlust

Geldverlust durch Systemfehler. Bei allen Zahlungssystemen sollte gewährleistet sein, daß die Transaktion vollständig ausgeführt oder wieder zurückgesetzt wird, falls eine Störung eintritt. Damit soll ein konsistenter Zustand bei Teilnehmern bestehen bleiben. Über solche Recovery-Funktionen verfügen heutige Zahlungssysteme jedoch nicht. Falls Systemfehler lokal auftreten, sollte bei Electronic Cash eine Möglichkeit bestehen, Münzen zu rekonstruieren.

Geldverlust durch Benutzerfehler. Das System sollte Sicherheitsfunktionen besitzen, damit Benutzer z.B. nicht versehentlich Münzdateien löschen kann. Bei SmartCards ist der Kartenverlust nicht immer mit Geldverlust gleichzusetzen, da der Restbetrag ermittelt werden kann und bei Verfall der Karte rückerstattet wird. Jedoch kann ein Finder (falls die Karte nicht über ein Paßwort geschützt ist) über das Geld verfügen.

Eng in Verbindung mit dem Beurteilungskriterium Geldverlust steht die *Kulanz* des teilnehmenden Finanzinstituts. Haftet das Finanzinstitut bei Mißbrauch (z.B. haften Kreditkartenunternehmen ab bestimmten Beträgen) wird der Kunde entlastet und ein potentieller Geldverlust nicht stark gewichtet.

Minimierung von Abhängigkeiten

Abhängigkeit von Anbietern gegenüber Nachfragern. Der Austausch von Geldmitteln und Waren erfolgt bei allen Systemen asynchron. Üblicherweise wird zuerst bezahlt, anschliessend die Information bzw. das Gut zur Lieferung freigeschaltet oder die Versendung veranlaßt. Eine Abhängigkeit der Anbieter ist daher nicht vorhanden bzw. minimal.

Abhängigkeiten von Nachfragern gegenüber Anbietern. Hier verhält es sich genau umgekehrt. Das Verhältnis der Geschäftspartner wird von [Waidner96a] mit „master-slave relation between seller's server and buyer's browser" beschrieben. Das Zahlungssystem NetCash ist bisher das einzige, das die erläuterte Abhängigkeit durch ein spezielles Verfahren, in welchem Münzen mit gleicher Seriennummer ausgegeben werden, eliminiert [Medvinsky/Neuman93, 4] [Frotscher95].

Weitere Abhängigkeiten bestehen generell bei der Auswahl des Zahlungssystems, da es sich bisher um geschlossene Geschäftskreise handelt, d.h. der Kunde kann nur bei Anbietern einkaufen, die sein Zahlungssystem unterstützen und umgekehrt.

3.3 Funktionale Anforderungen

Der Funktionsumfang elektronischer Zahlungssysteme beschränkt sich oft auf das Ausführen von Zahlungen, Geld abheben und deponieren (bei Cash-Systemen) und die Erstellung eines Kontoauszugs. Nachfolgende funktionale Anforderungen resultieren in bereits erläuterten technischen und betriebswirtschaftlichen Anforderungen:

⇒ **Konvertibilität**

Um einem Konsumenten Flexibilität in höchstem Maße zu bieten, muß er in der Lage sein, sein Geld zwischen verschiedenen Zahlungssystemen zu transferieren und somit Cyberwährungen zu konvertieren. Er kann durch diese Funktion seine Einkaufsmöglichkeiten um ein Vielfaches erhöhen. Auch für die Anbieter liefert die Konvertierbarkeit von Zahlungssystemen Vorteile, da der erreichbare Kundenkreis vergrößert wird.

⇒ **Übertragbarkeit**

Die Flexibilität erhöht sich, indem Geld an beliebige Markteilnehmer übertragen werden kann, also auch eine Kunde-zu-Kunde Zahlung möglich ist. Bei vielen Systemen ist jedoch nur eine Zahlung vom Kunden zum Anbieter vorgesehen.

⇒ **Quittungen**

Wie bei einem klassischen Einkauf sollte der elektronische Produkterwerb quittiert werden. Dies ist einerseits für den Anbieter von Bedeutung, da der Umsatz eventuell der Umsatzsteuer unterliegt und auch zur Ermittlung des Unternehmens-Ergebnisses erfaßt werden muß. Auch für den Kunden spielen steuerliche und auch rechtliche Aspekte (wie z.B. Garantie) eine entscheidende Rolle.

Um die Glaubwürdigkeit von Quittungen zu erhöhen, sollten sie mit zertifizierten Schlüsseln unterzeichnet oder von TTP's erstellt werden.

⇒ **Rückerstattungen**

Zahlungssysteme sind fast ausschließlich so konzipiert, daß sie lediglich Zahlungsaufträge generieren bzw. eine Zahlung veranlassen können.

Auch beim elektronischen Einkauf kann es vorkommen, daß Produkte beschädigt werden oder beim Kunden nicht ankommen. Eventuell ist der Kunde mit dem Produkt nicht zufrieden, was bei vorausbezahlter Ware eine Rückerstattung erfordert.

⇒ **Mehrere Währungen**

Aufgrund der bereits erwähnten Globalisierung der Märkte sind mehrere Währungen notwendig. Bei Kreditkarten-Zahlungssystemen besteht die Möglichkeit in Landeswährung zu bezahlen. Auch bei elektronischen Schecks u.a. kontenbasierten Systemen sind mehrere Währungen möglich. Diese Anforderung betrifft hauptsächlich bargeld-ähnliche Zahlungssysteme.

⇒ **Eignung für Micropayments**

Da das Internet als Vertriebskanal von Informationen (z.B. einzelne Artikel) prädestiniert ist, ist eine der Anforderungen, daß das Zahlungssystem über kleine Geldeinheiten verfügt. Dies kann durch eine Stückelung der Münzen bei Ausgabe („Prägung") erfolgen. Die andere Anforderung ist, das das Zahlungssystem eine ökonomische Ausführung von Zahlungen im Micropayment-Bereich erledigen kann.

⇒ **Bezahlung von Warenkörben**

Zahlungssysteme sollten eine Funktion „Rechnungserstellung" beinhalten oder an eine solche geknüpft werden können, damit der Kunde sich in Ruhe einen Warenkorb zusammenstellen kann. Zahlungssysteme, die eine Zahlungstransaktion per Produkt auslösen sind nur beschränkt geeignet für einen „Einkaufsbummel" in elektronischen Märkten.

3.4 Anforderungen in Bezug auf das Kosten/Nutzen-Verhältnis

Günstige Zahlungssystem- und Transaktionskosten

Alle Marktteilnehmer fordern günstige Kosten für eine Zahlungsabwicklung im Internet. Nachfolgend sind Kosten, die in Verbindung mit Zahlungssystemen und dem tatsächlichen Einkauf stehen, erläutert und anhand verschiedener Berechnungsbeispiele belegt.

Registrierungskosten (Konto SetUp-Gebühr) sind beim Einrichten des Zahlungssystems einmalig zu leisten. Beispiele: Kundenregistrierung Ecash bei der Mark Twain Bank zwischen US$ 11 und US$ 25; Kundenregistrierung bei First Virtual (FV-Zahlungsserver) US$ 2.

Kontoführungsgebühren und *Kontoauszugsgebühren* fallen i.d.R. monatlich an, wenn ein Konto für den Benutzer eingerichtet wird bzw. der Inhaber die Buchungen abruft. So kostet bei First Virtual eine Übersicht der Zahlungseingänge den Anbieter US$1.

Transaktionskosten können sich aus Kundensicht aus folgenden Kosten zusammensetzen:

- Kosten des Mittlers/elektronischen Marktes für die Dienstleistung der Zahlungsvermittlung (z.B. könnte die EMB Plattform bei jeder Zahlungstransaktion SFr. 0,20 oder 1% des Transaktionsbetrages einbehalten)
- Kosten des Finanz-Intermediärs für die Erstellung von digitalen Münzen (z.B. bezahlen Kunden der Mark Twain Bank 4-5% Gebühren für das Erstellen und Übertragen der Münzen) oder das Clearing eines Schecks
- Kosten für die Kommunikationsverbindung (Beispielberechnung):

  a) Provider Eunet Deutschland GmbH
  Dauer einer Zahlungstransaktion mit dem System Ecash: 15 Sekunden[3]

Providergebühren[4] ca. DM 7,00/Stunde, anteilig:	DM 0,03
Telefongebühren	DM 0,12
Summe Kommunikationskosten Beispiel A	DM 0,15

  b) Provider Swiss Online
  Dauer einer Zahlungstransaktion mit dem System First Virtual: 2 Minuten[5]

Providergebühren ca. SFr. 6,00/Stunde, anteilig:	SFr. 0,20
Telefongebühren (Zone 10 bis 100 km)	SFr. 0,53
Summe Kommunikationskosten Beispiel B	SFr. 0,73

  Die Beispiele der Berechnung der Kommunikationskosten zeigen auf, daß auch unabhängig vom tatsächlichen Betrag, der an den Internet-Provider zu entrichten ist (z.B. Festbetrag bei einer Universität oder Firma) diese Art von Kosten anfallen und getragen werden müssen.

Nachfolgend werden Berechnungsbeispiele von Ecash, First Virtual und der schweizerischen Wertkarte CASH aus Kunden- und Anbietersicht aufgestellt. Die Rahmenbedingungen und Prämissen werden anfangs erläutert.

Berechnungsbeispiele aus Kundensicht

Rahmenbedingungen und Annahmen für die Berechnungsbeispiele von Zahlungstransaktionen aus Sicht der Kunden werden nachfolgend erläutert:

- Ein Kunde tätigt fünf Einkäufe im Monat zu jeweils US$ (SFr.) 10,00.

[3] Die Dauer von Zahlungstransaktionen mit Ecash wurde im Ecash-Pilotversuch getestet.
[4] vgl. Preisliste der EUnet Deutschland GmbH: http://www.Germany.EU.net/com/forms/pl1960201t.html
[5] Die Dauer der Zahlungstransaktion wird mit 2 Minuten angesetzt, da der Kauf offline mit E-Mails erfolgt. Der Konsument muß zweimal eine Internet-Verbindung aufbauen; zuerst bei der Bestellung und dem Produktbezug, anschließend nochmals für die Ausführung der Zahlungsbestätigung.

- Providerkosten entsprechen Swiss Online; der Provider-Anwählknoten befindet sich in der Zone 10 - 100 km (entspricht 10 Rappen/22,6 Sekunden an Telefongebühren).
- Die Nutzung des Zahlungssystems erfolgt in der Zeitspanne eines Jahres; alle einmaligen Kosten werden auf diesen Zeitraum verteilt.
- Für Ecash werden die Gebührenstrukturen der Mark Twain Bank verwendet (sie bietet drei unterschiedliche Gebührenprogramme, abhängig von der Nutzungsintensität für den Kunden an).
- Der Ecash-Kunde besitzt weniger als US$ 500,00 Guthaben auf seinem Konto bei der Mark Twain Bank[6].
- Einmal im Monat bezieht der First Virtual Kunde einen Kontoauszug.
- Die jährliche Gebühr der CASH-Wertkarte (SFr. 20,00) fließt nicht mit in die Berechnung ein, da die Karte ebenso eine gewöhnliche EC-Karte repräsentiert und somit auch bei herkömmlichen Zahlungen verwendet werden kann.

	Ecash Progr. 1	Ecash Progr. 3	First Virtual	CASH[7]
	US$	US$	US$	SFr.
Einmalige Registrierungskosten	11,00	25,00	2,00	(Karten-leser)
FIXE Kosten im Monat				
SetUp-Gebühren/Registrierungskosten anteilig	0,92	2,08	0,17	-
Kontoführungsgebühren	1,00	5,00	-	-
Kontoauszug	-	-	2,00	-
Summe fixe Kosten pro Monat	1,92	7,08	2,17	-
fixe Kosten in % vom Umsatz	**3,84 %**	**14,16 %**	**4,34 %**	**-**
VARIABLE Kosten im Monat				
- Kosten des Finanzintermediärs[8]	2,50	2,00	-	-
- Kosten der Kommunikationsverbindung[9]	1,00	1,00	5,50	(minimal)
Summe variable Kosten pro Monat	3,50	3,00	5,50	-
variable Kosten in % vom Umsatz	**7,00 %**	**6,00 %**	**11,00 %**	-
Summe fixe und variable Kosten pro Monat	5,42	10,08	7,67	-
Gesamtkosten in % vom Umsatz	**10,84 %**	**20,16 %**	**15,34 %**	**-**
Kosten pro Transaktion	1,08	2,02	1,53	-

Tabelle 1: Zahlungstransaktionskosten aus Kundensicht

[6] Ab US$ 500 kann im Ecash Kundenprogramm 1 die Kontoführungsgebühr eingespart werden; ab US$ 1.500 beim Gebührenprogramm 3.

[7] CASH ist die Wertkarte der Schweizer Banken und der Schweizer Post, die seit Juli 1996 in einem Pilot getestet wird. Es wird sie in Form von EC-Cash-Karten und POSTCARD-Karten (beide kontengebunden) und als unpersönliche CASH-Karte (z.B. für Touristen) ab Januar 1997 landesweit geben. Sie ist bis SFR 300,00 an Bankomaten aufladbar, eine TA kostet 0,7% des TA-Betrages plus 2 Rappen.

[8] Die Mark Twain Bank berechnet 4-5% für die Erstellung digitaler Münzen.

[9] siehe vorherige Beispielrechnung der Kommunikationskosten; als Umrechnungskurs für US-Dollar wird 1.5 pauschal verwendet (z.B. SFR 0,13 x 1,5 = US$ 0,20); die Dauer der CASH-Zahlungstransaktion wird mit 5 Sekunden angesetzt, da die Prüfungen der Karte im Kartenleser stattfindet und nur eine minimale Kommunikation nötig ist.

Die Beispielberechnung gibt Einblick in die Höhe der tatsächlichen Transaktions- und Zahlungssystemkosten. Wie ersichtlich ist, tragen die Kommunikationskosten, die sich aus anteiligen Providergebühren und Telekommunikationskosten zusammensetzen, einen nicht zu vernachlässigenden Anteil zu den gesamten Kosten bei. Mit Blick auf die Zukunft läßt sich jedoch sagen, daß sich diese Kosten aufgrund zunehmender Konkurrenz zwischen den Providern und Telekommunikationsunternehmen und aufgrund besserer Übertragungsraten verringern werden. Dies führt zur Verminderung der Transaktionsdauer und somit zur Senkung der Transaktionskosten.

Das von der Mark Twain Bank angebotene Gebührenprogramm 3 ist für sehr intensive Nutzung gedacht[10]. Die Bank bietet auch bei den Verkäuferkonten unterschiedliche Gebührenprogramme an. Die ausschlaggebenden (Teil-) Kosten bei den Berechnungsbeispielen Ecash sind die hohen Gebühren der Münzerstellung der Mark Twain Bank. Wie die Kostenstrukturen bei der Deutschen Bank für Ecash bei dem Pilotprojekt ab Ende diesen Jahres gestaltet sein werden, bleibt abzuwarten.

Der Unterschied der Zahlungstransaktionskosten typischer Internet-Zahlungssysteme und der Wertkarte, mit der bisher nicht über das Internet bezahlt werden kann, ist enorm. Dieser Unterschied zeigt die Potentiale der SmartCard-Systeme auf, die durch ihre Offline-Eigenschaft kaum bzw. zu vernachlässigende Kommunikationskosten aufweisen. Außerdem ist bei den SmartCards nicht mit hohen Gebühren auf Kundenseite zu rechnen, da die Anbieter dieser Karten mit den Float[11] spekulieren (Wertkarte als pre-paid System). Die Anschaffung eines Kartenlesers ist das größte Hemmnis für diese Zahlungsart. Die Kosten für den Kartenleser wurde bei obigem Beispiel nicht berücksichtigt, da ein konkreter Betrag nicht vorliegt.

Berechnungsbeispiele aus Anbietersicht

Rahmenbedingungen und Annahmen für die Berechnungsbeispiele von Zahlungstransaktionen aus Sicht der Anbieter sind:

- Der Anbieter hat Umsätze von 250 Einkäufen á US$ (SFr.) 10,00.
- Providerkosten werden nicht auf die Zahlungstransaktion umgelegt, da diese primär durch die Präsenz im Internet entstehen. Telekommunikationskosten finden ebenso keinen Ansatz, da diese primär beim Kunden anfallen.
- Die Nutzung des Zahlungssystems erfolgt über drei Jahre; alle einmaligen Kosten werden auf diesen Zeitraum verteilt.
- Für Ecash werden Gebührenstrukturen der Mark Twain Bank zugrunde gelegt.
- Einmal im Monat bezieht der First Virtual Anbieter einen Kontoauszug.

	Ecash Progr. 5	Ecash Progr. 8	First Virtual	CASH[12]

[10] Unter der Annahme, daß ein Benutzer 50 Einkäufe á US$ 10,00 tätigt, ergeben sich beispielsweise Zahlungstransaktionskosten in Höhe von 7,42% des Umsatzes.

[11] Float entspricht den Zinsen eines Betrages, der erst zu einem späteren Zeitpunkt ausgegeben wird.

[12] CASH ist die Wertkarte der Schweizer Banken und der Schweizer Post, die seit Juli 1996 in einem Pilot getestet wird. Es wird sie in Form von EC-Cash-Karten und POSTCARD-Karten (beide kontengebunden) und als unpersönliche CASH-Karte geben (z.B. für Touristen). Im Januar 1997 wird die landesweite Einführung stattfinden.

	US$	US$	US$	SFr.
SetUp-Gebühren/Registrierungskosten (einmalig)	150,00	500,00	10,00	ca. 150,00
FIXE Kosten im Monat				
SetUp-Gebühren/Registrierungskosten anteilig	4,17	13,89	0,28	4,17
Kontoführungsgebühren	25,00	5,00	-	-
Kontoauszug	-	-	1,00	-
Summe fixe Kosten pro Monat	29,17	18,89	1,28	4,17
fixe Kosten in % vom Umsatz	**1,17 %**	**0,76 %**	**0,05 %**	**0,16 %**
VARIABLE Kosten im Monat				
- Kosten des Finanzintermediärs	70,00	50,00	72,50	22,50
- Kosten der Kreditkartenunternehmen	-	-	50,00	-
Summe variable Kosten pro Monat	70,00	50,00	122,50	22,50
variable Kosten in % vom Umsatz	**2,80 %**	**2,00 %**	**4,90 %**	**0,90 %**
Summe fixe und variable Kosten pro Monat	99,17	68,89	123,78	26,67
Gesamtkosten in % vom Umsatz	**3,97 %**	**2,76 %**	**4,95 %**	**1,06 %**
Kosten pro Transaktion	0,40	0,28	0,50	0,11

Tabelle 2: Zahlungstransaktionskosten aus Anbietersicht

Wie die Beispielberechnung ergibt, sind auf Anbieterseite ebenso relativ hohe Zahlungstransaktions- und Zahlungssystemkosten vorhanden. Verglichen mit der herkömmlichen Kreditkarten-Zahlung, bei welcher dem Anbieter üblicherweise zwei bis drei Prozent des Zahlungsbetrages von Kreditkartenunternehmen einbehalten wird, sind diese Prozentsätze (ausgenommen ist die CASH-Karte) noch höher.

Obwohl der von Seiten der Telekurs subventionierte Kartenleser mit ca. SFr. 150,00 zu Buche schlägt, stellt sich das SmartCard-System CASH in diesen Berechnungsbeispielen als das günstigste Zahlungssystem heraus.

Eignung für bestimmte Einkäufe

Die Eignung der Zahlungssysteme für den Einkauf im Internet ist abhängig von dem Preis und der Beschaffenheit des Gutes.

Micropayments. Unter Micropayments werden in dieser Arbeit Beträge im einstelligen Schweizer Frankenbereich verstanden. Beträge unter SFr. 1,00 haben eine besondere Stellung. Für Micropayments eignen sich Cash-Modelle (elektronische Münzen) und SmartCard-Modelle, da sie i.d.R. günstig und schnell abrechnen. Die vorangegangenen Berechnungsbeispiele zeigen, daß die bisherigen Zahlungssysteme mit elektronischen Münzen in Verbindung mit Telekommunikationskosten für Micropayments unter SFr. 1,00 noch zu teuer sind; bzw. die günstigen SmartCard-Anwendungen über das Internet bisher noch nicht realisiert sind. Falls sich die Kosten im Telekommunikationsbe-

Sie ist bis SFR 300,00 an Bankomaten aufladbar, eine TA kostet den Kunden 0,7% des TA-Betrages plus 2 Rappen.

reich ändern (z.B. freier Internet-Zugang, kostenlose Kommunikations-Verbindungen innerhalb bestimmter Zonen, schnellere Übertragungsraten durch Breitbandtechnik) werden auch Beträge unter SFr. 1,00 sinnvoll ökonomisch abgerechnet werden können, da die Transaktionskosten auf ein Minimun sinken. Billing-Systeme rechnen Micropayments kostengünstig ab.

Kauf von materiellen Gütern. Typisch ist hier, daß die Lieferung des gekauften Gutes zu einem späteren Zeitpunkt als die Zahlung stattfindet. Für diese Art von Güterkauf eignen sich Kreditkarten-Zahlungssysteme sehr, da Kreditinstitute die Zahlungstransaktionen aufzeichnen und somit bei ausbleibender Lieferung des Anbieters für den Kunden eine Sicherheit besteht. Nach der Zahlung wird ein Logistikprozeß angestoßen; hier spielt die Integration in das IT-System des Anbieters (z.B. in das Produktionsplanung- und Steuerung-System) eine große Rolle.

Kauf von immateriellen Gütern. Falls der Preis im Verhältnis zu den Zahlungstransaktionskosten steht, eignet sich grundsätzlich jedes Zahlungssystem. Besonderheiten vom Kauf immaterieller Güter sind die prompte Abwicklung dieser Markttransaktionen. Nach der Bezahlung kann das Produkt unverzüglich ausgeliefert werden. Bei eventueller Beschädigung des Produktes ist eine Wiederholung der Lieferung mit minimalen Mehrkosten möglich, da keine Verpackungs- und Logistikkosten anfallen.

4 Spezielle Zahlungssystem-Anforderungen der Marktteilnehmer

In diesem Kapitel wird auf die individuellen bzw. besonders stark ausgeprägten Anforderungen von Kunde, Anbieter und Finanzdienstleister eingegangen.

4.1 Kunden

Anonymität

Für den Kunden ist im Vergleich zum Anbieter und Finanzintermediär *Anonymität* wichtig, da er seine Kaufgewohnheiten (Kauf von Produkten, Einkaufszeit, Einkaufshäufigkeit, usw.) i.d.R. nicht publik machen will. Die meisten Zahlungssysteme wie Kreditkartensysteme, EDI mit E-Mail und Schecksysteme sind nicht anonym, weder im Internet noch bei der klassischen Zahlungsweise. Nur Zahlungssysteme auf Basis elektronischer Münzen und SmartCards können die Anonymität des Kunden wahren. Handelt es sich um den Kauf eines materiellen Gutes ist Anonymität ebenso nicht gewährleistet, da allgemein eine Empfängeradresse für die Lieferung angegeben werden muß.

[Czurda96] sieht als weitere Anforderung von Zahlungssystemen eine Wahlmöglichkeit der optionalen Anonymität[13].

Benutzerfreundlichkeit

[13] Die Option der wahlweisen Anonymität wurde im System CAFE realisiert.

[Weiler96] hat im August 1995 eine Studie[14] über die Befragung mit erfahrenen Internet-Benutzern erstellt. Die *Benutzerfreundlichkeit* hat dabei mit 78,9% den zweiten Platz erreicht. Unter Benutzerfreundlichkeit wird die komfortable und einfache Bedienung des Systems durch den Benutzer verstanden.

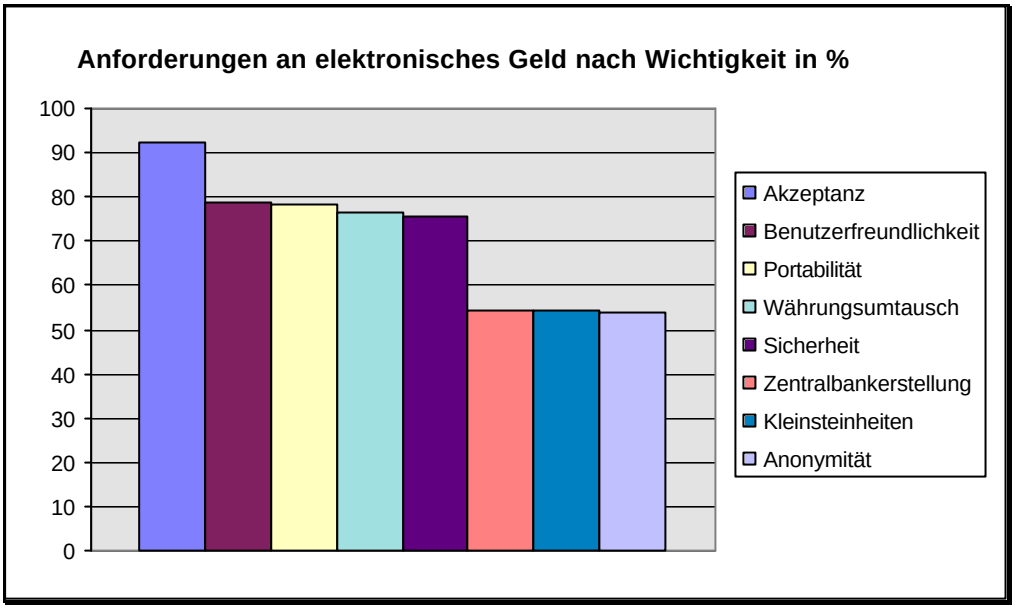

Abbildung 4.4: Bewertung der Zahlungssystem-Anforderungen nach [Weiler96]

Ebenso fällt unter den Begriff der Benutzerfreundlichkeit die Existenz von:

⇒ Help-Hotline zum Systemanbieter (für dringende Individual-Beratung),
⇒ Installationshilfen, Handbücher und ein generelles Online-Hilfe-System,
⇒ E-Mail-Diskussions-Liste und Newsgroups (um mit anderen Benutzern zu diskutieren) und
⇒ garantierte Updates.

[14] Bei den Befragten dieser Studie handelt es sich um Personen aus Großbritanien (24,5%), USA (39,7%) und 22 anderen Ländern bzw. Kontinenten, wobei der Hauptanteil aus Männern bestand (87,7%). Drei Viertel sind der Altersklasse 18 Jahre bis 35 Jahre zuzuordnen. URL: http://grah.ns.ic.ac.uk/results.

4.2 Anbieter

Sicherheitstechnische Risikominimierung

Server-Sicherheit. Auf dem Server des Anbieters müssen bestimmte Sicherheitsmaßnahmen getroffen werden. Gegen aktive Angriffe von außen muß z.B. der gesamte Server durch eine globale Zugangsdatei gesteuert werden, außerdem können einzelne Verzeichnisse speziell geschützt oder freigegeben werden. Firewalls bieten ebenso Schutz gegen Attacken, z.B. indem definierte Adressen gefiltert werden und Nutzer mit anderen Adressen nicht auf Daten zugreifen können. Desweiteren sind Sicherheitsmaßnahmen in den Räumlichkeiten des Server zu treffen; z.B. sollte der Raum stets gut verschlossen sein und nur wenige ausgewählte Personen sollten Zutritt haben. Durch Vergabe von Zugriffsrechten werden Server und Serverdaten durch unbefugte Änderung und Löschung geschützt.

Wirtschaftliche Risikominimierung

Ganz allgemein stellen Zahlungssysteme im Internet für den Anbieter heute noch ein wirtschaftliches Risiko dar. Die Nutzung einzelner Zahlungssysteme ist noch auf ein Minimun begrenzt und daher auch die zu erzielenden Umsätze. Da Zahlungssysteme im Internet geschlossene Systeme sind, schließt der Anbieter aufgrund der Auswahl eines bestimmten Zahlungssystems mögliche Kunden aus (die ein anderes Zahlungssystem benutzen).

Die Geschäftstätigkeit wird ebenso durch fehlende Rechtsvorschriften gehemmt[15]. Die Aufwendungen zur Teilnahme an Zahlungssystemen und die Zahlungstransaktionskosten sind noch verhältnismäßig hoch.

Integration in den Geschäftsprozeß

Für Anbieter und Geschäftskunden ist die *Einbindung* des Zahlungssystems in den gesamten Geschäftsablauf von vorrangigem Interesse. So sollen Transaktionsdaten beispielsweise in einem *standardisierten Format* (z.B. UN/Edifact) in das eigene DV-System eingehen, um im Sinne des Workflow-Gedanken folgende Vorteile aufgrund der überflüssig gewordenen Neuerfassung, zu erhalten:

⇒ Kostenersparnis
⇒ Zeitersparnis
⇒ Fehlerreduktion

4.3 Finanzintermedäre

Die Zurückhaltung der Finanzinstitute im Bereich Zahlungsabwicklung über das Internet ist mit der allgemein negativen Sicherheitsdarstellung in den Medien und dem Ergebnis einer von Unisys unter-

[15] siehe o.V. *Wer online Geld verdienen will, der sollte sich Verträge schriftlich bestätigen lassen.* Computerwoche vom 09.05.96 basierend auf dem Vortrag des Tobias H. Strömer, Internet Kongreß 96 in Karlsruhe

stützen Umfrage zu erklären: „Die meisten Institute fürchten, durch den Einsatz technisch unzureichender Systeme das Vertrauen ihrer Kundschaft einzubüßen“ [Gertz96, 45].

Sicherheitstechnische Risikominimierung

Hier gelten die gleichen Bestimmungen wie beim Anbieter.

Wirtschaftliche Risikominimierung

Die Investition in elektronische Zahlungssysteme im Internet ist wegen fehlender Standards noch ein finanzielles Risiko. Applikationen im Bereich des SET-Standards sind erst gegen Ende des Jahres 1996 zu erwarten und werden recht kostspielig sein[16]. Im Hinblick auf die aktuelle Teilnahme am Electronic Commerce lohnt sich die Implementation aus wirtschaftlicher Sicht heute kaum (selbst bei Ecash sind erst wenige Teilnehmer mit von der Partie[17]). Die Internet-Diskussion im Finanzbereich befassen sich neben den Sicherheitsbedenken, die nie ganz eleminiert werden können, mit der ungeklärten Rechtslage und der Änderung der Marktbedingungen [Anderer95].

Nicht-Duplizierbarkeit des Geldes

Eine Anforderung, die besonders von Finanzintermediären betont wird, ist, daß *keine Möglichkeit der Duplizierbarkeit* des elektronischen Geldes besteht. Daher begrüßen Finanzintermediäre Zahlungssysteme, deren Transaktionen bei Banken beginnen und enden (Beispiel: Kreditkarten-Zahlungen). Damit elektronisches Geld nicht dupliziert werden kann, sind bestimmte Sicherheitsmechanismen in das Zahlungssystem zu integrieren, wie z.B. Authentisierung von Teilnehmern bzw. Münzen und Verschlüsselung der elektronischen Münzen bzw. des elektronischen Geldversprechens.

Gelderstellung und Kontrolle durch die Zentralbank oder Regierung

Aufgrund der Existenz der Zahlungssysteme im Internet machen sich Ängste breit, daß das elektronische Geld an den Banken „vorbeiläuft“, und die Deutsche Bundesbank mit ihrer Zinspolitik an Wirkung einbüßen wird [Jünemann/Schütte/Wolf-Doettinchem95]. Möglichkeit zur Geldwäsche darf bei elektonischen Zahlungssystemen nicht bestehen.

Durch die Gelderstellung und Kontrolle (sowohl bei der Auszahlung als auch bei der Einzahlung/Überprüfung) durch eine höhere Instanz wie die Zentralbank oder die Regierung könnten die erwähnten Probleme einfacher überwacht werden. Dies entspricht jedoch nicht dem offenen, dezentralisierten Internet-Charakter und wird sich deshalb vermutlich nicht durchsetzen.

[16] Beispielsweise kosten die Lizenzen der RSA Lösung „SET Toolkit Suite“ $25.000 für den Kartenhalter, $50.000 für den Anbieter und $75.000 für die akquirierende Bank.

[17] siehe o.V., *Electronic Cash im Internet kommt langsam in Fahrt,* online aktuell, Nr. 13, 27. Juni 1996, S. 14-16. Die Bilanz der Mark Twain Bank, die seit Oktober 1995 mit Ecash Geschäfte abwickelt, ist ernüchternd. Nur fünfzig Anbieter und eintausend Kunden aus insgesamt dreißig Ländern beteiligen sich daran. Wobei sich die Finanzintermediär-Kosten für Ecash (Support, Set-Up, Lizenz, Hardware, Entwicklungen, Management, Werbung, u.a.) laut Auskunft von Bram Lebo, Digicash Amsterdam, im ersten Jahr auf zirca eine Million US Dollar beläuft.

5 Zusammenfassung der Anforderungen und Lösungsansätze

Die erläuterten Anforderungen aus unterschiedlichen Sichten werden nachstehend nochmals zusammengefaßt. Wie diese Anforderungen gelöst werden, bzw. welche neuen Anforderungen sie nach sich ziehen, wird in der Tabelle ebenso skizziert.

Anforderung	wird gelöst bzw. beeinflußt durch
Verfügbarkeit und Zuverlässigkeit	Zuverlässigkeit und Fehlertoleranz von Netzwerk, SW und HW
Vertraulichkeit	(asymmetrische) Verschlüsselung
Integrität	digitale Signaturen
Authentisierung	Paßwort, digitale Signaturen, Zertifikate
Autorisierung/Zugriffskontrolle	Paßwort, digitale Signaturen, Zertifikate
Non-Repudiation	Zertifikate
Vermeidung von Attacken	sichere Systemkonfiguration, -verwaltung und Software, Firewalls, Verschlüsselung, Zugangsrestriktionen
technische Integrationsfähigkeit	definierte, offengelegte Schnittstellen
Anwendungs-Integration	definierte Formate, Geschäftprozeß-Optimierung
Durchgängigkeit der IT-Mittel	Add-On's, die die Funktionalitäten abdecken, die das eigene System noch nicht beherrscht
Zahlungssystem-Kommunikation	(online - offline)
zusätzliche Hardware	(bei Chipkarten)
Portabilität	plattformunabhängige Entwicklung (JAVA)
Durchsatzgeschwindigkeit	mehrere Zahlungs-Server
hohes Entwicklungspotential	abhängig von Entwicklern und Nutzern
geographische Anwendbarkeit	mehrere Währungen, Kryptographie-Beschränkungen
betriebswirtschaftliche Integration	Re-Design von Internet-Geschäftsprozessen
Systemoffenheit	Plattform- und Browser-Unabhängigkeit
Datenschutz	Sicherheitseinrichtungen, Zugriffsrechte
Vermeidung von Geldverlust	Systemsicherheit
Minimierung von Abhängigkeiten	zertifizierte Quittungen als Nachweis von Geschäftstransaktionen
Konvertibilität	Funktionalität eines intelligenten Agenten
Übertragbarkeit	Geldannahme und Geldausgabe muß möglich sein
Quittungen	Zertifikate
Rückerstattungen	Geldannahme und Geldausgabe muß möglich sein
Eignung für Micropayments	kleine Geldeinheiten, geringe Transaktionskosten
Bezahlung von Warenkörben	integrierte Rechnungserstellung
günstige Zahlungssystem- und Transaktionskosten	Konkurrenz unter Zahlungssystem-Anbietern und Telekommunikations-Anbietern
Eignung für bestimmte Einkäufe	(systemabhängig)
Anonymität	asymmetrische Verschlüsselung
Benutzerfreundlichkeit	einfache Bedienung, komfortabel
Sicherheitstechnische Risikominimierung	sichere Systemkonfiguration, Systemverwaltung, Firewalls, Verschlüsselung, Zugangsrestriktionen
Wirtschaftliche Risikominimierung	Konkurrenz unter Zahlungssystem-Anbietern und Telekommunikations-Anbietern
Nicht-Duplizierbarkeit des Geldes	Verschlüsselung

Tabelle 3: Zusammenfassung der Anforderungen an elektronische Zahlungssysteme

6 Literaturverzeichnis

Im vorliegenden Bericht werden auch Literaturquellen verwendet, die lediglich elektronisch publiziert worden sind. Die angegebenen URLs sind eventuell nicht mehr verfügbar, oder der Dokumenteninhalt kann sich durch Überarbeitung verändert haben. Die URL's, die in vorliegender Arbeit vollständig als Fußnoten angemerkt sind, sind nicht nochmals im Literaturverzeichnis erwähnt.

[Anderer95] Anderer, Boris. *Sicherheit im Internet-Banking*. Geldinstitute, Nr. 11-12, 1995, S. 22-29.

[Bhimani96] Bhimani, Anish. *Securing the Commercial Internet.* Communications of the ACM, June 1996, S. 29 - 35.

[BSI-Zertifikate96] BSI-Zertifikate. *Sicherheit von IT-Produkten und -Systemen*. Bundesamt für Sicherheit in der Informationstechnik, Stand: Januar 1996.

[Czurda96] Czurda, Henrik. *Run auf Digital-Money und Cyberbucks.* Schweizer Bank, Nr. 6, 1996, S. 48 - 51.

[Frotscher95] Frotscher, Thilo. *Bezahlen im WWW*. Seminar im WS 1995/96, URL: http://www.informatik.th-darmstadt.de/VS/Lehre/WS95-96/Proseminar/frotschi

[Gertz96] Gertz, Winfried. *Banker betrachten Multimedia noch mit gemischten Gefühlen*. Computerwoche, Nr. 12 vom 22.03.1996, S. 45-46.

[Himmelspach/ Zimmermann96]. Himmelspach, Andrea und Hans-Dieter Zimmermann. *Elektronische Zahlungssysteme als kritischer Erfolgsfaktor des Electronic Commerce in offenen Telematikinfrastrukturen*. Informatik, Nr. 6, 1996 (in Vorbereitung)

[Janson/Waidner96a] Janson, Phil, und Michael Waidner. *Electronic Payment Systems*. SEMPER Activity Paper, 30.01.96, URL: http://www.zurich. ibm.com:80/Technology/Security/extern/ semper/index.html

[Jünemann/Schütte/Wolf-Doettinchem95] Jünemann, Bernhard, Schütte, Christian, und Lorenz Wolf-Doettinchem. *Electronic Cash - Vollkommen umgekrempelt*. WirtschaftsWoche, Nr. 31, 27.07.1995, S. 12-16.

[Medvinsky/Neuman93] Medvinsky, Gennady, und Clifford Neuman. *NetCash: A design for practical electronic currency on the Internet.* First ACM Conference on Computer and Communications Security (Paper), November 1993, S. 1-5, URL: http://nii.isi.edu/info/netcheque/documentation.html

[Meli96] Meli, Hans. *Sicherheitsarchitektur für eine Electronic Mall*. In: [Schmid95a].

[Muftic92] Muftic, Sead. *Sicherheitsmechanismen für Rechnernetze*. München, Wien: Carl Hanser, 1992.

[Pfitzmann95] Pfitzmann, Birgit. *Zahlungssysteme im Internet.* Folien zum Vortrag der DFN-Betriebstagung, Berlin, 11.10.1995, URL: http://www.informatik.uni-hildesheim.de/~sirene/lit/sirene.html

[Schonhardt95] Schonhardt, Ulrich. *Sicherheit im WWW*. Seminar, 19.06.95, URL: http://www.fh-karlsruhe.de/%7Escu10011/ wwwsecur.htm

[Waidner96a] Waidner, Michael. *Development of a Secure Electronic Marketplace for Europe*. SEMPER Activity Paper, 19.02.96, URL: http://www.zurich.ibm.com:80/Technology/Security/extern/ semper/ info/index.html

[Wayner96] Wayner, Peter. *Digital Cash: Commerce on the Net.* London: Academic Press Limited, 1996.

[Weiler96] Weiler, R. M. *Money, transactions, and trade in the Internet.* Imperial College, London, England, 1995. URL: http://graph.ms.ic.ac.uk/results. Zitiert in: Panurach, Patiwat. *Money in Electronic Commerce*. Communications of ACM, June 1996, S. 45-50.